ON SOME NON-NOETHERIAN DOMAINS

by

DİLEK BUYRUK

THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

OF

THE ABANT İZZET BAYSAL UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE

OF

MASTER OF SCIENCE

IN

THE DEPARTMENT OF MATHEMATICS

Bolu, Turkey

JULY 2005

Approval of the Graduate School of Natural and Applied Sciences.

Prof. Dr. Davut Köşker
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Oğuz Yılmaz
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality as a thesis for the degree of Master of Science.

Associate Prof. Dilek Pusat Yılmaz
Supervisor

Examining Committee Members

Prof. Cemal Koç

Associate Prof. Dilek Pusat Yılmaz

Assistant Prof. Cesim Çelik

ABSTRACT

ON SOME NON-NOETHERIAN DOMAINS

Buyruk, Dilek

Master, Department of Mathematics

Supervisor: Associate Prof. Dilek Pusat Yılmaz

JULY 2005, 84 pages

Let R be a commutative ring and M be an R-module. We say that M satisfies the radical formula (s.t.r.f.) if for every submodule N of M, radical of N in M is equal to the envelope of N in M. Since the Noetherian rings which s.t.r.f. are well-known, see [9],[13],[17],[19],[20], we are interested in non-Noetherian rings which s.t.r.f. For this reason we studied characteristics and structure of a valuation ring to understand the structure of a Prüfer domain. In chapter I, basic definitions and fundamental facts related to the concept of valuation rings and Prüfer domains are presented.

In Chapter II, we solved some selected exercises in [7] about valuation rings and Prüfer domains.

In Chapter III, we gave necessary definitions and characterizations of prime submodules.

Finally, the definitions and fundamental results about radical formula are given in chapter IV. In 4.2, which is our original work, we proved that if R is a Prüfer domain, then the R module $R \oplus R$ s.t.r.f.

Keywords: Prüfer domain, valuation ring, radical formula.

ÖZ

BAZI NOETHER OLMAYAN BÖLGELER

Buyruk,Dilek

Master Tezi, Matematik Bölümü

Tez Yöneticisi: Doç. Dr. Dilek Pusat Yılmaz

TEMMUZ 2005, 84 sayfa

R birimli, değişmeli bir halka ve M bir R-modül olsun. M'nin her N alt modülü için, N'nin M'deki radikali, zarfının üzettiği alt modüle eşit ise M radikal formülünü sağlar denir. Radikal Formülünü sağlayan Noether halkalar iyi bilindiği için, hangi durumlarda Noether olmayan halkaların radikal formülünü sağladığı araştırıldı. Bu nedenle Prüfer bölgelerinin yapısının anlaşılabilmesi için öncelikle valuation halkalarının yapısı ve özellikleri incelendi. Birinci bölümde, Prüfer bölgeleri ve valuation halkalarla ilgili temel tanım ve kavramlar anlatıldı.

İkinci bölümde, Prüfer bölgeleri ve valuation halkalarla ilgili [7]'den seçilmiş problemler çözüldü.

Üçüncü bölümde, asal alt modülün tanımı ve yapısı anlatıldı.

Son bölümde ise radikal formülüyle ilgili tanımlar ve bazı sonuçlar verildi. Orjinal çalışmamız olan Bölüm 4.2 de, R Prüfer bölgesi olmak üzere, R- modül olan $R \oplus R$ 'nin radikal formülü sağladığı gösterildi.

Anahtar Kelimeler: Prüfer bölgeleri, valuation halkalar, radikal formülü.

ACKNOWLEDGEMENTS

I would like to acknowledge my indebtedness to my supervisor Associate Prof. Dilek Pusat Yılmaz who has guided, encouraged and believed in me throughout this thesis. I strongly believe that I will feel her influence over the entire course of my mathematical life. I am grateful to her for a critical reading of my solutions and valuable suggestions in correcting my errors. I also like to thank to the other members of my Committee, Prof. Cemal Koç and Assistant Prof. Cesim Çelik for their assistance.

It is also a pleasure to acknowledge a special dept of my gratitude to Prof. Mehpare Bilhan for teaching me significant techniques to solve problems in valuation rings.

Finally, I would like to thank to my family for their unvanishing support and encouragement.

To My Family

TABLE OF CONTENTS

CHAPTER 1

PRELIMINARIES

1.1 Introduction

In this thesis, all rings are commutative. Throughout this chapter, all rings contain more than one element but need not contain 1.

Definition 1.1 *Let R be a ring and $x \in R$. If x is not a zero divisor, then x is called a* <u>*regular*</u> *element of R.*

Example: If $1 \in R$, then R contains a regular element.

Definition 1.2 *Let A be an ideal of a ring R. A is said to be a* <u>*regular*</u> *ideal if A contains a regular element of R.*

Remark 1.3 *$< x >$ is a regular ideal if and only if x is a regular element of R.*

Proof. Suppose x is not a regular element that is there exists a nonzero $y \in R$ such that $xy = 0$. Take $\alpha \in < x >$, then $\alpha = rx$ for some $r \in R$ and since R is commutative, $y\alpha = y(rx) = r(yx) = 0$. Hence, $< x >$ has no regular elements, so $< x >$ is not a regular ideal.

Conversely, let x be regular, then $x \in < x >$ implies $< x >$ is regular. $\square$

Definition 1.4 *Let R be a ring with identity. R is said to be* <u>*quasi-local*</u> *if R has a unique maximal ideal; R is called* <u>*semi-quasi-local*</u> *if R has only finitely many maximal ideals.*

A <u>*local ring*</u> *is a quasi-local Noetherian ring; a* <u>*semi-local ring*</u> *is a Noetherian semi-quasi-local ring.*

Definition 1.5 *A ring S containing R as a subring is said to be a* <u>*unitary ring extension*</u> *of R, if the identity element of R is also the identity element of S.*

Definition 1.6 *Let I be an ideal of a ring R. Then the ideal $\sqrt{I} = \{r \in R : r^n \in I$ for some positive integer $n\}$ is called the* <u>*radical of I*</u>*.*

Definition 1.7 *Let Q be a ideal of a ring R. Q is said to be* <u>*primary*</u> *whenever $Q \neq R$ and $ab \in Q$ for some $a, b \in R$ implies $a \in Q$ or $b \in \sqrt{Q}$. Also, if $\sqrt{Q} = \mathcal{P}$ for some prime ideal $\mathcal{P}$ of R, then Q is called* <u>*$\mathcal{P}$-primary*</u>*.*

Definition 1.8 *Let A be an ideal of a ring R such that A can be expressed as a finite intersection of primary ideals, $A = \bigcap_{i=1}^{n} Q_i$, then this representation of A is said to be a* <u>*shortest representation*</u> *of A if it is irredundant and if the ideals Q_i belong to distinct prime ideals.*

Definition 1.9 *Let R and S be rings and $f : R \to S$ be a ring homomorphism.*

(i) Whenever J is an ideal of S, then $f^{-1}(J) := \{r \in R | f(r) \in J\}$ is an ideal of R, called the <u>*contraction of J*</u> *to R and denoted by J^c.*

(ii) For each ideal I of R, the ideal $f(I)S$ of S generated by $f(I)$ is called the <u>*extension of I*</u> *to S and denoted by I^e.*

Remark 1.10 *[7, Theorem 4.10] Let A be an ideal of a ring R with identity, let $\{\mathcal{M}_\lambda\}_{\lambda \in \Lambda}$ be the set of maximal ideals of R, and for each $\lambda \in \Lambda$, let $A_\lambda = A^{e_\lambda c_\lambda}$, where e_λ and c_λ denote extension and contraction with respect to the ring $R_{\mathcal{M}_\lambda}$. Let Σ be the set of elements σ of Λ such that $A \subseteq \mathcal{M}_\sigma$.*

(i) $A = \bigcap\limits_{\lambda \in \Lambda} A_\lambda$.

(ii) $A = \bigcap\limits_{\sigma \in \Sigma} A_\sigma$.

And if R is also an integral domain,

(iii) $A = \bigcap\limits_{\lambda \in \Lambda} AR_{\mathcal{M}_\lambda} = \bigcap\limits_{\lambda \in \Lambda} A^{e_\lambda}$.

Proof.

(i) Clearly, $A \subseteq A_\lambda$ for all $\lambda \in \Lambda$. Then $A \subseteq \bigcap_{\lambda\in\Lambda} A_\lambda$ is clear. Other side of the inclusion follows from part (ii) i.e if part (ii) holds, then $\bigcap_{\lambda\in\Lambda} A_\lambda \subseteq \bigcap_{\sigma\in\Sigma} A_\sigma = A$.

(ii) One side of the inclusion is clear. To show that $\bigcap_{\sigma\in\Sigma} A_\sigma \subseteq A$, take an element $x \in \bigcap_{\sigma\in\Sigma} A_\sigma$. Since $x \in A_\sigma$, there exists $y_\sigma \in R \setminus \mathcal{M}_\sigma$ such that $xy_\sigma \in A$ for all $\sigma \in \Sigma$. Then $< y_\sigma > +A \subseteq (A :< x >)$ for all $\sigma \in \Sigma$, so $(A :< x >)$ is not contained in any maximal ideal of R. Hence $(A :< x >)$ is not a proper ideal of R. And since R contains identity, $(A :< x >) = R$. Then $x \in A$ and $\bigcap_{\sigma\in\Sigma} A_\sigma \subseteq A$.

(iii) Again we have to show $\bigcap_{\lambda\in\Lambda} AR_{\mathcal{M}_\lambda} \subseteq A$. Take $x \in \bigcap_{\lambda\in\Lambda} AR_{\mathcal{M}_\lambda}$. Consider the ideal $I = (A :< x >)$ of R, $I \nsubseteq \mathcal{M}_\lambda$ for all $\lambda \in \Lambda$. Then $I = R$ and $x \in A$ as we wished to show. $\square$

Remark 1.11 *An ideal Q of a ring R is $\mathcal{P}$-primary if and only if QR_S is $\mathcal{P}R_S$-primary in R_S where S is a multiplicatively closed subset of R and $Q \cap S = \emptyset$.*

Moreover, let Q be a primary ideal of a ring R , then $Q = QR_S \cap R$ when $Q \cap S = \emptyset$.

Proof. Let Q be $\mathcal{P}$-primary with $Q \cap S = \emptyset$. Take $(a/r)(b/s) \in QR_s$ where $a, b \in R$ and $r, s \in S$. Then $k(ab) \in Q$ for some $k \in S$. Since $k^n \notin Q$ for all $n \in \mathbb{Z}^+$, that is $ab \in Q$. Since Q is $\mathcal{P}$-primary, $a \in \mathcal{P}$ or $b \in Q$. Thus $a/r \in \mathcal{P}R_S$ or $b/s \in QR_S$. Conversely, let QR_S be $\mathcal{P}R_S$-primary, take $ab \in Q$ where $a, b \in R$, clearly, $(a/1)(b/1) \in QR_s$ and $a/1 \in \mathcal{P}R_s$ or $b/1 \in QR_S$, then there exist $k_1, k_2 \in S$ such that $ak_1 \in \mathcal{P}$ or $bk_2 \in Q$. Since $k_i^n \notin Q$ for all $n \in \mathbb{Z}^+$, $k_i \notin \mathcal{P}$ for $i = 1, 2$, that is, $a \in \mathcal{P}$ or $b \in Q$.

Also, we have $Q \subseteq QR_S \cap R$. Take $x/1 \in QR_S \cap R$, then there exists $s \in S$, such that $sx \in Q$. Since S is multiplicatively closed, $s^n \notin Q$ for all $n \in \mathbb{Z}^+$.

Hence $x \in Q$, as required. $\square$

1.2 Fractional Ideals

Definition 1.12 *Let R be a ring containing a regular element and let T be the total quotient ring of R. A subset S of T is said to be a fractional ideal of R if*

(i) S is an R-module and

(ii) $rS \subseteq R$ for some regular element $r \in R$.

Each ideal of R is a fractional ideal of R. The ordinary ideals of R will be referred to integral ideals.

If $\{s_1, ..., s_n\}$ is a finite subset of T, then the R-submodule of T generated by $\{s_1, ..., s_n\}$ is a fractional ideal of R. But if S is an arbitrary subset of T, then $< S >$, the R-submodule of T generated by S, need not be a fractional ideal of R, that is T is a fractional ideal of R only if $T = R$.

In fact, $< S >$ is a fractional ideal of R if and only if S is contained in a fractional ideal of R. S is called a generating set. A fractional ideal F is finitely generated if F admits a finite set of generators. F is principal if $F =< x >$ for some $x \in T$. We say that F is regular if F contains a regular element of T.

$< x >$ is a regular fractional ideal if and only if x is regular in T.

Notations:

$F(R)$: The set of nonzero fractional ideals of R.

$F^*(R)$: The subset of $F(R)$, consisting of finitely generated fractional ideals in $F(R)$.

Definition 1.13 *If $F_1, F_2 \in F(R)$, then addition and multiplication of F_1 and F_2 are defined as follows:*

$$F_1 + F_2 = \{x + y | x \in F_1, y \in F_2\}$$

$$F_1F_2 = \{\sum_{i=1}^{n} x_iy_i | x_i \in F_1, y_i \in F_2\}.$$

Also we define,

$$[F_1 : F_2]_T = \{x \in T | xF_2 \subseteq F_1\}.$$

If F_1, F_2 are integral ideals, then $(F_1 : F_2)$ is defined as $\{x \in R | xF_2 \subseteq F_1\}$. Hence $(F_1 : F_2)$ may be a proper subset of $[F_1 : F_2]_T$. In fact,

$$(F_1 : F_2) = [F_1 : F_2]_T \cap R.$$

Theorem 1.14 *[7, Theorem 3.1] Let R be a ring containing a regular element and let T be the total quotient ring of R.*

(i) $F(R)$ is closed under addition, intersection and multiplication. If F_1, $F_2 \in F(R)$ and if F_2 is regular, then $[F_1 : F_2]_T \in F(R)$.

(ii) If F_1, $F_2 \in F(R)$ and if S_i is a set of generators for F_i ($i = 1, 2$), then $S_1 \cup S_2$ is a set of generators for $F_1 + F_2$ and $\{st | s \in S_1, t \in S_2\}$ is a set of generators for F_1F_2.

Consequently, $F^*(R)$ is closed under addition and multiplication.

(iii) $F(R)$ is an abelian semigroup under multiplication with identity $R^* = \{r + ne | r \in R, n \in \mathbb{Z}\}$, the subring of T generated by R and e, the identity of T.

(iv) If A is an ideal of R and if r is a regular element of R, then $A/r = \{a/r | a \in A\}$ is a fractional ideal of R. We have $A/r = A < r^{-1} >$ and $A =< r > [A/r]$. Hence $A/r \in F^*(R)$ if and only if $A \in F^*(R)$.

(v) If $F \in F(R)$, there is an integral ideal A of R and a regular element r of R such that $F = A/r$.

The above theorem implies that

$$F(R) = F^*(R) \text{ if and only if } R \text{ is Noetherian.}$$

1.3 Invertible Ideals

If R is a ring containing a regular element and if T is the total quotient ring of R, the set $F(R)$ of fractional ideals of R is a multiplicative abelian semigroup with identity $R^* = \{r + ne | r \in R, n \in \mathbb{Z}\}$ where e is the identity of T. An element which is a unit of the semigroup $F(R)$ is said to be invertible. Hence the fractional ideal F is an invertible ideal if there is an element F_1 of $F(R)$ such that $FF_1 = R^*$. Since $F(R) = F(R^*)$, F is invertible as a fractional ideal of R if and only if F is invertible as a fractional ideal of R^*.

Theorem 1.15 *[7, Theorem 7.1] Let R be a ring containing a regular element, let T be the total quotient ring of R, let $R^* = \{r + ne | r \in R, n \in \mathbb{Z}\}$.*

(i) If F is an invertible fractional ideal of R, then $[R^* : F]_T$ is the unique inverse of F. Moreover, F is finitely generated and F contains a regular element of T.

(ii) If $\mu \in T$, $< \mu >$ is invertible if and only if μ is regular in T.

(iii) If A is an integral ideal of R and if r is a regular element of R, then A/r is invertible if and only if A is invertible.

Proof.

(i) Let F_1 be an inverse of F, say $FF_1 = R^*$. Then clearly $F_1 \subseteq [R^* : F]_T$ so that $R^* = FF_1 \subseteq F[R^* : F]_T \subseteq R^*$. Hence $FF_1 = F[R^* : F]_T$, and since F is an invertible ideal, $F_1 = [R^* : F]_T$ and $[R^* : F]_T$ is the unique inverse of F. There is a finite subset $\{x_i\}_{i=1}^n$ of F and a subset $\{y_i\}_{i=1}^n$ of $[R^* : F]_T$ such that

$$e = \sum_{i=1}^{n} x_i y_i.$$

Therefore, if $x \in F$, then $x = \sum_{i=1}^n x_i(y_i x) \in < x_1, ..., x_n >$, since $y_i x \in R^*$, where $i = 1, ..., n$. It follows that $F \subseteq < x_1, ..., x_n >$, and the reverse containment is obvious. Hence $\{x_i\}_{i=1}^n$ is a finite basis for F. Finally, since each $y_i \in T$, there exists a regular element $r \in R$ such that $ry_i \in R$, where $i = 1, ..., n$. Therefore, $r = \sum_{i=1}^n x_i(y_i r) \in < x_1, ..., x_n >= F$, and F contains a regular element of R which is also regular in T.

(ii) If μ is regular in T, μ is a unit of T. Furthermore,

$$< \mu >< \mu^{-1} >=< e >= R^*,$$

and μ is invertible. Since invertible ideals contain regular elements, $< \mu >$ is not invertible if μ is a zero divisor of T.

(iii) Since $A/r = A < r^{-1} >$ and since $< r^{-1} >$ is invertible, it follows that A/r and A are simultaneously invertible. □

If F is an invertible fractional ideal of the ring R, the above theorem shows that the inverse of F is unique, denoted by F^{-1}. We have,

$$F^{-1} = [R^* : F]_T \text{ and } (F^{-1})^{-1} = F.$$

Theorem 1.16 *[7, Theorem 7.2] Let R be a ring containing a regular element and let F_1, F_2 be fractional ideals of R such that F_2 is invertible and such that $F_1 \subseteq RF_2$, then there is an integral ideal A of R such that $F_1 = AF_2$. A fractional* *ideal F is invertible if and only if there is an integral ideal B such that BF is principal and is generated by a regular element.*

Proof. We have $F_1 = F_1F_2^{-1}F_2$. Further, if $A = F_1F_2^{-1}$, A is an integral ideal of R, since $F_1 \subseteq RF_2$.

If $BF =< r >$ for some integral ideal B and some regular element $r \in R$, then BF is invertible, therefore F is also invertible, which implies $FG = R^*$ for some fractional ideal G of R. We can write G in the form B/u for some integral ideal B of R and some regular element $u \in R$. Then $FB/u = R^*$ and $FB = uR^* =< u >$. □

Notation: Let S be a ring with identity and let A be an ideal of S, $\{\mathcal{M}_\lambda | \lambda \in \Lambda\}$ denotes the set of maximal ideals of S, and for each λ, e_λ, c_λ denote, respectively, extension and contraction of ideals with respect to the ring of quotients $S_{\mathcal{M}_\lambda}$.

Theorem 1.17 *[7, Theorem 7.3] If A is invertible in S and if N is a multiplicative system in S, then A^e, the extension of A to the ring of quotients S_N, is also invertible. Conversely, if B is a finitely generated regular ideal of S such that B^{e_λ} is invertible for each $\lambda \in \Lambda$, then B is invertible in S.*

Proof. We can use Theorem 1.16 to prove the first statement. Since A is invertible, $AC =< d >$ for some ideal C of S and some regular element $d \in S$. Hence $A^eC^e =< d >^e$. If ψ denotes the canonical embedding of S in S_N, $< d >^e$ is principal and generated by $\psi(d)$.

To prove B is invertible, choose a regular element b of B. Then $< b >\subseteq B$ and $< b >^{e_\lambda}\subseteq B^{e_\lambda}$ for any $\lambda \in \Lambda$. But B^{e_λ} is invertible, then there exists an ideal A of $S_{\mathcal{M}_\lambda}$ such that $AB^{e_\lambda} =< b >^{e_\lambda}$ and $A =< b >^{e_\lambda} (B^{e_\lambda})^{-1}$.

That is $A = [< b >^{e_\lambda} \colon B^{e_\lambda}]_T$. Since B is finitely generated, $[< b >^{e_\lambda} \colon B^{e_\lambda}]_T = [< b > \colon B]_T^{e_\lambda}$. By Remark 1.10,

$$< b >= \bigcap_{\lambda \in \Lambda} < b >^{e_\lambda} = \bigcap_{\lambda\Lambda} [< b > \colon B]_T^{e_\lambda} . B^{e_\lambda} = [< b > \colon B]_T . B$$

By Theorem 1.16, B is invertible. $\square$

Proposition 1.18 *[7, Proposition 7.4] Let A be an invertible ideal of the semi-quasi-local ring R. Then*

(i) A is principal

(ii) If R is quasi-local and if B is a basis for A, then $A =< b >$ for some $b \in B$.

Proof.

(i) Let $\{\mathcal{M}_i\}_{i=1}^r$ be the set of maximal ideals of R. For each integer s such that $1 \leq s \leq r$, $\mathcal{M}_s \not\supseteq \bigcap_{i \neq s} \mathcal{M}_i$. Since A is invertible in R, $A\mathcal{M}_s \not\supseteq A[\bigcap_{i \neq s} \mathcal{M}_i]$. We choose $a_s \in A[\bigcap_{i \neq s} \mathcal{M}_i] \setminus A\mathcal{M}_s$, for all s between 1 and r. Define $a = a_1 + \cdots + a_r$. It is clear that $a \in A \setminus A\mathcal{M}_s$ for all s. Hence $a \in A \setminus (\bigcup_{i=1}^{r} A\mathcal{M}_i)$. Since A is invertible, there is an ideal J of R such that $< a >= AJ$. Also $J \nsubseteq M_s$ for all s, since $a \in J$. Then $J = R$ and $A =< a >$.

(ii) If R is quasi-local, $A =< B >=< a >$, so there are subsets $\{a_i\}_{i=1}^n$ of B, and $\{e_i\}_{i=1}^n$ and $\{x_i\}_{i=1}^n$ of R such that $a_i = e_i a$ for each i and $a = \sum_{i=1}^{n} x_i a_i$. It follows that $a = a(\sum_{i=1}^{n} x_i e_i)$. Since $< a >$ is invertible, a is regular in R by Theorem 1.16 so that $1 = \sum_{i=1}^{n} x_i e_i$. Therefore $\sum_{i=1}^{n} x_i e_i$ is a unit in the quasi-local ring R. Hence e_k is a unit and $A =< a >=< e_k^{-1} a_k >=< a_k >$ for some k between 1 and n. $\square$

Lemma 1.19 *[7, Corollary 6.2] Let A and B be ideals of a ring with identity such that $AB = A$ and A is finitely generated. Then there exists an element $b \in B$ such that $a = ab$ for all $a \in A$.*

Proof. Let $A =< a_1, ..., a_n >$ where $a_i \in A$ for all $i = 1, ..., n$ and n is minimal. Since $AB = A$, $a_i = \sum\limits_{j=1}^{n} a_j b_{ij}$ for some $b_{ij} \in B$. Then we have a homogeneous system of equations linear in $a_1, ..., a_n$ such that

$$M_{n\times n}\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = 0 \text{ where } M_{n\times n} = \begin{bmatrix} 1-b_{11} & \dots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & 1-b_{nn} \end{bmatrix}.$$

Let d be the determinant of $M_{n\times n}$, then $da_i = 0$, $i = 1, ..., n$. So $da = 0$ for all $a \in A$. Clearly, $d = 1 - b$ for some $b \in B$ and $da = (1 - b)a = 0$ for all $a \in A$. □

Theorem 1.20 *[7, Theorem 7.6] Let $\mathcal{P}$ be an invertible proper prime ideal of the ring S with identity.*

(a) $\mathcal{P}$ has the property that if $x \in \mathcal{P}^k - \mathcal{P}^{k+1}$, and if $y \in \mathcal{P}^t - \mathcal{P}^{t+1}$ where $\mathcal{P}^0 = S$, then $xy \in \mathcal{P}^{k+t} - \mathcal{P}^{k+t+1}$.

Consequently, $\mathcal{P}_0 = \bigcap\limits_{k=1}^{n} \mathcal{P}^k$ is prime.

(b) $\{\mathcal{P}^k | k \in \mathbb{N}\}$ is the set of $\mathcal{P}$-primary ideals.

(c) If Q is a primary ideal of S such that $\sqrt{Q} \subset \mathcal{P}$, then Q is contained in $\mathcal{P}_0$. If Q is finitely generated, Q is the intersection of the set of all primary ideals contained in $\mathcal{P}$.

In particular, if $< 0 >$ is primary in S, then $< 0 >$ is the only finitely generated primary ideal of R with radical properly contained in $\mathcal{P}$.

(d) If A is an invertible ideal of S properly containing $\mathcal{P}$, then $A = S$.

Proof. (a) Since $\mathcal{P}$ is invertible, $\mathcal{P}^m$ is invertible for any nonnegative integer m. So there are ideals A and B of S where $A \nsubseteq \mathcal{P}$ and $B \nsubseteq \mathcal{P}$ such that $< x >= A\mathcal{P}^k$ and $< y >= B\mathcal{P}^t$. It follows $< xy >= AB\mathcal{P}^{t+k}$, where $AB \nsubseteq P$. Hence $xy \notin \mathcal{P}^{t+k+1}$.

(b) Let k be a positive integer and let $xy \in \mathcal{P}^k$ where $x \in S \setminus \mathcal{P}$ and $y \in S$. Then $y \in \mathcal{P}^k$ by part (a). Thus, $\mathcal{P}^k$ is $\mathcal{P}$-primary. Assume Q is a $\mathcal{P}$-primary ideal of S. Since $\mathcal{P}_0 \subset Q$ and there exists a positive integer m such that $Q \nsubseteq \mathcal{P}^m$, we can choose a positive integer k, such that $Q \subseteq \mathcal{P}^k$ and $Q \nsubseteq \mathcal{P}^{k+1}$. Then $Q = A\mathcal{P}^k$ for some ideal A of S such that $A \nsubseteq P$. Since Q is $\mathcal{P}$-primary, $\mathcal{P}^k \subseteq Q$. Hence, the equality holds.

