SOME FACTORIZATION PROPERTIES IN COMMUTATIVE RINGS

By

MUHAMMAD QASIM

Supervised by

DR. TARIQ SHAH

Department of Mathematics
Quaid-i-Azam University
Islamabad-Pakistan
2003

ACKNOWLEDGEMENT

In the name of Allah, the beneficent, the merciful, who enabled me to accomplish this task..

I wish to express my sincere thanks to my kind supervisor **Dr. Tariq Shah** for his invaluable suggestions and cooperation during this work. This study would have been impossible without his cooperation. I always found him ready to help me and work with me late nights in the department, which led to materialize this work.

It would be injustice if I donot admire the liberty of utilization of Department in late hours by the University without which this study would have not be completed.

I am pleased to acknowledge my deepest gratitude to all of my teachers for their kindness, moral support and valuable suggestions during my studies.

I wish to express deep sense of gratitude to my sweet mother and father, my brothers and sisters. This study would have been impossible without their prayers, love and affection.

I would like to thank my friends Saeed Islam and Shamsul Islam for their continuous encouragement.

It gives me pleasure to express my gratitude to my research fellows, especially Madad Khan, Asghar khan, M. Sohail Iqbal and Sohail Iqbal for their support, cooperation and encouragement.

Muhammad Qasim

DEDICATED TO
MY SUPERVISOR DR.
TARIQ SHAH

Content

Content

Preface

The classes of atomic domains, domains satisfying ascending chain condition for principal ideals (ACCP), bounded factorization domains (BFDs), irreducible divisors finite (idf) domains, finite factorization domains (FFDs) and half-factorial domains (HFDs) are frequently occurs in literature. These factorization classes or properties of domains which are weaker than unique factorizations, that is these classes of domains are generalizations of UFDs.

First we are giving the introduction of above factorization properties. Following Cohn [8], we say that D is an atomic domain if each non-zero non-unit of D is a product of a finite number of irreducible elements (atoms) of D. The well-known examples are UFD and Noetherian domains. We say that an integral domain D satisfies the ascending chain condition on principal ideals (ACCP) if there does not exist an infinite strictly ascending chain of principal ideals of D. Every ACCP is atomic but converse does not hold cf.[13] and [18]. An integral domain D satisfies ACCP if and only if $D[\{X_\alpha\}]$ satisfies ACCP [2, page 5], but by Roitman [17], if an integral domain D is atomic then not necessarily its polynomial extension is atomic. By [2], an atomic domain is bounded factorization domain (BFD) if there exist a bound on factorization of each non-zero non-unit element of D. By [2, proposition 2.2], Noetherian and Krull domains are BFDs. Also BFD satisfy ACCP but the converse is not true cf. [2, Example 2.1].

By [2], an integral domain is finite factorization domain (FFD) if each non-zero non-unit elements of D has only a finite number of non-associate divisors. By [2, Theorem 5.1], an integral domain D is FFD if and only if D is atomic idf-domain where an integral domain D is idf-domain if each non-zero element

of D has only finitely many non-associate irreducible divisors. A Krull domain is both atomic and idf therefore FFD, but a Noetherian domain not necessarily be an FFD. Of-course a UFD is FFD. By [2, proposition 5.3], D is FFD if and only if $D[X]$ is.

In [19] and [20] Zaks introduce the notion of half-factorial domains (HFDs), which is defined as; an atomic domain is half-factorial domain if for each non-zero non-unit element $x \in D$, if $x = x_1.x_2...x_m = y_1.y_2...y_n$, with each x_i, y_j irreducibles in D, then $m = n$. A UFD is an HFD and an HFD is BFD cf. [1]. Generally, HFDs do not response affirmatively under the polynomial extension. By [1, page 11], if $D[X]$ is an HFD then surely D is an HFD, but $D[X]$ need not be an HFD if D is an HFD. For example, $D = \mathbf{R}+X\mathbf{C}[X]$ is an HFD, but $D[Y]$ is not an HFD because $(X(1+iY))(X(1-iY)) = X^2(1+Y^2)$ are factors of an element in $D[Y]$ into irreducibles with different size. HFD does not imply FFD and vise versa, because $k[X^2, X^3]$, where k is finite field, an example of FFD but it is not HFD and the Noetherian domain $\mathbf{R}+X\mathbf{C}[X]$ is an HFD but not FFD.

In general,

$$\mathbf{idf-domain} \Longleftarrow \mathbf{UFD} \Longrightarrow \mathbf{HFD} \Longrightarrow \mathbf{BFD} \Longrightarrow \mathbf{ACCP} \Longrightarrow \mathbf{Atomic}.$$

and

$$\mathbf{idf-domain} \Longleftarrow \mathbf{UFD} \Longrightarrow \mathbf{FFD} \Longrightarrow \mathbf{BFD} \Longrightarrow \mathbf{ACCP} \Longrightarrow \mathbf{Atomic}.$$

But none of the above implication is reversible.

In [3, page 217], Anderson and Anderson define a criteria in order to measure how far an atomic domain is being an HFD, that is

$$\varrho(D) = \{m/n : x_1.x_2...x_m = y_1.y_2...y_n, \text{ each } x_i, y_i \in D \text{ is irreducible}\}.$$

Hence $1 \leq \varrho(D) \leq \infty$ and $\varrho(D) = 1$ if and only if D is HFD. $\rho(D)$ is known as the elasticity of D.

In this dissertation the work is in two folds.

In chapter 4, we review the paper [9] of Coykendall. The main result " Let D be an integral domain. If $D[X]$ is HFD then D is integrally closed" of this paper gives the characterization of polynomial rings with the half factorial property. For the sake of completion and better understanding we provided the explanation of [9] in this chapter.

In chapter 5 we characterize the semigroup rings with the half factorial property which is an attempt to generalize the polynomial case of Coykendall's results of [9], which are reviewed in chapter 4. We used the concepts of degree in semigroup rings which are coinciding the particular case of polynomial rings. Moreover, we introduced the notion of monic elements or pseudo monic polynomials in commutative semigroup rings to handle the situation. In this chapter we put condition on monoid S to be cyclic to use the same techniques of [9] and generalize Theorem 3.2.2 as "If $D[X;S]$ is half-factorial semigroup ring, then D is integrally closed" Theorem 4.2.5.

In chapter 6 we successfully attempt an open problem "when a semigroup ring is HFD ?". Before proving that when a semigroup ring is HFD, we established few new results and examples about the class group of semigroup rings and class group of semigroups. In this chapter we prove a criteria for a semigroup ring $D[X;S]$ relative to the class group of Krull semigroup rings that is " Let D be a Noetherian integrally closed domain and the monoid S, finitely generated by pure monomials $\{m_\alpha\}_{\alpha \in A}$ of indeterminates $\{X_i\}_{i=1}^n$ over D. Then $D[X;S]$ is HFD $\Leftrightarrow$ $Cl(D[X;S]) \simeq Z_2$ " which generalizes [20, Theorem 2.4].

In Chapter 1, we review some technical preliminaries for commutative ring theory which provides a necessary foundation for understanding the forth com-

ing concepts used in dissertation.

Chapter 2 consider some basic preliminaries of semigroups of specific nature like integrability and almost integrability. Moreover we also provided the structure of commutative semigroup rings and their integral closedness. This is a supply and quick understanding for notions used in chapter 4,5 and 6.

In chapter 3, we give the introduction of class groups and class monoid structure for both commutative semigroups and commutative rings. We also provided the relevant results and examples for the conveniens of the reader to understand the concepts clearly. What here we discussed is directly or indirectly related to our study and provides an immediate reference and supply to chapter 6.

Muhammad Qasim

Chapter 1

Preliminaries

1.1 Introduction

In this chapter we review some basic concepts and results which are directly helpful to provide the base and understanding of commutative ring theory. Here we consider the homomorphisms, polynomial rings, integral dependence, localization and factorization in the commutative rings. For general theory of these we shall follow [14, 12] and material other than these will be mentioned.

1.2 Commutative rings

Definition 1.2.1 *A ring $(R, +, .)$ is a set R together with two binary operations, an addition and a multiplication, such that,*

1: $(R, +)$ is an abelian group (an additive group of R)

2: The multiplication is associative i.e. $x(yz) = (xy)z$

3: The multiplication is distributive i.e. $(x+y)z = xz+yz$ and $z(x+y) = zx + zy$ for all $x, y, z \in R$.

Rings as defined above are also called associative rings, a non associative ring only has the properties (1) and (3). In all later sections we also require the concept of identity and zero element. In following we define these terms.

Identity element

An element say 1 is called identity element if $1.x = x = x.1$ for all $x \in R$.

The identity element is also called unity. A ring with an identity element is also called ring with identity or a ring with unity.

Invertible element

Given a ring $(R, +, .)$ with identity element 1 an element $a \in R$ is said to be invertible or unit, whenever a posses a two sided inverse with respect to multiplication i.e. there exist $a^{-1} \in R$ such that $a.a^{-1} = 1 = a^{-1}.a$.

Commutative ring

A commutative ring is a ring $(R, +, .)$ in which multiplication is a commutative operation i.e., $a.b = b.a$ for all $a, b \in R$.

Example 1.2.2 *If* $\mathbf{Z}, \mathbf{Q}, \mathbf{R}$ *represents the set of integers, rational and real numbers, then the structure* $(Z, +, .), (\mathbf{Q}, +, .)$ *and* $(\mathbf{R}, +, .)$ *are all example of commutative rings with all has a commutative identity* 1.

Example 1.2.3 *Let* X *be any given set and* $P(X)$ *be the collection of all subsets of* X. *The symmetric difference of two subsets* A, B *of* X *is the set* $A \triangle B$, *where* $A \triangle B = (A - B) \cup (B - A)$. *If we define addition and multiplication in* $P(X)$ *by*

$$A + B = A \triangle B \text{ and } A.B = A \cap B$$

then the system $(P(X), +, .)$ *forms a commutative ring with identity* X *and zero element* Φ.

Above are the examples of commutative rings. The following is the example for non-commutative structure.

Example 1.2.4 *Let* $M_n(R)$ *represents the set of square matrices of order* $n \times n$ *and with real entries. Now considering the usual addition and multiplication*

of matrices, we can see $(M_n(R), +, .)$ forms a ring. But note that as multiplication is non commutative in matrices, so structure is non-commutative.

Zero divisor

If R is a ring and $0 \neq a \in R$, then a is called a left(right) zero divisor in R if there exist some $b \neq 0$ in R such that $ab = 0 (ba = 0)$. A zero divisor is any element of R that is either a left or right zero divisor.

According to this definition, 0 is not a zero divisor, and if R contains an identity 1, then 1 is not a zero divisor nor is any element of R which happen to posses a multiplicative inverse. An obvious example of a ring with zero divisor is Z_n, where the integer $n > 1$ is composite; if $n_1 n_2 = n$ in Z $(0 < n_1, n_2 < n)$, then the product $\hat{n}_1 \hat{n}_2 = 0$ in Z_n.

Cancellative law

A ring R is said to satisfy cancellative law if $ab = ac$ and $ba = ca$, where $a \neq 0$, implies $b = c$ for all $a, b, c \in R$.

Note that a ring R is without zero divisor if and only if it satisfies the cancellation laws.

Integral Domain

By an *integral domain* is meant a commutative ring with identity which has no zero divisor. It is important to note that some authors do not insist on the presence of a multiplicative identity when defining integral domains.

Ring of integers is an example of integral domain. Now we change our direction somewhat to deal with the situation where a subset of a ring again constitutes a ring.

Subrings

Let $(R, +, .)$ be a ring and $S \subseteq R$ be a non empty subset of R. If the system $(S, +, .)$ is itself a ring (using the induced operations), then $(S, +, .)$ is said to be subring of $(R, +, .)$.

Alternaively, a subset S of a ring R is a subring of R if and only if S is a subgroup of $(R, +)$, is closed under multiplication.

A subring is called *unitary* if it contains the identity element of the ring.

1.2.1 Homomorphism

A *homomorphism* of a ring R into a ring S is a mapping $\varphi : R \to S$ which preserves both the operations:

$$\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y) \\ \varphi(xy) &= \varphi(x)\varphi(y), \text{ for all } x, y \in R. \end{aligned}$$

If R and S have identity elements, then the homomorphism of R into S is usually called to be a *homomorphism of rings with identity*, which also preserves the identity element;

$$\varphi(1_R) = 1_S.$$

The identity mapping 1_R on a ring R is a ring homomorphism . The composition of two ring homomorphisms $\varphi : R \to S$, $\upsilon : S \to T$ is a ring homomorphism $\upsilon \circ \varphi : R \to T$.

Isomorphism

An *isomorphism* of a ring R onto a ring S is a bijective homomorphism of R onto S. In this case rings R and S are said to be *isomorphism*.

