Modern Algebra and Applications

V. K. Bhat

Alpha Science

Modern Algebra and Applications

Alpha Science

Modern Algebra and Applications

V. K. Bhat

Alpha Science International Ltd.
Oxford, U.K.

Modern Algebra and Applications
248 pgs.

V. K. Bhat
Professor and Director
School of Mathematics
SMVD University
J and K

ALPHA SCIENCE INTERNATIONAL LTD.
7200 The Quorum, Oxford Business Park North
Garsington Road, Oxford OX4 2JZ, U.K.

www.alphasci.com

Printed from the camera-ready copy provided by the Author.

ISBN 978-1-84265-855-0
E-ISBN 978-1-78332-074-5

Printed in India

In memory of
Smt. Sunita Bhat
&
To my respected parents
Mr. A. N. Bhat and Mrs. Laxmi Shri

PREFACE

This book contains some aspects of algebra and its applications. The aim is to continue the study of algebra and its applications and show how these applications can be used to solve concrete problems. This text could be used as a course in abstract algebra for graduate students. Traditionally, these courses have covered the theoretical aspects of groups, rings, and modules. However, with the development of computing in the last several decades, applications that involve abstract algebra and discrete mathematics have become increasingly important, and many science, engineering, and computer science students are looking towards courses like this in mathematics. Though theory still occupies a central role in the subject of abstract algebra and no student should go through such a course without a good notion of what a proof is, the importance of applications such as coding theory and cryptography has grown significantly.

Until recent past, most abstract algebra texts included a few (if any) applications. However, one of the major problems in teaching an abstract algebra course is that for many students it is their first encounter with an environment that requires them to do rigorous proofs. Such students often find it hard to see the use of learning to prove theorems and propositions; applied examples help the instructor provide motivation.

The book is based on the following structures and concepts: Set theory and groups; Rings and polynomial rings; Modules with chain conditions; Skew polynomial rings and its primary decomposition; Applications, including coding and cryptography.

(1) **Set theory and groups:** sets, power set, cardinality, Zorn's lemma, groups, Cauchy's theorem, Sylow's theorem, Fundamental theorem.

(2) **Rings and polynomial rings:** rings; quotient rings; ideals; polynomial rings and the Euclidean algorithm for polynomials; irreducible polynomials and factorization of polynomials, Gauss theorem.

(3) **Modules with chain conditions:** Artinian/Noetherian Modules; Modules of Finite Length; Artinian/Noetherian Rings; Radicals.

(4) **Skew polynomial rings and it primary decomposition:** construction and results; primary decomposition of Modules/Noetherian rings/non-Noetherian rings/Rings with Quotient rings; Krull dimension; Associated prime ideals; Completely prime ideals; Transparent rings and their extensions.

(5) **Applications:** Coding theory; Block codes, Linear codes, Cyclic codes, BCH codes including Skew cyclic codes.

The book is organized into four parts. After a chapter summarizing certain prerequisites, Part I comprises of the basic notions like groups, rings, ideals, integral domains, Euclidean domains, factorization domains, polynomial rings, Gauss theorem and Eisentein's criterion. These concepts spread over Chapters 1 and 2.

Part II includes modules with chain conditions; maximum chain condition, minimum chain condition, Ascending chain condition, Descending chain condition, Artinian/Noetherian modules, modules of finite length, Artinian/Noetherian rings, Hilbert basis theorem, I. S. Cohen's theorem.

Part III includes the study of certain types of prime ideals of a ring R. The relation between these ideals and their extension in the extension of a ring R has also been investigated. Chapter 4 includes skew polynomial rings and several results related to Noetherian rings, 2-primal rings and weak σ-rigid rings, where σ is an endomorphism of R. Chapter 5 includes Krull dimension of polynomial and skew polynomial rings; and prime decomposition of modules, Noetherian/ non-Noetherian rings. This is linked with Chapter 6 which studies primary decomposition in non-commutative set up (known as Transparency of a ring). Here the Transparency of skew polynomial rings $R[x;\sigma,\delta]$ has been discussed, where σ is an automorphism of R and δ is a σ-derivation of R. This property has also been discussed for $\sigma(*)$-rings and weak σ-rigid rings.

Finally, Part IV deals with the developing of codes that have efficient encoding and decoding algorithms as well as the ability to detect and correct the errors in the communication. This chapter includes the study of skew codes, the codes over non-commutative polynomial rings which are a generalization of the usual ring of polynomials. This was motivated by a paper of Boucher, Geiselmann and Ulmer [19] where they introduce them. Thus, Chapter 7 serves as a quick introduction to basic principles of coding theory. It includes a large family of linear codes, and within

them, the cyclic codes and BCH codes. These facts are motivating factors for the study of cyclic codes. One is that they have a very rich algebraic structure, and another is that many important codes (BCH codes for example) are cyclic. Mathematically BCH codes they are interesting for their flexibility: apart from sharing many good properties with cyclic codes they allow for a certain control of minimum distance.

Though there are no specific prerequisites for a course in abstract algebra, students who have had other higher-level courses in mathematics will generally be more prepared than those who have not, because they will possess a bit more mathematical sophistication. Exercise sections are the heart of any mathematics text. An exercise set appears at the end of some chapters. The nature of the exercises ranges over several categories; computational, conceptual, and theoretical problems are included.

This books aims to be an accessible source for the material it contains and, whenever possible, worthwhile progress is made using elementary tools.

I now have the happy task of thanking all who have helped in producing this book. I thank all those who have helped me by discussing, explaining, correcting and advising including Ms. Smarti, Ms. Kiran, Ms. Meeru and Mr. Kuldip. I thank my son Chandan who has motivated me for writing this book.

During my work related to this book I could understand why one thanks his spouse, so, thank you Sampati !

The purpose of this book has been to provide a development of the subject-matter which is well motivated, rigorous and at the same time not too pedantic. Efforts have also been taken to present the proofs of the results in a simple form. I shall feel greatly rewarded if the users of this book find it really beneficial and friendly. Some errors are unavoidable in any work. I shall be grateful to the readers for bringing the errors to my notice.

V. K. Bhat

CONTENTS

NOTATIONS

All rings are associative with identity and all modules are unitary. We list some standard notation:

$\subset$	Proper subset.
$\mathbb{N}$	The set of positive integers.
$\mathbb{Z}$	The ring of integers.
$\mathbb{Q}$	The field of rational numbers.
$\mathbb{R}$	The field of real numbers.
$\mathbb{C}$	The field of complex numbers.
R	An associative ring with identity $1 \neq 0$.
$P(R)$	The prime radical of R.
$N(R)$	The set of nilpotent elements of R.
$\mathcal{C}(0)$	The set of regular elements of R.
$\|M\|_r$	The Krull dimensions of a right R-module M (if it exists).
$\|N\|_l$	The Krull dimensions of a left R-module N (if it exists).
$Spec(R)$	The set of prime ideals of R.
$C.Spec(R)$	The set of completely prime ideals of R.
$MinSpec(R)$	The set of minimal prime ideals of R.
$Ann(J)$	The annihilator of a subset J of an R-module M.
$Assas(M_R)$	The assassinator of a uniform R-module M.
M_R	A right module M over a ring R.
R_R	A ring R viewed as a right module over itself.
$Ass(M_R)$	The set of associated primes of M_R.
$P(S)$	Power set of a set S.
$P(S)^*$	is equal to $P(S) - \phi$.
$O(G)$	Order of a group G.
$U(R)$	Set of units in R.
$M_n(R)$	Set of $n \times n$ matrices over a ring R.
$A = \langle S \rangle$	Ideal A of a ring R generated by a subset S of R.
$F[x]$	Polynomial ring over a field F.
$a\|b$	a divides b.
μ_p^*	Abelian group of all complex p roots of unity.
$dim(V_F)$	Dimension of a vector space V over a field F.
$J(R)$	Jacobson radical of a ring R.
$\mathcal{O}_{\mathbf{q}}((k^\times)^n)$	Quantum torus.
$\mathcal{O}_{\mathbf{q}}(k^2)$	Quantum planes.
$I \lhd_r R$	I is a right ideal of R.
$N \subseteq_{ess} M$	A submodule N of M is essential in M.
$Q \rightsquigarrow P$	Q is right linked to P.

$\Omega^r(P)$	The right link closure of P.
$Q \subsetneqq P$	Q is a subset of P and $Q \neq P$.
$C'(I)$	The set $\{r \in R \mid r + I$ is right regular in $R/I\}$.
$R[[t]]$	Power series ring.
Σ^n	A set of all possible words of length 'n'.
$d(x, y)$	Hamming distance between two words x, y.
$w(x)$	Hamming weight of a codeword x.
$\overline{C}$	Algebraic closure of a field C.
$\mathbb{F}_q$	A finite field with q a prime power.

INTRODUCTION

The history of algebra began in ancient Egypt and Babylon, where people learned to solve linear ($ax = b$) and quadratic ($ax^2 + bx = c$) equations, as well as indeterminate equations such as $x^2 + y^2 = z^2$, whereby several unknowns are involved. The ancient Babylonians solved arbitrary quadratic equations by essentially the same procedures taught today. They also could solve some indeterminate equations.

The Alexandrian mathematicians Hero of Alexandria and Diophantus continued the traditions of Egypt and Babylon, but Diophantus's book Arithmetica is on a much higher level and gives many surprising solutions to difficult indeterminate equations. This ancient knowledge of solutions of equations in turn found a home early in the Islamic world, where it was known as the "science of restoration and balancing." (The Arabic word for restoration, al-jabru, is the root of the word algebra.) In the 9th century, the Arab mathematician al-Khwarizmi wrote one of the first Arabic algebras, a systematic expos of the basic theory of equations, with both examples and proofs. By the end of the 9^{th} century, the Egyptian mathematician Abu Kamil had stated and proved the basic laws and identities of algebra and solved such complicated problems as finding x, y, and z such that $x + y + z = 10$, $x^2 + y^2 = z^2$, and $xz = y^2$.

Ancient civilizations wrote out algebraic expressions using only occasional abbreviations, but by medieval times Islamic mathematicians were able to talk about arbitrarily high powers of the unknown x, and work out the basic algebra of polynomials (without yet using modern symbolism). This included the ability to multiply, divide, and find square roots of polynomials as well as a knowledge of the binomial theorem. The Persian mathematician, astronomer, and poet Omar Khayyam showed how to express roots of cubic equations by line segments obtained by intersecting conic sections, but he could not find a formula for the roots. A Latin translation of Al-Khwarizmi's Algebra appeared in the 12^{th} century. In the early 13^{th} century, the great Italian mathematician Leonardo Fibonacci achieved a close approximation to the solution of the cubic equation $x^3 + 2x^2 + cx = d$. Because Fibonacci had traveled in Islamic lands, he probably used an Arabic method of successive approximations.

Early in the 16^{th} century, the Italian mathematicians Scipione del

Ferro, Niccol Tartaglia, and Gerolamo Cardano solved the general cubic equation in terms of the constants appearing in the equation. Cardano's pupil, Ludovico Ferrari, soon found an exact solution to equations of the fourth degree (see quadratic equation), and as a result, mathematicians for the next several centuries tried to find a formula for the roots of equations of degree five, or higher. Early in the 19^{th} century, however, the Norwegian mathematician Niels Abel and the French mathematician Evariste Galois proved that no such formula exists.

An important development in algebra in the 16^{th} century was the introduction of symbols for the unknown and for algebraic powers and operations. As a result of this development, Book III of La geometrie (1637), written by the French philosopher and mathematician Rene Descartes, looks much like a modern algebra text. Descartes's most significant contribution to mathematics, however, was his discovery of analytic geometry, which reduces the solution of geometric problems to the solution of algebraic ones. His geometry text also contained the essentials of a course on the theory of equations, including his so-called rule of signs for counting the number of what Descartes called the "true" (positive) and "false" (negative) roots of an equation. Work continued through the 18^{th} century on the theory of equations, but not until 1799 was the proof published, by the German mathematician Carl Friedrich Gauss, showing that every polynomial equation has at least one root in the complex plane (see Number: Complex Numbers).

By the time of Gauss, algebra had entered its modern phase. Attention shifted from solving polynomial equations to studying the structure of abstract mathematical systems whose axioms were based on the behavior of mathematical objects, such as complex numbers, that mathematicians encountered when studying polynomial equations. Two examples of such systems are algebraic groups (see Group) and quaternions, which share some of the properties of number systems but also depart from them in important ways. Groups began as systems of permutations and combinations of roots of polynomials, but they became one of the chief unifying concepts of 19^{th}-century mathematics. Important contributions to their study were made by the French mathematicians Galois and Augustin Cauchy, the British mathematician Arthur Cayley, and the Norwegian mathematicians Niels Abel and Sophus Lie. Quaternions were discovered by British mathematician and astronomer William Rowan Hamilton, who extended the arithmetic of complex numbers to

quaternions while complex numbers are of the form a + bi, quaternions are of the form $a + bi + cj + dk$.

Immediately after Hamilton's discovery, the German mathematician Hermann Grassmann began investigating vectors. Despite its abstract character, American physicist J. W. Gibbs recognized in vector algebra a system of great utility for physicists, just as Hamilton had recognized the usefulness of quaternions. The widespread influence of this abstract approach led George Boole to write The Laws of Thought (1854), an algebraic treatment of basic logic. Since that time, modern algebra also called abstract algebrahas continued to develop. Important new results have been discovered, and the subject has found applications in all branches of mathematics and in many of the sciences as well.

Prior to the nineteenth century, algebra meant the study of the solution of polynomial equations. By the twentieth century algebra came to encompass the study of abstract, axiomatic systems such as groups, rings, and fields. This presentation provides an account of the history of the basic concepts, results, and theories of abstract algebra.

The development of abstract algebra was propelled by the need for new tools to address certain classical problems that appeared unsolvable by classical means. A major theme of the approach in this book is to show how abstract algebra has arisen in attempts to solve some of these classical problems, providing context from which the reader may gain a deeper appreciation of the mathematics involved.

This book is an introduction to abstract algebra. I have particularly tried to pay attention to the needs of under graduate students of Mathematics and post graduate students of Algebra. With this in mind I have chosen applications such as public key cryptography and error correcting codes which use basic algebra as well as a study of polynomials and their roots which is such a big part of pre-college mathematics.

Abstract mathematics is different from other sciences. In laboratory sciences such as chemistry and physics, scientists perform experiments to discover new principles and verify theories. Although mathematics is often motivated by physical experimentation or by computer simulations, it is made rigorous through the use of logical arguments.

By making use of more sophisticated ideas and mathematical concepts, we will study methods of encoding and transmitting information that allow us to both detect and correct errors. There are many places that use these so-called error correcting codes, from transmitting photographs from planetary probes to playing of compact discs and DVD movies.

In this book we will discuss one of the main methods of encrypting data, the RSA encryption system. The algebraic structure that is at the heart of this method is that of a group. Group theory, perhaps the first algebraic structure to be studied abstractly, is one of the most fundamental of structures. As we shall see, rings, fields, and vector spaces are all special examples of groups. What distinguishes groups from these other structures is that a group has only a single operation.

Cryptography is the subject of transmitting private data in a secure manner. If you make a purchase on the internet, you need to send to the merchant a credit card number. If somebody were to intercept the transmission of this information, they would have your number. Because of this, most internet sites encrypt such data. By doing so, anybody intercepting the transmission will see a useless string of digits instead of a valid credit card number. If, however, the interceptor were to know how the merchant replaces credit card numbers with other numbers, they would have a way of recovering the number. Because of this, merchants must use methods of encryption that are very difficult to "break". We will discuss one such system, the RSA encryption system.

Algebra is used in error-correcting codes. That is, if noise corrupts a bitstream encoded in a certain way, an algorithm can detect the erroneous bits and correct them (subject to certain assumptions about the corruption, such as the maximum number of corrupt bits per byte, etc.)

Abstract algebra is really a form of "meta-mathematics", where it studies the structure of mathematics itself. For example, while FEA methods are widely used for engineering applications, there are branches of mathematics that study the mathematics behind FEA techniques, so that the applicability to "real life applications" are indirect. Much of higher mathematics have only indirect value for real life matters. However, if I were to choose a candidate where abstract algebra and other "higher mathematics" such as co-homology theories can have a pretty direct bearing on "real life", it would be particle physics, which, today,

is about as real as it can be, with potentially (and significant) practical applications.

A certain amount of mathematical maturity is necessary to find and study applications of abstract algebra. A basic knowledge of set theory, mathematical induction, equivalence relations, and matrices is a must. Even more important is the ability to read and understand mathematical proofs.

Chapter

1

PRELIMINARIES

In what follows, some very basic knowledge of Group Theory and a little of Linear Algebra (vector spaces and matrices over fields such as real numbers, complex numbers, etc.) are assumed. We begin with the fundamentals of Ring Theory. While Group Theory involves the study of only one binary operation, Ring Theory involves two binary operations with some interrelations. We formally define what a ring is and give some examples interspersed with a few elementary properties of rings. The examples we give are what one usually comes across in various contexts (such as Algebra [Abstract, Linear, Differential]; Analysis [Real, Complex, Functional]; Topology; Modules; etc.) and they serve to illustrate or counter-illustrate different aspects of rings.

Groups are among the most rudimentary forms of algebraic structures. Because of their simplicity, in terms of their definition, their complexity is large. For example, vector spaces, which have very complex definition, are easy to classify; once the field and dimension are known, the vector space is unique up to isomorphism. In contrast, it is difficult to list all groups of a given order, or even obtain an asymptotic formula for that number.

In the study of vector spaces the objects are well understood and so one focuses on the study of maps between them. One studies canonical forms (e.g., the Jordan canonical form), diagonalization, and other special properties of linear transformations (normal, unitary, nilpotent, etc.). In contrast, at least in the theory of finite groups on which this course focuses, there is no comparable theory of maps. A theory exist mostly for maps into matrix groups (such maps are called linear representation and will not be studied in this course).

While we shall define such maps (called homomorphisms) between groups in general, there will be a large set of so called simple groups for which there are essentially no such maps: the image of a simple group

under a homomorphism is for all practical purposes just the group itself. The set of atoms is large, infinite in fact. The classification of all simple groups was completed in the second half of the 20^{th} century and has required thousands of pages of difficult math.

1.1 Set Theory and Groups

The concept of set is most basic in Mathematics. Indeed almost all mathematical systems are certain collections of sets. All these mathematical systems and their theories can be treated as parts of set theory. In the theory of sets, the concepts of set, object, equality and 'is an element of' are undefined. Intuitively speaking, a set is synonymous with a collection of objects.

The basic knowledge of Group Theory which is one of the fundamental building blocks of the subject and a little of Linear Algebra (Vector Spaces and matrices over fields such as real numbers, complex numbers etc.) are assumed. While Group Theory involves only one binary operation, Ring Theory involves two binary operations.The Group theory is based on the concepts of set theory and number theory which will be discussed first. Other notions introduced here are those of ideals, prime ideal, associated primes and assassinator, etc.

1.1.1 Sets:

A set is a collection of objects called the **elements** of the set. We write $a \in A$ to mean that a is an element of the set A.

1.1.2 Remarks:

Recall the following for sets:

(1) A set having no element is called a **null set** or **empty set**, denoted by $\varnothing$.

(2) A set S is a **subset** of a set A, written $S \subseteq A$, if every element of S is an element of A. When $S \subseteq A$ and $S \neq T$, we say that S is a **proper subset** of A.The number of subsets of a set containing n elements is 2^n.

(3) For any set S the collection of all subsets of S is a set of $P(S)$ called the **power set** of S. Also $P(S)^* = P(S) - \varnothing$.

(4) The **difference** of sets S and T is the set of elements which belong to S but not to T denoted by $S-T$; the **intersection** of S and T is $S \cap T = \{x \in S \text{ and } x \in T\}$; the **union** of S and T is $S \cup T = \{x \in S \text{ or } x \in T\}$.

(5) Two sets are said to be **disjoint** if there intersection is empty.

(6) If S is a finite set, the number of its elements is denoted by $|S|$, or card S, and is called the **cardinality** of S.

(7) The **cartesian product** of two sets A and B, denoted by $A \times B$, is defined as $\{(a, b) \mid a \in A \text{ and } b \in B\}$.

(8) Any $R \subseteq A \times B$ is a **relation** from the set A to the set B.When $A = B$ we say R is a relation on A.

(9) A relation R on a set S is called a **partially order** on S or a **poset** if

(i) R is **reflexive** if for every $s \in S$, $(s, s) \in R$.

(ii) R is **anti-symmetric** if both $(s, s_1), (s_1, s) \in R \Rightarrow s = s_1$.

(iii) R is **transitive** if both $(s, s_1), (s_1, s_2) \in R \Rightarrow (s, s_2) \in R$.

(10) **The Axiom of Choice:** For any non-empty set S there is a choice function $h : P(S)^* \to S$ satisfying $h(A) \in A$ for every $A \in P(S)^*$.

(11) If $\leq$ is a partial order on S then $T \subseteq S$ is a **chain** if for any t, $t' \in T$ either $t \leq t'$ or $t' \leq t$.

(12) For a poset S, $\varnothing \neq T \subseteq S$ has an **upper bound** $d \in S$ if $t \leq d$, for all $t \in T$.

(13) A **maximal element** of a poset is any $m \in S$ so that for $s \in S$, $m \leq s \Rightarrow m = s$.

(14) **Zorn's Lemma:** A non- empty poset S has a maximal element if every chain in S has an upper bound in S.

Before looking at the basics of the ring theory, we define a group, other concepts of the theory with relevant examples for the clarity of the same. Some of its fundamental results are also stated.

1.1.3 Group:

A non-empty set G together with a binary operation $*$ is called a group if it satisfies the following :

(1) a, b, $c \in G$ implies that $(a * b) * c = a * (b * c)$ (associative law).

(2) There exists an element $e \in G$ such that $a * e = e * a = a$, for all $a \in G$ (the existence of identity element in G).

(3) For every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$. Such b is called the inverse of a and is usually denoted by a^{-1}.

1.1.4 Remarks:

Recall the following for a group:

(1) A group is said to be **abelian** if commutative law holds, i.e., for every a, $b \in G$, $a * b = b * a$. Otherwise it is said to be non-abelian.

(2) Let G be a group. The number of elements of G is called the **order** of G and is denoted by $o(G)$.

(3) The following properties hold in a group G:

   (a) The identity element is unique.

   (b) The inverse of each element $a \in G$ is unique.

   (c) For every $a \in G$, $(a^{-1})^{-1} = a$.

   (d) For all a, $b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.

   (e) Cancelation laws hold in group G i.e., $a * b = a * c \Rightarrow b = c$ and $b * a = c * a \Rightarrow b = c$.

   (f) The equations $x * a = b$ and $a * y = b$ have a unique solution in G.

(4) A non-empty subset H of a group G is said to be a **subgroup** of G if under the operation in G, H itself forms a group. The criterion for a nonempty subset H to be a subgroup are:

   (a) H is a subgroup of G if and only if a, $b \in H \Rightarrow ab \in H$ and $a \in H \Rightarrow a^{-1} \in H$.

(b) If H is a non-empty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.

(5) If H is a subgroup of G, $a \in G$, then $Ha = \{ha \mid h \in H\}$. Ha is called a **right coset** of H in G. Similarly **left coset** is defined as $aH = \{ah \mid h \in H\}$. Following are some of the important results related to cosets:

(a) There is a one-to-one correspondence between any two right cosets of H in G.

(b) (**Lagrange's Theorem:**) If G is a finite group and H is a subgroup of G, then $o(H)$ is a divisor of $o(G)$.

(c) If G is a finite group $a \in G$, then $o(a)$ is a divisor of $o(G)$.

(d) (**Fermat Theorem:**) If p is a prime number and a is any integer, then $a^p \equiv a(modp)$.

(e) HK is a subgroup of G if and only if $HK = KH$, where $HK = \{x \in G \mid x = hk,\ h \in H,\ k \in K\}$.

(f) H, K are subgroups of the abelian group G, then HK is a subgroup of G.

(g) If H, K are finite subgroups of group G, then $o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$.

(h) **Cauchy's Theorem:** Suppose G is a finite abelian group and $p \mid o(G)$, where p is a prime number. Then there is an element $a \neq e \in G$ such that $a^p = e$.

(i) **Sylow's Theorem:** If G is an abelian group of order $o(G)$, and if p is a prime number, such that $p^\alpha \mid o(G)$, $p^{\alpha+1} \nmid o(G)$, then G is a subgroup of order p^α.

(6) A subgroup N of G is said to be a **normal subgroup** of G if for every $g \in G$, $n \in N$, $gng^{-1} \in N$. Recall the important facts of a normal subgroup as:

(a) N is a normal subgroup of G if and only if $gNg^{-1} = N$ for every $g \in G$.

(b) The subgroup N of a group G is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.

(c) A subgroup N of a group G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.

(d) If G is a group and N a normal subgroup of G, then $G/N = \{Na : a \in G\}$ is also a group. It is called the quotient group or factor of G by N.

(e) If G is a finite group and N a normal subgroup of G, then $o(G/N) = o(G)/o(N)$.

(7) A mapping ϕ from a group G into a group $\tilde{G}$ is said to a **homomorphism** if for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$. If $G = \tilde{G}$, then ϕ is said to be an **automorphism**.
Following are some of the important results of homomorphism:

(a) Suppose G is a group, N a normal subgroup of G. Define a mapping ϕ from G to G/N by $\phi(x) = Nx$, for all $x \in G$. Then ϕ is a homomorphism of G onto G/N.

(b) If ϕ is a homomorphism of G into $\tilde{G}$, the kernel of ϕ, K_ϕ, is defined by $K_\phi = \{x \in G \mid \phi(x) = \bar{e}, \bar{e} \text{ is identity of } \tilde{G}\}$.

(c) If ϕ is a homomorphism of G into $\tilde{G}$ with kernel K, then K is a normal subgroup of G.

(d) A homomorphism ϕ from G into $\tilde{G}$ is said to be an **isomorphism**, if ϕ is one-to-one. If ϕ is also onto, then G is **isomorphic** to $\tilde{G}$ and we write $G \approx \tilde{G}$.

(e) A homomorphism ϕ from G into $\tilde{G}$ with kernel K_ϕ is an isomorphism of G into $\tilde{G}$ if and only if $K_\phi = e$.

(f) **(Fundamental Theorem)**: Let ϕ be a homomorphism of G into $\tilde{G}$ with kernel K. Then $G/K \approx \tilde{G}$.

(g) If G is a group, then $A(G)$, the set of automorphisms of G, is a group.

1.1.5 Examples:

(1) The set of integers $\mathbb{Z}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ under usual addition form groups.

(2) The set of integers $\mathbb{Z}$ under usual subtraction does not form a group.

(3) Let $G = 1, -1$ under the multiplication of real numbers. Then G is an abelian group of order 2.

(4) G, the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over R is an infinite, non-abelian group under multiplication.

(5) G, the set of all 2×2 matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is an infinite, abelian group under multiplication.

(6) G, the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo p, p a prime number, such that $ad - bc \neq 0$ is a finite, non-abelian group.

(7) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$ under matrix multiplication. Let $H = \{\begin{pmatrix} a & b \\ o & d \end{pmatrix} \in G \mid ad \neq 0\}$. Then H is a subgroup of G.

(8) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$ under matrix multiplication. Let $N = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Then N is a normal subgroup of G.

(9) Let $M = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Then M is a group under usual addition of real numbers. Define $\sigma : M \to M$ by

$$\sigma(a + b\sqrt{2}) = a - b\sqrt{2},$$

for all a, $b \in \mathbb{Z}$. Then σ is an automorphism of M.

(10) Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = 2n$, for all $n \in \mathbb{Z}$. Then f is not an endomorphism.

(11) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$ under matrix multiplication. Let $\tilde{G}$ be the group of all non-zero real numbers under multiplication .
Define $\phi : G \to \tilde{G}$ by $\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$. Then ϕ is a homomorphism of G onto $\tilde{G}$.

The basics of groups have been recalled in this section. The abstract concept of a group has its origin in the set of mappings, or permutations, of a set onto itself. In contrast, rings stem from another and more familiar source, the set of integers. They are in fact generalizations of the algebraic aspects of the ordinary integers. A ring is quite different from a group in that it is a two- operational system; addition and multiplication. The analysis of rings will follow the pattern already laid out for groups.

1.2 Rings

Up-till now we have considered sets with one binary composition only. But there are non-void sets with more then one binary compositions namely the set of integers, the set of rational numbers etc. We would like to enrich the structure of group by attaching some additional properties to it. In this way we are lead to the concept of ring which we define as follows:

1.2.1 Ring:

A non-empty set R together with two binary operations called addition $(+)$ and multiplication $(.)$ is called a ring if it satisfies the following :

(1) $(R, +)$ is an abelian group.

(2) $(R, .)$ is a semi group and

(3) Distributive laws of multiplication over addition hold.

If there exists an element $u \in R$ such that $a.u = u.a = a$ for every $a \in R$; then R is a ring with identity element. u is usually denoted by 1.

A ring R is said to be commutative if $a.b = b.a$, for all a, $b \in R$.

Before proceeding further let us pause to see examples of rings.

1.2.2 Examples:

(1) The sets of integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ with usual addition and multiplication are rings. In fact, they are commutative rings with identity element 1.

(2) The set of even integers under the usual addition and multiplication is a commutative ring but it has no identity element.

(3) Let $n \in \mathbb{N}$. The set of all square matrices of order n over R is a ring with usual addition and multiplication of matrices. This ring is with identity element (the identity matrix of order n) but is non-commutative.

(4) $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ is a ring with respect to addition modulo n and multiplication modulo n.

We now give a brief about the use of $\mathbb{Z}_n$ in enciphering and deciphering:

Algebraic Cryptosystem:

We discuss how an algebraic system can be used to devise an enciphering algorithm. Let A be the common alphabet for a plaintext and the cipher text. Let S be a finite algebraic system such that $n(A) = n(S)$. Choose a fixed bijective map $\phi : A \to S$. Then for any permutation σ of S, the composite map $f = \phi^{-1}\sigma\phi : A \to A$ is bijective, and hence a permutation of A. Thus every permutation of S provide an enciphering key $A \to^{\phi} S \to^{\sigma} S \to^{\phi^{-1}} A$ More generally, if the plaintext alphabet and the cipher text alphabet are different, we have the following schemes:

$A \to^{\rho} S \to^{\sigma} S \to^{\psi} B$ where ρ and ψ are injective mappings. The mappings ρ and ψ are fixed, but σ is variable and determined by the values of the parameters in the algorithm. Clearly, the sets A, B and the mappings ρ and ψ have no bearing on the algorithm. In fact, we may treat S itself as the plain text alphabet as well as the cipher alphabet.

Now we describe examples of algebraic enciphering algorithms of this kind.

Modular enciphering and Affine Cipher:

Let n be the number of characters in the plain text alphabet A. Let $S = \mathbb{Z}_n$ be the ring of integers modulo n. An enciphering that makes use of the algebraic operations in $\mathbb{Z}_n$ is called modular enciphering. The simplest example of a modular enciphering is an affine cipher.

Let a, $b \in \mathbb{Z}_n$ and suppose a is relatively prime to n. Then a is an invertible element in the ring $\mathbb{Z}_n$. Hence the mapping $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $\sigma(x) = ax + b$ is bijective.

In the notation of the usual addition and multiplication operations in $\mathbb{Z}$, the mapping σ is given by $\sigma(x) = (ax + b) mod n$

(Recall that $xmodn$ denotes the remainder left on dividing x by n).

The inverse of the mapping σ is given by $\sigma^{-1}(y) = a^{-1}(y-b) = a^{-1}y - a^{-1}b$ (because $y = \sigma(x) = ax + b$ implies that $x = a^{-1}(y-b)$).

If the plain text alphabet A is the usual set of letters $A, B, ..., Z$, then $n = 26$. We take the preliminary mapping $\rho : A \to \mathbb{Z}_{26}$ as given in the table below.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Illustration:

Use the mapping $A \to \mathbb{Z}_{26}$ and the affine cipher $\sigma(x) = (5x+3)mod26$ to encipher UNIVERSITY.

Solution:

We note that $(5, 26) = 1$, so σ is bijective. We Replace each letter in the plaintext with its corresponding number x as given in the table mentioned above and apply the mapping σ. Then we write the letter corresponding to $\sigma(x)$ and encipher as follows.

plain text	U	N	I	V	E	R	S	I	T	Y
x	21	14	9	22	5	18	19	9	20	25
5x+3	108	73	48	113	28	93	98	48	103	128
(5x+3)mod26	4	21	22	9	2	15	20	22	25	24
cipher text	D	U	V	I	B	O	T	V	Y	X

Therefore, we have $UNIVERSITY \to DUVIBOTVYX$

Let us now decipher DUVIBOTVYX:

In $\mathbb{Z}_{26}$; $5^{-1} = 21$, therefore,

$$\sigma^{-1}(y) = a^{-1}(y-b) = a^{-1}y - a^{-1}b = 21y - 63 = 21y + 15$$

and we have the following table:

cipher text	D	U	V	I	B	O	T	V	Y	X
y	4	21	22	9	2	15	20	22	25	24
21y+15	99	456	477	204	57	330	435	477	540	519
mod 26	21	14	9	22	5	18	19	9	20	25
plain text	D	U	V	I	B	O	T	V	Y	X

1.2.3 Proposition:

The following properties hold in a ring R which can be proved easily by the reader. They are:

(1) The additive identity (known as zero element) is unique.

(2) The additive inverse of an element (known as negative of the element) is unique.

(3) The equations $xa = b$ and $ay = b$ have a unique solution in R.

(4) $0.a = 0 = a.0$, for all $a \in R$.

(5) $n(ab) = (na)b = a(nb)$, for all $a, b \in R$, $n \in \mathbb{Z}$.

(6) $(mn)a = m(na) = n(ma)$, for all $a, b \in R$, $m, n \in \mathbb{Z}$.

Further,

1.2.4 Remarks:

(1) If the semi-group $(R, .)$ has an identity, it is unique denoted by 1_R called the **identity element or unity** of R.

(2) Let R be a ring with 1. An element $u \in R$ is said to be a **unit or invertible** if there exists $v \in R$ such that $u.v = v.u = 1$. Such a v is called the multiplicative inverse (or just inverse) of u and is denoted by u^{-1}. The set of units in R is denoted by $U(R)$.

(3) For a ring R and $\phi \neq S \subseteq R$, S is a **sub-ring** of R if S itself is a ring under the operations of R.

We now have the following definitions:

1.2.5 Zero divisor:

An element $0 \neq a \in R$ is said to be a left zero-divisor if there exists $b \neq 0$ such that $a.b = 0$. Similarly a is called the right zero-divisor if there is a $c \neq 0$ such that $c.a = 0$. An element $a \in R$ is called a zero-divisor if a is either a left or a right zero divisor.

1.2.6 Remark:

In any ring R with at least two elements, 0 is the trivial zero-divisor.

1.2.7 Nilpotent element:

An element $a \in R$ is said to be nilpotent if there is a positive integer n (depending on a) such that $a^n = 0$.

1.2.8 Integral domain:

A non-zero ring R is called an integral domain if there are no non-trivial zero-divisors in R. The rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are integral domains.

1.2.9 Division ring:

A ring is said to be a division ring if its non- zero elements form a group under multiplication.

1.2.10 Field:

A field is a commutative division ring. The rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.

1.2.11 Remark:

Every field is an integral domain. But the converse is not true. For, $\mathbb{Z}$ is an integral domain but not a field.

1.2.12 Proposition:

A finite integral domain is a field.

Proof. Let $R = \{0, x_1, x_2, ..., x_n\}$. Total number of elements of $R = n+1$. Let $x_1 \neq 0$. Consider, $S = \{0, x_1^2, x_1x_2, ..., x_1x_n\}$. If $x_1x_i = x_1x_j, i \neq j \Rightarrow x_1(x_i - x_j) = 0$. But $x_1 \neq 0 \Rightarrow x_i = x_j$ which is a contradiction.Since all the entries of S are distinct. Clearly, since R is a ring, $S \subset R$. Number

of elements of S = Number of elements of $R = n + 1$. $S = R$. Now $1 \in R \Rightarrow 1 \in S$. Therefore $1 = x_1 x_j$ for some $x_j \in R$. But $x_j x_1 = x_1 x_j$. Hence $x_j x_1 = 1 = x_1 x_j$. By the same process every non-zero element has an inverse. R is a field. □

1.2.13 Proposition:

(1) There exists an element $1 \in D$ such that $a.1 = a$ for every $a \in D$.

(2) For every element $a \neq 0 \in D$ there exists an element $b \in D$ such that $a.b = 1$.

Proof. Let $x_1, x_2, ..., x_n$ be all the elements of D, and suppose that $a \neq 0 \in D$. Consider the elements $x_1 a, x_2 a, ..., x_n a$; they are all in D. We claim that they are all distinct. For suppose that $x_i a = x_j a$ for $i \neq j$; then $(x_i - x_j)a = 0$. Since D is an integral domain and $a \neq 0$. Therefore, $x_i - x_j = 0$ and so $x_i = x_j$, contradicting $i \neq j$. Thus $x_1 a, x_2 a, ..., x_n a$ are n distinct elements of D, which has exactly n elements. Therefore every element $y \in D$ can be written as $x_i a$ for some x_i. In particular, since $a \in D$, $a = x_{i0} a$ for some $x_{i0} \in D$. Since D is commutative, $a = x_{i0} a = a x_{i0}$. We will show that x_{i0} is a unit element for every element of D. Since $y = x_i a$ for some $x_i \in D$, and so $y x_{i0} = (x_i a) x_{i0} = x_i (a x_{i0}) = x_i a = y$. Thus x_{i0} is a unit element for D and we write it as 1. Similarly, by previous argument $1 \in D$, is a multiple of a; that is, there exists a $b \in D$ such that $1 = ba$. Hence the result. □

1.3 Ideals

In this section, we study one of the most important aspects of rings, namely the so called "ideals". Some of these (i.e., the two-sided ideals) correspond to the "normal" subgroups in the study of groups. Almost all properties of the two-sided ideals have their parallels for normal subgroups. Now let us define an ideal of a ring and see what are the different types of ideals.

1.3.1 Left ideal:

Let R be a ring. A subset I of R is called a left ideal of R if

(1) I is a subgroup of $(R, +)$ i.e., $a, b \in R \Rightarrow a - b \in I$ and

(2) I is closed for arbitrary multiplication on the left by elements of R i.e., $a \in I$, $r \in R \Rightarrow ra \in I$.

1.3.2 Right ideal:

A subset I of R is called a right ideal of R if

(1) I is a subgroup of $(R, +)$ i.e., $a, b \in R \Rightarrow a - b \in I$ and

(2) I is closed for arbitrary multiplication on the left by elements of R i.e., $a \in I$, $r \in R \Rightarrow ar \in I$. A subset I of R which is both a left ideal and a right ideal is called a two sided ideal.

1.3.3 Remarks:

(1) A subset I is a left/right/2-sided ideal in R implies I is a subring of R. The converse is not true. For example: Let R be ring of real numbers and $\mathbb{Z}$ be set of integers.Then $\mathbb{Z}$ is a subring of R but not an ideal of R because for $3 \in \mathbb{Z}$, $\frac{3}{4} \in R \Rightarrow 3.\frac{3}{4} = \frac{9}{4}$ is not an integer.

(2) Sum of two ideals of same kind is an ideal of same kind whose addition is defined as

$I + J = \{x + y \mid x, y \in I\} \subseteq R$ where I and J are ideals of R. Also addition of ideals is commutative and associative.

(3) Product of two ideals of same kind is again an ideal of same kind. Product of ideals is associative but need not be commutative. Product of ideals is defined as $IJ = \{x_1y_1 + x_2y_2 + ... + x_ny_n \mid x_i \in I, y_i \in J, 1 \leq i \leq n, n \in N\}$.

In fact,

(1) IJ is a left ideal if I is a left ideal and J a subset of R.

(2) IJ is a right ideal if J is a left ideal and I a subset of R.

(3) IJ is a two sided ideal if I is a left ideal and J a right of R.

(4) In commutative ring, the notions of left, right and two-sided ideals all coincide.

To clarify the concepts, let us see the examples of ideals:

1.3.4 Examples:

(1) (0) is an ideal in R called the zero ideal. R and (0) are ideals of R called trivial ideals.

(2) Let $R = M_2(\mathbb{Z})$, $I_1 = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z}\}$ and $I_2 = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{Z}\}$ are respectively right and left ideals of R.

1.3.5 Definition:

Let S be any subset of a ring R. Then ideal A of R is said to be generated by S if

(1) $S \subseteq A$

(2) for any ideal B of R, $S \subseteq B \Rightarrow A \subseteq B$.

We write $A =< S >$. Clearly, from the definition, $< S >$ is the intersection of all those ideals of R which contain S.

1.3.6 Principal ideal:

If an ideal A is generated by a singleton, say $A = (a)$, $a \in A$, then A is said to be a principal ideal written as $A = (a)$.

1.3.7 Maximal left ideal:

A left ideal I in R is said to be a maximal left ideal in R if

(1) $I \neq R$ and

(2) For a left ideal J of R, $I \subseteq J \subseteq R \Rightarrow J = I$ or $J = R$, i.e., there are no left ideals strictly in between I and R .

In other words, an ideal of R is said to be maximal if it is impossible to squeeze an ideal between it and the ring R. Given a ring it is not necessary that it has maximal ideals. If a ring has an identity element, this can be proved by applying axiom of choice (proved in the theorem that follows).

1.3.8 Minimal left ideal:

A left ideal I in R is said to be a minimal left ideal in R if

(1) $I \neq (0)$ and

(2) For a left ideal J of R, $(0) \subseteq J \subseteq I \Rightarrow J = (0)$ or $J = I$, i.e., there are no left ideals strictly in between (0) and I.

Maximal (respectively minimal) right/two-sided ideals are defined in a similar manner.

1.3.9 Theorem:

If R is a ring with 1 and I is a (left/right/two-sided) ideal of R such that $I \neq R$, then there is a maximal ideal M of the same kind such that $I \subseteq M$.

Proof. We shall prove the result for left ideals, it will be on the same lines for right ideals and hence will follow for 2-sided ideals. Let $I \neq R$ be a left ideal in R. Consider the family $\mathfrak{F}$ of all left ideals in R containing I except the unit ideal R, i.e., $\mathfrak{F} = \{J \mid J \text{ is a left ideal in } R,\ J \supseteq I,\ J \neq R\}$. The theorem is equivalent to showing that $\mathfrak{F}$ has a maximal element with set inclusion as the partial order(i.e., for all $J_1,\ J_2 \in \mathfrak{F}$, $J_1 \leq J_2$ if $J_1 \subseteq J_2$). Since $I \in \mathfrak{F}, \mathfrak{F} \neq \phi$. To apply Zorn's lemma to the family of $\mathfrak{F}$, we have to verify that every totally ordered subset $\mathcal{T}$ of $\mathfrak{F}$ has an upper bound in $\mathfrak{F}$. Given such a $\mathcal{T}$, let $T_O = \cup_{T \in \mathcal{T}} T$. We will show that $T_o \in \mathfrak{F}$. We have $T_o \supseteq I$.

(1) T_0 is a left ideal of R. Let $x,\ y \in T_o \Rightarrow x \in T_1$ and $y \in T_2$ for some $T_1,\ T_2 \in \mathcal{T}$. Since T is totally ordered, we have $T_1 \subseteq T_2$ or $T_2 \subseteq T_1$, say $T_1 \subseteq T_2$. Hence $x,\ y \in T_2$. But T_2 is a left ideal, hence $x - y \in T_2$ and so $x - y \in T_o$ i.e., T_o is an additive subgroup of R.

(2) $T_o \neq R$

For if $T_o = R$ then $1 \in T_o$. Hence $1 \in T$ for some $T \in \mathcal{T}$. But then $T = R$ which is a contradiction.

Now by Zorn's lemma, $\mathfrak{F}$ has a maximal element, say M. Since $M \in \mathfrak{F}$, we have $M \neq R$, $M \supseteq I$ and M is a left ideal.

(3) M is a maximal left ideal of R.

For, suppose J is a left ideal such that $M \subseteq J \subseteq R$. If $J \neq R$then $J \in \mathfrak{F}$. By maximality of M in $\mathfrak{F}$, we get that $M = J$, as required.

□

1.3.10 Example:

The above theorem is not true if R is without identity (even if R is commutative). $(\mathbb{Q}, +)$ is an abelian group which is a ring with trivial multiplication $(*)$, i.e., $a * b = 0$ for all $a, b \in \mathbb{Q}$. Since all sub-groups are ideals. Therefore, a maximal ideal in $(\mathbb{Q}, +, *)$ is simply a maximal subgroup of $(\mathbb{Q}, +)$. Clearly $(\mathbb{Q}, +)$ has no maximal subgroups, hence ring $(\mathbb{Q}, +, *)$ which is without 1, has no maximal ideals.

1.3.11 Remark:

Above theorem need not be true for minimal ideals of R even if R is commutative with 1. For example, let $R = \mathbb{Z}$ and $I = 2\mathbb{Z}$. Any ideal $J \subseteq 2\mathbb{Z}$ is of the form $J = 2k\mathbb{Z}$, $K \in \mathbb{N}$. Here J cannot be minimal as $J = 2k\mathbb{Z} \supseteq 4k\mathbb{Z} \neq (0)$ and $4k\mathbb{Z} \neq 2k\mathbb{Z}$.

1.3.12 Prime ideal:

Let R be a commutative ring. An ideal I of R is said to be a prime ideal if

(1) $I \neq R$

(2) $x, y \in R$, $xy \in I \Rightarrow$ either $x \in I$ or $y \in I$.

1.3.13 Example:

In the set of integers $\mathbb{Z}$, the ideal $Q = (p)$, the multiples of p is a prime ideal, whenever p is prime.

1.3.14 Remark:

Any nilpotent element in R is in all prime ideals of R i.e., if $N = \{a \in R \mid a^n = 0 \text{ for some } n \in \mathbb{N}\}$ and $N' = \cap_P P$ where the intersection is taken over all prime ideals of R, then $N \subseteq N'$.

We now have the following important theorem which establishes a relationship between set of nilpotent elements and prime ideals.

1.3.15 Theorem:

The set of all nilpotent elements in a commutative ring R with 1 is the intersection of all prime ideals, i.e., $N = N'$.

Proof. On the same lines as of Theorem (1.3.9) and above note. □

1.3.16 Prime radical:

The prime radical of a ring R is the intersection of all the prime ideals of R.
Note that a ring is semi prime if and only if its prime radical is zero.

1.3.17 Example:

(1) Let $R = \begin{pmatrix} F & F \\ 0 & F \end{pmatrix}$, where F is a field,
Then $P(R) = \begin{pmatrix} 0 & F \\ 0 & 0 \end{pmatrix}$

(2) Let $\mathbb{Z}_2$ be the ring of integers modulo 2 and $R = \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.
Then R is a commutative reduced ring with $P(R) = \{(0,0)\}$.

(3) Let $R = F[x]$ be the polynomial ring over a field F. Then R is a commutative domain, and so it is 2-primal with $P(R) = \{0\}$.

1.3.18 Completely prime ideals:

An ideal P of R is said to be completely prime if $ab \in P$ implies $a \in P$ or $b \in P$ for $a, b \in R$.

In commutative case completely prime ideal and prime have the same meaning. We also note that every completely prime ideal of a ring R is a prime ideal, but converse need not be true.

1.3.19 Example:

Let $R = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{pmatrix} = M_2(\mathbb{Z})$. If p is a prime number, then the ideal $P = M_2(p\mathbb{Z})$ is a prime ideal of R, but is not completely prime, since for $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, we have $ab \in P$, even though $a \notin P$ and $b \notin P$.

1.3.20 Nil ideal:

An ideal I in an ring R is called a nil ideal if every element of I is nilpotent.

1.3.21 Remarks:

(1) Every nilpotent ideal is a nil ideal but converse is not true. For this consider the following example. Let $R = \prod_{n=1}^{\infty} \mathbb{Z}_2^n$. Let I be an ideal of all nilpotent elements in R. Then I is a nil ideal. But I is not nilpotent, therefore if $I^n = (0)$ for some n, then $x^n = 0$, for all $x \in I$. Take $x_n = (0, 0, ..., \bar{2}, 0, 0, ...)$, with $\bar{2}$ at $(n+1)^{th}$ place. Then $x_n^{n+1} = 0$ but $x_n^n \neq 0$.

(2) In fact, for a commutative ring R, a nil ideal I is nilpotent if it is finitely generated.

1.3.22 Minimal prime ideal:

A minimal prime ideal in a ring R is any prime ideal of R that does not properly contain any other prime ideals.

For instance, if R is a prime ring, then 0 is a minimal prime ideal of R, and it is the only one.

1.3.23 Definition:

The set of prime ideals in a ring R is called the *prime spectrum* of R, denoted as $Spec(R)$.

1.3.24 Definition:

The set of minimal prime ideals in a ring R is called *minimal prime spectrum* of R, denoted as $MinSpec(R)$.

1.3.25 Quotient ring:

Let I be an ideal of a ring R. The set of all distinct cosets of I in R is denoted by the symbol R/I. It is a ring under addition and multiplication defined as $(a + I) + (b + I) = (a + b) + I$ and $(a + I)(b + I) = ab + I$, called the quotient ring.

1.3.26 Theorem:

Let R be a commutative ring with 1 and I an ideal in R. Then

(1) R/I is an integral domain if and only if I is a prime ideal in R.

(2) R/I is a field if and only if I is a maximal ideal in R. If I is maximal, R/I is called the residue field of R at I.

Proof. (1) Suppose I is an ideal of R such that R/I is an integral domain. To prove that I is a prime ideal, let $a, b \in R$ be such that $ab \in I$. We have to show that $a \in I$ or $b \in I$. Since $ab \in I$, we have $(a+I)(b+I) = ab+I = I$, i.e., $(a+I)(b+I) = 0$ in R/I. But R/I is an integral domain. Therefore, either $a+I = I$ or $b+I = I$, i.e., $a \in I$ or $b \in I$ as required.

Conversely, let I be a prime ideal in R. Let $a+I, b+I$ be non-zero elements of R/I. Then $a+I \neq I$ and $b+I \neq I$. Let $(a+I)$,$(b+I) \in R/I$ be such that $(a+I)(b+I) = I$. Then $ab+I = I \Rightarrow ab \in I$ which implies that $a \in I$ or $b \in I$ (because I is a prime ideal of R). So $a+I = I$ or $b+I = I$, i.e., R/I is an integral domain.

(2) Suppose R/I is a field. Then R/I contains at least two elements, i.e., $R/I \neq I$. This implies $I \neq R$. Suppose J is an ideal such that $I \subseteq J \subseteq R$. If $J \neq I$, then there is an a in $J - I$. Now $a+I \neq I$, i.e., $a+I \neq 0$ in R/I. Thus $a+I$ is invertible in R/I. Hence there is some $b \in R$ such that $(a+I)(b+I) = ab+I = 1+I$. This implies that $ab-1 \in I \subseteq J$. Since J is an ideal and $ab \in J$, we get that $1 = ab-(ab-1) \in J$. Hence $J = R$, as required.

Conversely, let I be a maximal ideal of R. Since $I \neq R$, we have $R/I \neq I$. Take any non-zero element $a+I \in R/I$. Since I is maximal, we get that $I+(a) = R$. Therefore $1 \in I+(a)$ which implies $1 = x+ya$ for some $x \in I$ and $y \in R$. Therefore $1+I = x+ya+I = (x+I)+(ya+I) = ya+I$ (since $x+I = I$). Then $1+I = ya+I = (y+I)(a+I)$ which implies $y+I$ is the inverse of $a+I$ in R/I. Hence R/I is a field.

□

Immediate consequence of this theorem are:

1.3.27 Corollary:

A maximal ideal (in a commutative ring) is a prime ideal but not conversely.

Proof. I is a maximal ideal in $R \Rightarrow R/I$ is a field $\Rightarrow R/I$ is an integral domain $\Rightarrow I$ is a prime ideal, as required.

In $\mathbb{Z}$, (0) is a prime ideal but not maximal.

□

1.3.28 Corollary:

For $2 \leq n \subseteq \mathbb{N}$, the ring $\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ is an integral domain $\Leftrightarrow n$ is a prime number.

Proof. The first implication is obvious since a field is an integral domain and secondly a finite commutative integral domain is a field. We now prove that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is a prime. Let $\mathbb{Z}/n\mathbb{Z}$ be an integral domain and if possible, suppose n is not a prime, say $n = n_1 n_2$ with $1 < n_1,\ n_2 < n$. Let $\bar{m} = m + n\mathbb{Z}$. Then $\overline{n_1}.\overline{n_2} = \overline{n_1 n_2} = \overline{n} = 0$ with $\overline{n_1} \neq 0$ and $\overline{n_2} \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. This is a contradiction. Therefore n is prime.

Conversely, suppose that n is prime. Consider any $x \neq 0 \in \mathbb{Z}/n\mathbb{Z}$. We may assume that $x \neq 1$, i.e., we can choose $a \in \mathbb{Z}$ such that $(a, n) = 1$(since n is prime). Then there exists r and $m \in \mathbb{Z}$ such that $ar+nm = 1$. This implies that $ra \equiv 1(modn)$. Therefore $\bar{r}\bar{a} = 1$ in $\mathbb{Z}/n\mathbb{Z}$ i.e., $\bar{a}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. Hence $\mathbb{Z}/n\mathbb{Z}$ is a field.

□

1.3.29 Square free:

Any $n \in \mathbb{N}$ is called square free if $d \in \mathbb{N}$ with $d^2 \mid n \Rightarrow d = 1$.

1.3.30 Example:

35 is square free.

1.3.31 Proposition:

For $n \geq 2$, the ring $\mathbb{Z}/n\mathbb{Z}$ has no non-trivial nilpotent element if and only if n is square free.

Proof. Suppose $\mathbb{Z}/n\mathbb{Z}$ has no non-trivial nilpotent elements. Let $n = p_1^{a_1}p_2^{a_2}...p_r^{a_r}$ be the prime decomposition of n, i.e., p_i's are distinct primes and $a_i \in \mathbb{N}$.

Let, if possible, n be not square free, say $a_1 \geq 2$. Consider $m = p_1p_2^{a_2}...p_r^{a_r}$ so that $m < n$, i.e., $\bar{m} \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. But $m^{a_1} = (p_1p_2^{a_2}...p_r^{a_r})^{a_1}$ which is a multiple of n. Thus $\overline{m}^{a_1} = 0$ in $\mathbb{Z}/n\mathbb{Z}$, i.e., $\overline{m}$ is non -trivial and nilpotent, a contradiction. Therefore n is square free.

Conversely, suppose n is square free and $\mathbb{Z}/n\mathbb{Z}$ has non-trivial nilpotent elements, say $\bar{a}^r = 0$ in $\mathbb{Z}/n\mathbb{Z}$ and $\bar{a} \neq 0$. Then n divides a^r but not a. Writing $n = p_1p_2...p_s$ as the product of distinct primes, we get that each p_i divides (n and hence divides)a^r which implies that p_i divides a. But then it follows that their product $p_1p_2...p_s = n$ divides a which is a contradiction. Therefore $\mathbb{Z}/n\mathbb{Z}$ has no non-trivial nilpotent element.

□

1.4 Divisibility

We assume R to be a commutative integral domain with 1 and $R^* = R-(0)$ unless otherwise stated and hence we've the following definitions, concerning divisibility concepts.

1.4.1 Divisor:

Let a, $b \in R$, $a \neq 0$. Then a divides b or a is a divisor (or factor) of b written $a|b$ if there exists $c \in R$ such that $b = ac$.

1.4.2 Associates:

Two elements a and b in R^* are said to be associates of each other if $a|b$ and $b|a$. a and b are associates of each other if and only if $(a) = (b)$.

1.4.3 Example:

In $\mathbb{Z}$, 3 and -3 are associates and in $\mathbb{Z}[i]$, 1, -1, i and $-i$ are associates.

1.4.4 Theorem:

Let R be a commutative ring with unity, then the following hold:

(1) The relation of being associates is an equivalence relation on R.

(2) If R is an integral domain and a, b are two non - zero elements of R then $a \sim b$ if and only if $a \mid b$ and $b \mid a$.

(3) If a, b are two non - zero elements of R then $a \mid b$ and $b \mid a$ if and only if $< a >=< b >$.

Proof. (1) For all $x \in R$, $x = 1.x$ i.e., $x \sim x$, so $\sim$ is reflexive. If $a \sim b$ then $a = bu$ for some unit $u \in R \Rightarrow b = au^{-1} \Rightarrow b \sim a$ as u^{-1} is again a unit in R. Thus $\sim$ is symmetric. Finally if $a \sim b$ and $b \sim c$ then $a = bu$ and $b = cv$ for some units u, $v \in R$. This gives $a = cuv$; however u, v being units in R implies that uv is again a unit in R. Thus $a \sim c$ and this implies that $\sim$ is transitive. Hence $\sim$ is an equivalence relation on R.

(2) If $a \sim b$ then $a = bu$ for some unit $u \in R \Rightarrow b \mid a$. Also $b = au^{-1} \Rightarrow b \mid a$. Conversely, if $a \mid b$ and $b \mid a$ we get $b = ac$ and $a = bd$ for some c, $d \in R$; thus $b = bdc \Rightarrow 1 = dc$ as $b \neq 0$ and R is an integral domain; thus d is a unit. Hence $a \sim b$.

(3) $a \sim b \Rightarrow b = ac$ for some $c \in R \Rightarrow b \in < a > \Rightarrow < b > \subseteq < a >$. Similarly, $b \mid a \Rightarrow < a > \subseteq < b >$, hence $< b >=< a >$. Conversely, $< a >=< b > \Rightarrow a \in < b > \Rightarrow a = br$ for some $r \in R \Rightarrow b \mid a$.In the same manner $< b >=< a > \Rightarrow a \mid b$.

□

1.4.5 Remark.

Being associates is an equivalence relation on R^*. For $a \in R^*$, the equivalence class through a is $\{ua \in R \mid u$ is a unit in $R\}$ i.e., the equivalence classes are orbits in R^*.

1.4.6 Irreducible element:

A non-zero, non-unit a$\in R$ is said to be irreducible if $a = bc$, then either b or c is a unit i.e., a cannot be written as a product of two non-units or equivalently, the only divisors of a are its associates or units.

1.4.7 Prime element:

A non-zero, non unit $a \in R$ is said to be a prime if $a|bc$ (b, $c \in R$), then either $a|b$ or $a|c$. Now let us prove some results on these concepts

1.4.8 Proposition:

A prime element is irreducible but not conversely.

Proof. Let p be a prime in R. Suppose $p = ab$. Then obviously $p|ab$, hence $p|a$ or $p|b$, say $p|a$. Then $a = pc$ for some $c \in R$. Now we have $p = ab = pcb$, hence $1 = cb$ by canceling (the non zero) p. Thus b is a unit in R. Hence p is irreducible, as required.

To see that the converse is not true. Consider $R = \mathbb{Z}[i\sqrt{3}]$. The only units in R are ± 1. Also the element $1 + i\sqrt{3}$ is irreducible but not prime. □

1.4.9 Theorem:

Let a be a non-zero non-unit in a commutative integral domain R. Then

(1) The element a is irreducible in R if and only if the ideal (a) is maximal among all principal ideals other than R, properly containing (a).

(2) The element a is prime in R if and only if the ideal (a) is a non-zero prime ideal in R.

Proof. (1) Suppose a is irreducible. Let $(a) \subseteq (b) \neq R$ for some $b \in R$. Now $a \in (b)$, implies that $a = bc$ for some $c \in R$. Since a is irreducible, either b or c is a unit in R. Since $(b) \neq R, b$ cannot be a unit. Therefore c must be a unit. But then, $b = c^{-1}a \in (a)$, i.e., $(b) \subset (a)$. Thus $(a) = (b)$, as required.

Conversely, suppose (a) is maximal among all principal ideals other than R. We show a is irreducible. Suppose that $a = bc$ and that b is not a unit. Then $(a) \subseteq (c)$ and $(a) \neq (c)$. This contradicts the maximality of (a) unless $(c) = R$ which means c is a unit, as required.

(2) Suppose a is a prime element of R. Since a is a non-unit, $(a) \neq R$. Suppose that $xy \in (a)$. So $xy = ab$ for some $b \in R$. Now $a|ab$, i.e., $a|xy$, hence $a|x$ or $a|y$, say $a|x$, i.e., $x = ac$ for some $c \in R$, hence $x \in (a)$, showing that (a) is a prime ideal in R and obviously it is a non-zero as $a \neq 0$.

Conversely, suppose (a) is a non-zero prime ideal in R. Since $(a) \neq R$, a is not a unit. If $a|xy$, then $xy \in (a)$, so either $x \in (a)$ or $y \in (a)$ as (a) is a prime ideal. Say, $x \in (a)$ which means $a|x$, i.e., a is a prime element of R.

□

1.5 Euclidean Domain

The class of rings that is discussed now is motivated by several examples already discussed - the ring of integers,the Gaussian integers and polynomial rings.

1.5.1 Definition:

A commutative integral domain R (with or without unity) is called an Euclidean domain if there is a map $d : R^+ \to \mathbb{Z}^+$.

(1) for all a, $b \in R^*$, $a|b \Rightarrow d(a) \leq d(b)$ or equivalently, $d(x) \leq d(xy)$ and

(2) for all $a \in R$ and $b \in R^+$, there exists q, $r \in R$ (depending on a and b) such that $b = qa + r$ with either $r = 0$ or else $d(r) < d(b)$.

The map d is called the algorithm map and the property (2) is called the Euclidean algorithm. The elements b, a, q and r in the equation $b = qa+r$ are respectively called the dividend, divisor, quotient and remainder.

1.5.2 Examples:

(1) Any field K is Euclidean with algorithm map as the constant map $d : K \to \mathbb{Z}^+$, i.e., $d(x) = 1$, for all $x \in K^+$.

(2) The ring of integers $\mathbb{Z}$ is Euclidean, with algorithm map as the absolute map $d : \mathbb{Z} \to \mathbb{Z}^+$, i.e., $d(n) = |n|$, for all $n \in \mathbb{Z}^+$.

1.5.3 Proposition:

An Euclidean domain R has unity and group of units of R is given by $U(R) = \{a \in R^+ \mid d(a) = d(1)\}$.

Proof. By definition of an integral domain, we have $R^* \neq \phi$. Now look at the image $d(R^*) \subseteq \mathbb{Z}^+$, i.e., $d(R^*)$ is a non-empty subset of $\mathbb{Z}$ and hence has a least element (by well the ordering -principle). Let $l \in d(R^*)$ be

the least in $d(R^*)$, say $l = d(e)$ for some $e \in R^*$. We have $d(e) \leq d(a)$, for all $a \in R^*$.

Claim: R has unity. First, we observe that $e|a$, for all $a \in R$. For, since $e \neq 0$, by the Euclidean algorithm, there exists $q, r \in R$ such that $a = qe + r$ with either $r = 0$ or else $d(r) \leq d(e)$, we get that r has to be zero.Thus $a = qe$, as required.