(c)We assume that $\sqrt{Q} = M \subset \mathcal{P}$. Since $\mathcal{P}$ is invertible, $Q = A\mathcal{P}$ for some ideal A of S. Since Q is primary and $\mathcal{P} \nsubseteq M$, $A \subseteq Q$ so that $Q = Q\mathcal{P}$. Therefore, $Q = Q\mathcal{P} = Q\mathcal{P}^k$ and $Q \subseteq \mathcal{P}^k$ for all positive integer k. It follows that $Q \subseteq \mathcal{P}_0$.

If Q is finitely generated, the equation $Q = Q\mathcal{P}$ implies the existence of an element p of $\mathcal{P}$ such that $q = qp$ for each $q \in Q$, by Lemma 1.19. Moreover, if Q_0 is a primary ideal contained in $\mathcal{P}$, then $q(1-p) = 0 \in Q_0$, with $1-p \notin \mathcal{P} \supseteq \sqrt{Q_0}$, so that $q \in Q_0$ for each $q \in Q$. Hence Q is the intersection of the set of primary ideals contained in $\mathcal{P}$.

(d) We have $\mathcal{P} = AB$ for some ideal B of S. Since $\mathcal{P}$ is prime and $A \nsubseteq \mathcal{P}$, $B \subseteq \mathcal{P}$ so that $B = \mathcal{P}$. Hence $\mathcal{P} = S\mathcal{P} = A\mathcal{P}$, and since $\mathcal{P}$ is a cancelation ideal, $S = A$. □

Remark 1.21 *[24, §4, Remark 1] In a domain R, every nonzero principal ideal is invertible.*

Proof. Let Ra be a nonzero ideal of R that is a is a nonzero element of R and a^{-1} is in the quotient field Q of R, hence $Ra^{-1} \in F(R)$ and $(Ra)(Ra^{-1}) = R$ that is Ra is invertible. □

Theorem 1.22 *[24, Theorem 4.16] If R is a domain, then a nonzero ideal I is projective if and only if it is invertible.*

Proof. If I is projective, there are elements $\{a_k | k \in K\}$ in I and maps $\phi_k : I \to R$. If $b \in I$, $b \neq 0$ and Q is the field of quotients of R, then define $q_k \in Q$ by $q_k = \phi_k(b)/b$.

Note that q_k does not depend on the choice of b: if $b' \in I, b' \neq 0$, then $b'\phi_k(b) = \phi_k(b'b) = \phi_k(bb') = b\phi_k(b')$ and so $\phi_k(b)/b = \phi_k(b')/b'$.

It follows that $q_k I \subset R$ for all k, for $bq_k = \phi_k(b)$ implies $bq_k = 0$ for almost all k, so that if $b \neq 0$, almost all $q_k = 0$. Finally, if $b \in I$,

$$b = \sum(\phi_k(b))a_k = \sum(q_k b)a_k = b(\sum q_k a_k),$$

so that if $b \neq 0$, we may cancel and get $1 = \sum q_k a_k$. Thus, I is invertible.

Suppose I is invertible, so there are elements a_k, q_k satisfying the definition. Define $\phi_k : I \to R$ by $\phi_k(a) = q_k a$. If $a \in I$, then

$$\sum(\phi_k(a))a_k = \sum q_k a a_k = a \sum q_k a_k = a.$$

Hence I is projective. □

CHAPTER 2

SOLUTIONS TO SELECTED EXERCISES IN [7]

2.1 Valuation Rings

Let K be a field and let D be a subring of K with identity. Let $K^* = K \setminus \{0\}$ be the multiplicative group of nonzero elements of K. The group U, units of D, is a subgroup of K^*. We write the group operation on the factor group $G = K^*/U$ as addition: $xU + yU = xyU$. For any $xU, yU \in G$, we define $xU \leq yU$ if and only if $y/x \in D$.

Remark 2.1 *$xU \leq yU$ if and only if Dx, the D-submodule of K generated by x, contains Dy, the D-submodule of K generated by y.*

Proof. $xU \leq yU \Leftrightarrow y/x \in D \Leftrightarrow y/x = d$ for some $d \in D \Leftrightarrow y = xd$ for some $d \in D \Leftrightarrow y \in Dx \Leftrightarrow Dy \subseteq Dx$. □

Moreover " $\leq$ " is a partial order on G such that

(i) $Dx \subseteq Dx$ for all $x \in K$.

(ii) $Dx \subseteq Dy$ and $Dy \subseteq Dx$ implies that $Dx = Dy$ for all $x, y \in K$.

(iii) $Dx \subseteq Dy$ and $Dy \subseteq Dz$ implies that $Dx \subseteq Dz$ for all $x, y, z \in K$.

Definition 2.2 *The partially ordered group G is called the group of divisibility of K with respect to D.*

The set of positive elements of G is

$$G_+ = \{xU|xU \geq U\} = \{xU|x \in D\},$$

the set of cosets of U that are contained, as sets, in D.

The proof of the following theorem was left as an exercise in [7].

Theorem 2.3 *[7, Theorem 16.3]Let D be an integral domain with identity with quotient field K, and let G be the group of divisibility of D. Then the following are equivalent:*

(i) G is totally ordered.

(ii) The set of principal fractional ideals of D is linearly ordered by inclusion.

(iii) The set of fractional ideals of D is linearly ordered by inclusion.

(iv) The set of principal integral ideals of D is linearly ordered by inclusion.

(v) The set of integral ideals of D is linearly ordered by inclusion.

(vi) If $x \in K \setminus \{0\}$, then x or x^{-1} is in D.

Proof.

$(i) \Rightarrow (ii)$ Let Dx, Dy be two principal fractional ideals of D where $x, y \in K^*$. Then $xU, yU \in G = K^*/U$. Since K is totally ordered, $xU \leq yU$ or $yU \leq xU$. Hence $Dy \subseteq Dx$ or $Dx \subseteq Dy$.

$(ii) \Rightarrow (iii)$ Let A, B be two fractional ideals of D. Let x be any element in A. Suppose $B \nsubseteq A$. Hence there exists $y \in B \setminus A$, so $Dy \nsubseteq A$. Thus $Dy \nsubseteq Dx$ and since principal fractional ideals are linearly ordered, we have $Dx \subseteq Dy \subseteq B$. Since it is true for any $x \in A$, we have $A \subseteq B$.

$(iii) \Rightarrow (iv)$ Let Da, Db be two principal integral ideals of D where $a, b \in D$. Then $D(a/1)$ and $D(b/1)$ are two fractional ideals of D. In this case either $Da = D(a/1) \subseteq D(b/1) = Db$ or $Db = D(b/1) \subseteq D(a/1) = Da$.

$(iv) \Rightarrow (v)$ Let M, N be two integral ideals of D and suppose $N \not\subseteq M$. Then there exists $s \in N \setminus M$. In this case $Ds \not\subseteq M$, so $Ds \not\subseteq Dm$ for all $m \in M$. Since principal integral ideals are totally ordered. $Dm \subseteq Ds \subseteq N$ for all $m \in M$. Hence, $M \subseteq N$.

$(v) \Rightarrow (vi)$ Let $x = a/b \in K^*$ where $a, 0 \neq b \in D$. Then Da and Db are integral ideals of D. Since they are linearly ordered, $Da \subseteq Db$ or $Db \subseteq Da$. Then by Remark 2.1, $aU \leq bU$ or $bU \leq aU$. Hence, either $x^{-1} = b/a \in D$ or $x = a/b \in D$.

$(vi) \Rightarrow (i)$ Let xU, yU be two elements in $G = K^*/U$. Then $m = x/y = xy^{-1} \in K^*$ which implies $m \in D$ or $m^{-1} \in D$ by condition (vi). Hence G is totally ordered. $\square$

Definition 2.4 *We call a domain satisfying the conditions of Theorem 2.3 a* <u>*valuation ring*</u> *on* K.

Lemma 2.5 *A valuation ring is quasi-local.*

Proof. Let V be a valuation ring and $\mathcal{M}$ be the set of nonunits of V. So $x \in \mathcal{M}$ if and only if $x = 0$ or $x^{-1} \notin V$. If $a \in V$ and $x \in \mathcal{M}$, we have $ax \in \mathcal{M}$, for otherwise $(ax)^{-1} \in V$ and therefore $x^{-1} = (ax)^{-1}a \in V$ which contradicts that x is a nonunit element.

Next let x, y be nonzero elements of $\mathcal{M}$ which means x^{-1} and $y^{-1} \notin V$. Since $xy^{-1} = x/y \in K^*$, xy^{-1} or $x^{-1}y$ is contained in V. If $xy^{-1} \in V$, then $x+y = (xy^{-1}+1)y \in V\mathcal{M} \subseteq \mathcal{M}$, similarly, $x^{-1}y \in V$ implies $x+y \in \mathcal{M}$. Hence $\mathcal{M}$ is an ideal. Therefore, V is a quasi-local ring. $\square$

Remark 2.6 *Let R be a commutative ring, then $\sum a_n x^n \in R[[x]]$ is invertible if and only if the constant coefficient a_0 is invertible in R. If R is a local ring, then so is $R[[x]]$. If R is a field, then $R[[x]]$ is a valuation ring.*

Remark 2.7 *If F is a field, we can consider the quotient field of the integral domain $F[[x]]$; it is denoted by $F((x))$. Its elements are called* <u>*formal Laurent series*</u> *which can be written uniquely in the form*

$$f = \sum_{n=-M}^{\infty} a_n x^n$$

where M is an integer which depends on the Laurent series f.

Proof. We will prove that every nonzero element of $F[[x]]$ has an inverse in $F((x))$. Let $f = \sum_{i=0}^{\infty} a_i x^i$ be a nonzero element of $F[[x]]$ such that $a_i \in F$ for all $i \in \mathbb{N}$.

If $a_0 \neq 0$, then define $g = \sum_{k=0}^{\infty} b_k x^k$ such that

$$b_0 = 1/a_0 \in F[[x]], b_1 = -a_1/a_0^2 \in F[[x]], b_2 = a_1^2/a_0^3 - a_2/a_0^2 \in F[[x]],$$
$$b_3 = -a_1^3/a_0^4 + 2a_1a_2/a_0^3 - a_3/a_0^2 \in F[[x]], \text{ and so on.}$$

Then $fg = 1$ and $g = f^{-1} \in F[[x]] \subseteq F((x))$. Hence every element of $F[[x]]$ with a nonzero constant term is unit in $F[[x]]$.

Since $f \in F[[x]]$ is nonzero, there exists a positive integer k, where k is the smallest index satisfying $a_k \neq 0$. Then we write f as

$$f = x^k g, \text{ where } g \in F[[x]] \text{ with a nonzero constant term.}$$

Since g is a unit of $F[[x]]$, there exist $h \in F[[x]]$ satisfying $gh = 1$. So $x^{-k}h$, the inverse of f is in $F((x))$.

Hence, the quotient field of $F[[x]]$ is $F((x))$. $\square$

Example 2.8 $D = \mathbb{Z}_{<2>} + x\mathbb{Q}[[x]]$ *is a valuation ring with the maximal ideal* $\mathcal{M} = 2\mathbb{Z}_{<2>} + x\mathbb{Q}[[x]]$.

Proof. Clearly, the quotient field of $\mathbb{Z}[[x]]$ and $\mathbb{Q}[[x]]$ is $\mathbb{Q}((x))$. Since $\mathbb{Z}[[x]] \subseteq D \subseteq \mathbb{Q}[[x]]$, then the quotient field K of D is $\mathbb{Q}((x))$.

Now we will prove that D is a valuation ring. Let $f = \sum_{i=-m}^{\infty} a_i x^i \in \mathbb{Q}((x))$ where $-m$ is the smallest index for $a_{-m} \neq 0$. We will prove that $f \in D$ or $f^{-1} \in D$. We have three cases:

- If $-m > 0$, then $f \in D$.
- If $-m = 0$, then $f = \sum_{i=0}^{\infty} a_i x^i$. In this case if $0 \neq a_0 \in \mathbb{Z}_{<2>}$, then $f \in D$. If $a_0 \notin \mathbb{Z}_{<2>}$, then by the above arguments $a_0^{-1} \in \mathbb{Z}_{<2>}$. Hence
$$f^{-1} = a_0^{-1} + (a_1/a_0^2)x + (a_1^2/a_0^3 - a_2/a_0^2)x^2 + \cdots \in D.$$
- If $-m < 0$, then $f = x^{-m}g$ where $g = \sum_{i=-m}^{\infty} a_i x^{i+m}$. Since the constant term $a_{-m} \neq 0$, g is a unit in $\mathbb{Q}[[x]]$ that is $g^{-1} \in \mathbb{Q}[[x]]$. So we have, $f^{-1} = x^m g^{-1} \in x\mathbb{Q}[[x]] \subseteq D$.

Hence, D is a valuation ring.

Moreover, we will prove that $\mathcal{M} = 2\mathbb{Z}_{<2>} + x\mathbb{Q}[[x]]$ is the unique maximal ideal of D, that is $D \setminus \mathcal{M}$ is precisely the set of units of D. Take $\alpha = \sum_{i=0}^{\infty} a_i x^i \in D \setminus \mathcal{M}$, then $a_0 = a/b \in \mathbb{Z}_{<2>} \setminus 2\mathbb{Z}_{<2>}$ for some $a, b \in \mathbb{Z}$, $b \neq 0$ such that $(a, b) = 1$. Then both of a and b are odd. Hence $\alpha^{-1} = a_0^{-1} + (a_1/a_0^2)x + \cdots \in D$. Hence α is a unit. Now let $\beta = \sum_{i=0}^{\infty} b_i x^i$ be a unit in D that is $\beta^{-1} \in D$ and $\beta\beta^{-1} = 1$. Then $b_0^{-1} \in \mathbb{Z}_{<2>}$. So $b_0 \notin 2\mathbb{Z}_{<2>}$ which implies $\beta \in D \setminus \mathcal{M}$. $\square$

Example 2.9 *Let D be as in Example 2.8. We will determine the ideals of D. Since D is a valuation ring, there are two cases.*

Case 1: *Assume $x\mathbb{Q}[[x]] \subsetneqq I$. If $f \in I \setminus x\mathbb{Q}[[x]]$, then f has the following form:*

$$f = a_0 + a_1 x + \cdots \text{ where } 0 \neq a_0 = \frac{2^k \alpha}{\beta}, \alpha, \beta \text{ odd integers and } k \in \mathbb{N}.$$

Take $f \in I \setminus x\mathbb{Q}[[x]]$ with minimal k such that

$$f = \frac{2^k \alpha}{\beta} + a_1 x + \cdots.$$

Then $h = \frac{\beta}{\alpha} f - \frac{\beta}{\alpha}(a_1 x + \cdots) = 2^k \in I$. So $2^k D \subseteq I$ and $2^{k-1} D \nsubseteq I$ since k is minimal. Hence

$$2^k D \subseteq I \subsetneqq 2^{k-1} D.$$

Suppose there exists $g \in I \setminus 2^k D$. Then $g = c_0 + c_1 x + \cdots$ and $c_0 \notin 2^k \mathbb{Z}_{<2>}$. Then $c_0 \mathbb{Z}_{<2>} \nsubseteq 2^k \mathbb{Z}_{<2>}$. Since $\mathbb{Z}_{<2>}$ is a discrete valuation ring with maximal ideal $2\mathbb{Z}_{<2>}$, every ideal of $\mathbb{Z}_{<2>}$ is of the form $2^r \mathbb{Z}_{<2>}$ for some $r \in \mathbb{N}$. That means

$$2^k \mathbb{Z}_{<2>} \subsetneqq c_0 \mathbb{Z}_{<2>} = 2^r \mathbb{Z}_{<2>} \subsetneqq 2^{k-1} \mathbb{Z}_{<2>},$$

which is a contradiction, since $r \in \mathbb{N}$. Therefore, $I = 2^k D$. Hence, the ideals of D containing $x\mathbb{Q}[[x]]$ are of the form $2^k D$ for some $k \in \mathbb{N}$ that is

$$\cdots \subset x\mathbb{Q}[[x]] \subset \cdots \subset 2^n D \subset \cdots \subset 2^2 D \subset 2D \subset D.$$

Case 2: *Now take an ideal I of D such that $I \subseteq x\mathbb{Q}[[x]]$. Then every $f \in I$*

has the following form:

$$f = x^k(a_k + a_{k+1}x + \cdots) = x^k g \text{ such that } a_k \neq 0, k \in \mathbb{Z}^+, i \geq k, a_i \in \mathbb{Q},$$

so $g \in \mathbb{Q}[[x]]$.

If there exists $f \in I$ *such that* $a_k \in \mathbb{Q} \setminus \mathbb{Z}_{<2>}$, *then let* k *be minimal with respect to this property, then* $a_k = a/b, (a,b) = 1, b$ *is even, so* a *is odd. Then*

$$1/g \in D \Rightarrow f/g = x^k \in I \Rightarrow x^k D \subsetneqq I, \text{ since } f \in I \setminus x^k D.$$

Hence $x^k D \subsetneqq I \subseteq x^k \mathbb{Q}[[x]]$. *Here* $I = x^k(A + x\mathbb{Q}[[x]])$ *where* $\mathbb{Z}_{<2>} \subsetneqq A \subseteq \mathbb{Q}$. *Clearly,* A *is a* $\mathbb{Z}_{<2>}$*-module. Take* $\alpha/\beta \in A$. *If there exists a maximal* $s \in \mathbb{Z}^+$ *such that* $2^s | \beta$, *then* $A =< 1/2^s >$, *otherwise* $A = \mathbb{Q}$.

- *If* $A =< 1/2^s >$, *then* $I = x^k(< 1/2^s > +x\mathbb{Q}[[x]])$. *In particular,* A *is a fractional ideal of* $\mathbb{Z}_{<2>}$.
- *If* $A = \mathbb{Q}$, *then* $I = x^k\mathbb{Q}[[x]]$. *So*

$$\cdots \subset xD \subset x(< 1/2 > +x\mathbb{Q}[[x]]) \subset \cdots \subset x(< 1/2^s > +x\mathbb{Q}[[x]]) \subset \cdots \subset x\mathbb{Q}[[x]] \subset \cdots.$$

Now if for all $f \in I$, $a_k \in \mathbb{Z}_{<2>}$, *then* $a_k = 2^t c/d$ *for some odd integers* c, d. *Choose* $f \in I$ *with minimal* t, *then*

$$f = 2^t x^k(c/d + b_{k+1}x + \cdots) = 2^t x^k g, \text{ where } g \text{ is a unit in } D.$$

Hence

$$g^{-1}f = 2^t x^k \in I \Rightarrow 2^t x^k D \subseteq I \subsetneqq 2^{t-1}x^k D.$$

Let $\varphi \in I \setminus 2^t x^k D$*, then* $\varphi = x^k(d_k + d_{k+1}x + \cdots)$ *and* $d_k \notin 2^t\mathbb{Z}_{<2>}$*. So we have*

$$2^t\mathbb{Z}_{<2>} \subseteq d_k\mathbb{Z}_{<2>} \subsetneqq 2^{t-1}\mathbb{Z}_{<2>},$$

which is a contradiction. Hence $I = 2^t x^k D$*.*

$$\cdots \subset 2^t xD \subset \cdots \subset 2xD \subset \cdots \subset xD \subset \cdots \subset x\mathbb{Q}[[x]] \subset \cdots.$$

Definition 2.10 *Let R be a ring with identity. R is called a* <u>*chained ring*</u> *if the set of ideals of R is linearly ordered by inclusion.*

Remark 2.11 *Every valuation ring is a chained ring. Converse does not hold. Let D be as in Example 2.8. Then* $D/8D$ *is a chained ring but not a valuation ring.*

Exercise 2.12 *[7, §16, Exercise 8] Prove that the following conditions, (1)-(3) are equivalent for a ring R. Condition (1) implies condition (4), but not conversely.*

(1) The set of fractional ideals of R is linearly ordered by inclusion.

(2) R is a chained ring.

(3) The set of principal integral ideals of R is linearly ordered by inclusion.

(4) R contains each zero divisor of S, the total quotient ring of R. Moreover, if x is a unit of S, then x or x^{-1} *is in R.*

Solution. Both (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) are clear.

(3) $\Rightarrow$ (1) First, we will prove that the principal fractional ideals of R are linearly ordered. Let $F_1 = R(a/s_1)$ and $F_2 = R(b/s_2)$ be two principal fractional ideals of R where $a, b, s_1, s_2 \in R$ and s_1, s_2 are regular elements. Then Ras_2

and Rbs_1 are principal integral ideals of R. Since they are linearly ordered, $Ras_2 \subseteq Rbs_1$ or $Rbs_1 \subseteq Ras_2$. Assume $Ras_2 \subseteq Rbs_1$ which means $bs_1|as_2$ such that $kbs_1 = as_2$ for some $k \in R$. Then $k(b/s_2) = a/s_1$ for some $k \in R$ which implies $a/s_1 \in R(b/s_2) = F_2$. So, $F_1 \subseteq F_2$ and principal fractional ideals of R are linearly ordered.

Now, assume F, F' are arbitrary fractional ideals of R such that $F \not\subseteq F'$, then there exists $x \in F \setminus F'$. For any $y \in F'$, $Rx \not\subseteq Ry$. Since principal fractional ideals are linearly ordered, $Ry \subseteq Rx$ for all $y \in F'$. Hence $F' \subseteq Rx \subseteq F$.

(1) $\Rightarrow$ (4) Let $x = x_1/s_1$ be a zero divisor of S, where $0 \neq x_1, s_1 \in R$, s_1 is regular, then there exists a nonzero $y = y_1/s_2 \in S$ where $0 \neq y_1, s_2 \in R$, s_2 is regular such that $xy = (x_1/s_1)(y_1/s_2) = (x_1y_1)/(s_1s_2) = 0$. This implies $x_1y_1 = 0$, so x_1 is a zero divisor of R. Suppose $x \notin R$. Since fractional ideals of R are linearly ordered, we have $R \subseteq Rx$. So $1 = rx$ for some $r \in R$ and $x^{-1} = s_1/x_1 \in R \subseteq S$. That is x_1 is a regular element of R. So x is not a zero divisor of S, which is a contradiction.

Let x be regular element of R, since fractional ideals of R are linearly ordered, we have $R \subseteq Rx$ or $Rx \subseteq R$. Hence $1 = r_1x$ or $x = r_2$ for some $r_1, r_2 \in R$. Then $x^{-1} = r_1 \in R$ or $x = r_2 \in R$. Let $R = \mathbb{Z}_6$. Clearly the quotient ring S is R itself and R satisfies condition (4). $< \overline{2} >$ and $< \overline{3} >$ are fractional ideals of R, but they are not linearly ordered. □

Exercise 2.13 *[7, §17, Exercise 7] Let A be an ideal of the chained ring V. Prove that V/A is a chained ring.*

Solution. We will prove the set of integral ideals are linearly ordered. Let $I/A, J/A$ be arbitrary integral ideals of V/A, then I, J are integral ideals of V, containing A. Assume $I \nsubseteq J$. Since the ideals of V are linearly ordered, $J \subseteq I$. Hence $J/A \subseteq I/A$. $\Box$

Exercise 2.14 *[7, §16, Exercise 9] Let R be a ring with identity with total quotient ring S. Of the following conditions, prove that (2) and (3) are equivalent and (1) implies (2). Moreover if each regular ideal of R is generated by its set of regular elements, then (2) implies (1).*

(1) The set of regular ideals of R is linearly ordered by inclusion.

(2) The set of regular principal ideals of R is linearly ordered.

(3) If x is a unit of S, then either x or x^{-1} is in R.

Solution. (2) $\Rightarrow$ (3) Let $x = x_1/s_1$ be a unit of S where $x_1, s_1 \in R$ and x_1, s_1 are regular in R, otherwise $x^{-1} = s_1/x_1 \notin S$, contradicting that x is a unit of S. Since the set of regular principal ideals of R is linearly ordered, $Rx_1 \subseteq Rs_1$ or $Rs_1 \subseteq Rx_1$. Hence $x_1 = rs_1$ or $s_1 = r'x_1$ for some $r, r' \in R$. Therefore $x = x_1/s_1 = r \in R$ or $x^{-1} = s_1/x_1 = r' \in R$.

(3) $\Rightarrow$ (2) Let Ra, Rb be arbitrary regular principal ideals of R that is a, b are arbitrary regular elements of R. Define $x = a/b$. Clearly x is a unit of S. Then by (3), $x = a/b \in R$ or $x^{-1} = b/a \in R$. Hence $xb = a$ or $x^{-1}a = b$. Thus $Ra \subseteq Rb$ or $Rb \subseteq Ra$.

(1) $\Rightarrow$ (2) is clear.

Assume that each regular ideal of R is generated by its set of regular elements.

(2) $\Rightarrow$ (1) Let I, J be arbitrary regular ideals of R such that $I \nsubseteq J$. Assume $I =< \{a_\lambda\}_{\lambda\in\Lambda} >$ and $J =< \{b_\gamma\}_{\gamma\in\Gamma} >$ where a_λ, b_γ are regular elements for all $\lambda \in \Lambda$ and $\gamma \in \Gamma$. Then there exists $a_{\lambda_0} \in I \setminus J$ that is $Ra_{\lambda_0} \nsubseteq Rb_\gamma$ for all

$\gamma \in \Gamma$. Since the set of regular principal ideals of R are linearly ordered, then $Rb_\gamma \subseteq Ra_{\lambda_0}$ for all $\gamma \in \Gamma$. Hence $J \subseteq Ra_{\lambda_0} \subseteq I$. $\square$

Exercise 2.15 *[7, §16, Exercise 20] Determine the group of divisibility of* $\mathbb{Z}[2i]$.

Solution. We will first find the units of $\mathbb{Z}[2i]$ Let $a + b2i \in \mathbb{Z}[2i]$ be a unit, then norm of this element over $\mathbb{Z}$ should be ± 1, and the solutions of $a^2 + b^2 4 = \pm 1$ are $a = \pm 1$ and $b = 0$. So the set of units U of $\mathbb{Z}[2i]$ is $\{\pm 1\}$.

Secondly, we will prove that the quotient field of $\mathbb{Z}[2i]$ is $K = \mathbb{Q}[i]$. Take $x/y \in K$ where $x = a+b2i$ and $y = c+d2i$ for $a, b, c, d \in \mathbb{Z}$ such that $c+d(2i) \neq 0$. Then

$$\frac{x}{y} = \frac{a + b2i}{c + d2i} = \frac{ac + 4bd}{c^2 + 4b^2} + \frac{2(bc - ad)}{c^2 + 4d^2} i \in \mathbb{Q}[i]$$

So, $K \subseteq \mathbb{Q}[i]$.

On the other hand, since $\mathbb{Q} \subseteq K$ and $2i \in K$, $i \in K$. Hence $\mathbb{Q}[i] \subseteq K$, and the equality follows.

