Theory of Rings

Farid Aliniaeifard

Contents

Abstract

Where does the name "ring" come from? Here what I found in stackexchange webpage at https://math.stackexchange.com/questions/61497/why-are-rings-called-rings: The name "ring" is derived from Hilbert's term "Zahlring" (number ring), introduced in his Zahlbericht for certain rings of algebraic integers. As for why Hilbert chose the name "ring", I recall reading speculations that it may have to do with cyclical (ring-shaped) behavior of powers of algebraic integers. Namely, if α is an algebraic integer of degree n then α^n is a $\mathbb{Z}$-linear combination of lower powers of α, thus so too are all higher powers of α. Hence all powers cycle back onto $1, \alpha, \cdots, \alpha^{n-1}$, i.e. $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module. Possibly also the motivation for the name had to do more specifically with rings of cyclotomic integers. In this course we start with category theory and then dive into the category of rings, and this category we first study commutative rings and modules, and then we talk about structure of rings and we will see the structures of semisimple rings, prime and semiprime rings, Algebras and devision algebras. In the end we talk about local rings, semilocal rings, and idempotents.

Chapter 1

Categories

1.1 Categories

Definition. *A* **category** *is a class $\mathcal{C}$ of objects together with*

(i) a class of disjoint sets hom(A, B) for any two arbitrary objects in $\mathcal{C}$ (any element $f : A \to B$ of hom(A, B) is called a morphism from A to B).

(ii) For morphisms $f : A \to B \in hom(A, B)$ and $g : B \to C \in hom(B, C)$, there is a morphism $gof : A \to C$ in hom(A, C) such that satisfies

(a) Associativity. If $f : A \to B$, $g : B \to C$, and $h : C \to D$ are morphisms of $\mathcal{C}$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

(b) Identity. For each object B of $\mathcal{C}$ there exists a morphism $1_B : B \to B$ such that for any $f : A \to B$, $g : B \to C$,

$$1_B \circ f = f \quad \text{and} \quad g \circ 1_B = g.$$

Definition. *In a category $\mathcal{C}$ a morphism $f : A \to B$ is called an* **equivalence** *if there is a morphism $g : B \to A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. If $f : A \to B$ is an equivalence, A and B are said to be* **equivalent**.

Example 1.1.1. *The following are examples of categories.*

1. *The class $\mathcal{S}$ of sets with hom(A, B) the set of all functions from A to B.*

2. *The class $\mathcal{G}$ of groups with hom(G, H) the set of all group homomorphisms from G to H.*

3. *The class of all partially ordered sets $\mathcal{P}$. A morphism $(S, \leq) \to (T, \leq)$ is a function that preserve the order.*

4. *The class $\mathcal{R}$ of rings with hom(R, S) the set of all ring homomorphisms from R to S.*

Chapter 2

Commutative Rings and Modules

2.1 Chain Condition

Definition. *A module A is said to be* **Noetherian** *if it satisfies the ascending chain condition (ACC) on its submodules, that is for every chain*

$$A_1 \subset A_2 \subset A_3 \subset \cdots$$

of submodules of A, there is an integer n such that $A_i = A_n$ for all $i \geq n$.

A module B is said to be **Artinian** *if it satisfies the descending chain condition (DCC) on its submodules, that is for every chain*

$$B_1 \supset B_2 \supset B_3 \supset \cdots$$

of submodules of B, there is an integer m such that $B_i = B_m$ for all $i \geq n$.

Example 2.1.1. *The $\mathbb{Z}$-module $\mathbb{Z}$ is not Artinian because we have*

$$2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \cdots$$

is never stable, but any ascending chain condition is stable (exercise).

Definition. *A ring R is* **left [resp. right) Noetherian** *if R satisfies the ascending chain condition on left [resp. right) ideals. R is said to be Noetherian if R is both left and right Noetherian. A ring R is* **left [resp. right) Artinian** *if R satisfies the descending chain condition on left [resp. right) ideals. R is said to be Artinian if R is both left and right Artinian.*

Example 2.1.2. *A division ring D is both Artinian and Noetherian since it has only two ideals $\mathbf{0}$ and D.*
Any PID is Noetherian (Exercise).

Definition. *A module A satisfies* **maximum [resp. minimum] condition** *on submodules if any subset of submodules of A has a maximal [resp. minimal] element.*

Theorem 2.1.3. *If A is a Noetherian [resp. Artinian] module if and only if it satisfies maximum [resp. minimum] condition on submodules.*

Proof. $\Rightarrow$) Suppose A is Noetherian and S is an arbitrary set of submodules. Suppose on the contrary that S does not have a maximal element. Choose an arbitrary element $B_0 \in S$. Since S has no maximal element, there is an element $B_1 \in S$ such that $B_0 \subset B_1$, also there is an element B_2 such that $B_0 \subset B_1 \subset B_2$. By continuing this process we will find a non-stable ascending chain, contradiction.
$\Leftarrow$) Consider an arbitrary chain

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$$

of submodules of A. Let $S = \{A_i : i \in \mathbb{N}\}$. Then S has a maximal, say A_m. Then for every $i \geq m$, we have $A_i = A_m$. Therefore, A is Noetherian. □

Theorem 2.1.4. *Let $0 \to A \overset{\alpha}{\to} B \overset{\beta}{\to} C \to 0$ be a short exact sequence of modules. Then B is Noetherian [resp. Artinian] if and only if A and C are Noetherian [resp. Artinian].*

Proof. If B is Noetherian, then A is isomorphic to a submodule of B and so A is Noetherian. Moreover, $B/ker(\beta) \cong C$. Therefore, C also must be Noetherian.

Conversely, If

$$B_0 \subset B_1 \subset B_2 \subset \cdots$$

is a chain of submodules of B. Let $A_i = \alpha^{-1}(\alpha(A) \cap B_i)$ and $C_i = g(B_i)$. Consider that the chains

$$A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \quad \text{and} \quad C_0 \subseteq C_1 \subseteq C_2 \subseteq \cdots$$

are stable. Let m be an integer such that for every $i \geq m$, $A_i = A_m$ and $C_i = C_m$. Thus

$$\alpha^{-1}(\alpha(A) \cap B_m) = \alpha^{-1}(\alpha(A) \cap B_i) \quad \text{and} \quad \beta(B_m) = \beta(B_i).$$

Let $b \in B_i$. Then $\beta(b) = \beta(b_m)$ for some $b_m \in B_m$. Thus $\beta(b - b_m) = 0$, and so $b - b_m \in ker(\beta) = Img(\alpha)$. Therefore, $b - b_m \in \alpha(A) \cap B_i = \alpha(A) \cap B_m$. We can conclude that $b \in B_m$, and so $B_i = B_m$. □

Corollary 2.1.5.

1. *Let B be a Noetherian [resp. Artinian] module, then for every submodule A of B we have A and B/A are Noetherian [resp. Artinian].*

2. *Let $\{A_i : i = 1, \ldots, n\}$ be a set of modules. Then $A_1 \oplus \ldots \oplus A_n$ is Noetherian [resp. Artinian] if and only if each A_i is so.*

Theorem 2.1.6. *If R is a left Noetherian [resp. Artinian] ring with identity, then every finitely generated unitary left R-module A satisfies the ascending [resp. descending) chain condition on submodules.*

Proof. Let $\{a_1, \dots, a_n\}$ be the set of generators for A. Consider the free R-module $F = \oplus_{i=1}^n R$. Then $\pi : F \to A$ defined by $(r_1, \dots, r_n) \mapsto r_1 a_1 + \dots + r_n a_n$ is a surjective homomorphism, and so A is a quotient submodule of F (by previous corollary F is Noetherian) and so it is Noetherian. □

Theorem 2.1.7. *A module A is Noetherian if and only if every submodule of A is finitely generated. In particular, a commutative ring R is Noetherian if and only if every ideal of R is finitely generated.*

Proof. If B is a submodule of A, then if A is not finitely generated, we can construct a non-stable chain of submodules.

Moreover, if we have a chain of submodules

$$A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$$

and $\cup_i A_i$ is generated by $a_1, \dots, a_n$, then there is A_m such that contains all a_i's and so for every $i \geq m$, we have $A_i = A_m$. □

Example 2.1.8. *Consider the ring $\mathbb{Q}[x_1, x_2, \dots]$ in infinitely many variables. Then this ring is a finitely generated module over itself, but its ideal $\langle x_1, x_2, \dots \rangle$ is not finitely generated.*

Definition. *A composition series for a module A is a series of submodules $A = A_0 \supset A_1 \supset A_2 \supset \dots \supset A_n = 0$ such that all factors A_i/A_{i+1} are simple.*

Theorem 2.1.9. *A nonzero module A has a composition series if and only if A satisfies both the ascending and descending chain conditions on submodules.*

Proof. Suppose that A has a composition series of length n. If either condition fails then one can find a normal series

$$A = A_0 \supset A_1 \supset A_2 \supset \dots \supset A_n \supset A_{n+1}.$$

This yields to the fact that we have a composition series of length at least $n + 1$, but all composition series have the same lengths.

Conversely, suppose A is both Noetherian and Artinian. First consider the set

$$S_1 = \{B \neq A, 0 : B \subseteq A\}.$$

If $S_1 = \emptyset$, then we have a composition series $A \supset 0$. If $S_1 \neq \emptyset$, by the fact that A is Noetherian, we can say S_1 has a maximal element, say A_1. Thus, we have $A = A_0 \supset A_1 \supset 0$. Now consider

$$S_2 = \{B \neq A_1, A, 0 : B \subset A\}.$$

If the set S_2 is empty then we already have a composition series, so let assume that there it is non-empty, and so it has a minimal element, say A_2. We now have $A = A_0 \supset A_1 \supset A_2 \supset 0$. Since A is Artinian continuing this process at some point we should arrive to some S_i such that it is empty and so we have a composition series. □

Corollary 2.1.10. *If D is a division ring, then the ring $Mat_n(D)$ $o\ f$ all $n \times n$ matrices over D is both Artinian and Noetherian.*

Proof. Let $R = Mat_n(D)$. We show that R has a composition series of left R-modules, and similarly it has a composition series of right R-modules. Let e_i be the matrix with 1 in the position (i, i) and zero in other places. Define $M_i = R(e_1 + \ldots + e_i)$. Then we want to show that

$$R = M_n \supset M_{n-1} \supset \ldots \supset M_1 \supset M_0 = 0.$$

Note that $M_i/M_{i-1} \cong Re_i$. If we show that Re_i is a simple module then the above normal series is a composition series. We leave it as an exercise. $\square$

2.2 Prime and Primary Ideals

- In a commutative ring R a **primary ideal** $Q(\neq R)$ is an ideal with the property that if $ab \in Q$ and $a \notin Q$, then $b^k \in Q$ for some positive integer k.
- In a commutative ring a **prime ideal** $P(\neq R)$ is an ideal with the property that if $ab \subseteq P$ where a and b are elements of R, then $a \in P$ or $b \in P$
- In a ring a **prime ideal** $P(\neq R)$ is an ideal with the property that if $AB \subseteq P$ where A and B are ideals, then $A \subseteq P$ or $B \subseteq P$.

Theorem 2.2.1. *An ideal $P(\neq R)$ in a commutative ring R is prime if and only if $R - P$ is a multiplicative set.*

Proof. If $a, b \in R - P$, then we have $ab \in P$ since P is a prime ideal. $\square$

Definition. *The set of all prime ideals in a ring R is called the spectrum of R.*

Theorem 2.2.2. *If S is a multiplicative subset of a ring R which is disjoint from an ideal I of R, then there exists an ideal P which is maximal in the set of all ideals of R disjoint from S and containing I. Furthermore any such ideal P is prime.*

In the other words, if $S \cap I = \emptyset$, then $\{P \cap S = \emptyset : I \subseteq P\}$ has a maximal element which is also prime.

Proof. Consider the set $\{P \cap S = \emptyset : I \subseteq P\}$. Assume that

$$P_1 \subseteq P_2 \subseteq P_3 \subseteq \ldots$$

is a total chain of the elements of the above set. Then $\cup P_i$ is an ideal that contains I and it has empty intersection with S. Thus $\cup P_i$ is a maximal element of the total chain and so by Zorn's lemma, the set $\{P \cap S = \emptyset : I \subseteq P\}$ has a maximal element, say M. Now suppose that $AB \subseteq M$, $A \nsubseteq M$ and $B \nsubseteq M$ for arbitrary ideals A and B. So we have $M + A$ and $M + B$ are not elements of the set $\{P \cap S = \emptyset : I \subseteq P\}$. Therefore, they must have intersection with S. Let $s_1 \in M + A \cap S$ and $s_2 \in M + B \cap S$. Therefore, $s_1 = m_1 + b$ and $s_2 = m_2 + a$, and

$$s_1 s_2 = m_1 m_2 + b m_2 + a m_1 + ab \in M,$$

which is a contradiction. Thus, M is a prime ideal. □

Theorem 2.2.3. *Let K be a subring of a commutative ring R. If $P_1, \ldots, P_n$ are prime ideals such that $K \subseteq P_1 \cup \ldots \cup P_n$, then $K \subseteq P_i$ for some i.*

Remark. When $n = 2$ we do not need to have the condition that all P_i's are prime.