In particular, $e|e$, say $e = q_0 e$ for some $q_0 \in R$. Now we shall show that this q_0 is the unity of R. Given $x \in R$, we have $xq_0e = xe$ (since $q_0e = e$). So we get $(xq_0 - x)e = 0$ which implies $xq_0 - x = 0$ (since $e \neq 0$). Thus $q_0 = 1$ is the unity of R.

To characterize the units in R, first note that $d(1) = d(e)$ because $d(1) \leq d(1e) = d(e)$ and $d(e)$ is the least in $d(R^*)$. Now suppose x is a unit in R. We have $d(x) \leq d(xx^{-1}) = d(1)$, so $d(x) = d(1)$. On the other hand, suppose $x \in R^*$ is such that $d(x) = d(1)$. Then, using Euclidean algorithm, there exists $q, r \in R$ such that $1 = qx + r$ with either $r = 0$ or else $d(r) < d(x) = d(1)$. But the latter is not possible and hence $r = 0$ which means x is a unit in R, as required. □

1.6 Principal Ideal Domain

1.6.1 Definition:

A commutative integral domain R is called a Principal ideal domain (PID) if every ideal of R is principal i.e., generated by one element.

1.6.2 Example:

The ring of integers $\mathbb{Z}$ is a PID.

1.6.3 Theorem:

Every Euclidean domain is a PID (with 1).

Proof. Let R be a Euclidean domain. By Proposition (1.5.3), R has a unity. Let I be an ideal in R. If $I = (0)$, it is a principal ideal. Assume that $I \neq (0)$. Now $I^* \neq \phi$, hence $d(I^*)$ is a non-empty subset of $\mathbb{Z}^+$ and so $d(I^*)$ has a least element, say $d(a)$ for some $a \in I^*$.

Claim: $I = (a)$. To see this, first note that $(a) \subset I$ since $a \in I$. To prove that $I \subset (a)$, take any $x \in I$. By Euclidean algorithm, there exists $q, r \in R$ such that $x = qa + r$ with either $r = 0$ or else $d(r) < d(a)$. Since $r = (x - qa) \in I$ and $d(a)$ is least in $d(I^*)$, it is not possible that $d(r) < d(a)$ and so $r = 0$, i.e., $x = qa \in (a)$, as required. □

1.6.4 Example:

The ring of even integers $R = 2\mathbb{Z}$ is a trivial example of a PID which is not Euclidean, since it has no unity.

1.6.5 Theorem:

Let R be a PID with 1. Then

(1) Every irreducible element is a prime in R.

(2) Every non- zero prime ideal is maximal in R.

Proof. (1) Let a be an irreducible element in R. We have to show that the ideal (a) is prime in R. In fact, we shall show that (a) is a maximal ideal. Since a is a non-unit, we have $(a) \neq R$ and hence, by Zorn's lemma, there exists a maximal ideal M such that $(a) \subseteq M$. Since R is a PID, $M = (p)$ for some p in R. Thus $(a) \subseteq (p)$ and hence a is an associate of p which means that a is a prime.

(2) Let P be non-zero prime ideal in R. Since R is a PID, $P = (p)$ for some prime p. We have already shown above in Theorem (1.4.9) that (p) is a maximal ideal. Hence the theorem.

□

1.6.6 Remark:

Every non- zero, non - unit element in a PID R is divisible by an irreducible element.

1.6.7 Unique factorization domain:

An integral domain R is a Unique factorization domain (UFD) if it satisfies the following conditions:

(1) Every non-unit of R is a finite product of irreducible factors.

(2) The factorization is unique up to order and unit factors. i.e., if $a = p_1p_2...p_m = q_1q_2...q_n$ where p_i and q_j are irreducible, then $m = n$ and p_i and q_j are associates $i = 1, 2, ..., m$.

1.6.8 Remark:

If only condition (1) is satisfied then R is called a **factorization domain.**

1.6.9 Examples:

(1) The ring of integers.

(2) The ring of polynomials in any number of indeterminate, with coefficients in a field.

(3) $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

1.6.10 Theorem:

An integral domain R is a UFD if and only if R is a factorization domain in which every element is a prime.

Proof. The implication $\Rightarrow$ is the theorem above. To prove the reverse implication $\Leftarrow$, we have to prove the uniqueness of factorization. Let $x \in R^*$ have two factorizations into irreducibles (i.e., primes), say$x = up_1p_2...p_r = vq_1q_2...q_s$ with u, v units and p_i, q_j primes. Now proceed by induction on r. If $r = 0$, then x is a unit implying that any factor of x is a unit and hence $s = 0$. Assume that $r \geq 1$ and the induction hypothesis. Note then that $s \geq 1$. Since $p_1|x$ and p_1 is a prime, we get that $p_1|q_j$ for some j. Now $q(j)$ is also a prime, it follows that p_i and q_j are associates, and so there exists a unit $\alpha \in R$ such that $q(j) = \alpha p_1$. Upon substituting for q_j in the factorizations of x and canceling p_1, we get that

$$\acute{x} = up_2...p_r = vq_1q_2...q_{i-1}q_{i+1}...q_s.$$

The result follows with the same process in a finite number of steps. □

1.6.11 Theorem:

In a UFD, every irreducible element is a prime.

Proof. Let R be a UFD and $a \in R$ be an irreducible element. Let $x, y \in R^*$ be such that $a|xy$. We have to show that either $a|x$ or $a|y$. Now $a|xy$, so there exists $b \in R^*$ such that $ab = xy$. Also R is a UFD implies that there exists units u, v and irreducibles $p_i, q_j; 1 \leq i \leq r, 1 \leq i \leq s$ such that $x = up_1p_2...p_r$ and $y = vq_1q_2...q_s$. Now we have $ab = xy = uvp_1p_2...p_rq_1q_2...q_s$. Since the irreducible a occurs in one factorization of xy, it should be an associate of some irreducible occurring in any other factorization of xy into irreducibles. Hence a is an associate of some p_i or q_j. Say, $a\alpha = p_i$ for some unit α. Thus we get that $x = up_1p_2...p_r = up_1p_2...p_{i-1}a\alpha\acute{x}$ for some $\acute{x} \in R^*$ and hence $a|x$, as required.

□

1.6.12 Remark:

An integral domain R is a UFD if and only if every non-zero non-unit in R can be factored into a product of primes.

1.6.13 Theorem:

Every PID is a UFD.

Proof. Let $a \in R$ be any non - zero, non - unit element. Then a is divisible by some irreducible element p_1. $p_1 \mid a \Rightarrow a = a_1p_1$ for some a_1. If a_1 is irreducible, we can express a_1 as a product of finite number of irreducible elements. Suppose a_1 is not irreducible, then there exists an irreducible element p_2 such that $p_2 \mid a_1 \Rightarrow a_1 = p_2a_2$ for some a_2. Continuing the above process and considering the chain of ideals $(a) \subseteq (a_1) \subseteq (a_2) \subseteq ...$, because as $x \in (a) \Rightarrow x = ar = p_1a_1r \in (a_1)$ etc. Thus we get an ascending chain of ideals which must terminate after a finite number of steps. Hence we get an irreducible element a_n so that $a = p_1p_2...p_na_n$ i.e., a is expressed as a product of finite number of irreducible elements. It can be easily shown that this representation is unique. Hence the theorem.

□

1.7 Modules

The notion of modules is a generalization of that of a vector space; here the scalars will be elements of an arbitrary ring. Let us discuss the modules, its types and important results.

1.7.1 Left module:

Let R be a ring (with or without 1, commutative or not). By a left R -module M, we mean, an abelian group $(M, +)$ together with a map $R \times M \to M$, $(a, x) \to ax$, called the scalar multiplication or the structure map, such that for all $a, b \in R$ and $x, y \in M$

(1) $a(x + y) = ax + ay$

(2) $(a + b)x = ax + bx$

(3) $(ab)x = a(bx)$.

Elements of R are called scalars.

A right $R-$ module is defined similarly.

1.7.2 Remarks:

(1) In case $M = (0)$, whatever R be, a left module on M with scalar multiplication, $a.0 = 0$ for all $a \in R$, called the zero module over R.

(2) In case R has 1 and the scalar multiplication defined as $1.x_0 = 0$ for all $x_0 \in M$, then $ax_0 = (a.1)x_0 = a(1.x_0 = a.0 = 0)$, for all $a \in R$. Thus if $1.x = 0$, for all $x \in M$. It follows that $a.x = 0$, for all $x \in R$ and $x \in M$. Thus M is a trivial left R-module.

1.7.3 Unitary Module:

A left R-module M is said to be a unitary left-module if $1.x = x$, for all $x \in M$.

1.7.4 Examples:

(1) Let V be a vector space over the field F. Then V is a right as well as a left F- module.

(2) Unitary modules over $\mathbb{Z}$ are abelian groups.

(3) If R is any ring, R is a left and also a right R- module with usual multiplication in R as the scalar multiplication.

1.7.5 Submodule:

Let M be a right R-module. A non-empty subset N of M is called an R-submodule of M if

(1) N is an additive subgroup of M i.e., $x, y \in N \Rightarrow x - y \in N$ and

(2) N is closed for scalar multiplication i.e., $x \in N$, $a \in R \Rightarrow ax \in N$. i.e., the restrictions to N of addition and scalar multiplication in M make N into an R-module.

1.7.6 Remark:

Suppose M and N are submodules of a module P over R. Then $M \cap N = (0)$ if and only if every element $z \in M + N$ can be uniquely written as $z = x + y$ with $x \in M$ and $y \in N$.

1.7.7 Direct sum:

If M is an R- module and if $M_1, M_2, ..., M_n$ are submodules of M, then M is said to be the direct sum of $M_1, M_2, ..., M_n$ if every element $m \in M$ can be written in a unique manner as $m = m_1 + m_2 + ... + m_n$, where $m_i \in M_i$, $1 \leq i \leq n$.

1.7.8 Definition:

Suppose M is an R-module and X a subset of M, then the *submodule generated or spanned* by X is defined as the smallest submodule of M containing X, or equivalently, it is the intersection of all the submodules N and M each containing X. Note that this intersection is over a non-empty family because M is a member of this family. It can be seen to be equal to $\{\Sigma_i^{finite} a_i x_i \mid a_i \in R, x_i \in X\}$ if R is with 1 and M is unitary. Otherwise, it is equal to $\{\Sigma_i^{finite}(n_i + a_i)x_i \mid a_i \in R, x_i \in X \text{ and } n_i \in \mathbb{Z}\}$.

1.7.9 Cyclic module:

An R- module M is said to be cyclic if there is an element $m_o \in M$ such that every $m \in M$ is of the form $m = rm_0$ where $r \in R$.

1.7.10 Example:

For R, the ring of integers, a cyclic $R-$ module is a cyclic group.

1.7.11 Remarks:

(1) The submodule generated by $\emptyset$ is (0).

(2) If $X = \{x\}$, then the submodule generated by x is $\{ax \mid a \in R\}$ if R is with 1 or $\{ax + nx \mid a \in R, n \in \mathbb{Z}\}$, otherwise. This is called the *cyclic or monogenic* submodule generated by x.

1.7.12 Finitely generated module:

An R- module M is said to be finitely generated if there exists elements $a_1, a_2, ..., a_n \in M$ such that every $m \in M$ is of the form $m = r_1a_1 + r_2a_2 + ... + r_na_n$ for $r_i \in R$.

1.7.13 Definition:

Given a submodule N of an R- module M, the quotient group M/N has a natural structure of an R-module viz

$$R \times (M/N) \to (M/N),$$

$(a, x + N) \to ax + N$, for all $a \in R$ and $x \in M$. Clearly, M/N is an R -module called the **quotient** of M by N.

1.7.14 Homomorphism of modules:

Given two $R-$ modules M and N then the mapping T from M into N is called a homomorphism if

(1) $T(m_1 + m_2) = T(m_1) + T(m_2)$

(2) $T(rm_1) = rT(m_1)$, for all $m_1, m_2 \in M$ and all $r \in R$.

1.7.15 Maximal submodule:

A submodule N of a module M is called a maximal submodule if

(1) $N \neq M$ and

(2) $N \subseteq P \subseteq M$, P a submodule of $M \Rightarrow P = N$ or $P = M$, i.e., the only submodules of M containing N are N and M.

1.7.16 Minimal submodule:

A submodule N of a module M is called a minimal submodule if

(1) $N \neq (0)$ and

(2) $P \subseteq N$, P a submodule of $M \Rightarrow P = (0)$ or $P = N$, i.e., the only submodules of M contained in N are (0) and N.

1.7.17 Simple module:

A module M is called simple module if

(1) $M \neq (0)$ and

(2) the only submodules of M are (0) and M.

1.7.18 Remarks:

(1) Any one-dimensional vector space is simple.

(2) Any minimal submodule is simple.

(3) A submodule N of M is maximal in $M \Leftrightarrow M/N$ is simple.

(4) A non-zero module M is simple $\Leftrightarrow$ 0 is a maximal submodule of $M \Leftrightarrow M$ is a minimal submodule of $M \Leftrightarrow$ every non-zero element of M generates M.

1.7.19 Some of the important results are stated as:

(1) **Fundamental Theorem on finitely generated modules**: Let R be a Euclidean ring; then any finitely generated $R-$ module, M, is the direct sum of a finite number of cyclic submodules.

(2) **Schur's Lemma**: Let N and M be simple R-modules. Then any R-linear map $f : M \to N$ is either 0 or an isomorphism. In particular, $D = End_R(M)$ is a division ring.

1.7.20 Annihilator:

Let A be a right module over a ring R. Given any subset $X \subseteq A$, the annihilator of X is the set $Ann(\{x\})$ or $Ann(x) = \{r \in R \mid xr = 0$, for all $x \in X\}$. It is also written as $r.Ann(X)$, as A is a right module. When X consists of a single element x, we write $Ann(\{x\})$.

1.7.21 Example:

The annihilator of a left ideal of R in a right $R-$ module A is a submodule of A, and similarly the annihilator of a right ideal of R in a left $R-$ module A is a submodule of A.

1.7.22 Remark:

For $X \subseteq R$, a left annihilator is defined and denoted as $l.Ann(X) = \{r \in R \mid rx = 0, \text{ for all } x \in X\}$.

1.7.23 Faithful:

A module A over a ring R is a faithful R -module if

$$Ann_R(A) = 0.$$

1.7.24 Examples:

(1) A faithful module over a non-zero ring must be non-zero.

(2) The annihilator of an $R-$ module A is an ideal of R and that A is a faithful module over $R/Ann_R(A)$.

(3) In a prime ring every non zero right or left ideal is faithful.

1.7.25 Fully faithful:

A right module A over a ring R is fully faithful provided A and all non zero submodules of A are faithful right R-modules. If A is a non zero R-module which is fully faithful on a module over $R/Ann_R(A)$, then A is called a prime module.

1.7.26 Proposition:

Let A be a non zero right module over a ring R. Suppose that there exists an ideal P maximal among the annihilators of non zero submodules of A. Then P is a prime ideal of R, and $Ann_A(P)$ is a fully faithful (R/P)-module.

Proof. Suppose that A is a right R-module. Then is a non zero submodule B in A such that $P = Ann(B)$, and $P \neq R$ because $B \neq 0$. Suppose that I and J are ideals of R, properly containing P, such that $IJ \subseteq P$.

Then $BI \neq 0$ and $Ann(BI) \supseteq J \supset P$, contradicting the maximality of P. Thus P is prime.

Now set $C = Ann_A(P)$ and note that C is a submodule of A with $P \subseteq Ann(C)$, because $B \subseteq C$. Thus C is a faithful right (R/P)- module. Any non zero submodule $D \subseteq C$, we have $P = Ann(C) \subseteq Ann(D)$, where $P = Ann(D)$ by maximality of P. Therefore C is fully faithful as a right (R/P)-module.

□

1.7.27 Uniform module:

A uniform right module is a non zero module A such that the intersection of any two non - zero submodules of A is non zero.

Note that all non - zero submodules are uniform.

1.8 Exercises

(1) Show that the intersection of two sub-rings of a ring is a sub-ring. What about the union. Justify with example. Under what condition will the union of two sub-rings be a sub-ring.

(2) In any ring R, show that ab is nilpotent if and only if ba is nilpotent.

(3) Show that an element in a finite ring with 1 is a unit if it is not a zero divisor.

(4) Show that the intersection of two prime ideals is a prime ideal if and only if one of them is contained in the other.

(5) Show that a prime ideal in a finite commutative ring with 1 is maximal.

(6) If A and B are submodules of M prove

   (a) $A \cap B$ is a submodule of M

   (b) $(A + B)/B$ is isomorphic to $A/(A \cap B)$.

(7) Let M be an R- module; if $m \in M$ let $\lambda(m) = \{x \in R \mid xm = 0\}$. Show that $\lambda(m)$ is a left ideal of R. It is called the *order of m*.

(8) Let M be an R- module and λ a left ideal of R. Show that for $m \in M$, $\lambda(m) = \{xm \mid x \in \lambda\}$ is a submodule of M.

(9) Let M be an $R-$ module and let $E(M)$ be the set of all $R-$ homomorphisms of M into M. Make appropriate definitions of addition and multiplication of elements of $E(M)$ so that it becomes a ring.

(10) Prove that in a UFD all minimal prime ideals are principal and are exactly those ideals which are generated by irreducible elements.

(11) Let R be a PID, then n non - zero elements $a_1, a_2, ..., a_n \in R$ are relatively prime if and only if there exists $x_1, x_2, ..., x_n \in R$ such that $a_1x_1 + a_2x_2 + ... + a_nx_n = 1$.

Chapter

2

POLYNOMIAL RINGS

Polynomials not only help us to construct new and useful examples of rings and fields but are of interest in themselves. The "ring" of polynomials in one variable has two binary operations - addition and multiplication. In mathematics, especially in the field of abstract algebra, a polynomial ring is a ring formed from the set of polynomials in one or more variables with coefficients in another ring. Polynomial rings have influenced much of mathematics, from the Hilbert basis theorem, to the construction of splitting fields, and to the understanding of a linear operator.

Many important conjectures involving polynomial rings, such as Serre's problem, have influenced the study of other rings, and have influenced even the definition of other rings, such as group rings and rings of formal power series. The polynomial ring $K[X]$ is remarkably similar to the ring $\mathbb{Z}$ of integers in many respects. This analogy and the arithmetic of the ring of polynomials were thoroughly investigated by Gauss and his theory served as a model for development of abstract algebra in the second half of the nineteenth century in the works of Kummer, Kronecker, and Dedekind.

The first property of the polynomial ring is elementary and says that a product of two non-zero polynomials is also a non-zero polynomial. The next property of the polynomial ring is much deeper. Already Euclid noted that every positive integer can be uniquely factored into a product of primes this statement is now called the fundamental theorem of arithmetic. Polynomial rings have been generalized in a great many ways, including polynomial rings with generalized exponents, power series rings, noncommutative polynomial rings, and skew-polynomial rings.

2.1 Ring of Polynomials

From the early school days we have been studying different types of polynomials, factoring them, adding, subtracting, multiplying, dividing and

simplifying them. We have also studied them as functions, checking their continuity, finding derivatives, their integrals, maxima and minima. Now we will study polynomials as elements of a certain ring and the theory based on it. In this direction we start with the following definitions.

2.1.1 Definition

Ring of polynomials: Let R be a ring. Let x be an indeterminate or a variable over R. Let $R[x]$ be the set of all polynomial expressions in x with coefficients in R, i.e.,

$$R[x] = \{a_0 + a_1x + a_2x^2 + ... + a_rx^r \mid a_i \in R, r \in \mathbb{Z}^+\}.$$

Equality in $R[x]$: Let $p(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$ and $q(x) = b_0 + b_1x + b_2x^2 + ... + b_sx^s$ be in $R[x]$. Then $p(x) = q(x)$ if and only if $r = s$ and $a_i = b_i$, for all i, $0 \leq i \leq r$. In particular, $a_0 + a_1x + a_2x^2 + ... + a_rx^r = 0$ if and only if $a_i = 0$, for all i. Thus two polynomials are equal if and only if their corresponding coefficients are equal.

Addition and multiplication in $R[x]$: Let $p(x) = a_0+a_1x+a_2x^2+ ... + a_rx^r$ and $q(x) = b_0 + b_1x + b_2x^2 + ... + b_sx^s$ be in $R[x]$, (assume $r \leq s$). Define

$p(x) + q(x)$

$= (a_0 + a_1x + a_2x^2 + ... + a_rx^r) + (b_0 + b_1x + b_2x^2 + ... + b_sx^s)$

$= (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+...+(a_r+b_r)x^r+b_{r+1}x^{r+1}+...+b_s)x^s.$

$p(x)q(x)$

$= (a_0 + a_1x + a_2x^2 + ... + a_rx^r)(b_0 + b_1x + b_2x^2 + ... + b_sx^s)$

$= (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + ... + (a_0b_i + a_1b_{i-1} + ... + a_ib_0)x^i + ... + (a_rb_s)x^{r+s}.$

It can be easily seen that the set $R[x]$ is a ring under the above operations. Elements of this ring are called polynomials in x with coefficients in R.

2.1.2 Definition:

If $p(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r \neq 0$, we may assume that $a_r \neq 0$. Then a_r is called the **leading coefficient** of $p(x)$ and r is called the **degree** of $p(x)$. Thus the degree is the largest integer i for which the coefficient of $p(x)$ is non- zero. We say a polynomial is constant if its

degree is 0.

The term a_0 is called the **constant term** of $p(x)$. A polynomial whose constant term is zero is called a polynomial **without** constant term. If R has 1, a non-zero polynomial whose leading coefficient is 1 is called a **monic polynomial**.

2.1.3 Remarks:

Let R be an integral domain. Then:

(1) If $p(x)$ and $q(x)$ are two non-zero elements of $R[x]$, then $deg(p(x)q(x)) = deg(p(x) + deg(q(x)$.

(2) $R[x]$ is an integral domain.

(3) **(Euclidean algorithm):** Given two polynomials $p(x)$ and $q(x) \neq 0$ in $R[x]$, there exist two polynomials $t(x), r(x) \in R[x]$ such that $p(x) = t(x)q(x) + r(x)$ where $r(x) = 0$ or $deg(r(x)) < deg(q(x))$.

Now let us discuss some of the important results involving rings and other concepts discussed in the previous chapter.

2.1.4 Theorem:

Suppose R is a commutative ring with 1. Then $a(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r \in R[x]$ is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, a_2, ..., a_r$ are all nilpotent in R.

Proof. Suppose $a(x) = a_0+a_1x+a_2x^2+...+a_rx^r$ is such that a_0 is a unit in R and $a_1, a_2, ..., a_r$ are all nilpotent in R. Since R is commutative, we get that $a_1x, a_2x^2, ..., a_rx^r$ are all nilpotent and hence also their sum, i.e., $z = a_1x + a_2x^2 + ... + a_rx^r$ is nilpotent. Now $a_0^{-1}z$ is nilpotent and so $1 + a_0^{-1}z$ is a unit. Thus $a(x) = a_0 + z = a_0(1 + a_0^{-1}z)$ which is a product of two units in $R[x]$ is a unit.

Conversely, suppose $a(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r$ is a unit in $R[x]$. It follows immediately that a_0 must be a unit in R. Now take any prime ideal P in R. For $a \in R$, let $\bar{a} = a + P$ in R/P. Look at the natural map $f_p : R[x] \to (R/P)[x]$, $b(x) = b_0 + b_1x + b_2x^2 + ... + b_sx^s \mapsto \bar{b}_0 + \bar{b}_1x + ... + \bar{b}_sx^s$. This f_p preserves addition and multiplication. Secondly, it takes identity of $R[x]$ to that of $(R/P)[x]$ and hence it takes

units to units. In particular, $f_p(a(x)) = \bar{a}_0 + \bar{a}_1 x + ... + \bar{a}_r x^r$ is a unit in $(R/P)[x]$. Since P is a prime ideal, R/P is an integral domain and hence $(R/P)[x]$ is an integral domain. Now $\bar{a}_0 + \bar{a}_1 x + ... + \bar{a}_r x^r$ is a unit in $(R/P)[x]$ means that $\bar{a}_0$ is a unit in R/P and $\bar{a}_1 = \bar{a}_2 = ... = \bar{a}_r = 0$, i.e., $a_1, a_2, ..., a_r \in P$. This shows that $a_1, a_2, ..., a_r$ belong to the intersection of all prime ideals in R which is nothing but the set of all nilpotent elements in R. Thus $a_1, a_2, ..., a_r$ are all nilpotent in R. □

2.1.5 Theorem:

Let I be an ideal of R, then $I[x]$ is an ideal of $R[x]$ and the quotient ring $R[x]/I[x]$ is naturally isomorphic to $(R/I)[x]$.

Proof. Let I be an ideal in R. Clearly, $I[x] = \{a_0 + a_1 x + a_2 x^2 + ... + a_r x^r \mid a_i \in I\}$ is an ideal in $R[x]$. Now look at the natural map $f : R[x] \to (R/I)[x]$, defined by $a(x) = a_0 + a_1 x + a_2 x^2 + ... + a_r x^r \mapsto \bar{a}_0 + \bar{a}_1 x + ... + \bar{a}_r x^r$ (where $\bar{a} = a + I$, for all $a \in R$). It can be easily checked that this is an epimorphism. Now
$Ker(f) = \{a(x) \in R[x] \mid \bar{a}_0 + \bar{a}_1 x + ... + \bar{a}_r x^r = \bar{0}\}$

$= \{a(x) \in R[x] \mid \bar{a}_0 = 0, \bar{a}_1 = 0, ..., \bar{a}_r = 0\}$

$= \{a_0 + a_1 x + a_2 x^2 + ... + a_r x^r \mid a_i \in I\} = I[x]$.

Hence, $R[x]/I[x] \approx (R/I)[x]$.

□

2.1.6 Remarks:

(1) Any field K is Euclidean. The algorithm map is the constant map $d : K^* \to \mathbb{Z}^+$, i.e., $d(x) = 1$, for all $x \in K^*$. The Euclidean algorithm is the trivial property that $x = (xa^{-1})a + 0$, for all $x \in K$ and for all $a \in K^*$.

(2) $R = K[x]$, the polynomial ring in one variable over a field K is Euclidean. The algorithm map is the degree map $d : K[x]^* \to \mathbb{Z}^+$, namely, $d(f(x)) =$ degree of $f(x)$ for a non-zero polynomial $f(x)$. The Euclidean algorithm is the usual division of polynomials.

2.1.7 Theorem:

For a commutative integral domain R with unity, the following are equivalent

(1) R is a field.

(2) $R[x]$ is an Euclidean domain.

(3) $R[x]$ is a PID.

Proof. By Remark (2.1.6) and Theorem (1.6.3), (1) $\Rightarrow$ (2) $\Rightarrow$ (3). We have only to show that (3) $\Rightarrow$ (1). Since x is a prime in $R[x]$, the ideal (x) is a non-zero prime ideal in $R[x]$ and hence maximal which implies that $\frac{R[x]}{x} \backsimeq R$ is a field.

□

To prove the most important theorem of Gauss for unique factorization domains in next section, we need the following definitions (here R stands for a UFD and $K = Q(R)$, its field of fractions). We begin with the following definition:

2.1.8 Greatest common divisor:

If a, $b \in R$ then $d \in R$ is said to be a greatest common divisor of a and b if

(1) $d|a$ and $d|b$.

(2) Whenever $c|a$ and $c|b$ then $c|d$. It is denoted by the symbol $d = (a, b)$.

2.2 Content of a Polynomial and Primitive Polynomials

2.2.1 Content of a polynomial:

Given a non-zero polynomial $f(x)$ in $R[x]$, the gcd of the coefficients of $f(x)$ is called the content of $f(x)$ and is denoted by $c(f(x))$ or simply $c(f)$.

2.2.2 Example:

Let $f(x) = 4x^2 - 6x + 12 \in \mathbb{Z}(x), c(f) = 2$.

2.2.3 Primitive polynomial:

A non-zero polynomial $f(x) \in R[x]$ is called primitive if its content is 1.

2.2.4 Example:

Let $f(x) = 9x^2 - 12x + 8 \in \mathbb{Z}(x), c(f) = 1$. Therefore $f(x)$ is primitive.

2.2.5 Remarks:

(1) Any non-zero polynomial $f(x) \in R[x]$ can be written as a product of a non-zero scalar and a primitive polynomial because $\frac{f(x)}{c(f(x))}$ is primitive and $c(f(x))$ is a non-zero scalar.

(2) Any irreducible polynomial is primitive.

2.2.6 Proposition:

The content of a product of polynomials is the product of their contents and in particular, the product of primitive polynomials is primitive.

Proof. In view of the Remark (2.1.6), it suffices to prove the result for the case of primitive polynomials. Let$f(x)$, $g(x)$ be primitive in $R[X]$. Let $h(x) = f(x)g(x)$. We have to show that $c(h)$ is identity in R. If not, take a prime divisor p of $c(h)$. Write

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$$

and

$$g(x) = b_0 + b_1x + b_2x^2 + ... + b_nx^n$$

where $a_mb_n \neq 0$. Since $c(f) = c(g) = 1$, we can find r, s least such that p is not a divisor of a_r or b_s, $0 \leq r \leq m$, $0 \leq s \leq n$. Note that

$$p|a_i,\ 0 \leq i \leq r-1 \text{ and } p|b_j,\ 0 \leq j \leq s-1$$

by the choice of r and s. Now look at the coefficient of $h(x)$, namely, $\Sigma_{i+j=r+s}a_ib_j$. Since p is a prime divisor of $c(h)$, it is a divisor of this coefficient of $h(x)$. On the other hand, since p is a divisor of a_i, $0 \leq i \leq r-1$ and of b_j, $0 \leq j \leq s-1$, it follows that p is a divisor of a_rb_s which is a contradiction to the fact that p is not a divisor of a_r or b_s. Hence $c(h) = 1$, as required. □

2.3 Ring of Polynomials over a UFD

2.3.1 Gauss Lemma:

[Theorem (4.5.11) of [71]]. A primitive polynomial $f(x) \in R[x]$ is irreducible in $R[x]$ if and only if $f(x)$ is irreducible in $K[x]$ where K is the field of fractions of R.

Proof. Assume that $f(x)$ is primitive and irreducible in $R[x]$. Let, if possible, $f(x)$ be irreducible in $K[x]$, say $f(x) = g(x)h(x)$ with $g(x), h(x) \in K[x]$. We can write $g(x) = (\frac{a}{b})p(x)$ and $h(x) = (\frac{c}{d})q(x)$ with a, b, c, $d \in R^*$, $p(x)$, $q(x) \in R[x]^*$ and both $p(x)$ and $q(x)$ primitive.

Now, we can write $f(x) = (\frac{\alpha}{\beta})p(x)q(x)$ for some $\alpha, \beta \in R^*$ with α, β coprime. Thus we get $\beta f(x) = \alpha p(x)q(x)$ and hence comparing contents on either side, we have $\beta c(f) = \alpha c(p)c(q)$, i.e., $\beta = \alpha$ which means $f(x) = p(x)q(x)$ in $R[x]$ contradicting the irreducibility of $f(x)$.

Conversely, if $f(x) \in R[x]$ is irreducible in $K[x]$, then it is obviously irreducible in $R[x]$ since $f(x)$ is primitive. □

2.3.2 Gauss Theorem:

[Theorem (4.5.12) of [71]]. Let R be an integral domain. Then $R[x]$ is a UFD if and only if R is a UFD.

Proof. If $R[x]$ is a FD so is R since (for degree reasons) all factors in $R[x]$ of an element in R belong to R. Moreover, elements of R are irreducible (resp. prime) in R if and only if they are irreducible (resp. prime) in $R[x]$. Consequently, if $R[x]$ is a UFD and $a \in R$ is irreducible, then a is prime in $R[x]$ and so a prime in R. Thus R is a UFD.

Conversely, suppose that R is a UFD. Since R is an FD, it is easy to see, for degree reasons, that $R[x]$ is also a FD. The difficult part is the uniqueness of factorization. It suffices to prove that every irreducible polynomial in $R[x]$ is a prime. This is assured by Gauss Lemma. To see this; let $p(x)$ be irreducible in $R[x]$ and suppose that $\frac{p(x)}{f(x)g(x)}$ in $R[x]$. Since $p(x)$ is irreducible in $R[x]$, by Gauss Lemma, it is is irreducible in $K[x]$. But $K[x]$ is a UFD since K is a field. Therefore $p(x)$ is prime in $K[x]$ and so $\frac{p(x)}{f(x)}$ or $g(x)$ in $K[x]$, say $\frac{p(x)}{f(x)}$, i.e., $f(x) = p(x)q(x)$ for some $q(x) \in K[x]$. We can write $q(x) = (\frac{a}{b})q_0(x)$ with a, $b \in R^*$,

a, b coprime and $q_0(x) \in R[x]^*$, $q_0(x)$ primitive. Now substituting we get $bf(x) = ap(x)q_0(x)$ in $R[x]$. Taking contents on either side, we get $bc(f) = a$ and hence on cancelation we get that $f(x) = c(f)p(x)q_0(x)$ in $R[x]$ which means $\frac{p(x)}{f(x)}$ in $R[x]$ implying $p(x)$ is a prime in $R[x]$, as required. □

2.4 Eisenstein's Irreducible Criterion

2.4.1 Theorem:

[Theorem (4.6.1) of [71]]. Let R be a UFD and $f(x) \in R[x]^*$ be a primitive polynomial, say

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_rx^r,\ a_r \neq 0.$$

Suppose there is a prime p in R such that

(i) $p|a_i$, $0 \leq i \leq r-1$ and $p \nmid a_r$, i.e., p divides all but the leading coefficient and

(ii) $p^2 \nmid a_0$. Then $f(x)$ is irreducible.

Proof. Let $f(x)$ be irreducible, say $f(x) = g(x)h(x)$ where $g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$ and $h(x) = c_0 + c_1x + c_2x^2 + ... + c_nx^n$ with $b_mc_n \neq 0$. We shall prove that either $g(x)$ or $h(x)$ is a unit. Since $f(x)$ is primitive, so are $g(x)$ and $h(x)$ by Gauss lemma. Since $p|a_0 = b_0c_0$, we get that $p|b_0$ or $p|c_0$, say $p|b_0$. Furthermore, p cannot divide c_0 since p^2 does not divide a_0. On the other hand, since p does not divide $a_r = b_mc_n$, p cannot divide b_m or c_n. Let l be least such that p does not divide b_l. We get that $1 \leq l \leq m$. If $n \neq 0$, we get that $l \leq m < m+n = r$. But then, $p|a_l$ where $a_l = \sum_{i+j=l} b_ic_j$ implying that $p|b_lc_0$ (since $p|b_i$, $0 \leq i \leq l-1$ and $p|a_l$). This is a contradiction. Hence $n = 0$ which means that c_0 is a unit since $h(x) = c_0$ is primitive. Thus $f(x)$ is irreducible. □

2.4.2 Remark:

The Eisenstein's Criterion is only a sufficient condition but not necessary.

For example, the polynomial $f(x) = 1+x+x^2+...+x^{p-1}$ is irreducible in $\mathbb{Z}[x]$ for any prime number p in $\mathbb{Z}$, yet obviously there is no prime satisfying the conditions of the criterion. To see the irreducibility of $f(x)$,

first note that $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. We have $f(x) = (\frac{(x^p-1)}{(x-1)}$ and so

$$f(x+1) = [(x+1)^p - 1]/x = x^{p-1} + px^{p-2} + ... + p.$$

This is a monic polynomial for which Eisenstein's Criterion can be applied with the prime p and hence irreducible, as required.

2.5 Exercises

(1) Show that the number of roots of a non-zero polynomial over a commutative integral domain R is atmost its degree.

(2) Let R be commutative with 1. Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$ in $R[x]$ be such that a_0 is a unit and $a_1, ..., a_n$ are all nilpotent in R. Show that $f(x)$ is a unit in $R[x]$.

(3) Show that $1+x^2$ is prime and is coprime to $1+x+x^3+x^6$ in $\mathbb{Z}[x]$.

(4) Let R be a commutative ring such that $R[x]$ has a non-trivial zero-divisor $f(x)$. Show that $af(x) = 0$ for some non-zero element $a \in R$. Is the commutativity of R essential?

(5) Show that $1+x+x^3+x^6$ is not irreducible in $R[x]$ for any domain R with 1.

(6) Let R be a domain and $f(x) \in R[x]$ be a polynomial of positive degree. Show that $f(x)$ is irreducible if and only if $f(x+a)$ is irreducible for any domain $a \in R$.

(7) Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. Suppose that a rational number r is a root of $f(x)$. Then show that r is an integer. Generalize this statement to an arbitrary UFD R in place of $\mathbb{Z}$, i.e., if an element x of $Q(R)$ is a root of a monic polynomial in $R[x]$, then show that $x \in R$.

(8) Show that for a commutative ring R, the principal ideal (x) is prime in $R[x]$ if and only if R is an integral domain.

(9) Show that for any prime ideal P of a commutative ring R,the ideal $P[x]$ is prime in $R[x]$.

(10) Prove that $R[x]$ is a commutative ring with unit whenever R is.

(11) If R is an integral domain with unit element, prove that any unit in $R[x]$ must already be a unit in R.

Chapter

3

MODULES WITH CHAIN CONDITIONS

In this chapter, we shall study the basic properties of an important class of modules and rings, ('Artinian and Noetherian'), which have some very special properties. Our study of ring theory in class covered a wide variety of areas in and uses of the topic. Field theory and polynomial rings were of particular interest with the end goal being Galois theory. One topic that was briefly introduced was Noetherian and Artinian rings.

These two characterizations for rings are worth deeper study. The essential features are the ascending and descending chain conditions on submodules. In a sense, Artinian and Noetherian rings have some measure of finiteness associated with them. In fact, the conditions for Artinian and Noetherian rings, called respectively the descending and ascending chain conditions, are often termed the minimum and maximum conditions. These properties make Artinian and Noetherian rings of interest to an algebraist. Furthermore, these two types of rings are related. In (1921), Emmy Noether introduced the ACC for the first time in mathematics literature. She was considering ideals in commutative rings. After Noether's introduction of the ACC, work in this area of ring theory exploded. Her results were expanded to non-commutative settings. In addition, other similar conditions for ideals in a ring were introduced. In particular, Emil Artin formulated the DCC in (1927), which provided a minimum condition to complement the maximum condition given by the ACC.

It was later discovered, first by Noether herself and then more formally by Hopkins and Levitzki, that the DCC is actually the stronger condition. Specifically, a consequence of the Akizuki Hopkins Levitzki Theorem (3.6.4) is that a left (right) Artinian ring is automatically a left (right) Noetherian ring. This is not true for general modules, that is, an Artinian module need not be a Noetherian module. Over a commutative ring, every cyclic Artinian module is also Noetherian, but over noncom-

mutative rings cyclic Artinian modules can have uncountable length. The Noetherian condition as well as the Artinian condition can also be defined on bimodule structures as well. It has proved advantageous to study these conditions separately - in the form of Noetherian modules and Artinian modules as well as together. Unless otherwise stated, R stands for a ring with 1 (commutative or not) and all modules considered are assumed to be unitary modules.

3.1 Chain Conditions: Artinian Modules, Noetherian Modules

Before we discuss Noetherian and Artinian rings, it is important to introduce the concepts behind them. In particular, we need definitions for the maximum and minimum conditions that characterize the two types of rings. We will state these definitions in terms of rings, but they can be generalized to apply to other algebraic objects besides rings. In addition, the definitions depend on ideals. Our discussion was primarily limited to commutative rings. Because of this, all ideals we discussed were two sided. In non-commutative rings, this does not have to be the case. In order to solidify what is meant, we provide the following definition.

3.1.1 Definition:

Let R be a ring and I be a subring of R. For an element $r \in R$, let $Ir = \{ar \mid a \in I\}$. I is a right ideal of R if $Ir \subset I$ for all $r \in R$.

Left ideals can be defined in an entirely analogous manner by replacing right with left and Ir with rI. In a commutative ring, it is clear that if the condition for a right ideal is met, then the condition for a left ideal must also be met. In non-commutative rings, right and left ideals do not have to coincide and in general do not. The definitions below use the term ideal loosely. That is, the term ideal can refer to right, left, or two-sided ideals. However, it is only referring to one type of ideal at a time. That being said, we introduce the following definition.

3.1.2 Ascending chain conditions ACC for modules:

Let R be a ring and M a right R-module. Then M satisfies the ACC for its submodules if any ascending sequence of submodules of M say

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq ... \subseteq M_i \subseteq M_{i+1} \subseteq ..... \tag{3.1}$$

is stationary.
i.e., there exists $n \in \mathbb{N}$ such that $M_n = M_{n+1} = ...$
In this case we say that the sequence (3.1) terminates.
i.e., $M_1 \subseteq M_2 \subseteq M_3 \subseteq ... \subseteq M_n$.

3.1.3 Definition:

Let R be a ring. Let $I_1, I_2, ...$ be an arbitrary chain of ideals in R such that $I_1 \subset I_2 \subset ....$
If there exists an $N \in \mathbb{N}$ such that $I_n = I_N$ for $n \geq N$, then R is said to satisfy the Ascending Chain Condition (ACC).

3.1.4 Definition:

Let R be a ring. Then a module M_R has the maximum condition for submodules if for any non-empty family $\mathcal{A}$ of submodules of M_R, has a maximal member.

i.e., $N \in \mathcal{A}$ is called maximal member of $\mathcal{A}$ if for $N' \in \mathcal{A}$ with $N \subseteq N'$, we have $N = N'$. ACC can be understood as a maximum condition on ideal chains in a ring R. A ring satisfying ACC has chains of ideals that always top out. Such a ring is called Noetherian. This name comes from the mathematician Emmy Noether. If ACC is met on right ideals, the ring is right Noetherian. If it is met on left ideals the ring is left Noetherian. The term Noetherian is reserved for rings that satisfy ACC on both right and left ideals. In commutative rings, all three of these conditions coincide.

Like ACC, there is a similar minimum condition for ideal chains in a ring. This condition is given in the definition below.

3.1.5 Descending chain conditions DCC for modules:

Let R be a ring and M a right R-module. Then M satisfies the DCC for its submodules if any descending sequence of submodules of M_R say

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq ... \supseteq M_i \supseteq M_{i+1} \supseteq ..... \tag{3.2}$$

is stationary.
i.e., there exists $n \in \mathbb{N}$ such that $M_n = M_{n+1} = ...$
In this case we say that the sequence (3.2) terminates.
i.e., $M_1 \supseteq M_2 \supseteq M_3 \supseteq ... \supseteq M_n$.

3.1.6 Definition:

Let R be a ring. Let $I_1, I_2, ...$ be an arbitrary chain of ideals in R such that $I_1 \supset I_2 \supset ...$.
If there exists an $N \in \mathbb{N}$ such that $I_n = I_N$ for $n \geq N$, then R is said to satisfy the Descending Chain Condition (DCC).

3.1.7 Definition:

Let R be a ring. Then a module M_R has the minimum condition for submodules if for any non-empty family $\mathcal{A}$ of submodules of M_R, has a minimal member.

i.e., $N \in \mathcal{A}$ is called minimal member of $\mathcal{A}$ if for $N' \in \mathcal{A}$ with $N' \subseteq N$, we have $N = N'$.

The minimum condition provided by DCC is equivalent to saying that all ideal chains in a ring R bottom out. Rings satisfying DCC are called Artinian after mathematician Emil Artin. As with ACC, the terms right and left Artinian come into play for right and left ideals respectively. Artinian rings meet DCC on left and right ideals. Once again, all three conditions coincide for commutative rings.

3.1.8 Definition:

Let R be a ring. A submodule N_R of a module M_R is said to be finitely generated if

$$N_R = x_1R + x_2R + ... + x_nR;\ x_i \in N$$

and $n \geq 1$ are integers.

In this case, $x_1, x_2, ..., x_n$ are called generators of N_R.

Historically, Hilbert was the first mathematician to work with the properties of finitely generated submodules. He proved an important theorem known as Hilbert's basis theorem which says that any ideal in the multivariate polynomial ring of an arbitrary field is finitely generated. However, the property is named after Emmy Noether who was the first one to discover the true importance of the property. Notice the similarity between the ACC and DCC definitions. Together, they provide some

sense of boundedness or finiteness for rings. It is also the case that Artinian and Noetherian rings share many properties.

3.1.9 Artinian Modules

Theorem: The following are equivalent for an R-module M.

(1) Descending chain condition holds for submodules of M.

(2) Minimum condition for submodules holds for M.

Proof. (1) $\Rightarrow$ (2): Let $\mathcal{F} = \{M_i, i \in I\}$ be a non-empty family of submodules of M. Pick any index $i_1 \in I$ and look at M_{i_1}. If M_{i_1} is minimal in $\mathcal{F}$, we are through. Otherwise, there is an $i_2 \in I$ such that $M_{i_1} \supset M_{i_2}, M_{i_1} \neq M_{i_2}$. If this M_{i_2} is minimal in $\mathcal{F}$, we are through again. Proceeding thus, if we do not find a minimal element at any finite stage, we would end up with a non-stationary descending chain of submodules of M, namely, $M_{i_1} \supset M_{i_2} \supset ... \supset M_{i_n} \supset .....$ contradicting (1).

(2) $\Rightarrow$ (1) Let $M_1 \supseteq M_2 \supseteq M_3 \supseteq ... \supseteq M_n \supseteq ... \supseteq ...$ be a descending chain of submodules of M. Consider the non-empty family $\mathcal{F} = \{M_i, i \in \mathbb{N}\}$ of submodules of M. This must have a minimal element, say M_r, for some r. Now we have $M_s \subseteq M_r$, for all $s \geq r$ which implies by minimality of M_r that $M_s = M_r$, for all $s \geq r$. □

3.1.10 Artinian module:

A module M is called *Artinian* if DCC (or equivalently, the minimum condition) holds for M.

3.1.11 Examples:

(1) A module which has only finitely many submodules is Artinian. In particular, finite abelian groups are Artinian as modules over $\mathbb{Z}$.

(2) Finite dimensional vector space are Artinian (for reasons of dimension) whereas infinite dimensional ones are not Artinian.

(3) Infinite cyclic groups are not Artinian. For instance, $\mathbb{Z}$ has a non-stationary descending chain of subgroups , namely,
$\mathbb{Z} = (1) \supset (2) \supset (4) \supset ... \supset (2^n) \supset ... \supset ...$

3.1.12 Proposition:

Let N be a submodule of a module M. Then M is Artinian if and only if N and M/N are both Artinian.

Proof. Let M be Artinian and N be a submodule of M. Any family of submodules of N is also one in M and hence the result follows. On the other hand, any descending chain of submodules of M/N corresponds to one in M (wherein each member contains N and hence the result).

Conversely, let

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq ... \supseteq M_n \supseteq ... \supseteq ...$$

be a descending chain in M. Intersecting with N gives the descending chain in N, namely,

$$N \cap M_1 \supseteq N \cap M_2 \supseteq N \cap M_3 \supseteq ... \supseteq N \cap M_n \supseteq ... \supseteq ...$$

which must be stationary, say $N \cap M_r = N \cap M_{r+1}$ for some r. On the other hand, we have the descending chain in M/N, namely,

$$\tfrac{N+M_1}{N} \supseteq \tfrac{N+M_2}{N} \supseteq \tfrac{N+M_3}{N} \supseteq ... \supseteq \tfrac{N+M_n}{N} \supseteq ... \supseteq ...$$

which must be also stationary, say

$$\tfrac{N+M_s}{N} = \tfrac{N+M_{s+1}}{N} = ...$$

for some s. Now we prove the following.

Claim : $M_n = M_{n+1}$, for all $n \geq (r+s)$.

This is an immediate consequence of the four facts , namely,

(1) $M_n \supseteq M_{n+1}$, $\forall\ n \in \mathbb{N}$,

(2) $N \cap M_n = N \cap M_{n+1}$, for all $n \geq r$,

(3) $\tfrac{N+M_n}{N} = \tfrac{N+M_{n+1}}{N}$, for all $n \geq s$ and

(4) $\tfrac{N+M_n}{N} \simeq \tfrac{M_n}{N \cap M_n}$, for all $n \geq \mathbb{N}$.

Putting together we get that

$$\tfrac{M_n}{N \cap M_n} = \tfrac{N+M_n}{N} = \tfrac{N+M_{n+1}}{N} = \tfrac{M_{n+1}}{N \cap M_{n+1}}$$

which implies the claim and hence the result. □

3.1.13 Corollary:

Any finite direct sum of Artinian modules is Artinian.

Proof. For, let $M_1, ..., M_n$ be Artinian submodules of a module M. Let $N = \sum_{i=1}^{n} M_i$. To prove N is Artinian, proceed by induction on n. If $n = 1$, there is nothing to prove. Let $n \geq 2$ and assume, by induction, that $N' = \sum_{i=1}^{n-1} M_i$ is Artinian. Now look at

$$\frac{N}{M_n} = \frac{N'+M_n}{M_n} \simeq \frac{N'}{N' \cap M_n}$$

which is Artinian being a quotient of the Artinian module N'. Thus both M_n and N/M_n are Artinian and hence N is Artinian, as required. the case of a direct sum is an immediate consequence because if

$$M = \oplus_{i=1}^{n} M_i,$$

then M is a finite sum of the Artinian submodules M_i and hence Artinian. □

3.1.14 Corollary:

If R is a right/left Artinian ring, then all finitely generated right/left R-modules are Artinian.

Proof. If R is a finitely generated right R-module, then $R \cong F/K$ for some finitely generated free right R-module F and some submodule $K \leq F$. Since F is isomorphic to a finite direct sum of copies of the Artinian module R_R, it is Artinian by Corollary (3.1.13). Then by Proposition (3.1.12), R must be Artinian. □

3.1.15 Remarks:

(1) Direct sum of an infinite family of non-zero Artinian modules is not Artinian (because it contains non-stationary descending chains).

(2) However, a sum of an infinite family of distinct Artinian modules could be Artinian. (For example, the Euclidean plane $\mathbb{R}^2$ is a sum of all the lines passing through the origin and is a direct sum of any two of them).

(3) Minimal submodules exist in a non-zero Artinian module because a minimal submodule is simply a minimal element in the family of all non-zero submodules of M.

3.1.16 Corollary:

Every non-zero submodule of an Artinian module contains a minimal submodules.(Obvious by Remark (3.1.15(3))).

3.1.17 Noetherian Modules

Theorem: The following are equivalent for an R-module M.

(1) Ascending chain condition holds for submodules of M.

(2) Maximum condition for submodules holds for M.

Proof. (1) $\Rightarrow$ (2): Let $\mathcal{F} = \{M_i, i \in I\}$ be a non-empty family of submodules of M. Pick any index $i_1 \in I$ and look at M_{i_1}. If M_{i_1} is maximal in $\mathcal{F}$, we are through. Otherwise, there is an $i_2 \in I$ such that $M_{i_1} \subset M_{i_2}$, $M_{i_1} \neq M_{i_2}$. If this M_{i_2} is maximal in $\mathcal{F}$, we are through again. Proceeding thus, if we do not find a maximal element at any finite stage, we would end up with a non-stationary ascending chain of submodules of M, namely,

$$M_{i_1} \subset M_{i_2} \subset ... \subset M_{i_n} \subset .....$$

contradicting (1).

(2) $\Rightarrow$ (3) Let N be submodule of M. Consider the family $\mathcal{F}$ of all finitely generated submodules of N. This family is non-empty since the submodule (0) is a member. This family has a maximal member, say $N_0 = (x_1, ..., x_r)$. If $N_0 = N$, pick an $x \in N$, $x \notin N_0$. Now

$$N_1 = N_0 + (x) = (x, x_1, x_2, ..., x_r)$$

is a finitely generated submodule of N and hence $N_1 \in \mathcal{F}$. But then this contradicts the maximality of N_0 in $\mathcal{F}$ since $N_0 \subset N_1$, $N_0 \neq N_1$ and so $N_0 = N$ is finitely generated.

(3) $\Rightarrow$ (1) Let $M_1 \subseteq M_2 \subseteq M_3 \subseteq ... \subseteq M_n \subseteq ... \subseteq ...$ be a ascending chain of submodules of M. Consider the submodule

$$N = \cup_{i=1}^{\infty} M_i$$

of M which must be finitely generated, say $N = (x_1, x_2, ..., x_n)$. It follows that $x_i \in M_r$, for all i, $1 \leq i \leq n$ for some $r(\gg 0)$. Now we have $N \subseteq M_s \subseteq N$, for all $s \geq r$ and so

$$N = M_r = M_{r+1} = ...$$

□

3.1.18 Noetherian module:

A module M is called *Noetherian* if ACC (or equivalently, the maximum condition or the finiteness condition) holds for M.

3.1.19 Note:

The *finiteness condition* has no parallel in the Artinian case. This additional property makes Noetherian modules rather special and the study more interesting.

3.1.20 Examples:

(1) A module which has only finitely many submodules is Noetherian. In particular, finite abelian groups are Noetherian as modules over $\mathbb{Z}$.

(2) Finite dimensional vector space are Noetherian (for reasons of dimension) whereas infinite dimensional ones are not Noetherian.

(3) Unlike the Artinian case, infinite cyclic groups are Noetherian because every subgroup of a cyclic group is again cyclic.

Our first few results concerning Noetherian modules are completely analogous to the corresponding results for Artinian modules (see Proposition (3.1.12), Corollary (3.1.13), Corollary (3.1.14)). The proofs of the Noetherian results may be obtained by imitating the proofs in the Artinian case, reversing inclusions when necessary.

3.1.21 Proposition:

Let N be a submodule of a module M. Then M is Noetherian if and only if N and M/N are both Noetherian.

3.1.22 Corollary:

Any finite direct sum of Noetherian modules is Noetherian.

3.1.23 Corollary:

If R is a right/left Noetherian ring, then all finitely generated right/left R-modules are Noetherian.

3.1.24 Remark:

(1) Direct sum of an infinite family of non-zero Noetherian modules is not Noetherian (because it contains non-stationary ascending chains).

(2) Maximal submodules exist in a non-zero Noetherian module because a maximal submodule is simply a maximal element in the family of all (proper) submodules N of M, $N \neq M$.

(3) However, maximal submodules exist in any finitely generated non-zero modules, even if the module is not Noetherian. (This is a simple consequence of Zorn's lemma applied to the family of all proper submodules of such a module). (See (3.1.27)(4) below, for an example of a finitely generated module which is not Noetherian).

3.1.25 Corollary:

Every non-zero submodule of a Noetherian module is contained in a maximal submodule. (Obvious by Remark (3.1.24)(2)).

3.1.26 Definition:

Consider the abelian group μ_{p^*} of all complex $(p^n)^{th}$ roots of unity or a fixed prime number p and all $n \in \mathbb{N}$. For each positive integer n, let μ_{p^n} denote the cyclic group of all complex $(p^n)^{th}$ roots of unity so that we have

$$\mu_p \subset \mu_{p^2} \subset ... \subset \mu_{p^n} \subset ... \subset$$

and hence

$$\mu_{p^*} = \bigcup_{n=1}^{\infty} \mu_{p^n}.$$

3.1.27 Some Pathologies:

(1) An Artinian module need not be finitely generated.

(2) Maximal submodules need not exist in an Artinian module.

(3) An Artinian module need not be Noetherian.

(4) A finitely generated module need not be Noetherian.

(5) Minimal submodules need not exist in an Noetherian module.

(6) An Noetherian module need not be Artinian.

(7) There are modules which are neither Artinian nor Noetherian.

Now we give some counter-examples.

Example A: The group μ_{p^*} is Artinian but not Noetherian, not finitely generated and does not have maximal subgroups. This justifies the statements (1), (2) and (3).

Example B: Let $R = \mathbb{Z}[X_1, X_2, ..., X_n, ..., ...]$ be the polynomial ring in infinitely many variables. We know that R, as a module over itself, is generated by 1 but R is not Noetherian because it has non-stationary ascending chain of ideals, namely,

$$(X_1) \subset (X_1, X_2) \subset (X_1, ..., X_n) \subset ... \subset ...$$

This serves the purpose for statement (4).

Example C: The finite cyclic group $\mathbb{Z}$ is Noetherian but not Artinian and it has no minimal subgroups. This justifies statements (5) and (6).

Example D: Direct sum of any infinite family of non-zero modules, in particular, an infinite dimensional vector space, is neither Artinian nor Noetherian.

3.2 Modules of Finite Length

Recall that a module M is called simple if

(1) $M \neq (0)$ and

(2) M has no submodules other than (0) and M.

3.2.1 Remark:

Simple submodules exist in a non-zero Artinian module while simple quotients exist for a non-zero Noetherian one.

3.2.2 Definition:

A composite series for a module A is a chain of submodules

$$A_0 = 0 < A_1 < ... < A_n = A$$

such that each of the factors A_i/A_{i-1} is a simple module. The number of gaps (namely n) is called the *length of the composition series*, and the factors A_i/A_{i-1} are called the *composition factors of* A corresponding to this composition series. By convention, the zero module is considered to have a composition series of length zero, with no composition factors. A *module of finite length* is any module which has a composition series.

3.2.3 Remark:

For a non-zero module M, a composition series may or may not exist. If one exists, we notice that M would have a simple submodule M_{m-1} and a maximal submodule M_1 (i.e., a simple quotient M_0/M_1).

3.2.4 Examples:

(1) A vector space V having a finite basis has a composition series of length m, namely,

$$V = V_0 \supset V_1 \supset ... \supset V_m = (0)$$

where V_i = span of $v_{i+1}, v_{i+2}, \cdots, v_m$ for all i, $0 \leq i \leq m$ with $V_m = 0$. (However, a vector space having an infinite basis cannot have a composition series.)

(2) A finite abelian group has a composition series.

(3) An infinite cyclic group cannot have a composition series since it has no minimal submodules.

3.2.5 Proposition:

A module A has a finite length if and only if A is both Noetherian and Artinian.

Proof. If A has finite length, then (since simple modules are clearly Noetherian and Artinian) it follows from Propositions (3.1.12) and (3.1.21) that A must be Noetherian and Artinian. Conversely, assume that A

satisfies both chain conditions and set $A_0 = 0$. If $A \neq 0$, then, by the DCC, A contains a minimal non-zero submodule A_1, that is, A_1 is simple. Similarly, if $A_1 < A$, then A/A_1 contains a simple submodule A_2/A_1 and we continue in this manner. By the ACC, the chain $A_0 < A_1 < A_2 < ...$ must terminate at some integer n. Then $A_n = A$, and the chain $A_0 < A_1 < ... < A_n$ is a composition series for A.

For instance, if R is an algebra over a field k, then any R-module which is finite dimensional over k has finite length. □

3.2.6 Theorem:

(1) Submodules and quotient modules of a module of finite length are modules of finite length.

(2) If a module M has a submodule N such that both N and M/N are of finite length, then M is of finite length.

Proof. Put together (3.1.12), (3.1.21) and (3.2.6) above. □

3.2.7 Theorem (Jordan-Holder):

[Theorem (4.11) of [41]]. If a module A has finite length, then any two composition series for A are isomorphic. In particular, all composition series for A have the same length.

Proof. Consider two composition series

$$A_0 = 0 < A_1 < ... < A_n = A$$

and

$$B_0 = 0 < B_1 < ... < B_t = A$$

By Theorem (4.10) [41], these two submodules have isomorphic refinements, say

$$C_0 = 0 < C_1 < ... < C_m = A$$

and

$$D_0 = 0 < D_1 < \cdots < D_m = A.$$

There is a permutation σ of $\{1, 2, ..., m\}$ such that $\frac{C_k}{C_{k-1}} \cong \frac{D_{\sigma(k)}}{D_{\sigma(k)-1}}$ for all $k = 1, ..., m$.

Since each of the factors A_i/A_{i-1} is simple, there are no submodules lying strictly between A_{i-1} and A_i. Consequently, the refined series $C_0 \leq C_1 \leq ... \leq C_m$ consists of the submodules $A_0, A_1, ..., A_n$ in order but with possible repetitions. Hence, among the factors C_k/C_{k-1}, each factor A_i/A_{i-1} occurs exactly once, and the remaining factors are all zero. Similarly, among the factors $D_{\sigma(k)}/D_{\sigma(k)-1}$, each factor B_j/B_{j-1} occurs once, and the remaining factors are all zero.

Since

$$\frac{C_k}{C_{k-1}} \neq 0$$

if and only if

$$\frac{D_{\sigma(k)}}{D_{\sigma(k)-1}} \neq 0,$$

we conclude that $n = t$ and that there exists a permutation π of $\{1, 2, ..., n\}$ such that, whenever

$$\frac{C_k}{C_{k-1}} = \frac{A_i}{A_{i-1}},$$

then

$$\frac{D_{\sigma(k)}}{D_{\sigma(k)-1}} = \frac{B_{\pi(i)}}{B_{\pi(i)-1}}.$$

Therefore

$$\frac{A_i}{A_{i-1}} \cong \frac{B_{\pi(i)}}{B_{\pi(i)-1}}$$

for $i = 1, ..., n$. Which proves that the given composition series are isomorphic. □

3.2.8 Definition:

If A is module of finite length, the common length of all composition series for A is called the *length (or the composition length) of* A, and we shall denote it by length(A).

For instance, the only module of length 0 is the zero module, and the modules of length 1 are precisely the simple modules. Note that a finitely generated semisimple module A has finite length, and if A is a direct sum of n simple submodules, then length$(A) = n$.

3.2.9 Proposition:

Let A be a module of finite length. If B is any submodule of A, then

$$\text{length}(A) = \text{length}(B)+\text{length}(A/B).$$

Proof. Since this is clear if either $B = 0$ or $B = A$, we may assume that $0 < B < A$. In this case, choose composition series

$$B_0 = 0 < B_1 < ... < B_m = B$$

$$C_0/B = 0 < C_1/B < ... < C_n/B = A/B$$

for B and A/B. Since the chain

$$B_0 = 0 < B_1 < ... < B_m < C_1 < ... < C_n = A$$

is a composition series for A, the result follows. □

In particular, if $A_1, ..., A_n$ are modules of finite length, then

$$\text{length}(A_1 \oplus ... \oplus A_n) = \text{length}(A_1) + ...+\text{length}(A_n).$$

3.3 Artinian Rings

3.3.1 Artinian ring :

A ring R is called (left) Artinian if it is Artinian as a left module over itself, i.e., DCC or minimum condition holds for left ideals of R.

3.3.2 Examples:

Fields, division rings, finite rings are all Artinian. The ring of integers $\mathbb{Z}$ is not Artinian.

3.3.3 Proposition:

A quotient ring of an Artinian ring is Artinian (whereas a subring need not be Artinian.)

Proof. If I is a 2-sided ideal of an Artinian ring R, then R/I is Artinian as a R-module. But the family of all left ideals of R/I is precisely the family of all left ideals of R each containing I and hence it follows that R/I is an Artinian ring, as required. The subring $\mathbb{Z}$ of the Artinian ring $\mathbb{Q}$ is not Artinian. □

3.3.4 Proposition:

A finitely generated module over an Artinian ring is Artinian.

Proof. If a module M is generated by n elements, then M is a quotient of cartesian product R^n which is Artinian (since R is Artinian) and hence M is Artinian, as required. □

3.3.5 Corollary:

Matrix rings over Artinian rings with unity, (in particular, over division rings), are Artinian.