Finally, we can define the group of divisibility G of $\mathbb{Z}[2i]$ as follows,

$$G = \mathbb{Q}[i]^*/U = \{(x + yi)U | x, y \in \mathbb{Q}, x + yi \neq 0\}$$

where

$$G \cong \{x + yi | x, y \in \mathbb{Q}, x > 0 \text{ or } x = 0 \text{ and } y > 0\}.$$

$\square$

2.2 Structure of Valuation Rings

Theorem 2.16 *[7, Theorem 17.1] Let V be a valuation ring which is not a field, and let A be a proper ideal of V.*

(i) If A is finitely generated, then A is principal.

(ii) $\sqrt{A}$ is a prime ideal of V.

(iii) $\bigcap_{n=1}^{\infty} A^n = \mathcal{P}_0$ is a prime ideal of V. If for some positive integer k, $A^k = A^{k+1}$, then A is an idempotent prime ideal.

(iv) Each prime ideal properly contained in A is contained in $\mathcal{P}_0$

(v) If B is an ideal of V such that $A \subset \sqrt{B}$, then B contains a power of A.

Proof.

(i) Let $A =< a_1, ..., a_n >$. The set $\{< a_i > | i = 1, ..., r\}$ of principal ideals is linearly ordered under inclusion, and hence there exists k, $1 \leq k \leq r$ such that $< a_i >$ is contained in $< a_k >$ so that A is principal.

(ii) Let S be the set of all minimal prime ideals of A. Since the set of prime ideals of V is linearly ordered under inclusion, S contains a single element which is $\mathcal{P}$. Therefore $\sqrt{A}$ is a prime ideal of V, since $\sqrt{A} = \bigcap_{\mathcal{P} \in S} \mathcal{P} = \mathcal{P}$.

(iii) We prove that $\mathcal{P}_0$ is a prime ideal by showing that $V \setminus \mathcal{P}_0$ is a multiplicative system. Hence if $x, y \in V \setminus \mathcal{P}_0$, then there are positive integers m, n such that $x \notin A^n$ and $y \notin A^m$. Therefore $A^n \subset< x >$ and $A^m \subset< y >$. Multiplying the first containment by the invertible ideal $< y >$, we obtain $A^n < y >\subset< xy >$, and since $A^m \subset< y >$, $A^{m+n} \subset A^n < y >$. Hence $A^{m+n} \subset< xy >$ and $xy \in V \setminus \mathcal{P}_0$.

If for some $k \in \mathbb{Z}^+$, $A^k = A^{k+1}$, then $\mathcal{P}_0 = A^k$. Therefore since $\mathcal{P}_0$ is prime, $A \subseteq \mathcal{P}_0 = A^k$, so that $A = A^k = A^{k+1}$. Thus $A^2 = A^{k+1} = A$ and A is prime.

(iv) If $\mathcal{P}$ is a prime ideal of V and if $\mathcal{P} \subset A$, then $\mathcal{P}$ contains no power of A. Therefore $\mathcal{P} \subset A^k$ for all $k \in \mathbb{Z}^+$, consequently, $\mathcal{P} \subseteq \bigcap\limits_{k=1}^{\infty} A^k = \mathcal{P}_0$.

(v) We will prove that for all positive integer k, $A^k \nsubseteq B$ implies that A is not contained in $\sqrt{B}$ properly. Let $A^k \nsubseteq B$ for all $k \in \mathbb{Z}^+$. Then $B \subset A^k$ for all $k \in \mathbb{Z}^+$, which implies $B \subset \mathcal{P}_0$. So $\sqrt{B} \subseteq \mathcal{P}_0 \subseteq A$ which means that A is not contained in $\sqrt{B}$ properly. $\square$

Exercise 2.17 *[7, §17, Exercise 1] More generally, parts (i),(ii),(iv),(v) of Theorem 2.16 are also valid for a chained ring V, but the assertions of part (iii) does not hold for V; take $V = \mathbb{Z}/ < 8 >, A =< 4 > / < 8 >$. If, however, A properly contains a prime ideal of V, then part (iii) of Theorem 2.16 is valid for V and A.*

Solution. It can be easily seen that (i),(ii),(v) of Theorem 2.16 are also valid for a chained ring V.

To prove (iv), we show that $\sqrt{A^k} = \sqrt{A}$ for all $k \in \mathbb{Z}^+$, where A is an ideal of a chained ring V. $\sqrt{A^k} \subseteq \sqrt{A}$ is obvious. Take $x \in \sqrt{A}$, then $x^s \in A$ for some $s \in \mathbb{Z}^+$, so $x^{sk} \in A^k$ which implies $x \in \sqrt{A^k}$. Hence $\sqrt{A^k} = \sqrt{A}$. Let $A^t \subseteq P$ for some $t \in \mathbb{Z}^+$, where $P \subsetneqq A$ is a proper prime ideal of V. Then $A \subseteq \sqrt{A} = \sqrt{A^t} \subseteq \sqrt{P} = P$, which contradicts that P is proper in A. Hence $A^k \nsubseteq P$ for all $k \in \mathbb{Z}^+$. Since ideals of V are linearly ordered, $P \subset A^k$ for all $k \in \mathbb{Z}^+$. Then P is contained in P_0.

We have $V = \mathbb{Z}/ < 8 >$ is a chained ring. To prove (iii) of Theorem 2.7 does not hold for V, let $A =< 4 > / < 8 >$. Then $A^2 =< 0_V >= A^3 = A^4 = \cdots$. Hence $\bigcap\limits_{n=1}^{\infty} A^n =< 0_V >$ which is not a prime ideal of V that is

$$(2+ < 8 >)(4+ < 8 >) =< 8 > \in < 0_V >, \text{ but } (2+ < 8 >), (4+ < 8 >) \notin < 0_V > .$$

Also $A^2 = A^3$, but $A \neq < 0_V >= A^2$. Thus A is not idempotent.

Let $\mathcal{P}$ be a prime ideal properly contained in A. Assume there exist $s_0 \in \mathbb{Z}^+$ such that $A^{s_0} \subseteq \mathcal{P}$. Then $A \subseteq \sqrt{A} = \sqrt{A^{s_0}} \subseteq \mathcal{P}$ which contradicts $\mathcal{P}$ is proper in A. Thus $\mathcal{P} \subsetneqq A^k$ for all positive integer k and $\mathcal{P} \subseteq \bigcap\limits_{n=1}^{\infty} A^n = \mathcal{P}_0$. To prove $V \setminus \mathcal{P}_0$ is a multiplicative system, take $x, y \in V \setminus \mathcal{P}_0$ that is $x \notin A^k$ and $y \notin A^m$ for some positive integer $k, m \in \mathbb{Z}^+$. Since V is a chained ring, $V/\mathcal{P}$ is also a chained ring by Exercise 2.13 and $< 0 > \subsetneqq A^k/\mathcal{P} \subsetneqq < x + \mathcal{P} >$ and $< 0 > \subsetneqq A^m/\mathcal{P} \subsetneqq < y + \mathcal{P} >$ in $V/\mathcal{P}$. Since $\mathcal{P}$ is prime, $V/\mathcal{P}$ is a domain and $y + \mathcal{P}$ is a regular element in $V/\mathcal{P}$. That implies $< y + \mathcal{P} >$ is an invertible ideal. Thus $(A^k/\mathcal{P}) < y + \mathcal{P} > \subsetneqq < xy + \mathcal{P} >$. Since $A^m/\mathcal{P} \subseteq < y + \mathcal{P} >$, we have $A^{k+m}/\mathcal{P} \subseteq (A^k/\mathcal{P}) < y + \mathcal{P} > \subsetneqq < xy + \mathcal{P} >$ that is $xy \notin A^{k+m}$ and $xy \in V \setminus \mathcal{P}_0$.

Assume $A^k = A^{k+1}$ for some positive integer k, then $\mathcal{P}_0 = A^k$ and

$$A^s \supseteq \mathcal{P}_0 = \sqrt{\mathcal{P}_0} = \sqrt{A^k} = \sqrt{A} \supseteq A \supseteq A^s \text{ for any positive integer } s.$$

Hence A is an idempotent ideal. $\square$

Remark 2.18 *A valuation ring is a Bezout domain.*

Exercise 2.19 *[7, §22, Exercise 12] If R is a Bezout ring, then R/I is a Bezout ring for each ideal I of R.*

Solution. If $I = R$, the result is clear. Let $N/I =< a_1 + I, ..., a_n + I >$ be a finitely generated ideal of R/I where I is a proper ideal of the Bezout ring R and $a_1, ..., a_n \in R$. Then $J =< a_1, ..., a_n >$ is a finitely generated ideal of R which is contained in N. Hence $J =< s >$ for some $s \in J$. We claim that $N/I = (J+I)/I$. Since $J, I \subseteq N$, clearly $(I + J)/J \subseteq N/I$. To show the other side of the inclusion, take $x + I \in N/I$ then, clearly, $x + I = \sum\limits_{i=1}^{n}(a_i r_i + I) = (\sum\limits_{i=1}^{n} a_i r_i) + I \in (J + I)/I$

where $r_i \in R$ for $i = 1, ..., n$. Hence,

$$N/I = (J + I)/I =< s + I >,$$

that is N/I is principal and R/I is a Bezout ring. $\square$

Definition 2.20 *A prime ideal $\mathcal{P}$ of a ring R is called <u>branched</u> if there exists a $\mathcal{P}$-primary ideal distinct from $\mathcal{P}$; if $\mathcal{P}$ is the only $\mathcal{P}$-primary ideal of R, then $\mathcal{P}$ is said to be <u>unbranched</u>.*

The following theorem deals with the set of primary ideals of a valuation ring.

Theorem 2.21 *[7, Theorem 17.3] Let V be a valuation ring which is not a field, and let $0 \neq \mathcal{P}$ be a prime ideal of V.*

(i) If Q is $\mathcal{P}$-primary and if $x \in V \setminus \mathcal{P}$, then $Q = Q < x >$. If Q is finitely generated, then $\mathcal{P}$ is a maximal ideal of V.

(ii) If $S = \{Q_\lambda | \lambda \in \Lambda\}$ is the set of $\mathcal{P}$-primary ideals, then S is closed under multiplication. In particular, $\{P^k\}_{k=1}^{\infty} \subseteq S$. If $\mathcal{P} \neq \mathcal{P}^2$, then $S = \{\mathcal{P}^k\}_{k=1}^{\infty}$.

(iii) If $\mathcal{P}$ is branched and Q is $\mathcal{P}$-primary, $Q \neq \mathcal{P}$, then $\bigcap_{n=1}^{\infty} Q^n = \bigcap_{\lambda \in \Lambda} Q_\lambda$.

(iv) $\mathcal{P}_0 = \bigcap_{\lambda \in \Lambda} Q_\lambda$ is a prime ideal of V, and there are no prime ideals of V properly between $\mathcal{P}_0$ and $\mathcal{P}$.

(v) The following are equivalent:

(a) $\mathcal{P}$ is branched.

(b) There is an ideal $A \neq \mathcal{P}$ such that $\mathcal{P} = \sqrt{A}$.

(c) $\mathcal{P}$ is the radical of a principal ideal.

(d) $\mathcal{P}$ *is not the union of the set of prime ideals of* V *properly contained in* $\mathcal{P}$.

(e) There is a prime ideal M *properly contained in* $\mathcal{P}$ *such that there are no primes of* V *properly between* M *and* $\mathcal{P}$.

Proof.

(i) Since $x \notin \mathcal{P}$, $Q \subset < x >$, and since $< x >$ is invertible, there exists an ideal A of V such that $Q = A < x > \subseteq A$. Moreover, Q is $\mathcal{P}$-primary and $x \notin \mathcal{P}$, so that $A \subseteq Q \subseteq A$. Hence $Q = Q < x >$.

If Q is finitely generated, Q is a nonzero principal ideal and hence an invertible ideal. Thus if x is any element of $V \setminus \mathcal{P}$, $< x >= V$, x is a unit of V, and consequently, $\mathcal{P}$ is a maximal ideal of V.

(ii) If $Q_1, Q_2 \in S$, we show that $Q_1Q_2 \in S$. We have

$$\sqrt{Q_1Q_2} = \sqrt{\sqrt{Q_1}\sqrt{Q_2}} = \mathcal{P}.$$

If $x, y \in V$ with $xy \in Q_1Q_2$ and $x \notin \mathcal{P}$, then by (i)

$$Q_1 = Q_1 < x > \ , \ < x >< y >=< xy > \subseteq Q_1Q_2 =< x > Q_1Q_2.$$

Therefore, $y \in Q_1Q_2$ and Q_1Q_2 is $\mathcal{P}$-primary.

If $\mathcal{P} \neq \mathcal{P}^2$, we show that each $\mathcal{P}$-primary ideal Q is a power of $\mathcal{P}$. By Theorem 2.16 (v), Q contains a power of $\mathcal{P}^2$, and hence a power of $\mathcal{P}$. We choose k minimal such that $\mathcal{P}^k \subseteq Q$. There exists $y \in \mathcal{P}^{k-1} \setminus Q$. Hence $Q \subset < y >$ and $Q = A < y >$ for some ideal A of V. Since Q is $\mathcal{P}$-primary and $y \notin Q$, it follows that $A \subseteq \mathcal{P}$. Hence $Q = A < y > \subseteq \mathcal{P} < y > \subseteq \mathcal{P}^k$, and Q is a power of $\mathcal{P}$.

(iii) Since $\{Q^n\}_{n=1}^{\infty} \subseteq S = \{Q_\lambda\}$, clearly $\bigcap\limits_{\lambda \in \Lambda} Q_\lambda \subseteq \bigcap\limits_{n=1}^{\infty} Q^n$ By Theorem 2.16 (v), each Q_λ contains a power of Q, hence the reverse containment also holds.

Hence $\bigcap\limits_{\lambda \in \Lambda} Q_\lambda = \bigcap\limits_{n=1}^{\infty} Q^n$.

(iv) If $\mathcal{P}$ is unbranched, it is obvious.

If $\mathcal{P}$ is branched, by (iii) $\mathcal{P}_0 = \bigcap\limits_{n=1}^{\infty} Q^n$ for each $\mathcal{P}$-primary ideal $Q \neq \mathcal{P}$. Therefore $\mathcal{P}_0$ is prime and each prime ideal properly contained in $\mathcal{P}$ is contained in $\mathcal{P}_0$ by Theorem 2.16(iii). Consequently, there are no prime ideal of V properly between $\mathcal{P}_0$ and $\mathcal{P}$.

(v) $(a) \Rightarrow (b)$ clear.

$(b) \Rightarrow (c)$ Suppose there exists $A \neq \mathcal{P}$ such that $\mathcal{P} = \sqrt{A}$. If $x \in \mathcal{P} \setminus A$, then $A \subseteq < x > \subseteq \mathcal{P}$, so that $\sqrt{< x >} \subseteq \mathcal{P} = \sqrt{A} \subseteq \sqrt{< x >}$, so $\mathcal{P} = \sqrt{< x >}$.

$(c) \Rightarrow (d)$ Suppose $\mathcal{P} = \sqrt{< x >}$, then x is not in any prime ideal of V properly contained in $\mathcal{P}$. Therefore, $\mathcal{P} \neq \bigcup\limits_{\substack{Q_\lambda \lhd_p V \\ Q_\lambda \subsetneqq \mathcal{P}}} Q_\lambda$.

$(d) \Rightarrow (e)$ Suppose $\mathcal{P} \neq \bigcup\limits_{\substack{Q_\lambda \lhd_p V \\ Q_\lambda \subsetneqq \mathcal{P}}} Q_\lambda$. Here Q_λ 's are linearly ordered since V is a valuation ring. So $\bigcup\limits_{\substack{Q_\lambda \lhd_p V \\ Q_\lambda \subsetneqq \mathcal{P}}} Q_\lambda$ is an ideal. Furthermore it is prime.

$(e) \Rightarrow (a)$ This is a consequence of the following lemma. □

Lemma 2.22 *[7, Lemma 17.4] Let $\mathcal{P}$ and $\mathcal{M}$ be proper prime ideals of the ring R such that $\mathcal{P} \subset \mathcal{M}$ and such that there are no prime ideals of R properly between $\mathcal{P}$ and $\mathcal{M}$. Then $\mathcal{P}$ is the intersection of the set of $\mathcal{M}$-primary ideals containing $\mathcal{P}$.*

Proof. By passage to $R/\mathcal{P}$, without loss of generality we may assume that R is a domain, $\mathcal{M}$ is minimal in R, and $\mathcal{P} =< 0 >$. And by further passage to $R_{\mathcal{M}}$, it is sufficient to prove the lemma for the case where $\mathcal{M}$ is the maximal ideal of the one-dimensional quasi-local domain R, and $\mathcal{P} =< 0 >$. In this case, we only need to show that if d is a nonzero element of $\mathcal{M}$, then there is an $\mathcal{M}$-primary ideal not containing d. But $d \notin < d^2 >$, and $< d^2 >$ is $\mathcal{M}$-primary since $\mathcal{M}$, the radical of $< d^2 >$, is maximal in R. $\square$

Exercise 2.23 *[7, §17, Exercise 4] Let $D = \mathbb{Z}_{<2>} + x\mathbb{Q}[[x]]$. D is a valuation ring. (See Example 2.8)*

(1) Prove that the second statement in (i) of Theorem 2.21 fails in a chained ring by taking Q to be the zero ideal of $D/x^2\mathbb{Q}[[x]]$.

(2) Prove that (ii) of Theorem 2.21 fails in a chained ring by taking $P = x\mathbb{Q}[[x]]/xD$.

(3) Prove that (iii) of Theorem 2.21 fails for $P = x\mathbb{Q}[[x]]/x^3D$ and $Q = x^2\mathbb{Q}[[x]]/x^3D$ in the chained ring D/x^3D; the same example shows that (iv) of Theorem 2.21 fails for a chained ring.

(4) Give examples to show that the implications (a) $\Rightarrow$ (e) and (b) $\Rightarrow$ (a) in part (v) of Theorem 2.21 need not hold in a chained ring.

Solution.

(1) If V is a chained ring, then V/A is a chained ring for any ideal A of V by Exercise 2.13. Since any valuation ring is a chained ring, D and $D/x^2\mathbb{Q}[[x]]$ are chained rings.

Fact 1: $\mathcal{P} = x\mathbb{Q}[[x]]$ is a prime ideal of D.

Let $f.g \in x\mathbb{Q}[[x]]$, where $f = \sum_{i=0}^{\infty} a_i x^i, g = \sum_{i=0}^{\infty} b_i x^i \in D$. Then $a_0 b_0 = 0$. However $\mathbb{Z}_{<2>}$ is a domain. So $a_0 = 0$ or $b_0 = 0$ that is $f \in x\mathbb{Q}[[x]]$ or $g \in x\mathbb{Q}[[x]]$.

Fact 2: $I = x^2\mathbb{Q}[[x]]$ is $\mathcal{P}$-primary ideal of D.

Take $f = \sum_{i=0}^{\infty} a_i x^i, g = \sum_{i=0}^{\infty} a_i x^i \in D$ with $f^k \notin I$ for all $k \in \mathbb{Z}^+$ such that $f.g \in x^2\mathbb{Q}[[x]]$. Clearly, $a_0 \neq 0$, $a_0 b_0 = 0$ and $a_0 b_1 + a_1 b_0 = 0$. So $b_0 = b_1 = 0$ that is $g \in I$. Also we have to show that $\sqrt{I} = \mathcal{P}$. Let $\mathcal{P}'$ be a prime ideal containing I. Take $f \in \mathcal{P}$, then $f^2 \in I \subset \mathcal{P}'$. So $\mathcal{P} \subseteq \mathcal{P}'$. Thus $\sqrt{I} = \mathcal{P}$. Hence I is a $\mathcal{P}$-primary ideal of D.

Fact 3: Q is a $\mathcal{P}$-primary (prime) ideal if and only if Q/I is a $\mathcal{P}/I$ primary (prime) ideal of R/I for all $I \subseteq Q$.

$(a+I)(b+I) \in Q/I$ if and only if $ab \in Q$ and Q is $\mathcal{P}$-primary that is $ab \in Q$ implies $a \in Q$ or $b^n \in Q$ for some $n \in \mathbb{Z}^+$ if and only if $a + I \in Q/I$ or $(b+I)^n \in Q/I$ when $(a+I)(b+I) \in Q/I$. Also $\sqrt{Q} = \mathcal{P}$ if and only if $\sqrt{Q/I} = \mathcal{P}/I$.

As a result of these three, we have $J = x\mathbb{Q}[[x]]/x^2\mathbb{Q}[[x]]$ is a prime ideal of $D/x^2\mathbb{Q}[[x]]$ and $< 0_{D/x^2\mathbb{Q}[[x]]} >$ is a J-primary ideal of $D/x^2\mathbb{Q}[[x]]$. Clearly $< 0_{D/x^2\mathbb{Q}[[x]]} >$ is finitely generated.

We know that $\mathcal{M} = 2\mathbb{Z}_{<2>} + x\mathbb{Q}[[x]]$ is the unique maximal ideal of D. Then $\mathcal{P} \subsetneqq \mathcal{M}$ which implies $\mathcal{P}/I \subsetneqq \mathcal{M}/I$ that is $\mathcal{P}/I$ is not maximal.

(2) We have $x^2\mathbb{Q}[[x]] \subset D$. If $f = \sum_{i=0}^{\infty} a_i x^i \in x^2 Q[[x]]$, then $a_0 = a_1 = 0$. Thus $f = x(0 + a_2 x + \cdots) \in xD$, since $0 + a_2 x + \cdots \in D$. Hence $\mathcal{P}^2 =< 0_{D/xD} >$. So $\mathcal{P} \neq \mathcal{P}^2$. We will prove that $\mathcal{P}^2 =< 0_{D/xD} >$ is not a primary ideal of D/xD. Take $m = 2/1 + xD, n = (1/2)x + xD \in D/xD$. Then $mn = xD \in \mathcal{P}^2$. Clearly neither m^k nor n is in $\mathcal{P}^2$ for all $k \in \mathbb{Z}^+$. Thus $\mathcal{P}^2$ is not in the set of primary ideals of D/xD.

(3) In part (1), Fact 2, we proved that $x^2\mathbb{Q}[[x]]$ is $x\mathbb{Q}[[x]]$-primary ideal of D. And by Fact 3 in part (1), Q is $\mathcal{P}$-primary ideal of D/x^3D and $Q \neq \mathcal{P}$. Then $\mathcal{P}$ is branched. Clearly, $Q^2 =< 0_{D/x^2D} >$, since $x^4\mathbb{Q}[[x]] \subseteq x^3 D$. Hence, $\bigcap_{n=1}^{\infty} Q^n =< 0_{D/xD} >$.

Let S be the set of $\mathcal{P}$-primary ideals of D/x^3D. We claim that $\mathcal{P}^3$ is the smallest $\mathcal{P}$-primary ideal of D/x^3D. First, let's prove that $\mathcal{P}^3$ is $\mathcal{P}$-primary ideal of D/x^3D. Clearly, $\sqrt{\mathcal{P}^3} = \mathcal{P}$. Take $m = a_0 + a_1x + a_2x^2 + a_3x^3 + x^3D$, $n = b_0 + b_1x + b_2x^2 + b_3x^3 + x^3D \in D/x^3D$ such that $mn \in \mathcal{P}^3$. Assume $m \notin \mathcal{P}$, then $a_0 \neq 0$, and $b_0 = b_1 = b_2 = 0$. So $n \in \mathcal{P}^3$ and $\mathcal{P}^3 \in S$. To show $\mathcal{P}^3$ is the smallest $\mathcal{P}$-primary ideal, take $0 \neq I/x^3D \in S$. Let $I/x^3D \subsetneqq \mathcal{P}^3$. Assume $I/x^3D \neq < 0_{D/x^3D} >$, then $x^3D \subsetneqq I \subsetneqq x^3\mathbb{Q}[[x]]$. By Example 2.9, I is of the form $x^3(< 1/2^s > +x\mathbb{Q}[[x]])$ for some $s \in \mathbb{Z}^+$. Assume $s = 1$, then $(4 + x^3D)((1/4)x^3 + x^3D) \in I/x^3D$, but $(4 + x^3D)^n, ((1/4)x^3 + x^3D) \notin I/x^3D$, for all $n \in \mathbb{Z}^+$. Hence I/x^3D is not primary. Let $I/x^3D =< 0_{D/x^3D} >$. Take $m = 2+x^3D, n = (1/2)x^3+x^3D \in D/x^3D$ such that $mn \in< 0_{D/x^3D} >$. However, neither m^k nor n is in $< 0_{D/x^3D} >$ for all $k \in \mathbb{Z}^+$, that is, $< 0_{D/x^3D} >$ is not primary. Then I/x^3D is not properly contained in $\mathcal{P}^3$. Since ideals of a chained ring are linearly ordered, we have $\mathcal{P}^3 \subseteq I/x^3D$. Thus $\mathcal{P}^3$ is the smallest element of S. Hence $\bigcap_{Q_\lambda \in S} Q_\lambda = \mathcal{P}^3$ and

$$\bigcap_{Q_\lambda \in S} Q_\lambda \neq \bigcap_{n=1}^{\infty} Q^n.$$

(4) Since $x\mathbb{Q}[[x]]$ is a prime ideal of D and $x^2D \subseteq x\mathbb{Q}[[x]]$, by Fact 3 we can say that $\mathcal{P} = x\mathbb{Q}[[x]]/x^2D$ is a prime ideal of D/x^2D. Similarly, by Fact 3, $\mathcal{P}^2$ is $\mathcal{P}$-primary ideal of D/x^2D. We also have $\mathcal{P} \neq \mathcal{P}^2$, so $\mathcal{P}$ is branched. Moreover, $< 0_{D/x^2D} >$ is not a prime ideal of D/x^2D that is

$$((1/2)x^2+x^2D)(2+x^2D) \in< 0_{D/x^2D} > \text{ where } ((1/2)x^2+x^2D), (2+x^2D) \notin< 0_{D/x^2D} > .$$

Let $\mathcal{N} \subsetneqq \mathcal{P}$ be a prime ideal. Then $\mathcal{N} \neq< 0_{D/x^2D} >$ and $\mathcal{N} = S/x^2D$ for some prime ideal S of D with $< 0_D >\neq x^2D \subsetneqq S \subsetneqq x\mathbb{Q}[[x]]$. But since D is a valuation ring, by parts (iii) and (iv) of Theorem 2.21, $< 0_D >= \bigcap_{k=1}^{\infty} x^{2k}\mathbb{Q}[[x]]$ is a prime ideal of D and there is no prime ideal between $< 0_D >$ and $x\mathbb{Q}[x]$. Hence there is no prime ideal $\mathcal{N}$ properly contained in $\mathcal{P}$.