Proof. Suppose on the contradiction that $K \nsubseteq P_i$ for all i. We can assume that n is minimal in the sense that $K \subseteq P_1 \cup \ldots \cup P_n$. Therefore, for each i, there is $a_i \in K \setminus \cup_{i \neq j} P_j$. We can see that $a_i \in P_i$. Now the element

$$a_1 + a_2 a_3 \ldots a_n \in K \subseteq \cup P_i.$$

We have $a_1 + a_2 a_3 \ldots a_n = b_j \in P_j$ for some j. If $j = 1$, then $a_2 \ldots a_n \in P_1$ and so for some $1 \leq i \leq n$, $a_i \in P_1$, a contradiction. If $j > 1$, then $a_1 \in P_j$, a contradiction. We conclude that $K \subseteq P_i$ for some i. □

Proposition 2.2.4. *If R is a commutative ring with identity and P is an ideal which is maximal in the set of all ideals of R which are not finitely generated, then P is prime.*

Proof. Suppose on the contrary that $ab \in P$, but $a \notin P$ and $b \notin P$. Because of the maximality of P, $P + \langle a \rangle$ and $P + \langle b \rangle$ are finitely generated. Therefore, $P + \langle a \rangle = \langle p_1 + r_1 a_1, \ldots, p_n + r_n a_n \rangle$ and $P + \langle b \rangle = \langle p_1' + r_1' b_1, \ldots, p_m' + r_m' b_m \rangle$. Define $J = \{r \in R : ra \in P\}$, the J is an ideal. Consider that $P + \langle b \rangle \subseteq J$ and so by the maximality of P, J is finitely generated and so $J = \langle j_1, \ldots, j_k \rangle$. If $x \in P$, then $x \in P + \langle a \rangle$. Therefore, there are $s_i \in R$ such that

$$x = \sum_i s_i(p_i + r_i a) = \sum_i s_i p_i + s_i r_i a.$$

So

$$\sum_i s_i r_i a = x - \sum_i s_i p_i \in P.$$

Thus, $\sum_i s_i r_i \in J$, and so for some t_i, we have $\sum_i s_i r_i = \sum_i t_i j_i$ and so $x = \sum_i s_i p_i + \sum_i t_i j_i a$. Therefore,

$$p_1, \ldots, p_n, j_1 a, \ldots, j_k a$$

is a set of generators for P and this is a contradiction. □

Definition. *Let I be an ideal in a commutative ring R. The* **radical (or nilradical)** *of I, denoted Rad I, is the ideal $\cap P$, where the intersection is taken over all prime ideals P which contain I, that is*

$$Rad\ I = \bigcap_{\substack{P\ prime \\ I \subseteq P}} P.$$

If the set of prime ideals containing I is empty, then Rad I is defined to be R.

What is happening when the ring has identity and I is proper? Each proper ideal is inside a maximal ideal so the Rad I is not R.

Theorem 2.2.5. *If I is an ideal in a commutative ring R, then Rad $I = \{r \in R : r^n \in I$ for some $n > 0\}$.*

Proof. If $I = R$, then $Rad\ I = R$, and clearly $\{r \in R : r^n \in R \text{ for some } n > 0\} = R$. So we may assume that $I \neq R$. If $r^n \in I$, then r is in any prime ideal containing I, therefore, $r \in Rad\ I$.

For the converse, we use contrapositive. Assume there is

$$r \notin \{r \in R : r^n \in I \text{ for some } n > 0\}.$$

Then for every $n > 0$, $r^n \notin I$. Thus, $S = \{r^n + x : n \in \mathbb{N} \setminus \{0\}, x \in I\}$ is a multiplicative set with $S \cap I = \emptyset$. Therefore, by Theorem 2.2.2, there is a prime ideal that contains I and its intersection with S is empty. Consider that $r^n \notin P$ and so it cannot be a member of $Rad\ I$. We can conclude that $Rad\ I \subseteq \{r \in R : r^n \in R \text{ for some } n > 0\}$. □

Theorem 2.2.6. *If $I_1, I_2, \ldots, I_n$ are ideals in a commutative ring R with identity, then*

1. *$Rad\ (Rad\ I) = Rad\ I$.*
2. *$Rad\ (I_1 I_2 \ldots I_n) = Rad\ (\cap_{j=1}^n I_j) = \cap_{j=1}^n Rad\ (I_j)$.*
3. *$Rad\ (I^m) = Rad\ I$.*

In the rest of this section all rings are with identity.

Theorem 2.2.7. *If Q is a primary ideal in a commutative ring R, then Rad Q is a prime ideal.*

Proof. Suppose that $ab \in Rad\ Q$, and $a \notin Rad\ Q$. Then we have that $a^n b^n \in Q$ for some positive integer n. Since $a \notin Rad\ Q$, thus $a^n \notin Q$, as Q is a primary ideal, we cans see that $(b^n)^m$ where m is a positive integer, is an element of Q, and so $b \in Rad\ Q$. □

Definition. *If Q is a primary ideal, then $P = Rad\ Q$ is called the* **associated prime ideal** *of Q, or we say Q is* P**-primary**, *or Q is primary for P.*

Theorem 2.2.8. *Let Q and P be ideals in a commutative ring R. Then Q is primary for P if and only if*

1. $Q \subseteq P \subseteq Rad\ Q$.

2. *If* $ab \in Q$ *and* $a \notin Q$*, then* $b \in P$.

Proof. Suppose (1) and (2) hold. If $ab \in Q$ and $a \notin Q$, then $b \in P$, and since $b \in Rad\ Q$, and so $b^m \in Q$ for some positive integer m. Therefore, Q is a primary ideal. Now we want to show that $P = Rad\ Q$. Let $b \in Rad\ Q$, then $b^n \in Q$ for some n. Let n be minimal. If $n = 1$, then $b \in Q \subseteq P$. If $n > 1$, then $b^{n-1}b = b^n \in Q$. By the minimality of n, $b^{n-1} \notin Q$, and so by (2), $b \in P$. □

Theorem 2.2.9. *If* $Q_1, Q_2, \cdots, Q_n$ *are primary ideals in a commutative ring* R*, all of* n *which are primary for the prime ideal* P*, then* $\cap Q_i$ *is also a primary ideal for* P.

Proof. Consider that $Rad\ \cap Q_i = \cap Rad\ Q_i = \cap P = P$. Now we show if $Q = \cap Q_i$, then the two conditions in the above theorem, i.e.,

$Q \subseteq P \subseteq Rad\ Q$;

If $ab \in Q$ and $a \notin Q$, then $b \in P$;
hold and so Q is P-primary. Since $Rad\ Q = P$, thus $Q \subseteq P \subseteq Rad\ Q$. Moreover, if $ab \in Q$ and $a \notin Q$, then there is at least a Q_i such that $ab \in Q_i$ and $a \notin Q_i$, since a is not in Q_i and Q_i is P-primary, we must have $b^n \in Q_i$ and so $b \in Rad\ Q_i = P$. □

Definition. *An ideal* I *in a commutative ring* R *has a primary decomposition if* $I = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ *with each* Q_i *primary. lf no* Q_i *contains* $Q_1 \cap \ldots Q_{i-1} \cap Q_{i+l} \cap \ldots \cap Q_n$ *and the radicals of the* Q_i *are all distinct, then the primary decomposition is said to be* **reduced (or irredundant)**.

Theorem 2.2.10. *Let* I *be an ideal in a commutative ring* R*. If* I *has a primary decomposition, then* I *has a reduced primary decomposition.*

Proof. Let $I = Q_1 \cap \ldots \cap Q_n$ be a primary decomposition for I, and we may assume that no Q_i has the intersection of other Q_i's as a subset, because otherwise we can delete Q_i. Let Q_i be primary ideal belonging to P_i. Let $Q_i^{'} = \cap_{\substack{j \in [1,\ldots,n] \\ Q_j \text{ is } P_i\text{-primary}}} Q_j$, then $\cap Q_i^{'} = I$ and all $Q_i^{'}$'s have different prime ideals. □

Questions: Which ideals have primary decomposition? Is a reduced primary decomposition unique in any way?

2.3 Primary Decomposition

Throughout this section are all commutative with identity and also modules are unitary. In this section we show that any ideal in a Noetherian ring has a primary decomposition.

Definition. *Let R be a commutative ring with identity and B an R-module. A submodule $A(\neq B)$ is* **primary** *provided that if $r \in R$ and $b \notin A$ but $rb \in A$, then there is a positive integer n such that $r^n B \subseteq A$.*

Example 2.3.1. *Consider the ring R as an R-module and let Q be a primary ideal of R, then Q is a submodule of R, moreover, if $r \in R$ and $b \notin Q$ with $rb \in Q$, then there is a positive integer n such that $r^n \in Q$, and so $r^n R \subseteq Q$.*

Theorem 2.3.2. *Let R be a commutative ring with identity and A a primary submodule of an R-module B. Then*

$$Q_A = \{r \in R : rB \subseteq A\}$$

is a primary ideal of R.

Proof. Consider that $Q_A \neq R$ since $1 \notin Q_A$ because otherwise $B \subseteq A$. Let $rs \in Q_A$ such that $s \notin Q_A$. Consequently $sB \nsubseteq A$. Therefore, there is $b \in B$ such that $sb \notin A$. Note that $r(sb) \in A$, and since A is primary $r^n B \subseteq A$ for some positive integer n. Thus, $r^n \in Q_A$. □

Definition. *Consider Q_A in the above Theorem. Since it is a primary ideal, then Rad $Q_A = P$ is a prime ideal. In this case, we say a primary submodule A of a module A is* **said to belong to a prime ideal** *P or to be a P*-**primary submodule** *of B if $P =$ Rad $Q_A = \{r \in R : r^n B \subseteq A \text{ for some } n > 0\}$.*

Definition. *Let R be a commutative ring with identity and B an R-module. A submodule C of B has a* **primary decomposition** *if $C = A_1 \cap A_2 \cap \ldots \cap A_n$, with each A_i a P_i-primary submodule of B for some prime ideal P_i of R. If no A_i contains $A_1 \cap \ldots \cap A_{i-1} \cap A_{i+1} \cap \ldots \cap A_n$ and if the ideals $P_1, \ldots, P_n$ are distinct, then the primary decomposition is said to be* **reduced**.

In the above definition a prime ideal P_i is **isolated** if it is minimal in the set $\{P_1, \ldots, P_n\}$. If P_i is not isolated it is said to be **embedded**.

Theorem 2.3.3. *Let R be a commutative ring with identity and B an R-module. If a submodule C of B has a primary decomposition, then C has a reduced primary decomposition.*

Proof. The proof is similar to that of Theorem 2.2.10. □

Theorem 2.3.4. *Let R be a commutative ring with identity and B an R-module. Let $C(\neq B)$ be a submodule of B with two reduced primary decompositions,*

$$A_1 \cap A_2 \cap \cdots \cap A_k = C = A_1^{'} \cap A_2^{'} \cap \cdots \cap A_s^{'},$$

where A_i is P_i-primary and $A_j^{'}$ is $P_j^{'}$-primary. Then $k = s$ and after reordering if it is necessary $P_i = P_i^{'}$. Furthermore if A_i and $A_i^{'}$ both are P_i-primary and P_i is an isolated prime, then $A_i = A_i^{'}$.

Proof. By changing notation if necessary we may assume that P_1 is maximal in the set $\{P_1, \dots, P_k, P_1', \dots, P_s'\}$. We want to show that $P_1 = P_j'$ for some j. Suppose on the contrary that $P_1 \neq P_j'$ for all j. Note that P_1 is maximal and also all P_i are distinct, then by contrapositive of Theorem 2.2.3 $P_1 \not\subseteq P_2 \cup \dots, P_k \cup P_1' \cup \dots \cup P_s'$. Therefore there is $r \in P_1 \setminus P_2 \cup \dots, P_k \cup P_1' \cup \dots \cup P_s'$.

We have $r^n B \subseteq A_1$ for some n since A_1 is P_1 primary. Let

$$C^* = \{x \in B : r^n x \in C\}.$$

We claim that for $k > 1$ $C^* = C$ and $C^* = A_2 \cap \dots \cap A_k$. Let $k > 1$. Suppose $a \in A_2 \cap \dots \cap A_k$, then $r^n a \in A_2 \cap \dots \cap A_k$ and also since $r^n B \subseteq A_1$, we have that $r^n a \in A_1$. Consequently, $r^n a \in A_1 \cap A_2 \cap \dots \cap A_k = C$ and so $A_2 \cap \dots \cap A_k \subseteq C^*$ and moreover, $C \subseteq C^*$.

Also, if $a \notin A_i$ for some $i \geq 2$, then $r^n a \notin A_i$ (otherwise $r^n \in P_i$, which yields to $r \in P_i$, a contradiction). As a result, $r^n a \notin C$, and so $a \notin C^*$. Therefore, $C^* \subseteq A_2 \cap \dots \cap A_k$. We conclude that $C^* = A_2 \cap \dots \cap A_k$. Furthermore, if $a \notin A_j'$ for $s \geq j \geq 1$, we must have $r^n a \notin C$ (otherwise, $r^n a \in A_j'$ and so $r^n \in P_j'$ which yields to $r \in P_j'$, a contradiction) and so $a \notin C^*$. Consequently, $C^* \subseteq A_1' \cap A_2' \cap \dots \cap A_s' = C$. Therefore, $C = C^*$.

If $k = 1$, then $C^* = B$ because A_1 is P_1-primary and $C = A_1$. With the same argument as above, we have $C^* \subseteq C$, which means $B = C$ which contradicts the assumption that $B \neq C$. If $k > 1$. Then $A_2 \cap \dots \cap A_k = C^* = C = A_1 \cap \dots \cap A_s$ and so $A_2 \cap \dots \cap A_k \subseteq A_1$ which contradict the fact that the decomposition is reduced. Therefore, we must have $P_1 = P_j'$ for some j, say $j = 1$.

We proceed by induction on k to show that $k = s$. If $k = 1$ and $s > 1$, then by similar argument we can show that $C^* = A_2' \cap \dots \cap A_s'$, and since $k = 1$ and A_1 is P_1-primary, we have $C^* = B$. Thus $B = C^* = A_2' \cap \dots \cap A_s'$. Whence $B = A_j'$ and so the second decomposition is not reduced, a contradiction. Therefore, $s = 1$.

Now assume that $k > 1$ and the theorem is true for every submodule with a reduced primary decomposition of less than k terms. Consider that $P_1 = P_1'$, and the argument above show that C^* has two primary decomposition

$$A_2 \cap \dots \cap A_k = C^* = A_2' \cap \dots \cap A_k'.$$

By induction hypothesis $k = s$ and after reordering $P_i = P_i'$ for every $i \geq 2$.