Proof. Let R be Artinian ring and $S = M_n(R)$ be a matrix ring over R. It is clear that any left ideal of S is also an R-submodule of S. But S is Artinian as a R-module since it is finitely generated over R, (in fact, it is a free R-module with a basis having n^2 elements). Hence S is an Artinian ring as required. □

3.3.6 Theorem:

Let R be an Artinian ring with unity. Then we have the following.

(1) Every non-zero divisor in R is a unit. In particular, an Artinian integral domain is a division ring.

(2) If R is commutative, every prime ideal is maximal. (In particular, a commutative Artinian integral domain is a field).

Proof. **(1).** Let $x \in R$ be a non-zero divisor. Note then that x^r is not a zero-divisor for any $r \in \mathbb{N}$. Since R is Artinian. the descending chain of principal left ideals, namely,

$$(x)_l \supset (x^2)_l \supset ... \supset (x^n)_l \supset ...$$

must be stationary, say

$$(x^r)_l = (x^{r+1})_l = ... =$$

for some $r \in \mathbb{N}$. Since $(x^r) \in (x^{r+1})_l$, we can write $(x^r) = y(x^{r+1})$ for some $y \in R$. This gives $(1 - yx)(x^r) = 0$ and hence $1 = yx$ (on canceling x^r which is not a zero-divisor). Now we have $x = x(yx) = (xy)x$ and hence $(1 - xy)x = 0$ implying $1 = xy$ (on canceling x). Thus we get that $yx = 1 = xy$.

(2). If R is commutative Artinian and P is a prime ideal in R, then R/P is an Artinian integral domain and hence every non-zero element (being not a zero-divisor) is a unit, i.e., R/P is a field, i.e., P is a maximal ideal, as required.

□

3.3.7 Corollary:

For a ring R, the following conditions are equivalent:

(a) R is right Artinian and semiprime.

(b) R is left Artinian and semiprime.

(c) R is semiprime.

Proof. Combine Theorem (3.6.2) and Corollary (3.6.5). □

3.3.8 Corollary:

For a ring R, the following conditions are equivalent:

(a) R is prime and right Artinian.

(b) R is prime and left Artinian.

(c) R is simple and right Artinian.

(d) R is simple and left Artinian.

(e) R is simple and semisimple.

(f) $R \cong M_n(D)$ for some positive integer n and some division ring D.

Proof. $(a) \Rightarrow (f)$ by Corollary (3.3.7) and Theorem (4.4) of [41], $(f) \Rightarrow (e)$ by Exercise $4G$ of [41], $(e) \Rightarrow (c)$ by Theorem (3.6.2), and $(c) \Rightarrow (a)$ is clear. By symmetry, (b), (d), and (f) are also equivalent. □

Because of the symmetry in Corollary (3.3.8), the rings characterized there are referred to as *simple Artinian rings*.

3.3.9 Theorem:

If R is a nonzero right or left Artinian ring, then all prime ideals in R are maximal.

Proof. If R contains a non maximal prime ideal P, then R/P is a prime right or left Artinian ring which is not simple, contradicting Corollary (3.3.8). □

3.3.10 Theorem:

If R is a commutative Noetherian ring, then R is Artinian if and only if all prime ideals in R are maximal.

Proof. Assume that all prime ideals in R are maximal. By Theorem (3.4) of [41] there are (minimal) prime ideals $P_1...P_n$ in R such that $P_1P_2...P_n = 0$. If $I_0 = R$ and $I_j = P_1P_2...P_j$ for $j = 1, ..., n$, then each of the factors I_{j-1}/I_j is finitely generated module over R/P_j. Moreover, since P_j is maximal, R/P_j is a field and hence Artinian. It follows from Corollary (3.1.14) that each I_{j-1}/I_j is Artinian, and we then conclude from Proposition (3.1.12) that R is Artinian. □

3.4 Noetherian Rings

3.4.1 Definition:

A ring R is called (left) Noetherian if it is Noetherian as a left module over itself, i.e., ACC or maximal condition holds for left ideals or every left ideal is finitely generated.

3.4.2 Examples:

Fields, division rings, finite rings, principal ideal rings, etc., are all Noetherian. In particular, the ring of integers $\mathbb{Z}$ is Noetherian.

3.4.3 Proposition:

A quotient ring of a Noetherian ring is Noetherian (whereas a subring need not be Noetherian).

Proof. If I is a 2-sided ideal of a Noetherian ring R, then R/I is Noetherian as an R-module. But the family of all left ideals of R/I is precisely

the family of all left ideals of R each containing I and hence it follows that R/I is a Noetherian ring, as required. □

3.4.4 Proposition:

A finitely generated module over a Noetherian ring is Noetherian.

Proof. If a module M is generated by n elements, then M is a quotient of the cartesian product R^n which is Noetherian (since R is Noetherian) and hence M is Noetherian, as required. □

3.4.5 Theorem:

In a right or left Noetherian ring R, there exist only finitely many minimal prime ideals, and there is a finite product of minimal prime ideals (repetitions allowed) that equals zero.

Note. The following proof does not require the full force of the right or left Noetherian hypothesis, but only ACC on two-sided ideals.

Proof. It suffices to prove that there exist prime ideals $P_1, ..., P_n$ in R such that $P_1P_2...P_n = 0$. To see this, note that after replacing each P_i by a minimal prime ideal contained in it, we may assume that each P_i is minimal. Since any minimal prime P contains $P_1P_2...P_n$, it must contain some P_j, whence $P = P_j$ by minimality. Thus the minimal prime ideals of R are contained in the finite set $\{P_1, ..., P_n\}$.

Suppose that no finite product of prime ideals in R is zero. Let $\mathcal{K}$ be the set of those ideals K in R that do not contain a finite product of prime ideals. Since $\mathcal{K}$ contain 0, it is nonempty. By the Noetherian hypothesis (not Zorn's Lemma!), there exists a maximal element $K \in \mathcal{K}$.

As R/K is a counterexample to the theorem, we may replace R by R/K. Thus we may assume, without loss of generality, that no finite product of prime ideals in R is zero, while all nonzero ideals of R contain finite products of prime ideals.

In particular, 0 cannot be a prime ideal. Hence, there exist nonzero ideals $I,\ J \in R$ such that $IJ = 0$. Then there exist prime ideals $P_1, ..., P_m,\ Q_1, ..., Q_n$ in R with $P_1P_2...P_m \subseteq I$ and $Q_1Q_2...Q_n \subseteq J$.

But then

$$P_1P_2...P_mQ_1Q_2...Q_n = 0,$$

contradicting our supposition.

Therefore some finite product of prime ideals in R is zero. □

3.4.6 Corollary:

Let S be a subring of a ring R. If S is right Noetherian and R is finitely generated as a right S-module, then R is right Noetherian.

Proof. By Corollary (3.1.23), R is Noetherian as a right S-module. Since all right ideals of R are also right S-submodules, the ACC on right ideals follows. □

Using Corollary (3.4.6), we obtain some easy examples of noncommutative Noetherian rings.

3.4.7 Proposition:

If R is a module-finite algebra over a commutative Noetherian ring S, then R is a Noetherian ring.

Proof. The image of S in R is a Noetherian subring S' of the center of R such that R is a finitely generated (right or left) S'-module. Apply Corollary (3.4.6). □

For instance, let $S = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$, a subring of the division ring $\mathbb{H}$. Since S is a finitely generated module over the Noetherian ring $\mathbb{Z}$, Proposition (3.4.7) shows that S is a Noetherian ring. For another example, Proposition (3.4.7) shows that, for any positive integer n, the ring of all $n \times n$ matrices over a commutative Noetherian ring is Noetherian. This also holds for matrix rings, as follows.

3.4.8 Corollary:

Matrix rings over Noetherian rings with unity, (in particular, over division rings), are Noetherian.

Proof. Let R be Noetherian and $S = M_n(R)$ be a matrix ring over R. It is clear that any left ideal of S is also an R-submodule of S. But S is Noetherian as an R-module since it is finitely generated over R, (in

fact, it is a free R-module with a basis having n^2 elements). Hence S is a Noetherian ring, as required. □

3.4.9 Theorem (Hilbert Basis theorem):

[Theorem (1.9) of [41]]. Let $S = R[x]$ be a polynomial ring in one indeterminate. If the coefficient ring R is right (left) Noetherian, then so is S.

Proof. The two cases are symmetric; let us assume that R is right Noetherian and prove that any right ideal I of S is finitely generated. We need only consider the case when $I \neq 0$.

Step 1. Let J be the set of leading coefficients of elements of I, together with 0. More precisely,

$$J = \{r \in R \mid rx^d + r_{d-1}x^{d-1} + ... + r_0 \in I \text{ for some } r_{d-1}.....r_0 \in R\}.$$

Then check that J is a right ideal of R. (Note that if $r, r' \in J$ are leading coefficients of elements s, $s' \in I$ with degrees d, d', then, after replacing s and s' by $sx^{d'}$ and $s'x^d$, we may assume that s and s' have the same degree.)

Step 2. Since R is right Noetherian, J is finitely generated. Let $r_1.....r_k$ be a finite list of generators for J; we may assume that they are all nonzero. Each r_i occurs as the leading coefficient of a polynomial $p_i \in I$ of some degree n_i. Set $n = max\{n_1, ..., n_k\}$ and replace each p_i by $p_i x^{n-n_i}$. Thus, there is no loss of generality in assuming that all the p_i have the same degree n.

Step 3. Set

$$N = R + Rx + ... + Rx^{n-1} = R + xR + ... + x^{n-1}R,$$

the set of elements of S with degree less than n. This is not an ideal of S, but it is a left and right R-submodule. Viewed as a right R-module, N is finitely generated, and so it is Noetherian by Corollary (3.1.23). Now $I \cap N$ is a right R-submodule of N, and consequently it must be finitely generated. Let $q_1.....q_t$ be a finite list of right R-module generators for $I \cap N$.

Step 4. We claim that $p_1, ..., p_k, q_1, ..., q_t$ generate I. Let I_0 denote the right ideal of S generated by these polynomials; then $I_0 \subseteq I$ and

it remains to show that any polynomial $p \in I$ actually lies in I_0. This is easy if p has degree less than n, since in that case $p \in I \cap N$ and $p = q_1a_1 + ... + q_ta_t$ for some $a_j \in R$.

Step 5. Suppose that $p \in I$ has degree $m \geq n$ and that I_0 contains all elements of I with degree less than m. Let r be the leading coefficient of p. Then $r \in J$, and so $r = r_1a_1 + ... + r_ka_k$ for some $a_i \in R$. Set $q = (p_1a_1 + ... + p_ka_k)x^{m-n}$, an element of I_0 with degree less than m. Now $p - q$ is an element of I with degree less m. By the induction hypothesis, $p - q \in I_0$, and $p \in I_0$.
Therefore $I = I_0$ ad we are done. □

It immediately follows that any polynomial ring $R[x_1, ..., x_n]$ in a finite number of indeterminates over a right(left) Noetherian ring R is right (left) Noetherian, since we may view $R[x_1, ..., x_n]$ as a polynomial ring in the single indeterminate x_n with coefficients from the ring $R[x_1, \cdots, x_{n-1}]$.

3.4.10 Corollary:

Let R be an algebra over a field k. If R is commutative and finitely generated as a k-algebra, then R is Noetherian.

Proof. Let $x_1, ..., x_n$ generate R as a k-algebra, and let

$$S = k[y_1, ..., y_n]$$

be a polynomial ring over k in n independent indeterminates. Since R is commutative, there exists a k-algebra map $\phi : S \to R$ such that $\phi(y_i) = x_i$ for each i, and ϕ is surjective because the x_i generate R. Hence,

$$R \cong \frac{S}{ker(\phi)}.$$

By the Hilbert Basis Theorem, S is a Noetherian ring, and therefore R is Noetherian. □

3.4.11 Theorem:

Let V be a vector space over a division ring D and $R = End_D(V)$ be the ring of D-linear endomorphism of V. Then the following are equivalent:

(1) R is Artinian.

(2) V is finite dimensional over D.

(3) R is Noetherian.

Proof. (1) $\Leftrightarrow$ (2): Let R be Artinian. Suppose V is not finite dimensional over D. Pick up any countably infinite linearly independent subset $\{v_1, v_2, ...v_n, ..., ...\}$ of V. For each $i \in \mathbb{N}$, let V_i be the subspace spanned by first i vectors $v_1, v_2, ..., v_i$. We get an infinitely ascending chain of subspaces of V, namely,

$$V_1 \subset V_2 \subset ... \subset V_n \subset ... \subset ...$$

This gives an infinitely descending chain of left ideals of R, namely,

$$I_1 \supset I_2 \supset ... \supset I_n \supset ... \supset ...$$

Where $I_i = \{f \in R \mid f(V_i) = 0, i \in \mathbb{N}\}$ contradicting (1). Hence V is finite dimensional. Conversely, if V is finite dimensional, then $R \approx M_r(D)$ where $r = dim_D(V)$ and so R is Artinian by (3.3.5) above.

(2) $\Leftrightarrow$ (3): If V is finite dimensional, then $R = M_r(D)$ which is Noetherian by (3.4.8) above. Conversely, suppose R is Noetherian and assume, if possible, V is not finite dimensional. As before choose any countably infinite linearly independent subset $\{w_1, w_2, ..., w_n, ..., ...\}$ of V. For each $i \in \mathbb{N}$, let W_i be the subspace spanned by omitting the first $i - 1$ vectors. We get an infinitely descending chain of subspaces of V, namely,

$$W_1 \supset W_2 \supset ... \supset W_n \supset ... \supset ...$$

This gives an infinitely ascending chain of left ideals of R, namely,

$$J_1 \subset J_2 \subset ... \subset J_n \subset ... \subset ...$$

Where $J_i = \{f \in R \mid f(W_i) = 0, i \in \mathbb{N}\}$ contradicting (3). Hence V is finite dimensional, as required. □

3.4.12 Corollary:

The ring $R = End_D(V)$ is a module of finite length as an R-module if and only if V is finite dimensional over D.

Proof. Immediate from (3.4.11) and (3.2.5) above.

□

3.4.13 Remark:

If $dim_D(V) = r$, then $R = End_D(V)$ is a module of finite length as a module over D as well as over itself. Its lengths are given by $l_R R = r$ whereas $l_D(R) = r^2$. The second follows simply because $dim_D(R) = dim_D(M_r(D)) = r^2$. The first follows because R has a composition series, namely, $R = R_0 \supset R_1 \supset ... \supset R_r = (0)$ where R_i is the left ideal consisting of all matrices whose first i columns are zero, $0 \leq i \leq r$.

In the rest of this section, R stands for a commutative ring with 1*, integral domain or not.*

3.4.14 Theorem (Cohen):

[Theorem (6.5.11) of [71]]. Let R be as above. Then R is Noetherian if and only if every prime ideal of R is finitely generated.

Proof. The implication " $\Rightarrow$ " is obvious since every ideal is finitely generated. The converse is the interesting part.

Suppose every prime ideal of R is finitely generated. Let $\mathcal{F}$ be the family of all ideals of R which are not finitely generated. we want to show that $\mathcal{F} = \phi$. Assume otherwise and apply Zorn's lemma to $\mathcal{F}$. If $\mathcal{T}$ is a chain in $\mathcal{F}$ and $T_0 = \cup_{T \in \mathcal{T}} T$, then T_0 is clearly an ideal of R and T_0 cannot be finitely generated (otherwise, it would follow that $T_0 = T' \in \mathcal{T} \subseteq \mathcal{F}$ implying that $\mathcal{F}$ contains a finitely generated ideal T_0 which cannot be). Thus $T_0 \in \mathcal{F}$ is an upper bound for $\mathcal{T}$ and hence $\mathcal{F}$ has a maximal element, say J. Since J is not finitely generated, J cannot be a prime ideal. Hence there exists $x, y \in R$ such that $x \notin J$ and $y \notin J$ but $xy \in J$.

Now the ideal $J + yR \supset J$, $J + yR \neq J$ and so $J + yR$ is not a member of $\mathcal{F}$ which means that $J + yR$ is finitely generated, say $J + yR = (y_1, y_2, ..., y_r)$. Each y_i can be written as $y_i = a_i + \alpha_i y$ for some $a_i \in J$ and $\alpha_i \in R$, $1 \leq i \leq r$. On the other hand, look at the ideal of R which contains J and the element x, namely,

$$J : yR = \{z \in R \mid zy \in J\}$$

This again is not a member of $\mathcal{F}$ and so finitely generated, say $J : yR = (x_1, x_2, ..., x_s)$. By definition, we have $b_j = x_j y \in J$, $1 \leq j \leq s$. It is an easy exercise to see now that J is finitely generated, in fact, we have

$$J = (a_1, a_2, ..., a_r; b_1 b_2, ..., b_s)$$

contradicting the fact that J is not finitely generated and so $\mathcal{F} = \phi$, as required. □

3.4.15 Theorem:

The ring R of Complex entire functions is neither Artinian nor Noetherian.

Proof. R is not Artinian because it is a commutative integral domain which is not a field. That R is not Noetherian follows because it is not even a factorization domain. However, we shall now give a direct argument (from first principles) as follows.

Consider the discrete subset $\mathbb{N}$ of $\mathbb{C}$ which is without limit points. For each $r \in \mathbb{N}$, let I_r be the set of all entire functions vanishing at the integral points $m \in \mathbb{N}$, for all $m \geq r$, i.e.,

$$I_r = \{f \in R \mid f(r) = f(r+1) = ... = 0\}$$

Thus we get an ascending chain of ideals of R, namely

$$I_1 \subset I_2 \subset ... \subset I_n \subset ... \subset ...$$

This chain is infinitely strictly ascending because of the following well known theorem.

Theorem (Weierstrass): For each positive integer r, there exists a Complex entire function $f(z)$ such that $f(r) \neq 0$ but $f(r+1) = f(r+2) = ... = 0$, i.e., $f(z) \in I_{r+1}$ but $f(z) \notin I_r$.

This is a very special case (for $D = \mathbb{N}$) of a much stronger theorem of Weierstrass which gives the existence of Complex entire functions with prescribed zeros (each of specified order) at any discrete set D without limit points. □

3.4.16 Theorem:

In a commutative Noetherian ring, every ideal contains a product of prime ideals.

Proof. Let $\mathcal{F}$ be the set of all ideals I in R such that I does not contain any product of prime ideals. If $\mathcal{F} \neq \phi$, it has a maximal element, say A. This A cannot be prime ideal itself and hence there exist $x, y \in R$ such that $xy \in A$ with $x, y \notin A$. Now let $I = A + Rx$ and $J = A + Ry$ so that $A \subseteq I \cap J$ and $A \neq I$ and $A \neq J$. Hence by maximality of A in $\mathcal{F}$, we get that $I, J \notin \mathcal{F}$,i.e., both I and J contain some products of prime ideals. But then it follows that IJ contains a product of prime ideals and so does A because $xy \in A$ and so we have $IJ = (A+Rx)(A+Ry) \subseteq A+Rxy = A$. This contradiction proves that $\mathcal{F} = \phi$, as required. □

3.4.17 Corollary:

In a commutative Noetherian ring the ideal (0) is a product of prime ideals, say

$$(0) = P_1^{\varepsilon_1}.P_2^{\varepsilon_2}...P_n^{\varepsilon_n} \tag{3.3}$$

with P_i distinct prime ideals and $\varepsilon_i \in \mathbb{N}$. Consequently, the set of minimal prime ideals of R is finite (it being the set of minimal elements in $\{P_1, ..., P_n\}$). This follows at once since any prime ideal contains the product in 3.3 and hence contain one of the $P_i's$.

3.5 Radicals

3.5.1 Radical ideal:

A two-sided ideal I in a ring R with 1 is called a radical ideal with respect to a specified property $\mathcal{P}$ if

(1) the ideal I posses the property $\mathcal{P}$ and

(2) the ideal I is maximal for the property $\mathcal{P}$, i.e., if J is a 2-sided ideal of R having the property $\mathcal{P}$, then $J \subseteq I$.

There are several kinds of radicals defined and studied in a ring in various contexts. Notable among them are two radicals called *nil radical* and the *Jacobson radical*. There are other like the *Amitsur radical*, the Brown-McCoy radical, the Levitzki radical, etc. We shall introduce the first two of these radicals and prove some basic properties thereof.

3.5.2 Nil Radical

Definition. The nil radical of a ring R is defined to be the radical ideal with respect to the property that "A 2-sided ideal is nil" and is denoted

by $N(R)$, i.e., $N(R)$ is the largest 2-sided ideal of R such that every element of $N(R)$ is nilpotent.

3.5.3 Examples:

(1) If R has no non-trivial nilpotent elements, in particular, R an integral domain, then $N(R) = (0)$.

(2) If R is commutative, then the set $N(R)$ of all nilpotent elements of R which is an ideal, is the nil radical of R. (If R has 1, then $N(R)$ is the intersection of all prime ideals of R.)

(3) If R is a nil ring, i.e., every element of R is nilpotent, then $N(R) = R$. For instance, $R = 2\mathbb{Z}/4\mathbb{Z}$ or $R =$ strictly upper triangular matrices over any ring.

(4) $N(M_r(D)) = (0)$ for any division ring D because $R = M_r(D)$ is not a nil ring and it has no 2-sided ideals other than (0) and R. (Note that R has nilpotent elements if $r \leq 2$ but they do not form an ideal.)

3.5.4 Theorem:

For any ring R, the nil radical $N(R)$ exists and it is characterized by $N(R) = \{a \in R \mid$ the principal 2-sided ideal (a) is a nil ideal$\}$.

Proof. We have to first prove that $N = N(R)$ as above is a 2-sided ideal and secondly that it is the largest for that property.

(1) Since $0 \in N$, $N \neq \phi$. If $a \in N$ and $x \in R$, then (xa) and (ax) and so both (xa) and (ax) are nil ideals hence ax,$xa \in N$. Thus we have only to prove the following.

(2) *N is an additive subgroup of R.*
To see this, for $a, b \in N$, we have to show that $(a-b)$ is a nil ideal. Since $(a-b) \subseteq (a) + (b)$, every element $x \in (a-b)$ can be written as $x = y + z$ for some $y \in (a)$ and $z \in (b)$. Since (a) and (b) are nil ideals, both y and z are nilpotent, say $y^n = 0$ and $z^n = 0$ for some $n \gg 0$. Now look at $x^n = (y+z)^n = y^n + z' = 0 + z'$ where z' is a sum of monomials in y and z in each of which z is a factor, i.e., $z' \in (z) \subseteq (b)$ and so z' is nilpotent and hence x is nilpotent, i.e.,

$(a-b)$ is a nil ideal, as required.

Finally, let I be any 2-sided nil ideal of R. Then trivially, $(a) \subseteq I$, for all $a \in I$ and hence (a) is a nil ideal, i.e., $I \subseteq N$, as required.

□

3.5.5 Corollary:

We have $N(R/N(R)) = (0)$ for any ring R.

Proof. Let $\overline{a} = a+N \in N(R/N)$ where $N = N(R)$ and $a \in R$. Then the 2-sided principal ideal $\overline{a}$ is a nil ideal in R/N, i.e., the 2-sided ideal (a) in R is nil modulo N. Hence it follows that (a) is a nil ideal in R (since N is a nil ideal), i.e., $a \in N$ and so $\overline{a} = o$, i.e., $a \in N$, as required. □

3.5.6 Jacobson Radical

Definition. The Jacobson radical of ring R with 1 is defined as the radical ideal of R with respect to the property that *"A 2-sided ideal I is such that $1-a$ is a unit in R for all $a \in I$"* and it is denoted by $J(R)$. In other words, $J(R)$ is the largest 2-sided ideal of R such that $1-a$ is a unit for all $a \in J(R)$.

3.5.7 Examples:

(1) $J(\mathbb{Z}) = (0)$.

(2) $J(M_r(D)) = (0)$, for all $r \in \mathbb{N}$ and D a division ring (since $M_r(D)$ has no 2-sided ideals other than (0) and $M_r(D$ and the latter cannot be a candidate).

(3) If R is a commutative local ring with its unique maximal ideal M, then obviously $J(R) = M$.

To prove the existence of the Jacobson radical, first we define the so called left and right Jacobson radicals, $J_l(R)$ and $J_r(R)$ and show them to be equal. Secondly, we show that $J_l(R) = J_r(R) = J(R)$ is the one we are looking for.

3.5.8 Examples:

For any ring R with 1, the intersection of all maximal left ideals of R is called the left Jacobson radical or simply the left radical of R and is denoted by $J_l(R)$.

In case R is commutative, $J_l(R)$ is the intersection of all maximal ideals of R.

3.5.9 Examples:

(1) The left radical of a division ring is (0). More generally, the left radical of $M_n(D)$ is (0) for all $n \in \mathbb{N}$ where D is a division ring.

(2) The (left) radical of $\mathbb{Z}$ is (0).

(3) The (left) radical of a local ring is its unique maximal ideal.

(4) The (left) radical of $\mathbb{Z}/n\mathbb{Z}$ is $m\mathbb{Z}/n\mathbb{Z}$ where m is the product of all distinct prime divisors of n. For instance, $J_l(\mathbb{Z}/36\mathbb{Z}) = (6\mathbb{Z}/36\mathbb{Z}), J_l(\mathbb{Z}/64\mathbb{Z}) = (2\mathbb{Z}/64\mathbb{Z})$ and $J_l(\mathbb{Z}/180\mathbb{Z}) = (30\mathbb{Z}/180\mathbb{Z})$.

3.5.10 Primitive ideals:

An ideal P in a ring is right (left) primitive provided $P = ann_R(A)$ for some simple right (left) R-module A. A right (left) *primitive ring* is any ring in which 0 is a right (left) primitive ideal, i.e., any ring which has a faithful simple right (left) module.

3.5.11 Theorem (Noether):

For any ring R, the following conditions are equivalent:

(a) All right R-modules are semisimple.

(b) All left R-modules are semisimple.

(c) R_R is semisimple.

(d) ${}_RR$ is semisimple.

(e) Either R is zero ring or $R \cong M_{n_1}(D_1) \times ... \times M_{n_k}(D_k)$ for some positive integers n_i and some division rings D_i.

Proof. See Theorem (4.4) of [41] □

3.5.12 Semi-simple ring:

A ring satisfying the conditions of Theorem (3.5.11) is called a semi-simple ring.

3.5.13 Local ring:

In ring theory, local rings are certain rings that are comparatively simple, and serve to describe what is called "local behaviour", in the sense of functions defined on varieties or manifolds, or of algebraic number fields examined at a particular place, or prime. Local algebra is the branch of commutative algebra that studies local rings and their modules.

In practice, a commutative local ring often arises as the result of the localization of a ring at a prime ideal.

For instance, all fields (and skew fields) are local rings, since 0 is the only maximal ideal in these rings.

3.5.14 Theorem:

For any ring R, its left radical $J_l(R)$ is the intersection of the annihilators of all simple left modules over R. In particular, $J_l(R)$ is a 2-sided ideal of R.

Proof. **(1).** If m is a maximal left ideal of R, then m is the annihilator of the non-zero element $\overline{1} = 1 + m$ in the simple R-module $S = R/m$.

(2). If S is a left simple R-module and $x \in S$ is a non-zero element, then $S = Rx$ and the natural map $f_x : R \to S$, defined by $f_x(a) = ax$ is an epimorphism whose kernel is the annihilator of the element x. Thus we have

$$\frac{R}{Ker(f_x)} \approx Rx = S$$

which is simple and hence $M_x = Ker(f_x)$ is a maximal left ideal of R. This shows that the annihilator of any non-zero element of a simple module is a maximal left ideal of R. In other words, the family of all maximal left ideals of R is the same as that of the annihilators of non-zero elements of all simple left modules over R.

(3). The annihilator of any left module M is a 2-sided ideal of R and it is the intersection of the annihilators of all elements of M.

(4). If $\mathcal{M}$ is the set of all maximal left ideals of R and $\mathcal{L}$ is the family of all simple left modules over R, then we have $J_l(R) = \cap_{M\in\mathcal{M}} M$ which in turn can be written as

$$J_l(R) = \cap_{S\in\mathcal{L}}(\cap_{x\in\mathcal{S}} M_x) = \cap_{S\in\mathcal{L}} Ann_R(S)$$

(where M_x is the annihilator of the element $x \in S$) and so $J_l(R)$ is the intersection of the family $\{Ann_R(S) \mid S \in \mathcal{L}\}$ of 2-sided ideals and hence 2-sided, as required.

□

3.5.15 Proposition:

Given a ring R with its left radical $J_l(R)$, the left radical of the quotient $R/J_l(R)$ is zero, i.e., $J_l(R/J_l(R)) = (0)$.

Proof. Let $\eta : R \to R/J_l(R)$ be the natural homomorphism. Then the assignment $M \mapsto \eta(M)$ is a bijection between the set $\mathcal{M}_R$ of all maximal left ideals of R and that of $R/J_l(R)$ since each $M \in \mathcal{M}_R$ contains $J_l(R)$. Hence it follows that

$$J_l(R/J_l(R)) = \cap_{M\in\mathcal{M}_\mathcal{R}} \eta(M).$$

But then we have

$$\cap_{M\in\mathcal{M}_\mathcal{R}} \eta(M) = \eta(\cap_{M\in\mathcal{M}_\mathcal{R}} M) = \eta(J_l(R)) = (0).$$

□

3.5.16 Theorem:

$J_l(R) = \{x \in R \mid 1 - yx$ is a unit, for all $y \in R\}$.

Proof. ($\Rightarrow$:) Let $x \in J_l(R)$. For any $y \in R$, if $1 - yx$ has no left inverse in R, we can find a maximal left ideal M containing $1 - yx$. But then $1 = (1 - yx) + yx$ would be in M since M is a left ideal containing x and $1 - yx$ which is a contradiction. Let $z \in R$ be such that $z(1 - yx) = 1$. If this z has no left inverse, we can find another maximal left ideal M' containing z. But then M' contains z as well as x and hence it contains

$1 = z(1 - yx) = z - zyx$ which is again a contradiction. Thus z is invertible whose inverse is $1 - yx$, i.e., $1 - yx$ is a unit, as required.

($\Leftarrow$:) Let $x \in R$ be such that $1 - yx$ is a unit for all $y \in R$. If $X \notin J_l(R)$, then $x \notin M$ for some $M \in \mathcal{M}$. But then we get that $M + Rx = R$ and so we can write that $z = 1 - ax$ for some $z \in M$ and $a \in R$ which means that $z = 1 - ax$ is invertible and is an element of the maximal left ideal M, a contradiction. Hence $x \in J_l(R)$. □

3.5.17 Theorem:

$J_l(R)$ is the largest left ideal of R such that $1 - a$ is a unit for every $a \in J_l(R)$.

Proof. By the theorem above, it is obvious that $1 - x$ is a unit for all $x \in J_L(R)$. Let now I be a left ideal of R such that $1 - a$ is a unit for every $a \in I$. Let $x \in I$ and $y \in R$ then $yx \in I$ since I is a left ideal of R. But then by assumption $1 - yx$ is a unit (no matter what y is) and so $x \in J_l(R)$, i.e., $I \subseteq J_l(R)$, as required. □

3.5.18 Right Jacobson radical:

For any ring R with 1, the intersection of all maximal right ideals of R is called the right Jacobson radical or simply the right radical of R and is denoted by $J_r(R)$.

3.5.19 Remarks:

Proceeding as above, we can prove that $J_r(R)$ has the following properties.

(1) $J_r(R)$ is a 2-sided ideal of R.

(2) $J_r(R) = \{x \in R \mid 1 - xy$ a unit, for all $y \in R\}$

(3) $J_r(R)$ is the largest right ideal of R such that $1 - b$ is a unit for all $b \in J_r(R)$.

3.5.20 Theorem:

For any ring R, the left and right Jacobson radicals coincide ant the 2-sided ideal $J(R) = J_l(R) = J_r(R)$ is the Jacobson radical of R. In

particular, the Jacobson radical of a local ring is its (unique) maximal ideal.

Proof. We have $J_r(R) \subseteq J_l(R)$ since $J_r(R)$ (being 2-sided) is also a left ideal such that $1-a$ is a unit for all $a \in J_r(R)$. Similarly, $J_l(R) \subseteq J_r(R)$, as required. □

3.5.21 Theorem:

For any ring R, $N(R) \subseteq J(R)$ and equality need not hold.

Proof. Let $a \in N(R)$. Since $N(R)$ is a nil ideal, a is nilpotent, say $a^n = 0$ for some $n \in \mathbb{N}$. Now we have

$$1 = 1 - a^n = (1-a)(1 + a + a^2 + ... + a^{n-1})$$

implying that $1 - a$ is a unit in R and so $a \in J(R)$, as required. □

3.5.22 Note:

For the local ring $\mathbb{Q}^p = \{a/b \in \mathbb{Q}, (p, b) = 1\}$ where p is a fixed prime number, we have $N(\mathbb{Q}^p) = (0)$ whereas $J(\mathbb{Q}^p) = (p) \neq (0)$.

3.5.23 Lemma (Nakayama):

[Lemma (6.6j.13) of [71]]. If M is a finitely generated module over a ring R such that $J(R)M = M$, then $M = (0)$. (Recall [71] (2.5.3)that for any subset A of R, the set AM stands for the submodule of M generated by elements of the form ax for all $a \in A$ and $x \in M$).

Proof. Suppose M is generated by $X = \{x_1, x_2, ..., x_r\}$, a finite subset of M. We may assume that X is a minimal set of generators in the sense that no proper subset of X generates M. Since $J = J(R)$ is a right ideal of R, we find that JM is the submodule of M generated by

$$\{ax_i \mid \text{for all } a \in J,\ 1 \leq i \leq r\}.$$

Since $x_i \in M = JM$ and J is a left ideal, we can write

$$x_1 = \Sigma_{i=1}^{r} a_i x_i$$

for some $a_i \in J$, $1 \leq i \leq r$. This gives

$$(1 - a_1)x_1 = \Sigma_{i=2}^{r} a_i x_i.$$

Since $a_1 \in J$, $(1 - a_1)$ is a unit in R and so by multiplying on the left with $b_1 = (1 - a_1)^{-1}$, we get $x_1 = \Sigma_{i=2}^{r} b_1 a_i x_i$ which means that x_1 is an R-linear combination of the $x_1's$, $2 \leq i \leq r$, i.e., the proper subset $X' = \{x_i,\, 2 \leq i \leq r\}$ of X generates M, a contradiction and so $X = \phi$, i.e., $M = (0)$. □

3.5.24 Remark:

The assumption that M is finitely generated is necessary in the Nakayama lemma. For instance, we have

$$J(\mathbb{Q}^p)\mathbb{Q} = (p)\mathbb{Q} = \mathbb{Q} \text{ but } \mathbb{Q} \neq (0)$$

because $\mathbb{Q}$ is not finitely generated over $\mathbb{Q}^p$. (see [71] (5.9.7)).

3.6 Radical of an Artinian Ring

3.6.1 Proposition:

The Jacobson radical of an Artinian ring is the intersection of some finitely many maximal left (resp. right) ideals.

Proof. Let R be an Artinian ring. Let $\mathcal{M}$ be the set of all maximal left ideals of R. Let $\mathcal{F}$ be the family of all left ideals of R each of which is an intersection of finitely many maximal left ideals of R. Obviously this family is non-empty since $\mathcal{M} \subseteq \mathcal{F}$. Since R is Artinian, $\mathcal{F}$ has a minimal member, say

$$J_0 = \textstyle\bigcap_{i=1}^{n} M_i,\ M_i \in \mathcal{M}.$$

We have $J \subseteq J_0$ where $J = J(R)$. On the other hand, if $M \in \mathcal{M}$, then $J_0 \cap M$ being a member of $\mathcal{F}$ must be equal to J_0 by the minimality of J_0 which means that $J_0 \subseteq M$, for all $M \in \mathcal{M}$. Thus we get that

$$J \subseteq J_0 \subseteq \textstyle\bigcap_{M \in \mathcal{M}} M = J$$

and hence $J = J_0$, as required. □

3.6.2 Theorem (Weddeburn, Artin):

[Theorem (4.13) of [41]]. For a ring R, the following conditions are equivalent:

(a) R is right Artinian and $J(R) = 0$.

(b) R is left Artinian and $J(R) = 0$.

(c) R is semisimple.

Proof. $(a) \Rightarrow (c)$: Let $\mathcal{B}$ be the set of those right ideals I of R such that R/I is a semisimple module and note that $\mathcal{B}$ is nonempty (e.g., $R \in \mathcal{B}$). Since R is right Artinian, we may choose a right ideal K minimal in $\mathcal{B}$. If $K \neq 0$, then, since $J(R) = 0$, there is a maximal right ideal M in R such that $K \nleq M$. Since M is maximal, $K + M = R$, and hence

$$\tfrac{R}{K \cap M} \cong \tfrac{R}{K} \oplus \tfrac{R}{M}$$

But then $R/(K \cap M)$ is semiprime, and since $(K \cap M) < K$, this contradicts the minimality of K. Therefore $K = 0$, and so R_R is semisimple.

$(c) \Rightarrow (a)$: Write $R_R = S_1 \oplus ... \oplus S_n$, where each S_i is a simple right R-module. (The direct sum must be finite because R_R is finitely generated.) Corollary (4.6) of [41] shows that R is right Artinian (since each S_i is clearly Artinian). Each of the annihilators $r.Ann_R(S_i)$ is a right primitive ideal of R and so contains $J(R)$. Thus $S_i J(R) = 0$ for each i, and consequently $J(R) = 0$.

$(b) \Leftrightarrow (c)$: By symmetry. □

3.6.3 Definition:

The *socle series of a module* A is the ascending chain

$$soc^0(A) \leq soc^1(A) \leq soc^2(A) \leq ...$$

of submodules of A defined inductively by setting $soc^0(A) = 0$ and

$$soc^{n+1}(A)/soc^n(A) = soc(A/soc^n(A))$$

for all nonnegative integers n.

For example, if $A = \mathbb{Z}/p^k\mathbb{Z}$ for some prime integer p and some positive integer k, then

$$soc^n(A) = p^{k-n}\mathbb{Z}/p^k\mathbb{Z}$$

for $n = 0, 1, ..., k$ and $soc^n(A) = A$ for all $n \geq k$.

3.6.4 Theorem (Hopkins, Levitzk):

[Theorem (4.15) of [41]]. If R is a right Artinian ring, then R is also right Noetherian, and $J(R)$ is nilpotent.

Proof. Set $J = J(R)$. Since the powers of J form a descending chain of ideals, there must exist a positive integer n such that $J^{n+1} = J^n$. In view of Proposition (4.14) [41], it follows that $soc^{n+1}(R_R) = soc^n(R_R)$. Hence, if $I = soc^n(R_R)$, then $soc((R/I)_R) = 0$.

If $I \neq R$, then R/I has a minimal nonzero right submodule M. But then M is a simple right submodule of R/I, contradicting the fact that $soc((R/I)_R) = 0$. Thus $I = R$. Hence, by Proposition (4.14) of [41], $I.Ann_R(J^n) = soc^n(R_R) = R$, and so $J^n = 0$. Therefore J is nilpotent.

Set $A_i = soc^i(R_R)$ for $i = 0, 1, ..., n$. These A_i form a chain

$$A_0 = 0 \leq A_1 \leq ... \leq A_n = R$$

of right ideals of R. Each of the factors A_i/A_{i-1} is a semisimple right R-module and so is a direct sum of simple modules, by Proposition (4.1) [41].

Suppose that one of the factors A_i/A_{i-1} is a direct sum of an infinite family $\mathcal{B}$ of simple modules. Choose distinct $B_1, B_2, ...$ in $\mathcal{B}$ and for $k = 1, 2, ...$ let $C_k = \oplus_{j=k}^{\infty} B_j$. Then $C_1 > C_2 > ...$ is strictly descending chain of submodules of A_i/A_{i-1}, whence A_i/A_{i-1} is not Artinian. As R_R is Artinian, this is impossible.

Thus A_i/A_{i-1} is a finite direct sum of simple right R-modules. As simple modules are Noetherian. Corollary (3.1.22) shows that A_i/A_{i-1} is Noetherian. Using Proposition (3.1.21), we consider that each A_i is Noetherian. Therefore, since $R_R = A_n$, the ring R is right Noetherian. □

3.6.5 Corollary:

For a right or left Artinian ring, the Jacobson radical equals the prime radical.

Proof. Since every primitive ideal is prime, the intersection of the primitive ideals contains the intersection of the prime ideals, so that the

Jacobson radical contains the prime radical in any ring. Conversely, Theorem (3.6.4) shows that the Jacobson radical of a right or let Artinian ring is nilpotent, and it is thus contained in the prime radical by Corollary (3.9) [41]. □

3.6.6 Theorem:

The Jacobson radical of an Artinian ring R is nilpotent. In fact, $J(R)$ is the largest nilpotent (left or right or 2-sided) ideal of R and consequently, $N(R) = J(R)$.

Proof. Sice R is Artinian, the descending chain of ideals

$$J \supseteq J^2 \supseteq ... \supseteq J^n \supseteq ... \supseteq$$

is stationary where $J = J(R)$. Say, $J^m = J^{m+1} = ... =$ for some $m \gg 0$. Write $I = J^m$. Now we have $I = I^2$ and $JI = I$. (If we know that I is finitely generated then Nakayama lemma would have implied that $I = (0)$ which is what we are looking for. But there seems no way to ensure this crucial fact.) The following is an elementary but a subtle argument to achieve the goal.

Assume, if possible, that $I \neq (0)$. Consider the family $\mathcal{F}$ of all left ideals K of R such that $IK \neq (0)$. Since $I^2 = I \neq (0)$, $I \in \mathcal{F}$ and so $\mathcal{F} \neq \phi$. Note that $(0) \neq \mathcal{F}$. Since R is Artinian, $\mathcal{F}$ has a minimal member, say K, i.e., K is a left ideal of R such that $IK \neq (0)$ and K is minimal for this property. On the other hand, since $IK \neq (0)$, we can find $a \in I$ and $b \in K$ such that $ab \neq 0$ which implies that $I(Rb) \neq (0)$, i.e., $Rb \in \mathcal{F}$. But $Rb \subseteq K$ and so $Rb = K$ by minimality of K. Thus K is a principal left ideal of R.

Finally, we have $(IJ).Rb = I \cdot Rb = Ib \neq (0)$ and $J.Rb = J.b \subseteq Rb$ and $J.Rb \neq (0)$ which give,(again by minimality of $K = Rb$ in $\mathcal{F}$), that $J.Rb = Rb$. Now Nakayama lemma gives that $K = Rb = (0)$, a contradiction to the assumption that $I \neq (0)$. Hence $I = J^n = (0)$. □

3.6.7 Corollary:

In an Artinian ring, every nil ideal is nilpotent (since such an ideal is contained in the radical which is nilpotent).

3.6.8 Theorem:

There are only finitely many maximal ideals in a commutative Artinain ring, i.e., it is a semi-local ring.

Proof. Let R be Artinian. We know by Proposition (3.6.1) above, that $J = J(R)$ is an intersection of finitely many maximal ideals, say

$$J = \bigcap_{i=1}^{n} M_i \supseteq M_1.M_2...M_n.$$

Claim: *The only maximal ideals of R are the $M_i's$, $1 \leq i \leq n$.*
For, since J is nilpotent, we have $J^r = (0)$ for some $r \in \mathbb{N}$ and

$$(0) = J^r \supseteq (M_1.M_2...M_n)^r = M_1^r.M_2^r...M_n^r.$$

If M is any maximal ideal of R, then $M \supseteq (0) = M_1^r.M_2^r...M_n^r$ and hence $M \supseteq M_i^r$, for some i $(1 \leq i \leq n)$. But then $M \supseteq M_i$ (because M is a prime ideal). Now both being maximal, it follows that $M = M_i$, as required. □

3.6.9 Remark:

We have seen examples of Artinian modules which are not Noetherian and vice-versa and some which are neither. On the other hand, there are Noetherian rings which are not Artinian and some which are neither. However, it is a remarkable fact that

"EVERY ARTINIAN RING IS NOETHERIAN".

We shall first prove this in the commutative case and offer a comment about the other case. We begin with the following easy but crucial step.

3.6.10 Theorem:

Let R be a commutative local ring whose maximal ideal is nilpotent. Then R is Artinian if and only if it is Noetherian.

Proof. Let M be the maximal ideal of R with $M^r = (0)$. Let $K = R/M$ be the residue field of R. It is obvious that R is Artinian (resp. Noetherian) if and only if M is so. Now M is Artinian (resp. Noetherian) if and only if both M/M^2 and M^2 are so, etc. Secondly, since M annihilates M^i/M^{i+1}, it is a vector space over the field K and the R-module

structure is the same as the vector space structure. But then we know that M^i/M^{i+1} is Artinian (resp. Noetherian) if and only if M^i/M^{i+1} is finite dimensional over K.

Suppose R is Artinian (resp. Noetherian). Then M^i/M^{i+1} is Artinian (resp. Noetherian) and hence finite dimensional over K, for all $i = 0, 1, ..., r-1$. Consequently, each is Noetherian (resp. Artinian). Now $M^{r-1} = M^{r-1}/M^r$ and M^{r-2}/M^{r-1} are both Noetherian (resp. Artinian) implies that M^{r-2} is Noetherian (resp. Artinian), etc. proceeding thus we get that M is Noetherian (resp. Artinian). □

3.6.11 Example:

A commutative local ring R whose maximal ideal is nilpotent but R is not Artinian (hence not Noetherian):-
Let K be a field and $R = K[X_i,\ i \in \mathbb{N}]/M^2$ where M is the ideal generated by X_i, $i \in \mathbb{N}$, The maximal ideal of R is of square 0 and is infinite dimensional over its residue field K.

3.6.12 Theorem:

A commutative Artinian ring is Noetherian and conversely a commutative Noetherian ring in which every prime ideal is maximal is Artinian.

Proof. Let R be a commutative Artinian ring. By (3.6.8) above, R is semi-local with its maximal ideals, (say) $M_1...M_n$ and

$$(0) = J^r = M_1^r...M_n^r.$$

Since the maximal ideals M_i are pairwise co-prime, their powers M_i^r are also pairwise co-prime, by (see [71] Exercise (2.9.25)). Consequently, by the Chinese Remainder Theorem, (see [71] Exercise (3.6.6)), we get that

$$R \simeq R/M_1^r \times ... \times R/M_n^r.$$

Since each R/M_i^r is Artinian local ring whose maximal ideal, i.e., M_i/M_i^r is nilpotent, it follows that it is Noetherian (by (3.6.10) above). Thus R is finite direct product of Noetherian rings, as required.

Conversely, suppose R is Noetherian in which every prime ideal is maximal. Then each maximal ideal is also a minimal prime ideal and so it is semi-local (by [71] (6.5.15)). Furthermore, we have

$$(0) = M_1^{\varepsilon_1} ... M_r^{\varepsilon_r}$$

for some maximal ideals M_i and $\varepsilon_i \in \mathbb{N}$, etc. but then it follows that

$$R \simeq R/M_1^{\varepsilon_1} \times ... \times R/M_n^{\varepsilon_r}$$

from where the argument is identical with the above. □

3.6.13 Remark:

The idea of the proof in the non-commutative Artinian case is just the same as above except for a little formalism required from the semi-simple rings (see [71] Exercise (5.10.21)), to prove the crucial facts that both J and R/J are Noetherian (using of course that J is nilpotent).

3.7 Exercises

(1) Let P and Q be submodules of a module M such that both M/P and M/Q are Artinian (resp. Noetherian). Show that $M/(P \cap Q)$ and $M/(P + Q)$ are Artinian (resp. Noetherian).

(2) Let M be a Noetherian R-module with its annihilator ideal $I = r_R(M)$. Show that R/I is a Noetherian ring.

(3) Show that for a Boolean ring R, the following are equivalent.

- R is Artinian.
- R is Noetherian.
- R is a finite Cartesian power of the field of 2 elements.

(4) Let R be a commutative Noetherian local ring with its maximal ideal M. Show that $I = \cap_{i=1}^{\infty} M^i = (0)$.

(5) Show that for any simple R-module S, (R commutative or not), $JS = (0)$.

(6) Let N be a submodule of a finitely generated R-module M such that $M = N + JM$. Then show that $N = M$.

(7) Show that the ring of real valued continuous functions on the closed interval $[0, 1]$ is neither Artinian nor Noetherian.

(8) Suppose that all the coefficients of an element $f(X) \in R[[X]]$ are nilpotent where R is a commutative Noetherian ring. Then show that $f(X)$ is nilpotent.

(9) Show that if a ring R is Noetherian then every homomorphism of R onto itself is $1 - 1$.

(10) Prove that every Artinian ring possesses a finite number of proper prime ideals.

(11) Show that R is Noetherian if and only if $R[[X]]$ is.

(12) Show that the following are equivalent for a semi-simple module M.

- M is finitely generated.
- M is Artinian.

- M is Noetherian.
- M is of finite length.

(13) Let I be a non-zero ideal of Principal Ideal Domain R. Prove that R/I is both Artinian and Noetherian.

(14) Prove that the intersection of all prime ideals in a Noetherian ring is nilpotent.

(15) Let R be a Noetherian ring. Show that the ring of $n \times n$ matrices R_n over R is also Noetherian.

(16) Let R be a left Artinian integral domain with more than one element. Show that R is a division ring.

(17) Show that a left Artinian ring cannot possess an infinite direct sum $\oplus\Sigma A_i$ of left ideals A_i of R.

Chapter

4

SKEW POLYNOMIAL RINGS

Skew polynomial rings in several variables with coefficients in a field K were introduced by Noether and Schmeidler (1920); one of the cases they were particularly interested in was $K[x_i, ..., x_n; \sigma_1, ..., \sigma_n]$, where K consists of $(\mathbb{C}^\infty)$ functions in variables $y_1, ..., y_n$ and each σ_i is the automorphism of K sending y_i to $y_i + 1$ and fixing the other y_j. It is desired, however, that each polynomial should be expressible uniquely in the form $\Sigma x^i a_i$ for some $a_i \in R$. This applies of course, to the elements ax, for any $a \in R$; but, in order that degrees behave appropriately, (i.e. $deg(f(x)g(x)) \leq degf(x) + degg(x)$, it is required that $ax \in xR + R$, $ax = x\sigma(a) + \delta(a)$ say. Under these conditions it is apparent that σ, δ are endomorphisms of the underlying additive group R^+ of R. Moreover,

$$(ab)x = x\sigma(ab) + \delta(ab)$$

and

$$a(bx) = x\sigma(a)\sigma(b) + \delta(a)\sigma(b) + a\delta(b).$$

Thus σ is a ring endomorphism of R and δ satisfies

$$\delta(ab) = \delta(a)\sigma(b) + a\delta(b)$$

which is the defining property of a σ-derivation. Note in particular that $\sigma(1) = 1$ and $\delta(1) = 0$. We continue the study of skew polynomial rings, by first discussing the case where the multiplication is twisted by a derivation, and then developing a general case. Since our main motivation for looking at skew polynomial rings is to be able to construct and work with further important examples of Noetherian rings.

We consider skew polynomial rings which have twists coming from automorphisms and derivations acting together. Also for efficiency's sake, it is good to develop a context in which the two different types of skew

polynomial rings can be treated simultaneously.

Later, Ore produced a systematic investigation of skew polynomial rings in one variable over a division ring (1933); he in particular observer that, in the relation $xr = \sigma(r)x + \delta(r)$, the map σ must be a ring endomorphism and the map δ must be an σ-derivation.

4.1 Endomorphisms and Derivations

A ring R always means an associative ring with identity. $\mathbb{Q}$ denotes the field of rational numbers. $Spec(R)$ denotes the set of prime ideals of R. $MinSpec(R)$ denotes the set of minimal prime ideals of R. $P(R)$ and $N(R)$ denote the prime radical and the set of nilpotent elements of R respectively. Let R be a ring and σ an automorphism of R. Let I be an ideal of R such that $\sigma^m(I) = I$ for some $m \in \mathbb{N}$. We denote $\cap_{i=1}^{m}\sigma^i(I)$ by I^0. For any two ideals I, J of R, $I \subset J$ means that I is strictly contained in J.

4.1.1 Derivation:

Let R be a ring, a map $\delta : R \to R$ is called a δ-derivation if for every a, $b \in R$

(1) $\delta(a + b) = \delta(a) + \delta(b)$

(2) $\delta(a.b) = \delta(a).b + a.\delta(b)$.

4.1.2 Example:

Let $R = F[x]$, where F is a field.
Define $\delta : R \to R$ by
$\delta(f(x)) = \frac{d}{dx}(f(x))$

Therefore, $\delta(f(x) + g(x)) = \frac{d}{dx}(f(x) + g(x))$
$= \frac{d}{dx}f(x) + \frac{d}{dx}g(x)$
$= \delta(f(x)) + \delta(g(x))$

Similarly, $\delta(f(x).g(x)) = \frac{d}{dx}(f(x).g(x))$
$= \frac{d}{dx}f(x).g(x) + f(x).\frac{d}{dx}g(x)$
$= \delta(f(x)).g(x) + f(x) \cdot \delta(g(x))$
Therefore, δ is a derivative.

4.1.3 Derivation (endomorphism type):

Let R be a ring and σ an endomorphism of R, a mapping $\delta : R \to R$ is called a σ-derivation if
$\delta(a.b) = \delta(a).\sigma(b) + a.\delta(b)$.

4.1.4 Example:

Let R ba a ring and $\delta : R \to R$ any map. Let $\phi : R \to R$ be a map defined by

$$\phi(r) = \begin{pmatrix} \sigma(r) & 0 \\ \delta(r) & r \end{pmatrix}$$

Then δ is a σ-derivation of R if and only if ϕ is a homomorphism.
For any $a, b \in R$,
$\phi(a+b) = \phi(a) + \phi(b)$

$$\text{implies } \begin{pmatrix} \sigma(a+b) & 0 \\ \delta(a+b) & a+b \end{pmatrix} = \begin{pmatrix} \sigma(a) & 0 \\ \delta(a) & a \end{pmatrix} + \begin{pmatrix} \sigma(b) & 0 \\ \delta(b) & b \end{pmatrix}$$

$$= \begin{pmatrix} \sigma(a)+\sigma(b) & 0 \\ \delta(a)+\delta(b) & a+b \end{pmatrix}$$

$$= \begin{pmatrix} \sigma(a+b) & 0 \\ \delta(a)+\delta(b) & a+b \end{pmatrix}$$

because, σ is an endomorphism .
Comparing both sides, we get
$\delta(a+b) = \delta(a) + \delta(b)$
Also, $\phi(a.b) = \phi(a).\phi(b)$

$$\text{Implies } \begin{pmatrix} \sigma(ab) & 0 \\ \delta(ab) & ab \end{pmatrix} = \begin{pmatrix} \sigma(a) & 0 \\ \delta(a) & a \end{pmatrix} \begin{pmatrix} \sigma(b) & 0 \\ \delta(b) & b \end{pmatrix}$$

$$= \begin{pmatrix} \sigma(a)\sigma(b)+0\delta(b) & \sigma(a)0+0b \\ \delta(a)\sigma(b)+a\delta(b) & ab \end{pmatrix}$$

$$= \begin{pmatrix} \sigma(a)\sigma(b) & 0 \\ \delta(a)\sigma(b)+a\delta(b) & ab \end{pmatrix}$$

$$= \begin{pmatrix} \sigma(ab) & 0 \\ \delta(a)\sigma(b)+a\delta(b) & ab \end{pmatrix}$$

Comparing both sides, we have
$\delta(ab) = \delta(a)\sigma(b) + a\delta(b)$
Therefore, δ is a σ-derivation.

4.1.5 2-Primal Rings:

A ring R is 2-primal if and only if set of nilpotent elements and prime radical of R are same if and only if the prime radical is a completely semi prime ideal.

4.1.6 Example:

(1) Let $R = F[x]$ be the polynomial ring over the field F. Then R is 2-primal with $P(R) = \{0\}$.

(2) Let $R = M_2(Q)$, the set of 2×2 matrices over Q. Then $R[x]$ is a prime ring with non-zero nilpotent elements and, so can not be 2-primal.

4.1.7 δ-Ring:

Let R be a ring. Let σ be an automorphism of R and δ be a σ-derivation of R. Then R is a δ-ring if $a\delta(a) \in P(R)$ implies $a \in P(R)$.

4.1.8 σ-Rigid:

A ring R is σ-rigid if there exists an endomorphism of R with the property that $a\sigma(a) = 0$ implies $a = 0$ for $a \in R$.

4.1.9 Example:

(1) Let $R = \mathbb{C}$ and $\sigma : \mathbb{C} \to \mathbb{C}$ be the map defined by

$$\sigma(a + ib) = a - ib; a, b \in \mathbb{R}.$$

Then σ is rigid endomorphism.

(2) Let $R = \begin{pmatrix} F & F \\ 0 & F \end{pmatrix}$ where F is a field.

Then $P(R) = \begin{pmatrix} 0 & F \\ 0 & 0 \end{pmatrix}$

Let $\sigma : R \to R$ defined by $\sigma(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$

Then σ is an endomorphism.
Let $0 \neq a \in F$. Then
$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \sigma(\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
but $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
Thus, R is not σ-rigid.

4.1.10 $\sigma(*)$-Ring:

Kwak defines a $\sigma(*)$-ring to be a ring if $a\sigma(a) \in P(R)$ implies $a \in P(R)$ for $a \in R$.

4.1.11 Examples:

(1) Let $R = \mathbb{C}$ and $\sigma : \mathbb{C} \to \mathbb{C}$ be the map defined by $\sigma(a + ib) = a - ib; a, b \in \mathbb{R}$. Then R is $\sigma(*)$-ring.

(2) Let $R = F[x]$ be the polynomial ring over the field F. Let $\sigma : R \to R$ be an endomorphism defined by $\sigma(f(x)) = f(0)$.
Then R is not a $\sigma(*)$-ring.

4.1.12 Remark:

Every $\sigma(*)$-ring is a 2-primal ring but converse need not be true.

4.1.13 Proposition:

Let R be a ring and σ an automorphism of R. Then R is a $\sigma(*)$-ring implies R is 2-primal.

Proof. Let $a \in R$ be such that $a^2 \in P(R)$. Then
$a\sigma(a)\sigma(a\sigma(a)) = a\sigma(a)\sigma(a)\sigma^2(a)$
$\in \sigma(P(R)) = P(R)$.
Therefore $a\sigma(a) \in P(R)$ and hence $a \in P(R)$. □

4.1.14 Example:

Let $R = F[x]$ be the polynomial ring over the field F. Then R is 2-primal with $P(R) = \{0\}$.
Let $\sigma : R \to R$ be an endomorphism defined by $\sigma(f(x)) = f(0)$.
Then R is not a $\sigma(*)$-ring.

4.1.15 Definition (Ouyang [76]):

Let R be a ring and σ an endomorphism of R such that $a\sigma(a) \in N(R)$ if and only if $a \in N(R)$ for $a \in R$. Then R is called a weak σ-rigid ring.

4.1.16 Example:

[Example (2.1) of Ouyang [76]]. Let σ be an endomorphism of a ring R such that R is a σ-rigid ring. Let

$$A = \{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} \mid a, b, c, d \in R \}$$

be a subring of $T_3(R)$, the ring of upper triangular matrices over R. Now σ can be extended to an endomorphism $\overline{\sigma}$ of A by $\overline{\sigma}((a_{ij})) = (\sigma(a_{ij}))$. Then it can be seen that A is a weak $\overline{\sigma}$-rigid ring.

Ouyang has proved in [76] that if σ is an endomorphism of a ring R, then R is σ-rigid if and only if R is weak σ-rigid and reduced.

4.1.17 Definition:

An ideal I of R is called 2-primal if $P(R/I) = N(R/I)$. A ring R is called *strongly* 2-*primal* if every proper ideal I of R is 2-primal, where the term proper means only $I \neq R$.

4.2 Skew Polynomial Rings of Endomorphism Type

In the prologue we saw several examples of rings that look like polynomial rings in one indeterminate but in which the indeterminate does not commute with the coefficients- rather, multiplication by the indeterminate has been "skewed" or "twisted" by means of an automorphism of the coefficient ring, or a derivation, or a combination of such maps. To help the reader get used to constructing and working with such twisted polynomial rings, we begin here by concentrating on the case where the twisting is done by an automorphism. In next sections, we move on to twists by derivations and then to general skew polynomial rings.

Thus let R be a ring, σ an automorphism of R, and x an indeterminate. Let S be the set of all formal expressions $a_0 + a_i x + ... + a_n x^n$,

where n is a nonnegative integer and the $a_i \in R$. It s often convenient to write such an expression as a sum $\Sigma_i a_i x^i$, leaving it understood that the summation runs over a finite sequence of nonnegative integers i, or by thinking of it as an infinite sum in which almost all of the coefficients a_i are zero. We define an addition operation in S in the usual way:

$$(\Sigma_i a_i x^i) + (\Sigma_i b_i x^i) = \Sigma(a_i + b_i)x^i.$$

As for multiplication, we would like the coefficients to multiply together as they do in R, and we would like the powers of x to multiply following the usual rules for exponents. We take the product of an element $a \in R$ with a power x^i (in that order) to be the single-term sum ax^i. It is in a product of the form $x^i a$ that the twist enters. We define xa to be $\sigma(a)x$ and iterate that rule to obtain $x^i a = \sigma^i(a)x$. This leads us to define the following multiplication rule in S:

$$(\Sigma_i a_i x^i)(\Sigma_j b_j x^j) = \Sigma_{i,j} a_i \sigma^i(b_j) x^{i+j} = \Sigma_k (\Sigma_{i+j=k} a_i \sigma^i(b_j)) x^k.$$

This leads us to the following definition.

4.2.1 Definition:

Let R be a ring and σ an automorphism of R. We write $S = R[x; \sigma]$ (where S and x may or may not already occur in the discussion) to mean that

(a) S is a ring, containing R as a subring;

(b) x is an element of S;

(c) S is a free left R-module with basis $\{1, x, x^2, ...\}$;

(d) $xr = \sigma(r)x$ for every $r \in R$.

Thus, the expression $S = R[x; \sigma]$ can be used either to introduce a new ring S (constructed as above) or to say that a given ring S and element x satisfy conditions $(a) - (d)$. Whenever $S = R[x; \sigma]$ we say that S is a skew polynomial ring over R.

Throughout this section R is an associative ring with identity. Recall that an ideal I of a ring R is called σ invariant if $\sigma(I) = I$. Also I is called completely prime if $ab \in I$ implies $a \in I$ or $b \in I$ for $a, b \in R$. We

also note that in a right Noetherian ring R, $MinSpec(R)$ is finite (Theorem (2.4) of Goodearl and Warfield [38], and for any $P \in MinSpec(R)$, $\sigma^i(P) \in MinSpec(R)$ for all integers $i \geq 1$. Therefore there exists an integer $u \geq 1$, such that $\sigma^u(P) = P$ for all $P \in MinSpec(R)$. We use the same u henceforth, and as mentioned above, we denote $\cap_{i=1}^{u}\sigma_i(P)$ by P^0.

The above discussion shows that, given R and σ, a skew polynomial ring $S = R[x;\sigma]$ does exist. As in the case for ordinary polynomial rings, we would like S to be unique, up to appropriate isomorphisms. We prove this with the help of the following *universal mapping property*, in which the map ψ may be thought as an analog of an evaluation map on ordinary polynomials in the commutative theory.

