2006

The structure of semisimple Artinian rings

Ravi Samuel Pandian

Follow this and additional works at: https://scholarworks.lib.csusb.edu/etd-project

Part of the Mathematics Commons

Recommended Citation
https://scholarworks.lib.csusb.edu/etd-project/2977

This Project is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.
THE STRUCTURE OF SEMISIMPLE ARTINIAN RINGS

A Project
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
Ravi Samuel Pandian
March 2006
THE STRUCTURE OF SEMISIMPLE ARTINIAN RINGS

A Project
Presented to the
Faculty of
California State University
San Bernardino

by
Ravi Samuel Pandian
March 2006

Approved by:

Davida Fischman, Committee Chair

Gary Griffing, Committee Member

Laura Wallace, Committee Member

Peter Williams, Chair
Department of Mathematics

Terry Hallett,
Graduate Coordinator
Department of Mathematics
ABSTRACT

We will prove two famous theorems attributed to J.M.H. Wedderburn, both of which concern the structure of non-commutative rings. In modern literature they are generally presented as follows: (1) Any semisimple Artinian ring is the direct sum of a finite number of simple rings; and (2) The Wedderburn-Artin Theorem: Let $R$ be a simple Artinian ring. Then $R$ is isomorphic to $D_n$, the ring of $n \times n$ matrices over a division ring $D$. Both $D$ and $n$ are unique up to isomorphism. Conversely, for any division ring $D$, $D_n$ is a simple Artinian ring. Taken together, the two theorems completely determine the structure of semisimple Artinian rings.

We begin by introducing the structure of an $R$-module, and will prove that any irreducible $R$-module is isomorphic as a module to the quotient ring $R/\rho$, where $\rho$ is a maximal regular right ideal of $R$. We will also prove that $R$ is homomorphically embedded in the ring of additive endomorphisms of $M$, $E(M)$, and that the set of elements of this ring of endomorphisms that commute with the elements
of $R$ forms a division ring. This is a famous result known as Schur's Lemma.

We then define the Jacobson radical of a ring to be the set of all elements of $R$ that annihilate all possible irreducible $R$-modules, and will prove that the Jacobson radical, $J(R)$, is the intersection of all maximal regular right ideals of $R$, and is itself a two-sided ideal of $R$. We will prove that the structure of $J(R)$ is right-quasi regular, and that any nil ideal or nilpotent ideal of $R$ is contained in $J(R)$. A semisimple ring is then defined to be a ring whose Jacobson radical is equal to the set $\{0\}$.

An Artinian ring $R$ is a ring such that any non-zero set of right ideals of $R$ has a minimal element. We prove that the Jacobson radical of any Artinian ring must be nilpotent, and we show that any ring that is both semisimple and Artinian must have a two-sided unit element. We introduce the idempotent, a non-zero element $e$ in the ring such that $e^2 = e$, and we demonstrate that any ideal of a semisimple Artinian ring can be described in terms of an idempotent. Finally, using a Pierce decomposition, we prove the first of the Wedderburn theorems.
In the final chapter we begin with the definition of primitive rings, and introduce the concept of density. We prove the Density Theorem: If $R$ is a primitive ring, and $M$ is a faithful irreducible $R$-module, then $R$ is a dense ring of linear transformations on $M$ over $C(M)$. With this tool in hand, we prove the Wedderburn-Artin Theorem.
ACKNOWLEDGMENTS

I'd like to acknowledge the entire Mathematics Department for their guidance and instruction during my time in this program. Thank you to Nancy and Paula and Tiffany, and a very special thanks to Dr. Terry Hallett who not only served as the Graduate Coordinator, but as my professor for two courses.

Of course I am most indebted to the members of my committee. Thank you Dr. Griffing for being so understanding when I had my car accident, and thank you Dr. Wallace for taking the time to help a student whom you knew nothing about. I deeply appreciate all of the effort you both have extended on my behalf.

Finally I'd like to thank Dr. Davida Fischman, who has been guide, mentor, and friend. Thank you for your patience, and for sharing your love of this subject with me. I have truly enjoyed this entire process: from the proofs to the meetings in your office to the coffee shops to the emails - all of it. I couldn't have asked for a better advisor :-).
DEDICATION

To Mummy and Appah.

I love you both very much.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>vi</td>
</tr>
<tr>
<td>CHAPTER ONE: NOTATION AND CONVENTIONS</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER TWO: MODULES</td>
<td>9</td>
</tr>
<tr>
<td>CHAPTER THREE: THE JACOBSON RADICAL</td>
<td>36</td>
</tr>
<tr>
<td>CHAPTER FOUR: SEMISIMPLE ARTINIAN RINGS</td>
<td>65</td>
</tr>
<tr>
<td>CHAPTER FIVE: THE WEDDERBURN-ARTIN THEOREM</td>
<td>98</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>116</td>
</tr>
</tbody>
</table>
In 1907, Joseph Henry Maclagen Wedderburn published *On Hypercomplex Numbers* in the *Proceedings of the London Mathematical Society*. It is worth noting that this was not the first time Wedderburn had published, having done so three times as a mere undergraduate at the University of Edinburgh. In *Hypercomplex Numbers*, the man who would later become one of the Princeton Preceptors, appointed by none other then Woodrow Wilson, presented two famous results. We list the modern interpretation of these results below. Throughout this paper, we shall refer to them as Theorem 1(a) and Theorem 1(b).

**Theorem 1(a)**

Let $R$ be a semisimple Artinian ring. Then $R$ is the direct sum of a finite number of simple Artinian rings.

**Theorem 1(b) The Wedderburn-Artin Theorem**

Let $R$ be a simple Artinian ring. Then $R$ is isomorphic to $D_n$, the ring of $n \times n$ matrices over a division ring $D$.

Both $D$ and $n$ are unique up to isomorphism. Conversely, for any division ring $D$, $D_n$ is a simple Artinian ring.
The goal of this project is to prove both of these results, after first establishing the necessary background material. Our approach will mirror that outlined in I.N. Herstein's monograph Noncommutative Rings. The proofs in this paper follow those outlined in that text, though many of the examples and details have been provided by this author.

In Chapter Two we start our examination in earnest. However, we take the time here to establish certain ground rules concerning structures, notation, etc. We intend to minimize any confusion during the reading of this project. We start with the definition of a ring.

**Definition 1.2** A ring

Let $R$ be a set equipped with an element $0$ and two operations $+: R \times R \to R$ and $\cdot: R \times R \to R$. We call $R$ a ring if for any $a, b, c \in R$:

i) $a + b = b + a$; (addition is commutative)

ii) $a + 0 = a$;

iii) for any $a \in R$ there exists an additive inverse $(-a) \in R$ such that $a + (-a) = 0$;

iv) $(a + b) + c = a + (b + c)$; (addition is associative)
v) $a*0=0=0*a$;

vi) $(a*b)c=a*(b*c)$; (multiplication is associative)

and

vii) $a*(b+c)=a*b+a*c$ and $(a+b)c=a*c+b*c$. (the distributive property)

Thus a ring is commutative under addition, but is not necessarily commutative under multiplication. Note also that no mention is made of a multiplicative identity or two-sided unit element, denoted \('l\'). Herstein worked with rings that did not by default have a \('l\'), and we will follow his approach. One of the advantages of this tack is that ideals of a ring may themselves be viewed as rings, as we demonstrate in Lemma 1.4. However, at times we will require a unit-like element, and we will use the concept of regularity to find one. We will see in Chapter Two that regularity is a generalization of the usual unit property.

As part of the examination of any class of rings, it is only natural to encounter ideals. As the rings we are studying are noncommutative, "handedness" becomes a necessary concern. A right ideal is defined as follows.
Definition 1.3 A right ideal

Let \( \rho \subseteq R \). We call \( \rho \) a right ideal of \( R \) if for all \( a, b \in \rho \) and \( r \in R \) the following are true:

i) \( 0 \in \rho \);

ii) \( a, b \in \rho \Rightarrow a - b \in \rho \); and

iii) \( a \in \rho, r \in R \Rightarrow ar \in \rho \).

The ideal \( \rho \) above is called a right ideal because it is closed under multiplication by elements of \( R \) from the right. We defined this property element-wise in part (iii) above, and can summarize this idea succinctly in the following manner: \( \rho R \subseteq \rho \). To define a left ideal, simply change property (iii) to \( a \in \rho, r \in R \Rightarrow ra \in \rho \), or \( R \rho \subseteq \rho \). A two-sided ideal \( \rho \) is defined to be both a left and a right ideal, i.e. \( R \rho R \subseteq \rho \).

Lemma 1.4

Let \( R \) be a ring, and let \( \rho \) be a right ideal of \( R \). Then \( \rho \) is a ring.

Proof: Since \( \rho \) is a right ideal of \( R \), \( 0 \in \rho \), and \( \rho \) is closed under subtraction. Moreover, \( \rho R \subseteq \rho \), which implies \( \rho \rho \subseteq \rho \), telling us that \( \rho \) is closed under multiplication.
with $\rho$. The remainder of the ring properties are inherited from $R$.

At times we will both add or multiply ideals to create new ones. The details of these constructions are given below.

**Lemma 1.5**

Let $\rho$ and $\gamma$ be right ideals of a ring $R$, and define

$$\rho\gamma = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \rho, b_i \in \gamma, n \in \mathbb{N} \right\}.$$  

Then $\rho\gamma$ is a right ideal of $R$.

**Proof:** Since $\rho$ and $\gamma$ are right ideals of $R$, they both contain the element $0$. Thus, $0 \cdot 0 = 0 \in \rho\gamma$. Because it is constructed to be so, $\rho\gamma$ is closed under addition. To see that it is closed under right multiplication by elements of $R$, recall that $\gamma$ is a right ideal of $R$ and observe that for any $a \in \rho$, $b \in \gamma$, $r \in R$, $abr = a(br) = ab'$ for some $b' \in \gamma$. Of course $ab' \in \rho\gamma$.

**Corollary 1.6**

If $\rho$ is a (left, right or two-sided) ideal of $R$, then $\rho^n = \rho \rho \ldots \rho$ (n times) is a (left, right or two-sided, respectively) ideal of $R$ for any $n \in \mathbb{N}$.
Lemma 1.7 A direct sum

Let $R$ be a ring, and let $\rho, \gamma$ be right ideals of $R$. If $\rho \cap \gamma = \{0\}$, we call $\rho \oplus \gamma = \{a + b | a \in \rho, b \in \gamma\}$ the direct sum of $\rho$ and $\gamma$. Then $\rho \oplus \gamma$ is a right ideal of $R$.

Proof: Since $\rho$ and $\gamma$ are both right ideals of $R$, zero must be an element of both, and so $0 + 0 = 0 \in \rho \oplus \gamma$. To show closure under subtraction, let $x, y \in \rho \oplus \gamma$. This implies that $x = a_1 + b_1$ and $y = a_2 + b_2$ for some $a_1, a_2 \in \rho, b_1, b_2 \in \gamma$. Therefore $x - y = (a_1 + b_1) - (a_2 + b_2)$. Noting that each $a_i$ and $b_i$ is just an element of $R$, and that as right ideals both $\rho$ and $\gamma$ are closed under subtraction,

$x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = a' + b'$ for some $a' \in \rho, b' \in \gamma$.

Thus $x - y \in \rho \oplus \gamma$. Finally, let $x \in \rho \oplus \gamma$, and let $r \in R$. Since $x$ must equal $a + b$ for some $a \in \rho$ and $b \in \gamma$, we see immediately that $xr = (a + b)r = ar + br$. But again $\rho$ and $\gamma$ are right ideals, so $ar \in \rho$ and $br \in \gamma$. Thus $xr \in \rho \oplus \gamma$.

Definition 1.8 A quotient ring

Let $R$ be a ring and let $\rho$ be a two-sided ideal of $R$. Define $R/\rho = \{a + \rho | a \in R\}$. Then $R/\rho$ has the structure of a ring.
Proof: Equip this set with the following operations:

\[ + : \mathbb{R}_\rho \times \mathbb{R}_\rho \to \mathbb{R}_\rho \] given by \( (a+\rho)+(b+\rho) \mapsto (a+b)+\rho \) and

\[ \cdot : \mathbb{R}_\rho \times \mathbb{R}_\rho \to \mathbb{R}_\rho \] given by \( (a+\rho)(b+\rho) \mapsto ab+\rho \) for all \( a,b \in R \).

As defined above, both addition and multiplication are single-valued. To see this for multiplication, let \( a+\rho = a' + \rho \) and \( b+\rho = b' + \rho \). This implies that \( a - a' \in \rho \) and \( b - b' \in \rho \). We must show the following to be true:

\[
(a' + \rho)(b' + \rho) = a'b' + \rho = ab + \rho = (a + \rho)(b + \rho).
\]

In other words, we must show that \( a'b' - ab \in \rho \). But we see that

\[
a'b' - ab = a'b' + ab' - ab - ab = (a' + a)b' - a(b' + b).
\]

Since \( \rho \) is a two-sided ideal, and the elements \( a - a', b - b' \in \rho \), we conclude that \( a'b' - ab \in \rho \). With addition and multiplication so defined, the ring properties of Definition 1.2 can be verified.

We note that the fact that \( \rho \) was a two-sided ideal of \( R \) was central to the proof of the ring structure \( \mathbb{R}_\rho \). If \( \rho \) is a right ideal of \( R \), the multiplication above cannot be shown to be single-valued. However, in this instance \( \mathbb{R}_\rho \)
still has a familiar structure, and we note it in the following definition:

**Definition 1.9 A quotient group**

Let $R$ be a ring and let $\rho$ be a right ideal of $R$. Define $\frac{R}{\rho} = \{a + \rho | a \in R\}$. Then $\frac{R}{\rho}$ has the structure of a group.

**Proof:** Equip $\frac{R}{\rho}$ with the addition listed above. It can be shown that such addition is well-defined, that $\frac{R}{\rho}$ has a 0 element, additive inverses, and is both commutative and associative for addition. In other words, $\frac{R}{\rho}$ has the structure of a group.

Please note that the symbols $\subset, \supset$ indicate proper containment and should be distinguished from the symbols $\subseteq, \supseteq$. Finally, $F^n$ refers to the $n$-dimensional vector space over the field $F$, while $F_n$ represents the ring of $n \times n$ matrices over $F$. 
CHAPTER TWO
MODULES

We begin our examination of non-commutative rings by studying how these structures interact with a classic algebraic object, the module.

Definition 2.1 An $R$-module

Given a ring $R$, we call the set $M$ an $R$-module if $M$ is an additive abelian group, and if there exists an operation $M \times R \to M$ that sends $(m,r) \mapsto mr$ (sometimes written $m \cdot r$) such that:

i) $m(r_1 + r_2) = mr_1 + mr_2$;

ii) $(m_1 + m_2)r = m_1r + m_2r$; and

iii) $(mr_1)r_2 = m(r_1r_2)$

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

$M$ is considered a right $R$-module because the elements of $R$ act on $M$ from the right. If the action were a function $R \times M \to M$, $M$ would be called a left $R$-module.

Fortunately, we will be dealing exclusively with right $R$-modules, and so for brevity will simply refer to them as $R$-modules.
Everything acts on $M$ from the right, including functions. Therefore at times we will utilize right-handed notation for functions whose domain is an $R$-module. For example, let $f:M \to M$ be given by $(m)f = m - m$. Then $(m)f = 0$. This form of function notation will serve us well when we compose functions involving $M$.

There are many examples of $R$-modules in mathematics. One important example is the vector space $\mathbb{R}^n$. This is an $\mathbb{R}_n$-module, where $\mathbb{R}_n$ is the ring of $n \times n$ matrices over $\mathbb{R}$. The module operation is matrix multiplication, and the verification of the module properties are straightforward exercises in linear algebra.

The intrinsic multiplication of any ring $R$ makes $R$ a module over itself, and that same operation would similarly make any right ideal of $R$ an $R$-module. We now give special attention to a less trivial example of an $R$-module that has also been constructed from $R$ itself. This module will be used repeatedly in later sections of this paper.
Lemma 2.2

Given a ring $R$ and a right ideal $\rho$ of $R$, the quotient ring $R/\rho$ is an $R$-module.

Proof: Define $*: R/\rho \times R \rightarrow R/\rho$ by $(m+\rho, r) \mapsto mr+\rho$. To show this mapping is well-defined, for let $m, m_1, r, r_1, r_2 \in R$,

$m_1 + \rho = m_2 + \rho$, and $r_1 = r_2$. This implies that $m_1 - m_2 \in \rho$, and because $\rho$ is a right ideal, $m_1 r_1 - m_2 r_2 \in \rho$. This tells us that $m_1 r_1 + \rho = m_2 r_2 + \rho$. Thus the module operation is well-defined.

Let us now verify that $R/\rho$ is in fact an $R$-module.

Let $m + \rho, m_1 + \rho, m_2 + \rho \in R/\rho$ and $r, r_1, r_2 \in R$.

To verify Definition 2.1.(i), let $a \in (m+\rho)(r_1+r_2)$. This implies that $a \in m(r_1 + r_2) + \rho$. Thus there exists some $q \in \rho$ such that $a = m(r_1 + r_2) + q$. We can simplify this equation to show that $a = mr_1 + 0 + mr_2 + q$, and thus conclude that

$a \in (mr_1 + \rho) + (mr_2 + \rho)$, which implies that $a \in (m+\rho)(r_1 + r_2) \subseteq (m+\rho)r_1 + (m+\rho)r_2$. We have shown that $(m+\rho)(r_1 + r_2) \subseteq (m+\rho)r_1 + (m+\rho)r_2$. To show the reverse inclusion, let $a \in (m+\rho)r_1 + (m+\rho)r_2$. This implies that $a \in (mr_1 + \rho) + (mr_2 + \rho)$. Thus there exists some $q, q_2 \in \rho$ such that

11
\[ a = mr_1 + q_1 + mr_2 + q_2. \] Simplifying, \( a = m(r_1 + r_2) + (q_1 + q_2), \) and utilizing the fact that \( q_1, q_2 \in \rho \Rightarrow q_1 + q_2 \in \rho, \) we may conclude that \( a \in m(r_1 + r_2) + \rho, \) i.e. \( a \in (m + \rho)(r_1 + r_2). \) The second part of Definition 2.1 is proven in a similar fashion. We conclude by proving part (iii). Let \( m + \rho \in \overset{R}{\rho}, \) and \( r_1, r_2 \in R. \) Observe that \( ((m + \rho)r_1)r_2 = (mr_1 + \rho)r_2 = (mr_1)r_2 + \rho = m(r_1r_2) + \rho. \) But
\[ m(r_1r_2) + \rho = (m + \rho)(r_1r_2), \] and so \( ((m + \rho)r_1)r_2 = (m + \rho)(r_1r_2). \) Thus \( \overset{R}{\rho} \) is an \( R \)-module.

Example 2.3

A nice example of an \( R \)-module can be constructed from the ring of integers \( \mathbb{Z}, \) and the right ideal \( n\mathbb{Z}, n \geq 2. \) Explicitly then, the quotient ring is
\[ \mathbb{Z}/n\mathbb{Z} = \{[0],[1],[2],\ldots,[n-2],[n-1]\} \] with the usual operations. If we define the module operation as \( ([p],q) \mapsto [pq] \) for all \( p \in \mathbb{Z}/n\mathbb{Z} \) and \( q \in \mathbb{Z}, \) then we will have constructed a \( \mathbb{Z} \)-module.

During the course of our examination, we will seek to utilize subsets of \( R \)-modules that retain the overall module structure, and at times we will seek to compare different modules over the same ring. The tools we will use are
submodules and module homomorphisms, and we define them here.

**Definition 2.4 A submodule**

Given a ring $R$ and an $R$-module $M$, we call a subset $N$ of $M$ a submodule of $M$ if:

i) $0 \in N$;

ii) $m,n \in N \Rightarrow m - n \in N$; and

iii) $NR \subseteq N$.

We take the time here to observe the similarity between the Definition 2.4 and Definition 1.3, a right ideal of $R$.

**Definition 2.5 A module homomorphism**

Given a ring $R$ and two $R$-modules $M$ and $N$, we say that a function $f : M \to N$ is a module homomorphism if:

i) $(m_1 + m_2)f = (m_1)f + (m_2)f \ \forall \ m_1,m_2 \in M$; and

ii) $(mr)f = (m)f \ r \ \forall \ m \in M$ and $r \in R$.

For a ring $R$, an $R$-module $M$, and the operation from $M \times R \to M$, a natural question arises: What elements of $R$ send the entire set $M$ to 0? While this question cannot be answered specifically without knowing more about the structure of $M$ and $R$, we can collect these elements of $R$.
and study their properties as an abstract set, the annihilators of $M$, or simply $A(M)$. This set will yield important information about the relationship between $M$ and $R$.

**Definition 2.6** $A(M)$ The set of annihilators of $M$

Let $A(M) = \{ x \in R | Mx = \{0\} \}$.

**Definition 2.7** Faithful $R$-modules

If $A(M) = \{0\}$ we call $M$ a faithful $R$-module.

We see that by construction $A(M)$ is a subset of $R$.

What else can be said about the structure of this set?

**Lemma 2.8**

$A(M)$ is a two-sided ideal of $R$.