Suppose A_i and A_i' are P_i-primary and P_i is an isolated prime. For convenience of notation assume $i = 1$. The prime ideal P_1 is isolated therefore for every $j \geq 2$ there is an element $r_j \in P_j \setminus P_1$, and so $t = r_2 \dots r_k \in P_j$ for $j \geq 2$ but $t \notin P_1$. Consequently, for every $j \geq 2$, there is a positive integer n_j such that $t^{n_j} B \subseteq A_j$. Similarly, for each $j \geq 2$ there is a positive integer m_j such that $t^{m_j} B \subseteq A_j'$. Pick the maximum of all n_j and m_j, call it n. Then $t^n B \subseteq A_j$ and $t^n B \subseteq A_j'$. Same as above let $C = A_1 \cap \dots \cap A_k$. Define $D = \{x \in B : t^n x \in C\}$. To proof that $A_1 = A_1'$ we shall show that $A_1 = D = A_1'$. If $x \in A_1$, then since for every $j \geq 2$, $t^n B \subseteq A_j$, we have that $t^n x \in A_1 \cap \dots \cap A_k = C$. Therefore,

$x \in D$, and $A_1 \subseteq D$. Now, let $x \in D$. However, $t^n x \in C \subseteq A_1$. If $x \notin A_1$, by the fact that A_1 is P_1-primary, there is a positive integer q such that $t^{nq} B \subseteq A_1$, which means $t^{nq} \in P_1$, a contradiction. Therefore, $x \in A_1$ and so $A_1 = D$. An identical argument also shows that $A_1^{'} = D$. $\square$

Now we give a partial answer to the question: which modules (ideals) have primary decompositions?

Theorem 2.3.5. *Let R be a commutative ring with identity and B a Noetherian R-module. Then every submodule $A(\neq B)$ has a reduced primary decomposition.*

Proof. Let
$$S = \{A \subset B : A \ \text{ not have a primary decomposition}\}.$$
Our goal is to show that $S = \emptyset$. If S is not empty as B is Noetherian , S must have a maximal element, say C. Since C is in S, it is not primary, and so there are $r \in R$ and $b \in B \setminus C$ such that $rb \in C$ but $r^n B \nsubseteq C$ for all $n > 0$.

Let $B_n = \{x \in B : r^n x \in C\}$. Each B_n is a submodule and we have
$$B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots$$
Since B is Noetherian, there is a positive integer k such that $B_k = B_i$ for all $i \geq k$. Define
$$D = \{x \in B : x = r^k y + c \text{ for some } \ y \in B, c \in C\}.$$

We want to show that
$$C = B_k \cap D \quad \text{ and } \quad B_k, D \notin S$$
which implies that C has a primary decomposition, a contradiction. Clearly $C \subseteq B_k \cap D$. If $x \in B_k \cap D$, then $x = r^k y + c$ and $r^k x \in C$, and so
$$r^{2k} y = r^k (r^k y) = r^k (x - c) = r^k x - r^k c \in C \Rightarrow y \in B_{2k} = B_k.$$
Consequently, $r^k y \in C$ and hence $x = r^k y + c \in C$. Therefore, $B_k \cap D \subseteq C$, whence $B_k \cap D = C$. Also, since $b \in B \setminus C$ and $r^k B \nsubseteq C$, and also if $D = B$, then $B_k = D \cap B_k = C$, we have $C \neq B_k \neq B$ and $C \neq D \neq B$. Thus by maximality of C both D, B_k are not in S, and so they have a primary decomposition, which yield to that C has a primary decomposition. Moreover, by one of the previous theorems every module with a primary decomposition has a reduced primary decomposition. $\square$

Corollary 2.3.6. *every submodule $A(\neq B)$ of a finitely generated module B over a commutative Noetherian ring R and every ideal $(\neq R)$ of R has a reduced primary decomposition.*

Proof. It follows from past results, find them. $\square$

2.4 Noetherian Rings and Modules

A rather strong form of the Krull Intersection Theorem is proved. Nakayama's Lemma and several of its interesting consequences are presented. In the second part of this section, which does not depend on the first part, we prove that if R is a commutative Noetherian ring with identity, then so are the polynomial ring $R[x_1, \ldots, x_n]$ and the power series ring $R[[x_1]]$. With few exceptions all rings are commutative with identity.

Proposition 2.4.1. *(I. S. Cohen) A commutative ring R with identity is Noetherian if and only if every prime ideal of R is finitely generated.*

Proof. Let S be the set of all ideals that are not finitely generated. By Zorn's lemma if S is not empty, then it has a maximal element P. By Proposition 2.2.4, P is prime and so it is finitely generate by hypothesis. Thus $S = \emptyset$. □

Definition. *If B is a module over a commutative ring R, then it is easy to see that $\mathrm{Ann}_R(B) = \{r \in R : rb = 0 \ \forall \ b \in B\}$ is an ideal of R.The ideal $\mathrm{Ann}_R(B)$ is called the* **annihilator** *of B in R. When there is no ambiguity that the module is over R, we omit R in the notation for annihilator.*

Lemma 2.4.2. *Let B be a finitely generated module and $\{b_1, \ldots, b_n\}$ is a set of generators for B. Then*

$$\mathrm{Ann}(B) = \mathrm{Ann}(Rb_1) \cap \cdots \cap \mathrm{Ann}(Rb_n).$$

Theorem 2.4.3. *Let B be a finitely generated module over a commutative ring R with identity. Then B is Noetherian (Artinian) if and only if $R/\mathrm{Ann}(B)$ is a Noetherian [resp. Artinian] ring.*

Proof. Let B be generated by $\{b_1, \ldots, b_n\}$. Then

$$\Theta : R/\mathrm{Ann}(B) \to R/\mathrm{Ann}(Rb_1) \times \cdots \times R/\mathrm{Ann}(Rb_n)$$

defined by

$$r + \mathrm{Ann}(B) \mapsto (r + \mathrm{Ann}(Rb_1), \cdots, r + \mathrm{Ann}(Rb_n))$$

is an injection of modules. Also, it is easy to check that $R/\mathrm{Ann}(Rb_1) \cong Rb_1$, and so

$$R/\mathrm{Ann}(Rb_1) \times \cdots \times R/\mathrm{Ann}(Rb_n) \cong Rb_1 \oplus \cdots \oplus Rb_n.$$

Consider that each Rb_i is a submodule of B and so it is Noetherian. Therefore, $R/\mathrm{Ann}(B)$ injects into a direct sum of Noetherian modules and so it is a Noetherian module.

Conversely, if $R/\mathrm{Ann}(B)$ is Noetherian, then B is a finitely generated $R/\mathrm{Ann}(B)$ module, and so it is Noetherian over $R/\mathrm{Ann}(B)$. If B is not Noetherian over R, then it has a non-stable ascending chain of R-submodules, which can be seen as a non-stable ascending chain of $R/\mathrm{Ann}(B)$ submodules, a contradiction. □

Exercise. Let I be any ideal in a ring with identity and B an R module, then

$$IB = \{\sum_{i=1}^{n} r_i b_i : r_i \in I; b_i \in B, n \in \mathbb{N}^*$$

is a submodule of B.

Lemma 2.4.4. *Let P be a prime ideal in a commutative ring with identity. If C is a P-primary submodule of the Notherian R-module A, then there exists a positive integer m such that $P^m A \subseteq C$.*

Proof. Consider that A is a $R/\text{Ann}(A)$-module and since C is P-primary, if $rA = 0$, then $r \in P$, consequently $\text{Ann}(A) \subseteq P$. Let $\overline{R}$ and $\overline{P}$ be $R/\text{Ann}(A)$ and $P/\text{Ann}(A)$, respectively. We claim that C is $\overline{P}$-primary submodule of A as a $\overline{R}$-module. To prove the claim assume that $\overline{r}a \in C$ and $a \in A \setminus C$. Then $ra \in C$, and since C is P-primary, we have $r^n A \subseteq C$ for some positive integer n. Therefore, $\overline{r}^n A \subseteq C$, and we can conclude that C is $\overline{P}$-primary.

Consider that since $\overline{P}$ is in a Noetherian ring it is finitely generated. Let $\{\overline{p_1}, \ldots, \overline{p_k}\}$ be a set of generators for $\overline{P}$. So for each $\overline{p_i}$ there is a n_i such that $\overline{p_i^n} A \subseteq C$. Consequently, $p_i^n A \subseteq C$. Therefore, if m is the largest amongst n_i's, then $P^m A \subseteq C$.

□

Theorem 2.4.5. *(Krull Intersection Theorem) Let R be a commutative with identity, I an ideal of R and A a Noetherian R-module. If $B = \cap_{n=1}^{\infty} I^n A$, then $IB = B$.*

Proof. If $IB = A$, then since $B \subseteq A$, we have $A = IB \subseteq B \subseteq A$, and so $IB = A = B$. Now, we may assume that $A \neq IB$. Then by Theorem 2.3.3, IB has a primary decomposition:

$$IB = A_1 \cap \ldots \cap A_s,$$

where each A_i is P_i-primary. Consider that $IB \subseteq B$, so if we show that $B \subseteq A_i$ for all i, then $IB = B$. Let i be fixed. Suppose that $I \subseteq P_i$. Then by previous lemma there is a positive integer m such that $P_i^m A \subseteq A_i$. Therefore,

$$B = \cap I^n A \subseteq I^m A \subseteq P^m A \subseteq A_i.$$

If $I \not\subseteq P_i$, then there is an element $r \in I \setminus P_i$. If $B \not\subseteq A_i$, then there is an element $b \in B \setminus A_i$. Note that $rb \in IB \subseteq A_i$, and $b \notin A_i$, thus there is a positive integer n such that $r^n A \subseteq A_i$. Consequently, $r \in P_i$ since A_i is P_i-primary, a contradiction.

□

Lemma 2.4.6. *(Nakayama) If J is an ideal in a commutative ring R with identity, then the following conditions are equivalent.*

(i) J is contained in every maximal ideal of R;

(ii) $1_R - j$ is a unit for every$j \in J$;

(iii) If A is a finitely generated R-module such that $JA = A$, then $A = 0$;

(iv) If B is a submodule of a finitely generated R-module A such that $A = JA + B$, then $A = B$.

Proof. $(i) \Rightarrow (ii)$ if $(1-j)$ is not a unit, then the ideal $\langle 1-j \rangle$ must be a subset of a maximal ideal M, and since both $1-j$ and j are in M, then $M = R$, a contradiction.
$(ii) \Rightarrow (iii)$ Since A is finitely generated and $A \neq 0$, then we have a minimal set of generators $\{a_1, \ldots, a_n\}$ for A, and so we must have $a_1 \neq 0$. Consider that $JA = A$ whence $a_1 = j_1a_1 + \ldots + j_na_n$ for some $j_i \in J$. Then we have $(1-j_1)a_1 = j_2a_2 + \ldots + j_na_n$. By hypothesis $(1-j_1)$ is invertible, thus $a_1 = (1-j_1)^{-1}(j_2a_2 + \ldots + j_na_n)$. As a result, if $n = 1$, then $a_1 = 0$, and if $n > 1$, then the set $\{a_1, \ldots, a_n\}$ is not a minimal set of generators. Therefore, any case yields a contradiction.
$(iii) \Rightarrow (iv)$ Verify that $J(A/B) = A/B$, thus $A/B = 0$ and so $A = B$.
$(iv) \Rightarrow (i)$ Consider that for any maximal ideal M, it follows that $JR + M = R$ or $JR + M = M$. In the former case by (iv) $R = M$ which is not possible, and in the latter case we have that $JR \subseteq M$. □

We now give several application of Nakayama's Lemma.

Proposition 2.4.7. *Let J be an ideal in a commutative ring R with identity. Then J is contained in every maximal ideal of R if and only if for every for every Noetherian R-module A, $\cap_{n=1}^{\infty} J^n A = 0$.*

Proof. $(\Rightarrow)$ If $B = \cap J^n A$, then by Krull intersection theorem $JB = B$. Consider that B is a submodule of A so it is Noetherian, and By Nakayama's lemma, we have $B = 0$.
$(\Leftarrow)$ We may assume that $R \neq 0$. If M is any maximal idela of R, then R/M is an R-module without any nontrivial submodule. Therefore, $A = R/M$ is a Noetherian module, and also $JA = A$ or $JA = 0$. If $JA = A$, then $J^n A = A$, and consequently, $\cap J^n A = A$, but $A \neq 0$. So we must have $JA = 0$, which means $JR = J \subseteq M$ □

Corollary 2.4.8. *If R is a Noetherian local ringwith maximal ideal M, then $\cap M^n = 0$.*

Proof. In the above lemma, if we let $J = M$ and $A = R$, then $\cap M^n = 0$. □

Theorem 2.4.9. *(Hilbert Basis Theorem) If R is a commutative Noetherian ring with identity, then so is $R[x_1, \ldots, x_n]$.*

Theorem 2.4.10. *If R is a commutative Noetherian ring with identity, then so is $R[[x_1, \ldots, x_n]]$.*

2.5 Dedekind Domains

The class of Dedekind domains lies between the class of principal ideal domains and the class of Noetherian integral domains.

Definition. *A* **Dedekind** *domain is an integral domain R in which every ideal ($\neq R$) is the product of a finite number of prime ideals. As an example of Dedekind domains we have principal ideal domains.*

Definition. *Let R be an integral domain with quotient field K. A* **fractional ideal** *of R is a nonzero R-submodule I of K such that $aI \subseteq R$ for some nonzero $a \in R$.*

Example 2.5.1. *Consider $\mathbb{Z}$. Then it's quotient field is Q. Every ideal $a\mathbb{Z}$ when $a \neq 0$ is a nonzero $\mathbb{Z}$-submodule of $\mathbb{Q}$ such that $1(a\mathbb{Z}) \subseteq \mathbb{Z}$. So any ideal of $\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$.*

Example 2.5.2. *Let R be an integral domain and K its quotient field. Any finitely generated R-submodule I of K is a fractional ideal of R. Let $I = Ra_1 + \ldots + Ra_k$. Since each $a_i \in K$, they are in the form of c_i/d_i for some c_i and nonzero d_i of R. Consider that $d_1d_2 \ldots d_k \in R$, and so each element of K can be written as $r_1a_1 + \ldots + r_ka_k$ such that $r_i \in R$ for all i. Thus, $d_1d_2 \ldots d_k(r_1a_1 + \ldots + r_ka_k) \in R$.*

Theorem 2.5.3. *If R is an integral domain with quotient field K, the the set of all fractional ideals of R forms a commutative monoid, with identity R and multiplication given by*

$$IJ = \{\sum_{i=1}^{n} a_ib_i : a_i \in I; b_i \in J; n \in \mathbb{N}^*\}.$$

Definition. *A fractional ideal I of an integral domain R is said to be invertible if it is invertible in the monoid of all fractional ideals, i.e., if there is an fractional ideal J such that $IJ = R$. As an example every non-zero principal ideal in an integral domain is invertible since $RaR(1/a) = R$.*

Lemma 2.5.4. *Let $I_1, \ldots, I_n$ be ideals in an integral domain R.*

1. *The ideal $I_1I_2 \ldots I_n$ is invertible if and only if each I_j is invertible.*

2. *If $P_1 \ldots P_m = I = Q_1 \ldots Q_n$ where each P_i and Q_i are prime ideals in R and every P_i isinvertible, then $m = n$ and after reordering the indexing if necessary $P_i = Q_i$ for $i = 1, \ldots, n$.*

Proof. (1) It is straightforward. (2) We proceed the proof by induction. If $m = 1$, then $P_1 = I = Q_1 \ldots Q_n$, and consequently, $Q_i \subseteq P_1$ for some i, let say $i = 1$. Moreover, $P_1 = I = Q_1 \ldots Q_n \subseteq Q_1$. Thus, $P_1 = Q_1$. Therefore, $P_1 = P_1Q_2 \ldots Q_n$, and since P_1 has an inverse, say P_1', then $P_1'P_1 = P_1'P_1Q_2 \ldots Q_n$. As a result, $R = Q_2 \ldots Q_n$ which means each Q_i equals to R, a contradiction unless $n = 1$.

