RINGS OVER WHICH A FREE MODULE IS GENERATED FROM FLAT MODULE

BY

AKINWANDE EMILY FUNMILAYO
NSU/NAS/MSC/MAS/005/15/16

M.sc MATHEMATICS

JUNE, 2017.

RINGS OVER WHICH A FREE MODULE IS GENERATED FROM FLAT MODULE

BY

AKINWANDE EMILY FUNMILAYO
NSU/NAS/MSC/MAS/005/15/16

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, NASARAWA STATE UNIVERSITY KEFFI, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER DEGREE OF SCIENCE IN MATHEMATICS

DEPARTMENT OF MATHEMATICAL SCIENCES,

FACULTY OF NATURAL AND APPLIED SCIENCES,

NASARAWA STATE UNIVERSITY, KEFFI.

NIGERIA

DECLARATION

I hereby declare that this dissertation titled **"rings over which a free module is generated from flat module"** has been written by me and it is a report of my research work. It has not been presented in any previous application for Master Degree of Science (M.sc) in mathematics.

All quotations are as indicated and sources of information are specifically acknowledged by means of references.

____

AKINWANDE EMILY FUNMILAYO

NSU/NAS/MSC/MAS/005/15/16

CERTIFICATION

The dissertation titled **“rings over which a free module is generated from flat module”** meets the regulations governing the award of master degree of science in mathematics, of the School of Postgraduate Studies, Nasarawa State University, Keffi, and is approved for its contribution to knowledge.

Dr. A. B Gimba **Date**
Chairman, Supervisory Committee

Dr. M.A. Yau **Date**
Member, Supervisory Committee

Prof. M.Y. Balla **Date**
Head of Department

Internal examiner **Date**

Prof. B. S. Jatau **Date**
Dean of Faculty

External Examiner **Date**

Prof. S. A. S. Aruwa **Date**
Dean, School Of Postgraduate Studies

DEDICATION

This dissertation is dedicated to God Almighty for his divine grace and protection and to my dear husband, Mr. T. A. Adebayo and my lovely children, Faridat Adebayo and Faruk Adebayo, for their moral and materials supports for the realization of this work.

ACKNOWLEDGEMENTS

I am grateful to Almighty God for his unfailing love and for the completion of my course works (MSC program). I am highly indebted to my supervisor Dr. A.B. Gimba for his patience, assistance, guidance, constructive criticism and suggestions throughout the stages of the dissertation.

I wish to extend my special gratitude to Dr. H.K. Oduwole whose previous seminar trainings were very relevant to the realization of this dissertation.

My gratitude goes to the Head of

Department Prof. M. Y. Balla and the Departmental P.G Coordinator Dr. M. O. Adenomon of the Department of Mathematical Science for their untiring and ceaseless supervision.

My profound gratitude goes to the Dean of Faculty of Natural and Applied Science, Faculty PG Rep, internal examiner, Dean School of Postgraduate Studies.

I will not fail to appreciate my lecturer Dr. M.A. Yau (Director ICT) and i immensely acknowledge the efforts of all the lecturers in the Department of Mathematics especially those who devoted their times to impact knowledge, God bless you all.

In the same vein, my inestimable appreciation goes to my children Faridat and Faruk, my darling husband Mr. T.A. Adebayo for his encouragement and financial support.

I wish to thank all my course mates for their co-operations, God bless you all.

Finally, I sincerely appreciate the works of the various authors on research topics consulted during this work.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

CHAPTER TWO
LITERATURE REVIEW

CHAPTER THREE
MATERIALS AND METHODS

CHAPTER FOUR
RESULTS

CHAPTER FIVE
DISCUSSION, CONCLUSION AND RECOMMENDATIONS

LIST OF TABLES

LIST OF FIGURES

NOTATIONS AND SYMBOLS

- $\otimes$: Tensor product
- $\oplus$: Direct sum
- $\mathbb{Q}$: set of rational numbers
- $\mathbb{Z}$**:** set of integers
- $\mathbb{R}$**:** set of real numbers
- $\mathbb{Z}[X]$:set of polynomial whose coefficients are integers
- $\mathbb{R}[X]$**:** set of polynomial whose coefficients are real numbers
- $\mathbb{Z}/n\mathbb{Z}$: integer mod n

ABSTRACT

The aim of this dissertation is to determine the rings over which a free module is generated from flat module. Modules are not always like vector spaces, Dylan (2010); therefore the purpose of this dissertation is to generate a module that behaves so much like vector spaces, that is a module with bases which are linearly independent. Over any rings, projective and flat modules are generated from free module but the reverse is not always true, Konrad (2012); rather, there are specific rings that need to be identified in order to generate free module from flat module. From the well-known fact that over a local ring a finitely generated flat module is free; therefore in order to generate free module from flat module, the elements of the local ring were mapped with the elements of an abelian group using the four module axioms. This dissertation considered rational number $\mathbb{Q}$ as a $\mathbb{Z}$-module (which is also flat module), an induction argument showed that any number of elements greater than two in $\mathbb{Q}$ are linearly dependent and cannot form basis for $\mathbb{Q}$, hence $\mathbb{Z}$-module $\mathbb{Q}$ are not free. The dissertation also considered the ring of rational numbers with even numerator and odd denominator as a local ring whose maximal ideal is 2 over module $\mathbb{Q}$ (flat module); the result showed that, ring of rational numbers with even numerator and odd denominator formed basis for rational number $\mathbb{Q}$ and the ring of rational numbers is a subset of $\mathbb{Q}$. An ideal S was also identified as a subset of $(\mathbb{Z}_6, +, \bullet)$ and the result showed that the set of generators formed basis for $\mathbb{Z}_6$ and S is the principal ideal generated by single element subset of $(\mathbb{Z}_6, +, \bullet)$. Therefore, $\mathbb{Z}$-module $\mathbb{Q}$ over ring of rational numbers with odd denominator and $\mathbb{Z}$-module $\mathbb{Z}_6$ over an ideal have generating sets consisting of linearly independent elements. The ring of rational numbers and ideal S formed the rings over which the free module is generated from flat module. Finally, a description of the Smith Normal Form algorithm and related examples were given; this provides ability to compute bases for $\mathbb{Z}$-modules and these bases are linearly independent; also the modules generated are free.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The concept of a ring first arose from attempts to prove Fermat's last theorem, starting with Richard Dedekind in the 1880s. After contributions from other fields, mainly number theory, the ring notion was generalized and firmly established during the 1920s by Emmy Noether and Wolfgang Krull, Wikipedia (2015). The study of rings originated from the theory of polynomial rings and the theory of algebraic integers, Sean (2011). Furthermore, the appearance of hyper complex numbers in the mid-19th century undercut the pre-eminence of fields in mathematical analysis. Modern ring theory is a very active mathematical discipline which studies rings in their own right, Sean (2011). To explore rings, Mathematicians have devised various notions to break rings into smaller, better, understandable pieces, such as ideals, quotient rings and simple rings. In addition to these abstract properties, ring theorists also make various distinctions between the theory of commutative rings and non-commutative rings, Wikipedia (2015). The commutative rings which belong to algebraic number theory and algebraic geometry are the objects of study for this dissertation.

Historically, the module theory has its origin in Number Theory and Linear Algebra, Wikipedia (2015). According to Sean (2011), the word *module* seems to have occurred for the first time in Number Theory and modules are very closely related to the representation theory of groups. He added that the most interesting objects ring acts on are modules and modules are used like group actions to show that certain rings have certain desirable properties. Modules are also one of the central notions of commutative algebra and homological algebra and are used widely in algebraic geometry and algebraic topology, Wikipedia (2015). A free module is just like a vector space which has basis (that is, a generating set consisting of linearly independent elements), Andreas (2005).

Projective modules were first introduced in 1956 in the influential book of Homological Algebra by Henri Cartan and Samuel Eilenberg. The class of projective modules enlarges the class of free modules over Ring, by keeping some of the main properties of free modules. The usual definition in line with category theory is the property of lifting that carries over from free to projective modules, Wikipedia (2015).

Flatness was introduced by Serre (1956), a flat module over a ring R is an R-module M such that taking the tensor product over R with M, preserves exact sequences. Vector spaces over a Field are flat modules; free modules, or more generally projective modules are also flat over any ring, Wikipedia (2015).

1.2 Statement of the Problem

The relation of projective modules to free and flats modules was subsumed by Konrad Voelkel (2012)' diagram of module properties.

Figure1.2: Relation between free, projective and flat modules

The left to right implication are true over any ring; while the right-to-left implication is true over the rings labeling them. Projective modules are direct summands of free modules, so one can choose an injection in a free module and use the basis of this to prove something for the projective module. Even weaker generalizations are flat modules, which still have the property that tensoring with them preserves exact sequences.

Following the properties of modules in commutative algebra and implications between them given by Konrad (2012); a free module is a projective module but the converse may be wrong over some rings, such as Dedekind rings. However, every projective module is a free module over a principal ideal Doman (PID) or local ring. Also projective modules (and thus free modules) are always flat while flat modules over perfect rings are always projective.