**Proof:** We need to first show $0 \in A(M)$. Let $m \in M$.

Since $M$ is an $R$-module, $m \cdot 0 = m(0+0) = m \cdot 0 + m \cdot 0$. Subtracting $m \cdot 0$ from both sides yields $0 = m \cdot 0$ for any $m \in M$. Therefore $0$ must be an element of $A(M)$. Next let us prove that $a, b \in A(M)$ implies $a - b \in A(M)$. Let $a, b \in A(M)$. This implies that $0 = ma = mb$ for all $m \in M$, which allows us to say that $0 = ma - mb = m(a - b)$. This implies that $m(a - b) = 0$ for all $m \in M$, which implies $a - b \in A(M)$. Finally, we must show that $A(M)$ is closed under left and right multiplication with
elements of $R$. Let $m \in M, r \in R$, and $a \in A(M)$. We see that $m(ra) = mr(a) \subseteq Ma = \{0\}$, and $m(ar) = (ma)r = 0 \cdot r = 0$. Thus $ra \in A(M)$ and $ar \in A(M)$ for all $r \in R, a \in A(M)$.

Since $A(M)$ is a two-sided ideal of $R$, $R/A(M)$ must have the structure of a ring as described above. It is given that $M$ is already an $R$-module, but how is $M$ related to $R/A(M)$?

**Lemma 2.9**

Via the operation $M \times R/A(M) \to M$, given by

$$(m, r + A(M)) \mapsto mr$$

for all $m \in M$ and $r \in R$, $M$ is a faithful $R/A(M)$-module.

**Proof:** Is this operation well-defined? Suppose $r + A(M) = r' + A(M)$. This implies that $r - r' \in A(M)$, and so $m(r - r') = 0$ for all $m \in M$, which forces $mr = mr'$ for all $m \in M$. Thus the operation is well-defined. The proof of the module properties are all similar in nature, and we prove only the third requirement of Definition 2.1 here.

Recalling that the multiplication of $R/A(M)$ sends

$$(a + A(M))(b + A(M)) \to ab + A(M)$$

for all $a, b \in R$, we must show
that \( m(r_2) = (mr_1)r_2 \) for all \( m \in M, r_1, r_2 \in R/A(M) \). But because \( M \) is an \( R \)-module, we see immediately that

\[
m(r_2 + A(M)) = m(r_2) = (mr_1)r_2 = mr_1(r_2 + A(M)) = [m(r_1 + A(M))](r_2 + A(M)).
\]

Finally, to prove faithfulness, we need to show that the set of annihilators of \( M \) in \( R/A(M) \) equals \( \{0\} \), i.e.

\[
M(r + A(M)) = \{0\} \text{ implies } r + A(M) = 0 + A(M). \text{ Let } r + A(M) \in R/A(M)
\]

for some \( r \in R \) such that \( m(r + A(M)) = \{0\} \) for all \( m \in M \). But,

\[
m(r + A(M)) = mr, \text{ so } mr = 0 \forall m \in M.
\]

This places \( r \) in \( A(M) \), which implies \( r + A(M) = 0 + A(M) \), the zero element of \( R/A(M) \).

We have seen that right ideals of \( R \) can be used to construct \( R \)-modules. Is there a tangible link between these ideals and arbitrary \( R \)-modules? In Theorem 2.19, we show that such a relationship exists. However, to present that result properly, we must develop some additional material.

**Definition 2.10 Irreductible \( R \)-modules**

An \( R \)-module \( M \) is called irreducible if:

i) \( MR \neq \{0\} \); and

ii) the only submodules of \( M \) are \( \{0\} \) and \( M \) itself.
Example 2.11

An irreducible \( \mathbb{Z} \)-module. Earlier we showed that \( \mathbb{Z}/n\mathbb{Z} \) is a \( \mathbb{Z} \)-module for \( n \geq 2 \). For some prime number \( p \), consider \( \mathbb{Z}/p\mathbb{Z} \) and the ring \( \mathbb{Z} \). With the module operation from \( \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \) which sends \( ([a],b) \mapsto [ab] \) for all \( [a] \in \mathbb{Z}/p\mathbb{Z} \) and \( b \in \mathbb{Z} \), \( \mathbb{Z}/p\mathbb{Z} \) is an irreducible \( \mathbb{Z} \)-module.

Proof: Since \([1] \cdot 1 = [1] \neq [0]\), we have that \( (\mathbb{Z}/p\mathbb{Z})^2 \neq \{0\} \).

Now suppose there exists a submodule \( N \) of \( \mathbb{Z}/p\mathbb{Z} \), \( N \neq \{0\} \).

This implies that \( N \) contains at least one non-zero element, call it \([x]\), for some \( x \in \mathbb{Z} \). \( N \) is a submodule however, and so must be closed for multiplication with \( \mathbb{Z} \). Thus \( \{[x \cdot 1], [x \cdot 2], \ldots, [x \cdot p]\} \subseteq N \). As \( p \) is prime, the set \( \{[x \cdot 1], [x \cdot 2], \ldots, [x \cdot p]\} \) will be comprised of \( p \) distinct elements, implying that \( \{[x \cdot 1], [x \cdot 2], \ldots, [x \cdot p]\} = \{[1], [2], \ldots, [p] = [0]\} \). We see then that \( \mathbb{Z}/p\mathbb{Z} \subseteq N \), and may conclude that the only possible submodules of \( \mathbb{Z}/p\mathbb{Z} \) are \( \{[0]\} \) and itself. And so, \( \mathbb{Z}/p\mathbb{Z} \) is an irreducible \( \mathbb{Z} \)-module.
Suppose $p$ was not prime. Would $\mathbb{Z}/p\mathbb{Z}$ still be an irreducible $\mathbb{Z}$-module? The answer is no, and to prove it we need only find a non-zero proper submodule of $\mathbb{Z}/p\mathbb{Z}$. Without loss of generality, let $p=ab$ for some primes $a,b \in \mathbb{N}$, and let $N=\{a\cdot x \mid x \in \mathbb{Z}\}$. $N$ contains $[0]$, is closed under subtraction, and is closed under multiplication with $\mathbb{Z}$. To show $N \subset \mathbb{Z}/p\mathbb{Z}$, consider the element $[ab+1] \in \mathbb{Z}/p\mathbb{Z}$, and suppose $[ab+1] \in N$. This implies that $a|ab+1$, and so $a$ divides 1. This cannot be, thus $[ab+1] \notin N$. $N$ is properly contained in $\mathbb{Z}/p\mathbb{Z}$, which tells us that $\mathbb{Z}/p\mathbb{Z}$ is not an irreducible $\mathbb{Z}$-module. 

Example 2.12

Given a field $F$ and $F_n$, the ring of $n \times n$ matrices over $F$, and the customary multiplication, the vector space $F^n$ is an irreducible $F_n$-module.

Proof: It is easy to see that $(F^n) \cdot F_n \neq \{(0,0,...,0)\}$. Suppose there exists a non-zero submodule $N$ of $F^n$. This implies that there exists some vector $m \in N$ of the form $m=(x_1,x_2,...,x_n)$ where each $x_i \in F$, and for some $k, x_k \neq 0$. Take the
Given a ring $R$, and a subset $\rho$ of $R$, we say that $\rho$ is a regular right ideal of $R$ if it is a right ideal of $R$ and if there exists some $a \in R$ such that $x-ax \in \rho$ for all $x \in R$.

In Chapter One, we declared that the rings we would be studying did not necessarily have a '1' element, usually referred to as a unit or multiplicative identity. When present, the defining property of this element is that $1 \cdot x = x = x \cdot 1$ for all $x \in R$. Regularity is a generalization of this property. If the element $a$ referenced in Definition 2.13 is a '1', then the statement $x-ax$ becomes $x-1 \cdot x$, and we see that $x-1 \cdot x = 0$ for all $x \in R$. The element $0$ of course must
be in every ideal. We summarize this notion in Corollary 2.14.

**Corollary 2.14**

If a ring $R$ has a two-sided or right unit element, then every ideal of $R$ is regular.

**Definition 2.15 Maximal right ideals**

We call $p$ a maximal right ideal of $R$ if it is a right ideal of $R$ and:

i) $p$ is properly contained in $R$, i.e., $p \subset R$; and

ii) if $I$ is a right ideal of $R$ and $p \subset I$, then $I = R$.

**Example 2.16**

Consider the ring $\mathbb{Z}$, and the ideal $p\mathbb{Z}$ for some prime number $p$. $p\mathbb{Z}$ is a 2-sided ideal of $\mathbb{Z}$, and so is certainly a right ideal of $\mathbb{Z}$. Suppose there existed an ideal $I$ of $\mathbb{Z}$ such that $p\mathbb{Z} \subset I$. $p\mathbb{Z} \neq \mathbb{Z}$. This implies that there exists some element $a \in I, a \notin p\mathbb{Z}$. If $a \notin p\mathbb{Z}$, then $a$ and $p$ must be relatively prime. Thus there exist integers $x, y \in \mathbb{Z}$ such that $ax + py = 1$. But note that $a$ and $p$ are elements of $I$, and $I$ is a right ideal of $\mathbb{Z}$. Thus $ax + py = 1 \in I$, and so $1 \cdot \mathbb{Z} = \mathbb{Z} \subseteq I$. Therefore $I = \mathbb{Z}$, and thus $p\mathbb{Z}$ is a maximal right ideal in $\mathbb{Z}$. 

20
Example 2.17

Given a field $F$, $\rho=\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in F \right\}$ is a maximal right ideal of $F_2$, the ring of $2 \times 2$ matrices over $F$.

Proof: Basic matrix calculations show that $0 \in \rho, a, b \in \rho \Rightarrow a-b \in \rho$, and $\rho F_2 \subseteq \rho$. To show $\rho$ is maximal, suppose there exists a right ideal $I$ of $F_2$, such that $\rho \subset I$.

This implies that there is some $x \in I$ such that $x \notin \rho$. If $x \notin \rho$, it must have the form $x=\begin{pmatrix} * & * \\ a & * \end{pmatrix}$ or $x=\begin{pmatrix} * & * \\ * & a \end{pmatrix}$, where $a \neq 0$.

Assume $x$ is the first type of matrix. As $I$ must be closed under multiplication with elements of $F_2$, $x\begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}=\begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix}$ must be in $I$, where $b$ is some element of $F$. $I$ must also be closed under addition, and since by definition $\begin{pmatrix} 1 & -b \\ 0 & 0 \end{pmatrix} \in I$:

$\begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix}+\begin{pmatrix} 1 & -b \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I$. Thus $F_2=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} F_2 \subseteq I$. Noting that a similar approach for the second case of $x$ would yield the same final result, we conclude that $I=F_2$ and thus $\rho$ is a maximal right ideal of $F_2$. 

21
Lemma 2.18

Let \( \rho \) be a maximal regular right ideal of \( R \) and let \( a \in R \) be an element such that \( x-ax \in \rho \) for all \( x \in R \). Then \( a \) is not an element of \( \rho \).

Proof: Suppose \( a \in \rho \). Because \( \rho \) is a right ideal, \( ax \in \rho \) for all \( x \in R \). But we know that \( \rho \) must be closed under addition. If \( x-ax \in \rho \) and \( ax \in \rho \), then \( x=x-ax+ax \in \rho \) for all \( x \in R \). Thus \( R \subseteq \rho \). This contradicts that \( \rho \) is maximal in \( R \). Thus the element \( a \) cannot be an element of \( \rho \).

There are compelling analogues between maximal ideals and irreducible modules. A maximal ideal cannot be contained in another ideal, short of the ring itself. An irreducible module cannot itself contain a submodule, short of the trivial one \( \{0\} \). Both are restrictions relating to size and structure. An irreducible module cannot be broken up into smaller pieces that still preserve a module structure, and the maximal ideal will not be a part of a larger ideal, excluding the largest one of all, the parent ring. Earlier we stated that a relationship exists between these two structures, and we present it here.
Theorem 2.19

If $M$ is an irreducible $R$-module, then $M$ is isomorphic as a module to $\frac{R}{\rho}$ for some maximal right ideal $\rho$ of $R$, which is regular. We will refer to such an ideal as a maximal regular right ideal of $R$. Conversely, if $\rho$ is a maximal regular right ideal of $R$, then $\frac{R}{\rho}$ is an irreducible $R$-module.

Proof: Since $M$ is an irreducible $R$-module, we know that $MR \neq \{0\}$. This implies that there exists some $m \in M$ such that $mR \neq \{0\}$. We notice however that (i) $mR \subseteq M$; (ii) $\forall r_1, r_2 \in R$, $r_1 - r_2 \in R$, and so $mr_1 - mr_2 = m(r_1 - r_2) \in mR$, and (iii) $(mR)R = m(RR) \subseteq mR$. Thus the set $mR$ is a submodule of $M$.

Since we know $M$ is irreducible, $mR \neq \{0\}$ implies that $mR = M$. Define $\phi: R \rightarrow M$ by $\phi(r) = mr$ for all $r \in R$. We wish to show that $\phi$ is a module homomorphism. For any $r_1, r_2 \in R$, observe that $\phi(r_1 + r_2) = m(r_1 + r_2) = mr_1 + mr_2 = \phi(r_1) + \phi(r_2)$, and we see that $\phi(r_1 r) = m(r_1 r) = (mr_1) r = \phi(r_1) r$ for any $r_1, r \in R$. We stated earlier that $R$ can be viewed as an $R$-module via multiplication, and so $\phi$ is a module homomorphism. The image of $\phi$ is $mR = M$, and let
\( \rho \) be the kernel of \( \phi \), i.e. \( \rho = \{ r \in R \mid mr = 0 \} \). A proof similar to that used in Lemma 2.8 demonstrates that \( \rho \) is a right ideal of \( R \). Now \( \frac{R}{\ker \phi} \) is isomorphic to the image of \( \phi \) as \( R \)-modules, and so \( \frac{R}{\rho} \cong M \) as modules.

We have identified our right ideal \( \rho \) and an appropriate isomorphism, but work remains. We must show \( \rho \) is maximal and regular in \( R \). To show \( \rho \) is maximal, suppose there exists a right ideal \( I \) of \( R \) such that \( \rho \subseteq I \). Then \( \phi(I) \) is a submodule of \( M \), and since \( I \) properly contains \( \rho \), \( \phi(I) \neq \{0\} \). This forces \( \phi(I) = M \), i.e. \( mI = M \). We'd like to show \( I = R \). By definition, \( I \subseteq R \). Now, let \( r \in R \). We know that \( mR = M = mI \). This implies that there exists some \( i \in I \) such that \( mr = mi \). This forces \( m(r-i) = 0 \), which tells us that \( r-i \in \rho \). But \( \rho \subseteq I \), so \( r-i \in I \). Since \( i \in I \) and \( I \) is an ideal, \( r \in I \). Thus \( R \subseteq I \), and \( I = R \). Therefore \( \rho \) is a maximal right ideal of \( R \). Finally, to show \( \rho \) is regular, we need to find the desired element \( a \in R \) such that \( x-ax \) in \( \rho \) for all \( x \in R \).

Recall that \( mR = M \). This implies that \( ma = m \) for some \( a \in R \), and so that \( max = mx \) for all \( x \in R \). Thus \( m(x-ax) = 0 \), which puts \( x-ax \) in \( \rho \).
We now turn to the proof of the converse. Let $\rho$ be a maximal regular right ideal of $R$. Lemma 2.2 allows us to conclude that $R/\rho$ has the structure of an $R$-module. We need to show that $R/\rho$ is irreducible. $R$ properly contains $\rho$, and $\rho$ is both maximal and regular. Thus there exists an $a \in R$, $a \notin \rho$ such that $x - ax \in \rho$ for all $x \in R$. Suppose

$$\frac{R}{\rho} \cdot R = \{0\}.$$  This implies that $(a + \rho)r = ar + \rho = 0 + \rho$ for all $r \in R$.

This implies $aR \subseteq \rho$, which combined with the regularity of $\rho$ puts all of $R$ in $\rho$. This contradicts that $\rho$ is a maximal ideal. Thus $\frac{R}{\rho}, R \neq \{0\}$. Define $\gamma : R \to \frac{R}{\rho}$ by $\gamma(r) = r + \rho$. If $r_1 = r_2$ then $r_1 - r_2 = 0$ which implies that $r_1 - r_2 \in \rho$ yielding $r_1 + \rho = r_2 + \rho$, i.e. $\gamma(r_1) = \gamma(r_2)$. Thus $\gamma$ is well-defined. Note also that $\gamma(r_1 + r_2) = (r_1 + r_2) + \rho = (r_1 + \rho) + (r_2 + \rho) = \gamma(r_1) + \gamma(r_2)$, for all $r_1, r_2 \in R$.

Now suppose there exists a submodule $N$ of $\frac{R}{\rho}$, $N \neq \{0\}$.

Let $S = \{x \in R | \gamma(x) \in N\}$. $S$ is a right ideal of $R$. First observe that $0 \in N$ implies $0 \in S$. Now let $a, b \in S$. This implies that $\gamma(a), \gamma(b) \in N$, and, because $N$ is a submodule, $\gamma(a) - \gamma(b) = \gamma(a - b) \in N$. This implies $a - b \in S$. Finally, let $a \in S$,
and \( r \in R \). Then \( \gamma(as) = as + \rho \). Now we know that \( a + \rho \in N \), but again, because \( N \) is a submodule, it must be closed under multiplication with \( R \); so we can safely conclude that \( as + \rho \in N \). This tells us that \( as \in S \).

So \( S \) is indeed a right ideal of \( R \). Since \( 0 \in N \) we have \( \rho \subseteq S \), and \( N \neq \{0\} \) implies that \( \rho \subseteq S \). But \( \rho \) is maximal in \( R \), so any ideal properly containing \( \rho \) must be \( R \) itself. \( S \) must equal \( R \), which implies \( N = \gamma(S) = \gamma(R) = R/\rho \). We have just shown that \( R/\rho \) is irreducible.

Thus, if we wish to study the structure of the set of irreducible \( R \)-modules, which is on its face a collection external to \( R \), we need to consider the set of maximal regular right ideals of \( R \), sets contained in \( R \). We have shifted the focus from structures outside of \( R \), to structures inside \( R \).

Example 2.20

In Example 2.12, we established that the vector space \( F^n \) is an irreducible \( F_n \)-module, where \( F \) is some field. By Theorem 2.19, it must be isomorphic to \( F_n/\rho \) for some maximal regular right ideal \( \rho \) of \( F_n \). Let
\[ \rho = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(n-1)1} & a_{(n-1)2} & \cdots & a_{(n-1)n} \\ 0 & 0 & 0 & 0 \end{pmatrix} \mathbf{a}_j \in F \}. \] Using a similar argument to that in Example 2.17, any ideal \( S \) that properly contains \( \rho \) must have a matrix with a non-zero element in the \( n^{th} \) row. \( S \) must be closed for multiplication by \( F_n \), which, because \( F \) is a field, would force \( S = F_n \). Thus \( \rho \) is maximal, and to show \( \rho \) is regular, observe that \( x-1 \cdot x=0 \in \rho \forall x \in F_n \), where \( 1 \) is the identity matrix. \( \rho \) is indeed a maximal regular right ideal of \( F_n \), and \( F_n / \rho \) creates co-sets of the following form:

\[ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} + \rho, \quad r_i \in F, \] which is isomorphic to \( F^n \), as Theorem 2.19 implies.

Is there another link between \( R \) and an \( R \)-module \( M \)? While not a direct one between the sets themselves, another relationship does exist between \( R \) and a special set of functions from \( M \to M \). As we will see, this link flows directly from part (ii) of Definition 2.1.
Definition 2.21 The additive endomorphisms of \( M \)

Let \( E(M) \) be the set of additive endomorphisms of \( M \), i.e. \( E(M) = \{ \phi : \phi : M \to M, \text{ and } (m_1 + m_2)\phi = (m_1)\phi + (m_2)\phi \ \forall m_1, m_2 \in M \} \).

Lemma 2.22

Equipped with point-wise addition and composition, \( E(M) \) is a ring.

Proof: The 0 element of \( E(M) \) is the mapping that sends every element of \( M \) to 0, and the 1 element is the identity function. Let \( \alpha, \beta \in E(M) \). Define \( (\alpha + \beta) : M \to M \) by \( (m)(\alpha + \beta) = (m)\alpha + (m)\beta \), and define \( (\alpha \beta) : M \to M \) by \( (m)(\alpha \beta) = ((m)\alpha)\beta \). As such both addition and multiplication will yield well-defined functions from \( M \to M \). To show that \( E(M) \) is closed under multiplication, observe that:

\[
(m_1 + m_2)(\alpha \beta) = ((m_1 + m_2)\alpha)\beta \\
= ((m_1)\alpha + (m_2)\alpha)\beta = ((m_1)\alpha)\beta + ((m_2)\alpha)\beta \\
= (m_1)(\alpha \beta) + (m_2)(\alpha \beta) \quad \text{for all } m_1, m_2 \in M.
\]

\( E(M) \) is also closed under addition. The various structural ring requirements can likewise be demonstrated, but we will prove associativity for multiplication and distributivity here. Let \( \alpha, \beta, \phi \in E(M) \), and \( m \in M \).

\[
(m)((\alpha \beta)\phi) = ((m)(\alpha \beta))\phi
\]
This proves associativity for multiplication. To show distributivity, observe that:

\[(m)(\alpha(\beta + \phi)) = (m)(\alpha(\beta + \phi))\]

\[= ((m)\alpha)\beta + ((m)\alpha)\phi = (m)(\alpha\beta) + (m)(\alpha\phi).\]

Equipped with this addition and multiplication, \(E(M)\) is a ring.