4.2.2 Lemma:

Let R be a ring, σ an automorphism of R and $S = R[x;\sigma]$. Suppose that we have a ring T, a ring homomorphism $\phi : R \to T$, and an element $y \in T$ such that $y\phi(r) = \phi\sigma(r)y + \phi\delta(r)$ for all $r \in R$. Then there is a unique ring homomorphism $\psi : S \to T$ such that $\psi|R = \phi$ and $\psi(x)y$.

Proof. Clearly any such map would have to be given by the rule

$$\psi(\Sigma_i a_i x^i) = \Sigma_i \phi(a_i) y^i$$

and so there is at most one possibility for ψ. This rule does give a well-defined function $\psi : S \to T$ such that $\psi|R = \phi$ and $\psi(x) = y$, and so we just need to show that ψ is a ring homomorphism. It is clear that ψ is additive and that $\psi(1) = 1$. The rule $y\phi(r) = \phi\sigma(r)y$ implies (by induction that) $y'\phi(r) = \phi\sigma'(r)y'$ for all $i \in \mathbb{Z}^+$ and $r \in R$. Hence,

First observe that if $t = \Sigma_j b_j x^j$ s an arbitrary element of S, then

$$[\psi(\Sigma_i a_i x^i)][\psi(\Sigma_j b_j x^j)] = [\Sigma_i \phi(a_i) y^i][\Sigma_j \phi(b_j) y^j]$$

$$= \Sigma_{i,j}\phi(a_i)\phi\sigma^i(b_j)y^{i+j} = \Sigma_k(\Sigma_{i+j}\phi(a_i)\phi\sigma^i(b_j))y^k$$

$$= \psi[\Sigma_k(\Sigma_{i+j=k}a_i\sigma^i(b_j))x^k] = \psi[(\Sigma_i a_i x^i)(\Sigma_j b_j x^j)]$$

for all elements $\Sigma_i a_i x^i$ and $\Sigma_j b_j x^j$ in S. Therefore ψ is a ring homomorphism, as required. □

4.2.3 Corollary:

Let R be a ring, σ an automorphism of R. Suppose that $S = R[x;\sigma]$ and $S' = R[x';\sigma]$. Then there is a unique ring isomorphism $\psi : S \to S'$ such that $\psi(x) = x'$ and $\psi|R$ is the identity map on R.

Proof. First apply Lemma (4.2.2) with $\phi : R \to S'$ being the inclusion map: we obtain a unique ring isomorphism $\psi : S \to S'$ such that $\psi(x) = x'$ and $\psi|R = \phi$. We may rephrase the last property by saying that $\psi|R$ is the identity on R. By symmetry, Lemma (4.2.12) also provides a ring homomorphism $\psi' : S' \to S$ such that $\psi'(x') = x$ and $\psi'|R$ is the identity on R.

Now $\psi'\psi : S \to S$ is a ring homomorphism such that $(\psi'\psi)(x) = x$ and $(\psi'\psi)|R$ is the identity on R. The identity map on S enjoys the same properties. Hence, the uniqueness part of Lemma (4.2.2) (where now $T = S$ and $y = x$) implies that $\psi'\psi$ equals the identity map on S. Similarly, $\psi\psi'$ equals the identity map on S'.

Therefore ψ and ψ' are mutually inverse isomorphisms □

4.2.4 Proposition:

[Proposition (2.1)[11]]. Let R be a right Noetherian ring. Let σ be an automorphism of R. Then $\sigma(N(R)) = N(R)$.

Proof. Denote $N(R)$ by N. We have $\sigma(N) \subseteq N$ as R is right Noetherian, therefore, $\sigma(N)$ is a nilpotent ideal of R by Theorem (5.18) of Goodearl and Warfield [38]. Now let $n \in N$. Then σ being an automorphism of R implies that there exists $a \in R$ such that $n = \sigma(a)$. Now $I = \sigma^{-1}(N) = \{a \in R \text{ such that } \sigma(a) = n \in N\}$ is an ideal of R. Now I is nilpotent, so $I \subseteq \sigma(N)$, which implies that $N \subseteq \sigma(N)$. Hence $\sigma(N) = N$. □

4.2.5 Proposition:

[Proposition (2.2)[11]]. Let R be a Noetherian ring. Let σ be as usual. Then $S(N(R)) = N(S(R))$.

Proof. It is easy to see that $S(N(R)) \subseteq N(S(R))$. We will show that $N(S(R)) \subseteq S(N(R))$. Let $f = \Sigma_{i=0}^{m} x^i a_i \in N(S(R))$. Then $(f)(S(R)) \subseteq N(S(R))$, and $(f)(R) \subseteq N(S(R))$. Let $((f)(R))k = 0, k > 0$. Then

equating leading term to zero, we get $(x^m a_m R)^k = 0$. This implies on simplification that

$$x^{km}\sigma^{(k-1)m}(a_m R).\sigma^{(k-2)m}(a_m R).\sigma^{(k-3)m}(a_m R)...a_m R = 0.$$

Therefore $\sigma^{(k-1)m}(a_m R).\sigma^{(k-2)m}(a_m R).\sigma^{(k-3)m}(a_m R)...a_m R = 0 \subseteq P$, for all $P \in MinSpec(R)$. Now there are two cases: $u \geq m$, or $m \geq u$. If $u \geq m$, then we have

$$\sigma^{(k-1)u}(a_m R).\sigma^{(k-2)u}(a_m R).\sigma^{(k-3)u}(a_m R)...a_m R \subseteq P.$$

This implies that $\sigma^{(k-j)u}(a_m R) \subseteq P$, for some $j, 1 \leq j \leq k$, i.e., $a_m R \subseteq \sigma^{-(k-j)u}(P) = P$. So we have $a_m R \subseteq P$, for all $P \in MinSpec(R)$. Therefore $a_m \in P(R) = N(R)$. Now $x^m a_m \in S(N(R)) \subseteq N(S(R))$ implies that $\Sigma_{i=0}^{m-1} x^i a_i \in N(S(R))$, and with the same process, in a finite number of steps, it can be seen that $a_i \in P(R) = N(R)$, $0 \leq i \leq m-1$. Therefore $f \in S(N(R))$. Hence $N(S(R)) \subseteq S(N(R))$ and the result. □

We now establish a relation between the minimal prime ideals of R and those of $S(R)$ in the following theorem.

4.2.6 Theorem:

[Theorem (2.3) [11]]. Let R be a Noetherian ring and σ be an automorphism of R. Then $P \in MinSpec(S(R))$ if and only if there exists $L \in MinSpec(R)$, such that $S(P \cap R) = P$ and $P \cap R = L^0$.

Proof. Let $L \in MinSpec(R)$. Then $\sigma^u(L) = L$ for some integer $u \geq 1$. Let $L_1 = L^0$. Then by [[68], (10.6.12)] and by [[38], Theorem (7.27)], $Q_2 = S(L_1) \in MinSpec(S(R))$.

Conversely, suppose that $P \in MinSpec(S(R))$. Then $P \cap R = U^0$ for some $U \in Spec(R)$ and U contains a minimal prime U_1. Now $P \supseteq S(R)U_1^0$, which is a prime ideal of $S(R)$. Hence $P = S(R)U_1^0$. □

4.2.7 Theorem:

[Theorem (2.4) [11]]. Let R be a 2-primal Noetherian ring. Then $S(R)$ is 2-primal Noetherian.

Proof. The fact that R is Noetherian implies $S(R)$ is Noetherian follows from Hilbert Basis Theorem, namely Theorem (1.12) of [38]. Now R

is 2-primal implies $N(R) = P(R)$ and Proposition (4.2.4) implies that $\sigma(N(R)) = N(R)$. Therefore $S(N(R)) = S(P(R))$. Now by Proposition (4.2.5) $S(N(R)) = N(S(R))$.

We now show that $S(P(R)) = P(S(R))$. It is easy to see that $S(P(R)) \subseteq P(S(R))$. Now let $g = \Sigma_{i=0}^{t} x^i b_i \in P(S(R))$. Then $g \in P_i$, for all distinct $P_i \in MinSpec(S(R))$. Now Theorem (4.2.6) implies that there exists $U_i \in MinSpec(R)$ such that $P_i = S((U_i)^0)$. Now it can be seen that P_i are distinct implies that U_i are distinct. Therefore $g \in S((U_i)^0)$. This implies that $b_i \in (U_i)^0 \subseteq U_i$. Thus we have $b_i \in U_i$, for all $U_i \in MinSpec(R)$. Therefore $b_i \in P(R)$, which implies that $g \in S(P(R))$. So we have $P(S(R)) \subseteq S(P(R))$, and hence $S(P(R)) = P(S(R))$. Thus we have $P(S(R)) = S(P(R)) = S(N(R)) = N(S(R))$. Hence $S(R)$ is 2-primal. □

4.2.8 Theorem:

Let R be a Noetherian ring, which is also an algebra over $\mathbb{Q}$. Letσ be an automorphism of R such that R is a $\sigma(*)$-ring and δ be a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$, for all $a \in R$ and R is a δ-ring. Then $R[x; \sigma, \delta]$ is 2-primal Noetherian.

Proof. We show that $\sigma(U) = U$ for all $U \in MinSpec(R)$. Suppose $U = U_1$ is a minimal prime ideal of R such that $\sigma(U) \neq U$. Let $U_2, U_3, ..., U_n$ be the other minimal primes of R. Now $\sigma(U)$ is also a minimal prime ideal of R. Renumber so that $\sigma(U) = U_n$. Let $a \in \cap_{i=1}^{n-1} U_i$. Then $\sigma(a) \in U_n$, and so $a\sigma(a) \in \cap_{i=1}^{n} U_i = P(R)$. Therefore $a \in P(R)$, and thus $\cap_{i=1}^{n-1} U_i \subseteq U_n$, which implies that $U_i \subseteq U_n$ for some $i \neq n$, which is impossible. Hence $\sigma(U) = U$. Now the rest is obvious. □

We now prove some of above results without the condition that $\sigma(\delta(a)) = \delta(\sigma(a))$, for all $a \in R$. Towards this we have the following:

4.2.9 Theorem:

Let R be a Noetherian $\mathbb{Q}$-algebra. Let σ be an automorphism of R and δ a σ-derivation of R. Then:

(1) $P_1 \in MinSpec(R)$ such that $\sigma(P_1) = P_1$ implies $O(P_1) \in MinSpec$ $(O(R))$.

(2) $P \in MinSpec(O(R))$ such that $\sigma(P \cap R) = P \cap R$ implies $P \cap R \in MinSpec(R)$.

Proof. (1) Let $P_1 \in MinSpec(R)$ with $\sigma(P_1) = P_1$. Let $T = \{a \in P_1$ such that $\delta^k(a) \in P_1$, for all positive integers $k\}$. The it can be seen that $T \in Spec(R)$. Also $\delta(T) \subseteq T$. Now $T \subseteq P_1$, and P_1 being a minimal prime ideal of R implies that $T = P_1$. Hence $\delta(P_1) \subseteq P_1$.
Now on the same lines as in Theorem (2.22) of Goodearl and Warfield [38], it can be easily seen that $O(P_1) \subseteq Spec(O(R))$. Suppose that $O(P_1) \notin MinSpec(O(R))$, and $P_2 \subset O(P_1)$ is a minimal prime ideal of $O(R)$. Then we have $P_2 = O(P_2 \cap R) \subset O(P_1) \in MinSpec(O(R))$. Therefore $P_2 \cap R \subset P_1$, which is a contradiction as $P_2 \cap R \in Spec(R)$. Hence $O(P_1) \in Spec(O(R))$.

(2) Let $P \in MinSpec(O(R))$ with $\sigma(P \cap R) = P \cap R$. Then on the same lines as in Theorem (2.22) of Goodearl and Warfield [38], it can be seen that $P \cap R \in Spec(R)$ and $O(P \cap R) \in Spec(O(R))$. Therefore $O(P \cap R) = P$. We now show that $P \cap R \in MinSpec(R)$. Suppose that $U \subset P \cap R$, and $U \in MinSpec(R)$. Then $O(U) \subset O(P \cap R) = P$. But $O(U) \in Spec(O(R))$ and, $O(U) \subset P$, which is not possible. Thus we have $P \cap R \in MinSpec(R)$. □

4.2.10 Theorem:

Let R be a Noetherian $\mathbb{Q}$-algebra, σ an automorphism of R and δ a σ-derivation of R such that R is a δ-ring, $\sigma(P) = P$ for all $P \in MinSpec(R)$ and $\delta(P(R)) \subseteq P(R)$. Then $O(R)$ is 2-primal.

Proof. Let $P_1 \in MinSpec(R)$. Then it is given that $\sigma(P_1) = P_1$, and therefore Theorem (4.2.9) implies that $O(P_1) \in MinSpec(O(R))$. Similarly for any $P \in MinSpec(O(R))$ such that $\sigma(P \cap R) = P \cap R$ Theorem (4.2.9) implies that $P \cap R \in MinSpec(R)$. Therefore, $O(P(R)) = P(O(R))$, and now the result is obvious by using Theorem (4.6.6). □

4.2.11 Corollary:

Let R be a Noetherian $\mathbb{Q}$-algebra, σ an automorphism of R and δ a σ-derivation of R such that R is a δ-ring, $\sigma(P) = P$ for all $P \in MinSpec(R)$. Then $O(R)$ is 2-primal.

Proof. Let $P_1 \in MinSpec(R)$ with $\sigma(P_1) = P_1$. Then as in the proof of Theorem (4.2.9) $\delta(P_1) \subseteq P_1$, and therefore $\delta(P(R)) \subseteq P(R)$. Now the rest is obvious using Theorem (4.2.10). □

4.2.12 Theorem:

Let R be a Noetherian ring, which is also an algebra over $\mathbb{Q}$. Let σ be an automorphism of R such that R is a $\sigma(*)$-ring and δ be a σ-derivation of R such that R is a δ-ring. Then $R[x; \sigma, \delta]$ is 2-primal Noetherian.

Proof. We show that $\sigma(U) = U$ for all $U \in MinSpec(R)$. Suppose $U = U_1$ is a minimal prime ideal of R such that $\sigma(U) \neq U$. Let $U_2, U_3, ..., U_n$ be the other minimal primes of R. Now $\sigma(U)$ is also a minimal prime ideal of R. Renumber so that $\sigma(U) = U_n$. Let $a \in \cap_{i=1}^{n-1} U_i$. Then $\sigma(a) \in U_n$, and so $a\sigma(a) \in \cap_{i=1}^{n} U_i = P(R)$. Therefore $a \in P(R)$, and thus $\cap_{i=1}^{n-1} U_i \subseteq U_n$, which implies that $U_i \subseteq U_n$ for some $i \neq n$, which is impossible. Hence $\sigma(U) = U$. Now the rest is obvious. □

4.3 Skew Polynomial Ring of Derivation Type

Several of the examples discussed in the Prologue [see [41]] appear as polynomial rings in which multiplication by the indeterminate is twisted by a derivation rather than by an automorphism. This situation has several new features - in particular, the characteristic of the ring plays an important role - but it is still significantly simpler than the general case, in which both an automorphism and a derivation act. Thus, we begin the section by studying the derivation case.

Differential operator ring $R[x.\delta]$ is the usual polynomial ring with coefficients in R in which multiplication is subject to the relation $ax = xa + \delta(a)$ for all $a \in R$. We take any $f(x) \in R[x, \delta]$ to be of the form $f(x) = \Sigma_{i=0}^{n} x^i a_i$. We denote $R[x, \delta]$ by $D(R)$. If I is δ-invariant (i.e., $\delta(I) \subseteq I$) ideal of R, then $I[x, \delta]$ is an ideal of $D(R)$. We denote $I[x, \delta]$ as usual by $D(I)$.

Let R be a ring, δ a derivation on R, and x an indeterminate. Let S be the set of all formal expressions $a_0 + a_1 x + ... + a_n x^n$, where $n \in \mathbb{Z}^+$ and the $a_i \in R$, and define addition on S in the usual way. Now we would like to build a multiplication in S such that $xa = ax + \delta(a)$ for all $a \in R$. To fully describe this multiplication, we must iterate the above

rule, which leads us to the formula $x^i a = \Sigma_{l=0}^{i} \binom{i}{l} \delta^{i-l}(a) x^l$ for $i \in \mathbb{Z}^+$ and $a \in R$. Thus, we define multiplication in S as follows:

$$(\Sigma_i a_i x^i)(\Sigma_j b_j x^j) = \Sigma_{i,j} \Sigma_{l=0}^{i} \binom{i}{l} a_i \delta^{i-l}(b_j) x^{l+j}$$

$$= \Sigma_k (\Sigma_{l=0}^{k} \Sigma_{i \geq l} \binom{i}{l} a_i \delta^{i-l}(b_{k-l})) x^k.$$

4.3.1 Exercise:

Verify that the set S together with the operations discussed above is a ring, containing R as a subring. Give a formal description of S without using the symbol x, analogous to Exercise $1H$ of [41].

4.3.2 Definition:

Let R be a ring and δ a derivation of R. We write

$$S = R[x; \delta]$$

to mean that

(a) S is a ring, containing R as a subring;

(b) x is an element of S;

(c) S is a free left R-module with basis $\{1, x, x^2, ...\}$;

(d) $xr = rx + \delta(r)$ for every $r \in R$.

In this situation we say that S is a skew polynomial ring over R or a formal differential operator ring over R. It is also a helpful way to distinguish between $R[x; \delta]$ and the skew polynomial rings $R[x; \sigma]$ studied in the previous section.

Note that, given R and δ, Exercise (4.3.1) shows that there does exist a differential operator ring $R[x; \delta]$.

4.3.3 Proposition:

[Proposition (1.1) [10]]. Let R be a Noetherian $\mathbb{Q}$-algebra. Let δ be a derivation of R. Then $\delta(P(R)) \subseteq P(R)$.

Proof. Let $P_1 \in MinSpec(R)$. Let $T = R[[t]]$, the formal power series ring. Now it can be seen that $e^{t\delta}$ is an automorphism of T and $P_1T \in MinSpec(T)$. We also know that $(e^{t\delta})^k(P_1T) \in MinSpec(T)$ for all integers $k \geq 1$. Now T is Noetherian by Exercise $(1ZA(c))$ of [38], and therefore Theorem (2.4) of [38] implies that $MinSpec(T)$ is finite. So exists an integer $n \geq 1$ such that $(e^{t\delta})^n(P_1T) = P_1T$; i.e., $(e^{nt\delta})(P_1T) = P_1T$. But R is a $\mathbb{Q}$-algebra, therefore, $e^{t\delta}(P_1T) = P_1T$. Now for any $a \in P_1$, $a \in P_1T$ also, and so $e^{t\delta}(a) \in P_1T$; i.e., $a + \delta(a) + t\delta(a) + (t^2/2!)\delta^2(a) + ... \in P_1T$, which implies that $\delta(a) \in P_1$. Therefore $\delta(P_1 \subseteq P_1$.

Now $P(R) \subseteq P$, for all $P \in MinSpec(R)$ implies that $\delta(P(R)) \subseteq \delta(P) \subseteq P$, for all $P \in MinSpec(R)$. Therefore

$$\delta(P(R)) \subseteq \cap_{p \in MinSpec(R)} P = P(R).$$

□

4.3.4 Proposition:

[Proposition (1.2) [10]]. Let R be a Noetherian $\mathbb{Q}$-algebra. Let δ be as usual. Then $D(N(R)) = N(D(R))$.

Proof. It is easy to see that $D(N(R)) \subseteq N(D(R))$. We will show that $N(D(R)) \subseteq D(N(R))$. Let $f = \Sigma_{i=0}^{m} x^i a_i \in N(D(R))$. Then $(f)(D(R)) \subseteq N(D(R))$, and $(f)(R) \subseteq N(D(R))$. Let

$$((f)(R))^k = 0, k > 0.$$

Then equating leading term to zero, we get $(x^m a_m R)^k = 0$. This implies on simplification that $x^{km}(a_m R)^k = 0$. Therefore $(a_m R)^k = 0 \subseteq P$, for all $P \in MinSpec(R)$. So we have $a_m R \subseteq P$, for all $P \in MinSpec(R)$. Therefore $a_m \in P(R) = N(R)$. Now $x^m a_m \in D(N(R)) \subseteq N(D(R))$ implies that

$$\Sigma_{i=0}^{m-1} x^i a_i \in N(D(R)),$$

and with the same process, in a finite number of steps, it can be seen that $a_i \in P(R) = N(R)$, $0 \leq i \leq m-1$. Therefore $f \in D(N(R))$. Hence $N(D(R)) \subseteq D(N(R))$ and the result. □

4.3.5 Theorem:

[Theorem (1.1) [10]]. Let R be a Noetherian $\mathbb{Q}$-algebra and δ be a derivation of R. Then $P \in MinSpec(D(R))$ if and only if $P = D(P \cap R)$ and $P \cap R \in MinSpec(R)$.

Proof. Let $P_1 \in MinSpec(R)$. Then $\delta(P_1) \subseteq P_1$ by Proposition (4.3.3). Therefore by [[68], (14.2.5) (ii)], $D(P_1) \in Spec(D(R))$. Suppose $P_2 \subset D(P_1)$ is a minimal prime ideal of $D(R)$. Then

$$P_2 = D(P_2 \cap R) \subset D(P_1) \in MinSpec(D(R)).$$

So $P_2 \cap R \subset P_1$ which is not possible.

Conversely suppose that $P \in MinSpec(D(R))$. Then $P \cap R \in Spec(R)$ by Lemma (2.21) of Goodearl and Warfield [38]. Let $P_1 \subset P \cap R$ be a minimal prime ideal of R. Then $D(P_1) \subset D(P \cap R)$ and as in first paragraph $D(P_1) \in Spec(D(R))$, which is a contradiction. Hence $P \cap R \in MinSpec(R)$. □

4.3.6 Theorem:

[Theorem (1.2) [10]]. Let R be a 2-primal Noetherian $\mathbb{Q}$-algebra. Then $D(R)$ is 2-primal Noetherian.

Proof. R is Noetherian implies $D(R)$ is Noetherian follows from Hilbert Basis Theorem, namely Theorem (1.12) of Goodearl and Warfield [38]. Now R is 2-primal implies $N(R) = P(R)$ and Proposition (4.3.3) implies that $\delta(N(R)) \subseteq N(R)$. Therefore $D(N(R)) = D(P(R))$. Now by Proposition (4.3.4) $D(N(R)) = N(D(R))$.

We now show that $D(P(R)) = P(D(R))$. It is easy to see that $D(P(R)) \subseteq P(D(R))$.

Now let

$$g = \Sigma_{i=0}^{t} x^i b_i \in P(D(R)).$$

Then $g \in P_i$, for all $P_i \in MinSpec(D(R))$. Now Theorem (4.3.3) implies that there exists $U_i \in MinSpec(R)$ such that $P_i = D(U_i)$. Now it can be seen that P_i are distinct implies that U_i are distinct. Therefore $g \in D(U_i)$. This implies that $b_i \in U_i$. Thus we have $b_i \in U_i$, for all $U_i \in MinSpec(R)$. Therefore $b_i \in P(R)$,which implies that $g \in D(P(R))$. So

we have $P(D(R)) \subseteq D(P(R))$, and hence $D(P(R)) = P(D(R))$.

Thus we have

$$P(D(R)) = D(P(R)) = D(N(R)) = N(D(R)).$$

Hence $D(R)$ is 2-primal. □

4.3.7 Proposition:

[Proposition (3.1) [10]]. Let R be a Noetherian $\mathbb{Q}$-algebra and δ be a derivation of R. Then $\delta(P) \subseteq P$, for all $P \in MinSpec(R)$ and $\delta(P(R)) \subseteq P(R)$.

Proof. See [[38], Lemma (2.20)]. □

4.3.8 Theorem:

[Theorem (3.3) [10]]. Let R be a 2-primal Noetherian $\mathbb{Q}$-algebra and let δ be a derivation of R such that $N(D(R)) = D(N(R))$. Then $D(R)$ is 2-primal Noetherian.

Proof. First of all we note that $D(P(R))$ is well defined by Proposition (4.3.7). Also $D(R)$ is Noetherian by Theorem (1.12) of [38]. Now R is 2-primal implies that $N(R) = P(R)$. We will show that $P(D(R)) = D(P(R))$. Now let

$$g = \Sigma_{i=0}^{t} x^i b_i \in P(D(R)).$$

Then $g \in P_i$, for all distinct $P_i \in MinSpec(S(R))$. Now Theorem (4.3.5) implies that $P_i \cap R \in MinSpec(R)$ and that $P_i = D(P_i \cap R)$. Denote $P_i \cap R$ by U_i. Now it can be seen that U_i are distinct. Therefore $g \in D(U_i)$. This implies that $b_i \in U_i$. Thus we have $b_i \in U_i$, for all $U_i \in MinSpec(R)$. Therefore $b_i \in P(R)$, which implies that $g \in D(P(R))$. So we have $P(D(R)) \subseteq D(P(R))$. Now let $h = \Sigma_{i=0}^{m} x^i c_i \in D(P(R))$. Then $c_i \in D(P(R)) \subseteq T_i$, for all distinct $T_i \in MinSpec(R)$. Now Theorem (4.3.5) implies that $D(T_i) \in MinSpec(D(R))$. Denote $D(T_i)$ by L_i. Now it can be seen that L_i are distinct and therefore $h \in L_i$ for all $L_i \in MinSpec(D(R))$. Thus $h \in P(D(R))$ and therefore $D(P(R)) \subseteq P(D(R))$.

So we have $P(D(R)) = D(P(R))$. Now it is given that $N(D(R)) = D(N(R))$ and thus we have

$$P(D(R)) = D(P(R)) = D(N(R)) = N(D(R)).$$

Hence $D(R)$ is 2-primal. □

4.4 Skew-Laurent Rings

One way to view a differential operator ring $R[\theta, \delta]$ is that it is a ring extension of R in which δ becomes an inner derivation (since $\delta(r) = \theta r - r\theta$ for all $r \in R$). If we start with an automorphism σ of R and seek a ring extension in which σ becomes an inner automorphism, we need a ring extension containing a unit θ such that $\sigma(r) = \theta r \theta^{-1}$ for all $r \in R$, that is, $\theta r = \sigma(r)\theta$ for all $r \in R$. This suggests constructing a ring extension of the skew polynomial ring $R[\theta; \sigma]$ in which θ has an inverse. We will give a direct construction of such a ring by analogy with Proposition (1.10) of [38] , where this time we will work with additive endomorphism of the Laurent polynomial ring $R[x, x^{-1}]$.

4.4.1 Definition:

Let R be a ring and σ an automorphism of R. We write

$$T = R[x^{\pm 1}; \sigma]$$

to mean that

(a) T is a ring, containing R as a subring;

(b) x is invertible element of T;

(c) T is a free left R-module with basis $\{1, x, x^{-1}, x^2, x^{-2}, ...\}$;

(d) $xr = \sigma(r)x$ for all $r \in R$.

When $T = R[x^{\pm 1}; \sigma]$, we say that S is a skew-Laurent ring over R, or a skew Laurent extension of R.

4.4.2 Definition:

Let k be a field and $q \in k^{\times}$. The quantized coordinate ring of $(k^{\times})^2$ (corresponding to the choice of q) is the k-algebra $\mathcal{O}((k^{\times})^2)$ presented by generators x, x', y, y' and relations

$$xx' = x'x = yy' = y'y = 1$$

$$xy = qyx.$$

In brief, we may say that $\mathcal{O}((k^\times)^2)$ is presented by generators $x^\pm$ and $y^\pm$ satisfying $xy = qyx$. In algebraic geometry, $(k^\times)^2$ is known as an algebraic torus (of rank 2), and hence $\mathcal{O}((k^\times)^2)$ picks up the nickname quantum torus.

4.4.3 Definition

Let k be a field and $\mathbf{q} = (q_{ij})$ a multiplicatively antisymmetric $n \times n$ matrix over k. The corresponding multiparameter quantum torus is the k-algebra $\mathcal{O}_\mathbf{q}((k^\times)^n)$ presented by $x_1^{\pm 1}, ..., x_n^{\pm 1}$ and relations $x_i x_j = q_{ij} x_j x_i$ for all i, j. The single parameter version $\mathcal{O}_\mathbf{q}((k^\times)^n)$, for $q \in k^\times$, is the special case when $q_{ij} = q$ for all $i < j$.

4.4.4 Proposition:

Let R be a ring and let σ be an automorphism of R. Then there exists a ring S, containing R as a subring, with a unit $\theta \in S$ such that S is a free left R-module with a basis of the form $1, \theta, \theta^{-1}, \theta^2, \theta^{-2}, ...$ and $\theta r = \sigma(r)\theta$ for all $r \in R$.

Proof. Let $E = End_\mathbb{Z}(R[x, x^{-1}])$ where x is an indeterminate, and embed R in E (as a subring) via left multiplications. Extend σ to an automorphism of $R[x, x^{-1}]$ where $\sigma(rx^i) = \sigma(r)x^i$ for all $r \in R$ and $i \in \mathbb{Z}$. Then define $\theta \in E$ according to the rule $\theta(f) = \sigma(f)x$, and observe that $\theta r = \sigma(r)\theta$ for all $r \in R$. Moreover, θ is invertible in E, and $\theta^{-1}(f) = \sigma^{-1}(f)x^{-1}$ for all $f \in R[x, x^{-1}]$. As in the proof of Proposition (1.10) of [38], the set $S = \Sigma_{i \in \mathbb{Z}} R\theta^i$ is a subring of E, and the powers of θ are left linearly independent over R. □

A SKEW HILBERT BASIS THEOREM

We derive a version of the Hilbert Basis Theorem for the skew polynomial rings $R[x; \sigma]$ discussed above; an analogous result for skew-Laurent rings will follow as a Corollary.

4.4.5 Theorem:

[Theorem (1.14) of [41]]. Let σ be an automorphism of a ring R and $S = R[x; \sigma]$. If R is right (left) Noetherian, then so is S.

Proof. Case I. Let us first assume that R is right Noetherian and prove that any nonzero right ideal I of S is finitely generated. We follow the steps in the proof of Theorem (3.4.9), but some details require extra care.

Step I. Let J be the set of leading coefficients of elements of I, together with 0:

$$J = \{r \in R \mid rx^d + r_{d-1}x^{d-1} + ... + r_0 \text{ for some } r_{d-1}, ..., r_0 \in R\}$$

As before, it is easy to see that J is an additive subgroup of R. Now consider elements $r \in J$ and $a \in R$; we need to show that $ra \in J$. There is some skew polynomial of the form $p = rx^d +$ [lower terms] in I. While $pa \in I$, this does not help us, since $pa = r\sigma^d(a)x^d +$ [lower terms], which only yields $r\sigma^d(a) \in J$. To obtain ra instead, we should replace a by $\sigma^{-d}(a)$. More precisely, we have $p\sigma^{-d}(a) \in I$ and

$$p\sigma^{-d}(a) = rax^d + \text{[lower terms]},$$

whence $ra \in J$. This shows that J is a right ideal of R.

Step 2. Since R is right Noetherian, J is finitely generated; say $r_1, ..., r_k$ is a finite list of nonzero generators for J. There exist $p_1, ..., p_k \in I$ such that p_i has leading coefficient r_i and some degree n_i. Set $n = max\{n_1, ..., n_k\}$, and note that $p - ix^{n-n_i}$ is an element of I with leading coefficient r_i but with degree n. Thus, there is no loss of generality in assuming that all the p_i have the same degree n, that is,

$$p_i = r_i x^n + \text{[lower terms]}.$$

Step 3. Set $N = R + Rx + ... + RX^{n-1}$,the set of elements of S with degree less than n. Observe that $N = R + xR + ... + X^{n-1}R$, since

$$b_0 + b_1x + ... + b_{n-1}x^{n-1} = b_0 + x\sigma^{-1}(b_1) + ... + x^{n-1}\sigma^{1-n}(b_{n-1})$$

$$c_0 + xc_1 + ... + x^{n-1}c_{n-1} = c_0 + \sigma(c_1)x + ... + \sigma^{n-1}(c_{n-1})x^{n-1}$$

for all $b_j, c_j \in R$. Consequently, N is a right (as well as left) R-module of S. Viewed as a right R-module, N is finitely generated, and so it is Noetherian by Corollary (3.1.23). Hence, its submodule $I \cap N$ is a finitely generated right R-module, say $q_1, ..., q_t$ generate $I \cap N$.

Step 4. Let I_0 be the right ideal of S generated by $p_1, ..., p_k, q_1, ..., q_t$. Then $I_0 \subseteq I$, and we claim that they are equal. If $p \in I$ with degree less than n, then $p \in I \cap N$ and $p = q_1a_1 + ... + q_ta_t$ for some $a_j \in R$, whence

$p \in I_0$.

Step 5. Now consider some $p \in I$ with degree $m \geq n$, and suppose that all elements of I with degree less than m lie I_0. Let r be the leading coefficient of p; thus

$$p = rx^m + \text{[lower terms]}$$

Since $p \in I$, its leading coefficient r is in J, and so $r = r_1a_1 + ... + r_ka_k$ for some $a_i \in R$. We wish to construct an element of I_0 which also has degree m and leading coefficient r, but the combination $(p_1a_1 + ... + P_ka_k)x^{m-n}$ that we used in the proof of Theorem (3.4.9) no longer works. The problem and solution are the same as in Step I- we should apply appropriate negative powers of σ to the a_i. More precisely, observe that

$$pi\sigma^{-n}(a_i) = r_ia_ix^n + \text{[lower terms]}$$

for all i. Consequently, if $q = (p_1\sigma^{-n}(a_1) + ... + p_k\sigma^{-n}(a_k))x^{m-n}$, then $q \in I_0$ and

$$q = rx^m + \text{[lower terms]}.$$

Now $p - q$ is an element of I with degree less than m. By induction hypothesis, $p - q \in I_0$, and thus $p \in I_0$.

This induction has shown that $I = I_0$, so that I is finitely generated. Therefore, S is right Noetherian.

Case II. Assume now that R is left Noetherian, and let I be an arbitrary nonzero left ideal of S. Here one should try to follow the line of Case I just enough to understand the difficulties. There is a pitfall right at the beginning in Case II, the set J as defined in Step 1 need not be closed under addition. (The problem is that, since we are only allowed to multiply elements of I on the left by power of x, we cannot guarantee that an element of J which occurs as the leading coefficient of some element of I with degree d will also occur as a leading coefficient for elements of I with degrees greater that d.)

The way around such difficulties is to reverse the order of multiplication in all our expressions - including those that just display coefficients of skew polynomials. In other words, for the duration of the proof of Case II, all elements of S should be written with right-hand coefficients (that this is always possible is shown by equations like those displayed

in Step 3). Note that this changes the definition of "leading coefficient" (but not that of "degree") for elements of S. With this change, analogs of Steps $1-5$ are easily carried out: we leave the details to the reader. A more efficient way to deal with the switch from left-hand to right-hand coefficients is to work with opposite rings - see Exercise $1Q$ of [41]. □

Immediate consequences of Theorem (4.4.5) are that the quantum planes $\mathcal{O}_{\mathbf{q}}(k^2)$ are Noetherian and (by induction) the quantum n-spaces $\mathcal{O}_{\mathbf{q}}(k^n)$ are Noetherian.

4.4.6 Corollary:

Let R be a ring and let σ be an automorphism of R. If R is right (left) Noetherian, then skew-Laurent ring $T = R[\sigma, \sigma^{-1}; \sigma]$ is right(left) Noetherian.

Proof. Set $S = R[x; \sigma] \subseteq S$ and remember that S is a subring of T. We proceed by relating the right ideals of T to those of S, as follows.

Claim: If I is a right ideal of T, then $(I \cap S)$ is right ideal of S and $I = (I \cap S)T$.

It is clear that $I \cap S$ is a right ideal of S and that $(I \cap S)T \subseteq I$. If $p \in I$, then

$$p = a_m x^m + a_{m+1} x^{m+1} + ... + a_n x^n$$

for some integers $m \leq n$ and coefficients $a_i \in R$. Since $px^{-m} \in I \cap S$ and $p = (px^{-m})x^m$, we see that $p \in (I \cap S)T$, and the claim is proved.

Now suppose that R is right Noetherian, and let $I_1 \subseteq I_2 \subseteq ...$ be an ascending chain of right ideals of T. Then $I_1 \cap S \subseteq I_2 \cap S \subseteq ...$ is an ascending chain of right ideals of S. Since S is right Noetherian by Theorem (4.4.5), there is an index n such that $I_m \cap S = I_n \cap S$ for all $m \geq n$. Thus

$$I_m = (I_m \cap S)T = (I_n \cap S)T = I_n$$

for all $m \geq n$, which establishes the ACC for right ideals of T. Therefore T is right Noetherian.

The left Noetherian case is proved symmetrically. □

From this Corollary we immediately obtain that all quantum tori $\mathcal{O}_{\mathbf{q}}((k^{\times})^n)$ are Noetherian.

4.4.7 Theorem (Hall):

[Theorem (1.16) of [41]]. If k is a field and G a polycyclic-by-finite group, then the group algebra $k[G]$ is a Noetherian ring.

Proof. By assumption, there exists subgroups

$$G_0 = (1) \subset G_1 \subset ... \subset G_n \subseteq G^{n+1} = G$$

such that each G_{i-1} is a normal subgroup of G_i and G_i/G_{i-1} is infinite cyclic for $i = 1, ..., n$, while G/G_n is finite. There is a corresponding ascending sequence of subalgebras

$$k[G_0] = k \subset k[G_1] \subset ... \subset k[G_n] \subset k[G],$$

and we shall prove that each $k[G_i]$ is Noetherian. This is clear for $i = 0$.

Now let $1 \leq i \leq n$ and assume that $k[G_{i-1}]$ is Noetherian. Choose a coset $G_{i-1}x$ which generates the infinite cyclic group G_i/G_{i-1}. Then G_i is the disjoint union of the cosets $G_{i-1}x^j$ for $j \in \mathbb{Z}$, and so the rule $(g, j) \mapsto gx^j$ gives a bijection $G_{i-1} \times \mathbb{Z} \to G_i$. Consequently,

$$k[G_i] = \bigoplus_{j\in\mathbb{Z}} \bigoplus_{g\in G_{i-1}} kgx^j = \bigoplus_{j\in\mathbb{Z}} (\bigoplus_{g\in G_{i-1}} kg)x^j = \bigoplus_{j\in\mathbb{Z}} k[G_{i-1}]x^j,$$

that is, $k[G_i]$ is a free left module over $k[G_{i-1}]$ with basis $\{x^j | j \in \mathbb{Z}\}$. Since G_{i-1} is a normal subgroup of G_i, we have $xG_{i-1}x^{-1} = G_{i-1}$, and hence $x(k[G_{i-1}])x^{-1} = k[G_{i-1}]$. As a result, the rule $\sigma(r) = xrx^{-1}$ defines an automorphism σ of $k[G_{i-1}]$. By definition of σ, we have $xr = \sigma(r)x$ for all $r \in k[G_{i-1}]$, and thus $k[G_i] = k[G_{i-1}][x^{\pm}; \sigma]$. Corollary (4.4.6) now shows that $k[G_i]$ is Noetherian.

Thus, by induction, we conclude that $k[G_n]$ is Noetherian. Now G is a finite union of cosets $, ..., G_n y_t$, and so $k[G] = \Sigma_{j=1}^{t} \Sigma_{g\in G_n} kgy_j = \Sigma_{j=1}^{t} k[G_n]y_j$, that is, $k[G]$ is finitely generated as a left $k[G_n]$-module. Therefore $k[G]$ is left Noetherian by Corollary (3.4.6), and by symmetry it is right Noetherian as well. □

SIMPLICITY IN SKEW LAURENT RINGS

4.4.8 Definition:

A simple ring is any nonzero ring R such that the only ideals of R are 0 and R. (This terminology is only supposed to suggest that the ideal theory of R is simple, not that the structure of R is necessarily simple in any other respect).

The only commutative simple rings are fields.

4.4.9 Definition:

Let σ be an automorphism of a ring R. An σ-ideal of R is any ideal I of R that is stable under σ, that is, $\sigma(I) = I$. The ring R is said to be σ-simple provided R is nonzero and its only σ-ideals are 0 and R.

4.4.10 Theorem:

Let $T = R[x^{\pm}; \sigma]$, where σ is an automorphism of R. Then T is a simple ring if and only if the following hold:

(a) R is an σ-simple ring,

(b) No positive power of σ is an inner automorphism of R.

Proof. As noted, Exercises 1T and 1U of [41] show the necessity of conditions (a) and (b). Conversely, assume that (a) and (b) hold.

Let I be a nonzero ideal of T; we must show that $I = T$. Set $S = R[x; \sigma]$ and recall from the proof of Corollary (4.4.6) that $I = (I \cap S)T$. Thus, $I \cap S \neq 0$. Since I is an ideal in T, we are allowed to multiply it by either x or x^{-1}. Thus $xIx^{-1} \subseteq I$ and $x^{-1}Ix \subseteq I$, whence $xIx^{-1} = I$. We also have $xSx^{-1} = S$ (Exercise 1R of [41]), and therefore $x(I \cap S)x^{-1} = I \cap S$.

Let n be the least degree that occurs for nonzero elements of $I \cap S$, and set

$$J = \{r \in R \mid rx^n + r_{n-1}x^{n-1} + r_0 \in I \cap S \text{ for some } r_{n-1}, ..., r_0 \in R\}.$$

As in step I of Theorem (4.4.5), we check that J is an ideal of R, nonzero by choice of n. Given $r \in J$, there is a skew polynomial $p \in I \cap S$ of the form $p = rx^n +$ [lower terms]. The skew polynomial $xpx^{-1} = \sigma(r)x^n +$ [lower terms] also lies in $I \cap S$, whence $\sigma(r) \in J$. Hence, $\sigma(J) \subseteq J$, and

a similar argument show that $\sigma - 1 \subseteq J$. Thus, $\sigma(J) = J$.

Now J is a nonzero σ-ideal of R. Since R is σ-simple, we must have $J = R$, whence $1 \in J$. Therefore there is an element $p \in I \cap S$ of the form

$$p = x^n + a_{n-1}x^{n-1} + ... + a_0$$

with the $a_i \in R$. If $a_0 = 0$, then $px^{-1} = x^{n-1} + a_{n-1}x^{n-2} + ... + a_1$ would be a nonzero element of $I \cap S$ with degree $n-1$, contradicting the minimality of n. Hence, $a_0 \neq 0$. Observe that

$$xpx^{-1} = x^n + \sigma(a_{n-1})x^{n-1} + ... + \sigma(a_0),$$

and so $xpx^{-1} - p$ is an element of $I \cap S$ with degree at most $n-1$. The minimality of n implies that $xpx^{-1} - p = 0$, and thus $\sigma(a_i) = a_i$ for all i.

Next, consider an arbitrary element $r \in R$, and note that

$$pr = \sigma^n(r)x^n + a_{n-1}\sigma^{n-1}(r)x^{n-1} + ... + a_0 r$$

$$\sigma^n(r)p = \sigma^n(r)x^n + \sigma^n(r)a_{n-1}x^{n-1} + ... + \sigma^n(r)a_0.$$

Then $pr - \sigma^n(r)p$ is an element of $I \cap S$ with degree at most $n-1$, and so $pr - \sigma^n(r)p = 0$. In particular, it follows that $a_0 r = \sigma^n(r)a_0$. Since this holds for any $r \in R$, we see that $a_0 R \subseteq Ra_0$. On the other hand, taking $r = \sigma^{-n}(r')$ yield $r'a_0 = a_0\sigma^{-n}(r')$ for all $r' \in R$, whence $Ra_0 \subseteq a_0 R$. Therefore $a_0 R = Ra_0$.

Now $a_0 R = Ra_0$ is a nonzero two-sided ideal of R, and it is an α-ideal because $\sigma(a_0) = a_0$. Since R is σ-simple, we find that $a_0 R = Ra_0 = R$, which tells us that a_0 is invertible in R. Consequently, the equations $a_0 r = \sigma^n(r)a_0$ imply that σ^n is an inner automorphism of R. Assumption (b) then forces $n = 0$. But now $p = 1$, and since $p \in I$, we conclude that $I = T$. Therefore T is a simple ring. □

4.4.11 Corollary:

Let k be a field and $q \in k^\times$. Then $\mathcal{O}_{\mathbf{q}}((k^\times)^2)$ is a simple ring if and only if q is not a root of unity.

Proof. Set $T = \mathcal{O}_{\mathbf{q}}((k^\times)^2)$. By Exercise $(1Q)$ of [41], $T = R[x^{\pm}; \sigma]$, where $R = K[y^{\pm 1}]$ and σ is the k-algebra automorphism of R such that

$\sigma(y) = qy$. Since R is commutative, the only inner automorphism of R is the identity.

If q is a root of unity, say $q^n = 1$ for some positive integer n, then σ^n is the identity on R, and so Theorem (4.4.10) shows that T is not simple in this case.

Conversely, assume that q is not a root of unity. Then $\sigma^n(y) = q^n y \neq y$ for all $n > 0$, and so no positive power of σ is inner. It remains to verify condition (a) of Theorem (4.4.10). Thus, let I be a non-zero σ-ideal of R; we must show that $I = R$.

Observe that $I \cap k[y]$ is nonzero, and choose a monic polynomial $f \in I \cap k[y]$ of minimal degree, say $f = y^m + a_{m-1}y^{m-1} + ... + a_0$ for some $m \in \mathbb{Z}^+$ and $a_i \in k$. Since I is a σ-ideal, we also have $\sigma(f) \in I \cap k[y]$. Now

$$\sigma(f) = q^m y^m + q^{m-1}a_{m-1}y^{m-1} + ... + a_0$$

and so $\sigma(f) - q^m f$ is a polynomial in $I \cap k[y]$ with degree at most $m-1$. By the minimality of m, we must have $\sigma(f) - q^m f = 0$, from which it follows that $q^i a_i = q^m a_i$ for all i, that is, $(q^{m-i} - 1)a_i = 0$. Since q is not a root of unity, we conclude that $a_i = 0$ for all $i \neq m$. Consequently, $f = y^m$, which is invertible in R. Therefore $I = R$, as desired. □

Observe that the quantum tori $\mathcal{O}_{\mathbf{q}}((k^\times)^2)$ are never division rings - for instance, $x + 1$ has no inverse in these algebras.

4.5 General Skew Polynomial Rings

The discussion above leads us to try to construct a skew polynomial ring in which the multiplication is twisted by a ring endomorphism and associated skew derivation. Our goal may be defined in parallel with the earlier cases, as follows.

4.5.1 Definition:

Let R be a ring, σ an endomorphism of R and δ a σ-derivation of R. The skew polynomial ring $R[x; \sigma, \delta]$ is the usual set of polynomials over R. We shall write $S = R[x; \sigma, \delta] = \{\sum_{i=0}^{n} x^i a_i : a_i \in R\}$ provided

(a) S is a ring, containing R as a subring;

(b) x is an element of S;

(c) S is a free left R-module with basis $\{1, x, x^2, ...\}$;

(d) $xr = \sigma(r)x + \delta(r)$ for every $r \in R$

Such a ring is called a skew polynomial ring over R, or an Ore extension of R (honoring O. Ore, who first systematically studied the general case).

Skew polynomial ring is also known as Ore-Extension. These rings were introduced by Oystein Ore in (1933). The reader should be warned that some authors prefer their skew polynomial rings to have right-hand coefficients. To achieve this, one starts with a ring R, an endomorphism σ of R, and a right σ-derivation δ on R. The corresponding skew polynomial ring is a free right R-module with a basis $\{1, x, x^2, ...\}$, where $rx = x\sigma(r) + \delta(r)$ for all $r \in R$.

In order to proceed as we did in the cases $R[x; \sigma] = R[x; \sigma, 0]$ and $R[x; \delta] = R[x; id_R, \delta]$, we would need to work out a general formula expressing $x^i r$, for any $i \in \mathbb{N}$ and $r \in R$, as a polynomial with left-hand coefficients. However, this soon gets rather involved - for instance,

$$x^3 r = \sigma^3(r)x^3 + [\delta\sigma^2(r) + \sigma\delta\sigma(r) + \sigma^2\delta(r)]x^2 + [\delta^2\sigma(r) + \delta\sigma\delta(r) + \sigma\delta^2(r)]x + \delta^3(r).$$

Exercise $(2E)$ [41] provides a clue as to how we might proceed. The point of that exercise was to show that any formal differential operator ring $R[x; \delta]$ isomorphic to a ring of actual differential operators on a ring T. If we had not already constructed $R[x; \delta]$, we could proceed to define the ring T and the derivation $\mathfrak{d}$ as in Exercise $2E$ [41], identify R with its image in $End_{\mathbb{Z}}(T)$ (as left multiplication operators), and then check that, the subring of $End_{\mathbb{Z}}(T)$ generated by $R \cup \mathfrak{d}$ is the required skew polynomial ring $R[x; \delta]$. Thus, let us try $R[x; \sigma, \delta]$ as a ring of operators (i.e., additive endomorphisms) of some abelian group. In particular, such a construction will give us the ring axioms for free.
Still anticipating the existence of $S = R[x; \sigma, \delta]$, we observe that S will embed in the additive endomorphism ring $End_{\mathbb{Z}}(S)$ as left multiplication operators. To express elements of R in this fashion only requires us to know the R-module structure of S, and multiplication by x will be given by the rule

$$x(\Sigma_i r_i x^i) = \Sigma_i(\sigma(r_i)x + \delta(r_i))x^i = \Sigma(\sigma(r_i)x^{i+1} + \delta(r_i)x^i).$$

In other words, we can readily express both x and elements of R as operators on the additive group of S, and can then construct S as the ring generated by these operators. To avoid confusion between the two roles S plays here - as abelian group and as skew polynomial ring - it is helpful to rewrite the abelian group $(S, +)$ as a polynomial ring in a new variable, say z.

In case, δ is zero map, then the ring $R[x; \sigma]$ is a skew polynomial ring, where multiplication is subject to the relation $ax = x\sigma(a)$. In case, σ is the identity map, then the ring $D(R) = R[x; \delta]$ is known as ring of differential operators, where multiplication is subject to the relation $ax = xa + \delta(a)$.

4.5.2 Proposition:

[Proposition (2.3) of [41]]. Given a ring R, a ring endomorphism σ of R, and an σ-derivation δ on R, there exists a skew polynomial ring $R[x; \sigma, \delta]$.

Proof. Let $E = End_{\mathbb{Z}}(R[z])$, where $R[z]$ is an ordinary polynomial ring over R. Since $R[z]$ is a left R-module, there is a ring homomorphism $\lambda : R \to E$ sending elements of R to left multiplication operators, that is, $\lambda(r)(p) = rp$ for $r \in R$ and $p \in R[z]$. Clearly, λ is injective (e.g., because $\lambda(r)(1) = r$ for all $r \in R$). Thus, we can identify R with the subring $\lambda(R) \subset E$.

Next,define $x \in E$ according to the rule

$$x(\Sigma_i r_i z^i) = \Sigma_i(\sigma(r_i)z^{i+1} + \delta(r_i)z^i),$$

and let S be the subring of E generated by $R \cup \{x\}$. For any $r \in R$ and any polynomial $p = \Sigma_i r_i z^i$ in $R[z]$, we compute that

$$(xr)(p) = x(\Sigma_i r r_i z^i) = \Sigma_i(\sigma(rr_i)z^{i+1} + \delta(rr_i)z^i)$$

$$= \Sigma_i \sigma(r)\sigma(r_i)z^{i+1} + \Sigma_i(\sigma(r)\delta(r_i) + \delta(r)r_i)z^i$$

$$= \sigma(r)\Sigma_i(\sigma(r_i)z^{i+1} + \delta(r_i)z_i) + \delta(r)\Sigma_i r_i z_i = (\sigma(r)x + \delta(r))(p).$$

Thus $xr = \sigma(r)x + \delta(r)$ for all $r \in R$. In particular, $xR \subseteq Rx + R$.

From the relation $xR \subseteq Rx + R$, it follows by induction that

$$x^i R \subseteq Rx^i + Rx^{i-1} + ... + Rx + R$$

for all $i \in \mathbb{Z}^+$, and consequently $(Rx^i)(Rx^j) \subseteq (Rx^{i+j}) + (Rx^{i+j-1}) + ... + (Rx^j)$ for all $i, j \in \mathbb{Z}^+$. Hence, the set $\Sigma_{i=0}^{\infty} Rx^i$ is a subring of E, and therefore $S = \Sigma_{i=0}^{\infty} Rx^i$. This shows that the set $\{1, x, x^2, ...\}$ generates S as a left R-module. All that remains is to show that this set is left linearly independent over R, so that S will be free left R-module with basis $\{1, x, x^2, ...\}$.

Thus, consider an operator $r_0 + r_1 x + ... + r_n x^n$ in S for some $r_i \in R$. We shall apply this operator to the element $1 = z^0 \in R[z]$. Note that $x(z^j) = z^{j+1}$ for all $j \geq 0$, whence $x^i(1) = z^i$ for all i. Consequently,

$$(r_0 + r_1 x + ... + r_n x^n)(1) = r_0 + r_1 z + ... + r_n z^n$$

and so the operator $r_0 + r_1 x + ... + r_n x^n$ can be the zero map only if the polynomial $r_0 + r_1 z + ... + r_n z^n$ is zero, and that happens only if all the $r_i = 0$. Therefore, the elements $1, x, x^2, ...$ are indeed left linearly independent over R, as required. □

4.5.3 Example:

Let $f = (xa + b)$ and $g = (xc + d) \in R[x]$

Therefore, $f + g = (xa + b) + (xc + d)$
$= xa + b + xc + d$
$= x(a + c) + b + d$

Also, $f.g = (xa + b)(xc + d)$
$= xa.xc + xa.d + b.xc + bd$
$= x(ax)c + xa.d + (bx)c + bd$
$= x(x\sigma(a) + \delta(a))c + xa.d + [x\sigma(b) + \delta(b)]c + bd$
$= x^2\sigma(a)c + x\delta(a)c + xad + x\sigma(b)c + \delta(b)c + bd$
and, $g.f = (xc + d)(xa + b)$
$= xcxa + xcb + dxa + db$
$= x(cx)a + xc.b + (dx)a + db$
$= x[x\sigma(c) + \delta(c)]a + xcb + [x\sigma(d) + \delta(d)]a + db$
$= x^2\sigma(c)a + x\delta(c)a + xcb + x\sigma(d)a + \delta(d)a + db$
Implies $f.g \neq g.f$ for every $f, g \in R[x]$.

4.5.4 Definition:

Let k be a field and $q \in k^x$. We write $A_1^q(k)$ to denote the k-algebra presented by two generators x and y and one relation $xy - qyx = 1$. This algebra is known as a *quantized Weyl algebra* over k. (Quantized Weyl algebras with more pairs of generators have been defined and extensively studied, but we shall not introduce them here). Of course, $A_1^q(k) = A_1(k) = k[y][x; d/dy]$ when $q = 1$. When $q \neq 1$, we obtain the skew polynomial ring given above.

4.5.5 Definition:

Let $R[x; \sigma, \delta]$ be a skew polynomial ring. Any non-zero element p in $R[x; \sigma, \delta]$ can be uniquely expressed in the form

$$p = r_n x^n + r_{n-1} x^{n-1} + ... + r_1 x + r_0$$

for some nonnegative integer n and some elements $r_i \in R$ with $r_n \neq 0$. The integer n is called the degree of p, abbreviated $deg(p)$, and the element r_n is called the leading coefficient of p. (In the differential operator ring case, namely $R[x; \sigma]$, it is common to call n the order of p rather that the degree.) The zero element of $R[x; \sigma, \delta]$ is defined to have degree $-\infty$ and leading coefficient 0.

Strictly speaking, n and r_n should be called the left degree and the left leading coefficient of p, since if p can be written with right-hand coefficients, that is,

$$p = x^m r'_m + x^{m-1} r'_{m-1} + ... + x r'_1 + r'_0$$

for some $r'_i \in R$ with $r'_m \neq 0$ (which is not always possible), it can easily happen that $n \neq m$ or that $r_n \neq r_m$. The Exercise $(2O)$ [41] implies that if $r'_m \in ker(\sigma^m)$, then $n < m$, while if $r'_m \notin ker(\sigma^m)$, then $n = m$ and $r_n = \sigma^n(r'_n)$.

Now let us show the uniqueness of skew polynomial rings $R[x; \sigma, \delta]$. This follows from a universal mapping property exactly parallel to Lemma (4.2.2) and Exercise $(2F)(a)$ [41]. However, the proof of the universal mapping property for $R[x; \sigma, \delta]$ is a bit different because we do not have an explicit formula for products in this ring.

4.5.6 Proposition:

[Proposition (2.4) of [41]]. Let $S = R[x; \sigma, \delta]$ be a skew polynomial ring. Suppose that we have a ring T, a ring homomorphism $\phi : R \to T$, and an element $y \in T$ such that $y\phi(r) = \phi\sigma(r)y + \phi\delta(r)$ for all $r \in R$. Then there is a unique ring homomorphism $\psi : S \to T$ such that $\psi|R = \phi$ and $\psi(x)y$.

Proof. There is well-defined additive map $\psi : S \to T$ given by the rule

$$\psi(\Sigma_i r_i x^i) = \Sigma_i \phi(r_i) y^i$$

with $\psi|R = \phi$ and $\psi(x) = y$. It is clear that this is the only possibility for ψ, and so it is enough to show that ψ is a ring homomorphism.

First observe that if $t = \Sigma_j b_j x^j$ s an arbitrary element of S, then

$$\psi(xt) = \psi(\Sigma_j \sigma(b_j) x^{j+1} + \Sigma_j \delta(b_j) x^j) = \Sigma_j \phi\sigma(b_j) y^{j+1} + \Sigma_j \phi\delta(b_j) y^j$$

$$\Sigma_j (\phi\sigma(b_j)y + \phi\delta(b_j)) y^j = \Sigma_j y\phi(b_j) y^j = y\psi(t).$$

It follows by induction that $\psi(x^i t) = y^i \psi(t)$ for all $i \in \mathbb{Z}^+$ and $t \in S$. Moreover, if $a \in R$, then

$$\psi(at) = \Sigma_j \phi(ab_j) y^j = \Sigma_j \phi(a)\phi(b_j) y^j = \phi(a)\psi(t).$$

Consequently, given any $s = \Sigma_i a_i x^i$ in S, we have

$$\psi(st) = \Sigma_i \psi(a_i x^i t) = \Sigma_i \phi(a_i) \psi(x^i t) = \Sigma_i \phi(a_i) y^i \psi(t) = \psi(s)\psi(t)$$

Therefore ψ is a ring homomorphism. □

4.5.7 Corollary:

[Corollary (2.5) of [41]]. Let R be a ring, σ a ring endomorphism of R, and δ an σ-derivation on R. If $S = R[x; \sigma, \delta]$ and $S' = R[x'; \sigma, \delta]$, there is a unique ring isomorphism $\psi : S \to S'$ such that $\psi(x) = x'$ and $\psi|R$ is the identity map on R.

Proof. As Corollary (4.2.3). □

• A GENERAL SKEW HILBERT BASIS THEOREM •

We now turn to the question whether (or when) $R[x; \sigma, \delta]$ is Noetherian. In our treatment of the case $R[x; \sigma]$ (Theorem (4.4.5)), we made several uses of the hypothesis that σ was an automorphism. In face,

that theorem can fail when σ is not an automorphism, as the following examples show. Consequently, we shall mainly restrict attention to skew polynomial rings $R[x;\sigma,\delta]$ when σ is an automorphism.

4.5.8 Exercises:

[Exercise (2P) of [41]].

(a) Let $R = k[t]$ be a polynomial ring over a field k, and let σ be the k-algebra endomorphism of R given by the rule $\sigma(f(t)) = f(t^2)$. Then $R[x;\sigma]$ is neither right nor left Noetherian.

(b) Now let $R = k[t]$ be the quotient field of $k[t]$ and extend σ to the k-algebra endomorphism of R given by the same rule $\sigma(f(t)) = f(t^2)$. Then $R[x;\sigma]$ is not right Noetherian.

4.5.9 Theorem:

[Theorem (2.6) of [41]]. Let $S = R[x;\sigma,\delta]$, where σ is an automorphism of R. If R is right (left) Noetherian, then so is S.

Proof. In the right Noetherian case, we can follow the same steps as in Theorem (4.4.5), with some help from Exercise $(2O)$ [41] to keep track of leading coefficients. The set equation $R + Rx + ... + Rx^{n-1} = R + xR + ... + X^{n-1}R$ in Step 3 still holds, although a bit more work is needed to check it (Exercise $(2O)$ [41] is helpful there too).

Now suppose that R is left Noetherian. Then R^{op} is right Noetherian, and Exercise $(2R)$ [41] shows that $R[x;\sigma,\delta] = R[x;\sigma^{-1},-\delta\sigma^{-1}]$, where σ^{-1} is viewed as an automorphism of R^{op}. By the case above, $R[x;\sigma,\delta]^{op}$ is right Noetherian, and therefore $R[x;\sigma,\delta]$ is left Noetherian. □

4.6 Skew Polynomial Rings (particular cases)

Let R be a ring and σ an endomorphism of a ring R. Recall that R is said to be a $\sigma(*)$-ring if $a\sigma(a) \in P(R)$ implies $a \in P(R)$ for $a \in R$, where $P(R)$ is the prime radical of R. We also recall that R is said to be a weak σ-rigid ring if $a\sigma(a) \in N(R)$ if and only if $a \in N(R)$ for $a \in R$, where $N(R)$ is the set of nilpotent elements of R. Also recall that when $P(R) = N(R)$, then R is a 2-primal ring.

4.6.1 Theorem:

Let R be a Noetherian $\mathbb{Q}$-algebra. Let σ be an automorphism of R and δ be a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$, for $a \in R$. Then $P \in MinSpec(O(R))$ such that $\sigma(P \cap R) = P \cap R$ implies $P \cap R \in MinSpec(R)$ and $P_1 \in MinSpec(R)$ such that $\sigma(P_1) = P_1$ implies $O(P_1) \in MinSpec(O(R))$.

Proof. Let $P_1 \in MinSpec(R)$ with $\sigma(P_1) = P_1$. Let $T = R[[t, \sigma]]$, the skew power series ring. Now it can be seen that $e^{t\delta}$ is an automorphism of T and $P_1T \in MinSpec(T)$. We also know that $(e^{t\delta})^k(P_1T) \in MinSpec(T)$ for all integers $k \geq 1$. Now T is Noetherian by Exercise $(1ZA(c))$ of [38], and therefore Theorem (2.4) of [38] implies that $MinSpec(T)$ is finite. So exists an integer $n \geq 1$ such that $(e^{t\delta})^n(P_1T) = P_1T$;i.e. $(e^{nt\delta})(P_1T) = P_1T$. But R is a $\mathbb{Q}$-algebra, therefore, $e^{t\delta}(P_1T) = P_1T$. Now for any $a \in P_1$, $a \in P_1T$ also, and so $e^{t\delta}(a) \in P_1T$;i.e. $a + \delta(a) + t\delta(a) + (t^2/2!)\delta^2(a) + ... \in P_1T$, which implies that $\delta(a) \in P_1$. Therefore $\delta(P_1 \subseteq P_1$.