This study is interested in "over which rings can a free module be generated from flat module?" since any module is the homomorphic image of some free modules.

1.3 Aim and Objectives of the Study

The aim of this dissertation is to determine the ring over which a free module can be generated from flat module.

The following are the objectives of this study.

- To generate projective module from free module
- To generate flat module from projective module
- To identify the ring over which free module can be generated from flat module.

1.4 Scope of the Study

The study intends to look in to the universal properties of free, projective and flat modules. Konrad Voelkel (2012)' diagram of module properties would be verified in the course of this study, that is: projective modules are exactly direct summands of free ones while flat modules are projective when tensor products commute with direct sums.

Efforts would be made to verify when flat modules are free by studying the rings in which flat module act upon.

1.5 Significance of the Study

The study of rings over modules establishes the usefulness of abstract vector spaces, linear map and modules; the information derived by abstract method can be used to study algebraic properties of matrices. A better motivation for caring about modules is to point out that they are the setting for linear algebra over a ring (that is, canonical form for linear operator through modules over principal ideal domain or polynomial ring). Much of motivation of R-module comes from wanting to apply the ideas of linear algebra in settings where nonzero "scalar" might not be invertible.

1.6 Limitation of the Study

The study is limited to commutative algebra where commutative rings are considered. Since commutative algebra is the branch of mathematics that investigate commutative rings and attendant structures, especially ideals and modules.

1.7 Definition of Terms

- **Basis:** A basis is a linearly independent spanning (or generating) set.
- **Direct sum:** The direct sum is a construction which combines several modules into a new, larger module. The direct sum of modules is the smallest module which contains the given modules as submodules with no "unnecessary" constraints, making it an example of a co-product**.**
- **Direct summand:** Given the direct sum of additive abelian groups $A \oplus B$, $A \text{ and } B$ are called direct summands.
- **Tensor products**: Tensor product of modules is a construction that allows arguments about bilinear maps (e.g. multiplication) to be carried out in terms of linear maps.

CHAPTER TWO
LITERATURE REVIEW

2.0 Introduction

This chapter will review literature under the following sub-titles: concept of rings, modules and submodules, generation of a module over a ring, free module and projective module, free module and flat module.

2.1 Concepts of Rings

The abstract definition of a ring was first formulated by Fraenkel in 1914 [Berrick and Keating 2000], although the term 'ring' had been introduced previously by Hilbert in 1892. Before then, the various types of ring such as polynomial rings, noncommutative algebras, and rings of algebraic integers had each been considered separately. Perhaps surprisingly, the idea of an ideal is much older, since it originates in number theory.

Ambrus, (2017) gave the definition of a ring as a quintuple $(A, +, \bullet, 0, 1)$ and also a commutative ring with identity, if A is a set, equipped with two binary operations; addition and multiplication and two elements $0,1 \in A$; he listed the following axioms:

1. The triple *(A,+,0)* is an abelian group,
2. Multiplication is associative, commutative and distributive over addition.
3. There is $x \cdot 1 = 1 \cdot x = x$

He added that, it is rather usual to drop the dot from the notation when we write the product of elements, that is, to write xy instead of $x.y$. It is also abuse of notation to let just the symbol 'A' denote this whole package. He gave a remark that, the identity element 1 is uniquely determined by its property in axiom (3). Ambrus**,** (2017) identified polynomial rings as the most important example of rings. The polynomial ring in the variable x with coefficient in ring R (i.e. R$[x]$) was described as formal sums:

$$a_0 + a_1x + a_2x^2 \dots\dots + a_nx^n = \sum_{l=0}^{n} a_ix^i \quad - \; - - - \qquad \text{(equation 2.1)}$$

James, (2014) in his summer lecture note stated that a ring is just a set where you can add, subtract and multiply. In some rings (like field) one can divide while it is impossible for others. There are many examples of rings in which the main ones fall into: “number system” and “functions”. He gave some examples like ring of integers, the familiar number systems ($\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$), ring of even integers, polynomial rings whose coefficients are integers, ring of integer mod n, power series with entries in rational numbers, the set of all continuous real-valued functions on the interval [0,1] and many others. He defined and investigated the relationship between the special classes of rings such as Fields, Euclidean Domains, Principal Ideal Domains, Unique Factorization Domains and Integral Domains.

Connell, (2004) stated that rings are additive Abelian groups with second operation called multiplication and the connection between the two operations is provided by the distribution law. Connell assumed the results of groups for rings, simply because ideals are normal subgroups and ring homomorphisms are also group homomorphisms. He identified integers $\mathbb{Z}$, rational number $\mathbb{Q}$, the real number $\mathbb{R}$ and complex numbers $\mathbb{C}$ as the basic commutative rings and $\mathbb{Z}_n$ (integer mod n) has a natural multiplication under which it is also a commutative ring. He stated that, if R is any commutative ring, R$[x_1, x_2, \dots\dots. x_n]$ is a polynomial ring in *n* variable, but if R is any ring, $n \geq 1$ and R_n is the collection of $n \times n\, matrices$ over R, with R_n as a basic example of a non-commutative ring.

Joseph,(2003) pointed out that some authors do not demand that commutative rings should have 1 and for them, the set of all even integers is a commutative ring but he did not recognize it as such. He gave a remark that, there are non-commutative rings having an additional and a multiplication which satisfy all the axioms of commutative rings except the axiom: $ab = ba$.[Actually, the definition replaces the axiom $1a = a$ by $1a = a = a1$ and it replaces the distributive law by two distributive laws, one on either side: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$].

For example, it is easy to see that the set of all $n \times n$ real matrices, equipped with the usual addition and multiplication satisfies all the new ring axioms.

Joseph, (2003) defined a subring of rings as a subset of a commutative ring if an identity is closed in the subset, also if subtraction and multiplication of elements are closed in the subset. He added that the subring of a commutative ring is also a commutative ring

Karl-Heinz, (2012) in a lecture note of module and homological algebra stated that, the theory of modules requires the choice of a base ring and the base ring was assumed to be "unital" (that is to admit a unit element 1∈R). The baserings were identified as commutative, integral domains (that is commutative without zero divisor≠0), a principal ideal domain (PID) and an associative k-algebra with unity.

Avinash, (2013) in his notes on ring theory defined subring, ideal and quotient ring as follows. "A subring is a subset of ring, if the subset itself is a ring under the operation induced from the ring. It will also follow that '0' from ring belongs to subset but the identity '1' may or may not belong to subset. A subring forms an additive subgroup of ring and has to be closed under multiplication. He gave the example of the set $3\mathbb{Z} = \{3n/n \in \mathbb{Z}\}$ as a subring of $\mathbb{Z}$ which does not contain the identity but if a subring of $\mathbb{Z}$ contain identity, then it is obvious that the subring coincides with $\mathbb{Z}$". Also a subset I of a ring R as a left ideal, if I is an additive subgroup of the ring and for element $a \in I$ and$x \in R$, $xa \in I$, which can be shortened as$RI \subset I$. He considered the set of additive cosets S=$\{x + I| \ x \in R\}$, since I is clearly a normal subgroup of additive group, and subring S is a well define (Abelian) quotient group, R/I is denoted as quotient ring.

Siddharth, (2015) gave an intuitive explanation of a local ring. He stated that the reason such rings are called local is because they are usually constructed through localization from the ring of functions on an affine algebraic variety. If R is this ring of functions, then the (closed) points of the variety are the maximal ideals of R. If M is a maximal ideal, then localization at M inverts all the elements that are not in M and gives a ring S with a unique maximal ideal that corresponds to M. This local ring is then the ring of local functions or the ring of germs near the point represented by M.

2.2 Modules and Submodules

Richard, (2010) in his lecture note on Abstract Algebra explained the term module as a generalization of Abelian groups and vector space. It is an object satisfying all the axioms of a vector space except that the scalars are allowed to come from any fixed ring instead of from a field. He stated that the basic problem in module theory is given a ring with nice properties and classify modules over this ring up to isomorphism, which meets with relatively little success for all modules, so one looks at classes of modules over the ring. He gave examples of a module over a given ring and established the analogue of the isomorphism theorems and correspondence principle. Richard mentioned that modules are nicer, in the sense that it does not require stronger property than submodules in order to state and prove these results compared to those needing normal subgroups and ideals in group and ring theory respectively, but the quotient module of any given module and a submodule always exists. He studied the special class of free modules which generalizes the notion of vector spaces.

According to Parvat (2014), vector spaces over a field, ideal in a ring, abelian group and ring of integers are all examples of modules.

