6-2017

SIMPLE AND SEMI-SIMPLE ARTINIAN RINGS

Ulyses Velasco
California State University - San Bernardino

Simple and Semi-Simple Artinian Rings

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Ulyses Velasco

June 2017

Simple and Semi-Simple Artinian Rings

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

by

Ulyses Velasco

June 2017

Approved by:

Dr. Gary Griffing, Committee Chair

Date

Dr. J. Paul Vicknair, Committee Member

Dr. Shawn McMurran, Committee Member

Dr. Charles Stanton, Chair,
Department of Mathematics

Dr. Corey Dunn
Graduate Coordinator,
Department of Mathematics

Abstract

The main purpose of this paper is to examine the road towards the structure of simple and semi-simple Artinian rings. We refer to these structure theorems as the Wedderburn-Artin theorems. On this journey, we will discuss R-modules, the Jacobson radical, Artinian rings, nilpotency, idempotency, and more. Once we reach our destination, we will examine some implications of these theorems. As a fair warning, no ring will be assumed to be commutative, or to have unity. On that note, the reader should be familiar with the basic findings from Group Theory and Ring Theory.

Acknowledgements

Primarily, I would like to give a special thanks to Dr. Gary Griffing for taking me on as his student just before he decided to (partially) retire. He did not have to, and he could have enjoyed his newly found free time greatly. Instead, he allowed me to have him as my advisor for my thesis project. Without him, this paper would not have been possible. Next, I would like to thank Dr. Shawn McMurran and Dr. J. Paul Vicknair for being part of my committee and for being great professors. On that note, I would like to thank every professor I had a chance to study under. Every single class I enrolled as an undergraduate and as a graduate has shaped me into the mathematician I am today. Last, but not least, I want to thank my parents for always encouraging me to continue with my education and supporting me on this difficult road. I could not have asked for better parents.

Table of Contents

Chapter 1

Introduction

We begin our path by introducing the notion of an R-module. An R-module "M" is an abelian group under addition that is susceptible to the influence of a ring R. We will go into full detail about R-modules in the next chapter. To give an idea, the most popular types of examples for R-modules are vector spaces over fields. If V is a vector space over a field F, then V is an F-module. In fact, one could argue that the idea of R-modules is an attempt to generalize the idea of vector spaces. Another approach to R-modules is that they are the generalization of abelian groups, seeing how every abelian group under addition is a $\mathbb{Z}$-module.

Naturally, if the elements of R can influence the elements of M, it begs the question: Are all rings efficient scalars for their modules? Since such a question is immensely broad, we put our attention into a ring R and its "simple" R-modules. In short, a simple R-module is an R-module that does not contain any other non-zero R-modules. With the constraint of simple R-modules, the answer to our previous question comes in the form of the Jacobson radical. We will see that the Jacobson radical is an ideal of R, and in the case for which the Jacobson radical happens to be the trivial ideal, we say the ring R is semi-simple. Thereafter, we eventually come upon a nice way to describe the Jacobson radical of a ring.

Once the Jacobson radical is demystified, we make our move toward the Wedderburn-Artin theorems. First, we explore the consequences of our findings with the added assumption that our rings are Artinian, which may be thought of as an abstraction of finite-dimensionality for vector spaces. Inevitably, we come across the idea of nilpotence and idempotence, which prove to be of vast help. Once we have the necessary theorems, we discover the structure of semi-simple Artinian rings. In a turn of events, it becomes apparent that the structure of semi-simple Artinian rings depends on the structure of simple Artinian rings. Accordingly, we embark on our last mission: to find the structure of simple Artinian rings.

After everything is said and done, we will explore concrete examples on how some semi-simple Artinian rings break down. Maschke's Theorem reveals how one can easily create semi-simple Artinian rings. Once we get our hands on a semi-simple Artinian ring, we will decompose it into a direct sum of simple Artinian rings.

This work is inspired primarily by Herstein's *Noncommutative Rings*, [Her]. Formal definitions are taken mostly from Hungerford's *Algebra*, [Hun], as a strong foundation for Ring Theory. Nevertheless, this paper is written so that no extra knowledge is necessary to understand this work other than the bare bones of abstract algebra. Although we shall consider every theorem in the noncommutative, nonunital way, this paper has been written with examples that are welcoming to those of us who are used to having elements commute and multiplicative identities!

1.1 Preliminaries

Before we begin, we should become accustomed with a few results from Ring Theory. We assume the reader has some previous knowledge on both Ring Theory and Group Theory. Still, we will quickly review a few theorems and lemmas that will frequently be called upon throughout this paper. Refer to [Hun] if needed for a more in depth review of Group Theory and Ring Theory.

A common theme throughout many of the proofs in this paper will be dealing with the sets $A + B$ and AB, which we define as follows:

Definition 1.1.1. For any nonempty subsets A, B of a ring R, $A + B = \{a + b \,|\, a \in A,\, b \in B\}$ and $AB = \{\sum_{i,j} a_i b_j \,|\, a_i \in A,\, b_j \in B\}$.

We define AB as sums of products in order to guarantee AB will be closed under addition. On that note, we can state our first lemma.

Lemma 1.1.1. *If A, B are (left, right, two-sided) ideals of R, then both $A + B$ and AB are (left, right, two-sided) ideals of R.*

Proof. We prove the case for left ideals A, B of R. First, since $0 \in A$ and $0 \in B$, then $0 + 0 = 0 \in A + B$ and $0 \cdot 0 = 0 \in AB$. Second, Let $x \in A + B$ with $x = a + b$ for some $a \in A$ and $b \in B$, and let $y \in AB$ with $y = \sum_{i,j} a_i b_j$ for some $a_i \in A$ and $b_j \in B$. Since a, $a_i \in A$ for all i and $b \in B$, where A and B are left ideals, then we know $-a$, $-a_i \in A$ and $-b \in B$ for all i. Hence, $(-a) + (-b) = -(a + b) = -x \in A + B$ and $\sum_{i,j}(-a_i)b_j = \sum_{i,j} -(a_i b_j) = -(\sum_{i,j} a_i b_j) = -y \in AB$. Third, suppose x, $x' \in A + B$ with $x = a + b$ and $x' = a' + b'$ for some a, $a' \in A$ and b, $b' \in B$, and suppose y, $y' \in AB$ with $y = \sum_{i,j} a_i b_j$ and $y' = \sum_{i,j} a_i' b_j$ for some a_i, $a_i' \in A$ and all $b_j \in B$. Then, $x + x' = (a + b) + (a' + b') = (a + a') + (b + b') \in A + B$ and $y + y' = \sum_{i,j} a_i b_j + \sum_{i,j} a_i' b_j = \sum_{i,j}(a_i + a_i')b_j \in AB$. Finally, let $r \in R$, $x \in A + B$ with $x = a + b$ for some $a \in A$ and $b \in B$, and $y \in AB$ with $y = \sum_{i,j} a_i b_j$ for some $a_i \in A$ and some $b_j \in B$. Then, $rx = r(a + b) = ra + rb \in A + B$ and $ry = r(\sum_{i,j} a_i b_j) = \sum_{i,j}(ra_i)b_j \in AB$ on account of A, B being ideals of R. Hence, both $A + B$ and AB are left ideals of R. □

Instinctively, we can define sums and products of ideals with more than two summands using the appropriate analogues and still have the previous result hold. Specifically, $A_1 + \cdots + A_n = \{a_1 + \cdots + a_n \,|\, a_i \in A_i,\ i = 1, \ldots, n\}$ and $A_1 \cdots A_n = \{\sum_j a_{1j} \cdots a_{nj} \,|\, a_{ij} \in A_i,\ i = 1, \ldots, n\}$ will be ideals of R provided $A_1, \ldots, A_n$ are ideals of R. Consequently, if A is an ideal of R, then the set $A^n = \{\sum a_1 \cdots a_n \,|\, a_i \in A\}$ $(= A \cdots A$ n-fold$)$ is an ideal of R.

Since we have established some facts about ideals, we now draw our focus on some facts about ring homomorphisms.

Canonical Projection Theorem. *If $f : R \to S$ is a homomorphism of rings, then the kernel of f is an ideal in R. Conversely, if I is an ideal in R, then the map $\pi : R \to R/I$ given by $r \mapsto r + I$ is a surjective homomorphism of rings with kernel I.*

Proof. Suppose R, S are rings and $f : R \to S$ is a homomorphism of rings. Consider $\operatorname{Ker} f = \{r \in R \,|\, f(r) = 0_S\}$. Of course, f being a homomorphism of rings implies $f(0_R) = 0_S$, so $0_R \in \operatorname{Ker} f$. Next, if $a \in \operatorname{Ker} f$, then $0_S = f(0_R) = f(a + -(a)) = f(a) + f(-a) = 0_S + f(-a) = f(-a)$, so $-a \in \operatorname{Ker} f$. Now, suppose a, $b \in \operatorname{Ker} f$, then $f(a + b) = f(a) + f(b) = 0_S + 0_S = 0_S$ and $f(ab) = f(a)f(b) = (0_S)^2 = 0_S$, so both ab and $a + b$ belong to $\operatorname{Ker} f$. Lastly, let $r \in R$ and $i \in \operatorname{Ker} f$, then $f(ri) = f(r)f(i) = f(r)0_S = 0_S = 0_S f(r) = f(i)f(r) = f(ir)$, so both ri and ir belong to $\operatorname{Ker} f$ for any r in R, so $\operatorname{Ker} f$ is an ideal of R.

Now, suppose I is an ideal of R and let the map $\pi : R \to R/I$ be given by $r \mapsto r + I$. Since I is an ideal of R, π is a mapping between two rings. First, let a, $b \in R$; then, $f(a+b) = (a+b)+I = (a+I)+(b+I) = f(a)+f(b)$ and $f(ab) = ab+I = (a+I)(b+I) = f(a)f(b)$, so f is indeed a ring homomorphism. Next, if $r + I$ is an arbitrary element of R/I, then surely $r \in R$ and $f(r) = r+I$, thus f is surjective. Lastly, note that $\text{Ker}\, f = \{r \in R \,|\, f(r) = 0 + I\} = \{r \in R \,|\, r + I = I\} = \{r \in R \,|\, r \in I\} = I$. $\square$

Any mapping defined in the same way as π is called a *canonical projection*. There will be many instances throughout this paper in which canonical projections are used. On the other hand, noting that the kernel of a ring homomorphism is an ideal of the domain will prove to be very valuable in the proofs to come.

The next two theorems are must-haves when it comes to ring homomorphisms. Although it is a very well-known and essential fact of Ring Theory, we introduce the First Isomorphism Theorem of rings in this paper solely for its extensive reappearance in many of the proofs. As for the Second Isomorphism Theorem of rings, a few crucial theorems rely on it.

First Isomorphism Theorem. *If $f : R \to S$ is a homomorphism of rings, then f induces an isomorphism of rings $R/Ker\, f \cong f(R)$.*

Proof. Let R, S be rings and let $f : R \to S$ be a homomorphism of rings. As we have seen, $\text{Ker}\, f$ is an ideal of R and $R/\text{Ker}\, f$ is a ring. Moreover, $f(R)$ is a subring of S. Naturally, $f(0_R) = 0_S$. Therefore, since $f(0_R) \in f(R)$, then $0_S \in f(R)$. Next, suppose $x \in f(R)$, then there exists $r \in R$ so that $x = f(r)$. Since $r \in R$, then $-r \in R$, meaning $f(-r) = -f(r) = -x \in f(R)$. So, $f(R)$ has additive inverses. Now, suppose x, $y \in f(R)$ and let r, $s \in R$ so that $x = f(r)$ and $y = f(s)$. Then, $x+y = f(r)+f(s) = f(r+s) \in f(R)$ and $xy = f(r)f(s) = f(rs) \in f(R)$ since R is a ring. Therefore, $f(R)$ is a subring of S.

Lastly, consider the function $\phi : R/\text{Ker}\, f \to f(R)$ given by $\phi(r + I) = f(r)$. We will show ϕ is well-defined. Let $r + \text{Ker}\, f$ and $s + \text{Ker}\, f$ be elements of $R/\text{Ker}\, f$ with $r + \text{Ker}\, f = s + \text{Ker}\, f$. Then $r - s \in \text{Ker}\, f$, meaning $f(r - s) = 0$. However, $f(r - s) = f(r) - f(s) = 0$ implies $f(r) = f(s)$, so $\phi(r + \text{Ker}\, f) = \phi(s + \text{Ker}\, f)$, ϕ is well-defined. Hence, the mapping $\phi : R/\text{Ker}\, f \to f(R)$ given by $\phi(r + I) = f(r)$ is a mapping of rings.

Now, we move on to show that ϕ is an isomorphism. First, we will show ϕ is a bijective function. Of course, if $f(r) = f(s)$, then $f(r - s) = 0$, meaning $r - s \in \text{Ker}\, f$.

Hence $r + \text{Ker}\, f = s + \text{Ker}\, f$, so f is injective. Moreover, let $y \in f(R)$ with $y = f(r)$ for some $r \in R$. Then $x = r + \text{Ker}\, f \in R/\text{Ker}\, f$ and $\phi(x) = \phi(r + \text{Ker}\, f) = f(r) = y$, so ϕ is surjective. Next, we will show ϕ is a homomorphism of rings. Let $r + \text{Ker}\, f$, $s + \text{Ker}\, f \in R/\text{Ker}\, f$, then $\phi(\,(r+\text{Ker}\, f)+(s+\text{Ker}\, f)\,) = \phi(\,(r+s)+\text{Ker}\, f\,) = f(r+s) = f(r)+f(s) = \phi(r+\text{Ker}\, f)+\phi(s+\text{Ker}\, f)$ and $\phi(\,(r+\text{Ker}\, f)(s+\text{Ker}\, f)\,) = \phi(rs+\text{Ker}\, f) = f(rs) = f(r)f(s) = \phi(r + \text{Ker}\, f)\phi(s + \text{Ker}\, f)$. Hence, ϕ is an isomorphism, meaning $R/\text{Ker}\, f \cong f(R)$. □

Second Isomorphism Theorem. *If I, J are ideals of a ring R, then there is an isomorphism of rings $(I + J)/J \cong I/(I \cap J)$.*

Proof. Let I, J be ideals of R. Recall that $I + J$ is therefore an ideal of R. Moreover, $J \subset I + J$. If $j \in J$, then $j = 0 + j \in I + J$. Consequently, $J \subset (I + J)$ and both J, $I + J$ being ideals of R imply that J is an ideal of $I + J$. Hence, $(I + J)/J$ is a ring. Now, consider the mapping $\phi : I \to (I + J)/J$ with $\phi(i) = i + J$ for all $i \in I$. Naturally, we regard $i = i + 0$ as an element of $I + J$, so $i + J = (i + 0) + J \in (I + J)/J$. Now, if $a, b \in I$ with $a = b$, then $a - b = 0 \in J$, so $a + J = b + j$. Hence, ϕ is well-defined. Of course, if a, $b \in I$ are arbitrary, then $\phi(a + b) = (a + b) + J = (a + J) + (b + J) = \phi(a) + \phi(b)$ and $\phi(ab) = ab + J = (a + J)(b + J) = \phi(a)\phi(b)$, so ϕ is a ring homomorphism. Moreover, ϕ is surjective: $(I + J)/J = \{(i + j) + J \,|\, i \in I,\, j \in J\} = \{i + J \,|\, i \in I\} = \phi(I)$. Lastly, note that $Ker\, \phi = \{i \in I \,|\, i + J = 0 + J\} = \{i \in I \,|\, i \in J\} = I \cap J$. Hence, by the First Isomorphism Theorem, $I/(I \cap J) \cong (I + J)/J$ as desired. □

The following lemma is a useful fact to have. Not only will it help prove the next theorem, but it will also come in handy for future theorems.

Lemma 1.1.2. *If $f : R \to S$ is a ring homomorphism and J is an ideal of S, then $f^{-1}(J)$ is an ideal of R that contains $Ker\, f$.*

Proof. Let $f : R \to S$ be a ring homomorphism and J be any ideal of S. Consider the set $f^{-1}(J) = \{r \in R \,|\, f(r) \in J\}$. Since $f(0_R) = 0_S$ and $0_S \in J$, then $0_R \in f^{-1}(J)$. Moreover, if $a \in f^{-1}(J)$, then $f(-a) = -f(a) \in J$, so $-a \in f^{-1}(J)$. Also, if a, $b \in f^{-1}(J)$, then $f(a + b) = f(a) + f(b) \in J$ on since $f(a)$ and $f(b)$ belong to J, an additive group. Thus $a + b \in f^{-1}(J)$. Lastly, let $r \in R$ and $i \in f^{-1}(J)$, then note that $f(ri) = f(r)f(i)$ and $f(ir) = f(i)f(r)$. Since $f(r) \in S$ and $f(i) \in J$, where J is a two-sided ideal, then both $f(ri)$ and $f(ir)$ belong to J. Thus, for any $r \in R$ and any $i \in f^{-1}(J)$, both ri and ir belong to $f^{-1}(J)$. Hence, $f^{-1}(J)$ is an ideal of R. Lastly, let $x \in Ker\, f$, then $f(x) = 0_S \in J$. In other words, $x \in f^{-1}(J)$, meaning $Ker\, f \subset f^{-1}(J)$. □

Note that if I is an ideal of R, and if we have $f : R \to S$ as a ring homomorphism, it need not imply that $f(I)$ is an ideal of S. However, if f happened to be surjective, then in fact $f(I)$ would be an ideal of S.

Since we will deal with many quotient rings, the following theorem will prove to be useful. While the following theorem is worded for rings and ideals, there is a similar statement for Group Theory that we might make note of in the future. We will see the correspondence between the ideals of a quotient ring and the original ring it came from.

Correspondence Theorem. *If I is an ideal in a ring R, then every ideal in R/I is uniquely of the form J/I, where J is an ideal of R which contains I.*

Proof. Let I be an ideal of R and let J/I be any ideal of R/I. Recall that the map $\pi : R \to R/I$ given by $r \mapsto r + I$ is a surjective homomorphism of rings with kernel I. By the previous lemma, we have that both $\phi^{-1}(J/I)$ is an ideal of R and $I \subset \pi^{-1}(J/I)$. If $x \in J$, then $\pi(x) \in J/I$, meaning that $x \in \pi^{-1}(J/I)$. Hence, $J \subset \pi^{-1}(J/I)$. Now, if $x \in \pi^{-1}(J/I)$, then we know that $\pi(x) \in J/I$. Yet, if $x + I \in J/I$, then $x \in J$. Hence, we have $\pi^{-1}(J/I) \subset J$. Therefore, $\pi^{-1}(J/I) = J$, meaning J is an ideal of R that contains I.

To show uniqueness, we will show that $\pi(\pi^{-1}(J/I)) = J/I$ and $\pi^{-1}(\pi(J)) = J$. Let $x \in \pi(\pi^{-1}(J/I))$, then $x = \pi(r)$, where $r \in \pi^{-1}(J/I)$. Since $r \in \pi^{-1}(J/I)$, then $\pi(r) \in J/I$. Since $x = \pi(r)$, then $x \in J/I$. Hence, $\pi(\pi^{-1}(J/I)) \subset J/I$. Now, suppose $x \in J/I$. Then, $x = j + I$, for some $j \in J$. Since $\pi(j) = x \in J/I$, then $j \in \pi^{-1}(J/I)$. Lastly, since $x = \pi(j)$ and $j \in \pi^{-1}(J/I)$, then $x \in \pi(\pi^{-1}(J/I))$. Thus, $J/I \subset \pi(\pi^{-1}(J/I))$, meaning $\pi(\pi^{-1}(J/I)) = J/I$. Next, suppose $x \in J$. Then, $\pi(x) \in \pi(J)$. However, if $\pi(x) \in \pi(J)$, then $x \in \pi^{-1}(\pi(J))$. So, $J \subset \pi^{-1}(\pi(J))$. On the other hand, suppose $x \in \pi^{-1}(\pi(J))$. If so, then $\pi(x) \in \pi(J)$. Therefore, for some $j \in J$, $\pi(x) = \pi(j)$. Consequently, since π is a ring homomorphism, $\pi(x) - \pi(j) = \pi(x - j) = 0$, meaning $x - j \in Ker\, \pi = I$. Since $I \subset J$, then we have $x - j \in J$. If $x - j = j'$, for some $j' \in J$, then we have $x = j + j' \in J$, since J is an ideal of R. Hence, $x \in J$, meaning $\pi^{-1}(\pi(J)) \subset J$ and thus $\pi^{-1}(\pi(J)) = J$. □

Now, while we assume the reader is familiar with a field, we will define what is meant by a *division ring.* Since we will not assume commutativity in any proof, division rings will be abundant in this paper. One way to visualize a division ring is simply by thinking of a field without commutativity.

Definition 1.1.2. A ring D with identity $1_D \neq 0$ in which every nonzero element is a unit is called a *division ring.*

The next part our preliminaries will consider is the ring of $n \times n$ matrices over a division ring. In particular, we will see that the ring of endomorphisms over vector spaces will be of great importance. As one can guess, we will see the relation between the ring of endomorphisms of a vector space V over a division ring D with dimension n and the ring of $n \times n$ matrices over D. Nevertheless, for the purposes of brevity, we will define what we mean by the ring of $n \times n$ matrices over a division ring.

Definition 1.1.3. We will use $Mat_n(D)$ to denote the ring of n×n matrices over a division ring D.

Finally, we will use Zorn's lemma and the axiom of choice for some key theorems. Zorn's lemma will aid us in proving a familiar theorem about maximal ideals in a ring with a new twist. As for the axiom of choice, having it at our disposal will grant us an alternative definition for an Artinian ring, which will be used throughout the second half of the paper. So, it is highly recommended that the reader become familiar with these two statements.

Axiom of Choice. *Let C be a collection of nonempty sets. Then we can choose a member from each set in that collection.*

Zorn's Lemma. *Every non-empty partially ordered set in which every chain has an upper bound contains at least one maximal element.*

Chapter 2

R-modules

In order to identify the structure of simple and semi-simple rings, the idea of *R-modules* is fundamental. Regardless, R-modules on their own are a rich subject to study. We shall cover the basics of modules before going deeper into Ring Theory topics. Without further ado, let us observe the most important definition of this paper:

Definition 2.0.1. Let R be a ring. A left *R-module* is an additive abelian group A together with a function $R \times A \to A$ (the image of (r, a) being denoted by ra) such that for all $r, s \in R$ and $a, b \in A$:

(i) $r(a + b) = ra + rb$

(ii) $(r + s)a = ra + sa$

(iii) $r(sa) = (rs)a$

If R has an identity element 1_R and

(iv) $1_R a = a$, $\forall a \in A$

then A is said to be a *unitary R-module* If R is a division ring, then a unitary R-module is called a (left) vector space.