How does the ring \(R\) relate to \(E(M)\)? Recall part (ii) of the definition of an \(R\)-module, \((m_1 + m_2)r = m_1r + m_2r\). We see that the action of \(R\) on \(M\) has the effect of an endomorphism. For any \(r \in R\), let us define the function \(T_r : M \to M\) by \((m)T_r = mr\). This function is an endomorphism of \(M\), in fact \(T_r \in E(M)\) for all \(r \in R\). Let us formalize this link by defining \(\Phi : R \to E(M)\) which sends \(r \to T_r\). Observe:

\[\Phi(r_1 + r_2) = T_{r_1 + r_2} = T_{r_1} + T_{r_2} = \Phi(r_1) + \Phi(r_2),\]

and

\[\Phi(r_1r_2) = T_{r_1r_2},\] where \(T_{r_1r_2} : M \to M\) by \((m)T_{r_1r_2} = m(r_1r_2) \quad \forall m \in M\).

But \(m(r_1r_2) = (mr_1)r_2 = ((m)T_{r_1})T_{r_2} = (m)(T_{r_1}T_{r_2})\). Thus

\[\Phi(r_1r_2) = T_{r_1r_2} = T_{r_1}T_{r_2} = \Phi(r_1)\Phi(r_2).\] Finally, \(\Phi(0) = T_0\), where

\[(m)T_0 = m \cdot 0 = 0 \quad \forall m \in M.\] \(T_0\) is the zero function of \(E(M)\). Thus the mapping \(\Phi\) is a ring homomorphism.
The kernel of $\Phi$ is the set $\{r \in R| T_r = 0, \text{i.e. } mr = 0 \forall m \in M\}$. This is simply $A(M)$, which we know is a two-sided ideal of $R$. Recall that if $R$ and $S$ are rings and $\phi: R \rightarrow S$ is a ring homomorphism, then $\frac{R}{\ker(\phi)} \cong \text{image}(\phi)$. Thus we have established:

**Theorem 2.23**

$\frac{R}{A(M)}$ is isomorphic to a subring of $E(M)$.

**Corollary 2.24**

If $M$ is a faithful $R$-module, i.e., $A(M) = \{0\}$, then $R$ is isomorphic to a subring of $E(M)$.

While our primary topic of study is non-commutative structures, we are also interested in indentifying commutation properties. The relationship between these $T_r$'s and $E(M)$ raises the question: what elements of $E(M)$ commute with the image of $\Phi$, these $T_r$ mappings?

**Definition 2.25** The commuting ring of $R$ on $M$

Let $C(M)$ be the commuting ring of $R$ on $M$, i.e. $C(M) = \{a \in E(M)| T_r a = a T_r, \forall r \in R\}$.

We justify our claim that the set above has the structure of a ring during our proof of the following theorem.
Theorem 2.26 (Schur's Lemma)

If $M$ is irreducible, then $C(M)$ is a division ring.

Proof: The zero and identity functions of $E(M)$ are certainly in $C(M)$. Now let $\alpha, \beta \in C(M)$, and let $T_r \in E(M)$ for any $r \in R$.

$$T_r(\alpha - \beta) = T_r\alpha - T_r\beta = \alpha T_r - \beta T_r = (\alpha - \beta)T_r,$$ and

$$T_r(\alpha \beta) = (T_r\alpha)\beta = \alpha(T_r\beta) = \alpha(\beta T_r) = (\alpha \beta)T_r.$$

So $C(M)$ is at the least a subring of $E(M)$. (While not directly relevant to this particular proof, we observe here that we have not utilized the fact that $M$ is irreducible at this point, i.e. $C(M)$ has the structure of a ring for any $R$-module $M$). To show the existence of multiplicative inverses, we will show that for any $\alpha \in C(M)$, $\alpha$ is one-to-one and onto. Let $\alpha \neq 0 \in C(M)$, and let $S$ be the image of $\alpha$, i.e. $S = (M)\alpha$. $S$ is a subset of $M$ by definition, and because $\alpha$ is an endomorphism of $M$, $\alpha, b \in S \Rightarrow \alpha - b \in S$. Finally, $\forall r \in R$:

$$Sr = (S)T_r = ((M)\alpha)T_r$$

$$= (M)(\alpha T_r) = (M)(T_r\alpha)$$

$$= ((M)T_r)\alpha.$$ But $(M)T_r \subseteq M$, so

$$(M)T_r \alpha \subseteq (M)\alpha$$, which is of course $S$. 

31
Thus \( SR \subseteq S \). We have shown \( S \) is a submodule of \( M \) and since by selection \( \alpha \neq 0 \), \((M)\alpha = S \neq \{0\}\). But \( M \) is irreducible, so if \( S \neq \{0\} \) then \( S \) must equal \( M \). Thus the mapping \( \alpha \) is onto.

To show that \( \alpha \) is one-to-one, let us first note that:

\[(m)\alpha \cdot r = (m)(\alpha_T) = (m)(T,\alpha) = ((m)T,\alpha) = (mr)\alpha.\]

In other words, \((m)\alpha \cdot r = (mr)\alpha\) for all \( m \in M \) and \( r \in R \). This combined with the fact that \( \alpha \) is an additive endomorphism make \( \alpha \) a module homomorphism from \( M \rightarrow S \). So it suffices to show that the kernel of \( \alpha \) is \( \{0\} \). Let \( K \) be the kernel of \( \alpha \).

\((0)\alpha = (0 + 0)\alpha = (0)\alpha + (0)\alpha\), which implies that \((0)\alpha = 0\), and so \( 0 \in K \).

Let \( a, b \in K \). \((a - b)\alpha = (a)\alpha - (b)\alpha = 0 - 0 = 0\). Thus \( a - b \in K \). Finally let \( a \in K \) and \( r \in R \). \((ar)\alpha = (a)\alpha \cdot r \cdot 0 = 0\), which tells us that \( ar \in K \). We have shown that \( K \) is a submodule of \( M \). If \( K \) were \( M \) this would imply that \((M)\alpha = \{0\}\), but \( \alpha \) by selection is not the zero function. Since \( M \) is irreducible and \( K \neq M \), \( K \) must be \( \{0\} \), which forces \( \alpha \) to be a one-to-one mapping.

Thus \( \alpha \) is a bijection, which implies that \( \alpha^{-1} \) exists.

Suppose that \( \alpha^{-1} \notin E(M) \). This implies that there exists \( m_1, m_2 \in M \) such that \((m_1 + m_2)\alpha^{-1} \neq (m_1)\alpha^{-1} + (m_2)\alpha^{-1}\). This implies that \((m_1 + m_2)\alpha^{-1}) \alpha \neq ((m_1)\alpha^{-1} + (m_2)\alpha^{-1}) \alpha\), forcing the contradiction.
that $m_1 + m_2 \neq m_1 + m_2$. Thus $\alpha^{-1} \in E(M)$. To show $\alpha^{-1} \in C(M)$, observe that $\alpha \in C(M) \Rightarrow T_r \alpha = \alpha T_r$ for all $r \in R$. Multiplying on the left and right by $\alpha^{-1}$ yields $\alpha^{-1} T_r = T_r \alpha^{-1}$ for all $r \in R$. Thus $\alpha^{-1} \in C(M)$.

Example 2.27

We showed earlier that for a field $F$, the vector space $F^n$ is an irreducible $F_n$-module, where $F_n$ is the ring of $n \times n$ matrices over $F$. Any element of $F^n$ can of course be written as the sum of basis vectors over the field $F$, and from linear algebra we know that the action of an additive endomorphism can be represented by a unique $n \times n$ matrix over $F$. In fact, $F_n$ is precisely the set of additive endomorphisms of $F^n$. That is, $E(F^n) = F_n$. Schur's lemma then tells us that the center of $F_n$ is a division ring.

Example 2.28

An algebra $A$ is a vector space over a field $F$ equipped with a multiplication that turns $A$ into a ring, and allows the field elements to pass through the ring multiplication, i.e., $(xy)f = x(yf) = (xf)y$ for all $x, y \in A$, and $f \in F$. Let $A$ be the algebra generated by the matrix $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ over $F$.  

33
Observing that $B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $B^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -B$, and $B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, any element of $A$ would have the form $x_1 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + x_2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x_2 & -x_1 \\ x_1 & x_2 \end{pmatrix}$ for some $x_1, x_2 \in F$. We claim that $F^2$ is an irreducible $A$-module.

**Proof:** Since $0 \neq B \in F^2 A$, $F^2 A \neq \{0\}$. Suppose there exists a submodule $N$ of $F^2$, $N \neq \{0\}$. This implies that there exists some $x \in N$ where $x = (a, b)$, each $a, b \in F$ and either $a \neq 0$ or $b \neq 0$. Without loss of generality, assume $a \neq 0$. $N$ is a submodule, thus it is closed under addition and closed under multiplication with $A$. Noting that $B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, we see that

$$x \begin{pmatrix} -b \\ a \end{pmatrix} = \begin{pmatrix} -b \\ a \end{pmatrix},$$
and

$$x \begin{pmatrix} 1 \\ b \\ a \end{pmatrix} = \begin{pmatrix} 1 \\ b \\ a \end{pmatrix}$$

must both be elements of $N$. If $b = 0$, then the vectors $(0,1)$ and $(0,0)$ are in $N$. If $b = a$, we can add and subtract the two vectors above to place $(-2,0)$ and $(0,2)$ in $N$. Multiplying these vectors by $\begin{pmatrix} \pm \frac{1}{2} B^4 \end{pmatrix}$ puts $(1,0)$ and $(0,1)$ in $N$. If $b \neq 0$ and $b \neq a$, then

$$\begin{pmatrix} 1 \\ b \\ a \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \in N, \text{ and } \begin{pmatrix} a \\ b \end{pmatrix} - \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} a^2 + b^2 \\ ab \end{pmatrix}$$

is an element.
of $N$. $F$ is a field, so $a \neq 0, b \neq 0$ imply that the fraction $rac{a^2 + b^2}{ab} \neq 0$. By multiplying the last vector with the matrix

$$\left( \frac{ab}{a^2 + b^2} B^4 \right),$$

we can place $(1,0)$ in $N$. Performing a similar computation will add $(0,1)$ to $N$. Thus in all cases the two vectors $(1,0)$ and $(0,1)$ are in $N$, and for any $c,d \in F$,

$$(c,d) = (1,0)(cB^4) + (0,1)(dB^4) \in N.$$  Thus $N$ must equal $F^2$, proving that $F^2$ is an irreducible $A$-module.

We may now apply Schur's Lemma to $F^2$. The Lemma tells us that the commuting ring of $A$ is a division ring. To find the commuting ring of $A$, we need only solve the following problem:

$$(a \ b)(0 \ -1) = (0 \ -1)(a \ b) \quad \text{for } a,b,c,d \in F.$$  

As long as this matrix commutes with $B$, it will commute with any matrix of the form $\sum_{i=1}^{n} x_i B^i$. Solving the equation above, we get $a = d$, and $b = -c$. This is a matrix of the form,

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

In the special case $F = \mathbb{R}$, the set of all such matrices is isomorphic to the field of complex numbers. \qed
CHAPTER THREE
THE JACOBSON RADICAL

When Nathan Jacobson passed away on December 5th, 1999, it marked the end of a long and distinguished career in mathematics. A student of J.H.M. Wedderburn at Princeton, his doctoral thesis entitled Noncommutative Polynomials and Cyclic Algebras was published in 1934. He taught mathematics at Johns Hopkins and Yale, serving as the department chair at the latter university from 1965-1968. He was president of the American Mathematical Society from 1971-1972, and vice-president of the International Mathematical Union from 1972-1974. He advocated a module-based approach to the study of algebraic systems, and in this chapter we focus on a structure that bears his name.

Definition 3.1(a) The Jacobson radical

The Jacobson radical of $R$, denoted $J(R)$, is the set of elements of $R$ which annihilate all the irreducible $R$-modules, i.e. $J(R)=\{ r \in R | Mr=\{0\} \}$ for all irreducible $R$-modules $M$. If $R$ has no irreducible modules we set $J(R)=R$. 

36
Definition 3.1(b) Semisimple rings

If the Jacobson radical of a ring is \( \{0\} \), we say the ring is semisimple.

There are other radicals that are used in the analysis of structures of rings. Our approach mirrors Herstein's, and we exclusively use the Jacobson radical. Thus, when we mention "radical" in this paper, we will always intend the Jacobson radical. Our goal in this chapter will be to describe the radical in terms of ideals of \( R \), and to do so, we must first introduce several structures.

Definition 3.2

For a right ideal \( \rho \) of \( R \), let \( (\rho: R) = \{a \in R | Ra \subseteq \rho\} \).

Lemma 3.3

The set \( (\rho: R) \) is a two-sided ideal of \( R \).

Proof: \( R \cdot 0 = 0 \subseteq \rho \), thus \( 0 \in (\rho: R) \). Let \( a, b \in (\rho: R) \). This implies that \( ra, rb \in \rho \) for all \( r \in R \). But \( \rho \) is a right ideal of \( R \), so \( ra - rb = r(a - b) \in \rho \) for all \( r \in R \). Thus \( a - b \in (\rho: R) \). For any \( a \in (\rho: R) \) and \( r \in R \), observe \( R(ar) = (Ra)r \subseteq (\rho)r \subseteq \rho \) since \( \rho \) is a right ideal of \( R \). Finally, we note that \( R(ra) = (Rr)a \subseteq Ra \subseteq \rho \). Thus \( (\rho: R) \) is a two-sided ideal of \( R \).
Definition 3.4 Right-quasi-regularity

An element $a$ in a ring $R$ is called right-quasi-regular in $R$ if there exists an $a' \in R$ such that $a + a' + aa' = 0$. We call $a'$ the right-quasi-inverse of $a$. Why right-quasi-regular? The element $a'$ acts on $a$ from the right. Left-quasi-regularity is similarly defined. An ideal of $R$ is called right-quasi-regular if each of its elements is right-quasi-regular.

Lemma 3.5

Let $a \in R$ be right-quasi-regular and left-quasi-regular in $R$. The left-quasi-inverse and right-quasi-inverse of $a$ are identical.

Proof: Let $b$ be a right-quasi-inverse of $a$, and let $c$ be a left-quasi-inverse of $a$. Thus $a + b + ab = 0$, and $a + c + ca = 0$. Left-multiplying both sides of the first equation by $c$ and right-multiplying both sides of the second equation by $b$ yields $ca + cb + cab = 0$, and $ab + cb + cab = 0$. Setting these two equations equal to one another yields $ca = ab$. Applying this equality back to our two original equations forces the result $b = c$. 

38
Lemma 3.6

Given a ring $R$ with a two-sided unit element, $a \in R$ is right-quasi-regular if and only if $1+a$ is right-invertible in $R$.

Proof: ($\Rightarrow$) $a$ is right-quasi-regular implies that there exists some $a' \in R$ such that $a+a'+aa'=0$. Thus, $a+(1+a)a'=0$, and $1+a+(1+a)a'=1$. Factoring out the common term, we end up with the desired result, $(1+a)(1+a')=1$.

($\Leftarrow$) $1+a$ is right-invertible implies there exists some $b \in R$ such that $(1+a)b=1$. Therefore $(1+a)ba=a$, and $a-ba-aba=0$. If we allow $a'=-ba$, we can rewrite the equation in the desired form, $a+a'+aa'=0$. \hfill \Box

Definition 3.7 Nil-nilpotent ideals and elements

Let $\rho$ be a right ideal of $R$. If there exists some $k \in \mathbb{N}$ such that $r_1 \cdot r_2 \cdot \ldots \cdot r_k = 0$ for any elements $r_1, r_2, \ldots, r_k \in \rho$, we call $\rho$ a nilpotent ideal. An individual element $x \in \rho$ is called nilpotent if there exists some $m \in \mathbb{N}$ such that $x^m = 0$. Finally, we say that $\rho$ is a nil ideal if all of its elements are nilpotent.
Corollary 3.8

If $\rho$ is a nilpotent ideal of $R$, then $\rho$ is a nil ideal of $R$.

Proof: If $\rho$ is a nilpotent ideal of $R$, then there exists some $k \in \mathbb{N}$ such that $r_1 \cdot r_2 \cdot \ldots \cdot r_k = 0$ for all $r_1, r_2, \ldots, r_k \in \rho$. In particular, $r \cdot r \cdot \ldots \cdot r = r^k = 0$ for any $r \in \rho$. 

Example 3.9

Consider $\mathbb{R}_3$, the ring of 3x3 matrices over $\mathbb{R}$. Let

$$S = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\} \subseteq \mathbb{R}_3.$$ Then $S$ is a ring under the operations inherited from $\mathbb{R}_3$. To show this, first observe that by choosing $a = b = c = 0$, the zero matrix is in $S$. The various ring properties are all inherited from $\mathbb{R}_3$, and closure under addition follows from the definition of matrix multiplication. Let $A = [a_{ij}], B = [b_{ij}] \in S$, and let $A \cdot B = C = [c_{ij}]$. To show that $S$ is closed under multiplication, we need to prove that component-wise, the first column, third row, and middle element of $C$ are all zero. For
\(i = 1, \ldots, 3\), see that 
\[ c_{ij} = \sum_{k=1}^{3} a_{ik} \cdot b_{kj} = \sum_{k=1}^{3} a_{ik} \cdot 0 = 0. \]
For \(j = 1, \ldots, 3\) note
\[ c_{3j} = \sum_{k=1}^{3} a_{3k} \cdot b_{kj} = \sum_{k=1}^{3} 0 \cdot b_{kj} = 0. \]
Finally observe that
\[ c_{22} = 0 \cdot b_{12} + 0 \cdot 0 + a_{23} \cdot 0 = 0. \]
Thus \(C\) is in \(S\), and \(S\) is closed under multiplication. \(S\) is a ring.

If \(S\) has the structure of a ring, it may certainly be considered a right ideal of itself.

Per definition 3.7, it follows that the matrix
\[
A = \begin{pmatrix}
0 & 1 & 1 \\
0 & 0 & 1 \\
0 & 0 & 0
\end{pmatrix}
\]
\(A \in S\) is nilpotent because \(A^3 = [0]\). In fact, any matrix of \(S\) if cubed will yield the zero matrix. This fact makes \(S\) nil. However, we note that the product is zero not because of the particular choice of matrix elements, but because of the structure of the matrices themselves. We can see this clearly using the matrix \(C\) above, the product of any two elements of \(S\). See that 
\[ c_{12} = 0 \cdot b_{12} + a_{12} \cdot 0 + a_{13} \cdot 0 = 0, \]
and that 
\[ c_{23} = 0 \cdot b_{13} + 0 \cdot b_{23} + a_{23} \cdot 0 = 0. \]
Taken together with what was shown earlier, we see that \(C\) is of the form
\[
\begin{pmatrix}
0 & 0 & \ast \\
0 & 0 & 0 \\
0 & 0 & 0
\end{pmatrix}
\]
if right (or left) multiplied by any element of \(S\), yields
the zero matrix. We have shown that for any $A_1, A_2, A_3 \in S$, the product $A_1 \cdot A_2 \cdot A_3 = [0]$. Thus $S$ is not just nil, but nilpotent, as a right ideal of $S$.

**Example 3.10**

Let $R$ be the ring $\mathbb{Z}/p\mathbb{Z}$, where $p$ is a prime number. We claim that $R$ does not have any non-zero nilpotent elements. Suppose it did. This implies that $(p+r)^m \equiv 0 \pmod{p}$ for some $r \in \mathbb{N}$ where $1 \leq r < p$, and so that $p$ divides $(p+r)^m$. This implies that $p | r^m$. But recall that $1 \leq r < p$, and so $p | r$. Since $p$ is prime, $p | r^m$. A contradiction. $\mathbb{Z}/p\mathbb{Z}$ does not have a non-zero nilpotent element. While we do not prove it here, it can be shown that if the prime factorization of a natural number $n$ does not have a prime factor of degree greater then $1$, then $\mathbb{Z}/n\mathbb{Z}$ will not have a nilpotent element.

**Lemma 3.11**

Every nil right ideal of $R$ is right-quasi-regular.

**Proof:** Let $\rho$ be a nil right ideal of $R$, and let $a \in \rho$. We know there exists some $m \in \mathbb{N}$ such that $a^m = 0$. For some $b \in \rho$, $b = -a + a^2 - a^3 + \ldots + (-1)^{m-1}a^{m-1}$. Right multiplying both sides
by $a$, yields $ab = -a^2 + a^3 - a^4 + \ldots + (-1)^{m-1}a^m$. Adding these two equations creates the equation $b + ab = -a + a^m$. But $a^m = 0$, so $a + b + ab = 0$. Thus $a$ is right-quasi-regular for every $a \in \rho$. \qed

Lemma 3.12

If $\rho$ is a regular right ideal of $R$ that is properly contained in $R$, there exists a maximal right ideal $\rho_0$ of $R$ that contains $\rho$. Further, $\rho_0$ is regular in $R$.

Proof: If $\rho$ is regular, there exists some $a \in R$ such that $x - ax \in \rho$ for all $x \in R$. If $a \in \rho$, $\rho = R$. (Lemma 2.18). However, $\rho$ is properly contained in $R$, so this is impossible. Thus $a \notin \rho$. Let $\Psi$ be the set of all proper right ideals of $R$ that contain $\rho$ and do not contain the element $a$. Certainly $\rho \in \Psi$ so the set $\Psi$ is nonempty. Zorn’s Lemma tells us that any partially-ordered set that has an upper bound has a maximal element. The upper bound of $\Psi$ is $R$, and the relation of set containment satisfies the partially-ordered condition. Thus the set $\Psi$ has a maximal element in $R$, call it $\rho_0$. Recall that $x - ax \in \rho$ for all $x \in R$. As an element of $\Psi$, this ideal $\rho_0$ properly
contains \( p \). Therefore \( x - ax \in p \subseteq p_0 \) for all \( x \in R \), and so \( p_0 \) is regular.