Amandeep, (2016) worked on comparative study of vector spaces and modules. He stated that vector space and modules seem to be the same in terms of definition but through deeply analysis, they are quite different. The properties of modules that emphasize differences between modules and vector space were given "In the case of vector spaces, every subspace has a complement. However, a sub-module of a module needs not to have a complement. For example, the set of integers Z is a Z-module (a module over itself). The sub-modules of the Z-modules are precisely the ideals of the ring Z and Z is a PID. Then the sub-modules of Z are precisely the set". He added that a vector space is finitely generated if and only if it has a finite basis. A submodule of a finitely generated module need not be finitely generated. For example, Let the ring$R = F[X]$ of all polynomials in infinitely many variables a finite sum, involves only finitely many variables. Then R is an R-module, and is finitely generated by the identity $P(X) = 1$. He analyzed that, In a vector space, a set S of vectors is linearly dependent if and only if some vectors in S is a linear combination of the other vectors in S. while, for arbitrary modules, this is not true. For example, considering Z-module Z_2, that consists of all ordered pairs of integers. Then the ordered pairs (2,0) and (3,0) are linearly dependent, since 3(2,0) – 2(3,0) = (0,0) but neither one of these ordered pairs is a linear combination of the other. Also in a vector space, a set of vector is a basis if and only if it is a minimal spanning set, or equivalently, a maximal linearly independent set. For the module the minimal spanning set is not necessarily a basis and a maximal linearly independent set is not necessarily a basis.

Finally there exist free modules with linearly independent sets that are not contained in a basis, and spanning sets do not contain a basis. This is to say that even free modules are not very much like vector space. For example, the set Z x Z is a free module over itself with basis{(1,1)}. To see this, observe that (1,1) is linearly independent, since (m, n)(1,1)=(0,0) implies (m, n)=(0,0). Also (1,1) spans Z x Z since (m, n)=(m, n)(1,1). But the sub-module Z x {0} is not free, since it has no linearly independent elements, and hence no basis.

Amandeep, (2016) concluded in his paper that the role of scalar field in vector space and the role of scalar ring in module create a big difference between the two concepts.

Dylan, (2010) stated that modules are not always like vector spaces. He justified this statement by considering the rational number $\mathbb{Q}$as a $\mathbb{Z}$-module and checked that $\mathbb{Q}$ is an $\mathbb{Z}$ -module by noting that $\mathbb{Q}$ forms an Abelian group under addition, and by noting that four module axioms hold. It was shown that $\mathbb{Z}$-module did not have a basis.

The primary goal of Dylan’s paper is to build enough vocabulary and theorem to prove the representation theorem for a finitely generated module over a principal ideal domain (PID).

Dylan, (2010) gave some examples of submodules which include subgroups of an Abelian group, which are ℤ-submodules, as well as ideas of a ring. Since every subgroup of an Abelian group is Abelian and since every Abelian subgroup is normal, there is a quotient module just like a quotient group.

Paul and Robert, (2012) listed some examples of modules: The first example was vector space over the field; secondly, any ring was considered to be a module over itself (that is elements of a ring can be added, subtracted, multiply and the usual rules of arithmetic can be applied). Thirdly, the set on n-tuples with components in ring is a module with usual definitions of addition and scalar multiplication (such as in Euclidean space). Fourthly, the set of all $m \times n$ matrices with entries in ring is a module where addition is ordinary matrix addition and multiplication of the scalar by the matrix means multiplication of each entry of matrix by scalar. Lastly, the ideals of the ring are modules and every Abelian group is a ℤ-module.

According to Wikipedia (2015), there are different types of modules which are: Finitely generated, cyclic free, projective, injective, flat, , simple, semi simple, indecomposable, faithful, torsion-free, Noetherian, Artinian, Graded and uniform modules; explanations for each type of modules were given.

2.3 Generation of a Module over a Ring

Any ring can be viewed as operators on an Abelian group in many ways; the Abelian group in which the ring acts is called a module over that ring. The generation of a module over a ring depends on the particular types of rings that act on specific types of modules stated in section 2.2. The results of these generations vary from each other.

The works, lecture notes, paper presentations and articles of different authors regarding modules over rings will be reviewed in this section.

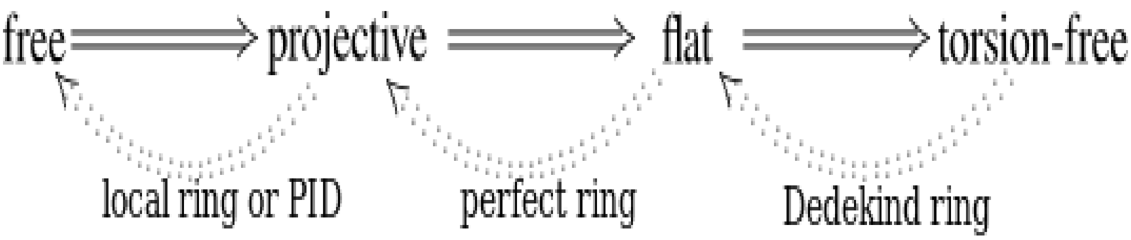
Parvati, (2014) identified the formal definition of module as a “map” just as follows.

A triple $(M,+,\bullet)$,where$(M,+)$ is an Abelian group and $\bullet : R \times M \to M$ is a map (called scalar multiplication) satisfying the following conditions; for $m, n \in M, r, s \in R$.

- $r(m+n) = rm + rn$
- $(r+s)\,m = rm + sm$
- $r.(s.m) = (rs).m$
- $1.m = m\, for\, all\, m \in M.$

Konrad, (2012) illustrated the generation of free, projective, flat and torsion -free modules through a diagram. The work which started in 2011, after series of corrections was finally completed in 2012.

Figure 2.2: Konrad’s diagram of modules properties



He stated that the left to right implication is true over any ring, that is, projective modules are generated from free modules over any cumulative ring; flat modules are generated from projective modules over any commutative ring; also torsion free modules are generated from flat modules over commutative ring. But the right to left implication is true over the rings labeling on them. He studied the properties of free, projective, flat and torsion-free modules and their rings then summarized the results as follows:

1. Free⟹Projective: Projective modules are exactly direct summand of free ones.
2. Projective⟹Flat: Same reason in 1, also tensor products commute with direct sum.
3. Flat⟹torsion-free: Torsion is the kernel of the tensor product.
4. Module torsion-free and ring Dedekind⟹ Module flat.
5. Module flat and ring Perfect ⟹Moduleprojective.
6. Module projective and ring local⟹ module free.
7. Module projective and ring PID⟹module free.

Travis, (2007) discussed the fundamental theorem of modules over a principal ideal domain and its applications. He stated that a principal ideal domain is an integral domain such that every ideal is the principal (that is generated by a single element). Any field, polynomial ring with the entry in field, integer and Gaussian integer are considered as examples of principal ideal domains. The concept of “Noetherian” was discussed also; it was stated that, any principal ideal domain is a Noetherian and Noetherian indicates that every ideal is finitely generated and every finitely generated module is a Noetherian Module. The applications of the fundamental theorem were described through Rational and Jordan Canonical forms. The proof of the fundamental theorem was given in Travis’ paper by using a generalization of Gaussian elimination matrices.

In many texts, a module over a principal ideal domain is an abelian group that also carries multiplication by a particular convenient ring of scalars. Indeed, when the scalar ring is integer, the module is precisely an abelian group.

The big picture of principal ideal domains arises in algebraic geometry and algebraic number theory. In algebraic geometry, the prototypical ring is a polynomial ring$K[\, x_1, \dots \dots . x_n]$. So we can see right away that principal ideal domains have limited application. $K[\, x_1, \dots \dots . x_n]$ is a principal ideal domain if and only if n$\leq$ 1. Here one can easily check that n>1 the ideal $[\, x_1, \dots \dots . x_n]$ is not principal. In fact $K[\, x_1, \dots \dots . x_n]$ is in some sense an "n-dimensional" ring, a concept to be made precise in spring but that certainly makes intuitive sense if one think of fields to be real numbers (K = ℝ). Principal ideal domains are in this same sense "1-dimensional" and hence in geometry, it is applied mainly to curves.

In algebraic number theory, the prototypical ring is integer. More generally one considers subrings of complex numbers that are finitely generated (hence free) as abelian groups. The familiar examples include the Gaussian integer and Cyclotomic integers. All of these rings are "1-dimensinoal" integral domains, but they need not to be principal ideal domains. A standard textbook example that is not a principal ideal domain is R = $\mathbb{Z}\sqrt{-5}$(number ring).

Thus, the principal ideal domain property is related to both singularities of algebraic curves and to unique factorization in number rings. To this, principal ideal domains are the simplest kind of commutative ring after fields and large parts of linear algebra appear as corollaries of their module theory; therefore, principal ideal domain are worthy objects of study.

2.4 Free Module and Projective Module

Encyclopedia of Mathematics, (2017) identified free module as a free object in a variety of modules over a fixed ring R. it was added that, if R is associative and has a unit, then a free module is a module with a basis, that is, a linearly independent system of generators. The cardinality of a basis of a free module is called its rank. The rank is not always defined uniquely, that is, there are rings over which a free module can have two bases consisting of a different number of elements. This is equivalent to the existence over R of two rectangular matrices A and B for which $AB = Im$, $BA = I_n$ $m \neq n$ where I_m and I_n denote the unit matrices of order m and n respectively. However, non-uniqueness holds only for finite bases; if the rank of a free module is infinite, then all bases have the same cardinality. In addition, over skew-field (over commutative ring) the rank of a free module is always uniquely defined.