Now assume that the theorem is true for all positive integers less than m. Assume that P_1 is a minimal element of the set $\{P_1, \ldots, P_m\}$. Then as $P_1 \supseteq P_1 \ldots P_m = I = Q_1 \ldots Q_n$ and P_1 is prime, there is an i such that $Q_i \subseteq P_1$. Without loss of generality assume that $i = 1$. Now, $P_1 \ldots P_m = I = Q_1 \ldots Q_n \subseteq Q_1$, there is j such that $P_j \subseteq Q_1$. Therefore, $P_j \subseteq Q_1 \subseteq P_1$, which contradiction unless $P_1 = Q_1$. Now, $P_1 P_2 \ldots P_m = I = P_1 Q_2 \ldots Q_n \subseteq Q_1$. Since P_1 has an inverse, say P_1', then $P_1' P_1 P_2 \ldots P_m = P_1^{`} P_1 Q_2 \ldots Q_n$. Therefore, $P_2 \ldots P_m = Q_2 \ldots Q_n$, and the result follows by induction. □

Theorem 2.5.5. *If R is a Dedekind domain, then every nonzero prime ideal of R is invertible and maximal.*

Proof. The proof follows from the following two lemmas. □

Lemma 2.5.6. *If R is a Dedekind domain, then every nonzero invertible prime ideal of R is maximal.*

Proof. In order to show that P is a maximal ideal, we must show that the ideal $P + Ra$ for $a \in R \setminus P$ is R. Suppose $P + Ra \neq R$, then since R is a Dedekind domain, every ideal can be written as an intersection of prime ideals, so there are prime ideals $P_1, \ldots, P_m$ and $Q_1, \ldots, Q_n$ such that

$$P + Ra = P_1 \ldots P_m \quad \text{and} \quad P + Ra^2 = Q_1 \ldots Q_n.$$

Let $\pi : R \to R/P$ be the canonical epimorphism. Then it is clear that both $\pi(P + Ra)$ and $\pi(P + Ra^2)$ are ideals of R/P and they are the same as ideals $\langle \pi(a) \rangle$ and $\langle \pi(a^2) \rangle$. Therefore, in R/P we can write

$$\langle \pi(a) \rangle = \pi(P_1) \ldots \pi(P_m) \quad \text{and} \quad \langle \pi(a^2) \rangle = \pi(Q_1) \ldots \pi(Q_n).$$

Consider that since R/P is an integral domain, every nonzero principal ideal is invertible ($Rx + R(1/x) = R$). Therefore, $\langle \pi(a) \rangle$ and $\langle \pi(a^2) \rangle$ are invertible and so each $\pi(P_i)$ and $\pi(Q_j)$ is invertible. Since

$$\pi(Q_1) \ldots \pi(Q_n) = \langle \pi(a^2) \rangle = \langle \pi(a) \rangle^2 = \pi(P_1)^2 \ldots \pi(P_m)^2.$$

We conclude that $n = 2m$ and after reindexing we can say $\pi(P_i) = \pi(Q_{2i}) = \pi(Q_{2i-1})$ for $i = 1, \ldots, m$. Dor each $i = 1, \ldots, m$,

$$P_i = \pi^{-1}\pi(P_i) = \pi^{-1}\pi(Q_{2i}) = Q_{2i}$$

and similarly $P_i = Q_{2i-1}$ for all $i = 1, 2, \ldots, m$. Consequently, $P^2 + Ra = (P + Ra)^2$ and $P \subseteq P + Ra^2 = (P + Ra)^2 \subseteq P^2 + Ra$. For every element $b \in P$, there are $c \in P^2$ and $r \in R$ such that $b = c + ra$ since $P \subseteq P^2 + Ra$. Note that $a \notin P$, but $ra = b - c \in P$, thus $r \in P$. Therefore

$$P \subseteq P^2 + Pa \subseteq P$$

and so $P^2 + Pa = P$ which means $P = P(P + Ra)$. Since P is invertible,

$$R = P^{-1}P = P^{-1}P(P + Ra) = R(P + Ra) = P + Ra,$$

a contradiction. Therefore, P must be a maximal ideal. $\square$

Lemma 2.5.7. *If R is a Dedekind domain, then every nonzero prime ideal of R is invertible.*

Proof. Let c be a nonzero element of P, then there are prime ideals $P_1, \ldots, P_n$ such that

$$\langle c \rangle = P_1 \ldots P_n.$$

Since $\langle c \rangle \subseteq P$, $P_1 \ldots P_n \subseteq P$, and so there is a P_i such that $P_i \subseteq P$. Since $\langle c \rangle$ is invertible, so is P_i. Thus by the first part since P_i is invertible and prime, it is a maximal ideal and therefore it must be equal to P which means that P is invertible. $\square$

Corollary 2.5.8. *The class of Dedekind domains sits inside the class of Noetherian domains. The reason for this is that in $F[x_1, x_2]$ which is a Noetherian ring there are invertible prime ideals $\langle x_1 \rangle$ and $\langle x_2 \rangle$ that are not maximal. Moreover, if R is an Dedekind domain, it must be Noetherian because if $I \subseteq J$ in a Dedekind domain then $J = P_1 \ldots P_k$ and $I = P_1 \ldots P_k P_{k+1} \ldots P_n$.*

Definition. *A* **discrete valuation ring** *is a principal ideal domain that has exactly one nonzero prime ideal.*

Definition.

1. *Let S be an extension ring of R and $s \in S$. If there exists a monic polynomial $f(x) \in R[x]$ such that s is a root of f, then s said to be* **integral** *over R. If every element of S is integral over R, S is said to be an* **integral extension** *of R.*

2. *If S is an extension of R, then $\hat{R}$ which is the set of all elements of S that are integral over R, is called integral closure of R in S. If $\hat{R} = R$, then R is said to be* **integrally closed in S.**

3. *A module P over a ring R is said to be* **projective** *of given any diagram if R-module homomorphisms*

$$\begin{tikzcd} & P \arrow[d] & \\ A \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

with bottom row exact, there exists an R-module homomorphism $h : P \to A$ such that

$$\begin{tikzcd} & P \arrow[dl] \arrow[d] & \\ A \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

is commutative.

Definition. *Let R be a commutative ring with identity and P a prime ideal of R. Then $S = R - P$ is a multiplicative subset of R. The ring of quotients $S^{-1}R = \{a/b : a \in R, b \in S\}$ is called the localization of R at P and is denoted R_P.*

Theorem 2.5.9. *The following conditions on an integral domain R are equivalent.*

(i) *R is a Dedekind domain;*

(ii) *every proper ideal in R is uniquely a product of a finite number of prime ideals;*

(iii) *every nonzero ideal in R is invertible;*

(iv) *every fractional ideal of R is invertible;*

(v) *the set of all fractional ideals of R is a group under multiplication;*

(vi) *every ideal in R is projective;*

(vii) *every fractional ideal of R is projective.*

(viii) *R is Noetherian, integrally closed and every nonzero prime ideal is maximal.*

(ix) *R is Noetherian and for every nonzero ideal P of R, the localization R_P of R at P is a discrete valuation ring.*

2.6 The Hilbert Nullstellensatz

In this section we prove the Nullstellensatz (Zero Theorem) of Hilbert.

Classical algebraic geometry studies the simultaneous solutions of system of polynomial equations

$$f(x_1, \dots, x_n) = 0 \quad (f \in S)$$

where K is a field and $S \subseteq K[x_1, \dots, x_n]$. Let F is an algebraically closed extension field of K.

Definition. *Let S and K be as the above. A zero of S in F^n is a tuple $(a_1, \dots, a_n) \in F^n$ such that for each $f \in S$, $f(a_1, \dots, a_n) = 0$. The set of all zeros of S is called the* **affine K-variety** *(or* **algebraic set***) in F^n defined by S and is denoted by $V(S)$. Thus,*

$$V(S) = \{(a_1, \dots, a_n) \in F^n : f(a_1, \dots, a_n) = 0 \text{ for all } f \in S\}.$$

Remark.

1. If I is an ideal generated by S, then $V(I) = V(S)$.

2. The assignments $S \mapsto V(S)$ defines a function form the set of all subsets of $K[x_1, \dots, x_n]$ to the set of all subsets of F^n.

3. For a subset Y of F^n define

$$J(Y) = \{f \in K[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in Y\}.$$

Define a function from F^n to $K[x_1, \dots, x_n]$ by the assignments $Y \mapsto J(Y)$.

What are the relations and properties of the correspondence J and V.

Theorem 2.6.1. *Let F be an algebraically closed field of K and let S, T be subsets of $K[x_1, \dots, x_n]$ and X, Y subsets of F^n. Then*

(i) $V(K[x_1, \dots, x_n]) = \emptyset; J(F^n) = \emptyset; J(\emptyset) = K[x_1, \dots, x_n]$;

(ii) $S \subseteq T \Rightarrow V(T) \subseteq V(S)$ *and* $X \subseteq Y \Rightarrow J(Y) \subseteq J(X)$;

(iii) $S \subseteq J(V(S))$ *and* $Y \subseteq V(J(Y))$;

(iv) $V(S) = V(J(V(S)))$ *and* $J(Y) = J(V(J(Y)))$.

Definition. *Let F be an extension field of K. A* **transcendence base (or basis)** *of F over K is a subset S of F which is algebraically independent over K and is maximal (with respect to set-theoretic inclusion) in the set of all algebraically independent subsets of F.*

Definition. *Let F be an extension field of K. The* **transcendence degree** *of F over K is the cardinal number $|S|$, where S is any transcendence base of F over K.*

Theorem 2.6.2. *(Lying-over theorem) Let S be an integral extension of R.*

1. P is a prime ideal of R, then there is a prime ideal Q in S such that $Q \cap R = P$.

2. In (1), P is maximal if and only if Q is maximal.

Theorem 2.6.3. *(Noether Normalization Lemma) Let R be an integral domain which is a finitely generated extension ring of a field K (that is, $R = K[X]$ for some $X \subseteq R$) and let r be the transcendence degree over K of the quotient field F of R. Then there exists an algebraically independent subset $\{t_1, \dots, t_r\}$ of R such that R is integral over $K[t_1, \dots, t_r]$.*

Lemma 2.6.4. *If F is an algebraiclay closed extension field of a field K and I is a proper ideal of $K[x_1, \dots, x_n]$, then the affine variety $V(I)$ define by I in F^n is nonempty.*

Sketch of the proof. In the proof of this lemma, for any $f \in P$, where P is a prime ideal containing I, we have $f(\phi(x_1), \dots, \phi(x_n)) = 0$ for some function ϕ where it will be defined in the next paragraph. So $(\phi(x_1), \dots, \phi(x_n))$ is a zero for all polynomials in I, and so $V(I) \neq \emptyset$.

What is ϕ? Let $R = K[x_1, \dots, x_n]/P$. The function ϕ is the composition of the following morphims

$$K[x_1, \dots, x_n] \xrightarrow{\pi} R \xrightarrow{\tau} \tau(R) \xrightarrow{\sigma} F.$$

- π: The morphism $\pi : K[x_1, \dots, x_n] \to R$ is the canonical morphism.

- τ: Let $\pi(x_i) = u_i$ and consider that $\pi(K)$ is a field, so $R = \pi(K)[u_1, \dots, u_n]$. Consider that R is a finitely generated extension of the field $\pi(K)$, then by Noether Normalization Lemma, there exists a subset $\{t_1, \dots, t_r\}$ of R such that it is algebraically independent over $\pi(K)$ and R is integral over $S = \pi(K)[t_1, \dots, t_r]$. Now let M be the ideal generated by $\{t_1, \dots, t_r\}$ in S, then $\pi(K) \to S/M$ is an isomorphism, so M is maximal in S. By lying-over theorem there is a maximal ideal N of R such that $N \cap S = M$. Let $\tau : R \to R/N$ be the canonical epimorphism. Note that $\tau(R) = R/N$ is a field.

- σ: By the second isomorphism problem we have

$$\begin{array}{ccccccccccc} K & \cong & \pi(K) & \cong & S/M & = & S/N \cap S & \cong & (S+N)/N & = & \tau(S) \\ a & \mapsto & \pi(a) & \mapsto & \pi(a) + M & = & \pi(a) + M & \mapsto & \pi(a) + N & = & \tau(\pi(a)). \end{array}$$

  Thus, the isomorphism from K to $\tau(S)$ can be extended to an isomorphim between their algebraic closures, so $\overline{K} \cong \overline{\tau(S)}$. Restricting the inverse of this isomorphism yields a monomorphism $\sigma : \tau(R) \to \overline{K} \subseteq F$.

Now if $f(x_1, \dots, x_n) \in P$, then $f(\phi(x_1), \dots, \phi(x_n)) = \phi(f(x_1, \dots, x_n)) = 0$.