It is worth noting that not every maximal right ideal is regular. Consider the ring \( 2\mathbb{Z} \), and the right ideal \( 4\mathbb{Z} \). It is easy to see that \( 4\mathbb{Z} \) is a maximal two-sided and certainly right ideal of \( 2\mathbb{Z} \). However, it is not regular. Suppose there existed some element \( a \in 2\mathbb{Z} \) such that \( x - ax \in 4\mathbb{Z} \) for all \( x \in 2\mathbb{Z} \). This statement must be true for all \( x \in 2\mathbb{Z} \), and in particular the element \( 6 \in 2\mathbb{Z} \). Thus \( 6 - a \cdot 6 \in 4\mathbb{Z} \). But \( a \in 2\mathbb{Z} \), which implies \( a = 2q \) for some \( q \in \mathbb{Z} \). If \( 6 - a \cdot 6 \in 4\mathbb{Z} \), then \( 6 - 2q \cdot 6 = 6(1 - 2q) \) must be divisible by 4. But \( (1 - 2q) \) is odd, and so this cannot be. No such \( a \) exists, i.e. \( 4\mathbb{Z} \) is not regular.

We are ready to begin our examination of the radical. Recall that \( J(R) \) is defined to be the set of elements of \( R \) that annihilate all irreducible \( R \)-modules. The zero element of \( R \) will always be in \( J(R) \), and so we know \( J(R) \neq \emptyset \). Remember that for any given \( R \)-module \( M \), we have collected its annihilators in \( R \) into one set, \( A(M) \). Thus \( J(R) = \cap A(M) \), as \( M \) ranges across all irreducible \( R \)-modules. Recall however that each \( A(M) \) is a two-sided ideal of \( R \) and that
the intersection of a set of two-sided ideals is a 2-sided ideal. Thus we have proven that:

**Lemma 3.13**

\[ J(R) \text{ is a two-sided ideal of } R. \]

We'd like to take this result one step further. Let \( R \) be a ring, and let \( M \) be an irreducible \( R \)-module. In Theorem 2.19, we proved that \( M \) is isomorphic to \( \frac{R}{\rho} \) for some maximal regular right ideal \( \rho \) of \( R \). In this instance, what is \( A(M) \)?

**Lemma 3.14**

Let \( R \) be a ring, and let \( M \) be an irreducible \( R \)-module. Then \( A(M) = (\rho:R) \), and the set \( A(M) = (\rho:R) \) is contained in \( \rho \).

**Proof:** As an irreducible \( R \)-module, \( M \cong \frac{R}{\rho} \) for some maximal regular right ideal \( \rho \) of \( R \). Now let \( x \in A(M) \). This implies that \( Mx = \{0\} \), or in other words, \((r+\rho)x = rx + \rho = 0 + \rho \) for all \( r \in R \). This implies that \( rx \in \rho \) for all \( r \in R \), which tells us that \( x \in (\rho:R) \). To prove the reverse inclusion, let \( x \in (\rho:R) \). This implies \( Rx \subseteq \rho \). For any \( r \in R \), there exists some \( a \in \rho \) such that \((r+\rho)x = rx + \rho = a + \rho \). But if \( a \in \rho \), then \( a + \rho \) is actually the zero element of \( \frac{R}{\rho} \), and so \((r+\rho)x = 0 + \rho \).
for all $r \in R$. The element $x$ annihilates all of $\frac{R}{\rho}$, and so $x \in A(M)$. We have shown that $A(M) = (\rho : R)$.

Now let's prove that $A(M)$ is contained in $\rho$. Let $x \in (\rho : R)$. The definition of $(\rho : R)$ tells us that $Rx \subseteq \rho$. Recall that, as a regular right ideal, there exists an $a \in R$ such that $x - ax \in \rho$. If $Rx \subseteq \rho$, certainly $ax \in \rho$. Finally, if $x - ax$ and $ax$ are in $\rho$, $(x - ax) + ax = x \in \rho$. \quad \square

Theorem 3.15

$J(R) = \cap \rho$, where $\rho$ ranges across all maximal regular right ideals of $R$. Further, $J(R)$ is both right-quasi-regular and left-quasi-regular in $R$.

Proof: To show that $J(R) \subseteq \cap \rho$, recall that $J(R) = \cap A(M)$, where $M$ ranges across all irreducible $R$-modules. However, each such $M$ is isomorphic to $\frac{R}{\rho}$ for some maximal regular right ideal $\rho$ of $R$. Moreover for any such $\rho$, $\frac{R}{\rho}$ is an irreducible $R$-module. (Theorem 2.19). Thus $J(R) = \cap A(\frac{R}{\rho})$, for all maximal regular right ideals $\rho$ of $R$. In Lemma 3.14, we showed that for such ideals, $A(\frac{R}{\rho}) = (\rho : R)$, and each
Thus \( J(R) = \cap (\rho : R) \subseteq \cap \rho \). We have proven the first inclusion.

To complete our proof, we need to show that \( \cap \rho \subseteq J(R) \). Let \( x \in \cap \rho \). We’d first like to show that \( x \) is right-quasi-regular.

Let \( S = \{ xy + y | y \in R \} \). Then \( S \) is a regular right ideal of \( R \), as follows. If we select \( y = 0 \), \( x \cdot 0 + 0 = 0 \in S \). Now let \( a, b \in S \). This implies that there exists \( y', y'' \in R \) such that \( a = xy' + y' \) and \( b = xy'' + y'' \). Observe that \( a - b = x(y' - y'') + (y' - y'') \), and since \( R \) is a ring, \( y' - y'' \in R \). This places \( a - b \in S \).

Similarly relying on \( R \)'s closure property for multiplication, we can show that \( a \in S, r \in R \Rightarrow ar \in S \). Hence \( S \) is a right ideal of \( R \). To prove that \( S \) is regular, we need to find a \( b \in R \) such that \( y - by \in S \) for all \( y \in R \). If we let \( b = -x \), the structural definition of \( S \) will make \( S \) regular.

We now wish to show \( S = R \). Suppose not. Lemma 3.12 tells us there must exist a maximal regular right ideal \( \rho_0 \) of \( R \) such that \( \rho_0 \supseteq S \). The intersection of right ideals is a right ideal, so if \( x \in \cap \rho \), \( xr \in \cap \rho \) for all \( r \in R \). This tells us that for all \( r \in R \), \( xr \in \rho \) for any maximal regular right ideal \( \rho \) of \( R \), including \( \rho_0 \). We also know \( \rho_0 \) contains \( S \),
which implies that $xr + r \in \rho_0$ for all $r \in R$. Taken together, $xr + r \in \rho_0$ and $xr \in \rho_0$ imply $r = xr + r - xr \in \rho_0$ for all $r \in R$. But then $\rho_0$ must equal $R$, which contradicts the fact that $\rho_0$ is maximal, hence proper, in $R$. Thus $S$ must equal $R$. This implies that every element of $R$ has the form $xy + y$ for some $y \in R$. Specifically, $-x = xz + z$ for some $z \in R$, in other words, $x + z + xz = 0$. We have shown that any element of $\cap \rho$ is right-quasi-regular.

Recall that our primary goal was to show that the $\cap \rho \subseteq J(R)$. Suppose not. This implies that there exists an irreducible $R$-module $M$ and an element $m \in M$ such that $m(\cap \rho) \neq \{0\}$. Since $M$ is an $R$-module, the set $m(\cap \rho)$ is a submodule of $M$. To prove this, we will show that $m(\cap \rho)$ is closed under subtraction and multiplication with $R$. Let $a, b \in m(\cap \rho)$. This implies that there exists $r_1, r_2 \in \cap \rho$ such that $a = mr_1$ and $b = mr_2$. But $\cap \rho$ is a right ideal of $R$, so $r_1, r_2 \in \cap \rho$ implies $r_1 - r_2 \in \cap \rho$. Thus $a - b = mr_1 - mr_2 = m(r_1 - r_2) \in m(\cap \rho)$. Again using the fact that $\cap \rho$ is a right ideal of $R$, we see that $m(\cap \rho) \cdot R = m(\cap \rho \cdot R) \subseteq m(\cap \rho)$. The set $m(\cap \rho)$ is a submodule of $M$. But $M$ is irreducible, so the only submodules of $M$ are $\{0\}$.
and $M$ itself. We established earlier that $m(\cap \rho) \neq \{0\}$, which forces $m(\cap \rho) = M$. This means that any element of $M$ is of the form $mr$ for some $r \in \cap \rho$. The element $-m$ is of course in $M$, thus $-m = mt$ for some $t \in \cap \rho$. Now because $t \in \cap \rho$, $t$ is right-quasi-regular. So there exists some $s \in R$ such that $t + s + ts = 0$. Left multiplying both sides by $m$ yields the equation $mt + ms + mts = 0$. Substituting with the expression $-m = mt$ yields $mt + (-mt)s + mts = 0$, or simply $mt = 0$. Since $-m = mt$, this implies $m = 0$, and $m(\cap \rho) = \{0\}$. This is a contradiction. Thus $\cap \rho \subseteq J(R)$, and with that, our result is proved: $J(R) = \cap \rho$. Since every element of $\cap \rho$ is right-quasi-regular, we may conclude that $J(R)$ is right-quasi-regular.

To show that $J(R)$ is left-quasi-regular, let $a \in J(R)$. Since $J(R)$ is right-quasi-regular, there exists some $a' \in R$ such that $a + a' + aa' = 0$, or $a' = -(a + aa')$. But $J(R)$ is a two-sided ideal of $R$, so $a \in J(R) \Rightarrow aa' \in J(R)$, and so $-(a + aa') \in J(R)$. This tells us that $a' \in J(R)$, and so must be right-quasi-regular. Thus there must exist some $a'' \in R$ such that $a' + a'' + a'a'' = 0$. We see then that $a'$ has $a$ as a left-quasi-inverse, and $a''$ as a right-quasi-inverse. By Lemma 3.5, we conclude that $a = a''$, and so that $a' + a + a'a = 0$. Thus the element $a$ is left-quasi-
regular in $R$. Since $a$ was an arbitrary element of $J(R)$, we may conclude that the radical is a left-quasi-regular ideal of $R$. □

Example 3.16

$Z$ is a semisimple ring. What is the Jacobson radical of $Z$? Theorem 3.15 tells us that $J(Z) = \bigcap \rho$, where $\rho$ ranges through all maximal regular right ideals of $Z$. Set theory tells us that the intersection of all maximal regular right ideals of $Z$ is contained in the intersection of any set of maximal regular right ideals of $Z$. Thus to prove $J(Z) = \{0\}$, we need only find a set of such ideals whose intersection is $\{0\}$. Consider the two-sided and therefore right ideal $pZ$, where $p$ is prime. $pZ$ is regular because $x - 1 \cdot x = 0 \in pZ$ for all $x \in Z$. To show $pZ$ is maximal, suppose there existed an ideal $S$ such that $pZ \subseteq S \subseteq Z$. Pick an $a \in S$ that is not in $pZ$. $a \notin pZ$ implies that $a$ and $p$ are relatively prime. Thus there exists $b, c \in Z$ such that $ab + pc = 1$. Since $S$ is a two-sided ideal, and $a, p \in S$, we may conclude that $1 \in S$. This puts all of $Z$ in $S$, a contradiction. $pZ$ is maximal, and the intersection of $pZ$ as $p$ ranges over the infinite set of
prime numbers is \( \{0\} \). Therefore, \( J(\mathbb{Z}) = \cap p \subseteq \cap p \mathbb{Z} = \{0\} \), and \( \mathbb{Z} \) is a semisimple ring.

Example 3.17

\( \mathbb{R}_2 \) is a semisimple ring. Let us use a similar approach to find \( J(\mathbb{R}_2) \), where \( \mathbb{R}_2 \) is the ring of \( 2 \times 2 \) matrices over \( \mathbb{R} \). In Example 2.17, we proved that the set of matrices over \( \mathbb{R}_2 \) \( \rho_1 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} | a, b \in \mathbb{R} \right\} \) is a maximal right ideal of \( \mathbb{R}_2 \). We need to prove this set is regular. Observe that \( x-\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot x = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \rho_1 \) for all \( x \in \mathbb{R}_2 \), and so \( \rho_1 \) is a maximal regular right ideal of \( \mathbb{R}_2 \). A similar approach will show that \( \rho_2 = \left\{ \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} | a, b \in \mathbb{R} \right\} \) is also a maximal regular right ideal of \( \mathbb{R}_2 \). Now \( J(\mathbb{R}_2) = \cap \rho \subseteq \rho_1 \cap \rho_2 \), and since \( \rho_1 \cap \rho_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} \), we have \( J(\mathbb{R}_2) = \{0\} \). Thus \( \mathbb{R}_2 \) is semisimple.

While our primary focus in this paper will be rings that are semisimple, we give brief attention to a ring whose Jacobson radical is not \( \{0\} \). Consider the ring \( 2\mathbb{Z} \). We showed earlier that the right ideal \( 4\mathbb{Z} \) of \( 2\mathbb{Z} \) is maximal
but not regular in \(2\mathbb{Z}\). In fact, \(2\mathbb{Z}\) has no maximal regular right ideals. Therefore by Theorem 2.19 \(2\mathbb{Z}\) has no irreducible \(2\mathbb{Z}\)-modules, and thus per Definition 3.1(a), 
\[ J(2\mathbb{Z}) = 2\mathbb{Z}. \]

We have learned several facts about the structure of 
\(J(R)\). It is a two-sided ideal of \(R\), it is a right-quasi-regular ideal, and it is the intersection of all of the maximal regular right ideals of \(R\). We can say more about the relationship of \(J(R)\) to other ideals of \(R\).

**Theorem 3.18**

Any right-quasi-regular right ideal of \(R\) is contained in \(J(R)\).

**Proof:** This proof is similar to that used in Theorem 3.15. Let \(\rho\) be a right-quasi-regular right ideal of \(R\), and suppose \(\rho \not\subset J(R)\). This implies that there exists an irreducible \(R\)-module \(M\) and an \(m \in M\) such that \(m\rho \neq \{0\}\). The fact that \(m\rho\) is a non-zero submodule of \(M\) and that \(M\) is irreducible forces \(m\rho = M\). This implies that there exists a \(t \in \rho\) such that \(mt = -m\). Since \(t \in \rho\), there exists an \(s \in R\) such that \(t + s + ts = 0\), which implies that 
\[ mt + ms + mts = 0. \]
Substituting for \( mt \) yields \(-m + ms + (-m)s = 0\). This implies \( m = 0 \), and \( m\rho = \{0\}\). A contradiction.

\[ \text{Corollary 3.19} \]

Every nil ideal and every nilpotent ideal of \( R \) is contained in \( J(R) \).

\[ \text{Proof:} \quad \text{In Corollary 3.8 we showed that every} \]

nilpotent ideal of \( R \) is nil, and in Lemma 3.11 we showed that every nil ideal is right-quasi-regular. Theorem 3.14 completes the proof.

We proved earlier that the radical is a two-sided ideal of \( R \). Because of this, we may create a quotient ring using \( J(R) \). For any \( a, b \in R \), addition in \( \frac{R}{J(R)} \) will be given by \((a + J(R)) + (b + J(R)) = ((a + b) + J(R))\) and the multiplication by \((a + J(R))(b + J(R)) = (ab + J(R))\). To prove that the multiplication is well-defined, let \( a + J(R) = a' + J(R) \) and \( b + J(R) = b' + J(R) \). This implies \( a - a', b - b' \in J(R) \). We see

\[ ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \]. But \( a - a', b - b' \in J(R) \), and \( J(R) \) is a two-sided ideal of \( R \). This tells us that

\( (a - a')b + a(b - b') = ab - a'b' \in J(R) \). Thus \( a + J(R) = a' + J(R) \), and so

\( (a + J(R))(b + J(R)) = (a' + J(R))(b' + J(R)) \).
Theorem 3.20

For every ring $R$, $R/J(R)$ is semisimple, i.e.

$J\left(\frac{R}{J(R)}\right) = \{0\}$.

Proof: Let $\overline{R} = \frac{R}{J(R)} = \{\overline{x} = x + J(R) | x \in R\}$. Define $\phi: R \to \overline{R}$ by $\phi(r) = \overline{r}$. We notice at once that $\ker \phi = J(R)$. We wish to show that $\phi$ is a ring homomorphism. For any $r_1, r_2 \in R$,

$\phi(r_1 + r_2) = (r_1 + r_2) + J(R) = (r_1 + J(R)) + (r_2 + J(R)) = \phi(r_1) + \phi(r_2)$, and

$\phi(r_1 r_2) = r_1 r_2 + J(R) = (r_1 + J(R))(r_2 + J(R)) = \phi(r_1)\phi(r_2)$. We see that $\phi$ is indeed a ring homomorphism.

Now let $\rho$ be a maximal regular right ideal of $R$, and let $\overline{\rho} = \phi(\rho)$, the image of $\rho$ in $\overline{R}$. We will prove that $\overline{\rho}$ is a maximal regular right ideal of $\overline{R}$. As $\rho$ is a right ideal of $R$, and because $\phi$ preserves ring structure, $\overline{\rho}$ will be a right ideal of $\overline{R}$. The fact that $\rho$ is regular implies that there exists an $a \in R$ such that $x - ax \in \rho$ for all $x \in R$. The corresponding element in $\overline{\rho}$ will be $\overline{a}$. Let $\overline{x} \in \overline{R}$. We need to show that $\overline{x} - \overline{ax} \in \overline{\rho}$. If $\overline{x} \in \overline{R}$ this implies that there exists an $x \in R$ such that $\phi(x) = \overline{x}$. We know that $x - ax \in \rho$. This places $\phi(x - ax) = \phi(x) - \phi(a)\phi(x) = \overline{x} - \overline{ax} \in \overline{\rho}$, and so $\overline{\rho}$ is regular. To
show that $\bar{\rho}$ is maximal, suppose not. This implies that there exists a right ideal $\bar{I}$ of $\bar{R}$, such that $\bar{\rho} \subseteq \bar{I} \subseteq \bar{R}$ or $\bar{\rho} = \bar{R}$. Let $S = \{x \in R \mid \phi(x) \in I\}$. As $\bar{I}$ is a right ideal of $\bar{R}$, and $\phi$ is a ring homomorphism, we may conclude that $S$ is a right ideal of $R$. Since $\bar{\rho} \subseteq \bar{I}$ we have that $S$ contains $\rho$. That fact makes $S$ regular. Finally, $\bar{I} \subseteq \bar{R}$ implies that there exists some $\bar{x} \in \bar{R}$, $\bar{x} \not\in \bar{I}$. As $\phi$ is an onto mapping, this implies that there exists at least one $a \in R$, $a \not\in S$. Thus $S$ is a proper subset of $R$, contains $\rho$, is regular, and is a right ideal of $R$. Taken together, this contradicts the fact that $\rho$ is a maximal regular right ideal of $R$. Thus the supposed $\bar{I}$ cannot exist. We have proven this statement: if $\rho$ is a maximal regular right ideal of $R$, $\bar{\rho}$ is a maximal regular right ideal of $\bar{R}$.

With this tool in hand, we return to our original goal, to show that $J(\bar{R}) = \{0\}$. By Theorem 3.15, we know that $J(\bar{R}) = \cap \bar{\rho}$, where $\bar{\rho}$ ranges across all the maximal regular right ideals of $\bar{R}$. Similarly, $J(R) = \cap \beta$ where $\beta$ ranges across all the maximal regular right ideals of $R$. We have
proven that for any $\beta$, $\overline{\beta}$ is a maximal regular right ideal of $\overline{R}$. Thus $\{0\} = \phi(J(R)) = \phi(\cap \beta) = \cap \overline{\beta}$. Since $J(\overline{R})$ is the intersection of all of the maximal regular right ideals of $\overline{R}$, it must be contained in the intersection of any maximal regular right ideals of $\overline{R}$, and so $J\left(\frac{R}{J(R)}\right) = J(\overline{R}) = \cap \rho \subseteq \cap \beta = \{0\}$. □

In later sections we will study the structure of rings that are semisimple. The importance of Theorem 3.20 is that if $R$ is a ring that is not semisimple, we may consider $R$ mod its radical, which is semisimple. The resulting ring, $\frac{R}{J(R)}$, though 'smaller' in some sense then $R$, preserves much of the ring structure of $R$. $\frac{R}{J(R)}$ represents a compromise. It has been modified to some extent to allow for further examination, but it has not been modified to such a degree as to lose the essential structure of the original ring. In some cases information from $\frac{R}{J(R)}$ may be "lifted" to $R$.  

56
We now have a technique by which to find the radical of a ring. Once the radical is known, we can use this information to derive the radical of ideals related to $R$.

**Theorem 3.21**

Let $A$ be a two-sided ideal of $R$. $A$ itself has the structure of a ring, and $J(A) = A \cap J(R)$.