Therefore, skew-fields can be characterized as rings over which all modules are free. For instance, over a principal ideal domain, a submodule of a free module is free and near to free modules are projective modules and flat modules.

Richard, (2010) in his lecture note on Abstract Algebra illustrated the universal property of free modules in the theorem below:

Theorem 2.4.1: Let $B = \{x_i\}_I$be a basis for a free R-module M. if N is an R-module and $y_i, i \in I$ are elements in N, then there exists a unique R-homomorphismf$: M \rightarrow N$ such that $x_i \rightarrow y_i$ for all i∈I.

The theorem above was proved as follows:

If z∈M, there exist unique $r_i \in R$. almost all $r_i = 0$ such that $z = \sum r_i x_i$. In particular, the uniqueness of the r_i implies that $f: M \to N$ given by $z \longmapsto \sum r_i y_i$ is well defined. Clearly, f is uniquely determined by $x_i \longmapsto y_i$ and f is an R-homomorphism.

In the notation of this theorem, it was stated that $x_i \longmapsto y_i$ extends linearly to a homomorphism$f: M \to N$. The theorem says that any R-homomorphism from a free module M to another R-module is completely determined by where a basis for M is sent.

Richard gave a better way of writing the universal property of free module as follows:

Let M be a free R-module on basis B and N an R-module. Given any set map $g: B \to N$ there exist a unique R-homomorphism $f: M \to N$ such that the diagram commutes and *inc* is the inclusion map.

According to Wikipedia, (2015)the usual definition in line with category theory is the property of lifting that carries over from free to projective modules. It can be summarized as follows: A module P is projective if and only if for every surjective module homomorphism $f: M \to N$ and every module homomorphism $g: P \to M$ there exists homomorphism$h: P \to N$ such that fh=g.

Wikipedia, (2015) defined a projective module in terms of split-exact sequences, direct summands of free modules, exactness and dual basis. The properties of projective module are: direct sums and direct summands of projective modules are projective; if $e = e^2$is an idempotent in the ring R then R_e is a projective left module over R; submodules of projective modules need not to be projective; the category of finitely generated projective modules over a ring is an exact category; every module over a field or skew field is projective (even free); over a Dedekind domain, a non-principal ideal is always a projective module that is not a free module; an abelian group (that is a module over$\mathbb{Z}$) is projective if and only if it is a free abelian group (the same is true for all principal idea domains, the reason is that for these rings any submodule of a free module is free);over a direct product of rings $R \times S$ where R and S are nonzero rings both $R \times 0$ and $S \times 0$are non-free projective modules; over a matrix ring $M_n(R)$ the natural module R^n is projective but not free; every module is projective but the zero ideal and the rings itself are the only free ideals; every projective module is flat but the converse is in general not true (the abelian group $\mathbb{Q}$ is a $\mathbb{Z}$-module which is flat but not projective); over a local ring every projective module is free; and a finitely related module is flat if and only if it is projective.

Jason, (2012) posted an article on projective module over a local ring and the definition of a local ring was given as ring in which the set of non-units form an ideal. His article was based on Kaplansky' theorem which state that projective modules over local ring are free. He added that, one might want to extend the concept of rank to other kinds of modules besides free modules and one way to do this is to note first that a finitely generated projective module over a local ring is free. Jason identified examples of projective non-free modules and they are direct products, infinite direct product, semi simple rings, ideals in Dedekind Domains, rings of continuous function, upper triangular matrix rings, vector bundles on sphere, and relation modules for infinite group rings.

Gennadi and Philipp, (2004) investigated the class of ring over which every finitely generated flat right module is projective. They stated the classical theorem of Bass (every flat right module over a ring is projective if and only if the ring is left perfect). They referred to the left perfect ring as right S-rings and gave examples of right S-rings as right Noetherian rings, since over such rings every finitely generated right module is finitely presented and over any ring, every finitely presented flat module is projective. It follows from another result of Bass, that every semi perfect ring is a right and left S-ring (Gennadi and Philipp 2004).

Udoye and Akoh, (2014) gave an insight on the projective module. In their works, they focused on some results of modules and projective modules, some aspects of modules by laying emphasis on its axioms, exactness and free module were discussed. They concluded that a module is finitely generated and projective if and only if it is a direct summand of a free module F with a finite base, then P is projective and also it is a homomorphic image of free module. Also, P being a finitely generated and projective module implies that there is an exact sequence $O \rightarrow P' \rightarrow F \rightarrow P \rightarrow O$ when F is free with finite base, P is projective implies that F is isomorphic to$P \oplus P'$.

Brett and Branden, (2013) stated in their works on computing free bases for projective modules that the Quillen-Suslin package for Macaulay 2 provides the ability to compute a free basis for a projective module over a polynomial ring with coefficients in rational numbers, integers or prime integers (z/p). A brief description of the underlying algorithm and the related tools were given. They reduced the statement of the Quillen-Suslin Theorem to a more concrete matrix theoretic problem concerning the completion of unimodular rows over polynomial rings to square invertible matrices.

Michiel, (2010) also in his note defined projective modules and proved some standard properties of projective modules, then classified finitely generated projective modules over Dedekind domains.

2.5 Free Module and Flat Module

Hazewinkel, (2013) in Encyclopedia of Mathematics explained flat module as a left (or right) module over an associative ring R such that the tensor product functor "$\otimes_R M$'' (corresponding $M \otimes_R$) is exact. The definition of flat module is equivalent to the module which can be represented in the form of a direct limit of free modules, also for any left ideal I of ring R, the canonical map (i.e. $I \otimes_R M \rightarrow IM$) is isomorphism. It was mentioned that projective modules and free modules are examples of flat modules. The class of flat modules over the ring of integers coincides with the class of Abelian group without torsion. All modules over a ring are flat if and only if the ring is regular in the sense of Von Neumann.

Konrad, (2010) clarified the definition of flat module by means of example and counter-example, he also show some nice and useful properties of flat module. He stated that a left R-module M is called flat, if the tensor product $\otimes M$ with it coverts short exact sequence of right R-module into short exact sequences of Abelian groups. Konrad noted that $\otimes M$ always preserves the surjectivity of the second map in the short exact sequence, and also preserves the exactitude at the middle (so the kernel of the second map is the same as the image of the first map).

Therefore, the word flat is used to distinguish between modules that preserve injectivity of the first map by tensoring from the right and those who do not.

Francois, (2007) worked on flat modules over valuation rings. He considered the properties of modules like P-flatness, flatness, content flatness, local projectivity, finite projectivity and single projectivity. The relations between these properties when R is a valuation ring were investigated. He added that for a module M over a ring R, there are implications that always hold such as;

M is projective ⇒ M is locally projective ⇒ M flat content

M is locally projective ⇓ M is finitely projective; M flat content ⇓ M is flat

M is finitely projective ⇒ M is flat

M is finitely projective ⇓ M is singly projective; M is flat ⇓ M is P-flat

M is singly projective ⇒ M is P-flat.

But they are not generally reversible. Francois commented that if R satisfies an addition condition, some equivalence will be gotten. He gave an instance by reviewing Bass (1960); Zimmerman-Huisgen (1976) and Azumaya (1987). ‘’Bass defined a ring R to be right perfect if each flat ring module is projective’’. According to Francois (2007), “In Zimmerman-Huisgen’s work, it was proved that a ring R is right perfect if and only if each flat right module is locally projective, and if and only if each locally projective right module is projective”. If R is a commutative arithmetic ring (that is a ring whose lattice of ideals is distributive), then any P-flat module is flat.

Francois, (2007) quoted Azumaya’s Proposition that if R is a commutative domain, each P-flat module is singly projective and any flat left module is finitely projective if R is a commutative arithmetic domain or a left Noetherian ring. Consequently, if R is a valuation domain each P-flat module is finitely projective. Finally, when R is a valuation ring, he proved that this result holds if and only if the ring of quotients of R is Artinian.

Rafail and Yilmaz, (2010) worked on test modules for flatness. In their paper, a right R-module M is said to be a test module for flatness (simply called f-test module) provided each left R-module N, Tor (M,N)=0 implies N is flat. F-test modules are flat version of the whitehead test modules for injectivity defined by Trlifaj. In their paper the properties of f-test modules were investigated and were used to characterize various families of rings. The structure of a ring over which every (finitely generated) right R-module is flat or f-test was investigated.

Majid and David, (2001) wrote on projective, flat and multiplication module all rings were commutative rings with identity and all modules were unital. They considered the behavior of projective, flat and multiplication modules under sums and tensor products. In particular, they proved that the tensor product of two modules is a module and under a certain condition the tensor product of a multiplication module with a projective (respectively flat) module is a projective (respectively flat) module. They investigated a theorem of Smith (1988) concerning the sum of multiplication modules and gave a sufficient condition on a sum of a collection of modules to ensure that all submodules are multiplications. Their result was applied to give an alternative proof of a result of El-Bast and Smith (1988) on external direct sums of multiplication modules. Finally, a module M is called a multiplication module if every submodule N of M has the form IM for some ideal I of ring R. for R is a commutative ring with identity and M is a unital R-module.

