11-2015

Direct sums decompositions: applications

Wahdan Mohammad Yousef Abuziadeh

United Arab Emirates University

College of Science

Department of Mathematical Sciences

DIRECT SUMS DECOMPOSITIONS: APPLICATIONS

Wahdan Mohammad Yousef Abuziadeh

This thesis is submitted in partial fulfillment of the requirements for the degree of Master of Science in Mathematics

Under the Supervision of Dr. Leonard Daus

November 2015

Declaration of Original Work

I, Wahdan Mohammad Yousef Abuziadeh, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled *"Direct Sums Decompositions: Applications"*, hereby, solemnly declare that this thesis is my own original research work that has been done and prepared by me under the supervision of Dr. Leonard Dăuş, in the College of Science at UAEU. This work has not previously been presented or published, or formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

Student's Signature ______________________ Date ______________

Approval of the Master Thesis

This Master Thesis is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Dr. Leonard Dăuş

Title: Assistant Professor

Department of Mathematical Sciences

College of Science

Signature ______________________ Date ______________

2) Member: Dr. Mohamed Salim

Title: Associate Professor

Department of Mathematical Sciences

College of Science

Signature ______________________ Date ______________

3) Member (External Examiner): Dr. Ayman Badawi

Title: Professor

Department of Mathematics and Statistics

Institution: The American University of Sharjah

Signature ______________________ Date ______________

This Master Thesis is accepted by:

Dean of the College of Science: Dr. Ahmed Murad (Acting Dean)

Signature ______________________ Date ____________

Dean of the College of Graduate Studies: Professor Nagi T. Wakim

Signature ______________________ Date ____________

Copy ________ of ________

Abstract

In this thesis we study the behavior of direct sum decompositions in the category of modules. We present some of the most important "classical" results involving direct sum decompositions for modules (e.g. Krull-Schmidt theorem, decomposition theorems for finitely generated modules over PID etc.). In the last part of the thesis we obtain new results, namely isomorphic refinement theorems for direct sum decompositions of regular modules. We also obtain a link between regular modules and the exchange property.

Keywords: Direct sums decompositions, Krull-Schmidt theorem, semisimple modules, regular modules, exchange property.

Title and Abstract (in Arabic)

تحليل الجمع المباشر: تطبيقات

الملخص

في هذه الأطروحة سوف نقوم بدراسة سلوك تحليل الجمع المباشر على البناء الجبري (الموديول). سوف نعرض أهم النظريات الكلاسيكية في تحليل الجمع المباشر مثل: نظرية كرول سمث ونظريات التحليل للموديولات المولدة بمجموعات متهية . في الجزء الأخير من الأطروحة حصلنا على نتائج جديدة تمثلت في نظريات التشاكل المحسنة لتحليل الجمع المباشر، كذلك حصلنا على علاقة بين الموديولات المنتظمة وخاصية التبادل.

مفاهيم البحث الرئيسية: تحليل الجمع المباشر ، نظرية كرول سمث ، الموديولات شبه البسيطة ، الموديولات المنتظمة ، خاصية التبادل.

Acknowledgements

I would like to thank Dr. Leonard Dăuş for his support during my study, for his helpfulness and his availability.

I would also like to extend my sincere appreciation to all professors at the department of mathematical sciences for their support and concern.

My special thanks go to my principal of Nazwa school Dr. Ismail Al Dorabi for his cooperation.

Last but not the least important, I would like to thank my family for their encouragement and support especially my mother.

Dedication

To my beloved mother and my beloved kids: Roa, Gana, Mohammed, and Abdulrahman

Table of Contents

Chapter 1: Introduction

The main purpose of this thesis is to study the direct sum decompositions of modules, in general, and to obtain new results in the particular case of regular modules. Usually, when we investigate complex algebraic structures, there are two important key steps:

1. we need to identify and to study the simplest constituents, the elementary pieces;

2. we have to analyze how these basic elements interact between them to generate the more complicated structure.

In the case of a module, the elementary pieces are the indecomposable modules. Thus the indecomposable modules can then be thought of as the "basic building blocks", the only objects that sometimes need to be studied, since a module, under some particular conditions, can be written as a direct sum of indecomposable submodules.

In Chapter 2, we present in a concise way some basic concepts related to the category of (left) modules over an arbitrary ring, and we also recall fundamental theorems that we will use in the later chapters.

The third chapter contains some of the most important "classical" results involving direct sum decompositions for modules. The direct sum decomposition problem can be traced back to the last decades of the 19th century: a well-known result of Frobenius and Stickelberger states that every finitely generated abelian group is isomorphic to a direct sum of primary cyclic groups and infinite cyclic groups, and this decomposition is unique. The next step was done by Wedderburn, in 1909. He proved that any two direct products decompositions of a finite group G into indecomposable factors

$$G = H_1 \times H_2 \times \cdots \times H_r = K_1 \times K_2 \times \cdots \times K_s$$

are isomorphic. Afterwards, in 1924 Krull and Schmidt extended this result to modules of finite length. This is a famous result known as Krull-Schmidt Theorem (Theorem 3.1.8). In 1950 Azumaya gave a strengthened form of the previous theorem to the case of arbitrary direct sums of modules having local endmorphism ring. In the last decades, the interest revived to determine new classes of modules and/or rings which satisfy a Krull-Schmidt Theorem. Second section of this chapter is devoted to the semisimple modules, while the last section deals with finitely generated modules over principal ideal domains (PID). The structure theorem for finitely generated modules over a principal ideal domain roughly states that finitely generated modules can be uniquely decomposed in much the same way that integers have a prime factorization.

In the final chapter we study regular modules, a concept introduced by Zelmanowith in 1972. The first section introduces the regular modules following the elementwise definition of Zelmanowitz, but it also contains a new posibility to define regular modules as a particular concept in the Theory of Generalized Inverses. A special attention is given to the link between the regular modules and the notion of locally split (for homomorphisms or modules). In fact, locally split property represents an important toll in the study of regular modules, finally leading to Theorem 4.1.7, showing that any finitely generated submodule of a regular module is a dirrect summand. This theorem was first obtained by Zelmanowith, but our proof is different and self-contained. The previous theorem is also one of the key steps to obtain direct sum decompositions for regular modules, which are given in the second section. One of the most important decomposition problems for modules (or more general, for objects in Grothendieck categories) involves two decompositions of a single module (object). In Theorem 4.2.2 we prove that any two direct sum decompositions of a finitely generated regular module over an arbitrary ring must have an isomorphic refinement. Last part of the fourth chapter is devoted to the exchange property for regular modules. This property, based on the direct sums, was introduced by Crawley and Jonsson for a large class of algebraic structures, called algebras in the sense of Jonsson-Tarski. We have to point out the contribution of Warfield to the systematic study of modules with the (finite) exchange property. One of his major contribution was to extend the Krull-Schmidt theorem, giving a proof based on the exchange property. Our main result in this part of the thesis is to prove that any finitely generated module have the finite exchange property (Theorem 4.3.2).

As a special remark, we have to mention that all the results of the fourth chapter (except those appearing in the first section and involving the notion of locally split) are genuinly new. These results represent a part of the submitted article [11] and they were presented with the occasion of the International Conference on Recent Advances in Pure and Applied Mathematics, 3-6 June 2015, Istanbul, Turkey.

Chapter 2: Module Fundamentals

Throughout this thesis (except Section 3.3), by R we denote an associative and unitary ring, not necessarily commutative.

2.1 Basic Definitions and Examples

Modules are a generalization of the vector spaces of linear algebra in which the "scalars" are allowed to be from an arbitrary ring, instead of a field.

Definition 2.1.1. Let R be a ring. A **left** $R-$**module** (or a left module over R) is an abelian group M together with a scalar multiplication $R \times M \to M$ denoted $(r,m) \longmapsto rm$ (sometimes we say that R acts on M) that satisfy the following axioms:

1. $r(m_1 + m_2) = rm_1 + rm_2$;

2. $(r_1 + r_2)m = r_1 m + r_2 m$;

3. $(r_1 r_2)m = r_1(r_2 m)$;

4. $1_R m = m$,

for any $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$.

Let R be an arbitrary ring and let R^{op} denote the same abelian group, but with new multiplication $\cdot$ defined by $r \cdot s = sr$, (where the multiplication on the right-hand side of this equation is that of R). If M is a left $R-$module. Then we can view M as a right $R^{op}-$module, by defining the right action on M by $mr = rm$ (where the multiplication on the right - hand side of this equation is the old action of R on M). Similarly any right $R-$module can be viewed as a left $R^{op}-$module. In the special case R is commutative ring, it follows $R^{op} = R$.

Example 2.1.1. Let R be a ring. Then R itself is a left $R-$module, where the action of R on itself is just the usual multiplication in the ring R.

Example 2.1.2. Let F be a field. Then each vector space over F is an $F-$module.

Example 2.1.3. Every abelian group M is a $\mathbb{Z}-$module. Indeed we consider the scalar multiplication defined as follows:

If $n > 0$, then $nm = m + m + \cdots + m$ (n times);

If $n < 0$, then $nm = -m - m \cdots - m$ ($-n$ times);

If $n = 0$, then $nm = 0$,

for all $n \in \mathbb{Z}, m \in M$.

Example 2.1.4. Let R be a ring, and let $M = M_{mn}(R)$ be the additive group of all $m \times n$ matrices over R. Then M is an $R-$module, where multiplication of the matrix A by the scalar r means multiplication of each entry of A by r.

Example 2.1.5. If R is a ring. Then $R^n = \{(r_1, r_2, ..., r_n) : r_i \in R\}$ is an $R-$module via componentwise addition and multiplication by elements of R :

$$(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$$

where $a_i, b_i \in R$ for all $i \in \mathbb{N}$, and

$$r(a_1, a_2, ..., a_n) = (ra_1, ra_2, ..., ra_n), r \in R$$

The module R^n is called the **free module** of rank n over R.

Example 2.1.6. Let I be a left ideal of the ring R. Then I is a left $R-$module and the scalar multiplication is just the multiplication of the ring R. Similarly, a right ideal is a right $R-$module, and a two-sided ideal is both a left and a right $R-$module.

Example 2.1.7. If R is a ring and I is an ideal. Then the quotient ring R/I is a left $R-$module via the scalar multiplication:

$$R \times R/I \longrightarrow R/I, (r_1, r_2 + I) \longmapsto r_1 r_2 + I.$$

Definition 2.1.2. Let R be a ring and M an $R-$module. A subset $N \subseteq M$ is called an $R-$**submodule** of M if N is a subgroup of M which is closed under the action of ring elements:

$$rn \in N \text{ for all } r \in R, n \in N.$$

If V is a vector space over a field F. Then an $F-$subfield of V is called *a* ***linear subspace*** of V.

Example 2.1.8. The left ideals of a ring R are considered as the $R-$ submodules of the $R-$module R.

Example 2.1.9. If M is any abelian group. Then M is a $\mathbb{Z}-$module, and the $\mathbb{Z}-$submodules of M are just the subgroups of M.

Lemma 2.1.1. *If M is an $R-$module and N is a nonempty subset of M. Then N is an $R-$submodule of M if and only if $an_1 + bn_2 \in N$ for all $n_1, n_2 \in N$ and $a, b \in R$.*

Lemma 2.1.2. *Let M be an $R-$ module and let $\{N_\alpha\}_{\alpha \in A}$ be a family of submodules of M. Then $N = \bigcap\limits_{\alpha \in A} N_\alpha$ is a submodule of M.*

2.2 Quotient Modules and Module Homomorphisms

Definition 2.2.1. Let M be a left $R-$module and let N be an $R-$submodule of M. We can form the quotient group $M/N = \{m + N : m \in M\}$ which becomes an $R-$module by defining $r(m+N) = rm+N$ for all $r \in R, m \in M$. We call M/N **the quotient** of M by N.

Definition 2.2.2. Let M and N be left $R-$modules. An $R-$**module homomorphism** from M to N is a map $\varphi : M \longmapsto N$ such that

1. $\varphi(m_1+m_2) = \varphi(m_1)+\varphi(m_2)$, for all $m_1, m_2 \in M$; and

2. $\varphi(rm) = r\varphi(m)$, for all $r \in R, m \in M$.

Equivalently, $\varphi(r_1m_1+r_2m_2) = r_1\varphi(m_1)+r_2\varphi(m_2)$, for all $r_1, r_2 \in R$, $m_1, m_2 \in M$.

The set of all $R-$module homomorphisms from M to N will be denoted $Hom_R(M,N)$.

If $M = N$, then a homomorphism from $M \to M$ is called **endomorphism** of M. We denoted the set of all endomorphisms by $End(M)$.

Remark. 1. If R is a field. Then $R-$module homomorphisms are called **linear transformations.**

Definition 2.2.3. The **Kernel** of a homomorphism φ is $Ker\varphi = \{m \in M : \varphi(m) = 0\}$, and the **Image** of φ is $Im(\varphi) = \{n \in N : n = \varphi(m)$ for all $m \in M\}$.

Remark. 2. $Ker\varphi$ is a submodule of M, and $Im(\varphi)$ is a submodule of N.

