FACTORIZATION OF IDEALS IN COMMUTATIVE DOMAINS AND SOME GENERALIZATIONS OF DEDEKIND DOMAINS

DEĞİŞMELİ HALKALARDA İDEALLERİN FAKTORİZASYONU VE DEDEKİND BÖLGELERİN BAZI GENELLEMELERİ

AKİF VURAL

ASSOC. PROF. DR. BÜLENT SARAÇ
Supervisor

Submitted to Institute of Sciences of Hacettepe University
as a Partial Fulfillment to the Requirements
for the Award of the Degree of Master of Science
in Mathematics

2015

This work named **"FACTORIZATION OF IDEALS IN COMMUTATIVE DOMAINS AND SOME GENERALIZATIONS OF DEDEKIND DOMAINS"** by **AKİF VURAL** has been approved as a thesis for the Degree of **MASTER OF SCIENCE IN MATHEMATICS** by the below mentioned Examining Committee Members.

Prof. Dr. Ahmet ARIKAN
Head

Assoc. Prof. Dr. Bülent SARAÇ
Supervisor
Bülent Saraç

Prof. Dr. Adnan TERCAN
Member

Prof. Dr. Ayşe Çiğdem ÖZCAN
Member

Prof. Dr. Yücel TIRAŞ
Member

This thesis has been approved as a thesis for the Degree of **MASTER OF SCIENCE IN MATHEMATICS** by Board of Directors of the Institute for Graduate School of Science and Engineering.

Prof. Dr. Fatma SEVİN DÜZ
Director of the Institute of
Graduate School of Science and Engineering

ETHICS

In this thesis study, prepared in accordance with the spelling rules of Institute of Graduate Studies in Science of Hacettepe University,

I declare that

- all the information and documents have been obtained in the base of academic rules
- all audio-visual and written information and results have been presented according to the rules of scientific ethics
- in case of using other Works, related studies have been cited in accordance with the scientific standards
- all cited studies have been fully referenced
- I did not do any distortion in the data set
- and any part of this thesis has not been presented as another thesis study at this or any other university.

20/07/2015

Akif Vural

ABSTRACT

FACTORIZATION OF IDEALS IN COMMUTATIVE DOMAINS AND SOME GENERALIZATIONS OF DEDEKIND DOMAINS

Akif VURAL

Master of Science, Department of Mathematics

Supervisor: Assoc. Prof. Bülent Saraç

July 2015, 117 pages

This thesis consists of six chapters. In the first chapter we give some conventions as well as some basic definitions and facts. In the second chapter we investigate Prüfer and Dedekind domains. In order to give a well-known characterization of Prüfer domains in terms of their localizations at prime ideals, as a preparation, we start chapter 2 with the concept of valuations and rings defined by valuations (called valuation rings). Besides the characterization of Prüfer domains using localizations we give many other equivalent conditions for a domain to be a Prüfer domain. Then we define Dedekind domains as Noetherian Prüfer domains and give a number of characterizations of them in a similar way as we do for Prüfer domains. Thus one can compare the properties determining Prüfer domains and Dedekind domains and see which properties of Dedekind domains can be transferred if the domain lacks of Noetherian condition. In the end of the second chapter, we prove that integral closures of a Dedekind domain R in any finite extension of the field of fractions is again a Dedekind domain. This result will be given analogously for almost Dedekind domains.

In the third chapter we give definition and important properties of almost Dedekind domains. Since almost Dedekind domains are defined as generalizations of Dedekind domains, we seek properties of Dedekind domains that remains valid for almost Dedekind domains. In the next chapter we continue the study of almost Dedekind domains and give an investigation of this class of rings with the perspective of multiplication cancellation of ideals. Also we consider the factorization of ideals into radical ideals (instead of prime ideals as we consider in the case of Dedekind domains) and give a number of equivalent conditions for an almost Dedekind domain to have the radical factorization property. In fact, we deduce that the class of rings in which the radical factorization is possible lies in the class of almost Dedekind domains.

In Chapter 5, we study partially ordered abelian groups and rings which can be produced from ordered abelian groups. Moreover, we study some correspondences between a certain kind of subsets (called segments) of a lattice ordered abelian group and the ideals of the ring induced by the group. We see that such correspondences can give us ideas to construct some rings with specified properties. Among these rings, Bezout domains are of particular importance in our study of almost Dedekind domains. Thus we give a method for constructing a Bezout domain from a lattice ordered abelian group. In the last chapter, we use this method for a special lattice ordered abelian group to give the first example of an almost Dedekind domain. In this chapter we give one more example of an almost Dedekind domain with a different character.

Keywords: Dedekind domain, Prüfer domain, Valuation, Valuation ring, almost Dedekind domain, prime ideal, radical ideal, integral extension.

ÖZET

DEĞİŞMELİ HALKALARDA İDEALLERİN FAKTORİZASYONU VE DEDEKİND BÖLGELERİN BAZI GENELLEMELERİ

Akif VURAL

Yüksek Lisans, Matematik Bölümü

Danışman: Doç. Dr. Bülent Saraç

Temmuz 2015, 117 sayfa

Değişmeli halkalar teorisi cebirsel geometri ve kompleks analitik geometri gibi alanların temellerinin oluşturulmasında önemli bir yere sahip olmakla beraber, analiz topoloji, homolojik cebir ve cebirsel sayılar teorisi gibi matematiğin birçok alanı ile de çesitli bağlantılara sahiptir.

$\mathbb{Z}$ tamsayılar halkasının sıfırdan farklı her elemanının asal sayıların (sıra gözetmeksizin) tek türlü çarpımı olarak yazılması, bu halkayı önemli bir halka sınıfı olan tek türlü çarpanlara ayırma bölgeleri içinde görmemizi sağlamaktadır. En temel değişmeli halka diyebileceğimiz $\mathbb{Z}$ halkasının bazı özellikleri, 1828 yılında Gauss tarafından $\mathbb{Z}[i]$ halkası kullanılarak bulunmuş, ve böylece ele alınan halkanın bazı özelliklerinin daha geniş halkalar içinde daha kolay elde edilebileceği görülmüştür. Ancak bu genişlemeler içindeki "tamsayı" adı verilen elemanların çarpanlarına tek türlü olarak ayrılamadığı 1844 yılında Kummer tarafından farkedilmiştir. Dedekind 1871 yılında ideal kavramını ortaya atarak eleman bazında tek türlü asal çarpanlara ayrılma özelliği bulunmayan bazı halkaların ideallerinin asal ideallerinin çarpımı şeklinde tek türlü yazılabildiğini göstermiş ve günümüzde son derece önemli kabul edilen Dedekind halkalarının temellerini oluşturmuştur.

Tezin giriş kısmında, gerekli tanımlar ve bazı notasyonlardan bahsedildi. İkinci kısımda Prüfer ve Dedekind bölgeler ile ilgili karakterizasyon vermek amacıyla, değerlendirmeler ve bu değerlendirmeler tarafından tanımlanan değerlendirme halkaları incelendi. Uyumlu bir tam sıralama bağıntısıyla donatılmış tam sıralı abel grupların ve

izole altgruplarının tanımlarının verilmesinin ardından, G bir değerlendirmenin değer grubu ve V bu değerlendirmenin tanımladığı değerlendirme halkası olmak üzere; G'nin izole altgrupları ile V'nin asal idealleri arasında var olan birebir karşılık gelme gösterildi. Daha sonra integral eleman tanımı verilerek integrallik özellikleri incelendi. Kesirsel ideallerin tanım ve bazı özelliklerinin verilmesinin ardından ikinci bölümün sonunda sırasıyla sonlu üretilmiş tüm ideallerinin tersinir olmasıyla tanımlanan Prüfer bölgeler ve tüm ideallerinin asal ideallerin çarpımı olarak yazılabilmesiyle tanımlanan Dedekind bölgeler karakterize edildi ve ideallerine ait özellikler çalışıldı. Dedekind bölgelerin karakterizasyonu aşağıdaki gibidir:

Theorem. [1]R bir Noether tamlık bölgesi olmak üzere aşağıdakiler denktir:

- R bir Dedekind bölgedir.
- R integral kapalıdır ve sıfırdan farklı her asal ideali maksimaldir.
- R'nin iki eleman ile üretilmiş sıfırdan farklı tüm idealleri tersinirdir.
- A, B, C R'nin idealleri olmak üzere $A \neq 0$ ve $AB = AC$ ise $B = C$'dir.
- Her M maksimal ideali için R_M bir değerlendirme halkasıdır.
- A, B, C R'nin idealleri olmak üzere, $A(B \cap C) = AB \cap AC$ sağlanır.
- A, B R'nin idealleri olmak üzere, $(A + B)(A \cap B) = AB$ sağlanır.
- A ve B R'nin $A \subseteq B$ koşulunu sağlayan idealleri ise $A = BC$ olacak şekilde R'nin bir C ideali vardır.
- A, B, C R'nin idealleri olmak üzere, $\big((A + B) : C\big) = (A : C) + (B : C)$ sağlanır.
- A, B, C R'nin idealleri olmak üzere $\big(C : (A \cap B)\big) = (C : A) + (C : B)$ sağlanır.
- A, B, C R'nin idealleri olmak üzere $A \cap (B + C) = (A \cap B) + (A \cap C)$ sağlanır.
- Her P maksimal ideali için $P^2 \subset I \subset P$ olacak şekilde I ideali yoktur.
- Her P maksimal ideali için P-primary idealler P'nin bir kuvvetidir.
- Her P maksimal ideali için P-primary idealler kümesi tam sıralıdır.

- R'nin her üsthalkası (overring) flat üsthalkadır.
- R'nin her üsthalkası integral kapalıdır.

Bu bölümde verdiğimiz önemli bir sonuç ise bir Dedekind bölgenin kesirler cisminin sonlu genişlemesi içindeki integral kapanışının yine bir Dedekind bölge olduğudur.

Tezin üçüncü kısmında bütün maksimal ideallerindeki yerelleştirmeleri Dedekind bölge olan hemen hemen Dedekind bölgeleri ve ideal yapısı incelendi. Bölüm sonunda Dedekind bölgeler için gördüğümüz bir teoremin hemen hemen Dedekind bölgeler için de sağlandığını söyledik:

Theorem. [2, Corollary 4]D hemen hemen Dedekind bölge, K D'nin kesirler cismi, L K'nın sonlu cisim genişlemesi ve D' D'nin L içindeki integral kapanışı ise, D' hemen hemen Dedekind bölgedir.

Dördüncü kısımda değişmeli halkalarda sadeleştirme kurallarından bahsedildi. R bir halka ve A, B ve C idealler olmak üzere $AB = AC$ olması $B = C$ olmasını $AB \neq 0$ koşulu altında gerektiriyorsa, R'ye "kısıtlanmış sadeleştirme kuralını (RCL) sağlar" denir. Bahsi geçen gerektirme $A \neq 0$ koşulu altında sağlanıyorsa R'ye "sadeleştirme kuralını (CL) sağlar" denir. $AB = AC$ eşitliği, $B = C$ eşitliğini $A \neq 0$ ve A sonlu üretilmiş olduğunda gerektiriyorsa, R'ye "sonlu sadeleştirme kuralını (FCL) sağlar" denir. Bu bölümde kısıtlanmış sadeleştirme kuralını sağlayan halkaların bir karakterizasyonu verildi. Ayrıca sonlu sadeleştirme kuralını sağlayan bir tamlık bölgesinin integral kapalı olduğu sonucu verildi. Daha önceki bölümde özelliklerini incelediğimiz hemen hemen Dedekind bölgelerin bir karakterizasyonu da bu bölümde aşağıdaki gibi yer aldı:

Theorem. [3, Theorem 3]D bir tamlık bölgesi olsun. Bu durumda D'de sadeleştirme kuralı sağlanır, ancak ve ancak D bir hemen hemen Dedekind bölgedir.

Tamlık bölgelerinde ideallerin tek türlü çarpanlara ayrılması hususunda Dedekind'in sonucunun geliştirilemeyeceğine dair aşağıdaki sonuca da bu kısımda yer verildi:

Theorem. [3, Theorem 8]S bir halka ve $\mathscr{S}$, S'nin idealerinin öyle bir ailesi olsun ki, S'nin her ideali $\mathscr{S}$'nin sonlu sayıda elemanının çarpımı olarak tek türlü ifade edilsin. Eğer S bir tamlık bölgesi ise, bu durumda S bir Dedekind bölge ve $\mathscr{S}$, S'nin asal ideallerinin kümesidir.

Yine bu kısımda tüm idealleri radikal ideallerin bir çarpımı olarak yazılabilen SP-bölgeler tanımlandı ve hemen hemen Dedekind bölgeler sınıfında karakterize edildi. Ve son olarak SP-bölgelerin hemen hemen Dedekind olduğuna dair Vaughan ve Yeagy'nin sonucuna yer verildi.

Theorem. [4, Theorem 2.1]R bir hemen hemen Dedekind bölge olmak üzere aşağıdakiler denktir:

- R bir SP-bölgedir.
- R'nin sıfırdan farklı her I öz ideali $J_1 \subseteq \ldots \subseteq J_n$ koşulunu sağlayan $J_i, i = 1, \ldots, n$ radikal idealleri için $I = J_1 \ldots J_n$ olarak tek türlü ifade edilebilir.

Theorem (Vaughan and Yeagy)**.** [5, Theorem 2.4]Her SP-bölge bir hemen hemen Dedekind bölgedir.

Beşinci kısımda, vereceğimiz bir hemen hemen Dedekind bölge örneği için gerekli altyapıyı sağlamak amacıyla kısmen sıralı abel gruplar ile latis sıralı abel gruplar incelendi. G latis sıralı abel grup, S G'nin bir altkümesi olmak üzere,

- $S \subset G^+$,
- S filtredir, yani $x \in S, y \in G$ ve $y > x$ ise $y \in S$ sağlanır,
- $x, y \in S$ ise $inf\{x, y\} \in S$

özelliklerini sağlarsa, S'ye G'nin bir segmenti denir. $x, y \in G^+ \setminus S$ durumunda $x + y \in G^+ \setminus S$ oluyor ise, S'ye bir asal segment denir.

G latis sıralı abel grup olsun. S G^+'nın $G^+ \setminus S$ filtre olacak şekildeki bir alt yarıgrubu olsun. $H_S = \{g_1 - g_2 | g_1, g_2 \in S\}$ şeklinde tanımlansın. P G'nin bir asal segmenti ve $S = G^+ \setminus P$ olduğu durumda G/H_s bölüm grubu G_P ile gösterilir ve G'nin P asal segmentindeki yerelleştirmesi olarak adlandırılır.

Bütün sonlu üretilmiş idealleri temel ideal olan tamlık bölgelerine Bezout bölge denir. Bu kısımda Bezout bölgeler ile latis sıralı abel gruplar arasındaki ilişkiye yer verildi. Öncelikli olarak bir Bezout bölgenin bölünebilirlik grubunun latis sıralı abel grup olduğunu söyledik. Daha sonra R bir Bezout bölge ve G R'nin bölünebilirlik grubu ise, R'nin öz idealleri ile G'nin segmentleri arasnda sıralamayı, asallık ve maksimallik ilişkilerini koruyan birebir karşılık gelmenin varlığı gösterildi. Kısım sonunda aşağıdaki teoreme yer verildi:

Theorem (Krull-Kaplansky-Jaffard-Ohm). *[6, p. 164]* G latis sıralı bir abel grup ise, bölünebilirlik grubu G'ye latis izomorf olan bir Bezout bölge vardır.

Son kısımda ise tez boyunca altyapısını oluşturduğumuz iki hemen hemen Dedekind bölge örneğine yer vererek tezi tamamladık.

Anahtar Kelimeler: Dedekind bölge, Prüfer bölge, Değerlendirme, Değerlendirme halkaları, hemen hemen Dedekind bölge, asal ideal, radikal ideal, integral genişleme.

ACKNOWLEDGEMENTS

I would like to gratefully acknowledge various people who have been journeyed with me in recent years as I have worked on this thesis. I would like to thank my supervisor Assoc. Prof. Bülent Saraç for sparing his precious time and for his help. It would not have been possible to complete this thesis without his comments and suggestions. I would like to thank Department of Mathematics of Hacettepe University and the members of it. I would also like to extend my appreciation to my committee members Prof. Dr. Ahmet Arıkan, Prof. Dr. Adnan Tercan, Prof. Dr. Ayşe Çiğdem Özcan and Prof. Dr. Yücel Tıraş for their advise during the research.

A special word of thanks goes to my parents for their continuous support and encouragement. Last 8 years I lived with my aunt and my grandparents, I would also like to thank them for their patience and support especially in the period of the study of this thesis. I would also like to dedicate this thesis to my grandparents. I believe that I am tremendously fortunate in my life to have grandparents who have shown me unconditional love and support. The relationships and bonds that I have with my grandparents hold an enormous amount of meaning to me.

It is impossible to mention all of my friends here one by one, so I would also like to thank all my friends who feel the excitement and exhaustion same as I feel. Thank all of you for being next to me when I need you.

Finally, I would like to say that, my study for this thesis was supported by TÜBİTAK (The Scientific and Technological Research Council of Turkey) and I would like to thank TÜBİTAK for their financial support (TUBITAK-3501 Career Development Program, Project No: 113F032).

Contents

1 INTRODUCTION

Multiplicative Ideal Theory began with the works of Julius Wilhelm Richard Dedekind, a famous German mathematician, at the end of the 19th century, by which he aimed to repair the lack of unique factorization property of elements in an integral domain. In these works, he considered integral domains in which factorizations of ideals into prime ideals are possible, which constitute an important class of rings in today's mathematics, called Dedekind domains. Dedekind domains play an important role in Algebraic Number Theory and Algebraic Geometry. In 20th century (mostly in the second half), there appeared many classes of integral domains which arise as generalizations of Dedekind domains, including Prüfer domains (and valuation rings in a particular case) and almost Dedekind domains. In this thesis, we study the classes of Prüfer domains and almost Dedekind domains and expose some properties in which these two classes differ from or resemble to Dedekind domains.

We assume that the reader has knowledge of groups, rings, fields and modules taught in first year graduate courses. Because the definitions of groups, rings and fields are widely known concepts, we only remark here that modules are defined in exactly the same way as vector spaces only with the difference on the scalar field which is taken to be a ring in this case. There is an extensive study of module theory in the literature; however, we need only some basic knowledge from that theory which can be found in [7].

The symbol $\subseteq$ will stand for "a subset of", and the symbol $\subset$ is spared for the strict inclusion. The set of rational numbers, integers and natural numbers, respectively, denoted by $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$.

Let A be a nonempty set and suppose that there is a relation $\leq$ defined on A. If $\leq$ is reflexive and transitive, that is, if $a \leq a$; and if $a \leq b$ and $b \leq c$ implies $a \leq c$ for all $a, b, c \in A$, respectively, then we say that $\leq$ is a preorder on A, or that A is preordered under $\leq$. Moreover, if, additionally, $\leq$ is anti-symmetric, that is $a \leq b$ and $b \leq a$ implies $a = b$ for all $a, b \in A$, then we say that $\leq$ is a partial order, and that A is partially ordered under $\leq$. In the case that we have $a \leq b$ or $b \leq a$ for all $a, b \in A$ in a partially ordered set A, we say that $\leq$ is a total order on A, or A is totally ordered under $\leq$. We shortly say A is ordered under $\leq$ if A is totally ordered under $\leq$.

One important case for partially ordered sets occurs when we consider the set of ideals of any ring. Recall that a nonempty set consisting of ideals of a ring is partially ordered by inclusion. Recall also that a commutative ring R is said to be Noetherian if every nonempty set of ideals of R satisfies the maximal condition, i.e., every nonempty set of ideals of R has a maximal element with respect to inclusion. This notion can also thought for modules over R by replacing the term "ideals" by "submodules". Thus a commutative ring R is a Noetherian ring if and only if it is Noetherian as a module over itself. One important result for Noetherian modules states that if M is a Noetherian R–module, then every submodule of M is finitely generated, and vice versa.

In our study, all rings considered are commutative with unity. Noetherian rings have an important property which we give in the following theorem, known as the Krull Intersection Theorem:

Theorem (Krull Intersection Theorem). *Let R be a Noetherian ring and I an ideal of R contained in the Jacobson radical of R (i.e., the intersection of all maximal ideals of R). Then*

$$\bigcap_{n>0} I^n = 0.$$

Let R be a ring and let S be a nonempty subset of R. We say that S is a multiplicatively closed subset of R, if $0 \notin S$ and $a, b \in S$ implies that $ab \in S$. If the inclusion relation between R and S is clear, we simply say S is a multiplicatively closed set. Recall that we can form a ring if we put a certain equivalence relation on $R \times S$, consider the set of all equivalence classes, written as fractions, and define addition and multiplication on this set, just as we do when constructing rationals from integers. The resulting ring is called the ring of fractions of R with respect to S, denoted by $S^{-1}R$ or R_S.

Let R be a ring, and let $a \in R$. If there exists $b \in R$ with $b \neq 0$ such that $ab = 0$, then a is called a zero-divisor of R. If $a \in R$ is not a zero-divisor, then it is called a regular element of R. If S is the set of all regular elements of R, then S becomes a multiplicatively closed set. In this case, $S^{-1}R$ is called the total quotient ring of R. In the case that R is an integral domain, S becomes $R \setminus \{0\}$ and so the total quotient ring $S^{-1}R$ becomes the field of fractions of R. The field of fractions K of an integral domain R is the smallest field that contains R. If K is the field of fractions of R, then $K = \{ab^{-1} | a, b \in R, b \neq 0\}$.

Let R be a ring and K be the total quotient ring of R. Then T is an overring of

R means that T is a ring such that $R \subseteq T \subseteq K$. If R is an integral domain, and if T is an overring of R, then T becomes an integral domain, and K becomes the field of fractions of R, in which case K becomes also the field of fractions of T.

Let R' be a ring and R be a subring of R'. For an $a \in R'$, if $b_0 + b_1 a + \ldots + b_{n-1}a^{n-1} + a^n = 0$ holds for some $b_0, \ldots, b_{n-1} \in R$ with $n \geq 1$, then we say that a is integral over R. If every element of R' is integral over R, then we say that R' is integral over R, or $R \subseteq R'$ is an integral extension of rings. If the set of elements of R' which are integral over R is equal to R, then we say that R is integrally closed in R'. In particular, if R' is the total quotient ring of R, then we simply say that R is integrally closed. It is well–known that the set of elements of R' which are integral over the ring R form a ring, called the integral closure of R in R'. When we just use the term "integral closure", we mean the integral closure in the total quotient ring, or in the field of fractions if R is an integral domain.

Let R be a ring and I be an ideal of R. We define the radical of I as the set $\{a \in R | a^n \in I \text{ for some } n \in \mathbb{N}\}$, and denote it by $\sqrt{I}$. We refer the reader to [8] for detailed information about radicals and their arithmetic properties. If we have an ideal Q of R such that $\sqrt{Q} = P$ and for $x, y \in R$ with $xy \in Q$, $x \notin Q$ implies that $y \in P$, then we call Q a P-primary ideal of R. Note that if Q is a P–primary ideal of R, then P is a prime ideal of R, but not conversely. Note also that any ideal whose radical is a maximal ideal, say M, is an M–primary ideal. It follows that if M is a maximal ideal of R, then every power M^i of M are M–primary ideals of R. The reader should be careful in that there may be M–primary ideals other than powers of M in general (see, for example [8, Example 4.11]).

2 PRUFER AND DEDEKIND DOMAINS

Throughout this section we use [1] as reference, so we do not mention it again in this section.

2.1 Valuations and Valuation Domains

Definition 2.1. An integral domain V is called a valuation ring, if it satisfies the property that for any ideals A and B, either $A \subseteq B$ or $B \subseteq A$.

Proposition 2.2. *The following statements are equivalent for an integral domain V:*

(1) *V is a valuation ring.*

(2) *For any $a, b \in V$, either $(a) \subseteq (b)$ or $(b) \subseteq (a)$.*

(3) *If K is the field of fractions of V and $x \in K$, then either $x \in V$ or $x^{-1} \in V$.*

Proof. (1) implies (2) is clear. To show (2) implies (3), let $x \in K$. So $x = a/b$ for some $a, b \in V$ with $b \neq 0$. If $(a) \subseteq (b)$, then $a = br$ for some $r \in V$, then $x = a/b = r \in V$. If $(b) \subseteq (a)$, then $b = ar$ for some $r \in V$, and this gives that $r = b/a = x^{-1} \in V$. For the last part of the proof, suppose for any element x of the field of fractions K of V, either x or x^{-1} belongs to V. Let A and B be ideals of V. Suppose $A \not\subseteq B$. Then there exists $a \in A \setminus B$. Let $b \in B$ be nonzero. If $a/b \in V$, then we have $a \in (b) \subseteq B$, which is a contradiction, so we have $b/a \in V$. Hence $b \in (a) \subseteq A$. Since b is an arbitrary nonzero element of B, then $B \subseteq A$, hence V is a valuation ring. □

Corollary 2.3. *Each overring of a valuation ring is a valuation ring.*

Proof. Let V be a valuation ring, and let V' be an overring of V. If K is the field of fractions of V, then $V \subseteq V' \subset K$. In this case K is also the field of fractions of V'. Since an arbitrary element of K or its inverse belongs to V by Proposition 2.2, $V \subseteq V'$ implies that it belongs to V', so this implies V' is a valuation ring. □

Proposition 2.4. *For a valuation ring V, the set of non-units of V is an ideal, which is the unique maximal ideal of V.*

Proof. Let P be the set of non-units of V. Let $a, b \in P \setminus \{0\}, c \in V$. Clearly ac is a non-unit of V so it belongs to P. We may assume without loss of generality that $a/b \in V$. Then $a - b = \left(\frac{a}{b} - 1\right) b \in P$. Thus P is an ideal of V. If I is a proper ideal of P, then every element of I is a non-unit, since otherwise we have $I = V$. Then we have $I \subseteq P$. Since every ideal is contained by P, then P is the unique maximal ideal of V. □

Proposition 2.5. *Valuation rings are integrally closed.*

Proof. Let V be a valuation ring with field of fractions K, and let $x \in K$ be integral over V. Say $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ for some $a_0, \ldots, a_{n-1} \in V$. If $x \notin V$, then $x^{-1} \in V$. By multiplying the equality with x^{1-n}, we have that $x = -(a_{n-1} + a_{n-2}x^{-1} + \ldots + a_0 x^{1-n}) \in V$, which is a contradiction. Hence an element which is integral over V must be an element of V. □

Proposition 2.6. *Let R be an integral domain and K be its field of fractions. Then there exists a valuation ring V such that $R \subseteq V \subset K$.*

Before proving this proposition, we shall give some definitions and state a lemma which we use for the proof.

Let K be a field. Let ϕ be a homomorphism from a proper subring K_ϕ of K into an algebraically closed field. ϕ is called a partial homomorphism on K. If we set $\mathscr{S}$ as the set of such pairs and define an ordering $\leq$ on $\mathscr{S}$ by $(\phi, K_\phi) \leq (\psi, K_\psi)$ if and only if $K_\phi \subseteq K_\psi$ and $\phi(a) = \psi(a)$ for all $a \in K_\phi$, then $\mathscr{S}$ becomes a partially ordered set under $\leq$. Then by Zorn's Lemma, if $(\phi, K_\phi) \in \mathscr{S}$, then there exists a maximal element of $\mathscr{S}$ which is greater than or equal to (ϕ, K_ϕ). Such a maximal element is called a maximal partial homomorphism.

Lemma 2.7. *Let K be a field and let $x \in K$ be nonzero. Let V be a subring of K with unique maximal ideal P. Then either $PV[x] \neq V[x]$ or $PV[x^{-1}] \neq V[x^{-1}]$.*

Proof. By the way of contradiction, assume that $PV[x] = V[x]$ and $PV[x^{-1}] = V[x^{-1}]$. Then we have

$$a_0 + a_1 x + \ldots + a_k x^k = 1 \tag{1}$$

and

$$b_o + b_1 x^{-1} + \ldots + b_m x^{-m} = 1 \tag{2}$$

for some $a_0, \dots, a_k, b_0, \dots, b_m \in P$. We shall choose m and k be the smallest integers satisfying above equations, and without loss of generality, assume that $k \leq m$. Multiplying equation 2 by x^k, we have $(1 - b_0)x^k = b_1 x^{k-1} + \ldots + b_k$. Since $b_0 \in P$ and P is the unique maximal ideal of V, then we have $1 - b_0$ is a unit in V, hence

$$\begin{aligned} x^k &= (1-b_0)^{-1} b_1 x^{k-1} + \ldots + (1-b_0)^{-1} b_k \\ &= c_1 x^{k-1} + \ldots + c_k \end{aligned}$$

where $c_1, \dots, c_k \in P$. If we use this in equation 1, we have

$$\begin{aligned} 1 &= a_0 + a_1 x + \ldots + a_{m-1} x^{m-1} + a_m x^{m-k}(c_1 x^{k-1} + \ldots + c_k) \\ &= d_0 + d_1 x + \ldots + d_{m-1} x^{m-1} \end{aligned}$$

where $d_0, \dots, d_{m-1} \in P$. This is a contradiction with the minimality of m, hence our assumption is false. □

Lemma 2.8. *Let V be a subring of the field K. Then if there exists a homomorphism ϕ from V into an algebraically closed field with (ϕ, V) is a maximal partial homomorphism, then V is a valuation ring with field of fractions K.*

Proof. Let L be an algebraically closed field. Let $\phi : V \to L$ be a homomorphism such that (ϕ, V) is a maximal partial homomorphism. Let $P = Ker\,\phi$. P is a prime ideal of V since $\phi(1) = 1$. Let $u \in V \setminus P$, then $\phi(u)$ is a unit in L, so there exists an extension $\phi' : V_P \to L$ of ϕ defined by $\phi'(\frac{a}{s}) = \frac{\phi(a)}{\phi(s)}$ for $a \in V, s \in V \setminus P$. This implies that $(V, \phi) \leq (V_P, \phi')$. But since (ϕ, P) is maximal, then $V_P = V$. This gives that P is the unique maximal ideal of V.

Now let $x \in K$ be nonzero. If we show that $x \in V$ or $x^{-1} \in V$, then we are done. By Lemma 2.7, we may assume that $PV[x] \neq V[x]$, without loss of generality. Then there exists $M \in Max(V[x])$ such that $PV[x] \subseteq M$, then $M \cap V = P$ since P is the only maximal ideal of V. It follows that $\sigma : \frac{V}{P} \to \frac{V[x]}{M}$ given by $\sigma(a + P) = a + M$ is an injective homomorphism. It follows that $\frac{V[x]}{M} = \sigma(\frac{V}{P})[x + M]$. Now $x + M$ is algebraic over $\sigma(\frac{V}{P})$ since $\frac{V[x]}{M}$ is a field. Hence, if $\bar{\phi} : \frac{V}{P} \to L$ is given by $\bar{\phi}(a + P) = \phi(a)$, then we can extend $\bar{\phi}\sigma^{-1} : \sigma(\frac{V}{P}) \to L$ to an injective homomorphism $\psi : \frac{V[x]}{M} \to L$. If we set $\pi : V[x] \to \frac{V[x]}{M}$ as the canonical homomorphism, then since for all $a \in V$, $\psi\pi(a) = \psi(a + M) = \bar{\phi}(a + P) = \phi(a)$ holds, we have $(\phi, V) \leq (\psi\pi, V[x])$. It follows by the maximality of (ϕ, V) that $V = V[x]$ or $x \in V$. Hence V is a valuation ring. $\square$

Proof of Proposition 2.6. Let R be a ring with field of fractions K. Since R is a subring of K, we can define a partial homomorphism ϕ_0 from R into an algebraically closed field L. If $\mathscr{S}$ is the family of all partial homomorphism, then clearly we have a maximal partial homomorphism (ϕ, V) such that $(\phi_0, R) \leq (\phi, V)$. This relation implies $R \subseteq V \subset K$, and by Lemma 2.8, the maximality of (ϕ, V) implies that V is a valuation ring. $\square$

Corollary 2.9. *Let R be an integral domain and let K be the field of fractions of R. The integral closure of R is the intersection of all the valuation rings of K which contains R.*

Proof. Denote the integral closure of R by $\bar{R}$. By Proposition 2.5 we have that valuation rings are integrally closed, then $\bar{R}$ must be contained in the intersection of all valuation rings of K which are containing R. Otherwise, there exist $x \in \bar{R}$ such that x is not belong to one of the valuation rings of K containing R. Since x is integral over R implies x is integral over the containing valuation rings, it is a contradiction since x doesn't belong to at least one of the valuation rings. If we show that for any element x of the field of fractions K, $x \notin \bar{R}$ implies that x doesn't belong to the intersection mentioned above, then the desired equality holds.

Let $x \in K \setminus \bar{R}$. Then $x \notin R[x^{-1}]$. For otherwise, there exists $f(X) \in R[X]$, of degree n, such that $x = f(x^{-1})$. By multiplying last equality with x^n, we have that $x^{n+1} - x^n f(x^{-1}) = 0$, which gives that $x \in \bar{R}$, a contradiction. Hence x^{-1} is not a unit in $R[x^{-1}]$, so there exists a maximal ideal P of $R[x^{-1}]$ such that $x^{-1} \in P$.

Let L be the algebraic closure of $\frac{R[x^{-1}]}{P}$. The canonical homomorphism $R[x^{-1}] \to \frac{R[x^{-1}]}{P}$ furnishes us with a homomorphism $\Pi : R[x^{-1}] \to L$. Let (ϕ, V) be a maximal partial homomorphism of K into L such that $(\Pi, R[x^{-1}]) \leq (\phi, V)$. By Lemma 2.8, V is a valuation ring of K, and $R \subseteq V$. Since we have $\phi(x^{-1}) = 0$, then $x \notin V$. Hence x is not in the intersection of all the valuation rings of K which contain R. So the desired equality holds. $\square$

For Noetherian rings, we can characterize valuation rings by much weaker conditions than for arbitrary rings.

Theorem 2.10. *Let V be a Noetherian integral domain which is not a field. Then the following statements are equivalent:*

(1) *V is a valuation ring.*

(2) *The set of non-units of V is a nonzero principal ideal.*

(3) *V is integrally closed and has exactly one nonzero prime ideal.*

Proof. Firstly, suppose V is a valuation ring and let P be the set of non-units. Since V is not a field, we have $P \neq (0)$ and clearly P is an ideal. The fact that V is Noetherian implies P is finitely generated, say $P = (a_1, \dots, a_n)$. Since V is a valuation ring, then the ideals $(a_1), \dots, (a_n)$ give us a chain, without loss of generality suppose $(a_1) \subseteq \dots \subseteq (a_n)$, and this implies $P = (a_n)$, a principal ideal.

Now, suppose that P is the ideal of non-units of V, and K be the field of fractions of V. Let $P = (a)$ for some $a \in P$ with $a \neq 0$. Clearly there is no maximal ideal other than P. By the Krull Intersection Theorem, we have $\bigcap\limits_{n \geq 1} P^n = (0)$, so if $I \neq (0)$ is a proper ideal of V, then there exists $k \geq 1$ such that $I \subseteq P^k$ but $I \nsubseteq P^{k+1}$. Let $b \in I \setminus P^{k+1}$, then $b = a^k u$ for some unit $u \in V$. Now if $c \in P^k$, then for some $d \in V$, $c = a^k d = bu^{-1}d \in I$. So this gives that $I = P^k$. Since every ideal of V is a power of P, and the only prime ideal which is a power of P is itself, then P is the only nonzero prime ideal of V.

Now let $c \in K$ be nonzero and integral over V, set $c = r/s$ for some $r, s \in V \setminus \{0\}$. Since r and s are both a product of a unit and some power of a, we may assume that either r or s is a unit. Since c is integral over V, then there exist $b_0, \dots, b_{n-1} \in V$ such that $b_0 + b_1 c + \dots + b_{n-1} c^{n-1} + c^n = 0$. If we multiply the equality by s^n, then we'll have $r^n + s\, b_{n-1} r^{n-1} + \dots + s^{n-1} b_1 r + s^n b_o = 0$ or $r^n = -s\,(s^{n-1} b_0 + s^{n-2} b_1 r + \dots + b_{n-1} r^{n-1})$. If s is unit, then $c \in V$. If s is a non-unit then by the last equality, $r^n \in P$ and so $r \in P$. So r is also non-unit, and this is a contradiction with our assumption. Hence s is unit and $c \in V$, thus V is integrally closed.

For the last part, assume that V is integrally closed and has exactly one nonzero prime ideal P. It suffices to show that P is principal.

Now let K be the field of fractions of V, and set $P^* = \{x \in K | xP \subseteq V\}$. Then P^*P is an ideal of V such that $P \subseteq P^*P \subseteq V$. If P^*P is strictly between P and V, then we must have a maximal ideal, hence a prime ideal which contains P^*P and it contradicts the fact that P is the only nonzero prime ideal, so we either have $P = P^*P$ or $P^*P = V$.

Assume that $P^*P = P$ and let $P = (a_1, \dots, a_n)$. Let $a \in P^*$, then we have $aP \subseteq P$. And this gives us $a\, a_i = \sum_{j=1}^{n} r_{ij}\, a_j$ where $r_{ij} \in V$. So we have that $\sum_{j=1}^{n} (\delta_{ij}a - r_{ij})a_j = 0$ for $i = 1, \dots, n$ where $\delta_{ij} = \begin{cases} 1 & , i = j \\ 0 & , i \neq j \end{cases}$. Hence, since $a_j \neq 0$ for at least one $j = 1, \dots, n$ and we are working in K, we have $det[\delta_{ij}a - r_{ij}] = 0$. Thus, a is integral over V and since V is integrally closed, $a \in V$. So $P^* \subseteq V$. This gives us $P^* = V$ since we clearly have $V \subseteq P^*$.

Now we shall show that $P^* = V$ leads us to a contradiction. Let $a \in P$ be nonzero. Set $S = \{a^n | n \in \mathbb{N} \setminus \{0\}\}$. Our claim is that $S^{-1}V = K$. By the way of contradiction, suppose $S^{-1}V$ is not the field of fractions of V, then $S^{-1}V$ has a nonzero maximal ideal P'. Since a is a unit in $S^{-1}V$, we have $a \notin P'$, hence $P' \cap V \neq P$, and consequently $P' \cap V = (0)$. However this can't be true, since if $\frac{c}{a^n} \in P' \setminus \{0\}$, then $c \neq 0$ and $c \in P' \cap V$. So we have $K = S^{-1}V$, which gives that every element of K can be written in the form b/a^n for some $b \in V$ and $n \in \mathbb{N}$.

Now if $c \in V$ is nonzero, then $\frac{1}{c} = \frac{b}{a^n}$ for some n, and so $a^n = cb \in (c)$. Thus, for each $a \in P$, some power of a is in (c). Since P is finitely generated, then we have $P^n \subseteq (c)$ for some smallest positive integer n. Let $d \in P^{n-1}, d \notin (c)$, then $dP \subseteq (c)$ and so $(\frac{d}{c})P \subseteq V$. This gives that $\frac{d}{c} \in P^*$, but $\frac{d}{c} \notin V$, hence $P^* \neq V$. This contradiction gives us $P^*P \neq P$, so we have $P^*P = V$.

Since $P^*P = V$, then there exist elements $a_1, \dots, a_k \in P$ and $b_1, \dots, b_k \in P^*$such that $\sum_{i=1}^{k} a_i b_i = 1$. So for some $i = 1, \dots, k$, we have $a_i b_i \notin P$. So we have elements $a \in P, b \in P^*$ with $ab = u$ for some unit u in V. Then we have $abu^{-1} = 1$, and by multiplying by c, we have $c = abcu^{-1}$. Now $bc \in V$ implies that $c \in (a)$, and since c is arbitrary in P, we have $P = (a)$.

Since the unique prime ideal P of V is principal, every nonzero ideal of V can be represented as a power of P as we have done above at paragraph 2 of this proof. Hence, the set of ideals of V is totally ordered under inclusion, and V is a valuation ring. □

Theorem 2.11. *Let V be a valuation ring and let I be an ideal of V. Then*

(1) $\sqrt{I}$ *is a prime ideal of V.*

(2) *If $J = \bigcap\limits_{n=1}^{\infty} I^n$, then J is a prime ideal of V such that every prime ideal of V which is properly contained in I is contained by J.*

Proof.

(1) We know that $\sqrt{I}$ is the intersection of minimal prime ideals of I. Since the set of ideals of V is totally ordered, then I has only one minimal prime ideal, which must be equal to $\sqrt{I}$.

(2) First, we shall show that J is a prime ideal. So let $a, b \notin J$, then $a \notin I^m, b \notin I^n$ for some $m, n \in \mathbb{N}$. Then we have that $I^m \subset (a)$ and $I^n \subset (b)$. We also have that $I^m(b) \subseteq (a)(b) = (ab)$. Actually we have $I^m(b) \neq (ab)$. Since we have $I^m \subset (a)$, then there exists $x \in V$ such that $xa \notin I^m$. If $I^m(b) = (ab)$, then $yb = xab$ for some $y \in I^m$. Since $b \neq 0$, this implies that $y = xa \in I^m$, a contradiction. Thus $I^m(b) \subset (ab)$. Hence we have that $I^{n+m} \subseteq I^m(b) \subset (ab)$, and this gives that $ab \notin I^{n+m}$, so $ab \notin J$. Hence J is a prime ideal of V.

Now if P is a prime ideal of V such that $P \subset A$, then every power of A lies outside of P. For otherwise, $A^n \subseteq P$ for $n \in \mathbb{N}$ implies $A \subseteq P$, which is impossible. Since V is a valuation ring, we have that $P \subset A^n$ for each $n \in \mathbb{N}$, and hence $P \subseteq J$.

□

Lemma 2.12. *Let V be a valuation ring and let K be the field of fractions of V. If A and B are ideals of V such that $A \subset \sqrt{B}$, then $A^k \subseteq B$ for some $k \in \mathbb{N}$.*

Proof. Suppose that $B \subset A^n$ for $n \geq 1$. Let $x \in A$. Since $A \subset \sqrt{B}$, then $x^k \in B$ for some $k \in \mathbb{N}$. But also since we have $B \subset A^n$ for all $n \geq 1$, then $x^k \in A^n$ for all $n \geq 1$. Then $x^k \in \bigcap\limits_{n \geq 1} A^n$ which is prime by (2) of Theorem 2.11, so $x \in \bigcap\limits_{n \geq 1} A^n$. Hence we have that $A \subseteq \bigcap\limits_{n \geq 1} A^n$, and so $A = A^n$ for all $n \geq 1$. Hence A is prime and $\sqrt{A^n} = \sqrt{A} = A$. Now, $B \subset A$ implies that $\sqrt{B} \subseteq \sqrt{A} = A$ which is a contradiction with $A \subset \sqrt{B}$. Hence our assumption is false, so B contains some power of A. □

Theorem 2.13. *Let V be a valuation ring and let $P \in Spec(V)$. Then*

(1) *If Q is P-primary and $x \in V \setminus P$, then $Q = Q\,(x)$.*

(2) *The product of P-primary ideals of V is again P-primary, and if $P \neq P^2$, then the complete set of P-primary ideals consists of powers of P.*

(3) *The intersection of all P-primary ideals is a prime ideal of V which contains all prime ideals properly contained by P.*

Proof. (1) Let K be the field of fractions of V. Since $x \notin P$, then $x \notin Q$, so we have $Q \subset (x)$. Let $A = \{y \in K | yx \in Q\}$. Since $Q \subset (x)$, then we have $A \subset V$. Furthermore, A is an ideal of V and $Q = A\,(x)$:

Let $a \in A, b \in V$, then $ax \in Q$, since Q is an ideal of V, then $abx \in Q$, hence $ab \in A$. If $a, b \in A$, then $ax, bx \in Q$, and this implies $ax + bx = (a+b)x \in Q$, so we have $a + b \in A$. Thus A is an ideal of V.

$A\,(x) \subseteq Q$ is clear. If $q \in Q \subseteq (x)$, then $q = ax$ for some $a \in V$, but since $ax = q \in Q$, then by definition of A, $a \in A$, so $q \in A\,(x)$. Hence $Q = A\,(x) \subseteq A$.

Since Q is P-primary and $(x) \nsubseteq P$, then we have $A \subseteq Q$. So $A = Q$. As a result, we have $Q = Q\,(x)$, as claimed.

(2) Let Q_1, Q_2 be P-primary ideals of V. Then we have $\sqrt{Q_1Q_2} = P$:

Since $Q_1Q_2 \subseteq Q_1$, then by taking radicals, we have $\sqrt{Q_1Q_2} \subseteq P$. If $x \in P = \sqrt{Q_1} = \sqrt{Q_2}$, then $x^{n_1} \in Q_1, x^{n_2} \in Q_2$ for some $n_1, n_2 \in \mathbb{N}$, then $x^{n_1+n_2} \in Q_1Q_2$, this implies $x \in \sqrt{Q_1Q_2}$. Hence $P \subseteq \sqrt{Q_1Q_2}$.