A (unitary) right R-module is defined similarly via a function $A \times R \to A$ denoted $(a, r) \mapsto ar$ and satisfying the obvious analogues for (i)-(iv). Still, from now on we will regard "R-module" as "left R-module" unless otherwise specified. Note that vector spaces over fields are actually a special case of R-modules, meaning the analogies we have been making thus far are well-founded. On the other hand, with the assumption that R is merely a ring and A some arbitrary additive abelian group, many of the linear algebra theorems are put on hold.

From the definition, we can contemplate the fact than the product of a ring element with a module element is another module element. That is, once a ring element makes contact with a module element, we are talking about element in the module thereafter. Let us establish some basic properties of these module elements.

Now, if A is an R-module, 0_A is the additive identity of A, and 0_R is the additive identity of R, then $\forall r \in R$, $\forall a \in A$:

$$r0_A = 0_A \text{ and } 0_R a = 0_A$$

Proof. Since A is an R-module, then we know that if $r \in R$, then $r0_A \in A$. let $b = r0_A$, then $b = r0_A = r(0_A + 0_A) = r0_A + r0_A = b + b$. Since $b \in A$, $-b \in A$. Hence, $0_A = b + (-b) = b + b + (-b) = b$, so $b = 0_A$, or $r0_A = 0_A$ as desired. Similarly, if $a \in A$, then $0_R a \in A$. Let $c = 0_R a$, then $c = 0_R a = (0_R + 0_R)a = 0_R a + 0_R a = c + c$, then $0_A = c + (-c) = c + c + (-c) = c = 0_R a$. □

Another notion that we will need to establish before we move on is the handling of additive inverses with respect to R-modules. That is, establishing the fact that $\forall r \in R$, $\forall a \in A$:

$$(-r)a = -(ra) = r(-a)$$

Proof. All that is necessary is to show that both $(-r)a$ and $r(-a)$ are the additive inverses of ra. Simple, since $ra+(-r)a = (r+(-r))a = 0_R a = 0_A$ and $ra+r(-a) = r(a+(-a)) = r0_A = 0_A$. A is abelian, thus adding the elements to the left will be the same as adding them from the right. Since additive inverses are unique, then $(-r)a = -(ra) = r(-a)$. □

There are many examples that show the idea of R-modules is not too foreign to the rest of ring theory. We will observe examples that show how natural R-modules can exists. Here are some examples of R-modules.

Example 2.0.1. Every additive abelian group G is a $\mathbb{Z}$-module, with $na = a + \cdots + a$ n-fold and $(-n)a = -na$ for $n > 0$ and $a \in G$.

Example 2.0.2. If R is a ring and S is a subring of R, then R is an S-module with the multiplication of R.

Example 2.0.3. If R is a ring, then $R[x]$ (the ring of polynomials in x with coefficients in R) is an R-module with the scalar multiplication for functions.

Example 2.0.4. If I is a left ideal of R, then I is a left R-module. Similarly, a right ideal of R is a right R-module.

Example 2.0.5. Let I be a left ideal of R. The additive quotient group R/I is not quite a ring. Still, with the action of R on R/I as $r(s+I) = rs + I$, R/I is an R-module. This action is well-defined, for if $a + I$, $b + I \in R/I$ and $a + I = b + I$, then for any $r \in R$ we have that $a - b \in I$, meaning $r(a - b) = ra - rb \in I$, and thus $ra + I = rb + I$.

Example 2.0.6. If R is a ring, then $Mat_n(R)$ is an R-module with the scalar multiplication $r(a_{ij}) = (ra_{ij})$ for any $(a_{ij}) \in Mat_n(R)$.

2.1 R-module homomorphism

In the comparison of R-modules to vector spaces over fields, R-module homomorphisms are the answer to linear transformations. In fact, when R is a division ring, an R-module homomorphism is indeed called a linear transformation. The full impact of the propositions following the next definition will be seen extensively once we focus on tackling the second Wedderburn-Artin theorem. For now, we will establish key facts about R-module homomorphisms.

Definition 2.1.1. A left *R-module homomorphism* is a homomorphism $f : A \to B$ of abelian groups where both A and B are R-modules, and also the following condition is met:

- $\forall r \in R, \forall a \in A, f(ra) = r(f(a))$

Example 2.1.1. Every homomorphism of abelian groups $f : A \to B$ is a $\mathbb{Z}$-module homomorphism since $f(na) = nf(a)$, for all $a \in A$ and $n \in \mathbb{Z}$.

Example 2.1.2. If R is a ring, then the mapping $\phi : R[x] \to R[x]$ with $\phi(f(x)) = x(f(x))$ (left multiplication by x) for all $f \in R[x]$ is an R-module homomorphism, but not a ring homomorphism.

Proposition 2.1.1. *If A and B are R-modules, then $Hom_R(A, B)$ (the set of all R-module homomorphisms $A \to B$) is an abelian group with $f + g$ given on $a \in A$ by $(f + g)(a) = f(a) + g(a)$. Additive identity is the zero map.*

Proof. $Hom_R(A, B) \neq \emptyset$ since B being an R-module implies B is an abelian group that has the additive identity 0. Consider the function $f : A \to B$ with $f(a) = 0, \forall a \in A$. The function f is a homomorphism since $f(a + b) = 0 = 0 + 0 = f(a) + f(b), \forall a, b \in A$. Also, $f(ra) = 0 = r0 = rf(a)$, hence f belongs in $Hom_R(A, B)$. Closure is given by having defined addition of functions as pointwise addition. Meaning, if $f, g \in Hom_R(A, B)$, then $\forall a \in A, (f + g)(a) \in Hom_R(A, B)$ since $(f + g)(a) = f(a) + g(a) \in B$. Moreover, $(f + g)(a + b) = f(a + b) + g(a + b) = f(a) + g(a) + f(b) + g(b) = (f + g)(a) + (f + g)(b)$ and $(f + g)(ra) = f(ra) + g(ra) = rf(a) + rg(a) = r(f(a) + g(a)) = r((f + g)(a))$. Next, if $f \in Hom_R(A, B)$, consider $g : A \to B$ with $g(a) = -f(a), \forall a \in A$. Since $(f + g)(a) = f(a) + g(a) = f(a) + (-f(a)) = 0, \forall a \in A$, then $f + g$ is the zero map, meaning g is the additive inverse of f. Still, we must show $g \in Hom_R(A, B)$. Clearly, $g(a + b) = -(f(a + b)) = -(f(a) + f(b)) = (-f(a)) + (-f(b)) = g(a) + g(b)$, so g is a homomorphism. Similarly, $g(ra) = -(f(ra)) = -(rf(a)) = r(-f(a)) = rg(a)$, so $g \in Hom_R(A, B)$. Since we are seeing $Hom_R(A, B)$ as a group under addition, it is understood that the operation is associative. □

Proposition 2.1.2. *$Hom_R(A, A)$ is a ring with identity, where multiplication is composition of functions.*

Proof. If A is an R-module, them we have already established why $Hom_R(A, A)$ is a group under addition. To make sense of $Hom_R(A, A)$ as a ring, we will define multiplication of two functions of $Hom_R(A, A)$ to be their composition of functions. Hence, to prove that $Hom_R(A, A)$ is closed under multiplication, we will show that if $f, g \in Hom_R(A, A)$, then $f \circ g \in Hom_R(A, A)$. Let $f, g \in Hom_R(A, A)$ and let $a, b \in A$. Then, $(f \circ g)(a + b) = f(g(a + b)) = f(g(a) + g(b)) = f(g(a)) + f(g(b)) = (f \circ g)(a) + (f \circ g)(b)$. Hence, $f \circ g$ is a homomorphism. Now, let $f, g \in Hom_R(A, A)$, $a \in A$, and $r \in R$. To show $f \circ g$ is linear over R, and thus and R-module homomorphism, consider $(f \circ g)(ra)$: $(f \circ g)(ra) = f(g(ra)) = f(rg(a)) = rf(g(a)) = r(f \circ g)(a)$. Hence, $Hom_R(A, A)$ is closed under multiplication, and thus a ring. $Hom_R(A, A)$ has the map $i : A \to A$, with $i(a) = a$, $\forall a \in A$ as the multiplicative identity: $f(i(a)) = f(a) = i(f(a))$, $\forall a \in A$, so $f \circ i = f = i \circ f$. □

Recall, $Hom_R(A, A)$ is denoted as $End_R(A)$. As we have shown, $End_R(A)$ is a ring with composition of functions as multiplication. One thing that has been hiding in the background is that the elements of $Hom_R(A, B)$ act on the elements of A. Even more interesting than that is how $End_R(A)$ has the necessary power over the elements of A to satisfy the R-module axioms. In particular, $End_R(A)$ is a unitary ring, where as $Hom_R(A, B)$ is just an additive group. Moreover, the "product" of an element of $End_R(A)$ with an element of A necessarily belongs to A, unlike $Hom_R(A, B)$. Additively, while $Hom_R(A, B)$ would satisfy parts (i) and (ii) from the definition of R-modules, $End_R(A)$ undoubtedly satisfies (i)-(iv). In light of this entire paragraph, we can claim the following proposition.

Proposition 2.1.3. *A is a left $End_R(A)$-module with $fa = f(a)$, for any $f \in End_R(A)$ and $a \in A$.*

As we have seen, V a vector space over a division ring D is a special case in the topic of modules. Nevertheless, $End_D(V)$ is certainly a ring as we have just shown. Of course, $End_D(V)$ is still the set of linear transformations from V onto itself. That being said, we will recall the connecting between the set of D-linear transformations from V onto itself and the ring of $n \times n$ matrices over D. While we know these are isomorphic when D is a field, we will observe the slight change if we restrict ourselves to division rings.

Definition 2.1.2. Let R be a ring. Then, the *opposite ring* of R, denoted R^{op}, is a ring with the same elements as R, the same addition as R, and multiplication "$\cdot$" given by

$$a \cdot b = ba$$

where ba is the product in R.

Theorem 2.1.1. *$End_D(V) \cong Mat_n(D^{op})$, for V a finite dimensional vector space over a division ring D with dimension n.*

Proof. Let V be an n-dimensional vector space over the division ring D with basis $\mathcal{B} = \{v_1, \ldots, v_n\}$. Define $\Phi : End_D(V) \to Mat_n(D^{op})$ with $\Phi(f) = (a_{ij})$, where $f(v_d) = \sum_c a_{cd}v_c$. To prove Φ is injective, suppose $\Phi(f) = \Phi(g)$. If so, then since every entry in both matrices agree, we have that $f(v_i) = g(v_i)$ for $i \in \{1, \ldots, n\}$. Since both f and g

agree in outputs for the basis vectors, then it must be that $f = g$. Now, for surjective, suppose $A \in Mat_n(D^{op})$. Let $u_1, \ldots, u_n$ be the column vectors of A in V with respect to $\mathcal{B}$, and define $h : V \to V$ to be a D-linear mapping that sends $h(v_i) = u_i$ for all i. Since h is a D-linear transformation from V to itself, we have that $h \in End_D(V)$. Since $h \in End_D(V)$ and $\Phi(h) = A$, Φ is surjective. Now, suppose $f, g \in End_n(D)$ and consider $\Phi(f+g)$. Since we have that $(f+g)(v_d) = f(v_d)+g(v_d) = \sum_c a_{cd}v_c+\sum_c b_{cd}v_c = \sum_c(a_{cd} + b_{cd})v_c$, then we can see that the i-jth entry for $\Phi(f + g)$ is precisely $a_{ij} + b_{ij}$. Hence, $\Phi(f+g) = (a_{ij}+b_{ij}) = (a_{ij})+(b_{ij}) = \Phi(f)+\Phi(g)$. Now, for multiplication, we need to show that $\Phi(f \circ g) = \Phi(f)\Phi(g)$, where $\circ$ is composition of functions (the multiplication of $End_D(V)$). Relative to the basis $\mathcal{B}$, say $f(v_k) = \sum_i a_{ik}v_i$ and $g(v_j) = \sum_k b_{kj}v_k$, for $i, j, k \in \{1, \ldots, n\}$. If $\Phi(f) = A$ and $\Phi(g) = B$, we can say that the a_{ik} are the entries of A and b_{kj} are the entries of B. Moreover, since $A, B \in Mat_n(D^{op})$, then the i-jth entry of AB is $\sum_l(a_{il} \cdot b_{lj})$, where $\cdot$ is the operation of D^{op} as described in Definition 2.1.2. On that note, we can see that $(f \circ g)(v_j) = f(g(v_j)) = f(\sum_k b_{kj}v_k) = \sum_k b_{kj}f(v_k) = \sum_k b_{kj}(\sum_i a_{ik}v_i) = \sum_i(\sum_k b_{kj}a_{ik})v_i = \sum_i(\sum_k(a_{ik} \cdot b_{kj}))v_i$. In other words, $(\sum_k(a_{ik} \cdot b_{kj}))$ is the i-jth entry of the matrix corresponding to $\Phi(f \circ g)$. As we stated before, $(\sum_k(a_{ik} \cdot b_{kj}))$ is the i-jth entry of the matrix AB. Hence, we have that $\Phi(f \circ g) = AB = \Phi(f)\Phi(g)$. Thus, Φ is an isomorphism of rings between $End_D(V)$ and $Mat_n(D^{op})$. □

2.2 Submodule

In abstract algebra, we have subgroups in group theory and we have subrings in ring theory. Clearly, module theory cannot lag behind on this aspect! Sadly, starting from the next section and thereafter, we will focus on R-modules that do not have proper, nontrivial submodules. In any case, we will explore briefly the idea of submodules.

Definition 2.2.1. Let R be a ring, A an R-module and B a nonempty subset of A. We say that B is a *submodule* of A provided that B is an additive subgroup of A and $rb \in B$ for all $r \in R$, $b \in B$.

Observe that merely being a subgroup of an R-module is not enough to claim the subgroup is a submodule. Mainly, the extra condition needed is that the product of a ring element and a subgroup element lands inside the subgroup. Also note that if A

is an R-module, it is not guaranteed that for any subset B of A, $RB \subset B$; only, it is guaranteed that $RA \subset A$.

Example 2.2.1. As stated before, if I is an ideal of R, then I is an R-module. Of course, R itself is an R-module and I is an additive subgroup of R. Hence, all (left, right, two-sided) ideals of R are submodules of the R-module R.

Example 2.2.2. Recall, $\mathbb{Q}$ is an additive subgroup of $\mathbb{R}$. Since both are abelian groups, they are $\mathbb{Z}$-modules. Hence, $\mathbb{Q}$ is a submodule of $\mathbb{R}$ over $\mathbb{Z}$.

Example 2.2.3. Consider the ring $Mat_2(\mathbb{Q})$. Of course, $Mat_2(\mathbb{R})$ is a $Mat_2(\mathbb{Q})$-module. Consider the subgroup $S = \{(a_{ij}) \in Mat_2(\mathbb{R}) \,|\, a_{ij} = 0 \text{ if } i \neq j\}$ of $Mat_2(\mathbb{R})$. Even though S is a subgroup of $Mat_2(\mathbb{R})$, S is not a submodule of $Mat_2(\mathbb{R})$ under $Mat_2(\mathbb{Q})$.

Example 2.2.4. let R be a ring and $f : A \to B$ be an R-module homomorphism. As we will see in a future proof, $Ker\, f$ is a submodule of A and $Im\, f = f(A)$ is a submodule of B.

2.3 Simple

The word "simple" will be the most recurring word in this paper. In order to be in the same page, we will define "simple" in the context of both modules and rings. As we will see, these are not necessarily the same idea.

Definition 2.3.1. A left module A over a ring R is *simple*, or *irreducible*, if $RA \neq (0)$ and A has no proper submodules. A ring R is *simple* if $R^2 \neq (0)$ and R has no proper (two-sided) ideals.

Suppose you have a ring R that is simple. Since $R^2 \neq (0)$ and R is its own an R-module, the definitions for simple modules and simple rings agree thus far. However, a ring with no ideals could still have nontrivial left (or right) ideals, thus R could have nontrivial proper submodules.

Example 2.3.1. If D is a division ring, then D has no nontrivial, proper left, right, or two-sided ideals. Recall that if I is a nonzero ideal of D, and if $a \neq 0$ is an element of I, then there exists $b \in D$ so that $ba = 1_D \in I$, meaning $D = D1_D \subset I$. Hence, we can see that D is both a simple ring and a simple D-module.

Proposition 2.3.1. *If D is a division ring, then $Mat_n(D)$ is a simple ring*

Proof. Let D be a division ring and suppose I is an ideal of $Mat_n(D)$ such that $I \neq (0)$; we will show $I = Mat_n(D)$. Let $A = (a_{ij})$ be a nonzero matrix of I. Since A is nonzero, without loss of generality suppose the entry $a_{mk} \neq 0$. Let the matrix $E_{xy} \in Mat_n(D)$ be one where the entry $e_{xy} = 1$ and all other entries are zero. If so, then it is easy to check that $E_{lm}AE_{kl} = a_{mk}E_{ll}$ for $l = 1, 2, \ldots, n$. Moreover, since $A \in I$, an ideal, then $a_{mk}E_{ll} \in I$ for $l = 1, 2, \ldots, n$. Furthermore, if we let $E \in Mat_n(D)$ be the identity matrix, then we can see that $\sum_{l=1}^{n} a_{mk}E_{ll} = a_{mk}E$ belongs to I. Of course, $((a_{mk})^{-1}E)(a_{mk}E) = E$, so $a_{mk}E$ is a unit of $Mat_n(D)$ that belongs in I. Hence, $I = Mat_n(D)$. □

Example 2.3.2. Let D be a division ring and let $R = Mat_n(D)$ with $n > 1$. For each k so that $1 \leq k \leq n$, $I_k = \{(a_{ij}) \in R \mid a_{ij} = 0 \text{ for } j \neq k\}$ is a simple left R-module (a quick proof of this is given in Example 4.3.4). Note that while R is a simple ring, the existence of left, right ideals shows R is not a simple R-module.

Definition 2.3.2. A left ideal I of a ring R is said to be a *minimal left ideal* if $I \neq (0)$ and for every left ideal J such that $(0) \subset J \subset I$, either $J = (0)$ or $J = I$

Example 2.3.3. A left ideal I of R such that $RI \neq (0)$ is a simple left R-module if and only if I is a minimal left ideal.

Proposition 2.3.2. *Every simple left R-module is cyclic; in fact, if A is simple, then $A = Ra$, $\forall a \in A, (a \neq 0)$.*

Proof. Let A be a simple left R-module and let $a \in A$, $a \neq 0$. First, we will show that Ra is a subgroup, and then a submodule, of A. $Ra = \{ra \mid r \in R\}$ is a subset of A since $a \in A$ and A is an R-module implies that $\forall r \in R$, $ra \in A$. First, $0_R \in R$, so $0_R a = 0_A \in Ra$, so Ra is non-empty. Second, if ra, $sa \in Ra$, then $ra + sa = (r + s)a \in Ra$, meaning there is closure in Ra. Third, if $ra \in Ra$, then $r \in R$, so $-r \in R$, so $(-r)a \in Ra$, meaning $-ra \in Ra$. Since Ra has identity, closure, and inverses, then Ra is a subgroup of A. For submodule, we must know show that $\forall r \in R$, $x \in Ra$, $rx \in Ra$. Of course, if $x \in Ra$, then $x = sa$, for some $s \in R$. So, $rx = r(sa) = (rs)a \in Ra$, meaning Ra is a submodule. Since Ra is a submodule of the simple R-module A, then by Definition 2.3.1 either $Ra = A$ or $Ra = (0)$. Now, consider $B = \{b \in A \mid Rb = (0)\}$. Clearly $0_A \in B$ since

$r0_A = 0_A$ for all $r \in R$ (and $0_A \in A$), So B is non-empty. If $x,\, y \in B$, then $\forall r \in R$, $r(x+y) = rx + ry = 0_A + 0_A = 0_A$, meaning $R(x+y) = (0)$, or that $x + y \in B$. Plus, if $x \in B$, then $\forall r \in R$, $rx = 0_A$. Hence, $r(-x) = -rx = -0_A = 0_A$ for all $r \in R$, meaning $-x \in B$. In short, B is a subgroup of A. To show B is a submodule, let $r \in R$ and $b \in B$. To show $rb \in B$, consider $R(rb)$. If $s \in R$, then $s(rb) = s(0) = 0$; meaning, $s(rb) = 0$ $\forall s \in R$, or $R(rb) = (0)$, and thus $rb \in B$. Since A is simple and B its submodule, again either $B = A$ or $B = (0)$. However, if $B = A$, then $\forall x \in A$, $Rx = (0)$, meaning $RA = (0)$, contradicting A as a simple R-module. Thus, $B = (0)$. Hence, if $a \neq 0$, then $a \notin B$, meaning $Ra \neq (0)$, thus $Ra = A$. □

The following theorem is the most powerful result from R-module homomorphism and simple R-modules: *Schur's lemma.* While it has many forms throughout abstract algebra, we shall focus on the module theory version.

Schur's Lemma. *Let A be a simple R-module and B any R-module:*

(i) Every nonzero R-module homomorphism $f : A \to B$ is injective.

(ii) Every nonzero R-module homomorphism $g : B \to A$ is surjective.

(iii) $End_R(A)$ is a division ring.

Proof. First, suppose A and B are as assumed, and suppose $f : A \to B$ is a nonzero R-module homomorphism. Consider $Ker\ f = \{a \in A \,|\, f(a) = 0\}$. We know $Ker\ f$ is a subgroup of A. We will show $Ker\ f$ is a submodule. Let $r \in R$ and $k \in Ker\ f$. Since f is an R-module homomorphism and $k \in A$ ($Ker\ f \subset A$), then $f(rk) = rf(k)$. Since $k \in Ker\ f$, then $f(k) = 0$, so $f(rk) = rf(k) = r0 = 0$, so $rk \in Ker\ f$. Thus, $rk \in Ker\ f$ for all $r \in R$, $k \in Ker\ f$, then $Ker\ f$ is a submodule of A. Since A is simple, then either $Ker\ f = A$ or $Ker\ f = (0)$. However, if $Ker\ f = A$, then f is the zero map, which we are assuming it is not. Hence, $Ker\ f = (0)$. Now, if $f(a) = f(b)$, then $f(a) - f(b) = f(a-b) = 0$. So, $a - b \in Ker\ f = (0)$, so $a - b = 0$, or $a = b$. Therefore, f is injective.