Now it can be easily seen that $O(P_1) \in Spec(O(R))$. Suppose that $O(P_1) \notin MinSpec(O(R))$, and $P_2 \subset O(P_1)$ is a minimal prime ideal of $O(R)$. Then we have $P_2 = O(P_2 \cap R) \subset O(P_1) \in MinSpec(O(R))$. Therefore $P_2 \cap R \subset P_1$, which is a contradiction as $P_2 \cap R \in Spec(R)$. Hence $O(P_1) \in Spec(O(R))$.

Conversely, let $P \in MinSpec(O(R))$ with $\sigma(P \cap R) = P \cap R$. Then it can be easily seen that $P \cap R \in Spec(R)$ and $O(P \cap R) \in Spec(O(R))$. therefore $O(P \cap R) = P$. We now show that $P \cap R \in MinSpec(R)$. Suppose that $P_3 \subset P \cap R$, and $P_3 \in MinSpec(R)$. Then $O(P_3) \subset O(P \cap R) = P$. But $O(P_3) \in Spec(O(R))$ and, $O(P_3 \subset P)$, which is not possible. Thus we have $P \cap R \in MinSpec(R)$. □

4.6.2 Proposition:

Let R be a 2-primal ring. Let σ be an automorphism of R and δ be a σ-derivation of R such that $\delta(P(R)) \subseteq P(R)$. If $P \in MinSpec(R)$ is such that $\sigma(P) = P$, then $\delta(P) \subseteq P$.

Proof. Let $P \in MinSpec(R)$. Now for any $a \in P$ there exists $b \notin P$ such that $ab \in P(R)$ by Corollary(1.10) of [86].

Now $\delta(P(R)) \subseteq P(R)$, and therefore $\delta(ab) \in P(R)$; i.e., $\delta(a)\sigma(b) + a\delta(b) \in P(R) \subseteq P$. Now $a\delta(b) \in P$ implies that $\delta(a)\sigma(b) \in P$. Also $\sigma(P) = P$ and by Proposition (1.11) of [86], P is completely prime, we have $\delta(a) \in P$. Hence $\delta(P) \subseteq P$. □

4.6.3 Theorem:

Let R be a δ-ring. Let σ and δ be as above such that $\delta(P(R)) \subseteq P(R)$. Then R is 2-primal.

Proof. Define a map $\rho : R/P(R) \to R/P(R)$ by $\rho(a + P(R)) = \delta(a) + P(R)$ for $a \in R$ and $\tau : R/P(R) \to R/P(R)$ a map by $\tau(a + P(R)) = \sigma(a) + P(R)$ for $a \in R$, then it is clear that τ is an automorphism of $R/P(R)$ and ρ is a τ-derivation of $R/P(R)$.Now $a\delta(a) \in P(R)$ if and only if $(a+P(R))\rho(a+P(R)) = P(R)$ in $R/P(R)$. Thus as in Proposition(5) of [47], R is a reduced ring and, therefore R is 2-primal. □

4.6.4 Proposition:

Let R be a ring. Let σ and δ be as usual. Then:

(1) For any completely prime ideal P of R with $\delta(P) \subseteq P$, $P[x;\sigma,\delta]$ is a completely prime ideal of $R[x;\sigma,\delta]$.

(2) For any completely prime ideal U of $R[x;\sigma,\delta]$, $U \cap R$ is a completely prime ideal of R.

Proof. (1) Let P be completely prime ideal of R. Now let $f(x) = \sum_{i=0}^{n} x^i a_i \in R[x;\sigma,\delta]$ and $g(x) = \sum_{j=o}^{m} x^j b_j \in R[x;\sigma,\delta]$ be such that $f(x)g(x) \in P[x;\sigma,\delta]$. Suppose $f(x) \notin P[x;\sigma,\delta]$. We will show that $g(x) \in P[x;\sigma,\delta]$. We use induction on n and m. For $n = m = 1$, the verification is easy. We check for $n = 2$ and $m = 1$. Let $f(x) = x^2a + xb + c$ and $g(x) = xu + v$. Now $f(x)g(x) \in P[x;\sigma,\delta]$ with $f(x) \notin P[x;\sigma,\delta]$. The possibilities are $a \notin P$ or $b \notin P$ or $c \notin P$ or any two out of these three do not belong to P or all of them do not belong to P. We verify case by case.

Let $a \notin P$. Since $x^3\sigma(a)u + x^2(\delta(a)u + \sigma(b)u + av) + x(\delta(b)u + \sigma(c)u + bv) + \delta(c)u + cv \in P[x;\sigma,\delta]$, we have $\sigma(a)u \in P$, and so $u \in p$. Now $\delta(a)u + \sigma(b)u + av \in P$ implies $av \in P$ and so $v \in P$. Therefore $g(x) \in P[x;\sigma,\delta]$.

Let $b \notin P$. Now $\sigma(a)u \in P$. Suppose $u \notin P$, then $\sigma(a) \in P$ and therefore $a, \delta(a) \in P$. Now $\delta(a)u + \sigma(b)u + av \in P$ implies that $\sigma(b)u \in P$ which in turn implies that $b \in P$, which is not the case. Therefore we have $u \in P$. Now $\delta(b)u+\sigma(c)u+bv \in P$ implies that $bv \in P$ and therefore $v \in P$. Thus we have $g(x) \in P[x; \sigma, \delta]$.

Let $c \notin P$. Now $\sigma(a)u \in P$. Suppose $u \notin P$, then as above $a, \delta(a) \in P$. Now $\delta(a)u+\sigma(b)u+av \in P$ implies that $\sigma(b)u \in P$. Now $u \notin P$ implies that $\sigma(b) \in P$; i.e., $b, \delta(b) \in P$. Also $\delta(b)u+\sigma(c)u+bv \in P$ implies $\sigma(c) \in P$ and therefore $\sigma(c) \in P$ which is not the case. Thus we have $u \in P$. Now $\delta(c)u + cv \in P$ implies $cv \in P$, and so $v \in P$. Therefore $g(x) \in P[x; \sigma, \delta]$.

Now suppose the result is true for k, $n = k > 2$ and $m = 1$. We will prove for $n = k + 1$. Let $f(x) = x^{k+1}a_{k+1} + x^k a_k + ... + xa_1 + a_0$, and $g(x) = xb_1 + b_0$ be such that $f(x)g(x) \in P[x; \sigma, \delta]$, but $f(x) \notin P[x; \sigma, \delta]$. We will show that $g(x) \in P[x; \sigma, \delta]$. If $a_{k+1} \notin P$, then equating coefficients of x^{k+2}, we get $\sigma(a_{k+1})b_1 \in P$, which implies that $b_1 \in P$. Now equating coefficients of x^{k+1}, we get $\sigma(a_k)b_1 + a_{k+1}b_0 \in P$, which implies that $a_{k+1}b_0 \in P$, and therefore $b_0 \in P$. Hence $g(x) \in P[x; \sigma, \delta]$.

If $a_j \notin P$, $0 \leq j \leq k$, then using induction hypothesis, we get that $g(x) \in P[x; \sigma, \delta]$. Therefore the statement is true for all n. Now using the same process, it can be easily seen that the statement is true for all m also.

(2) Let U be a completely prime ideal of $R[x; \sigma, \delta]$. Suppose a, $b \in R$ are such that $ab \in U \cap R$ with $a \notin U \cap R$. This means that $a \notin U$ as $a \in R$. Thus we have $ab \in U \cap R \subseteq U$, with $a \notin U$. Therefore we have $b \in U$, and thus $b \in U \cap R$.

□

4.6.5 Corollary:

Let R be a δ-ring, where σ and δ be as usual such that $\delta(P(R)) \subseteq P(R)$. Let $P \in MinSpec(R)$ be such that $\sigma(P) = P$. Then $P[x; \sigma, \delta]$ is a completely prime ideal of $R[x; \sigma, \delta]$.

Proof. R is 2-primal by Theorem(4.6.3) and so by Proposition (4.6.2) $\delta(P) \subseteq P$. Further more P is completely prime ideal by Proposition(1.11) of [53]. Now by Proposition(4.6.4) the result is obvious. □

4.6.6 Theorem:

Let R be a δ-ring, where σ and δ be as usual such that $\delta(P(R)) \subseteq P(R)$ and $\sigma(P) = P$ for all $P \in MinSpec(R)$. Then $R[x;\sigma,\delta]$ is 2-primal if and only if $P(R)[x;\sigma,\delta] = P(R[x;\sigma,\delta])$.

Proof. Let $R[x;\sigma,\delta]$ be 2-primal. Now by Corollary (4.6.5) $P(R[x;\sigma,\delta]) \subseteq P(R)[x;\sigma,\delta]$. Let $f(x) = \sum_{j=0}^{n} x^j a_j \in P(R)[x;\sigma,\delta]$. Now R is a 2-primal subring of $R[x;\sigma,\delta]$ by Theorem (4.6.3), which implies that a_j is nilpotent and thus $a_j \in N(R[x;\sigma,\delta]) = P(R[x;\sigma,\delta])$, and so we have $x^j a_j \in P(R[x;\sigma,\delta])$ for each j, $0 \leq j \leq n$, which implies that $f(x) \in P(R[x;\sigma,\delta])$. Hence $P(R)[x;\sigma,\delta] = P(R[x;\sigma,\delta])$.

Conversely, suppose $P(R)[x;\sigma,\delta] = P(R[x;\sigma,\delta])$. We will show that $R[x;\sigma,\delta]$ is 2-primal. Let $g(x) = \sum_{i=0}^{n} x^i b_i \in R[x;\sigma,\delta]$, be such that $(g(x))^2 \in P(R[x;\sigma,\delta]) = P(R)[x;\sigma,\delta]$. We will show that $g(x) \in P(R[x;\sigma,\delta])$. Now leading coefficient $\sigma^{2n-1}(b_n)b_n \in P(R) \subseteq P$, for all $P \in MinSpec(R)$. Now $\sigma(P) = P$ and P is completely prime by Proposition (1.11) of [53]. Therefore we have $b_n \in P$, for all $P \in MinSpec(R)$; i.e., $b_n \in P(R)$. Now since $\delta(P(R)) \subseteq P(R)$ and $\sigma(P) = P$ for all $P \in MinSpec(R)$, we get $(\sum_{i=0}^{n-1} x^i b_i)^2 \in P(R[x;\sigma,\delta]) = P(R)[x;\sigma,\delta]$ and as above we get $b_{n-1} \in P(R)$. With the same process in a finite number of steps we get $b_i \in P(R)$ for all i, $0 \leq i \leq n$. Thus we have $(g(x)) \in P(R)[x;\sigma,\delta]$;i.e. $(g(x)) \in P(R[x;\sigma,\delta])$. Therefore $P(R[x;\sigma,\delta])$ is completely semiprime. Hence $R[x;\sigma,\delta]$ is 2-primal. □

4.6.7 Theorem:

Let R be a δ-Noetherian $\mathbb{Q}$-algebra such that $\sigma(\delta(a)) = \delta(\sigma(a))$, for all $a \in R$; $\sigma(P) = P$ for all $P \in MinSpec(R)$ and $\delta(P(R)) = P(R)$, where σ and δ are as usual. Then $R[x,\sigma,\delta]$ is 2-primal.

Proof. We use Theorem (4.6.2) to get that $P(R)[x,\sigma,\delta] = P(R[x,\sigma,\delta])$ and now the result is obvious by using Theorem (4.6.5). □

4.6.8 Corollary:

Let R be a commutative δ-Noetherian $\mathbb{Q}$-algebra such that $\sigma(\delta(a)) = \delta(\sigma(a))$, for all $a \in R$; $\sigma(P) = P$ for all $P \in MinSpec(R)$, where σ and δ are as usual. Then $R[x, \sigma, \delta]$ is 2-primal.

Proof. Using Theorem (1) of [84] we get $\delta(P(R)) = P(R)$. Now rest is obvious. □

Now we give a relation between a $\sigma(*)$-ring and a weak σ-rigid ring. We also give a necessary and sufficient condition for a Noetherian ring to be a weak σ-rigid ring.

4.6.9 Proposition:

[Proposition (1) of [14]]. Let R be a ring and σ an automorphism of R. Then R is a $\sigma(*)$-ring implies $P(R)$ is completely semiprime.

Proof. See Proposition (4.1.13). □

4.6.10 Proposition:

[Proposition (2) of [14]]. Let R be a Noetherian ring and σ an automorphism of R. Then R is a $\sigma(*)$-ring implies that R is 2-primal.

Proof. By Proposition (4.6.9) $P(R)$ is completely semiprime. Therefore, R is 2-primal. □

4.6.11 Theorem:

Let R be a Noetherian ring, and σ an automorphism of R. Then R is a $\sigma(*)$-ring if and only if for each minimal prime U of R, $\sigma(U) = U$ and U is completely prime ideal of R.

Proof. Let R be a Noetherian ring such that for each minimal prime U of R, $\sigma(U) = U$ and U is completely prime ideal of R. Let $a \in R$ be such that $a\sigma(a) \in P(R) = \cap_{i=1}^{n} U_i$, where U_i are the minimal primes of R. Now for each $i, a \in U_i$ or $\sigma(a) \in U_i$ as U_i are completely prime. Now $\sigma(a) \in Ui = \sigma(Ui)$ implies that $a \in U_i$. Therefore $a \in P(R)$. Hence R is a $\sigma(*)$-ring.

Conversely, suppose that R is a $\sigma(*)$-ring and let $U = U_1$ be a minimal prime ideal of R. Now by Proposition (4.6.9), $P(R)$ is completely

semiprime. Let $U_2, U_3, ..., U_n$ be the other minimal primes of R. Suppose that $\sigma(U) \neq U$. Then $\sigma(U)$ is also a minimal prime ideal of R. Renumber so that $\sigma(U) = U_n$. Let $a \cap_{i=1}^{n-1} U_i$. Then $\sigma(a) \in U_n$, and so $a\sigma(a) \in \cap_{i=1}^{n} U_i = P(R)$. Therefore $a \in P(R)$, and thus $\cap_{i=1}^{n-1} \subseteq U_n$, which implies that $U_i \subseteq U_n$ for some $i \neq n$, which is impossible. Hence $\sigma(U) = U$.

Now suppose that $U = U_1$ is not completely prime. Then there exist $a, b \in R$ U with $ab \in U$. Let c be any element of $b(U_2 \cap U_3 \cap ... \cap U_n)a$. Then $c^2 \in \cap_{i=1}^{n} U_i = P(R)$. So $c \in P(R)$ and, thus $b(U_2 \cap U_3 \cap ... \cap U_n)a \subseteq U$. Therefore $bR(U_2 \cap U_3 \cap ... \cap U_n)Ra \subseteq U$ and, as U is prime, $a \in U, U_i \subseteq U$ for some $i \neq 1$ or $b \in U$. None of these can occur, so U is completely prime. □

4.6.12 Proposition:

[Proposition (3) of [14]]. Let R be a Noetherian ring which is also an algebra over $\mathbb{Q}$. Let σ be an automorphism of R such that R is a $\sigma(*)$-ring and δ a σ-derivation of R. Then $\delta(U) \subseteq U$ for all $U \in MinSpec(R)$.

Proof. We note that Proposition (4.6.9) implies that $P(R)$ is completely semiprime. Let $U \in MinSpec(R)$. Then Theorem (4.6.11) implies that $\sigma(U) = U$.

Let now $T = \{a \in U \mid \text{such that } \delta^k(a) \in U \text{ for all integers } k \geq 1\}$. First of all, we will show that T is an ideal of R. Let $a, b \in T$. Then $\delta^k(a) \in U$ and $\delta^k(b) \in U$ for all integers $k \geq 1$. Now $\delta^k(a - b) = \delta^k(a) - \delta^k(b) \in U$ for all $k \geq 1$. Therefore $a - b \in T$. Therefore T is a δ-invariant ideal of R.

We will now show that $T \in Spec(R)$. Suppose $T \notin Spec(R)$. Let $a \notin T, b \notin T$ be such that $aRb \subseteq T$. Let t, s be least such that $\delta^t(a) \notin U$ and $\delta^s(b) \notin U$. Now there exists $c \in R$ such that $\delta^t(a)c\sigma^t(\delta^s(b)) \notin U$. Let $d = \sigma^{-t}(c)$. Now $\delta^{t+s}(adb) \in U$ as $aRb \subseteq T$. This implies on simplification that $\delta^t(a)\delta^t(d)\sigma^t(\delta^s(b)) + u \in U$, where u is sum of terms involving $\delta^l(a)$ or $\delta m(b)$, where $l < t$ and $m < s$. Therefore by assumption $u \in U$ which implies that $\delta^t(a)\sigma^t(d)\sigma^t(\delta^s(b)) \in U$. This is a contradiction. Therefore, our supposition must be wrong. Hence $T \in Spec(R)$. Now $T \subseteq U$, so $T = U$ as $U \in MinSpec(R)$. Hence $\delta(U) \subseteq U$. □

4.6.13 Proposition:

[Proposition (4) of [14]]. Let R be a Noetherian ring which is also an algebra over $\mathbb{Q}$. Let σ be an automorphism of R such that R is a $\sigma(*)$-ring. Then $U \in MinSpec(R)$ implies that $UO(R) = U[x;\sigma,\delta]$ is a completely prime ideal of $O(R) = R[x;\sigma,\delta]$.

Proof. Proposition (4.6.9) implies that $P(R)$ is completely semiprime ideal of R. Let $U \in MinSpec(R)$. Then Theorem (4.6.11) implies that $\sigma(U) = U$ and U is completely prime. Also by Proposition (4.6.12) $\delta(U) \subseteq U$. Now Theorem (4.6.4) implies that $UO(R) = U[x;\sigma,\delta]$ is a completely prime ideal of $O(R) = R[x;\sigma,\delta]$. □

4.6.14 Theorem:

[Theorem (5) of [14]]. Let R be a Noetherian ring. Let σ be an automorphism of R such that R is a $\sigma(*)$-ring. Then R is a weak σ-rigid ring. Conversely a 2-primal weak σ-rigid ring is a $\sigma(*)$-ring.

Proof. Let σ be an automorphism of R such that R is a $\sigma(*)$-ring. Now Proposition (4.6.10) implies that R is 2-primal, i.e., $N(R) = P(R)$. Thus $a\sigma(a) \in N(R) = P(R)$ implies that $a \in P(R) = N(R)$. Hence R is weak σ-rigid ring.

Conversely let R be 2-primal weak σ-rigid ring. Then $N(R) = P(R)$ and $a\sigma(a) \in N(R)$ implies that $a \in N(R)$. Therefore, $a\sigma(a) \in P(R)$ implies that $a \in P(R)$. Hence R is a $\sigma(*)$-ring. □

4.6.15 Theorem:

[Theorem (6) of [14]]. Let R be a commutative Noetherian ring. Let σ be an automorphism of R. Then R is a weak σ-rigid ring implies that $N(R)$ is completely semiprime.

Proof. First of all we show that $\sigma(N(R)) = N(R)$. We have $\sigma(N(R) \subseteq N(R)$ as $\sigma(N(R))$ is a nilpotent ideal of R. Now for any $n \in N(R)$, there exists $a \in R$ such that $n = \sigma(a)$. So

$$I = \sigma^{-1}(N(R)) = \{a \in R \text{ such that } \sigma(a) = n \in N(R)\}$$

is an ideal of R. Now I is nilpotent, therefore $I \subseteq N(R)$, which implies that $N(R) \subseteq \sigma(N(R))$. Hence $\sigma(N(R)) = N(R)$.

Now let R be a weak σ-rigid ring. We will show that $N(R)$ is completely semiprime. Let $a \in R$ be such that $a^2 \in N(R)$. Then $a\sigma(a)\sigma(a\sigma(a)) = a\sigma(a)\sigma(a)\sigma^2(a) \in \sigma(N(R)) = N(R)$. Therefore $a\sigma(a) \in N(R)$ and hence $a \in N(R)$. So $N(R)$ is completely semiprime. □

4.6.16 Corollary:

[Corollary (1) of [14]]. Let R be a commutative Noetherian ring. Let σ be an automorphism of R. Then R is a 2-primal weak σ-rigid ring if and only if for each minimal prime U of R, $\sigma(U) = U$ and U is completely prime ideal of R.

Proof. Combine Theorem (4.6.11) and Theorem (4.6.15). □

4.6.17 Proposition:

[Proposition (5) of [14]]. Let R be a commutative Noetherian ring. Let σ be an automorphism of R such that R is a $\sigma(*)$-ring. Then $O(N(R)) = N(O(R))$.

Proof. Proposition (4.6.10) implies that R is 2-primal. Now it is easy to see that $O(N(R)) \subseteq N(O(R))$. We will show that $N(O(R)) \subseteq O(N(R))$. Let $f = \Sigma_{i=0}^{m} x^i a_i \in N(O(R))$. Then $(f)(O(R)) \subseteq N(O(R))$, and $(f)(R) \subseteq N(O(R))$. Let $((f)(R))k = 0, k > 0$. Then equating leading term to zero, we get

$$(x^m a_m R)^k = 0.$$

After simplification equating leading term to zero, we get

$$x^{km}\sigma^{(k-1)m}(a_m R).\sigma^{(k-2)m}(a_m R).\sigma^{(k-3)m}(a_m R)...a_m R = 0.$$

Therefore

$$\sigma^{(k-1)m}(a_m R).\sigma^{(k-2)m}(a_m R).\sigma^{(k-3)m}(a_m R)...a_m R = 0 \subseteq P,$$

for all $P \in MinSpec(R)$.This implies that $\sigma^{(k-j)m}(a_m R) \subseteq P$, for some $j, 1 \leq j \leq k$. Therefore, $a_m R \subseteq \sigma^{-(k-j)m}(P)$. But $\sigma^{-(k-j)m}(P) = P$ by Theorem (4.6.11). So we have $a_m R \subseteq P$, for all $P \in Min.Spec(R)$. Therefore, $a_m \in P(R)$, and R being 2-primal implies that $a_m \in N(R)$. Now $x^m a_m \in O(N(R)) \subseteq N(O(R))$ implies that $\Sigma_{i=0}^{m-1} x^i a_i \in N(O(R))$, and with the same process, in a finite number of steps, it can be seen that $a_i \in P(R) = N(R)$, $0 \leq i \leq m-1$. Therefore $f \in O(N(R))$. Hence $N(O(R)) \subseteq O(N(R))$ and the result. □

We note that if σ is an endomorphism of a ring R and δ a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$. Then σ can be extended to an endomorphism (say $\overline{\sigma}$) of $R[x;\sigma,\delta]$ by

$$\overline{\sigma}(\Sigma_{i=0}^{m} x^i a_i) = \Sigma_{i=0}^{m} x^i \sigma(a_i).$$

Also δ can be extended to a $\overline{\sigma}$-derivation (say $\overline{\delta}$) of $R[x;\sigma,\delta]$ by

$$\overline{\delta}(\Sigma_{i=0}^{m} x^i a_i) = \Sigma_{i=0}^{m} x^i \delta(a_i).$$

We now prove the following:

4.6.18 Theorem:

[Theorem (7) of [14]]. Let R be a 2-primal commutative Noetherian ring. Let σ be an automorphism of R and δ a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$. Then R is a weak σ-rigid ring implies that $O(R) = R[x;\sigma,\delta]$ is a weak $\overline{\sigma}$-rigid ring.

Proof. Let R be a weak σ-rigid ring. Then Theorem (4.6.14) implies that R is a $\sigma(*)$-ring. Also Proposition (4.6.17) implies that $O(N(R)) = N(O(R))$. We show that $R[x;\sigma,\delta]$ is a weak $\overline{\sigma}$-rigid ring.

Let $f \in O(R)$ (say $f = \Sigma_{i=0}^{m} x^i a_i$) be such that $f\overline{\sigma}(f) \in N(O(R))$. We use induction on m to prove the result. For $m = 1$, $f = xa_1 + a_0$. Now $f\overline{\sigma}(f) \in N(O(R))$ implies that $(xa_1 + a_0)(x\sigma(a_1) + \sigma(a_0)) \in N(O(R)) = O(N(R))$, i.e.,

$$x^2\sigma^2(a_1) + x\delta(a_1)\sigma(a_1) + x\sigma(a_0)\sigma(a_1) + \delta(a_0)\sigma(a_1) + xa_1\sigma(a_0) + a_0\sigma(a_0) \in O(N(R)) \quad (4.1)$$

Therefore, $\sigma^2(a_1) \in N(R)$. Now $\sigma(N(R)) = N(R)$ implies that $\sigma^i(a_1) \in N(R)$ for all $i \geq 1$. So (1) implies that $a_0\sigma(a_0) \in N(R)$, and R being a weak σ-rigid ring implies that $a_0 \in N(R)$. Therefore, $f \in O(N(R)) = N(O(R))$.

Suppose the result is true for $m = k$. We prove for $m = k + 1$. Now $f\overline{\sigma}(f) \in N(O(R))$ implies that

$$(x^{k+1}a_{k+1} + ... + a_0)(x^{k+1}\sigma(a_{k+1}) + ... + \sigma(a_0)) \in N(O(R)) = O(N(R)),$$

i.e.,

$$x^{2k+2}\sigma^{k+2}(a_{k+1}) + x^{2k+1}(\sigma^k(a_{k+1})\sigma(a_k) + \sigma^{k+1}(a_k)\sigma(a_{k+1})) + g\overline{\sigma}(g)$$

$$\in O(N(R)),$$

where$g = \Sigma_{i=0}^{k} x^i a_i$. Therefore, $\sigma^{k+2}(a_{k+1}) \in N(R)$ implies that $a_{k+1} \in N(R)$. Also $\sigma^k(a_{k+1})\sigma(a_k) + \sigma^{k+1}(a_k)\sigma(a_{k+1}) \in N(R)$ implies that $g\overline{\sigma}(g) \in N(O(R))$, but degree of g is k, therefore, by induction hypothesis, the result is true for all m. □

4.6.19 Corollary:

Let R be a Noetherian $\sigma(*)$-ring, where σ is an automorphism of R. Then $P \in MinSpec(S(R))$ if and only if there exists $Q \in MinSpec(R)$ such that $S(Q) = P$ and $(P \cap R) = Q$.

Proof. R is a Noetherian $\sigma(*)$-ring, therefore $U^0 = U$ for any $U \in MinSpec(R)$ by Theorem (4.6.11). Now use Theorem (2.4) of [9]. □

4.6.20 Corollary:

Let R be a Noetherian $\sigma(*)$-ring, where σ is an automorphism of R. Then $P(R)[x;\sigma] = P(R[x;\sigma])$.

4.6.21 Theorem:

Let R be a Noetherian $\sigma(*)$-ring, where σ is an automorphism of R. Then $R[x;\sigma]$ is also a Noetherian $\sigma(*)$-ring.

Proof. $R[x;\sigma]$ is Noetherian by Hilbert Basis Theorem (Theorem (1.12) of Goodearl and Warfield [38]). Now we have $P(R)[x;\sigma] = P(R[x;\sigma])$ by Corollary (4.6.20). Let $f(x) = \Sigma_{i=0}^{n} x^i a_i \in R[x;\sigma]$ be such that $f(x)\sigma(f(x)) \in P(R[x;\sigma]) = P(R)[x;\sigma]$; i.e.

$$(x^n a_n + ... + a_0)(x^n\sigma(a_n) + ... + \sigma(a_0)) \in P(R)[x;\sigma],$$

or

$$x^{2n}\sigma^n(a_n)\sigma(a_n) + ... + a_0\sigma(a_0) \in P(R)[x;\sigma],$$

which implies that $a_0\sigma(a_0) \in P(R)$, and therefore $a_0 \in P(R)$, as R is a $\sigma(*)$-ring.

Therefore $g(x)\sigma(g(x)) \in P(R)[x;\sigma]$, where $g(x) = \sigma_{i=1}^{n} x^i a_i$. With the same process as above, in a finite number of steps, we get that $a_i \in P(R)$ for all $i, 1 \leq i \leq n$. Thus $f(x) \in P(R)[x;\sigma] = P(R[x;\sigma])$. Hence $R[x;\sigma]$ is also a Noetherian $\sigma(*)$-ring. □

4.6.22 Proposition:

Let R be a Noetherian $\mathbb{Q}$-algebra, σ an automorphism and δ a σ-derivation of R. Then $e^{t\delta}$ is an automorphism of $T = R[[t, \sigma]]$, the skew power series ring.

Proof. The proof is on the same lines as in Seidenberg [84] and in the noncommutative case on the same lines as provided by Blair and Small in [18]. □

4.6.23 Lemma:

Let R be a Noetherian $\mathbb{Q}$-algebra, σ an automorphism and δ a σ-derivation of R. Then an ideal I of R is δ-invariant if and only if TI is $e^{t\delta}$-invariant.

Proof. Let TI be $e^{t\delta}$-invariant. Let $a \in I$. Then $a \in TI$. So $e^{t\delta}(a) \in TI$; i.e. $a + t\delta(a) + (t^2\delta^2/2!)(a) + ... \in TI$. Therefore $\delta(a) \in I$.

Conversely suppose that $\delta(I) \subseteq I$ and let $f = \Sigma t^i a_i \in TI$. Then $e^{t\delta}(f) = f + t\delta(f) + (t^2\delta^2/2!)(f) + ... \in TI$, as $\delta(a_i) \in I$. Therefore $e^{t\delta}(TI) \subseteq TI$. Replacing $e^{t\delta}$ by $e^{-t\delta}$, we get that $e^{t\delta}(TI) = TI$. □

Let σ be an automorphism of a ring R, and I be an ideal of R such that $\sigma(I) = I$. Then it is easy to see that $TI \subseteq IT$ and $IT \subseteq TI$. Hence $TI = IT$ is ideal of T.

4.6.24 Proposition:

Let R be a Noetherian $\sigma(*)$-ring and T as usual. Then:

(1) $U \in MinSpec(R)$ implies that $UT \in MinSpec(T)$.

(2) $P \in MinSpec(T)$ implies that $P \cap R \in MinSpec(R)$ and $P = (P \cap R)T$.

Proof. (1) Let $U \in MinSpec(R)$. Then $\sigma(U) = U$ by Theorem 4.6.11. Now $UT \in Spec(T)$. Suppose $UT \notin MinSpec(T)$ and $J \subset UT$ is a minimal Prime ideal of T. Then $(J \cap R) \subset UT \cap R = U$ which is a contradiction, as $(J \cap R) \in Spec(R)$. Therefore $UT \in Min.Spec(T)$.

(2) Let $P \in MinSpec(T)$. Then $P \cap R \in Spec(R)$. Suppose $(P \cap R) \notin MinSpec(R)$ and $M \subset P \cap R$ is a minimal prime ideal of R. Then $MT \subset (P \cap R)T \subseteq P$, which is a contradiction, as $MT \in Spec(R)$. Therefore $(P \cap R) \in MinSpec(R)$. Now it is easy to see that $(P \cap R)T = P$. □

4.6.25 Proposition:

Let R be a Noetherian $\sigma(*)$-ring which is also an algebra over $\mathbb{Q}$, where σ is an automorphism of R and δ a σ-derivation of R. Then $P \in MinSpec(R)$ implies $\delta(P) \subseteq P$.

Proof. Let T be as usual. Now by Proposition (4.6.22) $e^{t\delta}$ is an automorphism of T. Let $P \in MinSpec(R))$. Then by Proposition (4.6.24) $PT \in MinSpec(T)$.Therefore there exists an integer $n \geq 1$ such that $(e^{t\delta})^n(PT) = PT$;i.e. $(e^{nt\delta})(PT) = PT$. But R is a $\mathbb{Q}$-algebra, therefore, $e^{t\delta}(PT) = PT$ and now Lemma (4.6.23) implies $\delta(P) \subseteq P$. □

4.6.26 Proposition:

Let R be a $\sigma(*)$-ring, which is also an algebra over $\mathbb{Q}$ and σ is an automorphism of R. Let $U \in MinSpec(R)$. Then $U(O(R)) = U[x; \sigma, \delta]$ is a completely prime ideal of $O(R) = R[x; \sigma, \delta]$, where δ a σ-derivation of R.

Proof. Let $U \in MinSpec(R)$. Then $\sigma(U) = U$ by Theorem (4.6.11), and $\delta(U) \subseteq U$ by Proposition (4.6.25). Now R is 2-primal by Proposition (4.1.13) and furthermore U is completely prime by Theorem (4.6.11). Now we note that σ can be extended to an automorphism $\overline{\sigma}$ of R/U and δ can be extended to a $\overline{\sigma}$-derivation $\overline{\delta}$ of R/U. Now it is well known that $O(R)/U(O(R)) \simeq (R/U)[x; \overline{\sigma}, \overline{\delta}]$ and hence $U(O(R))$ is a completely prime ideal of $O(R)$. □

4.6.27 Theorem:

Let R be a Noetherian $\sigma(*)$-ring, which is also an algebra over $\mathbb{Q}$ and σ is an automorphism of R. Let δ be a σ-derivation of R. Then $P \in MinSpec(O(R))$ implies that $P \cap R \in MinSpec(R)$, and conversely $P_1 \in MinSpec(R)$ implies that $O(P_1) \in Min.Spec(O(R)$.

Proof. Let $P_1 \in MinSpec(R)$. Then $\sigma(P_1) = P_1$ by Theorem (4.2.8), and $\delta(P_1) \subseteq P_1$ by Proposition (4.6.25). Now it can be seen that $O(P_1) \in Spec(O(R))$. Suppose that $O(P_1) \notin MinSpec(O(R))$, and $P_2 \subset O(P_1)$ is a minimal prime ideal of $O(R)$. Then we have $P_2 = O(P_2 \cap R) \subset O(P_1) \in MinSpec(O(R))$. Therefore $P_2 \cap R \subset P_1$, which is a contradiction as $P_2 \cap R \in Spec(R)$. Hence $O(P_1) \in Spec(O(R))$.

Conversely, let $P \in MinSpec(O(R))$ with $\sigma(P \cap R) = P \cap R$. Then it can be easily seen that $P \cap R \in Spec(R)$ and $O(P \cap R) \in Spec(O(R))$. therefore $O(P \cap R) = P$. We now show that $P \cap R \in MinSpec(R)$. Suppose that $P_3 \subset P \cap R$, and $P_3 \in MinSpec(R)$. Then $O(P_3) \subset O(P \cap R) = P$. But $O(P_3) \in Spec(O(R))$ and, $O(P_3 \subset P)$, which is not possible. Thus we have $P \cap R \in MinSpec(R)$. □

4.6.28 Corollary:

Let R be a Noetherian $\sigma(*)$-ring, which is also an algebra over $\mathbb{Q}$ and σ is an automorphism of R. Let δ be a σ-derivation of R. Then $P(R[x;\sigma,\delta]) = P(R)[x;\sigma,\delta]$.

4.6.29 Theorem:

Let R be a Noetherian $\sigma(*)$-ring, which is also an algebra over $\mathbb{Q}$ and σ is an automorphism of R. Let δ be a σ-derivation of R. Then $R[x;\sigma,\delta]$ is 2-primal if and only$P(R[x;\sigma,\delta]) = P(R)[x;\sigma,\delta]$.

Proof. Let $R[x;\sigma,\delta]$ be 2-primal. Now by Proposition (4.6.26) $P(R[x;\sigma,\delta]) \subseteq P(R)[x;\sigma,\delta]$. Let $f(x) = \sum_{j=0}^{n} x^j a_j \in P(R)[x;\sigma,\delta]$. Now R is a 2-primal subring of $R[x;\sigma,\delta]$ by Proposition (4.1.13), which implies that a_j is nilpotent and thus $a_j \in N(R[x;\sigma,\delta]) = P(R[x;\sigma,\delta])$, and so we have $x^j a_j \in P(R[x;\sigma,\delta])$ for each j, $0 \leq j \leq n$, which implies that $f(x) \in P(R[x;\sigma,\delta])$. Hence $P(R)[x;\sigma,\delta] = P(R[x;\sigma,\delta])$.

Conversely, suppose $P(R)[x;\sigma,\delta] = P(R[x;\sigma,\delta])$. We will show that $R[x;\sigma,\delta]$ is 2-primal. Let $g(x) = \sum_{i=0}^{n} x^i b_i \in R[x;\sigma,\delta]$, be such that $(g(x))^2 \in P(R[x;\sigma,\delta]) = P(R)[x;\sigma,\delta]$. We will show that $g(x) \in P(R[x;\sigma,\delta])$. Now leading coefficient $\sigma^{2n-1}(b_n)b_n \in P(R) \subseteq P$, for all $P \in MinSpec(R)$. Now $\sigma(P) = P$ and P is completely prime by Theorem (4.6.11). Therefore we have $b_n \in P$, for all $P \in MinSpec(R)$; i.e., $b_n \in P(R)$. Now $\delta(P(R)) \subseteq P(R)$ for all $P \in MinSpec(R)$ by Proposition (4.6.25), we get $(\sum_{i=0}^{n-1} x^i b_i)^2 \in P(R[x;\sigma,\delta]) = P(R)[x;\sigma,\delta]$ and as above we get $b_{n-1} \in P(R)$. With the same process in a finite number of steps we get $b_i \in P(R)$ for all i, $0 \leq i \leq n$. Thus we have $(g(x)) \in P(R)[x;\sigma,\delta]$; i.e., $(g(x)) \in P(R[x;\sigma,\delta])$. Therefore $P(R[x;\sigma,\delta])$ is completely semiprime. Hence $R[x;\sigma,\delta]$ is 2-primal. □

4.6.30 Theorem:

Let R be a Noetherian $\sigma(*)$-ring, which is also an algebra over $\mathbb{Q}$ and σ is an automorphism of R. Let δ be a σ-derivation of R. Then $R[x;\sigma,\delta]$ is 2-primal Noetherian.

Proof. $R[x;\sigma,\delta]$ is Noetherian by Hilbert Basis Theorem (Theorem (1.12) of Goodearl and Warfield [38]). We now use Theorem (4.6.27) to get that, $P(R)[x;\sigma,\delta] = P(R[x;\sigma,\delta])$ and the result now follows from Theorem (4.6.28). □

The following example shows that if R is a Noetherian ring, then $R[x;\sigma,\delta]$ need not be 2-primal.

4.6.31 Example:

Let $R = \mathbb{Q} \oplus \mathbb{Q}$ with $\sigma(a,b) = (b,a)$. Then the only σ-invariant ideals of R are 0 and R and, so R is σ-prime. Let $\sigma : R \to R$ be defined by $\sigma(r) = ra - a\sigma(r)$, where $a = (0,\alpha) \in R$. Then δ is a σ-derivation of R and $R[x;\sigma,\delta]$ is prime and $P(R[x;\sigma,\delta]) = 0$. But $(x(1,0))^2 = 0$ as $\delta(1,0) = -(0,\alpha)$. Therefore $R[x;\sigma,\delta]$ is not 2-primal. If δ is taken to be the zero map, then even $R[x;\sigma]$ is not 2-primal.

The following example shows that if R is a Noetherian ring , then even $R[x]$ need not be 2-primal.

4.6.32 Example:

Let $R = M_2(\mathbb{Q})$, the set of 2×2 matrices over $\mathbb{Q}$. Then $R[x]$ is a prime ring with non-zero nilpotent elements and, so can not be 2-primal.

4.6.33 Theorem:

Let R be a Noetherian ring and σ an automorphism of R. Then:

(1) If $P \in MinSpec(S)$, then $P = (P \cap R)S$ and there exists $U \in MinSpec(R)$ such that $P \cap R = U^0$.

(2) If $U \in MinSpec(R)$, then $U^0S \in MinSpec(S)$.

Proof. (1) Let $P \in Min.Spec(S)$. Then $x \notin P$, as it is not a zero-divisor, therefore $P \cap R$ is a σ-prime ideal of R and $(P \cap R)S$ is a prime ideal of S by Lemma $(10.6.4)(ii,iii)$ and Proposition (10.6.12) of [68]. Hence $P = (P \cap R)S$. Now $(P \cap R)S$ is prime, so it the intersection $\cap_{i=1}^{n} U_i$ of

the primes that are minimal over it and these form a single orbit under σ. Therefore $P \cap R = U_i^0$ for each i. Let B be a minimal prime ideal of R with $B \subseteq U_i$. Then B^0 is σ-prime and $B^0 \subseteq U_i^0 = P \cap R$. Therefore B^0S is a prime ideal contained in $P = (P \cap R)S$. So $B^0S = (P \cap R)S$ and, hence $B^0 = P \cap R$.

(2) Let $U \in MinSpec(R)$. Then U^0 is σ-prime and U^0S is a prime ideal of S by Proposition (10.6.12) of [68]. Now it must contain a minimal prime ideal P of S (Proposition (2.3) of [38]). Now by paragraph (1) above $P = (P \cap R)S$ and $P \cap R = B^0$ for some $B \in MinSpec(R)$. Therefore $B^0S \subseteq U^0S$ and $B^0 \subseteq U^0$. So $\sigma^i(B) \subseteq U$ for some i and therefore $\sigma^i(B) = U$ by the minimality of U. Hence $B^0 = U^0$ and $U^0S = P$ is minimal. □

4.6.34 Proposition:

Let R be a $\sigma(*)$-ring and $U \in MinSpec(R)$ be such that $\sigma(U) = U$. Then $US = U[x;\sigma]$ is a completely prime ideal of $S = R[x;\sigma]$.

Proof. R is 2-primal by Proposition (4.1.13) and further more U is completely prime by Proposition (1.11) of Shin [86]. Now we note that σ can be extended to an automorphism $\overline{\sigma}$ of R/U. Now it is well known that $S/US \simeq (R/U)[x;\overline{\sigma}]$ and hence US is a completely prime ideal of S. □

4.6.35 Theorem:

Let R be a Noetherian $\sigma(*)$-ring, σ an automorphism of R. Then $R[x;\sigma]$ is 2-primal if and only if $P(R)[x;\sigma] = P(R[x;\sigma])$.

Proof. Let $R[x;\sigma]$ be 2-primal. Now by Proposition (4.6.34) $P(R[x;\sigma]) \subseteq P(R)[x;\sigma]$. Let $f(x) = \sum_{j=0}^{n} x^j a_j \in P(R)[x;\sigma]$. Now R is a 2-primal subring of $R[x;\sigma]$ by Proposition (4.1.13), which implies that a_j is nilpotent and thus $a_j \in N(R[x;\sigma]) = P(R[x;\sigma])$, and so we have $x^j a_j \in P(R[x;\sigma])$ for each j, $0 \leq j \leq n$, which implies that $f(x) \in P(R[x;\sigma])$. Hence $P(R)[x;\sigma] = P(R[x;\sigma])$.

Conversely, suppose $P(R)[x;\sigma] = P(R[x;\sigma])$. We will show that $R[x;\sigma]$ is 2-primal. Let $g(x) = \sum_{i=0}^{n} x^i b_i \in R[x;\sigma]$, be such that $(g(x))^2 \in P(R[x;\sigma]) = P(R)[x;\sigma]$. We will show that $g(x) \in P(R[x;\sigma])$. Now leading coefficient $\sigma^{2n-1}(b_n)b_n \in P(R) \subseteq P$, for all $P \in MinSpec(R)$. Now $\sigma(P) = P$ and P is completely prime by Proposition (1.11) of [86].

Therefore we have $b_n \in P$, for all $P \in MinSpec(R)$;i.e. $b_n \in P(R)$. Now since $\sigma(P) = P$ for all $P \in MinSpec(R)$ by , we get $(\sum_{i=0}^{n-1} x^i b_i)^2 \in P(R[x;\sigma]) = P(R)[x;\sigma]$ and as above we get $b_{n-1} \in P(R)$. With the same process in a finite number of steps we get $b_i \in P(R)$ for all i, $0 \leq i \leq n$. Thus we have $(g(x)) \in P(R)[x;\sigma]$;i.e. $(g(x)) \in P(R[x;\sigma])$. Therefore $P(R[x;\sigma])$ is completely semiprime. Hence $R[x;\sigma]$ is 2-primal. □

4.6.36 Theorem:

Let R be a Noetherian $\sigma(*)$-ring. Then $R[x;\sigma]$ is 2-primal.

Proof. We use Theorem (4.6.33) to get that $P(R)[x;\sigma] = P(R[x;\sigma])$, and now the result is obvious by using Theorem (4.6.35). □

4.6.37 Proposition:

Let R be a Noetherian $\mathbb{Q}$-algebra, σ an automorphism and δ a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$. Then $e^{t\delta}$ is an automorphism of $T = R[[t,\sigma]]$, the skew power series ring.

Proof. The proof is on the same lines as in Seidenberg [84] and in the noncommutative case on the same lines as provided by Blair and Small in [18]. □

4.6.38 Lemma:

Let R be a Noetherian $\mathbb{Q}$-algebra, σ an automorphism and δ a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$. Let I be an ideal of R such that $\sigma(I) = I$. Then I is δ-invariant if and only if IT is $e^{t\delta}$-invariant.

Proof. Let IT be $e^{t\delta}$-invariant. Let $a \in I$. Then $a \in IT$. So $e^{t\delta}(a) \in IT$; i.e. $a + t\delta(a) + (t^2\delta^2/2!)(a) + ... \in IT$. Therefore $\delta(a) \in I$.

Conversely, suppose that $\delta(I) \subseteq I$ and let $f = \Sigma t^i a_i \in IT$. Then $e^{t\delta}(f) = f + t\delta(f) + (t^2\delta^2/2!)(f) + ... \in IT$, as $\delta(a_i) \in I$. Therefore $e^{t\delta}(IT) \subseteq IT$. Replacing $e^{t\delta}$ by $e^{-t\delta}$, we get that $e^{t\delta}(IT) = IT$. □

Assumption: Henceforth we assume that R is a ring and T as usual such that for any $U \in MinSpec(R)$ with $\sigma(U) = U$, $UT \in MinSpec(T)$.

4.6.39 Proposition:

Let R be a Noetherian $\mathbb{Q}$-algebra. Let σ be an automorphism of R and δ a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$. Then $P \in MinSpec(R)$ with $\sigma(P) = P$ implies $\delta(P) \subseteq P$.

Proof. Let T be as usual. Now by Proposition (4.6.37) $e^{t\delta}$ is an automorphism of T. Let $P \in MinSpec(R))$. Then by assumption $PT \in MinSpec(T)$.Therefore there exists an integer $n \geq 1$ such that $(e^{t\delta})^n(PT) = PT$;i.e. $(e^{nt\delta})(PT) = PT$. But R is a $\mathbb{Q}$-algebra, therefore, $e^{t\delta}(PT) = PT$ and now Lemma (4.6.38) implies $\delta(P) \subseteq P$. □

4.6.40 Proposition:

Let R be a $\sigma(*)$-ring, which is also an algebra over $\mathbb{Q}$ and $U \in MinSpec(R)$. Then $U(O(R)) = U[x;\sigma,\delta]$ is a completely prime ideal of $O(R) = R[x;\sigma,\delta]$, where δ a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$.

Proof. Let $U \in MinSpec(R)$. Then $\sigma(U) = U$ by Theorem (4.6.11), and $\delta(U) \subseteq U$ by Proposition (4.6.39). Now R is 2-primal by Proposition (4.1.13) and furthermore U is completely prime by Theorem (4.6.11). Now we note that σ can be extended to an automorphism $\overline{\sigma}$ of R/U and δ can be extended to a $\overline{\sigma}$-derivation $\overline{\delta}$ of R/U. Now it is well known that $O(R)/U(O(R)) \simeq (R/U)[x;\overline{\sigma},\overline{\delta}]$ and hence $U(O(R))$ is a completely prime ideal of $O(R)$. □

4.6.41 Theorem:

Let R be a Noetherian $\mathbb{Q}$-algebra. Consider $O(R)$ as usual such that Let R be a $\sigma(*)$-ring and $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$. Then $P_1 \in MinSpec(R)$ with $\sigma(P_1) = P_1$ implies that $O(P_1) \in MinSpec(O(R)$.

Proof. Let $P_1 \in MinSpec(R)$. Then by Theorem (4.2.8) $\sigma(P_1) = P_1$, and by Proposition (4.6.39) $\delta(P_1) \subseteq P_1$. Now Proposition (3.3) of [39] implies that $O(P_1) \in Spec(O(R))$. Suppose $O(P_1) \notin MinSpec(O(R))$, and $P_2 \subset O(P_1)$ is a minimal prime ideal of $O(R)$. Then $P_2 = O(P_2 \cap R) \subset O(P_1) \in MinSpec(O(R))$. Therefore $P_2 \cap R \subset P_1$, which is a contradiction as $P_2 \cap R \in Spec(R)$. Hence $O(P_1) \in Spec(O(R))$.

Conversely, let $P \in MinSpec(O(R))$ with $\sigma(P \cap R) = P \cap R$. Then it can be easily seen that $P \cap R \in Spec(R)$ and $O(P \cap R) \in Spec(O(R))$.

therefore $O(P \cap R) = P$. We now show that $P \cap R \in MinSpec(R)$. Suppose that $P_3 \subset P \cap R$, and $P_3 \in MinSpec(R)$. Then $O(P_3) \subset O(P \cap R) = P$. But $O(P_3) \in Spec(O(R))$ and, $O(P_3 \subset P)$, which is not possible. Thus we have $P \cap R \in MinSpec(R)$. □

4.6.42 Theorem:

Let R be a Noetherian $\sigma(*)$-ring, which is also an algebra over $\mathbb{Q}$, σ an automorphism of R and δ a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$. Then $R[x; \sigma, \delta]$ is 2-primal if and only $P(R[x; \sigma, \delta]) = P(R)[x; \sigma, \delta]$.

Proof. Let $R[x; \sigma, \delta]$ be 2-primal. Now by Proposition (4.6.40) $P(R[x; \sigma, \delta]) \subseteq P(R)[x; \sigma, \delta]$. Let

$$f(x) = \sum_{j=0}^{n} x^j a_j \in P(R)[x; \sigma, \delta].$$

Now R is a 2-primal subring of $R[x; \sigma, \delta]$ by Proposition (4.1.13), which implies that a_j is nilpotent and thus

$$a_j \in N(R[x; \sigma, \delta]) = P(R[x; \sigma, \delta]),$$

and so we have $x^j a_j \in P(R[x; \sigma, \delta])$ for each j, $0 \leq j \leq n$, which implies that $f(x) \in P(R[x; \sigma, \delta])$. Hence $P(R)[x; \sigma, \delta] = P(R[x; \sigma, \delta])$.

Conversely, suppose that $P(R)[x; \sigma, \delta] = P(R[x; \sigma, \delta])$. We will show that $R[x; \sigma, \delta]$ is 2-primal. Let

$$g(x) = \sum_{i=0}^{n} x^i b_i \in R[x; \sigma, \delta], b_n \neq 0$$

be such that

$$(g(x))^2 \in P(R[x; \sigma, \delta]) = P(R)[x; \sigma, \delta].$$

We will show that $g(x) \in P(R[x; \sigma, \delta])$. Now leading coefficient $\sigma^{2n-1}(b_n)b_n \in P(R) \subseteq P$, for all $P \in MinSpec(R)$. Also $\sigma(P) = P$ and P is completely prime by Theorem (4.6.11). Therefore we have $b_n \in P$, for all $P \in MinSpec(R)$; i.e., $b_n \in P(R)$. Now $\delta(P(R)) \subseteq P(R)$ for all $P \in MinSpec(R)$ by Proposition (4.6.39), we get

$$(\sum_{i=0}^{n-1} x^i b_i)^2 \in P(R[x; \sigma, \delta]) = P(R)[x; \sigma, \delta]$$

and as above we get $b_{n-1} \in P(R)$. With the same process in a finite number of steps we get $b_i \in P(R)$ for all i, $0 \leq i \leq n$. Thus we have $(g(x)) \in P(R)[x;\sigma,\delta]$; i.e., $(g(x)) \in P(R[x;\sigma,\delta])$. Therefore $P(R[x;\sigma,\delta])$ is completely semiprime. Hence $R[x;\sigma,\delta]$ is 2-primal. □

4.6.43 Theorem:

Let R be a Noetherian, which is also an algebra over $\mathbb{Q}$. Let σ be an automorphism of R such that R is $\sigma(*)$-ring and δ a σ-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$ for all $a \in R$. Then $O(R) = R[x;\sigma,\delta]$ is 2-primal Noetherian.

Proof. $R[x;\sigma,\delta]$ is Noetherian by Hilbert Basis Theorem (Theorem (1.12) of Goodearl and Warfield [38]). We now use Theorem (4.6.41) to get that, $P(R)[x;\sigma,\delta] = P(R[x;\sigma,\delta])$ and the result now follows from Theorem (4.6.42). □

Chapter

5

PRIMARY DECOMPOSITION

The classical theory of primary decomposition due to Emmy Noether plays an important role in the study of commutative Noetherian rings (see for example Reid [79] or Sharp [85]). Generalizing this concept to the noncommutative case we have a primary decomposition theory which was first considered by Gordon in [43]. This approach reduces to the classical case when the ring is commutative and seems to be particularly useful. Unfortunately not all Noetherian rings admit such a decomposition as an example of Brown [[22], Example (6.4)] shows. However many reasonable classes of rings do. Gordon in [[43], Corollary (2.4)] shows that every right fully bounded right Noetherian ring has a right primary decomposition, and Jategaonkar [[50], Theorem (8.3.9)] proves the same result for Noetherian rings with the second layer condition. In this chapter we present a straight forward generalization of these results for both right and two sided Noetherian rings. Explicitly, it is shown that if the right associated prime ideals satisfy a version of the second layer condition, such rings must have a right primary decomposition (Theorem (5.3.2), Theorem (5.3.9)).

Investigation into the existence of primary decomposition of rings has largely taken place within a Noetherian setting (as an exception to this there are a couple of results in Nastasescu [72]). In this, there are some non-Noetherian cases also. It is shown that if the right associated prime ideals are minimal then both right Goldie rings, and rings with right Krull dimension, do have a right primary decomposition Theorem (5.7.3) and Proposition (5.7.4)). In this chapter, there are relationship between primary decomposition in rings and their quotient rings, for example, that a right primary decomposition is inherited by a right order in a right Noetherian quotient ring that has a right primary decomposition Theorem (5.8.7).

5.1 Associated Prime Ideals

All rings are associative with an identity element. All modules are unitary. If I is a right ideal of a ring R we may use the notation $I \lhd_r R$. For a two-sided ideal we write $I \lhd R$.

Let M_R be a right R-module and let X be a subset of M. The *(right) annihilator* of X in R is the right ideal $Ann(X) = \{r \in R \mid Xr = 0\}$. Similarly $l_M(Y) = \{m \in M \mid mY = 0\}$ is the annihilator of a subset Y of R in M.

5.1.1 Definition:

A submodule $N \subseteq M$ is *essential* in M, denoted $N \subseteq_{ess} M$, if N has non-zero intersection with all non-zero submodules of M.

For instance, $\mathbb{Z} \subseteq_{ess} \mathbb{Q}$. Given a prime integer p and a positive integer n, all nonzero submodules of $\mathbb{Z}/p^n\mathbb{Z}$ are essential. At the other extreme, the only essential submodules (subspace) of a vector space V is V itself.

5.1.2 Note:

(1) If I is an ideal of a ring R then $\mathcal{C}'(I) = \{c \in R \mid cx \in I$ implies that $x \in I\}$. Similarly $\mathcal{C} = \{c \in R \mid xc \in I$ implies that $x \in I\}$. The set of elements of elements that are *regular modulo* I is $\mathcal{C}(I) = \mathcal{C}(I) \cap \mathcal{C}'(I)$.

(2) A ring Q is called a *quotient ring* if every regular element of Q is invertible. Given a quotient ring Q, a subring R is called a right order in Q (or Q is said to be the right quotient ring of R) if each $q \in Q$ has the form rc^{-1} for some $r, c \in R$ with $c \in \mathcal{C}(0)$. Let $\mathcal{S}$ be a multiplicatively closed subset of a ring R. We say that $\mathcal{S}$ is a *right Ore set* if for any given $a \in R$ and $c \in \mathcal{S}$ there exist $b \in R$ and $d \in \mathcal{S}$ such that $ad = cb$. A ring R has a right quotient ring if and only if $\mathcal{S} = \mathcal{C}(0)$ is a right Ore set.

5.1.3 Annihilator prime:

An annihilator prime for right module m over a ring R is any prime ideal P of R which equals the annihilator of some non - zero submodule of M.

$Ann_M(P)$ is clearly non - zero and is a faithful (R/P)-module.

5.1.4 Associated prime:

A prime ideal P of a ring R is an *associated prime* of a right module M_R if there exists a non-zero submodule $N \subseteq M$ such that $P = r(N')$ for all non-zero submodules $N' \subseteq N$. The set of associated prime ideals of a Noetherian ring R (viewed as a right R-module over itself) is denoted by $Ass(R_R)$. We note that any ideal which is maximal among the annihilators of non-zero submodules of a module M is an associated prime of M.

Proposition (1.7.26) shows that any ideal maximal among the annihilators of non zero submodules of a right module A is an associated prime of A. Not every associated prime arises on a maximal annihilator, however. For instance, the $\mathbb{Z}$-module $\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})$ has two associated primes, 0 and $2\mathbb{Z}$, and 0 is certainly not maximal among the annihilators of nonzero submodules of this module. And the module A over the ring $\mathbb{Z}$, which is the direct sum of the cyclic modules $\mathbb{Z}/p\mathbb{Z}$ for all primes p is an example of a module whose annihilator is the prime ideal 0 but for which 0 is not an associated prime.

Over the ring $\mathbb{Z}$, the module A which is the direct sum of the cyclic modules $\mathbb{Z}/p\mathbb{Z}$ for all primes p is an example of a module whose annihilator is the prime ideal 0 but for which 0 is not an associated prime.

5.1.5 Remarks:

(1) If B is a submodule of a module A,then

$Ass(B_R) \subseteq Ass(A_R)$ and $Ass(A_R) \subseteq Ass(B_R) \cup Ass((A/B)_R)$.

(2) If every non zero submodule of A has a non zero intersection with B,then $Ass(A_R) = Ass(B_R)$.

5.1.6 Definition:

A right R-module M is called primary if it has a unique associated prime. In this case $Ass(M) = \{P\}$ we say that M is *P-primary.* A P-primary module M is called *P-prime* if $Ass(M_R) = P = Ann(M)$. It is easy to show that U_R is a uniform right module such that $Ass(U_R) \neq \phi$ then U is primary. Also it is well known (see for example Stenstrom [89], (7.1.2), (7.1.3)) that $Ass(N_R) \subseteq Ass(M_R)$ for any submodule $N \subseteq M$

and $Ass((\bigoplus_{i\in I} M_i)_R) = \bigcup_{i\in I} Ass((M_i)_R)$ for any right R-modules M_i and non-empty set I.

5.1.7 Definition:

A module M_R has a *primary decomposition* if it has finitely many submodules $N_1, ..., N_m$ such that $\bigcap_{i=1}^m N_i = 0$ and each $(M/N_i)_R$ is a primary module.

5.1.8 Definition:

A *right Goldie ring* is any ring R such that R_R has finite rank and R has the ascending chain condition on right annihilators.

For example, every right Noetherian ring is right Goldie. (Goodearl and Warfield [38])

5.1.9 Definition:

A ring R is called *right primary* if the module R_R is primary. We say a ring R has a *right primary decomposition* if there exist a finite number of ideals $T_1, ..., T_n$ in R such that $\bigcap_{i=1}^n T_i = 0$ and $(R/T_i)_R$ is a primary module for each i.

5.1.10 Definition:

Let R be a ring with a prime ideal P such that R/P is a right Goldie ring. Let U be a uniform P-primary right R-module. Then U is called *P-tame*, or simply *tame*, if $l_U(P)$ is torsion free as a right R/P-module. A right R-module is *tame* if all its uniform submodules are tame. A module M_R has a *tame decomposition* if it has a primary decomposition *right tame decomposition* if it has a right primary decomposition $\bigcap_{i=1}^n T_i = 0$, where each T_i is an ideal of R and each $(R/T_i)_R$ is a tame module.

5.1.11 Definition:

Let P and Q be prime ideals of a ring R. We say that Q is a *right linked* to P *(via A)*, denoted by $Q \rightsquigarrow P$, if there exist s an ideal A with $QP \subseteq A \subsetneqq Q \cap P$, such that $Q \cap P/A$ is torsion free as a right R/P-module and fully faithful as a left R/Q-module. A set of prime ideals X is said to be *right link closed* if $P \in X$ and $Q \rightsquigarrow P$ implies that $Q \in X$.

5.1.12 Definition:

The *right clique, or right link closure*, of a prime ideal P, denoted $\Omega^r(P)$, consists of P along with those $Q \in Spec(R)$ for which there exists a finite sequence $Q = P_1, ..., P_n = P$ of prime ideals with $P_i \rightsquigarrow P_{i+1}$ for each i. For a set $X \subseteq Spec(R)$ we use the notation $\Omega_r(X) = \bigcup_{P \in X} \Omega^r(P)$. A set X of prime ideals is said to satisfy the *incomparability condition* if for P, $Q \in X$ such that $P \in Q$ we must have $P = Q$.

5.1.13 Definition

A right R-module M is said to be *finitely annihilated* if there exist elements $m_1, ..., m_n \in M$ such that $Ann(M) = \bigcap_{i=1}^{n} Ann(m_i)$. We say M is a Δ-module if R satisfies the descending chain condition (d.c.c) on right annihilators of subsets of M. We note that if M is finitely annihilated then $(R/Ann(M))_R$ embeds in a finite direct sum of copies of M.

5.1.14 The Second Layer condition

Throughout the chapter there are a number of different variations of the definition of the second layer condition. This presents a confusing picture. To try to avoid this we will use the naming system as in Kim and Krause [54]. The following definition of the strong second layer condition was introduced by Jategaonkar [[50], pp.220].

A prime ideal P of a right Noetherian ring R satisfies the *right strong second layer condition* if for every prime ideal $Q \subsetneqq P$, every finitely generated P/Q-primary right R/Q-module is unfaithful over R/Q.

A prime ideal P of a right Noetherian ring R satisfies the *right restricted strong second layer condition* if for every prime $Q \subsetneqq P$, every finitely generated P/Q-tame right R/Q-module is unfaithful over R/Q.

A set X of prime ideals of R satisfies the *right (restricted) strong second layer condition* if every $P \in X$ does so. The ring R satisfies the *right (restricted) strong second layer condition* if $Spec(R)$ does. The *left (restricted) strong second layer condition* we mean both the left and right versions hold. For a P-tame right R-module M, We call $M/l_M(P)$ the *second layer* of M.

A prime ideal P in a right Noetherian ring R is said to satisfy the *right second layer condition* if every uniform module in the second layer of $E_R(R/P)$, the injective envelope of $(R/P)_R$ is tame.

Let P be a prime ideal of a right Noetherian ring. If P satisfies the right restricted strong second layer condition it satisfies the right second layer condition (Kim and Krause [54], Proposition (5.4)(i)). The converse does not hold as [Goodearl and Warfield [38], Exercise (11M)] shows. Now, we have the following results:

5.1.15 Proposition:

[Kim and Krause [54], Corollary (5.6)]. A right Noetherian ring satisfies the right restricted strong second layer condition if and only if it satisfies the right second layer condition.