Let $x, y \in V$ with $xy \in Q_1Q_2$. Suppose that $x \notin P$. Our aim is to show that $y \in Q_1Q_2$. Since Q_1 is P-primary, then we have $Q_1 = Q_1\,(x)$ by (1) of this theorem. Then by multiplying with Q_2, we have that $xy \in Q_1Q_2 = (x)Q_1Q_2$. Since V is a domain, then this gives that $y \in Q_1Q_2$, hence Q_1Q_2 is P-primary.

For the last part, suppose $P \neq P^2$. Let Q be a P-primary ideal of V. Since $P^2 \subset \sqrt{Q} = P$, then by Lemma 2.12, Q contains a power of P^2, and so contains a power of P. Set m be the minimal such power, so we have $P^m \subseteq Q$ but $P^{m-1} \nsubseteq Q$. Let $x \in P^{m-1} \setminus Q$, then we have $Q \subset (x)$. If $A = \{y \in K | yx \in Q\}$, then $Q = A\,(x)$. $x \notin Q$ implies $A \subseteq P$ under the fact that Q is P-primary. So $Q = A\,(x) \subseteq P\,(x) \subseteq P^m$, which gives that $Q = P^m$.

(3) If P is the only P-primary ideal, then there is nothing to prove. Suppose that Q is a P-primary ideal of V such that $Q \neq P$. Let $\{Q_\alpha\}_{\alpha\in\Gamma}$ be the set of all P-primary ideals of V. Since we know a product of P-primary ideals is again P-primary, then Q^n is P-primary for all $n \geq 1$. Hence $\bigcap\limits_{\alpha\in\Gamma} Q_\alpha \subseteq \bigcap\limits_{n\geq 1} Q^n$. However

by Lemma 2.12 each Q_α contains a power of Q, thus $\bigcap\limits_{\alpha\in\Gamma} Q_\alpha \supseteq \bigcap\limits_{n\geq 1} Q^n$. Hence $\bigcap\limits_{\alpha\in\Gamma} Q_\alpha = \bigcap\limits_{n\geq 1} Q^n$.

Since Q is P-primary, Q properly contains each prime ideal of R which is properly contained by P and by (2) of Theorem 2.11 every prime ideal which is properly contained by Q is also contained by $\underset{\alpha\in\Gamma}{\cap} Q_\alpha$ which is a prime ideal of V.

□

Let G be an abelian group with a defined total ordering $\leq$. If for arbitrary $a, b, c \in G$, $a \leq b$ implies that $a + c \leq b + c$, then we say that G is an ordered group. For example, the additive group of real numbers with the natural ordering of real numbers is an ordered abelian group. Each subgroup of an ordered group is again an ordered group with the induced ordering.

Let $n \in \mathbb{N}$ and $\{G_i\}_{i=1}^n$ be a family of ordered abelian groups. Let $G = \bigoplus\limits_{i=1}^{n} G_i$. We shall denote the elements of G by n-tuples $(a_1, \dots, a_n)$, where $a_i \in G_i, i = 1, \dots, n$. For any distinct elements $(a_1, \dots, a_n), (b_1, \dots, b_n) \in G$, we write $(a_1, \dots, a_n) < (b_1, \dots, b_n)$ if $a_1 < b_1$ or if $a_i = b_i$ for $i = 1, \dots, k-1$, and $a_k < b_k$ for some $k = 2, \dots, n$.

This is clearly a total order on G. So G, with this ordering, becomes an ordered abelian group. We may refer to this ordering as the lexicographic ordering of G.

Let G be an ordered abelian group and let $\{\infty\}$ be a set where ∞ is an element such that $\infty \notin G$. Set $G^* = G \cup \{\infty\}$. Define addition on G^* such that for $a, b \in G^*$,

$$a + b = \begin{cases} a + b \ (addition\ in\ G) & if\ a, b \in G \\ \infty & if\ a = \infty\ or\ b = \infty \end{cases}$$

With this addition, G^* becomes a commutative semigroup. Now we extend the ordering of G to an ordering of G^* by defining $a \leq \infty$ for all $a \in G^*$. Thus G^* is an ordered semigroup in the sense that $a \leq b$ implies that $a + c \leq b + c$ for all $a, b, c \in G^*$.

Definition 2.14. Let K be a field, and let G be an ordered abelian group. Define a surjective mapping $v : K \to G^*$. If v satisfies the following conditions, than v is called a valuation on K:

(1) $v(a) = \infty$ if and only if $a = 0$.

(2) $v(ab) = v(a) + v(b)$ for all $a, b \in K$.

(3) $v(a+b) \geq min\{v(a), v(b)\}$ for all $a, b \in K$.

If $v : K \to G^*$ is a valuation, then the group G is called the value group of the valuation v. The mapping v from a field K into G^* given by $v(a) = 0$ for all $a \in K \setminus \{0\}$ and $v(0) = \infty$ is clearly a valuation on K which is called a trivial valuation.

Let v be a valuation on a field K and set $V = \{a \in K | v(a) \geq 0\}$.

If $a, b \in V$, then $v(ab) \geq v(a) + v(b) \geq 0$ and $v(a+b) \geq min\{v(a), v(b)\} \geq 0$, so that $ab, a+b \in V$. Since $v(-1) = v(1) = 0$, and hence $-1 \in V$, we see that V is a subring of K.

Let $a \in K$ with $a \neq 0$. If $a \notin V$, then $v(a) < 0$, so $v(1/a) = -v(a) > 0$. Thus $1/a \in V$. Therefore V is a valuation ring. Note also that K is the field of fractions of V, and the maximal ideal of V is $M = \{a \in K | v(a) > 0\}$:

Let $a \in M, b \in V$. Then we have $v(a) > 0$ and $v(b) \geq 0$, so we have $v(ab) = v(a) + v(b) > 0$, hence $ab \in M$.

Let $a, b \in M$, then we have $v(a), v(b) > 0$, hence $v(a+b) \geq min\{v(a), v(b)\} > 0$, so $a + b \in M$.

So M is an ideal of V.

To show M is maximal, let $x \in V \setminus M$. Since $x \in V \setminus M$, then $v(x) = 0$. Since $v(1) = 0$, then $v(1/x) = v(1) - v(x) = 0$, hence $1/x \in V$, so x is a unit in V. Thus M contains every non-unit element of V.

For $x \in M$, we have $v(1/x) = v(1) - v(x) = -v(x) < 0$, so $1/x \notin V$, hence x is a non-unit. So, M is the set of non-units of V, therefore M is the unique maximal ideal of V.

We shall now show that all valuation rings are determined by valuations in this way.

Proposition 2.15. *Let V be a valuation ring, and let K be the field of fractions of V. Then there exists a valuation v on K such that $V = \{a \in K | v(a) \geq 0\}$.*

Proof. Let U be the group of non-units of V, then U is a subgroup of $K^* = K \setminus \{0\}$. Set $G = K^*/U$, with addition $aU + bU = abU$ for $a, b \in K^*$. Define a relation on G by $bU \leq aU$ if and only if $a/b \in V$. If $aU = a'U$ and $bU = b'U$, then we have $a'/a, b'/b \in U$, hence $a/b \in V$ if and only if $a'/b' \in V$ which means $\leq$ is a well-defined relation. This relation is a partial ordering:

Clearly $aU \leq aU$ since $a/a = 1 \in V$, hence $\leq$ is reflexive. If $aU \leq bU$ and $bU \leq cU$, then $b/a, c/b \in V$, hence $c/a = (b/a)\,(c/b) \in V$ and this implies that $aU \leq cU$, hence $\leq$ is transitive. To see $\leq$ is anti-symmetric, let $aU \leq bU$ and $bU \leq aU$. Then $a/b, b/a \in V$ hence $a/b \in U$ so $aU = bU$, hence $\leq$ is anti-symmetric.

Since V is a valuation ring, then $\leq$ is a total order on G since for $a, b \in K^*$, we have either $a/b \in V$ or $b/a \in V$. Finally, G is an ordered abelian group with $\leq$:

Let $aU, bU, cU \in G$ with $aU \leq bU$. Then $\frac{b}{a} \in V$. Clearly $\frac{cb}{ca} \in V$, and so $caU \leq cbU$, or equivalently $aU + cU \leq bU + cU$.

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

Clearly v is surjective.

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

$v(a + b) \geq min\{v(a), v(b)\}$ if $a = 0$ or $b = 0$.

Now suppose $a, b \in K^*$, with $aU \leq bU$. Then we have $\frac{b}{a} \in V$, and so $\frac{b}{a} + 1 \in V$. So $v(\frac{b}{a} + 1) \geq v(1) = 0$. Therefore $v(a + b) = v\left(a\left(\frac{b}{a} + 1\right)\right) = v(a) + v\left(\frac{b}{a} + 1\right) \geq v(a) \geq min\{v(a), v(b)\}$.

It follows that v is a valuation on K and $V = \{a \in K | v(a) \geq 0\}$. □

Definition 2.16. If V and v are related as in Proposition 2.15, we say that v is the valuation determined by V.

Definition 2.17. If v is an arbitrary valuation on a field K, then $\{a \in K | v(a) \geq 0\}$ is called the valuation ring of v.

Let v and v' be valuations on a field K, with value groups G and G' respectively. We say v and v' are equivalent valuations if and only if there exists an order-preserving isomorphism ϕ from G onto G' such that $v'(a) = \phi(v(a))$ for all $a \in K^*$. This relation between valuations are clearly an equivalence relation since it is reflexive, symmetric and transitive. It is also clear that equivalent valuations have the same valuation ring.

Conversely, if two valuations on a field K both have the same valuation ring, then they are equivalent. To verify this, we shall show that if v is a valuation on a field K, V is the valuation ring determined by v, and v' is the valuation determined by V, then v and v' is equivalent.

Let G be the value group of v and U be the group of units of V. Define $\phi : G \to K^*/U$ by $\phi(v(a)) = aU$. If $v(a) = v(b)$, then $v(a/b) = 1$ and this implies $a/b \in U$, hence $aU = bU$, which gives that ϕ is well-defined. Since $\phi(v(a)) = v'(a)$ for all $a \in K^*$, it is sufficient to show ϕ is an order preserving isomorphism. ϕ is a homomorphism since

$$\phi(v(a) + v(b)) = \phi(v(ab)) = v'(ab) = v'(a) + v'(b) = \phi(v(a)) + \phi(v(b))$$

ϕ is clearly surjective. If $aU = bU$, then $\frac{a}{b} \in U$ so $v(\frac{a}{b}) = 1$ and this gives that $v(a) = v(b)$, hence ϕ is injective. To see that ϕ is order-preserving, let $v(a) \leq v(b)$, then $0 = v(1) \leq v(\frac{b}{a})$ so $\frac{b}{a} \in V$. So $v'(\frac{b}{a}) \geq 0$, hence $v'(a) \leq v'(b)$, this is $\phi(v(a)) \leq \phi(v(b))$. It follows that ϕ is an order-preserving isomorphism, and this gives the desired equivalence between v and v'.

Definition 2.18. Let G be an ordered abelian group. For a subgroup H of G, if for each nonnegative element α of H, $0 < \beta \leq \alpha$ implies $\beta \in H$, then H is called an isolated subgroup of G. If H is an isolated subgroup of G and $H \neq G$, then H is called a proper isolated subgroup of G.

Definition 2.19. Let G be an ordered abelian group. If G has only finitely many proper isolated subgroups, then the number of these subgroups of G is called the rank of G. Thus, G has rank one if and only if $G \neq 0$ and the only proper isolated subgroup of G is 0. If G has rank n, then we say that both v and V have rank n.

Definition 2.20. Let K be a field, and v be a valuation on K. Let G and V be the value group and the valuation ring of v, respectively. If G is cyclic, then v is called a discrete valuation, and V is called a discrete valuation ring (DVR). If v is a non-trivial discrete valuation, then v has rank one.

Before we continue our study about the structure of valuation rings, we give some examples:

Example 2.21. Let K be a field, and let R be the formal power series in indeterminate X over K, i.e. $R = K[[X]]$. Then R is a discrete valuation ring:

We know that $R = \{\sum\limits_{i=0}^{\infty} k_i X^i | k_i \in K\}$ and an element of R is unit if and only if its constant term is unit. Hence XR is the set of all non-units of R. Let $f(X), g(X) \in R$, set $f(X) = X^i f_0(X), g(X) = X^j g_0(X)$, where $i, j \geq 0$ and $X \nmid f_0(X), g_0(X)$. Clearly we have $f_0(X)$ and $g_0(X)$ are units i R, then we have $\big(f(X)\big) = \big(X^i.f_0(X)\big) = (X^i)$ and similarly $\big(g(X)\big) = (X^j)$. Now if we have $i \leq j$, then $\big(g(X)\big) = (X^j) \subseteq (X^i) = \big(f(X)\big)$, otherwise $\big(f(X)\big) = (X^i) \subseteq (X^j) = \big(g(X)\big)$. Thus R is a discrete valuation ring with maximal ideal XR.

Example 2.22. Let $D = \mathbb{Z}_{(2)} + X\mathbb{Q}[[X]]$, where $\mathbb{Z}_{(2)}$ is the localization of $\mathbb{Z}$ at $2\mathbb{Z}$. Then D is a non-Noetherian valuation ring:

We clearly have $D \subseteq Q[[X]]$. Let $\alpha, \beta \in D$. Set $\alpha = a + Xs_1$ and $\beta = b + Xs_2$, where $a, b \in \mathbb{Z}_{(2)}$ and $s_1, s_2 \in \mathbb{Q}[[X]]$. Since $\alpha, \beta \in \mathbb{Q}[[X]]$, and $\mathbb{Q}[[X]]$ is a valuation ring, we may choose $\lambda \in \mathbb{Q}[[X]]$ such that $\alpha = \lambda\beta$. Set $\lambda = l + Xs_3$, where $l \in \mathbb{Q}$ and $s_3 \in \mathbb{Q}[[X]]$. $\alpha = \lambda\beta$ gives that $a = lb$. Set $a = \frac{a_1}{a_2}, b = \frac{b_1}{b_2}$ and $l = \frac{l_1}{l_2}$, where $2 \nmid a_2, b_2$ and $GCD(l_1, l_2) = 1$.

If $2 \nmid l_2$, then $l \in \mathbb{Z}_{(2)}$ hence $\lambda \in D$. So $\beta \mid \alpha$ in D. If $2 \mid l_2$, then since $GCD(l_1, l_2) = 1$, we have $2 \nmid l_1$. In the latter case, we have $l^{-1} \in \mathbb{Z}_{(2)}$ and so $\lambda^{-1} \in D$. It follows that $\alpha\lambda^{-1} = \beta$, so $\alpha \mid \beta$ in D. Thus D is a valuation ring.

To see D is non-Noetherian, consider the chain

$$(X) \subset (X, \frac{X}{2}) \subset (X, \frac{X}{2}, \frac{X}{2^2}) \subset \ldots \subset (X, \frac{X}{2}, \ldots, \frac{X}{2^n}) \subset \ldots$$

which is clearly infinite. Hence D is a non-Noetherian valuation ring.

To give another example, set $D = k + XK[[X]]$, where $K = k(Y)$ for some indeterminate Y such that $Y \neq X$. The fact that D is a valuation ring can be similarly obtained as the preceding example. Then if we consider the ideal $(X, \frac{X}{Y}, \frac{X}{Y^2}, \ldots, \frac{X}{Y^n}, \ldots)$ of D which is not finitely generated. We have that D is also a non-Noetherian valuation ring.

Now we shall explore the relation between the ideal structure of a valuation ring and the group structure of the value group of the valuation determined by that valuation ring.

Theorem 2.23. *Let K be a field, and let v be a valuation on K. Denote the value group and valuation ring of v by G and V, respectively. Then there exists a one-to-one order-reversing correspondence between the isolated subgroups of G and the prime ideals of V.*

Proof. Let $\mathscr{I}$ and $\mathscr{P}$ respectively denote the isolated subgroups of G and the set of prime ideals of V. For $I \in \mathscr{I}$, set $\pi(I) = \{x \in V | v(x) \notin I\}$, and for $P \in \mathscr{P}$, set $\kappa(P) = \{\alpha \in G | \alpha, -\alpha \in v(V \setminus P)\}$.

First of all, we shall show that π and κ are well-defined.

Let $I \in \mathscr{I}$. We show that $\pi(I)$ is a prime ideal of V.

Let $x \in \pi(I), y \in V$. Then $v(xy) = v(x) + v(y) \geq v(x)$. If we have $xy \notin \pi(I)$, then $v(xy) \in I$, and since $v(x), v(y) \geq 0$, then we have $v(x), v(y) \in I$, which is a contradiction with the fact that $v(x) \notin I$ or $x \in \pi(I)$. So we must have $xy \in \pi(I)$.

If $x, y \in \pi(I)$, then $v(x), v(y) \notin I$. Since $v(x + y) \geq min\{v(x), v(y)\}$, $v(x + y) \in I$ implies $v(x) \in I$ or $v(y) \in I$, hence $v(x + y) \notin I$, thus $x + y \in \pi(I)$.

So $\pi(I)$ is an ideal of V. Suppose that there exists a unit $u \in V$ such that $u \in \pi(I)$, then $v(u) = 0 \notin I$, since every subgroup must contain 0, it is a contradiction, so $\pi(I)$ is proper in V.

Now let $x, y \in V$ with $x, y \notin \pi(I)$, then $v(x), v(y) \in I$ and since I is a subgroup, then $v(x) + v(y) = v(xy) \in I$, hence $xy \notin \pi(I)$. Thus $\pi(I) \in \mathscr{P}$.

Now let $P \in \mathscr{P}$. We shall show that $\kappa(P)$ is an isolated subgroup of G.

Since $1 \in V \setminus P$, then $0 = v(1) \in v(V \setminus P)$, hence $0 \in \kappa(P)$.

Let $\alpha \in \kappa(P)$, then by definition $\alpha, -\alpha \in v(V \setminus P)$, so clearly we have $-\alpha \in \kappa(P)$.

Let $\alpha, \beta \in \kappa(P)$. Then we have $\alpha, \beta \in v(V \setminus P)$, set $\alpha = v(a), \beta = v(b)$, where $a, b \in V \setminus P$. Since $V \setminus P$ is multiplicatively closed, then $ab \in V \setminus P$ hence $v(ab) = v(a) + v(b) = \alpha + \beta \in v(V \setminus P)$, similarly we have $-(\alpha + \beta) \in v(V \setminus P)$, hence $\alpha + \beta \in \kappa(P)$. So $\kappa(P)$ is a subgroup of G.

Now let $g \in G^+, \alpha \in \kappa(P)$ with $g \leq \alpha$. Then $\alpha = v(a)$ for some $a \in V \setminus P$ and $g = v(x)$ for some $x \in V$. Since $\alpha - g = v(a) - v(x) = v(\frac{a}{x}) \geq 0$, then $\frac{a}{x} \in V$, hence $a \in (x)$. Since $a \notin P$, then we must have $x \notin P$. Thus $g = v(x) \in v(V \setminus P)$ so $g \in \kappa(P)$. Therefore, $\kappa(P)$ is an isolated subgroup of G.

Now we shall show that π and κ are inverses of each other.

Let $P \in \mathscr{P}$. Our aim is to show that $\pi(\kappa(P)) = P$.

If $x \in P$, then $v(x) \in v(P)$, hence $v(x) \notin \kappa(P)$, and this implies $x \in \pi(\kappa(P))$. So $P \subseteq \pi(\kappa(P))$. On the other hand, if $x \in V \setminus P$, then $v(x) \notin v(P)$, so $v(x) \in \kappa(P)$, which means $x \notin \pi(\kappa(P))$. Hence we have $P = \pi(\kappa(P))$.

Let $I \in \mathscr{I}$. Our claim is that $\kappa(\pi(I)) = I$.

Let $a \in I$, then there exists $x \in G^+$ such that $v(x) = a$. Since $v(x) \in I$, then

$x \in V \setminus \pi(I)$ and this implies that $a = v(x) \in v(V \setminus \pi(I))$, so by definition, $a \in \kappa(\pi(I))$.

If $a \in V \setminus I$, then there exists $x \in G^+$ such that $v(x) = a \notin I$. So $x \in \pi(I)$. Hence $a = v(x) \in v(\pi(I))$, which implies that $a \notin \kappa(\pi(I))$. Thus $\kappa(\pi(I)) = I$ as desired.

Since we know that κ and π are inverses of each other, showing one of them is order-reversing is sufficient for us.

Let $P, Q \in \mathscr{P}$ with $P \subseteq Q$. Our claim is that $\kappa(Q) \subseteq \kappa(P)$.

Let $\alpha \in \kappa(Q)$, then $\alpha \in v(V \setminus Q) \subseteq v(V \setminus P)$ by definition, and this gives that $\alpha \in \kappa(P)$, which completes the proof. □

From the correspondence defined in the proof of the theorem, we can say that if a valuation ring has rank n and if V is the valuation ring of this valuation, then there exists a chain $P_1 \subset \ldots \subset P_n$ of prime ideals of V, but no longer such chain exists.

We now show that a Noetherian valuation ring is either a field or has rank one and is discrete.

Theorem 2.24. *A valuation ring which is not a field is Noetherian if and only if it has rank one and is discrete.*

Proof. Let V be a Noetherian valuation ring and suppose that it is not a field. Let P be the unique maximal ideal of V. Then $P = (a)$ for some nonzero $a \in P$. By the Krull Intersection Theorem we have that $\bigcap\limits_{n \geq 1} P^n = (0)$. If $b \in V$ is nonzero, then $b = ua^n$ for some uniquely determined $n \in \mathbb{N}$ and a unit u in V. Actually, if K is the field of fractions of V, then every $x \in K$ may uniquely written as $x = ua^n$, where u is a unit in V and $n \in \mathbb{Z}$.

Let U be the multiplicative group of units in V, then $\phi : K^*/U \to \mathbb{Z}$ defined by $\phi(bU) = n$ if $b = ua^n$, is an order-preserving isomorphism:

ϕ is clearly surjective. To see it is injective, let $\phi(xU) = \phi(yU) = n$, then $x = u_1 a^n$ and $y = u_2 a^n$ for some $u_1, u_2 \in U$. Since $\frac{x}{y} = \frac{u_1}{u_2} \in U$, then $xU = yU$, hence ϕ is injective. ϕ is order-preserving since if $xU \leq yU$, then $\frac{y}{x} \in V$, and so $y = xt$ for some $t \in V$. Now if $x = u_1 a^n$ and $t = u_2 a^m$, then since $t \in V$, we have $m \geq 0$, and clearly $y = u_1 u_2 a^{m+n}$ implies that $\phi(xU) = n \leq m + n = \phi(yU)$.

Therefore, since V is order-isomorphic to $\mathbb{Z}$, then V has rank one and is discrete.

For the converse part, let V be a valuation ring which has rank one and is discrete. Let v be the valuation on K whose valuation ring and value group is V and $\mathbb{Z}$, respectively.

Let $I \neq (0)$ be an ideal of V. There exists $a \in I$ such that $v(a) = min\{v(b)|b \in I\}$. Let $c \in I \setminus \{0\}$, then $v(a) \leq v(c)$, hence $v(\frac{c}{a}) \geq 0$. This implies that $\frac{c}{a} \in V$ and so $c \in (a)$. Since c is an arbitrary nonzero element in I and we also have $a \in I$, then we have $I = (a)$. Since arbitrary ideal of V is finitely generated, in fact principal, then V is Noetherian. □

2.2 Integrality

Proposition 2.25. *Let R' be a ring and let R be subring of R', then for any $a \in R'$, the following statements are equivalent:*

(1) *a is integral over R.*

(2) *$R[a]$ is a finitely generated R-module.*

(3) *There exists a subring R'' of R' containing a, which is a finitely generated R-module.*

Proof. Suppose (1) holds. Then there exist $b_0, \ldots, b_{n-1} \in R$ and $n \geq 1$ such that $b_0 + b_1a + \ldots + b_{n-1}a^{n-1} + a^n = 0$ holds. Our aim is to show that $R[a] = R1 + Ra + \ldots + Ra^n$. Let $f(X) \in R[X]$ be such that $deg\, f(X) = d > n$. Set $f(X) = c_0 + c_1X + \ldots + c_dX^d$, then

$$\begin{aligned} f(a) &= c_0 + c_1a + \ldots + c_{d-1}a^{d-1} + c_da^{d-n}\, a^n \\ &= c_0 + c_1a + \ldots + c_{d-1}a^{d-1} + c_da^{d-n}(-b_0 - b_1a - \ldots - b_{n-1}a^{n-1}) \\ &= c_0' + c_1'a + \ldots + c_{d-1}'a^{d-1} \end{aligned}$$

By repeating this argument, we finally have $f(a) \in R1 + Ra + \ldots Ra^n$. Thus (2) holds.

Since its obvious that (2) implies (3), for the final part, suppose that (3) holds and let $a_1, \ldots, a_n$ be the generators of R'' as an R-module. For each $i = 1, \ldots, n$ we have $aa_i = \sum_{j=1}^{n} b_{ij}a_j$ where $b_{ij} \in R$ or $\sum_{j=1}^{n}(b_{ij} - \delta_{ij}a)a_j = 0$. If $d = det[b_{ij} - \delta_{ij}a]$, then $da_j = 0$ for each $j = 1, \ldots, n$. Since all elements of R'' can be written as a linear combination of a_j's, then $dc = 0$ for all $c \in R''$. In particular, since $1 \in R''$, then $1d = d = 0$. Since d can be viewed as a polynomial in $R[a]$ at degree n, and since a^n has 1 as coefficient, then (3) holds. □

Proposition 2.26. *Let R be a subring of a ring R. Let $R_0 = \{a \in R' | a \text{ is integral over } R\}$. Then R_0 is a subring of R', and $R \subseteq R_0$.*

Proof. It is clear that $R \subseteq R_0$. Let $a, b \in R_0$. Then $R[a]$ is a finitely generated R-module and $R[a, b] = R[a][b]$ is a finitely generated $R[a]$-module. So we have that $R[a, b]$ is a finitely generated R-module. Since $a - b, ab \in R[a, b]$, then they are integral over R, hence $a - b, ab \in R_0$, which gives that R_0 is a subring of R'. □

If R, R' and R_0 are defined as in the above proposition, then R_0 is called the integral closure of R in R', or just the integral closure of R if R' is the total quotient ring of R.

Proposition 2.27. *Let $R \subseteq R' \subseteq R''$ be a chain of subrings. If R' is integral over R and if $a \in R''$ is integral over R', then a is integral over R.*

Proof. Since a is integral over R', there exists $b_0, \ldots, b_n \in R'$ such that $b_0 + b_1 a + \ldots + b_{n-1} a^{n-1} + a^n = 0$. So a is integral over $R[b_0, \ldots, b_{n-1}]$. Hence by the equivalence of (2) of Theorem 2.25, $R[b_0, \ldots, b_{n-1}, a]$ is a finitely generated R-module. Since we clearly have $a \in R[b_0, \ldots, b_n, a]$, then by (3) of Theorem 2.25, a is integral over R. □

Proposition 2.28. *Let R' be a ring and R be a subring of R', and let S be a multiplicatively closed set in R. Then $S^{-1}R$ may be considered as a subring of $S^{-1}R'$. In this case, R' is integral over R implies that $S^{-1}R'$ is integral over $S^{-1}R$.*

Proof. Let $0_S = \{r \in R | rs = 0 \text{ for some } s \in S\}$ and $0'_S = \{r' \in R' | r's = 0 \text{ for some } s \in S\}$. We clearly have that $0_S \subseteq 0'_S \cap R$. So let $a \in 0'_S \cap R$. Then $sa = 0$ for some $s \in S$, and since $a \in R$, then this implies $a \in 0_S$. Hence $0_S = 0'_S \cap R$. So the mapping $\phi : S^{-1}R \to S^{-1}R'$ defined by $\phi\left(\frac{a}{s}\right) = \frac{a}{s}$ is an injective homomorphism. Since $S^{-1}R$ is isomorphic to $\phi(S^{-1}R)$, we can identify $\frac{a}{s}$ with its image, in this way we may consider $S^{-1}R$ as a subring of $S^{-1}R'$.

Now assume that R' is integral over R. Let $\frac{a}{s} \in S^{-1}R'$, where $a \in R', s \in S$. Since R' is integral over R then there exist $b_0, \ldots, b_{n-1} \in R$ such that $b_0 + b_1 a + \ldots + b_{n-1} a^{n-1} + a^n = 0$. By multiplying with $\frac{1}{s^n}$, we obtain that $\frac{b_0}{s} + \left(\frac{b_1}{s^{n-1}}\right)\left(\frac{a}{s}\right) + \left(\frac{b_2}{s^{n-2}}\right)\left(\frac{a}{s}\right)^2 + \ldots + \left(\frac{b_{n-1}}{s}\right)\left(\frac{a}{s}\right)^{n-1} + \left(\frac{a}{s}\right)^n = 0$ Therefore $\frac{a}{s}$ is integral over $S^{-1}R$. □

Lemma 2.29. *Let R, S be commutative rings with $R \subseteq S$. Let R' be the integral closure of R in S, and let U be a multiplicatively closed set in R. Then $U^{-1}R'$ is the integral closure of $U^{-1}R$ in $U^{-1}S$.*

Proof. Let $s \in R'$ be arbitrary. Since s is integral over R, then $s^n + r_{n-1}s^{n-1} + \ldots + r_1 s + r_0 = 0$ where $r_0, \ldots, r_{n-1} \in R$. Let $u \in U$ be arbitrary. If we multiply the equation by $\frac{1}{u^n}$, then we have

$$\left(\frac{s}{u}\right)^n + \left(\frac{r_{n-1}}{u}\right)\left(\frac{s}{u}\right)^{n-1} + \ldots + \left(\frac{r_1}{u^{n-1}}\right)\left(\frac{s}{u}\right) + \frac{r_0}{u^n} = 0$$

So $\frac{s}{u}$ is integral over $U^{-1}R$. Since $s \in R'$ is arbitrary, then $U^{-1}R'$ is integral over $U^{-1}R$.

Now we shall show that $\frac{s}{u} \in U^{-1}S$, where $s \in S, u \in U$ is integral over $U^{-1}R$ implies that $\frac{s}{u} \in U^{-1}R'$.

Since $\frac{s}{u}$ is integral over $U^{-1}R$, then there exists $n \in \mathbb{N}, r_0, \ldots, r_{n-1} \in R, u_0, \ldots, u_{n-1} \in U$ such that $\left(\frac{s}{u}\right)^n + \left(\frac{r_{n-1}}{u_{n-1}}\right)\left(\frac{s}{u}\right)^{n-1} + \ldots + \left(\frac{r_1}{u_1}\right)\left(\frac{s}{u}\right) + \left(\frac{r_0}{u_0}\right) = 0$.

Set $v = u_0 \ldots u_{n-1}$. Then multiplying the above equation by $\frac{uv}{1}$ gives that $\left(\frac{vs}{1}\right)^n + \left(\frac{r'_{n-1}}{1}\right)\left(\frac{vs}{1}\right)^{n-1} + \ldots + \left(\frac{r_{1'}}{1}\right)\left(\frac{vs}{1}\right) + \left(\frac{r'_0}{1}\right) = 0$. Thus there exists $x \in U$ such that $x\left((vs)^n + r'_{n-1}(vs)^{n-1} + \ldots + r'_1(vs) + r'_0\right) = 0$. Multiplying by x^{n-1} and by rearranging the coefficients, we see that xvs is integral in R, hence belongs to R'. Then $\frac{s}{u} = \frac{xvs}{xvu} \in U^{-1}R'$. □

Corollary 2.30. *Let R be a ring and U be a multiplicatively closed set in R. If R is integrally closed, then $U^{-1}R$ is integrally closed.*

Corollary 2.31. *Let R be an integral domain with field of fractions K, let L be an algebraic extension field of K, and let R' be the integral closure of R in L. If S is the set of all nonzero elements of R, then we have $S^{-1}R' = L$.*

Proof. Since $K = S^{-1}R$, it follows from, Lemma 2.29, that $S^{-1}R'$ is the integral closure of K in L, which yields that $S^{-1}R' = L$, as desired. □

Proposition 2.32. *Suppose R is an integrally closed domain with field of fractions K. Let L be an extension field of K and let $\alpha \in L$. Then the following statements are equivalent:*

1. *α is integral over R.*

2. *α is algebraic over K and the minimal polynomial $m(X)$ of α over K has coefficients in R.*

Proof. Since (2) clearly implies (1), then it suffices to show (2) holds under the assumption that $\alpha \in L$ is integral over K. Since α is integral over K, then there exists a monic polynomial $P(x) \in R[X]$ such that $P(\alpha) = 0$. Since we also have $P(X) \in K[X]$, then α is algebraic over K. Let $m(X)$ be the minimal polynomial of α over $K[X]$. Clearly $m(X)\big|P(X)$. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be all roots of $m(X)$ in an algebraic closure of K. Since $m(\alpha_i) = 0$ for each $i = 1, \ldots, n$ and $m(X)\big|P(X)$, then $P(\alpha_i) = 0$ for all $i = 1, \ldots, n$, hence each α_i is integral over K. Set $s_j = \sum\limits_{1 \leq i_1 < \ldots < i_j \leq n} (-1)^j \alpha_{i_1} \ldots \alpha_{i_j}$ for every $j = 1, \ldots, n$. Since we have $m(X) = X^n + s_1 X^{n-1} + \ldots + s_n \in K[X]$, $s_j \in K$ for all $j = 1, \ldots, n$. By the definition of s_j, each s_j is integral over R. Since R is integrally closed, then $s_j \in R$ for $i = 1, \ldots, n$, so $m(X) \in R[X]$ and the proof is complete. □

Corollary 2.33. *Let R be an integral domain with field of fractions K, and let R' be the integral closure of R in K. Let L be an extension field of K and assume that $\alpha \in L$ is integral over R. Then the minimal polynomial $m(X)$ of α over K lies in $R'[X]$. Hence each conjugate of α over K is also integral over R. Moreover, the ideal of $R'[X]$ consisting of those polynomials which have α as a root is principal generated by $m(X)$.*

Proof. Applying Proposition 2.32 for R' instead of R we obtain the first statement of the corollary. The second statement then follows easily since the conjugates of α are those elements of L which are roots of $m(X)$. The last statement follows easily from the fact that $m(X)$ is the minimal polynomial of α over K. □

Corollary 2.34. *Let R be an integrally closed domain with field of fractions K, and let $p(X) \in R[X]$ be a monic polynomial. If $P(X) = a(X)b(X)$ with $a(X), b(X) \in K[X]$ are monic polynomials, then $a(X), b(X) \in R[X]$.*

Proof. We use induction on $n = deg\, a(X)$. If $n = 1$, then $a(X) = X - c$ for some $c \in K$. Then $a(c) = 0$ implies that $P(c) = 0$, hence c is integral over R. Since R is integrally closed, we have $c \in R$, therefore $a(X) \in R[X]$.

Now let $n > 1$ and assume that the claim is true for a product $P(X)$ in which one of the factors has degree less than n. Consider an extension L of K such that L contains a root α of $a(X)$. Since α is also a root of $P(X)$, it is integral over R, hence by Proposition 2.32 it is algebraic over K with the minimal polynomial, say $m(X)$, lying in $R[X]$. Clearly $m(X)\big|a(X)$. Let $a(X) = m(X)a_1(X)$. If $a(X) = m(X)$, then we are done. Otherwise, $1 \leq deg\, a_1(X) < deg\, a(X)$, and since $P(X) = a_1(X)\big(m(X)b(X)\big)$, we have $a_1 \in R[X]$ by induction hypothesis . Since $a_1(X)$ and $m(X)$ lie in $R[X]$, then we have $a(X) \in R[X]$. By symmetry, we also see that $b(X) \in R[X]$, so the proof complete. □

A part of the following corollary states an important fact that if we have an integral extension $R \subseteq R'$ of domains where R is integrally closed, any prime ideal of R extends to R' properly. This fact will be used frequently, without giving any reference, when we consider the case where R is a domain with field of fractions K and R' is the integral closure of R in an extension field of K.

Corollary 2.35. *Let $R \subseteq S$ be an integral extension of rings where S is an integral domain and R is integrally closed, and let K be the field of fractions of R. If $s \in PS$, for some $P \in Spec(R)$, then with the exception of the leading term, all the coefficients of the minimal polynomial of s over K are elements of P. In particular, PS is a proper ideal of S.*

Proof. We can write $s = p_1s_1 + \ldots p_ms_m$ for some $p_1, \ldots, p_m \in P$ and $s_1, \ldots, s_m \in S$. Since $s_1, \ldots, s_m$ are all integral over R, the subring $T = R[s_1, \ldots, s_m]$ is a finitely generated R–module. Let $s \in PT$. Using the determinant argument, we can find a monic polynomial

$$p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

such that $a_0, \ldots, a_{n-1} \in P$ and $P(s) = 0$. Let $m(X)$ be the minimal polynomial of s over K. Then $m(X)\big|p(X)$. Write $p(X) = m(X)b(X)$ for some $b(X) \in K[X]$. By Corollary 2.34, $m(X), b(X) \in R[X]$. If we write $\overline{a(X)}$ for any $a(X) \in R[X]$ to denote the image of $a(X)$ in $(R/P)[X]$ under the natural homomorphism $R[X] \to (R/P)[X]$, we obtain

$$x^n = \overline{m(X)}.\overline{b(X)},$$

which gives that $\overline{m(X)}$ and $\overline{b(X)}$ are powers of X, completing the proof. □

2.3 Fractional Ideals

Let R be a ring, K be the total quotient ring of R and S be the set of regular elements of R. Then a subset A of K is called a fractional ideal if it satisfies the following conditions:

(1) A is an R-module, that is, if $a, b \in A$ and $r \in R$, then $a - b, ra \in R$.

(2) There exists $d \in S$ such that $dA \subseteq R$.

Note that for condition (2), it is enough to find $x \in K$ such that $xA \subseteq R$. Since we can write $x = \frac{d}{s}$, where $d, s \in R$, then $d = sx$ implies that $dA \subseteq s(xA) \subseteq R$.

The ideals of R are also fractional ideals of R since if I is an ideal of R, then $1I = I \subseteq R$. These ideals of R are called integral ideals instead of fractional ideals.

If K is the total quotient ring of R, and $x \in K$, then $xR = \{xr | r \in R\}$ is a fractional ideal of R, and denoted by (x), such a fractional ideal of R is called principal.

Summation and multiplication of fractional ideals of R are defined as for integral ideals of R. If A and B are fractional ideals of R, then $A + B$, AB and $A \cap B$ are also fractional ideals of R. Moreover, if B contains a regular element of R, then $[A : B] = \{x \in K | xB \subseteq A\}$ is a fractional ideal of R:

$[A : B]$ is clearly an R-module. Suppose that b and d are regular elements of R such that $b \in B$ and $dA \subseteq R$. Then we have $bd[A : B] \subseteq dA \subseteq R$. Hence $[A : B]$ is a fractional ideal of R. We also know that a fractional ideal of R is containing a regular element of R if and only if it contains a regular element of K, the total quotient ring of R.

The fractional ideal $[A : B]$ need not to be the same as $(A : B)$, since $(A : B)$ is defined as $(A : B) = \{x \in R | xB \subseteq A\} = [A : B] \cap R$.

We shall denote the set of all nonzero fractional ideals of R by $\mathcal{F}(R)$.

For $A \in \mathcal{F}(R)$, we say that A is invertible if and only if there exists a $B \in \mathcal{F}(R)$ such that $AB = R$.

Proposition 2.36. *Let R be a ring and let K be its total quotient ring.*

1. *If $A \in \mathcal{F}(R)$ is invertible, then A contains a regular element of R and is finitely generated as an R-module.*

2. *Let $A, B \in \mathcal{F}(R)$ be such that $A \subseteq B$ and suppose that B is invertible. Then there exists an integral ideal C of R such that $A = BC$.*

3. *Let $A \in \mathcal{F}(R)$. Then A is invertible if and only if there exists $B \in \mathcal{F}(R)$ such that $AB = (d)$ for some regular element d of K.*

Proof.

1. Let $B \in \mathcal{F}(R)$ be such that $AB = R$. So we have $1 = \sum_{i=1}^{n} a_i b_i$ for some $a_1, \dots, a_n \in A, b_1, \dots, b_n \in B$. Let $x \in A$ be arbitrary, then $xb_i \in AB = R$, hence $x = \sum_{i=1}^{n} a_i(xb_i)$. So $a_1, \dots, a_n$ generate A as an R-module. Now suppose that $dB \subseteq R$ for d, a regular element of R. Then $d \in dR = dAB = A(dB) \subseteq AR = A$. Thus A contains a regular element of R.

2. Since B is invertible, there exists $B' \in \mathcal{F}(R)$ such that $BB' = R$. Set $C = AB'$, then since $A \subseteq B$, we have $C = AB' \subseteq BB' = R$. It follows that $BC = B(AB') = A(BB') = AR = A$.

3. Let x be a regular element of K and $B \in \mathcal{F}(R)$ be such that $AB = (x)$, then $A(Bx^{-1}) = R$, hence A is invertible. Now let A is invertible, then there exists $C \in \mathcal{F}(R)$ such that $AC = R$. If $x \in K$ is a regular element of R, then $A(Cx) = (x)$, hence $B = Cx$ is the desired fractional ideal of R.

□

Let $A \in \mathcal{F}(R)$ be invertible, then by (1) of Proposition 2.36, we have $[R : A] \in \mathcal{F}(R)$.

Proposition 2.37. *Let $A \in \mathcal{F}(R)$ be invertible and let $B \in \mathcal{F}(R)$ be such that $AB = R$, then $B = [R : A]$.*

Proof. Since we have $AB = R$, then $B \subseteq [R : A]$. We also have $A[R : A] \subseteq R$ which implies that $[R : A] = R[R : A] = BA[R : A] \subseteq BR = B$. Hence $B = [R : A]$. □

Let $A \in \mathcal{F}(R)$ be invertible. We shall denote $[R : A]$ by A^{-1}, and call it the inverse of A. If $A, B \in \mathcal{F}(R)$ are both invertible, then AB is invertible, and $(AB)^{-1} = A^{-1}B^{-1}$.

Let K be the total quotient ring of R, and let $x \in K$. Then (x) is invertible if and only if x is a regular element of K. In the latter case $(x)^{-1} = (x^{-1})$.

Finally, let $A_1, \dots, A_k \in \mathcal{F}(R)$ and set $A = A_1 \dots A_k$. Then A is invertible if and only if A_i is invertible for all $i = 1, \dots, k$. If A is invertible, then $A_i^{-1} = A^{-1} \prod_{j \neq i} A_j$.

Let R be an integral domain. If $A, B \in \mathcal{F}(R)$, then all $A+B, AB, A\cap B$ and $[A : B]$ are fractional ideals of R. We have seen in Proposition 2.36 that invertible fractional ideals are finitely generated. Now we investigate the integral domains for which the converse is true.

2.4 Prüfer Domains

Definition 2.38. We call an integral domain R as Prüfer domain, in the case that each finitely generated ideal of R is invertible.

Let R be a Prüfer domain and let $A \in \mathcal{F}(R)$, then there exists a regular element $d \in R$ such that $dA \subseteq R$. Since R is Prüfer, then $dA = (d)A$ is invertible. Both dA and (d) is invertible gives that A is invertible.

Before giving a characterization of Prüfer domains, we mention a non-Noetherian example of a Prüfer domain, which is actually a Bezout domain.

Example 2.39. [9, p. 775, Exercise 23]Let $\mathscr{O}$ be the ring of integers in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Then $\mathscr{O}$ is a non-Noetherian Bezout domain.

Now we shall obtain some equivalent conditions for an integral domain to be a Prüfer domain.

Theorem 2.40. *Let R be an integral domain, then the following statements are equivalent:*

(1) *R is a Prüfer domain.*

(2) *A nonzero ideal of R which is generated by two distinct elements is invertible.*

(3) *Let A, B, C are ideals of R such that $A \neq (0)$. If $AB = AC$ and A is finitely generated, then $B = C$.*

(4) *For $P \in Spec(R)$ with $P \subset R$, R_P is a valuation ring.*

(5) *If A, B and C are ideals of R, then $A(B \cap C) = AB \cap AC$.*

(6) *If A and B are ideals of R, then $(A + B)(A \cap B) = AB$.*

(7) *If A is a finitely generated ideal of R and B is an ideal of R with $B \subseteq A$, then there exists an ideal C of R such that $B = AC$.*

(8) *Let A, B and C are ideals of R. If C is finitely generated, then $\big((A + B) : C\big) = (A : C) + (B : C)$.*

(9) *Let A, B and C are ideals of R. If A and B are finitely generated, then $\big(C : (A \cap B)\big) = (C : A) + (C : B)$.*

(10) *Let A, B and C are ideals of R. Then $A \cap (B + C) = (A \cap B) + (A \cap C)$.*

Proof. We begin the proof by showing that (1) and (2) are equivalent. Clearly (1) implies (2).