Example 2.2.1. The map $\pi : M \longmapsto M/K$ defined by $\pi(m) = m+K$ is an $R-$module homomorphism. Obviously, π is surjective.

Example 2.2.2. Let R be a ring and let $M = R^n$. Consider a natural number n. For each $i \in \{1,2,...,n\}$, the projection map $\pi_i : R^n \longmapsto R$ given by $\pi_i(r_1,r_2,...,r_n) = r_i$ is a surjective $R-$module homomorphism with Kernel equal to the submodule of n-tuples which have a zero in position i.

Example 2.2.3. $\mathbb{Z}-$modules homomorphisms are the same as abelian group homomorphisms.

Theorem 2.2.1. ***(First Isomorphism Theorem For Modules)***

Let M,N be $R-$modules and let $\varphi : M \longmapsto N$ be an $R-$module homomorphism. Then $M/Ker\varphi \simeq Im(\varphi)$.

Theorem 2.2.2. ***(Second Isomorphism Theorem For Modules)***

Let S and T be submodules of an $R-$module M, and let $S+T = \{s+t : s \in S, t \in T\}$. Then $S+T$ and $S \cap T$ are submodules of M and $(S+T)/T \simeq S/(S \cap T)$.

Remark. 3. $S+T$ is the smallest module that contains both S and T, and $S \cap T$ is the largest module included in both S and T.

Theorem 2.2.3. ***(Third Isomorphism Theorem For Modules)***

Let S and T be submodules of an $R-$module M, with $S \subseteq T \subseteq M$. Then $(M/S)/(T/S) \simeq M/T$.

Theorem 2.2.4. ***(Correspondence Theorem)***

Let N be a submodule of the $R-$module M and $\pi : M \to M/N$ the natural projection map. Then the function $P \mapsto P/N$ defines a one-to-one correspondence between the set of all submodules of M that contain N and the set of all submodules of M/N.

2.3 Direct Sums

Definition 2.3.1. Let R be a ring and let $(M_i)_{i\in I}$ be an indexed family of left $R-$modules. The **direct product** of the modules M_i denoted $\prod\limits_{i\in I} M_i$ is the cartesian product with coordinatewise addition and scalar multiplication:

$$(m_1, m_2, ..., m_n) + (m'_1, m'_2, ..., m'_n) = (m_1 + m'_1, m_2 + m'_2, ..., m_n + m'_n)$$

$$r(m_1, m_2, ..., m_n) = (rm_1, rm_2, ..., rm_n)$$

where $r \in R$ and $m_i, m_i' \in M_i$ for all $i \in I$.

Definition 2.3.2. The **(external) direct sum,** denoted $\bigoplus_{i \in I} M_i$, is the submodule of $\prod_{i \in I} M_i$ consisting of all elements $\prod_{i \in I} m_i$ such that only finitely many of the components m_i are nonzero.

Definition 2.3.3. Let M be a left $R-$module, and let $N_1, N_2, ..., N_k$ be submodules of M. We define M to be their **(internal) direct sum** $M = N_1 \oplus N_2 \oplus \cdots \oplus N_k$ if each $m \in M$ can be written uniquely as $m = a_1 + a_2 + \cdots + a_k$, where $a_i \in N_i$ for all $i = 1, 2, ..., k$.

Proposition 2.3.1. *Let $N_1, N_2, ..., N_k$ be submodules of the left $R-$module M. Then the following are equivalent:*

1. *The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ defined by*

$$\pi(a_1, a_2, ..., a_k) = a_1 + a_2 + \cdots + a_k$$

   is an $R-$module isomorphism.

2. $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ *for all* $j \in \{1, 2, ..., k\}$.

3. *Every $x \in N_1 + N_2 + \cdots + N_k$ can be written uniquely in the form*

$$x = a_1 + a_2 + \cdots + a_k$$

   with $a_i \in N_i$.

Proof: To prove (1) implies (2), suppose for some j that (2) fails to hold and let $a_j \in N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k)$ with $a_j \neq 0$. Then $a_j = a_1 + \cdots + a_{j-1} + a_{j+1} + \cdots + a_k$, for some $a_i \in N_i$, and $(a_1, ..., a_{j-1}, -a_j, a_{j+1}, ..., a_k)$ would be a nonzero element of $Ker\ \pi$, a contradiction.

To prove (2) implies (3), assume that (2) holds. If for some module elements $a_i, b_i \in N_i$

we have $a_1 + a_2 + \cdots + a_k = b_1 + b_2 + \cdots + b_k$, then for each j we have $a_j - b_j = (b_1 - a_1) + \cdots + (b_{j-1} - a_{j-1}) + (b_{j+1} - a_{j+1}) + \cdots + (b_k - a_k)$. The left hand side is in N_j and the right hand side belongs to $N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k$. Thus $a_j - b_j \in N_j \cap (\, N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k\,) = 0$. This shows $a_j = b_j$ for all j, and so (2) implies (3).

Finally, to see that (3) implies (1) observe first that the map π is clearly a surjective $R-$module homomorphism. Then (3) implies that π is injective, hence it is an $R-$module isomorphism. ■

Definition 2.3.4. The pair of homomorphisms $M_1 \xrightarrow{\psi} M_2 \xrightarrow{\varphi} M_3$ is said to be **exact** (at M_2) if $Im\ \psi = Ker\ \varphi$.

Definition 2.3.5. Let R be a ring. A sequence of left $R-$modules and homomorphisms $\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$ is said to be **exact (**at M_i) if $Im(f_i) = Ker(f_{i+1})$. The sequence is said to be **exact** if it is exact at each M_i.

Proposition 2.3.2. *Let M_1, M_2, M_3 be left $R-$modules over a ring R. Then:*

1. *The sequence $0 \longrightarrow M_1 \xrightarrow{\psi} M_2$ is exact (at M_1) if and only if ψ is injective.*
2. *The sequence $M_2 \xrightarrow{\varphi} M_3 \longrightarrow 0$ is exact (at M_3) if and only if φ is surjective.*

Proof: (1) The sequence $0 \longrightarrow M_1 \xrightarrow{\psi} M_2$ is exact if and only if $Im(0 \longrightarrow M_1) = 0 = Ker\ \psi$ if and only if ψ is injective.

(2) The sequence $M_2 \xrightarrow{\varphi} M_3 \longrightarrow 0$ is exact if and only if $Ker(M_3 \longrightarrow 0) = M_3 = Im\ \varphi$ if and only if φ is surjective. ■

Corollary 2.3.3. *The sequence $0 \longrightarrow M_1 \xrightarrow{\psi} M_2 \xrightarrow{\varphi} M_3 \longrightarrow 0$ is exact if and only if ψ is injective, φ is surjective, and $Im\ \psi = Ker\ \varphi$.*

Definition 2.3.6. The exact sequence $0 \longrightarrow M_1 \xrightarrow{\psi} M_2 \xrightarrow{\varphi} M_3 \longrightarrow 0$ is called a **short exact sequence.**

Example 2.3.1. Given modules M_1 and M_3, we can always form their direct sum

$M_2 = M_1 \oplus M_3$ and the sequence $0 \longrightarrow M_1 \xrightarrow{\iota} M_1 \oplus M_3 \xrightarrow{\pi} M_3 \longrightarrow 0$ where ι is the inclusion map $\iota(m_1) = (m_1, 0)$ and π is the projection map $\pi(m_1, m_3) = m_3$ for all $m_1 \in M_1$ and $m_3 \in M_3$ we have a short exact sequence.

Example 2.3.2. If $\varphi : M_1 \to M_2$ is a homomorphism we may form an exact sequence:

$$0 \to Ker\varphi \xrightarrow{\iota} M_1 \xrightarrow{\varphi} Im\ \varphi \to 0$$

where ι is the inclusion map.

Definition 2.3.7. A short exact sequence

$$0 \longrightarrow M_1 \xrightarrow{\psi} M_2 \xrightarrow{\varphi} M_3 \longrightarrow 0$$

is **split** if there exists a map $\xi : M_3 \longrightarrow M_2$ with $\varphi \circ \xi = 1_{M_3}$.

Proposition 2.3.4. *If an exact sequence*

$$0 \longrightarrow M_1 \xrightarrow{\psi} M_2 \xrightarrow{\varphi} M_3 \longrightarrow 0$$

is split. Then $M_2 \simeq M_1 \oplus M_3$.

Proof: Since the exact sequence is split, there exists $\xi : M_3 \longrightarrow M_2$ such that $\varphi \circ \xi = 1_{M_3}$. We want to prove that $M_2 = Im\psi + Im\xi$. Let $b \in M_2$, $\varphi(b) \in M_3$. We claim that $b - \xi(\varphi(b))$ is in $Ker\varphi$ since $\varphi(b - \xi(\varphi(b))) = \varphi(b) - \varphi(\xi(\varphi(b))) = \varphi(b) - (\varphi \circ \xi)(\varphi(b)) = \varphi(b) - \varphi(b) = 0$. But since $Im\psi = Ker\varphi$ (exactness at M_2), $b - \xi(\varphi(b))$ is in $Im\psi$, it means there exists an a in M_1 such that $\psi(a) = b - \xi(\varphi(b))$. Then $b = \psi(a) + \xi(\varphi(b))$; $\psi(a)$ is obviously in $Im\psi$, and $\xi(\varphi(b))$ is in $Im\xi$. Hence $M_2 = Im\psi + Im\xi$.

Next we need to prove that this sum is direct, equivalently, the intersection of $Im\psi$ and $Im\xi$ is 0. Assume that $x \in Im\psi \cap Im\xi$, $x = \psi(\acute{a}) = \xi(c)$ for some $\acute{a} \in M_1$ and $c \in M_3$, this implies that $\varphi(x) = \varphi(\psi(\acute{a})) = 0$ ($\psi(\acute{a}) \in Im\psi = Ker\varphi$) and $\varphi(x) = \varphi(\xi(c)) = (\varphi \circ \xi)(c) = 1_{M_3}(c) = c$. Hence $x = \xi(c) = \xi(0) = 0$. ■

Definition 2.3.8. Let M and N be $R-$modules, and let $\varphi : M \longmapsto N$ be an $R-$module homomorphism. The **Cokernel** of φ denoted by $CoKer(\varphi)$ is the quotient module $N/Im(\varphi)$.

Definition 2.3.9. A nonzero $R-$module M is ***simple*** *if* the only submodules of M are 0 and M.

Definition 2.3.10. An $R-$module M is said to be **indecomposable** if whenever $M = N_1 \oplus N_2$ for some submodules N_1, N_2, we have $N_1 = 0$ or $N_2 = 0$.

Remark. 4. Every simple module is indecomposable, but not-vice versa.

Lemma 2.3.5. *Let M be a nonzero $R-$module and let N be an indecomposable $R-$module. Suppose that $f : M \to N$ and $g : N \to M$ be two $R-$module homomorphisms such that $g \circ f : M \to M$ is an isomorphism. Then f and g are isomorphisms as well.*

Proof: As $g \circ f$ is isomorphism we obtain that f is injective and g is surjective. We have to prove that f is surjective and g is injective. Consider the two exact sequences $0 \to M \to N \to CoKer(f) = N/Im(f) \to 0$ and $0 \to Ker(g) \hookrightarrow N \to M \to 0$, these sequences are split. So $N \simeq Ker(g) \oplus M \simeq M \oplus CoKer(f)$. But by hypothesis M is a nonzero $R-$module and N is an indecomposable $R-$module. It follows that $Ker(g) = CoKer(f) = 0$. Thus g is injective and f is surjective. ■

Definition 2.3.11. A left R-module S is **cyclic** if there exists $s \in S$ with $S = \{rs : r \in R\}$. If M is an R-module and $m \in M$, then the **cyclic submodule generated** by m, denoted by $\langle m \rangle$, is $\langle m \rangle = \{rm : r \in R\}$. More generally, if X is a subset of an $R-$module M, then we denote

$$\langle X \rangle = \left\{ \sum_{finite} r_i x_i : r_i \in R \; and \; x_i \in X \right\},$$

the set of all R-linear combinations of elements in X. We will call $\langle X \rangle$ the **submodule**

generated by X.

Definition 2.3.12. A left $R-$module $M = \langle X \rangle$ is **finitely generated** if X is a finite set.

Example 2.3.3. A vector space V over a field K is a finitely generated $K-$module if and only if V is finite-dimensional.

Chapter 3: "Classical" Direct Sum Decompositions

3.1 Krull-Schmidt Theorem

Definition 3.1.1. Let R be a ring and M be an $R-$module. We shall say that M is **Artinian** if it satisfies any of the following two equivalent conditions:

1. The *minimum condition,* or *min,* if every nonempty collection of nontrivial submodules of M has a minimal element. This means that if Γ is a nonempty family of submodules, then there exists $N \in \Gamma$ such that N contains no other elements of Γ.

2. The *descending chain condition,* or *D.C.C.,* if every descending chain $M_1 \supseteq M_2 \supseteq \cdots$ of nontrivial submodules of M stabilizes, that is, for some r and all $n \geq 0$, $M_r = M_{r+n}.$

It is easy to prove that the two conditions are equivalent. Suppose M satisfies the minimum condition and let $M_1 \supseteq M_2 \supseteq \cdots$ be a descending chain of nontrivial submodules of M. Then the collection $\{M_1, M_2, ...\}$ contains a minimal element, say M_n, and the series stabilizes at n.