Let $\mathcal{P} = x\mathbb{Q}[[x]]/xD$ which is a prime ideal of D/xD by Fact 3. We claim that $< 0_{D/xD} >$ is not a primary ideal and $\sqrt{< 0_{D/xD} >} = \mathcal{P}$. We have $(2 + xD)((1/2)x + xD) \in< 0_{D/xD} >$ where $(2 + xD)^k$ and $((1/2)x+xD) \in D/xD\setminus < 0_{D/xD} >$ for all $k \in \mathbb{Z}$. So, clearly, $< 0_{D/xD} >$ is not a primary ideal. Assume there exists a nonzero primary ideal Q of D/xD which is properly contained in $\mathcal{P}$. Then, by fact 3, $Q = I/xD$ for some primary ideal I of D such that $xD \subsetneqq I \subsetneqq x\mathbb{Q}[[x]]$. Then by Example 2.9, $I = x(< 1/2^s > +x\mathbb{Q}[[x]])$ for some $s \in \mathbb{Z}^+$. Since $2((1/2^{s+1})x) \in I$ where $2^k, ((1/2^{s+1})x) \in D \setminus I$ for all $k \in \mathbb{Z}^+$, any ideal of this form is not primary. So there is not a primary ideal properly contained in $\mathcal{P}$ that also means there is not a prime ideal properly contained in $\mathcal{P}$. Hence $\sqrt{< 0_{D/xD} >} = \mathcal{P}$, but $\mathcal{P}$ is not branched. □

Exercise 2.24 *[7, §17, Exercise 30] Let V be a valuation ring with maximal ideal $\mathcal{M}$ and value group, the group of divisibility of the valuation ring V, $G = K^*/U$ where K is the quotient field of V and U is the set of units of V. Prove that $\mathcal{M}$ is principal if and only if G contains a smallest strictly positive element.*

Solution. Let $\mathcal{M} = xV$ for some $x \in V$, clearly, x is not a unit in V that is $\mathcal{M} = xV \subsetneqq V$ implies $xU > U$ in G by Remark 2.1. Take $y \in V$ such that $yU > U$ that is $yV \subsetneqq V$ and $1/y \notin V$. Hence $y \in \mathcal{M}$ and $y = kx$ for some $k \in V$, then $y/x = r \in V$ that is $yV \subseteq xV$ and $yU \geq xU$ in G. Thus G has a smallest strictly positive element.

Conversely, assume $aU \in G$ such that for all $xU > U$ in G, $xU \geq aU$, then clearly $aV \subsetneqq V$ and $a \in \mathcal{M}$. Take any $y \in \mathcal{M}$. Since y is nonunit in V and $yU > U$, by assumption, we have $yU \geq aU$. Hence $yV \subseteq aV$ and $\mathcal{M} = aV$. □

Exercise 2.25 *[7, §17, Exercise 13] Let V be a nontrivial valuation ring on the field L and assume that $V = K + \mathcal{M}$, where K is a subfield of L and $\mathcal{M}$ is the maximal ideal of V. Let D be a proper subring of K, and let $D_1 = D + \mathcal{M}$. Then prove:*

(1) If N is a multiplicative system in D, then $(D_1)_N = D_N + \mathcal{M}$. If $\mathcal{P}$ is a prime ideal in D_1 and if $\mathcal{P} \subset \mathcal{M}$, then $(D_1)_{\mathcal{P}} = V_{\mathcal{P}}$ so that $(D_1)_{\mathcal{P}}$ is a valuation ring.

(2) D_1 is a valuation ring if and only if D is a valuation ring on K.

Solution. Clearly, $K \cap \mathcal{M} = \{0\}$. Then $D \cap \mathcal{M} = \{0\}$ and any element $d \in D_1$ can uniquely be represented as $d = r + m$ where $r \in D$ and $m \in \mathcal{M}$.

(1) Let $(r + m)/s \in (D_1)_N$ where $r \in D$, $m \in \mathcal{M}$ and $0 \neq s \in N \subseteq D$, then $(r + m)/s = r/s + m/s \in D_N + \mathcal{M}$ since $0 \neq s \in D \subset K$, $1/s \in K$, $m/s \in \mathcal{M} = V\mathcal{M} = K\mathcal{M}$ for any $m \in \mathcal{M}$ that is $(D_1)_N \subseteq D_N + \mathcal{M}$

On the other hand, take $a/s+m \in D_N+\mathcal{M}$ where $a \in D$, $s \in N$ and $m \in M$, then $a/s + m = (a + ms)/s \in (D_1)_N$ since $\mathcal{M}$ is an ideal of V and $s \in D \subset V$. Thus equality holds.

Let $\mathcal{P}$ be a prime ideal of D_1 properly contained in $\mathcal{M}$, clearly $(D_1)_{\mathcal{P}} \subseteq V_{\mathcal{P}}$. To show the equality, take $\alpha \in V_{\mathcal{P}}$. Since $\mathcal{P} \subset \mathcal{M}$, there exists $n \in \mathcal{M} - \mathcal{P}$. So for any $v \in V$, $vn \in \mathcal{M}$. Then $\alpha = v/s = vn/sn \in \mathcal{M}(D_1)_{\mathcal{P}} \subseteq (D_1)_{\mathcal{P}}$, where $v \in V$ and $s \in D_1 - \mathcal{P}$. Hence $(D_1)_{\mathcal{P}}$ is a valuation ring.

(2) Assume D_1 is a valuation ring on L. Take a nonzero element k of K. Then k or $k^{-1} \in D_1$. If $k \in D_1$, $k = d + m$ for some $d \in D$ and $m \in \mathcal{M}$. This implies that $k - d = m \in K \cap \mathcal{M} = \{0\}$, hence $k \in D$. If $k^{-1} \in D_1$, then $k^{-1} \in D$ in a similar way, that is, D is a valuation ring on K. Let D be a valuation ring on K and let $0 \neq l \in L$. Since V is a valuation ring, we have

$l \in V$ or $l^{-1} \in V$. Then $l = k + m$ or $l^{-1} = k + m$ where $k \in K$ and $m \in \mathcal{M}$. Moreover, since D is a valuation ring, k or $k^{-1} \in D$. Assume $k \in D$, then clearly, l or $l^{-1} \in D_1$. Assume $k^{-1} \in D$ that is $k \neq 0$. Then for the first case $l^{-1} = 1/(k+m) = 1/k - m/(k+m) \in D_1$, since $(k+m) \notin \mathcal{M}$ implies it is a unit in V then $m/(k+m) \in \mathcal{M} = V\mathcal{M}$. Similarly, $l^{-1} \in V$ and $k^{-1} \in D$ implies $l = 1/(k+m) \in D_1$. Thus D_1 is a valuation ring. $\square$

Exercise 2.26 *[7, §20, Exercise 11] If $p(x) = ax + b$ is a polynomial in $K[x]$ of degree 1 where K is a field, prove that the valuation ring $V = K[x]_{<p(x)>}$ is the sum of K and the maximal ideal of V. The valuation ring $K[[x]]$ is of the same form.*

Solution. First, we will show that $p(x)V$ is the maximal ideal of V, that is, $V - p(x)V$ is the set of units of V. Since $p(x)$ is irreducible in $K[x]$ and $K[x]$ is a unique factorization domain, $p(x)$ is a prime element in $K[x]$ and any $\alpha \in V$ has a unique formal representation such that $\alpha = f(x)/g(x)$ where $f(x), g(x) \in K[x]$, $p(x) \nmid g(x)$ and $(f(x), g(x)) = 1$. Now, assume $\beta \in V$ is a unit with the formal representation $f(x)/g(x)$, then $\alpha^{-1} = g(x)/f(x) \in V$ and $p(x) \nmid f(x)$, therefore $\alpha \in V - p(x)V$. To show the equality, take $\gamma \in V - p(x)V$ where $\gamma = h(x)/g(x)$ formally represented, that is, $p(x) \nmid h(x)$ and $\gamma^{-1} \in V$. Hence $p(x)V$ is the unique maximal ideal of V and V is a valuation ring with the quotient field $F = \{f(x)/g(x) | 0 \neq g(x), f(x) \in K[x]\}$.

Secondly, we prove that $V = K + p(x)V$. It is easy to see that $K + p(x)V \subseteq V$. To prove the converse, take a formally represented element $\alpha = f(x)/g(x)$ of V. Then by division algorithm, $f(x) = p(x)f_1(x) + r$ and $g(x) = p(x)g_1(x) + s$, where $f_1(x), g_1(x), r, s \in K[x]$, $0 \leq deg(r(x)), deg(s(x)) < deg(p(x)) = 1$, so

$r, 0 \neq s \in K$. Therefore

$$\frac{f(x)}{g(x)} = \frac{p(x)f_1(x)}{g(x)} + \frac{r}{g(x)} = (rs^{-1}) + \frac{(f_1(x) - rs^{-1}g_1(x))p(x)}{g(x)} \in K + p(x)V.$$

□

Exercise 2.27 *[7, §19, Exercise 3] Prove that* $\{\mathbb{Z}_{<p>} | p \text{ is prime } \}$ *is the set of nontrivial valuation rings on* $\mathbb{Q}$.

Solution. Clearly, $\mathbb{Z}_{<p>} = \{\alpha = a/b \in \mathbb{Q} | a, b \in \mathbb{Z}, p \nmid b\}$ is a valuation ring on $\mathbb{Q}$ with unique maximal ideal $p\mathbb{Z}_{<p>}$.

Let $(V, \mathcal{M})$ be a nontrivial valuation ring on $\mathbb{Q}$. By definition, V is an integral domain with identity and $V \cap \mathbb{Z}$ is a nonzero subring of $\mathbb{Z}$ containing identity. That is $V \cap \mathbb{Z} = n\mathbb{Z}$ where $n \in \mathbb{Z}$ and $1 \in n\mathbb{Z}$. Then $n = \pm 1$, $\mathbb{Z} \subseteq V$. Moreover, $\mathcal{M} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. If $\mathcal{M} \cap \mathbb{Z} =< 0 >$, then $V = \mathbb{Q}$ which contradicts that V is nontrivial. So $\mathcal{M} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime integer p. This implies $p\mathbb{Z} \subseteq \mathcal{M}$, where $\mathcal{M}$ is the set of nonunits of V.

Claim: $\mathcal{M} = p\mathbb{Z}_p$ where $p\mathbb{Z}_p := \{\alpha = a/b \in \mathbb{Q} | a, b \in \mathbb{Z}, p|a, p \nmid b\}$.

Take $0 \neq \alpha = a/b \in \mathcal{M}$ where $a, b \in \mathbb{Z}$ and $(a, b) = 1$. Since $a = b.(a/b) \in \mathcal{M} \cap \mathbb{Z} = p\mathbb{Z}$ and $(a, b) = 1$, $p|a$ and $p \nmid b$. Thus $\mathcal{M} \subseteq S$. On the other hand, take $\beta = x/y \in S$. By definition, $p|x$ and $p \nmid y$ in $\mathbb{Z}$ and $x = y.(x/y) \in p\mathbb{Z} \subseteq \mathcal{M}$. Since $\mathcal{M}$ is prime and $y \notin \mathcal{M} \cap \mathbb{Z} = p\mathbb{Z}$, $x/y \in \mathcal{M}$. Hence $\mathcal{M} = p\mathbb{Z}_p$.

Take $\alpha = a/b \in \mathbb{Q}$ where $a, b \in \mathbb{Z}$ and $(a, b) = 1$. $\alpha \notin V$ if and only if $\alpha^{-1} = b/a \in \mathcal{M}$, since V is a valuation ring on $\mathbb{Q}$ and $\mathcal{M}$ is the set of nonunits of V. Thus, we have

$$Q \setminus V = \{\alpha = a/b \in \mathbb{Q} | a, b \in \mathbb{Z}, p|b, p \nmid a\}$$

which is equivalent to

$$V = \{\alpha = a/b \in \mathbb{Q} | a, b \in \mathbb{Z}, p \nmid b\} = \mathbb{Z}_{<p>}.$$

$\square$

Exercise 2.28 *[7, §19, Exercise 5] Let V be a valuation ring on a field K and let L be an extension of K. Prove that there is a valuation ring W on L such that $W \cap K = V$.*

Solution. Let V be a valuation ring on K with unique maximal ideal $\mathcal{M}$ and let $\mathcal{F} = \{S | V \subseteq S \subseteq L, S \text{ is a subring of } L, \mathcal{MS} \neq \mathcal{S}\}$ where $\mathcal{M}S$ is an ideal of S generated by $\mathcal{M}$ in S.

Clearly, $\mathcal{F} \neq \emptyset$ such that $V \in \mathcal{F}$, since V is a subring of K and L is an extension of K, V is a subring of L and $\mathcal{M}V = \mathcal{M} \neq V$. $\mathcal{F}$ is partially ordered with respect to inclusion. Let $\mathcal{H}$ be a nonempty totally ordered subset of $\mathcal{F}$.

Claim 1: $T = \bigcup_{S \in \mathcal{H}} S$ is an upper bound for $\mathcal{H}$.

Clearly, T is a ring and $V \subseteq T \subseteq L$. Assume $\mathcal{M}T = T$, then $1 = \sum_{i=1}^{n} a_i t_i$ where $a_i \in \mathcal{M}$ and $t_i \in T$. Since $\mathcal{H}$ is totally ordered, there exists $S_0 \in \mathcal{H}$ such that $t_i \in S_0$ for $i = 1, ..., n$. So $\mathcal{M}S_0 = S_0$ which contradicts that $S_0 \in \mathcal{F}$. Thus, $\mathcal{M}T \neq T$ and $T \in \mathcal{F}$. By construction, T is an upper bound for $\mathcal{H}$ in $\mathcal{F}$.

By Zorn's Lemma, $\mathcal{F}$ has a maximal element W, such that $R \subseteq W \subseteq L$, W is a subring of L, $\mathcal{M}W \neq W$ and W is maximal with respect to these properties.

Claim 2: W is a valuation ring on L.

W is a proper subring of L, since $\mathcal{M}W \neq W$. Assume there exist $0 \neq x \in L$ such that $x \notin W$ and $x^{-1} \notin W$, then $W[x]$ and $W[x^{-1}]$ are subrings of L. Since W is maximal with respect to the given properties, then $\mathcal{M}W[x] = W[x]$ and $\mathcal{M}W[x^{-1}] = W[x^{-1}]$. That is

$$1 = a_0 + \cdots + a_n x^n \ (1) \text{ and } 1 = b_0 + \cdots + b_m x^{-m} \ (2),$$

where n, m are minimal. So $a_0 \neq 1, a_n \neq 0$, $b_0 \neq 1$ and $b_m \neq 0$. Assume $n \geq m$. Multiply (1) by $(1 - b_0)$ and (2) by $a_n x^n$, we have

$$(1-b_0) = a_0(1-b_0) + \cdots + a_n(1-b_0)x^n \ (3) \text{ and } 0 = a_n(b_0-1)x^n + \cdots + a_n b_m x^{n-m} \ (4)$$

Summation of (3) and (4) gives $1 = (a_n b_1 + a_{n-1}(1-b_0))x^{n-1} + \cdots + (a_0 - a_0 b_0 + b_0)$ where not all the coefficient of x^i are zero and this contradicts the minimality of n. Thus, x or $x^{-1} \in W$ and W is a valuation ring on L.

Claim 3: $W \cap K = V$.

Clearly, $V \subseteq W \cap K$. Assume $W \cap K \nsubseteq V$ such that there exist $a \in W \cap K$ and $a \notin V$. Then $1/a \in V$ is nonunit. That is $1/a \in \mathcal{M}$, $1 = (1/a)a \in \mathcal{M}W$ and $\mathcal{M}W = W$, which contradicts $W \in \mathcal{F}$. Thus, $W \cap K \subseteq V$ and equality holds. □

Exercise 2.29 *[7, §19, Exercise 15] If R is a subring of the ring S, we say that R has property (C) with respect to S if each ideal of R is the contraction of an ideal of S.*

1. *The following are equivalent:*

(a) R has property (C) with respect to S.

(b) For each ideal A of R, $A = A^{ec}$; here e and c respective denotes the extension and contraction of ideals.

(c) For every finitely generated ideal A of R, $A = A^{ec}$.

2. *Assume that S is a subring of the ring T. If R has property (C) with respect to T, then R has property (C) with respect to S. If R has property (C) with respect to S and S has property (C) with respect to T, then R has property (C) with respect to T.*

3. *R has property (C) with respect to S if and only if R has property (C) with respect to S_i for each intermediate ring S_i which is a finitely generated ring extension of R.*

Solution.

(1) $(a) \Rightarrow (b)$ Let R has property (C) with respect to S, then there exist an ideal I of J for any ideal A of R such that $A = I^c$ that is $A^e = I^{ce}$. Using an elementary proof, it can be shown that $I^{cec} = I^c$. Hence

$$A = I^c = I^{cec} = (I^c)^{ec} = A^{ec} \text{ for any ideal } A \text{ of } R.$$

$(b) \Rightarrow (c)$ is clear.

$(c) \Rightarrow (a)$ Let $A = A^{ec}$ for any finitely generated ideal A of R. Let I be an ideal of R, then clearly, $I \subseteq IS \cap R$. Take $m \in IS \cap R$ such that $m = \sum_{i=1}^{n} s_i x_i$ where $s_i \in S$ and $x_i \in I$ for all i. Then $I_1 = \sum_{i=1}^{n} Rx_i$ is a finitely generated ideal of R which is contained in I and by assumption, $I_1 = I_1 S \cap R$. Since $m \in I_1 S \cap R$, $m \in I_1 \subseteq I$ and hence $I = IS \cap R$.

(2) Assume R has property (C) with respect to T, that is $I = IT \cap R$ for any ideal I of R by part (1). Then $IT \cap S$ is an ideal of S and $I = IT \cap R = IT \cap (S \cap R) = (IT \cap S) \cap R$ for all ideal I of R. To prove the second statement, assume $I = IS \cap R$ and $J = JT \cap S$ for any ideal I of R and J of S. Since IS is an ideal of S for any ideal I of R, $IS = IT \cap S$ and $I = (IT \cap S) \cap R = IT \cap (S \cap R) = IT \cap R$.

(3) The necessity follows from part (2). Let $I = IS_i \cap R$ for any ideal I of R where S_i is an intermediate ring such that $S_i = R[m_{i1}, ..., m_{in_i}]$ where $n_i \in \mathbb{Z}^+$. It is easily seen that $I \subseteq IS \cap R$ for any ideal I of R. Take $\alpha \in IS \cap R$ such that $\alpha = \sum_{i=1}^{n} s_i x_i$ where $s_i \in S$ and $x_i \in I$ for all i. Then $I_1 S_1 = \sum_{i=1}^{n} S_1 x_i$ is an ideal of the intermediate ring $S_1 = R[s_1, ..., s_n]$ containing α where $I_1 =< x_1, ..., x_n >$ is an ideal of R contained in I. Hence, by assumption, $\alpha \in I_1 S_1 \cap R = I_1 \subseteq I$.Thus, $I = IS \cap R$ and by part (1), R has property C with respect to S. $\square$

Exercise 2.30 *[7, §19, Exercise 16] Assume that J is an integral domain with identity and that D is a subring of J with identity.*

(1) If D has property (C) with respect to J and if N is a multiplicative system in D, then D_N has property (C) with respect to J_N.

(2) If $\{\mathcal{M}_\lambda\}_{\lambda \in \Lambda}$ is the family of maximal ideals of D and if for each $\lambda \in \Lambda$, $D_{\mathcal{M}_\lambda}$ has property (C) with respect to $J_{D \setminus \mathcal{M}_\lambda}$, then D has property (C) with respect to J.

(3) Each principal ideal of D is the contraction of an ideal of J if and only if $J \cap K = D$ where K is the quotient ring of D.

(4) If D is a Bezout domain, then D has property (C) with respect to J if and only if $J \cap K = D$.

Solution. (1) Let M be an ideal of D_N, then M is of the form ID_N where $I = M^c$ is an ideal of D and $I = IJ \cap D$, by assumption. So we should prove that $(IJ \cap D)D_N = IJ_N \cap D_N$. Clearly, $(IJ \cap D)D_N \subseteq IJ_N \cap D_N$. Take $\alpha = a/s \in IJ_N \cap D_N$ where $s \in N$ and $a \in IJ$. Since $\alpha \in D_N$, there exists $n \in N$ such that $an \in D$ that is $an \in D \cap IJ$ and $\alpha = an/sn \in (D \cap IJ)D_N$ and the equality follows.

(2) Let I be an ideal of D, then by Remark 1.10, $I = \bigcap\limits_{\lambda \in \Lambda} ID_{\mathcal{M}_\lambda}$ and $ID_{\mathcal{M}_\lambda} = IJ_{D \setminus \mathcal{M}_\lambda} \cap D_{\mathcal{M}_\lambda}$ for all $\lambda \in \Lambda$ by assumption. Thus

$$I = \bigcap_{\lambda \in \Lambda} ID_{\mathcal{M}_\lambda} = \bigcap_{\lambda \in \Lambda} (IJ_{D \setminus \mathcal{M}_\lambda} \cap D_{\mathcal{M}_\lambda}) = (\bigcap_{\lambda \in \Lambda} IJ_{D \setminus \mathcal{M}_\lambda}) \cap \bigcap_{\lambda \in \Lambda} D_{\mathcal{M}_\lambda}$$

$$= (\bigcap_{\lambda \in \Lambda} IJ_{D \setminus \mathcal{M}_\lambda}) \cap D = (\bigcap_{\lambda \in \Lambda} IJ_{D \setminus \mathcal{M}_\lambda}) \cap J \cap D,$$

where $(\bigcap\limits_{\lambda \in \Lambda} IJ_{D \setminus \mathcal{M}_\lambda}) \cap J$ is an ideal of J. Thus D has property (C) with respect to J.

(3) Let $Dx = Jx \cap D$ for all $x \in D$ and let $a/b \in J \cap K$ such that $a, 0 \neq b \in D$, then $a \in Db = Jb \cap D$ that is $a = db$ for some $d \in D$ and $a/b = db/b = d \in D$. Thus $J \cap K \subseteq D$ and the other inclusion is clear and equality holds.

Conversely, let $J \cap K = D$. Take $m \in Jx \cap D$ for some nonzero $x \in D$ that is $m = \alpha x$ for some $\alpha \in J$. Then $\alpha = m/x \in J \cap K = D$ and $m \in Dx$. Thus clearly $Dx = Jx \cap D$ for any nonzero $x \in D$. If $x = 0$, the result is clear. So we are done.

(4) Let the Bezout domain D have property (C), then $Dx = Jx \cap D$ for all $x \in D$ and the result follows from part (3).

Conversely assume $D = J \cap K$ and I is a finitely generated ideal of D that is $I = Dx$ for some $x \in D$. Then $I = Jx \cap D$ by part (3) and D has property (C) by part (1) of Exercise 2.29. $\square$

2.3 Structure of Prüfer Domains

Theorem 2.31 *[7, Theorem 22.1] Let D be an integral domain with identity. Then the following are equivalent:*

(i) $D_{\mathcal{P}}$ is a valuation ring for each proper prime ideal $\mathcal{P}$ of D.

(ii) $D_{\mathcal{M}}$ is a valuation ring for each maximal ideal $\mathcal{M}$ of D.

(iii) Each nonzero finitely generated ideal of D is invertible.

(iv) Each nonzero ideal of D with a basis of two elements is invertible.

Proof. $(i) \Rightarrow (ii)$ and $(iii) \Rightarrow (iv)$ are clear.

$(ii) \Rightarrow (iii)$ Let $\{\mathcal{M}_\lambda | \lambda \in \Lambda\}$ be the set of maximal ideals of D. If A is a nonzero finitely generated ideal of D, then $AD_{\mathcal{M}_\lambda}$ is a finitely generated ideal of the valuation ring $D_{\mathcal{M}_\lambda}$. Therefore $AD_{\mathcal{M}_\lambda}$ is principal for each $\lambda \in \Lambda$. Then A is invertible by Theorem 1.17 and Proposition 1.18.

$(iv) \Rightarrow (i)$ We will show that $D_{\mathcal{P}}$ is a valuation ring by showing that each pair of principal ideals of $D_{\mathcal{P}}$ compares under inclusion. If x, y are two nonzero elements of $D_{\mathcal{P}}$ such that $x = x_1/s_1$, $y = y_1/s_2$ where $x_1, y_1 \in D$, $s_1, s_2 \in D \setminus \mathcal{P}$. Then $xD_{\mathcal{P}} = x_1 D_{\mathcal{P}}$, $yD_{\mathcal{P}} = y_1 D_{\mathcal{P}}$. Since (iv) holds, $< x_1, y_1 >$ is invertible in D. By Theorem 1.17, $< x_1, y_1 > D_{\mathcal{P}}$ is invertible and Proposition 1.18 shows that $< x_1, y_1 > D_{\mathcal{P}}$ is either $x_1 D_{\mathcal{P}}$ or $y_1 D_{\mathcal{P}}$. Let's say $< x_1, y_1 > D_{\mathcal{P}} = x_1 D_{\mathcal{P}}$, then $yD_{\mathcal{P}} \subseteq xD_{\mathcal{P}}$ so that (i) holds. $\square$

Definition 2.32 *A domain satisfying the equivalent conditions of Theorem 2.31 is called a* *Prüfer domain.*

Remark 2.33 *[7, Proposition 5.8] Let N be a multiplicative system in the ring R and let A be an ideal of R disjoint from N. Then $R_N/A^e \cong (R/A)_{(N+A)/A}$ where A^e denotes the extension of A with respect to R_N.*

Proof. By definition, $(R/A)_{(N+A)/A}$ is the quotient ring of $(R/A)/(C/A)$ with respect to the multiplicative system $N_1 = \{(n+A)+(C/A)|n \in N\}$ where C is an ideal of R consisting of all elements x such that $xn \in A$ for some $n \in N$. Hence $C = A^{ec}$, extension and contraction being with respect to R_N. Further, N_1 is regular in $(R/A)/(C/A)$. Define

$$\begin{aligned} \phi : \quad (R/A)/(C/A) &\rightarrow R/C \\ x + A + (C/A) &\rightarrow x + C \end{aligned}$$

Clearly, ϕ is an isomorphism and $\phi(N_1) = \{n + C|n \in N\} = (N+C)/C$. Therefore, $(R/A)_{(N+A)/A} \cong (R/C)_{(N+C)/C} = \{(r+C)/(n+C)|r \in R, n \in N\}$.