(2) $\Rightarrow$ (1) : Assume that (2) holds and let $C = (c_1, \dots, c_n)$ be a nonzero ideal of R. We use induction on number of generators to see that C is invertible. The claim is true for $n = 1$ and also $n = 2$ by our assumption. Let $n > 2$, and assume that every nonzero ideal generated by $n-1$ elements is invertible. We may also assume that $c_1, \dots, c_n$ are all nonzero. Now set $A = (c_1, \dots, c_{n-1}), B = (c_2, \dots, c_n), D = (c_1, c_n)$ and $E = c_1A^{-1}D^{-1} + c_nB^{-1}D^{-1}$. Our aim is to show that $EC = R$.

$$\begin{aligned} CE &= C(c_1A^{-1}D^{-1}) + C(c_nB^{-1}D^{-1}) \\ &= (A + (c_n))(c_1A^{-1}D^{-1}) + (B + (c_1))(c_nB^{-1}D^{-1}) \\ &= c_1D^{-1} + c_1c_nA^{-1}D^{-1} + c_1c_nB^{-1}D^{-1} + c_nD^{-1} \\ &= c_1D^{-1}(R + c_nB^{-1}) + c_nD^{-1}(R + c_1A^{-1}) \end{aligned}$$

Since we have $(c_1) \subseteq A$, $(c_n) \subseteq B$, and A, B are invertible ideals, then $c_1A^{-1}, c_nB^{-1} \subseteq R$ this gives that $CE = c_1D^{-1} + c_nD^{-1} = (c_1 + c_n)D^{-1} = DD^{-1} = R$. Hence C is invertible.

Now we have that (1) and (2) are equivalent.

(1) $\Rightarrow$ (3) : Assume that $AB = AC$ where A is finitely generated, and nonzero. Since R is a Prüfer domain, then A is invertible, hence $B = A^{-1}(AB) = A^{-1}(AC) = C$.

(3) $\Rightarrow$ (4) : Assume that (3) holds. In this case if A is finitely generated, then $AB \subseteq AC$ implies $B \subseteq C$, since if $AB \subseteq AC$, then $AC = AB + AC = A(B + C)$, by assumption it gives that $C = B + C$, hence $B \subseteq C$.

Now let $P \in Spec(R)$ be proper in R. We shall show that if $\frac{a}{s}, \frac{b}{t} \in R_P$, we have either $(\frac{a}{s}) \subseteq (\frac{b}{t})$ or $(\frac{b}{t}) \subseteq (\frac{a}{s})$. However, $s, t \notin P$ implies that $\frac{1}{s}, \frac{1}{t}$ are units in R_P, hence it suffices to show that we have either $aR_P \subseteq bR_P$ or $bR_P \subseteq aR_P$. If we have either $a = 0$ or $b = 0$, our claim is true, so we may further assume that a and b are nonzero.

It is easy to check that we have $(ab)(a, b) \subseteq (a^2, b^2)(a, b)$, and by (3), it implies $(ab) \subseteq (a^2, b^2)$. So $ab = a^2x + b^2y$ for some $x, y \in R$. It follows that $(yb)(a, b) \subseteq (a)(a, b)$:

Let $(ybz)(au + bv) \in (yb)(a, b)$, where $z, u, v \in R$. Since we have $b^2y = ab - a^2x$, then

$(ybz)(au + bv) = abyzu + b^2y(zv) = abyzu + (ab - a^2x)(zv) = abyzu + abzv - a^2xzv \in$

$(a)(a, b)$.

Since $(yb)(a, b) \subseteq (a)(a, b)$ and (3) holds, then $(yb) \subseteq (a)$, which implies $yb = au$ for some $u \in R$. So $ab = xa^2 + yb^2 = xa^2 + abu$, or $xa^2 = ab(1 - u)$

Now if $u \notin P$, then $yb = au$ implies that $a = b(\frac{y}{u}) \in bR_P$. If $u \in P$, then $1 - u \notin P$, hence $xa^2 = ab(1 - u)$ implies that $b = a(\frac{x}{1-u}) \in aR_P$.

$(4) \Rightarrow (5)$: Assume that (4) holds, and let $P \in Spec(R)$. If A, B, C are ideals of R, then $A(B \cap C)R_P = AR_P(BR_P \cap CR_P)$. Since R_P is a valuation ring, we either have $BR_P \subseteq CR_P$ or $CR_P \subseteq BR_P$. Without loss of generality, suppose that $BR_P \subseteq CR_P$, then clearly $AR_PBR_P \subseteq AR_PCR_P$. Hence;

$$\begin{aligned} A(B \cap C)R_P &= AR_P(BR_P \cap CR_P) \\ &= AR_PBR_P \\ &= AR_PBR_P \cap AR_PCR_P \\ &= ABR_P \cap ACR_P \\ &= (AB \cap AC)R_P \end{aligned}$$

Since we have $A(B \cap C)R_P = (AB \cap AC)R_P$ for arbitrary $P \in Spec(R)$, then we have $A(B \cap C) = AB \cap AC$.

The result can be obtained similarly if we suppose $CR_P \subseteq BR_P$.

$(5) \Rightarrow (6)$: Suppose (5) holds, then we have $(A+B)(A\cap B) = (A+B)A\cap(A+B)B$. Since $AB \subseteq A(A + B)$ and $AB \subseteq (A + B)B$, then $AB \subseteq (A + B)(A \cap B)$.

For the converse inclusion, let $(a + b)x \in (A + B)(A \cap B)$, where $a \in A, b \in B, x \in A \cap B$. Then $ax \in AB$ and $bx \in AB$, hence $(a + b)x \in AB$, which proves that (6) holds.

$(6) \Rightarrow (2)$: Let $C = (c_1, c_2)$ be a nonzero ideal of R. If $c_1 = 0$ or $c_2 = 0$, then C is principal hence invertible. So we shall assume that both c_1 and c_2 are nonzero. Then clearly $A = (c_1)$ and $B = (c_2)$ are invertible. Then ,

$$C(A \cap B)A^{-1}B^{-1} = (A + B)(A \cap B)A^{-1}B^{-1} = ABA^{-1}B^{-1} = R$$

Hence C is invertible.

Up to now, we have shown that the conditions (1) through (6) are all equivalent. Now we shall show that (7) is also equivalent to these:

(1) $\Rightarrow$ (7) : Let R be a Prüfer domain, let A and B be ideals of R such that A is finitely generated and $B \subseteq A$. If $A = (0)$, then $B = AC$ for every ideal C of R. If $A \neq (0)$, then A is invertible since it is finitely generated. By Proposition 2.36, there exists an ideal C of R such that, $B = AC$.

(7) $\Rightarrow$ (4) : Assume that (7) holds and let $P \in Spec(R)$ with $P \subset R$. We shall show that if $a, b \in R$, then either $aR_P \subseteq bR_P$ or $bR_P \subseteq aR_P$. We clearly have $(a) \subseteq (a, b)$ hence by our assumption, there exists an ideal A of R such that $(a) = (a, b)A$. Let $a = ax + by$, for $x, y \in A$. If we have $x \in P$, then $1 - x \notin P$, hence $a = b\frac{y}{1-x} \in bR_P$. Since we have $bA \subseteq (a)$, then $bx \in (a)$, and so $bx = au$ for some $u \in R$. In the case that $x \notin P$, we have $b = a\frac{u}{x} \in aR_P$. Hence R_P is a valuation ring.

Now we have the equivalence of (1) through (7).

To complete the proof, we first show that (4) implies each of (8), (9) and (10), and after that each of these implies one of the equivalent conditions we proved above.

(4) $\Rightarrow$ (8) : Let A, B and C be ideals of R such that C is finitely generated. Let $P \in Max(R)$. Under the assumption that (4) holds, we have R_P is a valuation ring, then the equality in (8) holds for ideals of R_P. After we show that $(AR_P : BR_P) = (A : B)R_P$ for A, B are ideals of R with B finitely generated, we shall complete the proof as following:

$$\begin{aligned} ((A+B):C)\,R_P &= ((A+B)R_P : CR_P) \\ &= (AR_P + BR_P : CR_P) \\ &= (AR_P : CR_P) + (BR_P : CR_P) \\ &= (A:C)R_P + (B:C)R_P \\ &= ((A:C)+(B:C))\,R_P \end{aligned}$$

Since the equality holds for all $P \in Max(R)$, then $((A+B):C) = (A:C) + (B:C)$.

Now we shall prove that $(AR_P : BR_P) = (A : B)R_P$ for A, B ideals of R with B finitely generated:

Let $\frac{x}{1} \in (A : B)R_P$ with $x \in (A : B)$. Since $xB \subseteq A$, then clearly $xBR_P \subseteq AR_P$, thus $x \in (AR_P : BR_P)$. For the converse inclusion, suppose that $B = (b_1, \ldots, b_k)$. Let $\frac{r}{s} \in (AR_P : BR_P)$, where $r \in R, s \in R \setminus P$. Since for all $i = 1, \ldots$k, $\frac{r}{s}\frac{b_i}{1} \in AR_P$, then $\frac{rb_i}{s} = \frac{a_i}{t_i}$ for all $i = 1, \ldots, k$ with $a_i \in A, t_i \in R \setminus P$. Hence there exist $s'_i \in R \setminus P$ such that $rb_it_is'_i = sa_is'_i \in A$. Set $s'' = t_1 \ldots t_k.s'_1 \ldots s'_k$. Clearly we have $s'' \in R \setminus P$.

We have $s''rb_i \in A$ for all $i = 1, \ldots, k$. It follows that $s''rB \subseteq A$ since $\{b_i\}_{i=1}^k$ is the set of generators of B, hence $s''r \in (A : B)$. Therefore, $\frac{r}{s} = \frac{s''r}{s''s} \in (A : B)R_P$ since $s''r \in (A : B)$ and $s''s \in R \setminus P$. Thus we have the desired equality.

(4) ⇒ (9) : Suppose that (4) holds. Let $P \in Spec(R)$ and let A, B and C be ideals of R such that A and B are finitely generated. Then

$$\begin{aligned}(C : (A \cap B))\, R_P &\subseteq (CR_P : (A \cap B)R_P)\\ &= (CR_P : AR_P) + (CR_P : BR_P)\\ &= (C : A)R_P + (C : B)R_P\\ &= ((C : A) + (C : B))\, R_P\\ &\subseteq (C : (A \cap B))\, R_P\end{aligned}$$

Thus we have $(C : (A \cap B))\, R_P = ((C : A) + (C : B))\, R_P$. Since it is true for arbitrary $P \in Spec(R)$, then we have the desired equality.

(4) ⇒ (10) : Assume that (4) holds, let A, B and C be ideals of R, and let $P \in Max(R)$. Then we have

$$\begin{aligned}(A \cap (B + C))\, R_P &= AR_P \cap (B + C)R_P\\ &= AR_P \cap (BR_P + CR_P)\\ &= (AR_P \cap BR_P) + (AR_P \cap CR_P)\\ &= (A \cap B)R_P + (A \cap C)R_P\\ &= ((A \cap B) + (A \cap C))\, R_P\end{aligned}$$

Since the equality holds for arbitrary $P \in Max(R)$, then the desired equality holds.

(8) ⇒ (2) : Let $a, b \in R$ be nonzero, and suppose that (8) holds. Then we have

$$\begin{aligned}R &= \big((a, b) : (a, b)\big)\\ &= \big((a) + (b) : (a, b)\big)\\ &= \big((a) : (a, b)\big) + \big((b) : (a, b)\big)\\ &= \big((a) : (b)\big) + \big((b) : (a)\big)\end{aligned}$$

By this equality $1 = x + y$ for some $x, y \in R$ such that $xb \in (a)$ and $ya \in (b)$. So we have that $(xb)b \subseteq (ab)$ and $(ya)a \subseteq (ab)$, and this implies that $(a, b)(bx, ay) \subseteq (ab)$. But since $1 = x + y$, then $ab = abx + aby$, hence we have that $(ab) = (a, b)(bx, ay)$.

Now since (ab) is invertible, then (a, b) is invertible.

(9) ⇒ (2) : Let $a, b \in R$ be nonzero. Assume that (9) holds. Then

$$\begin{aligned} R &= \big((a) \cap (b) : (a) \cap (b)\big) \\ &= \big((a) \cap (b) : (a)\big) + \big((a) \cap (b) : (b)\big) \\ &= \big((b) : (a)\big) + \big((a) : (b)\big) \end{aligned}$$

So the result follows as above.

(10) ⇒ (4) : Assume that (10) holds. Let $P \in Spec(R)$ be proper in R and let $a, b \in R$. Since $a \in (b) + (a - b)$, then we have

$$\begin{aligned} (a) &= (a) \cap \big((b) + (a - b)\big) \\ &= \big((a) \cap (b)\big) + \big((a) \cap (a - b)\big) \end{aligned}$$

Let $a = t + c(a - b)$ where $t \in (a) \cap (b), c \in R$ and $c(a - b) \in (a)$. Set $t = bu$ for some $u \in R$. Since $ca - cb \in (a)$, then $cb \in (a)$, set $cb = av$ for $v \in R$. Since $a = t + c(a - b)$, then $a(1 - c) = t - cb = (u - c)b \in (b)$.

If $c \in P$, then $1 - c \notin P$, hence we have that $a = b\frac{u-c}{1-c} \in bR_P$. If $c \notin P$, then $b = a\frac{v}{c} \in aR_P$. Hence R_P is a valuation ring. □

The following corollary says that, to obtain R is a Prüfer domain, it is sufficient to check the localizations only at maximal ideals of R instead of at all prime ideals of R.

Corollary 2.41. *Let R be an integral domain. Then R is a Prüfer domain if and only if R_P is a valuation ring for all $P \in Max(R)$.*

Proof. Since for a Prüfer domain R, all localizations of R at prime ideals are valuation rings, it is enough for us to check the sufficiency part. Let $P \in Spec(R)$. Let $P' \in Max(R)$ be such that $P \subseteq P'$. Since we have $R \setminus P' \subseteq R \setminus P$, then we clearly have $R_{P'} \subseteq R_P$, and $R_{P'}$ is a valuation ring by our assumption. Now by Corollary 2.3, we have that R_P is a valuation ring, since it is an overring of the valuation ring $R_{P'}$. Hence we have R_P is a valuation ring for $P \in Spec(R)$, then the equivalence of (1) and (6) of Theorem 2.40 completes the proof. □

Lemma 2.42. *Let R be an integral domain. The following statements hold:*

(1) $R = \bigcap_{P \in Max(R)} R_P$.

(2) *Let I be an ideal of R, then $I = \bigcap\limits_{P \in Max(R)} (IR_P \cap R)$.*

(3) *Let Q be an ideal of R such that $\sqrt{Q} = P$, a prime ideal of R. If QR_M is PR_M-primary for each $M \in Max(R)$ with $M \supseteq P$, then Q is P-primary.*

Proof. (1) Since $R \subseteq R_P$ for all $P \in Max(R)$, then $R \subseteq \bigcap\limits_{P \in Max(R)} R_P$. Now let $\alpha \in \bigcap\limits_{P \in Max(R)} R_P$ be arbitrary. Set $I = \{x \in R | x\alpha \in R\}$. We check if I is an ideal of R:

Clearly $0 \in I$, hence $I \neq \emptyset$.

Let $x \in I, r \in R$. $x \in I$ implies $x\alpha \in R$, then $rx\alpha \in R$, and so $rx \in I$.

If $a, b \in I$, then $a\alpha, b\alpha \in R$. It follows that $a\alpha + b\alpha = (a+b)\alpha \in R$, thus $a+b \in I$.

Hence I is an ideal of R.

If we show that $I = R$, then $1 \in I$, and so $1\alpha = \alpha \in R$, which gives the desired equality since α is an arbitrary element of the intersection. So by the way of contradiction, suppose $I \subset R$. Then there exists $M \in Max(R)$ such that $I \subseteq M$. Since $\alpha \in R_M$, then $\alpha = \frac{x}{y}$, where $x \in R, y \in R \setminus M$. Since $y\alpha = x \in R$, then $y \in I \subseteq M$, but this is a contradiction since $y \notin M$. So we have $I = R$, and the proof is complete.

(2) Set $Max(R) = \{P_\lambda\}_{\lambda \in \Lambda}$. Then we clearly have $I \subseteq IR_{P_\lambda} \cap R$ for all $\lambda \in \Lambda$. Suppose that $\bigcap\limits_{\lambda \in \Lambda} (IR_{P_\lambda} \cap R) \setminus I \neq \emptyset$ and let $x \in \bigcap\limits_{\lambda \in \Lambda} (IR_{P_\lambda} \cap R) \setminus I$. Since $x \notin I$, then $(I : (x))$ is proper in R. So there exists $\lambda_0 \in \Lambda$ such that $(I : (x)) \subseteq P_{\lambda_0}$. Since $x \in IR_{P_{\lambda_0}}$, then there exists $c \in R \setminus P_{\lambda_0}$ such that $cx \in I$. It follows that $c \in (I : (x)) \subseteq P_{\lambda_0}$ which contradicts our choice of c. Hence such an x doesn't exist, so the equality holds.

(3) Since we have $Q = \bigcap\limits_{M \in Max(R)} (QR_M \cap R)$, if we suppose $xy \in Q$ with $x \notin P$, then $\frac{xy}{1} \in QR_M$ for all $M \in Max(R)$ with $M \supseteq P$. $x \notin P$ implies $\frac{x}{1} \notin PR_M$, since otherwise, if $\frac{x}{1} = \frac{p}{r}$ for some $p \in P, r \in R \setminus M$, then there exists $u \in R \setminus M$ such that $uxr = up \in P$ and since $ur \in R \setminus M \subseteq R \setminus P$, we have $x \in P$, a contradiction. Since we have $\frac{x}{1} \notin PR_M$, then since QR_M is PR_M-primary, we have $\frac{y}{1} \in QR_M$, and this is true for all $M \in Max(R)$ with $M \supseteq P$. Clearly,

$y \in QR_M \cap R$ for all $M \in Max(R)$ with $M \supseteq P$. So by (2) of this lemma, we have $y \in Q$, hence Q is P-primary.

□

Theorem 2.43. *Let R be a Prüfer domain and let $P \in Spec(R)$. Then the following conditions hold:*

(1) *If Q is a P-primary ideal of R and $x \in R \setminus P$, then we have $Q = Q[Q + (x)]$.*

(2) *The set of P-primary ideals of R is closed under ideal multiplication.*

Proof. Let $M \in Max(R)$ be arbitrary. The first claim is clear if $Q \not\subseteq M$, since it implies $QR_M = Q^2R_M = R_M$. So assume that $Q \subseteq M$. Then since Q is P-primary, we have QR_M is PR_M-primary in R_M. Since R_M is a valuation ring and $x \notin PR_M$, then by Theorem 2.13, we have $QR_M = Q(x)R_M$. This equality holds for arbitrary $M \in Max(R)$, so we have $Q = Q(x)$. Since $Q^2 \subseteq Q$, then $Q = Q^2 + Q(x)$.

For the second claim, let Q_1, Q_2 be P-primary ideals of R. Then we clearly have Q_1R_M and Q_2R_M are PR_M-primary ideals. Since R_M is a valuation ring, then by Theorem 2.13 we have $(Q_1R_M)(Q_2R_M) = Q_1Q_2R_M$ is PR_M-primary for all $M \in Spec(R)$ with $M \supseteq P$. We clearly have $\sqrt{Q_1Q_2} = P$, so by (3) of Lemma 2.42, we have Q_1Q_2 is a P-primary ideal of R, hence product of P-primary ideals is P-primary. □

Let R be a Prüfer domain. Let $P \in Spec(R)$ be such that there exists a P-primary ideal of R which is different from P. To obtain some information about the P-primary ideals of R, we shall use the correspondence between the P-primary ideals of R and the PR_P-primary ideals of R_P. First of all, the set of P-primary ideals of R is totally ordered by inclusion, and as a result of Theorem 2.13, if $\bar{P}$ is the intersection of all P-primary ideals of R, then $\bar{P}$ is prime and there is no prime ideal between P and $\bar{P}$. Hence the valuation ring $R_P/\bar{P}R_P$ has rank one.

Let $* : R \to R_P \to R_P/\bar{P}R_P$ be the composition of the natural homomorphisms. If I is an ideal of R, then we shall use the notation I^* instead of $*(I)$. In this case, there is a one-to-one order preserving correspondence between the P-primary ideals Q of R and the P^*-primary ideals Q^* of R^*. Under this correspondence Q and Q^* are the corresponded ideals of each other. This correspondence gives us the ability to focus only rank one valuation rings to prove some results on Prüfer domains as below.

Lemma 2.44. *Let V be a rank one valuation ring and let P be its maximal ideal. Let Q be a P-primary ideal of R. Then following statements hold:*

1. *If $Q \neq Q^2$, then $\bigcap\limits_{n\geq 1} Q^n = 0$.*
2. *If for some $i \in \mathbb{N}$, $Q^i = Q^{i+1}$, then $Q = Q^2 = P$.*

Proof. By Theorem 2.11, we have $\bigcap\limits_{n\geq 1} Q^n$ is a prime ideal of V. Now if $Q \neq Q^2$, then $\bigcap\limits_{n\geq 1} Q^n \subset Q \subseteq P$, and since V has rank one, we have $\bigcap\limits_{n\geq 1} Q^n = 0$. Suppose that there exists $i \in \mathbb{N}$ such that $Q^i = Q^{i+1}$, then $\bigcap\limits_{n\geq 1} Q^n = Q^i$ is a prime ideal of V. Since V is an integral domain, then $Q^i = 0$ implies $Q = 0$, so we must have $Q^i = P$. Therefore we have $P = Q^i \subseteq Q^{i-1} \subseteq \ldots \subseteq Q \subseteq P$ or simply $Q = Q^2 = P$. □

Proposition 2.45. *Let R be a Prüfer domain. If Q is a P-primary ideal of R, then $\bigcap\limits_{n=1}^{\infty} Q^n \in Spec(R)$.*

Proof. Observe that we immediately have

$$\bigcap_{n=1}^{\infty} Q^n \subseteq \left[\Big(\bigcap_{n=1}^{\infty} Q^n\Big) R_P\right] \cap R \subseteq \left(\bigcap_{n=1}^{\infty} (QR_P)^n\right) \cap R.$$

On the other hand, since Q^n is a P–primary ideal of R by Theorem 2.43 (2), we also have

$$\left(\bigcap_{n=1}^{\infty} (QR_P)^n\right) \cap R \subseteq Q^n R_p \cap R = Q^n$$

for each $n \geq 1$. It follows that

$$\bigcap_{n=1}^{\infty} Q^n = \left[\Big(\bigcap_{n=1}^{\infty} Q^n\Big) R_P\right] \cap R = \left(\bigcap_{n=1}^{\infty} (QR_P)^n\right) \cap R.$$

If $\bar{P}$ and the homomorphism $*$ are defined as above, then the correspondence constructed by $*$ and Lemma 2.44 complete the proof. □

Now we shall give a characterization of Prüfer domain in terms of their overrings. Before this, we need some definitions and theorems.

Theorem 2.46 (The Lying-Over Theorem). *Let R' be a ring and let R be its subring. If R' is integral over R, then for each $P \in Spec(R)$, there exists $P' \in Spec(R')$ such that $P' \cap R = P$. Moreover, P is a maximal ideal of R if and only if P' is a maximal ideal of R'.*

Recall that an R-module M is flat if for each embedding $f : N_1 \to N_2$ of R-modules, $1_M \otimes f : M \otimes_R N_1 \to M \otimes_R N_2$ is also an embedding, where 1_M is the identity homomorphism of M.

Definition. An overring T of a ring R is called a flat overring, if T is a flat R-module.

Lemma 2.47. *Let R be a ring and M be an R-module. Then there is a group isomorphism $\Psi : M \otimes_R R \to M$ defined by $\Psi(m \otimes a) = ma$ for all $a \in R$ and $m \in M$.*

Lemma 2.48. *Let R be a ring and M be an R-module such that, for an ideal I of R and $f : I \to R$ given by $f(a) = a$ for all $a \in I$, $1_M \otimes f$ is injective, then M is flat.*

Although flatness of a module mostly defined homologically, we shall give an element-wise characterization of flatness which is useful for our study.

Lemma 2.49. *Let R' be a ring and let R be a subring of R', let $x_1, \ldots, x_n$ be indeterminates. Then R' is a flat R-module if and only if for every solution $c_1, \ldots, c_n$ in R' of a system of equations*

$$\sum_{i=1}^{n} x_i a_{ih} = 0, h = 1, \ldots, r$$

where $a_{ih} \in R$ for each i and h, we have $d_1, \ldots d_k \in R'$ and $b_{ji} \in R$ for each i and j such that

$$c_i = \sum_{j=1}^{k} d_j b_{ji}, i = 1, \ldots, n \text{ and } \sum_{i=1}^{n} b_{ji} a_{ih} = 0, j = 1, \ldots, k, h = 1, \ldots, r.$$

Proposition 2.50. *Let R be an integral domain, and let T be an overring of R. Then the following statements are equivalent:*

(1) *For $P \in Spec(R)$, either $PT = T$ or $T \subseteq R_P$ holds.*

(2) *For all $\frac{x}{y} \in T$ with $x, y \in R$, $(y : x)T = T$.*

Proof. First, suppose that (1) holds. Let $\frac{x}{y} \in T$ and by the way of contradiction, suppose that $(y : x)T \neq T$. Then there exists $P \in Spec(R)$ such that $(y : x) \subseteq P$ and $PT \neq T$. By our assumption, $T \subseteq R_P$ and so $\frac{x}{y} \in R_P$. Hence there exist $a \in R, s \in R \setminus P$ such that $\frac{x}{y} = \frac{a}{s}$ and it follows that for some $u \in R \setminus P$ we have $xsu = ayu \in (y)$. So we have $su \in (y : x) \subseteq P$, which is a contradiction. Thus $(y : x)T = T$.

Now assume that (2) holds. Let $P \in Spec(R)$ with $PT \neq T$. Our aim is to show that $T \subseteq R_P$. So let $\frac{x}{y} \in T$. Then $(y : x)T = T$ and this gives $(y : x) \nsubseteq P$, since otherwise $(y : x)T = T$ implies $PT = T$, a contradiction. Now let $u \in (y : x) \setminus P$, then $ux = yr$ for some $r \in R$. So we have $\frac{x}{y} = \frac{r}{u} \in R_P$ since $u \notin P$, hence $T \subseteq R_P$. □

Proposition 2.51. *Let R be an integral domain and T be an overring of R. Then T is a flat overring if and only the equivalent conditions of Proposition 2.50 holds for T.*

Proof. First suppose that T is a flat overring of R. Our aim is to show that condition (1) of Proposition 2.50 holds. If $\frac{x}{y} \in T$, then $y\left(\frac{x}{y}\right) - x\,1 = 0$, so by Lemma 2.49, there exists $z_{jk} \in R, j = 1, \ldots, r, k = 1, 2$ and $b_1, \ldots, b_r \in T$ such that

$$\begin{aligned} \tfrac{x}{y} &= \sum_{j=1}^{r} b_j z_{j1}, \\ 1 &= \sum_{j=1}^{r} b_j z_{j2}, \\ z_{j1}y - z_{j2}x &= 0, \qquad\qquad j = 1, \ldots, r \end{aligned}$$

Let $P \in Spec(R)$. In the case that $z_{j2} \in P$, for $j = 1, \ldots, r$, then we clearly have $PT = T$. So suppose $z_{j2} \notin P$ for some $j = 1, \ldots, r$. It follows that $(y : x) \nsubseteq P$ and hence, we have either $PT = T$ or $(y : x) \nsubseteq P$ for all $\frac{x}{y} \in T$. If $PT = T$, then we are done, so suppose that $(y : x) \nsubseteq P$ for all $\frac{x}{y} \in T$. For each $\frac{x}{y} \in T$, there exists $s \in (y : x) \setminus P$ and this gives that, there exist $a \in R$ such that $ay = sx$, since $s \in R \setminus P$ we have that $\frac{x}{y} = \frac{a}{s} \in R_P$.

For the converse part of the proof, suppose that condition (2) of Proposition 2.50 holds for T. By lemmas 2.47 and 2.48, it suffices to prove that for an ideal I of R, the homomorphism $\phi : I \otimes_R T \to T$ given by $\phi(a \otimes b) = ab$ for all $a \in I, b \in T$ is injective.

So let $c \in I \otimes_R T$, then there exist $a_i \in I, b_i \in T$ for $i = 1, \ldots, s$ such that $c = \sum_{i=1}^{s} a_i \otimes b_i$. There exist $b, c_1, \ldots, c_s \in R$ such that $b_i = \frac{c_i}{b}$ for $i = 1, \ldots, s$; thus $c = \sum_{i=1}^{s} a_i \otimes \frac{ci}{b}$. By our assumption, $(b : c_i)T = T$ for $i = 1, \ldots, s$. It follows that if we set $C = \bigcap_{i=1}^{s} (b : c_i)$, then we have $CT = T$. Now suppose that $\phi(c) = \phi(\sum_{i=1}^{s} a_i \otimes \frac{c_i}{b}) = 0$, that is $\sum_{i=1}^{s} \frac{a_i c_i}{b} = 0$. Let $d \in C$, so we have $dc_i \in (b)$ for $i = 1, \ldots, s$, hence $\frac{dc_i}{b} \in R$ for

$i = 1, \ldots, s$; thus

$$\begin{aligned} dc &= \sum_{i=1}^{s} a_i \otimes \tfrac{dc_i}{b} &= \sum_{i=1}^{s} \left(\tfrac{da_i c_i}{b} \otimes 1 \right) \\ &= \left(d \sum_{i=1}^{s} \tfrac{a_i c_i}{b} \right) \otimes 1 &= 0 \end{aligned}$$

It follows that $cC = 0$ and so $0 = 0T = cCT = cT$. Since $c \in cT$, then we have $c = 0$, which gives that ϕ is injective. Hence T is a flat R-module. $\square$

Proposition 2.52. *Let R be an integral domain and T be an overring of R. Then the following statements are equivalent:*

(1) *T is a flat overring of R.*

(2) *$T_P = R_{P \cap R}$ for all $P \in Max(T)$.*

(3) *$T = \bigcap_{P \in Max(T)} R_{P \cap R}$.*

Proof. Assume that T is a flat overring of R and let $P \in Max(T)$. Our aim is to show that (2) holds. We clearly have $R_{P \cap R} \subseteq T_P$. So let $\frac{x}{y} \in T_P$, where $x, y \in T$ with $y \notin P$. Then there exist $u, v, s \in R$ such that $x = \frac{u}{s}$ and $y = \frac{v}{s}$. Set $C = (s : u) \cap (s : v)$. By Proposition2.51, we have $CT = T$, thus $C \nsubseteq P \cap R$. Let $z \in C \setminus (P \cap R)$. Then $zx, zy \in R$ and $zy \notin P$, hence $zy \notin P \cap R$. It follows that $\frac{x}{y} = \frac{zx}{zy} \in R_{P \cap R}$, and this gives $T_P \subseteq R_{P \cap R}$.

Now suppose (2) holds, then since we know $T = \bigcap_{P \in Max(T)} T_P$, by condition (2), this is $T = \bigcap_{P \in Max(R)} R_{P \cap R}$. So (2) implies (3).

Finally, suppose (3) holds. Let $Q \in Spec(R)$ be such that $QT \neq T$. Then $QT \subseteq P$ for some $P \in Max(R)$ and so $Q \subseteq P \cap R$. This gives $R_{P \cap R} \subseteq R_Q$. But since $T \subseteq R_{P \cap R}$, then we have $T \subseteq R_Q$. Hence T is a flat overring of R. $\square$

Proposition 2.53. *Let R be an integral domain and let T and T' be overrings of R such that $T \subseteq T'$. Then the following statements hold:*

(1) *T' is a flat overring of R implies that T' is a flat overring of T.*

(2) *If T' is a flat overring of T and T is a flat overring of R, then T' is a flat overring of R.*

Proof. For the first part, assume that T' is a flat overring of R. Let $a, b \in T$ be such that $\frac{a}{b} \in T'$. Since a and b are both elements of the field of fractions of R and finitely many elements of K can be written in a common denominator, then we can write $a = \frac{c}{s}$ and $b = \frac{d}{s}$, where $s, c, d \in R$. Then we have $\frac{a}{b} = \frac{c}{d} \in T'$. Hence by Proposition 2.51, we have $(d : c)T = T$. So there exist $t_1, \dots, t_k \in T'$ and $u_1, \dots, u_k \in (d : c)$ such that $1 = \sum_{i=1}^{k} t_i u_i$. Since $u_i \in (d : c)$, then $u_i c \in (d) = Td$ for $i = 1, \dots, k$. It follows that $u_i a \in Tb$ for $i = 1, \dots, k$. Hence, $(Tb : Ta)T' = T'$. Therefore, T' is a flat overring of T.

For the second part, let $P'' \in Max(T')$. Set $P' = P'' \cap T$ and $P = P' \cap R$. Clearly we have $P' \in Max(T)$ and $P \in Max(R)$. Moreover, we have $P = P' \cap R = P'' \cap T \cap R = P'' \cap R$. Since T' is a flat overring of T and for $P'' \in Max(T')$, $P' = P'' \cap T$ holds, then by Proposition 2.52, we have $(T')_{P''} = (T)_{P'}$. Similarly since T is a flat overring of R, and we have $P' \in Max(T)$, then again by Proposition 2.52, $P = P' \cap R$ implies that $(T)_{P'} = R_P$. Hence we have $(T')_{P''} = R_P$ for arbitrary $P'' \in Max(T')$. It again follows from Proposition 2.52 that, T'' is a flat overring of R. □

Theorem 2.54. *The only integral flat overring of an integral domain R is R itself.*

Proof. Let R be an integral domain and T be a flat overring of R. Let $\frac{x}{y} \in T$, then by Proposition 2.51, we have $(y : x)T = T$. If $P \in Spec(R)$, then by Lying-Over Theorem, there exists $P' \in Spec(T)$ such that $P' \subset T$ and $P' \cap R = P$. Since $PT \subseteq P'$, we have $PT \neq T$. It follows with the fact $(y : x)T = T$ that $(y : x)$ is not contained in any prime ideal of R, hence $(y : x) = R$. Thus $1x \in (y)$, and this implies $\frac{x}{y} \in R$. Hence $T = R$. □

Theorem 2.55. *Let R be an integral domain. Then R is Prüfer if and only if each overring of R is a flat R-module.*

Proof. Suppose first that each overring of R is flat. Let $P \in Max(R)$. By Proposition 2.53 since R_P is an overring of R and every overring of R which contains R_P is flat, then every overring of R_P is flat. Our aim is to show that R_P is a valuation ring, so let $a, b \in R_P$ be such that $aR_P \nsubseteq bR_P$. If $b = 0$, then we clearly have $bR_P \subseteq aR_P$, and this is what we aim to show, hence let $b \neq 0$. We have $(bR_P : aR_P) \neq R_P$, and so $(bR_P : aR_P) \subseteq PR_P$, since PR_P is the unique maximal ideal of R_P. The ring $R_P[\frac{a}{b}] = \left\{ f(\frac{a}{b}) | f(X) \in R_P[X] \right\}$ is an overring of R_P, so it is a flat overring of R_P.

By Proposition 2.51, since $\frac{a}{b} \in R_P[\frac{a}{b}]$, we have $(bR_P : aR_P)R_p[\frac{a}{b}] = R_P[\frac{a}{b}]$. So we have $x_1b_1 + \ldots + x_nb_n = 1$ for some $x_1, \ldots, x_n \in (bR_P : aR_P)$ and $b_{1,} \ldots, b_n \in R_P[\frac{a}{b}]$. For $i = 1, \ldots, n$ there exists $a_{ij} \in R_P$ where $j = 1, \ldots, s$ for some $s \in \mathbb{N}$ such that $b_i = \sum\limits_{j=0}^{s} a_{ij}(\frac{a}{b})^j$. Then we have $1 = \sum\limits_{i=1}^{n} x_ib_i = \sum\limits_{i=1}^{n} x_i \sum\limits_{j=0}^{s} a_{ij}(\frac{a}{b})^j = \sum\limits_{j=0}^{s} d_j(\frac{a}{b})^j$ where $d_j = \sum\limits_{i=1}^{n} x_ia_{ij} \in (bR_P : aR_P)$ for $j = 0, \ldots, s$. Since $(bR_P : aR_P) \neq R_P$, then d_j is not a unit in R_P for $j = 0, \ldots, s$. Since d_0 is not a unit, then $1 - d_0$ is a unit in R_p. If we multiply the equality by $(1 - d_0)^{s-1}(\frac{b}{a})^s$, then we have

$$\left((1 - d_0)\left(\frac{b}{a}\right)\right)^s - d_1\left((1 - d_0)\left(\frac{b}{a}\right)\right)^{s-1} - \ldots - d_s(1 - d_0)^{s-1} = 0$$

Thus $(1 - d_0)\left(\frac{b}{a}\right)$ is an integral element over R_P. Since $R_P\left[(1 - d_0)\left(\frac{b}{a}\right)\right]$ is a flat overring of R_P, by Theorem 2.54, $R_P = R_P\left[(1 - d_0)\left(\frac{b}{a}\right)\right]$, hence $(1 - d_0)\left(\frac{b}{a}\right) \in R_P$. Since $1 - d_0$ is a unit in R_P, then we have $b \in aR_P$ or equivalently $bR_P \subseteq aR_P$. Hence the localization R_P at an arbitrary prime ideal P is a valuation ring. Therefore, R is a Prüfer domain.

Now assume that R is a Prüfer domain, and let T be an overring of R. Let $P \in Max(T)$. Clearly T_P is an overring of the valuation ring $R_{P \cap R}$, hence T_P is a valuation ring.

Let $x \in T_P$. If $x \notin R_{P \cap R}$, then since $R_{P \cap R}$ is a valuation ring, we have $\frac{1}{x} \in R_{P \cap R}$ and since it is not a unit in $R_{P \cap R}$, then $\frac{1}{x} \in (P \cap R)R_{P \cap R} \subseteq PT_P$. This is a contradiction since $x \in T_P$, hence $\frac{1}{x}$ is a unit in T_P. So $T_P = R_{P \cap R}$. Since this is true for arbitrary maximal ideal of T, then T is a flat overring of R by Proposition 2.52. □

The following two corollaries can easily be obtained from Theorem 2.55, its proof, and Proposition 2.52.

Corollary 2.56. *Each overring of a Prüfer domain is a Prüfer domain.*

Corollary 2.57. *Let R be a Prüfer domain and T be an overring of R. If $\Gamma = \{P \in Spec(R) | PT \neq T\}$, then $T = \bigcap\limits_{P \in \Gamma} R_P$.*

We shall give another characterization of Prüfer domains in terms of their overrings.

Theorem 2.58. *Let R be an integral domain. Then R is a Prüfer ring if and only if each overring of R is integrally closed.*

Proof. Let R be a Prüfer domain, then by Corollary 2.57, each overring of R is an intersection of some valuation rings. Since valuation rings are integrally closed by Proposition 2.5, the same is true of their intersection R.

Now assume that each overring of R is integrally closed. Let $P \in Max(R)$. Our aim is to show that R_P is a valuation ring, for once this is done, R becomes Prüfer since P is an arbitrary maximal ideal of R. Let K be the field of fractions of R and let $a \in K \setminus R_P$ be nonzero, we shall show $\frac{1}{a} \in R_P$. Since $R_P[a^2]$ is an overring of R_P, then it is integrally closed. Clearly a is integral over $R_P[a^2]$, hence $a \in R_P[a^2]$. Then $a = b_0 + b_1a^2 + \ldots + b_na^{2n}$ for some $b_0, \ldots, b_n \in R_P$. Multiplying by b_0^{2n-1}/a^{2n}, we get $\left(\frac{b_0}{a}\right)^{2n} - \left(\frac{b_0}{a}\right)^{2n-1} + b_1b_0\left(\frac{b_0}{a}\right)^{2n-2} + \ldots + b_nb_0^{2n-1} = 0$. Hence $\frac{b_0}{a}$ is integral over R_P, so it belongs to R_P. Now if $\frac{b_0}{a}$ is unit in R_P, then $a \in R_P$. If $\frac{b_0}{a}$ is not a unit in R_P, then $1 - \frac{b_0}{a}$ is a unit in R_P. Multiplying the equation which we express a in terms of powers of a^2 by $\frac{1}{a^{2n}}$, we have

$$\left(1 - \frac{b_0}{a}\right)\left(\frac{1}{a}\right)^{2n-1} - b_1b_0\left(\frac{1}{a}\right)^{2n-2} - \ldots - b_n = 0$$

Since $\left(1 - \frac{b_0}{a}\right)$ is a unit in R_P, then $\frac{1}{a}$ is integral over R_P, thus $\frac{1}{a} \in R_P$. So R_P is a valuation ring and the result follows. □

2.5 Dedekind Domains

Definition 2.59. An integral domain is said to be a Dedekind domain, if every ideal of R is a product of prime ideals.

Proposition 2.60. *Let R be an integral domain and let I be a proper ideal of R such that $I = P_1 \ldots P_n$, where all P_i's are invertible prime ideals of R. Then this is the unique way of expressing I as a product of invertible prime ideals of R, up to the order of the factors.*

Proof. Let $I = P'_1 \ldots P'_m$, where P'_i is an invertible prime ideal of R for $i = 1, \ldots, m$. Without loss of generality, assume that P_1 is minimal among $P_1, \ldots, P_n$. Since $I = P'_1 \ldots P'_m \subseteq P_1$, then $P'_j \subseteq P_1$ for some $j = 1, \ldots, m$, say $P'_1 \subseteq P_1$. Similarly $I = P_1 \ldots P_n \subseteq P'_1$ implies that $P_i \subseteq P'_1$ for some $i = 1, \ldots, n$. Since this inclusion implies $P_i \subseteq P_1$, by the choice of P_1, we must have $i = 1$, hence $P_1 = P'_1$. Since P_1 is invertible, then we have $P_2 \dots P_n = P'_2 \dots P'_m$. By continuing in this way, we must have $n = m$, and there exists a permutation $\sigma \in S_n$ such that $P_i = P'_{\sigma(i)}$ for $i = 1, \dots, n$. □

Theorem 2.61. *Let R be a Dedekind domain, and let I be a nonzero proper ideal of R. Then I is expressible as a product of prime ideals of R. Moreover, this expression is unique up to the order of the factors.*

Proof. Firstly, we shall show that an invertible prime ideal of R is maximal. Let P be an invertible prime ideal of R. Our aim is to show P is maximal by proving that $P + (a) = R$ for any $a \in R \setminus P$.

Suppose that for some $a \in R \setminus P$, we have $P + (a) \subset R$, then $P + (a) = P_1 \dots P_k$ and $P + (a^2) = Q_1 \dots Q_m$, where P_i and Q_j are prime ideals for $i = 1, \dots, k$, $j = 1, \dots, m$. Let $\phi : R \to R/P$ be the canonical epimorphism, and let R', P'_i, Q'_j and a' be the images of R, P_i, Q_j and a, respectively, under ϕ. In this case, we clearly have $a'R' = P'_1 \dots P'_k$ and $a'^2 R' = Q'_1 \dots Q'_m$. Since $a' \neq 0$, then the ideals $a'R'$ and a'^2R' are both invertible, so it is also true for each P'_i and Q'_j. Since we have $P'^2_1 \dots P'^2_k = Q'_1 \dots Q'_m$, then by Proposition 2.60, $m = 2k$. So we may order the primes such that $Q_{2i-1} = Q_{2i} = P_i$ for $i = 1, \dots, k$. Hence $\big(P + (a)\big)^2 = P + (a^2)$, and it follows that $P \subseteq \big(P + (a)\big)^2 \subseteq P^2 + (a)$. So if $b \in P$, then $b = c + da$ for some $c \in P^2, d \in R$. $da = b - c \in P$ and $a \notin P$ together implies that $d \in P$, hence $P \subseteq P^2 + Pa$. Since P is invertible, then there exists a fractional ideal A such that $PA = R$. Then $R = PA \subseteq P^2A + PA(a) = P + (a)$. This contradicts with our assumption, hence P is maximal.

To complete the proof, we shall show that every nonzero prime ideal of R is invertible. Then our claim is clear by Proposition 2.60.