Conversely, suppose M satisfies D.C.C and let Γ be a nonempty collection of nontrivial submodules of M. Choose $M_1 \in \Gamma$. If M_1 is not minimal, then there exists $M_2 \in \Gamma$ with $M_1 \supset M_2$. If M_2 is not minimal, then we can find $M_3 \in \Gamma$ with $M_2 \supset M_3$. Continuing in this manner, we either find a minimal element of Γ or we construct an infinite descending chain $M_1 \supset M_2 \supset \cdots$ that does not stabilize, which a contradiction with D.C.C.

Lemma 3.1.1. *Let M be an $R-$module, and let N be a submodule of M. Then:*

1. *M is Artinian if and only if both N and M/N are Artinian.*

2. *Suppose $\{N_i \mid i \in I\}$ is a family of simple submodules of M and that $M = \sum_i N_i$. Then M is Artinian if and only if the index set I is finite.*

Proof: (1) Suppose first that M is Artinian. Since any descending chain of submodules of N is also a chain of submodules of M, it follows that N inherits D.C.C from M, so N is Artinian . Now let $\pi : M \to M/N$ be the natural $R-$epimorphism and let $M'_1 \supseteq M'_2 \supseteq \cdots$ be a descending chain of submodules of M/N. If we denote $M_i = \pi^{-1}(M'_i)$, then $\pi(M_i) = M'_i$ and $M_1 \supseteq M_2 \supseteq \cdots$ is a descending chain in M. But the latter chain must stabilize and hence, using $\pi(M_i) = M'_i$, we conclude that the original one does also. Therefore M/N is Artinian.
Conversely, suppose N and M/N satisfy D.C.C and let $M_1 \supseteq M_2 \supseteq \cdots$ be a descending chain of submodules of M. Then

$$(M_1 \cap N) \supseteq (M_2 \cap N) \supseteq \cdots \supseteq (M_i \cap N) \supseteq \cdots$$

is a descending chain of submodules of N and hence this chain must stabilize, say at p. Furthermore,

$$(M_1 + N)/N \supseteq (M_2 + N)/N \supseteq \cdots \supseteq (M_i + N)/N \supseteq \cdots$$

is a descending chain of submodules of M/N and hence this chain must also stabilize, say at q. In particular, if $t \geq p, q$, then $M_{t+1} \cap N = M_t \cap N$ and $M_{t+1} + N = M_t + N$. Thus since $M_t \supseteq M_{t+1}$, the Modular Law implies that $M_t = M_{t+1}$ and we conclude that the original series does indeed stabilize.

(2) If I is finite. Then M has only a finite number of submodules. Since in a finite family of modules we may always find a minimum member, then M is Artinian. On other hand, if I is infinite, then we can construct an infinite strictly descending chain of submodules of M by deleting one summand at a time from the direct sum

$M = \sum_i N_i$. ■

Definition 3.1.2. Let R be a ring and M be an $R-$module. We shall say that M is **Noetherian** if it satisfies any one of the following two equivalent conditions:

1. The *maximum condition,* or *max,* if every nonempty collection of nontrivial submodules of M has a maximal element. This means that if $\Gamma$is a nonempty family of nontrivial submodules, then there exists $N \in \Gamma$ such that N is contained in no other element of Γ.

2. The *ascending chain condition,* or *A.C.C,* if every ascending chain $M_1 \subseteq M_2 \subseteq \cdots$ of nontrivial submodules of M stabilizes, that is, for some r and all $n \geq 0$, $M_r = M_{r+n.}$

To prove that the two conditions are equivalent, we first assume that M satisfies the maximum condition and let $M_1 \subseteq M_2 \subseteq \cdots$ be an ascending chain of nontrivial submodules of M. Then the collection $\{M_1, M_2, ...\}$ contains a maximal element, say M_n, and the series stabilizes at n.

Conversely, suppose M satisfies A.C.C and let Γ be a nonempty collection of nontrivial submodules of M. Choose $M_1 \in \Gamma$. If M_1 is not maximal, then there exists $M_2 \in \Gamma$ with $M_1 \subset M_2$. If M_2 is not maximal, then we can find $M_3 \in \Gamma$ with $M_2 \subset M_3$. Continuing in this manner, we either find a maximal element of Γ or we construct an infinite ascending chain $M_1 \subset M_2 \subset \cdots$ that does not stabilize.

Lemma 3.1.2. *Let M be an $R-$module, and let N be a submodule of M. Then:*

1. *M is Noetherian if and only if both N and M/N are Noetherian.*

2. *M is Noetherian if and only if its submodules are all finitely generated.*

Proof: (1) This follows as in Lemma 3.1.2 (1).

(2) Assuming that M is Noetherian, then M satisfies max. We have to prove that every submodule of M is finitely generated.

Let N be a submodule of M. Since 0 is finitely generated submodule of N, it follows from max that there exists a submodule N' of N maximal with the property of being finitely generated. But if $n \in N$, then $N' + nR$ is also a finitely generated submodule of N. Thus maximality of N' implies that $n \in N'$and therefore that $N' = N$.

Conversely, suppose that all submodules of M are finitely generated. We have to prove that M is Noetherian.

Let $M_1 \subseteq M_2 \subseteq \cdots$ be an ascending chain of nontrivial submodules of M. If $N = \cup_{i=1}^{\infty} M_i$, then N is a submodule of M and hence it is finitely generated. But each generator of N is contained in some M_i and, by taking the largest of these finitely many subscripts, we see that all generators of N are contained in some M_t. Thus $N = M_t$ and we conclude that the series stabilize at t. ■

Definition 3.1.3. Let M be a module over a ring R. The **length** of M, written as $\ell(M)$, is the supremum of lengths n of chains $N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_n = M$ of submodules $N_i \subseteq M$. So $\ell(M) \in \mathbb{N} \cup \{\infty\}$.

If $\ell(M)$ is a finite number we say M has **finite length**, otherwise M has **infinite length**.

Example 3.1.1.

1. $\ell(M) = 0$ if and only if $M = \{0\}$.
2. An $R-$module M is simple if and only if $\ell(M) = 1$.
3. For m a positive integer, the $\mathbb{Z}-$ module $M = \mathbb{Z}/(m)$ has length equal the number of prime factors (with multiplicities) of m.
4. $\mathbb{Z}$ has infinite length as a module over itself.
5. If V is a vector space over a field F. Then $\ell(V) = \dim_F(V)$.

In the next theorem there are given some basic facts about the length of a module. For the proof we recommend [19, Theorem 12.3].

Theorem 3.1.3. *Let M be a module over a ring R.*

1. *M has finite length if and only if it is Artinian and Noetherian. In particular, R*

has finite length as a module over itself if and only if it is Artinian. (because an Artinian ring is also Noetherian).

2. *Let $N \subseteq M$ be a submodule. Then $\ell(M) = \ell(N) + \ell(M/N)$.*

3. *If M has finite length and N is a submodule of M. Then N has finite length as well, and we have $\ell(N) \leq \ell(M)$.*

   Furthermore, if N is a proper submodule of M, then $\ell(N) < \ell(M)$.

4. *If M_1, M_2 are both indecomposable. Then $\ell(M_1 \oplus M_2) = \ell(M_1) + \ell(M_2)$.*

Theorem 3.1.4. *(Fitting's lemma) Let M be an $R-$module and let $\varphi \in End(M)$.*

1. *If M is Noetherian. Then there exists a positive integer n such that:*

$$Ker\varphi^n \cap Im\varphi^n = 0.$$

2. *If M is Artinian. Then there exists a positive integer n such that:*

$$M = Ker\varphi^n + Im\varphi^n.$$

3. *If M is a module of finite length. Then there exists a positive integer n such that:*

$$M = Ker\varphi^n \oplus Im\varphi^n.$$

Proof: (1) Let M be a Noetherian module. Then we have $Ker\varphi \subseteq Ker\varphi^2 \subseteq Ker\varphi^3 \subseteq \cdots$ and $Ker\varphi^n = Ker\varphi^{n+1} = \cdots$ for some positive integer n. We have to show that $Ker\ \varphi^n \cap Im\ \varphi^n = 0$. If $x \in Ker\ \varphi^n \cap Im\ \varphi^n$ then $x \in Ker\ \varphi^n$ and $x \in Im\ \varphi^n$, this implies that $\varphi^n(x) = 0$ and there exist $y \in M$ such that $x = \varphi^n(y)$. It follows that

$\varphi^n(x) = \varphi^{2n}(y) = 0$. So $y \in Ker\ \varphi^{2n} = Ker\ \varphi^n$. Hence $x = \varphi^n(y) = 0$.

(2) Let M be an Artinian module. Then we have $Im\varphi \supseteq Im\varphi^2 \supseteq Im\varphi^3 \supseteq \cdots$ and $Im\varphi^n = Im\varphi^{n+1} = \cdots$ for some positive integer n. We have to show that $M = Ker\ \varphi^n + Im\ \varphi^n$.

Let $x \in M$ be arbitrary. As $Im\varphi^n = Im\varphi^{2n}$, there exists $y \in M$ such that $\varphi^n(x) = \varphi^{2n}(y)$. Write $x = (x - \varphi^n(y)) + \varphi^n(y)$. If we show that $x - \varphi^n(y) \in Ker\varphi^n$ then we done. Indeed $\varphi^n(x - \varphi^n(y)) = \varphi^n(x) - \varphi^{2n}(y) = 0$.

(3) By Theorem 3.1.3 (1) since M has finite length, M is Artinian and Noetherian. Using now (1) and (2) we obtain the conclusion. ∎

Definition 3.1.4. Let R be a ring.

1. An element $a \in R$ is called **idempotent** *element if* $a^2 = a$.

2. An element $a \in R$ is called **nilpotent** element if there exists $n \in \mathbb{N}^*$ such that $a^n = 0$.

Lemma 3.1.5. *An $R-$module M is indecomposable if and only if the only idempotents of the endomorphism ring of M are* 0 *and* 1.

Proof Let $e \in End(M)$ be idempotent element. Obviously $M = e(M) + (id - e)(M)$. We have to show that this sum is direct. In fact we have to show that $e(M) \cap (id - e)(M) = \{0\}$.

Let $x \in e(M) \cap (id - e)(M)$, then $x \in e(M)$ and $x \in (id - e)(M)$, this means that there exist $m_1, m_2 \in M$ such that $x = e(m_1)$ and $x = (id - e)(m_2) = m_2 - e(m_2)$ this implies that $e(x) = e(m_2 - e(m_2)) = e(m_2) - e(e(m_2)) = e(m_2) - e(m_2) = 0$. But $e(x) = e(e(m_1)) = e(m_1) = x$, hence $x = 0$. ∎

Lemma 3.1.6. *If a is a nilpotent element of a ring R, then $1 - a$ is invertible.*

Proof: If a is a nilpotent, then $a^n = 0$ for some $n > 0$. But then

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

and so $1-a$ is invertible. ■

Corollary 3.1.7. *Let M be an indecomposable $R-$module of finite length. Then every endomorphism of M is either nilpotent or isomorphism. In particular, the set of non-invertible elements of $End(M)$ is closed under addition.*

Proof: Since M is of finite length, it follows, by part (3) of Fitting's Lemma, that $M \simeq Ker\ \varphi^n \oplus Im\ \varphi^n$. As M is indecomposable, either $Ker\ \varphi^n = 0$ and $Im\varphi^n = M$, or $Ker\ \varphi^n = M$ and $Im\varphi^n = 0$. In the first case, we already noticed before that $Ker\varphi \subseteq Ker\varphi^2 \subseteq Ker\varphi^3 \subseteq \cdots \subseteq Ker\varphi^n = 0$, then $Ker\varphi = 0$ and so φ is injective. On the other hand we also noticed that $Im\varphi \supseteq Im\varphi^2 \supseteq Im\varphi^3 \supseteq \cdots \supseteq Im\varphi^n = M$, then $Im\varphi = M$ and so φ is surjective. Hence φ is an isomorphism. In the later case ($Ker\ \varphi^n = M$ and $Im\varphi^n = 0$) we have $\varphi^n = 0$ and hence φ is nilpotent. Now we have to show that $h = f+g$ is also a non-invertible element of $End(M)$ for every non-invertible $f, g \in End(M)$. Assume that h is invertible, so we obtain $id = h^{-1}f + h^{-1}g$. As f is non-invertible, so is $h^{-1}\ f$ and by the first part of the corollary, $h^{-1}\ f$ is nilpotent and so $h^{-1}g = id - h^{-1}\ f$ is invertible (by the above lemma) so is $g = h(id - h^{-1}\ f)$. But we assumed that $f, g \in End(M)$ are non-invertible, so our assumption that $h = f+g$ is invertible was wrong, so h is non-invertible. ■

Theorem 3.1.8. *(Krull-Schmidt Theorem). Let M be a finitely generated $R-$module and let*

$$M = U_1 \oplus U_2 \oplus \cdots \oplus U_m \simeq V_1 \oplus V_2 \oplus \cdots \oplus V_n$$

be two decompositions of M where $U_i's$ and $V_j's$ are indecomposable $R-$modules. Then $m = n$ and after a rearrangement of indices we have $U_i \simeq V_i$ for every i.