Ideal

An ideal of a ring R is a subgroup I of $(R, +)$ such that $x \in I$ implies $xy \in I$ and $yx \in I$ for all $y \in R$. This relationship is sometimes denoted by $I \trianglelefteq R$. Note that multiplication is always closed in ideals, so ideals are of-course subrings. A *proper* ideal also satisfies $I \neq R$.

The notion of an ideal carries with its natural equivalence relation. For, given an ideal I of the ring R, it is a routine matter to check that the relation defined by $a \sim b$ if and only if $a - b \in I$ is actually an equivalence relation on R. As such, relation induces a partition of R into equivalence classes, the exact nature of which is determined below.

Equivalence Classes

If I is an ideal of the ring R, then the equivalence classes of $b \in R$ for the relation $\sim$ is the set

$$\begin{aligned} [b] &= \{a \in R : \ a - b \in I\} \\ [b] &= \{a \in R : a - b = i, i \in I\} \\ [b] &= \{a \in R : a = b + i, i \in I\} \\ [b] &= b + I = \{b + i : i \in I\}. \end{aligned}$$

Quotient Ring

If I is an ideal of the commutative ring R with 1, let us employ the symbol R/I to denote the collection of all distinct equivalence classes of I in R; that is,

$$R/I = \{a + I \ : a \in R\}.$$

It is easy to verify that R/I is again a ring. R/I is called as quotient ring (or factor ring) of R by I.

Field

A commutative ring R with 1 is said to be a field provided that the set $R - \{0\}$ is a commutative group under the multiplication of R.

Example 1.2.5 *Here are some of the more standard illustration of fields: the rational field* $\mathbf{Q}$, *the real field* $\mathbf{R}$ *and the extension field* $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} :$

$a, b \in \mathbb{Q}\}$ *of* $\mathbb{Q}$. *In each case the operations are ordinary addition and multiplication.*

Principal ideal

An ideal I of the commutative ring R with 1 is said to be principal if $I =< a >$ for some $a \in R$ that is generated by single element.

Maximal ideal

An ideal I of the ring R is said to be maximal ideal provided that $I \neq R$ and whenever J is an ideal of R with $I \subset J \subseteq R$, then $J = R$ or $I = J$.

Expressed somewhat loosely, an ideal is maximal if it is not the whole ring and is not properly contained in any larger proper ideal. The only ideal to contain a maximal ideal is the ring itself. It is quite difficult to prove an ideal is maximal directly from its definition. We therefore need several theorems to achieve the goal in some what easy way. One such result is the following:

Theorem 1.2.6 *Let I be a proper ideal of the commutative ring R. Then I is maximal ideal if and only if $(I, a) = R$ for any element $a \in R$. Here (I, a) denoted the ideal generated by $I \cup \{a\}$.*

Example 1.2.7 *Consider the ring of integers $(\mathbf{Z}, +, .)$. Here the maximal ideals of Z corresponds to the prime numbers. More precisely: the principal ideal $(n), n > 1$, is maximal if and only if n is prime. To prove this let $(n), n > 1$, is a maximal ideal of Z. If the integer n is not prime, then $n = n_1 n_2$, where $1 < n_1 < n_2 < n$. This implies the ideal (n_1) and (n_2) are such that*

$$(n) \subset (n_1) \subset \mathbf{Z}, \qquad (n) \subset (n_2) \subset \mathbf{Z},$$

contrary to the maximality of (n).

In the opposite direction, assume now that the integer n is prime. If the principal ideal (n) is not maximal in Z, then either $(n) = Z$ or else there exists

some proper ideal (m) *satisfying* $(n) \subset (m) \subset Z$. *The first case is immediately ruled out by the fact that* I *is not a multiple of any prime number. The alternate possibility,* $(n) \subset (m)$, *means that* $n = km$ *for some integer* $k > 1$; *this is again an abused because* n *is prime not composite. At any rate, we conclude that* (n) *must be maximal ideal.*

Prime Ideal

An ideal I of the commutative ring R with 1 is prime ideal if, for all $a, b \in R$, $ab \in I$ implies that either $a \in I$ *or* $b \in I$.

By induction, the above definition can easily be extended to finitely many element: an ideal I of R is prime if, whenever a product $a_1.a_2...a_n$ of element of R belong to I, then at least one of the $a_i \in I$.

Example 1.2.8 *A commutative ring* R *with 1 is an integral domain if and only if the zero ideal* $\{0\}$ *is prime ideal of* R.

Example 1.2.9 *The prime ideals of the ring* Z *are precisely the ideals* (n), *where* n *is a prime number, together with the two trivial ideals* $\{0\}$ *and* Z. *Where on the other hand if* n *is composite* ($n \neq 0, 1$), *then we can write* $n = n_1 n_2$, *where* $1 < n_1, n_2 < n$. *Certainly the product* $n = n_1 n_2 \in (n)$. *However, Since neither* n_1 *nor* n_2 *is an integral multiple of* n, $n_1 \notin (n)$ *and* $n_2 \notin (n)$. *Hence, when* n *is composite then the ideal cannot be prime. Notice also that although* $\{0\}$ *is prime, it is not maximal ideal of* Z.

Example 1.2.10 *For an illustration of a ring possessing a nontrivial prime ideal which is not maximal, take* $R = Z \times Z$, *where the operations are performed component wise. One may readily verify that* $Z \times \{0\}$ *is a prime ideal of* R. *Since*

$$Z \times \{0\} \subset Z \times Z_e \subset R,$$

with $Z \times Z_e$ *an ideal of* $R, Z \times \{0\}$ *fails to be maximal.*

Now the prime ideals can be characterized in the following manner.

Theorem 1.2.11 *Let I be proper ideal of the ring R. Then I is prime ideal (resp. maximal) if and only if the quotient ring R/I is an integral domain (resp. Field).*

Now the following result gives an important relation between maximal and prime ideals.

Theorem 1.2.12 *In a commutative ring with identity, every maximal ideal is a prime ideal.*

Nil Radical

Let I be an ideal of the ring R. The nil radical of I, designated by $\sqrt{I} = \{r \in R : r^n \in I \text{ for some } n \in Z^+\}$

We observe that the nil radical of I may equally well characterized as the set of elements $r \in R$ whose image $r + I$ in the quotient ring R/I is nilpotent. The nil radical of the zero ideal is sometimes referred to as the nil radical of the ring R; this set consists of all nilpotent element of the ring R.

Example 1.2.13 *In the ring Z, consider $n=p_1^{k_1}p_2^{k_2}...p_r^{k_r}$ is a factorization of the positive integers $n \neq 1$ into distinct primes p_j, then*

$$\sqrt{< n >} =< p_1p_2...p_r >$$

Indeed, if the integer $n = p_1p_2...p_r$ and $k = \max\{k_1, k_2..., k_r\}$, then we have $a^k \in < n >$; this makes it clear that $< p_1p_2...p_r > \subseteq \sqrt{< n >}$. On the other hand, if $m \in \sqrt{< n >}$, then m itself must be divisible by each of the primes $p_1, p_2, ..., p_r$,and, hence a member of the ideal

$$< p_1 > \cap < p_2 > \cap ... \cap < p_r >=< p_1p_2...p_r >$$

Primary ideal

An ideal I of the ring R is called primary if the conditions $ab \in I$ and $a \notin I$ together imply $b^n \in I$ for some positive integer n.

Clearly, any prime ideal satisfies this definition with $n = 1$, and thus, the concept of a primary ideal may be viewed as a natural generalization of that of a prime ideal. On the other hand a primary ideal is not necessarily a primary ideal. Notice that the above definition can be viewed as "An ideal I is said to be primary ideal if $ab \in I$ and $a \notin I$ imply $b \in \sqrt{I}$".

In the ring $\mathbf{Z}$, the primary ideals are precisely the ideals $< p^n >$,where p is a prime number and $n \geqslant 1$, together with the two trivial ideals.

Theorem 1.2.14 *If Q is a primary ideal of the ring R, then its nil radical $\sqrt{Q}$ is a prime ideal, known as the associated prime ideal of Q.*

Corollary 1.2.15 *If $Q_1, Q_2, ..., Q_n$ are a finite set of primary ideal of the ring R, all of them having the same associated prime ideal P, then $Q = \cap_{i=1}^{n} Q_i$ is also a primary ideal with $\sqrt{Q} = P$.*

1.2.2 Polynomial Rings

The next step in our program is to apply some of the previously developed theory to a particular class of rings, the so called polynomial rings. For the moment, we shall merely remark that there are rings whose elements consist of "Polynomials" with coefficient from a fixed, but otherwise arbitrary, ring.

But before going to discuss the polynomial ring structure we first discuss an important structure, the *formal power series*; as this structure is the main reason in motivation in polynomial rings.

Formal Power Series

Consider a commutative ring R and $\mathbf{N}$ be the set of natural numbers including 0, let $R^{\mathbf{N}} = \{f : f : \mathbf{N} \to R\}$ represents the totality of all infinite

sequences

$$f = (a_0, a_1, a_2, ..., a_k, ...), \text{ where } a_i \in R$$

Such sequences are called *formal power series*, or merely *power series*, over the ring R.

We intend to introduce suitable operations in $R^{\mathbf{N}}$, so that the resulting system forms a ring containing R as a subring. For this let $f, g \in R^{\mathbf{N}}$ such that

$$f = (a_0, a_2, ...) \text{ and } g = (b_0, b_1, ...)$$

are considered to be equal if and only if they are equal term by term, that is

$f = g$ if and only if $a_k = b_k$ for all $k \geqslant 0$.

Now, the formal power series may themselves be added and multiplied as follows:

$$\begin{aligned} f + g &= (a_0 + b_0, a_1 + b_1, ...) \\ fg &= (c_0, c_1, ...) \end{aligned}$$

where, for each $k \geqslant 0$ is given by

$$c_k = \sum_{k=i+j} a_i b_j.$$

It is understood that the above summation runs over all $i, j \geqslant 0$ subject to the condition that $i + j = k$.

A routine check establishes that under these two operations $R^{\mathbf{N}}$ forms a ring. It is notice that $(0, 0, 0, ...)$ is a zero element of $R^{\mathbf{N}}$. Where the additive inverse of $(a_0, a_1, a_2, ...)$ is $(-a_0, -a_1, -a_2, ...)$. Hence $R^{\mathbf{N}}$ is a ring under above operations known as the ring of *formal power series over* R.

Having reached this stage, we shall no longer distinguish between an element $a \in R$ and the special sequence $(a, 0, 0, 0, ...)$ of $R^{\mathbf{N}}$. The element of R, regarded as a power series, are hereafter called *constant series* or just *constant*.

With the aid of some additional notation, it is possible to represent power series the way we would like them to look. As a first step in this direction, we let aX designated the sequence

$$(0, a, 0, 0, ...)$$

That is, aX is the specific member of $R^{\mathbf{N}}$ which has the element a for its second term and 0 for all other terms. More generally, the symbol aX^n, $n \geqslant 1$, will denote the sequence

$$(0, ..., 0, a, 0, ...),$$

where the element a appear as the $(n+1)$th term in this sequence; for example we have

$$\begin{aligned} aX^2 &= (0, 0, a, 0, ...) \\ aX^3 &= (0, 0, 0, a, 0, ...) \end{aligned}$$

By use of these definitions, each power series

$$f = (a_0, a_1, ..., a_n, ...)$$

can be uniquely expressed in the form

$$\begin{aligned} f &= (a_0, 0, 0, ...) + (0, a_1, 0, 0, ...) + ... + (0, ...0, a_n, 0, ...) + ... \\ &= a_0 + a_1X + a_2X^2 + ... + a_nX^n + ... \end{aligned}$$

With the obvious identification of a_0, with the sequence $(a_0, 0, 0, ...)$. Thus, there is no loss in regarding the power series ring $R^{\mathbf{N}}$ as consisting of all formal expressions

$$f = a_0 + a_1X + a_2X^2 + ... + a_nX^n + ...,$$

where the elements $a_0, a_1, ...$(the coefficient of f) lie in R. As a notational device, we shall often write this as $f = \sum a_kX^k$. We should emphasize that,

according to our definition, X is simply a new symbol, or indeterminate, totally unrelated to the ring R. To indicate the indeterminate X, it is common practice to write $R[[X]]$ for the set $R^{\mathbf{N}}$, and $f(X)$ for any member of the same. From now on, we will make exclusive use of these notation.