Let $P \in \mathit{Spec}(R)$ be nonzero. If $R = P$, then P is invertible, hence there is nothing to prove. So suppose that $P \subset R$. Let $a \in P$ be nonzero. Write $(a) = P_1 \dots P_s$, where each P_i is a prime ideal of R. Since (a) is invertible, then each P_i is invertible, hence maximal for $i = 1, \dots, s$. Then $(a) = P_1 \dots P_s \subseteq P$ implies that $P_i \subseteq P$ for some $i = 1, \dots, s$. By the maximality of P_i, we have $P = P_i$, thus P is invertible. □

Proposition 2.62. *Let R be an integral domain. Then R is a Dedekind domain if and only if the set of nonzero fractional ideals of R is a group with respect to ideal multiplication.*

Proof. Firstly, suppose that R is a Dedekind domain. Let $\mathcal{F}(R)$ be the set of nonzero fractional ideals of R. We have mentioned that $\mathcal{F}(R)$ is closed under multiplication of fractional ideals. With respect to this multiplication, $\mathcal{F}(R)$ is a semigroup with identity element R. By Theorem 2.61 and its proof, we have that every ideal of R is invertible, since it is a product of prime ideals of R, which are invertible. Let $A \in \mathcal{F}(R)$ be arbitrary, then there exists $d \in R$ such that $dA \subseteq R$. So there exists a fractional ideal B of R such that $(dA)B = R$. It follows that $(dB)A = R$, hence A has an inverse in $\mathcal{F}(R)$. Thus $\mathcal{F}(R)$ is a group.

For the sufficiency part, we shall show every ideal of R is a product of prime ideals. Let $\mathscr{S}$ be the set of all nonzero proper ideals of R which are not expressible as a product of prime ideals. Our aim is to show $\mathscr{S} = \emptyset$ if $\mathcal{F}(R)$ is a group. By the way of contradiction, assume that $\mathscr{S} \neq \emptyset$. Since every nonzero ideal of R is invertible, then R is Noetherian. So by the maximal condition, $\mathscr{S}$ has a maximal element, say A. Since A is proper in R, then $A \subseteq M$ for some $M \in Max(R)$. Clearly, $A \in \mathscr{S}$ implies $A \neq M$. Let $B \in \mathcal{F}(R)$ be such that $MB = R$. Since $A \subseteq M$, then we have $AB \subseteq MB = R$, and since $R = MB \subseteq B$, then $A = AR \subseteq AB$. If $A \subset AB$, then the maximality of A in $\mathscr{S}$ implies that $AB \notin \mathscr{S}$, hence AB is a product of some prime ideals. But it follows that $A = A(BM) = (AB)M$ is also a product of prime ideals which is a contradiction. So we must have $A = AB$, so $AM = (AB)M = A$. Since $A \in \mathcal{F}(R)$, then it is invertible, so we have $M = R$ which is impossible. Hence our assumption that $\mathscr{S} \neq \emptyset$ is false. Therefore, R is a Dedekind domain. □

From Theorem 2.61 and Proposition 2.62, the following corollary can be given:

Corollary 2.63. *Let R be an integral domain. Then R is a Dedekind domain if and only if every nonzero ideal of R is invertible.*

Corollary 2.64. *If R is a Dedekind domain, then R is a Noetherian domain with $Spec(R) = Max(R)$.*

Proof. It is clear from the proof of Theorem 2.61 that $Spec(R) = Max(R)$. It follows directly from Proposition 2.36 and Theorem 2.63 that every nonzero proper ideal of R is finitely generated. Hence R is Noetherian. □

Proposition 2.65. *Let R be a Dedekind domain and let I be an ideal of R. If $I = P_1 \dots P_n$ for some $P_1, \dots, P_n \in Spec(R)$, then $\{P_1, \dots, P_n\} = \{P \in Spec(R) | I \subseteq P\}$. Thus, every ideal in a Dedekind domain contained by only a finite number of prime ideals.*

Proof. Let $I = P_1 \dots P_n$ where $P_i \in Spec(R)$ for all $i = 1, \dots, n$. Let $P \in Spec(R)$ with $I \subseteq P$. Then we have $I = P_1 \dots P_n \subseteq P$, hence $P_i \subseteq P$ for some $i = 1, \dots, n$. By Corollary 2.64, we have $P_i = P$. Hence a prime ideal containing I must be occur in the factorization of I. Conversely, if $I = P_1 \dots P_n$, then we clearly have $I \subseteq P_i$ for all $i = 1, \dots, n$ which completes the proof. □

Now we shall give several characterizations for a Noetherian integral domain to be a Dedekind domain.

Theorem 2.66. *If R is Noetherian integral domain, then the following statements are equivalent:*

(1) *R is a Dedekind domain.*

(2) *R is integrally closed and every prime ideal of R is maximal.*

(3) *Each nonzero ideal of R which generated by two elements is invertible.*

(4) *If A, B, C are ideals of R such that $AB = AC$ with A is nonzero, then $B = C$.*

(5) *For $P \in Max(R)$, R_P is a valuation ring.*

(6) *If A, B and C are ideals of R, then $A(B \cap C) = AB \cap AC$.*

(7) *If A and B are ideals of R, then $(A + B)(A \cap B) = AB$.*

(8) *If A and B are ideals of R with $A \subseteq B$, then there exists an ideal C of R such that $A = BC$.*

(9) *If A, B and C are ideals of R, then $(A + B : C) = (A : C) + (B : C)$.*

(10) *If A, B and C are ideals of R, then $(A : B \cap C) = (A : B) + (A : C)$.*

(11) *If A, B and C are ideals of R, then $A \cap (B + C) = A \cap B + A \cap C$.*

(12) *If $P \in Max(R)$, then there are no ideals of R strictly between R and R^2.*

(13) *If $P \in Max(R)$, then every P-primary ideal of R is a power of P.*

(14) *If $P \in Max(R)$, then the set of P-primary ideals of R is totally ordered by inclusion.*

(15) *Each overring of R is a flat overring.*

(16) *Each overring of R is integrally closed.*

Proof. Let R be a Noetherian integral domain.By Theorem 2.63, being a Dedekind domain and being a Prüfer domain are equivalent for R. So by theorems 2.40, 2.55 and 2.58 we have all the conditions except $(2),(12),(13),(14)$ are equivalent. Thus it suffices to prove that these are also equivalent to others.

$(1) \Rightarrow (2)$: Let R be a Dedekind domain. Then R is integrally closed since it is a Prüfer domain. R has Krull dimension one by Corollary 2.64.

$(2) \Rightarrow (5)$: Assume that R is integrally closed and has the property that every prime ideal of R is maximal. Let $P \in Max(R)$ be nonzero. Then R_P is Noetherian. R_P is integrally closed by Corollary 2.30. Furthermore, PR_P is the only nonzero prime ideal of R_P. Therefore R_P is a valuation ring by Theorem 2.10.

$(5) \Rightarrow (12)$: Let $P \in Max(R)$. If $P = (0)$ the claim is obvious. So assume that $P \neq (0)$ and that R_P is a valuation ring. Let I be an ideal of R with $P^2 \subseteq I \subseteq P$. Clearly I is P-primary. It follows that $I = IR_P \cap R$. But $P^2R_P \subseteq IR_P \subseteq PR_P$ implies that we have either $PR_P = IR_P$ or $P^2R_P = IR_P$. Since $I = IR_P \cap R$, then we have either $P = I$ or $P^2 = I$.

$(12) \Rightarrow (5)$: Assume that (12) holds. Let $P \in Max(R)$ be nonzero. Then clearly $PR_P \neq (0)$ in R_P. By the Krull Intersection Theorem, we have $\bigcap\limits_{n\geq 1} P^nR_P = (0)$. It follows that $PR_P \neq P^2R_P$. By our assumption, there are no ideals between PR_P and P^2R_P. Let $\bar{P}$ denotes PR_P. Let $a \in \bar{P} \setminus \bar{P}^2$. Then clearly $\bar{P} = \bar{P}^2 + aR_P$. Multiplying by $\bar{P}$ gives that $\bar{P}^2 = \bar{P}^3 + aPR_P$, if we add aR_P at both sides, since $aPR_P \subseteq aR_P$, we have that $\bar{P} = \bar{P}^2 + aR_P = \bar{P}^3 + aR_P$. By continuing in this way, we have that $\bar{P} = \bar{P}^n + aR_P$ for all $n \in \mathbb{N}$. Hence $\bar{P} = \bigcap\limits_{n\geq 1} (aR_P + \bar{P}^n)$.

Since $\bar{P}/aR_p$ is the unique maximal ideal of the Noetherian valuation ring R_P/aR_P, we have the following:

$$\frac{\bar{P}}{aR_P} = \frac{\bigcap_{n\geq 1} \left(aR_P + \bar{P}^n\right)}{aR_P} = \bigcap_{n\geq 1} \frac{aR_P + \bar{P}^n}{aR_p} = \bigcap_{n\geq 1} \left(\frac{P'}{aR_p}\right)^n = (0)$$

This implies that $\bar{P} = aR_P$, and since the set of non-units $\bar{P}$ is principal, it follows from Theorem 2.10 that R_P is a valuation ring.

(1) $\Rightarrow$ (13) : Let R be a Dedekind domain, and let $P \in Max(R)$. If $P = 0$, then the only P-primary ideal of R is P. So suppose that $P \neq (0)$ and let Q be a P-primary ideal of R. Since R is a Dedekind domain, there exists $P_1, \ldots, P_n \in Spec(R)$ such that $Q = P_1 \ldots P_n$. Since we have $P = \sqrt{Q} = \sqrt{P_1 \ldots P_n} = \sqrt{P_1} \cap \ldots \cap \sqrt{P_n} = P_1 \cap \ldots \cap P_n$ and by the maximality of P, we have $P_i = P$ for $i = 1, \ldots, n$ hence $Q = P^n$.

(13) $\Rightarrow$ (12) : This is clear since an ideal between P and P^2 has radical P and so is P-primary.

(5) $\Rightarrow$ (14) : Since R_P is a valuation ring and so ideals of R_P are totally ordered, the order-preserving correspondence between the P-primary ideals of R and PR_P-primary ideals of R_P implies that the set of P-primary ideals of R is totally ordered.

(14) $\Rightarrow$ (12) : Let $P \in Max(R)$. If $P = (0)$ then there is nothing to prove. So assume that $P \neq (0)$ and the set of P-primary ideals of R is totally ordered. Clearly P/P^2 is a vector space over R/P. The set of subspaces of P/P^2, whose elements are of the form I/P^2, for some ideal I of R such that $P^2 \subseteq I \subseteq P$. Since such ideals are P-primary and has a total order, then the set of subspaces of P/P^2 is totally ordered. Therefore P/P^2 is one dimensional. Hence, if I is an ideal of R such that $P^2 \subseteq I \subseteq P$, then we have either $\frac{I}{P^2} = \frac{P}{P^2}$ or $\frac{I}{P^2} = \frac{P^2}{P^2}$, and it follows that we have either $I = P$ or $I = P^2$. □

Theorem 2.67. *Let R be an integral domain. R is a Dedekind domain if and only if*

(I) for any $a \in R$ there exists only finite number of prime ideals P such that $a \in P$.

(II) for every nonzero $P \in Spec(R)$, R_P is a DVR.

Proof. Let R be a Dedekind domain. Let $a \in R$ be nonzero. Then by Proposition 2.65, we have (a) is contained by only finitely many prime ideals of R, hence the same is true for the element a, therefore (I) holds. By Theorem 2.66, R_P is a valuation ring for all $P \in Spec(R)$, and it is clear that R_P is Noetherian since R is. Hence (II) holds.

Now, let R be an integral domain which satisfies conditions (I) and (II). By Theorem 2.66, it suffices to show that R is Noetherian. To this aim, we shall show that every nonzero proper ideal of R is finitely generated. Let I be such an ideal and let $a \in I$ be nonzero. Let $P_1, \ldots, P_n$ be all prime ideals that contains a. Since for $P \in Spec(R)$, R_P is a DVR, then there exists $c_i \in R_{P_i}$ such that $IR_{P_i} = c_i R_{P_i}$. We may assume that $c_i \in I$. Now, consider the ideal $C = Ra + Rc_1 + \ldots + Rc_n \subseteq I$. If $P \in Spec(R)$ with

$I \nsubseteq P$, then $\frac{1}{a} \in R_P$, hence $R_P = CR_P \subseteq IR_P \subseteq R_P$, and so $CR_P = IR_P$. If $P = P_i$ for some $i = 1, \ldots, n$, then $c_i \in C$ implies that $IR_{P_i} = c_i R_{P_i} \subseteq CR_{P_i} \subseteq IR_{P_i}$, and so $CR_P = IR_P$. It follows that $C = I$, hence I is finitely generated. □

Before we continue our study about Dedekind domains on overrings and integral closures in finite extension fields, we shall give an example of a Dedekind domain.

Let K be an extension field of $\mathbb{Q}$, an element $\alpha \in K$ is called an algebraic integer, if α is integral over $\mathbb{Z}$. The integral closure of $\mathbb{Z}$ in K is called the ring of integers of K, and is denoted by $\mathscr{O}_K$. If K is an extension of finite degree over $\mathbb{Q}$, then K is called a number field. Now we shall show that $\mathscr{O}_K$ is a Dedekind domain if K is a number field. To this aim we shall prove that K is the field of fractions of $\mathscr{O}_K$, hence it is integrally closed. Moreover, we shall prove $\mathscr{O}_K$ is Noetherian and has the property that every prime ideal of $\mathscr{O}_K$ is maximal.

Theorem 2.68. *Let K be a number field of degree n over $\mathbb{Q}$. Then the following statements hold:*

1. *For every $\beta \in K$, there exists some nonzero $d \in \mathbb{Z}$ such that $d\beta \in \mathscr{O}_K$. In particular, K is the field of fractions of $\mathscr{O}_K$.*

2. *If $\beta_1, \ldots, \beta_n$ is a $\mathbb{Q}$-basis of K, then there exists an integer d such that $d\beta_1, \ldots, d\beta_n$ is a basis for a free $\mathbb{Z}$-submodule of $\mathscr{O}_K$ of rank n. Each basis of the $\mathbb{Z}$-module $\mathscr{O}_K$ is also a basis for K as a vector space over $\mathbb{Q}$.*

3. *The ring $\mathscr{O}_K$ is a Noetherian ring and is a free $\mathbb{Z}$-module of rank n.*

Proof. Let $\beta \in K$, and let $x^k + a_{k-1}x^{k-1} + \ldots + a_0$ be the minimal polynomial of β over K. If d is a common denominator for the coefficients, then multiplying through by d^k gives that

$$(d\beta)^k + da_{k-1}(d\beta)^{k-1} + \ldots + d^{k-1}a_1(d\beta) + d^k a_0 = 0,$$

and $d^k a_0, d^{k-1}a_1, \ldots, da_{k-1} \in \mathbb{Z}$. Hence $d\beta \in \mathscr{O}_K$. It follows from $\beta = \frac{d\beta}{d}$ that K is the field of fractions of $\mathscr{O}_K$. Hence the proof of (1) is complete.

If now $\beta_1, \ldots, \beta_n$ is a $\mathbb{Q}$-basis for K over $\mathbb{Q}$, then there is a nonzero integer d such that $d\beta_1, \ldots d\beta_n \in \mathscr{O}_K$. These elements are still linearly independent over $\mathbb{Q}$, so in particular, are linearly independent over $\mathbb{Z}$, hence generate a free submodule of $\mathscr{O}_K$ of rank n, which proves the first statement in (2).

Since $\mathscr{O}_K$ is a subring of the field K, it is a torsion-free $\mathbb{Z}$-module. If $\mathscr{O}_K$ were contained in some finitely generated $\mathbb{Z}$-module, it would follow that $\mathscr{O}_K$ is also finitely generated over $\mathbb{Z}$, hence it is a free $\mathbb{Z}$-module. If L is a normal closure of K, in some algebraic closure of $\mathbb{Q}$, then $\mathscr{O}_K \subseteq \mathscr{O}_L$ and so it suffices to see that $\mathscr{O}_L$ is contained in a finitely generated $\mathbb{Z}$-module. Since L is a finite extension of K, then by the transitivity of dimensionality, we have L is a finite extension of $\mathbb{Q}$. Let $\alpha_1, \ldots, \alpha_m$ be a $\mathbb{Q}$-basis for L over $\mathbb{Q}$. Multiplying by an integer d, if necessary, we may assume that each α_i is an algebraic integer, i.e., $\alpha_1, \ldots, \alpha_n \in \mathscr{O}_L$. For each fixed $\theta \neq 0$ in L, the map $T_\theta : L \to \mathbb{Q}$ defined by $T_\theta(\alpha) = Tr_{L/\mathbb{Q}}(\theta\alpha)$ for each $\alpha \in L$, is a $\mathbb{Q}$-linear transformation. $T_\theta \neq 0$ since we have $T_\theta(\theta^{-1}) = Tr_{L/\mathbb{Q}}(1) = m$. It follows that the map

$$\begin{array}{rcl} L & \to & Hom_{\mathbb{Q}}(L, \mathbb{Q}) \\ \theta & \mapsto & T_\theta \end{array}$$

is an injective homomorphism of vector spaces over $\mathbb{Q}$. Since both spaces have the same dimension over $\mathbb{Q}$, the map is an isomorphism; in other words, every linear functional on L is of the form T_θ for some $\theta \in L$. In particular, there are elements $\alpha'_1, \ldots, \alpha'_m \in L$ such that $\{T_{\alpha'_1}, \ldots, T_{\alpha'_m}\}$ give the dual basis of $\alpha_1, \ldots, \alpha_m$, i.e.

$$Tr_{L/\mathbb{Q}}(\alpha_i \alpha'_j) = \begin{cases} 1 & , \quad i = j \\ 0 & , \quad i \neq j \end{cases}$$

Since $\alpha'_1, \ldots, \alpha'_m$ are linearly independent, they give a basis for L over $\mathbb{Q}$. Hence every element β of $\mathscr{O}_L$ can be written as

$$\beta = a_1\alpha'_1 + \ldots + a_m\alpha'_m$$

with $a_1, \ldots, a_m \in \mathbb{Q}$. Multiplying by α_j and taking the trace shows that

$$Tr_{L/\mathbb{Q}}(\beta\alpha_j) = a_1 Tr_{L/\mathbb{Q}}(\alpha'_1\alpha_j) + \ldots + a_i Tr_{L/\mathbb{Q}}(\alpha'_i\alpha_j) + \ldots + a_m Tr_{L/\mathbb{Q}}(\alpha'_m\alpha_j) = a_j$$

But β and α_j are both elements of $\mathscr{O}_L$, so also $\beta\alpha_j \in \mathscr{O}_L$ and this implies that $a_j =$

$Tr_{L/\mathbb{Q}}(\beta\alpha_j) \in \mathbb{Z}$ since we know that the trace of $\beta\alpha_j$ is a coefficient of the minimal polynomial of $\beta\alpha_j$ over $\mathbb{Q}$, which is an element of $\mathbb{Z}[X]$, as noted above. It follows that

$$\mathscr{O}_L \subseteq \mathbb{Z}\alpha_1' + \ldots \mathbb{Z}\alpha_m'$$

so that $\mathscr{O}_L$ is contained in a finitely generated $\mathbb{Z}$-module, proving that $\mathscr{O}_K$ is a free $\mathbb{Z}$-module.

Since we can embed $\mathscr{O}_K \otimes \mathbb{Q}$ into K, in a natural way, we have $rank_{\mathbb{Z}}\mathscr{O}_K = dim(\mathscr{O}_K \otimes \mathbb{Q}) \leq dim_{\mathbb{Q}}K = n$. Because $\mathscr{O}_K$ also contains a free $\mathbb{Z}$-module of rank n, it follows that $\mathbb{Z}$-rank of $\mathscr{O}_K$ is precisely n. Note that any $\mathbb{Z}$-linear dependence relation among elements in $\mathscr{O}_K$ is a $\mathbb{Q}$-linear dependence relation in K, and multiplying a $\mathbb{Q}$-linear dependence relation of elements of $\mathscr{O}_K$ in K by a common denominator for the coefficients yields a $\mathbb{Z}$-linear dependence relation in $\mathscr{O}_K$. Thus the second statement in (2) follows.

Finally, any ideal I in $\mathscr{O}_K$ is a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module of rank n, so is a free $\mathbb{Z}$-module of rank n at most, and a set of $\mathbb{Z}$-module generators for I is also a set of $\mathscr{O}_K$-generators, hence every ideal of $\mathscr{O}_K$ can be generated by at most n elements, which implies that $\mathscr{O}_K$ is a Noetherian ring and completes the proof. □

If P is a nonzero prime ideal in the ring of integer $\mathscr{O}_K$ of a number field K, then $P \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. If $\alpha \in P$ is nonzero, then the constant term of the minimal polynomial for α over $\mathbb{Q}$ is then an element in $P \cap \mathbb{Z}$, which shows that $P \cap \mathbb{Z} \neq \emptyset$. Hence $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p. Since $p\mathbb{Z}$ is maximal, it follows from the Lying-over Theorem that nonzero prime ideals P in $\mathscr{O}_K$ are maximal.

Now, since we have shown that $\mathscr{O}_K$ is a Noetherian ring which is integrally closed and has the property that every nonzero prime ideal is maximal, then by Theorem 2.66, $\mathscr{O}_K$ is a Dedekind domain.

Theorem 2.69. *If T is an overring of a Dedekind domain R, then T is also a Dedekind domain.*

Proof. Let R be a Dedekind domain. If R is a field then our claim is clear since R itself is the only overring of R. So suppose that R is not a field. Let T be an overring of R, which is not the field of fractions of R. Let $M \in Max(T)$ be nonzero. Since R is a Prüfer domain, by Proposition 2.52, we have that $T_M = R_{M\cap R}$. Hence, we have

$M \cap R \neq (0)$ since $R_{M\cap R}$ is not a field. It follows that $M \cap R \in Max(R)$, and so $T_M = R_{M\cap R}$ is a DVR.

Let I be an ideal of T. If $M \in Max(T)$, then there exists a nonnegative integer $x(M)$ such that $AT_M = M^{x(M)}T_M$. We clearly have $x(M) > 0$ if and only if $I \subseteq M$, and since $I = (I \cap R)T$, then $x(M) > 0$ for only finitely many $M \in Max(M)$. By (2) of 2.42, we have that $I = \bigcap_{M\in Max(T)} (IT_M \cap T) = \bigcap_{M\in Max(T)} M^{x(M)}$. Since the maximal ideals of T are pairwise comaximal, then it follows that $I = \prod_{M\in Max(T)} M^{x(M)}$. Hence T is a Dedekind domain. □

Let R be a Dedekind domain with field of fractions K. We shall show that if R' is the integral closure of R in a finite extension field K' of K, then R' is also a Dedekind domain. Since K' can be viewed as a purely inseparable extension of some separable extension of K, then we shall prove that in both cases the integral closure of R is a Dedekind domain.

Theorem 2.70. *Let R, R', K and K' be as in the preceding paragraph. If K'/K is finite and separable, then R' is a Dedekind domain.*

Proof. If we show that R' is a Noetherian ring, then by Theorem 2.66, it is sufficient for us to show that R' is integrally closed and has Krull dimension one. But since R' is the integral closure of R, it is integrally closed by definition. R' has Krull dimension one is a direct result of the Lying-Over Theorem. Hence if we show that R' is Noetherian, then we are done.

Clearly, K' is the field of fractions of R'. If $a \in K'$, then $a^k + b_{k-1}a^{k-1} + \cdots + b_1a + b_0 = 0$ for some $b_0, \ldots, b_{k-1} \in K$. Since each b_i has the form $\frac{c_i}{s_i}$ and there are a finite number of b_i, we can write them in a common denominator. So let $b_i = \frac{c_i}{s}$, where $c_i, s \in R$ for $i = 1, \ldots, k-1$. If we multiply the equation with s^k, we obtain $(sa)^k + c_{k-1}(sa)^{k-1} + \ldots + c_1s^{k-2}(sk) + c_0s^{k-1} = 0$, thus $sa \in R'$ and $a = \frac{sa}{s}$.

If $u_1, \ldots, u_n$ is a basis of K'/K, then there exists $v_1, \ldots, v_n, s \in R'$ such that $u_i = \frac{v_i}{s}$ for $i = 1, \ldots n$. As in the preceding paragraph we may choose $s \in R$. So $v_1, \ldots, v_n$ are linearly independent over K and they form a basis of K'/K. Without loss of generality, we may assume that $u_1, \ldots, u_n \in R'$.

Let $M = \{a_1u_1 + \ldots + a_nu_n | a_i \in R, i = 1, \ldots n\}$. M is clearly an R-module an $M \subseteq R'$. Set $M^* = \{b \in K' | T_{K'/K}(ab) \in R$ for all $a \in M\}$, where $T_{K'/K}$ is the trace mapping of K'/K. Define R'^* like above. By the properties of trace mapping, we have that M^* and R'^* are both R-modules, and we have that $M \subseteq R' \subseteq R'^* \subseteq M^*$. After we show that M^* is finitely generated R-module, then R' and all ideals of R' becomes finitely generated since any submodule of a finitely generated module over a Noetherian ring is again finitely generated, so we can conclude that R' is a Noetherian ring.

Let $w_1, \dots, w_n \in K$. Consider the following equations in n unknowns:

$$\sum_{j=1}^{n} T_{K'/K}(u_i u_j) x_j = w_i, i = 1, \dots, n$$

Since K'/K is separable, $det\left[T_{K'/K}(u_i u_j)\right] \neq 0$. Thus this system has a unique solution $a_1, \dots, a_n \in K$. It follows that $a = a_1 u_1 + \dots + a_n u_n$ is the unique common solution of the equations

$$T_{K'/K}(u_i x) = w_i, i = 1, \dots, n$$

Thus, for a fixed j, the equations

$$T_{K'/K}(u_i x) = \delta_{ij}, i = 1, \dots, n$$

has a unique common solution u'_i.

Now suppose that $c_1 u'_1 + \dots + c_n u'_n = 0$, for some $c_1, \dots, c_n \in K$. For $i = 1, \dots, n$, we have

$$\begin{array}{rcl} 0 & = & T_{K'/K}\big(u_i(c_1 u'_1 + \dots + c_n u'_n)\big) \\ & = & \sum\limits_{j=1}^{n} c_j \left(T_{K'/K}(u_i u'_j)\right) \\ & = & c_i \end{array}$$

It follows that $u'_1, \dots, u'_n$ are linearly independent in K, hence they form a basis of K'/K.

Now we shall show $u'_1, \dots u'_n \in M^*$ and they generate M^* as an R-module.

Let $a \in M$, then there exists $a_1, \dots, a_n \in R$ such that $a = a_1 u_1 + \dots + a_n u_n$. Then

$$\begin{array}{rcl} T_{K'/K}(a u'_j) & = & T_{K'/K}\big((a_1 u_1 + \dots + a_n u_n) u'_j\big) \\ & = & \sum\limits_{i=1}^{n} a_i T_{K'/K}(u_i u'_j) \\ & = & a_j \in R \end{array}$$

hence $u'_j \in M^*$ for $j = 1, \ldots, n$.

Finally, if $b \in M^*$ with $b = b_1 u'_1 + \ldots + b_n u'_n$ where $b_1, \ldots, b_n \in K$, then for $i = 1, \ldots, n$, we have $b_i = T_{K'/K}\big(u_i(b_1 u'_1 + \ldots + b_n u'_n)\big) \in R$. So the proof is completed. □

Theorem 2.71. *Let R, R', K and K' be as in the paragraph above Theorem 2.70. If K'/K is finite and purely inseparable, then R' is a Dedekind domain.*

Proof. Since K'/K is finite and purely inseparable, then K has prime characteristic p, and there exists $e \in \mathbb{N}^+$ such that for all $a \in K'$, $a^{p^e} \in K$.

If f is a positive integer, then set $K_f = \Big\{a \in K' | a^{p^f} \in K\Big\}$. Then K_f is a subfield of K', and we have $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_e = K'$. Clearly $a \in K_f$ implies $a^p \in K_{f-1}$ for all $f = 1, \ldots, e$. So it suffices to show that R' is a Dedekind domain in the case that $a^p \in K$ for all $a \in K'$.

Let K' be such that $a^p \in K$ for all $a \in K'$. Then we have $R' = \{a \in K' | a^p \in R\}$:

Clearly if $a^p \in R$, a is a root of $X^p - a^p \in R[X]$, hence $a \in R'$. Conversely if $a \in R'$, then $a^p \in K$ by our assumption, and clearly $a^p \in R'$, hence $a^p \in K \cap R^{'} = R$.

Let C be an algebraic closure of K such that $K' \subseteq C$. Let $K'' = \{c \in C | c^p \in K\}$, and let R'' be the integral closure of R in K''. Then we have $R'' = \{c \in K'' | c^p \in R\}$. In this case we have $K' \subseteq K''$ and $R' \subseteq R''$.

The surjective mapping $\phi : K'' \to K$ given by $\phi(c) = c^p$ for all $c \in K''$ is an isomorphism, so its restriction to R'', maps R'' isomorphically onto R. Therefore R'' is a Dedekind domain, since R is.

If I be a nonzero ideal of R', then IR'' is invertible by Theorem 2.63. By Proposition 2.37, we have that $(IR'')[R'' : IR''] = R''$. Let $1 = a_1 b_1 + \ldots + a_k b_k$ where $a_1, \ldots, a_k \in I$ and $b_1, \ldots, b_k \in [R'' : IR'']$. Then we have $1 = a_1^p b_1^p + \ldots + a_k^p b_k^p$. For all $i = 1, \ldots, k$, we have $b_i^p \in K$ and $b_i^p a \in R'' \cap K' = R'$ for all $a \in I$. Hence $b_i^p \in [R' : I]$. Since we have $a_i^p \in I$, for all $i = 1, \ldots, k$, it follows that $I[R' : I] = R'$, so I is an invertible ideal of R'. Thus, by Theorem 2.63, R' is a Dedekind domain. □

What we have done in Theorem 2.70 and Theorem 2.71 can be combined to obtain

Theorem 2.72. *If R is a Dedekind domain with field of fractions K and R' is the integral closure of R in a finite field extension of K, then R' is a Dedekind domain.*

Let R be a Dedekind domain with the field of fractions K, let L be a finite algebraic extension of K, and let R' be the integral closure of R in L. Then by Theorem 2.72,

R' is also a Dedekind domain. Therefore if P is a maximal ideal of R, then PR' can be expressed as a product of maximal ideals of R', say $PR' = M_1^{e_1} \dots M_g^{e_g}$. Observe that $M_1, \dots, M_g$ are all maximal ideals of R' containing P and they lie over P. Our next aim is to expose some arithmetic relations between the exponents e_i and the dimensionality $[L : K]$. But before, we need to give the following sequence of preparatory results.

Lemma 2.73. *[13, Exercise 39.6] Let R be a principal ideal ring (i.e., a ring in which every ideal is principal) and let $x_1, \dots, x_n, x \in R$. If $(x_1, \dots, x_n) = (x)$, then there exist $y_1, \dots, y_n \in R$ such that $x_i = y_i x$ for each $i = 1, \dots, n$ and $(y_1, \dots, y_n) = R$.*

Proof. It is easy to see the lemma if we take R to be a factor of a PID. However, if R is a principal ideal ring, then it is a finite product of homomorphic images of PIDs (see Theorem 1 of [2]). □

Lemma 2.74. *Let R be a principal ideal ring, let $r_1, \dots, r_n \in R$ be such that $(r_1, \dots, r_n) = R$, and let $M = Rx_1 + \cdots + Rx_n$ be a finitely generated R–module generated by n elements $x_1, \dots, x_n$. Then there exists a generator set of M with cardinality n containing $x = r_1x_1 + \cdots + r_nx_n$.*

Proof. We use induction on n. If $n = 1$, then r_1 is a unit element of R, so r_1x_1 generates M. Now consider the case where $n = 2$. By assumption, there exist $s_1, s_2 \in R$ such that $s_1r_1 + s_2r_2 = 1$. Let $x = r_1x_1 + r_2x_2$ and $y = s_2x_1 - s_1x_2$. Then $x_1 = s_1x + r_2y$ and $x_2 = s_2x - r_1y$. Hence x and y generate M.

Now assume that the lemma is valid for $n = k$. Let $M = Rm_1 + \cdots + Rm_k + Rm_{k+1}$ and let $(r) = (r_1, \dots, r_k)$. Choose $s_1, \dots, s_k \in R$ such that $r_i = s_ir$ for each $i = 1, \dots, k$ and $(s_1, \dots, s_k) = R$ by Lemma 2.73. If $u = s_1m_1 + \cdots + s_km_k$, then the induction hypothesis implies that u is one of a set of k generators of $Rm_1 + \cdots + Rm_k$, say $Rm_1 + \cdots + Rm_k = Ru_1 + \cdots + Ru_{k-1} + Ru$. We have $x = ru + r_{k+1}m_{k+1}$, where $(r, r_{k+1}) = (r_1, \dots, r_k, r_{k+1}) = R$. Therefore the case where $n = 2$ shows that $Ru + Rm_{k+1} = Rx + Ry$ for some y. It follows that

$$\begin{aligned} Rm_1 + \cdots + Rm_k + Rm_{k+1} &= Ru_1 + \cdots + Ru_{k-1} + Ru + Rm_{k+1} \\ &= Ru_1 + \cdots + Ru_{k-1} + Rx + Ry. \end{aligned}$$

This completes the inductive step. □

Theorem 2.75. *Let R be a principal ideal ring and let $M = Rx_1 + \cdots + Rx_n$ be a finitely generated R–module. Then there exist $t_1, \ldots t_m \in M$, with $m \leq n$, such that $M = Rt_1 \oplus \cdots \oplus Rt_m$.*

Proof. We use induction on n. If $n = 1$, then there is nothing to prove. Let $n > 1$ and assume that the theorem is valid for $n = k$. Let $M = Rm_1 + \cdots + Rm_{k+1}$. We consider the set $\mathcal{S}$ of all ideals B_y, where y is an element of any generator set of M of cardinality $k+1$. Since R is Noetherian, $\mathcal{S}$ contains a maximal member, say $B_x = (t)$. Let $\{x_1, \ldots, x_k, x\}$ be a generator set of M. Assume that we have a relation

$$r_1x_1 + \cdots + r_kx_k + rx = 0,$$

where $rx \neq 0$. Let $(r, t) = (s)$. Then we have $B_x = (t) \subset (s)$. Write $s = ar + bt$ where $a, b \in R$. Then $sx = arx + btx = arx$ so that

$$0 = ar_1x_1 + \cdots + ar_kx_k + arx = s_1x_1 + \cdots + s_kx_k + sx,$$

where $s_i = ar_i$ for each $i = 1, \ldots, k$. Let $(u) = (s_1, \ldots, s_k, s)$ and choose, by Lemma 2.73, $v_1, \ldots, v_k, v \in R$ such that $s_i = v_iu$ for each $i = 1, \ldots, k$, $s = vu$, and $(v_1, \ldots, v_k, v) = R$. If $m = v_1x_1 + \cdots + v_kx_k + vx$, then m is one of a set of $k+1$ generators of M by Lemma 2.74. Moreover, $u \in B_m$ implies that $B_m \supseteq (u) \supseteq (s) \supset (t) = B_x$, which contradicts with the choice of B_x. Therefore, a relation

$$r_1x_1 + \cdots + r_kx_k + rx = 0$$

implies that $rx = 0$. Thus $M = (Rx_1 + \cdots + Rx_k) \oplus Rx$. The induction hypothesis implies that $Rx_1 + \cdots + Rx_k = Ry_1 \oplus \cdots \oplus Ry_r$ for some $r \leq k$. This completes the proof. □

Lemma 2.76. *Let V be a valuation ring with maximal ideal M and let K be its field of fractions. Assume that V is a subring of a domain J with field of fractions L. If A is an ideal of J lying over M, we consider J/A as a vector space over V/M. If $\{s_1, \ldots, s_n\}$ is a linearly dependent subset of J over K, then $\{s_1 + A, \ldots, s_n + A\}$ is* *linearly dependent over V/M. Therefore, if $[L : K]$ is finite, then*

$$[J/A : V/M] \leq [L : K].$$

Proof. Since $\{s_1, \ldots s_n\}$ is linearly dependent over K and since K is the field of fractions of V, there exist elements $a_1, \ldots a_n$ of V, not all zero, such that $\sum_{i=1}^{n} a_i s_i = 0$. The ideal of V generated by $\{a_1, \ldots a_n\}$ is principal and is generated by some a_i. If $b_j = a_j/a_i$ for each $j = 1, \ldots, n$, then $b_j \in V$ for each $j = 1, \ldots, n$, and $b_i = 1$. Passing to residue classes modulo A, we obtain $\sum_{i=1}^{n} \bar{b}_j \bar{s}_j = \bar{0}$, where $\bar{b}_i = \bar{1} \neq 0$. It follows that $\{\bar{s}_1, \ldots, \bar{s}_n\}$ is linearly dependent over V/M. □

Theorem 2.77. *Let V be a DVR with maximal ideal M and field of fractions K, let L be a finite extension of K of degree n, and let V' be the integral closure of V in L. Assume that $MV' = M_1^{e_1} \ldots M_g^{e_g}$ is the prime factorization of MV' in V', and that $[V'/M_i : V/M] = f_i$ for each $i = 1, \ldots, g$. Then*

$$[V'/MV' : V/M] = \sum_{i=1}^{g} e_i f_i \leq n;$$

where equality holds if and only if V' is a finitely generated V–module.

Proof. Let i be fixed between 1 and g. Since V' is a Dedekind domain by Theorem 2.72, there are no ideals of V' properly between M_i^n and M_i^{n+1}, and so M_i^n/M_i^{n+1} is one–dimensional as a vector space over V'/M_i for each $n > 0$. Since $M_i^{e_i}$ lies over M in V, one can think of $V'/M_i^{e_i}$ as a vector space over V/M. Then $V'/M_i^{e_i} \supset M_i/M_i^{e_i} \supset \ldots \supset M_i^{e_i}/M_i^{e_i} = 0$ is a decreasing chain of subspaces, and the corresponding factor spaces are V'/M_i, M_i/M_i^2, ... , $M_i^{e_i-1}/M_i^{e_i}$ (to within isomorphism). It follows that $[V'/M_i^{e_i} : V/M] = e_i f_i$. Since the maximal ideals M_i of V' are distinct, we have a ring isomorphism

$$V'/MV' \cong V'/M_1^{e_1} \oplus \cdots \oplus V'/M_g^{e_g},$$

where the isomorphism can also be taken as an isomorphism of vector spaces over V/M. It follows that $[V'/MV' : V/M] = \sum_{i=1}^{g} e_i f_i$. Since MV' lies over M in V, we conclude from Lemma 2.76 that $\sum_{i=1}^{g} e_i f_i \leq n$.

Now let V' be a finitely generated module over V. Let $V' = \sum_{i=1}^{t} V m_i$, where $m_1, \ldots, m_t \in V'$. Then by Theorem 2.75, there exist $x_1, \ldots, x_s \in V'$ such that $V' =$

$Vx_1 \oplus \cdots \oplus Vx_s$. If N is the set of nonzero elements of V, then we have

$$V'_N = V_N x_1 \oplus \cdots \oplus V_N x_s = Kx_1 \oplus \cdots \oplus Kx_s.$$

But by Corollary 2.31, we have $L = V'_N$. Therefore, $\{x_1, \ldots, x_s\}$ is a vector space basis for L over K, and $s = n$. The ideal M of V is principal, say $M = (m)$. Thus, $MV' = MVx_1 \oplus \cdots \oplus MVx_n$, and

$$V'/MV' \cong (Vx_1/MVx_1) \oplus \cdots \oplus (Vx_n/MVx_n).$$

Each Vx_i/MVx_i is one dimensional over V/M. Hence $[V'/MV' : V/M] = n = \sum_{i=1}^{g} e_i f_i$.

Conversely, assume that $[V'/MV' : V/M] = n$. Choose elements $y_1, \ldots, y_n \in V'$ such that $\{y_1 + MV', \ldots y_n + MV'\}$ is linearly independent over V/M. By Lemma 2.76, $\{y_1, \ldots, y_n\}$ is a vector space basis for L/K. Let $y \in V'$. Then there exist elements $a_1, \ldots, a_n$ of K such that $y = a_1 y_1 + \cdots + a_n y_n$. If some a_i does not lie in V, then we can choose a positive integer k such that $m^k a_i \in V$ for each $i = 1, \ldots, n$, and such that $m^k a_{i_0}$ is a unit of V for some i_0. Therefore,

$$m^k y = (m^k a_1) y_1 + \cdots + (m^k a_n) y_n,$$

and passing to residue classes modulo MV', we have

$$\bar{0} = \overline{m^k a_1}\,\overline{y_1} + \cdots + \overline{m^k a_n}\,\overline{y_n},$$

where each $\overline{m^k a_i}$ is in V/M and hence $\overline{m^k a_{i_0}} \neq 0$. But this relation contradicts the linear independence of $\{\overline{y}_1, \ldots, \overline{y}_n\}$ over V/M. Thus each a_i lies in V, and $y \in Vy_1 + \cdots + Vy_n$. We conclude that $V' = Vy_1 + \cdots + Vy_n$; that is, V' is a finite V–module. □

Corollary 2.78. *Let D be a Dedekind domain with field of fractions K, let M be a maximal ideal of D, let L be an extension field of K such that $[L : K] = n$, and let D' be the integral closure of D in L. Assume that $MD' = M_1^{e_1} \ldots M_g^{e_g}$ is the prime factorization of MD' in D', and that $[D'/M_i : D/M] = f_i$ for each $i = 1, \ldots, n$. Then $[D'/MD' : D/M] = \sum_{i=1}^{g} e_i f_i \leq n$, where equality holds if and only if D'_N is a finite*

D_M–module, where $N = D \setminus M$.

Proof. Note that D'_N is the integral closure of the DVR D_M in L, and

$$MD'_N = MD_M D'_N = (M_1 D'_N)^{e_1} \dots (M_g D'_N)^{e_g}$$

is the prime factorization of MD'_N in D'_N. Moreover, $D'_N/M_i D'_N \cong D'/M_i$ and $D_M/MD_M \cong D/M$. Therefore, the corollary follows from the preceding theorem. □

For any ring R, an automorphism of R is a ring isomorphism of R onto itself. The set of all automorphisms of R is a group with respect to composition of mappings.

Proposition 2.79. *[8, Exercise 13.36]Let R be a ring and $\mathscr{A}$ be the group of automorphisms of R. Let G be a finite subgroup of $\mathscr{A}$. Then $R^G = \{r \in R | \sigma(r) = r, \text{ for all } \sigma \in G\}$ is a subring of R and R is integral over R^G. Now let $P \in Spec(R^G)$ and set $\Gamma = \{Q \in Spec(R) | Q \cap R^G = P\}$. Then for $Q_1, Q_2 \in \Gamma$ there exists $\tau \in G$ such that $Q_1 = \tau(Q_2)$.*

Remark 2.80. In Corollary 2.78, if L/K is a Galois extension, the ideals M_i are conjugate under elements of the Galois group of L/K. To see this consider the subring $(D')^G$ of D', where G is the Galois group of L/K. (Note that G is, clearly, a subgroup of the automorphism group of D'.) Since all the M_i's lie over $M(D')^G$, by Proposition 2.79, they are conjugate under the elements of G. Therefore, in this case, we have

$$e_1 = e_2 = \cdots = e_g \quad \text{and} \quad f_1 = f_2 = \cdots = f_g,$$

and we obtain that

$$MD' = (M_1 M_2 \dots M_g)^e$$

for some positive integer e, and if $[D'/M_1 : D/M] = f$, then $[D'/MD' : D/M] = efg \leq n$, where equality holds if and only if D'_N is a finitely generated module over D_M, where $N = D \setminus M$.

3 ALMOST DEDEKIND DOMAINS

In this section we mostly use the works in [2], and along this section we do not refer to the works in there.

Definition 3.1. We call an integral domain D as almost Dedekind domain, if D_P is a Dedekind domain for each $P \in Max(D)$.

Let D be an almost Dedekind domain and let $P \in Max(D)$. Since a Dedekind domain is a Prüfer domain, then D_P is a local Prüfer domain and since every localization of a Prüfer domain is a valuation ring, it follows that D_P is a valuation ring. Clearly D_P is Noetherian since it is Dedekind. Hence D_P is a DVR.

Theorem 3.2. *Let D be an integral domain. Then D is an almost Dedekind domain if and only if primary ideals of D are prime powers and every prime ideal of D is maximal.*

Proof. Suppose that D is an almost Dedekind domain. we first show that $Spec(D) = Max(D)$. So let $P \in Spec(D)$ be nonzero. Then there exists $M \in Max(D)$ such that $P \subseteq M$. Clearly we have $PD_M \subseteq MD_M$. Since extension of a prime ideal is prime in D_M, and D_M is a Dedekind domain, then we must have $PD_M = MD_M$. It follows that $P = PD_M \cap D = MD_M \cap D = M$, since both M and P are prime. Now let Q be a P-primary ideal of D. Then we have QD_P is PD_P-primary. By the equivalence of conditions (1) and (13) in Theorem 2.66, we have $QD_P = P^n D_P$ for some nonnegative integer n. Therefore, since maximality of P in D implies P^n is P-primary, we have $Q = QD_P \cap D = P^n D_P \cap D = P^n$.