**Proof:** Let $A$ be a two-sided ideal of $R$. By Lemma 1.4, $A$ has the structure of a ring. We will first show that $A \cap J(R) \subseteq J(A)$. Let $x \in A \cap J(R)$. This implies that $x \in A$ and $x \in J(R)$. As an element of $J(R)$, $x$ must be right-quasi-regular in $R$, i.e. there exists some $x' \in R$ such that $x + x' + xx' = 0$, or $x' = -x - xx'$. But if $x$ is an element of $A$, which is a two-sided ideal of $R$, $xx' \in A$. $A$ is an ideal of $R$ also forces $-x, -xx' \in A$. We see then that $x' = -x - xx' \in A$. The element $x$, and thus the set $A \cap J(R)$, is right-quasi-regular not only in $R$, but in $A$. Since $A$ and $J(R)$ are both two-sided ideals of $R$, their intersection will be a two-sided ideal of $R$. But clearly $A \cap J(R) \subseteq A$, so we can make a stronger claim, $A \cap J(R)$ is an ideal of $A$. Thus $A \cap J(R)$ is a right-quasi-regular right ideal of $A$, and so by Theorem 3.18 must be contained in $J(A)$. 

57
To prove the reverse inclusion, let $p$ be a maximal regular right ideal of $R$, and let $p_A = A \cap p$. Suppose $A \not\leq p$.

We'd like to show that $\frac{R}{p} \not\cong \frac{A}{p_A}$ as modules over $R$. First observe that $A + p$ is an ideal of $R$, and since $A \not\leq p$, $A + p$ properly contains $p$. But $p$ is maximal, which forces $A + p = R$. Thus $\frac{R}{p} = \frac{(A + p)}{p}$. We claim that $\frac{(A + p)}{p} = \frac{A}{p}$. To prove this, let $x \in \frac{(A + p)}{p}$. This implies that $x = (a + p_1) + p_2 = a + (p_1 + p_2)$ for some $a \in A$ and $p_1, p_2 \in p$. Because $p$ is an ideal, $p_1 + p_2 \in p$, and so $x$ is of the form $A + p$, which allows us to conclude that $x \in \frac{A}{p}$. Now let $x \in \frac{A}{p}$. This implies $x = a + p$ for some $a \in A$ and $p \in p$. Thus $x = (a + 0) + p$, and since $0 \in p$, $x$ is of the form $(A + p) + p$. $x \in \frac{(A + p)}{p}$, and $\frac{(A + p)}{p} = \frac{A}{p}$.

Finally, we claim that $\frac{A}{p} \not\cong \frac{A}{p_A}$ as modules over $R$.

Define $\phi: \frac{A}{p} \rightarrow \frac{A}{p_A}$ by $(a + p) \mapsto (a + p_A)$ for all $a \in A$. To show $\phi$ is well-defined, let $a_1 + p = a_2 + p$ for some $a_1, a_2 \in A$. This implies that $a_1 - a_2 \in p$. But $A$ is an ideal, so
\[ a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A. \] Thus \[ a_1 - a_2 \in A \cap \rho = \rho_A, \] and so \[ a_1 + \rho_A = a_2 + \rho_A. \]

\( \phi \) is well-defined. We see that \( \phi \) is onto, and to show \( \phi \) is one-to-one, we need to prove \( a_1 + \rho_A = a_2 + \rho_A \) implies \( a_1 + \rho = a_2 + \rho \) for all \( a_1, a_2 \in A \). This is essentially the reverse of what was done to prove \( \phi \) is well-defined. \( \phi \) is a bijection. All we have left to do is show that \( \phi \) is a module isomorphism. Let \( a_1 + \rho, a_2 + \rho \in A/\rho \) and \( r \in R \).

\[
((a_1 + \rho) + (a_2 + \rho))\phi = ((a_1 + a_2) + \rho)\phi \\
= (a_1 + a_2) + \rho_A = (a_1 + \rho_A) + (a_2 + \rho_A) \\
= (a_1 + \rho)\phi + (a_2 + \rho)\phi.
\]

Now see that

\[
((a_1 + \rho)r)\phi = (a_1 + \rho)\phi = a_1 r + \rho_A \\
= (a_1 + \rho_A)r = ((a_1 + \rho)\phi)r.
\]

\( \phi \) is a module isomorphism.

We have so far shown that \( R/\rho = (A + \rho)/\rho = A/\rho \cong A/\rho_A \). We next will prove that \( \rho_A \) is a maximal regular right ideal of \( A \). \( \rho_A \) by construction is a right ideal of \( A \). \( \rho \) is regular implies that there exists a \( b \in R \) such that \( x - bx \in \rho \) for all \( x \in R \). We must find an \( a \in A \) such that \( x - ax \in \rho_A \) for all \( x \in A \).

Recall that \( R = A + \rho \), so \( b = a + r \) for some \( a \in A \) and \( r \in \rho \). Let \( x \in A \). We know that \( x - bx \in \rho \), and substituting \( b = a + r \) yields
But \( r \in \rho \), and so \( rx \in \rho \). If 

\[(x-ax)-rx \in \rho \quad \text{and} \quad rx \in \rho, \]

\( x-ax \) must be in \( \rho \). Noting that by selection \( x, a \in A \), we may conclude that \( x-ax \in A \). Thus \( x-ax \in A \cap \rho = \rho_A \) for all \( x \in A \). \( \rho_A \) is regular in \( A \).

To prove that \( \rho_A \) is maximal in \( A \), assume it is not. Thus there exists some right ideal \( S \) such that \( \rho_A \subseteq S \subseteq A \).

Since \( S \) properly contains \( \rho_A \) and is itself a proper subset of \( A \), we may conclude that \( \frac{S}{\rho_A} \neq \{0\} \) and \( \frac{S}{\rho_A} \neq \frac{A}{\rho_A} \). \( \frac{S}{\rho_A} \) is a submodule of \( \frac{A}{\rho_A} \) over \( R \). But this implies that the isomorphic pre-image of \( \frac{S}{\rho_A} \) in \( \frac{R}{\rho} \) is also a non-zero proper submodule of \( \frac{R}{\rho} \) over \( R \). This cannot be true as \( R \) is irreducible. Thus the ideal \( S \) cannot exist, and \( \rho_A \) is a maximal regular right ideal of \( A \).

Recall that \( J(A) = \cap I \) as \( I \) ranges across all maximal regular right ideals of \( A \), and that each \( \rho_A = A \cap \rho \) for some maximal regular right ideal \( \rho \) of \( R \) that does not contain \( A \). We see that \( J(A) = \cap I \subseteq \rho_A \) as \( \rho \) ranges across all maximal regular right ideals of \( R \) that do not contain \( A \). If \( A \subseteq \rho \), \( \rho_A = A \cap \rho = A \), and the same statement holds true.
Concluding see that $J(A) \subseteq \cap \rho_A = \cap (\rho \cap A) = (\cap \rho) \cap A = J(R) \cap A$. We have proven our second set inclusion, and so our result. \(\Box\)

**Corollary 3.22**

If $R$ is semisimple, i.e. $J(R) = \{0\}$, then every two-sided ideal of $R$ is semisimple.

**Theorem 3.23**

Let $R$ be a ring. The Jacobson radical of the ring of $n \times n$ matrices over $R$ is the ring of $n \times n$ matrices over $J(R)$. That is, $J(R_n) = J(R)_n$.

**Proof:** Let $M$ be an irreducible $R$-module, and consider the additive abelian group $M'' = \{(m_1, \ldots, m_n) | \text{each } m_i \in M\}$ where addition is coordinate-wise. Equipped with matrix multiplication, $M''$ is a $R_n$-module. We first show $M''$ is irreducible. Suppose there exists a non-zero submodule $S$ of $M''$. $S \neq \{0\}$ implies that there exists some element $(s_1, s_2, \ldots, s_n) \in S$ where each $s_i \in M$ and $s_i \neq 0$ for some $i$. $S$ must be closed under multiplication with $R_n$, so let us multiply $(s_1, s_2, \ldots, s_n)$ by the matrix that has zero in every position, but for the $i^{th}$ row. In the $i^{th}$ row, let the elements vary over
Now let \( x = s_i \), and let \( S' = \{(xr_1, xr_2, ..., xr_n) | r_i \in R\} \). We see immediately that \( S' \subseteq S \), and since \( S \) is a proper subset of \( M^n \), \( S' \) must be a proper subset of \( M^n \). Every entry of \( S' \) has the form \( xR \). We have shown in earlier work that any set of the form \( xR \) is a submodule of \( M \). But \( M \) is irreducible, so \( s_iR = xR \neq 0 \) implies that \( xR = M \). This implies that every element of \( M \) can be written in the form \( xr \) for some \( r \in R \). This tells us that \( M^n \subseteq S' \). Thus any non-zero submodule of \( M^n \) must be \( M^n \), and so \( M^n \) is irreducible.

We will now prove that \( J(R_n) \subseteq J(R)_n \). Let \( A = [a_{ij}] \in J(R)_n \). This implies that for all \( m_i \in M \), \((m_1, m_2, ..., m_n) \cdot A = (0, 0, ..., 0) \). This can only be true if \( M \cdot a_{ij} = \{0\} \) for any \( i, j \). But that places each \( a_{ij} \in J(R) \), and the matrix \( A \) in \( J(R)_n \). Thus \( J(R_n) \subseteq J(R)_n \).

To finish the proof, we must show that \( J(R)_n \subseteq J(R_n) \).
We will show that $J(R)_n$ is a right-quasi-regular right ideal of $R_n$. Let $\rho_i = \begin{bmatrix} a_{i1} & \ldots & a_{in} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} | a_{ij} \in J(R)$ for $i,j = 1,n$. We showed earlier that this set has the structure of a right ideal of $J(R)_n$. Let $X = \begin{bmatrix} x_{ij} \end{bmatrix} \in \rho_i$. As $x_{ii} \in J(R)$, it must be right-quasi regular. Thus there must exist an $x_{ii}'$ such that $x_{ii} + x_{ii}' + x_{ii}x_{ii}' = 0$. Let $Y = \begin{bmatrix} y_{ij} \end{bmatrix} \in \rho_i$ where each element of $Y$ is zero except for $y_{ii}$, which shall equal $x_{ii}'$. Let $W = \begin{bmatrix} w_{ij} \end{bmatrix} = X + Y + XY$. Observe that $W$ is a matrix that is strictly triangular, i.e. the lower triangle is zero and the diagonal elements are zero, which implies that $W'' = 0$. Lemma 3.11 allows us to conclude that $W$ is right-quasi-regular. Thus there exists some matrix $W'$ such that $W + W' + WW' = [0]$. If we substitute for $W$ we get the equation $X + Y + XY + W' + (X + Y + XY)W' = [0]$, and rearranging terms yields $X + (Y + W' + YW') + X(Y + W' + YW') = [0]$. Thus $X$ is a right-quasi-regular element of $R_n$, and since it was chosen arbitrarily, we may state that the ideal $\rho_i$ is a right-quasi-regular right ideal of $R_n$, which implies $\rho_i \subseteq J(R_n)$. In a similar fashion, we can show that for $i=2,3,\ldots,n$, each right
ideal \( p_i = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a_{i1} & \ldots & a_{in} \\ 0 & 0 & 0 \end{pmatrix} \mid a_j \in J(R) \right\} \) is a right-quasi-regular right ideal of \( R_n \), and so must be contained in \( J(R_n) \). Since \( J(R_n) \) must be closed under addition, we may conclude that \( J(R)_n \subseteq J(R_n) \). \( \Box \)
Emil Artin was born on March 3rd, 1898 in Vienna, Austria. The son of an art dealer and opera singer, he possessed a love not only of mathematics, but of music as well. After fighting in the Austrian Army during World War I, he obtained his doctorate from the University of Leipzig in 1921. His accomplishments were many, but he is perhaps best known for his generalization of reciprocity laws. Here however, we focus on another of his interests, rings equipped with a minimal condition. Today, such rings are termed "Artinian." We define these Artinian rings in Definition 4.8(a). The Artinian property is particularly powerful when the ring is also semisimple, and we will spend the majority of this chapter examining such semisimple Artinian rings. Before we do so however, we must develop some prefatory material. Having defined maximal right ideals in chapter 2, we define minimal right ideals here analogously:
Definition 4.1 Minimal right ideals

Given a ring $R$, we say that a right ideal $\rho$ of $R$ is a minimal right ideal of $R$ if the only right ideal of $R$ that is properly contained in $\rho$ is $\{0\}$.

We will use minimal right ideals extensively during the proofs of this section, utilizing their restriction on size to force contradictions at necessary moments. We now introduce a second concept – an idempotent. If we can find such an element in an Artinian ring $R$, we will use it to describe certain ideals of $R$.

Definition 4.2 Idempotents

Let $R$ be a ring and let $e \in R$. We call $e$ an idempotent of $R$ if $e^2 = e$ and if $e$ is not equal to zero.

Example 4.3

For some odd prime $p$, consider the ring $\mathbb{Z}/(2p)\mathbb{Z}$, and the element $[p]$. As is true for all rings with an identity element, $[1]=[1]^2$ is an idempotent, but in addition note that in this quotient ring $[p]$ is an idempotent as well.
Proof: As \( p \) is odd, \( p = 2q + 1 \) for some \( q \in \mathbb{Z} \). Observe
\[
p^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4q^2 + 2q + 2q + 1 = 2q(2q + 1) + 2q + 1 = (2p)q + p.
\]
Thus \( p^2 \equiv p \pmod{2p} \).

Example 4.4

Consider \( F_n \), the ring of \( n \times n \) matrices over a field \( F \).

Any non-zero matrix of the form
\[
\begin{pmatrix}
a_{11} & 0 & 0 \\
0 & \ddots & 0 \\
0 & 0 & a_{nn}
\end{pmatrix},
\]
where \( a_{ij} \in \{0,1\} \) is an idempotent.

Proof: Let \( A = (a_{ij}) \) be a matrix of the given form, and let \( A^2 = (b_{ij}) \). We need to show that \( (a_{ij})^2 = (b_{ij}) \). First consider the elements \( b_{ij} \) where \( i > j \)
\[
b_{ij} = \sum_{k=1}^{n} a_{ik} a_{kj} = \sum_{k=1}^{i-1} 0 \cdot a_{ij} + \sum_{k=i+1}^{n} a_{ik} \cdot 0 = 0.
\]
Similarly, when \( i < j \), \( b_{ij} = 0 \). Finally, when \( i = j \),
\[
b_{ii} = \sum_{k=1}^{n} a_{ik} a_{kj} = \sum_{k=1}^{i-1} 0 \cdot a_{ij} + a_{ii} a_{ij} + \sum_{k=i+1}^{n} a_{ik} \cdot 0 = a_{ii} a_{ij} = a_{ii}^2.
\]
But if each
\[
a_{ii} \in \{0,1\}, \quad a_{ii}^2 = a_{ii}.
\]
We have shown that \( (b_{ij}) = \begin{pmatrix} a_{11} & 0 & 0 \\
0 & \ddots & 0 \\
0 & 0 & a_{nn}\end{pmatrix} \).

Theorem 4.5

Let \( R \) be a ring that does not have any nilpotent ideals, other than the trivial ideal \( \{0\} \). If \( \rho \) is a minimal
right ideal of $R$ and $\rho \neq \{0\}$, then $\rho = eR$ for some idempotent $e \in \rho$.

Proof: Suppose $\rho^2 = \{0\}$. This implies that for any $x_1, x_2 \in \rho$, $x_1 x_2 = 0$, i.e. $\rho$ is nilpotent. But $R$ has no nilpotent ideals, so this cannot be. Thus there is an $x \in \rho$ such that $x \rho \neq \{0\}$. But the set $x \rho$ is a right ideal of $R$, and since $x \in \rho$, and $\rho$ is a right ideal, $x \rho \subseteq \rho$. As $\rho$ is minimal, and $x \rho$ is a non-zero right ideal of $R$ that is contained in $\rho$, we must conclude that $x \rho = \rho$. In particular, there exists some element $e \in \rho$ such that $xe = x$. This implies that $xe^2 = xe$, which yields the equation $x(e^2 - e) = 0$. Now let $S$ equal the set of all elements from $\rho$ that, like the element $e^2 - e$, when right-multiplied with $x$ equal 0, i.e. $S = \{a \in \rho | xa = 0\}$. We claim $S$ is also a right ideal of $R$. To see this observe that $0 \in S$, and that $a, b \in S$ imply that $x(a - b) = xa - xb = 0 - 0 = 0$, which places $a - b \in S$. Finally, for any $a \in S, r \in R$ note that $x(ar) = (xa)r = (0)r = 0$. Thus $S$ is indeed a right ideal of $R$ that, by construction, is a subset of $\rho$. Recall that $x \rho \neq \{0\}$, which implies that there is some $b \in \rho$ such that $xb \neq 0$. This $b$ cannot be in $S$. We have shown that $S$ is a right ideal of
$R$ that is properly contained in $\rho$. Again, $\rho$ is minimal, and so the only right ideal of $R$ properly contained in $\rho$ must be $\{0\}$. Thus $S=\{0\}$, and since $e^2-e \in S$, $e^2-e=0$, or simply $e^2=e$. $x\rho \neq \{0\} \Rightarrow x \neq 0$, and since $xe=x$, we may assert that $xe \neq 0$. This implies that $e=e^2 \neq 0$. Using a similar argument as that given above, we observe that $eR$ is a non-zero right ideal of $R$ contained in the minimal right ideal $\rho$. We conclude that $eR=\rho$.

**Theorem 4.6**

Let $R$ be a ring that does not have any nilpotent ideals, other than the trivial ideal $\{0\}$, and let $e \neq 0$ be an idempotent of $R$. Then $eR$ is a minimal right ideal of $R$ if and only if $eRe$ is a division ring.

*Proof:* ($\Rightarrow$) Let $eR$ be a minimal right ideal of $R$. We first show that $eRe$ has the structure of a ring. Since any element of $eRe$ is also an element of $R$, all of the ring properties from $R$ pass to $eRe$. To show that $eRe$ is closed under multiplication, see that for some $er_1e, er_2e \in eRe$,

$$(er_1e)(er_2e)=e(r_1eer_2)e \in eRe.$$  For closure under subtraction, observe

$$er_1e-er_2e=e(r_1e-r_2e)=e(r_1-r_2)e \in eRe.$$
Thus $eRe$ is a ring. To show it is a division ring, we must find a unit element in $eRe$ and show that every non-zero element of $eRe$ has a multiplicative inverse. We see that the unit element is $e$: first note that $e = e^2 = e^3 \neq 0$, and that $e^3 = e \cdot e \cdot e \in eRe$. Therefore $e \neq 0$, and $e \in eRe$. Now see that for any $exe \in eRe$, $e(exe) = (ee)xe = exe = ex(ee) = exe(e)$. This implies that $e$ is a unit element of $eRe$. To complete this part of the proof, we need to show that for any non-zero element of $eRe$, there exists a companion element in $eRe$ such that their product will be $e$. Since $0 \neq e \in eRe$ the set $eRe \neq \{0\}$. Thus there exists some $a \in R$ such that $eae \neq 0$. Consider the right ideal $eaeR$, and the element $eae \in eaeR$. Since $eae = ea(ee) = eae \neq 0$, $eaeR \neq \{0\}$. Moreover, observe $eaeR = e(aeR) \subseteq eR$. The right ideal $eaeR$ is non-zero and contained in $eR$. Since $eR$ is minimal this forces the conclusion that $eaeR = eR$. Thus for some $x \in R$ $eae = ee = e$, and $eae = e^2 = e$. Using the same property of $e$, we conclude that $e = ea(e)xe = ea(ee)xe = (eae)(exe)$.

Recall that $a \in R$ was selected so that the product $eae \neq 0$. We have shown that for every non-zero element of $eRe$, we can find an $x \in R$, and so an element $exe \in eRe$ such that $(eae)(exe) = e$. Therefore $eRe$ is a division ring.
(⇐) To prove the converse, let $eRe$ be a division ring. We first observe that $e = e \cdot e \cdot e \neq 0 \in eRe$. Thus $eRe$ is non-zero. The fact that it is a division ring implies that there exists some $1 \in eRe$ such that $1 \cdot (eae) = eae = (eae) \cdot 1$ for all $eae \in eRe$. But this is true for $e$ as well. See that $e(eae) = eae = (eae)e$ for all $eae \in eRe$. Also, since $eRe$ is a division ring then for any non-zero $eae \in eRe$, there exists a non-zero $exe \in eRe$ such that $(eae)(exe) = 1$. Multiplying both sides by $e$, we see that $(eae)(exe)e = 1 \cdot e$, which implies that $(eae)(exe)e = e$. We have shown that $e$ is a unit element of $eRe$.

Recall our main objective: to prove that the right ideal $eR$ is minimal in $R$. Let $\rho$ be a non-zero right ideal of $R$ such that $\rho \subseteq eR$. Thus every element of $\rho$ has the form $e \cdot x$ for some $x \in R$. We claim that the set $\rho e \neq \{0\}$. Suppose $\rho e = \{0\}$. This would force $\rho^2 \subseteq \rho(eR) = (\rho e)R = 0 \cdot R = \{0\}$. Thus $\rho$ would be nilpotent, which cannot be in $R$. Hence $\rho e \neq \{0\}$.