Remark 1.2.16 *If the ring R happen to have a multiplicative identity 1, then X of-course is the member of the $R[[X]]$.*

In this case the power series X can be written as $(0, 1, 0, 0, ...)$. Thus from this view, aX become an actual product of the members of $R[[X]]$.

$$aX = (a, 0, 0, ...)(0, 1, 0, 0, ...).$$

Concerning the notation of power series, it is customary to omit terms with zero coefficients and to replace $(-a_k)X^k$ by $-a_kX^k$. Although X is not to be considered as an element of $R[[X]]$, we shall nonetheless take the liberty of writing the term $1X^k$ as X^k $(k \geqslant 1)$. With these conventions, one should view, for example, the power series

$$1 + X^2 + X^4 + ... + X^{2n} + ... \in \mathbf{Z}[[X]],$$

as representing the sequence (1,0,1,0,...).

An important definition in connection with power series is that of order, given below.

Definition 1.2.17 *If $f(X) = \sum a_kX^k$ is a nonzero power series (that is, if not all the $a_k = 0$) in $R[[X]]$, then the smallest integer n such that $a_n \neq 0$ is called the order of $f(X)$ and denoted by $ord(f(X))$.*

Suppose $f(X), g(X) \in R[[X]]$, with $ord(f(X)) = n$ and $ord(g(X)) = m$, So that,

$$\begin{aligned} f(X) &= a_nX^n + a_{n+1}X^{n+1} + ... \qquad (a_n \neq 0) \\ g(X) &= b_mX^m + b_{m+1}X^{m+1} + ... \qquad (\mathrm{b}_m \neq 0). \end{aligned}$$

From the definition of multiplication in $R[[X]]$, it can be seen easily that all the coefficient of $f(X)g(X)$ upto $(n+m)th$ are zero, Whence

$$f(X)g(X) = a_n b_m X^{n+m} + (a_{n+1}b_m + a_n b_{m+1})X^{n+m+1} + ...$$

If we assume that one of a_n and b_m is not a divisor of zero in R, then $a_n b_m \neq 0$ and

$$ord(f(X)g(X)) = n + m = ord(f(X)) + ord(g(X)),$$

this certainly holds when R is an integral domain. Generally, we have the following result:

Theorem 1.2.18 *If $f(X)$ and $g(X)$ are nonzero power series in $R[[X]]$, then*

1)either $f(X)g(X) = 0$ or $ord(f(X)g(X)) \geq ord(f(X)) + ord(g(X))$, with equality if R is an integral domain.

2)either $f(X)+g(X) = 0$ or $ord((f(X)+g(X)) \geq \min(ord(f(X), ord(g(X))$.

Corollary 1.2.19 *If R is an integral domain then so as its power series ring $R[[X]]$ is an integral domain.*

Lemma 1.2.20 *Let R be commutative ring with identity. A formal power series $f(X) = \sum a_k X^k$ is invertible in $R[[X]]$ if and only if the constant term a_0 has an inverse in R.*

Corollary 1.2.21 *A power series $f(X) = \sum a_k X^k \in K[[X]]$, Where K is a field, has an inverse in $K[[X]]$ if and only if its constant term $a_0 \neq 0$.*

Theorem 1.2.22 *Let R be a commutative ring with identity. There is a one to one correspondence between the maximal ideals M of the ring R and the maximal ideals $M[[X]]$ of its power series ring $R[[X]]$ in such a way that $M[[X]]$ corresponds to M if and only if $M[[X]]$ is generated by M and X; that is $M[[X]] =< M, X >$.*

Polynomials

Let $R[X]$ denote the set of all power series in $R[[X]]$ whose coefficients are zero from some index onward (the particular index varies from series to series):

$$R[X] = \{a_0 + a_1X^1 + ... + a_nX^n : a_n \in R, n \geq 0\}.$$

An element of $R[X]$ is called *polynomial* (in X) over the ring R.

In essence, we are defining the polynomial to be a finitely nonzero sequence of elements of R. It is easily verified that $R[X]$ constitutes the subring of $R[[X]]$, so called *ring of polynomials over* R (in an indeterminate X).

Running parallel to the idea of the order of the formal power series is that of the degree of a polynomial, which is introduced below.

Degree of a polynomial

Given the non zero polynomial

$$f(X) = a_0 + a_1X^1 + ... + a_nX^n \ (a_n \neq 0).$$

In $R[X]$, we call a_n the *leading coefficient* of $f(X)$; and the integer n, the *degree of the polynomial.*

The degree of a nonzero polynomial is therefore is a nonnegative integer; no degree is assigned to the zero polynomial. Notice that the polynomials of degree 0 are precisely the nonzero constant polynomial.

monic polynomial

If R is a ring with identity, a polynomial whose leading coefficient is 1 is said to be a *monic polynomial.*

As a matter of notation, we shall hereafter write $deg(f(X))$ for the degree of any nonzero polynomial $f(X) \in R[X]$. The result below is similar to that given for power series.

Theorem 1.2.23 *If $f(X)$ and $g(X)$ are nonzero polynomial in $R[X]$, then*

1)either $f(X)g(X) = 0$ or $deg(f(X)g(X)) \leq \deg(f(X)) + \deg(g(X))$,

2)either $f(X)+g(X)=0$ *or* $deg(f(X)+g(X)) \leq \max\{\deg(f(X)), \deg(g(X))\}$.

Corollary 1.2.24 *1)If D is an integral domain then it is simple to see that* $deg(f(X)g(X)) = deg(f(X)) + deg(g(X))$

2)If D is an integral domain, then so as its polynomial ring extension $R[X]$.

Example 1.2.25 *As an illustration of what might happen if R has zero divisors, consider* Z_8, *the ring of integers modulo* 8. *Taking*

$$f(X) = 1 + 2X,\ g(X) = 4 + X + 4X^2,$$

we obtain $f(X)g(X)=4+X+6X^2$, *so that,*

$$\deg(f(X)g(X)) = 2 < 1 + 2 = \deg(f(X)) + \deg(g(X)).n.$$

Although many properties of the ring R carry over to the associated polynomial ring $R[X]$, it should be pointed out that for no ring R does $R[X]$ form a field. In fact, when R is a field (or, for that matter, an integral domain), no element of $R[X]$ which has positive degree can posses a multiplicative inverse. with $deg(f(X)) > 0$ if $f(X)g(X) = 1$ for some $g(X) \in R[X]$,we could obtain the contradiction

$$0 = \deg(1) = \deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X)).$$

Theorem 1.2.26 *(Division Algorithm)*

Let R be commutative ring with identity and $f(X), g(X) \neq 0$ *in* $R[X]$ *with the leading coefficients of* $g(X)$ *an invertible element. Then there exist unique polynomials* $q(X), r(X) \in R[X]$ *such that*

$$f(X) = q(X)g(X) + r(X),$$

where, either $r(X) = 0$ *or* $deg(r(X)) < deg(g(X))$.

The polynomials $q(x)$ and $r(x)$ appearing in the division algorithm are called, respectively, the *quotient* and *remainder* on dividing $f(X)$ by $g(X)$.

Theorem 1.2.27 *(Remainder Theorem)*

Let R be commutative ring with identity. If $f(X) \in R[X]$ and $a \in R$, then there exist a unique polynomial $q(X)$ in $R[X]$ such that $f(X) = (X-a)q(X)+r(X)$.

Corollary 1.2.28 *The polynomial $f(X) \in R[X]$ is divisible by $(X-a)$ if and only if a is a root of $f(X)$.*

Theorem 1.2.29 *Let R be an integral domain and $f(X) \in R[X]$ be a nonzero polynomial of degree n. Then $f(X)$ can have at most n distinct roots in R.*

1.2.3 Integral Dependence

In this section we deal with some of the important features of commutative rings like ring extension, Integral elements, integral closedness etc.

Unitary ring Extension

$A \subseteq B$ be a unitary commutative ring extension if A has the identity of B.

integral element

Let $A \subseteq B$ be a unitary commutative ring extension then an element $b \in B$ is integral over A, if $f(b) = 0$ for some monic polynomial $f(X) \in A[X]$.

Integral extension

A ring extension $A \subseteq B$ is integral in case every element of B is integral over A.

Integral closedness

Let $A \subseteq B$ be any ring extension then, the integral closure of the ring A in B is the ring A' of all elements of B that are integral over A. The ring A is integrally closed in B in case $A' = A$.

1.2.4 Localization

Localization generalizes the construction of the field of fraction of a domain but applies to any commutative ring.

Ring of fraction

Let R be a commutative ring with identity element. A *multiplicative subset* of R is a subset S of R which contains an identity element and closed under multiplication (i.e, if $s, t \in S$, then $st \in S$).

It is straight forward that an equivalence relation $\sim$ on $R \times S$ is defined by

$$(a, s) \sim (b, t) \Longleftrightarrow atu = bsu \text{ for some u} \in \text{S}.$$

The equivalence class of $(a, s) \in R \times S$ is a fraction, we denote it by a/s. The *ring of fraction* of R with denominators in S is the set $\text{S}^{-1}R = (R \times S)/\sim$ of all fractions, with operations given by

$$\begin{aligned} (a/s) + (b/t) &= (at + bs)/st, \\ (a/s)(b/t) &= ab/st. \end{aligned}$$

It is straight forward that operations on $S^{-1}R$ are well defined and that $S^{-1}R$ is a ring, with zero element $0/1$ and identity element $1/1$. For all $s, t \in S$, s/t is a unit in $\text{S}^{-1}R$, with $(s/t)^{-1} = t/s$.

1.2.5 Factorization in Rings

This section deals with some important factorization properties like Eucldean domains, Principal ideal domains, Unique factorization domains, GCD domains, Dedekind domain, Valuation ring, Discrete valuation ring and Krull domains. The study of these classes were developed in previous decades, but now a days a very useful and fast activity is on factorization properties of domains known as HFDs (Half factorial domain), idf (irreducibles divisors finite) domains, FFDs (Finite factorization domains), BFDs (Bounded factorization

domain), ACCP (Ascending chain condition on principal ideals) and atomic domain, which are generalized than previous ones. But first we have to understand some basic concepts.

Prime element

A nonzero element p in a commutative ring R is called a prime if and only if p is not invertible and p divides ab implies that either p divides a or else p divides b.

Irreducible element

A nonzero element q in the ring R is said to be irreducible (or non-factorizable) if and only if q is not invertible and in every factorization $q = bc$ with $b, c \in R$, either b or c is invertible.

ED

An integral domain D is said to be Euclidean domain (ED) if there exist a map $\varphi : D \to \mathbf{N}$ *with* properties;

1) $\varphi(a) = 0$ if and only if $a = 0, a \in D$.

2) $\varphi(ab) = \varphi(a)\varphi(b)$, for all $a, b \in D$.

3) for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in D$ such that $a = bq + r$ where $\varphi(r) < \varphi(b)$.

PID

An integral domain is PID if every ideal in D is principal ideal. e.g Z,$Z[i]$ and $K[X]$, where K is field.

UFD

An integral domain D is said to be factorial domain or UFD, if every non-zero non-unit element $x \in D$ can be written as a product of irreducibles in D and this factorization is unique upto order and associates.

GCD Domain

An integral domain D is said to be GCD domain, if every pair of elements in D has greatest common divisor.

In general

$$\text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{GCD}.$$

But none of the above implication is reversible.

In such rings as division rings or fields where each element has its inverse is of no interest.

Theorem 1.2.30 *(Guass Theorem)*

When R is a UFD, then $R[X]$ is a UFD.

The application of above theorem can be seen in domains $Z[X]$ and $K[X]$ (where K is a field) are UFD.

Noetherian Ring

A commutative ring with identity R is Noetherian in case its ideals satisfies the ascending chain condition (acc) i.e. every ascending sequence

$$I_1 \subseteq I_2 \subseteq ... \subseteq I_j \subseteq I_{j+1} \subseteq ...,$$

of ideals of R terminates(that is there exist $n > 0$ such that $I_i = I_n$ for all $i \geq n$) or equivalently satisfies the following equivalent conditions.

1) There is no strictly ascending sequence of ideals of R, $I_1 \subset I_2 ... \subseteq I_j \subseteq I_{j+1} \subseteq ...$.

2)Every non-empty set S of ideals of R has a maximal element (an element M of S such that there is no $M \subseteq I \in S$).

Theorem 1.2.31 *(Hilbert Basis Theorem)*

Let R be a commutative ring with identity, if R is Noetherian then $R[X]$ is Noetherian.

Dedekind Domain

In this case the factorization can be carried out with ideals, using products rather than intersection. Before going to define the Dedekind domain, we must have the concept of fractional ideals and dimension of a ring.

Dimension of a Commutative ring

The maximum length of the chain of the prime ideals of the ring R is called the dimension of R. For example $\mathbf{Z}$ has dimension 1 and dimension of $R[X]$ is equal to the dimension of $R+1$. Therefore dimension of $\mathbf{Z}[X]$ is 2 and $K[X]$ has dimension 1, because field has dimension 0.