If we define B such that $B = \{x \in R|0 \in xN\}$, then by definition, $R_N = \{(r+B)/(n+B)|r \in R, n \in N\}$. Define

$$\begin{aligned} \theta : R_N \qquad &\longrightarrow \quad (R/C)_{(N+C)/C} \\ (r+B)/(n+B) &\rightarrow \quad (r+C)/(n+C) \end{aligned}$$

Since $B \subseteq C$, θ is well defined, and clearly, θ is a homomorphism and

$$ker\theta = \{(c+B)/(n+B)|c \in C\} = C^e = A^{ece} = A^e.$$

Therefore $R_N/A^e \cong (R/C)_{(N+C)/C} \cong (R/A)_{(N+A)/A}$. $\square$

Proposition 2.34 *[7, Proposition 22.5] Let D be a Prüfer Domain, let S be a multiplicative system in D, and let $\mathcal{P}$ be a proper prime ideal of D. Then D_S and $D/\mathcal{P}$ are Prüfer domains.*

Proof. If $\mathcal{Q}$ is a prime ideal of D_S, then $\mathcal{Q} = \mathcal{M}D_S$ for some prime ideal $\mathcal{M}$ of D with $\mathcal{M} \cap S = \emptyset$. Therefore $(D_S)_{\mathcal{Q}} = (D_S)_{\mathcal{M}D_S} = D_{\mathcal{M}}$ is a valuation ring, since D is a Prüfer domain. Hence D_S is a Prüfer domain.

Similarly each proper prime ideal of $D/\mathcal{P}$ is of the form $\mathcal{M}/\mathcal{P}$ for some proper prime $\mathcal{M}$ of D containing $\mathcal{P}$. Further Proposition 2.33 shows that $(D/\mathcal{P})_{\mathcal{M}/\mathcal{P}} = D_{\mathcal{M}}/\mathcal{P}^e$. Since D is Prüfer, $D_{\mathcal{M}}$ is a valuation ring. It follows that $D/\mathcal{P}$ is Prüfer. □

Lemma 2.35 *[7, Lemma 23.1] Let R be a ring with identity, let $\{\mathcal{M}_\lambda\}_{\lambda\in\Lambda}$ be the set of maximal ideals of R, and for all $\lambda \in \Lambda$, let e_λ and c_λ, respectively denote extension and contraction of ideals of R to $R_{\mathcal{M}_\lambda}$. If A is an ideal of R with prime radical P, and if A^{e_λ} is $\mathcal{P}^{e_\lambda}$-primary for all $\lambda \in \Lambda$, then A is $\mathcal{P}$-primary.*

Proof. We let that Q be the isolated $\mathcal{P}$-primary component of A; Q is the unique minimal $\mathcal{P}$-primary ideal of R containing A. But by hypothesis, $A^{e_\lambda c_\lambda}$ is $\mathcal{P}$-primary for each λ such that $P \subseteq \mathcal{M}_\lambda$, and if $A \nsubseteq \mathcal{M}_\lambda$, then $A^{e_\lambda c_\lambda} = R$. Therefore, $Q \subseteq \bigcap_{\lambda\in\Lambda} A^{e_\lambda c_\lambda} = A$ by Remark 1.10, so that $A = Q$ and A is $\mathcal{P}$-primary. □

Lemma 2.36 *[7, Lemma 23.2] Let $A =< a_1, ..., a_n >$ be an invertible ideal of the commutative ring R with identity. If $\mathcal{P}$ is a minimal prime ideal of A, then $\mathcal{P}$ is a minimal prime of one of the principal ideals $< a_1 >, ..., < a_n >$.*

Proof. Clearly $\sqrt{AR_{\mathcal{P}}} = \mathcal{P}R_{\mathcal{P}}$. Since $AR_{\mathcal{P}}$ is invertible, it is principal and equal to $< (a_i/1) >$ for some i, by Proposition 1.18. Then $\mathcal{P}R_{\mathcal{P}}$ is a minimal prime of $< (a_i/1) >$, and it follows that $\mathcal{P}$ is a minimal prime of $< a_i >$. □

Theorem 2.37 *[7, Theorem 23.3] Let $\mathcal{P}$ be a nonzero proper prime ideal of the Prüfer Domain D.*

(i) If Q is $\mathcal{P}$-primary and if $x \in D \setminus \mathcal{P}$, then $Q = Q[Q+ < x >]$. If Q is finitely generated, $\mathcal{P}$ is a maximal ideal in D.

(ii) If $S = \{Q_\lambda | \lambda \in \Lambda\}$ is the set of $\mathcal{P}$-primary ideals, then S is closed under multiplication. In particular, $\{P^k\}_{k=1}^{\infty} \subseteq S$. If $\mathcal{P} \neq \mathcal{P}^2$, then $S = \{\mathcal{P}^k\}_{k=1}^{\infty}$.

(iii) If $\mathcal{P}$ is branched and if Q is $\mathcal{P}$-primary, $Q \neq \mathcal{P}$, then $\bigcap\limits_{n=1}^{\infty} Q^n = \bigcap\limits_{\lambda \in \Lambda} Q_\lambda$.

(iv) $\mathcal{P}_0 = \bigcap\limits_{\lambda \in \Lambda} Q_\lambda$ is a prime ideal of D, and there are no prime ideals of V properly between $\mathcal{P}_0$ and $\mathcal{P}$.

(v) The following conditions are equivalent:

(a) $\mathcal{P}$ is branched.

(b) There is an ideal $A \neq \mathcal{P}$ such that $\mathcal{P} = \sqrt{A}$.

(c) $\mathcal{P}$ is a minimal prime of a principal ideal.

(d) $\mathcal{P}$ is a minimal prime of a finitely generated ideal.

(e) $\mathcal{P}$ is not the union of the set of primes of D properly contained in $\mathcal{P}$.

(f) There is a prime ideal M properly contained in $\mathcal{P}$ such that there are no primes of D properly between M and $\mathcal{P}$.

Proof.

(i) To show that $Q = Q(Q+ < x >)$, it is sufficient to show that $QD_{\mathcal{M}} = (Q^2 + Q < x >)D_{\mathcal{M}}$ for each maximal ideal $\mathcal{M}$ of D. If $Q \nsubseteq \mathcal{M}$, then $QD_{\mathcal{M}} = Q^2 D_{\mathcal{M}} = D_{\mathcal{M}}$. If $Q \subseteq \mathcal{M}$, then $QD_{\mathcal{M}}$ is $\mathcal{P}D_{\mathcal{M}}$-primary, where $D_{\mathcal{M}}$ is a valuation ring and where $x \notin \mathcal{P}D_{\mathcal{M}}$. By part (i) of Theorem 2.21,

$QD_{\mathcal{M}} = Q < x > D_{\mathcal{M}}$. And since $Q^2 \subseteq Q$, $QD_{\mathcal{M}} = [Q^2 + Q < x >]D_{\mathcal{M}}$. Hence, $Q = Q[Q+ < x >]$.

If Q is finitely generated, Q is a cancelation ideal, then $Q = Q[Q+ < x >]$ implies $D = Q+ < x >$ for all $x \in D \setminus P$. Therefore, $\mathcal{P}+ < x >= D$ for all $x \in D \setminus \mathcal{P}$, and $\mathcal{P}$ is maximal.

(ii) If $Q_1, Q_2 \in S$ and if $\mathcal{M}$ is a maximal ideal of D and $\sqrt{Q_1Q_2} = \sqrt{\sqrt{Q_1}\sqrt{Q_2}} = \sqrt{\mathcal{P}^2} = \mathcal{P}$, then $(Q_1D_{\mathcal{M}})(Q_2D_{\mathcal{M}}) = Q_1Q_2D_{\mathcal{M}}$ is $\mathcal{P}D_{\mathcal{M}}$-primary, by Theorem 2.21. Since Q_1Q_2 has radical $\mathcal{P}$, Q_1Q_2 is $\mathcal{P}$-primary by Lemma 2.35, that is, S is closed under multiplication. If $\mathcal{P} \neq \mathcal{P}^2$, then $\mathcal{P}D_{\mathcal{P}} \neq \mathcal{P}^2D_{\mathcal{P}}$, since $\mathcal{P}^2$ is $\mathcal{P}$-primary and $\mathcal{P}^2 = \mathcal{P}^2D_{\mathcal{P}} \cap D$. Hence $\{\mathcal{P}^kD_{\mathcal{P}}\}_{k=1}^{\infty}$ is the set of $\mathcal{P}D_{\mathcal{P}}$-primary ideals of $D_{\mathcal{P}}$ implies $\{\mathcal{P}^kD_{\mathcal{P}} \cap D\}_{k=1}^{\infty} = \{\mathcal{P}^k\}_{k=1}^{\infty}$ is the set of $\mathcal{P}$-primary ideals of D.

(iii) Since $Q_\lambda = Q_\lambda D_{\mathcal{P}} \cap D$ for all $\lambda \in \Lambda$, this part follows from (iii) of Theorem 2.21.

(iv) Similarly, this part follows from (iv) of Theorem 2.21.

(v) We note that $\mathcal{P}$ is branched if and only if $\mathcal{P}D_{\mathcal{P}}$ is branched, that $\mathcal{P}$ is the union of set of primes if and only if this property holds for $\mathcal{P}D_{\mathcal{P}}$ and that there is a prime ideal $M \subset \mathcal{P}$ such that there no primes between M and $\mathcal{P}$ if and only if the same holds for $\mathcal{P}D_{\mathcal{P}}$. Hence condition (a),(e) and (f) are equivalent by Theorem 2.21.

Clearly, (a) implies (b) and (c) implies (d). By Lemma 2.36 (d) implies (c).

$(c) \Leftrightarrow (e)$ This equivalence holds in any ring. One side of this implication is clear. To prove the other side, let (c) holds, where $\mathcal{P}$ is a minimal prime of the principal ideal $< x >$. Then there are no primes between $\mathcal{P}$ and $< x >$ so that any prime ideal contained in $\mathcal{P}$ does not contain x. Hence $\mathcal{P}$ is not the union of the set of primes which it contains properly.

$(b) \Rightarrow (a)$ Since $A \subset \mathcal{P}$, there is a maximal ideal $\mathcal{M}$ of D containing $\mathcal{P}$ such that $AD_{\mathcal{M}} \subset \mathcal{P}D_{\mathcal{M}}$. Further, $\mathcal{P}D_{\mathcal{M}} = \sqrt{AD_{\mathcal{M}}}$. Theorem 2.21 shows that $\mathcal{P}D_{\mathcal{M}}$ is branched, and consequently, $\mathcal{P}$ is branched. $\square$

Exercise 2.38 *[7, §23, Exercise 8]Assume that $R_{\mathcal{M}}$ is a chained ring for each maximal ideal $\mathcal{M}$ of R. Consider the analogs of parts (i) and (v) of Theorem 2.37 for the ring R. Prove*

(i') If Q is a $\mathcal{P}$-primary ideal of R and if $x \in R \setminus \mathcal{P}$, then $Q = Q[Q+ < x >]$. If Q is regular and finitely generated, then $\mathcal{P}$ is maximal in R

(v') For a nonzero proper prime ideal $\mathcal{P}$ of R, prove that the following implications hold among the six conditions of part (v) of Theorem 2.37: $(f) \Rightarrow (a) \Rightarrow (b) \Rightarrow (c) \Leftrightarrow (d) \Leftrightarrow (e)$.

Solution.

(i') We will prove that $QR_{\mathcal{M}} = Q[Q+ < x >]R_{\mathcal{M}}$ for each maximal ideal $\mathcal{M}$ of R. If $Q \nsubseteq \mathcal{M}$, $QR_{\mathcal{M}} = Q^2R_{\mathcal{M}} = R_{\mathcal{M}} \subseteq (Q^2 + Q < x >)R_{\mathcal{M}} \subseteq R_{\mathcal{M}}$ implies $QR_{\mathcal{M}} = (Q^2 + Q < x >)R_{\mathcal{M}}$. If $Q \subseteq \mathcal{M}$, then $QR_{\mathcal{M}}$ is $\mathcal{P}R_{\mathcal{M}}$-primary ideal of the chained ring $R_{\mathcal{M}}$.

$$QR_{\mathcal{M}} \subseteq \mathcal{P}R_{\mathcal{M}} \subseteq < x >, \text{ since } x \notin \mathcal{P}R_{\mathcal{M}}.$$

Then for all $\alpha \in QR_{\mathcal{M}}$, $\alpha = rx$, for some $r \in R_{\mathcal{M}}$. Let $I = \{r \in R_{\mathcal{M}} | rx \in QR_{\mathcal{M}}\}$. Clearly, I is an ideal of $R_{\mathcal{M}}$ and $I < x > = QR_{\mathcal{M}}$. Since $QR_{\mathcal{M}}$ is $\mathcal{P}R_{\mathcal{M}}$-primary,

$kx \in QR_{\mathcal{M}}$ and $x \notin \mathcal{P}R_{\mathcal{M}}$ for all $k \in I$ implies $k \in QR_{\mathcal{M}}$. Hence $I \subseteq QR_{\mathcal{M}} = I < x > \subseteq I$ implies $Q < x > R_{\mathcal{M}} = QR_{\mathcal{M}}$. Since $Q^2R_{\mathcal{M}} \subseteq QR_{\mathcal{M}}$, $QR_{\mathcal{M}} = Q[Q+ < x >]R_{\mathcal{M}}$. Thus $Q = Q[Q+ < x >]$.

Moreover if Q is finitely generated and regular, then we will show that $QR_{\mathcal{M}}+ < x >= R_{\mathcal{M}}$ for each maximal ideal $\mathcal{M}$ of R. If $Q \nsubseteq \mathcal{M}$, result is clear. Let $Q \subseteq \mathcal{M}$. then $QR_{\mathcal{M}}$ is finitely generated, regular and proper ideal of $R_{\mathcal{M}}$. Since $R_{\mathcal{M}}$ is a chained ring, $QR_{\mathcal{M}}$ is principal by Exercise 2.17. Thus by Remark 1.3,

$$QR_{\mathcal{M}} =< \alpha > \text{ for regular } \alpha \in R_{\mathcal{M}}.$$

Then $QR_{\mathcal{M}} = Q[Q+ < x >]R_{\mathcal{M}}$ implies $< \alpha >=< \alpha > [< \alpha > + < x >]$ that is $\alpha(1-\beta) = 0$ for some $\beta \in (< \alpha > + < x >)$. Since α is regular, that means $\beta = 1$. Hence

$$QR_{\mathcal{M}}+ < x >=< \alpha > + < x >= R_{\mathcal{M}} \text{ and } R = Q+ < x > \subseteq P+ < x > \subseteq R.$$

That implies $P+ < x >= R$ for all $x \in R \setminus P$. Hence P is maximal.

(v') $(f) \Rightarrow (a)$ follows from Lemma 2.22 and $(a) \Rightarrow (b)$ and $(c) \Rightarrow (d)$ are clear.

$(b) \Rightarrow (c)$ Since $A \neq \mathcal{P}$ and there exist a maximal ideal $\mathcal{M}$ of R containing $\mathcal{P}$, $AR_{\mathcal{M}} \neq \mathcal{P}R_{\mathcal{M}}$ and $\sqrt{AR_{\mathcal{M}}} = \mathcal{P}R_{\mathcal{M}}$. Take $x/s \in \mathcal{P}R_{\mathcal{M}} \setminus AR_{\mathcal{M}}$ where $x \in R$ and $s \in R \setminus \mathcal{M}$. Then $AR_{\mathcal{M}} \subseteq xR_{\mathcal{M}} = (x/s)R_{\mathcal{M}} \subseteq \mathcal{P}R_{\mathcal{M}}$. Thus $\sqrt{xR_{\mathcal{M}}} = \sqrt{< x >}R_{\mathcal{M}} = \mathcal{P}R_{\mathcal{M}}$. Hence, by Remark 1.11,

$$\sqrt{< x >} = \sqrt{< x >}R_{\mathcal{M}} \cap R = \mathcal{P}R_{\mathcal{M}} \cap R = P.$$

$(d) \Rightarrow (e)$ Let $\mathcal{P}$ be the minimal prime of $< a_1, ..., a_n >$, then $\mathcal{P}R_{\mathcal{M}}$ is minimal prime for $AR_{\mathcal{M}}$ which is principal when $A \subseteq \mathcal{M}$ for some maximal ideal $\mathcal{M}$ of R that is $\mathcal{P} \subseteq \mathcal{M}$ for some maximal ideal $\mathcal{M}$ of R. Since $AR_{\mathcal{M}} =< x >$ and $\sqrt{< x >} = \mathcal{P}R_{\mathcal{M}}$ for some $x \in R_{\mathcal{M}}$, then x is not in a prime ideal of $R_{\mathcal{M}}$ properly contained in $\mathcal{P}R_{\mathcal{M}}$ and $sx \in \mathcal{P}$ for some $s \in R \setminus \mathcal{M}$.

Let union of prime ideals of R, properly contained in $\mathcal{P}$ is $\mathcal{P}$. Then $sx \in \mathcal{P}_i$ for some prime ideal $\mathcal{P}_i$ properly contained in $\mathcal{P}$ and $x \in \mathcal{P}_i R_{\mathcal{M}}$ where $\mathcal{P}_i R_{\mathcal{M}}$ is a prime ideal properly contained in $\mathcal{P}R_{\mathcal{M}}$ which is a contradiction. Hence $\mathcal{P}$ is not union of primes which are properly contained in $\mathcal{P}$.

$(e) \Rightarrow (c)$ Assume $\mathcal{P}$ is not union of primes which are properly contained in $\mathcal{P}$. Then there exist $x \in \mathcal{P}$ which is not in the union, that is, $\sqrt{< x >} = \mathcal{P}$. $\square$

Exercise 2.39 *[7, §20, Exercise 8] Let V be a nontrivial valuation ring on the field L and assume that $V = K + \mathcal{M}$, where K is a subfield of L and $\mathcal{M}$ is the maximal ideal of V. Let D^* be a proper subring of K, and let $D_1 = D^* + \mathcal{M}$.*

(1) Prove that the set of finitely generated ideals of D_1 properly containing $\mathcal{M}$ is the set of ideals of the form $A_\alpha + \mathcal{M}$, where A_α is a nonzero finitely generated ideal of D^*.

(2) The finitely generated ideals A of D_1 contained in $\mathcal{M}$ can be obtained as follows: Let W be a nonzero finitely generated D^*-submodule of K, let $m \in \mathcal{M} \setminus \{0\}$ and let $A = Wm + \mathcal{M}m$

(3) Prove that D_1 is Noetherian if and only if V is Noetherian, D^* is a field, and $[K : D^*] < \infty$.

(4) If $\mathcal{P}^*$ is a proper prime ideal of D^*, prove that $(D_1)_{(\mathcal{P}^* + \mathcal{M})} = D^*_{\mathcal{P}^*} + \mathcal{M}$.

(5) Prove that D_1 is a Prüfer domain if and only if D^* is a Prüfer domain with quotient field K.

Solution. (1) Let $I = < b_1, ..., b_n >$ be a nonzero finitely generated ideal of D_1 containing $\mathcal{M}$. Since V is a valuation ring with maximal ideal $\mathcal{M}$, we have $K \cap \mathcal{M} = \{0\}$ that is $D^* \cap \mathcal{M} = \{0\}$. Then $D_1 = D^* \oplus \mathcal{M}$ and any $d \in D_1$ can uniquely be represented as $d = r + m$ where $r \in D^*$ and $m \in \mathcal{M}$. Define

$$\begin{array}{rccc} \psi : & I & \rightarrow & D^* \\ & r+m & \rightarrow & r \end{array}$$

Clearly ψ is a well-defined homomorphism, $\mathrm{Ker}\psi = \mathcal{M}$ and $\mathrm{Im}\psi = < \psi(b_1), ..., \psi(b_n) >$ is a finitely generated ideal of D^*. Set $A_\alpha = Im\psi$, then the short exact sequence

$$0 \longrightarrow \mathcal{M} \longrightarrow I \longrightarrow A_\alpha \longrightarrow 0$$

splits since A_α is projective. Thus $I \cong A_\alpha \oplus \mathcal{M}$ and $A_\alpha \oplus \mathcal{M} \subseteq I$ implies that $I = A_\alpha + \mathcal{M}$.

(2) Let A be a nonzero finitely generated ideal of D_1 contained in $\mathcal{M}$, then $A = < m_1, ..., m_n >$ where $0 \neq m_i \in \mathcal{M}$ for all i. Since V is a valuation ring, m_iV are linearly ordered. Without loss of generality, assume m_1V contains m_iV for all i. Thus, $m_i = (s_i + n_i)m_1$ where $s_i \in K$ and $n_i \in \mathcal{M}$ for all $i \geq 2$. Set $W = < 1, s_2, ..., s_n >$ as a D^*-submodule of K, then any $a \in A$, $a = \sum\limits_{i=1}^{n}(r_i + l_i)m_i$ where $r_i \in D^*$ and $l_i \in \mathcal{M}$ implies

$$a = \sum_{i=1}^{n} r_i s_i m_1 + \sum_{i=1}^{n}(r_i n_i + l_i(s_i + n_i))m_1 \in m_1W + m_1\mathcal{M}$$

and $A \subseteq m_1W + m_1\mathcal{M}$.

On the other hand, $m_1 s_i = m_i - n_i m_1 \in A$ and $m_1\mathcal{M} \subset m_1 D_1 \subset A$ implies $m_1W + m_1\mathcal{M} \subseteq A$.

Thus, $A = m_1W + m_1\mathcal{M}$.

(3) Let D_1 be Noetherian, then $\mathcal{M}$ is finitely generated, since $\mathcal{M}$ is an ideal of D_1. Let $\{m_i\}_{i=1}^n$ be the generating set of $\mathcal{M}$ in D_1. Moreover since V is a valuation ring, Vm_i are linearly ordered, that is, $\mathcal{M} = Vm_i$ for some i. Since any proper ideal I of V is contained in $\mathcal{M}$, I is an ideal of D_1, hence it is finitely generated in D_1, so principal in V and V is Noetherian. Moreover for any $k \in K$, $km_i \in \mathcal{M}$ implies $km_i = \sum_{j=1}^{n} d_{ij}m_j$ for $i = 1, ..., n$ where $d_{ij} \in D_1 = D^* + \mathcal{M}$. Equivalently,

$$(kI - M)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

where M is an $n \times n$ matrix over D_1 and I denotes the $n \times n$ identity matrix. Since m_i are not all zero, $kI - M$ has determinant 0. Hence we can produce a monic polynomial $f(x) \in D_1[x]$ of degree n such that $f(k) = 0$. Let

$$f(x) = x^n + (r_{n-1} + s_{n-1})x^{n-1} + \cdots + (s_0 + n_0) \text{ where } r_i \in D^*, s_i \in \mathcal{M}, 0 \leq i \leq n-1.$$

Then $k^n + r_{n-1}k^{n-1} + \cdots + r_0 = -s_{n-1}k^{n-1} - \cdots - s_0 \in K \cap \mathcal{M} = \{0\}$. Thus there exist a monic irreducible polynomial $g(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in D[x]$ such that $g(k) = 0$ which implies that k is algebraic over D^*. Now take a nonzero element a of D, then $a^{-1} \in K$. We proved that there exist a monic polynomial $f(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ of degree n over $D^*[x]$ such that $f(a^{-1}) = 0$, then $a^{-1} = -b_{n-1}a - \cdots - b_0a^{n-1} \in D^*$. Thus, D^* is a field.
Let $[K : D^*] = \infty$, then there exists a basis β of K over D^* containing infinitely many elements, say $\beta = \{\alpha_j\}_{j=1}^{\infty}$. Define $I_j =< \alpha_1m_1, ..., \alpha_jm_1 >$. Since $\alpha_jm_1 \in \mathcal{M} \subset D_1$, I_j are ideals of D_1 for all positive integer i. Then we have an

ascending chain of ideals such that

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_j \subseteq \cdots$$

Since D_1 is Noetherian, $I_k = I_{k+1}$ for some positive integer k. That is

$$\alpha_{k+1}m_1 = r_1\alpha_1 m_1 + \cdots + r_k\alpha_k m_1 \text{ where } r_j \in D_1 \text{ and } 1 \leq j \leq k.$$

Thus we have $(\alpha_{k+1} - r_1\alpha_1 - \cdots - r_k\alpha_k)m_1 = 0$ and $m_1 \neq 0$ in D_1 so in V. Since V is an integral domain, that implies $\alpha_{k+1} - r_1\alpha_1 - \cdots - r_k\alpha_k = 0$. r_j can uniquely be represented such that $r_j = s_j + n_j$ where $s_j \in D^*$, $n_j \in \mathcal{M}$ and $1 \leq j \leq k$. Thus

$$\alpha_{k+1} - s_1\alpha_1 - \cdots - s_k\alpha_k = n_1\alpha_1 + \cdots + n_k\alpha_k \in \mathcal{M} \cap K = \{0\}.$$

So $\alpha_{k+1} - s_1\alpha_1 - \cdots - s_k\alpha_k = 0$ which contradicts that β is a basis of K over D^*. Hence $[K : D^*] < \infty$.

Conversely, let I be a proper ideal of D_1, since D^* is a field, $I \subseteq \mathcal{M}$. If $I = M$, $\mathcal{M} = Vm$ for some $m \in \mathcal{M}$ since V is a Noetherian valuation ring. Moreover, since $[K : D^*] = n < \infty$, there exists a basis $\{\gamma_i\}_{i=1}^n$ in K such that any $t \in K$, $t = \sum_{i=1}^{n} d_i\gamma_i$ where $d_i \in D^*$, that is, $I = \mathcal{M} =< \gamma_1 m, ..., \gamma_n m >$ is finitely generated in D_1. Let $I =< \{a_i\}_{i\in\mathbb{N}} >$ be an ideal of D_1 properly contained in M where each $a_i \in \mathcal{M}$. Since V is a Noetherian valuation ring, $IV =< a_1, ..., a_k, ... > V = a_sV$ for some a_s in the generating set. Assume $IV = a_1V$, then $a_k = (t_i + n_i)a_1$ where $t_i \in K$ and $n_i \in \mathcal{M}$ for all $k \geq 2$. So $I =< 1, t_2, ..., t_k, ... > a_1 + \mathcal{M}a_1$ where $\mathcal{M} =< \gamma_1 m, ..., \gamma_n m >$. Let S be a linearly independent subset of $\{t_i\}_{i=1}^{\infty}$ where $t_1 = 1$. However, $[K : D^*] = n < \infty$ implies that S has at most n elements.

We may assume that $S = \{t_1, ..., t_n\}$. Then $r_j t_j = \sum_{k=1}^{n} r_k t_k$ where $j \geq n+1$ and $r_k \in D^*$. Since D^* is a field, $t_j = \sum_{k=1}^{n} (r_k/r_1) t_k \in < S >$, that is,

$$I = < 1, t_2, ..., t_n > a_1 + \mathcal{M} a_1 = < a_1, t_2 a_1, ..., t_n a_1, \gamma_1 m a_1, ..., \gamma_n m a_1 >$$

and I is finitely generated. Thus D_1 is Noetherian.