Second, suppose A and B are as assumed, and suppose $g : B \to A$ is a nonzero R-module homomorphism. Consider the image of B under g, $g(B) = \{g(b) \,|\, b \in B\}$. Again, $g(B)$ as the image of a homomorphism is a subgroup of the codomain A. Now, we will show $g(B)$ is a submodule of A. Let $r \in R$ and let $y \in g(B)$. Consider ry. If

$y \in g(B)$, then $\exists x \in B$ so that $y = g(x)$. Since g is an R-module homomorphism, then $ry = rg(x) = g(rx)$. Since $r \in R$, $x \in B$ and B an R-module, then $rx \in B$. Therefore, $ry = g(rx)$ and $rx \in B$, then $ry \in g(B)$. Now that we know $g(B)$ is a submodule of A, by simplicity either $g(B) = (0)$ or $g(B) = A$. If $g(B) = (0)$, then it would mean that g is the zero mapping, which is not. Therefore $g(B) = A$, which means g is surjective.

Third, Suppose A is a simple R-module. As we have seen before, $End_R(A)$ is a ring with unity. Now, let $h \in End_R(A)$, $h \neq 0$. By (i) and (ii), we know h is injective and surjective. Since h is bijective, then h has an inverse $h^{-1} : A \to A$. Lastly, to say $h^{-1} \in End_R(A)$, we need to show h^{-1} is an R-module homomorphism. Let a, $b \in A$. Since h is bijective, then $\exists x$, $y \in A$ so that $a = h(x)$ and $b = h(y)$ (Note this implies that $h^{-1}(a) = x$ and $h^{-1}(b) = y$). Then $h^{-1}(a + b) = h^{-1}(h(x) + h(y)) = h^{-1}(h(x + y)) = x + y = h^{-1}(a) + h^{-1}(b)$, so h^{-1} is a homomorphism. Now, let $a \in A$ and $r \in R$. Since h is bijective, say $a = h(x)$ for some $x \in A$. Then $h^{-1}(ra) = h^{-1}(rh(x)) = h^{-1}(h(rx)) = rx = rh^{-1}(a)$, so h^{-1} is an R-module homomorphism. □

Mainly, part (iii) will be of great importance. By Proposition 2.1.3, A being an R-module implies A is an $End_R(A)$-module. As we can see from Schur's lemma, whenever A is a simple R-module, then A is a *vector space* over the division ring $End_R(A)$. Just to let the weirdness sink in, notice this says that a simple module is a vector space with functions as scalars. Then again, the act of multiplying a vector by a scalar to get another vector makes it sound like scalars induce endomorphisms on a vector space. So, perhaps it is not so different after all. Also, let us not dismiss the fact that every R-module endomorphism of a simple module is automatically bijective.

Chapter 3

Regular, Quasi-regular, and The Jacobson Radical

Now that we have familiarized ourselves with the basics of R-modules, we will finally lean more towards ring theory. While we covered the definition of a simple ring, we have yet to mention the definition of a semi-simple ring. The reason for withholding the definition so far is that the definition for a semi-simple ring depends on what is known as the *Jacobson radical* of a ring. Consequently, before understanding the Jacobson radical we needed to dig into R-modules beforehand. Regardless, there are still a few notions we must cover before jumping into the Jacobson radical.

3.1 Regular Ideals

As we mentioned before, if I is a left ideal of R, then R/I is a left R-module. Upon close examination, we can see that there is a specific type of ideal that would guarantee R/I to have no submodules. However, in order to call it simple, having no nontrivial submodules is half of it. To guarantee the second condition, $R(R/I) \neq (0)$, we will need the idea of regular ideals.

Definition 3.1.1. A left ideal I of a ring R is *left regular* if there exists $a \in R$ such that $r - ra \in I$ for every $r \in R$. Similarly, a right ideal J of R is *right regular* if there exists $b \in R$ such that $r - br \in J$ for every $r \in R$.

While the definition for regular ideals seems wild, it is not as uncommon as one might think. We shall contemplate some examples of familiar ideals that are regular.

Example 3.1.1. If R is a ring with unity, then every (left, right, two-sided) ideal of R is regular. That is, for any ideal I of R, $r - r(1_R) = 0 \in I$ and $r - (1_R)r = 0 \in I$ for any r in R.

Example 3.1.2. Consider the non unital ring $2\mathbb{Z}$ and its ideal $10\mathbb{Z}$. Since $2\mathbb{Z}$ is commutative, right regular and left regular are the same notion. Now, consider $-4 \in 2\mathbb{Z}$: if $n \in 2\mathbb{Z}$, then $n = 2k$ for some integer k. Thus, $n - n(-4) = n + 4n = 5n = 5(2k) = 10k \in 10\mathbb{Z}$ for any n in $2\mathbb{Z}$. So, $10\mathbb{Z}$ is a regular ideal of $2\mathbb{Z}$.

There is an application of Zorn's lemma that declares the existence of maximal ideals on rings with unity. However, asking for a multiplicative identity is much more than necessary. As we shall prove, a ring need only have a proper regular ideal in order to contain a maximal ideal.

Lemma 3.1.1. *If ρ is a proper regular left ideal of R, then there exists a maximal regular left ideal ρ_0 of R so that $\rho \subset \rho_0$.*

Proof. Let ρ be a proper, regular left ideal of R and let $a \in R$ so that $r - ra \in \rho$ for all $r \in R$. Note that $a \notin \rho$, or else $ra \in \rho$ meaning $r \in \rho$, $\forall r \in R$, or $\rho = R$. Let $\mathcal{M}$ be the set of all proper left ideals of R which contain ρ. Note once more that if $\rho' \in \mathcal{M}$, then $a \notin \rho'$. Otherwise, since $r - ra \in \rho$ and $\rho \subset \rho'$ means both $r - ra$ and ra are in ρ' for all $r \in R$, then $r \in \rho$, $\forall r \in R$ contradicting ρ' as being a proper left ideal of R. Now, we will apply Zorn's lemma. Since $\rho \subset \rho$, then $\rho \in \mathcal{M}$, meaning $\mathcal{M}$ is nonempty. Moreover, $\mathcal{M}$ is a partially ordered set under set containment. Lastly, Suppose $\rho \subset \rho_1 \subset \rho_2 \subset \rho_3 \subset ...$ is a chain of ideals from $\mathcal{M}$. Let U be the union of all the ideals from the chain of ideals. Clearly, U is an upperbound to the chain of ideals as for set containment. Hence, all that is needed to show is that the set U belongs in $\mathcal{M}$. Hence, we have to show U is a left ideal of R that contains ρ. In fact, we know $\rho \subset U$ since U is the union of sets that contain ρ. Now, since $\rho \subset U$, then ρ being a left ideal of R implies $0 \in U$, so U is nonempty. Next, let $u \in U$. Since $u \in U$, $\exists \rho_u$ in the chain of ideals so that $u \in \rho_u$. Since ρ_u is a left ideal, it is certainly an additive subgroup of R, thus, $-u \in \rho_u$. Since $\rho_u \subset U$, $-u \in U$, meaning elements of U have additive inverses. Now, let x, $y \in U$. As explained before, $x \in \rho_x$ and $y \in \rho_y$ for some ρ_x, ρ_y in the chain of ideals. Since both ρ_x and ρ_y are both in the chain, either $\rho_x \subset \rho_y$ or $\rho_y \subset \rho_x$. Without loss of generality, suppose $\rho_x \subset \rho_y$. Then, $x \in \rho_x$ implies $x \in \rho_y$ and since both x and y are in ρ_y, ρ_y is a subring of R, then $x + y \in \rho_y$ and $xy \in \rho_y$. In other words, $x + y$ and xy belong in U, making U closed under addition and multiplication. Now that we have shown U is a subring of R, we need to establish U as a left ideal. Let $r \in R$ and $i \in U$. Say $i \in \rho_i$, where ρ_i is a left ideal from the chain. Then, by definition, $ri \in \rho_i$. So, $ri \in U$, making U a left ideal of R. Therefore, since U is a an upperbound on the chain of ideals and U is in $\mathcal{M}$, Zorn's lemma indicates that there is a maximal element of $\mathcal{M}$. Call the maximal element ρ_0. Note that if a proper left ideal J of R happened to contain ρ_0, it would imply that $J \in \mathcal{M}$, which in turn means J is contained in ρ_0. Therefore, ρ_0 is a maximal left ideal of R. Lastly, as hinted before, ρ_0 is regular since $r - ra \in \rho$ and $\rho \subset \rho_0$. □

Now that we have made ourselves familiar with regular ideals, let us digress to our previous discussion of creating simple modules. If R is a ring and I is a left ideal of R, then R/I will be without nontrivial submodules provided I is a maximal left ideal of R. However, to make sure R will not annihilate R/I, having I as a regular ideal will do the trick. Surprisingly, we will discover that any simple left R-module is isomorphic to a quotient group R/I where I is as maximal left ideal which is also regular.

Theorem 3.1.1. *A left R-module A is simple $\iff$ $A \cong R/\rho$ for some maximal left ideal ρ, which is regular.*

Proof. Let A be a simple R-module and let $a \in A$, $a \neq 0$. Recall that R is also an R-module and that $A = Ra$. Consider the mapping $\phi : R \to Ra$ with $\phi(r) = ra$. Suppose $r,\ s \in R$. Then, $\phi(r + s) = (r + s)a = ra + sa = \phi(r) + \phi(s)$, meaning ϕ is a group homomorphism. Now, to show that ϕ is an left R-module homomorphism, let $c \in R$ and $r \in R$, then $\phi(cr) = (cr)a = c(ra) = c\phi(r)$. Moreover, it is obvious that ϕ is surjective. Let $\rho = Ker\phi = \{r \in R \,|\, ra = 0\}$, then $R/\rho \cong A$ by the . Next, we will show that ρ is maximal left ideal. Since $\rho = Ker\phi$, then ρ is an additive subgroup of R. Now, if r, s $\in \rho$, then $(rs)a = r(sa) = r(0) = 0$, so $rs \in \rho$; thus, ρ is a subring of R. To show it is a left ideal, let $r \in R$ and $i \in \rho$. Since $(ri)a = r(ia) = r(0) = 0$, then $ri \in \rho$, meaning ρ is a left ideal. To show that ρ is left maximal, suppose that instead there is an left ideal J of R such that $\rho \subset J$. Then J/ρ is a submodule of R/ρ. However, since A is simple module, and $A \cong R/\rho$, then either $J/\rho = (0)$ or $J/\rho = R/\rho$. In other words, either $J = \rho$

or $J = R$. Therefore, ρ is maximal left ideal of R. Finally, to show ρ is regular, recall that $a \in A$ and $A = Ra$. Since $a \in A$, then $a \in Ra$. Therefore, $\exists s \in R$ so that $a = sa$. Then, for all $r \in R$, $ra = rsa$, which means $ra - rsa = (r - rs)a = 0$. In other words, $\forall r \in R$, $r - rs \in \rho$ where $s \in R$, then ρ is regular.

For the converse, suppose $A \cong R/\rho$ for some maximal regular left ideal ρ. Since ρ is maximal, R/ρ will have no submodules. By the Correspondence Theorem, any submodule of R/ρ is a submodule of the form J/ρ, where J is an ideal of R and $\rho \subset J$. Thus, either $J = \rho$ or $J = R$, meaning the submodule J/ρ is either the trivial subgroup or R/ρ itself. Now, to call R/ρ simple, we must show that $R(R/\rho) \neq (0)$. Suppose that instead, $R(R/\rho) = (0)$. We know that ρ is a maximal regular left ideal, and suppose that $s \in R$ so that $r - rs \in \rho$ for all $r \in R$. Since $R(R/\rho) = (0)$, then surely $r(s + \rho) = \rho$, $\forall r \in R$. This implies that $rs \in \rho$, $\forall r \in R$. However, if both $r - rs \in \rho$ and $rs \in \rho$, $\forall r \in R$, then $r \in \rho$, $\forall r \in R$. Hence, $R \subset \rho$, which contradicts ρ being a maximal ideal. $\square$

3.2 Jacobson Radical

When we talk about A being an R-module, we can think of the elements of A as objects that are being influenced by elements from R. That being said, we want to be aware of elements of R which "eliminate" the elements of A. On that note, we turn to the annihilator of an R-module M.

Definition 3.2.1. If M is an R-module, then $\mathcal{A}(M) = \{x \in R \,|\, xM = (0)\}$ is the left *annihilator* of M.

Example 3.2.1. Consider $\mathbb{Z}_6$ with the standard $\mathbb{Z}$-module structure for abelian groups. What is $\mathcal{A}(\mathbb{Z}_6)$? Note that even though $3 \cdot \overline{2} = \overline{0}$ and $3 \cdot \overline{4} = \overline{0}$, 3 does not annihilate all of $\mathbb{Z}_6$. Hence, $3 \notin \mathcal{A}(\mathbb{Z}_6)$. Upon close examination, we can see $\mathcal{A}(\mathbb{Z}_6) = 6\mathbb{Z}$. In general, $\mathcal{A}(\mathbb{Z}_n) = n\mathbb{Z}$.

Note that in the previous example, the annihilator of the module was an ideal of the ring. This is not an accident, as we shall see in the next lemma. In fact, the definition of an annihilator is strong enough to make ideals from mere subset of a module.

Lemma 3.2.1. *If A is a left R-module and $B \subset A$, then $\mathcal{A}(B) = \{r \in R \,|\, rb = 0, \forall b \in B\}$ is a left ideal of R. If B is a submodule of A, then $\mathcal{A}(B)$ is a two-sided ideal of R.*

Proof. First, we will show that if $B \subset A$, then $\mathcal{A}(B)$ is a left ideal. First, $0_R \in \mathcal{A}(B)$, so $\mathcal{A}(B)$ is nonempty. Second, suppose r, $s \in \mathcal{A}(B)$. Let $b \in B$ and consider $(r+s)b = rb + sb = 0 + 0 = 0$. Since $(r+s)b = 0$ for all $b \in B$, then $r + s \in \mathcal{A}(B)$. Third, if $r \in \mathcal{A}(B)$, then $(-r)b = -rb = -0 = 0$, meaning $-r \in \mathcal{A}(B)$. Thus, $\mathcal{A}(B)$ is a subgroup of R. Now, for subring, let r, $s \in \mathcal{A}(B)$ and let $b \in B$. Since $(rs)b = r(sb) = r(0) = 0$ for all $b \in B$, then $rs \in \mathcal{A}(B)$. Now that we know $\mathcal{A}(B)$ is a subring of R, we will now show that $\mathcal{A}(B)$ is a left ideal. Let $r \in R$ and $i \in \mathcal{A}(B)$. To show $ri \in \mathcal{A}(B)$, let $b \in B$. Then, $(ri)b = r(ib) = r(0) = 0$, $\forall b \in B$. Hence, $ri \in \mathcal{A}(B)$, making it a left ideal.

Now, suppose that this time B is a submodule of A. Since submodules are subsets, when know that $\mathcal{A}(B)$ is a left ideal. To show it is an ideal, we will show it is also a right ideal. Let $r \in R$, $i \in \mathcal{A}(B)$ and $b \in B$. To show $ir \in \mathcal{A}(B)$, we must show that $(ir)b = 0$ $\forall b \in B$. We know $(ir)b = i(rb)$, however, we do not know if $rb = 0$ since r is just a random element of R and b a random element of B. The difference from last time is that we know that B is an submodule of A, which means that we definitely know $rb \in B$. Since $i \in \mathcal{A}(B)$ and $rb \in B$, then we know $i(rb) = 0$, which means $(ir)b = 0$, meaning $\mathcal{A}(B)$ is a two-sided ideal. □

Clearly, the zero element is not the only element of a ring that can annihilate its module elements. However, if zero is the only element that ubiquitously annihilates every module element, we call the module *faithful*. In the case where the module also happens to be simple, we say the ring is *primitive*.

Definition 3.2.2. A (left) module M is *faithful* if its (left) annihilator $\mathcal{A}(M)$ is (0). A ring R is (left) *primitive* if there exists a simple faithful (left) R-module.

Example 3.2.2. Recall that $\mathbb{Q}$ as a subring of $\mathbb{R}$ implies $\mathbb{R}$ is a $\mathbb{Q}$-module. Now, since $\mathcal{A}(\mathbb{R})$ is an ideal of $\mathbb{Q}$ and clearly not all rational numbers annihilate $\mathbb{R}$, then $\mathbb{R}$ is a faithful $\mathbb{Q}$-module.

Example 3.2.3. Continuing with the above example, since $\mathbb{R}$ is also an $\mathbb{R}$-module where only zero annihilates all of $\mathbb{R}$, then $\mathbb{R}$ is a faithful $\mathbb{R}$-module. Moreover, since submodules of $\mathbb{R}$ translates to ideals of $\mathbb{R}$ in this case, we can see that $\mathbb{R}$ is a simple module. Therefore, $\mathbb{R}$ is a primitive ring.

The reason why fields were used as examples foreshadows an interesting fact about commutative primitive rings. We will take a closer look at primitive rings right before tackling the last Wedderburn-Artin theorem. For the moment, let us observe one more fact concerning annihilators.

Lemma 3.2.2. *If M is a left R-module, then M is a faithful left $R/\mathcal{A}(M)$-module.*

Proof. Let M be a left R-module. Recall from Lemma 3.2.1 that, since M is a submodule of itself, $\mathcal{A}(M)$ is an ideal of R. So, $R/\mathcal{A}(M)$ is a ring. Define for $m \in M$ and $r+\mathcal{A}(M) \in R/\mathcal{A}(M)$, the action $(r+\mathcal{A}(M))m = rm$. Let us show this action is well-defined: Suppose $a+\mathcal{A}(M) = b+\mathcal{A}(M)$. Then, $a-b \in \mathcal{A}(M)$. Therefore, $(a-b)m = 0$ for all $m \in M$. So, $am - bm = 0$ implies $am = bm$ for all $m \in M$. In short, $(a+\mathcal{A}(M))m = (b+\mathcal{A}(M))m$ for all $m \in M$, so the action of $R/\mathcal{A}(M)$ on M is well-defined. Now, recall that M is an R-module, so verifying the module axioms is almost trivial. First, let $r+\mathcal{A}(M) \in R/\mathcal{A}(M)$ and let $m, n \in M$. Then, $(r+\mathcal{A}(M))(n+m) = r(n+m) = rn+rm = (r+\mathcal{A}(M))n + (r+\mathcal{A}(M))m$. Second, let $r+\mathcal{A}(M)$, $s+\mathcal{A}(M) \in R/\mathcal{A}(M)$ and let $m \in M$, then $[(r+\mathcal{A}(M)) + (s+\mathcal{A}(M))]m = (r+s+\mathcal{A}(M))m = (r+s)m = rm+sm = (r+\mathcal{A}(M))m+(s+\mathcal{A}(M))m$. Third, let $r+\mathcal{A}(M)$, $s+\mathcal{A}(M) \in R/\mathcal{A}(M)$ and let $m \in M$, then $[(r+\mathcal{A}(M))(s+\mathcal{A}(M))]m = (rs+\mathcal{A}(M))m = (rs)m = r(sm) = (r+\mathcal{A}(M))[(s+\mathcal{A}(M))m]$. Thus, M is an $R/\mathcal{A}(M)$-module. Now, to show M is faithful, suppose $(r+\mathcal{A}(M))m = 0$ for all $m \in M$. Then, $rm = 0$ for all $m \in M$. This implies that $r \in \mathcal{A}(M)$; hence, if $(r+\mathcal{A}(M))m = 0$, then $r+\mathcal{A}(M) = 0+\mathcal{A}(M)$, the zero element. □

Example 3.2.4. Recall that $\mathbb{Z}_6$ is a $\mathbb{Z}$-module. Notice that the set $C = \{\overline{0}, \overline{2}, \overline{4}\}$ is a simple submodule of $\mathbb{Z}_6$ with $\mathcal{A}(C) = 3\mathbb{Z}$. By Lemma 3.2.2, C is a faithful $\mathbb{Z}/3\mathbb{Z}$-module. Hence, the ring $\mathbb{Z}/3\mathbb{Z}$ is primitive.

Given how a ring R could in fact have elements that turn all the module elements into the zero element, it would be nice to have a way to categorize a ring by how volatile it might be to its modules. While the annihilator of an R-module M can tell us which elements annihilate the elements of M, this set is only specific to the relevant R-module. Moreover, considering all of the modules of a ring sounds pretty daunting, so we would like to focus on the simple modules of a ring first. On that note, we introduce The Jacobson Radical.

Definition 3.2.3. The *Jacobson radical* of R, written as $J(R)$, is the set of all elements of R which annihilate all the simple R-modules. If R has no simple R-modules, then

$J(R) = R$ and we call R a *radical ring.* On the other hand, If $J(R) = (0)$, then we say R is *semi-simple.*

We have finally revealed the meaning of a semi-simple ring! In abstract algebra, the relationship between simple objects and semi-simple objects is, well, simple. We usually refer to semi-simple objects as those which are some type of product of other simple objects. While this definition for a semi-simple ring sounds out of place, it is simply a foreshadowing for things to come.

Notice that the Jacobson radical is the intersection of all simple module annihilators. That is, $J(R) = \bigcap \mathcal{A}(M)$, where each M is a simple R-module of R. Respectively, since each $\mathcal{A}(M)$ is a two-sided ideal of R, then $J(R)$ is also a two-sided ideal of R. Unfortunately, a ring could have many random modules, so exploring the annihilators of every single module to a identify ring's Jacobson radical is not a task we want to undertake. We now look for a better structure for the Jacobson radical of a ring.

Definition 3.2.4. If I is a left ideal of R, then $(I : R) = \{x \in R \,|\, xR \subset I\}$.

While an left ideal I of a ring R absorbs ring elements from the left, this new set consists of elements of R that absorb ring elements into I from the right. Naturally, if I is two-sided, then $I \subset (I : R)$. In any case, we will see this set is of great importance in moving our focus away from the modules themselves.