Proof: Let $\varphi : U_1 \oplus U_2 \oplus \cdots \oplus U_m \to V_1 \oplus V_2 \oplus \cdots \oplus V_n$ be an $R-$module isomorphism. We prove the result by induction on $m+n$. If $m+n = 2$ then $m = n = 1$ and the conclusion is immediate. Let $\pi_i : U_1 \oplus U_2 \oplus \cdots \oplus U_m \to U_i$ and $\pi'_j : V_1 \oplus V_2 \oplus \cdots \oplus V_n \to V_j$ be the canonical projections and let $\iota_i : U_i \hookrightarrow U_1 \oplus U_2 \oplus \cdots \oplus U_m$ and

$\iota'_j : V_j \hookrightarrow V_1 \oplus V_2 \oplus \cdots \oplus V_n$ be the canonical inclusions. Consider the endomorphisms ρ_{ij} of U_i which is the composition of $\pi'_j \circ \varphi \circ \iota_i : U_i \to V_j$ and $\pi_i \circ \varphi^{-1} \circ \iota'_j : V_j \to U_i$. We have two possibilities.

Case (1): If there exist two indices i and j such that ρ_{ij} is an isomorphism (say $i = j = 1$) then we have the isomorphism $\pi'_1 \circ \varphi \circ \iota_1 : U_1 \simeq V_1$ as well. We will prove $\varphi' := (\oplus_{s=2}^{n} \pi'_r) \circ \varphi \circ (\oplus_{r=2}^{m} \iota_s) : (\oplus_{r=2}^{m} U_r) \to (\oplus_{s=2}^{n} V_s)$ is an isomorphism.

For injectivity:

Suppose that $(u_2, ..., u_m)$ is in the kernel of this map. So $\pi'_s(\varphi(0, u_2, ..., u_m)) = 0$ for all $s = 2, ..., n$, but $\pi'_s : \oplus_{j=1}^{n} V_j \to V_s$. Hence $\varphi(0, u_2, ..., u_m) = (v_1, 0..., 0)$. It follows that $\varphi(0, u_2, ..., u_m) = \iota'_1(v_1)$. By applying the map $\pi_1 \circ \varphi^{-1}$ on both sides we get $0 = \pi_1 \circ \varphi^{-1} \circ\ \iota'_1(v_1)$. As $\pi_1 \circ \varphi^{-1} \circ\ \iota'_1$ is an isomorphism we obtain $v_1 = 0$ so $\varphi(0, u_2, ..., u_m) = (v_1, 0..., 0) = (0, 0, ..., 0)$, and so $(u_2, ..., u_m) = (0, ..., 0)$.

For surjectivity:

As $\varphi' : (\oplus_{r=2}^{m} U_r) \to (\oplus_{s=2}^{n} V_s)$ is injective so $\ell(\oplus_{r=2}^{m} U_r) = \ell(\varphi'(\oplus_{r=2}^{m} U_r)) = \ell(\oplus_{s=2}^{n} V_s)$ it follows that $\varphi'(\oplus_{r=2}^{m} U_r) = \oplus_{s=2}^{n} V_s$, hence φ' is surjective.

Case (2): if for every j, ρ_{ij} is not isomorphism, then by previous corollary ρ_{ij} is nilpotent and so $\sum_{j=1}^{n} \rho_{ij}$ is nilpotent as well. But $\sum_{j=1}^{n} \rho_{ij} = id_{U_i}$, a contradiction. ■

3.2 Semisimple Modules

A one-dimensional space is simple in the sense that it does not have a nontrivial proper subspace. Thus any vector space is a direct sum of simple subspaces. Starting from this idea, it is possible to consider a new class of modules, namely semisimple modules.

Theorem 3.2.1. *Let M be a nonzero $R-$module. The following conditions are equivalent.*

1. *M is a sum of simple modules;*

2. *M is a direct sum of simple modules;*

3. *If N is a submodule of M, then N is a direct summand of M, that is, there is a*

submodule $N^{'}$ of M such that $M = N \oplus N^{'}$.

Proof: $(1) \Rightarrow (2)$ Let M be the sum of simple modules $M_{i,}$ $i \in I$. If $J \subseteq I$, denote $\sum_{j \in J} M_j$ by $M(J)$. By Zorn's lemma, there is a maximal subset J of I such that the sum defining $N = M(J)$ is direct. We will show that $M = N$. First assume that $i \notin J$. Then $N \cap M_i$ is a submodule of a simple module $M_{i,}$ so it must be either 0 or $M_{i.}$ If $N \cap M_i = 0$, then $M(J \cup \{i\})$ is direct, contradicting maximality of J. Thus $N \cap M_i = M_{i,}$ so $M_i \subseteq N$. But if $i \in J$, then $M_i \subseteq N$ by definition of N. Therefore $M_i \subseteq N$ for all i, and since M is the sum of all M_i, we have $M = N$.

$(2) \Rightarrow (3)$ This is essentially the same as (1) implies (2). Let N be a submodule of M, where M is the direct sum of simple modules $M_{i,}$ $i \in I$. Let J be a maximal subset of I such that the sum $N + M(J)$ is direct. If $i \notin J$ then exactly as before, $M_i \cap (N \oplus M(J)) = M_i$, so $M_i \subseteq N \oplus M(J)$. This holds for $i \in J$ as well, by definition of $M(J)$. It follows that $M = N \oplus M(J)$.

$(3) \Rightarrow (1)$ First we make several observations:

(a) If M satisfies (3), so does every submodule N. [Let $N \leq M$, so that $M = N \oplus N^{'}$. If V is a submodule of N, hence of M, we have $M = V \oplus W$. If $x \in N$, then $x = v + w, v \in V, w \in W$. So $w = x - v \in N$ (using $V \leq N$). But v also belong to N, and consequently $N = (N \cap V) \oplus (N \cap W) = V \oplus (N \cap W)$.]

(b) If $D = A \oplus B \oplus C$, then $A = (A+B) \cap (A+C)$. [If $a + b = a^{'} + c$, where $a, a^{'} \in A, b \in B, c \in C$, then $a^{'} - a = b - c$, and since D is direct sum, we have $b = c = 0$ and $a = a^{'}$. Thus $a + b \in A$.]

(c) If N is a nonzero submodule of M, then N contains a simple submodule. [Choose a nonzero $x \in N$. By Zorn's lemma, there is a maximal submodule V of N such that $x \notin V$. By (a) we can write $N = V \oplus V'$, and $V' \neq 0$ by choice of x and V.

If $V^{'}$ is simple, we are finished, so assume that $V^{'}$ is not simple. Then $V^{'}$ contains a nontrivial proper submodule $V_{1,}$ so by (a) we can write $V^{'} = V_1 \oplus V_2$ with the V_j nonzero. By (b), $V = (V + V_1) \cap (V + V_2)$. Since $x \notin V$, either $x \notin V + V_1$ or $x \notin V + V_2$, which contradicts the maximality of V.]

To prove that $(3) \Rightarrow (1)$, let N be the sum of all simple submodules of M. By (3) we can write $M = N \oplus N'$. If $N' \neq 0$, then by (c), N' contains a simple submodule V. But then $V \leq N$ by definition of N. Thus $V \leq N \cap N' = 0$, a contradiction. Therefore $N' = 0$ and $M = N$. ■

Definition 3.2.1. A module M satisfying any of the previous three equivalent conditions is called **semisimple** or **completely reducible**.

Proposition 3.2.2. *Nonzero submodules and quotient modules of a semisimple module are semisimple.*

Proof: The submodule case follows from (a) of the proof of the previous theorem.
Let $N \leq M$, where $M = \sum_i M_i$ with the M_i simple. Applying the canonical map from M to M/N, we have

$$M/N = \sum_i (M_i + N)/N.$$

By The Second Isomorphism Theorem, $(M_i + N)/N$ is isomorphic to a quotient of the simple module M_i. But a quotient of M_i is isomorphic to M_i or to zero, and it follows that M/N is a sum of simple modules. By (1) of the previous theorem, M/N is semisimple. ■

Lemma 3.2.3. *(Schur's Lemma)*

1. *If $f \in Hom(M,N)$ where M and N are simple $R-$modules. Then f is either identically* 0 *or an isomorphism.*

2. *If M is a simple $R-$module. Then $End_R(M)$ is a division ring.*

Proof: (1) The kernel of f is either 0 or M, and the image of f is either 0 or N. If f is not the zero map, then the kernel is 0 and the image is N, so f is an isomorphism.
(2) Let $f \in End_R(M)$, f is not identically 0. By (1), f is an isomorphism, and therefore is invertible in the endomorphism ring of M. ■

Lemma 3.2.4. *Let M be a semisimple $R-$module, and let A be the endomorphism ring*

$End_R(M)$. [Note that M is an $A-$module; if $g \in A$ we take $g \bullet x = g(x), x \in M$.] If $m \in M$ and $f \in End_A(M)$. Then there exists $r \in R$ such that $f(m) = rm$.

Before proving the lemma, Let's look more carefully at $End_A(M)$. Suppose that $f \in End_A(M)$ and $x \in M$. If $g \in A$, then $f(g(x)) = g(f(x))$. Thus $End_A(M)$ consists of those abelian group endomorphisms of M that commute with every thing in $End_R(M)$. In turn, by the requirement that $f(rx) = rf(x)$, $End_R(M)$ consists of those abelian group endomorphisms of M that commute with R, more precisely with multiplication by r, for each $r \in R$.

Proof: By Theorem 3.2.1 part(3), we can express M as a direct sum $Rm \oplus N$. Now if we have a direct sum $U = V \oplus W$ and $u = v + w, v \in V, w \in W$, there is a natural projection of U on V, namely $u \to v$. In the present case, let π be the natural projection of M on Rm. Then $\pi \in A$ and $f(m) = f(\pi m) = \pi f(m) \in Rm$. The result follows. ■

To specify an $R-$module homomorphism ψ from a direct sum $V^* = \oplus_{j=1}^{n} V_j$ to a direct sum $W^* = \oplus_{i=1}^{m} W_{i,}$ we must give, for every i and j, the i^{th} component of the image of $v_j \in V_j$. Thus the homomorphism is described by a matrix $\left[\psi_{ij}\right]$, where ψ_{ij} is a homomorphism from V_j to $W_{i.}$ The i^{th} component of $\psi(v_j)$ is $\psi_{ij}(v_j)$, so the i^{th} component of $\psi(v_1 + ... + v_n)$ is $\sum_{j=1}^{n} \psi_{ij}(v_j)$. Consequently,

$$\psi(v_1 + ... + v_n) = \left[\psi_{ij}\right] \begin{bmatrix} v_1 \\ . \\ . \\ . \\ v_n \end{bmatrix}. \qquad (1)$$

This gives an abelian group isomorphism between $Hom_R(V^*, W^*)$ and $\left[Hom_R(V_j, W_i)\right]$, the collection of all m by n matrices whose ij entry is an $R-$module homomorphism from V_j to W_i. If we take $m = n$ and $V_i = W_j = V$ for all i and j, then $V^* = W^* = V^n$, the direct sum of n copies of V. Then the abelian group isomorphism given by (1) becomes

$$End_R(V^n) \simeq M_n(End_R(V)), \qquad (2)$$

the collection of all n by n matrices whose entries are $R-$ endomorphisms of V. Since composition of endomorphisms corresponds multiplication of matrices, (2) gives a ring isomorphism as well.

Theorem 3.2.5. *(Jacobson) Let M be a semisimple $R-$module, and let A be the endomorphism ring $End_R(M)$. If $f \in End_A(M)$ and $m_1,...,m_n \in M$. Then there exists $r \in R$ such that $f(m_i) = rm_i$ for all $i = 1,...,n$.*

Proof: f includes an endomorphism f_n of M^n, the direct sum of n copies of M, via

$$f_n(m_1 + \cdots + m_n) = f(m_1) + \cdots + f(m_n)$$

where $f(m_i)$ belongs to the i^{th} copy of M. The matrix that represents f_n is the scalar matrix fI, where I is an n by n identity matrix. If $B = End_R(M^n)$, then since a scalar matrix commutes with everything, $f_n \in End_B(M^n)$. If $m_1,...,m_n \in M$, then by Lemma 3.2.5, there exists $r \in R$ such that $f_n(m_1 + \cdots + m_n) = r(m_1 + \cdots + m_n)$. [Note that since M is semisimple, so is M^n]. This is equivalent to $f(m_i) = rm_i$ for all i. ■

Definition 3.2.2. For an R-module M, the set $E \subseteq M$ is a **basis** for M if:

1. E is a generating set of M ($M = \langle E \rangle$).

2. E is **linearly independent**, that is,

$$r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0$$

for $x_1,x_2,...,x_n$ distinct elements of E implies that $r_1 = r_2 = \cdots = r_n = 0$.