Fractional Ideal

A fractional ideal of R is the subset of quotient field $Q(R)$, which has the form

$$\frac{I}{c} = \{\frac{a}{c} \in Q : a \in I\},$$

where I is an ideal of R and $c \in R, c \neq 0$.

Example 1.2.32 *Let D be an integral domain and let $Q(D) = K$. Suppose $\{s_1, s_2, ..., s_n\} \subseteq K$. Then $F =< s_1, s_2, ..., s_n >$ is a fractional ideal, which is of-course finitely generated D-submodule of K. So this fractional ideal is finitely generated and can be written as*

$$F = Rs_1 + Rs_2 + ... + Rs_n.$$

A fractional ideal F is invertible in case there exist a fractional ideal F' of D such that $F.F' = D$.

Definition 1.2.33 *An integral domain D is a Dedekind domain if it satisfy any of the following conditions.*

(1) Every nonzero ideal of D is a product of prime ideals.

(2) Every nonzero ideal of D can be written uniquely as a product of positive powers of distinct prime ideals.

(3) Every nonzero ideal of D is invertible.

(4) Every nonzero fractional ideal of D is invertible.

Alternatively, one dimensional integrally closed Noetherian domain is said to be Dedekind.

Examples:[14, Page-407]

(1) $Z[\sqrt{10}]$ is Dedekind but not PID.

(2) $Z[i\sqrt{5}]$ is Dedekind but not PID, because if it is PID then by above assertions this implies that $Z[i\sqrt{5}]$ is UFD, but this is not true as

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Valuation Ring

Let $H \cup \{\infty\}$ be an ordered set with the conventions $\infty + \alpha = \infty$ and $\infty + \infty = \infty$.

A map $v : K \longrightarrow H \cup \{\infty\}$ is called additive valuation or just a valuation of the field K if it satisfies the conditions:

1) $v(xy) = v(x) + v(y)$;

2)$v(x + y) \geq \min(\{v(x), v(y)\}$;

3)$v(x) = \infty \Longleftrightarrow x = 0$. where $x, y \in K$.

If we write K^* for the multiplicative group of K then $v : K^* \longrightarrow H$ defines a homomorphism and $Im(v)$ is a subgroup of H. $Im(v)$ is called the value group of v. We say

$$\begin{aligned} R_v &= \{x \in K \mid v(x) \geq 0\} \text{ is valuatin ring of the field } K \text{and} \\ M_v &= \{x \in K \mid v(x) > 0\} \text{ is the maximal ideal of } \mathrm{R}_v. \end{aligned}$$

Notice that Z is not a valuation ring.

A valuation ring is said to be *discrete valuation ring* (DVR) if its value group is isomorphic to Z. A Noetherian valuation ring is DVR.

A ring between domain D and its quotient field K is said to be overring of D. If D is a valuation ring of the field K then every overring of D is a valuation ring.

Krull Domain

Let D be an integrally closed domain with quotient field K and $F = \{v_\lambda\}_{\lambda\in\gamma}$ be a family of valuation over-rings of D.

1) $D = \cap_\lambda V_\lambda$

2) Each V_λ is DVR.

3) The family F has finite character (that is if $0 \neq x \in K$, then x is a non-unit in only finitely many of the valuation rings in the family F).

4) Each V_λ is essential for D (A valuation over-ring of integral domain D is said to be essential for D if V is fraction ring of D).

Example 1.2.34 *DVRs, PIDs, Dedekind and UFDs are well known examples of Krull domains.*

Remark 1.2.35 *One dimensional Krull domains and Dedekind domains coincides [16, Theorem 12.5].*

Atomic Domain

Following Cohn [8], an integral domain D is atomic if each nonzero non-unit of D is a product of irreducible elements (atoms) of D.

ACCP

Following [2], an integral domain satisfies the ascending chain condition on principal ideals (ACCP), if there does not exist an infinite strictly ascending chain of principal integral ideals of D.

BFD

Following [2], an integral domain is a BFD, if D is atomic and for each nonzero non-unit of D, there is a bound on the length of factorization into products of irreducible elements.

HFD (*Half Factorization Domain*)

Following [19], an integral domain D is said to be HFD if D is atomic, and given any two irreducible factorizations of an element $a \in D$,

$a = \pi_1\pi_2...\pi_k = \xi_1\xi_2...\xi_m$,

then $k = m$.

idf-domain

An integral domain D is said to be irreducible-divisor-finite (idf) domain if every non-zero, non-unit element of D has a finite number of irreducible divisors.

FFDs

An integral domain D is said to be finite factorization domain (FFD), if every non-zero, non-unit element of D has a finite number of non-associate divisors.

An atomic idf domain is FFD.

In general,

$$\textbf{idf} - \textbf{domain} \Longleftarrow \textbf{UFD} \Longrightarrow \textbf{HFD} \Longrightarrow \textbf{BFD} \Longrightarrow \textbf{ACCP} \Longrightarrow \textbf{Atomic},$$

and

$$\textbf{idf} - \textbf{domain} \Longleftarrow \textbf{UFD} \Longrightarrow \textbf{FFD} \Longrightarrow \textbf{BFD} \Longrightarrow \textbf{ACCP} \Longrightarrow \textbf{Atomic}.$$

But none of the above implication is reversible.

In [18] Zaks and in [13] gives the examples of atomic domains, which are not satisfying ACCP.

Examples

(1) By [4], $R = K[X^2, X^3]$ (K is a field) is an atomic domain which is not HFD, since X^2 and X^3 are each irreducible element of R and $X^6 = X^3X^3 = X^2X^2X^2$.

(2) In general, by [4], for each integer $n \geq 2$, $R_n = K + X^nK[X] = K[X^n, X^{n+1}, ..., X^{2n-1}]$ is a one-dimensional Noetherian (and hence atomic)

domain which is not HFD, since X^n and X^{2n-1} are each irreducible elements of R_n and $X^{n(2n-1)} = (X^{2n-1})^n = (X^n)^{2n-1}$.

Chapter 2

Commutative Semigroups and Semigroup Rings

2.1 Introduction

In this chapter we review some specific properties of commutative semigroups, such as integral closedness and the almost integrability in the semigroups. Moreover we also provided the structure of commutative semigroup rings and their integral closedness. We refer to the reader to [12, chapter 1] and [15] for more detailed information on this topic.

Semigroup

A semigroup is a non empty set closed under an associative binary operation.

If $(S, *)$ is a semigroup, then S is commutative (or abelian) if it is commutative under the operation * , and S has an identity element if there exist an identity element with respect to *: a semigroup with identity is called monoid. Throughout in this discussion We will use additive abelian semigroups e.g, $\mathbf{N}$ (The set of natural numbers) is a semigroup under addition and Z (The set of integers), $\mathbf{Q}$ (The set of rational numbers} are the examples of additive monoids.

Numerical Semigroup and Monoid

Following [12, page 11-12], a semigroup S is said to be numerical semigroup if S is subset of $\mathbf{Z}^+$ and a monoid S is a numerical monoid if it is a sub-monoid of $\mathbf{Z}_0$. Where $\mathbf{Z}^+$ and $\mathbf{Z}_0$ are set of positive integers and non-negative integers respectively.

Totally Ordered Semigroup

If $\leq$ is a relation on a semigroup S then S is said to be totally order if for each $s_1, s_2 \in S$, either $s_1 \leq s_2$ or $s_2 \leq s_1$.

Sub-semigroup

A subset T of S is a sub-semigroup of S if T itself is a semigroup under the operation on S .

Prime Ideal

By [15], an ideal I of S is prime if $x + y \in I$ implies $x \in I$ or $y \in I$

Cancellative element

An element s of a semigroup S is said to be cancellative if $s + a = s + b$ implies $a = b$ for $a, b \in S$.

Remark 2.1.1 *The set of cancellative elements of S is denoted by C. This set may be empty; If $C \neq \Phi$, then C is a subsemigroup of S. If $S = C$ then S is said to be cancellative semigroup.*

Example 2.1.2 *$Z, \mathbf{Q}, \mathbf{R}$ are the examples of cancellative semigroup.*

Theorem 2.1.3 *[12, page 5-6] If C is a subsemigroup of an additive semigroup S and if each element of C is cancellative in S, then there exist an imbedding f of S into an abelian monoid T such that (1) $f(c)$ has an inverse $-f(c)$ in T for each $c \in C$, and (2) $T=\{f(s)-f(c): s \in S$ and $c \in C\}$. The monoid T is determined, up to semigroup isomorphism, by properties (1) and (2). If S is cancellative and $S = C$, then T is a group.*

Remark 2.1.4 *[12, page 5-6], the monoid T constructed as in the statement of above theorem is called the quotient monoid of S with respect to C. By abuse of notation, we write the elements of T in the form s-c instead of f(s)-f(c) and we consider S to be a subset of T. If S is cancellative, then the group T is called the quotient group of S; to within isomorphism it is the smallest group in which S can be imbedded.*

Ideal

An ideal of a semigroup S is a non-empty subset I of S such that $I \supseteq s + I = \{s + i : i \in I\}$ for each $s \in S$ .By [12, page 5-6]The intersection of a family of ideals of S is an ideal, provided it is non-empty.

Torsion Group[12, page-6]

An abelian group G is torsion-free if 0 is the only element of G of finite order. G is a torsion group, if each element of G has finite order, and G is called mixed if it contains elements of infinite order. and nonzero elements of finite order.

Remark 2.1.5 *If S is a cancellative semigroup with quotient group G, then the condition that G be torsion-free if and only if S satisfies the following condition.*

(a) For any positive integer n and any $x, y \in S$, the equality $nx = ny$ implies that $x = y$.

The condition (a) used as the definition of a torsion-free semigroup.

Torsion Free Semigroup

A semigroup S is said to be torsion-free [12, chapter 7], if for any positive integer n and any $x, y \in S$, the equality $nx = ny$ implies that $x = y$.

2.2 Integral Closedness in Semigroups

Let T be a monoid and let S be a submonoid of T containing 0. An element $t \in T$ is said to be integral over S if $nt \in S$ for some $n \in \mathbf{Z}^+$. The set S_0 of element $t \in T$, that are integral over S is a submonoid of T containing S. S_0 is called the integral closure of S in T. If $S = S_0$, we say S is integrally closed in T. Note that S_0 is integrally close in T. In case S is cancellative and T is the quotient group of S, then S_0 is called the integral closure of S and S is said to be integrally closed if $S = S_0$.

2.3 Almost integrability in Semigroups

An element $t \in T$ is almost integral over S if there exist $s \in S$ such that $s + nt \in S \ \forall \ n \in \mathbf{Z}^+$. The set S^* of all $t \in T$ that are almost integral over S is called the complete integral closure of S in T. It is completely integrally closed in T, if $S = S^*$. In general, S^* need not be completely integrally closed in T.

If T is the quotient group of S, then S^* is called the complete integral closure of S, and S is completely integraly closed if $S = S^*$.

Note that, if $t \in T$ is integral over S, then t is almost integral over S.

2.4 Commutative Semigroup Rings

By *[12] and [15]*, assume that R is an associative ring and that $(S, *)$ is a semigroup. Let J be the set of functions f from S into R that are finitely nonzero, with addition and multiplication defined in J as follows,

$$(f + g)(s) = f(s) + g(s)$$

$$(fg)(s) = \sum_{t*u=s} f(t)g(u), \tag{2.1}$$

Where the symbol $\sum_{t*u=s}$ indicates that the sum is taken over all pairs (t, u) of elements of S such that $t * u = s$, and it is understood that $(fg)(s) = 0$ if s is not expressible in the form $t * u$ for any $t, u \in S$. Now it is easy to verify that J is a ring under $+$ and '.' . This J is denoted by $R[X; S]$ and known as *semigroup ring* of S over R. If S is monoid, then T is called monoid ring.

Example 2.4.1 *Let us assume that* $S = Z_0$, *and* R *is an associative ring, then* J *is simply a polynomial ring* $R[X]$.

Example 2.4.2 *[4], let* $S =< n_1, n_2, ..., n_r >$, *where* $n_i \in N$ *and* $r > 1$. *Then of-course* S *is a proper numerical semigroup i.e. a proper submonoid of* Z^+ *under addition with* $Z^+ - S$ *is finite. Then the semigroup ring* $R = K[S] = \{\sum_{s \in S} a_s X^s : a_s \in K, .s \in S\} = K[X^{n_1}, X^{n_2}, ..., X^{n_r}]$ *is a one dimensional Noetherian(and hence atomic) domain which is not HFD, because* X^{n_1}, X^{n_r} *both irreducible elements of* R *and* $X^{n_1 n_r} = (X^{n_1})^{n_r} = (X^{n_r})^{n_1}$. *Also this implies* R *is not UFD.*

Representation of the elements of $R[X; S]$

If the semigroup operation in S is written as $+$, the elements of J are written either in the form $\sum_{s \in S} f(s)X^s$ or in the form $\sum_{i=1}^{n} f(s_i)X^{s_i}$($n$ represents number of nonzero function values) with addition and multiplication defined as for polynomials. Introduction of the symbol X and the notation X^s has the effect of transforming $(S, *)$ into the multiplicative semigroup $\{X^s / s \in S\}$ by means of the isomorphism $s \to X^s$. And it is recommended to use the above notation because, it is more understandable. It can be noted that X is not neccessarily be the element of $R[X; S]$. Now for convenience if R and S are considered to be unitary, then X belongs to $R[X; S]$.