Keerthi, (2017) in the book of commutative algebra explained equational criterion for flatness as follows: Suppose there is a solution set to a finite bunch of linear equations in a flat module M. then, one can find elements m'_1, - - - $m'_k \in M$ such that these solutions lie in the sub-module generated by the m'_i, and such that the coefficients of m'_i in the linear expansion of the solutions can themselves be chosen to be the solutions of the same linear equations.

Finally on this chapter, suppose there is a number system, and you want to glue copies of them together so that they all have the same zero or origin. You have a bunch of “pure” lines of numbers, but you can also add them to get “mixed” numbers. These objects are examples of modules, but sometimes the number lines wrap into themselves like loops rather than lines. A free module doesn't have any loops at all; we don't collapse any numbers unnecessarily, so we “freely” construct the module. A flat module is just one in which there are some lines that weren't collapsed into a loop. (Technically this describes a projective module, but for Noetherian rings it doesn't really matter).

CHAPTER THREE

MATERIALS AND METHODS

3.1 Axiomatic Approach of Generating Module.

Following the definition of module, generation of module can be viewed as a map between a ring and an abelian group. Therefore a module is generated by mapping the element of ring with element of an abelian group, in which the structure of the group is still preserved.

Consider a ring R and abelian group M with an operation of external multiplication of each element of R by each element of M on the left and on the right, such that for all $a, b \in M$ and $r, s \in R$. The following conditions are satisfied:

1. $(ra) \in M$

2. $r(a + b) = ra + rb$(Left distributive law)

3. $(r + s)a = ra + sa$

4. $a(rs) = (ar)s$

Then M is a module over R.

The notion of submodule cannot be over emphasized in the study of modules and their rings: consider R as a ring, G as a group and H as a subgroup of G, if G is a module over R and H is a module over R, then H is a submodule of G over R.

3.2 Generating Free Module from Flat Module.

The generation of free module from flat module can be viewed as a generalization of the well-known fact that over a local ring a finitely generated flat module is free.

Theorem3.2.1.*If* R *is Noetherian local ring and* M *is finitely generated and flat, then* M *is free.*

Proof. Indeed, let $m \subset R$ be the maximal ideal and k the residue field. Now M/mM is a finitely generated k-vector space; choose a basis. This induces an isomorphism

$k^n \to M/mM$

Which we can lift to a map

$R^n \to M$

Which is surjective by Nakayama's lemma, and which becomes an isomorphism upon being tensored with k. Let Q be the kernel:

$0 \to Q \to R^n \to M \to 0$

Then we have an exact sequence

$Tor^1(k, m) = 0 \to Q \otimes k \to k^n \to M/mM$

As a result $Q \otimes k = Q \,/\, mQ = 0$, this implies $Q = 0$ by Nakayama, so $R^n \to M$ is an isomorphism, The first illustration is to consider $\mathbb{Z}$-module$\mathbb{Q}$ as a flat module, then check for the conditions of module been free (that is basis and linear independences).

Consider the rational number $\mathbb{Q}$ as a $\mathbb{Z}$-module. We can check that $\mathbb{Q}$ is a $\mathbb{Z}$- module by noting that $\mathbb{Q}$ forms an abelian group under addition and by noting the four module axioms hold since for $a, b, c, d, m, n \in \mathbb{Z}$ and for $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$

- $n\,(m\frac{a}{b}) = (nm)\frac{a}{b}$
- $(n+m)\frac{a}{b} = n\frac{a}{b} + m\frac{a}{b}$
- $n\left(\frac{a}{b} + \frac{c}{d}\right) = n\frac{a}{b} + n\frac{c}{d}$
- $1_{\mathbb{Z}}\frac{a}{b} = \frac{a}{b}$

Therefore $\mathbb{Q}$ is a module over $\mathbb{Z}$ and it is a flat module, to generate free module from this particular module, we use the familiar properties of $\mathbb{Z}$ and $\mathbb{Q}$. We will show that $\mathbb{Z}$-module$\mathbb{Q}$ does not have a basis , where we use the definition of linear independence and basis from linear algebra, with vector space replaced by module and scalar field replaced by ring .we will show for any number of elements in $\mathbb{Q}$, they will not form a basis of $\mathbb{Q}$. A basis for $\mathbb{Q}$ cannot have one element, since if that were so, then there would exist an element$\frac{a}{b} \in \mathbb{Q}$ $\quad a, b \in \mathbb{Z}, \quad b \neq 0$ such that for some $r \in \mathbb{Z}$

$$r\frac{a}{b} = \frac{a}{b+1}$$

The equation above implies that;

$$r(b+1) = b$$

$$r = \frac{b}{b+1}$$

Since $b \neq 0$, implies $r \notin \mathbb{Z}$, that is a contradiction. We will also show that two elements of $\mathbb{Q}$ cannot form a basis of $\mathbb{Q}$. Let $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \in \mathbb{Q}, \frac{a_1}{b_1} \neq \frac{a_2}{b_2}$ with $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and consider for $r_1, r_2 \in \mathbb{Z}$ the relation of linear dependence

$$r_1 \frac{a_1}{b_1} + r_2 \frac{a_2}{b_2} = 0$$

If we let $r_1 = b_1 a_2$ and let $r_2 = -b_2 a_1$, the $r_1, r_2 \in \mathbb{Z}$ and the choice of scalars satisfy the relation of linear dependence above. Therefore, any two elements of $\mathbb{Q}$ are linearly dependent, and cannot form a basis of $\mathbb{Q}$. An induction argument shows that any number of elements greater than two in $\mathbb{Q}$ are linearly dependent and therefore cannot form basis for $\mathbb{Q}$. Therefore free module cannot be generated from $\mathbb{Z}$-module$\mathbb{Q}$.

Using Matsumura's Theorem, free module can be generated from flat module.

Theorem 3.2.2 (Matsumura's theorem): Let (A, m) be a local ring and M is

A-module, if $x_1, \dots, x_n \in M$ are such that their images$\bar{x}_1, \dots, \bar{x}_n \in \bar{M} = M/mM$ are such linearly independent over field A/m then $x_1, \dots, x_n$ are linearly independent over A, Hence if M is finite, or if M is nilpotent, then any minimal basis of M, and M is a free module.

Therefore, the rings of rational numbers are going to be considered as the local rings and we establish the properties of modules on it, then verify the properties of the modules generated if they are free or not.

The next illustration is to consider ring R of rational numbers with even numerator and odd denominators as a local ring whose maximal ideal is 2over module$\mathbb{Q}$. We check $\mathbb{Q}$ as an abelian group under addition, and also note the four module axioms of module $\mathbb{Q}$

over ring of rational number with even numerator and odd denominator. There is need to study ring of rational numbers in the perspective of rings and subrings as follows.

The criterion for a non-empty subset R of a given ring $\mathbb{Q}$ for being a subring of $\mathbb{Q}$, is that R contains always along with its two elements also their differences and products. Since the field $\mathbb{Q}$ of the rational numbers is (isomorphic to) the total ring of quotients of the ring of integers, any rational number is a quotient $\frac{m}{n}$ of two integers m and n. If now R is an arbitrary subring of $\mathbb{Q}$ and $\frac{m_1}{n_1}, \frac{m_2}{n_2} \in R$ with $m_1, n_1, m_2, n_2 \in \mathbb{Z}$ (and $n_1 n_2 \neq 0$) then one must have $\frac{m_1 n_2 - m_2 n_1}{n_1 n_2} \in R$, $\frac{m_1 m_2}{n_1 n_2} \in R$

Therefore, the set of possible denominators of the elements of R is closed under Multiplication, i.e. it forms a multiplicative set.

This can of course lead us to subsets S containing only positive integers. But along with any positive integer n_0, the set S has to contain also all positive divisors, inclusive 1 and the prime divisors of the number n_0, since the factorisation $n_0 = uv$ of the denominator of an element $\frac{m}{n_0}$ of R implies that the multiple: $u.\frac{m}{uv} = \frac{m}{v}$ belongs to R.

Accordingly, S consists of 1, a certain set of positive prime numbers and all finite products of these, thus being a free monoid on the set of those prime numbers.

Since R contains all multiples of each of its elements, it is apparent that the set of possible numerators form an ideal of $\mathbb{Z}$.

Theorem3.2.3. If R is a subring of $\mathbb{Q}$, then there a principal ideal (k) of $\mathbb{Z}$ and a multiplication subset $S$of integer $\mathbb{Z}$ such that S is a free monoid on certain set of prime numbers and any element $\frac{m}{n} of$ R is characterized by $\begin{cases} m \in (k) \\ n \in S \end{cases}$

The positive generator $k\ of(k)$ does not belong to S except when it is 1.