Corollary 3.2.6. *Let M be a faithful (see Definition 3.3.6), simple $R-$module, and* *let $D = End_R(M)$ (a division ring by the second part of Schur's Lemma). If M is a finite-dimensional vector space over D. Then $End_D(M) \simeq R$, a ring isomorphism.*

Proof: Let $\{x_1, ..., x_n\}$ be a basis for M over D. By Theorem 3.2.5, if $f \in End_D(M)$, there exists $r \in R$ such that $f(x_i) = rx_i$ for all $i = 1, ..., n$. Since the x_i form a basis, we have $f(x) = rx$ for every $x \in M$. Thus the map h from R to $End_D(M)$ given by $r \to gr =$ multiplication by r is surjective. If $rx = 0$ for all $x \in M$, then since M is faithful, we have $r = 0$ and h is injective. Since $h(rs) = g_r \circ g_s = h(r)h(s)$, h is a ring isomorphism. ■

3.3 Finitely Generated Modules over PID

We start with some definitions that will lead up to the notion of a Principal Ideal Domain *PID* .

Definition 3.3.1. A nonzero element a of a ring R is said to be a **zero-divisor** if there exists a nonzero element b in R such that $ab = 0$.

Definition 3.3.2. An **integral domain** is a unitary commutative ring, which has no zero-divisors.

Definition 3.3.3. A **principal ideal domain** (PID) is an integral domain in which every ideal is principal, i.e. generated by a single element.

Proposition 3.3.1. *If R is a P.I.D. Then every nonempty set of ideals of R has a maximal element and R is a Noetherian ring.*

Proof: Since any P.I.D. R satisfies the second condition of the Lemma 3.1.2, it follows R is Noetherian. ■

Definition 3.3.4. For any integral domain R the ***rank*** of an $R-$module M is the maximum number of $R-$linearly independent elements of M.

Proposition 3.3.2. *Let R be an integral domain and let M be a free $R-$module of rank $n < \infty$. Then any $n+1$ elements of M are $R-$linearly dependent, i.e., for any*

$y_1, y_2, \ldots, y_{n+1} \in M$ there are elements $r_1, r_2, \ldots, r_{n+1} \in R$, not all zero, such that

$$r_1y_1 + r_2y_2 + \cdots + r_{n+1}y_{n+1} = 0.$$

Proof: The quickest way of proving this is to embed R in its quotient field F (since R is an integral domain) and observe that since $M \simeq R \oplus R \oplus \ldots \oplus R$ (n times) we obtain $M \subseteq F \oplus F \oplus \ldots \oplus F$. The latter is an $n-$dimensional vector space over F so any $n+1$ elements of M are $F-$linearly dependent. By clearing the denominators of the scalars (by multiplying through by the product of all the denominators, for example), we obtain an $R-$linear dependence relation among the $n+1$ elements of M, which complete the proof. ■

Definition 3.3.5. If R is any integral domain and M is any $R-$module. Then

$$Tor(M) = \{x \in M \mid rx = 0 \text{ for some nonzero } r \in R\}.$$

is a submodule of M (called **the torsion submodule** of M) and if N is any submodule of $Tor(M)$, N is called **a torsion submodule of** M (so the torsion submodule of M is the union of all torsion submodules of M, *i.e.*, is the maximal torsion submodule of M). If $Tor(M) = 0$, the module M is said to be ***torsion free***.

Definition 3.3.6. For any submodule N of M, the ***annihilator*** *of* N is the ideal of R defined by

$$Ann(N) = \{r \in R \mid rn = 0 \text{ for all } n \in N\}.$$

If for a module M we have $Ann(M) = 0$ (the ideal zero). Then M is said to be a **faithful** module.

The following theorem plays a key role in the structure theory for finitely generated modules over PID.

Theorem 3.3.3. *Let R be a Principal Ideal Domain, let M be a free $R-$module of finite rank n and let N be a submodule of M. Then*

1. *N is free of rank m, $m \leq n$ and*

2. *there exists a basis $y_1, y_2, ..., y_n$ of M so that $a_1y_1, a_2y_2, ..., a_my_m$ is a basis of N where $a_1, a_2, ..., a_m$ are nonzero elements of R with the divisibility relations*

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

Proof: If $N = \{0\}$, the theorem is trivial. So we assume $N \neq \{0\}$. For each $\varphi \in Hom_R(M,R)$, the image $\varphi(N)$ of N is a submodule of R, i.e., an ideal in R. Since R is a *P.I.D*, this ideal must be principal, say $\varphi(N) = (a_\varphi)$, for some $a_\varphi \in R$. Let

$$\Sigma = \{(a_\varphi) \mid \varphi \in Hom_R(M,R)\}$$

be the collection of the principal ideals in R obtained in this way from the $R-$module homomorphism of M into R. Note $\Sigma \neq 0$ since $(0) \in \Sigma$. By Proposition 3.3.1, Σ has at least one maximal element i.e., there is at least one $v \in Hom_R(M,R)$ so that the principal ideal $v(N) = (a_v)$ is not properly contained in any other element of Σ. Let $a_1 = a_v$ for this maximal element and let $y \in N$ be an element mapping to the generator a_1 under the homomorphism $v : v(y) = a_1$.

We now show the element $a_1 \neq 0$. Let $x_1, x_2, ..., x_n$ be any basis of the free module M and let $\pi_i \in Hom_R(M,R)$ be the natural projection homomorphism onto the i^{th} coordinate with respect to this basis. Since $N \neq \{0\}$, there exists an i such that $\pi_i(N) \neq 0$, which in particular shows that Σ contains more than just the trivial ideal (0). Since (a_1) is a maximal element of Σ it follows that $a_1 \neq 0$.

We next shows that this element a_1 divides $\varphi(y)$ for every $\varphi \in Hom_R(M,R)$. To see this let d be a generator for the principal ideal generated by a_1 and $\varphi(y)$. Then d is a divisor of both a_1 and $\varphi(y)$ in R and $d = r_1a_1 + r_2\varphi(y)$ for some $r_1, r_2 \in R$. Consider the homomorphism $\psi = r_1v + r_2\varphi$ from M to R. Then $\psi(y) = (r_1v + r_2\varphi)(y) = r_1a_1 + r_2\varphi(y) = d$ so that $d \in \psi(N)$, hence also $(d) \subseteq \psi(N)$. But d is a divisor of a_1 so we also have $(a_1) \subseteq (d)$. Then $(a_1) \subseteq (d) \subseteq \psi(N)$ and by the maximality of (a_1) we must have the equality: $(a_1) = (d) = \psi(N)$. In particular $(a_1) = (d)$ shows that $a_1 \mid \varphi(y)$, since d divides $\varphi(y)$. If we apply this to the projection homomorphism π_i we see that a_1 divides $\pi_i(y)$ for all i. Write $\pi_i(y) = a_1b_i$ for some $b_i \in R$, $1 \leq i \leq n$ and define

$$y_1 = \sum_{i=1}^{n} b_i x_i.$$

Note that $a_1y_1 = y$. Since $a_1 = v(y) = v(a_1y_1) = a_1v(y_1)$ and a_1 is a nonzero element of the integral domain R this shows that

$$v(y_1) = 1.$$

We now verify that this element y_1 can be taken as one element in a basis for M and that a_1y_1 can be taken as one element in a basis for N, namely that we have:

(a) $M = Ry_1 \oplus Ker\ v$, and

(b) $N = Ra_1y_1 \oplus (N \cap Ker\ v)$.

To see (a) let x be an arbitrary element in M and write $x = v(x)y_1 + (x - v(x)y_1)$. Since

$$\begin{aligned} v(x - v(x)y_1) &= v(x) - v(x)v(y_1) \\ &= v(x) - v(x).1 \\ &= 0, \end{aligned}$$

we see that $x - v(x)y_1 \in Ker\ v$. This shows that x can be written as the sum of an element in Ry_1 and an element in $Ker\ v$, so $M = Ry_1 + Ker\ v$. To see that the sum is direct, suppose ry_1 is also an element in $Ker\ v$. Then $0 = v(ry_1) = rv(y_1) = r$ shows that this element is indeed 0.

For (b) observe that $v(x^{'})$ is divisible by a_1 for every $x^{'} \in N$ by the definition of a_1

as a generator for $v(N)$. if we write $v(x^{'}) = ba_1$ where $b \in R$ then the decomposition we used in (a) above is $x^{'} = v(x^{'})y_1 + (x^{'} - v(x^{'})y_1) = ba_1y_1 + (x^{'} - ba_1y_1)$ where the second summand is in the kernel of v and is an element of N. This shows that $N = Ra_1y_1 + (N \cap Ker\ v)$. The fact that the sum in (b) is direct is a special case of the directness of the sum in (a).

We now prove part (1) of the theorem by induction on the rank, m, of N. If $m = 0$, then N is a torsion module, hence $N = 0$ since a free module is torsion free, so (1) holds trivially. Assume then that $m > 0$. Since the sum in (b) above is direct we see easily that $N \cap Ker\ v$ has rank $m-1$. By induction $N \cap Ker\ v$ is then a free $R-$module of rank $m-1$. Again by the directness of the sum in (b) we see that adjoining a_1y_1 to any basis of $N \cap Ker\ v$ gives a basis of N, so N is also free (of rank m), which proves (1).

Finally, we prove (2) by induction on n, the rank of M. Applying (1) to the submodule $Ker\ v$ shows that this submodule is free and because the sum in (a) is direct, it is free of rank $n-1$. By the induction assumption applied to the module $Ker\ v$ (which plays the role of M) and its submodule $Ker\ v \cap N$ (which plays the role of N), we see that there is a basis $y_2, y_3, ..., y_n$ of $Ker\ v$ such that $a_2y_2, a_3y_3, ..., a_my_m$ is a basis of $N \cap Ker\ v$ for some elements $a_2, a_3, ..., a_m$ of R with $a_2 \mid a_3 \mid ... \mid a_m$. Since the sums (a) and (b) are direct, $y_1, y_2, ..., y_n$ is a basis of M and $a_1y_1, a_2y_2, ..., a_my_m$ is a basis of N. To complete the induction it remains to show that a_1 divides a_2. Define a homomorphism φ from M to R by defining $\varphi(y_1) = \varphi(y_2) = 1$ and $\varphi(y_i) = 0$, for all $i > 2$, on the basis for M. Then for this homomorphism φ we have $a_1 = \varphi(a_1y_1)$ so $a_1 \in \varphi(N)$ hence also $(a_1) \subseteq \varphi(N)$. By the maximality of (a_1) in Σ it follows that $(a_1) = \varphi(N)$. Since $a_2 = \varphi(a_2y_2) \in \varphi(N)$ we then have $a_2 \in (a_1)$ and thus $a_1 \mid a_2$. This completes the proof of the theorem. ■

We recall from chapter two :

An $R-$module C is a **cyclic** $R-$module if there is an element $x \in C$ such that $C = Rx$. We can then define an $R-$module homomorphism:$\pi : R \to C$ by $\pi(r) = rx$, which will be surjective by the assumption $C = Rx$.

The First Isomorphism Theorem gives an $R-$module isomorphism : $R/Ker\pi \simeq C$.

If R is a *P.I.D.*, $Ker\ \pi$ is a principal ideal, (a), so we see that the cyclic $R-$modules C are of the form $R/(a)$ where $(a) = Ann(C)$.

Theorem 3.3.4. *(Fundamental Theorem, Existence: Invariant Factor Form)*

Let R be a P.I.D. and let M be a finitely generated R−module. Then

1. *M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,*

$$M \simeq R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

   for some integer $r \geq 0$ and nonzero elements $a_1, a_2, ..., a_m$ of R which are not units in R and which satisfy the divisibility relations

$$a_1 \mid a_2 \mid \cdots \mid a_m.$$

2. *M is torsion free if and only if M is free.*

3. *In the decomposition in (1)*

$$Tor(M) \simeq R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

In particular M is a torsion module if and only if $r = 0$ and in this case the annihilator of M is the ideal (a_m).