5.1.16 Theorem:

[Kim and Krause [54], Theorem (4.2)]. Let R be a right Noetherian ring and P be a prime ideal of R with the right restricted strong second layer condition. Then any finitely generated P-tame right R-module is a Δ-module.

5.1.17 Assassinator primes:

If U is a uniform right module over a right Noetherian ring R, the unique associated prime of U is called the *assassinator of* U and is denoted by $Assas(U_R)$.

5.1.18 Lemma:

Let P be a prime ideal in a right Noetherian ring R, and let U be a uniform right ideal of R/P. Then $E(U_R)$ is a uniform injective right R-module, and its assassinator is P.

Proof. See Lemma (5.27) of [40]. □

5.2 Primary Decomposition of Modules

The following is an important characterization of primary modules:

5.2.1 Lemma:

Let P be a prime ideal of a ring R and let M_R be a non-zero module. Suppose that R has the property that every non -zero submodule of M has at least one associated prime. Then M is P-primary if and only if $l_M(P) \subseteq_{ess} M$ and P contains every ideal that annihilates a non-zero submodule of M.

Proof. Let M be P-primary and take any non-zero submodule $K \subseteq M$. There exists a non-zero submodule $K' \subseteq K$ such that $Ann(K') = Q$ where $Q \in Ass(K_R)$. Now $Ass(K_R) \subseteq Ass(M_R)$ and so $Q = P$. Hence $L = l_M(P)$ must be essential in M. Suppose P does not contain every ideal that annihilates a non-zero submodule of M. Let $I = Ann(N), 0 \neq N \subseteq M$ be such that $I \nsubseteq P$. We have $N \cap L \neq 0$ as L is essential in M, so replace N by $N \cap L$ and we may assume $I \supsetneqq P$. However there exists $Q \supseteq I$, where $Q \in Ass(N_R)$. Hence $Q \in Ass(M_R) = \{P\}$ and $I \subseteq P$.

For the converse note that $l_M(P) \subseteq_{ess} M$ we have P contained in every associated prime of M. We see that P contains every associated prime by the second part of the statement. □

5.2.2 Lemma:

Let M_R be a right R-module, and let $0 = N_1 \cap ... \cap N_n$ be a primary decomposition of M_R where the intersection is irredundant. Then $\bigcup_{i=1}^{n} Ass((M/N_i)_R) = Ass(M_R)$.

Proof. Suppose $(M/N_1)_R$ is P_1-primary. Set $\hat{N}_1 = N_2 \cap ... \cap N_n$ and note that this is non-zero. Now $(\hat{N}_1)_R$ embeds as a submodule of $(M/N_1)_R$. Thus $(\hat{N}_1)_R$ is P_1-primary. As $\hat{N}_1 \subseteq M_R$, we then have $P_1 \in Ass(M_R)$. Similarly $P_i \in Ass(M_R)$ for each i.

For the converse we note that as M embeds in $M/N_1 \oplus ... \oplus M/N_n$. We see that $Ass(M_R) \subseteq Ass(\bigoplus_{i=1}^{n}(M/N_i)_R) = \bigcup_{i=1}^{n} Ass((M/N_i)_R)$. □

5.2.3 Lemma:

Any module M_R with finite uniform dimension has a finite number of submodules $V_1, ..., V_n$ such that each M/V_i is uniform and $\bigcap_{i=1}^{n} V_i = 0$. Furthermore if we assume prime factor rings of R are right Goldie and M_R is also a tame module then each factor M/V_i is P_i-tame for some prime ideal $P_i \in Ass(M_R)$.

Proof. Choose a uniform submodule U_1 of M. By Zorn's lemma we can choose a submodule V_1 of M such that V_1 is maximal with respect to the property $U_1 \cap V_1 = 0$. Now U_1 embeds into $(M/V_1)_R$ and by maximality of V_1 we have M/V_1 uniform since U_1 is isomorphic to an essential submodule of it.

If $V_1 = 0$ then M is uniform and we are done. If $V_1 \neq 0$ there exists a uniform module $U_2 \subseteq V_1$. As before choose V_2 maximal with respect to $U_2 \cap V_2 = 0$. Now, $(U_1 + U_2) \cap (V_1 \cap V_2) = 0$ for otherwise there exists a nonzero element $u_1 + u_2 \in V_1 \cap V_2$, where $u_i \in U_i$. As $u_2 \in U_2 \subseteq V_1$ then $u_1 = (u_1 + u_2) - u_2 \in V_1$. Hence $u_1 \in U_1 \cap V_1 = 0$. Now $u_2 \in V_2$ and we have $u_2 = 0$.

As before U_2 is isomorphic to an essential submodule of M/V_2 and therefore M/V_2 is uniform. Hence if $V_1 \cap V_2 = 0$ we are done. Otherwise take a uniform module $U_3 \subseteq V_1 \cap V_2$ and choose V_3 maximal with respect to $U_3 \cap V_3 = 0$. Hence M/V_3 is uniform and similar to before $(U_1 + U_2 + U_3) \cap (V_1 \cap V_2 \cap V_3) = 0$.

We continue in this way and note that this process must stop because the sum $U_1 + ... + U_m$ is direct. Hence $V_1 \cap ... \cap V_n = 0$ for some n.

If M is a tame module then all of its uniform submodules are tame. Therefore U_i is P_i-tame for some prime ideal $P_i \in Ass(M_R)$. Let $L_i = l_{U_i}(P_i)$. Then L_i is isomorphic to a submodule $L_i^{'}$ of M/V_i. As $l_{M/V_i}(P_i)$ is an essential extension $L_i^{'}$ and essential extensions of torsion free modules are torsion free, we conclude that M/V_i is P_i-tame. □

This lemma is enough to give us a primary decomposition of a finite dimensional module over a ring which has the property that uniform modules are primary. In the next section we will use the primary decomposition of the module R_R to get a primary decomposition of the ring R.

5.3 Primary Decomposition in Noetherian Rings

5.3.1 Proposition:

[Kim and Krause [54], Proposition (3.1)]. Let R be a right Noetherian ring. Suppose a prime ideal P satisfies the right strong second layer

condition. If M is a finitely generated P-primary right R-module then the direct product M^I is P-primary for any non-empty set I.

Proof. Let M_R be finitely generated P-primary and suppose $Q \in Ass((M^I)_R)$. Choose $n = (n_i)_{i\in I} \in M^I$ such that $Q = Ann(nR)$. Now $Q = \bigcap_{i\in I} Ann(n_iR) = Ann(\sum_{i\in I} n_iR)$. Since M is Noetherian, $N = \sum_{i\in I} n_iR) \subseteq M$ is finitely generated P-primary. We must have $Q \subseteq P$, and N is a faithful R/Q-module. Since P satisfies the right strong second layer condition $Q = P$.
Note that this property is a characterization of primes with the right strong second layer condition (see Kim and Krause [54]). □

5.3.2 Theorem:

Let R be a right Noetherian ring and suppose the set $Ass(R_R)$ satisfies the right strong second layer condition. Then R has a right primary decomposition.

Proof. See Theorem (3.4.2) in Convington [28]. □

5.3.3 Corollary:

Any right Noetherian ring with the right strong second layer condition has a right primary decomposition.

5.3.4 Corollary:

[Gordon [43], Corollary (2.4)]. Let R be a right Noetherian ring fully bounded ring. Then R has a right primary decomposition.

Proof. Right fully bounded right Noetherian rings satisfy the right strong second layer condition. □

5.3.5 Corollary:

[Krause [55], Theorem (3.5) and Remark]. Let R be a right Noetherian ring such that $Ass(R_R) \subseteq MinSpec(R)$. Then R has a right primary decomposition.

Proof. Follows as minimal primes satisfy the strong second layer condition. □

5.3.6 Example:

Let $S = A_1(\mathbb{C})$ be the 1st Weyl Algebra over the complex numbers. Consider the following ring which is right but not left Noetherian and is not right fully bounded,

$$R = \begin{pmatrix} \mathbb{C} & S \\ 0 & S \end{pmatrix}.$$

The only prime ideals of R are

$$P = \begin{pmatrix} \mathbb{C} & S \\ 0 & 0 \end{pmatrix} \text{ and } P' = \begin{pmatrix} \mathbb{C} & S \\ 0 & S \end{pmatrix}.$$

so R satisfies the right strong second layer condition and therefore must have a primary decomposition. Indeed R is right P-primary.

We now take the left and right Noetherian case.

5.3.7 Proposition:

[Kim and Krause [54], Proposition (4.1)]. Let R be a right Noetherian ring. Suppose a prime ideal P satisfies the right restricted strong second layer condition. If M is a finitely generated P-tame right R-module then the direct product M_I is P-tame for any non-empty set I.

Proof. Firstly note that M_I is P-primary by a similar method to Proposition (5.3.1) Suppose that there exists a P-prime submodule xR of M_I that is torsion over the ring R/P. Then $Ann(x)/P$ is an essential right ideal of R/P. If $x = (m_i)_{i\in I}$, then $r(x) = \bigcap_{i\in I} Ann(m_i)$, so each $Ann(m_i)/P$ is essential as a right ideal of R/P. Similarly $Ann(m_i a)/P \subseteq_{ess} R/P$ for any $a \in R$. Thus $m_i R$ is a P-prime $\mathcal{C}(P)$-torsion submodule of M. This is impossible as M is assumed to be P-tame. □

5.3.8 Proposition:

Suppose R is a right Noetherian ring in which all ideals are finitely annihilated on the right. Then there exists an irredundant intersection $0 = \bigcap_{i=1}^{n} I_i$ of right ideals of R such that each R/I_i is a P_i-tame right module for some $P_i \in Ass(R_R)$.

Proof. It is straightforward to show that right ideals are also finitely annihilated on the right. Therefore if U is a uniform right ideal of R we have a P-prime submodule $V = l_U(P)$. As V is finitely annihilated $V_{R/P}$ must be torsion free. Hence U and therefore R_R is tame. The result now follows by Lemma (5.2.3). □

5.3.9 Theorem:

Let R be a right Noetherian ring in which ideals are finitely annihilated on the right. Suppose the set $Ass(R_R)$ satisfies the right restricted strong second layer condition. Then R has a right tame decomposition.

Proof. See Proposition (3.4.10) in Convington [28]. □

In particular ideals are finitely annihilated on the right in a left and right Noetherian ring. The following corollary is due to Jategaonkar.

5.3.10 Theorem:

[Jategaonkar [50], Theorem (8.3.9)]. Any Noetherian ring with the right second layer condition has a right primary decomposition.

Proof. Use Proposition (5.1.15) along with Theorem (5.3.9). □

5.4 Krull dimension

To discuss primary decomposition of non-Noetherian rings, we need the following:

5.4.1 Definition:

Let R be a ring and let M be a right R-module. The *Krull dimension* (named after Wolfgang Krull) of M, denoted by $k(M)$, if it exists, is defined as follows, $k(M) = -1$ if and only if $M = 0$. If $\alpha \geq 0$ is an ordinal such that all modules with Krull dimension strictly less than α are known, then $k(M) \leq \alpha$ if for every chain $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq ...$ of submodules of M there is a positive integer n such that $k(M_i/M_{i+1}) < \alpha$ for all $i \geq n$.

Note that $k(M) = 0$ if and only if M is nonzero Artinian. In this sense, the Krull dimension of a module can be thought of as a measure of how far the module is from being Artinian. It is interesting, however,

that many properties of modules with Krull dimension are similar (or identical) to those of Noetherian modules.

5.4.2 Definition:

A ring R is said to have *right Krull dimension* if the right R-module R_R has Krull dimension and is denoted by $r.k(R)$.

5.4.3 Lemma:

Let R be a ring, let M be a right R-module and let N be a submodule of M. Then $k(M) = sup\{k(M/N), k(N)\}$ if either exists.

Proof. See (McConnell and Robson [68], Lemma (6.2.4)). □

5.4.4 Corollary:

Let R be a ring with right Krull dimension and let M be a finitely generated right R-module. Then M has Krull dimension and $k(M) \leq r.k(R)$

Proof. This follows by repeated applications of Lemma (5.4.3). □

5.4.5 Lemma:

Let R be a ring and let M be a Noetherian right R-module. Then M has Krull dimension.

Proof. Suppose that the result is false. Using the Noetherian property we may assume that all proper factor modules of M have Krull dimension. Let

$$\alpha = \sup \{k(M/N) \mid N \text{ is a nonzero submodule of } M\}.$$

Let $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq ...$ be any descending chain of nonzero submodules of M. Then the factors in this chain have Krull dimension and satisfy $k(M_i/M_{i+1}) \leq \alpha$ for each $i \geq 0$. It follows that M has Krull dimension with $k(M) \leq \alpha + 1$, a contradiction. □

The following is one of many Noetherian-like properties of modules with Krull dimension.

5.4.6 Lemma:

A module with Krull dimension has finite uniform dimension.

Proof. Suppose that the result is false. Let M with Krull dimension, say $k(M) = \alpha$. Since M does not have finite uniform dimension there exist nonzero submodules N_i of M such that $M \supseteq \oplus_{i=1}^{\infty} N_i$. Set $M_n = \oplus_{j=1}^{\infty} N_{2^n j}$ for each integer $n \geq 0$. Then $M_0 \supseteq M_1 \supseteq M_2 \supseteq ...$ is a descending chain of submodules of M such that each factor M_n/M_{n+1} contains an infinite direct sum and so has infinite uniform dimension. Since $k(M_n/M_{n+1}) \leq k(M)$ it follows, by the minimality of α, that $k(M_n/M_{n+1}) = \alpha$ for all $n \geq 0$. Thus $k(M) > \alpha$, a contradiction. □

5.4.7 Lemma:

Let R be a ring and let M be a right R-module with Krull dimension such that M is a sum of submodules each of which has Krull dimension at most α for some ordinal α. Then $k(M) \leq \alpha$.

Proof. See (McConnell and Robson [68], Lemma (6.2.17)). □

5.4.8 Lemma:

Let R be a ring with right Krull dimension and let M be a right R-module. If M has Krull dimension then $k(M) \leq r.k(R)$.

Proof. This follows from Lemma (5.4.7), since M is the sum of its cyclic submodules, each of which is isomorphic to a factor module of R_R. □

5.5 Krull Dimension of Polynomial and Skew Polynomial Rings

Earlier the problem of Krull dimension was investigated only for some particular cases, namely for Weyl algebras (Rentschler and Gabriel [80]), a ring of differential operators (Goodearl and Lenagan [37]), as well as for rings of Laurent skew polynomials (Hodges [46]).

The rings we will study are mainly skew polynomial rings. Among these, the ordinary polynomial ring $R[x]$ is particularly important, and it also turns out that knowing the Krull dimension of $R[x]$ gives us some control on the Krull dimensions of more general skew polynomial rings $R[x; \sigma, \delta]$. The next lemma shows that the Krull dimensions of certain

modules over $R[x]$ are all that is needed to control the Krull dimension of $R[x]$ and of $R[x;\sigma,\delta]$.

Let $T = R[x]$, the polynomial ring over a right Noetherian ring R. If M is a right R-module, then there is a corresponding right T-module, namely $M \otimes_R T$. It is convenient to write this module as $M[x]$, since every element of $M \otimes_R T$ can be written as a polynomial

$$f = (m_0 \otimes 1) + (m_1 \otimes x) + ... + (m_n \otimes x^n) \equiv m_0 + m_1 x + ... + m_n x^n$$

for some $m_i \in M$. If n is the index of the largest nonzero term in an expression for f, then n is the degree of f and m_n is the leading coefficient. Similarly if $S = R[x;\sigma,\delta]$, we write the induced module $M \otimes_R S$ as $M[y]$, and we define degrees and leading coefficients for elements of $M[y]$ as in $M[x]$.

5.5.1 Lemma:

Let R be a right Noetherian ring, $S = R[x;\sigma,\delta]$ a skew polynomial ring, and $T = R[x]$ a polynomial ring. Assume that σ is an automorphism of R. If M is any finitely generated right R-module, then

$$k(M[y]) \leq k(M[x])$$

Moreover, if V is a nonzero S-submodule of $M[y]$, there exist a nonzero element $m \in M$ and a non-negative integer n such that

$$k(M[y]/V) \leq k(M[x]/mx^n T).$$

Proof. If A is a submodule of $M[y]$, then for $i = 0, 1, ...$ let $g_i(A)$ be the subset of M consisting of 0 together with the leading coefficients of the nonzero elements of A of degree i. Since σ is an automorphism, each $g_i(A)$ is a submodule of M. Note that $g_0(A) \leq g_1(A) \leq ....$ Now let

$$g(A) = g_0(A) + g_1(A)x + g_2(A)x^2 + ...$$

Clearly, $g(A)$ is a submodule of $M[x]$, and if $A \leq B \leq M[y]$, then $g(A) \leq g(B)$. Next observe that if A and B are submodules of $M[y]$ with $A < B$, then $g(A) < g(B)$. Suppose not; then $g(A) = g(B)$ and so $g_i(A) = g_i(B)$ for all i. Let b be an element of B not in A, and choose b

to be of least possible degree, say degree j. Since $g_j(A) = g_j(B)$, there is an element $a \in A$ of the same degree and with the same leading coefficient as b. But then $b - a$ is an element of B of lower degree and not in A, a contradiction. Thus $g(A) < g(B)$, as claimed.

Also, $k(M[y]) \leq k(M[x])$ from Exercise(15Q) of Goodearl and Warfield [41]. If V is a nonzero submodule of $M[y]$, choose a nonzero element of V, say with degree n and leading coefficient m, and note that $mx^nT \leq g(V)$. Now follows from second application of (15Q) of Goodearl and Warfield [41], using the map $A/V \mapsto g(A)/mx^nT$ from submodules of $M[x]/mx^nT$. □

5.5.2 Theorem:

[Rentschler-Gabriel [80]]. Let R be a right noetherian ring, M a nonzero finitely generated right R-module, and x an indeterminate. Then

$$k(M[x]) = k(M) + 1.$$

In particular, if R is nonzero, then $r.k(R[x]) = r.k(R) + 1$.

Proof. Let $T = R[x]$ and $U = M[x]$, and let $\beta = k(M)$. Now M can be made into a right T-module in a natural way, by letting x act trivially, and if we do this, then $k(M_R) = k(M_T)$. Next, note that $Ux^n/Ux^{n+1} \cong M$ (as right T-modules) and

$$k(Ux^n/Ux^{n+1}) = \beta$$

for all n, whence $k(U) > \beta$. (Here we use the fact that x is the central element of T)

Now use a critical composition series for M to reduce to the case in which M is a β-critical module, and we may assume by induction for ordinals smaller than β. We will show, in fact, that U is $(\beta + 1)$-critical.

To show that U is $(\beta + 1)$-critical, it is sufficient to show for every nonzero submodule V of U, that $k(U/V) \leq \beta$. Let us first assume that V has the special form $V = mx^nT$ (i.e., V is generated by a monomial). Now we already know that $k(U/Ux^n) \leq \beta$, and so we only need to consider the factor Ux^n/mx^nT, which is isomorphic to U/mT. Since $U/mT \cong (M//mR)[x]$ and M is β-critical, it follows by induction that

$$k(Ux^n/mx^nT) = k(U/mT) = k(M/mR) + 1 \leq \beta,$$

and hence that $k(U/mx^nT) \leq \beta$.

To prove the theorem, we reduce the general case to this specific case. If we set $\alpha = 1$ and $\delta = 0$ in Lemma (15.16) of Goodearl and Warfield [41], then $M[y] = M[x] = U$, and the lemma provides a nonzero element $m \in M$ and a non-negative integer n such that $k(U/V) \leq k(U/mx^nT)$. Then $k(U/V) \leq \beta$, which completes the proof of the theorem. □

5.5.3 Corollary:

Let R be a right Noetherian ring and $S = R[x; \sigma, \delta]$, where σ is an automorphism of R. If M is any finitely generated right R-module, then

$$k(M) \leq k(M \otimes_R S) \leq k(M) + 1.$$

In particular, $r.k(R) \leq r.k(S) \leq r.k(R) + 1$.

Proof. If $M = 0$, then M and $M \otimes_R S$ both have Krull dimension -1 and the desired inequalities are clear. Assuming $M \neq 0$, we have

$$k(M \otimes_R S) = k(M[y]) \leq k(M[x]) = k(M) + 1$$

by Lemma (5.5.1) and Theorem (5.5.2). On the other hand, since S is a free left R-module, it is left faithfully flat over R (Exercise 15T of Goodearl and Warfield [41]), and thus $k(M) \leq k(M \otimes_R S)$ by Exercise (15U) of Goodearl and Warfield [41]. □

5.5.4 Theorem:

If $S = R[x; \sigma]$, where R is a nonzero right Noetherian ring and σ an automorphism, then $r.k(S) = r.k(R) + 1$.

Proof. Let $\beta = r.k(R)$. Then $r.k(S) \leq \beta + 1$ by Corollary (15.18) of Goodearl and Warfield [41]. Observe that $R \cong S/yS$ as right R-modules and that, under this isomorphism, the right ideals of R correspond to the right S-submodules of S/yS. Hence, $k((S/yS)_S) = k(R_R) = \beta$. Since left multiplication by y provides an injective endomorphism of S_S, it follows from Lemma (15.6) of Goodearl and Warfield [41] that $r.k(S) \geq \beta + 1$, and the theorem is proved. □

5.6 Ideal Krull-symmetry of Polynomial rings

In this section we consider Krull dimension of right R-modules and left R-modules. We also discuss the Krull dimension of a ring R as a right R-module and as a left R-module. Therefore for the sake of convenience we have the following notations:

For any right R-module K, the *right Krull dimension* of K is denoted by $\mid K \mid_r$ and the *annihilator* of a subset S of K is denoted by $r(S)$. Similarly if J is a left R-module, then the *left Krull dimension* of J is denoted by $\mid J \mid_l$ and the annihilator of a subset L of K is denoted by $l(L)$. Recall that the *right Krull dimension* of a ring R is defined as the Krull dimension of R (viewed as a right module over itself). Left Krull dimension of a ring R is defined similarly.

5.6.1 Definition:

A ring R is said to be *Krull-symmetric* if $|R|_r = |R|_l$. R is said to be *right Krull-homogeneous* if $|R|_r = |I|_r$, for all nonzero right ideals I of R. *Left Krull-homogeneity* is defined in a similar way. We also recall that a ring R is said to be *ideal Krull-symmetric* if $\mid I \mid_r = \mid I \mid_l$, where I is any ideal of R.

5.6.2 Definition:

Let S be a ring and R a subring of S. We say an element $a \in S$ centralizes R if $ar = ra$ for each $r \in R$. If S_R has a finite set of generators $\{a_i,\ 1 \leq i \leq n\}$ each of which centralizes R, then S is called a *finite centralizing extension* of R.

5.6.3 Proposition:

Let R be a Noetherian ring and I_j, $1 \leq j \leq n$ be ideals of R such that $0 = \cap I_j$. Let $S = \Pi(R/I_j)$, $1 \leq j \leq n$. Then S is a finite centralizing extension of R.

Proof. It is easily seen that there exists a monomorphism $f : R \to S$. Let

$$x_1 = (1 + I_1, 0, ..., 0)$$

and

$$x_j = (0, 0, ..., 0, 1 + I_j, 0...0),\ 1 \leq j \leq n.$$

For any $s \in S$, let

$$s = (r_1 + I_1, r_2 + I_2, ..., r_n + I_n) = \sum(x_j)(r_j).$$

Now $(x_j)r = r(x_j)$ for all $r \in R$, $1 \leq j \leq n$. Hence the result. □

5.6.4 Proposition:

If S is a Noetherian centralizing extension of R, then:

(1) $| S |_r = | R |_r$ and $| S |_l = | R |_l$.

(2) For any ideal I of S, S/I is a finite centralizing extension of $R/(I \cap R)$.

Proof. **(1)**. See Corollary (10.1.11) of [68].
(2). See Lemma (10.2.2) of [68]. □

5.6.5 Proposition:

Let R be a Noetherian ring with ideals I_j such that $0 = \cap I_j$, $1 \leq j \leq n$ and each R/I_j is Krull-symmetric, right and left Krull-homogeneous. Then R is ideal Krull-symmetric.

Proof. Let $S = \Pi(R/I_j)$, $1 \leq j \leq n$. Now by Proposition (5.6.3) S is a centralizing extension of R. Let I be an ideal of R. Consider the ideal $\mathbb{I} = \Pi(I + I_j/I_j)$ of S. Now it is easy to see that $\mathbb{I}$ is a Krull-symmetric ideal of S. Therefore,

$$| \mathbb{I} |_r = | \mathbb{I} |_l.$$

Now

$$| \mathbb{I} |_r = | S/r(\mathbb{I}) |_r \text{ and } | \mathbb{I} |_l = | S/l(\mathbb{I}) |_l$$

Therefore,

$$| \mathbb{I} |_r = | S/r(\mathbb{I}) |_r = | S/l(\mathbb{I}) |_l = | \mathbb{I} |_l.$$

Now notice $r(I) = r(\mathbb{I}) \cap R$, where $r(\mathbb{I})$ is in S, and similarly $l(I) = l(\mathbb{I}) \cap R$. Now by Proposition (5.6.4) $S/r(I)$ is a centralizing extension of $R/r(I)$. Therefore,

$$| S/r(I) |_r = | R/r(I) |_r$$

by Proposition (5.6.4) and similarly,

$$| S/l(I) |_l = | R/l(I) |_l$$

and as noted above

$$| S/r(I) |_r = | S/l(I) |_l.$$

Thus $| I |_r = | I |_l$. □

5.6.6 Proposition:

Let R be a commutative Noetherian ring and A be any of $S(R)$, $L(R)$ or $D(R)$. Then A is Krull-symmetric.

Proof. $S(R)$ case:
R is commutative Noetherian implies that R is an FBN ring. Therefore Corollary (6.4.10) of [68] implies that R is Krull-symmetric. Now Proposition (6.5.4) (i) of [68] implies that $| R |_r = | S(R) |_r$. Therefore, $S(R)$ is Krull-symmetric.

For $L(R)$ and $D(R)$ case see (6.9.1) of [68]. □

5.6.7 Definition:

Let R be a commutative Noetherian ring and P a semiprime ideal of R. Let $k \geq 1$ be an integer. Then the *symbolic power* of P is denoted by $P^{(k)}$ and is defined as $P^{(k)} = \{a \in R \mid \text{there exists } d \in C(P) \text{ such that } ad \in P^k\}$.

5.6.8 Proposition:

Let R be a commutative Noetherian ring and P a semiprime ideal of R. Then $P^{(k)}$ is an ideal of R.

Proof. Let $a, b \in P^{(k)}$. Then there exist $d_1, d_2 \in C(P)$ such that $ad_1 \in P^k$ and $bd_2 \in P^k$. Now $ad_1d_2 \in P^k$ and $bd_1d_2 \in P^k$; i.e. $(a-b)d_1d_2 \in P^k$ and since $d_1d_2 \in C(P)$, so $(a-b) \in P^{(k)}$. Now let $a \in P^{(k)}$ and $r \in R$. Then there exists $d \in C(P)$ such that $ad \in P^k$. Now $ard \in P^k$ and since $d \in C(P)$, we have $ar \in P^{(k)}$. Hence $P^{(k)}$ is an ideal of R. □

5.6.9 Proposition:

Let R be a commutative Noetherian ring and σ be an automorphism of R. For any associated prime ideal P of R, we have:

(1) $\sigma^m(P) = P$ for some integer $m \geq 1$.

(2) $\sigma^m(P^{(k)}) = P^{(k)}$, m as above.

Proof. **(1)**. We know that $Ass(R_R)$ is a finite set and for any $P \in Ass(R_R)$ and any integer $j \geq 1$, $\sigma^j(P) \in Ass(R_R)$. Therefore, there exists an integer $m \geq 1$ such that $\sigma^m(P) = P$.

(2). Denote σ^m by θ. We have $\theta(P) = P$. Let $a \in P^{(k)}$. Then there exists some $d \in R$, $d \in C(P)$ such that $da \in P^k$. Therefore, $\theta(da) \in \theta(P^k)$; i.e., $\theta(d)\theta(a) \in (\theta(P))^k = P^k$. Now $\theta(d) \in C(P)$ implies that $\theta(a) \in P^{(k)}$. Therefore, $\theta(P^{(k)}) \subseteq P^{(k)}$. Hence $\theta(P^{(k)}) = P^{(k)}$. □

5.6.10 Proposition:

Let R be commutative Noetherian ring which is also an algebra over $\mathbb{Q}$. Let δ be a derivation of R. Let P be a semiprime ideal of R such that $\delta(P) \subseteq P$. Then $\delta(P^{(k)}) \subseteq P^{(k)}$.

Proof. Let $a \in P^{(k)}$. Then there exists $d \in C(P)$ such that $da \in P^k$. Let

$$da = p_1.p_2...p_k,\ p_i \in P.$$

Now $\delta(da) \in P^k$ as $\delta(P) \subseteq P$; i.e., $\delta(d)a + d\delta(a) \in P^k$. Now $\delta(d)a \in P^{(k)}$, therefore, there exists $d_1 \in C(P)$ such that $d_1\delta(d)a \in P^k$. Now $d_1\delta(d)a + d_1.d\delta(a) \in P^k$. Therefore $d_1 d\delta(a) \in P^k$, and since $d_1.d \in C(P)$, we have $\delta(a) \in P^{(k)}$. Hence $\delta(P^{(k)}) \subseteq P^{(k)}$. □

5.6.11 Theorem:

Let R be a commutative Noetherian ring and A be any of $S(R)$, $L(R)$ or $D(R)$ (In case of $D(R)$, R is a moreover an algebra over $\mathbb{Q}$). Then:

(1) A is ideal Krull-symmetric.

(2) For any ideal L of A, $| A/L |_r < | A |_r$ if and only if $| A/L |_l < | A |_l$.

Proof. **(1)** Since R is a commutative Noetherian ring, the ideal (0) has a reduced primary decomposition say $(0)= \cap I_j$, $1 \leq j \leq n$. For this see Theorem (4), page 209 of [92] . Let $\sqrt{I_j} = P_j$, where P_j is a prime ideal belonging to I_j. Now by Theorem (23), page 236 of [92] there exists a positive integer k such that $P_j^{(k)} \subseteq I_j$, $1 \leq j \leq n$. Therefore, $\cap P_j^{(k)} = 0$. Now by the first uniqueness Theorem $P_j \in Ass(R_R)$, $1 \leq j \leq n$. Now since $Ass(R_R)$ is finite and $\sigma^j(P) \in Ass(R_R)$ for any $P \in Ass(R_R)$, and for all integers $j \geq 1$, there exists an integer $m \geq 1$ such that $\sigma^m(P_j) = P_j$ and $\sigma^m(P_j^{(k)}) = P_j^{(k)}$ by Proposition (5.6.9). Now $\delta(P_j) \subseteq P_j$ by Theorem (1) of [84], and therefore, $\delta(P_j^{(k)}) \subseteq P_j^{(k)}$ by Proposition (5.6.10). Let

$$T_j = \cap \sigma^i(P_j^{(k)}),\ i = 1, 2, ..., m.$$

Then $\sigma(T_j) = T_j$ and so $T_j[x, \sigma]$ is an ideal of $S(R)$. Let $U_j = S(T_j^{(k)})$, $L(T_j^{(k)})$ and $D(P_j^{(k)})$ in case of $S(R)$, $L(R)$ and $D(R)$ respectively. Then $0 = \cap U_j$, $1 \leq j \leq n$.
Let

$$T = \prod (A/U_j),\ 1 \leq j \leq n.$$

Now by Proposition (5.6.3), T is a centralizing extension of A.

Let I be an ideal of A. Consider the ideal

$$I^* = \Pi(I + U_j/U_j),\ 1 \leq j \leq n$$

of T. Then it is easy to see that I^* is a Krull-symmetric ideal of T. Therefore,

$$|\ I^*\ |_r = |\ T/r(I^*)\ |_r = |\ T/l(I^*)\ |_l = |\ I^*\ |_l.$$

Let $f : A \to T$ be the natural monomorphism. Now $r(I) = r(I^*) \cap A$ and similarly $l(I) = l(I^*) \cap A$. Now by Proposition (5.6.4) $T/r(I^*)$ is a centralizing extension of $A/r(I)$. Therefore, Proposition (5.6.4) implies that

$$|\ T/r(I^*)\ |_r = |\ A/r(I)\ |_r$$

and similarly,

$$|\ T/l(I^*)\ |_l = |\ A/l(I)\ |_l.$$

But

$$|\ T/r(I^*)\ |_r = |\ T/l(I^*)\ |_l.$$

Therefore, we have

$$| I |_r = | I |_l.$$

Hence A is ideal Krull-symmetric.

(2) Let L be an ideal of A such that

$$| A/L |_l < | A |_l.$$

Suppose

$$| A/L |_r = | A |_r.$$

Now

$$| A/L |_r = | A/P |_r = | A |_r,$$

where P is a prime deal of A such that $L \subseteq P$. Now $N(A) = \cap S(P_j)$, $1 \leq j \leq n$ (in case $A = S(R)$) and since

$$I_j^* = S(P_j^k) \subseteq S(P_j^{(k)}) = I_j,$$

we have $\cap I_j^* = 0$, $1 \leq j \leq n$. Now every $S(P_j)$, $1 \leq j \leq n$ is associated to A, we get that P is associated to A and $P = S(P_j)$ for some j, $1 \leq j \leq n$. Let $A_1 = A/I_j$. Then since $L + I_j \subseteq P_j$ and $I_j \subseteq L + I_j \subseteq P_j$, we have

$$| A_1/L + I_j |_r = | A/L + I_j |_r = | A/P_j |_r.$$

Now

$$| A |_r = | A |_l,$$

and by Proposition (5.6.4) in $A_1 = A/I_j$, we have

$$| A_1/L + I_j |_l = | A_1/L + I_j |_r = | A/L |_l = | A |_l.$$

This is a contradiction. Hence

$$| A/L |_r < | A |_r.$$

The cases $A = L(R)$ or $D(R)$ can be proved in a similar way.

Converse on the same lines as above. □

5.7 Primary Decomposition in Non-Noetherian Rings

To proceed we recall some basic properties of modules and rings with Krull dimension. Firstly a module with Krull dimension has finite uniform dimension (McConnell [68], Lemma (6.26)). Any ring with right Krull dimension has the ascending chain condition on prime ideals (Gordon [43], Theorem (7.1)). Any ideal I in a ring with right Krull dimension contains a product of prime ideals where each of the prime ideals in the product contains I (Gordon [43], Theorem (7.4)). The following result is similar to [Gordon [43], Theorem (8.3)].

5.7.1 Proposition:

Let M be a right R-module over a ring R with right Krull dimension. Then $Ass(M_R) \neq \phi$.

Proof. Suppose $I = Ann(N)$ for some nonzero submodule $N \subseteq M$. We know that I contains a product of primes $P_1...P_n$ where $P_i \supseteq I$. We may assume $P_1...P_{n-1} \nsubseteq I$ (here we use the convention that a product of zero terms equals R). Therefore P_n annihilates a nonzero submodule of M, namely $NP_1...P_{n-1}$.

Among the (non-empty) set of prime ideals of R that annihilate nonzero submodules of M we can choose P maximal. Let $L = l_M(P)$ and we will show that L is P-primary. Suppose not, so choose $L' \subseteq L$ such that $Ann(L') \supsetneq P$. We know that $Ann(L')$ contains a product of primes, and by the method of above we see that there exist a prime ideal $Q \supseteq Ann(L')$ that annihilates a nonzero submodule of L'. This contradicts the maximality of P. Hence L is P-primary and $P \in Ass(M_R)$. □

5.7.2 Corollary:

Let R be a ring with right Krull dimension and let M be a right R-module with finite uniform dimension. Then M_R has a primary decomposition.

Proof. Use the decomposition in Lemma (5.2.3) and the observation that uniform modules over rings with right Krull dimension are primary.
We remark that in Corollary (5.7.2) if M is also a tame right R-module then we get a tame decomposition of the module M. □

5.7.3 Theorem:

Let R have right Krull dimension and $Ass(R_R) \subseteq MinSpec(R)$. Then the ring R has a right primary decomposition.

Proof. Choose a decomposition $\bigcap_{i=1}^{n} V_i = 0$ in terms of right ideals as in Corollary (5.7.2). It is enough to show that each ring $R/Ann(R/V_i)$ is right primary. Therefore we fix i, assume $Ann(R/V_i = 0)$ and replace V_i by its image in $R/Ann(R/V_i)$.

We know that $(R/V_i)_R$ is P-primary for some prime ideal P. Suppose that $Q = Ann(I) \in Ass(R_R)$ is a prime ideal of R where I is some right ideal of R. As V_i contains no non-zero ideals, we have $RI + V_i/V_i$ is a non-zero submodule of R/V_i. Now

$$RIx(RI + V_i/V_i) \subseteq V_i,$$

and as the left hand side is an ideal contained in V_i it must be equal to zero. In other words $Ann(RI + V_i/V_i) \subseteq Q$. Obviously $Q \subseteq Ann(RI + V_i/V_i)$ and so we have equality. As Q is the annihilator of a submodule of R/V_i, we must have $Q \subseteq P$. We now get $Q = P$ since P is a minimal prime.

We note that if R_R is also tame, for example when R has d.c.c on right annihilators, then it is possible to show that R has a right tame decomposition in the above situation.

The method of Theorem (5.7.3) could be used to prove the right Noetherian case of Theorem (5.3.2). To see this note that in the above $RI + V_i/V_i$ is a faithful P/Q-primary right R/Q-module. This contradicts P having the right strong second layer condition unless $Q = P$. Theorem (5.3.9) can also be proven in a similar way.

Along the same lines as Theorem (5.7.3) we can get another primary decomposition result. □

5.7.4 Proposition:

Let R be a right Goldie ring with $Ass(R_R) \subseteq MinSpec(R)$. Then R has a right primary decomposition.

Proof. We note that each uniform right ideal of R is primary as R has the ascending chain condition on right annihilators. We choose a decomposition $\bigcap_{i=1}^{n} V_i = 0$ of R_R as in Lemma (5.2.3). As each $(R/V_i)_R$ is an essential extension of a module isomorphic to a uniform right ideal U_i of R, it is easy to check that each $(R/V_i)_R$ is uniform and P_i-primary for some prime ideal $P_i, i = 1, ..., n$. The rest of the proof now follows in a similar way to Lemma (5.4.3), although we need to check that $Ass((R/Ann(R/V_i)_R))$ is non-empty. Let $X_i = Ann(R/V_i)$. We can reduce to the case where $\bigcap X_i = 0$ is an irredundant intersection. Hence each $(R/X_i)_R$ contains a submodule isomorphic to a right ideal of R. Therefore $Ass((R/X_i)_R)$ is non-empty. □

5.8 Primary Decomposition in Rings with Quotient Rings

In this section we look at the interplay between primary decomposition in rings that have quotient rings.

5.8.1 Proposition:

Let R have a right quotient ring Q. Then

(1) If $I \lhd_r R$ then $IQ \lhd_r Q$ and every element of IQ is expressible as xc^{-1}, where $x \in I$ and $c \in \mathcal{C}_R(0)$.

(2) If $K \lhd_r Q$ then $K \cap R \lhd_r R$ and $(K \cap R)Q = K$.

(3) If Q is right Noetherian and $A \lhd r$ then $AQ \lhd Q$.

(4) $R_R \subseteq_{ess} Q_R$.

(5) If $B \lhd_r Q$ and $B_Q \subseteq_{ess} Q_Q$ then $(B \cap R)_R \subseteq_{ess} R_R$.

Proof. See [McConnell [68], Proposition (2.1.16), Lemma (2.2.12)] and the proof of Goodearl and Warfield [[38], Lemma (5.11)]. □

5.8.2 Lemma:

[Chatters [24], Lemma (1.30)(a)]. Let R be a ring with the ascending chain condition on right annihilators, and let S be a right Ore set. Suppose $S \subseteq' \mathcal{C}(0)$. Then $S \subseteq C(0)$.

5.8.3 Proposition:

[Ludgate [64], Lemma (4)]. Let R have a right quotient ring Q. Suppose A is a proper ideal of R, then $\mathcal{C}_R(0) \subseteq \mathcal{C}_R(A)$ if and only if AQ is an ideal of Q and $AQ \cap R = A$.

5.8.4 Proposition:

Let R be a ring with the ascending chain condition on right annihilators. Let X be a non-zero right ideal of R, and set $A = Ann(X)$. Suppose R has a right quotient ring Q, then AQ is an ideal of Q.

Proof. First note that $A = AQ \cap R$ since $XAQ = 0$ implies $AQ \cap R \subseteq A$, and the reverse inclusion is obvious. Suppose $xc \in A$ where $x \in R$ and $c \in \mathcal{C}$. Now $xcc^{-1} \in R$, so $x \in A$ and $\mathcal{C}(0) \subseteq' \mathcal{C}(A)$.

We will now show that $\mathcal{C} \subseteq \mathcal{C}'(A)$, and then the result follows by Proposition (5.8.3). To do this it is enough to apply Lemma (5.8.2) to the ring R/A. Therefore it remains to show that R/A has a.c.c on right annihilators. This follows as R/A_R embeds in the direct product R_R^X via the map $r \to (xr)_{x \in X}$. As R has a.c.c on right annihilators, R has a.c.c on annihilators of subsets of R^X. To see this suppose xth coordinate of an element of Y. Thus $Ann(Y)$ is equal to a right annihilator of R. Now we see that R has a.c.c on right annihilators. □

The next result is our showing that a ring can inherit primary properties from its quotient ring.

5.8.5 Theorem:

Let R has a right quotient ring Q where Q has the ascending chain condition on right annihilators. Then if Q is right Π-primary for some prime ideal Π of Q, R is right $(\Pi \cap R)$-primary.

Proof. By Lemma (5.2.1), $L = l_Q(\Pi)$ is an essential right ideal of Q. Let $P = \Pi \cap R$ and $K = l_Q(P)$. Of course $K \supseteq L$. By Lemma (5.8.1), $L \cap R \subset_{ess} R_R$ and hence $K \cap R = l_R(P) \subseteq_{ess} R_R$. It remains to show that P is the unique maximal ideal among the annihilators of non-zero right ideals of R.

Suppose $A = Ann(B)$ for some non-zero right ideal B of R. By replacing B by the non-zero intersection $B \cap l_R(P)$ we may assume that

$A \supseteq P$. If $A \supsetneqq P$ then $AQ \supsetneqq PQ = \Pi$. However by Proposition (5.8.4), since R inherits the ascending chain condition on right annihilators from Q, we have AQ is an ideal of Q. Therefore $BQAQ = BAQ = 0$ and AQ annihilates a non-zero right ideal of Q. This cannot happen since Π is maximal among the annihilators of non-zero right ideals of Q. Therefore P must be the unique maximal right annihilator for R. This shows us that P is prime and R is right P-primary. □

5.8.6 Theorem:

Let R be a right P-primary ring, where P is a prime ideal of R. Suppose that R has a right quotient ring Q and also has the ascending chain condition on right annihilators. Then Q is right PQ-primary.

Proof. As $L = l_R(P)$ is an essential submodule of R_R, and hence Q_R, it follows that LQ is an essential right ideal of Q. Let $\Pi = PQ$. As P is a right annihilator of R, Π is an ideal of Q by Proposition (5.8.4). Now $LQ\Pi = L\Pi = LPQ = 0$. Hence $l_Q(\Pi)$ is an essential right ideal of Q. Suppose there exists $A = Ann_Q(X)$, where X is a non-zero right ideal of Q. If we replace X by $X \cap l_Q(\Pi) \neq 0$ we may assume that $A \supseteq \Pi$. Then $P \subseteq R \cap A \subseteq Ann(X \cap R)$, where $X \cap R$ is a non-zero right ideal of R. By the maximality of P among the annihilators of non-zero submodules of R_R, we have $P = R \cap A$ and therefore $PQ = (R \cap A)Q = A$. Hence Π must be maximal among the annihilators of non-zero right ideals of Q and therefore is a prime ideal of Q. The result now follows from the note after Lemma (5.2.1).

We now show that in certain situations a ring can inherit a primary decomposition from its quotient ring. □

5.8.7 Theorem:

Let R be a ring with a right quotient ring Q where Q is right Noetherian. If Q has a right primary decomposition, so does R.

Proof. Let $J_1 \cap ... \cap J_n$ be a right primary decomposition for Q, where J_i is an ideal of Q and $(Q|J_i)_Q$ is Π_i-primary for some prime ideal Π_i of Q. We will show that $(J_1 \cap R) \cap ... \cap (J_n \cap R)$ is a right primary decomposition for R, where each $R/(J_i \cap R)_R$ is $(\Pi_i \cap R)$ is a right primary decomposition for R, where each $R/(J_i \cap R_R)_R$ is $(\Pi_i \cap R)$-primary.

Without loss of generality we consider $(Q/J_1)_Q$. Now $L = l_{Q/J_1}(\Pi_1)$ is an essential Q-submodule of Q/J_1 by Lemma (5.2.1). Let $P = \Pi_1 \cap R$ and note $L = l_{Q/J_1}(PQ) = l_{Q/J_1}(P)$. We will now consider Q/J_1 as a right R-module. We claim that L is an essential submodule of $(Q/J_1)_R$. Choose any submodule N and let M be the inverse image of N in Q. Elements of M are of the form $m = rc^{-1}$, where $r \in R, c \in \mathcal{C}_R(0)$. Note that $r = mc \in R \cap M$. Similarly elements of MQ can be written in the form rc^{-1}, where $r \in M, c \in \mathcal{C}_R(0)$, and in particular $m \notin J_1$. However $mc^{-1}Q\Pi_1 \subseteq J_1$ as $n \in L$. Therefore $mQ\Pi_1 \subseteq J_1$. Hence $m + J_1 \in L \cap N$ proving the claim.

We now have

$$(Q/J_1)_R \supseteq (R + J_1/J_1)_R \cong (R/R \cap J_1)_R,$$

and P annihilates an essential submodule of all of these terms. The last step is to show that P is the unique maximal ideal among the annihilators of non-zero submodules of $(Q/J_1)_R$, and the theorem then follows using Lemma (5.2.1) to show that $(Q/J_1)_R$ is P-primary and hence so is $R/R \cap J_1$. Suppose not, let $A = Ann(B)$, where $B \subseteq (Q/J_1)_R$ is a non-zero submodule and $A \nsubseteq P$. Replace B by the non-zero intersection of B and L, the annihilator of P in $(Q/J_1)_R$, so that AQ is an ideal of Q, for as A annihilates a non-zero R- submodule of $(Q/J_1)_R$, it annihilates non-zero elements of $(Q/J_1)_Q$. Hence so does AQ. But if AQ is an ideal, this now means AQ annihilates a non-zero Q-submodule of $(Q/J_1)_Q$ and $AQ \supsetneqq PQ = \Pi_1$. This contradicts Q/J_1 being Π_1-primary.

The fact that AQ is an ideal follows from Proposition (5.8.1). It remains to note that as P is maximal among the annihilators of $(Q/J_1)_R$, it must be a prime ideal. □

Note that if R is right Noetherian then Q is automatically right Noetherian.

As right Artinian rings have a right primary decomposition and are also right Noetherian we get the following corollary:

5.8.8 Corollary:

If R is a ring with a right Artinian right quotient ring then R has a right primary decomposition. A version of this corollary can be found in [Nastasescu [72], Corollary (2.7)].

The following example is similar to [Chatters [24], Example (9.1)]. It illustrates the interplay between Theorem (5.8.5) and Theorem (5.8.6) in a non-Noetherian setting.

5.8.9 Example:

Let

$$R = \begin{pmatrix} \mathbb{Z} & \mathbb{C} \\ 0 & \mathbb{Z} \end{pmatrix} \text{ and } Q = \begin{pmatrix} \mathbb{Q} & \mathbb{C} \\ 0 & \mathbb{Q} \end{pmatrix},$$

Q is the quotient ring of R and Q (and therefore R) has the ascending chain condition on right annihilators. Let

$$P = \begin{pmatrix} \mathbb{Z} & \mathbb{C} \\ 0 & 0 \end{pmatrix} \text{ and } P' = \begin{pmatrix} \mathbb{Q} & \mathbb{C} \\ 0 & 0 \end{pmatrix}.$$

Then R is right P-primary and Q is right P'-primary.

5.9 Artinian Embedding

Many standard examples of Noetherian rings are known to be subrings of Artinian rings because they have a primary decomposition and the primary factors are subrings of Artinian rings. For example this is the case for Noetherian rings with the second layer condition, which have primary decomposition by Corollary (5.3.10) and the primary factors have Artinian quotient rings by [[50], Proposition (8.3.5)].

5.9.1 Theorem:

[Krause [55], Theorem (3.1), Proposition (3.2)]. Let k be a field. The following are equivalent for a right Noetherian right primary k-algebra with finite Gelfand- Kirillov dimension.

(1) Each ideal of R is finitely annihilated on the right.

(2) R embeds in a simple Artinian ring.

5.9.2 Theorem:

Let R be a right Noetherian k- algebra with finite Gelfand-Kirillov dimension. Suppose $Ass(R_R)$ satisfies the right restricted strong second layer condition. Then R embeds in an Artinian ring if and only if ideals of R are finitely annihilated on the right.

Proof. We can choose a right tame decomposition $0 = \bigcap_{i=1}^{n} J_i$, where each J_i is an ideal of R, by Theorem (5.3.9). It follows that each $R/J_1 \oplus ... \oplus R/J_n$, where each R/J_i is a primary k-algebra with d.c.c on right annihilators and finite Gelfand-Kirillov dimension, we use Theorem (5.9.1) to get an Artinian embedding.

The converse holds trivially. □

5.9.3 Corollary:

[Krause [55], Corollary (3.3)]. A right Noetherian, right fully bounded k-algebra with finite Gelfand-Kirillov dimension can be embedded in a simple Artinian ring. To finish we note that obtaining Artinian embedding using a primary decomposition is not restricted to Noetherian rings. Recall the following result of Goldie and Krause.

5.9.4 Theorem:

[Goldie [36], Corollary (2), Corollary (7)]. Let R be a ring that $Ass(R_R) \subseteq MinSpec(R)$ and ideals are finitely annihilated on the right. If $\Omega_r(P)$ satisfies the incomparability condition for every $P \in Ass(R_R)$ then R embeds in a right Artinian ring.

By inspecting the proof of [Goldie [36], Corollary (7)], and noting that each E_i in the proof is finitely annihilated, it is easy to see that this embedding result is obtained via a tame decomposition.

Looking at this form the other direction, we could use the primary decomposition result of Theorem (5.7.3) (in fact this is a tame decomposition if R has ideals finitely annihilated on the right), along with the following proposition to get Theorem (5.9.4). Precise details can be found in Convington [28].

5.9.5 Proposition:

Let R be a right P-primary ring with right Krull dimension, where P is a prime ideal of R. Then R has a right Artinian right quotient ring if and only if the following three conditions hold

(1) Ideals of R are finitely annihilated on the right.

(2) P is a minimal prime ideal.

(3) $\Omega^r(P)$ satisfies the incomparability condition.

Proof. If follows by inspecting the proof of [Goldie [36], Corollary (7)]. For the converse, (1) and (2) are easy to show. (3) can be proved using the methods of Goldie [36]. □

We note that condition (2) is superfluous if R is right Noetherian. Indeed so is condition (1) if R right and left Noetherian. For more details see Convington [28]. By way of illustration consider the following examples considered by Blair and Small in [18].

5.9.6 Example:

Consider the ring

$$R = \begin{pmatrix} f(0) & g(x) \\ 0 & f(x) \end{pmatrix}$$

where k is a field and $f(x), g(x) \in k[x]$. R is a right Noetherian affine k-algebra which is not left Noetherian. R has a prime ideal

$$P = \begin{pmatrix} 0 & k[x] \\ 0 & 0 \end{pmatrix}$$

and R is right P-primary. By applying Theorem (5.9.2) we see that R embeds in a simple Artinian ring. However $\Omega_r(P)$ doesnot satisfy the incomparability condition and R doesnot have a right Artinian right quotient ring.

Now consider the ring the nonembeddable right Noetherian ring.

$$T = \begin{pmatrix} \mathbb{C} & B \\ 0 & S \end{pmatrix},$$

where $S = A_1(\mathbb{C})$ and B is a simple right S-module. Note that we can view B as a left $\mathbb{C}$-module and hence as a $\mathbb{C} - S$-bimodule. We have a prime ideal

$$Q = \begin{pmatrix} \mathbb{C} & B \\ 0 & 0 \end{pmatrix}$$

and T is right Q-primary (but not Q-tame). The ring T has finite Gelfand-Kirillov dimension and Q satisfies the strong second layer condition. However the ideal

$$\begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix}$$

is not finitely annihilated so Theorem (5.9.2) does not apply.

Chapter

6

PRIMARY DECOMPOSITION OF SKEW POLYNOMIAL RINGS

The classical study of any commutative Noetherian ring is done by studying its primary decomposition. Further there are other structural properties of rings, for example the existence of quotient rings or more particularly the existence of Artinian quotient rings or more particularly the existence of Artinian quotient rings etc. which can be nicely tied to primary decomposition of a Noetherian ring.

It is shown in Blair and Small [18] that if R is embeddable in a right Artinian ring and has characteristic zero, then the differential operator ring $R[x;\delta]$ embeds in a right Artinian ring, where δ is a derivation of R. It is also shown in Blair and Small [18] that if R is a commutative Noetherian ring and σ is an automorphism of R, then the skew polynomial ring $R[x;\sigma]$ embeds in an Artinian ring.

6.1 Associated Prime Ideals of Skew Polynomial Rings of Automorphism Type

A non-commutative analogue of associated prime ideals of a Noetherian ring has also been discussed. We also note that considerable work has been done in the investigation of prime ideals (in particularly minimal prime ideals and associated prime ideals) of skew polynomial rings (K. R. Goodearl and E. S. Letzter [40], C. Faith [29], S. Annin [1], Leroy and Matczuk [62], Nordstrom [74] and Bhat [9]).

Carl faith has proved that if R is a commutative ring, then the associated prime ideals of the usual polynomial ring $R[x]$ (viewed as a module over itself) are precisely the ideals of the form $P[x]$, where P is an associated prime ideal of Goodearl and Warfield proved in (2ZA) of [38] that if R is a commutative Noetherian if σ is an automorphism of R, then an ideal I of R is of the form $P \cap R$ for some prime ideal P of $R[x;x^{-1},\sigma]$

if and only if there is a prime ideals of R and a positive integer m with $\sigma^m(S) = S$, such that $I = \cap_{i=1}^{m} \sigma^i(S)$. Gabriel proved in [33] that if R is a right Noetherian ring which is also an algebra over $\mathbb{Q}$ and P is a prime ideal of $R[x;\delta]$, then $P \cap R$ is a prime ideal of R. In Theorem (2.2) of [1], S. Annin has proved the following:

Theorem (2.2) of Annin [1]: Let R be a ring and M be a right R-module. Let σ be an endomorphism of R and $S = R[x;\sigma]$. Let M_R be σ-compatible. Then $Ass((M[x])_S)) = \{P[x]$ such that $P \in Ass(M_R)\}$.

H. Nordstrom has proved the following result in [74]:

Theorem (1.2) of Nordstrom [74]: Let R be a ring with identity and σ be a surjective endomorphism of R. Then for any right R-module M, $Ass((M[x;\sigma])_R) = \{I[x;\sigma]$, $I \in \sigma - Ass(M_R)\}$.

In Corollary (1.5) of [74], Nordstrom has been proved that if R is a Noetherian ring and σ is an automorphism of R, then $Ass((M[x,\sigma])_S)) = \{P_\sigma[x,\sigma]$, $P \in Ass(M_R)\}$, where $P_\sigma = \cap_{i\in N}\sigma^{-i}(P)$ and $S = R[x,\sigma]$.

Concerning associated prime ideals of full Ore extensions $R[x;\sigma,\delta]$, S. Annin generalizes the above in the following way:

Definition (2.1) of Annin [2]: Let R be a ring and M_R be a right R-module. Let σ be an endomorphism of R and δ be a σ-derivation of R. M_R is said to be σ-compatible if for each $m \in M$, $r \in R$, we have $mr = 0 \Leftrightarrow m\sigma(r) = 0$. Moreover M_R is said to be δ-compatible if for each $m \in M$, $r \in R$, we have $mr = 0 \Rightarrow m\delta(r) = 0$. If M_R is both σ-compatible and δ-compatible, M_R is said to be $(\sigma - \delta)$-compatible.

Theorem (2.3) of Annin [2]: Let R be a ring. Let σ be an endomorphism of R and δ be a σ-derivation of R and M_R be a right R-module. If M_R is $(\sigma - \delta)$-compatible, then $Ass((M[x])_S)) = \{P[x] \mid P \in Ass(M_R)\}$.

In [62] Leroy and Matczuk have investigated the relationship between the associated prime ideals of an R-module M_R and that of the induced S-module M_S, where $S = R[x;\sigma,\delta]$ (σ is an automorphism and δ is a σ-derivation of a ring R). They have proved the following:

Theorem (5.7) of Leroy and Matczuk [62]: Suppose M_R contains enough prime submodules and let for $Q \in Ass(M_S)$. If for every $P \in Ass(M_R)$, $\sigma(P) = P$, then $Q = PS$ for some $P \in Ass(M_R)$.

Bhat [9] has investigated the nature of associated prime ideals of certain skew polynomial rings over a Noetherian ring R and their relation with those of the coefficient ring R.

6.1.1 Proposition:

Let R be a right Noetherian ring and σ be an automorphism of R. Then there exists an integer $m \geq 1$ such that $\sigma^m(P) = P$ for all $P \in Ass(R_R)$.

Proof. We know that $Ass(R_R)$ is finite and $\sigma(P) \in Ass(R_R)$ for any $P \in Ass(R_R)$, therefore there exists an integer $m \geq 1$ such that $\sigma^m(P) = P$ for all $P \in Ass(R_R)$ □

6.1.2 Proposition:

Let R be a semiprime right Goldie ring. Let σ be an automorphism of R and δ be an σ-derivation of R. Let $O(R) = R[x; \sigma, \delta]$. If $f \in O(R)$ is a regular element, then there exists $g \in O(R)$ such that gf has leading coefficient regular in R.

Proof. Let $S = \{a_m \in R$ such that $x^m a_m + ... + a_0 \in O(R)$ for some $m\} \cup \{0\}$. Then since $O(R)$ is semiprime and Noetherian, $O(R)f$ is an essential left ideal of $O(R)$, and therefore S is an essential left ideal of R. So S contains a left regular element, and since R is semiprime, Proposition (3.2.13) of Rowen [83] implies that S contains a regular element. Therefore there exists $g \in O(R)$ such that gf has leading coefficient regular in R. □

6.1.3 Theorem:

(Proposition (2.3) of Bhat [9]). Let R be right Noetherian ring and σ be an automorphism of R. Let $K(R)$ be any of $S(R)$. Let $P \in Ass(K(R)_{K(R)})$. Then there exists $Q \in Ass(R_R)$ with $\sigma^m(Q) = Q$ for some integer $m \geq 1$ such that $P \cap R = Q^0 = \cap_{i=1}^m \sigma^i(Q)$. Also $K(P \cap R) = P$.

Proof. Choose a right ideal I of $K(R)$ with $P = Ann(I) = Assas(I_R)$, and choose $f \in I$ to be nonzero of minimal degree (with leading coefficient a_n). Without loss of generality, $Q = Ann(a_nR) = Assas((a_nR)_R)$. This implies that $fQ = 0$. Therefore $fK(R)Q^0 \subseteq fQK(R) = 0$. So $Q^0 \subseteq (P \cap R)$. But it is clear that $(P \cap R) \subseteq Q$, and $(P \cap R)$ is σ-invariant. Thus $(P \cap R) \subseteq Q^0$. Now by Jategaonkar [50], $K(P \cap R)$ is a prime ideal of $K(R)$. Suppose $K(P \cap R) \neq P$. Then by Proposition (6.1.2) there exists $g \in C(K((P \cap R))$, and $h_1 \in K(R)$ such that h_1g has leading co-efficient regular modulo $P \cap R$. Let $h_1g = \sum_{i=0}^{k} x^i d_i$. Now $P \subseteq Ann(f_rR)$, $r \in R$ and since $h_1g \in P$, we have $f_rRh_1g = 0$. Therefore $x^{n+k}\sigma^k(a_n)\sigma^k(r)Rd_k + ... + a_0rRd_0 = 0$. So $\sigma^k(a_n)\sigma^k(r)Rd_k = 0$; i.e. $\sigma^{-k}(d_k) \in Ann(a_nrR) = Q$, but $d_k \in C(P \cap R)$, therefore $d_k \in C(P \cap R)$, therefore $d_k \in C(\sigma^j(Q))$ for all $j \geq 1$ which is a contradiction. Hence $K(P \cap R) = P$. □

6.1.4 Theorem:

(Theorem (2.4) of Bhat [9]). Let R be a Noetherian ring and σ be an automorphism of R. Let $K(R)$ be any of $S(R)$. Then:

(1) $P \in Ass(K(R)_{K(R)})$ if and only if there exists $Q \in Ass(R_R)$ such that $K(P \cap R) = P$ and $(P \cap R) = Q^0$.

(2) $P \in MinSpec(K(R))$ if and only if there exists $Q \in MinSpec(R)$ such that $K(P \cap R) = P$ and $(P \cap R) = Q^0$.

Proof. (1) Let $Q = Ann(cR) = Assas((cR)_R)$, $c \in R$. Now $\sigma^m(Q) = Q$ for some integer $m \geq 1$ by Proposition (6.1.1). Now using Proposition (6.1.2) as used in Theorem (6.1.3), we have $K(Q^0) = Ann(chK(R))$ for all $h \in K(R)$. Therefore $K(Q^0) = Ann(cK(R)) = Assas((cK(R))_R)$. Converse is true by Theorem (6.1.3).

(2) Let $Q \in Min.Spec(R)$. Then $\sigma^m(Q) = Q$ for some integer $m \geq 1$. Let $Q_1 = Q^0$. Then by Proposition (10.6.12) of McConnell and Robson [68] and Theorem (7.27) of Goodearl and Warfield [38], $Q_2 = K(Q_1) \in MinSpec(K(R))$.

Conversely suppose that $P \in MinSpec(K(R))$. Then $P \cap R = Q^0$ for some $Q \in Spec(R)$ and Q contains a minimal prime Q_1. Then $P \supseteq K(R)Q_1^0$, which is a prime ideal of $K(R)$. Hence $P = K(R)Q_1^0$. □

In this section a structure of associated prime ideals and minimal prime ideals of the skew polynomial rings $S(R) = R[x;\sigma]$ and $L(R) = R[x;x^{-1},\sigma]$ is given, where σ is an automorphism of a right Noetherian ring R. This structure is also given for $R[x;\delta]$, where δ is a derivation of a right Noetherian $\mathbb{Q}$-algebra R.

6.2 Associated Prime Ideals of Skew Laurent Rings

Goodearl and Warfield proved in (2ZA) of [38] that if R is a commutative Noetherian ring, and if σ is an automorphism of R, then an ideal I of R is of the form $P \cap R$ for some prime ideal P of $R[x,x^{-1};\sigma]$ if and only if there is a prime ideal S of R and a positive integer m with $\sigma^m(S) = S$, such that $I = \cap\sigma^i(S)$, $i = 1,2,...,m$.