(4) Take $\alpha = (a/s) + m \in D^*_{\mathcal{P}^*} + \mathcal{M}$ where $a \in D^*$, $s \in D^* - \mathcal{P}^*$ and $m \in \mathcal{M}$. Clearly $\alpha = (a + ms)/s \in (D_1)_{(\mathcal{P}^* + \mathcal{M})}$.

On the other hand, let $\beta = (a+m)/(s+n) \in (D_1)_{(\mathcal{P}^*+\mathcal{M})}$, where $a \in D^*$, $m, n \in \mathcal{M}$ and $s \in D^* - \mathcal{P}^*$, that is, $s \neq 0$ and

$$\beta = a/(s+n) + m/(s+n) = a/s + (ms - an)/s(s+n) \in D^*_{\mathcal{P}^*} + \mathcal{M}, \text{since } s(s+n) \notin \mathcal{M},$$

that is, $s(s+n)$ is a unit in V and $(ms - an)/s(s+n) \in \mathcal{M}V = \mathcal{M}$. Hence

$$(D_1)_{(\mathcal{P}^*+\mathcal{M})} = D^*_{\mathcal{P}^*} + \mathcal{M}.$$

(5) Let D_1 be a Prüfer domain and let $\mathcal{P}^*$ be a proper prime ideal of D^*, then $\mathcal{P}^* + \mathcal{M}$ is a prime ideal of D_1, that is, for $a, b \in D^*$ and $m, n \in \mathcal{M}$ with $(a+m)(b+n) \in \mathcal{P}^* + \mathcal{M}$ implies that, $(ab) + (an + bm + mn) \in P^*\mathcal{M}$, by unique representation, $ab \in \mathcal{P}^*$ and since $\mathcal{P}^*$ is a prime ideal, we have a or $b \in \mathcal{P}^*$. Thus, $(a+m)$ or $(b+n) \in \mathcal{P}^* + \mathcal{M}$. Then by assumption and part (4), $(D_1)_{\mathcal{P}^*+\mathcal{M}} = D^*_{\mathcal{P}^*} + \mathcal{M}$ is a valuation ring. Exercise 2.25 implies $D^*_{\mathcal{P}^*}$ is a valuation ring with quotient field K for all prime ideal $\mathcal{P}^*$ of D^*. Thus, D^* is a Prüfer domain with quotient field K.

Conversely, let D^* be a Prüfer domain. Take a prime ideal $\mathcal{N}$ of D_1. By Exercise 2.25, if $\mathcal{N} \subseteq D^*$, then $(D_1)_{\mathcal{N}} = D^*_{\mathcal{N}} + \mathcal{M}$ is a valuation ring and if $\mathcal{N} \subseteq \mathcal{M}$, then $(D_1)_{\mathcal{N}} = V_{\mathcal{N}}$ is a valuation ring. So we will prove that if $\mathcal{N} \nsubseteq D^*$ and $\mathcal{N} \nsubseteq \mathcal{M}$ then $\mathcal{N} = \mathcal{P}^* + \mathcal{M}$ for some prime ideal $\mathcal{P}^*$ of D^*. Take $\alpha \in \mathcal{N} \setminus \mathcal{M}$, then α is a unit in V and for all $m \in \mathcal{M}$ $m/\alpha \in \mathcal{M}$ which implies $m = \alpha(m/\alpha) \in \mathcal{N}$ for all $m \in \mathcal{M}$. So $\mathcal{M} \subseteq \mathcal{N}$. In this case, we claim that $\mathcal{N} \cap D^*$ is a prime ideal of D^* and $\mathcal{N} = (\mathcal{N} \cap D^*) + \mathcal{M}$. Let $ab \in \mathcal{N} \cap D^*$ where $a, b \in D^*$ then $ab \in \mathcal{N}$ and hence a or $b \in \mathcal{N}$ and result follows. Clearly, $(\mathcal{N} \cap D^*) + \mathcal{M} \subseteq \mathcal{N}$. To show the other side, take $\alpha = a + m \in \mathcal{N}$ where $a \in D^*$ and $m \in \mathcal{M} \subset \mathcal{N}$. Hence, $a = \alpha - m \in \mathcal{N} \cap D^*$ and $\alpha = a + m \in (\mathcal{N} \cap D^*) + \mathcal{M}$ and we have the equality. In part (4), we proved that

$$(D_1)_{\mathcal{N}} = (D_1)_{(\mathcal{N} \cap \mathcal{D}^*)+\mathcal{M}} = D^*_{(\mathcal{N} \cap D^*)} + \mathcal{M}$$

and by Exercise 2.25, $D^*_{(\mathcal{N} \cap D^*)}$ is a valuation ring with quotient field K implies that $(D_1)_{\mathcal{N}}$ is a valuation ring. Thus D_1 is a Prüfer domain. $\square$

Exercise 2.40 *[7, §22, Exercise 1] If D is a Prüfer domain and if A and B are ideals of D such that $A^k = B^k$ for some positive integer k, then $A = B$.*

Solution. Since D is a Prüfer domain, $D_{\mathcal{M}}$ is a valuation ring for all maximal ideal $\mathcal{M}$ of D. If $A^k D_{\mathcal{M}} = B^k D_{\mathcal{M}} = D_{\mathcal{M}}$, clearly, $AD_{\mathcal{M}} = BD_{\mathcal{M}} = D_{\mathcal{M}}$.

Assume $A^k D_{\mathcal{M}} \neq D_{\mathcal{M}}$. Then $\sqrt{AD_{\mathcal{M}}} = \sqrt{A^k D_{\mathcal{M}}} = \sqrt{B^k D_{\mathcal{M}}} = \sqrt{BD_{\mathcal{M}}}$ is a proper prime ideal of D_M. Hence $AD_{\mathcal{M}}$ and $BD_{\mathcal{M}}$ are proper ideals of $D_{\mathcal{M}}$. Since $D_{\mathcal{M}}$ is a valuation ring either $AD_{\mathcal{M}}$ is contained in $BD_{\mathcal{M}}$ or $BD_{\mathcal{M}}$ is contained in $AD_{\mathcal{M}}$. We may assume that $AD_{\mathcal{M}} \subsetneqq BD_{\mathcal{M}}$. Then there exists $\alpha \in BD_{\mathcal{M}} \setminus AD_{\mathcal{M}}$. Hence $AD_{\mathcal{M}} \subsetneqq < \alpha >$ Since $< \alpha >$ is invertible, $(1/\alpha)AD_{\mathcal{M}} \subsetneqq D_{\mathcal{M}}$ implies that

$(1/\alpha)^k A^k D_{\mathcal{M}} \subsetneqq D_{\mathcal{M}}$, that is, $A^k D_{\mathcal{M}} \subsetneqq < \alpha^k > \subseteq B^k D_{\mathcal{M}}$ which is a contradiction. So $AD_{\mathcal{M}} = BD_{\mathcal{M}}$. Hence $AD_{\mathcal{M}} = BD_{\mathcal{M}}$ for all maximal ideal $\mathcal{M}$ of D.

Thus, by Remark 1.10 (iii),

$$A = \bigcap_{\lambda \in \Lambda} AR_{\mathcal{M}_\lambda} = \bigcap_{\lambda \in \Lambda} BR_{\mathcal{M}_\lambda} = B$$

□

Exercise 2.41 *[7, §22, Exercise 2] If D is a Prüfer domain, and if Q_1, Q_2 are primary ideals of D, then either Q_1 and Q_2 are relatively prime or one of Q_1 or Q_2 is contained in the other.*

Solution. Suppose Q_1 and Q_2 are not relatively prime. Then there exist a maximal ideal $\mathcal{M}$ of D such that $Q_1 + Q_2 \subseteq \mathcal{M}$. Hence $Q_1 D_{\mathcal{M}}$ and $Q_2 D_{\mathcal{M}}$ are proper ideals of the valuation ring $D_{\mathcal{M}}$. Thus one of them is contained in the other. Assume $Q_1 D_{\mathcal{M}} \subseteq Q_2 D_{\mathcal{M}}$. Then, by Remark 1.10,

$$Q_1 = Q_1 D_{\mathcal{M}} \cap D \subseteq Q_2 D_{\mathcal{M}} \cap D = Q_2.$$

□

Exercise 2.42 *[7, §22, Exercise 3] If D is a Prüfer domain and if A is an ideal of D such that $A^k = A^{k+1}$ for some positive integer k, then A is idempotent and semiprime.*

Solution. If $A = D$, clearly A is idempotent and semiprime.

Assume A is a proper ideal of D, then there exist a maximal ideal $\mathcal{M}$ of D containing A. So $A^k D_{\mathcal{M}}$ is a proper ideal of the valuation ring $D_{\mathcal{M}}$. Then, by Theorem 2.16(iii), $AD_{\mathcal{M}} = A^2D_{\mathcal{M}}$ is a prime ideal. Hence by Remark 1.11, $A = AD_{\mathcal{M}} \cap D = A^2D_{\mathcal{M}} \cap D = A^2$ is also prime, so semiprime.

Therefore A is idempotent and semiprime in any case. $\square$

Exercise 2.43 *[7, §22, Exercise 5] Suppose that A is a finitely generated proper ideal of the Prüfer domain J, that $\{P_\lambda\}_{\lambda\in\Lambda}$ is the set of minimal prime ideals of A, and that $N(\mathcal{P}_\lambda)$ is the intersection of the set of $\mathcal{P}_\lambda$-primary ideals of J.*

Prove that $\bigcap\limits_{n=1}^{\infty} A^n = \bigcap\limits_{\lambda\in\Lambda} N(\mathcal{P}_\lambda)$

Solution. Let $\{Q_{\lambda\gamma}\}_{\gamma\in\Gamma_\lambda}$ be the $\mathcal{P}_\lambda$-primary ideals of J. First we will prove that there exists $k_\gamma \in \mathbb{Z}^+$ such that $A^{k_\gamma} \subseteq Q_{\lambda\gamma}$ for all $\gamma \in \Gamma_\lambda$. Let $\mathcal{M}$ be a maximal ideal of J. If $A \nsubseteq \mathcal{M}$, then $A^kJ_{\mathcal{M}} = \mathcal{P}_\lambda J_{\mathcal{M}} = \sqrt{Q_{\lambda\gamma}}J_{\mathcal{M}} = Q_{\lambda\gamma}J_{\mathcal{M}}$ for all $k \in \mathbb{Z}^+$, $\gamma \in \Gamma_\lambda$ and $\lambda \in \Lambda$. Suppose $A \subseteq \mathcal{M}$ and $Q_{\lambda\gamma} \nsubseteq \mathcal{M}$, then the result is same. Let $A \subseteq \mathcal{M}$ and $Q_{\lambda\gamma} \subseteq \mathcal{M}$, then $AJ_{\mathcal{M}} \subsetneqq \mathcal{P}_\lambda J_{\mathcal{M}} = \sqrt{Q_{\lambda\gamma}}J_{\mathcal{M}}$. By Theorem 2.16(v), there exist $k_\gamma \in \mathbb{Z}^+$ such that $A^{k_\gamma}J_{\mathcal{M}} \subseteq Q_{\lambda\gamma}J_{\mathcal{M}}$ for all $\gamma \in \Gamma_\lambda$.

Hence, $A^{k_\gamma} = \bigcap\limits_{\mathcal{M}} A^{k_\gamma}J_{\mathcal{M}} \subseteq \bigcap\limits_{\mathcal{M}} Q_{\lambda\gamma}J_{\mathcal{M}} = Q_{\lambda\gamma}$ for all $\gamma \in \Gamma_\lambda$ and $\lambda \in \Lambda$. Thus $\bigcap\limits_{i=1}^{\infty} A^i \subseteq \bigcap\limits_{\gamma\in\Gamma_\lambda} A^{k_\gamma} \subseteq \bigcap\limits_{\gamma\in\Gamma_\lambda} Q_{\lambda\gamma} = N(\mathcal{P}_\lambda)$ for all $\lambda \in \Lambda$, that is $\bigcap\limits_{i=1}^{\infty} A^i \subseteq \bigcap\limits_{\lambda\in\Lambda} N(\mathcal{P}_\lambda)$.

On the other hand,$N(\mathcal{P}_\lambda) = \mathcal{P}_{0\lambda}$ is a prime ideal of J and there are no prime ideals of J between $\mathcal{P}_\lambda$ and $\mathcal{P}_{0\lambda}$, by Theorem 2.37(iv). Since $\mathcal{P}_\lambda$ are minimal primes of A, we have $\mathcal{P}_{0\lambda} \subsetneqq A$ for all $\lambda \in \Lambda$. Moreover, $\mathcal{P}_{0\lambda} \subsetneqq A^k$ for all $k \in \mathbb{Z}^+$. Otherwise $A^s \subseteq P_{0\lambda}$ for some $s \in \mathbb{Z}^+$ implies that $A \subseteq \sqrt{A} \subseteq \sqrt{A^s} \subseteq \mathcal{P}_{0\lambda}$ which contradicts that $\mathcal{P}_{0\lambda}$ is properly contained in A. Hence $\mathcal{P}_{0\lambda} \subseteq \bigcap\limits_{i=1}^{\infty} A^i$. Thus

$$\bigcap_{\lambda\in\Lambda} N(\mathcal{P}_\lambda) = \bigcap_{i=1}^{\infty} A^i.$$

$\square$

Definition 2.44 *If V and W are valuation rings on a field K, we say that V and W are* <u>*independent*</u> *if $< 0 >$ is the only common prime ideal of V and W.*

Exercise 2.45 *[7, §22, Exercise 9] Let $\{v_1, ..., v_n\}$ be a finite set of valuations on the field L; V_i is the valuation ring of v_i and G_i is the value group of v_i where*

$$\begin{array}{rccc} v_i : & L & \rightarrow & G_i = L^*/U_i \\ & x & \rightarrow & xU \end{array}$$

where U_i is the set of units of V_i, $i = 1, ..., n$. Assume that the following condition $(*)$ holds:

$(*)$ *If $\alpha_i \in G_i$ such that $\alpha_i \geq 0$ for all i, then there is an element $x \in L$ such that $v_i(x) = \alpha_i$, $i = 1, ..., n$.*

Prove that the valuation rings V_i are pairwise independent.

Solution. Let us take two distinct nonzero valuation rings V_i and V_j and any nonzero prime ideal $\mathcal{P}_i$ of V_i, then there exists a nonzero $x \in \mathcal{P}_i$ such that $xU_i > U_i$. Clearly, $xU_i \in G_i$. Set $\alpha_i = xU_i$ and $\alpha_j = U_j$, by $(*)$ there exists $y \in L$ such that $yU_i = xU_i$ and $yU_j = U_j$. Then y is nonzero and $y/x, x/y \in V_i$ and $y, 1/y \in V_j$ that is $y = (y/x)x \in \mathcal{P}_i$ and $y \notin \mathcal{P}_j$ for any nonzero prime ideal $\mathcal{P}_j$ of V_j. Thus there is no nonzero common prime ideal $\mathcal{P}_i$ of V_i and V_j, that is, $< 0 >$ is the only common prime ideal of V_i and V_j. $\square$

Exercise 2.46 *[7, §23, Exercise 6] Prove that each ideal of the ring T has prime radical if and only if the set of prime ideals of T is linearly ordered under inclusion.*

Solution. Let S be the set of prime ideals of T. If S is linearly ordered, clearly any ideal of T has prime radical.

Conversely, assume $\sqrt{I}$ is prime for any ideal I of T. Let $\mathcal{P}_i, \mathcal{P}_j \in S$ such that $\mathcal{P}_i \nsubseteq \mathcal{P}_j$, that is, there exists $a \in \mathcal{P}_i \setminus \mathcal{P}_j$. Then $\sqrt{\mathcal{P}_i \cap \mathcal{P}_j} = \mathcal{P}_i \cap \mathcal{P}_j$ is prime by assumption. For all $b \in \mathcal{P}_j$, $ab \in \mathcal{P}_i \cap \mathcal{P}_j$ and $a \notin \mathcal{P}_j$ implies $b \in \mathcal{P}_i \cap \mathcal{P}_j$, that is, $b \in \mathcal{P}_i$ for all $b \in \mathcal{P}_j$. Thus $\mathcal{P}_j \subseteq \mathcal{P}_i$ and S is linearly ordered under inclusion. □

Exercise 2.47 *[7, §23, Exercise 11] For a Prüfer domain J, prove that the following conditions are equivalent:*

(1) Primary ideals of J are prime powers.

(2) $J_{\mathcal{M}}$ is a discrete valuation ring for each maximal ideal $\mathcal{M}$ of J.

Solution.

(2) $\Rightarrow$ (1) Let A be a nonzero $\mathcal{P}$-primary ideal of J. Then there exist a maximal ideal $\mathcal{M}$ of J containing $\mathcal{P}$. Hence, by Remark 1.11, AJ_M is a $\mathcal{P}J_{\mathcal{M}}$-primary ideal of $J_{\mathcal{M}}$. By assumption, $AJ_{\mathcal{M}} = \mathcal{M}^k J_{\mathcal{M}}$ for some $k \in \mathbb{Z}^+$. Again by Remark 1.11, $A = \mathcal{M}^k$ and $\mathcal{M} = \mathcal{P}$. For $A =< 0_J >$ the result is clear. Thus (2) implies (1).

We claim that (1) does not implies (2). Let $J = \mathbb{Z}_{<2>} + x\mathbb{Q}[[x]]$. By Example 2.8, J is a valuation ring so it is a Prüfer domain. By Example 2.9 and Exercise 2.23, $2J$, $x\mathbb{Q}[[x]]$ are nonzero prime ideals of J and there is no prime between $< 0_J >$ and $x\mathbb{Q}[[x]]$. Moreover any ideal I properly containing $x\mathbb{Q}[[x]]$ is of the form $2^s J$ for some positive integer s by Example 2.9. So $\sqrt{I} = 2J$. That means there is no prime between $x\mathbb{Q}[[x]]$ and $2J$. So the prime ideals of J are precisely $< 0_J >$, $\mathcal{P} = x\mathbb{Q}[[x]]$ and $\mathcal{M} = 2J$. Clearly, the only $< 0_J >$-primary ideal is $< 0_J >$. Since $\mathcal{P}^2 \neq \mathcal{P}$, S, the set of $\mathcal{P}$-primary ideals of J, is $\{\mathcal{P}^j\}_{j=1}^{\infty}$ and $\mathcal{M}^2 \neq \mathcal{M}$, T, the set of $\mathcal{M}$-primary ideals of J, is $\{\mathcal{M}^i\}_{i=1}^{\infty}$ by part (ii) of Theorem 2.21. Thus any primary ideal of J is prime power. However, $J_{\mathcal{M}} = J$ and J is not Noetherian so it is not a discrete valuation ring. □

Exercise 2.48 *[7, §23, Exercise 13] Assume that D is a Prüfer domain and that Q, Q_1, Q_2 are $\mathcal{P}$-primary ideals of D. Prove:*

(a) If $Q_1 \subsetneqq \mathcal{P}$, then Q contains a power of Q_1.

(b) If $Q \subsetneqq \mathcal{P}$, then $Q^2 \subsetneqq Q\mathcal{P}$.

(c) If $Q_1 \subsetneqq Q_2$, then $(Q_1 : Q_2) = Q_1$ implies that $Q_2 = \mathcal{P} = \mathcal{P}^2$.

Solution. Since Q_1, Q_2, Q are $\mathcal{P}$-primary, $\sqrt{Q_1} = \sqrt{Q_2} = \sqrt{Q} = \mathcal{P}$.

(a)Let $\mathcal{M}$ be a maximal ideal of D containing $\mathcal{P}$. Then $Q_1 D_{\mathcal{M}}, Q_2 D_{\mathcal{M}}, Q D_{\mathcal{M}}$ are $\mathcal{P} D_{\mathcal{M}}$-primary ideals of the valuation ring $D_{\mathcal{M}}$ by Remark 1.11 and $Q D_{\mathcal{M}} \subsetneqq \mathcal{P} D_{\mathcal{M}}$. Moreover, $Q_1^k D_{\mathcal{M}}$ are $\mathcal{P} D_{\mathcal{M}}$-primary ideals of $D_{\mathcal{M}}$ for all $k \in \mathbb{Z}^+$ by Theorem 2.21 (ii). Since $Q_1 D_{\mathcal{M}} \subsetneqq \mathcal{P} D_{\mathcal{M}} = \sqrt{Q} D_{\mathcal{M}}$, then $Q D_{\mathcal{M}}$ contains a power of $Q_1 D_{\mathcal{M}}$ that is $Q_1^s D_{\mathcal{M}} \subseteq Q D_{\mathcal{M}}$ for some $s \in \mathbb{Z}^+$ by Theorem 2.16 (v). Thus $Q_1^s = Q_1^s D_{\mathcal{M}} \cap D \subseteq Q D_{\mathcal{M}} \cap D = Q$ by Remark 1.11.

(b) Clearly, $Q^2 \subseteq \mathcal{P} Q$. Assume $Q^2 = \mathcal{P} Q$. If $\mathcal{P}$ is idempotent, then $Q^3 = Q Q^2 = Q(Q\mathcal{P}) = Q^2 \mathcal{P} = Q \mathcal{P}^2 = Q\mathcal{P}$. By induction on n, $Q^n = Q\mathcal{P}$ where $1 \neq n \in \mathbb{Z}^+$. Since $\mathcal{P}$ is branched, by Theorem 2.37 (iii) and (iv) there is a prime ideal $\mathcal{P}_0 \neq \mathcal{P}$ such that there is no prime between $\mathcal{P}_0$ and $\mathcal{P}$ where $\mathcal{P}_0 = \bigcap_{i=1}^{\infty} Q^i$. Hence we have $\mathcal{P}_0 = Q\mathcal{P}$ and $Q \subseteq \mathcal{P}_0$ such that any $q \in Q$ and $p \in \mathcal{P} \setminus \mathcal{P}_0$ $qp \in \mathcal{P}_0$ and this implies $q \in \mathcal{P}_0$ which contradicts Q is $\mathcal{P}$-primary. So $\mathcal{P}_0 = \mathcal{P} = \mathcal{P} Q \subseteq Q \subseteq \mathcal{P}$. Thus $\mathcal{P} = Q$ which is a contradiction.

If $\mathcal{P}$ is not idempotent, by Theorem 2.37 (ii) $Q = \mathcal{P}^s$ for some $s \in \mathbb{Z}^+$ and since $Q \neq \mathcal{P}$, $s \neq 1$, $Q^2 = Q\mathcal{P}$ implies that $\mathcal{P}^{2s} = \mathcal{P}^{s+1}$, that is, $\mathcal{P}^{s+k} = \mathcal{P}^{s+1}$ for all $k \in \mathbb{Z}^+$. By Theorem 2.37 (ii) and (iv), $\mathcal{P}_0 = \mathcal{P}^{s+1} = \mathcal{P}$ and $\mathcal{P}$ is idempotent which contradicts our assumption. Hence $Q^2 \subsetneqq Q\mathcal{P}$.

(c) Suppose $\mathcal{P} \neq \mathcal{P}^2$, then $Q_1 = \mathcal{P}^s$ and $Q_2 = \mathcal{P}^t$ where $s > t$ and $s, t \in \mathbb{Z}^+$ by Theorem 2.37(ii). Then $(Q_1 : Q_2) = (\mathcal{P}^s : \mathcal{P}^t) \supseteq \mathcal{P}^{s-t} \supsetneqq \mathcal{P}^s = Q_1$. Hence $\mathcal{P} = \mathcal{P}^2$.

Let $Q_2 \subsetneqq \mathcal{P}$. Then by Theorem 2.37 (iii),

$$\bigcap_{i=1}^{\infty} Q_2^i = \mathcal{P}_0 \subsetneqq Q_1$$

Also, since $Q_1 \subsetneqq Q_2$, there exists $n \in \mathbb{Z}^+$ such that $Q_2^n \subseteq Q_1 \subsetneqq Q_2^{n-1}$. However, we have $Q_1 = (Q_1 : Q_2)$. Then $Q_1 \supseteq Q_2^{n-1}$, which contradicts that Q_1 is properly contained in Q_2^{n-1}. Hence

$$\mathcal{P} = \mathcal{P}^2 = Q_2.$$

□

CHAPTER 3

PRIME SUBMODULES

3.1 Basic Definitions

Definition 3.1 *Let R be a ring and M be an R-module, a proper submodule N of M is called* prime *if whenever $rm \in N$, for some $r \in R$, $m \in M$, then $m \in N$ or $rM \subseteq N$.*

Definition 3.2 *For any submodule N of M, $(N : M)$ denotes the set of elements $r \in R$ such that $rM \subseteq N$. This is usually called* residual by N . *Note that $(N : M)$ is the annihilator of the module M/N and $(N : M)$ is an ideal of R. For any ideal J of R $(N :_M J)$ denotes the set of elements $m \in M$ such that $Jm \subseteq N$.*

If N is a prime submodule of M with $\mathcal{P} = (N : M)$, then N is called $\mathcal{P}$-prime submodule.

Example 3.3 *(1) Every direct summand of a torsion-free module is prime.*

(2) The zero submodule is the only prime submodule of the $\mathbb{Z}$-module $\mathbb{Q}$ of rational numbers.

Lemma 3.4 *[[9], Lemma 1] Let R be a ring and M be an R-module. Then a submodule N of M is prime if and only if $\mathcal{P} = (N : M)$ is a prime ideal of R and the $R/\mathcal{P}$-module M/N is torsion-free.*

Proof. Let N be a prime submodule of M and let $ab \in \mathcal{P} = (N : M)$ where $a, b \in R$. Then $(ab)M \subseteq N$ so $a(bM) \subseteq N$ implies that $aM \subseteq N$ or $bM \subseteq N$ since N is prime. Hence $\mathcal{P} = (N : M)$ is a prime ideal of R.

Since $\mathcal{P}M \subseteq N$, M/N is an $R/\mathcal{P}$-module. Let $0 \neq r + \mathcal{P} \in R/\mathcal{P}$ and $m + N \in M/N$ such that $(r + \mathcal{P})(m + N) = 0$. Then $rm + N = 0$ implies that $rm \in N$. Hence either $m \in N$ or $rM \subseteq N$. Since $r \notin \mathcal{P}$, we have $m \in N$. Hence M/N is a torsion-free $R/\mathcal{P}$-module.