For the converse part of the proof, let D has the property that every prime ideal of D is maximal, and suppose that primary ideals of D are prime powers. Since $Spec(D) = Max(D)$, if $P \in Spec(D)$ is nonzero, then P is minimal. So PD_P is the unique nonzero prime ideal of D_P. If I is a proper ideal of D_P, then $\sqrt{I} = PD_P$ and since PD_P is maximal, then I is a PD_P-primary ideal of D_P. So $I \cap D$ is a P-primary ideal of D, and by our assumption $I \cap D = P^k$ for some $k \in \mathbb{N}$, and then we have, $I = (I \cap D)D_P = P^k D_P$. Therefore, every ideal of D_P is a prime power, which means has a prime factorization. Hence D_P is a Dedekind domain. Since P is an arbitrary prime ideal of D, then D is an almost Dedekind domain. □

Corollary 3.3. *Let D be an almost Dedekind domain and let I be a proper ideal of D, then $\bigcap\limits_{n\geq 1} I^n = (0)$.*

Proof. Let $P \in Spec(D)$ with $P \supseteq I$. For $n = 1, 2, \ldots$, we have $I^n \subseteq P^n \subseteq P^n D_P$. Since D_P is a Dedekind domain, then $\bigcap\limits_{n\geq 1} P^n D_P = (0)$ which implies that $\bigcap\limits_{n\geq 1} I^n = (0)$. □

Corollary 3.4. *Let D be an almost Dedekind domain and let $P \in Spec(R)$. Then there is no ideal I of D such that $P^2 \subset I \subset P$.*

Proof. Suppose that there exists an ideal I of D such that $P^2 \subset I \subset P$. By taking extension to D_P, we have $P^2 D_P \subset ID_P \subset PD_P$. But since D_P is a Dedekind domain, this is a contradiction by Theorem 2.66 and so such an ideal doesn't exist. □

Corollary 3.5. *Let D be an almost Dedekind domain and let $P \in Spec(D)$. Then the set of P-primary ideals are totally ordered under inclusion.*

Proof. Let $P \in Spec(D)$ and let $\{Q_i\}_{i\in I}$ be the set of P-primary ideals of D. Clearly $\{Q_i D_P\}_{i\in i}$ is the set of PD_P-primary ideals of D_P. Since D_P is a Dedekind domain, then $\{Q_i D_P\}_{i\in I}$ is totally ordered under inclusion. It follows that $\{Q_i\}_{i\in I} = \{Q_i D_P \cap D\}_{i\in I}$ is also totally ordered under inclusion. □

Lemma 3.6. *An almost Dedekind domain is integrally closed.*

Proof. Let D be an almost Dedekind domain, by (1) of Lemma 2.42, we have $D = \bigcap\limits_{P\in Max(D)} D_P$. Since every localization of D is a Dedekind domain, they are all integrally closed by Theorem 2.66 so the same is true for their intersection D. □

Lemma 3.7. *Let D be an almost Dedekind domain. Let A, B and C be ideals of D. Then the following statements hold:*

(1) $A \cap (B + C) = (A \cap B) + (A \cap C)$

(2) $(A : B \cap C) = (A : B) + (A : C)$

Proof. Let $P \in Spec(D)$. Since D_P is a Dedekind domain, for any ideals A, B, C of D, we clearly have

$$\big(A\cap(B+C)\big)R_P = AR_P\cap(BR_P+CR_P) = (AR_P\cap BR_P)+(AR_P\cap CR_P) = \big((A\cap B)+(A\cap C)\big)R_P$$

Since this equality holds for every $P \in Spec(D)$, then we have the first equality.

For the second one, we need to show that for any $P \in Spec(D)$, we have

$$(A : B \cap C)R_P = \big((A : B) + (A : C)\big)R_P$$

The desired equality holds for any ideals AR_P, BR_P, CR_P of R_P since D_P is a Dedekind domain. Since we know that $(A : B)R_P = (AR_P : BR_P)$, where A and B are ideals of D, the above equation also holds. Since P is arbitrary, then the desired equality holds for ideals of D, so the proof is complete. □

Now let D be an almost Dedekind domain and I be a nonzero ideal of D. Let $\{M_\lambda\}_{\lambda\in\Lambda}$ be the set of maximal ideals of D. Then for $I \not\subseteq M_\lambda$ we have $ID_{M_\lambda} = D_{M_\lambda}$, so $ID_{M_\lambda} \cap D = D = (M_\lambda)^0$. But for $I \subseteq M_\lambda$, we have that ID_{M_λ} is $M_\lambda D_{M_\lambda}$-primary. Since D_{M_λ} is a Dedekind domain, it follows from Theorem 2.66 that we have $ID_{M_\lambda} = M_\lambda^k D_{M_\lambda}$ for some nonnegative integer k, hence $ID_{M_\lambda} \cap D = M_\lambda^k$.

If $\mathscr{I}$ is the collection of nonzero ideals of D, then for each $\lambda \in \Lambda$, we set a function $f_\lambda : \mathscr{I} \to \mathbb{Z}$ such that, for $I \in \mathscr{I}$, $f_\lambda(I) = k$ if $ID_{M_\lambda} \cap D = M_\lambda^k$. By (2) of Lemma 2.42, it follows that

$$I = \bigcap_{\lambda\in\Lambda} M_\lambda^{f_\lambda(I)} = \bigcap_{\lambda\in\Lambda} (ID_{M_\lambda} \cap D) \tag{3}$$

for each $I \in \mathscr{I}$.

Furthermore, if we set $D^* = D \setminus \{0\}$, then for each $\lambda \in \Lambda$ we define $f_\lambda : D^* \to \mathbb{Z}$ by $V_\lambda(x) = f_\lambda\big((x)\big)$ for all $x \in D^*$. We shall introduce more details about the functions V_λ and f_λ. Before that, we shall give a small lemma.

Lemma 3.8. *Discrete valuation rings (DVR) are maximal subrings of their field of fractions.*

Proof. Let V be a DVR with field of fractions K, and let π be an irreducible element of V. Let V' be a subring of K such that $V \subseteq V' \subseteq K$. Let $r \in V' \setminus V$, then there is a unit $u \in V$ such that $r = u\pi^{-n}$ with $n > 0$. Then, $\pi^{-1} = u^{-1}\pi^{n-1}r \in V'$, and it follows that all powers of π, both positive and negative, are in V'. Since every element of K equals a unit in V times a power of π, we conclude that if $V \neq V'$, then $V' = K$. □

Theorem 3.9. *Let D be an almost Dedekind domain. Let $\{M_\lambda\}_{\lambda\in\Lambda}$ be the set of maximal ideals of D, $\mathscr{I}$ be the family of nonzero ideals of D. Let $D^*, I, f_\lambda, V_\lambda$ be as* *they defined above. Then the following statements holds:*

(i) $I \subseteq M_\lambda^k, I \nsubseteq M_\lambda^{k+1}$ for some integer k. Furthermore, $k = f_\lambda(I)$.

(ii) $V_\lambda(xy) = V_\lambda(x) + V_\lambda(y)$ and $V_\lambda(x+y) \geq min\{V_\lambda(x), V_\lambda(y)\}$ for all $x, y \in D^*$. So V_λ determines a valuation s_λ of the field of fractions K of D. Further, the valuation ring of s_λ is D_{M_λ}.

(iii) For $m_\lambda \in M_\lambda \setminus M_\lambda^2$ and for $0 \neq \xi \in K$, there exist $u, v \in D \setminus M_\lambda$ such that

$$\xi = \frac{u m_\lambda^{s_\lambda(\xi)}}{v}.$$

Proof. The existence of an integer k is obtained by Corollary 3.3. If t is such that $I \subseteq M_\lambda^t$ but $I \nsubseteq M_\lambda^{t+1}$, then $ID_{M_\lambda} = M_\lambda^r D_{M_\lambda}$ for all $r \geq t$. If $a \in I \setminus M_\lambda^{t+1}$, then since $M_\lambda^{t+1} = M_\lambda^{t+1} D_{M_\lambda} \cap D$ we have $a \in ID_{M_\lambda} \setminus M_\lambda^{t+1} D_{M_\lambda}$. Hence we have $ID_{M_\lambda} = M_\lambda^t D_{M_\lambda}$ and it follows that $t = f_\lambda(a)$ as claimed.

Let $x, y \in D^*$ and $\lambda \in \Lambda$. We first show that $V_\lambda(xy) = V_\lambda(x) + V_\lambda(y)$.

Set $V_\lambda(x) = a, V_\lambda(y) = b$ so $(x)D_{M_\lambda} \cap D = M_\lambda^a, (y)D_{M_\lambda} \cap D = M_\lambda^b$. Since $(xy) = (x)(y)$ we have $(xy)D_{M_\lambda} = (x)D_{M_\lambda}(y)D_{M_\lambda}$. Since we know $(x)_\lambda D_{M_\lambda} = \big((x)D_{M_\lambda} \cap D\big)D_{M_\lambda} = (x)D_{M_\lambda}$ and $(y)_\lambda D_{M_\lambda} = \big((y)D_{M_\lambda} \cap D\big)D_{M_\lambda} = (y)D_{M_\lambda}$, we have

$$(xy)D_{M_\lambda} = (x)D_{M_\lambda}(y)D_{M_\lambda} = \big((x)D_{M_\lambda} \cap D\big)D_{M_\lambda}\big((y)D_{M_\lambda} \cap D\big)D_{M_\lambda} = M_\lambda^a D_{M_\lambda} M_\lambda^b D_{M_\lambda} = M_\lambda^{a+b} D_{M_\lambda}$$

and so $(xy)D_{M_\lambda} \cap D = M_\lambda^{a+b}$ which implies

$$V_\lambda(xy) = a + b = V_\lambda(a) + V_\lambda(b)$$

Now we'll show that $V_\lambda(x+y) \geq min\{V_\lambda(x), V_\lambda(y)\}$:

By Equation (3) we have $(x) \subseteq M_\lambda^{f_\lambda(x)}$ and $(y) \subseteq M_\lambda^{f_\lambda(y)}$. Since we know $(x+y) \subseteq (x) + (y)$ then we have

$$(x+y) \subseteq (x) + (y) \subseteq M_\lambda^{f_\lambda(x)} + M_\lambda^{f_\lambda(y)} = M_\lambda^{min\{f_\lambda(x), f_\lambda(y)\}}$$

hence $f_\lambda(x+y) \geq min\{f_\lambda(x), f_\lambda(y)\}$.

Thus V_λ determines a valuation s_λ of the field of fractions K of D.

From (i), the valuation ring of s_λ contains D_{M_λ}, since for $x \in D_{M_\lambda}$ we have $s_\lambda(x) \geq 0 \Leftrightarrow (x) \subseteq D_{M_\lambda} = \left(M_\lambda D_{M_\lambda}\right)^0$. Because D_{M_λ} is a maximal subring of K by Lemma 3.8, and so D_{M_λ} is the valuation ring of s_λ.

We have $s_\lambda(m_\lambda) = 1$ by (i), hence if $y = \frac{\xi}{m_{\lambda^{s_\lambda(\xi)}}}$, then we have $s_\lambda(y) = 0$. It follows that y is a unit of D_{M_λ}. Set $y = \frac{u}{v}$ where $u \in D$ and $v \in D \setminus M_\lambda$. Since $s_\lambda(v) = 0$, we have $s_\lambda(u) = 0$, which gives that $u \notin M_\lambda$. □

Theorem 3.10. *Let D be an almost Dedekind domain. Then D is a Dedekind domain if and only if for each nonzero proper ideal I of D there exist only finitely many maximal ideals which contain I. In particular, an almost Dedekind domain with only a finite number of maximal ideals is a PID.*

Proof. First, let D be a Dedekind domain. Let I be a nonzero proper ideal of D. Then there exists $P_1, \ldots, P_n \in Max(D)$ such that $I = P_1 \ldots P_n$. We clearly have $I \subseteq P_i$ for $i = 1, \ldots, n$. If $P_0 \in Spec(D)$ is such that $I \subseteq P_0$, then since $P_1 \ldots P_n \subseteq P_0$, we have $P_i \subseteq P_0$ for some $i = 1, \ldots, n$. Since P_i is maximal, then $P_i = P_0$. Hence I is contained in finitely many maximal ideals of D.

Now let D be an almost Dedekind domain such that every ideal I of D contained in finitely many maximal ideals. Our aim is to show that D is a Dedekind domain.

Let I be an ideal of D and suppose that I is contained in $M_1, \ldots, M_k$ but not any other maximal ideal of D. It suffices to show that D is Noetherian. Let $a \in I$ be nonzero. Since D_{M_i} is a DVR for $i = 1, \ldots$,k then ID_{M_i} is generated by an element, since we can see I as a subset of ID_{M_i}, then we can choose the generator of ID_{M_i} as an element a_i of I, in fact $\frac{a_i}{1}$ generates ID_{M_i}. Then our aim is to show that $I = (a, a_1, \ldots, a_k)$.

We have $I = \bigcap\limits_{M \in Max(D)} ID_M \cap D = \bigcap\limits_{i=1}^{k} ID_{M_i} \cap D$. For the ideals $I_i = a_i D$, with $i = 1, \ldots, a_k$ and $I_0 = aD + a_1 D + \ldots + a_k D$ we have $ID_{M_i} = I_i D_{M_i} \subseteq I_0 D_{M_i}$. Since $I_0 = \bigcap\limits_{i=1}^{k} I_0 D_{M_i} \cap D \supseteq \bigcap\limits_{i=1}^{k} ID_{M_i} \cap D = I$, then I is finitely generated. Hence D is a Dedekind domain. □

Now we shall give some properties of overrings of an almost Dedekind domain.

Theorem 3.11. *Let D be an almost Dedekind domain with field of fractions K such that $D \neq K$. Let D' be an overring of D, and let $\Delta = \{P \in Spec(D) | PD' \neq D'\}$. Then the following statements hold:*

(a) If $M \in Max(D')$ and if $P = M \cap D$, then $D_P = D'_M$ and $M = PD_P \cap D'$. As a result, D' is an almost Dedekind domain.

(b) In the case that D is a Dedekind domain, we have D' is also a Dedekind domain.

(c) For $P \in Spec(D)$ with $P \subset D$, $P \in \Delta$ if and only if $D_P \supseteq D'$. Further, $D' = \bigcap\limits_{P \in \Delta} D_P$.

(d) Let I' be an ideal of D'. If $I = I' \cap D$, then we have $I' = ID'$.

(e) $\{PD'\}_{P\in\Delta}$ is the set of prime ideals of D'.

Proof. If $M \in Max(D')$, then clearly $P = M \cap D$ is a maximal ideal of D. If we set $S = R \setminus P$, then we have $D_P = S^{-1}D \subseteq S^{-1}D' \subseteq D'_M \subset K$. The only part we need to prove is $S^{-1}D' \subseteq D'_M$:

Let $\frac{x}{y} \in S^{-1}D'$ where $x \in D', y \in S$. Since $y \in D \setminus P$, then we have $y \notin M$. Since $D \subseteq D'$, then we clearly have $y \in D' \setminus M$, hence $\frac{x}{y} \in D'_M$.

By Lemma 3.8 we have that D_P is the maximal subring of K, so we have $D_P = D'_M$. Hence D'_M is a DVR and $MD'_M = PD_P$ is its maximal ideal. It follows that D' is almost Dedekind and we have $M = MD'_M \cap D' = PD_P \cap D'$.

Now suppose D is a Dedekind domain. By (a), D' is an almost Dedekind domain. By Theorem 3.10, it suffices to show that for an arbitrary nonzero ideal I' of D'. There are only finitely many maximal ideals of D' which contain I'. Now let I' be a nonzero proper ideal of D', let $I = I' \cap D$. Since D is a Dedekind domain, then $I = I' \cap D$ is contained in only finitely many maximal ideals of D, say $P_1, \ldots, P_n$. By (a) we have that $P_1D_{P_1} \cap D', \ldots, P_nD_{P_n} \cap D'$ are all the prime ideals of D' which contain I'. Hence D' is a Dedekind domain.

Let $P \in Spec(D)$ with $P \subset D$. If $D_P \supseteq D'$, then clearly $PD' \subseteq PD_P \subseteq D_P$. If we have $PD' = D'$, then $P = PD_P \cap D \supseteq PD' \cap D = D' \cap D = D$ which is a contradiction, hence we have $PD' \subset D'$. Now suppose that $P \neq (0)$ and that $PD' \subset D'$. Let $M \in Spec(D')$ be such that $PD' \subseteq M$. It follows that $P \subseteq PD' \cap D \subseteq M \cap D \subset D$. Since D is an almost Dedekind domain, then P is a maximal ideal, so we have $P = M \cap D$, thus by (a), we have $D_P = D'_M \supseteq D'$. Now if $Max(D') = \{M_\lambda\}_{\lambda\in\Lambda}$, then $D' = \bigcap\limits_{\lambda\in\Lambda} D'_{M_\lambda}$ by Lemma 2.42. By (a) and the first part of (c), we have for each $\lambda \in \Lambda$, $D'_{M_\lambda} = D_{(M_\lambda \cap D)}$ and $M_\lambda \cap D \in \Delta$. Thus the desired equality holds.

Let I' be an ideal of D'. If $I' = (0)$ or $I' = D'$, then the claim of (d) is clear. So suppose that $(0) \subset I' \subset D'$. We first prove that if $P = M \cap D$ for some $M \in Max(D')$, then $P^k = M^k \cap D$ for all $k \geq 1$:

$$\begin{aligned} P^k &= P^k D_P \cap D \\ &= M^k D'_M \cap D \\ &= M^k D'_M \cap (D' \cap D) \\ &= (M^k D'_M \cap D') \cap D \\ &= M^k \cap D \end{aligned}$$

Let $I = I' \cap D$, then $ID' = (I' \cap D)D' \subseteq I'$ and hence $f_\lambda(ID') \geq f_\lambda(I')$ for each $\lambda \in \Lambda$. Since for each nonzero ideal B of D' we have $B = \bigcap\limits_{\lambda \in \Lambda} M_\lambda^{f_\lambda(B)}$, it suffices to prove $f_\lambda(ID') = f_\lambda(I)$ for all $\lambda \in \Lambda$ in order to prove that $ID' = I'$.

By (a), it suffices to show that, if k is such that $I' \subseteq M_\lambda^k$ but $I' \nsubseteq M_\lambda^{k+1}$, then $ID' \nsubseteq M_\lambda^{k+1}$. Set $P_\lambda = M_\lambda \cap D$. Since we have $M_\lambda^{k+1} \cap D = P_\lambda^{k+1}$, then it suffices to show that $I \nsubseteq P_\lambda^{k+1}$. This follows essentially from (iii) of Theorem 3.9.

We clearly have $P_\lambda^2 = M_\lambda^2 \cap D \subset M_\lambda \cap D = P_\lambda$, so that if $m_\lambda \in P_\lambda \setminus P_\lambda^2$, then $m_\lambda \in M_\lambda \setminus M_\lambda^2$. If $\xi \in I' \setminus M_\lambda^{k+1}$, then $s_\lambda(\xi) = k$ and $\xi = \frac{um_\lambda^k}{v}$ for some $u, v \in D \setminus P_\lambda$. So we have $v\xi = um_\lambda^k \in I \setminus P_\lambda^{k+1}$, for otherwise, $s_\lambda(um_\lambda^k) \geq k+1$ which gives a contradiction. Hence $I \nsubseteq P_\lambda^{k+1}$, and the result follows.

By (d), if $P' \in Spec(D')$ with $P' \subset D'$, then $P' = PD'$ for some $P \in \Delta$. If $P \in \Delta$, then by (c), we have $D_P \supseteq D'$, so we have $PD_P \cap D' \in Spec(D')$. By (d), $PD_P \cap D' = \big((PD_P \cap D') \cap D\big)D' = PD'$. It follows that $PD' \in Spec(D')$ for $P \in \Delta$. □

The following corollary is another result about almost Dedekind domains, which is analogue of a theorem about Dedekind domains which we stated in Theorem 2.72.

Corollary 3.12. *Let D be an almost Dedekind domain with field of fractions K. Let L be a finite extension field of K and let D' be the integral closure of D in L. Then D' is almost Dedekind.*

Proof. Let $M \in Spec(D')$ be nonzero and proper, then $P = M \cap D \in Spec(D)$ is also nonzero and proper. If we set $S = D \setminus P$, then $D_P = S^{-1}D$. D' is integral over D implies that $S^{-1}D'$ is integral over $S^{-1}D = D_P$. Since D' is integrally closed in L, $S^{-1}D'$ is integrally closed in $S^{-1}L = L$. Hence $S^{-1}D'$ is the integral closure of the DVR $S^{-1}D$ in L. Consequently, $S^{-1}D'$ is a Dedekind domain, and it follows that $D'_M = (S^{-1}D')_{S^{-1}M}$ is a DVR. As a result, D' is an almost Dedekind domain. □

4 CANCELLATION LAW FOR IDEALS IN A COMMUTATIVE RING

Detailed information about this section can be found in [4], [10] and [3] which are our main references.

Let R be a commutative ring. If R satisfies the property that $AB = AC$ for arbitrary ideals A, B, C of R with $AB \neq (0)$ implies that $B = C$, then we say the restricted cancellation law (RCL) holds in R. RCL is a weakened form of the cancellation law (CL), which is $AB = AC$ for arbitrary ideals A, B, C of R with $A \neq (0)$ implies that $B = C$. A ring in which CL holds need to be an integral domain. In an integral domain, RCL is equivalent to CL.

In this section we aim to answer that if CL holds in an integral domain R, is R need to be a Dedekind domain. We shall show that if RCL holds in a ring R, then R is either an integral domain, R is a special primary ring, or R is a primary ring in which the product of any two non-units is zero. Furthermore, if RCL holds in a ring R, then R is either of these latter three types.

Let D be an integral domain, then CL holds for D if and only if for any $P \in Spec(D)$ with $P \subset D$, the localization D_P is a rank one discrete valuation ring.

Then, we consider a ring S which has a collection $\mathscr{S}$ of nonzero proper ideals of S such that every nonzero proper ideal of S is uniquely written as a product of finitely many elements of $\mathscr{S}$. RCL holds in such an S. If S is not an integral domain, the converse is also true.

4.1 Restricted Cancellation Law (RCL)

In this part, we shall investigate the structure of a ring D in which RCL holds. The case that D is also a domain is our main concern.

Lemma 4.1. *Let D be a ring which RCL holds, then CL holds in D if and only if D is an integral domain.*

Proof. Let D be an integral domain. Let A, B, C be ideals of D such that A is nonzero and $AB = AC$. In the case $AB = AC = (0)$, since $A \neq (0)$ and D is a domain, it follows that $B = C = (0)$. If $AB = AC \neq (0)$, then by RCL, we have $B = C$. Hence CL holds for D.

Now suppose that D is not an integral domain and let $x \in D$ be a nonzero zero-divisor of D. Then we have $ann(x) \neq (0)$. Since we know $(x).ann(x) = 0.ann(x)$ and $x \neq 0$, then CL doesn't hold for D. □

Lemma 4.2. *Let A, B, C be ideals of a ring D in which RCL holds. If $AB \subseteq AC \neq (0)$, then $B \subseteq C$ holds.*

Proof. If $AB \subseteq AC$, then we clearly have $AB + AC = A(B + C) = AC \neq (0)$, hence by RCL, we have $B + C = C$, and this implies $B \subseteq C$ as claimed. □

Theorem 4.3. *Let RCL holds for a ring D, then either D is a one-dimensional integral domain, or D is a special primary ring, or D is a primary ring with maximal ideal M in which $M^2 = (0)$. Conversely, RCL holds for a special primary ring or for a primary ring with maximal ideal M such that $M^2 = (0)$.*

Proof. Suppose that $P \in Spec(D)$ with $P \subset D$. Let $x \in D \setminus P$. Then

$$\begin{aligned}[P + (x)]^4 &= P^4 + P^3(x) + P^2(x^2) + P(x^3) + (x^4) \\ &= [P + (x)]^2[P^2 + (x^2)]\end{aligned}$$

$x^4 \notin P$ implies that $[P + (x)]^4 \supseteq (x)^4 \neq 0$ so that we have $[P + (x)]^2 = P^2 + (x^2)$ since $[P + (x)]^2 \neq 0$. It follows that we have

$$(x)P \subseteq P^2 + (x^2) \tag{4}$$

For $p \in P$, there exist $q \in P^2$ and $r \in D$ such that $rx^2 = px - q$. It follows from the facts $rx^2 \in P$ and $x^2 \notin P$ that, $r \in P$. Since $px = rx^2 + q$, then we have $(x)P \subseteq P^2 + P(x^2) = P[P + (x^2)]$. Now there are two possible cases we need to consider:

1. For arbitrary $P \in Spec(D)$ with $P \subset D$ and for all $x \in D \setminus P$, we have

$$P[P + (x^2)] \neq (0)$$

2. For some $P \in Spec(D)$ with $P \subset D$ and for some $x \in R \setminus P$, we have

$$P[P + (x^2)] = (0)$$

In the first case, D is not an integral domain since the inequality doesn't hold for (0), and so it is not a prime ideal of D. If M is a prime ideal of D and if $x \in D \setminus M$, since RCL holds for D, and since we know $M(x) \subseteq M[M+(x^2)]$, and $M[M+(x^2)] \neq (0)$, it follows that $(x) \subseteq M+(x^2)$. This implies that $x - rx^2 = x(1-rx) \in M$ for some $r \in D$. Hence $1 - rx \in M$, and thus $M + (x) = D$, which means M is maximal. Since M is an arbitrary prime ideal of D, then M is also minimal. Since by localizing at M we have $MR_M = \sqrt{0R_M}$, then for $m \in M$, we have $\left(\frac{m}{1}\right)^k = 0$ for some integer k, then there exists an element $t \in D \setminus M$ such that $m^k t = 0$. It follows that $(m^{2k}) = (m^k)(m^k, t)$. If $(m^{2k}) \neq (0)$, then by RCL, we have $(m^k) = (m^k, t)$ which is impossible since $t \notin M$. Hence $m^{2k} = 0$, so every element of M is nilpotent. Since the set of nilpotent elements of D is an ideal of D, then D is a primary ring with maximal ideal M.

Now if $M^2 = (0)$ then we are done, so suppose $M^2 \neq (0)$. We have $M \supset M^2 \supset M^3 \supset \ldots$ for otherwise RCL implies that $M = D$, a contradiction. If I is the ideal generated by $M \setminus M^2$, then $M = M^2 + I$. It follows that $M^2 = M^4 + M^2 I + I^2 = M^2[M^2 + I] + I^2 = M^3 + I^2$. Since we have $M^2 \neq M^3$, then $I^2 \neq (0)$. Hence there exist $x, y \in I$ such that $xy \neq 0$. If $x^k = 0$, then

$$\begin{aligned}
[M^2 + (x)]^k &= \sum_{i=0}^{k} M^{2i}(x)^{k-i} = \sum_{i=1}^{k} M^{2i}(x)^{k-i} \\
&= M^2 \sum_{i=0}^{k-1} M^{2i}(x)^{k-1-i} = M^2[M^2 + (x)]^{k-1}
\end{aligned}$$

Since $M^2 \neq M^2 + (x)$, we have $[M^2 + (x)]^k = (0)$ and since $\left(M^2\right)^k \subseteq [M^2 + (x)]^k = (0)$, we have that $M^{2k} \subseteq (x)$. We shall show that $M \subseteq (x)$ by induction, and this implies $M = (x)$. After this, we shall show that $\{(x^i) | i = 1, \ldots, k\}$ is the complete set of proper ideals of D. Hence D is a special primary ring.

To this end, suppose that $M^i \subseteq (x)$, where $i \geq 2$. Set $I = \left(M^i : (x)\right)$. We clearly have $M^i = I(x)$. Since $x \notin M^i$ and $I \subset D$, then we have $I \subseteq M$. Hence $M^i \subseteq M(x)$. Since $y \in M \setminus M^2$ is such that $xy \neq 0$, then $M(x) \neq (0)$. It follows that by Lemma 4.2, we have $M^{i-1} \subseteq (x)$, hence we have $M = (x)$ by induction.

Now let I be a nonzero proper ideal of D, our aim is to show that I is principal and generated by a power of x. Since $x^k = 0 \in I$, then there exists an integer j such that $x^j \in I$ but $x^{j-1} \notin I$. If we show $I = (x^j)$, we are done. Since $(x^j) \subseteq I$, suppose by the way of contradiction that the inclusion is strict and let $a \in I \setminus (x^j)$. Since M

is the unique maximal ideal of D, then we have $a \in M$. It follows that $a = rx^i$ for some $r \in D \setminus M$ and an integer i. Clearly r is a unit of D and so $r^{-1}a = x^i \in I$. Since $a = rx^i$ and $a \notin (x^j)$, then we must have $i < j$. Since $x^i \in I$ and $x^{j-1} \notin I$, then $i > j - 1$. Since such an integer i doesn't exist, then we must have $I = (x^j)$. Since arbitrary proper ideal of D is generated by a power of x, then the set of all the proper ideals is $\{(x), (x^2), \ldots, (x^k) = (0)\}$. This proves that the claim of the theorem holds in the first case.

For the second case, since $P^2 \subseteq P[P + (x^2)] = (0)$, then there exists a prime ideal P of D such that $P^2 = (0)$. So P is the unique minimal prime ideal of D. For otherwise, if Q is a minimal prime ideal of D, then $(0) = P^2 \subseteq Q$ implies that $P \subseteq Q$, and so we have $P = Q$ by the minimality of Q.

If P is maximal, then R is a primary ring and P is its unique maximal ideal such that $P^2 = (0)$.

If P is non-maximal, and if M is a prime ideal distinct from P, since P is unique minimal ideal of D, then $M \supset P$. If $t \in D \setminus M$, then we have $M[M + (t^2)] \neq (0)$, since for otherwise, $M^2 = (0) \subseteq P$ gives a contradiction. It follows as in the first case that M is maximal.

Now if b is a non-unit of D, then for some maximal ideal N of D, we have that $b \in N$ and $N \supset P$. Thus $P + (b) \subseteq N$. If $P^2 + P(b^2) \neq (0)$, then P becomes maximal as in the proof of the first case, which is not possible. Hence $P^2 + P(b^2) = (0)$. By Equation 4, we have that $(b)P \subseteq P^2 + P(b^2)$ so $(b)P = P^2 + P(b^2) = (0)$. If $b \notin P$, then $(b^2) = (b)[(b) + P]$ and $(b^2) \neq (0)$ so $(b) = (b) + P$ which implies $P \subseteq (b)$. It follows that for some ideal C of D, $P = (b)C$. Since P is a prime ideal of D and $b \notin P$, $P = C$, and so $P = (b)P = (0)$. As a result, D is a one-dimensional integral domain.

For the last part of the proof, let S be a special primary ring. Let A, B, C be ideals of S such that $AB = AC$ and $AB \neq (0)$. Let M be the unique maximal ideal of S. Then we have $AB = M^k$, $A = M^a$ for some $k, a \in \mathbb{N}$. Suppose $B \neq C$, then there exist $b, c \in \mathbb{N}$ such that $B = M^b$ and $C = M^c$. So $M^a M^b = AB = M^k = AC = M^a M^c$ so $M^{a+b} = M^{a+c} = M^k$. Since distinct powers of M are distinct if they are nonzero, we have $b = c$ and thus $B = C$ which is a contradiction, hence $B = C$ and RCL holds in S.

Now let T be a primary ring with maximal ideal M such that $M^2 = (0)$. If we have

$AB = AC \neq (0)$, we have either $A = R$ or $B = C = R$, since for otherwise, if A and B are both proper ideals, then $A, B \subseteq M$ and so $AB \subseteq M^2 = (0)$. In the case that $A = R$, we have $B = AB = AC = C$ so in both cases RCL holds. $\square$

Let R be an integral domain. We say that the finite cancellation law (FCL) holds in R precisely when for arbitrary ideals A, B, C of R with $A \neq (0)$ is finitely generated, $AB = AC$ implies $B = C$.

Theorem 4.4. *Let R be an integral domain. If FCL holds for R, then R is integrally closed.*

Proof. Let K be the field of fractions of R and let $x \in K$ be integral over R. Then the fractional ideal F of R generated by 1 and all positive powers of x is finitely generated an idempotent. There exists a nonzero element $d \in R$ such that $dF = A$ is a finitely generated ideal of R. So we have

$$A^2 = (d^2)F^2 = (d^2)F = (d)dF = (d)A$$

Since A is finitely generated and FCL holds in R, then we have $A = (d)$. By FCL, $(d)F = A$ and $(d) = A$ together implies that $F = R$, hence $x \in F = R$, which gives that R is integrally closed. $\square$

Theorem 4.5. *Let D be an integral domain. Then CL holds in D if and only if D is an almost Dedekind domain.*

Proof. Suppose first that CL holds in D. Let $P \in Spec(R)$ with $P \subset D$. Since CL implies FCL and by Theorem 2.40, we have that D is a Prüfer domain, hence D_P is a valuation ring. By Theorem 4.3, since the only domain case is being a one dimensional integral domain, then D_P has rank-one. Now $P \subset D$ so that $P^2 \subset PD = P$ since CL holds in D. Since P^2 has radical P, a maximal ideal of D, then P^2 is a P-primary ideal of D. It follows that $P^2D_P = (PD_P)^2 \subset PD_P$. If $m \in PD_P \setminus P^2D_P$ then we have $mD_P = PD_P$. Hence D_P is a rank-one DVR, so D is an almost Dedekind domain.

The converse part is straightforward since $AB = AC$ with $A \neq (0)$ implies that for all $P \in Max(R)$, we have $AR_P \neq (0)$ and $(AR_P)(BR_P) = (AR_P)(CR_P)$. Since R_P is a Dedekind domain, we have $BR_P = CR_P$ by Theorem 2.66. It follows that $B = \bigcap_{P \in Max(R)} (BR_P \cap R) = \bigcap_{P \in Max(R)} (CR_P \cap R) = C$. $\square$

4.2 Rings With Unique Ideal Factorization

In this section, S will be a ring in which there exists a collection $\mathscr{S}$ of nonzero proper ideals of S, such that every nonzero proper ideal of S can be uniquely written as a product of elements of $\mathscr{S}$. RCL holds in such a ring is a direct result of the uniqueness of the representation. Clearly, if $AB = AC$ with $AB \neq (0)$, then AB and A can be expressed as a product of the elements of $\mathscr{S}$. The factor which are appear in the factorization of AB but does not appear in the factorization of A gives the expression of B. In the same way we can obtain C, and this implies that $B = C$.

In the view of Theorem 4.3, we obtain the following theorem:

Theorem 4.6. *If S has proper divisors of zero, then one of the following statements hold:*

1. *S is a special primary ring and $\mathscr{S}$ is the set of maximal ideals of S.*
2. *S is a primary ring with maximal ideal M such that $M^2 = (0)$, and $\mathscr{S}$ is the set of all nonzero proper ideals of S.*

Proof. Since S has proper zero-divisors, then S is not an integral domain. Then by Theorem 4.3 and its proof, we have either S is a special primary ring or a primary ring with maximal ideal M such that $M^2 = (0)$.

If S is a special primary ring with maximal ideal M, then by definition every ideal of S is a power of M, so we have $\mathscr{S} = \{M\}$.

If S is a primary ring with maximal ideal M such that $M^2 = (0)$, then for a nonzero ideal I of S, we must have $I \in \mathscr{S}$, for otherwise , if $I = AB$ for some $A, B \in \mathscr{S}$, then $I = AB \subseteq M^2 = (0)$, which is a contradiction. Hence we have $\mathscr{S}$ is the set of all nonzero proper ideals of S. □

Theorem 4.7. *Let S be an integral domain. Then S is Dedekind and $\mathscr{S}$ is the set of all nonzero prime ideals of S.*

Proof. If S is a field, both conclusion follows. Suppose that S is not a field. By Theorem 4.3, we have that S is one-dimensional. If every nonzero ideal of S is invertible, then we conclude that S is a Dedekind domain by Theorem 2.63.

To this aim, we first show that an invertible ideal $S' \in \mathscr{S}$ is prime. If $xy \in S'$, then since S' is invertible, $(x)(y) = (xy) = S'I$ for some ideal I of S. From the uniqueness of representation, S' must be a factor either of (x) or of (y). For otherwise, this implies that S' has a factorization other that itself, hence it contradicts with $S' \in \mathscr{S}$. Since S' is a factor of either (x) or (y), then we have $x \in S'$ or $y \in S'$. So S' is a prime ideal.

Let $P \in Spec(R)$ and let $p \in P$. Let $(p) = S_1 \dots S_k$ for some $S_1, \dots, S_k \in \mathscr{S}$. Clearly, $S_i \in \mathscr{S}$ is invertible for each $i = 1, \dots, k$, hence maximal by previous paragraph. We have $(p) = S_1 \dots S_k \subseteq P$, so we must have $S_{i_0} \subseteq P$ for some $i_0 = 1, \dots, k$. It follows by the maximality of S_{i_0} that $S_{i_0} = P$, hence arbitrary prime ideal of S is invertible and maximal. Therefore, we have that S is Dedekind, and every element of $\mathscr{S}$ is invertible, therefore prime. Since we show that $\mathscr{S}$ consists of all nonzero prime ideals of S, then the proof is complete. □

4.3 Factoring With Radical Ideals and SP-Domains

Let R be a ring and let I be an ideal of R. If there exist finitely many radical ideals $J_1, \dots, J_k$ of R such that $I = J_1 \dots J_k$, then we say that I has radical factorization or I is an SP-ideal. If every ideal of R is an SP-ideal, then R is called as an SP-ring. In the latter case if R is an integral domain, then R is called an SP-domain. Our aim in this section is to show SP-domains are almost Dedekind domains.

Before showing an SP-domain is an almost Dedekind domain, we give a characterization of SP-domains in the class of almost Dedekind domains. To this aim we introduce some required notations and facts:

1. If A and B are finitely generated ideals of a Prüfer domain R, then we have $A \cap B$ is finitely generated.

   Proof: Since A and B are finitely generated ideals of a Prüfer domain, then they are invertible and so AB is invertible, so by Theorem 2.40, we have that $AB = (A \cap B)(A + B)$ and this implies $A \cap B$ is invertible, hence finitely generated.

2. If R is a Prüfer domain and $P \in Spec(R)$, then $\bigcap\limits_{i \geq 1} P^i$ is a prime ideal of R by Proposition 2.45.

3. A maximal ideal M of a domain R is critical if and only if for each finite subset $A \subseteq M$, there exists $N \in Max(R)$, need not to be distinct from M, such that

$A \subseteq N^2$. Another characterization for $M \in Max(R)$ to be critical can be given as, M is critical if and only if every finitely generated ideal I of R such that $I \subseteq M$ is contained in the square of some maximal ideal.

4. Let R be an almost Dedekind domain and let $a \in R$ be nonzero. Define the mapping $\gamma_a : Max(R) \to \mathbb{Z}$ by $\gamma_a(M) = v_M(a)$, where v_M is the rank one discrete valuation corresponding to the valuation ring R_M. This mapping is upper semi-continuous if for all $n \in \mathbb{Z}$, the set $\gamma_a^{-1}([n, \infty))$ is closed.

Theorem 4.8. *Let R be an almost Dedekind domain. Then the following statements are equivalent:*

1. *R is an SP-domain, i.e. R has radical factorization.*
2. *R has no critical maximal ideals.*
3. *If $A \subset R$ is a finitely generated ideal, then $\sqrt{A}$ is also finitely generated.*
4. *Each proper principal ideal of R is an SP-ideal.*
5. *For each nonzero $a \in R$, the function $\gamma_a : Max(R) \to \mathbb{Z}$ is upper semi-continuous and has finite image.*
6. *For each proper ideal A of R, there exist radical ideals $J_1 \subseteq J_2 \subseteq \ldots \subseteq J_n$ such that $A = J_1 J_2 \ldots J_n$.*
7. *Every proper nonzero ideal A of R can be represented uniquely as a product $A = J_1 J_2 \ldots J_n$ where $J_i, i = 1, \ldots n$ are radical ideals such that $J_1 \subseteq J_2 \subseteq \ldots \subseteq J_n$.*

Proof.

(1) $\Rightarrow$ (2) : Let $M \in Max(R)$ and let, $a \in R$ be nonzero. By (1), we have $(a) = J_1 \ldots J_n$ for some radical ideals $J_1, \ldots, J_n$ of R. Since $(a) = J_1 \ldots J_n \subseteq M$, then for some $i_0 \in \{1, \ldots, n\}$, we have $J_{i_0} \subseteq M$. J_{i_0} is invertible since (a) is, hence J_{i_0} is finitely generated. If there exists $N \in Max(R)$ with $J_{i_0} \subseteq N$, then since R_N is one-dimensional, we have $J_{i_0} R_N = N R_N$, so $J_i \nsubseteq N^2$. Hence, we found a finitely generated ideal of R that contained in M but not in the square of any maximal ideals. Hence M is not critical. Since $M \in Max(R)$ is arbitrary, then (2) holds.

(2) $\Rightarrow$ (3) : To prove this part, we first show that for $M \in Max(R)$ and a finitely generated ideal $A \subseteq M$, we have $A \subseteq J \subseteq M$ for some finitely generated radical ideal J of R. By our assumption, there exists a finitely generated ideal B such that $B \subseteq M$ and $B \not\subseteq N^2$ for arbitrary $N \in Max(R)$. Set $J = A + B$. Clearly $A \subseteq J \subseteq M$ and since A and B are both finitely generated, so is J. If $N \in Max(R)$ such that $J \subseteq N$, then $JR_N \subseteq NR_N$. By assumption, $BR_N \not\subseteq N^2R_N$, for otherwise $B \subseteq BR_N \cap R \subseteq N^2R_N \cap R = N^2$. Hence $BR_N = NR_N$. Since we have $B \subseteq J \subseteq N$, we must have $JR_N = NR_N$. Since the last equality holds for arbitrary maximal ideal of R, then $J = \bigcap\limits_{N \in Var(J)} (JR_N \cap R) = \bigcap\limits_{N \in Var(J)} (NR_N \cap R) = \bigcap\limits_{N \in Var(J)} N = \sqrt{J}$. Thus J is a radical ideal.

Now let A be a proper ideal of R which is finitely generated and set $J = \sqrt{A}$. Our aim is to show that J is finitely generated. If $A = (0)$, then there is nothing to prove, so assume that A is nonzero. If we show that $[R : J]R_M = [R_M : JR_M]$ for all $M \in Max(R)$, then since JR_M is principal for all $M \in Max(R)$, we have that $[R : J]J = R$, which proves J is invertible, hence finitely generated.

Let K be the field of fractions of R, let $M \in Max(R)$ and let $q \in K$ be such that $qJ \subseteq R_M$. Our aim is to find $b \in R \setminus M$ such that $bqJ \subseteq R$. As we have showed before, there is a finitely generated ideal J_1 of R with $A \subseteq J_1 \subseteq M$. Since A and J_1 are both invertible, there exists a finitely generated ideal B_1 of R such that $A = J_1B_1$. If $B_1 \subseteq M$, then by repeating this argument, we have an ideal B_2 of R such that $B_1 = J_2B_2$. This repetition must stop after finitely many steps and we may have $A = J_1 \ldots J_nB_n$, for some $B_n \not\subseteq M$ and $J_1, \ldots, J_n$ radical ideals. For otherwise, we have $A \subseteq J_1 \ldots J_k$ for all $k \geq 1$ and since $J_i \subseteq M$, it follows that $A \subseteq \bigcap\limits_{n \geq 1} M^n = (0)$, which is a contradiction.

Now $J = \sqrt{A} = \sqrt{J_1 \ldots J_nB_n} = J_1 \cap \ldots \cap J_n \cap \sqrt{B_n}$, so since $qJR_M \subseteq R_M$ and $\sqrt{B_n} \not\subseteq M$, we have $q(J_1 \cap \ldots \cap J_n) \subseteq R_M$. Since $J_1 \cap \ldots \cap J_n$ is the intersection of finitely generated ideals, then it is also finitely generated. It follows that there exists $b \in R \setminus M$ such that $bq(J_1 \cap \ldots \cap J_n) \subseteq R$. Hence $bqJ \subseteq R$, as claimed. It follows that $q \in [R : J]R_M$, and thus $[R_M : J] = [R : J]R_M$ for all $M \in Max(R)$ such that $M \supseteq A$. If $xJ \subseteq R_M$, then clearly $xJR_M \subseteq R_M$. If $yJR_M \subseteq R_M$, then since $J \subseteq JR_M$, we have $yJ \subseteq yJR_M \subseteq R_M$, hence $[R_M : J] = [R_M : JR_M]$ for all $M \in Max(R)$. So the result follows.