Thus there exists an $ex \in \rho$ ($\rho \subseteq eR$) such that $(ex)e \neq 0$. Thus $exe \in eRe$, and is non-zero. Since $eRe$ is a division ring, there must exist an $eye \in eRe$ such that $exe(eye) = e$. But $\rho$ is a right ideal of $R$, so if $ex \in \rho$, then $ex(eeye) = exe(eye) = e \in \rho$. If
$e \in \rho$, and $\rho$ is a right ideal of $R$, $eR \subseteq \rho$. By selection $\rho \subseteq eR$. Thus the two sets are equal. We have shown that any non-zero right ideal of $R$ that is contained in $eR$ must equal $eR$. Therefore $eR$ is a minimal right ideal of $R$.

During the last proof we introduced the structure $eRe$, and showed that it is a ring. As such, it naturally has a radical. The radical of $eRe$ can be expressed succinctly in terms of the radical of $R$, and we present this fact in the following theorem.

**Theorem 4.7**

Given a ring $R$ and an idempotent $e \in R$, $J(eRe) = eJ(R)e$.

**Proof:** We will first prove that $J(eRe) \subseteq eJ(R)e$. Our strategy will be to show that any irreducible $R$-module $M$ is annihilated by $J(eRe)$, which would force the conclusion that $J(eRe) \subseteq J(R)$. Noting then that $e \cdot x = x = x \cdot e$ for any $x \in eRe$, and that the set $J(eRe) \subseteq eRe$, we shall conclude that $J(eRe) = eJ(eRe)e \subseteq eJ(R)e$.

To begin, let $M$ be an irreducible $R$-module. We claim $Me = \{0\}$ or $Me$ is an irreducible $eRe$-module. If $Me \neq \{0\}$ there must exist some $m \in M$ such that $me \neq 0$. Recalling an argument used at the beginning of the proof of Theorem
2.19, we observe that $m_R$ is a submodule of $M$. And since $m = m e e m e R$, it is a non-zero submodule of $M$. But $M$ is irreducible, so we must conclude that $m_R = M$. This implies that $m_R e = M$. We claim $M e$ is an irreducible $e_R$-module. We know $m e \neq 0$. This implies that $m(e e e) = m e \neq 0$, and since $e e e e e = M(e R R) \neq 0$. Now suppose there exists a non-zero submodule $N$ of $M e$. Then for some $n e M, n e N$ and $n e \neq 0$. $N$ must be closed under multiplication with the ring, and so $n e (e R) \subseteq N$. But $n e \neq 0$ and $M$ is irreducible imply that $n R = M$, and so $n(e_R) = (n_r) = M e$. Thus $N$ must equal $M e$, and so $M e$ is an irreducible $e R$-module. Therefore, by the definition of the radical, $M e$ must be annihilated by the radical of $e R$, i.e. $(M e)(e R) = \{0\}$. But recall $e J(e R) = J(e R)$, and so $\{0\} = (M e)(e R) = (M) e J(e R) = (M)(e R)$. Thus, if $M e \neq \{0\}$, $M : J(e R) = \{0\}$. And, if $M e = \{0\}$, $(M)(e R) = (M e)(e R) = (0)(e R) = \{0\}$. In either case then, if $M$ is an irreducible $R$-module, it is annihilated by $J(e R)$. Thus $J(e R) \subseteq J(R)$, and finally, $J(e R) = e \cdot J(e R) = e \cdot e \cdot J(R)$.

To prove the reverse inclusion, we will show that $e J(R) e$ is a right-quasi-regular ideal in $e R$, and so
Theorem 3.18 must be contained in $J(eRe)$. Since $J(R)$ is a two-sided ideal of $R$, any $a \in eJ(R)e$ is also an element of $J(R)$. Thus there must exist a right-quasi-inverse $a' \in J(R)$ such that $a + a' + aa' = 0$. If we left and right-multiply this equation by $e$, we obtain $eae + ea'e + eaa'e = 0$. But recall that $a \in eJ(R)e$, and so has the form $ere$ for some $r \in J(R)$. We see then that $e(a)e = e(ere)e = ere = a$. Thus $eae = a$, and if we multiply on both sides by $e$, $ae = eae = ea$. Substituting these two expressions into $eae + ea'e + eaa'e = 0$ yields $a + ea'e + aea'e = 0$. This tells us that the element $ea'e$ is the right-quasi-inverse of $a$. But such an inverse is unique, and so $a' = ea'e$. We have shown that any $a \in eJ(R)e$ is right-quasi-regular in $eRe$. Thus $eJ(R)e$ is a right-quasi-regular right ideal of $eRe$, and must be contained in $J(eRe)$.

We are now prepared to examine Artinian rings. In the literature these rings are often referred to as those that satisfy the "descending chain condition," and we show next that these two definitions are equivalent.

**Definition 4.8(a) Artinian Rings**

A ring is said to be right Artinian if any non-empty set of right ideals has a minimal element.
Definition 4.8(b) Descending chain condition

If a ring $R$ satisfies the descending chain condition, then any descending chain of right ideals of $R$ becomes stationary. In other words, for any descending chain of right ideals of $R$, $\rho_1 \supseteq \rho_2 \supseteq \rho_3 \supseteq \ldots \supseteq \rho_n \ldots$, there exist some $i \in \mathbb{N}$ such that $\rho_i = \rho_{i+1} = \rho_{i+2} = \ldots$

Lemma 4.8(c)

$R$ is Artinian if and only if $R$ satisfies the descending chain condition.

Proof: ($\Rightarrow$) Let $R$ be an Artinian ring and let $\rho_i$ be a descending chain of right ideals of $R$. Define the set $S = \{\rho_i\}$. As $S$ is non-empty, $R$'s classification as Artinian implies that there must exist a minimal element of $S$, call it $\rho_i$. If this element is minimal, every ideal that follows in the chain must be equal to $\rho_i$, i.e. $\rho_i = \rho_{i+1} = \rho_{i+2} = \ldots$ The chain has become stationary.

($\Leftarrow$) To prove the reverse direction, let $R$ be a ring that satisfies the descending chain condition, and let $S$ be a non-empty set of right ideals of $R$. Pick a right ideal from $S$ and call it $\rho_i$. This element of $S$ is either minimal...
in $S$ or not. If it is, we're done. If it is not, there must exist some ideal in $S$, call it $\rho_2$, such that $\rho_1 \supset \rho_2$. This element $\rho_2$ is either minimal or it is not. If not, we now have $\rho_3 \in S$ such that $\rho_1 \supset \rho_2 \supset \rho_3$. Proceeding in this fashion, and utilizing the axiom of choice, we generate a chain of ideals. Since $R$ satisfies the descending chain condition, this chain must have a minimal element, $\rho_r$.

Thus, $S$ must have a minimal element.

Theorem 4.9

The following statements regarding Artinian rings are true:

i) any division ring is Artinian.

ii) the homomorphic image of an Artinian ring is Artinian.

iii) if $R$ is an Artinian ring, then any quotient ring of $R$ is also Artinian.

iv) if $R$ is an Artinian ring with a two-sided unit, then $R_n$ is an Artinian ring.

v) if $R$ is a ring with a finite number of elements, then $R$ is Artinian.
Proof: i) Any division ring $R$ will only have two right ideals, $\{0\}$ and $R$ itself. If presented with a non-empty set of right ideals of $R$ simply ask, is $\{0\}$ in the set? If it is, that is the minimal element. If it is not, then $R$ is the minimal element.

ii) Let $R$ be an Artinian ring, let $\phi: R \rightarrow S$ be a ring homomorphism, and let $T$ be the image of $\phi$. Since $\phi$ is a ring homomorphism, $T$ is a subring of $S$, and so of course possesses a ring structure itself. Suppose that $T$ is not Artinian. Thus there exists a proper descending chain of right ideals $\rho_i$ of $T$ that do not become stationary. For each such $\rho_i$, define $R_i = \{r \in R | \phi(r) \in \rho_i\}$. As $\phi$ is a ring homomorphism, each $R_i$ is a right ideal of $R$. Moreover $\rho_i \supset \rho_{i+1}$ implies that $R_i \supset R_{i+1}$. We see that the $R_i$'s are a descending chain of right ideals of $R$. But $R$ is Artinian, and so there must exist an $i \in \mathbb{N}$ such that $R_i = R_{i+1} = R_{i+2} = \ldots$ This implies that $\rho_i = \rho_{i+1} = \rho_{i+2} = \ldots$ A contradiction. Thus $T$ must be Artinian.

iii) Let $R$ be an Artinian ring, and let $\overline{R} = R/\rho$ for some right ideal $\rho$ of $R$. Let $\phi: R \rightarrow \overline{R}$ send $r \mapsto r + \rho$ for
all \( r \in R \). The mapping \( \phi \) is a ring homomorphism, and we see that the image of \( \phi \) is \( R/\rho \). Since \( R/\rho \) is the homomorphic image of an Artinian ring, by Theorem 4.9(ii) above we conclude that it must be Artinian.

iv) Let \( R \) be a ring with a two-sided unit element, and suppose that \( R_n \) is not Artinian. This implies that there exists an infinite proper descending chain of right ideals \( \rho_i \) of \( R_n \) that do not become stationary. Consider the first ideal in the chain, \( \rho_1 \). Let \( \rho_{1-1} = \{ (a_{ij}) | a_{ij} = b_{ij} \text{ for some } (b_{ij}) \in \rho, a_j = 0 \text{ otherwise} \} \). Thus \( \rho_{1-1} \) is a set of matrices with zero elements but for row 1. For each matrix in \( \rho_{1-1} \), the first row matches the first row of some matrix in the original ideal \( \rho_1 \). Similarly, construct the sets

\[
\rho_{1-k} = \{ (a_{ij}) | a_{ij} = b_{ij} \text{ for some } (b_{ij}) \in \rho, a_j = 0 \text{ otherwise} \}.
\]

We see that \( \rho_1 = \rho_{1-1} \oplus \rho_{1-2} \oplus \ldots \oplus \rho_{1-n} \). Next, because \( \rho_1 \) and therefore each \( \rho_{1-i} \) is closed under addition and right multiplication with \( R_n \), each \( \rho_{1-i} \) is a right ideal of \( R_n \). Moreover, for those reasons, and also because \( R \) has a two-sided unit element, the row of each \( \rho_{1-i} \) must equal \( (x_1, x_2, \ldots, x_n) \) where
each $x_k$ is an element of some right ideal $S_{l-i}$ of $R$. Recall that $\rho_2$ is a proper subset of $\rho_1$. This implies that for at least one $i$, $\rho_{l-i}$ has been reduced to create a new proper subset $\rho_{2-i}$. Thus $S_{l-i} \supset S_{2-i}$. Continuing, we know that $\rho_2 \supset \rho_3$. This implies that for at least one $k$, $\rho_{2-k}$ has been reduced, and so $S_{2-k} \supset S_{3-k}$. For each descending step down the chain, ultimately one such right ideal $S_{a-b}$ of $R$ must be reduced. To suggest that the $n$ such right ideals of $R$ could continue to be reduced indefinitely, is to suggest that at least one of those ideals has a proper infinite descending chain. This is a contradiction, and so $R_n$ must be Artinian.

v) If $R$ has a finite number of elements, it is clear that any descending chain of right ideals of $R$ must eventually become stationary. \hfill \Box

Example 4.10

For an example of a ring that is not Artinian, consider $\mathbb{Z}$. Construct a chain of ideals $\rho_i$ of $\mathbb{Z}$ in the following way: let $\rho_i=(2^i)\mathbb{Z}$ for all $i \in \mathbb{N}$. Thus

$\rho_1=\{...,-4,-2,0,2,4,...\}$, $\rho_2=\{...,-8,-4,0,4,8,...\}$, and so on. We see that
\[ \rho_1 \supseteq \rho_2 \supseteq \rho_3 \ldots \supseteq \rho_n \supseteq \ldots \] and that this chain will never become stationary. Thus \( Z \) is not Artinian.

In chapter 3, we defined the radical of a ring, and presented several results regarding the radical \( J(R) \) for an ring \( R \). We now use the descending chain condition to show that the radical of an Artinian ring has special structure.

**Theorem 4.11**

If \( R \) is an Artinian ring, then \( J(R) \) is a nilpotent ideal.

**Proof:** Let \( J = J(R) \), and consider the chain \( J \supseteq J^2 \supseteq J^3 \ldots \) As \( J \) is a two-sided and in particular a right ideal of \( R \), using Corollary 1.6 we may conclude that each \( J^i \) is a right ideal of \( R \). Thus \( J \supseteq J^2 \supseteq J^3 \ldots \) is a descending chain of right ideals, and must become stationary. For some \( n \in \mathbb{N} \), \( J^n = J^{n+1} = \ldots = J^{2n} \ldots \) If we can show that \( J^n = \{0\} \), this would imply that \( r_1 \cdot r_2 \ldots \cdot r_n = 0 \) for any \( r_i \in J(R) \), i.e. \( J(R) \) is nilpotent, the desired result.

Suppose \( J^n \neq \{0\} \), and let \( S = \{ x \in J \mid xJ^n = \{0\} \} \). \( S \) is a two-sided ideal of \( R \). To show this, let \( a, b \in S \), and observe that \( (a+b)J^n = aJ^n + bJ^n = \{0\} \). See also that for any \( a \in S \) and \( r \in R \),
\((ar)J^n = a(rJ^n) \subseteq aJ^n = \{0\}\), and that \((ra)J^n = r(aJ^n) = r(0) = 0\). Thus \(S\) is a two-sided ideal of \(R\). If \(J^n \subseteq S\), we see that
\[\{0\} = S \cdot J^n \supseteq J^n J^n = J^{2n} = J^n,\]
which is impossible.

On the other hand, if \(J^n \not\subseteq S\), let \(\overline{R} = R / S\). Since \(J^n\) is not contained in \(S\), \(\overline{J^n} \neq \{0\}\). We shall prove the following statement: for any \(\overline{x} \in \overline{R}\), \(\overline{x} J^n = \{0\}\) implies \(\overline{x} = \overline{0}\). If \(\overline{x} J^n = \{0\}\) for some \(\overline{x} \in \overline{R}\), this implies \(x J^n \subseteq S\) for any \(x \in R\) that maps onto \(\overline{x}\). It follows that \(\{0\} = (x J^n) J^n = x J^{2n} = x J^n\). Thus each \(x\) must be in \(S\), and so \(\overline{x} = \overline{0}\). The statement has been proved.

We established earlier that \(\overline{J^n} \neq \{0\}\). Let \(\Psi\) be the set of non-zero right ideals of \(\overline{R}\) contained in \(\overline{J^n}\). \(\overline{J^n} \in \Psi\), and so \(\Psi\) is non-empty. \(R\) is Artinian implies that \(\overline{R}\) is Artinian, and so \(\Psi\) must have some minimal element, call it \(\overline{\rho}\). We would like to prove that \(\overline{\rho}\) is an irreducible \(\overline{R}\)-module.

Suppose \(\overline{\rho} \cdot \overline{R} = \{0\}\). \(\overline{J^n} \subseteq \overline{R}\), and this implies \(\overline{\rho} \cdot \overline{J^n} = \{0\}\). By the statement we proved earlier, any element \(\overline{x} \in \overline{\rho}\) would have to equal \(\overline{0}\), which implies \(\overline{\rho} = \{0\}\). But as an element of \(\Psi\), \(\overline{\rho}\) is non-zero. Thus \(\overline{\rho} \cdot \overline{R} \neq \{0\}\). Now let \(\overline{N}\) be a non-zero submodule
of $\bar{\rho}$. As such, it must contain $0$, be closed under subtraction and be closed under right multiplication with $\bar{R}$. $\overline{N}$ is not only a submodule of $\bar{\rho}$, but a non-zero right ideal of $\bar{R}$ properly contained in $\bar{\rho}$. This contradicts $\bar{\rho}$'s minimality in $\bar{R}$. We can see then that $\bar{\rho}$ is irreducible and will be annihilated by $J(\bar{R})$. Since $J^n \subseteq J = J(R)$, $\bar{J}^n \subseteq J(\bar{R})$.

Thus $\bar{\rho} \cdot \bar{J}^n = \{0\}$ which implies $\bar{\rho} = \{0\}$ which is a contradiction, and so $J^n = \{0\}$. Thus $J(R)$ is nilpotent.

Corollary 4.12

If $R$ is Artinian then any nil right ideal of $R$ is nilpotent.

Proof: Every nil right ideal of $R$ is right-quasi-regular and so contained in $J(R)$. If $J(R)$ is nilpotent, every subset of $J(R)$ is nilpotent.

Earlier we saw that idempotents, under certain conditions, can be used to describe the structure of ideals of $R$. Are there conditions upon which the existence of an idempotent can be guaranteed? The following theorem provides a crucial step for the determination of the structure of ideals in a semisimple Artinian ring.
Theorem 4.13

Let $R$ be an Artinian ring, and let $\rho$ be a non-zero right ideal of $R$ that is not nilpotent. Then $\rho$ contains an idempotent.

Proof: Theorem 4.11 tells us that the radical of an Artinian ring is nilpotent. Since $\rho$ is not nilpotent, $\rho \not\subseteq J(R)$. Now let $\overline{R} = R/J(R)$. We proved in Theorem 3.20 that $\overline{R}$ is semisimple, i.e. $J(\overline{R}) = \{0\}$. Any nilpotent and therefore any nil right ideal of $\overline{R}$ must be contained in $J(\overline{R}) = \{0\}$. We conclude then that $\overline{R}$ does not have any nilpotent ideals other than $\{0\}$. Recalling that $\rho \not\subseteq J(R)$, we infer that $\overline{\rho} \neq \{0\}$. As $\overline{R}$ is Artinian, there must exist some right ideal $\overline{\gamma} \subseteq \overline{\rho}$ that is a minimal non-zero right ideal of $\overline{R}$. By Theorem 4.5, $\overline{\gamma} = e\overline{R}$ for some idempotent $e \in \overline{\gamma}$. Select an $a \in \gamma$ such that after the modulo action $a = \overline{e}$. This modulo action is in fact a ring homomorphism, and we may conclude that $\overline{(a^2 - a)} = \overline{a^2 - a} = \overline{e^2 - e} = \overline{e} - \overline{e} = 0$. This implies that $a^2 - a \in J(R)$, which is a nilpotent ideal. Thus for some $m \in \mathbb{N}$, $(a^2 - a)^m = 0$.  

83
Binomial expansion yields the polynomial
\[ a^{2m} + b_1 a^{2m-1} + b_2 a^{2m-2} + \ldots + (-1)^n a^n = 0 \]
where each \( b_i \in \mathbb{Z} \). We can rewrite this equation so that \( a^n = a^{m+1} p(a) \), where \( p(x) \in \mathbb{Z}[x] \) and has degree \( 2m-(m+1)=m-1 \). Observe that:

\[ a^n = a^{m+1} p(a) \text{ or } a^n = a \cdot a^m p(a). \]

Substituting for \( a^m \) on the right, we get
\[ a^n = a(a^{m+1} p(a))p(a) = a^{m+2} p(a)^2. \]
Repeating this process yields
\[ a^n = a^{2m} p(a)^m. \]

We seek to find an idempotent \( e \in \rho \). Let \( e = a^m p(a)^m \).

Recalling that the powers of \( a \) do commute, we see that
\[ e^2 = a^m p(a)^m a^m p(a)^m = (a^{2m} p(a)^m) p(a)^m = a^m p(a)^m = e. \]

We need to show that \( e \neq 0 \). Suppose that \( a^n = 0 \). Recalling that under the modulo action \( a \) maps onto \( \bar{e} \), we see \( a^n = 0 \Rightarrow \bar{e}^m = 0 \). But \( \bar{e} \) is an idempotent in \( \bar{R} \), and so \( \bar{e} = \bar{e}^2 = \bar{e}^m \neq 0 \). This is a contradiction, and so \( a^n \neq 0 \). Now suppose \( e = a^m p(a)^m = 0 \). If this were true, \( a^m = a^{2m} p(a)^m = a^m (a^m p(a)^m) = a^m(0) = 0 \), another contradiction. \( e \neq 0 \), and as we have shown \( e^2 = e \). \( e \) is an idempotent of \( R \), and since by selection \( a \in \rho \), \( e \), which is just the summation of powers of \( a \), must also be in \( \rho \). □
Having introduced the notion of Artinian rings, we now turn our attention to rings that are both semisimple and Artinian, i.e. Artinian rings \( R \) such that \( J(R)=\{0\} \). It turns out that the ideals of these rings are easily determined.

**Theorem 4.14**

Given a semisimple Artinian ring \( R \), and a non-zero right ideal \( \rho \) of \( R \). \( \rho = eR \) for some idempotent \( e \in \rho \).