Since k may be greater than 1, the ring R is not necessarily the ring of quotients $S^{-1}\mathbb{Z}$ that is, in the case, $R = \left\{\frac{2a}{3^S} : a \in \mathbb{Z}, \quad S \in \mathbb{Z}_+\right\}$,

3.3 Smith Normal Form of Computing Bases.

It is a good thing to motivate the Smith normal form with the problem of trying to relate basis elements $(x_1, \dots, x_n)$ of a free R-module M of rank n to the generators $(u_1, \dots, u_m)$ with $m \leq n$ of a finitely generated submodule. The generators of the submodule will naturally have a representation relative to the basis elements. Just as in linear algebra, we can change bases from $X = (x_1, \dots, x_n)^T$ to $Y = (y_1, \dots, y_n)^{\mathrm{T}}$ with multiplication by an invertible matrix P so that $Y = PX$. We can also change the generator from $V = (v_1, \dots, v_n)^T$ to $W = (w_1, \dots, w_m)^T$ with multiplication by an invertible matrix Q. Since the generators are linear combinations of the bases elements, such that, we have

$$U = AX$$

Where A is a matrix of the coefficients of the elements in the linear combination, therefore;

$$V = QU = QAX = QAP^{-1}Y$$

So the new matrix coefficients is QAP^{-1}.

CHAPTER FOUR

RESULTS

4.1 Modules and Submodules

Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ be an abelian group and $\langle \mathbb{Z}, +, \bullet \rangle$ be a ring. There is need to verify that $\langle \mathbb{Z}_6, + \rangle$ *is an abelian group*

Table 4.1: Abelian group of order 6

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table4.1 above is an abelian group with binary operation (+), it indicates that all the properties of abelian group are satisfied; it is associative, identity exists, inverse exists and it is commutative.

Therefore $\langle \mathbb{Z}_6, + \rangle$ is an abelian group under addition.

Now to verify $\mathbb{Z}_6$ as a module over ring $\langle \mathbb{Z}, +, \bullet \rangle$, there are four conditions that need to be satisfied: Given $M = \mathbb{Z}_6$ *and* $R = \mathbb{Z}$ *such that* $0, 1, 2, 3, 4, 5 \in \mathbb{Z}_6$ and$1, 2 \in \mathbb{Z}$

The following conditions are satisfied:

- $2(2+4) = 2.2 + 2.4 = 2 + 8 \equiv 4 mod\ 6 \in M$
- $(1+2)3 = 1.3 + 2.3 = 3 + 6 \equiv 3 mod\ 6 \in M$
- $1.(2.4) = (1.2).4 \equiv 2 mod\ 6 \in M$
- $1.3 = 3\ for\ 3 \in M$

Clearly $\mathbb{Z}_6\ is\ a\ module\ over\ \mathbb{Z}\ or\ simply\ \mathbb{Z} - module.$

Now, let us check for submodule of M, consider $H = \{0, 2, 4\}$ as a subgroup of an abelian group $\mathbb{Z}_6$ under the operation (+)

Table 4.2: Subgroup H of an abeian group

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Table 4.2 indicates that the properties of abelian group are closed in H, therefore H is a group under addition and it is a subgroup of $\mathbb{Z}_6$. For every element in H and element in $\mathbb{Z}$, consider $z \in \mathbb{Z}$, $hz \in H$, that is, 4 multiplied by any element of $\mathbb{Z}$, the result is in H. Thus H is a $\mathbb{Z} - module$. Since H is a$\mathbb{Z} - module$, then H is a submodule of $\mathbb{Z}_6$ over $\mathbb{Z}$.

Let $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ be an abelian group and $\langle \mathbb{Z}, +, \bullet \rangle$ be a ring. There is need to verify that $\langle \mathbb{Z}_8, + \rangle$ *is an abelian group*

Table 4.3: Abelian group of order 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Table4.3 above is an abelian group with binary operation (+), it indicates that all the properties of abelian group are satisfied; it is associative, identity exists, inverse exists and it is commutative.

Therefore $\langle \mathbb{Z}_8, + \rangle$ is an abelian group under addition.

Now to verify $\mathbb{Z}_8$ as a module over ring $\langle \mathbb{Z}, +, \bullet \rangle$, there are four conditions that need to be satisfied: Given $M = \mathbb{Z}_8$ *and* $R = \mathbb{Z}$ *such that* $0, 1, 2, 3, 4, 5, 6, 7 \in \mathbb{Z}_8$ and $1, 2 \in \mathbb{Z}$

The following conditions are satisfied:

- $2(2 + 4) = 2.2 + 2.4 = 2 + 8 \equiv 2 \; mod \; 8 \in M$

- $(1+2)3 = 1.3 + 2.3 = 3 + 6 \equiv 1 \, mod \, 8 \in M$
- $1.(2.4) = (1.2).4 \equiv 0 \, mod \, 8 \in M$
- $1.3 = 3 \, for \, 3 \in M$

Clearly $\mathbb{Z}_8$ $is\ a\ module\ over\ \mathbb{Z}\ or\ simply\ \mathbb{Z} - module.$

Now, let us check for submodule of M, consider $H = \{0, 2, 4, 6\}$ as a subgroup of an abelian group $\mathbb{Z}_8$ under the operation (+)

Table 4.4: Subgroup H of an abelian group

+	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

Table 4.4 indicates that the properties of abelian group are closed in H, therefore H is a group under addition and it is a subgroup of $\mathbb{Z}_8$. For every element in H and element in $\mathbb{Z}$, consider $z \in \mathbb{Z}$, $hz \in H$, that is, 6 multiplied by any element of $\mathbb{Z}$, the result is in H. Thus H is a $\mathbb{Z} - module$. Since H is a $\mathbb{Z} - module$, then H is a submodule of $\mathbb{Z}_8$ over $\mathbb{Z}$.

4.2 Generating Free Module from Flat Module

Example4.2.1. Consider $\mathbb{Z}-module\mathbb{Q}$ as a flat module and ring of rational numbers as the ring.

Given that $R=\left\{\frac{2a}{3^S}: a\in\mathbb{Z}, \quad S\in\mathbb{Z}_+\right\}, M=\mathbb{Q}=\left\{\frac{a}{b}\in\mathbb{Q},\ a,b\in\mathbb{Z}\, for\ b\neq o\right\}$

For $R\subset\mathbb{Q}$, therefore R form a basis for $\mathbb{Q}$ since it is a subset of $\mathbb{Q}$.

Let $R=\{x_i\}$ be a basis for $\mathbb{Z}-module\ \mathbb{Q}$, if S is $\mathbb{Z}-module$ and $y_{i,}i\in I$ are elements in S, then there exists a unique R-homomorphism $f:\mathbb{Q}\to S$ such that $x_i\to y_i for\ all\ i\in I.$

If $n\in M$, there exist unique $z_i\in\mathbb{Z}$, almost all $z_i=0$ such that $n=\sum z_i x_i$. In particular, the uniqueness of z_i implies that $f:\mathbb{Q}\to S$ given by $n\to\sum z_i y_i$ is well-defined. Clearly, f *is* uniquely determined by $x_i\longmapsto y_i$ and f is an R-homomorphism.

Example4.2.2. In theorem 3.1, a Noetherian local ring was identified as an ideal that is finitely generated. A convenient method of defining an ideal is to specify a set of generators.

Given a subset$\{r_i|i\in I\}\ of\ R$, where I is some index set, possibly infinite, we say that $r_i=0$ for almost all i, or for all except a finite set of indices, if the set of indices i with $r_i\neq 0$ is finite.

Now let $X=\{x_i|i\in I\}$ be a subset of R. Then the right ideal is generated by X is the set of expressions $\sum_{i\in I}x_i r_i$

Where $r_i=0$, for all except a finite set of indices, X is called a set of generators for a. When $X=\{x_1,\ldots\ldots x_n\}$ is finite, we write $a=x_1R+\cdots+x_nR$;

If $X = \{x\}$, then $a = xR$ is the principal right ideal generated by x. The left ideal generated by X is defined in a similar way.

For instance, consider $R = \langle \mathbb{Z}_{6,} +, \bullet \rangle$ as a ring and $S = \{0, 2, 4\}$ as a subset of R

$$S \subset R$$

To verify that S is an ideal for R, pick any element from $\mathbb{Z}_6$ say 3 multiply by elements of S. i.e. $3s = s3$ for $s \in S$

- $3.0 = 0.3 = 0 \in S$
- $3.2 = 2.3 = 0 \in S$
- $3.4 = 4.3 = 0 \in S$

Therefore S is an ideal in $\mathbb{Z}_{6,}$ now let $X = \{0, 2\} \in S$. Then the right ideal is generated by$X$, then, $a = xR$, $x \in X$

$a = 2\mathbb{Z}_{6,} = S = \{0, 2, 4\}$. Therefore X is a set of generators for a.Therefore $a = xR$ is the principal right ideal generated by single element $\{2\} \in X$. The left ideal generated by X can be define in a similar way.