6.2.1 Theorem:

(Proposition (2.3) of Bhat [9]). Let R be right Noetherian ring and σ be an automorphism of R. Let $K(R)$ be any of $L(R)$. Let $P \in Ass(K(R)_{K(R)})$. Then there exists $Q \in Ass(R_R)$ with $\sigma^m(Q) = Q$ for some integer $m \geq 1$ such that $P \cap R = Q^0 = \cap_{i=1}^m \sigma^i(Q)$. Also $K(P \cap R) = P$. (Same as Theorem (6.1.3)).

Proof. Choose a right ideal I of $K(R)$ with $P = Ann(I) = Assas(I_R)$, and choose $f \in I$ to be nonzero of minimal degree (with leading coefficient a_n). Without loss of generality, $Q = Ann(a_nR) = Assas((a_nR)_R)$. This implies that $fQ = 0$. Therefore $fK(R)Q^0 \subseteq fQK(R) = 0$. So $Q^0 \subseteq (P \cap R)$. But it is clear that $(P \cap R) \subseteq Q$, and $(P \cap R)$ is σ-invariant. Thus $(P \cap R) \subseteq Q^0$. Now by Jategaonkar [50], $K(P \cap R)$ is a prime ideal of $K(R)$. Suppose $K(P \cap R) \neq P$. Then by Proposition (6.1.2) there exists $g \in C(K((P \cap R))$, and $h_1 \in K(R)$ such that h_1g has leading co-efficient regular modulo $P \cap R$. Let $h_1g = \sum_{i=0}^k x^i d_i$. Now $P \subseteq Ann(f_rR)$, $r \in R$ and since $h_1g \in P$, we have $f_rRh_1g = 0$. Therefore $x^{n+k}\sigma^k(a_n)\sigma^k(r)Rd_k + ... + a_0rRd_0 = 0$. So $\sigma^k(a_n)\sigma^k(r)Rd_k = 0$; i.e., $\sigma^{-k}(d_k) \in Ann(a_nrR) = Q$, but $d_k \in C(P \cap R)$, therefore $d_k \in C(P \cap R)$, therefore $d_k \in C(\sigma^j(Q))$ for all $j \geq 1$ which is a contradiction. Hence $K(P \cap R) = P$. □

6.2.2 Theorem:

(Theorem (2.4) of Bhat [9]). Let R be a Noetherian ring and σ be an automorphism of R. Let $K(R)$ be any of $L(R)$. Then:

(1) $P \in Ass(K(R)_{K(R)})$ if and only if there exists $Q \in Ass(R_R)$ such that $K(P \cap R) = P$ and $(P \cap R) = Q^0$.

(2) $P \in MinSpec(K(R))$ if and only if there exists $Q \in MinSpec(R)$ such that $K(P \cap R) = P$ and $(P \cap R) = Q^0$. (Same as Theorem (9.4)).

Proof. (1) Let $Q = Ann(cR) = Assas((cR)_R)$, $c \in R$. Now $\sigma^m(Q) = Q$ for some integer $m \geq 1$ by Proposition (9.1). Now using Proposition (6.1.2) as used in Theorem (6.1.3), we have $K(Q^0) = Ann(chK(R))$ for all $h \in K(R)$. Therefore $K(Q^0) = Ann(cK(R)) = Assas((cK(R))_R)$.

Converse is true by Theorem (6.1.3).

(2) Let $Q \in MinSpec(R)$. Then $\sigma^m(Q) = Q$ for some integer $m \geq 1$. Let $Q_1 = Q^0$. Then by Proposition (10.6.12) of McConnell and Robson [68] and Theorem (7.27) of Goodearl and Warfield [38], $Q_2 = K(Q_1) \in MinSpec(K(R))$.

Conversely suppose that $P \in MinSpec(K(R))$. Then $P \cap R = Q^0$ for some $Q \in Spec(R)$ and Q contains a minimal prime Q_1. Then $P \supseteq K(R)Q_1^0$, which is a prime ideal of $K(R)$. Hence $P = K(R)Q_1^0$. □

6.3 Associated Primes Ideals of Skew Polynomial Rings of Derivation Type

Goodearl and Warfield in Theorem (2.22) of [38] that if δ is a derivation of a commutative Noetherian ring R which is also an algebra over $\mathbb{Q}$ and P is a prime ideal of $R[x;\delta]$, then $P \cap R$ is a prime ideal of R and if S is a prime ideal of R with $\delta(S) \subseteq S$, then $S[x;\delta]$ is a prime ideal of $R[x;\delta]$. Gabriel proved in [33] that if R is a right Noetherian ring which is also an algebra over $\mathbb{Q}$ and P is a prime ideal of $R[x;\delta]$, then $P \cap R$ is a prime ideal of R.

6.3.1 Proposition:

Let R be a Noetherian $\mathbb{Q}$-algebra, σ an automorphism of R and δ be a derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$, for all $a \in R$. Then $e^{t\delta}$ is an automorphism of $T = R[[t]]$.

Proof. The proof is on the same lines as in Seidenberg [84] and a sketch in the non-commutative case is provided in Blair and Small [18]. □

6.3.2 Lemma:

Let R be a Noetherian $\mathbb{Q}$-algebra and δ be a derivation of R. Let T as usual. Then an ideal I of R is δ-invariant if and only if IT is $e^{t\delta}$-invariant.

Proof. Proof is obvious. □

6.3.3 Proposition:

Let R be a ring and T as usual. Then:

(1) $Q \in Ass(R_R)$ implies that $QT \in Ass(T_T)$.

(2) $P \in Ass(T_T)$ implies that $(P \cap R) \in Ass(R_R)$ and $P = (P \cap R)T$.

Proof. Proof is obvious □

6.3.4 Proposition:

Let R be a ring and T be as usual. Then:

(1) $P \in MinSpec(T)$ implies that $(P \cap R) \in MinSpec(R)$ and $P = (P \cap R)T$.

(2) $Q \in MinSpec(R)$ implies that $QT \in MinSpec(T)$.

Proof. (1) Let $P \in MinSpec(T)$. Then $(P \cap R) \in Spec(R)$. Let $(P \cap R) \notin MinSpec(R)$. Suppose $P_1 \subset (P \cap R)$ is a minimal prime ideal of R. Then $P_1T \subset (P \cap R)T \subseteq P$.

(2) Let $Q \in MinSpec(R)$. Then $QT \in Spec(T)$. Let $QT \notin MinSpec(T)$. Suppose $Q_1 \subset QT$ is a minimal Prime ideal of T. Then $(Q_1 \cap R) \subset QT \cap R = Q$ □

6.3.5 Theorem:

(Theorem (3.6) of Bhat [9]). Let R be a Noetherian $\mathbb{Q}$-algebra and δ be a derivation of R. Let $P \in Ass(R_R) \cup MinSpec(R)$. Then $\delta(P) \subseteq P$.

Proof. Let $T = R[[t]]$. Now by Proposition (6.3.1) $e^{t\delta}$ is an automorphism of T. Let $P \in Ass(R_R) \cup MinSpec(R)$. Then by Proposition (6.3.3) and Proposition (6.3.4) $PT \in Ass(T_T) \cup MinSpec(T)$. Therefore there exists an integer $n \geq 1$ such that $(e^{t\delta})^n(PT) = PT$; i.e., $e^{nt\delta}(PT) = PT$. But R is a Q-algebra, therefore $e^{t\delta}(PT) = PT$, and now Lemma (6.3.2) implies that $\delta(P) \subseteq P$. □

6.3.6 Proposition:

(Theorem (3.7) of Bhat [9]). Let R be a Noetherian $\mathbb{Q}$-algebra and δ be a derivation of R. Then:

(1) $P \in Ass(D(R)_{D(R)})$ if and only if $P = D(P \cap R)$ and $P \cap R \in Ass(R_R)$.

(2) $P \in MinSpec(D(R))$ if and only if $P = D(P \cap R)$ and $P \cap R \in MinSpec(R)$.

Proof. (1) Let $P_1 \in Ass(R_R)$. Then $\delta(P_1) \subseteq P_1$ by Theorem (6.3.5). Let $P_1 = Ann(cR) = Assas((cR)_R), c \in R$. Now by Proposition (14.2.5)(ii) of McConnell and Robson [68] $D(P_1) \in Spec(D(R))$ and for any $h \in D(R)$, $D(P_1) = Assas((ch.D(R))_R)$.
Converse can be proved on the same lines as in Theorem (6.2.1).

(2) Let $P_1 \in MinSpec(R)$. Then $\delta(P_1) \subseteq P_1$ by Theorem (6.3.5). Therefore by Proposition (14.2.5)(ii) of McConnell and Robson [68] $D(P_1) \in Spec(D(R))$. Suppose $P_2 \subset D(P_1)$ is a minimal prime ideal of $D(R)$. Then $P_2 = D(P_2 \cap R) \subset D(P_1) \in MinSpec(D(R))$. So $P_2 \cap R \subset P_1$ which is not possible.

Conversely suppose that $P \in MinSpec(D(R))$. Then $P \cap R \in Spec(R)$ by Lemma (2.21) of Goodearl and Warfield [38]. Let $P_1 \subset P \cap R$ be a minimal prime ideal of R. Then $D(P_1) \subset D(P \cap R)$ and as in first paragraph $D(P_1) \in Spec(D(R))$, which is a contradiction. Hence $P \cap R \in MinSpec(R)$. □

For more details and some basic results for the rings $R[x; \sigma, \delta]$, $R[x; \sigma]$ and $R[x; \delta]$, refer to Chapters (1) and (2) of Goodearl and Warfield [38], [41].

6.4 Completely Prime Ideals of Skew Polynomial Rings

We begin with the following:

6.4.1 Lemma:

Let R be a ring. Let σ be an automorphism of R.

(1) If P is a prime ideal of $S(R)$ such that $x \notin P$, then $P \cap R$ is a prime ideal of R and $\sigma(P \cap R) = P \cap R$.

(2) If U is a prime ideal of R such that $\sigma(U) = U$, then $S(U)$ is a prime ideal of $S(R)$ and $S(U) \cap R = U$.

Proof. The proof follows on the same lines as in Lemma (10.6.4) of McConnell and Robson [68]. □

6.4.2 Lemma:

[Theorem (3.22) of Goodearl and Warfield [41]]. Let R be a commutative Noetherian $\mathbb{Q}$-ring. Let δ be an derivation of R.

(1) If P is a prime ideal of $D(R)$, then $P \cap R$ is a prime ideal of R and $\delta(P \cap R) \subseteq P \cap R$.

(2) If U is a prime ideal of R such that $\delta(U) \subseteq U$, then $D(U)$ is a prime ideal of $D(R)$ and $D(U) \cap R = U$.

Proof. 1) This is contained in Lemmas (3.18) and (3.21) of Goodearl and Warfield [41].

2) See Lemma (3.19) of Goodearl and Warfield [41]. □

Regarding the relation between the completely prime ideals of a ring R and those of $O(R)$, we have the following:

6.4.3 Theorem:

(Theorem (2.4) of Bhat [13]). Let R be a ring, σ an automorphism of R and δ a σ a σ-derivation of R. Then:

(1) For any completely prime ideal P of R with $\delta(P) \subseteq P$ and $\sigma(P) = P$, $O(P)$ is a completely prime ideal of $O(R)$.

(2) For any completely prime ideal U of $O(R)$, $U \cap R$ is a completely prime ideal of R.

Proof. (1) Let P be a completely prime ideal of R. Now let

$$f(x) = \sum_{i=0}^{n} x^i a_i \in O(R) \text{ and } g(x) = \sum_{j=0}^{m} x^j b_j \in O(R)$$

be such that $f(x)g(x) \in O(P)$. Suppose $f(x) \neq O(P)$. We will show that $g(x) \in O(P)$. We use induction on n and m. For $n = m = 1$ the verification is easy. We check for $n = 2$ and $m = 1$. Let

$$f(x) = x^2 a + xb + c \text{ and } g(x) = xu + v.$$

Now $f(x)g(x) \in O(P)$ with $f(x) \neq O(P)$. The possibilities are $a \neq P$ or $b \neq P$ or $c \neq P$ or any two out of these three do not belong to P. We verify case by case.

Let $b \notin P$. Now $\sigma(a)u \in P$. Suppose $u \notin P$, then $\sigma(a) \in P$ and therefore, $a \in P$, $\delta(a) \in P$. Now $\delta(a)u + \sigma(b)u + av \in P$ implies that $\sigma(b)u \in P$ which in turn implies that $b \in P$, which is not the case. Therefore we have $u \in P$. Now $\delta(b)u + \sigma(c)u + bv \in P$ implies that $bv \in P$ and therefore, $v \in P$. Thus we have $g(x) \in O(P)$.

Let $c \notin P$. Now $\sigma(a)u \in P$. Suppose, $u \notin P$, then as above $a \in P$, $\delta(a) \in P$. Now $\delta(a)u + \sigma(b)u + av \in P$ implies that $\sigma(b)u \in P$. Now $u \notin P$ implies that $\sigma(b) \in P$; i.e. $b \in P$, $\delta(b) \in P$. Also $\delta(b)u + \sigma(c)u + bv \in P$ implies $\sigma(c)u \in P$ and therefore, $\sigma(c) \in P$ which is not the case. Thus we have $u \in P$. Now $\delta(c)u + cv \in P$ implies $cv \in P$, and so $v \in P$. Therefore $g(x) \in O(P)$.

Now suppose the result is true for k, $n = k > 2$ and $m = 1$. We will prove for $n = k + 1$. Let

$$f(x) = x^{k+1}a_{k+1} + x^k a_k + ...xa_1 + a_0, \text{ and } g(x) = xb_1 + b_0$$

be such that $f(x)g(x) \in O(P)$, but $f(x) \notin O(P)$. We will show that $g(x) \in O(P)$. If $a_{k+1} \notin P$, then equating coefficients of x^{k+2}, we get $\sigma(a_{k+1})b_1 \in P$, which implies that $b_1 \in P$. Now equating coefficients of x^{k+1}, we get $\sigma(a_k)b_1 + a_{k+1}b_0 \in P$, which implies that $a_{k+1}b_0 \in P$, and therefore, $b_0 \in P$. Hence $g(x) \in O(P)$.

If $a_j \notin P$, $0 \leq j \leq k$, then using induction hypothesis, we get that $g(x) \in O(P)$. Therefore the statement is true for all n. Now using the same process, it can be easily seen that the statement is true for all m also.

(2) Let U be a completely prime ideal of O(R). Suppose $a, b \in R$ are such that $ab \in U \cap R$ with $a \notin U \cap R$. This means that $a \notin U$ as $a \in R$. Thus we have $b \in U$, and thus $b \in U \cap R$. □

6.5 Strongly Prime Ideals of Skew Polynomial Rings

Recall that a prime ideal P of a ring R is said to be strongly prime if for all a, $b \in R$, either $aP \subseteq bR$ or $bR \subseteq aP$.

The following example shows that extension of a strongly prime ideal need not be a strongly prime ideal:

6.5.1 Example:

(Bhat [13]). Let $R = \underline{\mathbb{Q}[t]} = (t^2)$. Let $\sigma = id$ and $\delta = 0$. For all $pt \notin Q[t]$, we denote by $\overline{p(t)}$ the image of $p(t)$ under the natural projection $\mathbb{Q}[t] \to R$.

Now $P = \bar{t}R$ is a strongly prime ideal of R. Let $a = 1$ and $b = x$ and $J = PR[x] = \bar{t}R[x]$. Then neither $aJ \subseteq bR[x]$ nor $bR[x] \subseteq aJ$. Therefore, J is not a strongly prime ideal of R[x].

6.5.2 Example:

(Bhat [13]). Let $R = \mathbb{Z}_p$. This is in fact a discrete valuation domain, and therefore, its maximal ideal $P = pR$ is strongly prime. But $pR[x]$ is not strongly prime in $R[x]$ because it is not comparable with $xR[x]$ (so the condition of being strongly prime in $R[x]$ for $a = 1$ and $b = x$).

Motivated by these developments we introduce a stronger type of primary decomposition (known as transparency) for a non-commutative Noetherian ring.

6.6 Transparent Rings and Their Extensions

We begin this section with the following:

6.6.1 Definition:

A Noetherian ring R is said to be a *transparent ring* if there exist irreducible ideals I_j, $1 \leq j \leq n$ such that $\cap_{j=1}^{n} I_j = 0$ and each R/I_j has a right Artinian quotient ring. It can be easily seen that an integral domain is a transparent ring, a commutative Noetherian ring is a transparent ring and so is a Noetherian ring having an Artinian quotient ring. A fully bounded Noetherian ring is also a transparent ring.

6.6.2 Corollary:

Let R be a semiprime Noetherian ring and σ an automorphism of R. Then $T = R[[x; \sigma]]$ is also a semiprime Noetherian ring.

6.6.3 Lemma:

Let R be a Noetherian ring and T as usual. Then:

(1) Let $U \in MinSpec(R)$ be such that $\sigma(U) = U$. Then $UT \in MinSpec(T)$.

(2) $P \in MinSpec(T)$ implies $P \cap R \in MinSpec(R)$ and $P = (P \cap R)T$.

Proof. (1) Let $U \in MinSpec(R)$. Then $UT \in Spec(T)$ by Corollary (8.6). Suppose $UT \notin MinSpec(T)$. Let $U_1 \subset UT$ be a minimal prime ideal of T. Then $U_1 \cap R \subset UT \cap R = U$ which is not possible as $U_1 \cap R \in Spec(R)$ and $U \in MinSpec(R)$. Therefore $UT \in MinSpec(T)$.

(2) Let $P \in MinSpec(T)$. Then $P \cap R \in Spec(R)$. Suppose $(P \cap R) \notin MinSpec(R)$. Let $P_1 \subset P \cap R$ be a minimal prime ideal of R. Then $P_1T \subset (P \cap R)T \subset P$ which is not possible as $P \in MinSpec(T)$ and $P_1T \in Spec(T)$. Therefore $P \cap R \in MinSpec(R)$. □

We also know that if R is a Noetherian ring and $U \in Min.Spec(R)$, then $\sigma^j(U) \in MinSpec(R)$ for all positive integers j. Also $MinSpec(R)$ is finite by Theorem (2.4) of Goodearl and Warfield [38]. Therefore there exists a positive m such that $\sigma^m(U)$ for all $U \in MinSpec(R)$. In Lemma (3.4) of [33], Gabriel proved that if R is a Noetherian $\mathbb{Q}$-algebra and δ is a derivation of R, then $\delta(P) \subseteq P$ for all $P \in MinSpec(R)$. In this chapter we generalize this results for a σ-derivation δ and prove the following:

6.6.4 Lemma:

Let R be a Noetherian $\mathbb{Q}$-algebra. Let σ be an automorphism of R and δ a σ-derivation of R. Then:

(1) $\sigma(N(R)) = N(R)$.

(2) If $P \in MinSpec(R)$ is such that $\sigma(P) = P$, then $\delta(P) \subseteq P$.

Proof. (1) The proof is obvious.

(2) Let T be as usual. Now by Lemma (6.3.1) $e^{t\delta}$ is an automorphism of T. Let $P \in MinSpec(R)$. Then by Lemma (6.6.3) $PT \in MinSpec(T)$. So there exists an integer $n \geq 1$ such that $(e^{t\delta})^n(PT) = PT$; i.e., $e^{nt\delta}(PT) = PT$. But R is a $\mathbb{Q}$-algebra, therefore $e^{t\delta}(PT) = PT$, and so Lemma (6.3.2) implies that $\delta(P) \subseteq P$. □

6.6.5 Lemma:

Let R be a right Noetherian ring. Then there exists irreducible ideals $I_j, 1 \leq j \leq n$ of R such that $\cap_{j=1}^{n} I_j = 0$ (proof is obvious)

6.6.6 Lemma:

Let R be a Noetherian ring having a right Artinian quotient ring. Then R is a transparent ring.

Proof. Let $Q(R)$ be the right quotient ring of R. Now for any ideal J of $Q(R)$, the contraction J^c of J is an ideal of R and the extension of J^c is J; i.e., $J^{ce} = J$. For this see Proposition (9.19) of Goodearl and Warfield [38]. Let $I_j, 1 \leq j \leq n$ be the irreducible ideals of $Q(R)$ such that $0 = \cap_{j=1}^{n} I_j$. Also each $Q(R)/I_j$ is an Artinian ring. Let $I_j^c = K_j$. Then it is not difficult to see that R/K_j has Artinian quotient ring $Q(R)/I_j$. Moreover $\cap_{j=1}^{n} K_j = 0$. Hence R is a transparent ring. □

6.6.7 Definition:

Let P be a prime ideal of a commutative ring R. Then the symbolic power of P for a positive integer n is denoted by $P^{(n)}$ and is defined as $P^{(n)} = \{a \in R$ such that there exists some $d \in R, d \notin P$ such that $da \in P^n\}$. Also if I is an ideal of R, define as usual $\sqrt{I} = \{a \in R$ such that $a^n \in I$ for some $n \in \mathbb{Z}$ with $n \geq 1\}$.

6.6.8 Lemma:

Let R be a commutative Noetherian ring and let σ be an automorphism of R. Then there exists a positive integer m such that, for all $P \in Ass(R_R)$:

(1) $\sigma^m(P) = P$.

(2) $\sigma^m(P^{(k)}) = P^{(k)}$ for all $k \geq 0$.

Proof. (1) Since $Ass(R_R)$ is a finite set and $\sigma^j(P) \in Ass(R_R)$ for any integer $j \geq 1$ whenever $P \in Ass(R_R)$, there exists an integer $m \geq 1$ such that $\sigma^m(P) = P$.

(2) Denote σ^m by θ. We have $\theta(P) = P$. Let $a \in P^{(k)}$. Then there exists some $d \in R, d \notin P$ such that $da \in P^k$. Therefore $\theta(da) \in \theta(P^k)$; i.e., $\theta(d)\theta(a) \in (\theta(P))^k = P^k$. Now $\theta(d) \notin P$ implies that $\theta(a) \in P^{(k)}$. Therefore $\theta(P^{(k)}) \subseteq P^{(k)}$. Hence $\theta(P^{(k)}) = P^{(k)}$. □

6.6.9 Lemma:

Let R be a commutative Noetherian $\mathbb{Q}$-algebra. Let σ be an automorphism of R and δ a σ-derivation of R. Let P be a prime ideal of R such that $\sigma(P) = P$ and $\delta(P) \subseteq P$. Then $\delta(P^{(k)}) \subseteq P^{(k)}$, for any integer $k \geq 1$.

Proof. Let $a \in P^{(k)}$. Then there exists $d \notin P$ such that $da \in P^k$. Let $da = p_1p_2...p_k$, $p_i \in P$. Then

$$\begin{aligned}
\delta(da) &= \delta(p_1p_2...p_{k-1})\sigma(p_k) + p_1p_2...p_{k-1}\delta(p_k) \\
&= \delta(p_1p_2...p_{k-2})\sigma(p_{k-1})\sigma(p_k) + p_1p_2...p_{k-2}\delta(p_{k-1})\sigma(p_k) + p_1p_2...p_{k-1}\delta(p_k) \\
&\;\;\vdots \\
&= \delta(p_1)\sigma(p_2...p_k) + ... + p_1p_2...p_{k-2}\delta(p_{k-1})\sigma(p_k) + p_1p_2...p_{k-1}\delta(p_k).
\end{aligned}$$

This lies in P^k as $\sigma(P) = P$ and $\delta(P) \subseteq P$; i.e., $\sigma(d)\delta(a) + \delta(d)a \in P^k$. Now $a \in P^{(k)}$, and, therefore $\sigma(d)\delta(a) \in P^{(k)}$. Now $d_1\sigma(d)\delta(a) + d_1\delta(d)a \in P^k$, which implies that $d_1\sigma(d)\delta(a) \in P^k$ and since $d_1\sigma(d) \notin P$, we have $\delta(a) \in P^{(k)}$ □

6.6.10 Theorem:

(Theorem (2.11) of Bhat [8]). Let R be a ring which is an order in a right Artinian ring S. Then $O(R)$ is an order in a right Artinian ring.

Proof. By using (Proposition (2.1), Lemma (2.5) and Theorem (2.6)) of Bhat [8], we get a result. □

6.6.11 Theorem:

Let R be a commutative Noetherian $\mathbb{Q}$-algebra, σ be an automorphism of R. Then there exists an integer $m \geq 1$ such that the skew-polynomial ring $R[x; \alpha, \delta]$ is a transparent ring, where $\sigma^m = \alpha$ and δ is an α-derivation of R such that $\alpha(\delta(a)) = \delta(\alpha(a))$, for all $a \in R$.

Proof. $R[x; \alpha, \delta]$ is Noetherian by Hilbert Basis Theorem, namely Theorem (1.12) of Goodearl and Warfield [38]. Now R is a commutative Noetherian $\mathbb{Q}$-algebra, therefore, the ideal (0) has a reduced primary

decomposition. Let $I_j, 1 \leq j \leq n$ be irreducible ideals of R such that $(0) = \cap_{j=1}^{n} I_j$. For this see Theorem (4) of Zariski and Samuel [92]. Let $\sqrt{I_j} = P_j$, where P_j is a prime ideal belonging to I_j. Now by Theorem (23) of Zariski and Samuel [92] there exists a positive integer k such that $P_j^{(k)} \subseteq I_j, 1 \leq j \leq n$. Therefore we have $\cap_{j=1}^{n} P_j^k = 0$. Now $P_j \in Ass(R_R), 1 \leq j \leq n$ by first uniqueness Theorem. Now each P_j contains a minimal prime ideal U_j by Proposition (2.3) of Goodearl and Warfield [38] and since $MinSpec(R)$ is finite, there exists an integer $m \geq 1$ such that $\sigma^m(U_j) = U_j$. Denote σ^m by α. Now $\alpha(U_j) = U_j$, and therefore, $\alpha(U_j^{(k)}) = U_j^{(k)}$ by Lemma (6.6.8). Also $\delta(U_j) \subseteq U_j$ by Lemma (6.6.4) and therefore, $\delta(U_j^{(k)}) \subseteq U_j^{(k)}$ by Lemma (6.6.9). Thus $U_j^{(k)}[x; \alpha, \delta]$ is an ideal of $R[x; \alpha, \delta]$. Now $R/U_j^{(k)}$ has no embedded primes, therefore $R/U_j^{(k)}$ has an Artinian quotient ring by Theorem (2.11) of Robson [81]. Now by Theorem (6.6.10) $R[x; \alpha, \delta]/U_j^{(k)}[x; \alpha, \delta]$ has an Artinian quotient ring. Moreover $\cap_{j=1}^{n} U_j^{(k)}[x; \alpha, \delta] = 0$, therefore, Lemma (6.6.6) implies that $R[x; \alpha, \delta]$ is a transparent ring. □

6.6.12 Remarks:

(1) Let R be a Noetherian ring having an Artinian quotient ring. Let σ be an automorphism of R and δ a σ-derivation of R. Then $R[x; \sigma, \delta]$ is a transparent ring.

(2) Let R be a commutative Noetherian ring and σ be an automorphism of R. Then the skew polynomial ring $R[x; \sigma]$ is a transparent ring.

(3) Let R be a commutative Noetherian ring and σ be an automorphism of R. Then the skew Laurent polynomial ring $R[x; x^{-1}, \sigma]$ is a transparent ring.

(4) Let R be a commutative Noetherian $\mathbb{Q}$-algebra and δ a derivation of R. Then the differential operator ring $R[x; \delta]$ is a transparent ring.

6.7 Transparent Skew Polynomial Rings (special cases)

In this section we study the Transparent ring property for $O(R) = R[x; \sigma, \delta]$.

6.7.1 Corollary:

Let R be a Noetherian $\sigma(*)$-ring and $U \in MinSpec(R)$. Then $U(S(R)) = U[x;\sigma]$ is a completely prime ideal of $S(R) = R[x;\sigma]$.

Proof. Let $U \in MinSpec(R)$. Then $\sigma(U) = U$ by Theorem (4.6.11). Now result follows from Proposition (4.6.9). □

6.7.2 Proposition:

(Proposition (4) of Bhat [15]). Let R be a Noetherian $\sigma(*)$-ring which is also an algebra over $\mathbb{Q}$ and δ a σ-derivation of R such that $\delta(\sigma(a)) = \sigma(\delta(a))$, for all $a \in R$. Then $\delta(U) \subseteq U$ for all $U \in MinSpec(R)$.

Proof. Let $U \in MinSpec(R)$. Then $\sigma(U) = U$ by Theorem (4.6.11). Consider the set

$$T = \{a \in U | \text{ such that } \delta^k(a) \in U \text{ for all integers } k \geq 1\}.$$

First of all, we will show that T is an ideal of R. Let $a, b \in T$. Then $\delta^k(a) \in U$ and $\delta^k(b) \in U$ for all integers $k \geq 1$. Now $\delta^k(a-b) = \delta^k(a) - \delta^k(b) \in U$ for all $k \geq 1$. Therefore $a - b \in T$. Therefore T is a δ-invariant ideal of R.

We will now show that $T \in Spec(R)$. Suppose $T \notin Spec(R)$. Let $a \notin T$, $b \notin T$ be such that $aRb \subseteq T$. Let t, s be least such that $\delta^t(a) \notin U$ and $\delta^s(b) \notin U$. Now there exists $c \in R$ such that $\delta^t(a)c\sigma^t(\delta^s(b)) \notin U$. Let $d = \sigma^{-t}(c)$. Now $\delta^{t+s}(adb) \in U$ as $aRb \subseteq T$. This implies on simplification that

$$\delta^t(a)\sigma^t(d)\sigma^t(\delta^s(b)) + u \in U,$$

where u is sum of terms involving $\delta^l(a)$ or $\delta^m(b)$, where $l < t$ and $m < s$. Therefore by assumption $u \in U$ which implies that $\delta^t(a)\sigma^t(d)\sigma^t(\delta^s(b)) \in U$. This is a contradiction. Therefore, our supposition must be wrong. Hence $T \in Spec(R)$. Now $T \subseteq U$, so $T = U$ as $U \in MinSpec(R)$. Hence $\delta(U) \subseteq U$. □

6.7.3 Remark:

In above Proposition the condition that $\delta(\sigma(a)) = \sigma(\delta(a))$, for all $a \in R$ is necessary. For example if $s = t = 1$, then $a \in U$, $b \in U$ and therefore, $\sigma^i(a) \in U$, $\sigma^i(b) \in U$ for all integers $i \geq 1$ as $\sigma(U) = U$. Now $\delta^2(adb) \in U$ implies that

$$\delta(a)\sigma(d)\delta(\sigma(b)) + \delta(a)\sigma(d)\sigma(\delta(b)) \in U.$$

If $\delta(\sigma(a)) \neq \sigma(\delta(a))$, for all $a \in R$, then we get nothing out of it and if $\delta(\sigma(a)) = \sigma(\delta(a))$, for all $a \in R$, we get $\delta(a)\sigma(d)\sigma(\delta(b)) \in U$ which gives a contradiction.

6.7.4 Theorem:

Let R be a commutative Noetherian $\sigma(*)$-ring, which is also an algebra over $\mathbb{Q}$, (σ an automorphism of R). Let δ be a σ-derivation of R such that $\delta(\sigma(a)) = \sigma(\delta(a))$, for all $a \in R$. Then $O(R) = R[x; \sigma, \delta]$ is a Transparent ring.

Proof. R is a commutative Noetherian $\mathbb{Q}$-algebra, therefore, the ideal (0) has a reduced primary decomposition. Let I_j, $1 \leq j \leq n$ be irreducible ideals of R such that $(0) = \cap_{j=1}^{n} I_j$. For this see Theorem (4) of Zariski and Samuel [92]. Let $\sqrt{I_j} = P_j$, where P_j is a prime ideal belonging to I_j. Now $P_j \in Ass(R_R)$, $1 \leq j \leq n$. Therefore we have $\cap_{j=1}^{n} P_j^{(k)} = 0$. Now each P_j contains a minimal prime ideal U_j by Proposition (2.3) of Goodearl and Warfield [38], therefore $\cap_{j=1}^{n} U_j^{(k)} = 0$. Now Theorem (4.6.11) implies that $\sigma(U_j) = U_j$, for all j, $1 \leq j \leq n$. Therefore Proposition (6.7.2) implies that $\delta(U_j) \subseteq U_j$, for all j, $1 \leq j \leq n$. Now Lemma (6.6.8) implies that $\sigma(U_j)^{(k)} = U_j^{(k)}$ and Lemma (6.6.9) implies that $\delta(U_j)^{(k)} \subseteq U_j^{(k)}$, for all j, $1 \leq j \leq n$ and for all $k \geq 1$. Therefore $O(U_j^{(k)})$ is an ideal of $O(R)$ and $\cap_{j=1}^{n} O(U_j^{(k)}) = 0$.

Now $R/U_j^{(k)}$ has an Artinian quotient ring, as it has no embedded primes, therefore $O(R)/O(U_j)^{(k)}$ has also an Artinian quotient ring by Theorem (2.11) of Bhat [8]. Hence $O(R) = R[x; \sigma, \delta]$ is Transparent ring. □

Before we study the transparency of Ore extensions over weak σ-rigid rings, we have the following:

Recall that an ideal I of a ring R is said to be completely semiprime if $a^2 \in I$ implies that $a \in I$.

We now have the following Theorem:

6.7.5 Theorem:

(Theorem (6) of Bhat [16]). Let R be a Noetherian ring such that $N(R)$ is an ideal of R. Let σ be an automorphism of R. Then R is a weak σ-rigid ring implies that $N(R)$ is completely semiprime.

Proof. See Theorem (4.6.15). □

6.7.6 Corollary:

Let R be a commutative Noetherian ring. Let σ be an automorphism of R. Then R is a weak σ-rigid ring if and only if $N(R)$ is completely semiprime ideal of R.

Proof. R is commutative Noetherian implies that $N(R)$ is an ideal of R. It is easy to see that $\sigma(N(R)) = N(R)$.

Now let R be a weak σ-rigid ring. We will show that $N(R)$ is completely semiprime. Let $a \in R$ be such that $a^2 \in N(R)$. Then

$$a\sigma(a)\sigma(a\sigma(a)) = a\sigma(a)\sigma(a)\sigma^2(a) \in \sigma(N(R)) = N(R).$$

Therefore, $a\sigma(a) \in N(R)$ and hence $a \in N(R)$. So $N(R)$ is completely semiprime.

Conversely let $N(R)$ be completely semiprime. We will show that R is a weak σ-rigid ring. Let $a \in R$ be such that $a\sigma(a) \in N(R)$. Now $a\sigma(a)\sigma^{-1}(a\sigma(a)) \in N(R)$ implies that $a^2 \in N(R)$, and so $a \in N(R)$. Hence R is a weak σ-rigid ring. □

6.7.7 2-primal skew polynomial rings

Recall that a ring R is called a 2-primal if $P(R) = N(R)$, i.e. if the prime radical is a completely semiprime ideal. Minimal prime ideals of 2-primal rings have been discussed by Kim and Kwak in [53]. 2-primal near rings have been discussed by Argac and Groenewald in [3].

2-primal rings have been studied in recent years and are being treated by authors for different structures. In [65], G. Marks discusses the 2-primal property of $R[x;\sigma,\delta]$, where R is a local ring, σ an automorphism of R and δ a σ-derivation of R. In G. Marks [65], it has been shown that for a local ring R with a nilpotent maximal ideal, the ore extension $R[x;\sigma,\delta]$ will or will not be 2-primal depending on the δ-stability of the

maximal ideal of R. In the case where $R[x;\sigma,\delta]$ is 2-primal, it will satisfy an even stronger condition; in the case where $R[x;\sigma,\delta]$ is not 2-primal, it will fail to satisfy an even weaker condition.

We note that a reduced ring (i.e., a ring with no non-zero nilpotent elements) is 2-primal and a commutative ring is also 2-primal. For further details on 2-primal rings, we refer the reader to [3, 10, 53, 65].

Example: Let $R = \mathbb{Q} \oplus \mathbb{Q}$ with $\sigma(a,b) = (b,a)$. Then the only σ-invariant ideals of R are 0 and R, and so R is σ-prime. Let δ: $R \to R$ be defined by $\delta(r) = ra - a\sigma(r)$, where $a = (0,\alpha) \in R$. Then δ is a σ-derivation of R and $R[x;\sigma,\delta]$ is prime and $P(R[x;\sigma,\delta]) = 0$. But $(x(1,0))^2 = 0$ as $\delta(1,0) = -(0,\alpha)$. Therefore $R[x;\sigma,\delta]$ is not 2-primal. If δ is taken to be the zero map, then even $R[x;\sigma]$ is not 2-primal.

6.7.8 Proposition:

(Proposition (2) of Bhat [16]). Let R be a 2-primal right Noetherian ring which is also an algebra over $\mathbb{Q}$. Let σ be an automorphism of R such that R is a weak σ-rigid ring and δ a σ-derivation of R. Then $\sigma(U) = U$ and $\delta(U) \subseteq U$ for all $U \in MinSpec(R)$.

Proof. Let R be 2-primal weak σ-rigid ring. Then $N(R) = P(R)$, i.e. P(R) is completely semiprime.

We next show that $\sigma(U) = U$ for all $U \in MinSpec(R)$. Let $U = U_1$ be a minimal prime ideal of R. Now Theorem (2.4) of Goodearl and Warfield [38] implies that $MinSpec(R)$ is finite. Let $U_2, U_3, ..., U_n$ be the other minimal primes of R. Suppose that $\sigma(U) \neq U$. Then $\sigma(U)$ is also a minimal prime ideal of R. Renumber so that $\sigma(U) = U_n$. Let $a \in \cap_{i=1}^{n-1} U_i$. Then $\sigma(a) \in U_n$, and so $a\sigma(a) \in \cap_{i=1}^{n} U_i = P(R)$. Now $P(R)$ is completely semiprime implies that $a \in P(R)$ and thus $\cap_{i=1}^{n-1} U_i \subseteq U_n$ which implies that $U_i \subseteq U_n$ for some $i \neq n$, which is impossible. Hence, $\sigma(U) = U$ for all $U \in MinSpec(R)$.

Let now $T = \{a \in U|$ such that $\delta^k(a) \in U$ for all integers $k \geq 1\}$. First of all, we will show that T is an ideal of R. Let $a, b \in T$. Then $\delta^k(a) \in U$ and $\delta^k(b) \in U$ for all integers $k \geq 1$. Now $\delta^k(a-b) = \delta^k(a) - \delta^(k)(b) \in U$ for all $k \geq 1$. Therefore $a - b \in T$. Therefore T is a

δ-invariant ideal of R.

We will now show that $T \in Spec(R)$. Suppose $T \notin Spec(R)$. Let $a \notin T$, $b \notin T$ be such that $aRb \subseteq T$. Let t, s be least such that $\delta^t(a) \notin U$ and $\delta^t(b) \notin U$, i.e. $\delta^m(a) \in U$ and $\delta^k(b) \in U$ for $m < t$ and $k < s$.

Now there exists $c \in R$ such that $\delta^t(a)c\sigma^t(\delta^s)(b) \notin U$. Let $d = \sigma^{-t}(c)$. Now $\delta^{t+s}(abd) \in U$ as $aRb \subseteq T$. This implies on simplification that $\delta^t(a)\sigma^t(d)\sigma^t(\delta^s(b)) + u \in U$, where u is sum of terms involving $\delta^l(a)$ or $\delta^m(b)$, where $l < t$ and $m < s$. Therefore by assumption $u \in U$ which implies that $\delta^t(a)\sigma^t(d)\sigma^t(\delta^s(b)) \in U$. This is a contradiction. Therefore, our supposition must be wrong. Hence $T \in Spec(R)$. Now $T \subseteq U$, so $T = U$ as $U \in MinSpec(R)$. Hence $\delta(U) \subseteq U$. □

6.7.9 Lemma:

Let R be a right Noetherian ring which is also an algebra over $\mathbb{Q}$. Let σ be an automorphism of R such that R is a weak σ-rigid ring and δ be a σ-derivation of R. Then

(1) If U is a minimal prime ideal of R, then $O(U)$ is a minimal prime ideal of $O(R)$ and $O(U) \cap R = U$

(2) If P is a minimal prime ideal of $O(R)$, then $P \cap R$ is a minimal prime ideal of R.

Proof. (1) Let U be a minimal prime ideal of R. Then by Proposition (6.7.8) $\sigma(U) = U$ and $\delta(U) \subseteq U$. Now on the same lines as in Theorem (2.22) of Goodearl and Warfield [38] we have $O(U) \in Spec(O(R))$. Suppose $L \subset O(U)$ be a minimal prime ideal of $O(R)$. Then $L \cap R \subset U$ is a prime ideal of R, a contradiction. Therefore $O(U) \in MinSpec(O(R))$. Now it is easy to see that $O(U) \cap R = U$.

(2) We note that $x \notin P$ for any prime ideal P of $O(R)$ as it is not a zero divisor. Now the proof follows on the same lines as in Theorem (2.22) of Goodearl and Warfield [38] using Lemma(2.1) and Lemma(2.2) of Bhat [7] and Proposition (6.7.8). □

6.7.10 Theorem:

(Theorem (5) of Bhat [16]). Let R be a commutative Noetherian weak σ-rigid ring, which is also an algebra over $\mathbb{Q}$. Let σ be an automorphism

of R and δ a σ-derivation of R. Then $O(R) = R[x; \sigma, \delta]$ is a Transparent ring.

Proof. Now R is a commutative Noetherian $\mathbb{Q}$-algebra, therefore, the ideal (0) has a reduced primary decomposition. Let $I_j, 1 \leq j \leq n$ be irreducible ideals of R such that $(0) = \cap_{j=1}^{n} I_j$. For this see Theorem (4) of Zariski and Samuel [92]. Let $\sqrt{I_j} = P_j$, where P_j is a prime ideal belonging to I_j. Now $P_j \in Ass(R_R), 1 \leq j \leq n$ by first uniqueness Theorem. Now by Theorem (23) of Zariski and Samuel [92], there exists a positive integer k such that $P_j^{(k)} \subseteq I_j, 1 \leq j \leq n$. Therefore we have $\cap_{j=1}^{n} P_j^k = 0$. Now each P_j contains a minimal prime ideal U_j by Proposition (2.3) of Goodearl and Warfield [38], therefore $\cap_{j=1}^{n} U_j^k = 0$. Now R is commutative implies that R is 2-primal, and therefore, Proposition (6.7.8) implies that $\sigma(U_j) = U_j$ and $\delta(U_j) \subseteq U_j$, for all j, $1 \leq j \leq n$. Now Lemma (6.6.8) implies that $\sigma(U_j)^{(k)} = U_j^{(k)}$ and Lemma (6.6.9) implies that $\delta(U_j^{(k)}) \subseteq U_j^{(k)}$, for all $j, 1 \leq j \leq n$ and for all $k \geq 1$. Therefore, $O(U_j^{(k)})$ is an ideal of $O(R)$ and $\cap_{j=1}^{n} O(U_j^{(k)}) = 0$.
Now $R/U_j^{(k)}$ has an Artinian quotient ring, as it has no embedded primes, therefore $O(R)/O(U_j^{(k)})$ has also an Artinian quotient ring by Theorem (2.11) of Bhat [8]. Hence $O(R) = R[x; \sigma, \delta]$ is *transparent ring.* □

Now we take the case, when R is not necessarily commutative.

6.7.11 Theorem:

(Theorem (6) of Bhat [16]). Let R be a semiprime Noetherian weak σ-rigid ring, which is also an algebra over $\mathbb{Q}$. Let σ be an automorphism of R and δ a σ-derivation of R. Then R is a transparent ring and $O(R) = R[x; \sigma, \delta]$ is also a Transparent ring.

Proof. R is Noetherian therefore, Theorem (2.4) of Goodearl and Warfield [38] implies that $MinSpec(R)$ is finite. Also R is semiprime implies that $\cap_{P \in MinSpec(R)} P = 0$. Now Proposition (6.7.8) implies that $\sigma(P) = P$ and $\delta(P) \subseteq P$, for all $P \in MinSpec(R)$. Therefore $O(P) = P[x; \sigma, \delta]$ is an ideal of $O(R)$ and $\cap_{P \in MinSpec(R)} O(P) = 0$. In fact $O(P)$ is a minimal prime ideal of $O(R)$ by Lemma (6.7.9). Now R/P has a right Artinian quotient ring by Theorem (5.12) of Goodearl and Warfield [38], and $\cap_{P \in MinSpec(R)} P = 0$ implies that R is a Transparent ring. Now Theorem (2.11) of Bhat [8] implies that $O(R)/O(P)$ has a right Artinian quotient

ring and hence $\cap_{P \in MinSpec(R)} O(P) = 0$ implies that $O(R) = R[x; \sigma, \delta]$ is a Transparent ring. □

Chapter

7

APPLICATIONS OF SKEW POLYNOMIAL RINGS

Over the past ten years, Skew polynomials have been successfully applied in many areas, including for example solving Ordinary differential Equations (see Bronstein and Petkousek [21], Chyzak and B. Salvy [25], Van Hoeij [90] and Singer [87], e.t.c.), Control Theory (see Chyzak - Quadrat - Robertz [26], Fliess Mounier [30] and Gluesing-Luerssen [35], etc.) and Coding Theory (see McEliece [69] and Piret [77], etc.)

7.1 Coding Theory

The problem of reliable communication is a very old one. Coding theory on the other hand is rather young. It was born in a now classic paper from (1948) "A mathematical theory of communication" by Shannon. The model is as follows. A sender wants to communicate a message to the receiver. Rather than sending it directly, the sender encodes the message and sends it through the noisy communication channel. When the message is received it might contain errors. We would like to prevent errors like this occurring in the digital world and somehow make sure we received the right message before we decode it. This ground breaking ideal of error correcting codes is due to Hamming. He developed it in his famous paper "error detecting and error correcting codes" in (1950). The coding theory is thus concerned with developing codes that have efficient encoding and decoding algorithms as well as the ability to detect and correct the errors in the communication.

This chapter is related to study of Skew codes, the codes over non-commutative polynomial rings which are a generalization of the usual ring of polynomials This was motivated by a paper of Boucher, Geiselmann and Ulmer [19] where they introduce them. Chapter 7 gives an introduction to basic principles of coding theory. It introduces a large family of linear codes, and within them, the cyclic codes and BCH (Bose Chaudhuri Hocquenbghem) codes.

7.1.1 Block Codes

By a *code* we will always mean a block code. A *block code* is a set of words (codewords, blocks) of length n, that take entries from an alphabet $\sum$ with q symbols and can be decoded independently from each other. If we denote by $\sum^n$ a set of all possible words of length n that take entries from $\sum$, then a block code C is a subset of $\sum^n$.

Codes that are not block codes, i.e. that have words which are not of constant length, are called convolutional codes.

We begin with some important definitions that we will use through out the chapter.

7.1.2 Definition:

The *Hamming distance* $d(x, y)$ between two words x, $y \in \sum^n$ is defined as a number of positions in which they differ:

$$d(x, y) = \sharp\{i : x_i \neq y_i, 1 \leq i \leq n\}$$

It can easily be checked that Hamming distance is a metric on $\sum^n$:

(1) $d(x, y) = d(y, x)$;

(2) $d(x, z) \leq d(x, y) + d(y, z)$;

(3) $d(x, y) = 0 \Leftrightarrow x = y$.

7.1.3 Definition:

The *minimum distance of code* C is

$$\min \{d(x, y) : x, y \in C, x \neq y\}.$$

7.1.4 Definition:

The *Hamming weight* $w(x)$ of a codeword x is the number of non-zero coordinates of x.

7.1.5 Hamming Codes:

Let $n := \frac{q^k-1)}{(q-1)}$. The [n, n-k] Hamming code over $\mathbb{F}_q$ is a code for which the parity check matrix has columns that are pairwise linearly independent (over $\mathbb{F}_q$), i.e. the columns are a maximal set of pairwise linearly independent vectors.

7.1.6 Theorem:

[Theorem (3.3.2) in Lint [63]]. Hamming codes are perfect.

Proof. By definition of a Hamming code of length n and dimension k over $\mathbb{F}_q$ we have $n = \frac{q^k-1)}{(q-1)}$. We know Hamming codes are 1-error correcting, so we want to consider disjoint spheres of radius one centered around codewords of C. Let c be a codeword. Then the number of n-tuples in $\mathbb{F}_q$ in a sphere of radius one centered around c, $|B_1(c)|$, is

$$|B_1(c)| = \begin{pmatrix} n \\ 0 \end{pmatrix} + \begin{pmatrix} n \\ 1 \end{pmatrix} = 1 + n(q-1) = q^k.$$

The number of codewords of C is q^{n-k}. Then $q^{n-k}q^k = q^n$, which is all of the $\mathbb{F}_q^n$. Thus C is perfect. □

7.1.7 Example:

[Example (3.3.3) in Lint [63]]. The [7, 4] binary Hamming code C has parity check matrix

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

If we consider two columns of H and the sum of these two (e.g. the first three columns of H), then there is a word of weight 3 in C with 1s in the positions corresponding to these columns (e.g. (1110000)). Therefore C has seven words of weight 3 which listed as rows of a matrix, form PG(2, 2).

7.1.8 Definition:

A code that is able to detect up to e errors is called e- *error detecting*. If it correct up to e errors, We call such a code e- *error-correcting*.

To introduce some algebraic structure into codes, we let the alphabet $\sum$ be a finite field $\mathbb{F}_q$ with q a prime power. The space $\sum^n$ then becomes an n-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$.

7.1.9 Linear Codes

Let $\mathbb{F}_q$ be a field with q elements and n an integer. A linear code C of length n and dimension k is a k dimensional linear subspace of $\mathbb{F}_q^n$. We use notation $[n, k]$ to refer to such a code. In other words, a *linear code* C is a subset of $\mathbb{F}_q^n$ such that

(1) $0 \in C$

(2) if x, $y \in C$, then $x + y \in C$

(3) for all $x \in C$ and $\lambda \in \mathbb{F}_q$, we have $\lambda x \in C$.

Codewords of a linear code are thus n-tuples over $\mathbb{F}_q$. An advantage of a linear code over a nonlinear one is that it is very easy to represent it. For a linear $[n, k]$ code C any $k \times n$ matrix whose rows from a basis for C completely determines the code. We call such a matrix a *generating matrix* of a code C.

We saw that the information rate of a code was defined as $\frac{log_q|C|}{n}$. For a linear code the number of codewords is $|C| = q^k$ so the information rate then simplifies to $\frac{k}{n}$. Another simplification we gain from imposing structure on a code is in computing its minimum distance. For an arbitrary, unstructured code one must check the distances between all possible pairs of words in order to find the minimum distance.

7.1.10 Theorem:

[Theorem (3) in Lekic [61]]. Let C be a linear code. Then its minimum distance is equal to the minimum weight.

Proof. Note that the weight function of a codeword x was defined as the number of non-zero coordinates of x and so we have $w(x) = d(0, x)$. Then

$$\begin{aligned} d(x, y) &= d(x - y, 0) \\ &= w(x - y) \\ &= w(z) \end{aligned}$$

Since x and y are in C which is linear, it follows that z is also a word in C. □

7.1.11 Cyclic Codes

Cyclic codes are a small subset of the set of linear codes. They are the most common block codes used in practice. These are a few reasons cyclic codes are nice to study. One is that they have a very rich algebraic structure, and another is that many important codes (BCH codes for example) are cyclic.

7.1.12 Definition:

A code C of length n is called *cyclic* if for every codeword

$$c = (c_0, c_1, ..., c_{n-1}) \text{ in } C.$$

We have that

$$c^{'} = (c_{n-1}, c_0, ..., c_{n-2}) \text{ is also in } C.$$

Even though we said cyclic codes were linear, it is not clear why that is the case from this definition. In principle it is possible to have nonlinear cyclic codes since the way we defined them does not require linearity. However, because of the advantages of imposing linearity it is common to only consider linear cyclic codes.

For a given $c \in C$ any number of right or left shifts on c also gives a codeword. This suggest the following construction. Let G denote a set of all possible right shifts of a word c. Then the linear span of G is the smallest linear cyclic code C containing c. By this construction it is clear that a single word determines a code. We call such a word a generator. A generator need not be unique. This deserves a more precise treatment. In order to do that it is convenient to think of codewords as polynomials in the following way. Let $\mathbb{F}_q$ denote a finite field of q elements and $\mathbb{F}_q[x]$ a ring of polynomials in x with coefficients in $\mathbb{F}_q$. To every codeword

$$c = (c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_q^n$$

we associate the code polynomial

$$c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1).$$

With this convention established we can sometimes abuse the notation and call a code polynomial $c(x)$ a codeword in C.

Note that a shifted codeword $c^{'} = (c_{n-1}, c_0, ..., c_{n-2})$ in C has associated polynomial

$$c^{'}(x) = c_{n-1} + c_0x + ... + c_{n-2}x^{n-1}$$

and that $c^{'}(x) = xc(x)$ modulo $x^n - 1$. In this way we can represent a single right cyclic shift between two codewords in C with a multiplication by x in a ring of polynomials modulo $x^n - 1$.

We know that applying any number of cyclic shifts on $c \in C$ gives us another codeword

$$x^{'}c(x) \bmod x^n - 1 \in C$$

so that any linear combination of words in C produces another word in C

$$\sum_{i=0}^{d} a_i x^i c(x) \bmod x^n - 1 \in C$$

where $a_i \in \mathbb{F}_q$. In other words, for any polynomial $a(x) \in \mathbb{F}_q[x]/(x^n - 1)$ and any codeword $c(x) \in C$ the product $a(x)c(x)$ is also in C.

7.1.13 Example:

Over $\mathbb{F}_2$ we have

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

There are altogether eight cyclic codes of length 7. One of these has 0 as the only code word and one contains all possible words. The code with generator $x - 1$ contains all words of even weight. The [7, 1] cyclic code has 0 and 1 as codewords. The remaining four codes have dimension 3, 3, 4 and 4 respectively. For example, taking $g(x) := (x-1)(x^3+x+1) = x^4 + x^3 + x^2 + 1$, we find a [7, 3] cyclic code. This code is an example

of the irreducible cyclic codes(Minimal cyclic codes are called *irreducible cyclic codes*).

7.1.14 BCH Codes

This class of cyclic codes was discovered by R. C. Bose and D. K. Ray-Chaudhuri in (1960) and independently by A. Hocquenbghem in (1959) and thus the codes are known as BCH codes. Practically they are interesting because of a simple decoding procedure that requires only a very simple decoding device rather than a computer. Mathematically they are interesting for their flexibility: apart from sharing many good properties with cyclic codes they allow for a certain control of minimum distance.

7.1.15 Definition:

A BCH code of designed distance δ is a cyclic code of length n over $\mathbb{F}_q$ whose generating polynomial $g(x)$ is a least common multiple of the minimal polynomials of $\beta^l, \beta^{l+1}, ..., \beta^{l+\beta-2}$, where β is a primitive nth root of unity and l some integer.

Usually l in the definition above is taken to be $l = 1$. We call such a coda a *narrow-sense* BCH code. Note that β is a primitive element of $\mathbb{F}_{q^m}$ we call such a code a *primitive* BCH code. Note that if β is a primitive element of $\mathbb{F}_{q^m}$ an nth root of unity, then $n = q^m - 1$.

7.1.16 Theorem:

[Theorem (5) in Lekic [61]]. The minimum distance of a BCH code C with designed distance d is greater than or equal to d.

The above theorem is usually called the *BCH bound*. From now on we usually consider narrow sense BCH codes. If we start with $l = 0$ instead of $l = 1$ we find the even weight subcode of the narrow sense code.

7.1.17 Example:

[Lint [63]]. Let $n = 31$, $m = 5$, $q = 2$ and $d = 8$. Let α be a primitive element of $\mathbb{F}_{32}$. The minimal polynomial of α is

$$(x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}).$$

In the same way we find the polynomial $m_3(x)$. But

$$m_5(x) = (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^9)(x - \alpha^{18}) = m_9(x).$$

It turns out that $g(x)$ is the least common multiple of $m_1(x)$, $m_3(x)$, $m_5(x)$, $m_7(x)$ and $m_9(x)$. Therefore the minimum distance of the primitive BCH code with designed distance 8 (which are obviously at least 9) is in fact at least 11.

Skew Cyclic Codes

In this section we discuss a generalization of cyclic codes by considering more general polynomial rings with the usual addition of polynomials and non-commutative multiplication. The reason these codes are interesting is that they share most of the properties of cyclic codes and their class is much larger, so the chance of finding good codes is also better. The idea of defining codes over noncommutative polynomial rings was developed in (1985) in a paper of Gabidulin [32]. Boucher, Geiselmann and Ulmer gave a slightly different approach in (2007) in [19]. Later Boucher and Ulmer generalized their approach in [20] to consider an even larger class of codes, not necessarily cyclic, over skew rings.
We start this section by introducing skew rings and their properties. After that we will discuss both skew cyclic and general skew codes as described by Boucher and Ulmer [20].

7.2 Codes over Skew polynomial rings

Let $\mathbb{F}_q$ denote a finite field of q elements, θ an automorphism on $\mathbb{F}_q$ and $|\langle\theta\rangle|$ its order. Let $\mathbb{F}_q[x, \theta]$ denote a set of all polynomials with coefficients always written on the left

$$\mathbb{F}_q[x, \theta] = \{a_0 + a_1x + ... + a_{n-1}x^{n-1} : a_i \in \mathbb{F}_q, n \in N\}.$$

Define $a_0 + a_1x + ... + a_{n-1}x^{n-1} = b_0 + b_0x + ... + b_{n-1}x^{n-1}$ if $a_i = b_i$ $\forall i$. Let addition of elements of $\mathbb{F}_q[x, \theta]$ be given by $(a_0 + a_1x + ...) + b_0 + b_1x + ...) = (a_0 + b_0) + (a_1 + b_1)x + ...$ and let multiplication be defined by the rule

$$xa = \theta(a)x.$$

This rule is further extended to all elements of $\mathbb{F}_q[x,\theta]$ by application of the distributive law. Note that multiplication defined in this way is not commutative. The set $\mathbb{F}_q[x,\theta]$ with operations defined as forms a ring called the *skew polynomial ring* over $\mathbb{F}_q$ with automorphism θ.

7.2.1 Example:

Consider $\mathbb{F}_4[x,\theta]$. Then Frobenius automorphism is given by

$$\begin{array}{c}\theta : \mathbb{F}_4 \to \mathbb{F}_4 \\ \alpha \mapsto \alpha^2.\end{array}$$

Let α be a generator of the multiplicative group of $\mathbb{F}_4$. Take $f = x + a$ and $g = ax^2 + 1$ for example. Then

$$\begin{aligned} fg &= (x+a)(ax^2)+1 \\ &= xax^2 + x + a^2x^2 + a \\ &= \theta(a)x^3 + a^2x^2 + x + a \\ &= a^2x^3 + a^2x^2 + x + a \end{aligned}$$

If $f = a_0 + a_1x + ... + a_nx^n$ with $a_n \neq 0$ we say f has degree n. It is not hard to see that $f, g \in \mathbb{F}_q[x,\theta]$ we have that $deg(fg) = deg(f) + deg(g)$ and $deg(f+g) \leq max\{deg(f), deg(g)\}$. This also implies that there are no zero divisors.

7.2.2 Example:

Note that $\mathbb{F}_q[x,\theta]$ is not a unique factorization domain. Consider again $\mathbb{F}_4[x,\theta]$. Listed below are all monic right factors of degree 2 of $x^6 + ax^3$.

$$\begin{aligned} x^6 + ax^3 &= (x^4 + ax)(x^2) \\ &= (x^4 + ax^3 + x^2)(x^2 + ax) \\ &= (x^4 + ax^3)(x^2 + ax + 1). \end{aligned}$$

Furthermore, $\mathbb{F}_q[x,\theta]$ is a ring endowed with right and left division algorithms. The right division algorithm is analogous to the one in commutative Euclidean domain: given two polynomials $f, g \in \mathbb{F}_q[x,\theta]$ we are looking for $h, r \in \mathbb{F}_q[x,\theta]$ such that

$$f = hg + r \text{ and } deg(r) < deg(g).$$

Polynomials h and r obtained in the right division algorithm are unique in $\mathbb{F}_q[x,\theta]$. Existence of right division implies the existence of right Euclidean algorithm, which in turn implies the existence of greatest common right divisors ($gcrd$) and least common left multiples ($lclm$). The $gcrd$ of f_1 and f_2 is the unique monic polynomial $g \in \mathbb{F}_q[x,\theta]$ of highest degree such that there exist $k_1, k_2 \in \mathbb{F}_q[x,\theta]$ with $f_1 = k_1 g$ and $f_2 = k_2 g$. The $lclm$ of f_1, f_2 is the unique monic h of lowest degree such that there exist $l_1, l_2 \in \mathbb{F}_q[x,\theta]$ with $h = l_1 f_1$ and $h = l_2 f_2$.

The left division is similarly defined. Given two polynomials $f, g \in \mathbb{F}_q[x,\theta]$ we are looking for two polynomials $h^{'}, r^{'} \in \mathbb{F}_q[x,\theta]$ such that

$$f = gh^{'} + r^{'} \text{ and } deg(r^{'}) < deg(g^{'}).$$

Recall that a *left ideal* I is a subset of a non-commutative ring R such that I is an additive subgroup of R and for all $r \in R$ and all $a \in I$

$$ra \in I.$$

Similarly, a *right ideal* I is an additive subgroup of R such that for all $r \in R$ and all $a \in I$

$$ar \in I.$$

7.2.3 Lemma:

Let $\mathbb{F}_q$ be a field with q elements and θ an automorphism. Then every right ideal in $\mathbb{F}_q[x,\theta]$ principal.

Proof. To see that $\mathbb{F}_q[x,\theta]$ is a principal right ideal domain, let I be any of its non-zero right ideals. Let $g \in I$ be a polynomial of least degree not equal to zero. Let f be some polynomial in I. By left division algorithm we have that there exist h and r such that $f = gh + r$ with $deg(r) < deg(g)$. But $r = f - gh$ is in I and so it must be that $r = 0$ by minimality of g in I. Then $f = gh$ and I is a principal right ideal domain. □

Similar argument shows that any left ideal is principal.

7.2.4 Lemma:

A polynomial $g \in \mathbb{F}_q[x, \theta]$ generates a two sided ideal if and only if g is of the form $g = x^t h$ with t a fixed integer, $h \in \mathcal{F}[x^m, \theta]$ and m the order of θ.

Proof. $\Leftarrow$ First we show that g of such form generates a two-sided ideal. Note that h is a central element and thus (h) is two sided. It is clear that x^t also generates a two-sided ideal. Then for every $f \in \mathbb{F}_q[x, \theta]$ we have

$$gf = x^t hf = x^t fh = f' x^t h = f' g.$$

for some $f' \in \mathbb{F}_q[x, \theta]$. The first and last equality hold by definition, while the second equality holds because h commutes with all elements of $\mathbb{F}_q[x, \theta]$ and third because (x^t) is two sided. Similarly, for any s in $\mathbb{F}_q[x, \theta]$ we have

$$sg = sx^t h = x^t s' h = x^t h s' = g s'$$

for some polynomial s' in $\mathbb{F}_q[x, \theta]$. We conclude that (g) is a two sided ideal.