**Proof:** If \( \rho \) is a nilpotent right ideal of \( R \), it would certainly be nil and so contained in \( J(R) \). But \( R \) is semisimple, which implies that \( J(R)=\{0\} \). Thus \( \rho \subseteq \{0\} \), which contradicts the fact that \( \rho \) is non-zero. Therefore \( \rho \neq \{0\} \) is not nilpotent, and so via Theorem 4.13 there must exist at least one idempotent \( e \in \rho \). For any such element \( e \), let \( A_e = \{x \in \rho | ex=0\} \). We see immediately that each such \( A_e \) is a right ideal of \( R \). Let \( \Psi \) be the set of \( A_e \)'s. It is non-empty and, as \( R \) is Artinian, must have a minimal element, call it \( A_{e_0} \), where \( e_0 \) is an idempotent in \( \rho \). We will show that \( A_{e_0} = \{0\} \). Suppose not. As a non-zero right ideal of \( R \), it also must contain an idempotent \( e \). By construction,
$A_\circ \subseteq \rho$, and so $e_1 \in \rho$. Since $e_1 \in A_\circ$, $e_0 e_1 = 0$. Now let

$$e_2 = e_0 + e_1 - e_0 e_1,$$

and remember $(e_1)^2 = e_1$ and $(e_0)^2 = e_0$. Observe that:

$$(e_2)^2 = e_0^2 + e_0 e_1 - e_0 e_1 e_0 + e_1 e_0 - e_1 e_0 e_0 - e_0 e_1 e_0 + e_0 e_1 e_0 e_1$$

$$= e_0 + 0 - e_0 e_1 + e_1 - e_0 e_1 - e_0 - e_0 + e_1 + 0 = e_1 = 0.$$

We have shown that $(e_2)^2 = e_2$, and $e_2 \neq 0$. It must be an idempotent, and since it is the sum of elements from $\rho$, must be contained in $\rho$. Thus there exists a set

$$A_\circ = \{ x \in \rho \mid e_2 x = 0 \} \in \Psi.$$ 

Let $x \in A_\circ$. This implies $e_2 x = 0$. But $e_2 = e_0 + e_1 - e_0 e_1$, and thus $0 = (e_0 + e_1 - e_0) x$. Left-multiply both sides by $e_0$ and $0 = e_0 (e_0 + e_1 - e_0) x = e_0 e_0 x + e_0 e_1 x - e_0 e_0 e_0 x = e_0 x + 0 = e_0 x$.

However, if $e_0 x = 0$, $x$ must be an element of $A_\circ$. $A_\circ \subseteq A_\circ$.

Recall that $e_1 \in A_\circ$, and now suppose $e_1 \in A_\circ$. This implies $e_2 e_1 = 0$. But we showed earlier that $e_2 e_1 \neq 0$, so this is a contradiction. Thus $e_1 \in A_\circ$, and $e_1 \notin A_\circ$. Recalling that $e_2 \neq 0 \in A_\circ$, we see that $A_\circ$ is a non-zero right ideal of $R$ properly contained in $A_\circ$. This contradicts the minimality of $A_\circ$, and so, $A_\circ = \{ 0 \}$. As such, for any $x \in \rho$, note that

86
Thus \( x - e_0 x = x - e_0 e_0 x \) for all \( x \in \rho \). Using the fact that \( e_0 \) is an element of the right ideal \( \rho \), we may conclude \( \rho = e_0 \rho \subseteq e_0 R \), and that \( e_0 R \subseteq \rho \).

**Example 4.15**

Consider \( F_n \), the ring of \( n \times n \) matrices over a field \( F \),

\[
0 = e_0 x - (e_0)^2 x = e_0 (x - e_0 x).
\]

and the ideal \( S = \{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \mid a_{ij} \in F \} \). Utilizing parts (i) and (iv) of Theorem 4.9, we see that if the field \( F \) is Artinian then \( F_n \) must itself be Artinian. An argument similar to that used in Example 3.17 will show that this ring is semisimple. Thus Theorem 4.14 applies, and since \( S \) is a non-zero right ideal of \( F_n \), \( S \) must equal \( eF_n \) for some idempotent \( e \in F_n \). By examination we see that

\[
S = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} e \\ & e \\ & & \ddots \\ & & & e \end{pmatrix}.
\]

The implications of Theorem 4.14 are clear. If one wants to understand the structure of the right ideals of a
semisimple Artinian ring, one need only look for the idempotents of that ring. In the following theorem we extend this notion to two-sided ideals of $R$.

**Theorem 4.16**

If $R$ is a semisimple Artinian ring, and $A$ is a two-sided ideal of $R$, then $A = eR = Re$ for some idempotent $e \in A$. Moreover, $e \cdot x = x \cdot e$ for all $x \in R$, i.e. $e$ commutes with every element of $R$.

**Proof:** If $A$ is a two-sided ideal of $R$, it is certainly a right ideal of $R$, and so by Theorem 4.14 $A = eR$ for some idempotent $e \in A$. Let $B = \{ x - xe \mid x \in A \}$. Since every element $x$ of $A$ has the form $x = e \cdot r$ for some $r \in R$, we see immediately that $ex = eer = er = x$ for all $x \in A$. Similarly, note that every element $y \in B$ has the form $y = x - xe$ for some $x \in A$. Since $ye = xe - xee = xe - xe = 0$, we may conclude that $Be = \{ 0 \}$, and that $BA = BeR = \{ 0 \} \cdot R = \{ 0 \}$. We claim that $B$ is a left ideal of $R$. $0 \in A \Rightarrow 0 \in B$, and since $A$ is closed under subtraction and left-multiplication with $R$, $B$ will be likewise. Thus $B$ is a left ideal of $R$ and since $B \subseteq A$, $B^2 \subseteq BA = \{ 0 \}$, $B$ is a nilpotent left ideal of $R$. While we have not shown this explicitly for left ideals, a similar argument to that for
right ideals shows that such an ideal must be contained in the radical of $R$, in this case $\{0\}$. If $B=\{0\}$, then $x-xe=0$ for all $x \in A$, i.e. $x=xe$. We have shown that for any $x \in A$, $x=xe$. This implies that $A= Ae \subseteq Re$. To show $Re \subseteq A$, recall that $e \in A$, and that $A$ is a two-sided ideal of $R$. Thus $Re \subseteq A$, and $A= Re = eR$.

To show the $e$ commutes with all elements of $R$, let $a \in R$. Since $A= eR= Re$, both $ae$ and $ea \in A$. Since $e$ is a two-sided unit of $A$, we may conclude that $ae= eae$ and that $ea= eae$. This forces $ae= eae= ea$ for any $a \in R$. □

Corollary 4.17

If $R$ is a semisimple Artinian ring, then $R$ must have a two-sided unit element, i.e. there exists some $1 \in R$ such that $1 \cdot r = r = r \cdot 1$ for all $r \in R$.

Proof: $R$ is a two-sided ideal of $R$, and so Theorem 4.16 applies. □

Example 4.18

Consider the ring $\mathbb{Z}/15\mathbb{Z} = \{[0],[1],[2],\ldots,[14]\}$. $\mathbb{Z}/15\mathbb{Z}$ is finite, which implies that any descending chain of right ideals must become stationary. That is, $\mathbb{Z}/15\mathbb{Z}$ is Artinian.
To prove semisimplicity, note that \{[0],[5],[10]\} and 
\{[0],[3],[6],[9],[12]\} are both maximal right ideals of \(\mathbb{Z}/15\mathbb{Z}\), and 
their intersection is \{[0]\}. By Theorem 3.15 we conclude 
that \(J(\mathbb{Z}/15\mathbb{Z})=\{[0]\}\), i.e. \(\mathbb{Z}/15\mathbb{Z}\) is semisimple. Therefore 
Theorem 4.16 applies and by direct calculation we see the 
idempotents of \(\mathbb{Z}/15\mathbb{Z}\) are \{[1],[6],[10]\}. This implies that the 
only two-sided ideals of \(\mathbb{Z}/15\mathbb{Z}\) are \([1]\cdot\mathbb{Z}/15\mathbb{Z}=\mathbb{Z}/15\mathbb{Z}\), \n\([6]\cdot\mathbb{Z}/15\mathbb{Z}=\{[0],[3],[6],[9],[12]\}\), and \([10]\cdot\mathbb{Z}/15\mathbb{Z}=\{[0],[5],[10]\}\).

The following Lemma provides a first step towards 
writing a semisimple Artinian ring as a direct sum of 
simple rings.

Lemma 4.19

Let \(R\) be a semisimple Artinian ring, and let \(A\neq\{0\}\) be 
a two-sided ideal of \(R\). Then:

i) \(R=A\oplus R(1-e)\) for some idempotent \(e\in A\), and \(R(1-e)\) is 
a two-sided ideal of \(R\); and

ii) \(A\) is a semisimple Artinian ring.

Proof: i) Theorem 3.21 implies that every two-sided 
ideal of a semisimple ring is also semisimple, so to prove
part (ii) of the Lemma we need only show that $A$ is Artinian. Theorem 4.16 and Corollary 4.17 imply that $A = eR = Re$ for some idempotent $e \in A$, and that $R$ has a two-sided unit element. Utilizing these two elements, for any $x \in R$ we see that $x = x \cdot 1 + xe - xe$, or $x = xe + x(1 - e)$. This is called the Peirce decomposition of $R$ relative to $e$, named after the American mathematician Benjamin O. Peirce. (Peirce is credited with several results involving idempotents and their use with arbitrary rings). This decomposition implies that $R = Re + R(1 - e)$, or $R = A + R(1 - e)$.

We claim that $R(1 - e)$ is a two-sided ideal of $R$. The element $0 = 0(1 - e) \in R(1 - e)$, and $R(1 - e)$ is closed under subtraction. To show closure under multiplication with $R$ from the left, recall that $R$ has a 1, which implies that $RR = R$, and so $R(R(1 - e)) = (RR)(1 - e) = R(1 - e)$. Now let $a \in R(1 - e)$, and $r \in R$. This implies that $a = a'(1 - e)$ for some $a' \in R$. Because 1 is a two-sided unit element, and because $e$ is in the center of $R$, we may conclude that:

$$ar = a'(1 - e)r = a' \cdot 1 \cdot r - a' er = a' \cdot r \cdot 1 - a' \cdot r \cdot e = a' r(1 - e) \in R(1 - e).$$

The set $R(1 - e)$ is also closed under multiplication with $R$ from the right, and so is a two-sided ideal of $R$. 

91
Next we will prove that $A \cap R(1-e) = \{0\}$. To show this let $x \in A \cap R(1-e)$. As an element of $A = Re, x = re$ for some $r \in R$. This implies $xe = ree = re = x$. As an element of $R(1-e)$, $x = a(1-e) = a - ae$ for some $a \in R$. Utilizing both of these expressions for $x$, we get that $x = xe = (a - ae)e = ae - aee = ae - ae = 0$. Since $R = A + R(1-e)$, and since $A \cap R(1-e) = \{0\}$, we may conclude that $R = A \oplus R(1-e)$.

ii) Let the homomorphism $\phi : R \to R/R(1-e)$ be given by $\phi(r) = r + R(1-e)$ for all $r \in R$. The kernel of $\phi$ is $R(1-e)$, and since $R = A \oplus R(1-e)$, the image of $\phi$ is strictly $A$. We conclude that $R/R(1-e) \cong A$. If $R$ is Artinian, any quotient of $R$ is Artinian. Since $A$ is the homomorphically image of an Artinian ring, by Theorem 4.9(ii) $A$ is Artinian.

With Lemma 4.19 in hand, we near the proof of the first of the Wedderburn theorems. Having defined a semisimple ring in chapter 2, we now define a ring that is simple:

Definition 4.20 A simple ring

Let $R$ be a ring. $R$ is called simple if $R^2 \neq \{0\}$ and the only two-sided ideals of $R$ are $\{0\}$ and $R$ itself.
In this next Lemma, we show that in many cases "simple" Artinian is a special case of semisimple Artinian.

Lemma 4.21

Let $R$ be a simple Artinian ring. If $R$ has a left, right or two-sided unit element, then $R$ must be semisimple.

Proof: We need to show that $J(R) = \{0\}$. Since $R$ is simple and $J(R)$ is a two-sided ideal of $R$, $J(R)$ must either be $\{0\}$ or $R$. Suppose $J(R) = R$. Since $R$ is Artinian, by Theorem 4.11 $J(R)$ is nilpotent. Thus there exists an $m \in \mathbb{N}$ such that $J(R)^m = R^m = \{0\}$. But $R$ has a unit element (which could be either left, right or two-sided), and so $1^m = 1 \in R^m$, and so we see $R^m \neq \{0\}$. This is a contradiction. $J(R)$ must equal $\{0\}$, and therefore $R$ is a semisimple ring.

Theorem 1(a)

Let $R$ be a semisimple Artinian ring. Then $R$ is the direct sum of a finite number of simple Artinian rings.

Proof: We first prove that if $A$ is a minimal two-sided ideal of a semisimple Artinian ring $R$, then $A$ is a simple ring. Let $A$ be such an ideal. We need to show that $A^2 \neq \{0\}$ and that the only two-sided ideals of $A$, viewed as a
ring, are \( \{0\} \) and \( A \) itself. By Theorem 4.16, \( A = eR = Re \) for some idempotent \( e \in A \), where \( e \) is a unit element of \( A \). This implies that \( e \cdot e = e^2 = e \neq 0 \in A^2 \), and thus \( A^2 \neq \{0\} \). Now suppose there exists some non-zero two-sided ideal of \( A \), call it \( S \), such that \( \{0\} \subset S \subset A \). \( S \) must be closed under multiplication with \( A \) from the left and right, and so \( AS \subseteq S \), and \( SA \subseteq S \), which implies that \( ASA \subseteq S \subset A \). Since \( A \) is a two-sided ideal of \( R \), \( ASA \) is also a two-sided ideal of \( R \). But \( A \) is minimal in \( R \), so if \( ASA \) is a two-sided ideal of \( R \) properly contained in \( A \), it must be \( \{0\} \). Because \( e \in A \), \( eSe \subseteq ASA \) and so \( eSe = \{0\} \).

Since \( S \) is a subset of \( A \), any element of \( S \) is of the form \( eR \) and \( Re \). \( S \) was selected such that \( \{0\} \subset S \), thus there must exist some \( x \neq 0 \in S \) such that \( x = er = r'e \) for some \( r, r' \in R \). If the set \( eSe = \{0\} \), then the element \( exe = 0 \). But observe that \( e(x)e = e(er)e = ere = (er)e = (r'e)e = r'e = x \neq 0 \), a contradiction. Such an ideal \( S \) does not exist, and we conclude that the only ideals of the ring \( A \) are \( \{0\} \) and \( A \). Thus, \( A \) is a simple ring.

Returning to our original goal, let \( R \) be a semisimple Artinian ring, and let \( A \) be a minimal two-sided ideal of \( R \). If such an ideal does not exist in \( R \), then \( R \) is simple, and
we are done. If $A_i$ does exist, then by Lemma 4.19, $R= \bigoplus A_i \oplus R_i$, where $R_i$ is a two-sided ideal of $R$. By Lemma 4.19, $R_i$ is itself semisimple Artinian, and certainly may be viewed as a ring. Now let $A_2$ be a minimal two-sided ideal of $R$ contained in $R_i$. If such an ideal does not exist, $R_i$ must be minimal. Then $R= A_i \oplus R_i$ and we are done. If $A_2$ does exist, then $R_i= A_2 \oplus R_2$ where $R_2$ is a two-sided ideal of $R$, and so $R= A_i \oplus A_2 \oplus R_2$. Continuing this process creates a chain, where each $A_i$ is a minimal two-sided ideal of $R$. The chain shall become stationary. If it did not, this would imply that $R= A_i \oplus A_2 \oplus \ldots \oplus A_n \oplus \ldots$. From this infinite direct sum of ideals, we can create an infinite descending chain of ideals of $R$:

$$R=(A_i \oplus A_2 \oplus \ldots \oplus A_n \oplus \ldots) \supseteq (A_2 \oplus A_3 \oplus \ldots \oplus A_n \oplus \ldots) \supseteq (A_3 \oplus A_4 \oplus \ldots \oplus A_n \oplus \ldots)$$

But $R$ is Artinian, and so every descending chain of ideals of $R$ must become stationary. This implies that for some $k \in \mathbb{N}$, $R= A_i \oplus A_2 \oplus \ldots \oplus A_k$, where each $A_i$ is a minimal two-sided ideal of $R$. As we proved at the outset, each $A_i$ has the structure of a simple ring. ☐
It is natural to wonder if this partition of $R$ into simple rings/minimal two-sided ideals is unique, excluding order. It is, and we close chapter 4 with the proof.

**Corollary 4.22**

Let $R$ be a semisimple Artinian ring. Then $R$ is the direct sum of a finite number of simple Artinian rings, i.e. $R = A_1 \oplus A_2 \oplus \ldots \oplus A_k$ for some $k \in \mathbb{N}$. If $\rho$ is a non-zero minimal two-sided ideal of $R$, then $\rho = A_j$ for some $j \in \{1, 2, \ldots, k\}$.

**Proof:** Let $R$ be a semisimple Artinian ring, and let $\rho$ be a non-zero minimal two-sided ideal of $R$. By Theorem 1(a), $R = A_1 \oplus A_2 \oplus \ldots \oplus A_k$ for some $k \in \mathbb{N}$, where each $A_i$ is a simple ring. Recall that during the proof of Theorem 1(a) we also showed that each $A_i$ is a minimal two-sided ideal of $R$.

Since $R$ is semisimple and Artinian, by Corollary 4.17 $R$ must have a unit element. Since $\rho \neq \{0\}$, $1 \cdot \rho \neq \{0\}$, and the ideal $R \rho \neq \{0\}$. But $R = A_1 \oplus A_2 \oplus \ldots \oplus A_k$, and thus $(A_1 \oplus A_2 \oplus \ldots \oplus A_k) \rho \neq \{0\}$. This implies that for some $i \in \{1, 2, \ldots, k\}$, $A_i \rho \neq \{0\}$. Both $A_i$ and $\rho$ are two-sided ideals of $R$, and so
$A_i \rho \subseteq \rho$, and $A_i \rho \subseteq A_i$. But both $A_i$ and $\rho$ are minimal as well, thus $A_i \rho = \rho$ and $A_i \rho = A_i$. We see $\rho = A_i$. \qed
CHAPTER FIVE

THE WEDDERBURN-ARTIN THEOREM

At the end of Chapter Four, we proved the first of the Wedderburn theorems: any semisimple Artinian ring $R$ is the direct sum of a finite number of simple rings. In this chapter, we will prove a second famous Wedderburn result, and the one which bears his name - the Wedderburn-Artin Theorem. This theorem fully describes the structure of simple Artinian rings, and taken with the first result, the structure of semisimple rings is also completely determined. To begin, we introduce the notion of a primitive ring.

**Definition 5.1  A primitive ring**

Let $R$ be a ring. We say that $R$ is primitive if it has a faithful irreducible $R$-module.

Thus, to prove a ring $R$ is primitive, it is sufficient to show that there exists some irreducible $R$-module $M$ such that for any $r \in R$, $Mr = \{0\}$ implies $r = 0$. Technically, the definition above should read "right primitive ring," but even as with $R$-modules we will omit the "right" for ease of use.
Lemma 5.2

\( \mathbb{Z} \) is not primitive.

Proof: Suppose there exists an irreducible \( \mathbb{Z} \)-module \( M \) that is faithful. This implies that \( M \) is isomorphic to \( \mathbb{Z}/\rho \) for some maximal regular right ideal \( \rho \) of \( \mathbb{Z} \), and that \( \mathbb{Z}/\rho \cdot x = [0] \Rightarrow x = 0 \) for any \( x \in \mathbb{Z} \). However, using the fact that \( \mathbb{Z} \) is commutative and that \( \rho \) is a maximal and therefore non-zero ideal of \( \mathbb{Z} \), any non-zero element of \( \rho \) would force a contradiction. Let \( y \neq 0 \in \rho \). See that \( (r+\rho)y = ry + \rho \) for all \( r \in \mathbb{Z} \). But if \( y \in \rho \), \( ry = yr \in \rho \) for all \( r \in \mathbb{Z} \). Thus \( ry + \rho = 0 + \rho \) for any \( r \in \mathbb{Z} \), and we see that \( \mathbb{Z}/\rho \cdot y = [0] \Rightarrow y = 0 \). \( \mathbb{Z} \) is not primitive.

\[ \square \]

Lemma 5.3

Any field \( F \) is primitive.

Proof: Let \( F \) be a field, and observe that \( F \) is an \( F \)-module. As a field, any non-zero submodule \( \rho \) of \( F \) will have an invertible element \( x \in \rho \) such that, when multiplied with \( x^{-1} \in F \), will put the unit \( 1 \in \rho \). This implies \( 1 \cdot F = F \subseteq \rho \). We have shown that the only submodules of \( F \) are \( \{0\} \) and \( F \).
itself, and so $F$ is an irreducible $F$-module. Because $F$ has no zero-divisors, $F \cdot x = \{0\} \Rightarrow x = 0$ for any $x \in F$. Thus $F$ is a primitive ring.

**Lemma 5.4**

Let $F$ be a field. Then $F^n$ is a primitive ring.

**Proof:** To show that $F^n$ is primitive, we must find an irreducible $F^n$-module that is also faithful. In Example 2.12, we showed that the vector space $F^n$ is an irreducible $F^n$-module. To show that it is faithful, suppose it is not. This implies that there exists some non-zero $A = (a_j) \in F^n$ such that $(x_1, x_2, \ldots, x_n) \cdot A = (0, 0, \ldots, 0)$ for all $x_i \in F$. Since $A$ is non-zero, there must exist some $i, j$ such that $a_j \neq 0$. Let $(0, 0, \ldots, 1, \ldots, 0, 0) \in F^n$ where $1$ is in the $i^{th}$ column. We see that $(0, 1, \ldots, 0) \cdot A = (\ast, \ast, \ldots, a_j, \ast, \ast, \ast) \neq (0, 0, 0)$, a contradiction. Thus $F^n$ is an irreducible $F^n$-module that is faithful, which implies that $F^n$ is primitive.

While it is useful to study specific examples, we would like to state general conditions that when present, allow us to conclude that a ring is primitive. This leads
us to the following result. Note that this result is stated only in terms of the ring properties of $R$.