Example 4.2.3: Consider $R[x]$: rings of polynomials in one variable with coefficients in a field. The set $A = \{1, x, x^2 \dots\dots\}$, then certainly A generates $R[x]$ as an R-module. Suppose there is some finite linear combination of elements of A that equals zero. Since a finite linear combination is just a polynomial

$$a_0 + a_1x + \cdots + a_nx^n = 0.$$

However, this implies that each of the a_i's is zero, it is concluded that A is a linearly independent set, and so A forms a basis for $R[x]$ which is also free. Since free modules are flat, then $R[x]$ is a flat R-module.

4.3 Smith Normal Algorithm of Calculating Bases

Example 4.3.1. Consider$\mathbb{Z}$- module M with basis $\{x_1, x_2, x_3, x_4\}$, and a submodule K generated $u_1, u_2, u_3,$ where $u_1 = 22x_3, u_2 = -2x_1 + 2x_2 - 6x_3 - 4x_4, u_3 = 2x_1 + 2x_2 + 6x_3 + 8x_4$. [Paul, G. and Robert, B. (2012), Problem 6, section 4.5]

The coefficient matrix yields

$$\begin{bmatrix} 0 & 0 & 22 & 0 \\ -2 & 2 & -6 & -4 \\ 2 & 2 & 6 & 8 \end{bmatrix}$$

The first step is to bring the smallest positive integer to the 1-1 position. Thus interchange row 1 and 3 to obtain:

$$\begin{bmatrix} 2 & 2 & 6 & 8 \\ -2 & 2 & -6 & -4 \\ 0 & 0 & 22 & 0 \end{bmatrix}$$

Since all entries in column 1, and similarly in row 2, are divisible by 2, we can pivot about the 1-1 position, in other words use the 1-1 entry to produce zeros. Thus add row 1 to row 2 to get:

$$\begin{bmatrix} 2 & 2 & 6 & 8 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 22 & 0 \end{bmatrix}$$

Add -1 times column 1 to column 2, then add -3 times column 1to column 3, add -4 times column1 to column 4. The result is:

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 22 & 0 \end{bmatrix}$$

Add -1 times column 2 to column 4, and have:

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 22 & 0 \end{bmatrix}$$

The first row and column has been peeled off, and the smallest positive integer has been brought to the 3-3 position. But 22 is not a multiple of 4, therefore add row 3 to row 2 to get:

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 22 & 0 \\ 0 & 0 & 22 & 0 \end{bmatrix}$$

Add -5 times column 2 to column 3,

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 2 & 0 \\ 0 & 0 & 22 & 0 \end{bmatrix}$$

Interchange column 2 and column 3 to get:

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 \\ 0 & 22 & 0 & 0 \end{bmatrix}$$

Add -11times row 2 to row 3 to obtain:

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 0 \\ 0 & 0 & -44 & 0 \end{bmatrix}$$

Finally, add -2 times column 2 to column 3, (to get rid of minus sign) multiply row 3 (or column 3) by -1, the result is:

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 44 & 0 \end{bmatrix}$$

There is a new basis $y_1, y_2, y_3, y_4\ for\ M,$ and new generators $v_1, v_2, v_3\ for\ K,$ where $v_1 = 2y_1, v_2 = 2y_2, and\ v_3 = 44y_3$. In fact since the $v_j{}'$s are nonzero multiples of the corresponding $y_j{}'$s, they are linearly independent, and K is a free ℤ-submodule of M.

Example 4.3.2.Let us assume, we have ℤ- module M with basis$\{x_1\ , x_2\ , x_3, x_4\}$, Let K be a ℤ-submodule K generated by V_1, V_2 and V_3; where $V_1 = 2x_1 + x_2 - 3x_3 - x_4$; $V_2 = x_1 - x_2 - 3x_3 + x_4\ and\ V_3 = 4x_1 - 4x_2 + 16x_4$ [Dylan, P. (2010)]

Then, the coefficient Matrix

$$A = \begin{bmatrix} 2 & 1 & -3 & -1 \\ 1 & -1 & -3 & 1 \\ 4 & -4 & 0 & 16 \end{bmatrix}$$

Bringing A into Smith normal form

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 & -3 & -1 \\ 1 & -1 & -3 & 1 \\ 4 & -4 & 0 & 16 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$R_1 \leftrightarrow R_2$ $$\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&-1&-3&1\\2&1&-3&-1\\4&-4&0&16\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$$

$-2R_1+R_2;-4R_1+R_3$ $$\begin{bmatrix}0&1&0\\1&-2&0\\0&-4&1\end{bmatrix}\begin{bmatrix}1&-1&-3&1\\0&3&3&-3\\0&0&12&12\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$$

C_1+C_2 ; $3C_1+C_3$;$-1C_1+C_4$:

$$\begin{bmatrix}0&1&0\\1&-2&0\\0&-4&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&3&3&-3\\0&0&12&12\end{bmatrix}\begin{bmatrix}1&1&3&-1\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$$

$-C_2+C_3$; C_2+C_4:

$$\begin{bmatrix}0&1&0\\1&-2&0\\0&-4&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&3&0&0\\0&0&12&12\end{bmatrix}\begin{bmatrix}1&1&2&0\\0&1&-1&1\\0&0&1&0\\0&0&0&1\end{bmatrix}$$

$-C_3+C_4$:

$$\begin{bmatrix}0&1&0\\1&-2&0\\0&-4&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&3&0&0\\0&0&12&0\end{bmatrix}\begin{bmatrix}1&1&2&-2\\0&1&-1&2\\0&0&1&-1\\0&0&0&1\end{bmatrix}$$

= Q B P^{-1}

Note that, the smallest integer was first brought to the (1, 1) entry, then made every other entry in the 1st row and 1st column equal to zero. The process was repeated by (2,2) entry.

It is straight forward to check that $QAP^{-1} = B$. Therefore, the new basis for $M\{y_1, y_2, y_3, y_4\}$ and the generators for K are $w_1 = y_{1,} w_2 = 3y_2, and\ w_3 = 12y_3$. Since the w_i generated k and the y_i and hence the w_i are linearly independent, the w_i forms a basis for K. therefore K is a free-ℤ-sub module.

CHAPTER FIVE

DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1 Discussion

The motivation behind this study was given by Konrad Voelkel's diagram of module properties. He characterized free, projective, flat and torsion-free module through their properties. The left to right implication is true over any commutative ring while the right to left implication is true over the rings labeled on them. Following this regard, the aim of this research is to determine the rings over which a free module is generated from flat module. The usual method of constructing module over a ring was applied and this was carried out by allowing the elements of the ring to act on the elements of an abelian group. The study considered the set of rational numbers$\mathbb{Q}$ over the ring of integers$\mathbb{Z}$, the result showed that$(\mathbb{Q},+)$ is an abelian group and $(\mathbb{Z},+,\bullet)$ is the ring of integers, then $\mathbb{Q}$ is a module over $\mathbb{Z}$ ($\mathbb{Z}-$module$\mathbb{Q}$) and it was a flat module, but two elements of $\mathbb{Q}$ could not form a basis for $\mathbb{Q}$, therefore elements of $\mathbb{Q}$ are linearly dependent which agreed with Dylan, (2010).

Tables 4.1 and 4.3 showed that $\mathbb{Z}_6$ and $\mathbb{Z}_8$ are abelian groups of order 6 and 8 respectively under addition and the results also showed that $\mathbb{Z}_6$ and $\mathbb{Z}_8$ are modules over ring of integers. Tables 4.2 are 4.4 showed that the subgroups of abelian groups are also submodules of $\mathbb{Z}_6$ and $\mathbb{Z}_8$ over the ring of integers. Therefore, an abelian group, an ideal and ring of integers are modules; mentioned by Parvati, (2014). Similarly the result in Example4.2.1 showed that the elements of the ring of rational numbers with even numerator and odd denominator is a subset of $\mathbb{Q}$ that formed bases for module $\mathbb{Q}$ and they are linearly independent.

The result in Example 4.2.2 showed that an ideal of the ring of integer mod 6 ($\mathbb{Z}_6, +, \bullet$) which is also subset, formed bases for the ring. Example4.2.1 and Example4.2.2 showed that the rings over which a free module is generated from flat module are constructed through localization from the ring of functions; which agreed with the explanation given by Siddharth, (2015). The result in Example 4.2.3 indicates that ring of polynomial in one variable with coefficients in a field is a flat module that is also free, Ambrus, (2017) identified this in equation 2.1.

Finally, the Smith Normal Form Algorithm in examples 4.3.1 and 4.3.2 showed that the submodules formed bases for the modules and the new bases are linearly independent, which are also free. The results from Smith Normal Algorithm agreed with Richard, (2010) that the classification of modules is based on their submodules. This demonstrates the usefulness of linear algebra through module theory.