Proposition 3.2.1. *If $M = R/\rho$ for some maximal regular left ideal ρ, then $\mathcal{A}(M) = (\rho : R)$, and $(\rho : R)$ is the largest two-sided ideal of R inside ρ.*

Proof. Suppose $M = R/\rho$ for some maximal regular left ideal ρ. Let $x \in \mathcal{A}(M)$, Then $xM = (0)$; meaning, $x(r + \rho) = \rho$ for all $r \in R$. Therefore, $xr \in \rho$, $\forall r \in R$. Hence, $xR \subset \rho$ and thus $x \in (\rho : R)$. Now, let $x \in (\rho : R)$. Then, since $xR \subset \rho$, $xr \in \rho$, $\forall r \in R$. Then, $\rho = xr + \rho = x(r + \rho)$, $\forall r \in R$. So $x(R/\rho) = (0)$, implying $x \in \mathcal{A}(M)$. Therefore, $\mathcal{A}(M) = (\rho : R)$. Moreover, Since ρ is regular, $\exists a \in R$ so that $r - ra \in \rho$ for all $r \in R$. Let $x \in (\rho : R)$. Consequently, $x \in R$, then $x - xa \in \rho$. However, since $x \in (\rho : R)$ and $a \in R$, then $xa \in \rho$. If $xa \in \rho$ and $x - xa \in \rho$, then $x \in \rho$. Hence, $(\rho : R) \subset \rho$. To show that $(\rho : R)$ is the largest ideal of ρ, suppose there is an ideal J of ρ so that $(\rho : R) \subset J \subset \rho$. If $j \in J$, then $j \in R$. Now, $j \in J$, a two-sided ideal, and $J \subset \rho$ implies $jr \in \rho$ for all $r \in R$; hence by definition, $j \in (\rho : R)$. Therefore, $J \subset (\rho : J)$. □

Hence, for any ring R, $J(R) = \bigcap(\rho : R)$, where ρ runs over all regular maximal left ideal of R. Now, all there is left to do is to keep track of $(\rho : R)$ for each maximal regular left ideals ρ of R. While it sounds better than looking at every simple module of a ring, it still feels unsatisfactory. We can still do better, as we will see in the next section.

3.3 Quasi-regular

If the idea of regular ideals seemed bizarre, then we are in for a treat with the introduction of *quasi-regular* ideals. While the definition of a regular ideal states nothing about the element of the ideal, a quasi-regular ideal is an ideal where all of its elements are quasi-regular.

Definition 3.3.1. An element $a \in R$ is said to be *left-quasi-regular* if there is an element $b \in R$ such that $b + a + ba = 0$. We call b a *left-quasi-inverse* of a. Similarly, $c \in R$ is said to be *right-quasi-regular* if there is an element $d \in R$ such that $c + d + cd = 0$ and d is the *right-quasi-inverse* of c. We say that a (left, right, two-sided) ideal of R is left-quasi-regular if all of its elements are left-quasi-regular. Similarly, a (left, right, two-sided) ideal of R is right-quasi-regular if all of its elements are right-quasi-regular.

Example 3.3.1. In $\mathbb{R}$, every element is quasi-regular except -1. If $(-1)+y+(-1)y = 0$, then $-1 = 0$. If neither x nor y is -1 and y is the quasi-inverse of x, then $y = -\frac{x}{x+1}$.

Example 3.3.2. In $\mathbb{Z}$, the only quasi-regular elements are 0 and -2, where they are both their own quasi-inverse. (Again, observe the solutions to $y = -\frac{x}{x+1}$ for x, $y \in \mathbb{Z}$.)

Apparently quasi-regular elements are not as strange as we originally thought. Certainly, a question one might have is "why do we care for quasi-regular elements in a ring?" In a weird turn of events, quasi-regular elements are the key for a better structure of the Jacobson radical. Foremost, let us state an important fact about quasi-regular ideals.

Lemma 3.3.1. *If I is a left-quasi-regular left ideal of R, then $I \subset J(R)$.*

Proof. Let I be a left-quasi-regular left ideal of R. Suppose then that $I \not\subset J(R)$. If so, then for some simple R-module M, we must have $IM \neq (0)$. In turn, it must mean that there is at least one element $m \in M$ so that $Im \neq (0)$. Consequently, it turns out that Im is a submodule of M. Since $0 \in I$, $0m = 0 \in Im$, so Im is nonempty. Now, if $a \in Im$, then $a = im$ for some $i \in I$. Since $i \in I$, then $-i \in I$, meaning $(-i)m = -im = -a \in Im$. Now, if a, $b \in Im$, say $a = im$ and $b = jm$, then $a + b = im + jm = (i + j)m \in Im$. Now that we know Im is a subgroup of M, let us confirm the module part. Let $r \in R$ and let $b \in Im$ with $b = jm$, $j \in I$. Consider $rb = r(jm) = (rj)m$: since $r \in R$ and $j \in I$, I a left ideal of R, then $rj \in I$. Hence, $rb \in Im$ for all $r \in R$, $b \in Im$, so Im is a submodule of M. However, since Im is a nonzero submodule of M, then $Im = M$. Well, $-m \in M$ implies $-m \in Im$, so $\exists t \in I$ so that $-m = tm$. Moreover, t is a member of a left-quasi-regular ideal, so $\exists s \in R$ so that $s + t + st = 0$. It follows that $0 = 0m = (s+t+st)m = sm+tm+stm = sm+(-m)+s(-m) = sm-sm-m = -m$. Since $-m = 0$, then $m = 0$, which would make $Im = (0)$, a contradiction. Therefore, it must be that $I \subset J(R)$. □

As Lemma 3.3.1 shows, from now on we can instantly declare that any quasi-regular ideal is contained in the Jacobson radical. This will prove be immensely useful. One application we can observe is that if a ring is semi-simple, then the only quasi-regular ideal is the trivial ideal. Still, the most crutial implication of Lemma 3.3.1 is the following theorem.

Theorem 3.3.1. *$J(R) = \bigcap \rho$, where ρ runs over all maximal regular left ideals of R.*

Proof. We know that $J(R) = \bigcap(\rho : R)$ and that $(\rho : R) \subset \rho$, therefore $J(R) \subset \bigcap \rho$, where ρ runs over all the maximal regular left ideals. Now, for the converse, suppose $x \in \bigcap \rho$. Consider the set $S = \{y+yx \mid y \in R\}$. We claim $R = S$. Otherwise, suppose S is a proper subset of R. As it happens, the set S is a left ideal of R. Since $0 \in R$, then $0+0x = 0 \in S$. Next, assume $a \in S$, then $\exists c \in R$ so that $a = c + cx$. Since $c \in R$, then $-c \in R$, meaning $(-c) + (-c)x \in S$. Of course, $(-c) + (-c)x = -c - cx = -(c + cx) = -a$, so $-a \in S$. Moreover, if a and b belong in S, say $a = c + cx$ and $b = d + dx$ for some c, $d \in R$, then $a+b = (c+cx)+(d+dx) = (c+d)+(c+d)x \in S$ and $ab = a(d+dx) = (ad)+(ad)x \in S$ (Note this last part shows both closure under multiplication and the general ideal of how S is a left ideal). Therefore, S is a left ideal of R. Furthermore, since $r - r(-x) \in S$ for all $r \in R$, then S is regular. By Lemma 3.1.1, since S is a proper regular left ideal of R, S is contained in a maximal regular left ideal ρ_0. Now, since $\bigcap \rho$ is the intersection of all the maximal regular left ideal of R and ρ_0 is a maximal regular left ideal of R, then we see that $x \in \rho_0$. However, since $y + yx \in \rho_0$ ($S \subset \rho_0$) and $yx \in \rho_0$ (x is in the left ideal ρ_0) for all $y \in R$, then $R \subset \rho_0$. This contradicts ρ_0 being a maximal ideal. Therefore, S is not a proper subset but instead all of R. Now, since $R = \{y + yx \mid y \in R\}$ and $-x \in R$, $\exists w \in R$ so that $-x = w + wx$, or in other words $w + x + wx = 0$. In conclusion, if $x \in \bigcap \rho$, then x is left-quasi-regular. This makes $\bigcap \rho$ a left-quasi-regular left ideal of R, and thus $\bigcap \rho \subset J(R)$ by Lemma 3.3.1. □

Finally, we have a pleasant way to describe the Jacobson radical of a ring. In order to examine the radical of a ring, we must first take note of the ring's maximal regular left ideals. For example, note that since in a division ring the trivial ideal is maximal and regular (D has unity), then every division ring is semi-simple. On the other hand, the next example show why the ring of integers is semi-simple

Example 3.3.3. Since $\mathbb{Z}$ has unity, every ideal of $\mathbb{Z}$ is regular. Now, recall that every maximal ideal of $\mathbb{Z}$ is of the form $p\mathbb{Z}$, where p is a prime number. Moreover, if n and m are integers, then $n\mathbb{Z} \cap m\mathbb{Z} = d\mathbb{Z}$, where d is the least common multiple of n and m. The point being, the intersection of all maximal ideals of $\mathbb{Z}$ is principal and generated by the only common multiple across all prime numbers: 0. Hence, $J(\mathbb{Z}) = (0)$

Let us backtrack a bit. Notice that in the proof, since we showed that both $J(R) = \bigcap \rho$ and that $\bigcap \rho$ is a left-quasi-regular ideal of R, then $J(R)$ is a left-quasi-regular ideal of R. Moreover, by Lemma 3.3.1, $J(R)$ is the biggest (contains every other) left-quasi-regular ideal of R. Hence, we have the next theorem

Theorem 3.3.2. *$J(R)$ is a left-quasi-regular ideal of R and contains all the left-quasi-regular left ideals of R. Moreover, $J(R)$ is the unique maximal left-quasi-regular left ideal of R.*

Now, suppose there are elements a, b and c in a ring R where b is the left-quasi-inverse of a and c is the right-quasi-inverse of a. So, we know $b + a + ba = 0$ and $a + c + ac = 0$. Then, we have $(b + a + ba)c = bc + ac + bac = 0$ and $b(a + c + ac) = ba + bc + bac = 0$. In other words, we get $bc + ac + bac = ba + bc + bac$. Subtract bc and bac from both sides, we get $ba = ac$. Again, since $b + a + ba = 0 = a + c + ac$, subtracting the elements that are equal we get $b = c$. Therefore, if an element has a left and a right quasi-inverse, the two quasi-inverses are the same.

Let us look specifically at the elements of $J(R)$. If $a \in J(R)$, and thus a is left quasi-regular, then there exists $a' \in J(R)$ so that that $a' + a + a'a = 0$. Hence, $a' = -a - a'a \in J(R)$ since $a \in J(R)$. Now, since $a' \in J(R)$, then a' is also left-quasi-regular element and there exists $a'' \in R$ so that $a'' + a' + a''a' = 0$. Since a is the left-quasi-inverse of a' and a'' is the right-quasi-inverse of a', we have by the above paragraph, $a = a''$. Therefore, we can say that a is right-quasi-regular ($0 = a''+a'+a''a' = a+a'+aa'$). As a result, $J(R)$ is a right-quasi-regular ideal of R.

The fact that $J(R)$ is a left-quasi-regular ideal and a right-quasi-regular ideal of R implies that there is only one Jacobson radical. Indeed, if everything we have done thus far is in regards to left modules and left ideals, then we should regard $J(R)$ as the left Jacobson radical. Similarly, if we do the analogues for right modules and right ideals, we would end up with a right Jacobson radical. Denote $J(R)_l$ as the left Jacobson radical and $J(R)_r$ as the right Jacobson radical. Note that the analogue for Lemma 3.3.1 would state that any right-quasi-regular ideal of R is contained in $J(R)_r$. Since we have shown $J(R)_l$ is right-quasi-regular, then $J(R)_l \subset J(R)_r$. Similarly, we could prove that $J(R)_r$ is left-quasi-regular, hence $J(R)_r \subset J(R)_l$. As we all know, this implies $J(R)_l = J(R)_r$, meaning there is only one Jacobson radical! As a last note, we can therefore say that the Jacobson radical is the intersection of all maximal regular right ideals of R.

Another note of interest is an analogy to Lemma 3.2.2 for the Jacobson radical. Lemma 3.2.2 depicts how a module can turn into a faithful module over a different ring. The following theorem shows how one can go from a ring to a semi-simple ring.

Theorem 3.3.3. $J(R/J(R)) = (0)$*; that is,* $R/J(R)$ *is semi-simple.*

Proof. Consider $R/J(R)$ and let ρ be a maximal regular left ideal of R. We know that $J(R) \subset \rho$ by Theorem 3.3.1. Now, we will prove that $\rho/J(R)$ is maximal in $R/J(R)$. Suppose $\rho/J(R) \subset I/J(R) \subset R/J(R)$ and $\rho/J(R) \neq I/J(R)$. Then, consequently $\rho \subset I \subset R$, where $\rho \neq I$. However, since ρ is maximal in R, it implies $I = R$. Hence, $I/J(R) = R/J(R)$, meaning $\rho/J(R)$ is maximal in $R/J(R)$. Moreover, since ρ is left regular in R, $\rho/J(R)$ will also be regular in $R/J(R)$. Say $a \in R$ so that $r - ra \in \rho$, $\forall r \in R$, then $(r + J(R)) - (r + J(R))(a + J(R)) = (r + J(R)) - (ra + J(R)) = (r - ra) + J(R) \in \rho/J(R)$ $\forall r \in R$. In short, the image of all of the maximal regular left ideals of R will remain maximal regular left ideals in $R/J(R)$. However, this does not imply that all of the maximal regular left ideals of $R/J(R)$ come from R. On that note, if $J(R) = \bigcap \rho$, then $(\bigcap \rho)/J(R) = J(R)/J(R) = (0)$ in $R/J(R)$. One thing that we can say is that $(\bigcap \rho)/J(R) = \bigcap(\rho/J(R))$. Let $x + J(R) \in (\bigcap \rho)/J(R)$, then $x \in \bigcap \rho$, so $x + J(R) \in \rho/J(R)$ for all ρ, and thus $x + J(R) \in \bigcap(\rho/J(R))$. On the other hand, let $x + J(R) \in \bigcap(\rho/J(R))$, then $x + J(R) \in \rho/J(R)$ for all ρ. Moreover, if $x + J(R) \in \rho/J(R)$ for each ρ, then $x \in \rho$ for each ρ: Say $x + J(R) = r + J(R)$ for some $r \in \rho$, then $x - r \in J(R) \subset \rho$; since both $x - r$ and r belong to ρ, then $x \in \rho$. Therefore, $x + J(R) \in \rho/J(R)$ for all ρ implies x is in all ρ and thus $x \in \bigcap \rho$, meaning $x + J(R) \in (\bigcap \rho)/J(R)$. Recalling that $J(R/J(R))$ is the intersection of all maximal regular left ideals of $R/J(R)$, we can show why $R/J(R)$ is a semi-simple ring: $J(R/J(R)) \subset \bigcap(\rho/J(R)) = (\bigcap \rho)/J(R) = (0)$. □

Let us talk about the relation between the two-sided ideals of a ring and the ring's Jacobson radical. Let A be an ideal of a ring R. If A is an ideal of R, then A is a subring of R. So, if A is an ideal of a ring, then A itself is a ring. If that is the case, can we relate the Jacobson radical of A with the Jacobson radical of R? The answer turns out to be quite satisfying, as we see in the following theorem and corollary.

Theorem 3.3.4. *If A is an ideal of R, then $J(A) = A \cap J(R)$.*

Proof. Let A be an ideal of R. Now, let $a \in A \cap J(R)$. So, $a \in J(R)$. Since $J(R)$ is left-quasi-regular, then $\exists b \in R$ so that $b + a + ba = 0$. Solving for b, we get $b = -a - ba$. Since also $a \in A$, an ideal, and $b \in R$, then both ba and $-a$ belong in A, meaning $b = -a - ba \in A$. Explicitly, this shows that $A \cap J(R)$ is a left-quasi-regular ideal of A, therefore $A \cap J(R) \subset J(A)$ by Lemma 3.3.1.

Now, suppose ρ is a maximal regular left ideal of R. Let $\rho_A = \rho \cap A$. If $A \subset \rho$, then $\rho_A = A$, meaning $J(A) \subset \rho_A$. In other words, $J(A)$ is a subset of ρ_A for all maximal regular left ideal ρ of R that contain A. Then, let us examine all of the maximal regular left ideals of R that do not contain A. If $A \not\subset \rho$, then the maximality of ρ forces $A+\rho = R$. That is, since both A and ρ are left ideals of R, then $A + \rho$ is a left ideal of R. Moreover, since $A \not\subset \rho$, then $\exists a \in A$ so that $a \notin \rho$. Since $a \in A$ and $0 \in \rho$, then $a = a + 0 \in A + \rho$. Therefore, ρ is a proper subset of $A + \rho$. As a result, since ρ is a left maximal ideal of R and $A + \rho$ a bigger left ideal than ρ in R, then $A + \rho = R$. Now, we can apply the Second Isomorphism Theorem:

$$R/\rho = \frac{A+\rho}{\rho} \cong \frac{A}{A\cap\rho} = A/\rho_A$$

Now, since R/ρ is simple, then A/ρ_A is simple, making ρ_A a maximal left ideal of A. Moreover, since ρ is regular, $\exists b \in R$ so that $x - xb \in \rho$ for all x in R. Yet, since $b \in R = A+\rho$, $b = a+r$ for some $a \in A$, $r \in \rho$. Then, $x-xb = x-x(a+r) = x-xa-xr \in \rho$. Of course, since $r \in \rho$, $xr \in \rho$, which implies that really $x-xa \in \rho$ for all $x \in R$. Therefore, if we let instead $x \in A$, then we know $x - xa \in \rho$ and also $x - xa \in A$ (A is an ideal, so both x and xa belong in A), meaning $\exists a \in A$ so that $x - xa \in \rho_A$ for all $x \in A$; so ρ_A is a regular left ideal in A specifically. In fact, ρ_A is a maximal regular left ideal of (specifically) A. Therefore, whether $A \subset \rho$ or $A \not\subset \rho$, $J(A) \subset \rho_A$ for all maximal regular left ideals ρ of R. Hence, $J(A) \subset \bigcap \rho_A = (\bigcap \rho) \cap A = J(R) \cap A$. So, $A \cap J(R) \subset J(A)$ and $J(A) \subset A \cap J(R)$, so $A \cap J(R) = J(A)$. □

Corollary 3.3.1. *If R is semi-simple, then so is every ideal of R.*

Proof. If $J(R) = 0$, then $J(A) = J(R) \cap A = (0) \cap A = (0)$, meaning A is semi-simple. □

Chapter 4

Nilpotency, Idempotency, and Artinian Rings

Now that we have covered semi-simple rings, let us move on to Artinian rings. We will see that an Artinian ring is a ring in which every descending chain of ideals becomes stationary. Meaning, there is an ending point to every descending chain of proper ideals. Notice there are two key components for a desending chain of ideals in an Artinian ring: finiteness and stability. Finiteness in the respect that, in a chain of ideals, there is eventually an end to the difference in size of the ideals and a final destination is reached. Stability in the sense that once a certain point is reached, the ideals remain the same thereafter. As we shall see, nilpotency and idempotency respectively exemplify these characteristics and are closely related to Artinian rings.

In this chapter, we will see what nilpotency, idempotency, and Artinian rings have to say about the Jacobson radical. First, we will explore what nilpotency has to do with the Jacobson radical. Next, we will start assuming our ring to be Artinian and see what implications arise. Finally, idempotency will prove to be ever present in Artinian rings. Once we explore these three facets of Artinian rings, we will make our way to the Wedderburn-Artin theorems.

4.1 Nilpotence

Nilpotence, in essence, is to be extinguished by oneself. That is, a nilpotent entity is one that becomes nothing after multiple applications of itself. What this means for ring theory, we observe in the following definition.

Definition 4.1.1. Let R be a ring, then:

(i) $a \in R$ is *nilpotent* if there exists $n \in \mathbb{N}$ such that $a^n = 0$.

(ii) (right, left, two-sided) ideal I is *nil* if all elements of I are nilpotent.

(iii) An ideal J is *nilpotent* if there exists $m \in \mathbb{N}$ such that $J^m = (0)$. It is equivalent to say that there exists $m \in \mathbb{N}$ such that $a_1 a_2 \cdots a_m = 0$, $\forall a_i \in J$.

Out of all the topics outside basic ring theory, nilpotency is the least strange. While studying rings such as $\mathbb{Z}_n$ and $Mat_n(D)$, nilpotent elements have been present.

Example 4.1.1. In $\mathbb{Z}_{p^k}$, clearly $\overline{p}$ is nilpotent. Moreover, any multiple of $\overline{p}$ is also nilpotent.

Example 4.1.2. For any ring R and any positive integer n, any matrix in $Mat_n(R)$ that is either upper triangular or lower triangular is nilpotent.

Lemma 4.1.1. *If a is nilpotent, then a is quasi-regular (left and right).*

Proof. Say $a^m = 0$, construct $b = -a + a^2 - a^3 + ... + (-1)^{m-1}a^{m-1}$. Then, we get that:

$$\begin{aligned} b + a + ba &= \left(-a + a^2 - a^3 + \ldots + (-1)^{m-1}a^{m-1}\right) + a \\ &\quad + \left(-a^2 + a^3 + \cdots + (-1)^{m-2}a^{m-1} + (-1)^{m-1}a^m\right) \\ &= (-1)^{m-1}a^m \\ &= 0 \end{aligned}$$

Similarly:

$$\begin{aligned} a + b + ab &= a + \left(-a + a^2 - a^3 + \ldots + (-1)^{m-1}a^{m-1}\right) \\ &\quad + \left(-a^2 + a^3 + \cdots + (-1)^{m-2}a^{m-1} + (-1)^{m-1}a^m\right) \\ &= (-1)^{m-1}a^m \\ &= 0 \end{aligned}$$

Therefore, a is both left and right quasi-regular. □

Lemma 4.1.1 illustrates the importance of nilpotency. The lemma implies that every nil right or left ideal of a ring R is left or right quasi-regular, thus contained in $J(R)$. On the other hand, if R is semi-simple, then there are no nonzero nil ideals. Similarly, if R is a nil ideal of R, then it is a radical ring.

Example 4.1.3. Recall that in $\mathbb{Z}_{p^k}$, the set $P = \{\overline{pm} \,|\, m \in \mathbb{Z}\}$ contains only nilpotent elements. Additionally, P is an ideal of $\mathbb{Z}_{p^k}$, so P is a nil ideal. Therefore, P itself as a ring is a radical ring (that is, $J(P) = P$).