Each non-zero element f of $R[X;S]$ has a unique representation in the form $f = \sum_{i=1}^{n} f_i X^{s_i}$, where $f_i \neq 0$ and $s_i \neq s_j$ for $i \neq j$. This representation is called the canonical form of f. The support of f is denoted by $supp(f) = \{s_i\}_i^n$. The subset $<\{s_i\}_i^n>$ is the supporting semigroup of f. The ideal of R generated by $\{f_i\}_i^n$ is called the content of f and is denoted by $C(f)$.

2.4.1 Integrability in Semigroup Rings

Definition 2.4.3 *[12, Corollary 12.11]*

Let D be a unitary integral domain and let S be a torsion free cancellative monoid. Then the integral closure of $D[S]$ is $\acute{D}[\acute{S}]$, where $\acute{D}$ is the integral closure of D and $\acute{S}$ is the integral closure of S and $D[S]$ is integrally closed if and only if D and S are integrally closed.

Chapter 3

Class Groups

3.1 Introduction

In this chapter we give the introduction of class groups and class monoid structure for both semigroups and rings. We also provide the relevant results and examples for the convenience of the reader to understand the concepts clearly. Most of the material in this chapter is followed by [12] and [11]. What here we discussed is directly or indirectly related and provide an immediate reference and supply to chapter 6.

3.2 Class Group of Semigroups

Fractional Ideal

Let S be a cancellative monoid with quotient group G. A non-empty subset I of G is called a fractional ideal of S if

1. $S + I \subseteq I$
2. $\exists\ s \in S$ such that $s + I \subseteq S$.

Note that, I is not neccessarily the semigroup of G.

Principal Fractional Ideal

A fractional ideal is said to be principal if $I = x + S$ for some $x \in G$.

Assume that $\mathcal{F}(S)$ represents the set of all fractional ideals of S. Now one can see $\mathcal{F}(S)$ is commutative monoid with zero element S under the binary operation

$$I + J = \{i + j : i \in I, j \in J\}.$$

Definition 3.2.1 *If $I, J \in \mathcal{F}(S)$, then $I : J$ is defined as $\{x \in G : x + J \subseteq I\}$.*

Remark 3.2.2 *$I : J \in \mathcal{F}(S)$ that is $I : J$ is again a fractional ideal.*

Divisorial Ideal

$S : (S : I)$ is denoted by I_v and I is called the divisorial ideal associated with S, if $I = I_v$, then I is called divisorial.

Remark 3.2.3 *[12, Theorem 16.4]*

(1) If $I, J \in F(S)$, then $I : J \in F(S)$.

(2) $I : (x + J) = -x + (I : J)$ for each $x \in G$. In particular, $S : (S : (x + S)) = S : (-x + S) = x + S$,

so $x + S$ is divisorial.

(3) If $J_1 \subseteq J_2$, then $I : J_1 \supseteq I : J_2$. Hence, $(J_1)_v \subseteq (J_2)_v$.

(4) I_v is the intersection of the family of all principal fractional ideals of S that contain I.

(5) $(I_v)_v = I_v$.

(6) $(x + I)_v = x + I_v$ for all $x \in G$, $I \in F(S)$.

(7) $(I + J)_v = (I_v + I_v)_v$

If S is a cancellative monoid with quotient group G. Then the v-operation induces an equivalence relation $\sim$ on $\mathcal{F}(S)$ defined by $I \sim J$ if $I_v = J_v$.

For $I \in \mathcal{F}(S)$, $div(I)$ represents the equivalence class of I under $\sim$ and $\check{D}(S)$ denotes the set of all divisor classes of S. Part (7) of remark 3.2.3 shows that the operation on $\check{D}$(S) defined by

$$div(I) + div(J) = div(I + J)$$

is well defined.

Under '+' the set $\check{D}(S)$ forms a commutative with zero element $div(S)$. Moreover, $\rho(S) = \{div(x+S) : x \in G\}$ is a subgroup of the group of invertible elements of $\check{D}(S)$.

Divisor Class Group

The factor $Cl(S) = \check{D}(S)/\rho(S)$ is called the divisor class monoid of S. If every fractional ideal is invertible then $Cl(S)$ become a group and called divisor class group. Also if S is completely integrally closed and cancellative monoid then $Cl(S)$ becomes a group c.f. [12, Theorem 16.5].

3.3 Class Group of Rings

Here we start this section by another look of the fractional ideal.

Fractional Ideal

Let R be a commutative ring with 1(resp. integral domain) and, the total fractional ring of R, $Q(R) = K$ (resp. quotient field of R), then $F \subseteq K$ is said to be a fractional ideal of R if F is an $R-$submodule of K such that

$$rF \subseteq R, \text{ where } r \text{ is regular element of } R.$$

Note that regular elements are those elements which are not zero divisors.

Example 3.3.1 *Let D be an integral domain and let $Q(D) = K$. Suppose $\{x_1, x_2, ..., x_n\} \subseteq K$. Consider $F =< x_1, x_2, ..., x_n >$ i.e. if $s \in F$, then $s = \sum_{i=1}^{n} r_i x_i$, where $r_i \in D$. It can be verify that F is R-submodule of K. Now let $s_i = \frac{r_i}{r_i'} \in K$, where $r_i' \in D$. and let $r = \text{lcm}(r_1', r_2', ..., r_n')$. Then easily $rF \subseteq D$. So F is a fractional ideal of K.*

Remark 3.3.2 *If $F \subseteq K$, then S may not be fractional ideal of D. Specially, when F is not finitely generated. As not then neccessary such r in D exists such that $rF \subseteq D$. It is possible when K is a fractional ideal of $D \Leftrightarrow K = D$.*

Proposition 3.3.3 *Let $S \subseteq K$ is a semigroup, then $< S >$ is a fractional ideal of D if and only if $< S >$ is contained in a fractional ideal of D.*

Remark 3.3.4 *(1) A fractional ideal F is finitely generated if it admits a finite set of generators and so principle if $F =< x >$ for some $x \in K$.*

(2). A pincipal fractional ideal $< x >$ is regular if and only if x is regular.

Definition 3.3.5 *Let D be the unitary integral domain with quotient field K then $f(D)$ represents the set of all fractional ideals of D in K.*

Definition 3.3.6 *If $F \in f(D)$, then we define*

$$F^{-1} = D : F = \{x \in K : xF \subseteq D\},$$

and

$$(F^{-1})^{-1} = D : (D : F) = \{x \in K : xF^{-1} \subseteq D\}.$$

We denote $(F^{-1})^{-1}$ by F_v.

Remark 3.3.7 *Note that F_v is the intersection of the family of principal fractional ideals of D that contains F.*

Definition 3.3.8 *The mapping $F \to F_v$ is called v-operation on D.*

Definition 3.3.9 *A fractional ideal F is called divisorial or v-ideal if $F = F_v$.*

3.3.1 Equivalence Classes

Define a relation $\sim$ on $f(D)$ by $I \sim J$ if and only if $I_v = J_v$.

Now, it is easy to prove $\sim$ is an equivalence relation

1. Reflexive:

Of-course if $I \in f(D)$, then $I_v = I_v$ implies $I \sim I$.

2. Symmetric:

If $I, J \in f(D)$ and $I \sim J$ easily implies that $J \sim I$.

3. Transitive:

Now if $I, J, L \in f(D)$ such that $I \sim J$ and $J \sim L$ implies $I_v = J_v$ and $J_v = L_v$. Follows that $I_v = L_v$, this gives the required result.

Hence $\tilde{}$ is an equivalence relation.

Definition 3.3.10 *The equivalence classes under $\sim$ are called divisor classes of D. The class of $I \in f(D)$ is denoted by div(I).*

Definition 3.3.11 *The set of all divisor classes of D is denoted by $\check{D}(D)$.*

The operation defined on $\check{D}(D)$ are as,

$$div(I) + div(J) = div(IJ),$$

under this operation $\check{D}$(D) is a commutative monoid with zero element $div(D)$. It is simple to prove that if div(I), div$(J) \in \check{D}(D)$, then

$$div(I) + div(J) = div(IJ) \in \check{D}(D) \text{ as } IJ \in f(D), \ .$$

and also associative. Further,

$$div(I) + div(D) = div(ID) = div(I),$$

as $ID = I$, because I is $D-$submodule of K.

Remark 3.3.12 *$\check{D}(D)$ is a group if and only if D is completely integrally closed [12, page 208-209].*

Remark 3.3.13 *The set $\rho(D) = \{div(xD) : x \in K, x \neq 0\}$ is a subgroup of the group of invertible elements of $\check{D}(D)$. Because,*

$$div(xD) + div(x^{-1}D) = div(D).$$

This implies $div(xD) \in Inv(D)$, where $Inv(D)$ represents the set of all invertible divisorial classes of D. Hence $\rho(D) \subseteq Inv(D)$ If $div(xD), div(yD) \in \rho(D)$, then $div(xD) + [div(yD)]^{-1} = div(xy^{-1}D) \in \rho(D)$, as $xy^{-1} \in K$. Hence gives the required result.

Definition 3.3.14 *The divisor class monoid of D, $Cl(D)$ is defined as $Cl(D) = \check{D}(D)/\rho(D)$.*

Now the elements of $Cl(D)$ are $[div(I)] = div(I) + \rho(D)$ for $I \in F(D)$. Now under the following operation $Cl(D)$ can easily be seen as monoid.

$$\begin{aligned} [div(I)] + [div(J)] &= (div(I) + \rho(D)) + (div(J) + \rho(D)) \\ [div(I)] + [div(J)] &= (div(I) + div(J)) + \rho(D) \\ [div(I)] + [div(J)] &= div(IJ) + \rho(D) = [div(IJ)] \end{aligned}$$

Note that if D is completely integrally closed then $Cl(D)$ is divisor class group.

Remark 3.3.15 *If D is UFD, then it is easy to verify that every fractional ideal is invertible and hence $\rho(D) = \check{D}(D)$. This implies that $Cl(D)$ is trivial, c.f.[12, page 209].*

Chapter 4

Characterization of Polynomial Rings with the Half-Factorial Property

4.1 Introduction

In this chapter we review the paper [9] of Coykendall.

The main result of this paper gives the characterization of polynomial rings with the half factorial property. Which is stated as " Let R be an integral domain. If $R[X]$ is HFD then R is integrally closed". For the sake of completion and better understanding, here we are providing the explanation of [9].

4.2 Characterization of Polynomial Rings with the Half-Factorial Property

We start this chapter by the following:

Lemma 4.2.1 *[9, Lemma2.1] Let $p(X)$ be irreducible in $R[X]$ and $0 \neq r \in R$. If $rp(X) = r_1 r_2 ... r_t f_1 f_2 ... f_k$ with $r_i \in R$ for $1 \leq i \leq t$ and $f_i \in R[X]$ with $0 < deg(f_i) < deg(p)$ for $1 \leq i \leq k$, then no f_i is monic.*

Proof: We prove the result by contrary. Let some f_i is monic, then if

$$p(X) = q_{n+m}X^{n+m} + q_{n+m-1}X^{n+m-1} + ... + q_1X + q_0,\ q_i \in R$$

then $rp(X)$ can be written as,

$$rp(X) = (r_nX^n + ... + r_0)(X^m + s_{m-1}X^{m-1} + ... + s_0) = g_1(X)g_2(X), \quad n \geq 1.$$

Now equating the co-efficient of $X^{m+n}, X^{m+n-1}, ..., X^m$. *i.e*

$$\begin{aligned} r_n &= rq_{n+m} \\ r_{n-1} + r_ns_{m-1} &= rq_{m+n-1} \end{aligned}$$

continuing this, we get

$$r_0 + r_1s_{m-1} + ... + r_ms_0 = rq_m$$

By above equations we have $r \mid r_n \in R$ as $q_{n+m} \in R$. In the same manner, we get r$\mid r_i$ for each $0 \leq i \leq n$. So, r is the factor of $r_n, ..., r_0$. Now $g_1(X) = rg(X)$ for $g(X) \in R[X]$, here

$$\begin{aligned} rp(X) &= rg(X)g_2(X) \\ \Rightarrow \quad & p(X) = g(X)g_2(X). \end{aligned}$$

Since deg(g) and deg(g_2) > 0,therefore $g(X)$ and $g_2(X)$ are non-unit. Hence $p(X)$ is reducible. This contradicts the given hypothesis. So all f_i's are non-monic.