(3) $\Rightarrow$ (4) :Let A be a proper principal ideal of R. If $A = (0)$, then the claim is true. So suppose that $A \neq (0)$. If we set $J_1 = \sqrt{A}$, since both J_1 and A are invertible, then there exists an invertible ideal B_1 such that $A = J_1B_1$. If $B_1 = R$, then we are done. So suppose that $B_1 \neq R$. By setting $J_2 = \sqrt{B_1}$, we have that $A = J_1J_2B_2$ for some finitely generated ideal B_2 of R. Since J_1 is finitely generated and $J_1 = \sqrt{A}$, then $J_1^n \subseteq A \subseteq J_2$ for some $n \geq 1$. Since J_2 is a radical ideal of R, it follows that $J_1 \subseteq J_2$. To continue in this manner, either we have that A is an SP-ideal, or we obtain an infinite chain of radical ideals $J_1 \subseteq J_2 \subseteq \dots$ such that $A \subseteq J_1 \dots J_k$ for each $k \geq 1$. In the latter case, if $M \in Max(R)$ with $\bigcup\limits_{k\geq 1} J_k \subseteq M$, then $A \subseteq \bigcap\limits_{n\geq 1} M^n = (0)$, which contradicts the fact that A is nonzero. Therefore, A must have a radical factorization.

(4) $\Rightarrow$ (5) : Let $\alpha \in R$ be nonzero. We first show that γ_α has finite image. By our assumption, $\alpha R = J_1^{e_1} \dots J_k^{e_k}$, for some $k, e_1, \dots, e_k \in \mathbb{N}$ and for some $J_1, \dots, J_k$. Let $M \in Max(R)$ such that $\alpha \in M$. Set $X = \big\{i \in \{1, \dots, k\} | J_i \subseteq M\big\}$. For each $i \in X$, since J_i is a radical ideal and R_M is a Dedekind domain, hence a DVR, we have that $J_iR_M = MR_M$. We clearly have $J_iR_M = R_M$ for $i \notin X$. So we have $J_1^{e_1} \dots J_k^{e_k}R_M = \prod\limits_{i\in X} M^{e_i}R_M$, and thus $\gamma_\alpha(M) = v_M(\alpha) = \sum\limits_{i\in X} e_i$. It follows that for $M \in Max(R)$, either $\gamma_\alpha(M) = 0$, or it equals to a sum of some of e_i's. Hence, γ_α has finite image.

Now, let n be a positive integer. Set $V = \gamma_\alpha^{-1}\big([n, \infty)\big) = \{M \in Max(R) | \alpha \in M^n\}$. Our aim is to show that V is closed in $Max(R)$. Let $M \in V$, and let X defined as above. Then, as noted above, $\sum\limits_{i\in X} e_i = \gamma_\alpha(M) \geq n$. Thus the set $F = \big\{X \subseteq \{1, \dots, k\} | \sum\limits_{i\in X} e_i \geq n\big\}$ is not empty. Set $A = \bigcap\limits_{X\in F} \big(\sum\limits_{i\in X} J_i\big)$. If we show $V = Var(A) = \{M \in Max(R) | M \supseteq A\}$, then we conclude that V is closed in $Max(R)$.

If $M \in V$, as we have established above, there exists $X \subset \{1, \dots, k\}$ such that $\sum\limits_{i\in X} e_i \geq n$ and $M \supseteq \sum\limits_{i\in X} J_i \supseteq A$. Thus, $V \subseteq \{M \in Max(R) | M \supseteq A\}$.

If $M \in Max(R)$ with $M \supseteq A$, then since F has at most 2^n elements, A is a finite intersection. It follows that we have $\sum\limits_{i\in X} J_i \subseteq M$, for some $X \in F$. For otherwise, if there exist $\alpha_X \in \big(\sum\limits_{i\in X} J_i\big) \setminus M$ for all $X \in F$, then $\prod\limits_{X\in F} \alpha_X \in \bigcap\limits_{X\in F} \big(\sum\limits_{i\in X} J_i\big) \setminus M = A \setminus M$, which is a contradiction. Thus, $J_i \subseteq M$ for all $i \in X$, therefore $\alpha R = J_1^{e_1} \dots J_k^{e_k} \subseteq \prod\limits_{i\in X} J_i^{e_i} \subseteq \prod\limits_{i\in X} M^{e_i} \subseteq M^n$. Hence $\alpha \in M^n$, and this implies $M \in V$.

Since we have $V = Var(A)$, it is closed in $Max(R)$ by definition.

(5) $\Rightarrow$ (6) : Let A be a nonzero proper ideal of R. Let $M \in Max(R)$. Set $v_M(A)$

be the smallest element in $\{v_M(a)|a \in A\}$. Set $X = \{v_M(A)|M \in Max(R), A \subseteq M\}$. We first show that X is finite. If $\alpha \in A$ is nonzero, then by our assumption γ_α has finite image, so $\{v_M(\alpha)|M \in Max(R)\}$ is finite. Since we have $v_M(A) \leq v_M(a)$ for all $M \in Max(R)$, then X is finite, say $X = \{f_1, \ldots, f_n\}$ be such that $0 < f_1 < f_2 < \ldots < f_n$. Set $V_i = \{M \in Max(R)|A \subseteq M^{f_i}\}$ for $i = 1, \ldots, n$. Our claim is that each V_i is a closed subset of $Max(R)$. For each i, we have the following:

$$\begin{aligned} V_i &= \{M \in Max(R)|\forall a \in A, a \in M^{f_i}\} \\ &= \big\{M \in Max(R)|\forall a \in A, M \in \gamma_\alpha^{-1}\big([f_i, \infty)\big)\big\} \\ &= \bigcap_{a \in A} \gamma_\alpha^{-1}\big([f_i, \infty)\big) \end{aligned}$$

By our assumption, we have $\gamma_\alpha^{-1}\big([f_i, \infty)\big)$ is a closed subset of $Max(R)$, so V_i is closed since it is the intersection of closed subsets.

For each i, set $J_i = \bigcap\limits_{M \in V_i} M$. Since $V_n \subseteq V_{n-1} \subseteq \ldots \subseteq V_1$, we have $A \subseteq J_1 \subseteq \ldots \subseteq J_n$. Now set $B = J_1^{f_1} J_2^{f_2 - f_1} \ldots J_n^{f_n - f_{n-1}}$. Our aim is to show that $A = B$, and we shall show this by proving that $AR_M = BR_M$ for all $M \in Max(R)$.

Let $M \in Max(R)$ be such that $B \subseteq M$. Let $k \leq n$ be the largest integer such that $J_k \subseteq M$. Then $BR_M = J_1^{f_1} J_2^{f_2 - f_1} \ldots J_k^{f_k - f_{k-1}} R_M = M^{f_k} R_M$.

For $M \in Max(R)$, in the case that $J_i \subseteq M$, we have $J_i = \bigcap\limits_{M \in V_i} M \subseteq M$, so there exists $M_0 \in V_i$ such that $M_0 \subseteq M$. Then $M_0 \in Max(R)$ implies that $M \in V_i$. Conversely, $M \in V_i$ clearly implies $M \supseteq \bigcap\limits_{M \in V_i} M = J_i$. As a result, we have for $M \in Max(R)$, $M \supseteq J_i$ is equivalent to $M \in V_i$. By this equivalence, V_k is the smallest member of the chain $V_n \subseteq \ldots \subseteq V_1$ such that $M \in V_k$. Since $v_M(A) \in \{f_1, \ldots, f_n\}$, it follows that $v_M(A) = f_k$. Hence $AR_M = M^{f_k} R_M = BR_M$.

Now suppose that $M \in Max(R)$ is such that $A \subseteq M$. Then $v_M(A) = f_k$ for some $k \leq n$, so $AR_M = M^{f_k} R_M$. Thus $M \in V_k$ but $M \notin V_m$ for $k < m \leq n$. Each V_i closed implies that $J_1 \subseteq \ldots \subseteq J_k \subseteq M$ but $J_m \nsubseteq M$ for $k < m \leq n$. Hence we have $BR_M = J_1^{f_1} \ldots J_k^{f_k - f_{k-1}} R_M = M^{f_k} R_M = AR_M$.

If $M \in Max(R)$ is such that $A, B \nsubseteq M$, then clearly $AR_M = R_M = BR_M$.

Since the equality holds for arbitrary maximal ideal, we can conclude that $A = B$.

(6) ⇒ (7) : Let A be a nonzero proper ideal of R. Let $J_1 \ldots J_n = A = K_1 \ldots K_m$ be such that $J_1 \subseteq \ldots \subseteq J_n$ and $K_1 \subseteq \ldots \subseteq K_m$, where $J_1, \ldots, J_n, K_1, \ldots, K_m$ are all

radical ideals of R. By taking radicals, we have that $\sqrt{A} = \sqrt{J_1 \dots J_n} = \sqrt{J_1} \cap \dots \cap \sqrt{J_n} = \sqrt{J_1} = J_1$. Similarly we can obtain $\sqrt{A} = K_1$. Since R is an almost Dedekind domain, we have CL holds in R, hence $J_1 = K_1$ implies that $J_2 \dots J_n = K_2 \dots K_m$. The proof now can be completed by induction.

By definition we clearly have (7) implies (1), hence the proof is complete.

□

An integral domain R is said to have property (α) if every primary ideal of R is a power of its radical. If R has property (α), it is easy to see that for any $P \in Spec(R)$, R_P and R/P both have property (α). Now we shall give some properties of domains having property (α).

Lemma 4.9. *Let R be a local integral domain with property (α). Let $M \in Max(R)$. If M is minimal over an ideal of the form $tR + P$ for some non-maximal prime ideal P and for some $t \in M \backslash P$, then $\bar{M} = \bigcap_{n \geq 1} M^n$ is a prime ideal of R such that $P \subseteq \bar{M} \subset M$.*

Proof. If M is minimal over the ideal $I_1 = tR + P$, then I_1 is M-primary. If we set $I_k = t^k R + P$ for $k \geq 1$, then the same conclusion holds. For each $k \in \mathbb{N}$, we have $I_k \supset I_{k+1}$ since $t^k \in I_k \setminus I_{k+1}$. Suppose otherwise, then $t^k = t^{k+1} r + p$ for some $r \in R$ and $p \in P$, then we have $t^k(1 - tr) = p$. Since $t \in M \backslash P$ and $p \in P$, we have $1 - tr \in P$. This implies $1 \in tR + P = I_1$, which is impossible. By property (α), for each k, there exists an integer $m_k \geq 1$, such that $I_k = M^{m_k}$. Since $M^{m_k} = I_k \supset I_{k+1} = M^{m_{k+1}}$, then each power of M is distinct. Hence as a result of property (α), $M^n = bR + M^m$ for each $b \in M^n \setminus M^{n+1}$ and all positive integers $m > n$.

Now let $\bar{M} = \bigcap_{n \geq 1} M^n = \bigcap_{k \geq 1} M^{m_k} \supseteq P$. Since all powers of M are distinct, then $M \supset \bar{M}$. For $x, y \in M \setminus \bar{M}$, there are integers m, n such that $x \in M^n \setminus M^{n+1}$ and $y \in M^m \backslash M^{m+1}$. This implies $M^n = xR + M^{n+1}$ and $M^m = yR + M^{m+1}$. By multiplying these equalities, we have $M^{m+n} = xyR + xM^{m+1} + yM^{n+1} + M^{m+n+2}$. Since every power of M is distinct, then $M^{m+n} \supset M^{m+n+1}$. Since $xM^{m+1} + yM^{n+1} + M^{m+n+2} \subseteq M^{m+n+1}$, then we must have $xy \notin M^{m+n+1}$, hence $\bar{M}$ is a prime ideal of R such that $P \subseteq \bar{M} \subset M$. □

Lemma 4.10. *Let R be an integral domain with property (α). Let $P \in Spec(R)$. If $Q \in Spec(R)$ is minimal over an ideal of the form $tR + P$ for some $t \in R \setminus P$, then $\bar{Q} = \bigcap_{n \geq 1} Q^n$ is a prime ideal of R such that $P \subseteq \bar{Q} \subset Q$.*

Proof. Since R_Q has property (α) with QR_Q is minimal over tR_Q+PR_Q, by Lemma 4.9, we have $\bigcap\limits_{n\geq 1} Q^nR_Q$ is a prime ideal of R_Q that contains PR_Q and is properly contained in QR_Q. For each integer $k \geq 1$, set $I_k = t^kR+P$. By localizing I_k at Q and then taking contraction back to R, we obtain Q-primary ideals which are powers of Q by property (α). Set m_k be the integer such that $Q^{m_k} = I_kR_Q \cap R$. Now Lemma 4.9 implies that $\bigcap\limits_{k\geq 1} I_kR_Q$ is a prime ideal which contains PR_Q and is properly contained in QR_Q. Since QR_Q is minimal over I_1, then by Lemma 4.9 $\bigcap\limits_{n\geq 1} Q^nR_Q$ is a prime ideal. It follows that $\bigcap\limits_{k\geq 1} I_kR_Q$ is a prime ideal since $\bigcap\limits_{n\in\mathbb{N}} Q^nR_Q = \bigcap\limits_{k\in\mathbb{N}} Q^{m_k}R_Q = \bigcap\limits_{k\in\mathbb{N}} \big[(I_kR_Q\cap R)R_Q\big] = \bigcap\limits_{k\in\mathbb{N}} I_kR_Q$. Hence there exists $Q_0 \in Spec(R)$ with $Q_0 \subset Q$ such that $\bigcap\limits_{k\in\mathbb{N}} I_kR_Q = Q_0R_Q$ with $P \subseteq Q_0 \subseteq Q^n$ for each $n \geq 1$. It follows that $Q_0 = \bigcap\limits_{n\geq 1} Q^n \subset Q$. □

Lemma 4.11. *Let R be an integral domain with property (α). Let $N \in Spec(R)$ with $N \neq (0)$. Then $\bar{N} = \bigcap\limits_{n\geq 1} N^n$ is a prime ideal of R such that for all $P \in Spec(R)$ with $P \subset N$ we have $P \subseteq \bar{N}$. Moreover, in the case that $N \neq N^2$, we have NR_N is principal.*

Proof. Let $N \in Spec(R)$ with $N \neq (0)$. Let $P \in Spec(R)$ with $P \subset N$ and let $t \in N \setminus P$. Then there exists $Q \in Spec(R)$ with $Q \subseteq N$ such that Q is minimal over $tR+P$. By Lemma 4.10, $\bigcap\limits_{n\geq 1} Q^n$ is a prime ideal that contains P and properly contained in Q. It is clear that $\bigcap\limits_{n\geq 1} N^n$ contains $\bigcap\limits_{n\geq 1} Q^n$. Therefore $\bigcap\limits_{n\geq 1} N^n$ contains every prime ideal P of R such that $P \subset N$. In the case that $N = N^2$, we have $\bigcap\limits_{n\geq 1} N^n = N$ and we are done. Hence, in the rest of the proof, we assume that $N \neq N^2$.

Set $\bar{Q} = \bigcap\limits_{n\geq 1} N^n$ and let $r \in N \setminus N^2$. Since $\bar{Q}$ contains each prime ideal that is properly contained in N and $r \notin \bar{Q}$, N is a minimal prime over the ideal rR. It follows that NR_N is the radical of rR_N. Thus rR_N is NR_N-primary. By property (α), the only possibility is to have $NR_N = rR_N$. So the last statement of the lemma has proved.

Now it remains to show that $\bar{Q}$ is a prime ideal of R. Since $NR_N = rR_N$ is principal, each power of NR_N is distinct. It follows that

$$\bar{Q} \subseteq (\bigcap_{n\geq 1} N^nR_N) \cap R \subset N$$

Since NR_N is a minimal prime over rR_N, choosing $P = 0$ in Lemma 4.9, we have that $\bigcap\limits_{n\geq 1} N^nR_N$ is a prime ideal of R_N. Hence $\big(\bigcap\limits_{n\geq 1} N^nR_N\big) \cap R$ is a prime ideal of R

that is properly contained in N, so it is contained in $\bar{Q}$. Therefore

$$\bar{Q} = \big(\bigcap_{n\geq 1} N^n R_N\big) \cap R \in Spec(R)$$

$\square$

Lemma 4.12 (Nakayama's Lemma). *Let R be a ring and let M be a finitely generated R-module. Let I be an ideal such that $I \subseteq Jac(R)$, i.e. the intersection of all maximal ideals of R. If $M = IM$, then $M = 0$.*

Lemma 4.13. *Let R be a local integral domain with maximal ideal M. Let M be the radical of a finitely generated ideal. Then M is principal if and only if $\{M^n | n \geq 1\}$ is the complete set of M-primary ideals. Furthermore, in the case that M is principal, we have $\bigcap_{n\geq 1} M^n$ is a non-maximal prime ideal that contains each non-maximal prime ideal of R.*

Proof. Let $M = (a)$ be principal. Our aim is to show that the only M-primary ideals are powers of P and powers of M are distinct. Let Q be an M-primary ideal. Since $\sqrt{Q} = M$, then we have $a^n \in Q$ but $a^{n-1} \notin Q$ for some positive integer n. Our claim is that $Q = (a^n)$. Suppose there exists $x \in Q \setminus (a^n)$. Then $x = a^{n-k}r$ for some $r \in R \setminus M$ and $k > 0$. Since r is a unit in R, then $(a^{n-k}) = (x) \subseteq Q$, but this contradicts our assumption that $a^{n-1} \notin Q$. So we must have $Q = (a^n)$. Moreover, by Nakayama's Lemma, we have $M^i \neq M^j$ for $i \neq j$ since M is finitely generated.

Conversely, assume that M is the radical of a finitely generated ideal I of R, and let $\{M^n | n \geq 1\}$ be the complete set of M-primary ideals of R. Since M is maximal, $\sqrt{I} = M$ implies that I is M-primary, hence $I = M^n$ for some $n \in \mathbb{N}$. Then $M^{2n} = I^2 \subset I$ and therefore $M \supset M^2 \supset \dots$ i.e. all powers of M are distinct. Moreover, for each $b \in M^{n-1} \setminus M^n$, we have $M^{n-1} = bR + M^n$. Thus M^{n-1}, and by the same way, M^k is finitely generated for $k \leq n$. In particular, M is finitely generated.

To see that M is principal, suppose by the way of contradiction that M is minimally generated by $n > 1$ elements. Let $M = (a_1, \dots, a_n)$. Since $M \neq M^2$, suppose without loss of generality that $a_n \notin M^2$. Since $M^2 \subset (a_1^2, \dots, a_{n-1}^2, a_n) \subseteq M$ and the minimal prime ideal of $(a_1^2, \dots, a_{n-1}^2, a_n)$ is M, $(a_1^2, \dots, a_{n-1}^2, a_n)$ becomes an M-primary ideal and must therefore be equal to M. Consider the equation

$$a_1 = r_1 a_1^2 + r_2 a_2^2 + \ldots + r_{n-1} a_{n-1}^2 + r a_n$$

This implies that $a_1(1 - r_1 a_1) \in (a_2, \ldots, a_n)$. Since $a_1 \in M$ and M is the Jacobson radical of R, then $1 - r_1 a_1$ is a unit in R, hence $a_1 \in (a_2, \ldots, a_n)$ which is a contradiction with our assumption. So M must be principal.

Let $M = (a)$. Now suppose that for some $Q \in \mathit{Spec}(R) \setminus \mathit{Max}(R)$, and some $k \geq 1$, we have $Q \subseteq M^k$ but $Q \nsubseteq M^{k+1}$. It follows that $Q + M^{k+1}$ is M-primary and must be equal to M^k. So we have $a^k = q + t a^{k+1}$, where $t \in R, q \in Q$. It follows that $a^k(1 - ta) \in Q$. Since Q is a prime, we have either $a \in Q$ or $1 - ta \in Q$. If $a \in Q$, then we have $(a) = M \subseteq Q \subset M$, a contradiction. If $1 - ta \in Q$, then $1 \in Q + aR = Q + M = M$, a contradiction again. Hence if $Q \in \mathit{Spec}(R) \setminus \mathit{Max}(R)$, then $Q \subseteq \bigcap_{n \geq 1} M^n$.

Continue with the assumption that $M = (a)$ and let $x, y \notin \bigcap_{n \geq 1} M^n$, so for some $k, t \in \mathbb{N}$, $x \in M^k \setminus M^{k+1}$ and $y \in M^t \setminus M^{t+1}$. Then $x = a^k r_1$ and $y = a^t r_2$ for some $r_1, r_2 \in R \setminus M$. It follows that $xy = a^{k+t} r_1 r_2 \in M^{k+t} \setminus M^{k+t+1}$. Hence $\bigcap_{n \geq 1} M^n$ is a prime ideal of R. $M \neq M^2$ implies that $\bigcap_{n \geq 1} M^n \subset M$, which means it is not a maximal ideal of R. □

Lemma 4.14. *Let R be an integral domain, and let $P \in \mathit{Spec}(R)$ with $P \neq (0)$. If A is a radical ideal contained in P but P is not minimal over A, then we have $(R : P) \subseteq (A : A)$.*

Proof. Let $x \in (R : P)$, then $xP \subseteq R$. Since $A \subset P$ we have $xA \subseteq R$. The fact that $xP \subseteq R$ also implies that $xPA \subseteq A$. Let Q be a minimal prime ideal of A. Then we have $xPA \subseteq A \subseteq Q$. Since $P \nsubseteq Q$, and $Q \in \mathit{Spec}(R)$ then we have $xA \subseteq Q$. Then xA contained in each minimal prime ideal of A. Clearly this implies that $xA \subseteq \bigcap_{P \in Min(A)} P = \sqrt{A} = A$. It follows that $x \in (A : A)$. □

We have now able to prove that an SP-domain is an almost Dedekind domain.

Theorem 4.15 (Vaughan and Yeagy [5, Theorem 2.4]). ***[10, p.43, Theorem. 3.1.7]*** *If R is an integral domain with radical factorization, then R is an almost Dedekind domain.*

Proof. Let $P \in Spec(R)$ with $P \neq (0)$ and let Q be a P-primary ideal of R. Let $k \in \mathbb{N}$, and $Q = J_1 \dots J_k$ be the radical factorization of Q. Since Q is P-primary, if some $J_{i_0} \nsubseteq P$, then $\prod\limits_{i \neq i_0} J_i \subseteq Q = \prod\limits_{i=1}^{n} J_i \subseteq \prod\limits_{i \neq i_0} J_i$. Hence $Q = \prod\limits_{i \neq i_0} J_i$ which is a contradiction. Thus we have $J_i \subseteq P$ for all $i = 1, \dots, n$. But since $Q \subseteq J_i \subseteq P$, by taking radicals, we have $J_i = P$ for all i, hence $Q = P^n$. Therefore, R has property (α). If P is a minimal prime of the zero ideal, then PR_P is the only nonzero prime ideal of R_P, hence the only way a nonzero ideal of R_P can factor into radical ideals is as a power of PR_P. Thus it suffices to show that R is one dimensional.

Suppose that $dim\, R > 1$. Let $P, N \in Spec(R)$ with $P \subset N$ be such that P is minimal over a nonzero principal ideal sR, and N is minimal over an ideal of the form $tR + P$ for some $t \in N \setminus P$. Then $NR_N \neq N^2 R_N$ by Lemma 4.9 and so by Lemma 4.11, NR_N is principal and $\bigcap\limits_{n \geq 1} N^n \subset N$ contains each prime ideal that is properly contained in P.

Let sR_N be such that $sR_N = I_1 \dots I_n R_N$ with each $I_i R_N$ is a radical ideal of R_N. Each $I_i R_N$ is invertible and at least one of them is contained in PR_N. Without loss of generality, suppose $I_1 R_N \subseteq PR_N$. Then NR_N is not minimal over $I_1 R_N$, hence by Lemma 4.14, we obtain the following

$$(R_N : NR_N) \subseteq (I_1 R_N : I_1 R_N)$$

This inclusion leads us to a contradiction since we have $(I_1 R_N : I_1 R_N) = R_N$ and $R_N \subset (R_N : NR_N)$. We shall prove that the strict inclusion holds. We know that NR_N is principal, so set $NR_N = \left(\frac{n}{s}\right)$ for some $n \in N, s \in R \setminus N$. We clearly have $\frac{1}{n}$ in the field of fractions of R, but $\frac{1}{n} \notin R_N$. For otherwise, there exist $r \in R, p \in R \setminus N$ such that $\frac{1}{n} = \frac{r}{p}$. It follows that for some $u \in R \setminus N$, $unr = up \in N$. Since $u \notin N$, and $N \in Spec(R)$, then we have $p \in N$, which is a contradiction.

We have $\frac{1}{n}\frac{n}{s} = \frac{1}{s} \in R_N$, since $\frac{n}{s}$ is the generator of NR_N, it follows that $\frac{1}{n} NR_R \subseteq R_N$. Hence $\frac{1}{n} \in (R_N : NR_N) \setminus R_N$. So we have $R_N \subset (R_N : NR_N)$. □

Corollary 4.16. *An integral domain R is an SP-domain if and only if R is a Prüfer domain having no critical ideals and every prime ideal of R is maximal.*

Proof. Let R be an SP-domain, then by Theorem 4.15, R is an almost Dedekind domain, hence a Prüfer domain. It follows that every prime ideal of R is maximal by

Theorem 3.2 and by Theorem 4.8, R has no critical maximal ideals.

Conversely, assume that R is a Prüfer domain with no critical maximal ideals and let $Spec(R) = Max(R)$. Since an idempotent maximal ideal is critical, then we have $M \neq M^2$ for all $M \in Max(R)$. Since R_M is a valuation domain, it follows that MR_M is a principal ideal of R_M. With the fact that every prime ideal of R is maximal, R becomes an almost Dedekind domain. By Theorem 4.8, R is an SP-domain. □

5 RINGS PRODUCED BY ORDERED ABELIAN GROUPS

We construct this section using the well-known theory of the ordered abelian groups with the informations and definitions in [11] and [12].

5.1 Partially Ordered Abelian Groups

In this section, we shall study Abelian groups which has an order relation compatible with the group operation. First of all we shall give some definitions in set theory.

If G is an abelian group and if $\leq$ satisfies the property that $a \leq b$ implies $a+c \leq b+c$ for all $a, b, c \in G$, then we say that $\leq$ is compatible with the group operation on G. G is called a partially (respectively totally) ordered group, if $\leq$ is compatible with the group operation of G and $\leq$ is a partial (respectively total) order.

Let G be a partially ordered group under $\leq$. For a $g \in G$, we say that g is positive if $g \geq 0$ and g is negative if $g \leq 0$. We set $G^+ = \{g \in G | g \geq 0\}$ as the set of positive elements of G. G^+ clearly satisfies the properties that, $0 \in G^+$, $G^+ \cap (-G^+) = \{0\}$ where $-G^+$ is the set of inverses of element of G^+, and lastly, G^+ is a subsemigroup of G. Furthermore, if G is a totally ordered group, then for all $g \in G$, either $g \in G^+$ or $-g \in G^+$ is true. This is also a sufficient condition for G to be totally ordered, since if $x, y \in G$ we either have $x - y \leq 0$ or $x - y \geq 0$.

Let S be a partially ordered set, if for any $a, b \in S$, there exists $c \in S$ such that $a, b \leq c$ (or $c \leq a, b$) then we say S is filtered to the right (or left). If G is a partially ordered group, then being filtered to the right and being filtered to the left are equivalent for G. If these conditions are satisfied, then we say that G is filtered. For a partially ordered group G, it is necessary and sufficient condition that G^+ generates G as a group.

Let S be a partially ordered set and let $A \subseteq S$ be nonempty. If $b \in S$ satisfies $a \leq b$ for all $a \in A$, then we say that b is an upper bound of A. If b is an upper bound of A and it satisfies $b \leq c$ for all upper bounds $c \in S$, then we say that b is the least upper bound of A, and denote $b = sup(A)$. Lower bound and the greatest lower bound are defined similarly, and the greatest lower bound of A is denoted by $inf(A)$.

We shall give some basic properties of $sup(A)$ and $inf(A)$ in the following theorem.

Theorem 5.1. *Let G be an abelian group which is partially ordered. Let $A, B \subseteq G$ be nonzero, and let $a, b, x \in G$. Then following conditions hold:*

(1) *$sup(A)$ exists if and only if $inf(-A)$ exists. If $sup(A)$ exists, then $sup(A) = inf(-A)$.*

(2) *If two of $sup(A), sup(B)$ and $sup(A+B)$ exist, then third one also exists. In the latter case, the equality $sup(A) + sup(B) = sup(A+B)$ holds.*

(3) *$sup(A)$ exists if and only if $sup(A+x)$ exists where $A + x = \{a + x | a \in A\}$, if $sup(A)$ exists, then we have $sup(A+x) = sup(A) + x$.*

(4) *$sup(a, b)$ exists if and only if $inf(a, b)$ exists. If $inf(a, b)$ exists, then $a + b = sup(a, b) + inf(a, b)$.*

(5) *If $sup(A) = x$ and $sup(B) = y$ exists, and if $sup(x, y)$ exists, then $sup(A \cup B)$ exists and $sup(A \cup B) = sup(x, y)$.*

Proof.

1. Suppose $sup(A)$ exists and equals to x. Then for all $a \in A$, we have $x \geq a$. This implies $-x \leq -a$ for all $a \in A$, since $-A = \{-a | a \in A\}$, then $-x$ is a lower bound for $-A$. Now let y be a lower bound for $-A$, then $y \leq -a$ for all $a \in A$, hence $a \leq -y$ for all $a \in A$. Since $-y$ becomes an upper bound for A and $sup(A) = x$, then we have $x \leq -y$ or $y \leq -x$. It gives that $-x = inf(-A)$ and the result follows. Similarly, we can see existence of $inf(A)$ implies that $sup(-A)$ exists. By choosing $-A$ as A, the result directly follows from the fact that $-(-A) = A$.

2. Suppose that $sup(A) = x$ and $sup(B) = y$. We clearly have $x + y \geq a + b$ for all $a \in A, b \in B$, hence $x + y$ is an upper bound for $A + B$. Let t be an upper bound of $A + B$. Let $a' \in A$. Since $t \geq a' + b$ for all $b \in B$, we have $t - a' \geq b$. Since $t - a'$ is an upper bound, then we have $t - a' \geq y$, which implies $t - y \geq a'$. Since a' is an arbitrary element of A, then we must have $t - y \geq x$ which gives that $t \geq x + y$. So we have $sup(A) + sup(B) = x + y = sup(A + B)$.
   Now let $sup(A) = x$ and $sup(A+B) = z$. Our aim is to show that $sup(B)$ exists. Let $b' \in B$, then $z \geq a + b'$ for all $a \in A$, hence $z - b' \geq a$ implies that $z - b' \geq x$.

It follows that $z - x \geq b'$, and since b' is arbitrary, then we must have $z - x$ is an upper bound of B. If w is an upper bound of B, then $x+w$ is an upper bound of $A+B$, hence $z \leq x+w$, it follows that $z - x \leq w$ which means $z - x = sup(B)$. We can prove the last possibility that $sup(B)$ and $sup(a+B)$ exist implies $sup(A)$ exists by using a similar way, so the proof is complete.

3. Suppose that $sup(A) = y$, then $y \geq a$ for all $a \in A$. Since $A+x = \{a+x | a \in A\}$, then $x + y \geq a + x$ for all $a \in A$ which implies $x + y$ is an upper bound of $A+x$.Let z be an upper bound of $A+x$, hence $z \geq a+x$ for all $a \in A$, it follows that $z - x \geq a$ for all $a \in A$, and so $z - x \geq y$. Thus $z \geq x + y$ which gives $sup(A) + x = x + y = sup(A + x)$.
   If we choose $A+x$ as A and $-x$ as x, then $sup\big((A+x)+(-x)\big) = sup(A+x)+(-x)$ or $sup(A) = sup(A+x) - x$, hence existence of $sup(A+x)$ implies $sup(A)$ exists.

4. Suppose that $sup(a, b) = x$, then we shall show that $inf(a, b) = a + b - x$. Since $a - x \leq 0$ and $b - x \leq 0$, then we have $a + b - x \leq b$ and $a + b - x \leq a$, then $a + b - x$ is a lower bound of a and b. Set y be a lower bound of a and b, then $a, b \leq a + b - y$, hence $a + b - y$ is an upper bound of a and b, then $x \leq a + b - y$ and consequently $y \leq a + b - x$. Hence $inf(a, b) = a + b - x = a + b - sup(a, b)$. Similarly we can obtain that if $inf(a, b)$ exists, then $sup(a, b)$ exists and equal to $a + b - inf(a, b)$. If $sup(a, b)$ exists it follows from the equalities above that $a + b = sup(a, b) + inf(a, b)$.

5. Let $sup(A) = x$, $sup(B) = y$ and $sup(x, y) = k$. Let $u \in A \cup B$. If $u \in A$, then we have $u \leq x \leq k$, and if $u \in B$, then $u \leq y \leq k$. Therefore, k is an upper bound of $A \cup B$. Let m be an upper bound of $A \cup B$. Then we have $m \geq a$ for all $a \in A$ and $m \geq b$ for all $b \in B$. By definition of supremum, we have that $m \geq x$ and $m \geq y$. It follows from $sup(x, y) = k$ that $m \geq k$. Hence $sup(A \cup B) = k = sup(x, y)$.

□

If G is a partially ordered abelian group under $\leq$, then the relation $\leq'$ on G which is defined by $a \leq' b$ if and only if $b \leq a$ is clearly a partially order on G. It follows that conditions $(1), (2)$ and (3) of Theorem 5.1 also hold for the infimums.

Now let $a, b \in G$. If $inf(a, b)$ exists and $inf(a, b) = 0$, then we say that a and b are disjoint, or a is disjoint with b. By (4) of Theorem 5.1, it is the case that $sup(a, b)$ exists and $sup(a, b) = a + b$.

In particular, $sup(a, 0)$ exists if and only if $inf(a, 0)$ exists. If $sup(a, 0)$ exists we denote $sup(a, 0)$ and $-inf(a, 0)$ by a^+ and a^-, respectively.

Proposition 5.2. *Let G be a partially ordered abelian group and let $a, b, c, x, y \in G$. Then the following statements hold:*

(1) *If $a = x - y$ for some $x, y \in G^+$ and if $sup(a, 0)$ exists, then $inf(x, y)$ exists, $x = a^+ + inf(x, y)$ and $y = a^- + inf(x, y)$. Clearly $a^+ \leq x$ and $a^- \leq y$, and if x and y are disjoint, then $x = a^+$ and $y = a^-$. In particular, a^+ and a^- are disjoint.*

(2) *If $a, b, c \in G^+$ is such that a and c are disjoint, the existence of $inf(a, b)$ implies $inf(a, b + c)$ exists and $inf(a, b + c) = inf(a, b)$.*

(3) *If $a, b, c \in G^+$ is such that a and b are both disjoint with c, then $a + b$ is also disjoint with c. Additionally, if $d \in G^+$, then $a \leq c + d$ implies that $a \leq d$.*

(4) *If $sup(a, b)$ exists and if n is a nonnegative integer, then $sup(na, nb)$ exists and $sup(na, nb) = n\, sup(a, b)$. A similar statement holds for $inf(a, b)$.*

Proof.

1. Suppose $a^+ = sup(a, 0)$ exists and let $a = x - y$ for some $x, y \in G^+$. Since we have $sup(-x, -y) = -inf(x, y)$ by (1) of Theorem 5.1, then we have $a^+ = sup(a, 0) = sup(x - y, 0) = sup(x - y, x - x) = x + sup(-y, -x) = x - inf(x, y)$. It follows that $x = a^+ + inf(x, y)$. Similarly, we have $a^- = -inf(a, 0) = -inf(x - y, 0) = -inf(x - y, y - y) = y - inf(x, y)$, hence $y = a^- + inf(x, y)$. It is clear that $x \geq a^+$ and $y \geq a^-$. If x and y are disjoint, that is $inf(x, y) = 0$, then we have $x = a^+$ and $y = a^-$. Since $a = a^+ - a^-$, then we have $a^+ = a^+ + inf(a^+, a^-)$, thus a^+ and a^- are disjoint, as claimed.

2. Let $inf(a, b) = k$, then $k \leq a$ and $k \leq b$. Since $c \geq 0$, then $k \leq b \leq b + c$. So k is a lower bound of a and $b + c$. Now let s be a lower bound for a and $b + c$. Then $s \leq a$ and $s \leq b + c$. Since $b \geq 0$, then we have $s \leq a \leq a + b$. Equivalently we

have $s-b \leq a$ and $s-b \leq c$. It follows that $s-b \leq 0$ or $s \leq b$. So we have $s \leq a$ and $s \leq b$, which implies $s \leq k$. So $k = inf(a, b+c)$.

3. Let $inf(a,c) = inf(b,c) = 0$. We clearly have $a, b, c \geq 0$, hence $a+b, c \geq 0$ which means 0 is a lower bound for $a+b$ and c. If k is a lower bound for $a+b$ and c, then $a+b \geq k$ and $c \geq k$ and since $b \in G^+$, then we have $a \geq k-b$ and $c \geq k-b$. $inf(a,c) = 0$ now implies that $0 \geq k-b$ or $b \geq k$. Since we have $b \geq k$ and $c \geq k$, then $inf(b,c) = 0$ implies that $k \leq 0$. Hence $0 = inf(a+b, c)$.
   Now let $a \leq c+d$ for some $d \in G^+$. Then we have $a \geq a-d$ and $c \geq a-d$. Since $inf(a,c) = 0$ it follows that $0 \geq a-d$ or $a \leq d$ equivalently.

4. Since $sup(a,b)$ exists, then we have $(a-b)^+ = sup(a-b, 0) = sup(a,b) - b$. We have $a-b = (a-b)^+ - (a-b)^-$, and $inf\big((a+b)^+, (a+b)^-\big) = 0$. It follows from (3) that $inf\big(n(a-b)^+, n(a-b)^-\big) = 0$. Moreover, $n(a-b) = n(a-b)^+ - n(a-b)^-$. By (1), $sup(na-nb, 0)$ exists and we have $n(a-b)^+ = sup(na-nb, 0) = n\big(sup(a,b) - b\big) = n\, sup(a,b) - nb$. Hence we have that $sup(na, nb)$ exists, and $sup(na, nb) = sup(na-nb, 0) + nb = n\, sup(a,b)$. Now (4) of 5.1 implies that $inf(na, nb)$ exists and $inf(na, nb) = na + nb - sup(na, nb) = n\big(a+b-sup(a,b)\big) = n\, inf(a,b)$.

□

5.2 Lattice Ordered Abelian Groups

We call a partially ordered abelian group G as lattice ordered, if for each $a, b \in G$, $sup(a,b)$ exists. If this is the case, the partial order on G is called a lattice order.

Theorem 5.3. *Let G be a partially ordered abelian group.*

1. *If G is filtered, then the following conditions are equivalent:*

   (a) The order on G is a lattice order.

   (b) For all $a, b \in G^+$, $sup(a,b)$ exists.

   (c) For all $a, b \in G^+$, $inf(a,b)$ exists.

2. *If G is lattice ordered, for each finite subset $A = \{a_1, \ldots, a_n\}$ of G, $sup(A)$ and $inf(A)$ exists.*

3. *If G is lattice ordered and if $A = \{a_1, \ldots, a_n\} \subseteq G^+$, then the following conditions are equivalent:*

   (a) $inf(A) = 0$.

   (b) *For each $x \in G^+$ with $x \neq 0$, there exists $y \in G$ with $0 < y \leq x$ such that $inf(y, a_i) = 0$ for some $a_i \in A$.*

Proof.

1. By definition, (a) implies (b) is clear. By (4) of 5.1, we have (b) and (c) are equivalent. Hence it suffices to show (b) implies (a) to complete the proof. Let $g, h \in G$. Choose $t \in G$ such that $t \leq g$ and $t \leq h$. Then $g - t, h - t \in G^+$, and by assumption, $sup(g-t, h-t)$ exists. Since we have $sup(g-t, h-t)+t = sup(g, h)$, then $sup(g, h)$ exists. Thus G is a lattice ordered group.

2. Let G be a lattice ordered group. Since we have $sup(a_1, a_2)$ exists for $a_1, a_2 \in G$, then suppose as induction hypothesis that supremum exists for arbitrary set which has $n - 1$ or less elements of G. Let $A = \{a_1, \ldots, a_n\}$, and $A' = \{a_1, \ldots, a_{n-1}\}$. By induction hypothesis, $sup(A')$ exists, say $x = sup(A')$. Set $sup(x, a_n) = k$. Our claim is that $sup(A) = k$. Clearly, $k \geq x \geq a_i$ for $i = 1, \ldots, n-1$ and $k \geq a_n$, hence k is an upper bound of A. Let m be an upper bound of A. It follows that $m \geq a_i$ for all $i = 1, \ldots, n$. Since m is an upper bound of A', then we have $m \geq x$. But then $m \geq x$ and $m \geq a_n$ together implies that $m \geq k$. Hence $k = sup(A)$. For a finite subset A of G, existence of $inf(A)$ can be obtained similarly.

3. Let $A = \{a_1, \ldots, a_n\} \subseteq G^+$. First suppose that $inf(A) = a > 0$. Suppose that $y \in G$ be such that $0 < y \leq a$ with $inf(y, a_i) = 0$ for some $i = 1, \ldots, n$. Since $y \leq a$ and $a \leq a_i$, then we have $y \leq a_i$ and so $inf(y, a_i) = y = 0$. This is a contradiction with $0 < y$. Hence such an element doesn't exist. Conversely, let $inf(A) = 0$ and let $x > 0$. The we have that $x \geq inf(x, a_1) \geq inf(x, a_1, a_2) \geq \ldots \geq inf(x, a_1, \ldots, a_n) = 0$. If $inf(x, a_1) = 0$, then choosing $y = x$ gives the desired result. Otherwise, choose $y = inf(x, a_1, \ldots, a_i)$ such that $inf(x, a_1, \ldots, a_i) \neq 0$ but $inf(x, a_1, \ldots, a_i, a_{i+1}) = 0$. This gives that $inf(y, a_{i+1}) = 0$. Since we find such a y, then the proof is complete.

□

Theorem 5.4. *Let G be a partially ordered abelian group, then G is lattice ordered if and only if each element of G can be expressed as a difference of two disjoint elements of G^+.*

Proof. Let G be a lattice ordered group, then for $a \in G$, $a^+ = sup\{a, 0\}$ exists. By (4) of Theorem 5.1, we have $a = a^+ - a^-$. By (1) of Proposition 5.2, we have $inf\{a^+, a^-\} = 0$ so we are done.

Now let $a, b \in G$. Our aim is to show, under the assumption that each element of G can be expressed as a difference of two disjoint elements of G^+, $sup\{a, b\}$ exists. Set $a = x_1 - y_1$ where $x_1, y_1 \in G^+$ and $inf\{x_1, y_1\} = 0$.

$sup\{a, 0\} = sup\{x_1 - y_1, y_1 - y_1\} = sup\{x_1, y_1\} - y_1 = x_1 + y_1 - y_1 = x_1$, so $a^+ = sup\{a, 0\} = x_1$. Similarly, $a^- = -inf\{a, 0\} = y_1$. Thus our assumption implies that for every element x of G, $x^+ = sup\{x, 0\}$ and $x^- = -inf\{x, 0\}$ exist.

Now let $a, b \in G$, our claim is that $sup\{a, b\}$ exists. Since $sup\{a, b\} = sup\{a - b, 0\} + b$ and $sup\{a - b, 0\}$ exists, then $sup\{a, b\}$ exists. Hence G is lattice ordered. □

Let R be an integral domain with the field of fractions Q, and let U be the multiplicative group of units of R. Set $G = Q^*/U$ where Q^* denotes the set of nonzero elements of Q, and set $\Pi : Q^* \to G$ be the canonical epimorphism. In this case G is called the group of divisibility of R.

Define an ordering on G by

$$aU \leq bU \iff a^{-1}b \in R$$

We shall view G as additive group with addition $aU + bU = abU$. Then $(G, +)$ becomes a partially ordered group with $G^+ = \Pi(R^*) = \big\{aU | a \in R^* = R \setminus \{0\}\big\}$.

Let G be a totally ordered group and let $v : Q^* \to G$ be a valuation. If $R = \{x \in Q^* | v(x) \geq 0\} \cup \{0\}$ then R is a valuation domain, Q is the field of fractions of R, and G is order-isomorphic to the group of divisibility of R.