Lemma 4.1.2. *All nilpotent ideals are nil ideals.*

Proof. Let I be a nilpotent ideal of a ring R and let $m \in \mathbb{N}$ so that $I^m = (0)$. So, if $a \in I$, then $a^m \in I^m$. Hence, $a^m \in (0)$, meaning $a^m = 0$. Thus, every element of I is nilpotent, making I a nil ideal. □

Since all nil ideals are contained in the Jacobson radical of a ring, then all nilpotent ideals are contained in the radical. Thus, if a ring R is semi-simple, then we know there are no nonzero nilpotent (and no nil) ideals. Again, if R is a nilpotent ideal of R, then R is a radical ring.

Example 4.1.4. Let n be a positive integer and consider $\mathbb{Z}_n$. Suppose $n = p_1^{k_1} \cdots p_r^{k_r}$, where p_i are prime numbers and $k_i \geq 1$ for all i. Let $m = p_1 \cdots p_r$, then $\overline{m}$ is nilpotent in $\mathbb{Z}_n$. Particularly, if $k = max\{k_i \,|\, 1 \leq i \leq r\}$, then $m^k = p_1^k \cdots p_r^k = nq$, for some $q \in \mathbb{Z}$. On that note, the ideal $M = \{\overline{ms} \,|\, s \in \mathbb{Z}\}$ is nilpotent since $M^k = (0)$. Again, as a ring, M is a radical ring.

4.2 Artinian Rings

Finally, we can discuss Artinian rings. Artinian rings generalize finite rings as well as rings that are finite-dimensional vector spaces over division rings. In addition, Artinian rings are seen as the duals to Noetherian rings in respect to chains of ideals. Regardless, Artinian rings are those in which any non-empty set of ideals has a minimal element under set containment. We shall show that an Artinian ring is equivalently a ring in which any descending chain of ideals terminates. Afterwards, we shall briefly explore facts about Artinian rings.

Definition 4.2.1. A ring is said to be (left, right) *Artinian* if any non-empty set of (left, right) ideals has a minimal element.

From now on, we shall say Artinian for left Artinian, as we still have many left ideals to deal with. There is a famous, equivalent definition for Artinian rings that we will use frequently. Theorem 4.2.1 illustrates what an Artinian ring means in terms of chains of ideals. In various cases, we will deal with descending chains of ideals. Therefore, Theorem 4.2.1 will be of great use. Also, note that the Axiom of Choice is necessary for the converse of the theorem.

Theorem 4.2.1. *A ring R is Artinian if and only if any descending chain of left ideals of R becomes stationary.*

Proof. Let R be an Artinian ring and let $I_1 \supset I_2 \supset I_3 \supset \cdots$ be a descending chain of left ideals of R. Consider the set $\mathcal{M} = \{I_i\}$ composed of these ideals. Since R is Artinian, then $\mathcal{M}$ has a minimal element I_m. However, if $k > m$, then $I_k \subset I_m$. Hence, $I_i = I_m$ for $i \geq m$.

Now, let R be a ring in which any descending chain of left ideals of R becomes stationary. Let $\mathcal{M}$ be a non-empty set of left ideals of R. Using the Axiom of Choice, pick $I_1 \in \mathcal{M}$. If I_1 is minimal, we are done. So, suppose I_1 is not minimal. Then, we pick $I_2 \in \mathcal{M}$ such that $I_1 \supset I_2$. Again, either I_2 is minimal, or we continue to pick an $I_3 \in \mathcal{M}$ such that $I_2 \supset I_3$. In this manner, suppose we get a chain $I_1 \supset I_2 \supset I_3 \supset \cdots$. Since this chain of left ideals becomes stationary, then there is an m so that $I_m = I_i$ for $i \geq m$. Then, I_m is a minimal element of $\mathcal{M}$. □

Artinian rings posses multiple helpful properties. For this paper, we shall recall a handful of facts that will prove to be invaluable.

Lemma 4.2.1. *If R is a Artinian ring and $I \neq (0)$ is a left ideal of R, then I contains a minimal left ideal of R.*

Proof. Let R be an Artinian ring and let $I \neq (0)$ be a left ideal of R. Let $\mathcal{M}$ be the set of all nontrivial left ideals of R that are contained in I. Of course, $I \subset I$, so $\mathcal{M}$ is not empty. Since $\mathcal{M}$ is a set of left ideals of R and R is Artinian, then there exists a left ideal μ in $\mathcal{M}$ that is minimal in $\mathcal{M}$. To prove that μ is a minimal ideal of R, suppose there exists a left ideal $J \neq (0)$ of R such that $(0) \subset J \subset \mu$. If so, then $J \subset \mu \subset I$ and J being nontrivial left ideal of R implies $J \in \mathcal{M}$. However, if J is a proper subset of μ, then we have a contradiction of μ being a minimal element of $\mathcal{M}$. Hence, $J = \mu$, meaining μ is a minimal left ideal of R. $\square$

Example 4.2.1. Any division ring is Artinian. Recall that every (left, right, two-sided) ideal is either the trivial ideal or the entire ring.

Theorem 4.2.2. *If D is a division ring, then $Mat_n(D)$ is Artinian.*

Proof. Let D be a division ring and let $I_1 \supset I_2 \supset I_3 \supset \cdots$ be a descending chain of left ideals of $Mat_n(D)$. Note that $Mat_n(D)$ is a D-module, meaning $Mat_n(D)$ is a vector space over D. Moreover, if I is a left ideal of $Mat_n(D)$, then I is a left vector subspace of $Mat_n(D)$. By definition of left ideal, we know $I \subset Mat_n(D)$, $0 \in I$ and I is closed under addition. To show I is closed under scalar multiplication, suppose $a \in D$ and $v \in I$. Let e be the $n \times n$ identity matrix, then $av = aev = (ae)v$. Since ae is an element of $Mat_n(D)$ and v belongs to a left ideal of $Mat_n(D)$, then $(ae)v \in I$. Hence, $av \in I$, we have that I is closed under scalar multiplication and thus a left subspace of $Mat_n(D)$. Therefore, the descending chain of left ideals $I_1 \supset I_2 \supset I_3 \supset \cdots$ is also a descending chain of left vector subspaces of $Mat_n(D)$. Of course, every subspace I_i has a basis $\mathcal{B}_i$, and since $Mat_n(D)$ is n^2-dimensional, then we know that both $|\mathcal{B}_1| \geq |\mathcal{B}_2| \geq |\mathcal{B}_3| \geq \cdots$ and $|\mathcal{B}_1| \leq n^2$. Since $\{|\mathcal{B}_1|, |\mathcal{B}_2|, |\mathcal{B}_3|, \cdots\}$ is a set on non-negative integers, it must have a minimal element, say $|\mathcal{B}_m|$. Since, for any $k \geq m$, $|\mathcal{B}_m| = |\mathcal{B}_k|$ ($|\mathcal{B}_m| \leq |\mathcal{B}_k|$ and $|\mathcal{B}_m| \geq |\mathcal{B}_k|$) and $I_m \supset I_k$, I_k as a subspace of equal dimension to I_m implies $I_m = I_k$ for any $k \geq m$. Hence, the descending chain of left ideals $I_1 \supset I_2 \supset I_3 \supset \cdots$ becomes stationary. Therefore, $Mat_n(D)$ is an Artinian ring. $\square$

Lemma 4.2.2. *A homomorphic image of an Artinian ring is Artinian*

Proof. Let R be an Artinian ring and let $f : R \to S$ be a ring homomorphism. We want to show that $f(R)$ is an Artinian ring. Certainly, $f(R)$ is a ring since f is a ring homomorphism. Now, suppose $J_1 \supset J_2 \supset J_3 \supset \cdots$ is a descending chain of left ideals of $f(R)$. Then, we know that $f^{-1}(J_i)$ is a left ideal of R for all i. Moreover, $f^{-1}(J_i) \supset f^{-1}(J_{i+1})$ for all i: if $x \in f^{-1}(J_{i+1})$, then $f(x) \in J_{i+1} \subset J_i$, meaning $x \in f^{-1}(J_i)$. Therefore, $f^{-1}(J_1) \supset f^{-1}(J_2) \supset f^{-1}(J_3) \supset \cdots$ is a chain of descending ideals of R. Since R is Artinian, there exists an ideal I that is minimal in the chain. In other words, I is a left ideal of R and $I \subset f^{-1}(J_i)$ for all i. On that note, we can see that $f(I) \subset J_i$ for all i. Let $x \in f(I)$ with $x = f(a)$, for some $a \in I$. Since $I \subset f^{-1}(J_i)$ for all i, then $a \in f^{-1}(J_i)$ for all i. Therefore, $f(a) \in J_i$, meaning $x \in J_i$. Lastly, in order to claim $f(I)$ is the minimal element in the descending chain, we must be sure that $f(I)$ is an ideal of $f(R)$. Of course, I being a subring of R makes $f(I)$ a subring of $f(R)$. Now, let $f(r) \in f(R)$ and $f(i) \in f(I)$, then $f(r)f(i) = f(ri) \in f(I)$ since $ri \in I$. Hence, $f(I)$ is a left ideal of $f(R)$, making $f(I)$ the minimal element in the chain $J_1 \supset J_2 \supset J_3 \supset \cdots$. □

Recall that in the previous section, we discovered that all nilpotent ideals of a ring R are contained in the Jacobson radical $J(R)$. Mainly, we noted that all nilpotent ideals are nil ideals and all nil ideals are quasi-regular ideals. In turn, not only did $J(R)$ contain all of the quasi-regular ideals of R, but $J(R)$ itself was quasi-regular. Similarly, since we know that $J(R)$ contains all nil and nilpotent ideals, can we say that $J(R)$ is either of them?

Theorem 4.2.3. *If R is Artinian, then $J(R)$ is nilpotent.*

Proof. Let $J = J(R)$; consider the descending chain of left ideals $J \supset J^2 \supset \ldots \supset J^n \supset \ldots$. Since R is Artinian, there is an integer n such that $J^n = J^{n+1} = \ldots = J^{2n} = \ldots$. We want to prove that $J^n = (0)$; so, assume that $J^n \neq (0)$. Let $W = \{x \in J \mid J^n x = (0)\}$; we will show W is an ideal of R. First, $0 \in J$ (since J is an ideal) and $j0 = 0$, $\forall j \in J^n$, so $0 \in W$. Next, suppose that $a \in J$ and $ja = 0$, $\forall j \in J^n$. Then, $-a \in J$ and $j(-a) = -ja = -0 = 0$, $\forall j \in J^n$, meaning $-a \in W$. Next, let a, $b \in W$; then, $j(a+b) = ja+jb = 0+0 = 0$ and $j(ab) = (ja)b = 0b = 0$, $\forall j \in J^n$. Of course, J an ideal implies both $a+b$ and ab belong to J, so W is closed under addition and multiplication. Now, suppose $r \in R$ and $w \in W$ and consider both rw and wr. Since $w \in J$, both rw and wr belong to J. Now, let $j \in J^n$; then, $jrw = (jr)w = 0$ and $jwr = (jw)r = 0r = 0$ ($j \in J^n$, an ideal, implies $jr \in J^n$, thus w annihilates it). Therefore, W is an ideal. Now, if $J^n \subset W$, then $J^n J^n = (0)$; meaning, $J^n = J^{2n} = J^n J^n = (0)$, proving our statement. So naturally, consider the case in which $J^n \not\subset W$. If so, then R/W is a ring and $J^n/W \neq (0)$ is an ideal.

Now, consider the elements $x+W$ such that $(J^n/W)(x+W) = (0)$. If $(J^n/W)(x+W) = (0)$, then $(j+W)(x+W) = W$ for all $j \in J^n$. In other words, $jx \in W$ for all $j \in J^n$, therefore, we can say $J^n x \subset W$. Consequently, we can deduce $(0) = J^n(J^n x) = J^n J^n x =$

$J^{2n}x = J^n x$, placing x in W. Therefore, if $(J^n/W)(x+W) = (0)$, then $x+W = 0+W$, the zero element of R/W.

Finally, since $J^n/W \neq (0)$ and R/W the homomorphic image of an Artinian ring, Lemma 4.2.1 implies that there exists a minimal left ideal μ of R/W contained in J^n/W. However, μ being a minimal left ideal of R/W implies that μ is a simple R/W-module and thus annihilated by $J(R/W)$. Additionally, $J^n/W \subset J(R/W)$: If $a \in J^n$, then $a \in J(R)$, so there exists $b \in R$ so that $b + a + ba = 0$. Hence, $(b+W)+(a+W)+(b+W)(a+W) = (b+a+ba)+W = 0+W \in R/W$, meaning that J^n/W is a left-quasi-regular ideal of R/W and thus a subset of $J(R/W)$. That being said, since $J^n/W \subset J(R/W)$ and μ is a simple R/W-module, then $(J^n/W)\mu = (0)$. From the last line of the paragraph above, this implies that every element of μ is the zero element, contradicting μ being a minimal left ideal (minimal ideals are nonzero ideals). Therefore, $J^n = (0)$ and thus $J(R)$ is nilpotent. □

While we have seen that every nilpotent ideal is a nil ideal, the converse is not always true. However, if a nil ideal is an ideal of an Artinian ring, then Theorem 4.2.3 shows why such an ideal must also be nilpotent.

Corollary 4.2.1. *If R is Artinian, then any nil ideal of R is nilpotent.*

Proof. Let I be a nil one-sided ideal. Since every element of I is nilpotent, then by Lemma 4.1.1 every element of I is quasi-regular. Hence, $I \subset J(R)$. Now, since R is Artinian, $J(R)$ is nilpotent; let $m \in \mathbb{N}$ such that $(J(R))^m = (0)$. Hence, all there is left to do is prove $I^m \subset (J(R))^m$. Let $x \in I^m$ with $x = a_1 a_2 \ldots a_m$, where $a_i \in I$ for $i = 1, 2, \ldots, m$. Since $I \subset J(R)$, then we can say $x = a_1 a_2 \ldots a_m$, with $a_i \in J(R)$ for $i = 1, 2, \ldots, m$. Hence, $x \in (J(R))^m$. So, $I^m \subset (J(R))^m \subset (0)$, so I^m is nilpotent. □

4.3 Idempotency

Idempotent elements are those which remain unchanged when raised to a higher power. Mainly, as we may notice, the square of an element need only be itself in order to have the element to be idempotent. In any case, since idempotent elements are ever present in Artinian rings, we shall prove some valuable theorems involving idempotent elements. But first, let us look at the definition, and some examples, of idempotent elements.

Definition 4.3.1. An element $e \neq 0$ in R is an *idempotent* if $e^2 = e$.

Example 4.3.1. In $\mathbb{Z}_{10}$, both $\overline{5}$ and $\overline{6}$ are idempotent.

Example 4.3.2. Let D be a division ring and consider $Mat_n(D)$ for $n > 1$. Let E_{xy} be the $n \times n$ matrix with $e_{xy} = 1$ and all other entries equal to zero $(1 \leq x, y \leq n)$. Then, not only are all E_{ii} idempotent, but also $E_{11} + E_{nn}$. For a concrete example, in $Mat_2(\mathbb{Z})$, any matrix such that $a_{11} = a_{12} = k$ and $a_{21} = a_{22} = 1 - k$ for $k \in \mathbb{Z}$ is idempotent.

Lemma 4.3.1. *Let R be a ring having no nonzero nilpotent ideals. Suppose that $\mu \neq (0)$ is a minimal left ideal of R. Then $\mu = Re$ for some idempotent $e \in R$.*

Proof. Suppose R is a ring having no non-zero nilpotent ideals and suppose that $\mu \neq (0)$ is a minimal left ideal of R. Since R has no non-zero nilpotent ideal and $\mu \neq (0)$, then we know $\mu^2 \neq (0)$. So, it is safe to say that there exists $x \in \mu$ so that $\mu x \neq (0)$. Moreover, μx is a left ideal of R. First, since μ is a left ideal, $0 \in \mu$, therefore $0x = 0 \in \mu x$, so μx is non-empty. Second, suppose $a \in \mu x$ with $a = mx$, where $m \in \mu$, then $-m \in \mu$ and thus $(-m)x = -mx = -a \in \mu x$, so μx has inverses. Third, suppose $a, b \in \mu x$ with $a = mx$, $b = nx$ $(m, n \in \mu)$, then $a + b = mx + nx = (m + n)x \in \mu x$ $(m + n \in \mu)$. Moreover, $ab = (mx)(nx) = ((mx)n)x \in \mu x$ since $n \in \mu$ (a left ideal) implies $(mx)n \in \mu$ (this last part shows also why μx is a left ideal of R). Additionally, since $x \in \mu$, then $mx \in \mu$ for all $m \in \mu$, meaning $\mu x \subset \mu$. Since $\mu x \subset \mu$, $\mu x \neq (0)$, then μ being a minimal ideal of R implies $\mu x = \mu$. Therefore, since $x \in \mu$, there exists an element $e \in \mu$ so that $x = ex$. On that note, by multiplying e on the left, we get $ex = e^2x$; in other words, $(e^2 - e)x = 0$. Consider the set $C = \{c \in \mu \,|\, cx = 0\}$; C is a left ideal of R. First, $0 \in \mu$ and $0x = 0$, so $0 \in C$. Second, let $c \in C$. Then, $cx = 0$ implies $(-c)x = -cx = -0 = 0$. Of course, $c \in C$ implies $c \in \mu$, so $-c \in \mu$; Hence, C has inverses. Third, let $c, d \in C$, then $c + d \in \mu$ and $(c + d)x = cx + dx = 0 + 0 = 0$, so $c + d \in C$. Lastly, let $r \in R$ and $c \in C$, then $c \in \mu$ implies $rc \in \mu$ and $(rc)x = r(cx) = r0 = 0$, so C is a left ideal of R. By definition, $C \subset \mu$. Since μ is a minimal left ideal, either $C = \mu$ or $C = (0)$. However, if $C = \mu$, then it would imply $\mu x = (0)$. Of course, $\mu x \neq (0)$, so $C \neq \mu$. Thus, $C = (0)$. Since $e^2 - e \in C$, then $e^2 - e = 0$, so $e^2 = e$. Also, since $\mu x \neq (0)$, we can be sure that $x \neq 0$. Consequently, since $ex = x \neq 0$, we can be sure that $e \neq 0$. We conclude that e is an idempotent of R. Now, consider the left principal ideal Re. If $re \in Re$, since $e \in \mu$, then $re \in \mu$; so, $Re \subset \mu$. Again, μ being a minimal ideal of R implies $Re = (0)$ or $Re = \mu$.

Still, since $e \in \mu$ and $\mu \subset R$, we can say $ee = e^2 = e \in Re$; since $e \neq 0$, then $Re \neq (0)$. Thus, $Re = \mu$ for some idempotent e in R. □

There are a few things to note about the previous lemma. First, recall that a semi-simple ring is a ring that has no nonzero nilpotent ideals. Hence, we can apply Lemma 4.3.1 to any semi-simple ring. Furthermore, since any nonzero left ideal of an Artinian ring contains a minimal left ideal, we shall take full advantage of this lemma for the structure of semi-simple Artinian rings. As for rings that are Artinian but not semi-simple, there is a theorem that guarantees the existence of idempotent elements on nonzero left ideals. First, however, we must prove the following peculiar lemma.

Lemma 4.3.2. *Let R be a ring and suppose that for some $a \in R$, $a^2 - a$ is nilpotent. Then either a is nilpotent or, for some polynomial $q(x)$ with integer coefficients, $e = aq(a)$ is a non-zero idempotent.*

Proof. Let R be a ring and suppose that for some $a \in R$, $k \in \mathbb{N}$, $(a^2 - a)^k = 0$. Expanding $(a^2 - a)^k = a^{2k} + \ldots + (-a)^k = 0$ and solving for a^k, we get $a^k = a^{k+1}p(a)$, where $p(x)$ has integer coefficients. Of course, $a^{k+1} = a^k a$, then $a^k = a^{k+1}p(a) = a^k ap(a) = (a^{k+1}p(a))ap(a) = a^{k+2}p(a)^2$. Therefore, repeating this process, eventually we get that $a^k = a^{2k}p(a)^k$. Now, either $a^k = 0$ or $a^k \neq 0$. However, if $a^k = 0$, then by definition a is nilpotent. So, suppose $a^k \neq 0$, then $e = a^k p(a)^k \neq 0$ and $e^2 = a^{2k}p(a)^{2k} = (a^{2k}p(a)^k)p(a)^k = a^k p(a)^k = e$. Say $q(a) = a^{k-1}p(a)^k$, then e is the non-zero idempotent we were looking for. □

Theorem 4.3.1. *If R is an Artinian ring and $I \neq (0)$ is a non-nilpotent left ideal of R, then I contains a non-zero idempotent element.*

Proof. Let R be an Artinian ring and $I \neq (0)$ be a non-nilpotent left ideal of R. By Theorem 4.2.3, I being non-nilpotent implies $I \not\subset J(R)$. Consider the ring $R/J(R)$. By Theorem 3.3.3, we know $R/J(R)$ is semi-simple; Thus, $R/J(R)$ contains no non-zero nilpotent ideals. Now, since $I \not\subset J(R)$, then $I/J(R) \neq (0)$. Moreover, since $R/J(R)$ is the image of an Artinian ring and $I/J(R)$ is a non-zero ideal, then there is a minimal ideal $\mu/J(R)$ inside of $I/J(R)$. Consequently, since $R/J(R)$ has no non-zero nilpotent ideals and $\mu/J(R)$ is minimal in $R/J(R)$, then there is an idempotent element $e' + J(R) \in \mu/J(R)$. Let $a \in \mu$ map onto $e' + J(R)$; then $a^2 - a$ maps onto $(e' + J(R))^2 - (e' + J(R)) =$

$((e')^2 - e') + J(R) = J(R)$, meaning $a^2 - a \in J(R)$. Therefore, Since R being Artinian makes $J(R)$ nilpotent, then $a^2 - a$ is nilpotent. By Lemma 4.3.2, either a is nilpotent or $e = aq(a)$ is an idempotent element. Suppose that for some $k \in \mathbb{N}$, $a^k = 0$, then $a^k + J(R) = 0 + J(R)$. However, $J(R) = a^k + J(R) = (a + J(R))^k = (e' + J(R))^k = e' + J(R)$ contradicts $e' + J(R)$ as being idempotent. Thus, a is not nilpotent. Since $e = aq(a)$ is an idempotent and $a \in \mu$, then $e \in \mu$. Finally, $\mu/J(R) \subset I/J(R)$ implies $\mu \subset I$. Hence, $e \in I$ is an idempotent contained in I. □

The last result of this chapter will be used to find minimal ideals. The more we progress, the more is evident that minimal ideals are becoming integral to the study of semi-simple Artinian rings. Still, the following theorem will be used mainly in our conclusion chapter and will allow us to test and find minimal ideals by using idempotent elements.