Theorem 2.6.5. *(Hilbert Nullstellensatz) Let F be an algebraically closed extension field of a field K and I a proper ideal of $K[x_1, \dots, x_n]$. Let $V(I) = \{(a_1, \dots, a_n) \in F^n : g(a_1, \dots, a_n) = 0 \ \forall g \in I\}$. Then*

$$Rad\ I = J(V(I)) = \{f \in K[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \ \forall (a_1, \dots, a_n) \in V(I)\}.$$

In other words, $f(a_1, \dots, a_n) = 0$ for every zero $(a_1, \dots, a_n)$ of I in F^n if and only if $f^m \in I$ for some $m \geq 1$.

Proof. Let $f \in Rad\ I$, then $f^m \in I$ for some positive integer m. Consider that $JV(I)$ is the set of all polynomials that has the roots of all polynomials of I as a subset of its roots. So if $(a_1, \dots, a_n)$ is the root of all polynomials in I, then it is a root of f^m, and therefore, $0 = f^m(a_1, \dots, a_n) = (f(a_1, \dots, a_n))^m$. Since F is a field we have $f(a_1, \dots, a_n) = 0$, which means $f \in JV(I)$. Thus $Rad\ I \subseteq JV(I)$.

Conversely, suppose that $f \in JV(I)$. We may assume that $f \neq 0$ since $0 \in Rad\ I$. Consider the ring $K[x_1, \dots, x_n]$ as a subring of $k[x_1, \dots, x_n, y]$ in $n+1$ indeterminates over K. Let

$$L = \langle f', yf - 1_F : f' \in I \rangle.$$

If $(a_1, \dots, a_n, b)$ is a zero of L in F^{n+1}, then clearly $(a_1, \dots, a_n)$ is a root of I in F^n. But

$$(yf - 1_F)(a_1, \dots, a_n, b) = bf(a_1, \dots, a_n) - 1_F = -1_F$$

for all zeros $(a_1, \ldots, a_n)$ of I in F^n. Therefore, L has no zeros in F^{n+1}; that is, $V(L)$ is empty. Consequently, $L = K[x_1, \ldots, x_n, y]$ and so $1_F \in L$. Thus

$$1_F = \sum_{i=1}^{t-1} g_i f_i' + g_t(yf - 1_F),$$

where $f_i' \in I$ and $g_i \in K[x_1, \ldots, x_n, y]$. Define an evaluation homomorphism as follows

$$\begin{array}{ccc} K[x_1, \ldots, x_n, y] & \to & K(x_1, \ldots, x_n) \\ x_i & \mapsto & x_i \\ y & \mapsto & 1_K/f(x_1, \ldots, x_n). \end{array}$$

Then in the field $K(x_1, \ldots, x_n)$

$$1_F = \sum_{i=1}^{t-1} g_i(x_1, \ldots, x_n, f^{-1}) f_i'(x_1, \ldots, x_n).$$

Let m be a positive integer larger than the degree of g_i in y for every i $(1 \leq i \leq t-1)$. Then for each i, $f^m(x_1, \ldots, x_n) g_i(x_1, \ldots, x_n, f^{-1})$ lies in $K[x_1, \ldots, x_n]$, and thus

$$f^m = f^m 1_F = \sum_{i=1}^{t-1} f^m(x_1, \ldots, x_n) g_i(x_1, \ldots, x_n, f^{-1}) f_i'(x_1, \ldots, x_n) \in I.$$

Therefore, $f \in Rad\ I$ and hence $JV(I) \subseteq Rad\ I$. $\square$

We close this section with an informal attempt to establish the connection between geometry and algebra. Let K be a field. Every polynomial $f \in K[x_1, \ldots, x_n]$ determines a function $F^n \to F$ by substitution: $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$. If $V = V(I)$ is an affine variety contained in F^n, the restriction of f on V is called a **regular function** on V. The set of all regular functions on V, denoted $\Gamma(V)$, forms a ring which is isomorphic to

$$K[x_1, \ldots, x_n]/J(V(I)).$$

This ring is called **coordinate ring** of V.

Lemma 2.6.6. *1. A ring is the coordinate ring of some affine variety if and only if it is a finitely generated algebra over K with no nonzero nilpotent element.*

2. There is a one-to-one correspondence between affine varieties and a class of commutative rings.

3. The affine varieties form a category as do the class of commutative rings in (2), and this correspondence is an equivalence of categories. Thus the statements about affine varieties are equivalent to certain statements of commutative algebra.

Chapter 3

The structure of rings

Complete structure theorems are available for certain classes of rings. We intuitively describe the basic method for determining such a class of rings. We single out a "undesirable' 'property P that satisfies certain conditions, in particular, that every ring has an ideal which is maximal with respect to having property P. This ideal is called P-radical of the ring. Then we attempt to find structure theorems for the class of rings with zero P-radical.

3.1 Simple and primitive rings

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

Example 3.1.1.

1. *Every division ring is simple and a simple D-module.*
2. *Let D be a division ring and let $R = Mat_n(D)$ $(n > 1)$. For each k $(1 \leq k \leq n)$,*

$$I_k = \{(a_{ij}) \in R : a_{ij} = 0 \textit{ for } j \neq k\}$$

   is a simple left R-module.

3. *The preceding example shows that $M_n(D)$ is not a simple left $M_n(D)$-module, however it is a simple ring. Consider that $M_n(D) \cong End_D(V, V)$ where V is an n-dimensional D-module. Therefore, $End_D(V, V)$ is a simple ring.*
4. *A left ideal I of a ring R is said to be a* **minimal left ideal** *if $I \neq 0$ and for every left ideal J such that $0 \subseteq J \subseteq I$, either $J = 0$ or $J = I$. A left ideal I of R such that $RI \neq 0$ is a simple left R-module if and only if I is a minimal left ideal.*

Remark 3.1.2. *For many algebraic objects like groups, rings, and modules, a simple object C can be defined as an object such that any non-zero morphism from C to another object is injective.*

Definition. *A left ideal I in a ring R is* **regular** *(or* **modular***) if there exists $e \in R$ such that $r - re \in I$ for every $r \in R$. Similarly, a right ideal J is* **regular** *if there exists $e \in R$ such that $r - er \in J$ for every $r \in R$.*

Remark 3.1.3. *Every left ideal in a ring R with identity is regular, take $e = 1$.*

Theorem 3.1.4. *A left module A over a ring R is simple if and only if A is isomorphic to R/M for some regular maximal left ideal M.*

Proof. Suppose that A is simple and $0 \neq a \in A$. Then the map $R \to Ra = A$ defined by $r \to ra$ is a homomorphism whose kernel is a maximal ideal. We now show that this maximal ideal is a regular left ideal. Note that $a \in A$, so there is an element $e \in R$ such that $ea = a$. For every $r \in R$, consider that $(r - re)a = ra - rea = r - r = 0$, and so $r - re \in M$, and M is a regular left ideal.

Conversely, let M be a regular left module, so there is an element e such that for every $r \in R$, $r - re \in M$. we only need to show that $R(R/M) \neq 0$. If this is not the case, then for every element $r \in R$ such that $r(e + M) \in M$. Thus $re \in M$ and since $r - re \in M$, it follows that $r \in M$. Therefore, $M = R$, a contradiction. □

Theorem 3.1.5. *The left annihilator of a subset B of an R-module A,*

$$Ann(B) = \{r \in R : rb = 0 \ \forall b \in B\}$$

is a left ideal of R and if B is a submodule of A, then $Ann(B)$ is an ideal of R.

Definition. *A (left) module A is* **faithful** *if its (left) annihilator is 0. A ring R is* **(left) primitive** *if there exists a simple faithful left R-module.*

Proposition 3.1.6. *A simple ring R with identity is primitive.*

Proof. Consider that R contains a maximal left ideal M and since R has identity, thus M is regular and so R/M is a simple R-module by the above theorem. Also since R has identity, the annihilator of R/M is zero. Thus we have that R is primitive. □

Proposition 3.1.7. *A commutative ring R is primitive if and only if R is a field.*

Proof. By the previous proposition we have that if R is a field, the it is primitive. Conversely, if R is primitive and commutative, then there is a simple faithful R-module A. By Theorem 3.1.4 there is a maximal ideal I that is regular and $A \cong R/I$. We have that $I \subset Ann(R/I) = Ann(A) = 0$. Therefore, $I = 0$. Since I is regular, there is an element $e \in R$ such that for every $r \in R$, we have $r - re = 0$, and so $r = re$. Since R is commutative, we can conclude that R has an identity which is e. Moreover, I is an ideal because R is commutative. Therefore, R is a commutative ring with identity that 0 is its maximal ideal. This implies that R must be a field. □

Example 3.1.8. *Not every primitive ring is a simple ring. Consider that if V is a n-dimensional vector space over a division ring D, then $End(V) \cong M_n(D)$ and so it is simple, but if we assume that V is not finite dimensional, then $End(V)$ is not simple, since the set of all element of $End(V)$ with finite dimensional images produce an ideal of $End(V)$. However, always V is a $End(V)$-module in which the scalar product define as $\theta.v = \theta(v)$. Consider that V is a simple left $End(V)$-module and it is faithful, so $End(V)$ even if V is not finite dimensional is a primitive ring.*

Definition. *Let V be a vector space over a devision ring. A subring R of the endomorphism ring $\mathrm{Hom}_D(V, V)$ is called a* **dense ring of endomorphisms** *of V (or a* **dense subring** *of $\mathrm{Hom}_D(V, V)$) if for every positive integer n, every linearly independent subset $\{u_1, \ldots, u_n\}$ of V and every arbitrary subset $\{v_1, \ldots, v_n\}$ of V, there exists $\theta \in R$ such that $\theta(u_i) = v_i (i = 1, \ldots, n)$.*

Example 3.1.9. $\mathrm{Hom}_D(V, V)$ *is always a dense subring of itself, moreover if V is finite dimensional, then the only dense subring of* $\mathrm{Hom}_D(V, V)$ *is itself.*

Theorem 3.1.10. *Let R be a dense ring of endomorphisms of a vector space V over a division ring D. Then R is left Artinian if and only if $\dim_D V$ is finite, in which case $R = \mathrm{Hom}_D(V, V)$.*

Proof. If R is Artinian and dimension of V is infinite, then there is an infinite linear independent set $\{u_1, u_2, \ldots\}$ in V. Consider that V is a $\mathrm{Hom}_D(V, V)$-module by the product

$$(\theta, v) \mapsto \theta(v),$$

and so it is also an R-module too. For each n, let

$$I_n = \mathrm{Ann}_R(\{u_1, \ldots, u_n\}).$$

In order to show that

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$$

is a non-stable chain of ideals in R, we need to accomplish that $I_n \supset I_{n+1}$. Since R is a dense ring, for the linearly independent set $\{u_1, \ldots, u_n, u_{n+1}\}$ and arbitrary subset $\{v_1, \ldots, v_n, w\}$ where each $v_i = 0$ and $w \neq 0$, there is a map $\theta \in R$ such that

$$\theta(v_i) = 0 \ \forall i \quad \theta(v_{n+1}) = w.$$

Consider that $\theta \in I_n = \mathrm{Ann}(\{u_1, \ldots, u_n\}) \setminus \mathrm{Ann}(\{u_1, \ldots, u_n, u_{n+1}\}) = I_{n+1}$. Consequently, R is not Artinian and this yields a contradiction. Therefore $\dim_D V$ is finite.

Conversely, if $\dim_D V$ is finite and $\{u_1, \ldots, u_n\}$ is a basis for V, then every transformation is determined by its action on the set $\{u_1, \ldots, u_n\}$. Since R is dense for every $f \in \mathrm{Hom}_D(V, V)$ and the set $\{\theta(u_1), \ldots, \theta(u_n)\}$, there is a map $\theta \in R$ such that $\theta(u_i) = f(u_i)$ for all i, therefore $\theta = f$ and so $f \in R$. Consequently, $R = \mathrm{Hom}_D(V, V)$. Moreover, $\mathrm{Hom}_D(V, V)$ is isomorphic to the ring of $n \times n$ matrices over D, and it is Artinian. □

Lemma 3.1.11. *(Schur) Let A be a simple module over a ring R and let B be any R-module.*

(i) Every nonzero R-module homomorphism $f : A \to B$ is a monomorphism;

(ii) every nonzero R-module homomorphism $g : B \to A$ is a epimorphism;

(iii) the endomorphism ring $D = \mathrm{Hom}_R(A, A)$ is a division ring.