This lemma will play a useful role in proving the main theorem.

Theorem 4.2.2 *[9, Theorem 2.2] Let R be an integral domain. If $R[X]$ is an HFD, then R is integrally closed.*

Proof: Here we are given that $R[X]$ is an HFD $\Rightarrow$ R is HFD (If not then $R[X]$ will not be an HFD [2]). So in this whole proof R will be assume to be

HFD. Now to prove the result let R is not integrally closed. We will prove $R[X]$ is not HFD. Now if R is not integrally closed then there exist $w \in K \backslash R$, where K is the quotient filed of R such that w satisfies following irreducible monic polynomial $P(X) \in R[X]$,

$$P(X) = X^n + p_{n-1}X^{n-1} + ... + p_1X + p_0, \quad p_{i,s} \in R$$

We can assume that $w = r/s$, $r, s \in R$, such that $(r, s) = 1$ and of-course $s \neq 0$. (It is possible as R is HFD). Now consider

$$s^nP(X) = s^nX^n + s^np_{n-1}X^{n-1} + ... + s^np_1X + p_0s^n$$

Since $P(w) = 0$, therefore $s^nP(w) = 0$. Hence we can write,

$$s^nP(X) = (sX - r)q(X), \quad q(X) \in R[X]$$

One can verify that $s.r/s - r = 0 \Rightarrow s^nP(w = r/s) = 0$. Now if s has m irreducible factors then,

1. s^n has mn irreducible factors and $s^nP(X)$ has $mn+1$ irreducible factors as $P(X)$ is irreducible.

2. Polynomial $(sX - r)$ is irreducible in $R[X]$ as $(r, s) = 1$.

Now we check how many irreducible factors $q(X)$ has. Note that as we take s common from $s^nP(X)$, so leading co-efficient of $q(X)$ is s^{n-1}. Let

$$q(X) = f_1(X)f_2(X)...f_k(X)r_1r_2...r_t$$

$f_i \in R[X]$ is irreducible and $r_i \in R$ is irreducible.

Now by above lemma as

$$\begin{aligned} s^nP(X) &= (sX - r)q(X) \\ s^nP(X) &= (sX - r)f_1(X)f_2(X)...f_k(X)r_1r_2...r_t \end{aligned}$$

$\Rightarrow$ each f_i is non-monic. Since $(sX - r) \in R[X]$ and $\deg(sX - r) < \deg(P)$. Now as s^{n-1} is the leading coefficient of $q(X)$ so, each f_i contributes a factor for f_i so let

$$s^{n-1} = L_1 L_2 ... L_k r_1 r_2 ... r_t$$

With each L_i is non-unit leading coefficient of f_i, as each f_i is non-monic. Now $s^{n-1} \in R$ and R is HFD, So

$k+t \leq m(n-1)$ as m no of factors of s and so $m(n-1)$ is the no factors of s^{n-1}

So the number of factors of s^n are $m(n-1)+1$. Now

$$k + t + 1 \leq m(n-1) + 1 \leq mn + 1$$

Since as $R[X]$ is HFD. Therefore, the number of factors of s^n for each expression are equal, So $m(n-1)+1 = mn+1$ possible only when $m = 0 \Rightarrow s = 0$. Hence $w \notin K \backslash R$. A contradiction to the supposition, so we have the result.

Remark 4.2.3 *If $R[X]$ is a BFD, then by a result $R[X]$ is BFD $\Longleftrightarrow$ R is BFD. Now here it is not necessary that it is integrally closed. As it is known that every Noetherian is not necessarily integrally closed and also we know that every Noetherian is BFD. So, we can not generalize this result for BFDs.*

Remark 4.2.4 *Here note that if the coefficient ring R is HFD does not necessarily implies R is integrally closed for example let $R = Z[i\sqrt{3}] = \{a + bi\sqrt{3} : a, b \in Z\}$ is a commutative ring which is HFD but not integrally closed because closure of R $(\acute{R})$ is given by*

$$\acute{R} = \mathbf{Z}\left[\frac{-1 + i\sqrt{3}}{2}\right]$$

Hence R is not integrally closed. Further note that R is not Krull as if R is Krull then R must be then integrally closed.

Corollary 4.2.5 *[9, Corollary 2.3] Let R be a Noetherian ring. Then the following conditions are equivalent*

(1) R is a Krull domain with $|cl(R)| \leq 2$.

(2) $R[X]$ is an HFD.

(3) $R[X_1, X_2, ..., X_n]$ is an HFD for all $n \geq 1$.

(4) $R[X_1, X_2, ..., X_n]$ is an HFD for some $n \geq 1$.

Proof: We can observe that (3) $\Rightarrow$ (4) and (4) $\Rightarrow$ (2) are very obvious. Only (1) $\Rightarrow$ (3) and (2) $\Rightarrow$ (1) remains to prove.

(1) $\Rightarrow$ (3)

Given that R is a Krull domain and $|cl(R)| \leq 2$ then $R[X_1, X_2, ..., X_n]$ is also a Krull domain with $|cl(R[X_1, X_2, ..., X_n])| = |Cl(R)|$ [7, chapter 7, Proposition 13]. Since if R is a Krull domain then $R[X]$ is an HFD if and only if $|Cl(R)| \leq 2$ [20, Theorem 2.4].Using above both results we prove the required result inductively.

If $n = 1$ then as R is Krull and $|Cl(R)| \leq 2$ then $R[X_1]$ is HFD.

Suppose it is true for $n = k$ then $R[X_1, X_2, ..., X_k]$ is HFD. Now it is to verify the second condition that $R[X_1, X_2, ..., X_{k+1}]$ is HFD. Now as R is a Krull domain and $|Cl(R)| \leq 2$.

So, $R[X_1, X_2, ..., X_{k+1}]$ is Krull with $|cl(R[X_1, X_2, ..., X_{k+1}])| = |Cl(R)| \leq 2$.

$\Rightarrow R[X_1, X_2, ..., X_{k+1}]$ is HFD. Hence the result.

(2) $\Rightarrow$ (1)

We assume that $R[X]$ is an HFD, then by previous theorem R is integrally closed. Now as R is Noetherian so R is a Krull domain. Again, by [20, Theorem 2.4], $R[X]$ is HFD so $|Cl(R)| \leq 2$. Which is the desired result.

Chapter 5

Characterization of Semigroup Rings with the Half-Factorial Property

5.1 Introduction

In this chapter we characterize the semigroup rings with the half factorial property which is an attempt to generalize the polynomial case of Coykendall's [9, Theorem 2.2]. The details are already given in chapter 4. Here we used the concepts of degree in semigroup rings which are coinciding the particular case of polynomial rings. Moreover, we introduced the term of monic elements or pseudo monic polynomials in commutative semigroup rings.

5.2 Characterization of Semigroup Rings with the Half-Factorial Property

We are starting by introducing the notions in semigroup rings which coincides to the polynomial structure.

Concept of Degree and Order in Semigroup Ring

The concept of degree and order are not generally defined in semigroup rings. They actually depends upon the relation under which S is totally or-

dered.

If the semigroup S is ordered under a fixed total ordered, then the usual notion of degree and order of elements of semigroup ring $R[X;S]$ can be defined. Thus, if $f = \sum_{i=1}^{n} f_i X^{si}$ is the canonical form of the non-zero element $f \in R[X;S]$, where $s_1 < s_2 < ... < s_n$, then s_n is called the degree of f and we write $\deg(f) = s_n$ and similarly the order of f written as $ord(f) = s_1$. Now if R is integral domain, then we have as usual,

$$\begin{aligned} \deg(fg) &= \deg(f) + \deg(g) \\ ord(fg) &= ord(f) + ord(g) \quad \text{for } f, g \in R[X;S] \end{aligned}$$

Monic Element (*pseudo monic polynomial*)

Now we are in position to define the monic element (pseudo monic polynomial) of $R[X;S]$. The element f of $R[X;S]$ is monic if $f_n = 1_R$ (Of-course possible when R is unitary).

Pseudo Integral Element

Let D be an integral domain and S be a cyclic semigroup. Then an element of $Q(D)$ is said to be integral over D if it satisfies a monic element (pseudo monic polynomial) of $D[X;S]$. Similarly, if D_* represents the set of all pseudo integral element then D is said to be pseudo integrally closed if $D_* = D$.

Note that all elements of the coefficient ring D of $D[X;S]$ (with D is unitary and S is cyclic monoid have at least one positive integer) are pseudo integral as if $r \in D$ then r satisfies $r^s - X^s \in D[X;S]$, where s is positive integer in S.

Lemma 5.2.1 *Let S be semigroup. Then S is cyclic if and only if $s_{m+n} = s_m + s_n$ for all $s_{m+n}, s_m, s_n \in S$ and $m, n \in \mathbf{Z}^+$.*

Proof: Let $S =< a >$ then we prove that $s_{m+n} = s_m + s_n$ for all $s_{m+n}, s_m, s_n \in S$ and $m, n \in \mathbf{Z}^+$. By given hypothesis we can write that

$s_m = ma$ and similarly $s_n = na$, this implies that $s_{m+n} = s_m + s_n$, which is required.

Conversely suppose that $s_{m+n} = s_m + s_n$ for all $s_{m+n}, s_m, s_n \in S$ and $m, n \in \mathbf{Z}^+$, then we want to prove that S is cyclic. For this let $s_m \in S$. We can write $s_m = ma = (m-1)a + a$, continuing this we get at the end

$$s_m = a + a + ... + a, \text{ m times},$$

$\Rightarrow s_m = ms_1 \Rightarrow S =< s_1 >$. Also it is easy to verify that s_1 is the least generator for s_m. Hence the result.

Remark 5.2.2 *Let S be cyclic monoid which has no invertible element and D be the integral domain then the unit elements of the semigroup ring $D[X;S]$ are same as that of the coefficient ring D, it is deduced from [12, Theorem 11.1].*

Irreducible elements in $D[X;S]$

Let S be the cyclic semigroup and D be the integral domain then an element $f \in D[X;S]$ is said to be irreducible if $f = hk$ for some $h, k \in D[X;S] \Rightarrow$ either h is unit or k is unit.

By using these concepts we develop the following lemma.

Lemma 5.2.3 *Let D be an integral domain and S is a cyclic monoid. Let $p(X)$ be irreducible in $D[X;S]$, and $0 \neq r \in D$. If $rp(X)=r_1r_2...r_tf_1f_2...f_k$ with $r_i \in D$ for $1 \leq i \leq t$ and $f_i \in D[X;S]$ with $0 < deg(f_i) < deg(p(X))$ for all $1 \leq i \leq k$, then no f_i is monic.*

Proof : As given S is a cyclic. Let $S =< a >$. We define an element $s \in S$ by s_m if $s = ma$ and a total ordered operation $<$ by $s_m < s_n$ if and only if $m < n$ for all $m, n \in Z^+$. Consider

$$p(X) = r_{s_{n+m}}X^{s_{n+m}} + r_{s_{n+m-1}}X^{s_{n+m-1}} + ... + r_{s_0}X^{s_0} \in D[X;S]$$

such that $s_0 < s_1 < ... < s_{m+n}$. Hence the leading coefficient is $r_{s_{n+m}}$ and the degree of $p(X)$ is s_{m+n}. To prove the required result, let us suppose there are some $f_{i's}$ are monic. Now write,

$$\begin{aligned} rp(X) &= (r'_{s_n}X^{s_n} + r'_{s_{n-1}}X^{s_{n-1}} + ... + r'_{s_0}X^{s_0})(X^{s_m} + r'_{s_{m-1}}X^{s_{m-1}} + ... + r'_{s_0}X^{s_0}) \\ &= g_1(X)g_2(X) \text{ where } g_1(X), g_2(X) \in D[X;S]. \end{aligned}$$

Note that here by using above lemma we can write, $s_{m+n} = s_m + s_n$ for all $m, n \in Z^+$. Now equating co-efficient of $X^{s_{n+m}}, X^{s_{n+m-1}}, ..., X^{s_0}$ we get,

$$\begin{aligned} r'_{s_n} &= r.r_{s_{n+m}} \\ r'_{s_{n-1}} + r'_{s_n}r'_{s_{m-1}} &= r.s_{m+n-1} \end{aligned}$$

and similarly continuing this we get,

$$r'_{s_0} + r'_{s_1}r'_{s_{m-1}} + ... + r'_{s_m}r'_{s_0} = r.r_{s_m}.$$

Consequently, we have $r \mid r'_{s_n}$ as $r_{s_{m+n}} \in D \Rightarrow r \mid r'_{s_{n-1}}$ and by continuing this, we have $r \mid r'_{s_0}$. Hence we get that $r \mid r'_{s_i}$ for all $0 \leq i \leq n$. So, we can write,

$$\begin{aligned} rp(X) &= rg(X)g_2(X), \text{ where } g(X) \in D[X;S] \\ p(X) &= g(X)g_2(X), \end{aligned}$$

where $g(X)$ and $g_2(X)$ are non-unit $\Rightarrow p(X)$ is reducible. A contradiction. Hence no f_i is monic.