Theorem 4.3.2. *Let R be a ring having no nonzero nilpotent ideals and suppose that e is an idempotent element in R. Then, Re is a minimal left ideal of R if and only if eRe is a division ring.*

Proof. Let R be a ring having no nonzero nilpotent ideals and suppose Re is a minimal left ideal of R with e being idempotent. First, we can see that eRe is a ring with unity e. First, $e0e = 0 \in eRe$. Second, if $eae \in eRe$, then $e(-a)e = -eae \in eRe$. Third, if eae, $ebe \in eRe$, then $eae + ebe = e(ae + be) = e((a + b)e) = e(a + b)e \in eRe$ and $(eae)(ebe) = eae^2be = e(aeb)e \in eRe$. To show e is the multiplicative identity of eRe, surely $eee = e \in eRe$ and for any $eae \in eRe$, we have $e(eae) = e^2ae = eae = eae^2 = (eae)e$. Lastly, to prove eRe is a division ring, consider a nonzero element $eae \in eRe$. Obviously, $Reae$ is a principal left ideal of R. Now, note that $Reae \subset Re$: if $reae \in Reae$, then since $rea \in R$, we get $(rea)e \in Re$. Moreover, since $e \in R$, then $e(eae) = eae \in Reae$, meaning $Reae \neq (0)$. Since $Reae$ is a nonzero left ideal inside the minimal left ideal Re, then $Re = Reae$. Since $e = ee \in Re$, there exists $b \in R$ so that $e = beae$. Upon further calculation, we see that $e^2 = ebeae$, meaning $e = (ebe)(eae)$. Therefore, eae has a multiplicative inverse, which means eRe is a division ring.

Now, for the converse, suppose R is a ring that has no nonzero nilpotent ideals and e an idempotent of R with eRe being a division ring. To prove Re is a minimal left ideal, suppose $\mu \subset Re$ and $\mu \neq (0)$. If $e\mu = (0)$, then we can see that $\mu^2 = \mu\mu \subset$

$(Re)\mu = (0)$, meaning μ is a nonzero nilpotent ideal of R, contradicting the hypothesis. So, $e\mu \neq (0)$. On that note, since $e\mu \neq (0)$, there must be some $m \in \mu$ such that $em \neq 0$. Since $\mu \subset Re$, then $m \in Re$. Consequently, $em \in eRe$. Since $em \neq 0$ and eRe is a division ring, there must be a multiplicative inverse $ese \in eRe$ so that $(ese)(em) = e$. Upon close inspection, we can see that $e = (esee)m \in Rm$ and also since $m \in \mu$, a left ideal, then $Rm \subset \mu$. In short, e belongs to μ. Since $e \in \mu$, then $Re \subset \mu$. Therefore, $\mu = Re$, so Re is a minimal ideal of R. □

Corollary 4.3.1. *If R has no nonzero nilpotent ideals and if e is an idempotent in R, then Re is a minimal left ideal of R if and only if eR is a minimal right ideal of R.*

Proof. Since the right analogue of Theorem 4.3.2 holds, we can say that eR is a minimal right ideal if and only if eRe is a division ring. Thus, Re being a minimal ideal of R is logically equivalent to eR being a minimal ideal of R. □

Example 4.3.3. Since $\mathbb{Z}_{10}$ is unitary, every ideal of $\mathbb{Z}_{10}$ is regular. By intersecting the only two maximal ideals of $\mathbb{Z}_{10}$, $\langle\overline{2}\rangle$ and $\langle\overline{5}\rangle$, we see that $\mathbb{Z}_{10}$ is semi-simple. Therefore, $\mathbb{Z}_{10}$ has no nonzero nilpotent ideals. Of course, since there are a finite number of ideals, $\mathbb{Z}_{10}$ is Artinian. Recall that $\overline{6} \in \mathbb{Z}_{10}$ is idempotent. We can see that $\overline{6}\mathbb{Z}_{10} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ is a principal ideal of $\mathbb{Z}_{10}$ and is minimal since $|\overline{6}\mathbb{Z}_{10}| = 5$, a prime number. Therefore, $\overline{6}\mathbb{Z}_{10}\overline{6}$ is a division ring. In fact, since $\mathbb{Z}_{10}$ is commutative, $\overline{6}\mathbb{Z}_{10}\overline{6} = \overline{6}\mathbb{Z}_{10}$ is a field with $\overline{6}$ as its unity.

Example 4.3.4. Let D be a division ring and let $R = Mat_n(D)$ with $n > 1$. For each k so that $1 \leq k \leq n$, $I_k = \{(a_{ij}) \in R \,|\, a_{ij} = 0 \text{ for } j \neq k\}$. Recall that matrix E_{kk} is idempotent in R. Moreover, $I_k = R(E_{kk})$ for all k. Since $I_k^2 \neq (0)$ for any k, we have that I_k is a minimal ideal of R if and only if $(E_{kk})R(E_{kk})$ is a division ring. As it turns out, $(E_{kk})R(E_{kk}) = \{cE_{kk} \,|\, c \in D\}$ is a division ring; E_{kk} is the unity of $(E_{kk})R(E_{kk})$, and if $cE_{kk} \neq 0$, then $c \neq 0$, so there exists $d \in D$ such that $cd = 1$, then $dE_{kk} \in (E_{kk})R(E_{kk})$ and $(cE_{kk})(dE_{kk}) = E_{kk}$. Hence, I_k is a minimal ideal for all k.

Chapter 5

Wedderburn-Artin Theorems

Finally, we have arrived at the main purpose of this paper. The first Wedderburn-Artin theorem illustrates the structure of semi-simple Artinian rings. As a result, all theorems leading to it will be about semi-simple Artinian rings. The second Wedderburn-Artin theorem demontrates the structure of simple Artinian rings. As for the theorems leading to it, primitivity will play an important role.

5.1 Semi-simple Artinian Rings

First, we will establish the fact that every left ideal of a semi-simple Artinian ring is principal and generated by an idempotent element. This is an improvement from Theorem 4.3.1. In addition, the two corollaries that follow Theorem 5.1.1 will detail important information about two-sided ideals of semi-simple Artinian rings.

Theorem 5.1.1. *Let R be a semi-simple Artinian ring and $I \neq (0)$ is a left ideal of R. Then, $I = Re$ for some idempotent $e \in R$.*

Proof. Let R be a semi-simple Artinian ring and $I \neq (0)$ be a left ideal of R. Since R is semi-simple, I is not nilpotent. Moreover, since I is a non-zero non-nilpotent left ideal of R, by Theorem 4.3.1, there exists an idempotent e in I. Let $A(e) = \{x \in I \,|\, xe = 0\}$, we will show $A(e)$ is a left ideal of R. Of course, $0 \in I$ and $0e = 0$, so $0 \in A(e)$. Next, say $a \in A(e)$, then $-a \in I$ and $(-a)e = -ae = -0 = 0$, so $-a \in A(e)$. Also, if a, $b \in A(e)$, then $a + b \in I$ and $(a + b)e = ae + be = 0 + 0 = 0$, so $a + b \in A(e)$. Finally, suppose $r \in R$ and $a \in A(e)$, then $ra \in I$ and $(ra)e = r(ae) = r0 = 0$, so $ra \in A(e)$. Now, consider the set $\mathcal{M} = \{A(e) \,|\, e^2 = e \neq 0 \text{ and } e \in I\}$, the set of all $A(e)$ for idempotent elements e from I. Since we know there is at least one idempotent element in I, then $\mathcal{M}$ is a non-empty set of left ideals of R. Since R is Artinian, $\mathcal{M}$ has a minimal element $A(e_0)$.

Suppose $A(e_0) \neq (0)$. As a nonzero, nonnilpotent left ideal of the semi-simple Artinian ring R, $A(e_0)$ must have an idempotent e_1. By the definition of $A(e_0)$, $e_1 \in I$ and $e_1 e_0 = 0$. Consider the element $e^* = e_0 + e_1 - e_0 e_1$. Not only is $e^* \in I$, but e^* is idempotent:

$$\begin{aligned}(e^*)^2 &= (e_0 + e_1 - e_0 e_1)(e_0 + e_1 - e_0 e_1)\\ &= [(e_0)^2 + e_1 e_0 - e_0 e_1 e_0] + [e_0 e_1 + (e_1)^2 - e_0 (e_1)^2] + [-(e_0)^2 e_1 - e_0 e_1 e_0 + e_0 e_1 e_0 e_1]\\ &= [e_0 + (0) - e_0(0)] + [e_0 e_1 + e_1 - e_0 e_1] + [-e_0 e_1 - e_0(0) + e_0(0) e_1]\\ &= e_0 + e_1 - e_0 e_1.\\ &= e^*\end{aligned}$$

Moreover, $e_1 e^* = e_1(e_0 + e_1 - e_0 e_1) = e_1 \neq 0$, So se can safely claim $e^* \neq 0$. Since we have proved e^* is an idempotent of I, then $A(e^*)$ belongs to $\mathcal{M}$. Upon close examination, it turns out $A(e^*) \subset A(e_0)$. Let $x \in A(e^*)$, then $x(e_0 + e_1 - e_0 e_1) = 0$. If $x(e_0 + e_1 - e_0 e_1) = 0$, then $x(e_0 + e_1 - e_0 e_1)e_0 = 0$. However, $x(e_0 + e_1 - e_0 e_1)e_0 = x(e_0)^2 + x e_1 e_0 - x e_0 e_1 e_0 = x e_0$, meaning $x e_0 = 0$, or $x \in A(e_0)$. Moreover, $e_1 e^* = e_1(e_0 + e_1 - e_0 e_1) = e_1 e_0 + (e_1)^2 - e_1 e_0 e_1 = e_1 \neq 0$ implies $e_1 \notin A(e^*)$, so $A(e^*)$ is a proper subset of $A(e_0)$. We have arrived at a contradiction to $A(e_0)$ being a minimal element of $\mathcal{M}$. So, $A(e_0) \neq (0)$ cannot happen.

Now, suppose $A(e_0) = (0)$. Note that for any $x \in I$, $(x - x e_0) e_0 = x e_0 - x(e_0)^2 = x e_0 - x e_0 = 0$, meaning $x - x e_0 \in A(e_0) = (0)$. This would imply $x = x e_0$ for all $x \in I$. Therefore, $I = I e_0 \subset R e_0$. However, $e_0 \in I$, a left ideal of R, implies $R e_0 \subset I$. Therefore, $I = R e_0$ for some idempotent e_0. □

Corollary 5.1.1. *If R is semi-simple Artinian ring and $A \neq (0)$ is an ideal of R, then $A = Re = eR$, for some idempotent e in the center of R.*

Proof. Suppose R is a semisimple Artinian ring and $A \neq (0)$ is an ideal of R. Since A is an ideal, then certainly it is a left ideal. Hence, by the previous theorem, $A = Re$ for some idempotent element e in R. Note that if $x \in A$, then $xe = x$: if $x \in A$, then

$x = re$ for some $r \in R$, meaning $xe = (re)e = re^2 = re = x$. Now, consider the right ideal $B = \{x - ex \,|\, x \in A\}$. Clearly, $e(x - ex) = ex - e^2x = ex - ex = 0$ for all $x \in A$, so $eB = (0)$. Therefore, $AB = ReB = R(0) = (0)$. Consequently, $B \subset A$ implies $B^2 \subset AB = (0)$, so $B^2 = (0)$. Since R is semi-simple and B is nilpotent, then $B = (0)$. Hence, $x - ex = 0$ implies $x = ex$ for all $x \in A$. Therefore, if $x \in A$, then $x = ex \in eR$, so $A \subset eR$. Of course, since $e \in R$, $ee = e \in Re$; yet $e \in A$, A an ideal, implies $eR \subset A$. Thus, $A = eR$ as desired.

Note that we have $ex = x = xe$ for all $x \in A$, meaning e is a unity for A. To prove that e is in the center of R, let $y \in R$. Since $ye \in A$ and e is a unity for A, then surely $e(ye) = ye$. Similarly, $ey \in A$ and e a unity for A implies $(ey)e = ey$. Therefore, for all $y \in R$, $ey = eye = ye$, so e is in the center of R. □

Corollary 5.1.2. *A semi-simple Artinian ring has a two-sided unit element.*

Proof. A ring R is also an ideal of R. Therefore, as we have seen from the previous corollary, there is a multiplicative identity element in the ideal R for all of the elements of R. In other words, R has unity. □

In order to tackle the First Wedderburn-Artin theorem, we will use the notion of a *Peirce decomposition*. As we have shown, semi-simple Artinian rings always contain a two-sided unit element. Suppose we have an idempotent element e not equal to 1. Then for any element x of a ring R, we can say $x = 1x = 1x + xe - xe = xe + x(1 - e)$; in other words, $R = Re + R(1 - e)$. As it will turn out, the sum between Re and $R(1 - e)$ is a direct sum; that is, $Re \bigcap R(1 - e) = (0)$. This is a Peirce decomposition. Let us observe the statement and the proof before I give everything away in this paragraph.

Lemma 5.1.1. *An ideal of a semi-simple Artinian ring is a semi-simple Artinian ring*

Proof. Let R be a semi-simple Artinian ring and $A \neq (0)$ be an ideal of R. Of course, A is a ring in its own right. Moreover, by Corollary 3.3.1, R being semi-simple makes A a semi-simple ring. Now, all there is to do is show A is Artinian.

Since R is a semi-simple Artinian ring and $A \neq (0)$ is an ideal, we know by Corollary 5.1.1 that $A = Re$ for an idempotent e in the center of R. Moreover, we know R has unity $1 \in R$. Suppose $x \in R$, then $x = 1x + xe - xe = xe + (1 - e)x$; therefore, $R = Re + R(1 - e)$. Note that $1 - e$ is in the center of $R: r(1 - e) = r1 - re = 1r - er =$

$(1-e)r$, $\forall r \in R$. Of course, $R(1-e)$ is an ideal (principal) of R. Next, we will show $Re \cap R(1-e) = (0)$. Suppose $x \in Re \cap R(1-e)$. Note that if $x \in Re \cap R(1-e)$, then $x = re$ and $x = s(1-e)$ for some r, $s \in R$. Therefore, $xe = (re)e = re^2 = re = x$ and $xe = [s(1-e)]e = s(e-e^2) = s(0) = 0$, then $x = 0$. So, if $x \in Re \cap R(1-e)$, then $x = 0$ and so $Re \cap R(1-e) = (0)$. Hence, R is the direct sum of ideals A and $R(1-e)$. Now, we can apply the Second Isomorphism Theorem:

$$R/R(1-e) = \frac{A+R(1-e)}{R(1-e)} \cong \frac{A}{A \cap R(1-e)} = A/(0) \cong A$$

Since A is isomorphic to $R/R(1-e)$, as a homomorphic image of the Artinian ring R, A is Artinian. □

To tackle the first Wedderburn-Artin theorem, we shall use a Peirce decomposition over and over until we cannot longer do so. Note that minimal ideals always exist in Artinian rings. For a ring R, since R is an ideal of R, either R is minimal or it contains a minimal ideal. Suppose A is a proper minimal ideal of R, then we know there exists an idempotent element e in R so that $A = Re$. Hence, we can see that $R = A \oplus R(1-e)$. Again, since $R(1-e)$ is an ideal of R, either it is simple or there is a minimal ideal inside of it that is also generated by an idempotent element. Suppose we say $R(1-e) = R_1$ and e_1 generates a minimal ideal A_1 in R_1, then $R(1-e) = A_1 \oplus R_1(1-e_1)$. In short, R is starting to decompose as $R = A \oplus A_1 \oplus \ldots$. The ring being Artinian will guarantee that this decomposition does not go on forever. Lastly, it should be noted that these minimal ideals are simple Artinian rings, hence our interest in the structure of simple Artinian rings.

Wedderburn-Artin 1. *A semi-simple Artinian ring is the direct sum of a finite number of simple Artinian rings.*

Proof. Let $A \neq (0)$ be a minimal ideal in a semi-simple ring R. We will show A is a simple ring. Of course, R being semi-simple and $A \neq (0)$ imply $A^2 \neq (0)$. Now, suppose $B \neq (0)$ is an ideal of A, then ABA is an ideal of R and $ABA \subset B$. We can see that ABA is a subset of B since B is an ideal of A, therefore elements of B should absorb elements of A from both the left and the right. However, since B being an ideal of A does not guarantee B to be an ideal of R, we will have to formally show ABA is an ideal of R. Mainly, since ABA is a subgroup of A (Both A and B are ideals of A, so ABA is definitely an ideal of A), and thus a subgroup of R, we need only show that ABA absorbs elements of R both from the left and from the right. Let $r \in R$ and $\sum_{i,j,k} a_i b_j a_k \in ABA$, then $r(\sum_{i,j,k} a_i b_j a_k) = \sum_{i,j,k}(ra_i)b_j a_k \in ABA$ and $(\sum_{i,j,k} a_i b_j a_k)r = \sum_{i,j,k} a_i b_j (a_k r) \in ABA$ since both ra_i and $a_k r$ belong to the ideal A for all i, k.

Now, since A is also a semi-simple Artinian ring by Corollary 5.1.2, there is $1_A \in A$ guaranteeing $ABA \neq (0)$. Hence, by the minimality of A in R, $ABA = A$. Of course, $A = ABA \subset B \subset A$ implies $B = A$, therefore A is a simple ring.

Recall from the Peirce decomposition, $R = A \oplus T_0$, where T_0 is an ideal of R. Of course, T_0 an ideal of R implies T_0 is also a semi-simple Artinian ring by Lemma 5.1.1. Therefore, since T_0 contains a minimal ideal by Lemma 4.2.1, repeat the process and pick a minimal ideal A_1 of R lying in T_0. As we have seen, A_1 is a simple Artinian ring and by Peirce decomposition $T_0 = A_1 \oplus T_1$. Hence, we get $R = A \oplus T_0 = A \oplus A_1 \oplus T_1$. Continuing we get $A = A_0, A_1, \cdots, A_k, \ldots,$ distinct, simple ideals of R, each of which is Artinian, and such that the sums $A_0 + \cdots + A_k$ are all direct. The sum is direct since if $i \neq j$ and $A_i \bigcap A_j \neq (0)$, then $A_i \bigcap A_j$ is an ideal smaller than both A_i and A_j, contradicting their minimality. Lastly, we claim that for some $n \in \mathbb{N}$, $R = A_0 \oplus \cdots \oplus A_n$. That is, eventually we will reach a T_{n-1} that is minimal, making $T_{n-1} = A_n$ and finishing the process. If not, and this process goes on forever, define $R_0 = A_0 \oplus A_1 \oplus \cdots$, $R_1 = A_1 \oplus A_2 \oplus \cdots$, $R_m = A_m \oplus A_{m+1} \oplus \cdots$. Then, $R_0 \supsetneq R_1 \supsetneq \cdots \supsetneq R_m \supsetneq \cdots$ is a descending chain of proper ideals of R that will not stop, contradicting R as Artinian. Thus, it must be that $R = A_0 \oplus \cdots \oplus A_n$ for some n in $\mathbb{N}$. □

Lemma 5.1.2. *If R is a semi-simple Artinian ring and $R = A_1 \oplus \cdots \oplus A_k$ where the A_i are simple, then the A_i account for all the minimal ideals of R.*

Proof. Recall that if A is both an ideal of R and simple, then A is a minimal ideal of R. That is, if $\mu \neq (0)$ is an ideal of R and $\mu \subset A$, then by simplicity, $\mu = A$. Now, let R be a semi-simple Artinian ring and $R = A_1 \oplus \cdots \oplus A_k$, where the A_i are simple. Let $B \neq (0)$ be a minimal ideal of R. Since R is a semi-simple Artinian ring, then we know there exists $1 \in R$. Hence, we know $RB \neq (0)$. Note that $RB = A_1 B \oplus \cdots \oplus A_k B \neq (0)$, so it must be that for some i between 1 and k, $A_i B \neq (0)$. Of course, both A_i, B being ideals of R makes $A_i B$ an ideal of R. Note that since $A_i B \subset A_i$, by the minimality of A_i and $A_i B \neq (0)$, then $A_i B = A_i$. Similarly, $A_i B \subset B$ implies, by the minimality of B, that $A_i B = B$. Thus, $B = A_i$ for some i. □

5.2 Simple Artinian Rings

With everything we have covered up to this point, finding the structure of simple Artinian rings will be swift. For simple Artinian rings, primitivity will make a comeback. Consequently, we shall revisit R-modules; simple, faithful R-modules to be precise. The one topic that will be new in this chapter is *density*. While there is a connection between this use of density and density in the topological sense, density here refers to the ring of endomorphisms over a vector space. Once we reach Jacobson's density theorem, we will be ready to prove the second Wedderburn-Artin theorem.

We shall now start using an alternative definition for primitive rings. Theorem 5.2.1 will give us a definition that only deals in ring theory. Since we have managed to put the Jacobson radical in terms of maximal regular ideals, this new definition connects semi-simplicity with primitivity.

Theorem 5.2.1. *A ring R is primitive $\iff$ $\exists$ maximal regular left ideal $\rho \subset R$ such that $(\rho : R) = (0)$.*

Proof. Suppose R is a primitive ring. Then, by definition, there exists a simple, faithful R-module M. By Theorem 3.1.1, $M \cong R/\rho$ for some maximal regular left ideal ρ. Since $\mathcal{A}(M) = (\rho : R)$ by Proposition 3.2.1 and M is faithful, then $(\rho : R) = (0)$. Hence, there exists a maximal regular left ideal $\rho \subset R$ such that $(\rho : R) = (0)$.

Now, suppose there exists a maximal regular left ideal $\rho \subset R$ such that $(\rho : R) = (0)$. By Theorem 3.1.1, R/ρ is a simple R-module. Of course, since $\mathcal{A}(M) = (\rho : R)$, then R/ρ is faithful. Thus, R is primitive. $\square$

Recall that Proposition 3.2.1 implies $J(R)$ to be the intersection of all $(\rho : R)$ over all maximal regular left ideals ρ. If just one $(\rho : R)$ happened to be the trivial ideal, R would then be semi-simple. In light of the alternative definition for primitivity, we can see that any primitive ring R is therefore semi-simple.