R is a valuation domain if and only if its group of divisibility is totally ordered.

G is a lattice ordered group if G is a partially ordered group such that $inf\{g, h\}$ and $sup\{g, h\}$ exist in G for all $g, h \in G$. Since $sup\{g, h\} = -inf\{g, h\}$, it is sufficient for us to check only infimums of supremums exist.

If G is a lattice ordered group and $X \subseteq G$, then X is a sublattice of G if $inf_X\{x,y\} = inf_G\{x,y\}$ for all $x, y \in X$.

If G and G' are lattice ordered groups and $f : G \to G'$, then f is a lattice homomorphism provided that f is a group homomorphism and $f(inf\{g,h\}) = inf\{f(g), f(h)\}$ for all $g, h \in G$. Clearly such an f will also satisfy $f(sup\{g,h\}) = sup\{f(g), f(h)\}$ for all $g, h \in G$. And as a result, f is an order homomorphism, and $f(G)$ is a sublattice of G'.

Let $\{G_\alpha | \alpha \in \Gamma\}$ be a family of partially ordered groups, and let $G = \prod\limits_{\alpha \in \Gamma} G_\alpha$. Then G can be ordered in two different ways as follows:

(I) For $(x_\alpha), (y_\alpha) \in G$, define $(x_\alpha) \leq (y_\alpha)$ if $x_\alpha \leq y_\alpha$ for all $\alpha \in \Gamma$. This is called the product ordering on G and makes G into a partially ordered group. If each of G_α is a lattice ordered group, then G is also a lattice ordered group with the product ordering.

(II) For $(x_\alpha), (y_\alpha) \in G$, define $(x_\alpha) \leq (y_\alpha)$ if $(x_\alpha) = (y_\alpha)$ or $x_{\alpha_0} < y_{\alpha_0}$ where $\alpha_0 = inf\{\alpha \in \Gamma | x_\alpha \neq y_\alpha\}$. This is called the lexicographic ordering on G, and makes G a partially ordered group. If each of G_α is a totally ordered group, then G is also a totally ordered group with the lexicographic ordering.

Definition 5.5. Let G be a lattice ordered group. A subset S of G is called a segment of G if it satisfies the following conditions:

(i) $S \subset G^+$

(ii) S is filtered, i.e. $x \in S, y \in G$ and $y > x$ implies $y \in S$.

(iii) $x, y \in S$ implies $inf\{x,y\} \in S$.

S is called a prime segment of G, if S is a segment of G and $G^+ \setminus S$ is a semigroup, i.e. $x, y \in G^+ \setminus S$ implies $x + y \in G^+ \setminus S$. Note that the empty set is always a prime segment. We shall denote the set of prime segments in a lattice ordered group G with $Spec(G)$.

Notation. Let G be a lattice ordered abelian group, and let S be a subsemigroup of G^+ such that $G^+ \setminus S$ is filtered. Define $H_S = \{g_1 - g_2 | g_1, g_2 \in S\}$. Evidently, H_S is a subgroup of G (generated by S). Now form the quotient group G/H_S, which we shall denote by G_S.

Theorem 5.6. *With the above notation, the following statements hold:*

(1) *G_S is a lattice ordered group with the ordering defined by*

$$g_1 + H_S \leq g_2 + H_S \iff \exists h \in H_S \text{ such that } g_2 - g_1 + h \geq 0$$

Moreover, the canonical mapping $\pi : G \to G_S$ is a lattice homomorphism.

(2) *If A is a segment of G with $A \cap S = \emptyset$, then $\pi(A)$ is a segment of G_S. Conversely, if $\mathcal{A}$ is a segment of G_S, then $\pi^{-1}(\mathcal{A})$ is a segment of G such that $\pi^{-1}(\mathcal{A}) \cap S = \emptyset$. Moreover, every segment of G_S is of the form $\pi(A)$, where A is a segment of G such that $A \cap S = \emptyset$.*

(3) *If B is a segment of G such that $B \cap S \neq \emptyset$, then $\pi(B) = G_S^+$.*

(4) *If P is a prime segment of G such that $P \cap S = \emptyset$, then $\pi(P)$ is a prime segment of G_S. Conversely, if $\mathcal{P}$ is a prime segment of G_S, then $\pi^{-1}(\mathcal{P})$ is a prime segment of G such that $\pi^{-1}(\mathcal{P}) \cap S = \emptyset$. Moreover, $\pi^{-1}(\pi(P)) = P$ for any prime segment P of G such that $P \cap S = \emptyset$.*

(5) *There is a one-to-one correspondence between prime segments P of G such that $P \cap S = \emptyset$ and prime segments $\mathcal{P}$ of G_S defined by*

$$\Phi : P \to \pi(P)$$

whose inverse is given by

$$\Psi : \mathcal{P} \to \pi^{-1}(\mathcal{P})$$

Proof. (1) Clearly, the given relation is reflexive and transitive. To see the anti-symmetry, let $g_1 + H_S \leq g_2 + H_S$ and $g_2 + H_S \leq g_1 + H_S$ for some $g_1, g_2 \in G$. Then, by definition, there exist $h, h' \in H_S$ such that $g_2 - g_1 + h \geq 0$ and $g_1 - g_2 + h' \geq 0$. By adding suitable element of S to h and h', we may assume that $h, h' \in S$. Then

$$(g_1 - g_2 + h') + (g_2 - g_1 + h) = h' + h \in S$$

If $g_2 - g_1 + h \in G^+ \setminus S$, then since $g_2 - g_1 + h \leq (g_1 - g_2 + h') + (g_2 - g_1 + h) = h' + h$, and since $G^+ \setminus S$ is filtered, we have $h + h' \in G^+ \setminus S$, a contradiction. It follows that, $g_2 - g_1 + h \in S$, and so $g_2 - g_1 = g_2 - g_1 + h - h \in H_S$. Therefore,

$g_1 + H_S = g_2 + H_S$.

Now, if $g_1 + H_S \leq g_2 + H_S$, then $g_2 - g_1 + h \geq 0$ for some $h \in H_S$. For any $g \in G$, $(g_2 + g) - (g_1 + g) + H \geq 0$, and so

$$(g_1 + H_S) + (g + H_S) \leq (g_2 + H_S) + (g + H_S)$$

It therefore follows that G_S is an ordered abelian group. It remains to show that infimums of any two elements of G_S exists. Let $g_1, g_2 \in G$, and let $g = inf\{g_1, g_2\}$. It is immediate that $g + H_S \leq g_i + H_S$ for $i = 1, 2$. Let $g' \in G$ be such that $g' + H_S \leq g_i + H_S$ for $i = 1, 2$. Then there exist $h_1, h_2 \in H_S$ such that $g_i - g' + h_i \geq 0$ for $i = 1, 2$. As before, we may assume that $h_1 = h_2 = h \in S$. Since $g_i \geq g' - h$ for $i = 1, 2$, then we have $g \geq g' - h$, and so $g - g' + h \geq 0$, which gives that $g' + H_S \leq g + H_S$. Thus $g + H_S = inf\{g_1 + H_S, g_2 + H_S\}$. Hence, G_S is a lattice ordered abelian group.

The fact that π is a lattice homomorphism is straightforward since for $g_1, g_2 \in G$, $inf\{g_1 + H_S, g_2 + H_S\} = inf\{g_1, g_2\} + H_S$.

(2) Let A be a segment of G with $A \cap S = \emptyset$. If $\pi(A) = G_S^+$, then there exists $a \in A$ such that $\pi(a) = a + H_S = H_S$ and this implies $a \in H_S$. So there exist $s_1, s_2 \in S$ such that $a = s_1 - s_2$, or $s_1 = a + s_2 \geq a$. Since A is a segment and $a \in A$, this gives that $s_1 \in A$, contrary to our assumption $A \cap S = \emptyset$. So $\pi(A) \subset G_S^+$.

Let $\pi(a) = a + H_S \in \pi(A)$ and $g + H_S \in G_S^+$ be such that $\pi(a) = a + H_S \leq g + H_S$. Then there exists $h \in H_S$ such that $g - a + h \geq 0$, clearly we may assume that $h \geq 0$. So we have $g + h \geq a$, and since A is a segment, then we have $g + h \in A$. Thus $\pi(g + h) = g + h + H_S = g + H_S \in \pi(A)$.

Let $a + H_S, b + H_S \in \pi(A)$, where $a, b \in A$. Since A is a segment, we have $inf\{a, b\} \in A$, and so $inf\{a + H_S, b + H_S\} = inf\{a, b\} + H_S = \pi(inf\{a, b\}) \in \pi(A)$.

Thus $\pi(A)$ is a segment of G_S.

Now let $\mathcal{A}$ be a segment of G_S. Since $\mathcal{A} \subset G_S^+$, then we have $\pi^{-1}(\mathcal{A}) \subset G^+$, for otherwise, if $\pi^{-1}(\mathcal{A}) = G^+$, then since π is surjective we have $\mathcal{A} = \pi(\pi^{-1}(\mathcal{A})) = G_S^+$, a contradiction.

Let $a \in \pi^{-1}(\mathcal{A})$ and $g \in G^+$ be such that $a \leq g$. Then we have $\pi(a) \leq \pi(g)$, and since $\mathcal{A}$ is a segment and $\pi(a) \in \pi(\pi^{-1}(\mathcal{A})) = \mathcal{A}$, then $\pi(g) \in \mathcal{A}$ which implies $g \in \pi^{-1}(\mathcal{A})$.

Let $a, b \in \pi^{-1}(\mathcal{A})$, then $\pi(a) = a + H_S, \pi(b) = b + H_S \in \mathcal{A}$, since $\mathcal{A}$ is a segment of G_S^+, then we have $inf\{a + H_S, b + H_S\} = inf\{a, b\} + H_S = \pi(inf\{a, b\}) \in \mathcal{A}$, then $inf\{a, b\} \in \pi^{-1}(\mathcal{A})$.

Thus $\pi^{-1}(\mathcal{A})$ is a segment of G.

Suppose that $\pi^{-1}(\mathcal{A}) \cap S \neq \emptyset$. Let $x \in \pi^{-1}(\mathcal{A}) \cap S$, then $\pi(x) = x + H_S \in \mathcal{A}$ and $\pi(x) = x + H_S \in \pi(S) = S + H_S = \{s + H_S | s \in S\}$. But since $S \subseteq H_S$, then we have $x \in H_S$. This is a contradiction since $x + H_S = 0 + H_S \in \mathcal{A}$ and this implies that $\mathcal{A} = G_S^+$. So we must have $\pi^{-1}(\mathcal{A}) \cap S = \emptyset$.

Since we have $\pi(\pi^{-1}(\mathcal{A})) = \mathcal{A}$ for all segments $\mathcal{A}$ of G_S, and $\pi^{-1}(\mathcal{A})$ is a segment of G such that $\pi^{-1}(\mathcal{A}) \cap S = \emptyset$, then the last sentence of our claim is already proved.

(3) Let B is a segment of G such that $B \cap S \neq \emptyset$. Let $b \in B \cap S$, then $\pi(b) = b + H_S \in \pi(B)$. Since $b \in S \subseteq H_S$, then $b + H_S = 0 + H_S$. We can show $\pi(B)$ is filtered as we have showed $\pi(A)$ is filtered in (2) of this proof. Since $0 + H_S \in \pi(B)$, we have $\pi(B) = G_S^+$.

(4) Let P be a prime segment of G such that $P \cap S = \emptyset$, by (2) of this proof $\pi(P)$ is a segment of G_S. Now let $a + H_S, b + H_S \in G_S^+ \setminus \pi(P)$. We claim that $a, b \in G^+ \setminus P$. If $a < 0$, then $a + H_S \leq 0 + H_S$, and since $a + H_S \in G_S^+$, then $a \in H_S$. So $a = s_1 - s_2$ for some $s_1, s_2 \in S$. Then since $G^+ \setminus S$ is filtered, $a = s_1 - s_2 \leq s_1$ and $s_1 \in S$ implies $a \in S \subseteq G^+$, a contradiction. Then we have $a \in G^+$, and similarly, $b \in G^+$. Clearly if $a, b \in P$, then $\pi(a), \pi(b) \in \pi(P)$. Thus we have $a, b \in G^+ \setminus P$. Since P is a prime segment, this implies $a + b \in G^+ \setminus P$.

Now our claim is that if $x \in G^+ \setminus P$, then $\pi(x) \in G_S^+ \setminus \pi(P)$. Let $x \in G^+ \setminus P$. $x \in G^+$ implies that $x \geq 0$ and so $x + H_S \geq 0 + H_S$. Thus $x + H_S \in G_S^+$. Now suppose that $x \notin P$ and $\pi(x) = x + H_S \in \pi(P)$. Then $x + H_S = p + H_S$ for some $p \in P$. And this implies $p - x \in H_S$ and so $p - x = s_1 - s_2$ for some $s_1, s_2 \in S$. Then $p + s_2 = x + s_1 \geq p$, and since $p \in P$, then we have $x + s_1 \in P$. The facts that P is a prime segment and $x \notin P$ implies that $s_1 \in P$. But then we have $s_1 \in S \cap P$ which is a contradiction. So our claim is true.

Since we have shown that $a+b \in G^+ \setminus P$, then we have $\pi(a+b) = \pi(a) + \pi(b) \in G_S^+ \setminus \pi(P)$. Hence, $\pi(P)$ is a prime segment of G_S.

Now let $\mathcal{P}$ be a prime segment of G_S. It has shown in (2) of this proof that $\pi^{-1}(\mathcal{P})$ is a segment of G such that $\pi^{-1}(\mathcal{P}) \cap S = \emptyset$. The only part we shall show that $\pi^{-1}(\mathcal{P})$ is prime. Let $a, b \in G^+ \setminus \pi^{-1}(\mathcal{P})$, then as we have shown above, $\pi(a), \pi(b) \in G_S^+ \setminus \pi\left(\pi^{-1}(\mathcal{P})\right) = G_S^+ \setminus \mathcal{P}$. Then $\pi(a+b) = \pi(a) + \pi(b) \in G_S^+ \setminus \mathcal{P}$ since $\mathcal{P}$ is a prime segment of G_S. And this implies that $a + b \in G^+ \setminus \pi^{-1}(\mathcal{P})$ as in the first paragraph of this part of the proof. So $\pi^{-1}(\mathcal{P})$ is a prime segment of G.

Now, let P be a prime segment of G such that $P \cap S = \emptyset$. It is well-known from set theory that $P \subseteq \pi^{-1}\left(\pi(P)\right)$. So we shall show the converse inclusion. Since π is an order homomorphism, then $\pi^{-1}\left(\pi(P)\right) \subseteq G^+$. So let $x \in \pi^{-1}\left(\pi(P)\right)$, then $\pi(x) \in \pi(P)$. Since we have shown above that for any prime segment P of G with $P \cap S = \emptyset$, if $x \in G^+ \setminus P$, then $\pi(x) \in G_S^+ \setminus \pi(P)$. Then $\pi(x) \in \pi(P)$ implies that $x \in P$. Thus $P = \pi^{-1}\left(\pi(P)\right)$.

(5) Let $\mathscr{P}$ and $\mathscr{P}_S$ denote respectively the prime segments P of G with $P \cap S = \emptyset$ and the prime segments of G_S.

Set $\Phi : \mathscr{P} \to \mathscr{P}_S$ defined by $\Phi(P) = \pi(P)$ for all $P \in \mathscr{P}$, and set $\Psi : \mathscr{P}_S \to \mathscr{P}$ defined by $\Psi(\mathcal{P}) = \pi^{-1}(\mathcal{P})$ for all $\mathcal{P} \in \mathscr{P}_S$.

We have shown in (4) that both Φ and Ψ are well-defined mappings. We shall show that Φ and Ψ are inverses of each other:

For any $P \in \mathscr{P}$, $\Psi\left(\Phi(P)\right) = \pi^{-1}\left(\pi(P)\right) = P$ as we have shown in (4), and by the same part, we have that $\Phi\left(\Psi(\mathcal{P})\right) = \pi\left(\pi^{-1}(\mathcal{P})\right) = \mathcal{P}$ for any $\mathcal{P} \in \mathscr{P}_S$.

Thus these mappings give us the desired correspondence.

□

Corollary 5.7. *Let G be a lattice ordered group and let P be a prime segment of G. If $S = G^+ \setminus P$, then G_S is a lattice ordered group with unique maximal segment $\pi(P)$.*

Every segment of G_S is of the form $\pi(I)$ for some segment I of G with $I \subseteq P$. In particular, G_S is totally ordered.

Definition 5.8. If G is a lattice ordered group, and if $S = G^+ \setminus P$ for a prime segment P of G, then G_S will be called as the localization of G at P, and denoted as G_P.

Now we turn our attention to totally ordered groups G and show that we can construct valuation domains whose group of divisibility is lattice-isomorphic to G. But before, we need to give the following lemma:

Lemma 5.9. *Let R be a domain with field of fractions Q, let G be a totally ordered group, and set $v : R^* \to G^+$ be a mapping which satisfies the following properties:*

(1) *v is surjective.*

(2) *$v(ab) = v(a) + v(b)$ for all $a, b \in R^*$.*

(3) *$v(a + b) \geq min\{v(a), v(b)\}$ for all $a, b \in R^*$.*

Then $\bar{v} : Q^* \to G$ defined by $\bar{v}(a/b) = v(a) - v(b)$ is a valuation on Q.

Proof. Since for $a \in R^*$, we have $\bar{v}(1/a) = v(1) - v(a) = -v(a)$ and v is surjective, then $\bar{v}$ is clearly surjective.

Let $a, b \in Q^*$, then $a = x_1/y_1, b = x_2/y_2$ for some $x_1, x_2, y_1 y_2 \in R^*$.

$$\begin{aligned}
\bar{v}(ab) &= \bar{v}(x_1x_2/y_1y_2) = v(x_1x_2) - v(y_1y_2) = v(x_1) + v(x_2) - v(y_1) - v(y_2) \\
&= v(x_1) - v(y_1) + v(x_2) - v(y_2) = \bar{v}(x_1/y_1) + \bar{v}(x_2/y_2) \\
&= \bar{v}(a) + \bar{v}(b)
\end{aligned}$$

$$\begin{aligned}
\bar{v}(a + b) &= \bar{v}(x_1/y_1 + x_2/y_2) = \bar{v}\left((x_1y_2 + x_2y_1)/y_1y_2\right) \\
&= v(x_1y_2 + x_2y_1) - v(y_1y_2) \\
&\geq min\{v(x_1y_2), v(x_2y_1)\} - v(y_1y_2) \\
&= min\{v(x_1y_2) - v(y_1y_2), v(x_2y_1) - v(y_1y_2)\} \\
&= min\{\bar{v}(x_1/y_1), \bar{v}(x_2/y_2)\} \\
&= min\{\bar{v}(a), \bar{v}(b)\}
\end{aligned}$$

Thus $\bar{v}$ is a valuation on Q. □

Theorem 5.10 (W. Krull [6, p. 164]). *[11, Theorem 1.1] If G is a totally ordered group, then there exists a valuation domain whose group of divisibility is order-isomorphic to G.*

Proof. Let K be a field and let S be the group algebra $K[G] = \left\{ \sum\limits_{i=1}^{n} k_i g_i | n \in \mathbb{N}, k_i \in K, g_i \in G \right\}$. Let Q be the field of fractions of S, and define $v : Q^* \to G$ by

$$v \left(\frac{\sum\limits_{i=1}^{m} \lambda_i g_i}{\sum\limits_{j=1}^{n} \mu_j g_j'} \right) = inf\{g_i\}_{i=1}^{m} - inf\{g_j'\}_{j=1}^{n}$$

where $\lambda_i, \mu_j \in K^*, g_i, g_j' \in G$. Our claim is to show that v is a valuation. To this aim, we shall show that $v' : S^* \to G^+$ where G^+ denotes the positive elements of G, defined by $v' \left(\sum\limits_{i=1}^{m} \lambda_i g_i \right) = inf\ \{g_i\}_{i=1}^{m}$ for $\lambda_i \in K, g_i \in G$, satisfies the properties in Lemma 5.9. Then since $v(a/b) = v'(a) - v'(b)$, v becomes a valuation on G.

Since every element of G^+ is also an element of S, then for $g \in G^+$, $v'(g) = g$, hence v' is surjective.

Let $a, b \in S$ with $a = \sum\limits_{i=1}^{m} \lambda_i g_i, b = \sum\limits_{j=1}^{n} \mu_j g_j'$ where $\lambda_i, \mu_j \in K, g_i, g_j' \in G$. Then $v'(ab) = v' \left(\sum\limits_{i=1}^{m} \sum\limits_{j=1}^{n} (\lambda_i \mu_j)(g_i g_j') \right)$. By definition, $v'(a) = inf\{g_i\}_{i=1}^{m}$ and $v'(b) = inf\{g_j'\}_{j=1}^{n}$. Since G is a totally ordered group, then we have $v'(a) = g_{i_0}$ and $v'(b) = g_{j_0}'$ for some $i_0 \in \{1, \ldots, m\}$ and $j_0 \in \{1, \ldots, n\}$. Then clearly $g_{i_0} g_{j_0}' \leq g_\alpha g_\beta'$ for all $\alpha = 1..m, \beta = 1..n$, which gives us $v'(ab) = v'(a)v'(b)$.

$$\begin{aligned}
v'(a + b) &= v'(\sum_{i=1}^{m} \lambda_i g_i + \sum_{j=1}^{n} \mu_i g_j') \\
&= inf\{g_i, g_j'\}_{(i,j)=(1,1)}^{(m,n)} \\
&= inf\ \left\{ inf\{g_i\}_{i=1}^{m}, inf\{g_j'\}_{j=1}^{n} \right\} \\
&= inf\{v'(a), v'(b)\} \\
&= min\{v'(a), v'(b)\}
\end{aligned}$$

Now set $R = \{x \in Q^* | v(x) \geq 0\} \cup \{0\}$, the valuation ring corresponding to the valuation v, then R is the desired ring since if $\bar{v}$ is the valuation determined by R, and as a result, v and $\bar{v}$ are equivalent:

Set U be the group of units of R, then $\bar{v} : Q^* \to Q^*/U$. Define $\phi : G \to Q^*/U$ by $\phi(v(a)) = aU = \bar{v}(a)$ for all $a \in Q^*$. If $v(a) = v(b)$, then $v(a/b) = 1$ so $a/b \in U$ and then $\bar{v}(a) = aU = bU = \bar{v}(b)$, thus ϕ is well-defined. Since $\phi(v(a)) = \bar{v}(a)$, then it remains to show that ϕ is an order-preserving isomorphism:

ϕ is a homomorphism, since $\phi(v(a) + v(b)) = \phi(v(ab)) = abU = aU + bU =$

$\phi(v(a)) + \phi(v(b))$. It is injective since $\phi(v(a)) = 0$ implies $a \in U$ and so $v(a) = 0$. It is clear that ϕ is surjective. Thus ϕ is an isomorphism. Now we shall show that ϕ is order-preserving. If $v(a) \leq v(b)$, then $b/a \in R$, so $aU \leq bU$, thus $\phi(v(a)) \leq \phi(v(b))$, which means ϕ is order-preserving. □

5.3 Constructing Bezout Domains

In the end of the preceding section we have shown that for any totally ordered abelian group G there corresponds a valuation ring whose group of divisibility is isomorphic to G. In this section, we look for a similar correspondence when we take the group to be a lattice ordered abelian group.

Definition 5.11. An integral domain is called a Bezout domain if every finitely generated ideal of R is principal.

Proposition 5.12. *Let R be a Bezout domain. For any $a, b \in R^*$, $aR + bR = cR$ implies $inf\{aU, bU\} = cU$.*

Proof. Let $a, b \in R^*$ with $aR + bR = cR$, then we have $aR \subseteq cR$ and $bR \subseteq cR$. So $c^{-1}a, c^{-1}b \in R$, and this implies $cU \leq aU$ and $cU \leq bU$. Let $qU \leq aU$ and $qU \leq bU$ for some $q \in R^*$, then since $q \in Q^*$, we have $q^{-1}a, q^{-1}b \in R$. And this gives us $aR \subseteq qR$ and $bR \subseteq qR$, which implies $cR = aR + bR \subseteq qR$, thus $q^{-1}c \in R$. Hence $qU \leq cU$, which proves that $inf\{aU, bU\} = cU$. □

Proposition 5.13. *Let R be a Bezout domain, then the group of divisibility of R is a lattice ordered group.*

Proof. Let Q be the field of fractions of R, and let G be the group of divisibility of R. It is sufficient for us to show that for any $x, y \in Q^*$, $inf\{xU, yU\}$ exists. Since $x, y \in Q^*$, there exists $d \in R^*$ such that $dx, dy \in R^*$. Set $cR = dxR + dyR$, where $c \in R^*$, such an element exists since R is a Bezout domain. Then by Proposition 5.12, $inf\{dxU, dyU\} = cU$. Since $dxR \subseteq cR$, then we have $c^{-1}dx \in R$. So we have $(c^{-1}d)^{-1}U \leq xU$, or $d^{-1}cU \leq xU$. Similarly, since $dyR \subseteq cR$, we have $d^{-1}cU \leq yU$. Now let $z \in Q^*$ with $zU \leq xU$ and $zU \leq yU$. Then $z^{-1}x, z^{-1}y \in R$, and this implies $xR \subseteq zR$ and $yR \subseteq zR$, or $xR + yR \subseteq zR$. Hence we have $cR = dxR + dyR \subseteq dzR$. Since $cR \subseteq dzR$, we have $(dz)^{-1}c = z^{-1}d^{-1}c \in R$, and this implies $zU \leq d^{-1}cU$. Thus $inf\{xU, yU\} = d^{-1}cU$. And this proves that G is a lattice ordered group. □

Lemma 5.14. *Let R be a Bezout domain. If $a, b \in R^*$, then $sup\{aU, bU\} \in R^*$ and if $sup\{aU, bU\} = qU$, then $qR = aR \cap bR$.*

Proof. Let $a, b \in R^*$ and let $qU = sup\{aU, bU\}$, where $q \in Q^*$. Then since $aU \leq qU$ and $bU \leq qU$, we have $a^{-1}q, b^{-1}q \in R$, so $q \in aR \cap bR$. Thus we have $q \in R^*$, and so $qR \subseteq aR \cap bR$. Let r be a nonzero element of $aR \cap bR$. Write $r = ar_1 = br_2$ where $r_1, r_2 \in R$. $rU = ar_1U = aU + r_1U \geq aU$. Similarly, $rU \geq bU$. Then $rU \geq qU$, which implies $q^{-1}r \in R$, and so $r \in qR$. Thus we have $qR = aR \cap bR$. □

Corollary 5.15. *Intersection of two principal ideals in a Bezout domain is principal. The converse is not true in general.*

As a counter example, let K be a field and let $R = k[X, Y]$, the polynomial ring over K with indeterminates X and Y. Intersection of any two principal ideal of R is principal but R is not a Bezout domain. By divisibility properties in R we know that $fR \cap gR = LCM\{f, g\}R$ for any $f, g \in R^*$. But the ideal (X, Y) is not principal but finitely generated, so R is not a Bezout domain.

Proposition 5.16. *Let G be the group of divisibility of R, let Q be the field of fractions of R and let $\Pi : Q^* \to G = Q^*/U$ be the canonical epimorphism and suppose that R is a Bezout domain. Then, there is a one-to-one order-preserving correspondence between the set of all proper ideals of R and the set of all segments of G. A proper ideal J of R corresponds to the segment $\Pi(J^*)$ of G. Under this correspondence, prime (respectively maximal) ideals correspond to prime (respectively maximal) segments.*

Proof. Set $\Psi : \mathscr{I}_R^* \to \mathscr{S}_G$ defined by $\Psi(I) = \Pi(I^*)$ for all $I \in \mathscr{I}_R^*$, and set $\Phi : \mathscr{S}_G \to \mathscr{I}_R^*$ defined by $\Phi(S) = \Pi^{-1}(S) \cup \{0\}$ for all $S \in \mathscr{S}_G$. We shall show that Ψ and Φ are well-defined and inverses of each other, then these mappings give us the desired correspondence.

First of all, we shall show that, for any nonzero ideal I of R, $\Psi(I)$ is a segment of G.

Let I be a nonzero proper ideal of R. Then $\Psi(I) = \Pi(I^*)$. Since $I^* \subset R^*$, then $\Psi(I) = \Pi(I^*) \subset \Pi(R^*) = G^+$.

Let $\Pi(a) = aU \in \Pi(I^*)$ and $qU \in G^+$ with $aU \leq qU$. Then $a^{-1}q \in R$. Since $a \in I^*$, then $a(a^{-1}q) = q \in I^*$, and so $\Pi(q) = qU \in \Pi(I^*)$.

Now, let $a, b \in I^*$. Then $\Pi(a) = aU, \Pi(b) = bU \in \Pi(I^*)$. Set $cR = aR + bR$ where $c \in R^*$. Since $a, b \in I^*$, then $aR, bR \subseteq I^*$ and so $cR \subseteq I^*$, thus $c \in I^*$. Now by Proposition 5.12, we have $\Pi(c) = cU = inf\{aU, bU\} \in \Pi(I^*)$.

Thus $\Psi(I) = \Pi(I^*)$ is a segment of G.

Secondly, we shall show that, for any nonempty segment S of G, $\Phi(S)$ is an ideal of R.

Let S be a nonempty segment of G. Then $\Phi(S) = \Pi^{-1}(S) \cup \{0\}$.

Let $a, b \in \Pi^{-1}(S)$ be nonzero, then $\Pi(a) = aU, \Pi(b) = bU \in S$. Set $cR = aR + bR$ with $c \in R^*$. By Proposition 5.12, $cU = inf\{aU, bU\}$ and since S is a segment, then we have $cU \in S$. Since $cR \supseteq (a+b)R$, then we have $(a+b)U \geq cU$. And again since S is a segment, we have $(a+b)U = \Pi(a+b) \in S$. Thus $a + b \in \Pi^{-1}(S)$.

Let $a \in \Pi^{-1}(S)$ be nonzero and $r \in R^*$. Then we have $\Pi(a) \in S$ and $\Pi(r) \in G^+$. Since we have $0 \leq \Pi(r)$, then by adding $\Pi(a)$ at both sides, we have $\Pi(a) \leq \Pi(a) + \Pi(r) = \Pi(ar)$. So because S is a segment of G, we have $\Pi(ar) \in S$ and so $ar \in \Pi^{-1}(S)$. Hence $\Phi(S)$ is an ideal of R.

Lastly, if $S = \emptyset$, then $\Phi(\emptyset) = \Pi^{-1}(\emptyset) \cup \{0\} = \{0\}$ is an ideal. And if $I = 0$, then $\Psi(0) = \Pi(\emptyset) = \emptyset$, is a segment.

Thus we have shown that both mappings are well-defined.

Let S be a segment of G. $\Psi(\Phi(S)) = \Psi(\Pi^{-1}(S) \cup \{0\}) = \Pi(\Pi^{-1}(S)) = S$, last equality holds since Π is surjective.

Let I be a proper ideal of R. $\Phi(\Psi(I)) = \Phi(\Pi(I^*)) = \Pi^{-1}(\Pi(I^*)) \cup \{0\}$.

Now we shall to show that $\Pi^{-1}(\Pi(I^*)) = I^*$ holds:

$I^* \subseteq \Pi^{-1}(\Pi(I^*))$ is a well-known fact in set theory, so we shall prove the converse inclusion. Let $a \in \Pi^{-1}(\Pi(I^*))$, then $\Pi(a) = aU \in \Pi(I^*)$. So there exists $b \in I^*$ such that $\Pi(a) = \Pi(b)$ or $aU = bU$. Then we have $a/b \in R$. Since $b \in I^*$, then we have $b(a/b) = a \in I^*$. Thus we have $\Pi^{-1}\big(\Pi(I^*)\big) = I^*$ and if we use this fact, we have $\Phi(\Psi(I)) = I^* \cup \{0\} = I$.

So Φ and Ψ are inverses of each other.

Now we shall show Ψ is order-preserving. Since Φ is its inverse, it also becomes order-preserving after this:

Let I, J be ideals of R such that $I \subseteq J$. Then we have $I^* \subseteq J^*$. Let $\Pi(a) \in \Pi(I^*)$ where $a \in I^*$, then we clearly have $a \in J^*$ and so $\Pi(a) \in \Pi(J^*)$. So $\Psi(I) = \Pi(I^*) \subseteq$

$\Psi(J) = \Pi(J^*)$. Thus both Ψ and Φ are order-preserving.

Now let P be a prime ideal of R. Our aim is to show that $\Psi(P) = \Pi(P^*)$ is a prime segment of G. Let $aU, bU \in G^+ \setminus \Pi(P^*)$. Then by the definition of G^+, we have $a, b \in R^* \setminus P^*$. Then since P^* is prime, we have $ab \in R^* \setminus P^*$. And hence $abU = aU + bU \in G^+ \setminus \Pi(P^*)$. So $\Psi(P)$ is a prime segment of G.

Let S be a prime segment of G. Our aim is to show that $\Phi(S) = \Pi^{-1}(S) \cup \{0\}$ is a prime ideal of R. Let $a, b \in R \setminus \Pi^{-1}(S)$ be nonzero, then $aU, bU \in G^+ \setminus S$. Since S is a prime segment, we have $aU + bU = abU \in G^+ \setminus S$. Since $abU \notin S$, then $ab \notin \Pi^{-1}(S)$. Since a and b are both nonzero and R is a domain, then $ab \neq 0$. So we have $ab \in R \setminus (\Pi^{-1}(S) \cup \{0\}) = R \setminus \Phi(S)$. Thus $\Phi(S)$ is a prime ideal of R.

After we showed that these mappings are order-preserving and the correspondence between proper ideals of R and segments of G, the correspondence between maximal ideals of R and maximal segments of G is straightforward by their definitions. □

Let G be the group of divisibility of R and suppose that R is a Bezout domain. Let $P \in Spec(R)$. Define H to be the subgroup of G generated by $G^+ \setminus \pi(P^*)$, i.e.,

$$\begin{aligned} H &= \left\{ \sum_{i=1}^{k} n_i g_i | k \in \mathbb{N}, n_i \in \mathbb{Z}, g_i \in G^+ \setminus \pi(P^*) \right\} \\ &= \{ g_1 - g_2 | g_1, g_2 \in G^+ \setminus \pi(P^*) \} \\ &= \{ g_1 - g_2 | g_1, g_2 \in \pi(R^* \setminus P^*) = \pi(R \setminus P) \} \\ &= \{ rU - sU | r, s \in R \setminus P \} \end{aligned}$$

G/H is an ordered group with the ordering given by

$$g_1 + H \geq g_2 + H \text{ if there exists } h \in H \text{ such that } g_1 - g_2 + h \geq 0.$$

Indeed, the only challenging part is anti-symmetry.

Suppose $g_1 + H \geq g_2 + H$ and $g_2 + H \geq g_1 + H$. Then there exist $h_1, h_2 \in H$ such that $g_1 - g_2 + h_1 \geq 0$ and $g_2 - g_1 + h_2 \geq 0$. By considering h_1, h_2 as differences of elements of $G^+ \setminus \pi(P^*)$, we may add suitable positive elements in G to have $h := h_1 = h_2 \geq 0$. So we have $g_1 - g_2 + h \geq 0$ and $g_2 - g_1 + h \geq 0$. Then we have $-h \leq g_1 - g_2 \leq h$.

Now our claim is that if $g \in G, h \in H^+$ be such that $-h \leq g \leq h$, then $g \in H$. For once this is proved, we have $g_1 - g_2 \in H$ and so $g_1 + H = g_2 + H$, which gives that the relation defined above is anti-symmetric, and so is an ordering.

Let $h \in H^+$, then $h \notin \pi(P^*)$, for otherwise, let $h \in \pi(P^*)$ and set $h = h_1 - h_2$, where $h_1, h_2 \in G^+ \setminus \pi(P^*)$. Then $h_1 = h + h_2 \geq h$ which implies $h_1 \in \pi(P^*)$, which is a contradiction.

Since we have $-h \leq g$, then $g + h \in G^+$. If $g + h \in \pi(P^*)$, then since $\pi(P^*)$ is a prime segment, we have either $g \in \pi(P^*)$ or $h \in \pi(P^*)$. Since $h \in H$ implies $h \notin \pi(P^*)$, and $g \leq h$ implies $g \notin \pi(P^*)$, then we must have $g + h \notin \pi(P^*)$. So $g + h \in G^+ \setminus \pi(P^*) \subseteq H$. Then we have $g = (g + h) - h \in H$, since both $g + h$ and h are elements of $G^+ \setminus \pi(P^*)$.

Proposition 5.17. *If P is a prime ideal of a Bezout domain R, then the group of divisibility of R_P is order-isomorphic to G_P.*

Proof. Let $G = Q^*/U$ be the group of divisibility of R, where Q is the field of fractions of R and U is the multiplicative group of units of R. Let U_P be the group of units in R_P, where $P \in Spec(R)$, and set $G' = Q^*/U_P$ be the group of divisibility of R_P. Set $\pi : Q^* \to Q^*/U$ be the canonical epimorphism.

Let $\Psi : \frac{G}{H} \to G' = \frac{R_P^*}{U_P}$ defined by $\Psi(aU + H) = aU_P$. Our aim is to show that Ψ is an order isomorphism.

First of all, we shall show that Ψ is well-defined.

Let $aU + H = bU + H \in G/H$, then $aU - bU \in H$, then $ab^{-1}U = rs^{-1}U$ for some $r, s \in R \setminus P$. Then $ab^{-1} = rs^{-1}u$ for some $u \in U$. Since $ru \in R \setminus P$ and $s \in R \setminus P$, then $ab^{-1} \in U_P$, so $aU_P = bU_P$. Thus Ψ is well-defined.

Ψ is clearly surjective, now we shall show Ψ is injective.

Let $aU_P = bU_P$, so we have $ab^{-1} \in U_P$, and so $a, b \in R \setminus P$. Since $aU, bU \in \pi(R \setminus P)$, then $(ab^{-1})U = aU - bU \in H$, so $aU + H = bU + H$. Hence Ψ is injective.

To see that Ψ is a homomorphism, let $aU + H, bU + H \in G/H$.

$\Psi\left((aU + H) + (bU + H)\right) = \Psi(abU + H) = abU_P = aU_P + bU_P = \Psi(aU + H) + \Psi(bU + H)$.

Now let $aU + H, bU + H \in G/H$ be such that $aU + H \leq bU + H$. Then there exists $h \in H$ such that $bU - aU + h \geq 0$, since $h \in H$, then there exist $r, s \in R \setminus P$ such that $h = rU - sU$. So we have $bU - aU + rU - sU \geq 0$, which implies $\frac{br}{as}U \geq 0$, hence $\frac{br}{as} \in R$. Since $R \subseteq R_P$, then $\frac{br}{as} \in R_P$, and since $\frac{r}{s} \in U_P$, then we have $\frac{b}{a} = \frac{br}{as} \cdot \frac{s}{r} \in R_P$. And this gives that $aU_P \leq bU_P$. Thus Ψ is order-preserving. Since Ψ is an isomorphism, Ψ^{-1} is also order-preserving.

Lastly, we shall show that $\Psi(inf\{aU+H, bU+H\}) = inf\{\Psi(aU+H), \Psi(bU+H)\}$ for all $aU+H, bU+H \in G/H$.

Set $cU+H = inf\{aU+H, bU+H\}$.Then our claim is that $\Psi(cU+H) = cU_P = inf\{\Psi(aU+H), \Psi(bU+H)\}$.

$cU+H \leq aU+H$ implies that $\frac{ar_1}{cs_1} \in R$ for some $r_1, s_1 \in R \backslash P$, and $cU+H \leq bU+H$ implies that $\frac{br_2}{cs_2} \in R$ for some $r_2, s_2 \in R \setminus P$.

So we have

$$\frac{a/s_1}{c/r_1}, \frac{b/s_2}{c/r_2} \in R \subseteq R_P$$

This gives that $(\frac{c}{r_1})U_P \leq (\frac{a}{s_1})U_P$ and $(\frac{c}{r_2})U_P \leq (\frac{b}{s_2})U_P$.

$(\frac{c}{r_1})U_P \leq (\frac{a}{s_1})U_P$ implies that $cU_P - r_1U_P \leq aU_P - s_1U_P$, so we have $cU_P - aU_P \leq r_1U_P - s_1U_P = (r_1/s_1)U_P = U_P$, hence $cU_P \leq aU_P$. Similarly, we have $cU_P \leq bU_P$.

Now if $xU_P \leq aU_P$ and $xU_P \leq bU_P$, then $\Psi(xU+H) \leq \Psi(aU+H)$ and $\Psi(xU+H) \leq \Psi(bU+H)$. Since Ψ^{-1} is order-preserving, then $xU+H \leq aU+H$ and $xU+H \leq bU+H$, so $xU+H \leq cU+H$ since $cU+H = inf\{aU+H, bU+H\}$. Now since Ψ is order-preserving, we have $xU_P = \Psi(xU+H) \leq \Psi(cU+H) = cU_P$. Hence $cU_P = inf\{\Psi(aU+H), \Psi(bU+H)\}$. □

Proposition 5.18. *Let $\{G_\alpha\}_{\alpha\in\Gamma}$ be a family of lattice ordered groups, and let $G = \bigoplus_{\alpha\in\Gamma} G_\alpha$ be ordered with product ordering. Set $\pi_\alpha : G \to G_\alpha$ be the canonical epimorphism for all $\alpha \in \Gamma$. If $P \in Spec(G)$, then either $P = \emptyset$ or there exists $\alpha \in \Gamma$ and $P_\alpha \in Spec(G_\alpha)$ such that $P = G^+ \cap \pi_\alpha^{-1}(P_\alpha)$.*

Proof. There exists $\alpha \in \Gamma$ such that $\pi_\alpha(x) \neq 0$ for all $x \in P$. For otherwise, suppose that for all $\alpha_i \in \Gamma$, there exists $x_i \in P$ such that $\pi_{\alpha_i}(x_i) = 0$. Since P is a segment of G, then $inf\{x_i\} = 0 \in P$, which is a contradiction. Thus such an $\alpha \in \Gamma$ exists.

Set $P_\alpha = \pi_\alpha(P)$. Our aim is to show that $P_\alpha \in Spec(G_\alpha)$ and $P = G^+ \cap \pi_\alpha^{-1}(P_\alpha)$.

First of all, we need to show that P_α is a segment of G_α.

Clearly, π_α is order-preserving. We know that $P_\alpha = \pi_\alpha(P)$ and by the way we choose α, $0 \notin P_\alpha$, so $P_\alpha \subset G_\alpha^+$.

Let $x \in P_\alpha, y \in G_\alpha$ be such that $y > x$. Set $\tilde{x}, \tilde{y} \in G$ be such that $\pi_\alpha(\tilde{x}) = x$, $\pi_\alpha(\tilde{y}) = y$ and $\pi_\gamma(x) = \pi_\gamma(y)$ for all $\gamma \neq \alpha$. Then clearly $\tilde{x} \in P$, $\tilde{y} \in G$ and $\tilde{y} > \tilde{x}$. Since P is filtered, then $\tilde{y} \in P$, and so $\pi_\alpha(\tilde{y}) = y \in P_\alpha$. Thus P_α is filtered.

Let $x, y \in P_\alpha$. Our aim is to show that $inf\{x, y\} \in P_\alpha$. Let $\tilde{x}, \tilde{y} \in P$ be such that $\pi_\alpha(\tilde{x}) = x$ and $\pi_\alpha(\tilde{y}) = y$. Since P is a segment, then $inf\{\tilde{x}, \tilde{y}\} \in P$. We have $inf\{x, y\} = inf\{\pi_\alpha(\tilde{x}), \pi_\alpha(\tilde{y})\} = \pi_\alpha(inf\{\tilde{x}, \tilde{y}\}) \in \pi_\alpha(P) = P_\alpha$. So P_α is a segment of G_α.

Now let $x, y \in G_\alpha^+ \setminus P_\alpha$. Then there exist $\tilde{x}, \tilde{y} \in G^+ \setminus P$ such that $\pi_\alpha(\tilde{x}) = x$ and $\pi_\alpha(\tilde{y}) = y$. Since $P \in Spec(G)$, then $\tilde{x}+\tilde{y} \in G^+ \setminus P$, and so $\pi_\alpha(\tilde{x}+\tilde{y}) = \pi_\alpha(\tilde{x}) + \pi_\alpha(\tilde{y}) = x + y \in \pi_\alpha(G^+ \setminus P) = G_\alpha^+ \setminus P_\alpha$. Thus $P_\alpha \in Spec(G_\alpha)$.

Now we shall prove that $P = G^+ \cap \pi_\alpha^{-1}(P_\alpha)$. We know that $P \subseteq G^+ \cap \pi_\alpha^{-1}(P_\alpha)$. We suppose by the way of contradiction that $P \subset G^+ \cap \pi_\alpha^{-1}(P_\alpha)$.