Proof: (1) The module M can be generated by a finite set of elements by assumption so let $x_1, x_2, ..., x_n$ be a set of generators of M of minimal cardinality. Let R^n be the free $R-$module of rank n with basis $b_1, b_2, ..., b_n$ and define the homomorphism $\pi : R^n \to M$ by defining $\pi(b_i) = x_i$ for all i, which is automatically surjective since $x_1, x_2, ..., x_n$ generate M. By the First Isomorphism Theorem for modules we have $R^n/Ker\ \pi \simeq M$. Now, by Theorem 3.3.3 applied to R^n and the submodule $Ker\ \pi$ we

can choose another basis $y_1, y_2, ..., y_n$ of R^n so that $a_1y_1, a_2y_2, ..., a_my_m$ is a basis of Ker π for some elements $a_1, a_2, ..., a_m$ of R with $a_1 \mid a_2 \mid \cdots \mid a_m$. This implies $M \simeq R^n/Ker$ $\pi = (Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_my_m)$.
To identify the quotient on the right hand side we use the natural surjective $R-$module homomorphism

$$Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n \to R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$$

that maps $(\alpha_1y_{1,}\ \alpha_2y_{2,}..., \alpha_ny_n)$ to $(\alpha_1 \bmod (a_1), ..., \alpha_m \bmod (a_m), \alpha_{m+1}, ..., \alpha_n)$. The kernel of this map is clearly the set of elements where a_i divides α_i, $i = 1, 2, ..., m$, i.e., $Ra_1y_1 \oplus Ra_2y_2 \oplus ... \oplus Ra_my_m$. Hence we obtain

$$M \simeq R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

If a is a unit in R then $R/(a) = 0$, so in this direct sum we may remove any of the initial a_i which are units. This gives the decomposition in (1) (with $r = n - m$).
(2) Since $R/(a)$ is a torsion $R-$module for any nonzero element a of R, (1) immediately implies M is a torsion free module if and only if $M \simeq R^r$.
(3) This part is immediate from the definitions since the annihilator of $R/(a)$ is evidently the ideal (a). ■

We shall shortly prove the uniqueness of the decomposition in Theorem 3.3.4, namely that if we have

$$M \simeq R^{r'} \oplus R/(b_1) \oplus R/(b_2) \oplus \cdots \oplus R/(b_{m'})$$

for some integer $r' \geq 0$ and nonzero elements $b_1, b_2, ..., b_{m'}$ of R which are not units with

$$b_1 \mid b_2 \mid \cdots \mid b_{m'},$$

then $r = r^{'}, m = m^{'}$ and $(a_i) = (b_i)$ (so $a_i = b_i$ up to units) for all i. It is precisely the divisibility condition $a_1 \mid a_2 \mid \cdots \mid a_m$ which give the uniqueness.

Definition 3.3.7. The integer r in Theorem 3.3.4 is called the ***free*** *rank* or the ***Betti number*** of M and the elements $a_1, a_2, ..., a_m \in R$ are called the ***invariant factors*** *of* M.

Theorem 3.3.5. *(Fundamental Theorem, Existence: Elementary Divisor Form) Let R be a P.I.D. and let M be a finitely generated $R-$module. Then M is the direct sum of a finite number of cyclic modules whose annihilators are either* (0) *or generated by powers of primes in R, i.e.,*

$$M \simeq R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

where $r \geq 0$ is an integer and $p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_t^{\alpha_t}$ are positive powers of (not necessarily distinct) primes in R and called the ***elementary divisors*** *of M.*

Proof: Suppose M is a finitely generated torsion module over the Principal Ideal Domain R. If for the distinct primes $p_1, p_2, ..., p_n$ occurring in the decomposition in Theorem 3.3.5 we group together all the cyclic factors corresponding to the same prime p_i we see in particular that M can be written as a direct sum

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_n$$

where N_i consists of all the elements of M which are annihilated by some power of the prime p_i. This result holds also for modules over R which may not be finitely generated. ■

Theorem 3.3.6. *(The Primary Decomposition Theorem)*

Let R be a P.I.D. and let M be a nonzero torsion $R-$module (not necessarily finitely generated) with nonzero annihilator a. Suppose the factorization of a into distinct *prime powers in R is*

$$a = up_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha n}$$

and let $N_i = \{x \in M \mid p_i^{\alpha_i} x = 0\}$, $1 \leq i \leq n$. *Then* N_i *is a submodule of* M *with annihilator* $p_i^{\alpha_i}$ *and is the submodule of* M *of all elements annihilated by some power of* p_i. *We have*

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_n.$$

If M *is finitely generated. Then each* N_i *is the direct sum of finitely many cyclic modules whose annihilators are divisors of* $p_i^{\alpha_i}$. *The submodule* N_i *is called the* p_i-***primary component*** *of* M.

Proof: If M is finitely generated, we already proved. It is clear that N_i is a submodule of M with annihilator dividing $p_i^{\alpha_i}$, since $(p_i^{\alpha_i}) \subseteq$Ann(N$_i$). We can modify the proof of the Chinese Remainder Theorem to conclude $M = N_1 \oplus N_2 \oplus \cdots \oplus N_n$ and this implies $p_i^{\alpha_i} = Ann(N_i)$. ■

Notice that with this terminology the elementary divisors of finitely generated module M are just the invariant factors of the primary components of $Tor(M)$.
We now prove the uniqueness statements regarding the decompositions in the Fundamental Theorem.
Note that if M is any module over a commutative ring R and a is an element of R then $aM = \{am \mid m \in M\}$ is a submodule of M. Recall also that in a Principal Ideal Domain R the nonzero prime ideals are maximal, hence the quotient of R by a nonzero prime ideal is a field.

Lemma 3.3.7. *Let* R *be a P.I.D. and let* p *be a prime in* R. *Let* F *denote the field* $R/(p)$.

1. *Let* $M = R^r$. *Then* $M/pM \simeq F^r$.

2. *Let* $M = R/(a)$ *where* a *is a nonzero element of* R.

Then

$$M/pM \simeq \begin{cases} F, \text{ if } p \text{ divides } a \text{ in } R, \\ 0, \text{ if } p \text{ does not divide } a \text{ in } R. \end{cases}$$

3. *Let* $M = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k)$ *where each* a_i *is divisible by* p*. Then* $M/pM \simeq F^k$.

Proof: (1) There is a natural map from R^r to $(R/(p))^r$ defined by mapping $(\alpha_1,...,\alpha_r)$ to $(\alpha_1 \bmod (p),...,\alpha_r \bmod (p))$. This is clearly a surjective $R-$module homomorphism with kernel consisting of the $r-$tuples all of whose coordinates are divisible by p, i.e., pR^r, so $R^r/pR^r \simeq (R/(p))^r$, which is (1).
(2) This follows from the Isomorphism Theorems: note first that $p(R/(a))$ is the image of the ideal (p) in the quotient $R/(a)$, hence is $(p)+(a)/(a)$. The ideal $(p)+(a)$ is generated by a greatest common divisor of p and a, hence is (p) if p divides a and is $R = (1)$ otherwise. Hence $pM = (p)/(a)$ if p divides a and $R/(a) = M$ otherwise. If p divides a then $M/pM = (R/(a))/((p)/(a) \simeq R/(p)$, and if p does not divide a then $M/pM = M/M = 0$, which proves (2).
(3) This follows from (2) as in the proof of part (1) of Theorem 3.3.4. ■

Theorem 3.3.8. *(Fundamental Theorem, Uniqueness) Let R be a P.I.D.*

1. *Two finitely generated* $R-$*modules* M_1 *and* M_2 *are isomorphic if and only if they have the same free rank and the same list of invariant factors.*

2. *Two finitely generated* $R-$*modules* M_1 *and* M_2 *are isomorphic if and only if they have the same free rank and the same list of elementary divisors.*

Proof: If M_1 and M_2 have the same free rank and list of invariant factors or the same free rank and list of elementary divisors then they are clearly isomorphic. Suppose that M_1 and M_2 are isomorphic. Any isomorphism between M_1 and M_2 maps the torsion in M_1 to the torsion in M_2 so we must have $Tor(M_1) \simeq Tor(M_2)$. Then $R^{r_1} \simeq M_1/Tor(M_1) \simeq M_2/Tor(M_2) \simeq R^{r_2}$ where r_1 is the free rank of M_1 and r_2 is the free rank of M_2 . Let p be any nonzero prime in R. Then from $R^{r_1} \simeq R^{r_2}$ we obtain $R^{r_1}/pR^{r_1} \simeq R^{r_2}/pR^{r_2}$. By (1) of the previous lemma, this implies $F^{r_1} \simeq F^{r_2}$ where F is the field R/pR. Hence we have an isomorphism of an r_1-dimensional vector space over F with an r_2-dimensional vector space over F, so that $r_1 = r_2$ and M_1 and M_2 have the same free rank. ■

Chapter 4: Direct Sum Decompositions of Regular Modules

In 1936, John von Neumann [21] defined a ring R to be **regular** if for any $r \in R$ there exists $s \in R$ such that $r = rsr$. Motivated by the coordinatization of projective geometry, which was being reworked at that time in terms of lattice, von Neumann introduced regular rings as an algebraic tool for studying certain lattices.
As generalizations of the concept of Von Neumann's regular rings to the module case, there have been considered three types of modules by David Fieldhouse [17], Roger Ware [26] and Julius Zelmanowitz [30], each called regular. The Fieldhouse-regular module was defined to be a module whose submodules are pure submodules and the Ware-regular module was defined as a projective module in which every cyclic submodule is a direct summand.

4.1 Regular Modules

To introduce a regular module, Zelmanowitz followed the original elementwise definition of Von Neumann:

Definition 4.1.1. A left module M over an arbitrary ring R is called **regular module** if for each element $m \in M$ there exists a homomorphism $g \in Hom_R(M,R)$ such that

$$m = g(m)m.$$

Throughout this chapter by regular module we understand a regular module in Zelmanowitz's sense.

Remark. 5. As direct consequences of the previous definition we obtain:

1. A regular ring R is regular as left $R-$module.

2. A submodule of a regular module is also regular. In particular, every left ideal of a regular ring is regular module. This provides an ample suorce of regular modules which are not projective. Ware's regular modules are "a priori" projective modules.

3. The maximal regular ideal of an arbitrary ring is a regular module, as is any regular ideal. (An ideal of an arbitrary ring is called **regular ideal** if all its elements are regular.)

Remark. 6. Obviously, the concept of Von Neumann regular element in a ring extends the notion of invertible element, and therefore, any field is a Von Neumann regular ring. The following result is not only an equivalent definition of regular modules, but it also shows how regular modules fit into the theory of generalized inverses:

Lemma 4.1.1. *A left $R-$module M is regular if and only if for any homomorphism $f : R \to M$ there exists a homomorphism $g : M \to R$ such that $f = f \circ g \circ f$.*

Proof: We first assume M is regular module. Let $f : R \to M$ arbitrary homomorphism of $R-$modules. It follows $f(r) = rf(1) = rx_0$, for any $r \in R$, where we denoted $x_0 = f(1) \in M$. Since M is regular, it follows that there exists a homomorphism $g : M \to R$ such that $x_0 = g(x_0)x_0$. Then we have:

$$f(g(f(r))) = f(g(rx_0)) = g(rx_0)x_0 = rg(x_0)x_0 = rx_0 = f(r),$$

for any $r \in R$, showing that $f = f \circ g \circ f$.

Conversely, let m be an arbitrary element of M. We consider the homomorphism $f : R \to M$, $f(r) = rm$ for any $r \in R$. Then there exists a homomorphism $g : M \to R$ such that $f = f \circ g \circ f$. It follows $f(g(f(1))) = f(1)$, which is equivalent with $f(g(m)) = m$ and therefore $g(m)m = m$. So M is a regular module. ■

Let A, B be arbitrary sets and let $f : A \to B$, $h : B \to A$ be two maps. We say that h is a generalized inverse of f if $f = f \circ h \circ f$ and $h = h \circ f \circ h$ (see [6] for more details regarding the theory of generalized inverses). It is easy to see that the homomorphism $f : A \to B$ has a generalized inverse if and only if there exists a homomorphism $g : B \to A$ such that $f = f \circ g \circ f$. Indeed, an easy computation shows that $h = g \circ f \circ g$ is a generalized inverse of f. Thus, by the previous proposition we immediately obtain the following corollary:

Corollary 4.1.2. *A left $R-$module M is regular if and only if for any homomorphism $f : R \to M$ has a generalized inverse.*

In the paper [23], Ramamurthi and Rangaswamy introduced the notion of a split submodule (by the name of strongly pure submodule) and they obtained the first link between the notion of locally split and regular modules.

Definition 4.1.2. Let M, Q be left modules over the ring R and let $h : Q \to M$ be a homomorphism of $R-$modules. h is called **locally split** if for any $x_0 \in h(Q)$ there exists a homomorphism $q : M \to Q$ such that $h(q(x_0)) = x_0$.

Proposition 4.1.3. *Let $h : Q \to M$ be a locally split homomorphism of $R-$modules. Then for any finite number of elements $x_1, x_2, ..., x_n \in h(Q)$, there exists a homomorphism $q : M \to Q$ such that $h(q(x_i)) = x_i$, for all $i = 1, 2, ..., n$.*

Proof: We will prove by induction on n. Obviously, our assertion is true for $n = 1$, by definition of a locally split homomorphism.

Consider now $n > 1$ and we assume the proposition holds for $n-1$. Then there exists a homomorphism $q_1 : M \to Q$ such that $h(q_1(x_i)) = x_i$, for all $i = 1, 2, ..., n-1$. Since $x_n - h(q_1(x_n)) \in h(Q)$, there exists a homomorphism $q_2 : M \to Q$ such that

$$h(q_2(x_n - h(q_1(x_n)))) = x_n - h(q_1(x_n)).$$

We define

$$q : M \to Q, q = q_1 + q_2 - q_2 \circ h \circ q_1.$$

Then, on one hand

$$\begin{aligned} h(q(x_n)) &= h(q_1(x_n)) + h(q_2(x_n)) - h(q_2(h(q_1(x_n)))) \\ &= h(q_1(x_n)) + h(q_2(x_n - h(q_1(x_n)))) \\ &= h(q_1(x_n)) + x_n - h(q_1(x_n)) = x_n, \end{aligned}$$

and on the other hand

$$\begin{aligned} h(q(x_i)) &= h(q_1(x_i)) + h(q_2(x_i)) - h(q_2(h(q_1(x_i)))) \\ &= x_i + h(q_2(x_i)) - h(q_2(x_i)) = x_i, \end{aligned}$$

for all $i = 1, 2, ..., n-1$. Hence q is the requested homomorphism. ■

Definition 4.1.3. A submodule N of a module M is called **split** in M if the inclusion homomorphism $i : N \hookrightarrow M$ is locally split, i.e. for any $x_0 \in N$ there exists a homomorphism $j : M \to N$ such that $j(x_0) = x_0$.