Example 5.2.4 *Let $S = \mathbf{Z}_0$ or $\mathbf{Z}$, the set of non-negative integers or set of integers is a total order monoid and also $s_{n+m} = s_n + s_m$, where $s_n = n$, $s_m = m$ and $s_{m+n} = m + n$ for all $m, n \in S$. Now if D is an integral domain then the monoid ring obeys the above lemma.*

Now, we are able to develop a generalized form of Coykendall's [9, Theorem 2.2] in the following

Theorem 5.2.5 *Let D be an integral domain and S is cyclic monoid have at least one positie integer. If $D[X;S]$ is an HFD, then D is pseudo integrally closed.*

Proof: Here we are given that $D[X;S]$ is an HFD $\Rightarrow$ D is HFD. So in this whole proof D will assume to be HFD. Since S is cyclic therefore $S =< a >$. So we can write $s_m = ma$ and $s_{m+n} = s_m + s_n$ for all $m, n \in Z^+$. Define a total order relation on S by $s_m < s_n$ if and only if $m < n$.

Let us suppose D is not integrally closed. Now, if D is not integrally closed then there exist $w \in K\backslash D$, where $K = Q(D)$ such that w satisfies following irreducible pseudo monic polynomial $p(X) \in D[X;S]$,

$$p(X) = X^{s_n} + r_{s_{n-1}}X^{s_{n-1}} + ... + r_{s_0}X^{s_0}, r_{si} \in D.$$

Where $s_0 < s_1 < ... < s_n$, so s_n is the degree of $p(X)$ and the leading coefficient is 1. Note $w \notin D$ shows D is not integrally closed. Also we can assume that $w = r/s$, $r, s \in D$, such that $(r, s) = 1$ and of-course $s \neq 0$. (It is possible as D is HFD). Now consider

$$s^n p(X) = s^n X^{s_n} + s^n r_{s_{n-1}}X^{s_{n-1}} + ... + s^n r_{s_0}X^{s_0}.$$

Since $p(w) = 0$, therefore $s^n p(w) = 0$, hence we can write,

$$s^n P(X) = (sX - r)q(X), \quad q(X) \in D[X;S].$$

Now one can verify $s.r/s - r = 0 \Rightarrow s^n p(w = r/s) = 0$. Now if s has m irreducible factors then,

1. s^n has mn irreducible factors and $s^n p(X)$ has $mn+1$ irreducible factors as $p(x)$ is irreducible.

2. Polynomial $(sX - r)$ is irreducible in $D[X;S]$ as $(r,s) = 1$.

Now we check how many factors $q(X)$ has? Note that as we take s common from $s^n p(X)$, so the leading co-efficient of $q(X)$ is s^{n-1}. Let

$$q(X) = f_1(X)f_2(X)...f_k(X)r_1r_2...r_t, \text{ such that}$$

$f_i \in D[X;S]$ are irreducible and $r_i \in D$ are irreducible. By lemma 5.2.3

$$\begin{aligned} s^n p(X) &= (sX - r)q(X) \\ s^n p(X) &= (sX - r)f_1(X)f_2(X)...f_k(X)r_1r_2...r_t. \end{aligned}$$

Thus, each f_i is non-monic. Note $(sX - r) \in D[X;S]$ and $\deg(sX - r) < \deg(p)$. Now as s^{n-1} is the leading coefficient of $q(X)$ so, each f_i contributes a factor for $q(X)$ so let

$$s^{n-1} = L_1L_2...L_kr_1r_2...r_t.$$

Where each L_i is non-unit, as each f_i is non-monic and leading coefficient of f_i. Now $s^{n-1} \in D$ and D is HFD, So

$$k + t \leq m(n-1) \text{ and } m(n-1) \text{ is the number of factors of } s^{n-1}.$$

So number of factors of s^n are $m(n-1) + 1$.

Now

$$k + t + 1 \leq m(n-1) + 1 \leq mn + 1.$$

But as $D[X;S]$ is HFD. Therefore, the number of factors of s^n for each expression are equal, So $m(n-1) + 1 = mn + 1$ is possible only when $m = 0 \Rightarrow s = 0 \Rightarrow w \notin K \backslash D$. A contradiction. Hence the proof.

Chapter 6

Factorization Properties in Semigroup Rings

6.1 Introduction

In this chapter we generalize the result of [20, Theorem 2.4], which is stated as "if R is Krull with $|Cl(R)| \leq 2$, then $R[X]$ is HFD" for the semigroup ring $R[X;S]$, whenever the coefficient ring R to be Krull with $|Cl(R)| \leq 2$.

We begin by an example of trivial class group of a commutative ring.

Example 6.1.1 *Let D =Z and of-course $Q(D) = \mathbf{Q} = K$(say). Now first we find the fractional ideals of D. It is easy to verify that D has the fractional ideal of the type $S =< x_1, x_2, ..., x_n >$, where $x_i \in K$. Now, let $r \in D$ such that $r = \text{lcm}(r_1, r_2, ..., r_n)$ where $x_i = s_i/r_i$, $s_i, r_i \in \mathbf{Z}$, then it is easy to verify that $rS \subseteq D$. It is observe that $S =< x_1, x_2, ... >$ is not fractional ideal, infact there does not exist an $r \in D$ such that $rS \subseteq D$. Hence at the end we get that*

$$f(D) = \{S \subseteq K : S =< x_1, x_2, ..., x_n >, x_i \in K\}.$$

Since we know that F_v is the intersection of the family of principal fractional ideals that contains F, Therefore, F is contained in a principal fractional ideal. Hence it is principal fractional by itself. Thus, by [12, page-208] $F_v = F$. This

means, $\check{D}(D)$ and $\rho(D)$ coincides and hence,

$$Cl(D) = \{\rho(D)\}$$

6.2 Construction of trivial class group of a semigroup

Now, we wish to derive some conditions that yields $Cl(S)$ is trivial (where S is a semigroup). For this we are establishing the following:

Proposition 6.2.1 *Let S be a cancellative completely integrally closed semigroup. Let $I \in F(S)$ and $x \in G$,the quotient group of S, then there exist $y \in G$ such that $(x + I + S)_v = (y + S)_v$ if and only if $Cl(S) = \{\rho(S)\}$(trivial class group).*

Proof: Suppose for all $I \in F(S)$ and $x \in G$, there exist $y \in G$ such that $(x + I + S)_v = (y + S)_v$. We want to show that the class group of S is trivial. For this consider,

$$\begin{aligned} Cl(S) &= \{div(I) + \rho(S)\} \\ &= \{\{div(I + x + S) : x \in G\}\} \\ &= \{\{div(y + G) : y \in G\}\} \\ &= \{\rho(S)\}. \end{aligned}$$

Conversely, let $Cl(S) = \{\rho(S)\}$. Let $div(I) + \rho(S) \in Cl(S)$, then by given hypothesis,

$$\begin{aligned} div(I) + \rho(S) &= \rho(S) \\ &\Rightarrow \{div(x + I + S) : x \in G\} = \{div(x + S) : x \in G\} \\ &\Rightarrow div(x + I + S) = div(y + S) \\ &\Rightarrow (x + I + S)_v = (y + S)_v. \end{aligned}$$

Proposition 6.2.2 *Let G be a quotient group of a cancellative completely integrally closed semigroup S. Suppose $x+(I+S)=S$ for all $x \in G$ and for all $I \in F(S)$ and $\bigcup_i I_i = G$ for all $I_i \in F(S)$, then $Cl(S) = \{\{\{S\}\}\}$.*

Proof: This is to show that $Cl(S) = \{\{\{S\}\}\}$ or equivalent to show that

$$div(x+(I+S)) = \{S\}$$

or equivalently, to show that

$$\begin{aligned} x+(I+S) &\sim S. \text{ Since } x+(I+S)=S \text{ but } x+(I+S) \sim x+(I+S). \\ \text{It means } (x+(I+S))_v &= S_v. \end{aligned}$$

For this let

$$x+(I+S) = J,$$

then

$$\begin{aligned} J_v &= S:(S:J) \\ J_v &= S:\{\acute{x} \in G : \acute{x}+J \subseteq S\}. \\ \text{Since } x+(I+S) &= S \text{ for all } x \in G, \text{ therefore } J_v = S:G. \\ \text{Now } S_v &= S:(S:S). \\ \text{This implies } S_v &= S:\{x \in G : x+S \subseteq S\} \end{aligned}$$

Now as $x \in I$, for some I$\in F(S)$ as $UI_i = G$, therefore

$$\begin{aligned} 0+x+S &\subseteq S, \text{ as } 0 \in S \\ \text{This implies } S_v &= S:G, \text{ so } J_v = S_v. \\ \text{Hence } J_v &= S_v \\ \text{i.e. } (x+I+S)_v &= S_v. \\ \text{Thus } x+(I+S) &\sim S. \end{aligned}$$

Now, it is remain to show that,

$$x + (I + S) \nsim J \neq S \text{ for all } J \in F(S)$$

$$\begin{aligned} \text{Since, } (x + (I + S))_v &= S : G \\ \text{Now, } J_v &= S : (S : J) \\ &= S : \{x \in G : x + J \subseteq S\} \end{aligned}$$

Now we want to show that $\{x \in G : x + J \subseteq S\} \neq G$.

As G is a group $\Rightarrow 0 \in G$ and let $y \in J$ such that $y \notin S$.

We can do this because $J \neq S$. We have $0 + y \notin S$, so, $0 + J \subseteq S$. Hence we have

$$\begin{aligned} G &\neq \{x \in G : x + J \subseteq S\} \\ &\Rightarrow J_v \neq S : G \\ &\Rightarrow x + (I + S) \nsim J. \end{aligned}$$

Hence we have,

$$div(x + (I + S)) = \{S\},$$

which gives the required result.

Remark 6.2.3 *(1) Let S be a cancellative completely integrally closed semigroup. If $Cl(S) = \{\{\{S\}\}\}$, then $Cl(S) = \{\rho(S)\}$. Indeed; Let $div(I) + \rho(S) \in Cl(S)$. Then by given hypothesis, we have*

$$\begin{aligned} div(I) + \rho(S) &= \{\{S\}\} \\ \text{and similarly } \rho(S) &= \{\{S\}\}. \end{aligned}$$

Hence, $div(I) + \rho(S) = \rho(S) \Rightarrow Cl(S) = \{\rho(S)\}$.

(2) Both the propositions 6.2.1 and 6.2.2 gives the conditions on a cancellative completely integrally closed semigroup S that make its class group

trivial. But in the proposition 6.2.2 the conditions on S are stronger then the proposition 6.2.1.

The following example justify the above proposition 6.2.2.

Example 6.2.4 *Let $S = Z$ a completely integrally closed cancellative monoid, then quotient group $G = Z$ by considering a cancellative subsemigroup $C = 2Z$ or $C = Z$ of S. Now S is a fractional ideal of itself. Now let $I \subseteq G$ be any proper subset of S. We prove that I is not a fractional ideal of S. Now of-course I satisfies second condition of fractional ideals as given above i.e. $\forall s \in S$ such that $s + I \subseteq S$. We check it for the second condition $s + I \subseteq I$ in otherwords $s + i \in I$ for all $i \in I$ and $s \in S$. Now as I is a proper subset of Z so there exist $s' \in Z$ such that $s' \notin I$. Now if $i \in I$ then i can be written as*

$$i = s' + t,$$

for some $t \in Z$. Now here $t + i = s' \notin I$. Which means I is not a fractional ideal of S. Hence S is the only fractional ideal of itself. So $F(S) = \{S\}$ and hence

$$\begin{aligned} div(S) &= \{S\} \Rightarrow f(S) = \{\{S\}\} \text{ and} \\ \check{D}(S) &= \{div(x + S)/x \in G\} \\ \check{D}(S) &= \{div(S)\} \\ \check{D}(S) &= \{\{S\}\} \end{aligned}$$

$\Rightarrow$

$$Cl(S) = \check{D}(S)/\rho(S) = \{S\} + \{\{S\}\} = \{\{S\}\} = 0,$$

identity of $Cl(S)$. A trivial group.