Let $x \in (G \cap \pi_\alpha^{-1}(P_\alpha)) \setminus P$. Then $x \in G^+$ and $\pi_\alpha(x) \in P_\alpha = \pi_\alpha(P)$. So there exists $y \in P$ such that $\pi_\alpha(x) = \pi_\alpha(y)$.

Now let $y_1, y_2 \in G$ be such that $\pi_\gamma(y_1) = y$ for $\gamma \neq \alpha$, and $\pi_\alpha(y_1) = 0$, and $y_2 = y - y_1$. Since $y = y_1 + y_2 \in P$ and P is a prime segment of G, then either $y_1 \in P$ or $y_2 \in P$. If $y_1 \in P$, then $\pi_\alpha(y_1) = 0 \in \pi_\alpha(P) = P_\alpha$, which is a contradiction, then we have $y_2 \in P$. In this case, we have $\pi_\alpha(x) = \pi_\alpha(y_2)$, and all other components of y_2 are zero. Then we have $y_2 \leq x$. So $y_2 \in P$ implies $x \in P$, which is again a contradiction. Thus such an x doesn't exist. Hence we have $P = G^+ \cap \pi_\alpha^{-1}(P_\alpha)$. □

Proposition 5.19. *Let G be a lattice ordered group. Then every segment of G is contained in a maximal segment.*

Proof. Let Γ be the set of segments of G such that, for $S \in \Gamma$, S is not contained in a maximal segment. Our aim is to show that $\Gamma = \emptyset$ by using Zorn's Lemma.

Suppose $\Gamma \neq \emptyset$. Let $S_{\alpha_1} \subseteq S_{\alpha_2} \subseteq \ldots$ be a chain of segments in Γ. Then $S = \bigcup\limits_{\alpha_i} S_{\alpha_i}$ is a segment of G:

If $S = G^+$, then $0 \in S = \bigcup\limits_{\alpha_i} S_{\alpha_i}$, so $0 \in S_{\alpha_j}$ for some j, which contradicts with the fact that S_{α_j} is a segment. So $S \subset G^+$.

Let $x \in S, y \in G^+$ be such that $y > x$. Since $s \in S$, then there exist j such that $x \in S_{\alpha_j}$, and since S_{α_j} is a segment of G, then $y \in S_{\alpha_j} \subseteq S$.

Let $x, y \in S$, then there exist j, k such that $x \in S_{\alpha_j}$ and $y \in S_{\alpha_k}$. Then we have either $x, y \in S_{\alpha_j}$ or $x, y \in S_{\alpha_k}$. It is clear that, in both cases we have $inf\{x, y\} \in S$.

Now if $S \notin \Gamma$, then S contained in a maximal segment M. In this case, all S_{α_i}'s are contained in that maximal segment M, which is a contradiction. So we must have $S \in \Gamma$.

By Zorn's Lemma, Γ has a maximal element, say T. T is not a maximal segment since $T \in \Gamma$, so there exist a segment T' of G such that $T \subseteq T'$. Since T is maximal in Γ, then $T' \notin \Gamma$ and hence contained in a maximal segment M'. This is again contradiction, since we have that $T \subseteq T' \subseteq M'$. So our assumption that $\Gamma \neq \emptyset$ is false, and every segment of G contained in a maximal segment. □

Proposition 5.20. *If G is a lattice ordered group with unique maximal segment, then G is totally ordered.*

Proof. Let M be the unique maximal segment of G. Let $a \in G^+ \setminus \{0\}$. Set $S_a = \{x \in G^+ | x \geq a\}$. Our claim is that, S_a is a segment of G:

Since $a \in G^+ \setminus \{0\}$, then $a > 0$ and so $0 \notin S_a$, which implies $S_a \subset G^+$.

Let $x \in S_a, y \in G^+$ with $y > x$. Then $y > x \geq a$, implies that $y \in S_a$.

Let $x, y \in S_a$, then we have that $x \geq a$ and $y \geq a$, so $inf\{x, y\} \geq a$, which gives that $inf\{x, y\} \in S_a$.

So S_a is a segment of G. Then by Proposition 5.19, S_a is contained in a maximal segment, in this case, the unique maximal segment M.

We have that for any $a \in G^+ \setminus \{0\}$, $a \in S_a \subseteq M$, hence $G^+ \setminus \{0\} = M$.

Now let $x \in G$. Then by Theorem 5.4, $x = y - z$ for some $y, z \in G^+$ with $inf\{y, z\} = 0$. If $y, z \in G^+ \setminus \{0\} = M$, then since M is a segment, we have $inf\{y, z\} = 0 \in M$, which is impossible. So either $y = 0$ or $z = 0$. If $y = 0$, then $x \in G^-$, if $z = 0$, then $x \in G^+$. Since every element of G is either positive or negative, then G is totally ordered. □

Lemma 5.21. *Let $\{G_i\}_{i \in I}$ be a family of totally ordered groups. Let $v_i : Q^* \to G_i$ be valuations on Q. Then $v = \prod\limits_{i \in I} v_i : Q^* \to v(Q^*) \subseteq \prod\limits_{i \in I} G_i$ is a valuation.*

Proof. Let $x, y \in Q^*$. Then

$$\begin{aligned} v(xy) &= (v_i(xy))_{i \in I} \\ &= (v_i(x) + v_i(y))_{i \in I} \\ &= (v_i(x))_{i \in I} + (v_i(y))_{i \in I} \\ &= v(x) + v(y) \end{aligned}$$

and

$$\begin{aligned} v(x+y) &= (v_i(x+y))_{i\in I} \\ &\geq (min\{v_i(x), v_i(y)\})_{i\in I} \\ &= min\left\{(v_i(x))_{i\in I}, (v_i(y))_{i\in I}\right\} \\ &= min\left\{v(x), v(y)\right\} \end{aligned}$$

Hence $v = \prod\limits_{i\in I} v_i$ is a valuation. □

Theorem 5.22 (***Krull-Kaplansky-Jaffard-Ohm***). *If G is a lattice ordered group, then there exists a Bezout domain whose group of divisibility is lattice isomorphic to G.*

Proof. Let G be a lattice ordered group and let Γ be the set of maximal segments of G. By Corollary 5.7 G_M is a totally ordered group for every $M \in \Gamma$. Then

$$f = \prod_{M\in\Gamma} f_M : G \longrightarrow \prod_{M\in\Gamma} G_M = G'$$

is a lattice embedding of G into G', where G' has the product ordering:

We know that $H_M = \{g_1 - g_2 | g_1, g_2 \in G^+ \setminus M\}$. Let $x \in H_M$, then $x = g_1 - g_2$ for some $g_1, g_2 \in G^+ \setminus M$. Since $x \leq g_1$, then $x \notin M$.

If $x \in \bigcap\limits_{M\in Max(G)} H_M$, then $x \notin M$ for all $M \in Max(G)$. Since for all $x \in G^+ \setminus \{0\}$, $S_x = \{g \in G | g \geq x\}$ is a segment of G and must contained in a maximal segment, then we have $x = 0$. Thus $\bigcap\limits_{M\in Max(G)} H_M = 0$.

Hence the kernel of the homomorphism f is zero, and so f is an embedding.

Let π_M be the canonical projection of G' into G_M, for all $M \in \Gamma$. Let k be a field and let $\{Y_g | g \in G\}$ be a set of indeterminates over k, indexed by G. Let $Q = k\left(\{Y_g\}_{g\in G}\right)$. We shall define a valuation $v_M : Q^* \to G_M$.

First, consider monomials in S^*, where $S = k\left[\{Y_g\}_{g\in G}\right]$ and define

$$v_M(cY_{g_1}^{n_1} Y_{g_2}^{n_2} \ldots Y_{g_r}^{n_r}) = \sum_{i=1}^{r} n_i (\pi_M \circ f)(g_i)$$

where $c \in k^*, g_i \in G$ and $n_i \in \mathbb{Z}^+$. For any $p \in S^*$, we define $v_M(p)$ to be the infimum of $v_M(m_i)$'s where the m_i's are distinct monomials which appear in p. With these definitions, we have v_M satisfies the following properties:

1. $v_M(pq) = v_M(p) + v_M(q)$

2. $v_M(p+q) \geq min\{v_M(p), v_M(q)\}$

Let $p, q \in S$. Then $v_M(pq) = inf\{v_M(m_in_j)\}$, where m_i's and n_j's are distinct monomials respectively in p and q. We clearly have $v_M(p) = v_M(m_{i_0})$ and $v_M(q) = v_M(n_{j_0})$ for some i_0 and j_0. We have $v_M(m_{i_0}) + v_M(n_{j_0}) = v_m(m_{i_0}n_{j_0})$ since $v_M(cY_{g_1}^{n_1}Y_{g_2}^{n_2} \ldots Y_{g_r}^{n_r}) = \sum_{i=1}^{r} n_i(\pi_M \circ f)(g_i) = \sum_{i=1}^{r} n_i\, f_M(g_i)$. Then $v_M(pq) = inf\{v_M(m_in_j)\} = inf\{v_M(m_i) + v_M(n_j)\} = inf\{v_M(m_i)\} + inf\{v_M(n_j)\} = v_M(p) + v_M(q)$.

Let $p, q \in S$. Our aim is to show that $v_M(p + q) \geq min\{v_M(p), v_M(q)\}$. Set $v_M(p+q) = v_M(s_i)$ where $s_i$is one of the monomials in $p+q$. Since s_i is a monomial in p, in q or in both, we have that $v_M(p) \leq v_M(s_i), v_M(q) \leq v_M(s_i)$ or both. This clearly implies that $v_M(p + q) \geq min\{v_M(p), v_M(q)\}$.

Now for $p, p' \in S^*$, we let

$$v_M(\frac{p}{p'}) = v_M(p) - v_M(p')$$

This defines $v_M : Q^* \to G_M$, which is a valuation by Lemma 5.9. Now, define $v : Q^* \to G'$ by $v = \prod_{M \in \Gamma} v_M$. Then v is a valuation by Lemma 5.21.

Let $R = \{x \in Q^* | v(x) \geq 0\} \cup \{0\}$. Then R is an integral domain with field of fractions Q and with divisibility group $v(Q^*)$. Note that if $g \in G$, then $v(Y_g) = f(g)$, and so $f(G) \subseteq v(Q^*)$. Now let $p/p' \in Q^*$, then $v(p/p') = v(p) - v(p')$. Since $v_M(cY_{g_1}^{n_1} \ldots Y_{g_r}^{n_r}) = \sum_{i=1}^{r} n_i\, \pi_M \circ f(g_i)$, then $v(cY_{g_1}^{n_1} \ldots Y_{g_r}^{n_r}) = \sum_{i=1}^{r} n_i\, f(g_i) = f\left(\sum_{i=1}^{r} n_i g_i\right) \in f(G)$. Thus $v(Q^*) = f(G) \cong G$. Thus the group of divisibility of R is lattice isomorphic to G.

Now it remains to show that R is a Bezout domain. To this aim, we shall show that if $x, x' \in R$ with $x \neq x'$, then the ideal (x, x') is principal.

Let $x \in R^*$. Then $v(x) = f(g) \geq 0$ for some $g \in G$. Notice that $v(cY_{g_1}^{n_1} \ldots Y_{g_r}^{n_r}) = \sum_{i=1}^{r} n_i\, f(g_i) = f\left(\sum_{i=1}^{r} n_i g_i\right)$, and the valuation of any element in Q^* is a difference of such elements.

Let $x' \in R^*$ with $x \neq x'$, for which $v(x') = f(g') \geq 0$ where $g' \in G$. Since $v(x) = v(Y_g)$ and $v(x') = v(Y_{g'})$, x/Y_g and $x'/Y_{g'}$ are unit elements of R. Then $(x, y) = (Y_g, Y_{g'})$. If $f(g) \geq f(g')$, then $Y_g/Y_{g'} \in R$, and so $(Y_g, Y_{g'}) = (Y_{g'})$. Similarly, if $f(g) \leq f(g')$, then $(Y_g, Y_{g'}) = (Y_g)$. Otherwise, $inf\{f(g), f(g')\} < f(g)$ and $inf\{f(g), f(g')\} < f(g')$, and so $(Y_g, Y_{g'}) = (Y_g + Y_{g'})$ since $Y_g/(Y_g + Y_{g'}), Y_{g'}/(Y_g + Y_{g'}) \in R$. In any case, we have $(x, y) = (Y_g, Y_{g'})$ is principal, and R is a Bezout domain. □

6 TWO EXAMPLES OF ALMOST DEDEKIND DOMAINS

6.1 A Bezout Domain Example

Proposition 6.1. *Let G, H be lattice ordered groups and let $\phi : G \to H$ be a surjective lattice homomorphism. Then there is a correspondence between the prime segments P of G with $P \cap Ker\phi = \emptyset$ and the prime segments of H given by*

$$\begin{array}{ccc} \{P \in Spec(G) | P \cap Ker\phi = \emptyset\} & \longleftrightarrow & Spec(H) \\ P & \xrightarrow{\Phi} & \phi(P) \\ \phi^{-1}(\mathcal{P}) \cap G^{+} & \xleftarrow{\Psi} & \mathcal{P} \end{array}$$

Moreover, we have $\Psi(\Phi(P)) = P$ for $P \in Spec(G)$ with $P \cap Ker\phi = \emptyset$, and $\Phi(\Psi(\mathcal{P})) = \mathcal{P}$ for $\mathcal{P} \in Spec(H)$.

Proof. We denote $\{P \in Spec(G) | P \cap Ker\phi = \emptyset\}$ by $Spec'(G)$.
Let $P \in Spec'(G)$. Our aim is to show that $\phi(P) \in Spec(H)$.
First of all we shall show that $\phi(P)$ is a segment of H.
Since $P \cap Ker\phi = \emptyset$, then $0 \notin \phi(P)$, and since ϕ is an order homomorphism, then we have $\phi(P) \subset H^{+}$.
Let $\phi(p) \in \phi(P)$ and $h \in H$ be such that $\phi(p) < h$. Since ϕ is surjective, then there exists $g \in G$ such that $\phi(g) = h$, so we have $\phi(p) < \phi(g)$. If $g \leq p$, then we must have $\phi(g) \leq \phi(p)$, so we have that $p < g$. Since $p \in P$ and P is a segment, last inequality implies that $g \in P$ and so $\phi(g) = h \in \phi(P)$.
Now let $\phi(x), \phi(y) \in \phi(P)$, where $x, y \in P$. $x, y \in P$ implies that $inf\{x, y\} \in P$, and since ϕ is a lattice homomorphism, then $inf\{\phi(x), \phi(y)\} = \phi(inf\{x, y\}) \in \phi(P)$.
Thus $\phi(P)$ is a segment of H.
Now we shall show that $\phi(P)$ is a prime segment.
Let $x + y \in \phi(P)$, set $x + y = \phi(p)$ for some $p \in P$. Since ϕ is surjective, then $x = \phi(g_1), y = \phi(g_2)$ for some $g_1, g_2 \in G$. If we set $g = inf\{g_1 + g_2, p\}$, then $\phi(g) = \phi(inf\{g_1 + g_2, p\}) = inf\{\phi(g_1 + g_2), \phi(p)\} = inf\{x + y, x + y\} = x + y$. Then $\phi(p - g) = \phi(p) - \phi(g) = 0$, hence $p - g \in Ker\phi$, and this implies that $p - g \notin P$. Since $p = (p - g) + g \in P$ and $P \in Spec(G)$, then we have $g \in P$. Since $g \leq g_1 + g_2$, then

$g_1 + g_2 \in P$. Again, since $P \in Spec(G)$, then we have either $g_1 \in P$ or $g_2 \in P$. So we have either $x = \phi(g_1) \in \phi(P)$ or $y = \phi(g_2) \in \phi(P)$. Hence $\phi(P) \in Spec(H)$.

Now let $\mathcal{P} \in Spec(H)$. Our aim is to show that $P := \phi^{-1}(\mathcal{P}) \cap G^+ \in Spec'(G)$.

First of all we shall show that P is a segment of G. Clearly $P \subseteq G^+$and if $0 \in P$, then $0 = \phi(0) \in \phi(P) \subseteq \mathcal{P}$, and this contradicts with the fact that $\mathcal{P}$ is a segment of H. Then we have $P \subset G^+$.

Let $x \in P, y \in G$ with $0 < x < y$. Then $\phi(x) \leq \phi(y)$ and since $\phi(x) \in \phi(P) \subseteq \mathcal{P}$, so $\phi(x) > 0$. Then $\phi(y) > 0$, and this implies $y \notin Ker\phi$. Since $y < 0$ implies $\phi(y) \leq 0$, then we have $y \in \phi^{-1}(\mathcal{P}) \cap G^+ = P$.

Let $x, y \in P$. Our aim is to show that $inf\{x, y\} \in P$.

Since $x, y \in G^+$, we have $inf\{x, y\} \in G^+$. So it suffices to show that $\phi\left(inf\{x, y\}\right) \in \mathcal{P}$. $\phi(inf\{x, y\}) = inf\{\phi(x), \phi(y)\}$, and since $\phi(x), \phi(y) \in \mathcal{P}$ and $\mathcal{P}$ is a segment of H, then $inf\left\{\phi(x), \phi(y)\right\} = \phi\left(inf\{x, y\}\right) \in \mathcal{P}$.

Hence $P = \phi^{-1}(\mathcal{P}) \cap G^+$ is a segment of G.

Clearly $P \cap Ker\phi = \emptyset$, for otherwise $0 \in \phi(P)$ implies that $0 \in \mathcal{P}$, which is impossible.

Now we shall show that $P \in Spec(G)$.

Let $g_1, g_2 \in G^+$ with $g_1 + g_2 \in P$, so we have $\phi(g_1 + g_2) = \phi(g_1) + \phi(g_2) \in \mathcal{P}$, since $\mathcal{P} \in Spec(H)$, then either $\phi(g_1) \in \mathcal{P}$ or $\phi(g_2) \in \mathcal{P}$, and this implies $g_1 \in \phi^{-1}(\mathcal{P})$ or $g_2 \in \phi^{-1}(\mathcal{P})$. So we have that $g_1 \in P$ or $g_2 \in P$, hence $P \in Spec(G)$.

Now we show that Ψ and Φ are inverses of each other.

Let $P \in Spec'(G)$. We first show that $\Psi(\Phi(P)) = \phi^{-1}(\phi(P)) \cap G^+ = P$.

It is well-known in set theory that $P \subseteq \phi^{-1}(\phi(P))$ and since $P = P \cap G^+$, then $P \subseteq \phi^{-1}(\phi(P)) \cap G^+$. So we shall prove the reverse inclusion. Let $g \in G^+$ with $\phi(g) \in \phi(P)$. Then there exists $p \in P$ such that $\phi(p) = \phi(g)$. So we have $g - p \in Ker\phi$. Set $g' = inf\{g, p\}$. $\phi(g') = \phi(inf\{g, p\}) = inf\{\phi(g), \phi(p)\} = \phi(g) = \phi(p)$. Then $p - g' \in Ker\phi \cap G^+ \subseteq G^+ \setminus P$. Since $p = (p - g') + g'$ and $P \in Spec'(G)$, then $p - g' \notin P$, so $g' \in P$. With the fact that $g' \leq g$, we have $g \in P$. Hence $P = \Psi(\Phi(P)$.

Let $\mathcal{P} \in Spec(H)$. We show that $\Phi(\Psi(\mathcal{P})) = \phi(P) = \mathcal{P}$, where $P = \phi^{-1}(\mathcal{P}) \cap G^+$. Clearly $\phi(P) \subseteq \mathcal{P}$. Now let $h \in \mathcal{P}$. Since ϕ is surjective, then $h = \phi(g)$ for some $g \in G$. Clearly $h = \phi(g) \in H^+$. Set $g^+ = sup\{g, 0\}$ and $g^- = -inf\{g, 0\}$. Then we have that $g = g^+ - g^-$, where $g^+, g^- \in G^+$. Now $h = \phi(g) = \phi(g^+) - \phi(g^-) \in \mathcal{P}$.

$\phi(g^-) = \phi(-inf\{g, 0\}) = -inf\{\phi(g), 0\} = 0$, then we have $\phi(g) = \phi(g^+) \in \mathcal{P}$. So $g^+ \in$

$\phi^{-1}(\mathcal{P}) \cap G^+ = P$, which implies that $h = \phi(g^+) \in \phi(P)$. Hence $\mathcal{P} = \Phi(\Psi(\mathcal{P}))$. $\square$

Example 6.2. Let $N = \{1, 2, 3, \ldots\}$ and $\mathbb{Z}^+ = \{0, 1, 2, \ldots\}$.

Let G be the group of all sequences of elements of $\mathbb{Z}^+$ indexed by N such that all components are constant after some integer n. We shall call the constant part of such an element f of G by the infinite block of f, and denote by f_∞. G is a lattice ordered group with the ordering $f \leq g$ if and only if $f_i \leq g_i$ for all $i \in N$.

Let $P_i = \{f \in G^+ | f_i > 0\}$ and $P_\infty = \{f \in G^+ | \exists n \in N, \forall i > n, f_i > 0\} = \{f \in G^+ | f_\infty > 0\}$.

We first show that for arbitrary $i \in N$, P_i and P_∞ are prime segments of G. Let $i \in N$.

Clearly, $0 \notin P_i$ and $0 \notin P_\infty$ so by definitions, we have $P_i, P_\infty \subset G^+$.

Let $f \in P_i, g \in G$ with $f \leq g$, then $0 < f_i \leq g_i$, and so $g \in P_i$. Let $f \in P_\infty, g \in G$ with $f \leq g$, then $0 < f_\infty \leq g_\infty$ implies that $g \in P_\infty$.

If $f, g \in P_i$, then $f_i, g_i > 0$. Then $inf\{f_i, g_i\} = min\{f_i, g_i\} > 0$, hence $(inf\{f, g\})_i > 0$ and this implies $inf\{f, g\} \in P_i$.

If $f, g \in P_\infty$, then $f_\infty > 0$ and $g_\infty > 0$. Then we have that $(inf\{f, g\})_\infty = inf\{f_\infty, g_\infty\} = min\{f_\infty, g_\infty\} > 0$, and this implies that $inf\{f, g\} \in P_\infty$. So P_i and P_∞ are segments of G.

Now let $f, g \in G^+ \setminus P_i$, then $f_i = g_i = 0$, so $(f+g)_i = f_i + g_i = 0$. Let $j \in N$ with $j \neq i$, then since $f_i, g_i \geq 0$ we have $(f+g)_i = f_i + g_i \geq 0$. Thus $f + g \in G^+ \setminus P_i$. Hence P_i is a prime segment.

Let $f, g \in G^+$ such that $f+g \in P_\infty$, our aim is to show that either $f \in P_\infty$ or $g \in P_\infty$. Suppose that $f \notin P_\infty$, then $f_\infty = 0$. Since we know that $0 < (f+g)_\infty = f_\infty + g_\infty = g_\infty$, then $g \in P_\infty$. Thus P_i and P_∞ are prime segments of G. Note that for $i, j \in N \cup \{\infty\}$ with $i \neq j$ we have $P_i \not\subseteq P_j$ since if $f \in G^+$ with $f_i > 0$ and $f_j = 0$, then $f \in P_i \setminus P_j$.

Let Q be a segment of G, our claim is that Q is contained in either P_∞ or one of the P_i's:

Suppose by the way of contradiction that $Q \not\subseteq P_i$ for all $i \in N$ and $Q \not\subseteq P_\infty$. Since for $i \in N$, $Q \not\subseteq P_i$, then there exists $f^i \in Q$ such that $f^i \notin P_i$, i.e., $(f^i)_i = 0$. Since $Q \not\subseteq P_\infty$, then there exists $f \in Q$ such that $f_\infty = 0$, i.e., there exists $n \in N$ such that for all $i > n$, $f_i = 0$. Now since $f, f^1, \ldots, f^n \in Q$, then $inf\{f, f^1, \ldots, f^n\} = 0 \in Q$, which is impossible. Thus our claim is true.

Since P_i's and P_∞ are prime segments of G, for which they do not contain each other, and every other segment must be included by at least one of them. Then these are the only maximal segments of G.

Now define $\phi_i : G \to \mathbb{Z}, i = 1, 2, \ldots, \infty$ defined by $\phi_i(f) = f_i, i = 1, 2, \ldots$ and $\phi_\infty(f) = f_\infty$. All ϕ_i's are lattice homomorphisms of G onto $\mathbb{Z}$. Now we shall show that $\mathbb{Z}$ has unique prime segment $\mathbb{Z}^+ \setminus \{0\}$. Let S be a prime segment of $\mathbb{Z}$. Then S has a minimum element x, our aim is to show that $x = 1$. Suppose that, by the way of contradiction, $x > 1$. Then we have $x - 1, 1 \in \mathbb{Z}^+$. Since $(x-1) + 1 = x \in S$, then either we have $x - 1 \in S$ or $1 \in S$. Both cases contradicts with the minimality of x in S. Hence we must have $x = 1$, and so $S = \mathbb{Z}^+ \setminus \{0\}$.

Since $\mathbb{Z}$ has unique prime segment, it follows from the correspondence between prime segments under a lattice homomorphism defined above, P_i contains no prime segment properly. Thus P_i's are the only prime segments of G for $i = 1, 2, \ldots, \infty$; and for $i = 1, 2, \ldots, \infty$, G_{P_i}'s are order isomorphic to $\mathbb{Z}$.

Now we shall show that $f = 1 \in G$ has infinitely many minimal prime divisors:

Clearly, since $f_i > 0$ for all $i = 1, 2, \ldots \infty$, we have that $f \in P_i$ for all $i = 1, 2, \ldots, \infty$. Since we have shown that for $i \neq j$, $P_i \not\subseteq P_j$ for $i, j = 1, 2, \ldots, \infty$, then all P_i's are the minimal prime divisors of $f = 1$, and this implies that G is not Noetherian.

By Theorem 5.22 there exists a Bezout domain R, whose group of divisibility is lattice isomorphic to G. Let I be the ideal of R which corresponds to $f = 1$ under the correspondence given by Proposition 5.16. Let $\bar{P_i}$ and $\bar{P_\infty}$ be ideals of R which correspond to P_i and P_∞ for all $i \geq 1$, respectively. Then we have $I \subseteq \bar{P_i}$ for all $i \geq 1$ and $I \subseteq \bar{P_\infty}$. Moreover we have $\bar{P_i} \not\subseteq \bar{P_j}$ for $i = 1, 2, \ldots, \infty$. Hence $\{\bar{P_i}\}_{i=1}^{\infty}$ is the set of minimal prime ideals of I, and since I has infinitely minimal prime divisors, then R is not Noetherian. The correspondence of Proposition 5.16 clearly holds between the ideals and segments of localizations of R and G, hence we have each localization $R_{\bar{P_i}}$ is also order isomorphic to $\mathbb{Z}$, hence the Bezout domain R is an almost Dedekind domain.

6.2 An Example in Algebraic Integers

We give another example of an almost Dedekind domain which consists of algebraic integers. The idea of construction is based on starting from an almost Dedekind (or Dedekind) domain D_0 (which will be $\mathbb{Z}$ in our case) with field of fractions K_0 and considering an algebraic extension K of K_0 which is expressed as the union of an ascending net $\{K_\lambda\}_{\lambda\in\Lambda}$ of intermediate fields, each of which is finite over K_0. Then we form the ring $D = \bigcup\limits_{\lambda\in\Lambda} D_\lambda$, where D_λ denotes the integral closure of D_0 in K. Note that D is the integral closure of D_0 in K. If we fix a maximal ideal P of D and set $P_\lambda = P \cap D_\lambda$, then there are only a finite number of maximal ideals of D_λ lying over $P_0 = P \cap D_0$, and P_λ is one of them, and P_0D_λ is a finite product of powers of the maximal ideals of D_λ containing P_0. Assume that P_λ occurs as a factor of P_0D_λ to the exponent e_λ. One important result in [13] (see Corollary 42.2) says that if the set $\{e_\lambda\}$ is bounded for every maximal ideal P of D, then D is an almost Dedekind domain. We shall use this result (without giving a proof) in Example 6.5 below. Before giving Example 6.5, we need the following two results.

Lemma 6.3. *Let R be a ring. Let $\{A_1, \ldots A_n\}$ be a set of pairwise comaximal ideals of R. Then for any finite subset $\{f_1, \ldots f_n\}$ of $R[X]$, where every f_i is monic of degree k, there exists a monic polynomial $f \in R[X]$ of degree k such that $f \equiv f_i \pmod{A_i[X]}$ for every $i = 1, \ldots, n$.*

Proof. We use induction on n. Let $n = 2$. Since A_1 and A_2 are comaximal, we may pick $a_1 \in A_1$, $a_2 \in A_2$ such that $a_1 + a_2 = 1$. Letting

$$f = a_2f_1 + a_1f_2,$$

we obtain that f is monic of degree k,

$$f - f_1 = (a_2 - 1)f_1 + a_1f_2 = a_1(f_2 - f_1) \in A_1[X],$$

and

$$f - f_2 = a_2(f_1 - f_2) \in A_2[X].$$

Now assume that there exists a monic polynomial $g \in R[X]$ of degree k such that $g \equiv f_i \pmod{A_i[X]}$ for $i = 1, \ldots, n-1$. Then since $A_1 \ldots A_{n-1}$ and A_n are comaximal, the case where $n = 2$ gives rise to a monic polynomial f of degree k such that $f \equiv g \pmod{A_1 \ldots A_{n-1}[X]}$ and such that $f \equiv f_n \pmod{A_n[X]}$. Consequently, $f \equiv f_i \pmod{A_i[X]}$ for each $i = 1, \ldots, n$. □

Let v be a rank one valuation on the field F. Let V be the valuation ring associated with v. Let M be the maximal ideal of V and let L be an algebraic extension field of F. We say that a valuation ring W on L is an extension of V to L if $W \cap K = V$. Let $\{V_\lambda\}_{\lambda \in \Lambda}$ be the set of extensions of V to L, and for each $\lambda \in \Lambda$, let M_λ be the maximal ideal of V_λ. If $|\Lambda| = 1$ and $M_1 = MV_1$, we say that v is *inertial with respect to L*; if $|\Lambda| = 1$ and $M_1 \supset MV_1$, then v *ramifies with respect to L*. If $|\Lambda| > 1$, then v *decomposes with respect to L*; and if $M_\lambda = MV_\lambda$ for every $\lambda \in \Lambda$, then v *is unramified with respect to L*. If R is an integrally closed domain with field of fractions K and if P is a prime ideal of R such that R_P is a DVR, then we say that P *is inertial, ramifies, decomposes,* or *is unramified with respect to L* if R_P is inertial, ramifies, decomposes, or is unramified with respect to L.

Theorem 6.4. *Let D be a Dedekind domain with field of fractions K and let $\{P_1, \ldots, P_r\}$, $\{Q_1, \ldots, Q_s\}$, and $\{M_1, \ldots, M_t\}$, where $r \geq 1$, be three sets of distinct maximal ideals of D, each with finite residue field. Then there exists a simple quadratic extension field $K(u)$ of K, with u integral over D and separable over K, such that each P_i is inertial with respect to $K(u)$, each Q_i ramifies with respect to $K(u)$, and each M_i decomposes with respect to $K(u)$.*

Proof. Since D/P_i is a finite field (by assumption) for each $i = 1, \ldots, r$, there is a separable monic polynomial $f_i(X) \in D[X]$ of degree 2 such that $f_i(X)$ is irreducible modulo $P_i[X]$. Since D is a Dedekind domain $Q_i \neq Q_i^2$ for each $i = 1, \ldots, s$; so we may choose $q_i \in Q_i \setminus Q_i^2$. Since the ideals $\{P_1, \ldots, P_r\}$, $\{Q_1^2, \ldots, Q_s^2\}$, $\{M_1, \ldots, M_t\}$ are pairwise comaximal, by Lemma 6.3, there exists a monic polynomial $f \in D[X]$ of degree 2 such that

$$\begin{aligned} f &\equiv f_i \pmod{P_i[X]}, \quad 1 \leq i \leq r; \\ f &\equiv X^2 + q_i \pmod{Q_i^2[X]}, \quad 1 \leq i \leq s; \\ f &\equiv X(X+1) \pmod{M_i[X]}, \quad 1 \leq i \leq t. \end{aligned}$$

Notice that f is irreducible in $D[X]$ as it is monic and irreducible modulo $P_1[X]$. Hence f is also irreducible in $K[X]$ by Corollary 2.34 since D is integrally closed. Now f has the form $X^2 + aX + b$. If $a \neq 0$, then f is separable over K. (Note that if $t \geq 1$, then we must have $a \neq 0$ since $f \equiv X^2 + X \pmod{M_1[X]}$.) On the other hand if $a = 0$, then we choose a nonzero element y in

$$(\bigcap_{i=1}^{r} P_i) \cap (\bigcap_{i=1}^{s} Q_i^2).$$

Replacing f by $f + yX$, we get a separable polynomial which satisfies the congruences given above. In any case, we can assume that f is separable over K. Let u be a root of f in an extension field of K and let D' be the integral closure of D in $K(u)$. Note that $K(u)/K$ is a Galois extension since any separable extension of degree 2 is Galois. If P is a maximal ideal of D and if $PD' = (P_1 \dots P_{g(P)})^{e(P)}$ (using Remark 2.80), where $[D'/P_{g(P)} : D/P] = f(P)$, then $e(P)f(P)g(P) = 2$ since $[D'/PD' : D/P] \leq [K(u) : K] = 2$ by Lemma 2.76 and since $[D'/PD' : D/P] > 1$ as $u \in D' \setminus D$. Hence to prove that each M_i decomposes with respect to $K(u)$, it is sufficient to show that M_i is contained in two distinct maximal ideals of D'; to show that each Q_i ramifies with respect to $K(u)$, it is sufficient to show that Q_i is contained in the square of a maximal ideal of D'; and to show that P_i is inertial with respect to $K(u)$, it is sufficient to show that there is a maximal ideal U_i of D' lying over P_i such that $[D'/U_i : D/P_i] \geq 2$.

Note that the kernel of the canonical homomorphism $D[X] \to D[u]$ is the principal ideal generated by f by Corollary 2.33. Then for each maximal ideal P of D, we have

$$\begin{aligned} D[u]/P[u] &\cong [D[X]/(f)]/[(P(X) + (f))/(f)] \\ &\cong D[X]/(P[X] + (f)) \\ &\cong (D[X]/P[X])/[(P[X] + (f))/P[X]] \\ &\cong (D/P)[X]/(\bar{f}), \end{aligned}$$

where $\bar{f}$ denotes the image of f under the canonical mapping $D[X] \to (D/P)[X]$.

If $P = P_i$, then $\bar{f}$ is irreducible in $(D/P)[X]$ and has degree 2 so that $(D/P)[X]/(\bar{f})$ is a field extension of degree 2 over D/P. Therefore $P[u]$ is a maximal ideal in $D[u]$ and $[D[u]/P[u] : D/P] = 2$. Since u is integral over D, $D[u] \subseteq D'$. Thus there exists a maximal ideal P' of D' lying over $P[u]$. Therefore, $D/P \subset D[u]/P[u] \subseteq D'/P'$ and $[D'/P' : D/P] \geq 2$. Hence P_i is inertial with respect to $K(u)$ for each $i = 1, \dots, r$.

If $P = Q_i$, then $\bar{f} = X^2$. In this case $D[u]/P[u]$ has a unique maximal ideal $H_i = P[u] + (u)$. Also we have $H_i^2 \subseteq P[u]$. We shall show that $P[u] \subseteq H_i^2$. It suffices to show that

$$P \subseteq H_i^2 = P^2[u] + uP[u] + (u^2).$$

By choice of q_i, we have $P = P^2 + (q_i)$ since P is a maximal ideal in the Dedekind domain D (which implies that there are no ideals properly between P and P^2). Since, clearly, $P^2 \subseteq H_i^2$, we need only show that $q_i \in H_i^2$. We have $f \equiv X^2 + q_i \pmod{Q_i^2[X]}$, and hence $f = X^2 + aX + b$ for some $a \in Q_i^2$, and $b \in D$ such that $b - q_i \in Q_i^2$. We have

$$b = -u^2 - au \in (u^2) + uP^2[u] \subseteq H_i^2,$$

and $b - q_i \in Q_i^2 \subseteq H_i^2$. It follows that $q_i \in H_i^2$, which gives that $P[u] = H_i^2$, as claimed. Again, since D' is integral over $D[u]$, there exists a maximal ideal of D', P' say, lying over H_i. Therefore, $P \subseteq H_i^2 \subseteq (P')^2$ and P ramifies with respect to $K(u)$.

Finally, if $P = M_i$, then $\bar{f} = X(X+1)$, in which case $(D/P)[X]/(\bar{f})$ has exactly two maximal ideals. It follows that there exist distinct maximal ideals U_1 and U_2 of $D[u]$ containing $P[u]$, and that there exist maximal ideals U_1' and U_2' of D' lying over U_1 and U_2, respectively. Therefore, U_1' and U_2' are distinct maximal ideals of D' lying over P and P decomposes with respect to $K(u)$. □

Example 6.5. Let $\{p_1, p_2, \ldots\}$ be the sequence of prime numbers. By the preceding theorem, there exists an algebraic integer u_1 of degree 2 over $\mathbb{Q}$ such that (p_1) decomposes with respect to $\mathbb{Q}(u_1)$. Let Z_1 be the integral closure of $\mathbb{Z}$ in $F_1 = \mathbb{Q}(u_1)$. Assume that $p_1 Z_1 = M_1^{(1)} M_2^{(1)}$. Again by the preceding theorem, we may choose an algebraic integer u_2 such that u_2 has degree 2 over F_1, $M_1^{(1)}$ and each prime of Z_1 lying over (p_2) in $\mathbb{Z}$ is inertial with respect to $F_2 = F_1(u_2)$, and such that $M_2^{(1)}$ decomposes with respect to F_2. Thus if Z_2 is the integral closure of $\mathbb{Z}$ in F_2, then $M_2^{(1)} Z_2 = M_2^{(2)} M_3^{(2)}$. If $M_1^{(1)} Z_2 = M_1^{(2)}$, then $\{M_1^{(2)}, M_2^{(2)}, M_3^{(2)}\}$ is the set of primes of D_2 lying over (p_1) in $\mathbb{Z}$.

By induction we may choose algebraic integers $u_1, u_2, \ldots, u_k$ such that if $F_i = \mathbb{Q}(u_1, \ldots u_i)$ and if Z_i is the integral closure of $\mathbb{Z}$ in F_i for each $i = 1, \ldots, k$, then the following are satisfied:

1. $[F_{i+1} : F_i] = 2$ for $1 \le i \le k-1$.
2. For each $i = 1, \ldots, k-1$, there exist $i+1$ prime ideals $\{M_1^{(i)}, M_2^{(i)}, \ldots, M_{i+1}^{(i)}\}$ of Z_i lying over (p_1) in $\mathbb{Z}$ such that $M_1^{(i)}, M_2^{(i)}, \ldots, M_i^{(i)}$ decomposes with respect

to F_{i+1}, and $M_j^{(i+1)} = M_j^{(i)} Z_{i+1}$, and such that $M_{i+1}^{(i)}$ decomposes with respect to F_{i+1}, say $M_{i+1}^{(i)} Z_{i+1} = M_{i+1}^{(i+1)} M_{i+2}^{(i+1)}$.

3. Each prime ideal of Z_i lying over any of the primes (p_2), (p_3), ... , (p_{i+1}) of $\mathbb{Z}$ is inertial with respect to F_{i+1} for $i = 1, \ldots, k-1$.

Then the union of $\{M_1^{(k)}, \ldots, M_{k+1}^{(k)}\}$ and the set of maximal ideals of Z_k lying over one of the primes (p_2), ... , (p_{k+1}) of $\mathbb{Z}$ is a finite set of prime ideals of the Dedekind domain Z_k, each with finite residue field. It follows from Theorem 6.4 that there is an algebraic integer u_{k+1} of degree 2 over F_k such that if Z_{k+1} is the integral closure of Z_k in $F_{k+1} = F_k(u_{k+1})$, then each of $M_1^{(k)}, \ldots, M_k^{(k)}$ and each maximal ideal of Z_k lying over any of the prime ideals (p_2), (p_3), ... , (p_{k+1}) of $\mathbb{Z}$ is inertial with respect to Z_{k+1}; and $M_{k+1}^{(k)}$ decomposes with respect to Z_{k+1}. Now let $M_j^{(k+1)} = M_j^{(k)} Z_{k+1}$ for $i = 1, \ldots, k$, and let $M_{k+1}^{(k)} Z_{k+1} = M_{k+1}^{(k+1)} M_{k+2}^{(k+1)}$. Then, clearly, $\{M_1^{(k+1)}, \ldots, M_{k+2}^{(k+1)}\}$ is a set of $k+2$ maximal ideals of Z_{k+1} lying over (p_1) in $\mathbb{Z}$. If M is a maximal ideal of Z_{k+1} lying over (p_1) in $\mathbb{Z}$, then M must lie over a maximal ideal of Z_k which lies over (p_1) in $\mathbb{Z}$, that is, $M \cap Z_k \in \{M_1^{(k)}, \ldots, M_{k+1}^{(k)}\}$, so that $M \in \{M_1^{(k+1)}, \ldots, M_{k+2}^{(k+1)}\}$. Therefore, conditions (1)-(3) hold for each $i = 1, \ldots, k$.

By induction, there exists a sequence $\{u_1, u_2, \ldots\}$ of algebraic integers such that if $F_i = \mathbb{Q}(u_1, \ldots, u_i)$ and Z_i is the integral closure of $\mathbb{Z}$ in F_i, then conditions (1)-(3) are valid for each $i > 0$.

Now let $F = \bigcup\limits_{i=1}^{\infty} F_i$ and $Z' = \bigcup\limits_{i=1}^{\infty} Z_i$. Then Z' is the integral closure of $\mathbb{Z}$ in F. It follows from [13, Corollary 42.2] (applied for $D_0 = \mathbb{Z}$) that Z' is an almost Dedekind domain. However, Z' is not Dedekind since p_1 belongs to infinitely many maximal ideals of Z'.

References

[1] Larsen, M. D. and McCarthy, P. J., *Multiplicative theory of ideals*, Elsevier, **1971**.

[2] Gilmer, R. W., Integral domains which are almost Dedekind, *Proceedings of the American Mathematical Society*, 15.5: 813-818, **1964**.

[3] Gilmer, R. W., The cancellation law for ideals in a commutative ring, *Canadian Journal of Mathematics*, 17: 281-287, **1965**.

[4] Olberding, B., *Factorization into radical ideals*, Vol. 241, Chapman & Hall, **2005**.

[5] Vaughan, N. H. and Yeagy, R. W., Factoring ideals into semiprime ideals, *Canadian Journal of Mathematics*, 30.6: 1313-1318. **1978**.

[6] Krull, W., Allgemeine Bewertungstheorie, *Journal für die reine und angewandte Mathematik,* 167, 160-196, **1932**.

[7] Anderson, F. W. and Fuller, K. R., *Rings and categories of modules*, Vol. 13, Springer Science & Business Media, **2012**.

[8] Sharp, R. Y., *Steps in commutative algebra,* No. 51, Cambridge university press, **2000**.

[9] Dummit, D. S. and Foote, R. M., *Abstract Algebra*, Vol. 1999, Englewood Cliffs: Prentice Hall, **1991**.

[10] Fontana, M. and Houston, E. and Lucas, T., *Factoring ideals in integral domains*, Vol. 14, Springer Science & Business Media, **2012.**

[11] Brandal, W., Constructing Bezout domains, *Journal of Mathematics*, 6.3, **1976**.

[12] Heinzer, W. and Ohm, J., Locally Noetherian commutative rings, *Transactions of the American Mathematical Society*, 158.2: 273-284, **1971**.

[13] Gilmer, R. W., *Multiplicative Ideal Theory*, Vol. 12, M. Dekker, **1972**.

CURRICULUM VITAE

Credentials:

Name, Surname:	Akif VURAL
Place of Birth:	Yenimahalle/ANKARA
Marital Status:	Single
E-mail:	akivura@gmail.com
Address:	Macun Mh. 204. Cd. C14 Blok D:16 Yenimahalle/ANKARA

Education:

Primary School:	1996-2004 Çamlıca Coşkun Primary School, İstanbul
High School:	2004-2007 Kasımoğlu Coşkun Science High School, İstanbul
BSc.	2007-2012 Hacettepe University, Department of Mathematics
MSc.	2013-2015 Hacettepe University, Department of Mathematics

Foreign Languages:

English

Work Experience: -

Areas of Experiences: -

Projects and Budgets:

TUBITAK-3501 Career Development Program (Project No: 113F032)

Publications: -

Oral and Poster Presentations: -