Proposition 4.1.4. *Let $h : Q \to M$ be a homomorphism of $R-$modules and let $\bar{h} : Q \to h(Q)$ be the homomorphism satisfying $\bar{h}(x) = h(x)$, for any $x \in Q$. Then h is locally split if and only if $\bar{h}$ is locally split and $h(Q)$ is a split submodule in M.*

Proof: We first assume that h is locally split. Consider x_0 an arbitrary element in $h(Q)$. Then there exists a homomorphism $q : M \to Q$ such that $h(q(x_0)) = x_0$. This yields that the homomorphism $s = \bar{h} \circ q : M \to h(Q)$ satisfies $s(x_0) = x_0$, and therefore $h(Q)$ is a split submodule in M. Moreover, if we denote by $\bar{q} : h(Q) \to Q$ the restriction of q to $h(Q)$, then we obtain $\bar{h}(\bar{q}(x_0)) = h(q(x_0)) = x_0$, showing that $\bar{h}$ is locally split.

Conversely, we now assume that $\bar{h}$ is locally split and $h(Q)$ is a split submodule in M. Let x_0 an arbitrary element in $h(Q)$. Then there exist homomorphisms $\bar{q} : h(Q) \to Q$ and $j : M \to h(Q)$ such that $\bar{h}(\bar{q}(x_0)) = x_0$ and $j(x_0) = x_0$. If we denote $q = \bar{q} \circ j : M \to Q$, it follows

$$h(q(x_0)) = \bar{h}(q(x_0)) = \bar{h}(\bar{q}(j(x_0))) = \bar{h}(\bar{q}(x_0)) = x_0,$$

showing that h is locally split. ■

The next theorem shows the link between the notion of locally split and regular modules.

Theorem 4.1.5. *Let M be a left $R-$module. Then the following assertions are equivalent:*

1. *M is a regular module.*
2. *for any module Q, every homomorphism $h : Q \to M$ is locally split.*
3. *every homomorphism $f : R \to M$ is locally split.*

Proof: $(1) \Rightarrow (2)$ Let x_0 be an arbitrary element of $h(Q)$. Then there exists $\alpha_0 \in Q$ such that $h(\alpha_0) = x_0$. Since M is a regular module, then there exists a homomorphism $g : M \to R$ such that $g(x_0)x_0 = x_0$. Consider $q : M \to Q$, $q(m) = g(m)\alpha_0$, for any $m \in M$. Obviously q is a homomorphism of modules and

$$h(q(x_0)) = h(g(x_0)\alpha_0) = g(x_0)h(\alpha_0) = g(x_0)x_0 = x_0,$$

which shows that h is locally split.
$(2) \Rightarrow (3)$ Clear.
$(3) \Rightarrow (1)$ Let x_0 be an arbitrary element of M and consider $f : R \to M$ the homomorphism defined by $f(r) = rx_0$. Since f is locally split, then there exists a homomorphism $g : M \to R$ such that $f(g(x_0)) = x_0$. It follows

$$x_0 = f(g(x_0)) = g(x_0)f(1) = g(x_0)x_0$$

and thus M is a regular module. ■

As a direct consequence of the implication $(1) \Rightarrow (2)$, and of Definition 4.1.3, we have the following

Corollary 4.1.6. *If M is a regular module. Then any submodule N of M is split in M.*

Theorem 4.1.7. *If a left $R-$module M is regular module. Then every finitely generated submodule of M is a direct summand of M.*

Proof: Let N be a finitely generated submodule of M. Then there exist $x_1, x_2, ..., x_n \in N$ such that

$$N = Rx_1 + Rx_2 + \cdots + Rx_n.$$

By the Corollary 4.1.6, since M is a regular module, then N is split. Therefore, by using Proposition 4.1.3 for the inclusion map $i : N \hookrightarrow M$, we can find a homomorphism $s : M \to N$ such that $s(x_i) = x_i$, for $i \in \{1, ..., n\}$. Since N is generated as $R-$module by the elements $x_1, x_2, ..., x_n$, it follows $s(x) = x$, for all $x \in N$. This implies that N is a direct summand of M. ■

4.2 Isomorphic Refinement Theorem for Regular Modules

Proposition 4.2.1. *Let $M_1, M_2, ..., M_n$ be regular modules over an arbitrary ring R and let N be a finitely generated submodule of $M_1 \oplus M_2 \oplus \cdots \oplus M_n$. Then, for every $i \in \{1, ..., n\}$, there exist decompositions $M_i = M_{i1} \oplus M_{i2}$ such that*

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n = N \oplus M_{12} \oplus M_{22} \oplus \cdots \oplus M_{n2}$$

and

$$N \simeq M_{11} \oplus M_{21} \oplus \cdots \oplus M_{n1}.$$

Proof: We proceed by induction on n.
For $n = 1$, N is a finitely generated submodule of M_1, which is a regular module. By Theorem 4.1.7 it follows N is a direct summand of M_1. Threfore there exists M_{12} such

that $M_1 = N \oplus M_{12}$ and we denote $M_{11} = N$.

Consider $n > 1$ and we assume the proposition is true for $n-1$. We consider the canonical projections

$$\pi_1 : M_1 \oplus M_2 \oplus \cdots \oplus M_n \to M_1$$

and,

$$\pi_2 : M_1 \oplus M_2 \oplus \cdots \oplus M_n \to M_2 \oplus \cdots \oplus M_n$$

Since $\pi_2(N)$ is a submodule of $M_2 \oplus \cdots \oplus M_n$, it follows $\pi_2(N)$ is a regular module. But $\pi_2(N)$ is also finitely generated module, therefore $\pi_2(N)$ is projective module (according [30, Corollary 1.7]). Thus the following short exact sequence

$$0 \longrightarrow N \cap M_1 \longrightarrow N \longrightarrow \pi_2(N) \longrightarrow 0$$

splits, so $N \simeq (N \cap M_1) \oplus \pi_2(N)$. If we denote $M_{11} = N \cap M_1$, then M_{11} is a finitely generated submodule of the regular module M_1, hence it is a direct summand of M_1: $M_1 = M_{11} \oplus M_{12}$, for a submodule M_{12} of M_1.

Since $\pi_2(N)$ is a finitely generated submodule of $M_2 \oplus \cdots \oplus M_n$, by the induction hypothesis, for every $i \in \{2, ..., n\}$ we obtain the following decompositions $M_i = M_{i1} \oplus M_{i2}$ such that

$$M_2 \oplus \cdots \oplus M_n = \pi_2(N) \oplus M_{22} \oplus \cdots \oplus M_{n2}$$

and

$$\pi_2(N) \simeq M_{21} \oplus \cdots \oplus M_{n1}.$$

We remark that

$$M_{11} \oplus M_{21} \oplus \cdots \oplus M_{n1} \simeq (N \cap M_1) \oplus \pi_2(N) \simeq N.$$

But $\pi_2(N) = (Id - \pi_1)(N)$ is a submodule of $N + M_1$, hence $M_2 \oplus \cdots \oplus M_n = \pi_2(N) \oplus$

$M_{22} \oplus \cdots \oplus M_{n2}$ is a submodule of $(N+M_1)+(M_{22} \oplus \cdots \oplus M_{n2})$, and hence

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n = (N+M_1)+(M_{22} \oplus \cdots \oplus M_{n2}). \tag{4.1}$$

Since $M_1 = M_{11} \oplus M_{12}$ is a submodule of $N+M_{12}$, relation (4.1) yields

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n = N+(M_{12} \oplus M_{22} \oplus \cdots \oplus M_{n2}).$$

We denote $Q = N \cap (M_{12} \oplus M_{22} \oplus \cdots \oplus M_{n2})$ and we want to prove $Q = 0$. Remark that $\pi_2(Q) \subseteq \pi_2(N) \cap \pi_2(M_{12} \oplus M_{22} \oplus \cdots \oplus M_{n2}) = \pi_2(N) \cap (M_{12} \oplus M_{22} \oplus \cdots \oplus M_{n2}) = 0$. Therefore $Q \subseteq Ker\pi_2 = M_1$, so

$$Q \subseteq N \cap M_1 = M_{11}. \tag{4.2}$$

On the other hand, since $Q \subseteq M_1$, we obtain

$$Q = \pi_1(Q) \subseteq \pi_1(M_{12} \oplus M_{22} \oplus \cdots \oplus M_{n2}) = M_{12}. \tag{4.3}$$

By (4.2) and (4.3) it follows $Q \subseteq M_{11} \cap M_{12} = 0$, so

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n = N \oplus M_{12} \oplus M_{22} \oplus \cdots \oplus M_{n2}$$

and the induction is now complete. ■

We are now in the position to prove the main result of this section, namely the isomorphic refinement theorem for finitely generated regular modules:

Theorem 4.2.2. *Let $M_1, M_2, ..., M_n, N_1, N_2, ..., N_k$ be finitely generated regular modules* *over an arbitrary ring R such that*

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n \simeq N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

Then for every $i \in \{1,...,n\}$ there exist decompositions

$$M_i = M_{i1} \oplus \cdots \oplus M_{ik}$$

such that

$$M_{1j} \oplus \cdots \oplus M_{nj} \simeq N_j$$

for $j \in \{1,...,k\}$.

Proof: By induction on k.

If $k = 1$, it is enough to consider $M_{i1} = M_i$, for all $i \in \{1,...,n\}$.

For $k = 2$ we have the following isomorphism $M_1 \oplus M_2 \oplus \cdots \oplus M_n \simeq N_1 \oplus N_2$. Then there exist the modules $N_1' \simeq N_1$ and $N_2' \simeq N_2$ such that $M_1 \oplus \cdots \oplus M_n = N_1' \oplus N_2'$. For every $i \in \{1,...,n\}$, by Proposition 4.2.1, there exists a direct sum decomposition $M_i = M_{i1} \oplus M_{i2}$ such that

$$M_1 \oplus \cdots \oplus M_n = N_1' \oplus M_{12} \oplus \cdots \oplus M_{n2}$$

and

$$M_{11} \oplus \cdots \oplus M_{n1} \simeq N_1' \simeq N_1.$$

We now assume the theorem holds for $k-1$, where k is an arbitrary integer > 2. By the case $k = 2$, for each $i \in \{1,...,n\}$, there exists a direct sum decomposition $M_i = M_{i1} \oplus Q_i$ such that

$$M_{11} \oplus \cdots \oplus M_{n1} \simeq N_1$$

and

$$Q_1 \oplus \cdots \oplus Q_n \simeq N_2 \oplus \cdots \oplus N_k.$$

Using the inductive hypothesis for $k-1$, there exist decompositions $Q_i = M_{i2} \oplus \cdots \oplus M_{ik}$, for every $i \in \{1,...,n\}$, such that

$$M_{1j} \oplus \cdots \oplus M_{nj} \simeq N_j,$$

for each $j \in \{2,...,k\}$.

To complete the proof, we have to remark that

$$M_i = M_{i1} \oplus Q_i = M_{i1} \oplus M_{i2} \oplus \cdots \oplus M_{ik},$$

for every $i \in \{1,...,n\}$. ■

Notation: If M and N are two $R-$modules such that M is isomorphic with a submodule of N (i.e there exists a submodule M' of N such that $M \simeq M'$). Then we denote: $M \lesssim N$.

Corollary 4.2.3. *Let $M_1, M_2, ..., M_n, N_1, N_2, ..., N_k$ be finitely generated regular modules over an arbitrary ring R such that*

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n \lesssim N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

1. *Then for every $i \in \{1,...,n\}$ there exist decompositions $M_i = M_{i1} \oplus \cdots \oplus M_{ik}$ such that*

   $$M_{1j} \oplus \cdots \oplus M_{nj} \lesssim N_j$$

   for $j \in \{1,...,k\}$.