Proof. (i) If $f : A \to B$ is a homomorphism of R-modules, then as $ker(f)$ is a submodule of A, we have either $ker(f) = 0$ or $ker(f) = A$. Note that f is a nonzero map, thus $ker(f) = 0$, and so f is a monomorphism.
(ii) The image of g is a submodule of A and since f is nonzero, we must have $Img(f) = A$.
(iii) It follows from (i) and (ii). □

Example 3.1.12. *If A is a simple R-module, then A is a vector space over the division ring $\mathrm{Hom}_R(A, A)$ with $f.a = f(a)$.*

Lemma 3.1.13. *Let A be a simple module over a ring R. Consider A as a vector space over the division ring $D = \mathrm{Hom}_R(A, A)$. If V is a finite dimensional D-subspace of the D-vector space A and $a \in A \setminus V$, then there exists $r \in R$ such that $ra \neq 0$ and $rV = 0$.*

Theorem 3.1.14. *(Jacobson Density Theorem) Let R be a primitive ring and A a faithful simple R-module. Consider A as a vector space over the division ring $\mathrm{Hom}_R(A, A) = D$. Then R is isomorphic to a dense ring of endomorphisms of the D-vector space A.*

Proof. Define a map

$$\begin{array}{cccc} \alpha & R & \to & \mathrm{Hom}_D(A, A) \\ & r & \mapsto & \alpha_r \end{array}$$

where $\alpha_r(a) = ra$. This map is a homomorphism and moreover, if $\alpha_r = 0$ for some $r \in R$, then $rA = 0$. Since A is faithful, we must have $r = 0$, and so α is a monomorphism and R is isomorphic to the image of α. To complete the proof it is enough to show that $Img(\alpha)$ is dense subring of $\mathrm{Hom}_D(A, A)$. Let $U = \{u_1, \ldots, u_n\}$ be a linearly independent subset of A and $\{v_1, \ldots, v_n\}$ be an arbitrary subset of A. Let

$$\widehat{U_i} = D\text{-span}\{u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n\}.$$

Then by the previous lemma, there is $r_i \in R$ such that $r_i u_i \neq 0$ and $r_i \widehat{U_i} = 0$. By reapplying the previous lemma to the D-span of $\{r_i u_i\}$ and zero subspace, there is $s_i \in R$ such that $s_i r_i u_i \neq 0$ and $s_i 0 = 0$. Thus $R r_i u_i \neq 0$ and since A is simple, we have $R r_i u_i = A$. Therefore, there is $t_i \in R$ such that $t_i r_i u_i = v_i$. Now consider the homomorphism $\alpha_{t_1 r_1 + \ldots + t_n r_n}$. Then for each i,

$$\alpha_{t_1 r_1 + \ldots + t_n r_n}(u_i) = t_i r_i u_i = v_i.$$

Consequently, the image of α is dense subring of $\mathrm{Hom}_D(A, A)$. □

Corollary 3.1.15. *If R is a primitive ring, then for some division ring D either R is isomorphic to the endomorphism ring of a finite dimensional vector space over D or for every positive integer m there is a subring R_m of R and an epimorphism of rings $R_m \to \mathrm{Hom}_D(V_m, V_m)$, where V_m is an m-dimensional vector space over D.*

Proof. In the notation of the previous theorem

$$\alpha : R \to \mathrm{Hom}_D(A, A)$$

is a monomorphism such that $R = Img(\alpha)$ is dense in $\mathrm{Hom}_D(A, A)$. Therefore, if $dim_D A$ is finite, then $Img\alpha = \mathrm{Hom}_D(A, A)$. If $dim_D A$ is infinite and $\{u_1, u_2, \dots\}$ is an infinite linearly independent set, then let V_m be the m-dimensional D-subspace of A spanned by $\{u_1, \dots, u_m\}$. Verify that $\{r \in R : rV_m \subseteq V_m\}$ is a subring of R. Consider the map

$$\begin{array}{ccc} R_m & \to & \mathrm{Hom}_D(V_m, V_m) \\ r & \mapsto & \alpha_r|V_m. \end{array}$$

Since $R \cong Img\alpha$ is dense in $\mathrm{Hom}_D(A, A)$, then for each $\tau \in \mathrm{Hom}_D(V_m, V_m)$, we have that there is an $\alpha_r \in \mathrm{Hom}_D(A, A)$ such that $\alpha_r(u_i) = \tau(u_i)$ which means $\alpha_r = \tau$. Note that $\alpha_r|V_m \subseteq V_m$, and so $r \in R_m$. Thus the map

$$\begin{array}{ccc} R_m & \to & \mathrm{Hom}_D(V_m, V_m) \\ r & \mapsto & \alpha_r|V_m. \end{array}$$

is a well-defined ring epimorphism. □

Theorem 3.1.16. *(Wedderburn-Artin) The following conditions on a left Artinian ring R are equivqlent.*

(i) R is simple.

(ii) R is primitive.

(iii) R is isomorphic to the endomorphism ring of a nonzero finite dimensional vector space V over a division ring D.

(iv) For some positive integer n, R is isomorphic to the ring of all $n \times n$ matrices over a division ring.

Proof. $(i) \Rightarrow (ii)$ Since R is left Artinian, the set of all non-zero left ideals of R has a minimal element, say J. We show that J is a faithful simple R-module and so R is primitive. We only need to show that J is faithful that is $Ann(J) = 0$. Suppose on the contrary $Ann(J) \neq 0$, then as R is simple we must have $Ann(J) = R$. Thus for every $u \in J$, $Ru = 0$. Thus $J \subseteq I = \{r \in R : Rr = 0\}$ however I is an ideal of R and since R is simple and $R^2 \neq 0$, it implies that $I = 0$, and so $J = 0$, a contradiction. Therefore, we must have $Ann(J) = 0$, and J is faithful and $RJ \neq 0$. Therefore, J is a faithful simple R-module, and so R is primitive.

$(ii) \Rightarrow (iii)$ By Jacobson Density Theorem R is isomorphic to a dense subring T of endomorphism of a vector space V over a division ring D. Since R is left Artinian, $R \cong T = \mathrm{Hom}_D(V, V)$.

$(iii) \Rightarrow (iv)$ It follows from that fact that $\mathrm{Hom}_D(V, V)$ is isomorphic to the $n \times n$ matrices over D where n is the dimension of V.

$(iv) \Rightarrow (i)$ It follows from the fact that the set of $n \times n$ matrices over D is simple. $\square$

If R is a simple left Artinian ring, then we have already showed that $R \cong M_n(D) \cong \mathrm{Hom}_D(V, V)$. We close this section by proving that if R is a simple left Artinian ring, then n, D, and dimension of V are unique.

Lemma 3.1.17. *Let V be a finite dimensional vector space over a division ring D. If A and B are simple faithful modules over the endomorphism ring $R = \mathrm{Hom}_D(V, V)$, then A and B are isomorphic of R-modules.*

Proof. Since R is an Artinian, so there is a minimal left ideal I of R. Now consider that since $Ann(A) = 0$, there is $a \in A$ such that $Ia \neq 0$, and as Ia is a left submodule of A, we must have $Ia = A$. Thus, the map $i \mapsto ia$ is a R-module isomorphism, so $I \cong A$. Similarly, we can show that $I \cong B$. Therefore, A and B are isomorphic. $\square$

Lemma 3.1.18. *Let V be a nonzero vector space over a division ring D and let R be the endomorphism ring $\mathrm{Hom}_D(V, V)$. If $g : V \to V$ is a homomorphism of additive groups such that $gr = rg$ for all $r \in R$, then there exists $d \in D$ such that $g(v) = dv$ for all $v \in V$.*

Proof. Let u be a nonzero element of V. We claim that u and $g(u)$ are linearly dependent. If $dim_D V = 1$, then u and $g(u)$ are dependent. Now assume that $dim_D V \geq 2$, and $\{u, g(u)\}$ are linearly independent. As R is dense in itself, we have an element $r \in R$ such that $r(u) = 0$ and $r(g(u)) \neq 0$ but as we have $rg = gr$, then we must have $r(g(u)) = 0$. Therefore, $\{u, g(u)\}$ are linearly dependent. So there is $d \in D$ such that $g(u) = du$. If $v \in V$, there is $s \in R$ such that $s(u) = v$. Now consider that

$$g(v) = g(s(u)) = sg(u) = s(du) = d(s(u)) = dv.$$

$\square$

Proposition 3.1.19. *For $i = 1, 2$ let V_i be a vector space of finite dimension n_i over the division ring D_i.*

1. *If there is an isomorphism of rings $\mathrm{Hom}_{D_1}(V_1, V_1) \cong \mathrm{Hom}_{D_2}(V_2, V_2)$, then $dim_{D_1} V_1 = dim_{D_2} V_2$ and D_1 is isomorphic to D_2.*

2. *If there is an isomorphism of rings $Mat_{n_1} D_1 \cong Mat_{n_2} D_2$, then $n_1 = n_2$ and D_1 is isomorphic to D_2.*

Proof. For $i = 1, 2$ consider that V_i is a faithful simple $\mathrm{Hom}_{D_i}(V_i, V_i)$-module. Let $R = \mathrm{Hom}_{D_1}(V_1, V_1)$ and let

$$\sigma : R \to \mathrm{Hom}_{D_2}(V_2, V_2)$$

be an isomorphism. Then V_2 is a faithful simple R_2-module by $rv = \sigma(r)(v)$ for $r \in R$ and $v \in V_2$. Therefore, both V_1 and V_2 are faithful simple R-modules, then by Lemma 3.1.17 there is an R-isomorphism between $\phi : V_1 \to V_2$. For each $v \in V_1$ and $f \in R$,

$$\phi(f(v)) = f\phi(v) = (\sigma(f))[\phi(v)]$$

whence

$$\phi f \phi^{-1} = \sigma(f)$$

and we can consider it as a homomorphism of additive groups $V_2 \to V_2$. For each $d \in D_i$ let $\alpha_d : V_i \to V_i$ be the homomorphism of additive groups defined by $x \mapsto dx$. For every $f \in R = \mathrm{Hom}_{D_1}(V_1, V_1)$ and every $d \in D_1$, $f\alpha_d = \alpha_d f$. Consequently,

$$[\phi\alpha_d\alpha^{-1}](\sigma f) = \phi\alpha_d\phi^{-1\phi f\phi^{-1}} = \phi\alpha_d f\phi^{-1} = \phi f\alpha_d\phi^{-1} =$$

$$\phi f\phi^{-1}\phi\alpha_d\alpha^{-1} = (\sigma f)[\phi\alpha_d\alpha^{-1}].$$

Since σ is surjective, by the previous lemma there exists $d^* \in D_2$ such that $\phi\alpha_d\alpha^{-1} = \alpha_{d^*}$. Let $\tau : D_1 \to D_2$ be the map given by $\tau(d) = d^*$. Then for every $d \in D_1$,

$$\phi\alpha_d\phi^{-1} = \alpha_{\tau(d)}.$$

Consider that if $\tau(d) = \tau(d_1)$, then $\alpha_d = \alpha_{d_1}$, then $d = d_1$ so τ is a monomorphism of rings. Reversing the role of D_1 and D_2 and replacing ϕ and σ by ϕ^{-1} and σ^{-1} respectively, the preceding argument yields that for every $k \in D_2$ there is an element $d \in D_1$ such that

$$\alpha^{-1}\alpha_k\phi = \alpha_d : V_1 \to V_1$$

thus

$$\alpha_k = \phi\alpha_d\phi^{-1} = \alpha\tau(d).$$

Consequently, $k = \tau(d)$ and hence τ is surjective. Therefore, τ is an isomorphism. Furthermore, for every $d \in D_1$ and $v \in V_1$,

$$\phi(dv) = \phi\alpha_d(v) = \alpha_{\tau(d)}\phi(v) = \tau(d)\phi(v).$$

Using this fact we can show that if $\{u_1, \dots, u_n\}$ are D_1 linearly independent in V_1 yields to $\{\phi(u_1), \dots, \phi(u_n)\}$ is D_2-linearly independent and so $dim_{D_1}V_1 = dim_{D_2}V_2$.

□

3.2 The Jacobson Radical

There is little hope at present of classifying all rings up to isomorphism. Consequently we shall attempt to discover classes of rings for which some reasonable structure theorems are obtainable. Here is a classic method of determining such a class. Single out some "bad" or "undesirable" property of rings and study only those rings that do not have this property. In order to make this method workable in practice one must make some additional assumptions.

Let P be a property of rings and call an ideal [ring] I a P-ideal [P-ring] if I has property P. Assume that
(i) the homomorphic image of a P-ring is a P-ring;
(ii) every ring R (or at least every ring in some specified class $\mathcal{C}$) contains a P-ideal $P(R)$ (called the P-radical of R) that contains all other P-ideals of R;
(iii) the P-radical of the quotient ring $R/P(R)$ is zero;
(iv) the P-radical of the ring $P(R)$ is $P(R)$.
A property P that satisfies (i)-(iv) is called a radical property.

The P-radical may be thought of as measuring the degree to which a given ring possesses the "undesirable" property P. If we have chosen a radical property P, we then attempt to find structure theorems for those "nice" rings whose P-radical is zero. Such a ring is said to be P-radical free or P-semisimple. In actual practice we are usually more concerned with the P-radical itself rather than the radical property P from which it arises. By condition (iii) every ring that has a P-radical has a P-semisimple quotient ring. Thus the larger P-radical is, the more one discards (or factors out) when studying P-semisimple rings. The basic problem is to find radicals that enable us to discard as little as possible and yet to obtain reasonably deep structure theorems.

Definition. *An ideal P of a ring R is said to be* **left (right) primitive** *if the quotient ring R/P is a left (right) primitive ring.*

Let R be a commutative ring with identity. Then if $(1+r)(1+a) = 1+r+a+ra$, and so if $(1+a)$ is invertible, we have an element $r \in R$ such that $r \circ a := r+a+ra = 0$. If R does not have identity, the elements a for which there is an element $r \in R$ such that $r+a+ra = 0$ are called **left quasi-regular** elements.

Definition. *An element a in a ring R is said to be* **left quasi-regular** *if there exists $r \in R$ such that $r+a+ra = 0$. The element r is called a* **left quasi-inverse** *of a. A (right, left, or two-sided) ideal I of R is said to be* **left quasi-regular** *if every element of I is left quasi-regular. Similarly, $a \in R$ is said to be* **right quasi-regular** *if there exists $r \in R$ such that $a+r+ar = 0$. Right quasi-inverse and right quasi-regular ideals are defined analogously.*

Remark 3.2.1. *If the class $\mathcal{C}$ of those subsets of a ring R that satisfy a given property is empty, then $\cap_{I \in \mathcal{C}} I$ is defined to be R.*

Theorem 3.2.2. *If R is a ring, then there is an ideal $J(R)$ of R such that:*

(i) $J(R)$ is the intersection of all the left annihilators of simple left R-modules;

(ii) $J(R)$ is the intersection of all regular maximal left ideals of R;

(iii) $J(R)$ is the intersection of all the left primitive ideals of R;

1. [(*iv*)] *$J(R)$ is a left quasi-regular left ideal which contains every left quasi-regular left ideal of R;*

(v) Statements (i)-(iv) are also true if "left" is replaced by "right".