Conversely, suppose $\mathcal{P} = (N : M)$ is a prime ideal and M/N is a torsion free $R/\mathcal{P}$-module. Let $r \in R$, $m \notin N$ and $rm \in N$; then $(r + \mathcal{P})(m + N) = 0$. Since $m \notin N$, we have $r \in \mathcal{P}$. Hence $rM \subseteq N$. Therefore N is a prime submodule of M. □

Example 3.5 *It is not difficult at all to give examples of modules which have no prime submodules: As a $\mathbb{Z}$-module, the Prüfer group $\mathbb{Z}(p^\infty)$ has no prime submodules.*

Lemma 3.6 *[[20], Result 1.1] Let M, M' be R-modules with $\varphi : M \to M'$ an R-module epimorphism and N be a submodule of M such that $N \supseteq K = Ker\varphi$. Then there exists a one-to-one order preserving correspondence between the proper submodules of M containing N and the proper submodules of M' containing $\varphi(N)$. Furthermore, for any submodule N' of M', there exists a submodule L of M such that $L \supseteq K$ and $\varphi(L) = N'$.*

Lemma 3.7 *[[20], Result 1.2] Assume the hypothesis given in Lemma 3.6. Then*

(i) If P is a prime submodule of M containing N, then $\varphi(P)$ is a prime submodule of M' containing $\varphi(N)$.

(ii) If P' is a prime submodule of M' containing $\varphi(N)$, then $\varphi^{-1}(P')$ is a prime submodule of M containing N.

Proof. (i) Since P is a prime submodule of M containing N, by Lemma 3.6 $\varphi(N) \subseteq \varphi(P)$ and since $P \neq M$, $\varphi(P) \neq \varphi(M) = M'$. Let $r \in R$,

$m' \in M'$ and $rm' \in \varphi(P)$. There exists $m \in M$ such that $\varphi(m) = m'$. So $r\varphi(m) = \varphi(rm) \in \varphi(P)$. Then $rm \in P$ and since P is a prime submodule, $m \in P$ or $rM \subseteq P$. If $m \in P$, then $\varphi(m) = m' \in \varphi(P)$. If $rM \subseteq P$, then $rM' \subseteq \varphi(P)$. Therefore $\varphi(P)$ is a prime submodule of M'.

(ii) Since P' is a prime submodule of M', by Lemma 3.6 there exists a submodule L of M such that $L \supseteq K$ and $\varphi(L) = P'$. Let $n \in N$. Then $\varphi(n) \in \varphi(N) \subseteq \varphi(L)$, so $\varphi(n) = \varphi(l)$ for some $l \in L$. Then $(n - l) \in K \subseteq L$ and hence $n \in L = \varphi^{-1}(P')$. Let $r \in R$, $m \in M$ and $rm \in \varphi^{-1}(P')$. Then $\varphi(rm) = r\varphi(m) \in P'$. Since P' is a prime submodule of M' we have $\varphi(m) \in P'$ or $rM' \subseteq P'$. If $\varphi(m) \in P' = \varphi(L)$, then there exists $x \in L$ such that $\varphi(m) = \varphi(x)$. Then $\varphi(m - x) = 0_{M'}$ so that $m - x \in K \subseteq L$ and $m = x + y$ for some $y \in L$. Hence $m \in L = \varphi^{-1}(P')$. If $rM' \subseteq P'$, then $rm' \in P'$ for all $m' \in M'$. Then there exists $\bar{m} \in M$ such that $\varphi(\bar{m}) = m'$ for all $m' \in M'$. It gives that $\varphi(r\bar{m}) \in \varphi(L)$ and $r\bar{m} \in L$. Hence $rM \subseteq L = \varphi^{-1}(P')$. $\square$

Theorem 3.8 *[[14], Theorem 1] Let N be a proper submodule of an R-module M with $(N : M) = \mathcal{P}$. Then the following statements are equivalent.*

(i) N is a prime submodule of M;

(ii) M/N is torsion-free $R/\mathcal{P}$-module;

(iii) $(N :_M \langle r\rangle) = N$ for every $r \in R - \mathcal{P}$;

(iv) $(N :_M J) = N$ for every ideal $J \nsubseteq \mathcal{P}$;

(v) $(N : \langle e\rangle) = \mathcal{P}$ for every $e \in M - N$;

(vi) $(N : L) = \mathcal{P}$ for every submodule L of M properly containing N;

(vii) $Ass(M/N) = \{\mathcal{P}\}$;

(viii) $\mathcal{P} = Z_R(M/N)$ where $Z_R(M/N)$ is the set of all zero divisors of M/N.

Proof. $(i) \Rightarrow (ii)$ By Lemma 3.4.

$(ii) \Rightarrow (iii)$ Clearly $N \subseteq (N :_M \langle r \rangle)$. Now suppose M/N is a torsion free $R/\mathcal{P}$-module. Then for any $r \in R$ and for all $m \in M - N$, $(r + \mathcal{P})(m + N) = 0$ implies that $r \in \mathcal{P}$. Now let $m \in (N :_M \langle r \rangle)$ for some $r \in R - \mathcal{P}$. Then $rm \in N$ and $(r + \mathcal{P})(m + N) = 0$ gives $m \in N$ since $r \notin \mathcal{P}$. Hence $(N :_M \langle r \rangle) \subseteq N$.

$(iii) \Rightarrow (iv)$ Clearly $N \subseteq (N :_M J)$. Suppose $(N :_M \langle r \rangle) = N$ for every $r \in R - \mathcal{P}$. Let J be an ideal of R such that $J \nsubseteq \mathcal{P}$. Then there exists $x \in J - \mathcal{P}$ such that $(N :_M \langle x \rangle) = N$. Now let $m \in (N :_M J)$. Then $Jm \subseteq N$. In particular $xm \in N$. Hence $m \in N$ since $(N :_M \langle x \rangle) = N$. Thus $(N :_M J) \subseteq N$. Therefore $(N :_M J) = N$.

$(iv) \Rightarrow (v)$ Suppose $(N :_M J) = N$ for every ideal $J \nsubseteq \mathcal{P}$. Let $e \in M - N$. Clearly $\mathcal{P} \subseteq (N : \langle e \rangle)$. Now let $r \in (N : \langle e \rangle)$. Then $re \in N$. If $r \notin \mathcal{P}$, then $e \in (N :_M \langle r \rangle) = N$, which is a contradiction. Hence $r \in \mathcal{P}$, that is, $(N : \langle e \rangle) \subseteq \mathcal{P}$.

$(v) \Rightarrow (vi)$ Suppose $(N : \langle e \rangle) = \mathcal{P}$ for every $e \in M - N$. Clearly $\mathcal{P} \subseteq (N : L)$ for all submodules L of M such that $N \subsetneqq L$. Let $r \in (N : L)$. Then
$(N : L) = (N : (\sum\limits_{l \in L} Rl)) = \bigcap\limits_{l \in L} (N : Rl) = \mathcal{P}$.

$(vi) \Rightarrow (vii)$ Suppose $(N : L) = \mathcal{P}$ for all submodule L of M such that $N \subsetneqq L$. Let $Q \in Ass(M/N)$. Then $Q = Ann_R(x + N)$ for some $x \in M - N$. Note that $N \subsetneqq \langle x \rangle + N$ and $\langle x \rangle + N$ is a submodule of M. Since $(N : (\langle x \rangle + N)) = \mathcal{P}$, $\mathcal{P}(\langle x \rangle + N) \subseteq N$ and $\mathcal{P}x \subseteq N$. Hence $\mathcal{P} \subseteq Ann_R(x + N) = Q$. Conversely let $r \in Q = Ann_R(x + N)$. Then $rx \in N$ for some $x \in M - N$. So $r(\langle x \rangle + N) \subseteq N$ and $r \in (N : (\langle x \rangle + N)) = \mathcal{P}$. Hence $Q \subseteq \mathcal{P}$.

$(vii) \Rightarrow (viii)$ Suppose $Ass(M/N) = \mathcal{P}$, that is, $\mathcal{P} = Ann_R(m + N)$ for all $m \in M - N$. Clearly $\mathcal{P} \subseteq Z_R(M/N)$. Now let $x \in Z_R(M/N)$. Then $xm \in N$ for some $m \in M - N$. Hence $x \in Ann_R(m + N)$ for some $m \in M - N$. So $x \in \mathcal{P}$

and hence $Z_R(M/N) \subseteq \mathcal{P}$.

$(viii) \Rightarrow (i)$ Suppose $\mathcal{P} = Z_R(M/N)$. Let $r \in R$, $m \in M - N$ such that $rm \in N$. Then $r \in Z_R(M/N) = \mathcal{P} = (N : M)$. Thus $rM \subseteq N$. Therefore N is a prime submodule of M. $\square$

3.2 The Behavior of Prime Submodules Under Localization

In this section M will denote an R-module and S will denote a multiplicatively closed subset of R which contains 1 but not 0. Let M_S be the localization of M at S and $f : M \to M_S$ be a natural map.

Proposition 3.9 *(i) For any prime R-submodule P of M with $M_S \neq P_S$, $(P_S)^c = P$.*

(ii) For any R_S-submodule Q of M_S, $(Q^c)_S = Q$.

Proof. (i) Let $x \in P$. Then $f(x) \in P_S$ and hence $x \in (P_S)^c$. Thus $P \subseteq (P_S)^c$. Now let $y \in (P_S)^c$. Then $f(y) \in P_S$, that is, $sy/s \in P_S$. There exist $p \in P$ and $t \in S$ such that $sy/s = p/t$. Then $usty = usp \in P$ for some $u \in S$. Hence $y \in P$ or $(ust)M \subseteq P$. If $y \in P$, then it is clear. If $(ust)M \subseteq P$, then for all $m \in M$ we have $(ust)m \in P$. Then we can write for any $x \in M$, $x = x.1/1 = ustx/ust \in P_S$. Thus $M_S = P_S$. This contradicts our assumption. Therefore $(P_S)^c \subseteq P$.

(ii) Let $a/s \in (Q^c)_S$. Then there exist $b \in Q^c$ and $s^{'} \in S$ such that $a/s = b/s^{'}$. Then $us^{'}a = usb \in Q^c$ for some $u \in S$. Since $us^{'}a \in Q^c$, $f(us^{'}a) = us^{'}at/t \in Q$ for some $t \in S$. Hence $a/s = us^{'}ta/sus^{'}t \in Q$. Conversely let $x \in Q$. Then $x = a/s \in Q$ where $a \in Q^c$ and $s \in S$. So $f(a) = xs = as/s \in (Q^c)_S$ and $x = (1/s)(as/s) \in (Q^c)_S$. $\square$

Proposition 3.10 *[[17], Proposition 2.1] (i) If P is a prime submodule of M with $M_S \neq P_S$, then P_S is a prime R_S-submodule of M_S.*

(ii) If Q is a prime R_S-submodule of M_S, then Q^c is a prime R-submodule of M.

Proof.(i) Let $r \in R_S$, $m \in M_S$ and $rm \in P_S$ such that $r = x/s$, $m = y/s^{'}$ for some $x \in R$, $y \in M$ and $s, s^{'} \in S$. Then $rm = xy/ss^{'} \in P_S$. There exist $z \in P$, $t \in S$ such that $xy/ss^{'} = z/t$ and $u \in S$ with $(ut)xy = (uss^{'})z \in P$. Then $y \in P$ or $(utx)M \subseteq P$ since P is a prime submodule. If $y \in P$, then $m = y/s^{'} \in P_S$. If $(utx)M \subseteq P$, then $(utx)m_1 \in P$ for all $m_1 \in M$. Hence $(utx)m_1/s \in P_S$ and $(x/s)(uts^{'}m_1/s^{'}) \in P_S$ for all $m_1 \in M$. Thus $rM_S \subseteq P_S$. Therefore P_S is a prime submodule of M_S.

(ii) Suppose $Q^c = M$. Then for all $m \in M$, $f(m) \in Q$. Since $Q = Q^c_S$ by Proposition 3.9, $Q = M_S$. Therefore $Q^c \neq M$. Let $r \in R$, $m \in M$ and $rm \in Q^c$. Then

$$f(rm) = s(rm)/s = (rs/s)(sm/s) \in Q.$$

Thus $(rs/s)M_S \subseteq Q$ or $sm/s \in Q$. If $(rs/s)M_S \subseteq Q$, then $(rs/s)(tm_1/t) \in Q$ for all $m_1 \in M$. Then $(rst/st)m_1 = st(rm_1)/st = f(rm_1) \in Q$ and $rm_1 \in Q^c$ for all $m_1 \in M$. Hence $rM \subseteq Q^c$. If $(rs/s)M_S \nsubseteq Q$, then $sm/s \in Q$. Hence $f(m) \in Q$, that is, $m \in Q^c$. Therefore Q^c is a prime submodule of M. $\square$

Corollary 3.11 *[[17], Corollary 2.2] Let $A = \{P : P$ is a prime R-submodule of M with $M_S \neq P_S\}$ and $B = \{Q : Q$ is a prime R_S-submodule of $M_S\}$. Then φ which is defined by $\varphi(P) = P_S$ is a bijective order preserving map from A to B. Its inverse map is given by $\varphi^{-1}(Q) = Q^c$.*

CHAPTER 4

RADICAL FORMULA

4.1 Definitions and Fundamental Results

Let M be an R-module, I be an ideal of R and N be a submodule of M. As it is well-known, the radical of I defined as the intersection of all prime ideals containing I, has the characterization $\sqrt{I} = \{r \in R : r^n \in I$, for some $n \in \mathbb{Z}^+\}$. A natural question arises as to whether there is a similar characterization for the prime radical of a submodule, in particular, a characterization in which knowledge of prime submodules (indeed even prime ideals) is not necessary. We will show that under certain conditions such a characterization is provided by the concept of the envelope of a submodule.

Definition 4.1 *Let M be a module over a ring R and N be a submodule of M with $N \neq M$. The prime radical of N in M, $rad_M(N)$, is defined to be the intersection of all prime submodules of M containing N. If there is no prime submodule containing N, then $rad_M(N) = M$. In particular $rad_M(M) = M$. We also define the radical $RadM$ of a module M as the intersection of all maximal proper submodules.*

Definition 4.2 *Let M be an R-module and N a submodule of M. The envelope of N in M which is denoted by $E_M(N)$ is defined to be the set*

$$\{rm : r \in R, m \in M \text{ such that } r^n m \in N \text{ for some } n \in \mathbb{Z}^+\}.$$

Lemma 4.3 *[[20], Lemma 1.4] Assume the hypothesis given in Lemma 3.6. Then*

(i) $\varphi(E_M(N)) = E_{M'}(\varphi(N))$*;*

(ii) $\langle \varphi^{-1}(E_{M'}(N')) \rangle = \langle E_M(\varphi^{-1}(N')) \rangle$.

Proof.(i) Let $x \in \varphi(E_M(N))$. Then $x = \varphi(y)$ for some $y \in E_M(N)$. So $y = rm$ such that $r \in R$, $m \in M$ and $r^n m \in N$ for some positive integer n. Then $x = \varphi(rm) = r\varphi(m)$. Since $r^n m \in N$ we have $\varphi(r^n m) = r^n \varphi(m) \in \varphi(N)$ and $r\varphi(m) \in E_{M'}(\varphi(N))$. Hence $x = r\varphi(m) \in E_{M'}(\varphi(N))$. Now assume that $z \in E_{M'}(\varphi(N))$. Then $z = sm'$ such that $s \in R$, $m' \in M'$ and $s^t m' \in \varphi(N)$ for some positive integer t. Since φ is onto, there exists $\bar{m} \in M$ such that $\varphi(\bar{m}) = m'$. Then $z = s\varphi(\bar{m}) = \varphi(s\bar{m})$ and $s^t\varphi(\bar{m}) = \varphi(s^t\bar{m}) \in \varphi(N)$. This implies that $s^t\bar{m} \in N$, that is, $s\bar{m} \in E_M(N)$. Hence $z \in \varphi(E_M(N))$.

(ii) Assume that $x \in E_M(\varphi^{-1}(N'))$. Then there exist $r \in R$, $m \in M$ such that $x = rm$ and $r^n m \in \varphi^{-1}(N')$. This gives that $\varphi(r^n m) = r^n\varphi(m) \in N'$ and so $r\varphi(m) = \varphi(rm) \in E_{M'}(N')$. Hence $x = rm \in \varphi^{-1}(E_{M'}(N'))$ and thus $\langle E_M(\varphi^{-1}(N')) \rangle \subseteq \langle \varphi^{-1}(E_{M'}(N')) \rangle$. Now assume $x' \in \varphi^{-1}(E_{M'}(N'))$. Then $\varphi(x') \in E_{M'}(N')$, so there exist $s \in R$, $m' \in M'$ and $k \in \mathbb{Z}^+$ such that $\varphi(x') = sm'$ and $s^k m' \in N'$ and also $\varphi(y) = m'$ for some $y \in M$. We get $s^k\varphi(y) = \varphi(s^k y) \in N'$. Then $s^k y \in \varphi^{-1}(N')$ and $sy \in E_M(\varphi^{-1}(N'))$. Since $\varphi(x') = s\varphi(y)$, $x' - sy \in ker\varphi \subseteq \varphi^{-1}(N') \subseteq E_M(\varphi^{-1}(N')) \subseteq \langle E_M(\varphi^{-1}(N')) \rangle$ and $x' \in \langle E_M(\varphi^{-1}(N')) \rangle$. Hence $\langle \varphi^{-1}(E_{M'}(N')) \rangle \subseteq \langle E_M(\varphi^{-1}(N')) \rangle$. □

Corollary 4.4 *Assume the hypothesis given in Lemma 3.6. Let S be any subset of M' containing 0. Then $\varphi^{-1}(\langle S \rangle) = \langle \varphi^{-1}(S) \rangle$.*

Proof. Let $x \in \varphi^{-1}(\langle S \rangle)$. Then $\varphi(x) \in \langle S \rangle$ and thus $\varphi(x) \in N$ for all submodules N of M' containing S and $x \in \varphi^{-1}(N)$. Hence $x \in \langle \varphi^{-1}(S) \rangle$. Now let

$y \in \langle \varphi^{-1}(S) \rangle$. Then $y = r_1 m_1 + \cdots + r_n m_n$ for some $r_i \in R$ and $m_i \in \varphi^{-1}(S)$ $(1 \leq i \leq n)$. Hence $\varphi(y) = \varphi(r_1 m_1 + \cdots + r_n m_n) = r_1 \varphi(m_1) + \cdots + r_n \varphi(m_n)$ such that $\varphi(m_i) \in S$. Then $\varphi(y) \in \langle S \rangle$ and $y \in \varphi^{-1}(\langle S \rangle)$. $\square$

Lemma 4.5 *[[20], Corollary 1.3] Let M and M' be R-modules with $\varphi : M \to M'$ an R-module epimorphism and N be a submodule of M such that $N \supseteq K = Ker\varphi$. Then*

(i) $\varphi(rad_M(N)) = rad_{M'}(\varphi(N))$.

(ii) If N' is a submodule of M', then $\varphi^{-1}(rad_{M'}(N')) = rad_M(\varphi^{-1}(N'))$.

Proof. (i) Let $x \in \varphi(rad_M(N))$. Then $x = \varphi(y)$ for some $y \in rad_M(N)$. So that $y \in P_i$ where P_i is a prime submodule of M containing N for all i. Then $\varphi(y) \in \varphi(P_i)$. By Lemma 3.7, $\varphi(P_i)$ is a prime submodule of M' containing $\varphi(N)$. Hence $\varphi(y) \in \bigcap_{i \in I} \varphi(P_i) = rad_{M'}(\varphi(N))$. Hence $x \in rad_{M'}(\varphi(N))$.

Let $m' \in rad_{M'}(\varphi(N))$. Then $m' \in Q_j$ for all prime submodules Q_j of M' containing $\varphi(N)$. There exists $m \in M$ such that $\varphi(m) = m' \in Q_j$. Then $m \in \varphi^{-1}(Q_j)$ such that $\varphi^{-1}(Q_j)$ is a prime submodule of M containing N by Lemma 3.7. Hence $m \in rad_M(N)$. So that $m' = \varphi(m) \in \varphi(rad_M(N))$.

(ii) Let $n' \in \varphi^{-1}(rad_{M'}(N'))$. Then $\varphi(n') \in rad_{M'}(N')$, that is, $\varphi(n') \in P$ for all prime submodule of M' containing N'. Hence $n' \in \varphi^{-1}(P)$ and $n' \in rad_M(\varphi^{-1}(N'))$. Let $\bar{n} \in rad_M(\varphi^{-1}(N'))$. Then $\bar{n} \in P'$ for all prime submodules P' of M containing $\varphi^{-1}(N')$ and $\varphi(\bar{n}) \in \varphi(P')$. Since $\varphi(P')$ is a prime submodule of M' containing N', $\varphi(\bar{n}) \in rad_{M'}(N')$. Then $\bar{n} \in \varphi^{-1}(rad_{M'}(N'))$. Hence $rad_M(\varphi^{-1}(N')) = \varphi^{-1}(rad_{M'}(N'))$. $\square$ $\square$

Definition 4.6 *A module M satisfies the radical formula (M s.t.r.f.), if for every submodule N of M, the prime radical of N is the submodule generated by its* *envelope, that is, $rad_M(N) = \langle E_M(N)\rangle$. A ring R s.t.r.f. provided that for every R-module M, M s.t.r.f.*

Theorem 4.7 *[[20], Theorem 1] Let R be a ring. Then R s.t.r.f. provided that any one of the following is satisfied.*

(i) For every free R-module F, F s.t.r.f.,

(ii) For every faithful R-module M, M s.t.r.f.,

(iii) For every R-module M, $rad_M(0) = \langle E_M(0)\rangle$,

(iv) R is a ring homomorphic image of S, where S s.t.r.f.

Proof. Let (i) or (ii) be satisfied. Since every module M is a homomorphic image of both a free R-module and a faithful R-module, then R s.t.r.f. by Theorem 4.8.

(iii) Let N be a submodule of M and apply Theorem 4.8, letting $M' = M/N$, $N' = N$ and $\varphi = \pi$ where $\pi : M \to M/N$ is the canonical epimorphism.

(iv) Let $\varphi : S \to R$ be an epimorphism. Suppose S s.t.r.f.. An R-module M is realized as an S-module by the standard pullback along φ. Since φ is an epimorphism, every S-submodule of M is also an R-submodule, and vice-versa. Indeed, in this case, a submodule of M is prime as an S-submodule if and only if it is prime as an R-submodule. Furthermore, it is easily shown that for any submodule N of M, $E_M({}_SN) = E_M({}_RN)$. Since S-linear combinations coincide with R-linear combinations, we have

$$rad_M({}_RN) = rad_M({}_SN) = \langle E_M({}_SN)\rangle = \langle E_M({}_RN)\rangle.$$

Therefore R s.t.r.f. $\square$

Theorem 4.8 *[[20], Lemma 1.5] Assume the hypothesis given in Lemma 3.6.*

(i) If $rad_M(N) = \langle E_M(N)\rangle$, then $rad_{M'}(\varphi(N)) = \langle E_{M'}(\varphi(N))\rangle$,

(ii) If N' is a submodule of M' and $rad_{M'}(N') = \langle E_{M'}(N')\rangle$, then $rad_M(\varphi^{-1}(N')) = \langle E_M(\varphi^{-1}(N'))\rangle$.

Proof. (i) Suppose that $rad_M(N) = \langle E_M(N)\rangle$. We know that $rad_{M'}(\varphi(N)) = \varphi(rad_M(N))$. So we must show that $\varphi(\langle E_M(N)\rangle) = \langle E_{M'}(\varphi(N))\rangle$. Let $x \in \varphi(\langle E_M(N)\rangle)$. Then there exist $y \in \langle E_M(N)\rangle$, $r_i \in R$ $(1 \leq i \leq n)$ and $x_i \in E_M(N)$ such that $x = \varphi(y)$ and $y = r_1x_1 + \cdots + r_nx_n$. Also we have $x_i = a_ib_i$ such that $a_i \in R$, $b_i \in M$ and $a_i^{t_i}b_i \in N$ for some positive integer t_i and for all i. Then $x = \varphi(y) = \varphi(r_1x_1 + \cdots + r_nx_n) == r_1a_1\varphi(b_1) + \cdots + r_na_n\varphi(b_n)$ and $x \in \langle E_{M'}(\varphi(N))\rangle$, since each $a_i\varphi(b_i) \in E_{M'}(\varphi(N))$. Now let $x' \in \langle E_{M'}(\varphi(N))\rangle$. Then $x' = s_1m_1 + \cdots + s_km_k$ for some $s_i \in R$ and $m_i \in E_{M'}(\varphi(N))$ $(1 \leq i \leq k)$. Then $m_i = d_iy_i$ such that $d_i \in R$, $y_i \in M'$ and $d_i^{m_i}y_i \in \varphi(N)$ for some $m_i \in \mathbb{Z}^+$. Since $y_i \in M'$, there exist $y_i' \in M$ such that $y_i = \varphi(y_i')$ for all i. Hence we get

$$x' = s_1d_1y_1 + \cdots + s_kd_ky_k = s_1d_1\varphi(y_1') + \cdots + s_kd_k\varphi(y_k') = \varphi(s_1d_1y_1' + \cdots + s_kd_ky_k').$$

Since $d_i^{m_i}y_i \in \varphi(N)$, $d_i^{m_i}y_i' \in N$, $x' \in \varphi(\langle E_M(N)\rangle)$.