Also we can verify that S satisfies the conditions of 6.2.2. as S is the only fractional ideal of S, so $x + (I + S) = S$ for all $x \in S$ and $I = S$ is the

only fractional ideal of S. And the second condition is very obvious, that is $\cup I = G = S$. *Hence this example verify the above propositon 6.2.2 and the Remark 6.2.3.*

Lemma 6.2.5 *Let S be any finitely generated semigroup. Let* $s, s' \in S$, *than there exist* $t \in S$ *such that* $s = s' + t$.

Proof: Let $S =< s_1, s_2, ..., s_n >$. As $s, s' \in S$, so we can write

$$\begin{aligned} s &= n_1 s_1 + n_2 s_2 + ... + n_n s_n \text{ for } n_i \in \mathbf{Z}^+ \text{ and} \\ s' &= n_1' s_1 + n_2' s_2 + ... + n_n' s_n \text{ for } n_i' \in \mathbf{Z}^+ \end{aligned}$$

As n_i and n_i' are integers, therefore we can write

$$n_i = n_i' + l_i \text{ for some } l_i \in \mathbf{Z}^+$$

Suppose

$$t = l_1 s_1 + l_2 s_2 + ... + l_n s_n \in S$$

This implies that $s = s' + t$. Hence the result.

In the following, we are giving another example, which justify the proposition 6.2.2 and Reamark 6.2.3.

Example 6.2.6 *Let S be any abelian group. Here note that as S is a group then it is obvious that S is completely integrally closed and cancellative. Since S is an abelian group so* $S = G$, *where G is the quotient group of S.*

Since S is a group so $0 \in S$. *Now let* $I \subseteq G$ *is any fractional ideal of S. Here note that* $G = S$, *so* $I \subseteq S$. *We want to prove that* $x + (I + S) = S$ *for all* $x \in G = S$ *and for all* $I \in F(S)$. *Also to prove that* $\bigcup_i I_i = G$ *for all* $I_i \in F(S)$.

First we ahve to prove $x + (I + S) = S$ *for all* $x \in G = S$ *and for all* $I \in F(S)$. *Now as* $x \in S$ *and* $I \subseteq S$ *so this implies* $x + (I + S) \subseteq S$. *So,* $S \subseteq x + (I + S)$ *is remain to prove.*

For this let $s' \in S$. Let $i \in I \Rightarrow i \in S \Rightarrow -i \in S$. But as I is a fractional ideal of S, so $S + I \subseteq I \Rightarrow i + (-i) \in I \Rightarrow 0 \in I$. Now, we can write $s' = s' + (0 + 0) \in x + (I + S)$. This implies $S = x + (I + S)$.

Now, we prove that $\bigcup_i I_i = G$, for all $I_i \in F(S)$. But here we have $I \subseteq S = G$ and S is of-course the fractional ideal of S means S is the largest or maximal fractional ideal of S. This leads us to the required proof. Hence we prove that S satisfies both the conditions as specified in the lemma 6.2.5. Now to verify that lemma we show that $Cl(S)$ is trivial.

We first find (S), the set of all divisorial classes. For this let $I \in F(S)$, then

$$\begin{aligned}
S &: I = \{x \in G = S : x + I \subseteq S\} \\
S &: I = \{x' - i : \forall i \in I \text{ and } x' \in S\}. \\
\text{Now, } S &: (S : I) = \{x' \in G = S : x' + (S : I) \subseteq S\} \\
&= \{x' \in S : x' + (x - i) \in S \forall i \in I \text{ and } x \in S\} \\
&= \{x' + (x - i) : \forall x', x \in S \text{ and } i \in I\} \\
&= \{y - i : \forall y \in S \text{ and } i \in I\}.* \qquad (6.1)
\end{aligned}$$

As $I \subseteq S$, this implies $S : (S : I) \subseteq S$.

Conversly, let $s \in S$. Since $0 \in I$, so by (*) $s = s - 0 \in S : (S : I)$ $\Rightarrow S \subseteq S : (S : I)$. Hence

$$I_v = S : (S : I) = S, \quad \text{for all } I \in F(S).$$

This implies $\check{D}(S) = \{div(I)\}$.

$$\begin{aligned}
Cl(S) &= (S)/\rho(S) \\
&= \{div(I)\}/\{div(x + S) : x \in G\} \\
&= \{div(I) + div(x + S) : \forall x \in G\} \\
&= \{div(x + (I + S)) : \forall x \in G\}
\end{aligned}$$

But we know that $I_v = S$, for all $I \in F(S) \Rightarrow Cl(S)$ is singleton, i.e. it has only one divisorial class. So

$$\begin{aligned} Cl(S) &= \{div(x + I + S) : x \in G\}. \\ \text{Also, } Cl(S) &= \{div(x + S) : x \in G\} \\ &= \{\rho(S)\}, \text{ a trivial class group.} \end{aligned}$$

Hence the result.

6.3 Half Factorial Semigroup Rings

In this section we established a criteria for a semigroup ring to be an HFD.

Following [12, page 192], let F=$\sum_{i\in I} \mathbf{Z}e_i$ be a free abelian group with free basis $\{e_i\}_{i\in I}$. For $j \in I$, the mapping $\pi_j : F \to \mathbf{Z}$ denoted by $\pi_j . \sum_{i\in I} n_i e_i = n_j$ is called the jth projection map on F. It is, ofcourse, rank-one discrete valuation on F. The family $\{\pi_i\}_{i\in I}$ is of finite character, and we denote by F_+ the krull monoid determined by this family; thus $F_+ = \{\sum_{i\in I} n_i e_i : n_i \geq 0 \text{ for each } i \in I\}$, the positive cone of F under the cordinal order.

Remark 6.3.1 *[12, Theorem 15.2] Let H be the group of invertible elements of S. The following conditions are equivalent.*

(1) S is a krull monoid.

(2) S is of the form $H \oplus T$, where T is of the form $M \cap F_+$ for some free group F and some subgroup M of F.

(3) S is of the form $H \oplus T$, with T is of the form $G \cap F_+$ where F is a free group and G is the quotient group of T.

By [12, pge 205], if T is of the form $M \cap F_+$, where $F = \sum_{\alpha\in A} \mathbf{Z}e_\alpha$ is free on $\{e_\alpha\}_{\alpha\in A}$, the monoid domain $D[T]$ can be as a regarded as a subring of the polynomial ring $D[\{X_\alpha\}_{\alpha\in A}]$ over D. Moreover, $D[T]$ is generated as ring over

D by "pure monomials" $X_{\alpha_1}^{e_1} X_{\alpha_2}^{e_2} ... X_{\alpha_n}^{e_n}$, with $e_i \geq 0$, for each i. Conversely, each ring $D[\{m_\beta\}_{\beta \in B}]$, where each m_β is a pure monomial in the indeterminates X_α, is of the from $D[U]$, where U is the submonoid of F_+.

We start by recording [12, Theorem 15.2] as

Remark 6.3.2 *Let D be a Noetherian integrally closed domain and $\{X_i\}_{i=1}^n$ is a finite set of indeterminates X_i. Let T be the monoid generated by the pure monomials $\{m_\alpha\}_{\alpha \in A}$ of X_i, s, then for $R = D[\{m_\alpha\}_{\alpha \in A}] = D[T]$, the following assertions are equivalent*

(a) T is finitely generated and integrally closed.

(b) R is Noetherian and integrally closed.

(c) R is a Krull domain.

Now we are asking the following

Conjecture

Is there exist a monoid which is finitely generated by pure monomials $\{m_\alpha\}_{\alpha \in A}$ of indeterminates $\{X_i\}_i^n$ over the Noetherian integrally closed domain D ?

The response of said conjecture is in affirmation. For this we pass the following stages. Given D is Noetherian, so every ascending chain of ideals in $D[X_1, X_2, ..., X_n]$ is stationary. So, therefore we consider the terminating ascending chain of principal ideals generated by pure monomials;

$$< m_{\alpha_1} > \subseteq < m_{\alpha_2} > \subseteq ... \subseteq < m_{\alpha_k} >$$

$\Rightarrow m_{\alpha_k} \mid m_{\alpha_{k-1}}, m_{\alpha_{k-1}} \mid m_{\alpha_{k-2}}, ..., m_{\alpha_2} \mid m_{\alpha_1}$.

Hence obviously there exist a monoid generated by $\{m_{\alpha_i}\}_{i=1}^k$.

In the following we are giving, when the class group of semigroup ring is same as the class group of its coefficient ring.

Theorem 6.3.3 *Let D be an integral domain and G be a quotient group of a cancellative completely integrally closed semigroup S such that $x+(I+S) = S$ for all $x \in G$ and for all $I \in F(S)$ and $\bigcup_i I_i = G$ for all $I_i \in F(S)$. If $D[X;S]$ is Krull domain, then $Cl(D[X;S]) = Cl(D)$.*

Proof: Since for a Krull domain $D[X;S]$, we have $Cl[D[X;S]) \simeq Cl(D) \oplus Cl(S)$. It is due to [12, Corollary 16.8]. Now using above proposition 6.2.2 and Remark 6.2.3 to get $Cl[D[X;S]) \simeq Cl(D)$, because $Cl(S) \simeq \{\rho(S)\}$ a trivial class group.

Remark 6.3.4 *In above theorem if $Cl(D[X;S]) \simeq Z_2$, then $Cl(D) \simeq Z_2$.*

Now we are able to say about Half Factorial semigroup rings authentically as;

Theorem 6.3.5 *Let D be a Noetherian integrally closed domain and the integrally closed monoid S which is finitely generated by pure monomials $\{m_\alpha\}$ of indeterminates $\{X_i\}_{i=1}^n$ over D. Then $D[X;S]$ is HFD $\Leftrightarrow$ $Cl(D[X;S]) \simeq Z_2$.*

Proof: By Remark 6.3.2 $D[X;S]$ is krull and due to [12, Corollary 16.8] $Cl(D[X;S]) = Cl(D) \oplus Cl(S)$. Now, let us suppose $D[X;S]$ is HFD $\Leftrightarrow |Cl(D[X;S])| \leq 2, c.f.$ [20, Theorem 2.4]. This implies $Cl(D[X;S]) \simeq Z_2$.

Conversly, suppose $Cl(D[X;S]) \simeq Z_2$. Since $D[X;S]$ is krull,and hence HFD, c.f. [20] .

Remark 6.3.6 *(1) The above theorem generalizes the [20, Theorem 2.4].*

(2) In the case if $D[X;S]$ is HFD, D must be integrally closed, which is same as the Coykendall's [9, Theorem 2.2] for the case of polynomial ring.

(3) $Cl(D[X;S]) \simeq G \oplus Cl(S)$, where G is an abelian group for which D is Dedekind domain [10, Theorem 14.10]. If $Cl(D[X;S]) \simeq Z_2$ and $G = \{0\}$, then $Cl(S) \simeq Z_2$. So, $D[X;S]$ will be HFD.

Example 6.3.7 *Since* $D = Z[\sqrt{-5}]$ *is Dedekind domain and let* S *is finitely generated by pure monomials* $\{X^2, XY, Y^2\}$, *therefore for Krull domain* $D[X;S] = \mathbf{Z}[\sqrt{-5}][X^2, XY, Y^2]$, $Cl(D[X;S]) = Z/2Z \oplus Z/2Z$ *[6, Example 4.7(1)]. Hence by theorem 6.3.5* $D[X;S]$ *is not HFD.*

pure and applied mathematics, Marcel Dekker (New York), 189(1997), 291-294.

[10] R.M. Fossum, *The divisor class group of a Krull domain*, Springer-verlag, New York, (1973).

[11] R. Gilmer, *Multiplicative Ideal Theory.* Marcel Dekker, New York, (1972).

[12] R.Gilmer, *Commutative Semigroup Rings*, The Univ. Chicago Press, (1984).

[13] A. Grams, *Atomic domains and the ascending chain condition for principal ideals.* Proc. Camb. Phil. Soc., **75**, (1974), 321-329.

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

[15] R.Matsuda, *Semigroups and Semigroup Rings*, Commutative ring theory, Lecture notes in pure and applied mathematics, Marcel Dekker (New York), 185(1997), 387-399.

[16] R. Matsumura, *Commutative ring theory*, Cambridge University Press, (1986).

[17] M. Roitman, *Polynomial extensions of atomic domains.* J. Pure Appl. Algebra, **87**, (1993), 187-199.

[18] A. Zaks, *Atomic rings without a.c.c. on principal ideals.* J. Algebra, **74**, (1982), 223-231.

[19] A. Zaks, *Half-factorial domain.* Bull. Amer. Math. Soc., **82**, (1976), 721-723.

[20] A. Zaks, *Half factorial domains*, Israel J. Math., 37(1980), 281-302.