$\Rightarrow$ Let $g = g' x^t = g_0 x^t + g_1 x^{t+1} + ... + g_d x^{t+d}$. Since x^t generates a two-sided ideal, it is clear that g generates a two-sided ideal if and only if g' does. Thus we may assume that $g = g' = g_0 + g_1 x + ... + g_d x^d$ with $g_0 \neq 0$. So let $g = g_0 + g_1 x + ... + g_d x^d$ with $g_0 \neq 0$ be a generator of a two-sided ideal. This means that for all $a \in \mathbb{F}_q$ there exists $b \in \mathbb{F}_q[x, \theta]$ such that $ag = gb$. In fact, from examining the degrees it follows that $b \in \mathbb{F}_q$. Then from

$$\begin{aligned} ag &= ag_0 + ag_1 x + ... + ag_d x^d, \\ gb &= g_0 b + g_1 xb + ... + g_d x^d b \\ &= g_0 b + g_1 \theta(b) x + ... + g_d \theta^d(b) x^d. \end{aligned}$$

We get that $a = b = \theta(b) = \theta^2(b) = ... = \theta^d(b)$. But since a is an arbitrary element of $\mathbb{F}_q$ we must have that all powers of x are multiples of m, the order of θ. Thus $g(x)$ is of the form $g(x) = g_0 + g_1 x^m + ... + g_d x^{dm}$. □

7.2.5 Definition:

[Definition (1) in Boucher, Geiselmann and Ulmer [19]]. Let $\mathbb{F}_q$ be a finite field with q elements and θ an automorphism. A linear code C of length n is called θ-*cyclic* if for every codeword

$$c = (c_0, c_1, ..., c_{n-1}) \in C$$

we have that

$$c^{'} = (\theta(c_{n-1})), \theta(c_0)), ..., \theta(c_{n-2})) \in C$$

Similarly to how polynomial representation of cyclic codes was defined over commutative polynomial rings $\mathbb{F}[x]$, here we associate to every word

$$c = (c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_q^n$$

its skew polynomial representation

$$c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1} \in \mathbb{F}_q[x, \theta]/(x^n - 1).$$

The observation that $c^{'}(x) = c(x)x \mod x^n - 1$ leads to the following important results about the structure of the cyclic code.

7.2.6 Lemma:

[Lemma (1) in Boucher [19]]. Let $\mathbb{F}_q$ be a finite field, θ an automorphism and n an integer divisible by the order $|\langle\theta\rangle|$ of θ. Then

(1) The ideal generated by $x^n - 1$ in $\mathbb{F}_q[x, \theta]$ is a two sided ideal.

(2) Ring $\mathbb{F}_q[x, \theta]/(x^n - 1)$ is a principal left ideal ring in which ideals are generated by right divisor of $x^n - 1$ in $\mathbb{F}_q[x, \theta]$.

Proof. Proof as same as Lemma (1) in Boucher, Geiselmann and Ulmer [19]. □

7.3 The length of a θ-code

We will study that any $g \in F_q[X, \theta]$ divides a polynomial $f \in \mathbb{F}_q[X, \theta]$ generating a two sided ideal and therefore is the generating polynomial of some code. For more details, see Boucher and Ulmer [20].

7.3.1 Definition:

[Jacobson [49]]. An element $P \in F_q[X, \theta]$ is *bounded* if the left ideal (P) contains a two sided ideal (P^*). The monic polynomial P^* of minimal degree is the bound of P.

Since P^* generates a two sided ideal, it must be of the form $(b_0 + b_1X^m + b_2X^{2m} + ... + b_sX^{s-m})X^t$, where $m = | < \theta > |$ and $b_i \in \mathbb{F}_q^\theta$ the fixed field of θ. From Theorem (15) in Jacobson [49] we get that all elements of $F_q[X, \theta]$ are bounded. The discussion before Theorem (15) also shows:

7.3.2 Lemma:

Let $m = | < \theta > |$ and $t = [\mathbb{F}_q : (\mathbb{F}_q)^\theta]$. If $P \in \mathbb{F}_q[X, \theta]$ is of degree n, then the bound P^* is of degree at most $m.t.n$.

Proof. The elements in $F_q[X, \theta]$ of degree less than n form a $\mathbb{F}_q$ vector space of dimension n and therefore a $(\mathbb{F}_q)^\theta$ vector space of dimension $t.n$. Considering the remainders of the division

$$X^{m.i} = P.Q_i + R_i,\ i = 0, 1..., t.n,$$

with $deg(R_i) < n$, there exists a non trivial linear combination

$$\sum_{i=0}^{t.n} \delta_i R_i = 0$$

where $\delta \in (\mathbb{F}_q)^\theta$. This shows that

$$\textstyle\sum_{i=0}^{t.n} \delta_i X^{m.i} = P.\Big(\sum_{i=0}^{t.n} \delta_i Q_i\Big).$$

The above polynomial $\sum_{i=0}^{t.n} \delta_i X^{m.i}$ is a bound for P. According to Theorem (12) in Jacobson [49], the bound P^* of P is a divisor of this polynomial. □

This proves that an element $g \in \mathbb{F}_4[X, \theta]$ of degree r has a bound of degree at most $4r$. Computations tend to suggest the conjecture that the degree of the bound of g is at most $2r$. The existence of θ-codes of type $[n, k]$ for $k < \frac{n}{2}$ is due to the fact that the degree of the bound of g can be less than $2r$.

7.3.3 Lemma:

[Lemma (5) in Lekic [61]]. The bound of a polynomial of degree r in $\mathbb{F}_4[X, \theta]$ is of degree at most $2r$.

Proof. Let

$$\begin{aligned} g &= \sum_{i=0}^{r} g_i x^i \\ \widetilde{g} &= \sum_{i=0}^{r} \theta^{i+1}(g_i) x^i = \sum_{i=0}^{r} x^i \theta(g_i). \end{aligned}$$

Then we compute $g\widetilde{g}$ and order the terms:

$$\begin{aligned} g\widetilde{g} &= \sum_{i,j}^{r} g_i x^{i+j} \theta(g_i) \\ &= \sum_{k=0}^{2r} \sum_{i+j=k} g_i x^k \theta(g_i) \\ &= \sum_{k=0}^{2r} \sum_{i+j=k} g_i \theta^{k+1}(g_i) x^k. \end{aligned}$$

Let

$$a_k = \textstyle\sum_{i+j=k} g_i \theta^{k+1}(g_j).$$

Consider now the parity of k. For terms with odd k we use the fact that $k+1$ is even and that we are in $\mathbb{F}_{2^2}$ which implies that every even power of θ is an identity map and $k+1$ terms cancel out:

$$\begin{aligned} a_k &= \sum_{i+j=k} g_i \theta^{k+1}(g_j) \\ &= \sum_{i+j=k} g_i(g_j) \\ &= g_0 g_k + g_1 g_{k-1} + \ldots + g_{k-1} g_1 + g_k g_0 \\ &= 2g_0 g_k + \ldots + 2g_{\frac{k-1}{2}} g_{\frac{k+1}{2}} \\ &= 0. \end{aligned}$$

For terms with even k, we have

$$\begin{aligned} a_k &= \sum_{i+j=k} g_i \theta^{k+1}(g_j) \\ &= \sum_{i+j=k} g_i \theta(g_j). \end{aligned}$$

But note that

$$\begin{aligned} \theta(a_k) &= \sum_{i+j=k} \theta^{k+1}(g_i) g_j \\ &= \sum_{i+j=k} \theta(g_i) g_j \\ &= a_k. \end{aligned}$$

So $a_k \in \mathbb{F}_2$ and because $a_k = 0$ for odd k we have that $g\widetilde{g} \in \mathbb{F}_2[x^2]$. The degree of $g\widetilde{g}$ is $2r$ and it generates a two sided ideal. Thus the bound on g is of degree at most $2r$. □

7.3.4 Example:

Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$, $\theta(\alpha) = \alpha^2$. In $\mathbb{F}_4[X, \theta]$, the polynomial

$$g = X^{12} + X^{11} + \alpha X^{10} + X^9 + \alpha^2 X^8 + X^6 + X^5 + \alpha^2 X^4 + X^2 + X + \alpha^2$$

is a right divisor of $f = X^{14} + X^{12} + X^{10} + 1 \in F_4[X, \theta]$. Therefore the bound of g is of degree at most 14 and $(g)/(f) \subset F_4[X, \theta]/(f)$ is a θ-code which is a [14, 2, 11] code with best possible distance 11.

Lemma (7.2.4) gives a constructive way to compute the bound of a given polynomial. An alternative approach is to note that the bound of a product is a divisor of the product of the bounds of its factors (Jacobson [49], Theorem (12)).

7.3.5 Example:

In the above example, the polynomial

$$g = X^{12} + X^{11} + \alpha X^{10} + X^9 + \alpha^2 X^8 + X^6 + X^5 + \alpha^2 X^4 + X^2 + X + \alpha^2$$

factors as $g = (X^4 + X + 1)^2(X + \alpha)(X + \alpha)(X + 1)^2$. Furthermore the bound of $X + \alpha$ is $X^2 + 1$ whereas $(X^4 + X + 1)^2$ and $(X + 1)^2$ are both polynomials of $\mathbb{F}_2[X^2]$. So one can construct the bound of g as the product $(X^4 + X + 1)^2(X + 1)(X + 1)(X + 1)^2 = X^{14} + X^{12} + X^{10} + 1$ which is the polynomial f of above example. The following table reproduces the best distance for $[n, k]\theta$-codes over $\mathbb{F}_4$. We write C_d if this code is cyclic of distance d, C_d^θ if the code is θ-cyclic of distance d and θ_d if the code is θ-central of distance d. If we don't obtain such a code matching the distance of the best known code in Magma 2.13 , then we indicate the difference in the distance by a negative number. The notation C_{3a}^θ means that the code is θ-cyclic of distance 3 and autodual.

n/r	2	3	4	5	6	7	8	9	10
4	C_{3a}^θ	C_4							
6	C_2	C_4	C_4^θ	C_6					
8	C_2	C_3^θ	C_{4a}^θ	C_5^θ	C_6^θ	C_8			
10	C_2	θ_3	C_4^θ	C_5^θ	C_6^θ	θ_6	θ_8	C_{10}^θ	
12	C_2	θ_3	θ_4	C_4	C_{6a}^θ	C_6^θ	C_7^θ	C_8^θ	C_9^θ
14	C_2	C_3^θ	C_4^θ	C_4^θ	C_5^θ	C_{6a}^θ	C_7^θ	-1	-1
16	C_2	-1	-1	C_4^θ	-1	-1	-1	-1	C_8^θ
18	C_2	-1	θ_3	θ_4	-1	-1	C_6^θ	-1	C_8^θ
20	-1	θ_3	θ_3	θ_4	-1	-1	θ_6	C_7^θ	C_8^θ
22	θ_2	θ_2	θ_3	θ_4	θ_4	θ_5	-1	C_6^θ	C_7^θ
24	C_2^θ	C_2^θ	θ_3	C_4^θ	C_4^θ	-1	-1	C_6^θ	C_7^θ
26	θ_2	θ_2	θ_3	θ_4	θ_4	-1	-1	C_6^θ	-1
28	C_2^θ	C_2^θ	θ_3	C_4^θ	C_4^θ	-1	θ_5	C_6^θ	C_6^θ
30	C_2^θ	C_2^θ	C_3^θ	C_4^θ	C_4^θ	-1	C_5^θ	C_6^θ	C_6^θ
32	C_2^θ	C_2^θ	-1	-1	θ_4	-1	θ_5	C_2^θ	θ_6
34	θ_2	θ_2	-1	-1	θ_4	-1	C_5^θ	C_6^θ	C_6^θ
36	C_2^θ	C_2^θ	-1	-1	θ_4	-1	-1	-1	θ_6
38	θ_2	θ_2	-1	-1	θ_4	-1	-1	-1	θ_6
40	C_2^θ	C_2^θ	-1	-1	θ_4	-1	-1	-1	θ_6
42	C_2^θ	C_2^θ	-1	C_3^θ	C_4^θ	-1	-1	-1	C_6^θ
44	C_2^θ	C_2^θ	-1	θ_3	θ_4	θ_4	-1	-1	-1

The table indicates that, with increasing length, the best θ-codes are no longer all cyclic or θ-cyclic. We note that the best codes given in Magma often have a poor weight distribution and that the θ-codes allow to find codes with a much better distribution.

7.4 Skew polynomial rings for an analysis of control system

Some applications of the theory of non-commutative rings to control theory are due to Jezek [52]. However, Jezek's works are rather focused on the background mathematics of non-commutative rings than control theory itself. A real application to control systems is done in (Moog et al. [70]) where a class of nonlinear time-delay systems is studied. The disturbance decoupling problem for nonlinear time-delay systems is tackled in (Moog et al. [70]) and the system inversion of nonlinear time-delay systems is discussed in Marquez-Martinez, Moog, and Velasco-villa [67].

This section describe some results concerning modules over Ore rings that are directly related to the algebraic approach to control systems and it also fills some mathematical gaps in the study of nonlinear time-delay systems (Marquez-Martinez and Moog [66]; Moog et al. [70]). We then study a special class of nonlinear systems with delays, called Generalized Roesser Systems.

7.4.1 Nonlinear time-delay systems

Consider a nonlinear system with time delays described by

$$\begin{aligned} \dot{x}(t) &= F(t) := f(x(t-i), i \in S_-) + \sum_{j=0}^{s} g_j(x(t-i), i \in S_-)u(t-j) \\ y(t) &= h(x(t-i), i \in S_-) \end{aligned} \tag{7.1}$$

$$x(t) = \varphi(t); u(t) = u_0, \forall t \in [t_0 - s, t_0]$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$, $y \in \mathbb{R}^p$ denote the state, input, output of the system, respectively, and f, g_j and h are meromorphic functions, $S_- := \{0, 1, ..., s$ is a finite set of constant time delays, $f(x(t-i), i \in S_-) := f(x(t), x(t-1), ..., x(ts))$, and φ denotes a continuous function of initial conditions; see (Conte, Moog, and Perdon [27]; Marquez-Martinez, Moog, and Velasco-villa [67]; Moog et al. [70]). It is further assumed that no relationship like

$$\phi(x(t-i), u(t-i), ..., u^{(k)}(t-i)) = 0 \tag{7.2}$$

exists for a non-trivial meromorphic function ϕ.

Let $\mathcal{C} := \{x(t-i), u^{(k)}(t-i); i, k \in Z_+\}$ and let $\mathcal{K}$ denote the field of meromorphic functions of a finite number of variables from C.

For any element $a \in \mathcal{K}$, the derivative along the dynamics of (7.1) is defined as usual, and it is easy to see that $\dot{a} \in \mathcal{K}$. Note that an element of $\mathcal{K}$ can be regarded as a time function $a = a(t)$ if the dependence on x and u is not emphasized.

Denoting now the differentials of $x(t-i), u^{(k)}(t-i); i, k \geq 0$ by $dx(t-i), du^{(k)}(t-i); i, k \geq 0$. Then the normal differentials of the functions in $\mathbb{K}$ span over the field $\mathbb{K}$ an vector space $\mathcal{E}$, that is, $\mathcal{E} = span_{\mathcal{K}} d\mathcal{K}$. $\mathcal{E}$ is endowed with a natural differential structure (Conte, Moog, and Perdon [27]) and it can also be used in the case of systems with delays.

7.4.2 The ring of polynomials

Let $\mathcal{K}(\delta]$ denote the set of polynomials of the form

$$a(\delta] = a_0(t) + a_1(t)\delta + ... + a_{r_a}(t)\delta^{r_a}, \tag{7.3}$$

in which $a_i(t) \in \mathcal{K}$. If addition in $\mathcal{K}(\delta]$ is defined as usually, while multiplication by

$$a(\delta].b(\delta] = \sum_{k=0}^{r_a+r_b} \sum_{i+j=k}^{i\leq r_a, j\leq r_b} a_i(t) b_j(t-i)\delta^k, \tag{7.4}$$

then $\mathcal{K}(\delta]$ is a ring. Unlike the usual polynomial ring $\mathcal{K}[\delta]$, $\mathcal{K}(\delta]$ is not commutative. In addition, this ring is not a skew polynomial ring, due to the definition of $\mathcal{K}$ (Jezek [52]).

The ring $\mathcal{K}(\delta]$ introduce the concept of a module over it, which is the basic step in founding an algebraic framework for the analysis and synthesis of non-linear delay systems.

7.4.3 Lemma:

For any $a(\delta], b(\delta] \in \mathcal{K}(\delta]$, there exist non-zero polynomials $c(\delta].a(\delta] = d(\delta].b(\delta]$. Due to this lemma, we have the following:

7.4.4 Theorem:

$\mathcal{K}(\delta]$ is a left Ore ring. Also $\mathcal{K}(\delta]$ has the following properties:

7.4.5 Theorem:

Suppose $\mathcal{M}$ and $\mathcal{N}$ are two modules over $\mathcal{K}(\delta]$, and $\mathcal{N}$ is a submodule of $\mathcal{M}$. $\mathcal{S}$ and $\mathcal{T}$ are two bases of $\mathcal{N}$. Then $|\mathcal{S}| = |\mathcal{T}|$.

7.4.6 Theorem:

A finitely generated submodule $\mathcal{N}$ of $\mathcal{M}$ over $\mathcal{K}(\delta]$ is Noetherian.

7.4.7 Roesser Systems

We generalize the above algebraic approach to a class of nonlinear systems of the following format:

$$\begin{aligned} \dot{x}(t) &= \mathcal{F}(t) := f(x(t), z(t), u(t)) \\ z(t+1) &= g(x(t), z(t), u(t)) \\ y(t) &= h(x(t), z(t), u(t)) \end{aligned} \tag{7.5}$$

in which the continuous state $x \in \mathbb{R}^n$, the discrete state $z \in \mathbb{R}^q$, the input $u \in \mathbb{R}^m$ and the output $y \in \mathbb{R}^p$. f, g and h are meromorphic functions.

This class of systems can be seen as a nonlinear extension of the Roesser model (Roesser [82]) widely used for studying linear 2-D systems. Also, since model (7.5) displays a continuous and discrete dynamics, it has been considered as a particular class of hybrid dynamic system by some authors (Ye, Michel, and Hou, [91]; Iglesias, [48]; Francis and Georgiou, [31]).

The form of a time-delay system (7.1) is not closed under *pure shifted dynamic compensator* defined in (Moog et al. [70]). However, the class of systems (7.5) is closed under such feedback.

It synthesizes theoretically three broad classes of systems. In particular, the nonlinear time-delay systems (7.1) can also be written in the above format. Actually, if $q \in N$ is the maximal delay occurring in the equations of (7.1), then defining, for $i = 1, ..., q$, $z_{1i} = x(t-i)$, $z_{2i}(t) = u(t-i)$, then we have the following discrete-time dynamics for the delay system:

$$z_1(t+1) = A_1 z_1(t) + B_1 x(t) \tag{7.6}$$

$$z_2(t+1) = A_2 z_2(t) + B_2 u(t) \tag{7.7}$$

in which $A_i = \begin{bmatrix} 0 & 0 & \dots & 0 & 0 \\ I_i & 0 & \dots & 0 & 0 \\ & & & & \\ & & \ddots & & \\ 0 & 0 & \dots & I_i & 0 \end{bmatrix}$, $B_i = \begin{bmatrix} I_i \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ and I_1 is the n dimensional identity matrix, I_2 is the m dimensional identity matrix.

To generalize the algebraic framework to the system (7.5), let $\mathcal{C} = \{x(t-i), u^{(k)}(t-i), k \geq 0, i \in N\}$, let $\mathcal{K}$ be the field of meromorphic functions of the variables in $\mathcal{C}$. We also include the meromorphic function of infinite number of variables of $\mathcal{C}$ in $\mathcal{K}$.

Define the ring of polynomials $\mathcal{K}(\delta]$ exactly as before. then we have all the properties of the ring of the polynomials. In particular, $\mathcal{K}(\delta]$ is a left Ore ring.

Since $\mathcal{K}(\delta]$ is a left Ore ring, it admits a classical left ring of fractions. We denote this ring by $\mathcal{K}\langle\delta)$. We also denote any element $b(\delta]\ a(\delta] \in \mathcal{K}\langle\delta)$ by $b^{-1}(\delta]a(\delta]$, and any element, denoted by $\omega\langle\delta)$, of $\mathcal{K}\langle\delta)$ is called a rational function.

Similarly, we define the following sequence of modules over $\mathcal{K}\langle\delta)$.

Given a set of symbols $\{dx, du, d\dot{u}, ..., du^{(k)}, ...\}$, an increasing sequence of left $\mathcal{K}\langle\delta)$ modules can be defined by

$$\mathcal{M}_k = \text{span}_{\mathcal{K}\langle\delta)}\{dx, du, d\dot{u}, ..., du^{(k)}\}.$$

The limit of this sequence is denoted by $\mathcal{M}$. Following the algebraic tradition, those modules over the division ring $\mathcal{K}\langle\delta)$ are called vector spaces over $\mathcal{K}\langle\delta)$.

Still the normal differentials of the function in $\mathcal{K}$ span over the field $\mathcal{K}$ span over the field $\mathcal{K}$ a vector space $\mathcal{E}$, that is, $\mathcal{E} = span_{\mathcal{K}} d\mathcal{K}$, and any differential one from $\omega \in \mathcal{E}$ can be associated with an element in $\mathcal{M}$. For simplicity, we will abuse the notation $d\alpha$ to denote also its association in $\mathcal{M}_s$.

From the second equation of the system (7.5), we can generate the following nonlinear equation in $z(t)$:

$$z(t) = g(x(t-1), z(t-1), u(t-1)) \tag{7.8}$$

If there is an element $\phi \in \mathcal{K}$ such that when $z(t) = \phi$ satisfies the equation (7.8), then the system (7.5) is called well-posed.

It can be easily seen that the nonlinear time-delay system (7.1) is well posed, because the solution to the corresponding equation (7.8) is $z_{1i}(t) = x(t-i-1)$, $z_{2i}(t) = u(t-i-1)$.

Now we extend the operation of differentiation to elements in $\mathcal{K}\langle\delta\rangle$ and vectors in $\mathcal{M}$:

(1) for any element $a(x(t-i), u_{(k)}(t-i), i \in N, k \geq 0) \in \mathcal{K}$, the derivative along the dynamics of the system (7.5) is defined usual, in which $z(t)$ is replaced by ϕ in the expression of $\mathcal{F}(t)$.

(2) for any polynomial $a[\delta] = \sum_{i=0}^{r_a} a_i \delta^i \in \mathcal{K}[\delta]$, the derivative $\dot{a}$ along the dynamics of the system (7.5) is a fraction in $\mathcal{K}\langle\delta\rangle$ defined by $\dot{a}_i$ is the derivative of $a_i \in \mathcal{K}$ along the dynamics of (7.5).

(3) for any element $\omega\langle\delta\rangle = b^{-1}[\delta]a[\delta] \in \mathcal{K}\langle\delta\rangle$, the derivative along the dynamics of (7.5) is defined by

$$\dot{\omega}\langle\delta\rangle = (db)^{-1}(d\dot{a} - ca). \tag{7.9}$$

(4) for any vector $\omega \in \mathcal{M}_k$ (or $\mathcal{M}$), the derivative $\dot{\omega}$ of $\omega = \kappa_{-1}dx + \sum_{i=0}^{k} \kappa_i du^{(i)}$ along the dynamics of (7.5) is a vector of some $\mathcal{M}_s$, $s > k$, (or $\mathcal{M}$), defined by $\dot{\omega} = \dot{\kappa}_{-1}dx + \sum_{i=0}^{k} \dot{\kappa}_i du^{(i)} + \kappa_{-1}df + \sum_{i=0}^{k} \kappa du^{(k+1)}$, in which $\dot{\kappa}_i$, for $i = -1, 0, 1, ..., k$, are the derivative of κ_i along the dynamics of (7.5), $df \in \mathcal{M}_s$ is the association of differential of f.

Because of the natural association, we will also call an element in $\mathcal{M}_\kappa$ (or $\mathcal{M}$) a differential one form. For any $\kappa \in \mathcal{K}$, $d\kappa = \overbrace{d\kappa}$.

The above development seems to be dependent on the availability of the solution $z(t) = \Phi$ to the equation (7.8). This is however unnecessary for many of our purposes. Remember that our analysis and design of

the system (7.5) usually begins with the differential dq of a function (as the output of the system, for example) of the form $q = q(x(t), z(t), u(t))$. The idea is to treat dq as a vector in $\mathcal{M}$. Since

$$dq = \frac{\partial q}{\partial x(t)}dx(t) + \frac{\partial q}{\partial z(t)}dz(t) + \frac{\partial q}{\partial u(t)}du(t),$$

we need only find dz to put dq in $\mathcal{M}$.

To find dz, we do not actually need the explicit form of the solution $z(t) = \Phi$.

If we write the second equation of the system (7.5) as $z(t+1) = g(x(t), z(t), u(t))$, we can define a symbol dz for discrete variable $z(t)$ by doing some formal manipulation on the above equation

$$dz = (I - \delta a)^{-1}(\delta b dx + \delta c du). \tag{7.10}$$

where I is the identity matrix and $a = \frac{\partial g}{\partial z(t)}$, $b = \frac{\partial g}{\partial x(t)}$, $c = \frac{\partial g}{\partial u(t)}$.

Applying the above to the discrete dynamics (7.6) and (7.7) of nonlinear time-delay systems, we have that $dz_{1i} = \delta^i dx$, $dz_{2i} = \delta^i du$. Note that in this case dz_{ij} are linear combinations of dx and du with coefficients in the ring of polynomials $\mathcal{K}(\delta]$. This also helps to explain why modules over $\mathcal{K}(\delta]$ were used to study nonlinear time-delay systems (Moog et al., [70]).

7.4.8 Observability of Nonlinear Time-Delay systems

To study the observability of the nonlinear time-delay system (7.1), we have two approaches. The first one sees the system as one over $\mathcal{K}(\delta]$. Define

$$Y_k = \text{span}_{\mathcal{K}(\delta]}\{dy, d\dot{y}, ..., dy^k\}$$

$$\mathcal{U} = \text{span}_{\mathcal{K}(\delta]}\{du, d\dot{u}, ...\}$$

and $\mathcal{X} = \text{span}_{\mathcal{K}(\delta]}\{dx\}$. Then

$$(\mathcal{Y}_0 + \mathcal{U}) \cap \mathcal{X} \subset (\mathcal{Y}_1 + \mathcal{U}) \cap \mathcal{X} \subset ... \subset (\mathcal{Y}_k + \mathcal{U}) \cap \mathcal{X} \subset ...$$

is an increasing sequence of submodules of $\mathcal{X}$. By Theorem (7.4.6), for $k \geq n$

$$(\mathcal{Y}_k + \mathcal{U}) \cap \mathcal{X} = (\mathcal{Y}_n + \mathcal{U}) \cap \mathcal{X}$$

Denote $\mathcal{O} = (\mathcal{Y}_n + \mathcal{U}) \cap \mathcal{X}$ and $\mathcal{O}$ is called the polynomial observation submodule of the system (7.1).

The second approach sees the system as one over $\mathcal{K}\langle\delta)$, and similarly define

$$\bar{Y}_k = \text{span}_{\mathcal{K}\langle\delta)}\{dy, d\dot{y}, ..., dy^k\}$$

$$\bar{\mathcal{U}} = \text{span}_{\mathcal{K}\langle\delta)}\{du, d\dot{u}, ..., \}$$

and $\bar{\mathcal{X}} = \text{span}_{\mathcal{K}(\delta]}\{dx\}$. Then, the corresponding increasing sequence of submodules of $\bar{\mathcal{X}}$

$$(\bar{\mathcal{Y}}_0 + \bar{\mathcal{U}}) \cap \bar{\mathcal{X}} \subset (\bar{\mathcal{Y}}_1 + \bar{\mathcal{U}}) \cap \bar{\mathcal{X}} \subset ... \subset (\bar{\mathcal{Y}}_k + \bar{\mathcal{U}}) \cap \bar{\mathcal{X}} \subset ...$$

will stabilize in a finite number of steps. Thus,

$$(\bar{\mathcal{Y}}_k + \bar{\mathcal{U}}) \cap \bar{\mathcal{X}} = (\bar{\mathcal{Y}}_n + \bar{\mathcal{U}}) \cap \bar{\mathcal{X}}$$

Denote $\bar{\mathcal{O}} = (\bar{\mathcal{Y}}_n + \bar{\mathcal{U}}) \cap \bar{\mathcal{X}}$ and define $\bar{\mathcal{O}}$ as the rational observation submodule of the system (7.1).

We will say that the system (7.1) is weakly observable if $rank_{(\mathcal{K}\langle\delta)}\bar{\mathcal{O}} = n$.

7.5 Ordinary Differential equation with Skew polynomial rings

Skew polynomial rings have a number of important structural properties which make them mathematically rich, correspond to real applications, and also allow for effective and efficient algorithms.

One important property of skew polynomials is that $R[x; \sigma, \delta]$ is a principal right ideal domain if σ is injective and R is a division ring.

Therefore, the Euclidean algorithms hold in skew polynomial rings.

One of the significant differences between the usual polynomial rings and skew polynomial rings is that skew polynomial rings are not unique factorization domains. For example, let $k = \mathbb{C}(X)$ and $L = \partial^2$. Then there are two factorizations $\partial^2 = \partial o \partial = (\partial + \frac{f'}{f})(\partial - \frac{f'}{f})$ with f a monic polynomial in z of degree ≤ 1. If we only consider the degrees, Ore [75] gave the following uniqueness theorem, which can be proven as a consequence of the Jordan-Holder theorem, see Jacobson [49].

7.5.1 Theorem:

(Ore [75]). If $f \in R[x; \sigma, \delta]$ factors completely as

$$\begin{aligned} f &= f_1 f_2 \dots f_n \\ &= g_1 g_2 \dots g_m \end{aligned}$$

where $f_1, \dots, f_n,\ g_1, \dots, g_m \in R[x; \sigma, \delta]$ are irreducible, then $n = m$ and there exists a permutation ϕ of $1, \dots, n$ such that for $1 \leq i \leq n$, $deg(f_i) = deg(g_{\phi(i)})$.

We refer to Singer and van der Put [88] for more details. Moreover, the usual Gauss lemma does not apply. An indicative example of this is as follows:

7.5.2 Example:

Let $R = \bar{C}[t][x; \delta]$, with $\delta(t) = 1$ be a polynomial ring, where $\bar{C}$ is the algebraic closure of a field C. It is easy to check that

$$tx^2 + t^2x - t = (x + t)(tx - 1)$$

Clearly the GCD of the leading coefficients of $x + t$ and $tx - 1$ is 1, but the coefficients of the left hand side can be divided by t. That is, Gauss lemma does not hold! This unfortunate property makes the study of skew polynomials considerably more difficult than that of the usual polynomials. In particular, factoring algorithms are inherently much more complex.

Since the (1990)'s skew polynomials have attracted the interest of many computer algebraists. A primary reason is that one can use them

to compute with ordinary differential equations. In fact, this was Ore's starting point in the (1930)'s, but development was not continued, possibly due to the lack of computers at that time. Many authors worked on differential factoring algorithms, for example, Brostein and Petkovsek [21], Giesbrecht [34], van Hoeij [90] and Singer [87].

Algorithms for factoring and decomposing skew polynomials are very important in computer algebra, and are used for solving systems of differential and difference operators, for example in Maple. The earliest and most famous method for factoring differential operators goes back to Beke [4] in (1894). Since then a number of authors have pursued different approaches, and developed a number of distinct algorithms. Some of these have been implemented in well-known mathematical software systems such as Mathematica and Maple. However, none of these previous algorithms run in time polynomial in the input size.

In the (1920)'s, J. L. Burchnall and T. W. Chaundy [23], discovered in a series of papers a remarkable connection between complex algebraic curves and pairs of commuting differential connection between complex algebraic curves and pairs of commuting differential operators. They found that given two operators

$$P := \sum_{i=0}^{n} p_i \partial^i \text{ and } Q := \sum_{i=0}^{m} q_i \partial^i, \text{ such that } PQ - QP = 0,$$

and where $p_i, q_i \in \mathbb{C}[[t]]$ are analytic, there is a canonical, and explicity computable, complex algebraic curve $\mathcal{BC}$ with equation $F(x, y) \in \mathbb{C}[x, y]$ such that $F(P, Q) = 0$. This curve is computable via a differential resultant, i.e., the determinant of the matrix formed by the coefficients in

$$\partial^k(P - x), k = 0, 1, ..., m - 1, \partial^l(Q - y), l = 0, 1, ..., n - 1.$$

It is then a fact that the power of t in all terms of the expanded determinant are the same and can thus be factored out, leaving a polynomial in x, y with complex coefficients annihilating the operators P and Q.

Moreover, the points (x, y) on the curve $\mathcal{BC}$ are exactly the eigenvalues of the joint eigen problem $P\psi = x\psi$ and $Q\psi = y\psi$. This defines a vector bundle over $\mathcal{BC}$ with sections being the eigen functions.

Hellstrom and Silvestrov [45] was proved an analogous theorem of Burchnall and Chaundy for q-difference operators. This q-analog simply showed the existence of an annihilating curve, no procedure was given to actually construct one. However, in Larsson and Silvestrov [60], an analog of the resultant scheme of Burchnall and Chaundy [23] was proposed and proved in a series of examples to yield a correct annihilating curve. No general proof was given to the effect of showing that this construction works in all cases.

This problem was addressed in Jeu, Svensson and Silvestrov [51], where a proof was given that this q-resultant scheme actually works to produce such an annihilating curve of two commuting q-difference operators. To be precise, they produce a family of algebraic curves annihilating the two given operators.

The first thing to note is that q-difference operators are special cases of so called σ-differential operators, built from σ (twisted) derivations in the same way differential operators are built from derivations. A σ-derivation is a k-linear maps ∂_σ on a k-algebra A such that

$$\partial_\sigma(ab) = \partial_\sigma(a)b + \sigma(a)\partial_\sigma(b),$$

where σ is a k-algebra endomorphism. In the case of q-difference operators on an algebra of functions (say over $\mathbb{C}$),

$$\sigma(f(x)) = f(qx) \text{ and } \partial_\sigma(f(x)) = \sigma(f(x)) - f(x) = f(qx) - f(x).$$

There are also various options of re-scaling these operators. Then a σ-differential operator is an operator on the form:

$$P = \textstyle\sum_{i=0}^{n} p_i \partial_\sigma^i, \text{ where } p_i \in A.$$

Secondly, we use a representation of these twisted operators as elements of Ore extension ring (skew-polynomial rings). Now, given two commuting skew-polynomials representing two commuting twisted operators P and Q, the result of Li [93] is used to produce a family of commutative polynomials in two indeterminates (over subrings of the ring A generated by the coefficients of P and Q) annihilating P and Q.

In the beginning we will define a general version of Ore extensions and we call these M-valued Ore extensions. We also give a general definition of twisted derivation operators and then show how to represent such operators in terms of an elements of an Ore extension.

7.5.3 M-valued Ore Extensions

Let k be a commutative ring, A a k- algebra and M an A-module. We denote the action of $a \in A$ on $m \in M$ by $a.m$.

Assume further that $\sigma \in End_k(A)$ and that Δ_A is a σ-derivation on A, this is k-linear map satisfying the σ-twisted Leibnitz rule

$$\Delta_A(ab) = \Delta_A(a)b + \sigma(a)\Delta_A(b).$$

Extend Δ_A to a k-linear $\partial_\sigma : M \to M$ by

$$\partial_\sigma(a.m) := \Delta_A(a).m + \sigma(a)\partial_\sigma(m).$$

In fact, by the associativity of the module structure of M, it is also necessary that Δ_A is a σ-derivation on A.

Let π_i^n denote the sum of all permutations of $(n-i)$ mappings ∂_σ and i mappings σ Lam and Leroy [58]. As an example $\pi_1^3 = \partial_\sigma^2 o\sigma + \partial_\sigma o\sigma o\partial_\sigma + \sigma o\partial_\sigma^2$. Note in particular that $\pi_k^k = \sigma^k$ and $\pi_0^k = \partial_\sigma^k$. We also put $\pi_k^n = 0$ for $n < k$ and $k < 0$. The lemma and proposition below can be found in Lam and Leroy [58].

7.5.4 Lemma:

$\pi_k^{n+1} = \partial_\sigma o\pi_k^n + \sigma o\pi_{k-1}^n$.

Proof. Simple induction. □

7.5.5 Proposition:

The following holds on an algebra A (not necessarily commutative)

(1) $\pi_k^n(ab) = \sum_{i=k}^n \pi_i^n(a)\pi_i^n(a)\pi_k^i(b)$ for $i \leq n$ and $a, b \in A$.

(2) $\partial_\sigma^n(ab) = \sum_{i=0}^n \pi_i^n(a)\partial_\sigma^n(a)\partial_\sigma^i(b)$ (Leibnitz's rule for σ-derivations).

Proof. 1) Follows by an induction on n using the above Lemma and (2) follows from (1) by taking $k = 0$. An alternative and much simpler way to prove (1) is indicated in Lam and Leroy [58]. □

Put $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ and form

$$A[\mathbb{N}_0] := \bigoplus_{i \in \mathbb{N}_0} Ae_i.$$

This is clearly a left A-module. We impose a right A-module structure as well by putting

$$e_n a := \sum_{i=0}^{n} \pi_i^n(a) e_i,$$

where π_i^n is the sum of all possible permutations of i-times σ and $(n-i)$ times Δ_A. The A-bimodule $A[\mathbb{N}_0]$ can be made into an $\mathbb{N}_0$-graded A-algebra when A is commutative by declaring $e_i e_j = e_{i+j}$. From this follows that $e_0 = 1_A[\mathbb{N}_0]$ act on M by the rule

$$ae_i(m) := a.\partial_\sigma^i(m).$$

7.5.6 Lemma:

[Lemma (2.3) in Larsson [59]]. This action is well-defined, that is, the action is associative

$$ae_i(be_j(m)) = (ae_i be_j(m)).$$

Proof. The proof follows easily by induction and the associativity of ∂_σ^n as follows. we have for $j \geq 0$.

$$ae_0(be_j(m)) = abe_j(m) = ((ab).\partial_\sigma^i)(m) = (a.\partial_\sigma^0 b.\partial_\sigma^j)(m) = (ae_0 be_j)(m).$$

Assume that $i \geq 0$ and that the result holds for $i-1$. Then

$$\begin{aligned} ae_i(be_j(m)) &= ae_{i-1}(\sigma(b)e_{j+1} + \Delta_A(b)e_j)(m) \\ &= ae_{i-1}(\sigma(b)e_{j+1}(m) + ae_{i-1}\Delta_A(b)e_j)(m) \\ &= (ae_{i-1}(\sigma(b)e_{j+1})(m) + (ae_{i-1}\Delta_A(b)e_j)(m) \\ &= (ae_i be_j)(m). \end{aligned}$$

Extending linearly proves the theorem. □

We refer to the pair $(A[\mathbb{N}_0], M)$ as an *M-valued Ore extension on M*. Elements in $(A[\mathbb{N}_0], M)$ are called *skew-polynomials (or Ore polynomials)*. The classical case of Ore extensions is when $M = A[\mathbb{N}_0]$ and $\partial_\sigma = \Delta_A$. We will follow the traditional way of writing $A[\mathbb{N}_0]$ as a polynomial ring $A[z]$.

7.6 General derivations and σ-differential operators

Let Λ and M be A-modules and suppose given a k-linear action μ of Λ on M, $\mu : \Lambda \otimes M \to M$. Then a *general derivation* on (A, Λ, M) is a quadruple $(\sigma, \tau, \Delta, \partial_\sigma)$ where

- $\sigma, \Delta : \Lambda \to \Lambda$, and
- $\tau, \partial_\sigma : M \to M$,

are all k-linear maps such that

$$\begin{aligned} \partial_\sigma(\mu(g \otimes m)) &= \partial_\sigma(g.m) \\ &= \mu(\Delta(g) \otimes \tau(m)) + \mu(\sigma(g) \otimes \partial_\sigma(m)) \\ &= \Delta(g).\tau(m) + \sigma(g).\partial_\sigma(m), g \in \Lambda, m \in M. \end{aligned}$$

In our case $\tau = id$.

7.6.1 Difference modules

Recall that all algebras are assumed to be integral domains.

Assume that $f : A \to B$ is a morphism of k-algebras. Then a *σ-differential equation)* is an equation of the form

$$P\Psi = \sum_{i=0}^{n} p_i \partial_\sigma^i \Psi = 0, \text{ where } p_1 \in A \text{ and } \Psi \in B.$$

We will assume that $A = B$ for simplicity. There is another, closely related, and in fact in many cases equivalent, formulation of σ-differential equations.

7.6.2 Definition:

A *σ-difference ring* is a ring A together with a $\sigma \in End(A)$; a (Φ, σ)-difference module (M, Φ, σ) is a module over a difference ring (A, σ)

together with a σ-linear endomorphism Φ.

To recall, the notion σ-linear means that

$$\Phi(am) = \sigma(a)\Phi(m), \text{ for } a \in A, m \in M.$$

A σ-difference equation is an equation of the form

$$\sum_{i=0}^{n} p_i \sigma^i \Psi = 0, \text{ where } \Psi, pi \text{ are elements in } A$$

We will assume that all difference modules are free.

To every difference equation can be associated a difference module and conversely. Notice first that, just as in the case of differential equations, a difference equation $\sum_{i=0}^{n} p_i \sigma^i \Psi = 0$, with $p_n = 1$ can be written as

$$\sigma\bar{X} = P\bar{X}, \bar{X} = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}, x_i \in A \tag{7.11}$$

with

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{n-2} & -p_{n-1} \end{pmatrix}$$

invertible, i.e., $p_0 \neq 0$. Then the associated difference module is $(A^n, P^{-1}\sigma)$. A solution to (7.11) lies in $ker(id - \Phi)$, where $\Phi := P^{-1}\sigma$. Conversely, any element in $ker(id - \Phi)$ is a solution to (7.11). It is easy to see that Φ is a σ-linear and $\Phi a = \sigma(a)\Phi$.

On the other hand, given a difference module (M, Φ), we can always turn this into a difference equation by

$$\sigma\bar{X} = P^{-1}\sigma\bar{X},$$

where P is the matrix of Φ in the basis for M. This can easily be shown to be independent on the choice of basis, in that a different choice yields an equivalent structure. For all this see Marius and Singer [78].

7.6.3 Proposition:

(Proposition 2.4 in Larsson [59])Every σ-difference operator $\sum_i a_i\sigma^i$ over a σ-difference ring (A,σ) can uniquely be expressed as a σ-differential operator $\sum_i c_i\partial_\sigma^i$, where $\partial_\sigma := a(id-\sigma)$ for some $a \in A$. The converse statement also holds, i.e., given $P = \sum_i c_i\partial_\sigma^i$ with $\partial_\sigma := a(id-\sigma)$, we can re-write this uniquely as $P = \sum_{i=1}^n c_i\sigma^i$.

Proof. Notice first that if $\partial_\sigma := a(id-\sigma)$ then ∂_σ^n can be written as a linear combination of terms $(id-\sigma)$ with coefficients in A, Indeed, for $n=2$ we have

$$\partial_\sigma^2 = a\partial_\sigma(a)(id-\sigma) + a\sigma(a)(id-\sigma)^2$$

and the general case is exactly the same. Therefore every operator $P = \sum_{i=1}^n p_i\partial_\sigma^i$ can also be written as a linear combination of powers of $(id-\sigma)$ after re-arranging. Hence, expanding the powers of $(id-\sigma)$ and re-arranging once more yield the last statement. The first follows immediately from the following lemma (after suitable re-arrangement). □

7.6.4 Lemma:

Prove

$$\sigma^n = \sum_{i=0}^{n-1} \left(\begin{array}{c} n \\ i \end{array} \right) (id-\sigma)^i + (-1)^n(id-\sigma)^n. \tag{7.12}$$

Proof. We will use the following identities

(a) $\left(\begin{array}{c} n \\ i \end{array} \right)\left(\begin{array}{c} n \\ j \end{array} \right) = \left(\begin{array}{c} n-j \\ i-j \end{array} \right)$;

(b) $\sum_{i=0}^k (-1)^i \left(\begin{array}{c} n \\ i \end{array} \right) = (-1)^k \left(\begin{array}{c} n-1 \\ k \end{array} \right)$.

It is easily seen that formula (7.12) holds for $n=2$ and $n=3$. For induction assume that it holds for all $i<n$.
From the binomial identity $(id-\sigma)^n = \sum_{i=0}^n (-1)^i \left(\begin{array}{c} n \\ i \end{array} \right)\sigma^i$ follows that

$$(-1)^{n+1}\sum_{i=0}^{n-1}(-1)^i \left(\begin{array}{c} n \\ i \end{array} \right)\sigma^i + (-1)^n(id-\sigma)^n.$$

To simplify notation we use $\alpha := id - \sigma$. Using the induction hypothesis we have

$$\begin{aligned}
\sigma^n &= (-1)^{n+1}\sum_{i=0}^{n-1}(-1)^i \begin{pmatrix} n \\ i \end{pmatrix} \sigma^i + (-1)^n\alpha^n \\
&= (-1)^{n+1}\sum_{i=0}^{n-1}(-1)^i \begin{pmatrix} n \\ i \end{pmatrix} \sum_{j=0}^{i}(-1)^j \begin{pmatrix} i \\ j \end{pmatrix} \alpha^j + (-1)^n\alpha^n \\
&= (-1)^{n+1}\sum_{i=0}^{n-1}\sum_{j=0}^{i}(-1)^{i+j}\alpha^j + (-1)^n\alpha^n.
\end{aligned}$$

After some re-arranging this can be written as

$$\sigma^n = (-1)^{n+1}\textstyle\sum_{i=0}^{n-1}\sum_{j=i}^{n-1}(-1)^{i+j} \begin{pmatrix} n \\ j \end{pmatrix} \begin{pmatrix} j \\ i \end{pmatrix} \alpha^i + (-1)^n\alpha^n$$

By the identity (a) above this can be written as

$$\begin{aligned}
\sigma^n &= (-1)^{n+1}\sum_{i=0}^{n-1}\sum_{j=i}^{n-1}(-1)^{i+j} \begin{pmatrix} n \\ j \end{pmatrix} \begin{pmatrix} j \\ i \end{pmatrix} \alpha^i + (-1)^n\alpha^n \\
&= (-1)^{n+1}\sum_{i=0}^{n-1}(-1)^i \begin{pmatrix} n \\ i \end{pmatrix} \sum_{j=i}^{n-1}(-1)^j \begin{pmatrix} n-i \\ j-i \end{pmatrix} \alpha^i + (-1)^n\alpha^n.
\end{aligned}$$

By shifting indices in the innermost sum, putting $l = j - i$, that sum can be computed as

$$\textstyle\sum_{l=0}^{n-i-1}(-1)^{l+i} \begin{pmatrix} n-i \\ l \end{pmatrix} = (-1)^i \sum_{l=0}^{n-i-1}(-1)^l \begin{pmatrix} n-i \\ l \end{pmatrix},$$

and using (b) this can be written as

$$(-1)^i \textstyle\sum_{l=0}^{n-i-1}(-1)^l \begin{pmatrix} n-i \\ l \end{pmatrix} = (-1)^{n-1} \begin{pmatrix} n-i-1 \\ n-i-1 \end{pmatrix} = (-1)^{n-1}.$$

Hence,

$$\begin{aligned}
\sigma^n &= (-1)^{n+1}\sum_{i=0}^{n-1}(-1)^i \begin{pmatrix} n \\ i \end{pmatrix} \sum_{j=i}^{n-1}(-1)^j \begin{pmatrix} n-i \\ j-i \end{pmatrix} \alpha^i + (-1)^{n+1} \\
&= (-1)^{n+1}\sum_{i=0}^{n-1}(-1)^i \begin{pmatrix} n \\ i \end{pmatrix} (-1)^{n-1}\alpha^i + (-1)^{n+1}\alpha^n \\
&= (-1)^{n+1}\sum_{i=0}^{n-1}(-1)^{n+i-1} \begin{pmatrix} n \\ i \end{pmatrix} \alpha^i + (-1)^{n+1}\alpha^n \\
&= \sum_{i=0}^{n-1}(-1)^i \begin{pmatrix} n \\ i \end{pmatrix} \alpha^i + (-1)^{n+1}\alpha^n,
\end{aligned}$$

proving the lemma. □

References

[1] Annin, S. *Associated primes over skew polynomial rings*, Comm. Algebra, 30 (2002), no. 5, 2511-2528.

[2] Annin, S. *Associated primes over Ore extension rings*, J. Algebra Appl., 3 (2004), no. 2, 193-205.

[3] Argac N. ; Groenewald, N. J. *A generalization of 2-primal near rings*, Quaest. Math., 27: 4(2004), 397-413.

[4] Beke, E. *Die irreducibilitat der homogenen linearen differentialgleichungen*, Math. Ann. 45 (1894), 278-300.

[5] Bhat, V. K. *A note on Krull dimension of skew polynomial rings*, Lobachevskii J. Math. 22(2006), 3-6.

[6] Bhat, V. K. *Decomposability of iterated extension*, Int. J. Math. Game Theory Algebra, 15:1 (2006), 45-48.

[7] Bhat, V. K. *Polynomial rings over pseudovaluation rings*, Int. J. Math. and Math. Sc., (2007), Art. ID 20138.

[8] Bhat, V. K. *Ring extensions and their quotient rings*, East-West J. Math., 9:1 (2007), 25-30.

[9] Bhat, V. K. *Associated prime ideals of skew polynomial rings*, Beitr. Algebra Geom., 49:1 (2008), 277-283.

[10] Bhat, V. K. *Differential operator rings over 2-primal rings*, Ukr. Math. Bull., 5(2) (2008), 153-158.

[11] Bhat V. K.; Raina Ravi *Ore extensions over* 2*-primal rings*, Vietnam J. Math., 36:4(2008)455-461.

[12] Bhat, V. K. *Transparent rings and their extensions*, New York J. Math., 15(2009), 291-299.

[13] Bhat, V. K. *A note on Completely prime ideals of Ore extensions*, Internat. J. Algebra and Comput., 3 (2010), 457-463.

[14] Bhat, V. K. *Ore extensions over Weak σ-rigid Rings and $\sigma(*)$-rings*, Eur. J. Pure Appl. Math., Vol.3, No.4, (2010), 695-703.

[15] Bhat, V. K. *Transparent Ore extensions over $\sigma(*)$-rings*, Europ. J. Pure Appl. Math., 3 (2011), 221-229.

[16] Bhat, V. K.; Kiran Chib *Transparent Ore extensions over weak σ-rigid rings*, Sib. Elektron. Mat. Izv., 8(2011), 116-122

[17] Bhat, V. K. *Ideal Krull-symmetry of skew polynomial rings*, Beitr. Algebra Geom., (2012) 53:507514.

[18] Blair, W. D.; Small L.W. *Embedding differential and skew-polynomial rings into artinain rings*, Proc. Amer. Math. Soc., Vol. 109(4)(1990), 881 – 886.

[19] Boucher, D.; Geiselmann, W.; Ulmer, F. *Skew-cyclic codes*, Appl. Algebra Enggr., Comm. Comput., 18 (2007), 379-389.

[20] Boucher, D.; Ulmer F. *Coding with Skew polynomial rings*, J. Symbolic Comput., 44 (2009), 1644-1656.

[21] Bronstein, M.; Petkovsek, M. *An introduction to pseudo-linear algebra*, Theoretical Computer Science, 157(1996), 3-33 .

[22] Brown, K. A. *Module Extensions over Noetherian rings*, J. Algebra, (1981), 69, 247-260.

[23] Burchnall, J. L.; Chaundy, T. W. *Commuting ordinary differential operators*, Proc. Lond. Math. Soc., 21 (1922), 420-440.

[24] Chatters, A. W.; Hajarnavis, C. R. *Rings with Chain Conditions*, Res. Notes in Math., Vol. 44 (1980), 919-924.

[25] Chyzak, F.; Salvy B. *Non-commutative elimination in Ore algebras proves multivariate identities*, J. Symbolic Comput., 26 (1998), 187-227.

[26] Chyzak, F.; Quadrat, A.; Robertz, D. *Linear control systems over Ore algebras: Effective algorithms for computation of parametrizations*, preprint, (2004).

[27] Conte, G.; Moog, C. H.; Perdon, A. M. *Nonlinear Control Systems: an Algebraic Setting*, Lecture Notes in Control and Inform. Sci., Vol. 242 (1999), Springer Verlag, London.

[28] Covington, A. *Primary Decomposition in Non-commutative Rings*, Ph.D Thesis, Warwick University, (2001).

[29] Faith, C. *Associated primes in commmutative polynomial rings*, Comm. Algebra, Vol. 28 (2000), 3983-3986.

[30] Fliess, M.; Mounier, H. *Controllability and observability of linear delay systems: an algebraic approach*, ESAIM COCV, vo.. 3 (1998), pp. 301-314.

[31] Francis, B. A.; Georgiou, T. T. *Stability theory for linear time invariant plants with periodic digital controllers*, IEEE Trans. Automat. Control, AC-33, (1988), pp. 820-832.

[32] Gabidulin, E. M. *Theory of Codes with Maximum Rank Distance*, Problem Peredachi Informatsii, 21 (1985), no. 1, 3-16.

[33] Gabriel, P. *Representations des algebras de Lie resolubles*, Seminaire Bourbaki, 1968/69, No. 347 (1971) 1-22. Zbl 0225.17004.

[34] Giesbrecht, M. *Factoring in skew-polynomial rings over finite fields*, J. Symbolic Comput. 24, 5 (1998), 463-486.

[35] Gluesing-Luerssen, H. *Linear Delay-Differential Systems with Commensurate Delays: An Algebraic Approach*, Lecture Notes in Math., 1770, Springer, (2002).

[36] Goldie, A. W.; Krause, G. *Embedding Rings with Krull dimension in Artinian rings*, J. Algebra, 1996, 182, 534-545.

[37] Goodearl, K. R.; Lenagan, T.H. *Krull dimension of differential operator rings, Noncommutative coefficients*, Trans. Amer. Math. Soc., 275(1983), No. 2, 833-859.

[38] Goodearl, K. R.; Warfield, R. B.*An introduction to Noncommutative Noetherian rings*, Camb. Uni. Press, (1989).

[39] Goodearl K. R., *Prime Ideals in Skew Polynomial Rings and Quantized Weyl Algebras*, J.Algebra, (1992), no. 150, 324-377.

[40] Goodearl, K. R.; Kenneth R.; Letzter, E.S. *Prime ideals in skew and q-skew polynomial rings*, Mem. Amer. Math. Soc., 109 (1994), no. 521.

[41] Goodearl, K. R.; Warfield, R. B.*An introduction to Noncommutative Noetherian rings*, Second Edition, Camb. Uni. Press, (2004).

[42] Gordon, R.; Robson, J. C. *Krull Dimension*, Mem. Amer. Math. Soc., (1973), 133.

[43] Gordon, R., *Primary Decomposition in Right Noetherian Rings*, Comm. Algebra, (1974), 2, 491-524.

[44] Hazewinkel, M.; Kirichenko, V. V. *Algebras, rings and modules*, Vol. 1, Mathematics and its applications, Kluwer Academic Press, (2004).

[45] Hellstrom, Lars; Silvestrov, Sergei D. *Commuting elements in q-deformed Heisenberg algebras*, World Scientific Publishing Co.Inc., River Edge, NJ, 2000.

[46] Hodges, T. J. *The Krull Dimension of skew Laurent extensions of commutative Noetherian Noetherian rings*, Comm. Algebra, 12(1984), No. 11-12, 1301-1310.

[47] Hong C. Y.; Kim N. K.; Kwak T. K. *Ore-extensions of baer and p.p.-rings*, J. Pure Applied Algebra, 151(3), (2000), 215-226.

[48] Iglesias, P. A. *On the stability of sampled data linear time-varying feedback systems* In. Proc IEEE Conference on Decision and Control, Lake Buena Vista, FL, (1994) 219-224.

[49] Jacobson, N. *The Theory of Rings*, American Math. Society, Vol. 2, (1943).

[50] Jategaonkar, A. V. *Localization in Noetherian Rings*, London Math. Soc. Lecture Notes Ser., Camb. Uni. Press: Cambridge, (1986); Vol. 98.

[51] Jeu, Marcel de; Svensson, Christian; Silvestrov, Segei *Algebraic curves for commuting elements in the q-deformed Heisenberg algebra*, J. Algebra, 321 (4), (2009), 1239-1255.

[52] Jezek, J. *Rings of Skew polynomials in algebraic approach to control theory*, Kybernetika, Vol. 32 (1996), 63-80.

[53] Kim, N. K.; Kwak, T. K. *Minimal prime ideals in 2-primal rings*, Math. Japon., 50:3 (1999), 415-420.

[54] Kim, P.; Krause, G. *Relative FBN Rings and the Second Layer Condition*, J. Pure Appl. Algebra, 133 (1998) 163-178.

[55] Krause, G. *Flat Embeddings of Noetherian Algebras in Artinian Rings*, Israel J. Math., 77 (1992), 97-114.

[56] Krempa, J. *Some examples of reduced rings*, Algebra Colloq., Vol. 3 (4) (1996), 289-300.

[57] Kwak, T.K. *Prime radicals of skew-polynomial rings*, Int. J. Math. Sci., Vol. 2(2), (2003) 219-227.

[58] Lam, T. Y.; Leroy, A. *Vandermonde and Wronskian matrices over division rings*, J. Algebra, 119 (2), (1988) 308-336.

[59] Larsson, Daniel; *Burchnall-Chaundy theory, Ore extensions and σ-Differential operators*, (2008).

[60] Larsson, Daniel; Silvestrov, Sergei D. *Burchnall-Chaundy theory for q-difference operators and q-deformed Heisenberg algebras*, J. Nonlinear Math. Phys., 10, (2003), 151-217.

[61] Lekic N. *Skew Coding and Skew Factorization*, Master Thesis, University of Utrecht, (2011).

[62] Leroy, Andre; Matczuk, Jerzy *On induced modules over Ore extensions*, Comm. Algebra, 32 (2004) 2743-2766.

[63] Lint J. H., *Introduction to coding theory*, Graduate texts in Mathematics, Springer, 2008 (Reprint).

[64] Ludgate, A. T. *A Note on Noncommutative Noetherian Rings*, J. Lond. Math. Soc., 5 (1972), 406-408.

[65] Marks, G. *On 2-primal Ore extensions*, Comm. Algebra, 29:5 (2001), 2113-2123.

[66] Marquez-Martinez, L. A.; Moog, C. H. *New results on the analysis and control of nonlinear time-delay systems*, In. Proc IEEE Conference on Decision and Control, Phoenix, USA (1999).

[67] Marquez-Martinez, L. A.; Moog, C. H.; Velasco- Villa, M. *The structure of nonlinear time-delay systems*, Kybernetika, Vol. 36, (2000), 53-62.

[68] McConnell, J. C.; Robson, J. C. *Noncommutative Noetherian Rings*, Wiley(1987); revised edition: American Math.Society (2001), Zbl 0980.16019.

[69] McEliece, R. J. *The algebraic theory of convolutional codes*, In V. Pless and W. Huffman, edits, Handbook of Coding Theory, Vol. 1, (1998), 1065-1138, Elsevier, Amsterdam.

[70] Moog, C. H.; Castro-Linares, R.; Velasco- Villa, M.; Marquez-Martinez, L. A. *The disturbance decoupling problem for time-delay non-linear systems*, IEEE Trans. Automat. Control, AC-45, (2000), 305-309.

[71] Musili C. *Introduction to Rings and Modules*, Second Edition, Narosa Publishing House, (2006).

[72] Nastasescu, C. Δ-*Anneaux et Modules* Δ-*Injectifs*, Applications aux Categories Localement Artiniennes. Comm. Algebra, (1981), 9 (19), 1981-1996.

[73] Noether E.; Schmeidler, W. *Moduln in nichtkommutativen Bereichen*, insbesondere aus Differential-und Differenzanusdruchen Mathematische Zeitschrift, (1920), 1-35.

[74] Nordstorm, H. E. *Associated primes over Ore extensions*, J. Algebra, 286 (2005), 69-75.

[75] Ore, O. *Theory of non-commutative polynomials*, Ann. of Mathematics, (1933)34: 480-508.

[76] Ouyang, L. *Extensions of generalized* α*-rigid rings*, Int. Electron. J. Algebra, 3 (2008), 3(2008), 103-116.

[77] Piret, P. *Structure and Constructions of cyclic convolutional codes*, IEEE Trans. Inform. Theory, (1976), 22:147-155.

[78] Put, Marius van der; Singer, Michael F. *Galois theory of difference equations*, volume 1666 of Lecture Notes in Math., Springer-Verlag, Berlin, 1997.

[79] Reid, M. *Undergraduate Commutative Algebra*, Wiley(1987); Lond. Math. Society Student Texts; Camb. Uni. Press: Cambridge, (1995); Vol. 29.

[80] Rentschler, R.; Gabriel, P. *Sur la dimension des anneaux et ensembles ordonnes*, C. R. Acad. Sci. Paris (A), 265(1967), 712-715.

[81] Robson, J. C. *Artinian quotient rings*, Proc. Lond. Math. Soc., (3) 17 (1967), 600-616.

[82] Roesser, R. P. *A discrete state-space model for linear image processing*, IEEE Trans. Automat. Control, Vol. 20, (1975), 1-10.

[83] Rowen, L. H. *Ring Theory*, Academic Press (Pure and Applied Math. Society), Inc (1991).

[84] Seidenberg, A. *Differential ideals in rings of finitely generated type*, Amer. J. Math, 89 (1967), 22-42.

[85] Sharp, R. Y. *Steps in Commutative Algebra*; London Math. Soc. Student Texts; Cambridge, (1990); Vol. 19.

[86] Shin, G. Y. *Prime ideals and sheaf representations of a pseudo symmetric ring*; Trans. Amer. Math. Soc. (1973); Vol. 184, 43-60.

[87] Singer, M. F. *Testing reducibility of linear differential operators: A group theoretic perspective*, Appl. Algebra in Engrg, Comm. Comput., 7 (2), (1996): 77-104.

[88] Singer, M.; Put, van der *Galois Theory of linear differential equations*, Grundlehren der mathematischen Wissenschaften, Volume 328, Springer, (2003).

[89] Stenstrom, B. *Rings of Quotients*; Springer-Verlag; Berlin-Heidelberg-New York, (1975).

[90] Van Hoeij, M. *Rational solutions of the mixed differential equation and its application to factorization of differential operators*, In Proc. ISSAC'96, (1996), 219-225.

[91] Ye, H.; Michel, A. N.; Hou, L. *Stability theory for hybrid dynamical systems*, IEEE Trans. Automat. Control, AC-43, (1998), 461-474.

[92] Zariski, O.; Samuel, P. *Commutative Algebra*, Vol. I, D. Van Nostrand Company, Inc. (1967).

[93] Ziming, Li *A subresultant theory for Ore polynomials with applications*, In Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation, New York (1998) 132-139.

SUBJECT INDEX