(ii) Suppose that $rad_{M'}(N') = \langle E_{M'}(N')\rangle$. By Lemma 4.5, $rad_M(\varphi^{-1}(N')) = \varphi^{-1}(rad_{M'}(N')) = \varphi^{-1}(\langle E_{M'}(N')\rangle)$. It is enough to show that $\varphi^{-1}(\langle E_{M'}(N')\rangle) = \langle E_M(\varphi^{-1}(N'))\rangle$. Let $x \in \varphi^{-1}(\langle E_{M'}(N')\rangle)$. Then $\varphi(x) \in \langle E_{M'}(N')\rangle$, so $\varphi(x) = r_1x_1 + \cdots + r_nx_n$ for some $r_i \in R$, $x_i \in E_{M'}(N')$ $(1 \leq i \leq n)$. Since $x_i \in E_{M'}(N')$, there exist $a_i \in R$ and $b_i \in M'$ such that $x_i = a_ib_i$ and $a_i^{t_i}b_i \in N'$ for some positive integer t_i. Then $x_i = a_i\varphi(c_i)$ for some $c_i \in M$ and $a_i^{t_i}\varphi(c_i) \in N'$. Hence $a_i^{t_i}c_i \in \varphi^{-1}(N')$ and so $a_ic_i \in E_M(\varphi^{-1}(N'))$. Then $\varphi(x) = r_1x_1 + \cdots + r_nx_n = \varphi(r_1a_1c_1 + \cdots + r_na_nc_n)$. Hence

$$x - (r_1a_1c_1 + \cdots + r_na_nc_n) \in ker\varphi \subseteq \langle E_M(\varphi^{-1}(N'))\rangle.$$

Thus $x \in \langle E_M(\varphi^{-1}(N'))\rangle$. Now let $y \in \langle E_M(\varphi^{-1}(N'))\rangle$. Then $y = s_1y_1+\cdots+s_ky_k$ for some $s_i \in R$, $y_i \in E_M(\varphi^{-1}(N'))$ $(1 \leq i \leq k)$. Then $y_i = u_im_i$ for some $u_i \in R$, $m_i \in M$ such that $u_i^{l_i}m_i \in \varphi^{-1}(N')$ for some positive integer l_i. This gives that $u_i\varphi(m_i) \in E_{M'}(N')$ for all i. Then

$$y = s_1u_1m_1 + \cdots + s_ku_km_k \text{ and } \varphi(y) = s_1u_1\varphi(m_1) + \cdots + s_ku_k\varphi(m_k).$$

Since $\varphi(y) \in \langle E_{M'}(N')\rangle$, $y \in \varphi^{-1}(\langle E_{M'}(N')\rangle)$. $\square$

Lemma 4.9 *Let M be an R-module and S be a multiplicatively closed subset of R. Then $\langle E_M(N)\rangle_S = \langle E_{M_S}(N_S)\rangle$ for every R-submodule N of M.*

Proof. Let $x \in E_{M_S}(N_S)$. Then $x = rm$ for some $r \in R_S$, $m \in M_S$ and $r^nm \in N_S$ for some $n \in \mathbb{Z}^+$. Then $x = (r_1/s_1)(m_1/s_2)$ and $(r_1^nm_1/s_1^ns_2) \in N_S$ for some $r_1 \in R$, $m_1 \in M$ and $s_1, s_2 \in S$. There exist $v \in N$, $s_3 \in S$ such that $(r_1^nm_1/s_1^ns_2) = v/s_3$ and $u \in S$ such that $(us_1^ns_2)v = (us_3)r_1^nm_1 \in N$. This implies that $(us_3r_1)^nm_1 \in N$ and hence $us_3r_1m_1 \in E_M(N)$. Thus

$$(us_3r_1m_1/us_3s_1s_2) = (r_1m_1/s_1s_2) = x \in \langle E_M(N)\rangle_S.$$

Therefore $\langle E_{M_S}(N_S)\rangle \subseteq \langle E_M(N)\rangle_S$. Now let $y \in \langle E_M(N)\rangle_S$. Then $y = a/s$ for some $a \in \langle E_M(N)\rangle$ and $s \in S$. There exist $r_i' \in R$, $m_i' \in M$ such that

$$a = r_1'm_1' + \cdots + r_k'm_k' \text{ with } (r_i')^{n_i}m_i' \in N, 1 \leq i \leq k$$

Then $(r_i')^{n_i}m_i'/s^{n_i} = (r_i'/s)^{n_i}m_i \in N_S$ for all i. Hence $(r_i'/s)m_i \in E_{M_S}(N_S)$ and $y = a/s \in \langle E_{M_S}(N_S)\rangle$. Therefore $\langle E_M(N)\rangle_S = \langle E_{M_S}(N_S)\rangle$. $\square$

Lemma 4.10 *[25, Proposition 1.6] Let M be an R-module and S be a multiplicatively closed subset of R. Then $(rad_M(N))_S \subseteq rad_{M_S}(N_S)$ for every R-submodule N of M.*

Proof. Let $m = \alpha/s \in (rad_M(N))_S$ for some $\alpha \in rad_M(N)$, $s \in S$. So α is contained in any prime R-submodule of M containing N. Let $\mathcal{Q}$ be a prime submodule of M_S containing N_S. Let $\mathcal{P} = \{x \in A | x/1 \in \mathcal{Q}\}$. Clearly, $\mathcal{P}$ is an R submodule of M containing N.

We claim that $\mathcal{P}$ is prime, let $ra \in \mathcal{P}$ where $r \in R$ and $a \notin \mathcal{P}$. Then $(r/1)(a/1) = (ra)/1 \in \mathcal{Q}$. Since $\mathcal{Q}$ is prime and $(a/1) \notin \mathcal{Q}$. Then $(r/1)M_S \subseteq \mathcal{Q}$. Take $y \in M$, then $(ry)/1 = (r/1)(y/1) \in (r/1)M_S \subseteq \mathcal{Q}$. So $ry \in \mathcal{P}$ which implies $rM \in \mathcal{P}$ and $\mathcal{P}$ is prime.

Therefore $\alpha \in \mathcal{P}$ and $m = \alpha/s = (1/s)(\alpha/1) \in \mathcal{Q}$ and $m \in rad_{M_S}(N_S)$.

Hence, $(rad_M(N))_S \subseteq rad_{M_S}(N_S)$ for every R-submodule N of M □

4.2 Modules over Prüfer Domains which Satisfy the Radical Formula

The question of what kind of rings and modules s.t.r.f. has drawn the attention of many authors, for example [9], [13], [17], [19], [20]. In [9], Jenkins and Smith proved that Dedekind domains s.t.r.f. In [13], Leung and Man proved that the only Noetherian rings which s.t.r.f. are of at most dimension one. He gave a complete characterization of Noetherian rings which s.t.r.f. Hence Noetherian rings which s.t.r.f. are well-known. Now we are looking for non-Noetherian rings which s.t.r.f. For that reason we investigated whether modules over Prüfer domains s.t.r.f. We proved that if R is a Prüfer domain, then the R-module $R \oplus R$ s.t.r.f. by Theorem 4.15.

Throughout $R \oplus R$ will be denoted by R^2.

Theorem 4.11 *[25, Proposition 1.8(i)] Let R be a ring. If the $R_{\mathcal{M}}$-module $R_{\mathcal{M}} \oplus R_{\mathcal{M}}$ satisfies the radical formula for any maximal ideal $\mathcal{M}$ of R, then the R-module R^2 satisfies the radical formula.*

Proof. By Lemma 4.9 and Lemma 4.10, we have

$$(\frac{rad_{R^2}(N)}{\langle E_{R^2}(N)\rangle})_{\mathcal{M}} \cong \frac{(rad_{R^2}(N))_{\mathcal{M}}}{\langle E_{R^2}(N)\rangle_{\mathcal{M}}} \subseteq \frac{rad_{R^2}(N_{\mathcal{M}})}{\langle E_{R^2_{\mathcal{M}}}(N_{\mathcal{M}})\rangle} = \frac{\langle E_{R^2_{\mathcal{M}}}(N_{\mathcal{M}})\rangle}{\langle E_{R^2_{\mathcal{M}}}(N_{\mathcal{M}})\rangle} = 0$$

for every R-submodule N of R^2. Thus $rad_{R^2}(N) = \langle E_{R^2}(N)\rangle$ for all R-submodule N of R^2 and the R-module R^2 satisfies the radical formula. $\square$

Lemma 4.12 *Let R be a commutative ring, and N be a submodule of R^2. If $N = I \oplus J$ for some ideals I, J of R, then N s.t.r.f. in R^2.*

Proof. Clearly, for any prime ideal $\mathcal{P}$ of R containing I, $\mathcal{P} \oplus R$ is a prime submodule of R^2 containing N. Thus, $rad_{R^2}(N) \subseteq \sqrt{I} \oplus R$. Similarly, $rad_{R^2}(N) \subseteq R \oplus \sqrt{J}$. Hence $rad_{R^2}(N) \subseteq \sqrt{I} \oplus \sqrt{J}$. Now take $(x, y) \in \sqrt{I} \oplus \sqrt{J}$. That is $x^k \in I$ and $y^t \in J$ for some $k, t \in \mathbb{Z}^+$ and $x^k(1,0), y^t(0,1) \in N$. Then $(x, y) = x(1,0) + y(0,1) \in \langle E_{R^2}(N)\rangle$. Since we always have the other inclusion, $rad_{R^2}(N) = \sqrt{I} \oplus \sqrt{J} = \langle E_{R^2}(N)\rangle$ and N s.t.r.f. in R^2. $\square$

Lemma 4.13 *Let D be a valuation ring and let N be a D-submodule of D^2. If (m, n) is an element of N such that $(m^k, 0) \in N$ or $(0, n^{k'}) \in N$ for some $k, k' \in \mathbb{Z}^+$, then $\sqrt{Dm} \oplus \sqrt{Dn} \subseteq \langle E_{D^2}(N)\rangle$.*

Proof. For any $x \in \sqrt{Dm}$ there exists $d \in D, l \in \mathbb{Z}^+$ such that $x^l = dm$. Hence $x^{kl}(1,0) = d^k m^k(1,0) \in N$ implies that $\sqrt{Dm}(1,0) \subseteq \langle E_{D^2}(N)\rangle$.

If $Dm \subseteq Dn$, then $m/n \in D$. Take a nonzero $s \in \sqrt{Dn}$ that is $s^t = rn$ for some nonzero $r \in D$ and $t \in \mathbb{Z}^+$. Since $s^t((m/n), 1) = (rm, rn) \in N$, and $(s(m/n))^{tk}(1, 0) = r^k(m/n)^{tk-k}(m^k, 0) \in N$ we have

$$(0, s^t) = (rm, rn) - (rm, 0) \text{ and } (0, s) = s((m/n), 1) - s(m/n)(1, 0) \in \langle E_{D^2}(N)\rangle.$$

Therefore $\sqrt{Dn}(0, 1) \subset \langle E_{D^2}(N)\rangle$.

If $Dn \subseteq Dm$, then $n/m \in D$ and $(0, n^k) = n^{k-1}(m, n) - (n/m)^{k-1}(m^k, 0) \in N$. Thus $\sqrt{Dn}(0, 1) \in \langle E_{D^2}(N)\rangle$.

In any case, $\sqrt{Dm} \oplus \sqrt{Dn} \subseteq \langle E_{D^2}(N)\rangle$.

If $(0, n^{k'}) \in N$, then the proof can be done in a similar way. $\square$

Theorem 4.14 *Let D be a valuation ring with unique maximal ideal $\mathcal{M}$. Then D^2 s.t.r.f.*

Proof. Let N be a nonzero submodule of D^2 where N is generated by $S = \{(a_i, b_i)_{i \in I}\}$. Consider the canonical projections $\pi_\lambda : D^2 \to D$ given by $\pi_\lambda(d_1, d_2) = d_\lambda$ where $d_1, d_2 \in D$, $\lambda = 1, 2$. We have $\pi_1(N) =< \{a_i\}_{i \in I} >$ and $\pi_2(N) =< \{b_i\}_{i \in I} >$.

Case 1: If $N = \pi_1(N) \oplus \pi_2(N)$, then N satisfies the radical formula in D^2 by Lemma 4.12.

Case 2: If $\pi_1(N) + \pi_2(N)$ is a finitely generated ideal of D, then $\pi_1(N) + \pi_2(N) = \sum\limits_{finite} Da_i + \sum\limits_{finite} Db_i$. Since D is a valuation ring and the ideals of D are totally ordered. So, we may assume $\pi_1(N) + \pi_2(N) = Db_1$. Then $Da_1 \subseteq Db_1$, hence $a_1/b_1 \in D$. Note that $\{(a_1/b_1, 1), (1, 0)\}$ forms a basis for D^2.

Define

$$\begin{aligned} \phi : D \oplus D &\rightarrow D \oplus D \\ (a_1/b_1, 1) &\rightarrow (0,1) \\ (1,0) &\rightarrow (1,0) \end{aligned}$$

Clearly ϕ is an isomorphism and $\phi(N) = B \oplus Db_1$ where B is an ideal of D and $B \cong N \cap (D \oplus 0)$. By case 1, $\phi(N)$ s.t.r.f. in D^2. Then by Theorem 4.8, N s.t.r.f. in D^2.

Case 3: Suppose $\pi_1(N) + \pi_2(N)$ is not a finitely generated ideal, but $\pi_1(N)$ or $\pi_2(N)$ is finitely generated. We may assume that $\pi_1(N)$ is finitely generated. Clearly $\pi_1(N)$ is nonzero. (If it is zero then N satisfies Case 1 and result is clear.) Then $\pi_1(N) = Da_i$ for some $i \in I$. Let $i = 1$. Since $\pi_1(N) + \pi_2(N)$ is not finitely generated there are infinitely many principal ideals generated by elements of $\pi_2(N)$ containing Da_1. To prove $\sqrt{\pi_1(N)} \oplus \sqrt{\pi_2(N)} \subseteq \langle E_{D^2}(N) \rangle$, take $(a_1, b_1) \in \sqrt{\pi_1(N)} \oplus \sqrt{\pi_2(N)}$. Then there exists an element $(a_s, b_s) \in S$ such that $Da_1 + Db_1 \subsetneqq Db_s$, $s \in I$. Hence $Da_sb_1 \subseteq Da_1b_1 \subsetneqq Da_1b_s$, that is $a_sb_1/a_1b_s \in \mathcal{M}$ and $1 - a_sb_1/a_1b_s$ is a unit in D. Then

$$b_s(a_1, b_1) - b_1(a_s, b_s) = (1 - a_sb_1/a_1b_s)(a_1b_s, 0) \in N, \text{ so } (a_1b_s, 0) \in N.$$

Note that $a_1^2(1,0) \in D(a_1b_s, 0) \subseteq N$, and hence $(a_i^2, 0) \in N$ for any $i \in I$. By Lemma 4.13, $\sqrt{Da_i} \oplus \sqrt{Db_i} \subseteq \langle E_{D^2}(N) \rangle$ for all $i \in I$.

Hence,

$$rad(N) \subseteq \sqrt{\pi_1(N)} \oplus \sqrt{\pi_2(N)} = \bigcup_{i \in I} \sqrt{Da_i} \oplus \bigcup_{i \in I} \sqrt{Db_i} \subseteq \langle E_{D^2}(N) \rangle.$$

Case 4: Let N be a submodule of $D \oplus D$ where $\pi_1(N)$ and $\pi_2(N)$ are not finitely generated. Recall that $S = \{(a_i, b_i)_{i \in I}\}$ is the set of generators of N. We may order the principal ideals generated by the first components of S as follows:

$$\cdots \subseteq Da_{-1} \subseteq Da_0 \subseteq Da_1 \subseteq \cdots \subseteq Da_i \subseteq \cdots .$$

We do not know how Db_i's are ordered. Define $\mathcal{P}_i = \sqrt{Da_i}$ and $\mathcal{Q}_i = \sqrt{Db_i}$ then $\sqrt{\pi_1(N)} = \bigcup \mathcal{P}_i$ and $\sqrt{\pi_2(N)} = \bigcup \mathcal{Q}_i$.

Subcase 1: For any $i \in I$, if one of the following is satisfied, then $\mathcal{P}_i \oplus \mathcal{Q}_i \subseteq < E_{D^2}(N) >$ and N s.t.r.f. in D^2.

(a) There exists $j > i$ such that $Db_j \subsetneqq Db_i$.

(b) There exists $k < i$ such that $Db_i \subsetneqq Db_k$.

(c) There exists $j_0 > i$ such that $Da_ib_{j_0} \neq Da_{j_0}b_i$ while $Db_i \subseteq Db_j$ for all $j > i$,

(d) There exists $j_1 > i$ such that $Da_ib_{j_1} \subseteq D(u_{j_1} - 1)$ while for all indices $j > i$, $Db_i \subseteq Db_j$, and $a_ib_j = u_ja_jb_i$ for some unit u_j .

Proof of Subcase 1: It is enough to prove for any i, $\mathcal{P}_i \oplus \mathcal{Q}_i \subseteq \langle E_{D^2}(N)\rangle$. Assume both a_i and b_i are nonzero, otherwise the result is clear.

Let condition (a) be satisfied. Then by assumption we have $(a_j, b_j) \in S$ such that

$$Da_ib_j \subsetneqq Da_ib_i \subseteq Da_jb_i \text{ and } a_ib_j/a_jb_i \in \mathcal{M}.$$

- if $Da_j \subseteq Db_i$, then $b_j(a_i, b_i) - b_i(a_j, b_j) = a_jb_i(a_ib_j/a_jb_i - 1)(1, 0) \in N$. Since $a_ib_j/a_jb_i - 1$ is a unit, $(a_jb_i, 0) \in N$ and s $(a_i^2, 0) \in Da_jb_i(1, 0) \subseteq N$. Hence by Lemma 4.13, $\mathcal{P}_i \oplus \mathcal{Q}_i \subseteq \langle E_{D^2}(N)\rangle$.

- If $Db_i \subseteq Da_j$, then $a_j(a_i, b_i) - a_i(a_j, b_j) = a_jb_i(1 - a_ib_j/a_jb_i)(0, 1) \in N$ and $1 - a_ib_j/a_jb_i$ is a unit implies $a_jb_i(0, 1) \in N$ that is $(0, b_i^2) \in Da_jb_i(0, 1) \subseteq N$ and $\mathcal{Q}_i(0, 1) \subseteq \langle E_{D^2}(N)\rangle$. By Lemma 4.13, $\mathcal{P}_j \oplus \mathcal{Q}_j \subseteq \langle E_{D^2}(N)\rangle$. Hence,

$$\mathcal{P}_i \oplus \mathcal{Q}_i \subseteq \mathcal{P}_j \oplus \mathcal{Q}_i \in < E_{D^2}(N) > .$$

Let condition (b) be satisfied. That is there is a $k < i$ such that $Db_k \supsetneqq Db_i$. Assume $a_k \neq 0$ (otherwise result is clear), then

$$Da_kb_i \subsetneqq Da_kb_k \subseteq Da_ib_k \text{ and } a_kb_i/a_ib_k \in \mathcal{M}.$$

- if $Da_i \subseteq Db_k$, then $b_k(a_i, b_i) - b_i(a_k, b_k) = a_ib_k(1 - a_kb_i/a_ib_k)(1, 0) \in N$. Since $1 - a_kb_i/a_ib_k$ is a unit, $(a_ib_k, 0) \in N$. Then $(a_i^2, 0) \in Da_ib_k(1, 0) \subseteq N$ and $\mathcal{P}_i(1, 0) \in \langle E_{D^2}(N)\rangle$. By Lemma 4.13, $\mathcal{P}_k \oplus \mathcal{Q}_k \subseteq \langle E_{D^2}(N)\rangle$ and hence $\mathcal{P}_i \oplus \mathcal{Q}_i \subseteq \mathcal{P}_i \oplus \mathcal{Q}_k \subseteq \langle E_{D^2}(N)\rangle$.
- If $Db_k \subseteq Da_i$, then $a_k(a_i, b_i) - a_i(a_k, b_k) = a_ib_k(a_kb_i/a_ib_k - 1)(0, 1) \in N$ and $1 - a_kb_i/a_ib_k$ is a unit implies $a_ib_k(0, 1) \in N$ and $(0, b_i^2) \in Da_ib_k(0, 1) \subseteq N$. Hence we have $\mathcal{P}_i \oplus \mathcal{Q}_i \subseteq \langle E_{D^2}(N)\rangle$ by Lemma 4.13.

Let (c) be satisfied. That is there exists $j_0 \in I$ such that $j_0 > i$ and $Da_ib_{j_0} \neq Da_{j_0}b_i$. Then one of these ideals of D is contained in the other. Let $Da_ib_{j_0} \subsetneqq Da_{j_0}b_i$ that is $a_ib_{j_0}/a_{j_0}b_i \in \mathcal{M}$ and $(a_{j_0}b_i, 0) \in N$ again we have two cases,such that $Da_{j_0} \subseteq Db_i$ or $Db_i \subseteq Da_{j_0}$.

$Da_{j_0} \subseteq Db_i$ implies $(a_i^2, 0) \in Da_{j_0}b_i(1, 0) \subseteq N$ and $Db_i \subseteq Da_{j_0}$ implies $(0, b_i^2) \in N$. For two of them, using Lemma 4.13, we have $\mathcal{P}_i \oplus \mathcal{Q}_i \in \langle E_{D^2}(N)\rangle$.

Let (d) be satisfied. That is, $a_i/a_j = u_j(b_i/b_j)$ for some unit u_j for all $j > i$. By the above argument, $a_ib_j(1 - u_j)(1, 0)$ and $a_ib_j(1 - u_j)(0, 1) \in N$ for all $j > i$. By assumption, there is $j_1 \in I$ with $j_1 > i$ such that $Da_ib_{j_1} \subseteq D(1 - u_{j_1})$ for some $j_1 > i$. Then $(a_i^4, 0)$ or $(0, b_i^4) \in N$. By Lemma 4.13, we have $\mathcal{P}_i \oplus \mathcal{Q}_i \subseteq \langle E_{D^2}(N)\rangle$ Since this equality holds for all $i \in I$, we have

$$rad(N) = \sqrt{\pi_1(N)} \oplus \sqrt{\pi_2(N)} = \bigcup \mathcal{P}_i \oplus \bigcup \mathcal{Q}_i \subseteq \langle E_{D^2}(N)\rangle.$$

Subcase 2: Suppose the possibilities in subcase 1 does not occur for some $i \in I$, then there exists $j > i$ such that $Db_i \subsetneqq Db_j, a_ib_j = u_ja_jb_i$ for some unit u_j and $D(1-u_j) \subseteq Da_ib_j$. In this case N s.t.r.f. in D^2.

<u>Proof of Subcase 2:</u> Similar to the proof of subcase 1, we have $a_ib_j(1-u_j)(1,0)$ and $a_ib_j(1-u_j)(0,1) \in N$ that is $((1-u_j)^2, 0) \in N$ for all $j > i$. Now we may assume that $Da_i \subseteq Db_i$ then define

$$\begin{array}{ccc} \phi : D \oplus D & \to & D \oplus D \\ (\frac{a_i}{b_i}, 1) & \to & (0,1) \\ (1,0) & \to (1,0) & \end{array}$$

Then $\phi(N) = (B \oplus Db_i) + < (a_k(1-u_k), b_k)_{k=i+1}^{\infty} >$ by case 2 where B is an ideal of D such that $B \cong (D \oplus 0) \cap < (a_s, b_s)_{s=1}^{i} >$. Since $((1-u_j)^2, 0) \in N$ then $(a_j(1-u_j)^2, 0) = \phi(a_j(1-u_j)^2, 0) \in \phi(N)$. By Lemma 4.13,

$$\sqrt{Da_j(1-u_j)} \oplus \sqrt{Db_j} \subseteq \langle E_{D^2}(\phi(N)) \rangle,$$

for all $j > i$. Combining this result by Lemma 4.12, we have

$$rad(\phi(N)) = \sqrt{\pi_1(\phi(N))} \oplus \sqrt{\pi_2(\phi(N))} \subseteq \langle E_{D^2}(\phi(N)) \rangle.$$

Thus $(\phi(N))$ s.t.r.f. in D^2 and by Theorem 4.8, N s.t.r.f. in D^2. $\square$

Theorem 4.15 *Let R be a Prüfer domain, then the R-module R^2 satisfies the radical formula.*

Proof. For any maximal ideal $\mathcal{M}$ of R, $R_{\mathcal{M}}$ is a valuation ring. Then by Theorem 4.14, the $R_{\mathcal{M}}$-module $R_{\mathcal{M}} \oplus R_{\mathcal{M}}$ satisfies the radical formula. By Theorem 4.11, R^2 satisfies the radical formula. $\square$

REFERENCES

[1] J.H. Alajbegovic, Noncommutative Prüfer Rings, *J. Algebra* **135**(1990), 165-176.

[2] F.W. Anderson and K.R. Fuller, *Rings and Categories of Modules* (Springer-Verlag 1974).

[3] M.F. Atiyah and I.G. Macdonald, *An Introduction to Commutative Algebra*, Reading, Mass. Addison-Wesley Publishing Company, Inc. 1969.

[4] K. Divaani-Aazar and M.A. Esmkhani, Associated Prime Submodule of Finitely Generated Modules, *Comm. Algebra, preprint*.

[5] M. Fontana, J.A. Huckaba, I.J. Papick *Prüfer Domains* (Marcel Dekker, New York 1997).

[6] S.M. George, R.L. McCasland and P.F. Smith, A Principal Ideal Theorem analogue for modules over commutative rings, *Comm. Algebra* **22**(1994), 2083-2099.

[7] R. Gilmer *Multiplicative Ideal Theory* (Queen's Papers in Pure and Applied Mathematics 1992).

[8] T.W. Hungerford, *Algebra*, (Holt, Rinehart and Winston, 1974).

[9] J. Jenkins and P.F. Smith, On the prime radical of a module over a commutative ring, *Comm. Algebra* **20**(1992), 3593-3602.

[10] I. Kaplansky, Modules over Dedekind rings, *Trans. Amer. Math. Soc.* **72**(1952), 327-340.

[11] I. Kaplansky, A Characterization of Prüfer Rings, *J. Indian. Math. Soc.* **24**(1960), 279-281.

[12] S. Kılıçarslan, *On Modules Which Satisfy The Radical Formula* (Bolu 2004).

[13] Ka Hin Leung and S. H. Man, On Commutative Noetherian Rings which Satisfy the Radical Formula, *Glasgow Math.J.*, **39** (1997), 285-293

[14] C.P. Lu, Prime submodules of modules, *Comm. Math. Univ. Sancti Pauli* **33**(1984), 61-69.

[15] C.P. Lu, M-radicals of submodules in modules, *Math. Japon.* **34**(1989), 211-219.

[16] C.P. Lu, M-radicals of submodules in modules II, *Math. Japon.* **35**(1990), 991-1001.

[17] S.H. Man, One dimensional domains which satisfy the radical formula are Dedekind domains, *Arch. Math.*, **66**(1996), 276-279.

[18] H. Matsumura, *Commutative Ring Theory*, Cambridge studies in advenced mathematics **8**.

[19] R.L. McCasland and M.E. Moore, On radicals of submodules of finitely generated modules, *Canad. Math. Bull.* **29**(1), 1986, 37-39.

[20] R.L.McCasland and M.E.Moore, On Radicals of Submodules, *Comm. Algebra*, **19**(5) (1991), 1327-1341.

[21] R.L.McCasland and M.E.Moore, Prime submodules, *Comm. Algebra* **20**(1992), 1803-1817.

[22] R.L. McCasland and P.F. Smith, Prime submodules of Noetherian modules, *Rocky Mtn. J.* **23**(1993), 1041-1062.

[23] P. Morandi, Noncommutative Prüfer Rings Satisfying a Polynomial Identity, *J. Algebra* **161**(1993), 324-341.

[24] J.J. Rotman, *Notes on Homological Algebra*, Litton Educational Publishing 1970.

[25] H. Sharif, Y. Sharifi and S. Namazi, Rings satisfying the radical formula, Acta Math. Hungar. **71**(1996), 103-108.

[26] R.Y. Sharp, *Steps in Commutative Algebra*, London Mathematical Society Student Texts 19, Cambridge University Press 1990.

[27] O. Zariski and P. Samuel, *Commutative Algebra Volume I*, The University Series in Higher Mathematics, Van Nostrand, Princeton, 1958.

INDEX