2. *Then for every $j \in \{1,...,k\}$ there exist decompositions $N_j = N_{j1} \oplus \cdots \oplus N_{jn}$ such*

that

$$M_i \simeq N_{1i} \oplus \cdots \oplus N_{ki}$$

for $i \in \{1, ..., n-1\}$, *and*

$$M_n \lesssim N_{1n} \oplus \cdots \oplus N_{kn}.$$

Proof: By [30, Theorem 2.8], the set of all regular modules of an arbitrary ring is closed under finite direct sums, so $N_1 \oplus \cdots \oplus N_k$ is a regular module. On the other hand, since $M_1, ..., M_n$ are finitely generated modules, it follows that $M_1 \oplus \cdots \oplus M_n$ is a finitely generated module. Hence $M_1 \oplus \cdots \oplus M_n$ is isomorphic with a finitely generated submodule of the regular module $N_1 \oplus \cdots \oplus_k$. Therefore, according Theorem 4.1.7, $M_1 \oplus \cdots \oplus M_n$ is isomorphic with a direct summand of $N_1 \oplus \cdots \oplus N_k$:

$$M_1 \oplus \cdots \oplus M_n \oplus M_{n+1} \simeq N_1 \oplus \cdots \oplus N_k,$$

for some finitely generated module M_{n+1}.
(1) By Theorem 4.2.2, for every $i \in \{1, ..., n+1\}$ there exists decompositions $M_i = M_{i1} \oplus \cdots \oplus M_{ik}$ such that

$$M_{1j} \oplus \cdots \oplus M_{n+1,j} \simeq N_j$$

for $j \in \{1, ..., k\}$, and thus

$$M_{1j} \oplus \cdots \oplus M_{nj} \lesssim N_j$$

for $j \in \{1, ..., k\}$. ■

4.3 The Exchange Property for Regular Modules

In paper [8], Crawley and Jonsson introduced the concept of exchange property:

Definition 4.3.1. A module M has the **(finite) exchange property** if for any (finite) index set I and any two direct sum decompositions

$$L = M' \oplus N = \oplus_{i \in I} N_i,$$

with $M' \simeq M$, there exist submodules $N_i' \subseteq N_i$ such that

$$L = M' \oplus \left(\oplus_{i \in I} N_i' \right).$$

They used this concept to prove theorems on isomorphic refinement of direct decompositions for modules. In fact, Crawley and Jonsson's results were proved for a large class of algebraic structures, namely for algebras in the sense of Jonsson-Tarski. The systematic study of modules with the finite exchange property was initiated by Warfield in papers [27] and [28]. Using the exchange property, Warfield gave a strengthened form of the Krull-Schmidt theorem (see [27, Theorem 1]).

Remark. 7. Definition 4.3.1 is equivalent to the following:

The module M has the exchange property if and only if for any direct sum $\oplus_{i \in I} N_i$ which contains M as a direct summand, then there exist submodules N_i' of N_i, for each $i \in I$, such that

$$\oplus_{i \in I} N_i = M \oplus \left(\oplus_{i \in I} N_i' \right).$$

Remark. 8. By the previous remark it follows that, if M is a finitely generated module, then the finite exchange property is equivalent to the exchange property for any cardinal number.

Nicholson [22], introduced the class of suitable rings and he also gave the connection between the finite exchange property of a module and the "suitability" of its endomorphisms ring.

Definition 4.3.2. (see [22, Proposition 1.1] and [22, Definition 1.2]) A ring R is called

suitable if each element $x \in R$ satisfies the following equivalent conditions:

1. There exists $e^2 = e \in R$ with $e - x \in R\left(x - x^2\right)$.

2. There exists $e^2 = e \in Rx$ and $c \in R$ such that $(1-e) - c(1-x) \in J(R)$.

3. There exists $e^2 = e \in Rx$ such that $R = Re + R(1-x)$.

4. There exists $e^2 = e \in Rx$ such that $1 - e \in R(1-x)$.

5. If $x, y \in R$, with $x + y = 1$, then there exist $a, b \in R$ such that $ax + by = 1$ and ax, by are idempotents.

Theorem 4.3.1. *([22, Theorem 2.1]) If R is a ring and M is a left $R-$modules. Then the following conditions are equivalent:*

1. *M has the finite exchange property;*

2. *the endomorphism ring $End(M)$ is suitable.*

To prove that any finitely generated regular module has the exchange property, we will use the following notions:

Definition 4.3.3. Let R be a ring and let X be an additive subgroup of R. We say the idempotents can be **lifted** modulo X if, given $x \in R$ with $x - x^2 \in X$, there exists an idempotent element $e \in R$ such that $e - x \in X$.

Definition 4.3.4. For a ring R, the **Jacobson radical** of R is the intersection of the annihilators of all simple left $R-$modules and it is denoted $J(R)$:

$$J(R) = \bigcap_{M \text{ simple module}} Ann(M)$$

Definition 4.3.5. We call a ring R **semiregular** if $R/J(R)$ is von Neumann regular and idempotents can be lifted modulo $J(R)$, where $J(R)$ is the Jacobson radical of the ring

R.

Theorem 4.3.2. *If M is a finitely generated regular module. Then M has the exchange property.*

Proof: If M is a finitely generated regular module, then the endomorphism ring $End(M)$ is von Neumann regular ring (see [30, Corollary 4.2]). Hence $End(M)$ is a semiregular ring. By [22, Proposition 1.6], it follows $End(M)$ is a suitable ring. Using now Theorem 4.3.1, we obtain that M has the exchange property. ■

Appendix

Zorn's Lemma

Zorn's lemma is a result in set theory that appears in proofs of some non-constructive existence theorems throughout mathematics.

Definition .0.6. A ***partial ordering*** *on a* (*nonempty*) *set* S is a binary relation on S, denoted $\leq$, which satisfies the following properties:

1. for all $s \in S$, $s \leq s$,

2. if $s \leq s^{'}$ and $s^{'} \leq s$ then $s = s'$.

3. if $s \leq s^{'}$ and $s^{'} \leq s^{''}$ then $s \leq s^{''}$.

When we fix a partial ordering $\leq$ on S, we refer to S (or, more precisely, to the pair $(S, \leq)$) as **a partially ordered set**. It is important to notice that we do not assume all pairs of elements in S are comparable under $\leq$: for some s and $s^{'}$ we may have neither $s \leq s^{'}$ nor $s^{'} \leq s$. If all pairs of elements can be compared (that is, for all s and $s^{'}$ in S either $s \leq s^{'}$ or $s^{'} \leq s$) then we say S is **totally ordered** with respect to $\leq$.

Example .0.1. The usual ordering relation on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or in $\mathbb{Z}^+$ is a partial ordering of these sets. In fact it is a total ordering on either set. This ordering on $\mathbb{Z}^+$ is the basis for proofs by induction.

Example .0.2. On $\mathbb{Z}^+$, declare $a \leq b$ if $a \mid b$. This partial ordering on $\mathbb{Z}^+$ is different from the one in the previous example and is called ordering by *divisibility.* It is one of the central relations in number theory.

Unlike the ordering on $\mathbb{Z}^+$ in the previous example, $\mathbb{Z}^+$ is not totally ordered by divisibility: most pairs of integers are not comparable under the divisibility relation. For instance, 3 doesn't divide 5 and 5 doesn't divide 3. The subset $\{1, 2, 4, 8, 16, ...\}$ of powers of 2 is totally ordered under divisibility.

Example .0.3. Let S be the set of all subgroups of a given group G. For $H,K \in S$ (that is, H and K are subgroups of G), declare $H \leq K$ if H is a subset of K. This is a partial ordering, called ordering by *inclusion.* It is not a total ordering: for most subgroups H and K neither $H \subset K$ nor $K \subset H$.

In these examples, only the first example is totally ordered. This is typical: most naturally occurring partial orderings are not total orderings. However (and this is important) a partially ordered set can have many subsets that are totally ordered.

Definition .0.7. An ***upper bound*** on a subset T of a partially ordered set S is an $s \in S$ such that $t \leq s$ for all $t \in T$. When we say T has an upper bound in S, we do not assume the upper bound is in T itself; it is just in S.

Example .0.4. In $\mathbb{R}$ with its natural ordering, the subset $\mathbb{Z}$ has no upper bound while the subset of negative real numbers has the upper bound 0 (or any positive real). No upper bound on the negative real numbers is a negative real number.

Example .0.5. In the proper subgroups of $\mathbb{Z}$ ordered by inclusion, an upper bound on the set $\{4\mathbb{Z}, 6\mathbb{Z}, 8\mathbb{Z}\}$ is $2\mathbb{Z}$ since $4\mathbb{Z}, 6\mathbb{Z}$ and $8\mathbb{Z}$ all consist entirely of even numbers (Note $4\mathbb{Z} \subset 2\mathbb{Z}$, not $2\mathbb{Z} \subset 4\mathbb{Z}$.)

Definition .0.8. A **maximal element** m of partially ordered set S is an element that is not below any element to which it is comparable: for all $s \in S$ to which m is comparable, $s \leq m$.

Equivalently, m is **maximal** when the only $s \in S$ satisfying $m \leq s$ is $s = m$. This does not mean $s \leq m$ for all s in S since we don't insist that maximal elements are actually comparable to every element of S. A partially ordered set could have many maximal elements.

Example .0.6. If we partially order the proper subgroups of $\mathbb{Z}$ by inclusion then the maximal elements are $p\mathbb{Z}$ for prime numbers p.

Theorem .0.3. (*Zorn's lemma*). *Let S be a partially ordered set. If every totally ordered subset of S has an upper bound, then S contains a maximal element.*

Bibliography

[1] W.A. Adkins, S.H. Weintraub, Algebra - An approach via module theory, Springer, 1992

[2] A. Amini, B. Amini, A. Facchini, Weak Krull-Schmidt for infinite direct sum of cyclically presented modules over local rings, Rend. Semin.Math. Univ.Padova, 122: 39-54, 2009

[3] F.W. Anderson, K.R. Fuller, Rings and categories of modules, 2nd edition, Springer, 1992

[4] G. Azumaya, Corrections and Supplementaries to my paper concerning Krull-Remak-Schmidt's theorem, Nagoya Math. J., 1: 117-127, 1950

[5] G. Azumaya, Some Characterizations Of Regular Modules, Publications Matematiques, Vol. 34 (1990), 241-248

[6] A. Ben-Israel; T.N.E. Greville. Generalized inverses. Theory and applications. Second edition.CMS Books in Mathematics, 15. Springer-Verlag, New York, 2003

[7] A.J. Berrick, M.E. Keating. An Introduction to Rings and Modules with K-theory in view, Cambridge University Press, 2000

[8] P. Crawley, B. Jonsson, Refinements for infinite direct decompositions of algebraic systems, *Pacific J. Math.* 14:797-855, (1964)

[9] S. Dăscălescu, C. Năstăsescu, A. Tudorache and L. Dăuş, Relative regular object in categories, Applied Categorical Structures 14 (5-6), 2006, 567-577

[10] L. Dăuş, Relative regular modules. Applications to von Neumann regular rings, Applied Categorical Structures, 19(6), 2011, 859-863

[11] L. Dăuş, W. Abuziadeh, An isomorphic refinement theorem for regular modules, submitted (paper presented with the occasion of the International Conference on Recent Advances in Pure and Applied Mathematics, 3-6 June 2015, Istanbul, Turkey)

[12] L. Dăuş, M. Salim. From regular modules to von Neumann regular rings via coordinization. Rom.J.Math. Comput. Sci. 4(2014), no. 2, 125-130

[13] D.S. Dummit, R.M Foote, Abstract Algebra, 3rd edition, Wiley, 2004

[14] S. Ecevit, A. Facchini and M.T.Ko,san, Kernels of homomorphisms between indecomposable injective modules, Glasgow Math. J., 52(A): 69-82, 2010.

[15] A. Facchini, D. Herbera, L.S. Levy, and P. Va'mos. Krull-Schmidt fails for artinian modules. Proc. Amer. Math. Soc., 123(12):3587-3592, 1995

[16] C. Faith, Algebra.Rings, modules and categories, vol. I, Springer, 1973

[17] D.J. Fieldhouse, Pure theories, Math. Ann 184 (1969), 1-18.

[18] G. Frobenius and L. Stickelbeger, Uber gruppen von vertaushbaren elements, J. Reine Angew. Math., 86: 217-262, 1879

[19] G. Kemper, A Course in Commutative Algebra, Springer, 2011

[20] W. Krull, Uber verallgemeinerte endiche abelsche gruppen, Math.Z.,3: 161-196, 1925

[21] J. von Neumann, On regular rings, Proc.Natl. Acad. Sci. U.S.A., 22(12), 1936, 707-713

[22] W.K. Nicholson, Lifting idempotents and exchange rings, *Trans. Amer. Math. Soc.* 239:269-278, (1977)

[23] V.S Ramamurthi And K.M. Rangaswamy, On finitely injective modules, J. Austral Math. Soc. 16 (1973), 239-248.

[24] R. Remak, Uber die zerlegung der endlichen gruppen in direkte unzer leghare faktoren, J. Reine Angew. Math., 139: 293-308, 1911

[25] O. Schmidt Uber unendiche gruppen mit endicher kette, Math.Z., 29: 34-41, 1928

[26] R. Ware, Endomorphism rings of projective modules, Trans. Amer. Math. Soc. 155 (1971), 233-259.

[27] Warfield, R.B. (1969). A Krull-Schmidt theorem for infinite sums of modules, *Proc. Amer. Math. Soc.* 22:460-465

[28] Warfield, R.B. (1972). Exchange rings and decompositions of modules, *Math. Ann.* 199:31-36

[29] J.H.M. Wedderburn. On the direct product in the theory of finite groups, Ann. Math., 10: 173-176, 1909

[30] J. Zelmanowitz, Regular modules, Trans. Amer. Math. Soc. 163 (1972)