Now, we take a moment to observe some facts about primitive rings.

Proposition 5.2.1. *A simple ring which is semi-simple is primitive*

Proof. Suppose a ring R is both simple and semi-simple. Consider the ideals $(\rho : R)$ over all of the maximal regular left ideals ρ of R. By the simplicity of R, either $(\rho : R) = (0)$ or $(\rho : R) = R$ for each ρ. If $(\rho : R) = R$ for every ρ, then $\bigcap_\rho (\rho : R) = J(R) = R$, contradicting R being semi-simple. Thus, for some maximal regular left ideal ρ_0, $(\rho_0 : R) = (0)$. Hence, R is primitive. □

Proposition 5.2.2. *A simple ring R with unity is primitive*

Proof. Let R be a simple ring and say $1 \in R$. Therefore, the trivial ideal (0) is a regular. By Lemma 3.1.1, there exists a maximal regular left ideal ρ in R that contains (0). Therefore, R/ρ is a simple R-module. Moreover, on account of R/ρ being simple, by definition $R(R/\rho) \neq (0)$; thus, $\mathcal{A}(R/\rho) \neq R$. Since R is simple and $\mathcal{A}(R/\rho)$ is an ideal, then $\mathcal{A}(R/\rho) = (0)$. Hence, R/ρ is a simple, faithful R-module. Hence, R is primitive. □

Proposition 5.2.3. *A commutative ring R is primitive if and only if R is a field.*

Proof. Suppose R is a primitive ring and M is a simple, faithful R-module. Then, $A \cong R/\rho$ for some maximal regular left ideal ρ of R. Since R is commutative, ρ is in fact a two-sided ideal and $\rho \subset (\rho : R) = \mathcal{A}(M) = (0)$. Moreover, since $\rho = (0)$ is regular, there exists $e \in R$ such that $r - re \in (0)$ for all $r \in R$. Meaning, $r = re$ for all $r \in R$. Since R is commutative, e is the multiplicative identity of R. Since R is a commutative ring with unity and $\rho = (0)$ is maximal, then $R/(0) \cong R$ is a field.

Conversely, if R is a field, then R is simple and has unity. By the previous proposition, R is primitive. Of course, R being a field means R is commutative. □

Definition 5.2.1. Let M be a (left) vector space over a division ring Δ. A ring R is said to be *dense* on M if for ever $n \in \mathbb{N}$ and $v_1, \cdots, v_n$ in M which are linearly independent over Δ and arbitrary elements $w_1, \cdots, w_n$ in M, there is an element $r \in R$ such that $rv_i = w_i$ for $i = 1, 2, \cdots, n$.

Why are we talking about rings and vector spaces? Recall that whenever we have a simple R-module M, then by Schur's Lemma the set of R-module endomorphisms, denoted as $End_R(M)$, is a division ring. Consequently, M is thus not just an mere $End_R(M)$-module, but a vector space over $End_R(M)$. Hence, we can see an example where the elements of a ring R act on a vector space over a division ring. It is this specific relation between ring, module, and division ring that Jacobson's density theorem explores.

Jacobson's density theorem connects density and primitive rings. Additionally, the second Wedderburn-Artin theorem depends heavily on Jacobson's density theorem.

As a sneak peek, know that it is possible to prove that a simple Artinian ring is semi-simple, and thus by Proposition 5.2.1 it is primitive.

Jacobson Density Theorem. *Let R be a primitive ring and let M be a simple, faithful R-module. If $\Delta = End_R(M)$, then R is a dense ring of linear transformations of M over Δ.*

Proof. Let R be a primitve ring and let M be a simple, faithful R-module. As we have seen, M is a left vector space over $\Delta = End_R(M)$. Let V be a finite-dimensional subspace of M over Δ. We will prove by induction on the dimension of V over Δ that if $V \subset M$ is of finite dimension over Δ and $m \in M$, $m \notin V$, then there exists an $r \in R$ such that $rV = (0)$ but $rm \neq 0$. Suppose that $dim_\Delta(V) = 0$, then $V = (0)$ meaning $m \neq 0$. Hence, since M being simple implies $R(M) \neq (0)$, there exists $r \in R$ such that $rm \neq 0$. Of course, $V = (0)$ implies $rV = (0)$. Therefore, the statement is true for the base case $dim_\Delta(V) = 0$.

Now, suppose $V = V_0 + \Delta w$, where $dim_\Delta(V_0) = dim_\Delta(V) - 1$ and where $w \notin V_0$. By the induction hypothesis, if $\mathcal{A}(V_0) = \{x \in R \,|\, xV_0 = (0)\}$, then for $y \in M$, $y \notin V_0$, there is an $r \in \mathcal{A}(V_0)$ such that $ry \neq 0$; Notice this last fact shows that if $y \notin V_0$, then $\mathcal{A}(V_0)y \neq (0)$ since $r \in \mathcal{A}(V_0)$ and $ry \neq 0$. In particular, since $w \notin V_0$, then $\mathcal{A}(V_0)w \neq (0)$. Recall that by the mere fact that V_0 is a subset of M that $\mathcal{A}(V_0)$ is a left ideal of R. Therefore, we can show $\mathcal{A}(V_0)w$ is a submodule of M. Of course, for any $a \in \mathcal{A}(V_0) \subset R$, $aw \in M$, so $\mathcal{A}(V_0)w \subset M$. First, $0 \in \mathcal{A}(V_0)$ implies $0w = 0 \in \mathcal{A}(V_0)w$. Second, suppose $aw \in \mathcal{A}(V_0)w$ with $a \in \mathcal{A}(V_0)$, then $-a \in \mathcal{A}(V_0)$ and $(-a)w = -(aw) \in \mathcal{A}(V_0)w$. Third, let aw, $bw \in \mathcal{A}(V_0)w$ with a, $b \in \mathcal{A}(V_0)$, then $aw + bw = (a+b)w \in \mathcal{A}(V_0)w$ since $a + b \in \mathcal{A}(V_0)$. Lastly, let $r \in R$ and $aw \in \mathcal{A}(V_0)w$ with $a \in \mathcal{A}(V_0)$, then $\mathcal{A}(V_0)$ being a left ideal of R implies $ra \in \mathcal{A}(V_0)$, meaning $r(aw) = (ra)w \in \mathcal{A}(V_0)w$, thus $\mathcal{A}(V_0)w$ is an R-module. Since we have confirmed $\mathcal{A}(V_0)w$ is a submodule of M, and M is simple, $\mathcal{A}(V_0)w \neq (0)$, we have $\mathcal{A}(V_0)w = M$.

Suppose there is an $m \in M$, $m \notin V$ so that whenever $rV = (0)$ then $rm = 0$; We will show this cannot happen. Let $m \in M$, $m \notin V$, have the property that whenever $rV = (0)$ then $rm = 0$. Since $M = \mathcal{A}(V_0)w$, consider the mapping $\tau : M \to M$ by $\tau(aw) = am$, for all a in $\mathcal{A}(V_0)$. First, we will show τ is well-defined. Say $a_1w = a_2w$ for some a_1, $a_2 \in \mathcal{A}(V_0)$, then $(a_1 - a_2)w = 0$. Note that if $v \in V$ with $v = v_0 + cw$, for some $v_0 \in V_0$ and $c \in \Delta$, then $a_1 - a_2 \in \mathcal{A}(V_0) \subset R$ and $c \in End_R(M)$ imply

$(a_1 - a_2)v = (a_1 - a_2)v_0 + (a_1 - a_2)(cu) = 0 + c[(a_1 - a_2)w] = c0 = 0$. In other words, $(a_1 - a_2)V = (0)$. By m's peculiar property, we have that $(a_1 - a_2)m = 0$. Therefore, $a_1 m = a_2 m$, meaning $\tau(a_1 w) = \tau(a_2 w)$. Hence, τ is a well-defined function. As it turns out, $\tau \in End_R(M)$. Say $aw,\ bw \in M$, then $\tau(aw + bw) = \tau(\,(a+b)w\,) = (a+b)m = am + bm = \tau(aw) + \tau(bw)$. Moreover, let $r \in R$ and $aw \in M$, then $\tau(r(aw)) = \tau((ra)w) = (ra)m = r(am) = r\tau(aw)$. Thus, τ is an R-module homomorphism from M to M. Moreover, Since $\mathcal{A}(V_0) \subset R$, it must be that for any $x \in M$ and any $a \in \mathcal{A}(V_0)$, $\tau(ax) = a\tau(x)$. Therefore, since $am = \tau(aw) = a\tau(w)$, then $a(m - \tau(w)) = 0$ for any $a \in \mathcal{A}(V_0)$, meaning $\mathcal{A}(V_0)(m - \tau(w)) = (0)$. Recall that one way to state our induction hypothesis is that if $y \notin V_0$, then $\mathcal{A}(V_0)y \neq (0)$. Therefore, it is also true to say that if $\mathcal{A}(V_0)y = (0)$, then $y \in V_0$. The point being, if $\mathcal{A}(V_0)(m - \tau(w)) = (0)$, then $(m - \tau(w)) \in V_0$. Hence, $(m - \tau(w)) + \tau w = m \in V_0 + \Delta w = V$, contradicting $m \notin V$. In conclusion, whenever there is an $r \in R$ so that $rV = (0)$, then it must be that $rm \neq 0$ for all $m \in M$, $m \notin V$.

Now that we know we can find an $r \in R$ for any $m \in M$, $m \notin V$, so that $rV = (0)$ but $rm \neq 0$ for any finite dimensional subspace V of M, we can finally finish this proof. Suppose you have arbitrary linearly independent vectors $v_1, \ldots, v_n \in M$ over Δ and arbitrary vectors $w_1, \ldots, w_n$ in M. Let $V_i = span\{v_j \mid j \neq i\}$, then $v_i \notin V_i$ for all i. Hence, we can find $r_i \in R$ so that $r_i v_i \neq 0$ but $r_i V_i = (0)$ for all i. Now, since $r_i v_i \neq 0$, as we have seen before $R(r_i v_i)$ is a nonzero submodule of M, thus $R(r_i v_i) = M$ for all i. In particular, since $w_i \in M$, we can find $s_i \in R$ so that $s_i(r_i v_i) = w_i$ for all i. Let $t_i = s_i r_i$ for all i, then we see that both $t_i v_i = w_i$ and $t_i V = (s_i r_i)V = s_i(r_i V) = s_i(0) = (0)$ for all i. Hence, let $t = t_1 + \cdots + t_n$, then $tv_k = (t_1 + \cdots + t_n)v_k = t_k v_k = w_k$ for all i. Therefore, R is dense on M. □

Finally, we have arrived to the second Wedderburn-Artin theorem. Once we discover the structure of simple Artinian rings, the true nature of semi-simple Artinian rings will be revealed. Without further delay, let us dig into the last Wedderburn-Artin theorem.

Wedderburn-Artin 2. *Wedderburn: Let R be a simple Artinian ring. Then R is isomorphic to $Mat_n D$, for some division ring D and $n \in \mathbb{N}$. Conversely, for any division ring D, $Mat_n D$ is a simple Artinian ring.*

Proof. Let R be a simple Artinian ring. Recall that R being simple implies either $J(R) = (0)$ or $J(R) = R$. Since R is Artinian, $J(R)$ is nilpotent. However, by definition, R a simple ring implies $R^2 \neq (0)$, meaning $R^2 = R$ (R^2 is an ideal of R). Therefore, R is not a nilpotent ideal. Consequently, $J(R)$ cannot be R (if $J(R) = R$, then R is nilpotent), so $J(R) = (0)$. Since R has been shown to be both simple and semi-simple, by Proposition 5.2.1 R is primitive. Let M be a simple, faithful R-module, then M is a left vector space over the division ring $\Delta = End_R(M)$.

We will show M is finite-dimensional over Δ by contradiction. So, suppose that instead $\{v_1, \ldots, v_n, \ldots\}$ is an infinite set of linearly independent vectors over Δ. Let $B_m = \{v_1, \ldots, v_m\}$, then since $B_m \subset M$ for all $m \in \mathbb{N}$, $\mathcal{A}(B_m)$ are all left ideals of R. Moreover, by Jacobson's density theorem, for any $i \in \mathbb{N}$, $\mathcal{A}(B_{i+1}) \subsetneq \mathcal{A}(B_i)$. Of course, if $x \in \mathcal{A}(B_{i+1})$, then $xv_k = 0$ for $k = 1, 2, \ldots, i+1$, meaning $x \in \mathcal{A}(B_i)$. Moreover, since $v_{i+1} \notin span(B_i)$, by density there exists $r \in R$ so that $r(span(B_i)) = (0)$, but $rv_i \neq 0$; in other words, $r \in \mathcal{A}(B_i)$ but $r \notin \mathcal{A}(B_{i+1})$. Therefore, $\mathcal{A}(B_1) \supsetneq \mathcal{A}(B_2) \supsetneq \cdots \supsetneq \mathcal{A}(B_m) \supsetneq \cdots$ is a descending chain of proper left ideals of R that has never stops. This is a contradiction to R being Artinian. Hence, M is finite-dimensional over Δ.

Now that we know M is finite-dimensional over Δ, say $dim_\Delta(M) = n$, we can prove R is isomorphic to $End_\Delta(M)$ and thus isomorphic to $Mat_n(\Delta^{op})$. Let $\{v_1, \ldots, v_n\}$ be a basis for M and define $\Phi : R \to End_\Delta(M)$ with $\Phi(r) = \Phi_r$ and define Φ_r with $\Phi_r(x) = rx$ for all $x \in M$. First, we will show Φ is injective. Suppose $\Phi_a = \Phi_b$, then $ax = bx$ for all $x \in M$. Hence, $(a-b)x = 0$ for all $x \in M$, meaning $a-b \in \mathcal{A}(M)$. However, M is a faithful R-module, so $a - b \in (0)$, hence $a = b$. Next, since R acts densely on M, we can show Φ is surjective. Let $f \in End_\Delta(M)$; recall that a function $f \in End_\Delta(M)$ is defined by the output of the basis elements under f. Since $f(v_i) \in M$ for all i and R is dense in M, there exists $r \in R$ so that $rv_i = f(v_i)$ for all i. Since $\Phi_r(v_i) = f(v_i)$ for all i, Φ_r and f agree with the outputs of the basis elements. Thus $\Phi_r = f$. Hence, for any $f \in End_\Delta(M)$, there exists $r \in R$ so that $\Phi(r) = f$, so Φ is surjective. Now, suppose $a, b \in R$, then $\Phi(a+b) = \Phi_{a+b} = (a+b)x = ax + bx = \Phi_a + \Phi_b = \Phi(a) + \Phi(b)$ and $\Phi(ab) = \Phi_{ab} = (ab)x = a(bx) = \Phi_a(bx) = \Phi_a(\Phi_b) = \Phi_a\Phi_b$ (composition of functions is the multiplication of $End_\Delta(M)$). Hence, Φ is an isomorphism between R and $End_\Delta(M)$, so $R \cong End_\Delta(M)$. Since $Mat_n(\Delta^{op}) \cong End_\Delta(M)$ by Theorem 2.1.1, then $Mat_n(\Delta^{op}) \cong R$. Of course, since Δ is a division ring, so is Δ^{op}. Let $D = \Delta^{op}$, then $R \cong Mat_n(D)$.

Now, for the converse, we will show that for any division ring D, $Mat_n(D)$ is a simple Artinian ring. Of course, by Theorem 4.2.2 we saw that for any division ring D, $Mat_n(D)$ is an Artinian ring. Moreover, by Proposition 2.3.1, $Mat_n(D)$ is a simple ring. Hence, $Mat_n(D)$ is a simple Artinian ring. $\square$

Chapter 6

Implications

It is time we put our theorems to the test. Since the Wedderburn-Artin theorems talk about semi-simple Artinian rings, we shall look at some of those. Mainly, we will observe the impact of these theorems on some finite rings and finite-dimensional group algebras over fields. These two types of rings exemplify the notion of Artinian rings.

First, we will take a look at $\mathbb{Z}_n$. Since $\mathbb{Z}_n$ is finite for all $n \in \mathbb{N}$, it is certainly Artinian. That is, $\mathbb{Z}_n$ has a finite number of elements, thus has a finite number of possible subsets. If the number of subsets is finite, so must the number of ideals. Hence, any chain of ideals will always stabilize. Now, while all $\mathbb{Z}_n$ are all Artinian, not all are semi-simple. Before we dive into theorems about $\mathbb{Z}_n$, let us fist observe one $\mathbb{Z}_n$ that is semi-simple. After we observe this example, we can then see what drives the theorems we shall explore soon after.

Example 6.0.1. Consider the Artinian ring $\mathbb{Z}_{30}$. Since $\mathbb{Z}_{30}$ is commutative and unitary, all left ideals are two-sided and all ideals are regular. Hence, the Jacobson radical of $\mathbb{Z}_{30}$, $J(\mathbb{Z}_{30})$, is the intersection of all the maximal ideals of $\mathbb{Z}_{30}$. The maximal ideals of $\mathbb{Z}_{30}$ are $\langle\overline{2}\rangle$, $\langle\overline{3}\rangle$, and $\langle\overline{5}\rangle$, hence $J(\mathbb{Z}_{30}) = \langle\overline{2}\rangle \cap \langle\overline{3}\rangle \cap \langle\overline{5}\rangle = (0)$, so $\mathbb{Z}_{30}$ is semi-simple. Now, to find minimal ideals, we first find an idempotent element of $\mathbb{Z}_{30}$ and construct a principal ideal with it. To check that is a minimal ideal, we test it using Theorem 4.3.2. Luckily, finding an idempotent element in $\mathbb{Z}_{30}$ proves to not be as difficult as $\overline{6}$ fits the bill. Now, let us observe $\overline{6}\mathbb{Z}_{30} = \langle\overline{6}\rangle = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\}$. As we can see, $\langle\overline{6}\rangle$ is not only minimal, but a field! Now, as we did in First Wedderburn-Artin theorem, we have $\mathbb{Z}_{30} = \overline{6}\mathbb{Z}_{30} \oplus (\overline{1} - \overline{6})\mathbb{Z}_{30}$. Note that $\overline{1} - \overline{6} = \overline{25}$, so we have $\mathbb{Z}_{30} = \overline{6}\mathbb{Z}_{30} \oplus \overline{25}\mathbb{Z}_{30}$. As it becomes evident, $\overline{25}\mathbb{Z}_{30} = \langle\overline{25}\rangle = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}\}$ is not a minimal ideal. Regardless, what we must do is now find a minimal ideal of $\mathbb{Z}_{30}$ inside $\langle\overline{25}\rangle$. Note that $\overline{10}$ is also idempotent in $\mathbb{Z}_{30}$, and $\langle\overline{10}\rangle$ is a minimal ideal of $\mathbb{Z}_{30}$. Hence, if $R_1 = \langle\overline{25}\rangle$, and since $\overline{25}$ is the unity of R_1, then we have that $R_1 = \overline{10}R_1 \oplus (\overline{25} - \overline{10})R_1$. Note that if I is an ideal or a ring R and $e \in I$ is an idempotent element of R, then $eI = eR$: Since $I \subset R$, then $eI \subset eR$. On the other hand, since $e \in I$, $eR \subset I$. Hence, $e(eR) \subset e(I)$; of course, $e(eR) = e^2R = eR$, we have $eR \subset eI$. Hence, we can simply say that $\langle\overline{25}\rangle = \langle\overline{10}\rangle \oplus \langle(\overline{25} - \overline{10})\rangle$ with respect to $\mathbb{Z}_{30}$, not R_1. Finally, $(\overline{25} - \overline{10})R_1 = \langle\overline{15}\rangle$ is also minimal ideal, so we stop the Peirce decomposition on $\mathbb{Z}_{30}$. Therefore, we have $\mathbb{Z}_{30} = \langle\overline{6}\rangle \oplus \langle\overline{10}\rangle \oplus \langle\overline{15}\rangle$, the direct sum of simple (the minimal ideals are fields) Artinian rings.

So, why did $\mathbb{Z}_{30}$ work so nicely? Well, we knew $\mathbb{Z}_{30}$ was Artinian, so that was half the battle. If we also had that it was semi-simple, our theorems should do the rest of the work. Why was $\mathbb{Z}_{30}$ semi-simple?