The rings over which a free module is generated from flat module were identified as local rings which are also subrings of the given rings. The results of this study showed that the types of modules that exist strongly depend on the module's base ring and modules classification also depends on properties of submodules. Therefore, due to the results obtained from this research and the theorems of Matsumura and Kaplansky (which states that a projective module is free over a local ring), it is natural to say that free modules can be generated from any other types of module if the base rings are local. Since the rings of rational numbers are examples of fields (see figure 2.1), James, (2014) and the results of this study showed that the ring of rational numbers formed bases and the bases are linearly independent. The base ring in this study is from fields; therefore modules are vector spaces, this contradicts the work of Amandeep, (2016). Since linear algebra is a subset of abstract algebra, then modules can also have the same real-life applications with vector spaces.

5.2 Conclusions

From the findings of this dissertation, the following conclusions are drawn:

1. The rings of integers over rational numbers (flat module) did not generate free modules because two or more elements of rational numbers are linearly dependent and they cannot form bases for rational numbers.
2. The rings over which a free module is generated from flat module were identified as local rings which are subrings of the ring of function.
3. The ring of rational numbers with even numerator and odd denominator over rational numbers (flat module) formed bases for module $\mathbb{Q}$ and they are linearly independent.
4. An ideal S of the ring of integers mod 6 over the ring itself formed bases and they are linearly independent.
5. Ring of polynomial in one variable with coefficients in a field has generating sets that are linearly independent.
6. The Smith Normal Algorithm of calculating bases established the fact that subrings and ideals are submodules which are generating sets that are linearly independent.

5.3 Contributions to Knowledge

Based on the findings of this dissertation, the study of rings and modules consist of calculating items based upon fixed numbers and numbers that multiply variables. These components are used in equations, which show the relationship between particular numbers. This form of study touches many areas of modern life, such as business, construction, public works, health and cooking. Those who enter these career paths must know and use knowledge from algebra to produce and price items, assure that buildings are constructed safely and according to plans and properly administer drugs and fitness programs.

1. Business owners and financial officers use algebra to set prices according to desired profit margin and the cost of producing or acquiring an item or service for sale.
2. Knowledge from this dissertation assists chefs in having the right amount of ingredients to prepare food and serve diners, chefs can use a matrix to identify foods on a menu, the ingredients and the quantity of each ingredient and then multiply the matrix by the number of diners. Restaurant owners use algebra to calculate the cost of cooking a dish and determine how to price the dish.
3. Algebraic ideas allow fitness professionals to figure a person's current body fat and what amount of weight loss will achieve a desired body-fat percentage. Fitness trainers may use algebra to determine the ratio of diet to exercise needed for achieving and maintaining weight loss.
4. In manufacture companies, parts of machines are technically coupled together using the knowledge of rings and modules; this is achieved by identifying parts of machines that are compatible.

5. The minutes on a clock form a ring, often called $\mathbb{Z}_{60}$ or $\mathbb{Z}/60\mathbb{Z}$. Basically, you can add and multiply as usual, but if you go below 0 or over 59, you wrap around again.

5.4 Recommendations

Based on the findings of this dissertation, the following recommendations are proffered:

1. The study of the set of solution of systems of linear differential equations with constant coefficients is facilitated by the realization that they form a R[D]-module
2. In the theory of error-correcting code, decoding algorithms for certain codes uses Gröbner bases of modules over the ring of polynomials. For instance, rings, modules, and algebraic varieties are used in error correction and, more generally, coding theory. Specifically, there is an abstract error correcting scheme (algebraic-geometry codes) which generalizes Reed-Solomon codes and Chinese Remainder codes. The scheme is basically to take your messages to come from a ring R and encode it by taking its residues modulo many different ideals in ring R. Under certain assumptions about ring R, one can prove that this makes a decent error correcting code.
3. In telecommunications engineering, signal constellation design is facilitated by the use of modules over an algebraic number field.
4. In cryptograph, the construction of NTRU cryptosystem similarly uses a structure that IIRC is best viewed as a module over the ring of modular polynomials.

5.5 Suggestions for Further Studies

This dissertation intends to extend the study of local rings, free and flat modules to algebraic geometry in further study, since algebraic geometry is referred to as the study of geometric problems through algebraic methods (and sometimes vice versa). Algebraic geometry as understood today is very much a 20th century development. Building on ideas of e.g. Riemann and Dedekind, it was realized that there is an intimate connection between properties of the set of solutions of a system of polynomial equations (called an algebraic variety) and the behavior of the set of polynomial functions on that variety (called the coordinate ring).

REFERENCES

Amandeep, K. (2016), "Comparative Study of Vector Space and Modules" *International Journal of Applied Research*, 2(8): pp 374 – 376.

Ambrus, P. (2017), Notes for commutative algebra. Accessed from www.imperial.ac.uk/-apa14/commalgnotes.pdf.on15th April, 2017

Andreas, H. (2005), Abstract Algebra. "Basics, Polynomial, Galois Theory Categorical and Commutative Algebra", pp 167. Accessed from www.mathematik.uni-tuebingen.de/ab/algebra/index.html on 6th April 2017

Avinash, S. (2013), Notes on Ring Theory. Accessed from www.ms.uky.edu/-sohum/ma362/doc/ring-theory-notes.pdf on 10th April, 2017

Berrick, A. J. and Keating, M. E. (2000), "An Introduction to Rings and Modules with k-theory in view".pp1, Cambridge University Press.

Brett, B. and Branden, S. (2013), "Computing Free Basis Projective Modules" *Journal of software for Algebra and Geometry.pp26– 32*

Connell, E. H. (2014), Elements of Abstract and linear Algebra, Department of

Mathematics University of Miami U.S.A

Dylan, P. (2010), Modules: An introduction available at http://www.gnu.org/copyleft/fdi.html.

Francois, C. (2007), "Flat modules over valuation rings" .*Journal of pure and applied algebra, Elsevier, vol 211, pp 235 – 247.*

Gennadi, P. and Philip, R. (2004), "when every finitely generated flat module is projective" .*Journal of Algebra* 277(2)

Hazewinkel, M. (2013), Flat Module. Encyclopedia of Mathematics, accessed from http://www.encyclopediaofmath.org/index.php. On 6th January, 2017

James, M. (2014) Notes on Rings Theory (Math113).Accessed from https://math.berkeley.edu/~gmelvin/math113su14/math113su14notes2.pdf on 15th April, 2017.

Jason, P. (2012). Projective Modules Over local rings are free. http://blog.jpolak.org/. Accessed on 15th April, 2017

Jason, P. (2014), Examples: Projective Modules That are Not Free. . http://blog.jpolak.org/. Accessed on 15th April 2017

Joseph, J. R. (2003), Advanced Modern Algebra Prentice Hall. 1st Edition

Karl-Heinz, F. (2012), Lecture Notes on Modules and Homological Algebra.

Keerthi, M. (2017), "Commutative Algebra" Accessed from www.math.Uchicago.edu/ -keerthi/file/CA.pdf.on 10th April 2017

Konrad, V. (2010),"Flat module" Accessed from www.konradvoelkel.com/2010/10/flat module, on 15th April 2017.

Konrad, V. (2012), Properties of Modules in commutative algebras and implications between them, Accessed fromhttp://en.wikipedia.org/ on 6thFebruary, 2017.

Majid, M. A. and David J. S.(2001). "Projective, flat and multiplication modules" .*New Zealand Journal of Mathematics* Vol 3, (2002), pp 115-129

Matsumura, H. (2000), Commutative ring theory, translated by M. Reid University Press Cambridge.

Michiel, K. (2010), Projective Modules over Dedekind Domains. Accessed from www.math.leidenuniv.nl/redix/tag-2009/michiel - 3 pdf on 20th January, 2017

Parvati, S. (2014), Lecture Note on ***Modules over principal ideal domains.*** Department of Mathematics. University of Mumbai

Paul, G and Robert, B. A. (2012), "Introduction to Abstract Algebra''(Edited by National Mathematical Centre, Abuja).

Rafail, A. and Yilmaz, D.(2010), "Test modules for flatness" *European mathematical society.*

Richard, E. (2010), Lecture Notes in Advanced Abstract Algebra. Accessed from http://neise.org//clemenson on 10th January, 2017

Sean, S. W. (2011), Rings, Modules and Linear Algebra. Accessed from http://www.ndsu.edu/pubweb/ssatherw/ on 10th April, 2017

Siddharth, V. (2015), An intuitive explanation of a local ring. Accessed from https://www.quora.com on 15th April 2017

Travis, S. (2017), Fundamental theorem of modules over a principal ideal domain and applications. Accessed from: www.math.uchicago.edu- /womp/2017/pidmod2007.pdf on 7th January, 2017

Udoye, A. M. and Akor, D. (2014), "Insight on the projective module" *American journal of Engineering Research* Volume 3 Issue 08, pp 248 – 262

Wikipedia (2015), Modules http://en.wikipedia.org/w/index.php.Accessed on 21st March, 2017

Wikipedia (2015), Rings http://en.wikipedia.org/w/index.php. Accessed on 6th April, 2017

Wikipedia (2015), Flat Module http://en.wikipedia.org/w/index.php.Accessed on 6th March, 2017

Wikipedia (2015), Projective Modules http://en.wikipedia.org/w/index.php.Accessed on 10th April, 2017