**Theorem 5.5**

A ring $R$ is primitive if and only if there exists a maximal regular right ideal $\rho$ in $R$ such that $(\rho:R)=\{0\}$.

**Proof:** ($\Rightarrow$) Let $R$ be a primitive ring. Thus there exists an irreducible $R$-module $M$ that is faithful. Since $M$ is irreducible, $M$ must be isomorphic to $\frac{R}{\rho}$ for some maximal regular right ideal $\rho$ of $R$. Since $M$ is faithful, $A(M)=\{0\}$. During the proof of Lemma 3.14, we showed that when $\rho$ is a maximal regular right ideal of $R$, $A(M)=(\rho:R)$. Thus $(\rho:R)=\{0\}$.

($\Leftarrow$) Let $\rho$ be a maximal regular right ideal of $R$ such that $(\rho:R)=\{0\}$. By Theorem 2.19, we know that $\frac{R}{\rho}$ is an irreducible $R$-module, and again, $\{0\}=(\rho:R)=A\left(\frac{R}{\rho}\right)$. This implies that $\frac{R}{\rho}$ is an irreducible $R$-module that is faithful, which in turn implies that $R$ is primitive.

It turns out that semisimplicity is a special case of being primitive.
Lemma 5.6

If $R$ is primitive, then $R$ is semisimple.

Proof: In Theorem 5.5 we showed that $R$ is primitive implies that there exists a maximal regular right ideal $\rho$ of $R$ such that $(\rho:R)=A(M_1)=\{0\}$, where $M_1=R/\rho$ is a faithful irreducible $R$-module. Recall that $J(R)=\cap A(M)$ as $M$ ranges across all possible irreducible $R$-modules. Therefore

$$J(R)=\cap A(M) \subseteq A(M_1)=\{0\}.$$ 

Let $M$ be an $R$-module. Recall that $E(M)$ is the ring of all additive endomorphisms of $M$, and that each $r \in R$ can be thought of as an element of $E(M)$ via the function $T_r:M \to M$ given by $(m)T_r=mr$. In Chapter Two, we defined the commuting ring of $R$ on $M$, or $C(M)$, to be $C(M)=\{\alpha \in E(M) | \alpha T_r=T_r \alpha \ \forall r \in R\}$, and proved that when $M$ is irreducible, $C(M)$ is a division ring. This is the famous Schur's Lemma. The relationship between $M$ and $C(M)$ can be expressed in another way.

Lemma 5.7

If $M$ is an irreducible $R$-module, $M$ is a right vector space over $C(M)$. 

102
Proof: Since $M$ is an irreducible $R$-module, $C(M)$ is a division ring. We note that as $M$ is an additive abelian group, all of the additive right vector space properties are satisfied. We need only prove the four properties that tie in the "scalars" from $C(M)$ to the "vectors" from $M$. Since $C(M)$ is a division ring, the multiplication of $C(M)$ elements will not be commutative. However, this is not requisite for the structure of a right vector space. We will preserve the order of any multiplication of $C(M)$ elements.

To start, we observe that since each $\alpha \in C(M)$ is an additive endomorphism of $M$, $(m_1+m_2)\alpha = (m_1)\alpha + (m_2)\alpha$ for all $m_1,m_2 \in M$. Continuing, because the addition in $E(M)$ was defined to be point-wise, $(m)(\alpha + \beta) = (m)\alpha + (m)\beta$ for all $\alpha, \beta \in C(M)$ and $m \in M$. Also, because we defined multiplication in $C(M) \subseteq E(M)$ to be composition of functions, $((m)\alpha)\beta = (m)(\alpha \beta)$ for all $\alpha, \beta \in C(M)$ and $m \in M$. We finish by noting that the identity function $I$ is an element of $C(M)$, and $(m)I = m$ for all $m \in M$. 

We will take this linear algebra theme one step further. To do so, we introduce the idea of density, with
which we tie in the action of $R$ on $M$ to the right vector space $M$ over $C(M)$.

**Definition 5.8 Density**

Let $M$ be an $R$-module, and let $C(M)$ be the commuting ring of $R$ on $M$. $R$ acts densely on $M$ if for every $n \in \mathbb{N}$ where $m_1, m_2, \ldots, m_n \in M$ are linearly independent over $C(M)$, and for any $v_1, v_2, \ldots, v_n \in M$, there exists some $r \in R$ such that:

$m_1 r = v_1,$ $m_2 r = v_2,$ $m_3 r = v_3,$ $\ldots,$ and $m_n r = v_n.$

**Lemma 5.9**

Let $M$ be a faithful $R$-module that is finite-dimensional over $C(M)$, and let $R$ act densely on $M$. Then $R$ is isomorphic to $C(M)_n$, the ring of $n \times n$ matrices over $C(M)$, where $n$ is the dimension of $M$ over $C(M)$.

**Proof:** Let $n$ be the dimension of $M$ over $C(M)$, and let $m_1, m_2, \ldots, m_n \in M$ be a linearly independent set of elements of $M$ over $C(M)$. This implies that for any $v \in M$, there exists $c_1, c_2, \ldots, c_n \in C(M)$ such that $v = (m_1)c_1 + (m_2)c_2 + \ldots + (m_n)c_n$. Next, let $v_1, v_2, \ldots, v_n \in M$. Since $R$ is dense on $M$, there exists some $r \in R$ such that: $m_1 r = v_1,$ $m_2 r = v_2,$ $m_3 r = v_3,$ $\ldots,$ and $m_n r = v_n$. Now, since each $v_i$ is an element of $M$, there exist $c_{i1}, c_{i2}, \ldots, c_{in} \in C(M)$
such that \( v_i = (m_1)c_{i1} + (m_2)c_{i2} + \ldots + (m_n)c_{in} \). Let \( C = (c_{ij}) \), an \( n \times n \) matrix in the ring \( C(M) \). We see immediately that the action of \( r \) has been replicated, i.e. \( (m_1, m_2, \ldots, m_n) \cdot C = (v_1, v_2, \ldots, v_n) \). The action of \( r \) and \( C \) on the vectors \( m_1, m_2, \ldots, m_n \) is identical.

We know \( C \) is a linear transformation from the right vector space \( M^n \) over \( C(M) \) to the right vector space \( M^n \) over \( C(M) \), but we prove here that \( r \) is one as well. The linearity of \( r \) flows directly from the \( R \)-module relationship with \( M \), and to show the second property of linear transformations, we utilize the fact that every element of \( C(M) \) by construction commutes with every element of \( R \). Thus \( ((m)c)r = (m)(cr) = (m)(rc) = ((m)r)c \) for all \( m \in M \) and \( c \in C(M) \). We conclude that each element \( r \) induces a linear transformation from \( M^n \rightarrow M^n \) over \( C(M) \).

We know that \( C(M)_n \) represents the set of all possible linear transformations from the right vector space \( M^n \) over \( C(M) \) to the right vector space \( M^n \) over \( C(M) \). Let \( \phi : R \rightarrow C(M)_n \) be given by \( \phi(r) \mapsto A \), where \( A \) is the matrix of \( C(M)_n \) that replicates the action of \( r \) on the elements \( m_1, m_2, \ldots, m_n \). Matrix representations of linear transformations are unique, and
so this function is well-defined. Since every element of $R$ induces a linear transformation from $M^n \to M^n$, and $C(M)_n$ represents the set of all possible linear transformations from $M^n \to M^n$, we conclude that the function is defined for all $r \in R$. To show that $\phi$ is onto, let $A \in C(M)_n$. This implies that $(m_1, m_2, ..., m_n) \cdot A = (x_1, x_2, ..., x_n)$ for some $x_1, x_2, ..., x_n \in M$. But because $R$ is dense on $M$, there must exist some $r \in R$ such that $m_1 r = x_1$, ..., $m_n r = x_n$. Thus $\phi(r) = A$. This function $\phi$ is onto, and while we will not prove it here, is a ring homomorphism. What is the kernel of $\phi$? The set of all elements of $R$ that map to the zero matrix of $C(M)_n$. Because $M$ is a faithful $R$-module, the only such element is $r = 0$.

Taking all of this together, we conclude that

$$\frac{R}{\text{ker}(\phi)} \cong \text{image}(\phi), \text{ i.e. } R \cong C(M)_n.$$  

We now come to a powerful theorem that provides a crucial step in the proof of the Wedderburn-Artin Theorem. Simply called the Density Theorem, it is credited to N. Jacobson and C. Chevalley.
Theorem 5.10  The Density Theorem

Let $R$ be a primitive ring, and let $M$ be a faithful irreducible $R$-module. Then $R$ is a dense ring of linear transformations on $M$ over $C(M)$.

Proof: In Lemma 5.7, we showed that $M$ is a right vector space over $C(M)$. To prove the density theorem, we will first prove the following statement: If $V$ is a finite dimensional right subspace of the right vector space $M$ over $C(M)$, and if there exists an $m \in M$ such that $m \not\in V$, then there exists an $r \in R$ such that $Vr = \{0\}$ and $mr \neq 0$.

We will do this by induction on the dimension $n$ of $V$. If $n=0$, $V_0 = \{0\}$. Since $M$ is irreducible, $MR \neq \{0\}$ and so there must exist some $m \in M$, such that $m \not\in V_0$. For the same reason, there exists an $r \in R$ such that $mr \neq 0$. Of course, $V_0 \cdot r = \{0\} \cdot r = \{0\}$. Thus the statement is true for $n=0$.

Now assume the statement is true for some $k$. Thus for any $k$-dimensional right subspace $V_k$ of $M$ over $C(M)$, if there exists an $m \in M$ such that $m \not\in V_k$, there must exist an $r \in R$ such that $V_k r = \{0\}$ but $mr \neq 0$. 

107
Let $V_{k+1}$ be a $k+1$-dimensional right subspace of $M$ over $C(M)$. Since $V_{k+1}$ has dimension $k+1$, $V_{k+1} = \{e_1c_1 + \ldots + e_kc_k + e_{k+1}c_{k+1} | c_i \in C(M)\}$ for some basis vectors $\{e_1, e_2, \ldots, e_k, e_{k+1}\} \subseteq M$. Since the basis vectors $e_i$ are linearly independent, observe that the span of the vectors $\{e_1, \ldots, e_k\}$ over $C(M)$ is a $k$-dimensional right subspace of $M$ over $C(M)$. Let $V_k$ be the span of $\{e_1, \ldots, e_k\}$ over $C(M)$, and observe that $V_{k+1} = V_k + e_{k+1} \cdot C(M)$. Since $\{e_1, e_2, \ldots, e_k, e_{k+1}\}$ are linearly independent, observe further that $e_{k+1} \notin V_k$. So in fact, $V_{k+1} = V_k + e_{k+1} \cdot C(M)$.

Now, define the set $A_k = \{x \in R | V_k x = \{0\}\}$. $A_k$ is a right ideal of $R$, and is the set of all elements of $R$ that annihilate $V_k$ from the right. Since $e_{k+1} \notin V_k$, by assumption we know that there must exist at least one such $r \in R$ such that $e_{k+1}r \neq 0$. If no such $r$ exists, $e_{k+1}$ cannot be outside of $V_k$. This can be summarized as follows: $e_{k+1} \cdot A_k = \{0\} \Rightarrow e_{k+1} \in V_k$.

However, because we have assumed the statement to be true for $k$, we may safely conclude that $e_{k+1} \cdot A_k \neq \{0\}$. Thus $e_{k+1} \cdot A_k$ must be a submodule of $M$, and since $M$ is irreducible and $e_{k+1} \cdot A_k \neq \{0\}$, we have that $e_{k+1} \cdot A_k = M$. 

108
Select some \( y \in M \) such that \( y \notin V_{k+1} \). We'd like to show that \( V_{k+1} r = \{0\} \Rightarrow yr \neq 0 \) for some \( r \in R \). Suppose this is not the case, i.e. that \( yr = 0 \) for all \( r \in R \) that annihilate \( V_{k+1} \).

Since \( e_{k+1} A_k = M \), every element of \( M \) has the form \( e_{k+1} a \) for some \( a \in A_k \). Let \( \phi : M \to M \) be given by \( (x)\phi = ya \) for all \( x \in M \), where \( a \in A_k \) such that \( x = e_{k+1} a \). The function \( \phi \) takes an element \( x \in M \), finds the element \( a \in A_k \) such that \( x = e_{k+1} a \), and then maps to the element \( ya \). To see that \( \phi \) is well-defined, let \( x = 0 \). Thus \( x = 0 = e_{k+1} a \) for some \( a \in A_k \). Since \( C(M) \) commutes with every element of \( R \supseteq A_k \), and since \( a \in A_k \), which annihilates all of \( V_k \), we see that

\[
V_{k+1} a = (V_k + e_{k+1} C(M)) a = V_k a + e_{k+1} C(M) a = \{0\} + e_{k+1} a \cdot C(M) = \{0\} + \{0\} = \{0\}.
\]

Hence \( a \) annihilates \( V_{k+1} \), and so by our supposition, \( ya = 0 \).

Thus \( 0 = x = (x)\phi = ya = 0 \), and since \( \phi \) is linear, we have shown that is it well-defined. To verify that \( \phi \) is linear, observe that for any \( x_i \in M \), \( x_i = e_{k+1} a_i \) for some \( a_i \in A_k \), and:

\[
(x_1 + x_2) \phi = (e_{k+1} a_1 + e_{k+1} a_2) \phi = (e_{k+1} (a_1 + a_2)) \phi = y(a_1 + a_2) = ya_1 + ya_2 = (e_{k+1} a_1) \phi + (e_{k+1} a_2) \phi = (x_1) \phi + (x_2) \phi.
\]
Recalling that $A_k$ is a right ideal of $R$, $a \in A_k \Rightarrow ar \in A_k$ for any $r \in R$. Thus $(xr)\phi = ((e_{k+1}a)r)\phi$, where $x = e_{k+1}a$ for some $a \in A_k$.

But $((e_{k+1}a)r)\phi = (e_{k+1}(ar))\phi = y(ar) = (ya)r = (x)\phi \cdot r$. This implies that $\phi$ commutes with every element of $r$, and so must itself be an element of the commuting ring of $R$ on $M$, $C(M)$. Thus for any $a \in A_k$, $ya = (e_{k+1}a)\phi = (e_{k+1})\phi \cdot a$, which implies 

$\phi = (y - (e_{k+1}))a = 0 \ \forall a \in A_k$. But earlier we showed that $e_{k+1} \cdot A_k = \{0\} \Rightarrow e_{k+1} \in V_k$. Therefore $y - (e_{k+1})\phi \in V_k$, which implies that $y \in V_k + (e_{k+1})\phi \subseteq V_k + e_{k+1} \cdot C(M) = V_{k+1}$. But by selection $y \notin V_{k+1}$, thus this is a contradiction. There must exist some $r \in R$ such that $V_{k+1} \cdot r = \{0\}$ and $yr \neq 0$. We have shown the statement to be true for $k+1$.

Thus if $V$ is a finite dimensional right subspace of the right vector space $M$ over $C(M)$, and if there exists an $m \in M$ such that $m \notin V$, then there exists an $r \in R$ such that $Vr = \{0\}$ and $mr \neq 0$. We will now use this statement to show that $R$ is a dense ring of linear transformations on $M$ over $C(M)$. In Lemma 5.9 we proved that each element of $R$ induced a linear transformation on $M$ over $C(M)$, thus all that remains is to show the density of $R$ on $M$. Let $m_1, m_2, ..., m_n \in M$
be linearly independent over $C(M)$, and let $v_1, v_2, \ldots, v_n \in M$. Let $U_i$ be the span of the vectors $\{m_k \mid k \neq i\}$ over $C(M)$. For example, $U_3 = \{m_1c_1 + m_2c_2 + m_3c_3 + \ldots + m_nc_n \mid c_i \in C(M)\}$. If $\{m_1, m_2, \ldots, m_n\}$ are linearly independent, every non-zero subset of these vectors will also be linearly independent, and so each $U_i$ is an $n-1$ dimensional subspace of $M$. And, because of the linear independence of $\{m_1, m_2, \ldots, m_n\}$, we may safely state that $m_i \notin U_i$. We use our statement to claim that there must exist some $r \in R$ such that $U_i \cdot r = \{0\}$ and $m_i r \neq 0$. Since $M$ is an irreducible $R$-module, $m_i r \neq 0$ implies that $m_i r R = M$. Thus any element of $M$ has the form $m_i r x$ for some $x \in R$. In particular, $v_i = m_i r s_i$ for an $s_i \in R$. Observe too that $U_i \cdot r s_i = (U_i \cdot r) s_i = \{0\} \cdot s_i = \{0\}$. Now let $s = s_1 + s_2 + \ldots + s_n$. Observe that:

$$m_i(s) = m_i(rs_1 + rs_2 + \ldots + rs_n) = m_i rs_1 + m(rs_1 + \ldots + rs_n) = v_1 + 0 = v_1,$$

and

$$m_i(s) = m_i(rs_1 + rs_2 + \ldots + rs_n) = m_i rs_1 + m(rs_1 + \ldots + rs_{i-1} + rs_{i+1} + \ldots + rs_n) = v_i.$$

We have shown that $R$ is dense on $M$. 

With the Density Theorem in hand, we come at last to the Wedderburn-Artin. This Theorem fully describes the structure of simple Artinian rings, and taken together with
the first Wedderburn theorem, Theorem 1(a), completely determines the structure of semisimple Artinian rings.

**Theorem 1(b) The Wedderburn-Artin Theorem**

Let $R$ be a simple Artinian ring. Then $R$ is isomorphic to $D_n$, the ring of $n \times n$ matrices over a division ring $D$. Both $D$ and $n$ are unique up to isomorphism. Conversely, for any division ring $D$, $D_n$ is a simple Artinian ring.

**Proof:** We first wish to show that $R$ is primitive. In Theorem 4.11, we showed that the radical of any Artinian ring is nilpotent, and in Lemma 3.13 we established that the radical is a two-sided ideal of $R$. But $R$ is simple, and so has only two ideals, $\{0\}$ and $R$ itself. If $J(R) = R$, this implies that $R$ is nilpotent, i.e. $R^m = \{0\}$ for some $m \in \mathbb{N}$. But since $R$ is simple, $R^2 = R$, which implies that $R^m = R$ for all $m \in \mathbb{N}$. This is a contradiction. If $J(R) \neq R$, then $J(R) = \{0\}$. Thus $R$ is semisimple and simple. $R$ then may be viewed as a faithful, irreducible $R$-module. Since we have shown the existence of such an $R$-module, we conclude that $R$ is primitive.
We have already shown that any such faithful, irreducible $R$-module $M$ is a right vector space over $C(M)$. If we can show that $M$ is finite-dimensional, then the Density Theorem would directly apply. Suppose $M$ is infinite-dimensional over $C(M)$. This implies that there exists an infinite set of vectors that are linearly independent in $M$ over $C(M)$: $m_1, m_2, \ldots, m_n, \ldots$ Construct ideals of $R$ in the following way. First let

$$V_k = \{m_1c_1 + m_2c_2 + \ldots + m_kc_k \mid c_i \in C(M)\},$$

i.e. $V_k$ is the finite-dimensional subspace generated by the first $k$ vectors in the $m_i$ list. For each $V_k$, let $A_k = \{x \in R \mid V_k \cdot x = \{0\}\}$. The statement that we utilized in the proof of the Density Theorem implies that the chain $A_1 \supseteq A_2 \supseteq A_3 \supseteq \ldots \supseteq A_k \supseteq \ldots$ is in fact a properly descending chain of right ideals of $R$. Since $R$ is Artinian this chain must become stationary. This implies that for some $n \in \mathbb{N}$, $A_n = \{0\}$. But that implies that the set $\{m_1, m_2, \ldots, m_n\}$ are linearly dependent, which implies that $M$ is finite-dimensional, a contradiction. Therefore the Density Theorem does apply, and we may conclude that $R$ is dense on $M$. Moreover, Lemma 5.9 allows us to conclude
that $R \cong C(M)_n$, and since $C(M)$ is a division ring, $R \cong D_n$ for a division ring $D$.

To show both $n$ and $D$ are unique up to isomorphism, suppose $R \cong D_n$, and $R \cong S_m$ for some division rings $D, S$ and for some $m, n \in \mathbb{N}$. If $R \cong D_n$, and $R \cong S_m$, then $D_n \cong S_m$. Since they are isomorphic, we have immediately that $m = n$. Let $\phi: D_n \to S_m$ be a ring isomorphism.

Now let $e = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix} \in D_n$, and let $\phi(e) = f$. This element $e \in D_n$ is an idempotent of $D_n$, and because $\phi$ preserves ring structure, $f$ must be an idempotent of $S_m$. We see that by construction $eD_ne \subseteq D$, and likewise $f \cdot S_m \cdot f \subseteq S$. Utilizing the isomorphism $\phi$, we conclude that $D \cong eD_ne \equiv \phi(eD_ne) = f \cdot S_m \cdot f \subseteq S$. We have proven that $n = m$, and $D \cong S$.

To prove the converse, recall that by Theorem 4.9(i), any division ring $D$ is Artinian, and by Theorem 4.9(iv) $D_n$ must also be Artinian. Using arguments similar to those found in Example 3.17 and Example 2.20, we claim $D_n$ is semisimple. Thus Theorem 4.20 allows us to conclude that
$D_n$ has a two-sided unit element. Thus $D_n$ is semisimple, Artinian, and contains a two-sided unit element. It must be simple.
BIBLIOGRAPHY