Lemma 6.0.1. *Let n, $m \in \mathbb{N}$. If m divides n, then $\mathbb{Z}_n/\langle\overline{m}\rangle \cong \mathbb{Z}_m$*

Proof. Let n, $m \in \mathbb{N}$ and say $m|n$, where $n = mq$, $q \in \mathbb{N}$. Consider the map $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ with $\phi(\overline{a}) = \overline{a}$. First, we will show ϕ is well-defined. Suppose $\overline{r}, \overline{s} \in \mathbb{Z}_n$ and $\overline{r} = \overline{s}$. If so, then $r \equiv s \, mod(n)$, meaning $r - s = nk$, where $k \in \mathbb{Z}$. Since $n = mq$, then $r - s = (mq)k = m(qk)$. Thus, $r \equiv s \, mod(m)$, so $\overline{r} = \overline{s}$ in $\mathbb{Z}_m$. Now, suppose $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Recall that in both $\mathbb{Z}_n$ and $\mathbb{Z}_m$, $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a}\overline{b}$. Thus, $\phi(\overline{a} + \overline{b}) = \phi(\overline{a+b}) = \overline{a+b} = \overline{a} + \overline{b} = \phi(\overline{a}) + \phi(\overline{b})$ and $\phi(\overline{a}\overline{b}) = \phi(\overline{ab}) = \overline{ab} = \overline{a}\overline{b} = \phi(\overline{a})\phi(\overline{b})$. Moreover, ϕ is surjective. Let $\overline{y} \in \mathbb{Z}_m$, then consider $\overline{y} \in \mathbb{Z}_n$ and note that $\phi(\overline{y}) = \overline{y}$. Hence, ϕ is a ring homomorphism from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ with $\phi(\mathbb{Z}_n) = \mathbb{Z}_m$. Lastly, $Ker\phi = \{\overline{a} \in \mathbb{Z}_n \,|\, \phi(\overline{a}) = \overline{0}\} = \{\overline{a} \in \mathbb{Z}_n \,|\, m|a\} = \langle\overline{m}\rangle$. Therefore, by the First Isomorphism Theorem, $\mathbb{Z}_n/\langle\overline{m}\rangle \cong \mathbb{Z}_m$. $\square$

Theorem 6.0.1. *If $n = p_1^{k_1} \cdots p_r^{k_r}$, p_i's all distinct primes, then $J(\mathbb{Z}_n) = \langle\overline{p_1 \cdots p_r}\rangle$.*

Proof. Let $n = p_1^{k_1} \cdots p_r^{k_r}$, where the p_i's are all distinct primes. Of course, $\mathbb{Z}_n$ is a unitary commutative ring, so $J(\mathbb{Z}_n)$ is the intersection of all maximal ideal of $\mathbb{Z}_n$ by Theorem 3.3.1. Of course, with Lemma 6.0.1, we can quickly prove that $\langle\overline{p_i}\rangle$ is maximal in $\mathbb{Z}_n$ for all i: $\mathbb{Z}_n/\langle\overline{p_i}\rangle \cong \mathbb{Z}_{p_i}$, so $\mathbb{Z}_n/\langle\overline{p_i}\rangle$ being a field implies $\langle\overline{p_i}\rangle$ is a maximal ideal. Thus, $J(\mathbb{Z}_n) = \langle\overline{p_1}\rangle \cap \cdots \cap \langle\overline{p_r}\rangle$. Now, if $\overline{x} \in \langle\overline{p_1 \cdots p_r}\rangle$, then $\overline{x} = (\overline{p_1 \cdots p_r})\overline{q}$, where $\overline{q} \in \mathbb{Z}_n$. Therefore, $\overline{x} \in \langle\overline{p_i}\rangle$ for every i, thus $x \in \langle\overline{p_1}\rangle \cap \cdots \cap \langle\overline{p_r}\rangle$. Likewise, if $x \in \langle\overline{p_1}\rangle \cap \cdots \cap \langle\overline{p_r}\rangle$, then $x \in \langle\overline{p_i}\rangle$

for all i. If so, then p_i divides x for all i. Hence, $p_1 \cdots p_r$ divides x; say, $x = (p_1 \cdots p_r)t$, for $t \in \mathbb{Z}$. Hence, $\overline{x} = \overline{(p_1 \cdots p_r)t} \in \langle \overline{p_1 \cdots p_r} \rangle$, so $\langle \overline{p_1 \cdots p_r} \rangle = \langle \overline{p_1} \rangle \cap \cdots \cap \langle \overline{p_r} \rangle = J(\mathbb{Z}_n)$, as desired. □

Corollary 6.0.1. *if $n = p_1 \cdots p_r$, p_i all distinct, then $\mathbb{Z}_n$ is semi-simple.*

Proof. Since $\overline{p_1 \cdots p_r} = \overline{0}$ in $\mathbb{Z}_{p_1 \cdots p_r}$, then $J(\mathbb{Z}_{p_1 \cdots p_r}) = \langle \overline{p_1 \cdots p_r} \rangle = (0)$. □

Hence, we have pinpointed which $\mathbb{Z}_n$ are semi-simple. Now that we know which $\mathbb{Z}_n$ to pick, let us step back and analyze our example on $\mathbb{Z}_{30}$ to generalize on how to decompose a semi-simple Artinian $\mathbb{Z}_n$. First, we know from Lemma 5.1.2 that a semi-simple $\mathbb{Z}_n$ will split into direct sums of all its minimal ideals. Particularly, if $n = p_1 \cdots p_r$, then the principal ideals $\langle (\overline{\frac{n}{p_i}}) \rangle$ will be all the minimal ideals of $\mathbb{Z}_n$ (they are all of prime order). With such knowledge beforehand, the Peirce decomposition is no longer necessary for the structure of $\mathbb{Z}_n$.

Let us move on to group algebras. While $\mathbb{Z}_n$ shows how to one might approach finite semi-simple rings in general, group algebras will give us an insight on how to deal with vector spaces over fields. This time around, looking for the order of ideals will be rendered useless as a tactic to spot minimal ideals. Instead, ideas from linear algebra will prove to have a better effect. The reason why we shall explore group algebras as opposed to random vector spaces is the result of *Maschke's Theorem*, which guarantees semi-simplicity. Of course, let us define what a group algebra is and prove a lemma before jumping right into the theorem.

Definition 6.0.1. Let F be a field and let G be a finite group of order n. We define *the group algebra of G over F*, denoted by $F(G)$, as the set $\{\sum_i \alpha_i g_i \,|\, \alpha_i \in F,\, g_i \in G\}$ of formal sums, where the group elements are considered to be linearly independent over F, addition is defined naturally, and multiplication is defined by the distributive laws and with $(\alpha_i g_i)(\beta_j g_j) = \alpha_i \beta_j g_i g_j$.

Lemma 6.0.2. *Let N be a nilpotent linear transformation on a finite-dimensional vector space V over a division ring D. Then, there exists basis $\mathcal{W} = \{w_1, \ldots, w_n\}$ of V such that $N(w_1) = 0$ and $N(w_i) \in Span\{w_1, \ldots, w_{i-1}\}$ for $2 \leq i \leq n$.*

Proof. Let $N \in End_D(V)$ be (non-zero) nilpotent. We will prove the lemma by induction on the dimension of V over D.

Say $dim_D(V) = 1$. Since N is nilpotent in $End_D(V)$, there exists $k \in \mathbb{N}$ so that $N^k = 0$ in $End_D(V)$. Let $M = \{s \in \mathbb{N} \mid N^s = 0\}$; since $k \in M$, as a non-empty subset of the natural numbers, M must have a minimal element m. Note that $m \geq 2$ ($m \neq 1$), or else it contradicts N as a non-zero map. Therefore, we can say $N^{m-1} \neq 0$ in $End_D(V)$. Otherwise, $m - 1 \in M$, contradicting m as the smallest element in M. If $N^{m-1} \neq 0$ in $End_D(V)$, then there must be some $w \in V$ so that $N^{m-1}(w) \neq 0$. Hence, let $w_1 = N^{m-1}(w)$. Since $w_1 \neq 0$, $\mathcal{W} = \{w_1\}$ is a basis for V and $N(w_1) = N(N^{m-1}(w)) = N^m(w) = 0$, as desired.

Now, assuming that we can find such a basis for any vector space with dimension $n-1$ or less, we will show we can do so for a vector space of dimension n. Let V be a vector space of dimension n and basis $\{v_1, \ldots, v_n\}$, and let N be a nilpotent linear transformation on V. Consider $V' = Span\{v_1, \ldots, v_{n-1}\}$. By the induction hypothesis, V' has a basis $W = \{w_1, \ldots, w_{n-1}\}$ of V' such that $N(w_1) = 0$ and $N(w_i) \in Span\{w_1, \ldots, w_{i-1}\}$ for $2 \leq i \leq n-1$. Now, let $w \notin Span(W)$, $w \in V$. If $N(w) \in Span(W)$, then $w_n = w$, $\mathcal{W} = W \cup \{w\}$ is the desired basis for V; we are finished. So, suppose $N(w) \notin Span(W)$. Then, there exists $l \in \mathbb{N}$ so that $N^l(w) \notin Span(W)$ but $N^{l+1}(w) \in Span(W)$. Otherwise, suppose that for all $l \in \mathbb{N}$ so that $N^l(w) \notin Span(W)$ then $N^{l+1}(w) \notin Span(W)$, since $N(w) = N^1(w) \notin Span(W)$, then really $N^d(w) \notin Span(W)$ for any natural number d. However, since N is nilpotent, $N^k = 0$ for some $k \in \mathbb{N}$, surely $N^k(w) = 0 \in Span(W)$. So, since $k \in \mathbb{N}$, $N^k(w) \notin Span(W)$, yet $N^k(w) \in Span(W)$ since $N^k(w) = 0$, contradiction. Therefore, for some $l \in \mathbb{N}$ we have $N^l(w) \notin Span(W)$ but $N^{l+1}(w) \in Span(W)$. Hence, let $w_n = N^l(w)$, then $\mathcal{W} = W \cup \{N^l(w)\}$ is the basis for V that we are looking for. □

Maschke's Theorem. *If G is a finite group of order n and F is a field of characteristic 0 or p, where $p \nmid n$, then $F(G)$ is semi-simple.*

Proof. Let G be a finite group of order n and let F be a field of characteristic 0 or p, where $p \nmid n$. For $a \in F(G)$ we define the mapping $T_a : F(G) \to F(G)$ by $T_a(x) = ax$ for all $x \in F(G)$. This is called the *left regular representation* of $F(G)$. As we can see, for any $a \in F(G)$, T_a is an F-module homomorphism from $F(G)$ to itself and thus an F-linear transformation on $F(G)$. Surely, for any $x, y \in F(G)$ and $a \in F(G)$, $T_a(x+y) = a(x+y) = ax + ay = T_a(x) + T_a(y)$. Moreover, for any $c \in F$, $a \in F(G)$ and $x \in F(G)$, $T_a(cx) = a(cx) = a(c)x = (c)ax = c(ax) = cT_a(x)$. Now, since we are seeing $F(G)$ as a vector space over F, we can say that, for any $a \in F(G)$, $T_a \in End_F(F(G))$. Of course, by Theorem 2.1.1, $End_F(F(G)) \cong Mat_n(F)$ (since F is commutative, opposite ring is not needed). Define, for any $a \in F(G)$, $M_a = [T_a(g_1), \ldots, T_a(g_n)]$; the matrix composed of the coefficients of $T_a(g_i)$ as the i-th column vector (just as in Theorem 2.1.1).

We will note two things about M_g, for $g \in G$. If e is the identity element of G, then the trace of M_e, $tr(M_e)$, is n, and since $eg = g = ge$ for any $g \in G$, then M_e is the identity matrix. On the other hand, if $g \neq e$, then $tr(M_g) = 0$ since $gh \neq h \neq hg$ for any $h \in G$.

Let J be the Jacobson radical of $F(G)$. Since $F(G)$ is finite dimensional over F, thus Artinian, then J is nilpotent by Theorem 4.2.3. To prove $J = (0)$, suppose instead that $J \neq (0)$. Let $v \in J$ be a nonzero element. Say, $v = a_1g_1 + \cdots + a_ng_n$, with at least $a_k \neq 0$. Since J is an ideal, then $g_k^{-1}v \in J$ and $g_k^{-1}v = a_ke + a_2'g_2' + \cdots + a_n'g_n'$; say $g_k^{-1}v = v'$. Since $v' \in J$ and J is nilpotent, then v' is nilpotent. However, since v' is nilpotent, then $T_{v'}$ is a nilpotent linear transformation. Since $T_{v'}$ is a nilpotent linear transformation, by Lemma 6.0.2 we have a basis $\mathcal{W}$ of $F(G)$ so that $T_{v'}(w_1) = 0$ and $T_{v'}(w_i) \in Span\{w_1, \ldots, w_{i-1}\}$ for $2 \leq i \leq n$. Note that $[M_{v'}]_{\mathcal{W}}$ is a matrix so that the entries a_{ij} equal zero if $i \geq j$, meaning $tr([M_{v'}]_{\mathcal{W}}) = 0$. On that note, let P be the change of basis matrix from $\{g_1, \ldots, g_n\}$ to $\mathcal{W}$, then $[M_{v'}]_{\mathcal{W}} = PM_{v'}P^{-1}$ and $tr([M_{v'}]_{\mathcal{W}}) = tr((PM_{v'})P^{-1}) = tr(P^{-1}(PM_{v'})) = tr(M_{v'})$. Hence, $tr(M_{v'}) = 0$. On the other hand, $T_{v'} = v'x = (a_ke + a_2'g_2' + \cdots + a_n'g_n')x = a_k(ex) + a_2'(g_2'x) + \cdots + a_n'(g_n'x) = a_kT_e + a_2'T_{g_2'} + \cdots + a_n'T_{g_n'}$, so $tr(M_{v'}) = a_k\, tr(M_e) + a_2'\, tr(M_{g_2'}) + \cdots + a_n'\, tr(M_{g_n'}) = a_kn$, so $a_kn = 0$. Since $a_k \neq 0$, then $n = 0$ in F. If F has characteristic 0 and $n(a_k) = 0$, $a_k \neq 0$, then $n1_F = na_k(a_k)^{-1} = 0$, contradicting F as having characteristic 0. On the other hand, if the characteristic of F is p, it must be that $p|n$, which contradicts the given hypothesis. Hence, it must be that $J = (0)$, so $F(G)$ is semi-simple. □

Let us explore an example of a group algebra decomposed as a direct sum of simple rings. Note that we shall eventually use a strategy implemented in Jacobson, pg. 49 [J], for picking a particular basis.

Example 6.0.2. Let $\langle\alpha\rangle$ be the cyclic group of order 3 generated by α. Consider the group algebra $\mathbb{R}(\langle\alpha\rangle) = \{c_1e + c_2\alpha + c_3\alpha^2 \,|\, c_i \in \mathbb{R}\}$. By Maschke's Theorem, we know $\mathbb{R}(\langle\alpha\rangle)$ is a semi-simple (and Artinian) ring. Note that the element $\frac{e+\alpha+\alpha^2}{3}$ is a nonzero idempotent element of $\mathbb{R}(\langle\alpha\rangle)$. In fact, if we say $\zeta = \frac{e+\alpha+\alpha^2}{3}$, then $\zeta(c_1e + c_2\alpha + c_3) = c_1\zeta e + c_2\zeta\alpha + c_3\zeta\alpha^2 = c_1\zeta + c_2\zeta + c_3\zeta = (c_1 + c_2 + c_3)\zeta$. In other words, the product of any element of $\mathbb{R}(\langle\alpha\rangle)$ and ζ results in a scalar multiple of ζ. On that note, we can observe how $[\mathbb{R}(\langle\alpha\rangle)]\zeta$ is a field with unity ζ ($\zeta \in \mathbb{R}(\langle\alpha\rangle)$ implies $\zeta\zeta = \zeta^2 = \zeta \in [\mathbb{R}(\langle\alpha\rangle)]\zeta$). By Theorem 4.3.2, we have that $[\mathbb{R}(\langle\alpha\rangle)]\zeta$ is a minimal ideal. Hence, $\mathbb{R}(\langle\alpha\rangle) = [\mathbb{R}(\langle\alpha\rangle)]\zeta \oplus [\mathbb{R}(\langle\alpha\rangle)](e-\zeta)$. Sadly, proving $[\mathbb{R}(\langle\alpha\rangle)](e-\zeta)$ is a minimal ideal (and a field) is no easy task, so we will use a different strategy. Recall, $\mathbb{R}(\langle\alpha\rangle)$ is still a vector space over $\mathbb{R}$, so we shall pick basis $\mathcal{B} = \{\zeta, \alpha - e, \alpha^2 - \alpha\}$; let $u_1 = \zeta$, $u_2 = \alpha - e$, and $u_3 = \alpha^2 - \alpha$. Since $\mathcal{B}$ is a basis for $\mathbb{R}(\langle\alpha\rangle)$, we can say $\mathbb{R}(\langle\alpha\rangle) = Span_{\mathbb{R}}\{u_1\} \oplus Span_{\mathbb{R}}\{u_2, u_3\}$. From our previous conversation on $[\mathbb{R}(\langle\alpha\rangle)]\zeta$, we can see that $[\mathbb{R}(\langle\alpha\rangle)]\zeta = Span_{\mathbb{R}}\{u_1\}$. Hence, it must be that $Span_{\mathbb{R}}\{u_2, u_3\} = [\mathbb{R}(\langle\alpha\rangle)](e-\zeta)$. Correspondingly, we will show that $Span_{\mathbb{R}}\{u_2, u_3\}$ is a minimal ideal by showing that it does not contain a smaller ideal. Of course, we will do so by contradiction. Suppose there exists an ideal I of $\mathbb{R}(\langle\alpha\rangle)$ such that $(0) \subset I \subset Span_{\mathbb{R}}\{u_2, u_3\}$ and $Span_{\mathbb{R}}\{u_2, u_3\} \neq I$. We can quickly show I is a vector subspace of $\mathbb{R}(\langle\alpha\rangle)$. By definition, I being an ideal implies it is closed under addition and contains zero (the zero vector). Now, to show I is closed under scalar multiplication, let $c \in \mathbb{R}$ and $v \in I$, then $cv = cev = (ce)v$. Since $ce \in \mathbb{R}(\langle\alpha\rangle)$, $v \in I$, and I an ideal of $\mathbb{R}(\langle\alpha\rangle)$, we have that $(ce)v \in I$; hence, $cv \in I$. Now, since I is a subspace of $\mathbb{R}(\langle\alpha\rangle)$ and a proper subset of $Span_{\mathbb{R}}\{u_2, u_3\}$, I must be either (0) or a 1-dimensional subspace of $Span_{\mathbb{R}}\{u_2, u_3\}$. If I is a 1-dimensional subspace of $Span_{\mathbb{R}}\{u_2, u_3\}$, say the basis of I is $\{v\}$ ($v \neq 0$), it must be that for any $x \in \mathbb{R}(\langle\alpha\rangle)$, $xv = \lambda v$ for some $\lambda \in \mathbb{R}$. Of course, if $x \in \mathbb{R}(\langle\alpha\rangle)$, then x is a formal sum of powers of α. Hence, we need only check if there exists a scalar $\lambda \in \mathbb{R}$ such that $\alpha v = \lambda v$, for some $\lambda \in \mathbb{R}$. Since u_2, u_3 form a basis for $Span_{\mathbb{R}}\{u_2, u_3\}$, $\alpha u_2 = u_3$ and $\alpha u_3 = -u_2 - u_3$, we can say the linear transformation on $Span_{\mathbb{R}}\{u_2, u_3\}$ induced by α is

$$T_\alpha = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

Hence, we must see if there exists scalar $\lambda \in \mathbb{R}$ such that $T_\alpha v = \lambda v$. Upon a simple calculation of eigenvaules, we see that the characteristic polynomial of T_α is $\lambda^2 + \lambda + 1$, which is irreducible over $\mathbb{R}$. Since no such λ exists in $\mathbb{R}$, I cannot be 1-dimensional. Hence, $I = (0)$, which means $Span_{\mathbb{R}}\{u_2, u_3\}$ is a minimal ideal of $\mathbb{R}(\langle\alpha\rangle)$. Therefore, $\mathbb{R}(\langle\alpha\rangle) = [\mathbb{R}(\langle\alpha\rangle)]\zeta \oplus [\mathbb{R}(\langle\alpha\rangle)](e-\zeta)$ is the full Peirce decomposition of $\mathbb{R}(\langle\alpha\rangle)$.

Lastly, to show what these two simple rings are isomorphic to, consider the ring of endomorphisms for both of the rings. Say, $R_1 = [\mathbb{R}(\langle\alpha\rangle)]\zeta$ and $R_2 = [\mathbb{R}(\langle\alpha\rangle)](e-\zeta)$.

Recall that R_1, R_2 being fields imply that they are primitive rings by Proposition 5.2.3. As such, they must have simple, faithful modules which can be taken to be R_1 and R_2 themselves respectively. On that note, $D_1 = End_{R_1}(R_1)$ and $D_2 = End_{R_2}(R_2)$ are division rings by Schur's Lemma. Lastly, Wedderburn's second theorem shows that $R_1 \cong End_{D_1}(R_1)$ and $R_2 \cong End_{D_2}(R_2)$. Now, we need only consider what $End_{D_1}(R_1)$ and $End_{D_2}(R_2)$ are. For R_1, it is clear to see that $\mathbb{R} \cong R_1 \cong End_{D_1}(R_1)$. As for $End_{D_2}(R_2)$, since we need D_2-module homomorphisms on R_2 we need only check all of the linear transformation of R_2 that commute with α, or rather T_α. Hence consider the 2×2 matrices such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then we have that $b = -c$ and $d = a - c$; a and c remain free. In fact, if E is the 2×2 identity matrix, then any matrix that commutes T_α is actually a linear combination of E and T_α. Furthermore, if $I = \frac{1}{\sqrt{3}}E + \frac{2}{\sqrt{3}}T_\alpha$, then $I^2 = -E$. Since we know $R_2 \cong End_{D_2}(R_2)$, and R_2 a 2-dimensional field over $\mathbb{R}$, and there is an element I such that $I^2 = -E$, we can see that it is not hard to prove $End_{D_2}(R_2) \cong \mathbb{C}$, the complex numbers! Hence, we have that R_1 and R_2 are 1×1 matrices over familiar fields. That is, $\mathbb{R}(\langle\alpha\rangle) = Mat_1(\mathbb{R}) \times Mat_1(\mathbb{C})$.

In both examples, we had our rings be a direct sum of fields. Such is the consequence of dealing with commutative rings. In general, if we assume our ring to be commutative on top of being semi-simple Artinian, then the ring will decompose into a direct sum of fields. That is, if a ring R is semi-simple Artinian, then the first Wedderburn-Artin theorem states that it will be a finite direct sum of simple Artinian rings. Then, Lemma 5.1.2 states that these simple rings are all of the minimal (two-sided) ideals of R. Next, we observe Corollary 5.1.1 which states that every minimal ideal of R is of the form Re_i for some idempotent elements e_i or R. Lastly, we note Theorem 4.3.2 and recall that in the commutative case, both $Re = eRe$ and eRe would be a commutative division ring. Hence, the minimal ideals Re_i would all be fields, meaning R is a direct sum of fields. Our group algebra example also came out this way since $F(G)$ is commutative if and only if both F and G are commutative. Hence, one could try an example with a group G

that is not commutative and have simple modules that are not fields. Sadly, this is the end of the road. We have proved the Wedderburn-Artin theorems and have given quick examples of the theorems in action. While we could explore the results of the theorems in more dept, that sounds like a paper for another day. Quite honestly, this paper cold have ended with chapter 5, but I figured a quick display of our theorems would be of great use. Now, taking the examples we have covered thus far, the reader can explore semi-simple rings on their own if they wish to. Good luck!

Bibliography

[C] Curtis, C. W., Reiner, I. *Representation Theory of Finite Groups and Associative Algebras*. Wiley, 1988

[Her] Herstein, I. N. *Noncommutative Rings*, Carus Mathematical Monographs, Vol. 15, Mathematical Association of America, Washington, D.C., 1968.

[Hun] Hungerford, T., *Algebra*. Graduate Texts in Mathematics, Vol. 73, Springer-Verlag, New York, 1974.

[J] Jacobson, N., *Basic Algebra II*, W. H. Freeman and Company, San Francisco, 1980.