Lemma 3.2.3. *If $I(\neq R)$ is a regular left ideal of a ring R, then I is contained in a maximal left ideal which is regular.*

Proof. Since I is regular, there is an element $e \in R$ such that $r - re \in I$ for every $r \in R$. Thus any left ideal J containing I is regular. Consider the following set $S = \{I \subseteq L \subset R\}$. If we have a total chain in the set S, then the union of the elements in the total chain, say J, is an ideal that contains R, and moreover J must be regular because $r - re \in J$ for every $r \in R$. Therefore, S has a maximal element and moreover it is regular. □

Lemma 3.2.4. *Let R be a ring and let K be the intersection of all regular maximal left ideals of R. Then K is a left quasi-regular left ideal of R.*

Proof. It is clear that K is a left ideal. We only need to show that K is a left quasi-regular. Pick an arbitrary element $a \in K$, then we claim that $T := \{r + ra : r \in R\} = R$ and so it follows that there is an $r \in R$ such that $r+ra = -a$, and so $r+a+ra = 0$ which means a is a left quasi-regular element. To prove the claim consider that if $e = -a$, then for every $r \in R$, $r - (-ra) = r + ra \in T$ and so T is a regular left ideal. By the previous lemma if $T \neq R$, then there is a maximal left regular ideal M that is regular and contains K. Consider that for every $r \in R$, $ra \in M$ since $a \in K$. Now since K is regular we must have $r+ra \in K \subseteq M$ which yields $r \in M$, and so $R = M$, a contradiction. □

Lemma 3.2.5. *Let R be a ring that has a simple left R-module. If I is a left quasi-regular left ideal of R, then I is contained in the intersection of all the left annihilators of simple left R-modules.*

Proof. If $I \not\subseteq \cap Ann(A)$, wehre the intersection is taken over all simple left R-modules A, then $IB \neq 0$ for some simple left R-module B whence there is a $b \in B$ such that $Ib \neq 0$ and so we must have $Ib = B$. Thus there is $a \in I$ such that $ab = -b$. Consider that I is a left quasi-regular ideal, so $r + a + ra = 0$ for some $r \in R$. Therefore,

$$0 = 0b = (r + a + ra)b = rb + ab + rab = rb - b - rb = -b,$$

a contradiction. So we must have $I \subseteq \cap Ann(A)$. □

Lemma 3.2.6. *An ideal P of a ring R is left primitive if and only if P is the left annihilator of a simple left R-module.*

Proof. If P is a left primitive ideal, then R/P is a primitive ring and so there is a simple left R/P-module A, consider that A is a R-module with ra defined to be $(r+P)a$. Then $RA = (R/P)A \neq 0$ and every R-submodule of A is an R/P-submodule of A, thus since A is a simple R/P-module, it is also a simple R-module. Consider that if $r \in Ann(A)$, then $(r+P)A = 0$ and since A is faithful as a R/P-module we must have $r \in P$. Therefore, $Ann(A) = P$.

Conversely, suppose that P is the annihilator of a simple left R-module A. Then we can see that A is a R/P-module. We show that A is a faithful simple R/P-module and so R/P is a primitive ring which result in P is a left primitive ideal. Note that A is a simple as an R/P-module since it is a simple R-module, moreover, if $(r+P) \in Ann(A)$, then $rA = 0$, and so $r \in P$, thus $r + P = 0$, we must have A is a faithful R/P-module. □

Lemma 3.2.7. *Let I be a left ideal of a ring R. If I is left quasi-regular, then I is right quasi-regular.*

Proof. If I is left quasi-regular and $a \in I$, then there exists $r \in R$ such that $r \circ a = r + a + ra = 0$. Since $r = -a - ra \in I$, there is $s \in R$ such that $s \circ r = s + r + sr = 0$, so s is right quasi-regular. The operator $\circ$ is associative. Thus,

$$a = 0 \circ a = (s \circ r) \circ a = s \circ (r \circ a) = s \circ 0 = s.$$

Therefore, a and hence I, is right quasi-regular. □

Theorem 3.2.8. *If R is a ring, then there is an ideal $J(R)$ of R such that:*

(i) $J(R)$ is the intersection of all the left annihilators of simple left R-modules;

(ii) $J(R)$ is the intersection of all regular maximal left ideals of R;

(iii) $J(R)$ is the intersection of all the left primitive ideals of R;

1. *[(iv)] $J(R)$ is a left quasi-regular left ideal which contains every left quasi-regular left ideal of R;*

(v) Statements (i)-(iv) are also true if "left" is replaced by "right".

Proof. Let $J(R)$ the intersection of all the left annihilators of simple left R-modules. Then $J(R)$ is an ideal. We have two cases:

Case 1: R has no simple left R-module. Then by convention we have that $J(R)$ the intersection of all the left annihilators of simple left R-modules is R. Now consider if R has a regular maximal left ideal M, then R/M is a simple left R-module, a contradiction and so the intersection of all regular maximal left ideals of R is R too. By Lemma 3.2.6, R has no left primitive ideal and so again the intersection of all the left primitive ideals of R is R. Finally, R is a left quasi-regular left ideal which contains every left quasi-regular left ideal of R.

Case 2: R has a simple left R-module and so $J(R)$ the intersection of all the left annihilators of simple left R-modules is not R.

2-1: $J(R)$ is the intersection of all regular maximal left ideals of R? Let K be the intersection of all regular maximal left ideals of R. Then by Lemma 3.2.4 K is a left quasi-regular left ideal of R, whence by Lemma 3.2.5 it is a subset of the intersection of all the left annihilators of simple left R-modules. Therefore, $K \subseteq J(R)$. Let $c \in J(R)$. Consider that $J(R)$ is the intersection of the left annihilators of the quotients R/I where I runs over all regular maximal left ideals of R. For each regular maximal ideal I there exists $e \in R$ such that $c - ce \in I$. Since $c \in Ann(R/I)$, we have $cr \in I$ for every $r \in R$; in particular, $ce \in I$, and consequently, $c \in I$. Thus $J(R) \subseteq \cap I$ where the intersections runs over all regular maximal ideal I. Therefore. $K = J(R)$.

3-1: If follows from Lemma 3.2.6 that the intersection of all left primitive ideals is the same as the intersection of all the left annihilators of simple left R-modules.

4-1: We have already showed that $J(R)$ is the same as the intersection of all regular maximal left ideals of R, whence by Lemma 3.2.4 it is a left quasi-regular left ideal of R. Also, by Lemma 3.2.5, $J(R)$ contains every left quasi-regular left ideal of R.

□

Corollary 3.2.9. *Let $J_1(R)$ be the intersection of the right annihilators of all simple right R-modules. If $J(R)$ be the same as the above theorem $J_1(R) = J(R)$.*

Proof. Consider that the above theorem is true if we replace every "left" by "right". By Lemma 3.2.7 $J(R)$ is right quasi-regular and by part (iv) of the above theorem $J(R) \subseteq J_1(R)$. Similarly, $J_1(R) \subseteq J(R)$. □

Example 3.2.10. *Let R be a local ring with unique maximal ideal M. We shall show that $J(R) = M$. Consider that since every ideal is inside a maximal ideal we must have $J(R) \subseteq M$. Moreover, if $r \in M$, then $1 + r$ is a unit and so there is an element $a \in R$ such that $a + r + ar = 0$, thus every element of M is left-quasi regular, whence M is left quasi-regular and so it must be inside $J(R)$.*

As some examples, $J(F[[x]]) = \langle x \rangle$ and $J(\mathbb{Z}_{p^n}) = \langle p \rangle$.

Definition. *A ring R is said to be* **(Jacobson) semisimple** *if its Jacobson radical $J(R)$ is zero. R is said to be a radical ring if $J(R) = R$.*

Remark 3.2.11. *Throughout this book "radical" always means "Jacobson radical" and "semisimple" always means "Jacobson semisimple."*

Example 3.2.12. *Every maximal ideal in $\mathbb{Z}$ is of the form $\langle p \rangle$ with p prime. Consequently, $J(\mathbb{Z}) = \cap \langle p \rangle = 0$, whence $\mathbb{Z}$ is Jacobson semisimple.*

Example 3.2.13. *If D is a division ring, then the polynomial ring*

$$R = D[x_1, \dots, x_n]$$

is semisimple. We should show that $J(R) = 0$. Let $f \in J(R)$, since f is left and right quasi-regular, we must have $(1 + f)$ is invertible, therefore, $(1 + f)$ is an element of D, and so since $1 \in D$, we must have $f \in D$. Consequently, $J(R)$ is an ideal of D and since $1 \notin J(R)$ and D is a division ring, it follows that $J(R) = 0$.

Theorem 3.2.14. *Let R be a ring.*

1. *If R is primitive, then R is semisimple.*

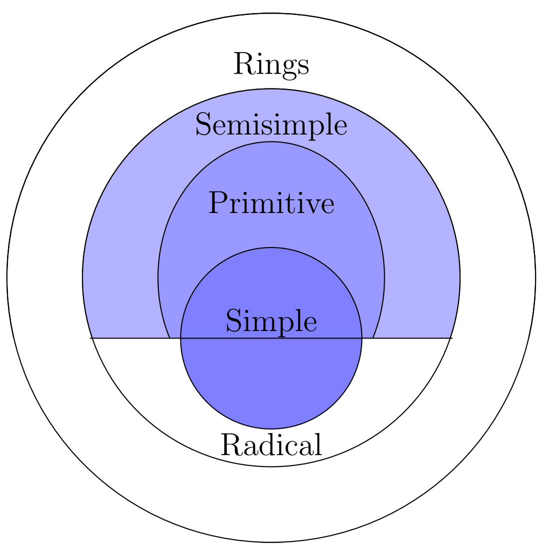
2. *If R is simple and semisimple, then R is primitive.*

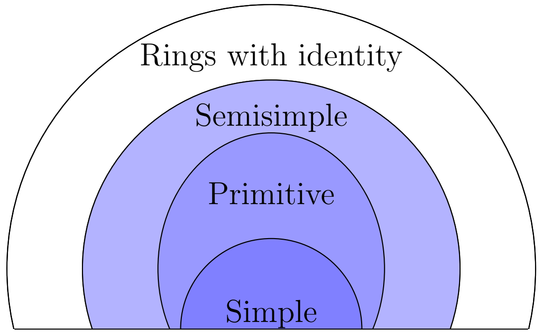
3. *If R is simple, then R is either a primitive semisimple or a radical ring.*

Proof. (1) If R is primitive, then there is a faithful simple R-module A. Since $J(R)$ is the intersection of all annihilators of simple left R-modules, we conclude that $J(R) \subseteq Ann(A) = 0$.

(2) Consider that since R is simple, we have $R \neq 0$, and moreover there must exist a simple R-module A, otherwise $J(R) = R \neq 0$, contradicting semisimplity. Note that $Ann(A)$ is a two-sided ideal of R and furthermore $Ann(A) \neq R$ since $RA \neq 0$. Therefore, $Ann(A) = 0$ and so A is a faithful simple $R - module$, whence R is semisimple.

(3) Since R is simple, $J(R)$ is either 0 or R. In the former case, R is semisimple and so primitive, and in the latter case R is a radical ring. $\square$





Example 3.2.15. *The set of $n \times n$ matrices over a division ring is a simple ring, and moreover it is semisimple.*

Definition. *An element a of a ring R is nilpotent if $a^n = 0$ for some positive integer n. A (left, right, two-sided) ideal I of R is nil if every element of l is nilpotent; I is nilpotent if $I^n = 0$ for some integer n.*

Theorem 3.2.16. *If R is a ring, then every nil right or left ideal is contained in the radical $J(R)$.*

Proof. If I is nil right or left ideal, and $a \in I$. Then $a^n = 0$ for some positive integer n. Now consider the element $r = -a + a^2 - a^3 + \ldots + (-1)^{n-1}a^{n-1}$. Verify that $r + a + ra = 0 = r + a + ar = 0$, whence a is both left and right quasi-regular. Therefore, every nil left or right ideal is a left (right) quasi-regular, so it is contained in $J(R)$ by the Theorem 3.2.8. □

Proposition 3.2.17. *If R is a left [resp. right) Artinian ring, then the radical $J(R)$ is a nilpotent ideal. Consequently every nil left or right ideal of R is nilpotent and $J(R)$ is the unique maximal nilpotent left (or right) ideal of R.*

Proof. Consider the following chain of ideals

$$J(R) \supseteq J(R)^2 \supseteq J(R)^3 \supseteq J(R)^4 \supseteq \cdots$$

Since we have a left Artinian ring there is a positive integer k such that $J(R)^k = J(R)^{k+1}$. Suppose that $J(R)^k \neq 0$. Now consider the following set

$$S = \{I \lhd R : J(R)^k I \neq 0\}.$$

Consider that this set is not empty since $J(R)^k J(R)^k = J(R)^{2k} = J(R)^k \neq 0$. Again as the ring is left Artinian, S has a minimal element, say I, so $J^k I \neq 0$. Let $a \in I$ such that

$J^k a \neq 0$. Note that $J^k a \subseteq I$, and also $J^k(J^k a) = J^{2k} a = J^k a \neq 0$. Therefore, we must have $J^k a = I$. Thus there exists $r \in J^k$ such that $ra = a$. Since $r \in J$, so it is a left quasi-regular element and there os an element $s \in R$ such that $s - r - sr = 0$. Consequently,

$$a = ra = -(-ra) = -(-ra + 0) = -(-ra + sa - sa) =$$

$$-(-ra + sa - s(ra)) = -(-r + s - sr)a = -0a = 0.$$

This contradicts the fact that $a \neq 0$. Therefore, $J^k = 0$. The last statement is an immediate consequence of Theorem 3.2.16. □

Finally we wish to show that left quasi-regularity is a radical property as defined in the introduction to this section. Its associated radical is clear that Jacobson radical and a left quasi-regular ring is precisely a radical ring. Since a ring homomorphism necessarily maps left quasi-regular elements onto left quasi-regular elements, the homomorphic image of a radical ring is also a radical ring. To complete the discussion we must show that $R/J(R)$ is sernisimple and that $J(R)$ is a radical ring.

Theorem 3.2.18. *If R is a ring, then the quotient ring $R/J(R)$ is semisimple.*

Proof. We must show that $J(R/J(R)) = 0$. Consider the canonical projection $\pi : R \to R/J(R)$ where $\pi(r) = r + J(R) = \overline{r}$. Note that $J(R/J(R))$ is the intersection of all regular maximal left ideals of $R/J(R)$. Let $\overline{M}$ be a regular maximal left ideal of $R/J(R)$. Then there is a left maximal ideal such that $M/J(R) = \overline{M}$. Moreover, since there is an element $e \in R$ such that for every $\overline{r} \in R/J(R)$, $\overline{r} - \overline{r}e + J(R) \in M/J(R)$, we have that $r - re + J(R) \subseteq M$. It follows $r - re \in M$. Therefore, M is a regular maximal left ideal. Consequently, if $\overline{r} \in \cap M/J(R)$ where the intersection runs over all regular maximal left ideals M of R. Thus, r is in every regular maximal left ideal of R and so it is in $J(R)$ and $\overline{r} = 0$. □

Lemma 3.2.19. *Let R be a ring and $a \in R$.*

1. *If $-a^2$ is left quasi-regular, then so is a.*

2. *$a \in J(R)$ if and only if Ra is a left quasi-regular left ideal.*

Proof. (1) If $r + (-a^2) + r(-a^2) = 0$, let $s = r - a - ra$. Then $s + a + sa = r - a - ra + a + (r - a - ra)a = r - a - ra + a + ra - a^2 - ra^2 = r - a^2 - ra^2 = 0$.

(2) Let $a \in J(R)$, then since $J(R)$ is a left-quasi regular ideal and $Ra \subseteq J(R)$, it follows that Ra is a left-quasi regular left ideal. Conversely, suppose Ra is a left quasi-regular left ideal. Consider the following subset of R,

$$K = \{ra + na : r \in R, n \in \mathbb{Z}\}$$

is a left ideal of R that contains both a and Ra. We claim that K is left quasi-regular. Let $ra + na \in K$, then $-(ra + na)^2 \in Ra$ and so $-(ra + na)^2$ is left quasi-regular, whence by the first part $ra + na$ is left quasi-regular. It follows that K is a left quasi-regular left ideal. So we must have $a \in K \subseteq J(R)$. □

Theorem 3.2.20. *(1) If an ideal of I is considered as a ring, then $J(I) = I \cap J(R)$.*

(2) If R is semisimple, then so is every ideal of R.

(3) $J(R)$ is a radical ring.

Proof. The first two statements are immediate consequences of (1). So we only need to proof (1).

Consider that $I \cap J(R)$ is a left ideal of I, and moreover if $a \in I \cap J(R)$, then a is left quasi-regular whence there exists $r \in R$ such that $r + a + ra = 0$. However, $r = -a - ra \in I$. Consequently, a is left quasi-regular in I and so it must be an element of $J(I)$. Therefore, $I \cap J(R) \subseteq J(I)$.

Now let $a \in J(I)$. Thus for every $r \in R$, $-(ra)^2 = -(rar)a \in IJ(I) \subseteq J(I)$, and so it must be a left quasi-regular element in I, consequently, it is a left quasi-regular element of R, and so by the part (1) of the previous lemma, ra is regular in R. It now follows that Ra is a left quasi-regular left ideal of R, and by the second part of the previous lemma we must have $a \in J(R)$. Therefore, $J(I) \subseteq I \cap J(R)$. $\square$

Theorem 3.2.21. *If $\{R_i : i \in I\}$ is a family of rings, then $J(\prod_{i\in I} R_i) = \prod_{i\in I} J(R_i)$.*

Proof. If (a_i) is in $\prod_{i\in I} J(R_i)$, then each a_i is left quasi-regular in R_i, and it is easy to verify that (a_i) is a left quasi-regular element of $\prod_{i\in I} R_i$, consequently, $\prod_{i\in I} J(R_i) \subseteq J(\prod_{i\in I} R_i)$.

For any $i \in I$, let π_i be the projection to the ith component. Then verify that each element of projection of $J(\prod_{i\in I} R_i)$ to its ith component, i.e., each element of $\pi_i(J(\prod_{i\in I} R_i))$ is left quasi-regular in R_i, and so we must have $J(\prod_{i\in I} R_i) \subseteq \prod_{i\in I} J(R_i)$. $\square$

3.3 Semisimple Rings

Definition. *A ring R is said to be a* **subdirect product** *of the family of rings $\{R_i : i \in I\}$ if R is a subring of the direct product $\prod_{i\in I} R_i$ such that $\pi_k(R) = R_k$ for every $k \in I$, where $\pi_k : \prod_{i\in I} R_i \to R_k$ is the canonical epimorphism.*

Remark 3.3.1. *A ring S is isomorphic to a subdirect product of the family of rings $\{R_i : i \in I\}$ if and only if there is a monomorphism of rings $\phi : S \to \prod_{i\in I} R_i$ such that $\pi_k(\phi(S)) = R_k$ for every $k \in I$.*

Example 3.3.2. *Let P be the set of prime integers. Define the map*

$$\phi : \mathbb{Z} \to \prod_{p\in P} \mathbb{Z}_p$$

given by $k \mapsto \{k_p\}_{p\in P}$ where k_p is k modulo p. Consider that $\pi_p\phi(\mathbb{Z}) = \mathbb{Z}_p$ for every $p \in P$. Thus $\mathbb{Z}$ is isomorphic to a subdirect product of the family of fields $\{\mathbb{Z}_p : p \in P\}$.

Proposition 3.3.3. *A non-zero ring R is semisimple if and only if R is isomorphic to a subdirect product of primitive rings.*

Proof. Let R be a non-zero semisimple ring, and let $\mathcal{P}$ be the set of all left primitive ideals of R. So for each $P \in \mathcal{P}$, we have that R/P is a left primitive ring. We show that R is a subdirect product of the family of primitive rings $\{R/P : P \in \mathcal{P}\}$. Consider the following map $\phi : R \to \prod_{P\in\mathcal{P}} R/P$. If $r \in ker(\phi)$, then $r + P = 0$, and so $r \in P$. Therefore, $r \in \cap_{P\cap\mathcal{P}} P = 0$. Thus ϕ is injective. Also $\pi_Q(\phi(R)) = R/Q$. Consequently, R is isomorphic to a subdirect product of primitive rings.

Conversely, suppose that R is isomorphic to a subdirect product of primitive rings. We want to show that $J(R) = 0$. So let $\phi : R \to \prod_{i\in I} R_i$ be injective and $\pi_k(\phi(R)) = R_k$. Note that $R/ker(\pi_k \circ \phi) = R_k$ is a left primitive ring, therefore, we must have $ker(\pi_k \circ \phi)$ is a left primitive ideal. Therefore, $J(R) \subseteq \cap ker(\pi_k \circ \phi)$. If $\pi_k \circ \phi(r) = 0$, then the kth component of $\phi(r)$ is zero in $\prod R_i$. Thus if $r \in \cap ker(\pi_k \circ \phi)$, we must have $\phi(r) = 0$. Since ϕ is injective $r = 0$. Therefore, $J(R) \subseteq \cap ker(\pi_k \circ \phi) = 0$. □

Theorem 3.3.4. *(Chinese Remainder Theorem) Let $A_1, \ldots, A_n$ be ideals of R such that $R^2 + A_i = R$ for all i and $P_i + P_j = R$ for all $i \neq j$. If $b_1, \ldots, b_n \in R$ there exists $b \in R$ such that*

$$b \equiv b_i(mod\ A_i)(i = 1, 2, \ldots, n).$$

Furthermore b is uniquely determined up to congruence modulo the ideal

$$A_1 \cap A_2 \cap \ldots \cap A_n.$$

Theorem 3.3.5. *(Wedderburn-Artin) The following conditions on a ring R are equivalent.*

(i) R is a nonzero semisimple left Artinian ring;

(ii) R is a direct product of a finite number of simple ideals of whcih is ismorphic to endomorphism ring of a finite dimensional vector space over a division ring R.

(iii) there exist division rings $D_1, \ldots, D_n$ and positive integers $n_1, \ldots, n_t$ such that R is isomorphic to the ring $Mat_{n_1}D_1 \times \ldots \times Mat_{n_t}D_t$.

Proof. $(ii) \Leftrightarrow (iii)$ It follows from some theorems that have been proven before.

$(ii) \Rightarrow (i)$ By hypothesis $R \cong \prod_{i=1}^{t} R_i$ where each R_i is isomorphic to the ring of endomorphisms of a finite dimensional vector space. We have shown in an example that the ring of endomorphisms of a finite dimensional vector space over a division ring is primitive, and by Theorem 3.2.14, each R_i is semisimple. Thus $J(R) \cong \prod J(R_i) = 0$ and so R is semisimple. Moreover we already have seen that the product of endomorphisms of finite dimensional vector spaces is left Artinian.

$(i) \Rightarrow (ii)$ For each P_i consider that R/P_i is semisimple left Artinian ring and so each R/P_i is isomorphic to endomorphisms of a finite dimensional vector space over a division ring. It follows that R/P_i is simple ring and so P_i is maximal ideal. Consequently, we can say that $P_i + P_j = R$ if P_i and P_j are distinct primitive ideals and since R/P_i is simple, $(R/P_i)^2 \neq 0$, thus $R^2 + P_i = R$. Consider that

$$R^2 = (P_1 + P_2)(P_1 + P_3) = P_1^2 + P_1P_3 + P_2P_1 + P_2P_3 \subseteq P_1 + P_2P_3.$$

Also,

$$R = R^2 + P_1 \subseteq P_1 + P_2P_3 + P_1 \subseteq P_1 + P_2 \cap P_3.$$

Inductively, we can show that for any set of primitive ideals $P_1, \ldots, P_n$, we have

$$R = P_n + (P_1 \cap \ldots \cap P_{n-1}).$$

First we show that R has finitely many primitive ideals. Suppose on the contrary R has infinitely many primitive ideals $P_1, P_2, \ldots$. Then since R is left Artinian, the following chain is stable, $P_1 \supseteq P_1 \cap P_2 \supseteq P_1 \cap P_2 \cap P_3 \supseteq \ldots$. Therefore there is a positive integer k such that $P_1 \cap \ldots \cap P_k \subseteq P_{k+1}$. However by the above argument

$$P_{k+1} + P_1 \cap \ldots \cap P_k = R,$$

a contradiction. Therefore, R has finitely many primitive ideals $P_1, \ldots, P_k$.

Now consider that by Chinese Remainder Theorem

$$R = R/0 = R/J(R) = R/\cap P_i \cong R/P_1 \times \ldots \times R/P_k.$$

Therefore, R is the direct product of the preimage of simple ideals R/P_i where each preiamge of R/P_i is isomorphic to ring of the endomorphisms of a finite dimensional vector space over a division ring. □

Corollary 3.3.6. *(i)A semisimple left Artinian ring has an identity.*
(ii) A semisimple ring is left Artinian if and only if it is right Artinian.
(iii) A semisimple left Artinian ring is both left and right Noetherian.

Proposition 3.3.7. *If I is an ideal in a semisimple left Artinian ring R, then $I = Re$, where e is an idempotent which is in the center of R.*

Theorem 3.3.8. *The following conditions on a nonzero module A over a ring R are equivalent.*
(i) A is the sum of a family of simple submodules.
(ii) A is the (internal) direct sum of a family of simple submodules.
(iii) For every nonzero element a of A, $Ra \neq 0$; and every submodule B of A is a direct summand (that is, $A = B \oplus C$ for some submodule C).

A module that satisfies the equivalent conditions of the above theorem is said to be **semisimple or completely reducible**.

Definition. *A subset* $\{e_1, e_2, \ldots, e_m\}$ *of* R *is a set of* **orthogonal idempotenet** *if* $e_i^2 = e_i$ *for all* i *and* $e_i e_j = 0$ *for all* $i \neq j$.

Theorem 3.3.9. *The following conditions on a nonzero ring* R *with identity are equivalent.*

(i) R *is semisimple left Artinian;*

(ii) Every nonzero unitary left R*-module is semisimple;*

(iii) R *is itself unitary semisimple left* R*-module;*

(iv) Every left ideal of R *is of the form* Re *with* e *idempotent;*

(v) R *is the (internal) direct sum (as a left* R*-module) of minimal left ideals* $K_1, \ldots, K_m$ *such that* $K_i = Re_i (e_i \in R)$ *for* $i = 1, 2, \ldots, m$ *and* $\{e_1, \ldots, e_m\}$ *is a set of orthogonal idempotents with* $e_1 + e_2 + \ldots + e_m = 1_R$.

Proof. We shall prove the implications $(ii) \Rightarrow (iv) \Rightarrow (v) \Rightarrow (iii) \Rightarrow (i) \Rightarrow (v) \Rightarrow (ii)$.

$(ii) \Rightarrow (iv)$ Since every left ideal L of R is its submodule, and R is semisimple $R = L \oplus I$ for some left ideal I of R. Consequently, there are $e_1 \in L$ and $e_2 \in I$ such that $1 = e_1 + e_2$. We show that $Re_1 = L$. Clearly, $Re_1 \subseteq L$. Let $r \in L$. Then $r = r.1 = re_1 + re_2$. Consider that $re_2 = r - re_1 \in L \cap I = 0$, therefore, $r = re_1 \in Re_1$. We conclude that $Re_1 = L$. In particular, we have $e_1 e_1 = e_1$ and so e_1 is an idempotent.

$(iv) \Rightarrow (iii)$ Let I be an ideal of R, we show that I is a direct summand of R. Consider that $I = Re$, and we can show that $R = Re + R(1 - e)$, and so R is a semisimple ring. □

$(iii) \Rightarrow (i)$ Since R is itself unitary semisimple left R-module, we have $R = \sum_{i \in I} B_i$ where each B_i is a simple submodule. Consider that each $B_i = Re_i$ for some $e_i \neq 0$. Therefore, after relabeling we have $1 = e_1 + \ldots + e_n$. If $r \in J(R)$, then $r = re_1 + \ldots + re_n$. Since r is in the intersection of all simple modules we have $re_i = 0$ for all i and so we must have $r = 0$. Therefore, $J(R) = 0$ and thus R is semisimple. Since B_i is simple and

$$(B_1 \oplus \ldots \oplus B_i)/(B_1 \oplus \ldots \oplus B_{i-1}) \cong B_i,$$

the series

$$R = B_1 \oplus \ldots \oplus B_n \supset B_1 \oplus \ldots \oplus B_{n-1} \supset \ldots \supset B_1$$

is a composition series for R. Therefore, R is left Artinian.

$(i) \Rightarrow (v)$ It follows from Wedderburn-Artin Theorem.

$(v) \Rightarrow (ii)$ Let A be a a unitary R-module. Consider the following set

$$\{K_i a : 1 \leq i \leq m; a \in A; K_i a \neq 0\}$$

is a family of submodules of A that generates A, because for every $a \in A$, $a = 1.a = e_1 a + \ldots + e_m a \in K_1 a + \ldots + K_m a$. Now since K_i, for each i, is a minimal left ideal, the map $K \to K_i a$ is an isomorphism by Schur's lemma. Therefore, A is the sum of a set of simple modules and so it is semisimple.