An Introduction to Commutative Rings

Mehmet Kaan Bengi

Abstract

This purpose of this paper is to investigate some concepts of commutative rings. Its goal is to give the reader a thorough introduction to the study of rings and their ideals. We begin from the most basic definition of the ring and proceed to investigate the various ideals that pertain to these structures. There will be a thorough treatment of the properties of each type of ideal, particularly prime ideals and maximal ideals, which are central tools in commutative algebra and algebraic geometry. We will conclude the paper by exploring some applications of rings and ideals in algebraic geometry.

Contents

1 Introduction

This paper is meant for readers who are encountering commutative rings for the first time. A fundamental knowledge of group theory is assumed as well as a familiarity with important theorems such as the Isomorphism Theorems and Zorn's Lemma. The contents of this paper are fairly abstract, and though examples for each structure are provided, we recommend that readers keep in mind the sets $\mathbb{Z}$ and $\mathbb{R}[x]$ (both of which are rings) in order to convince

themselves of the truth of the properties and theorems. This paper primarily draws its contents from M.F. Atiyah and I.G. MacDonald's *Introduction to Commutative Algebra* [1]. A list of all the resources used in compiling this paper are included in the citations for those wishing to immerse themselves deeper in the subject.

2 Rings

We begin by defining a ring in the most general terms.

Definition 1 (Ring)**.** *A **ring** A is a set equipped with two binary operations called addition and multiplication such that:*

- *A is an Abelian group with respect to addition (namely, A has a zero element (0), and for each $x \in A$, there exists $-x \in A$; A is closed under addition)*
- *Multiplication is associative $[(xy)z = x(yz)]$ and distributive over addition $[x(y+z) = xy + xz,\ (y+z)x = yx + yz]$.*

*A ring is **commutative with identity** if*

- *$xy = yx$ (commutativity)*
- *there exists $1 \in A$ such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in A$ (multiplicative identity)*

As this paper focuses on commutative rings, we will only consider commutative rings with an identity element. Thus, from this point forward, the term ring will be used to describe a commutative ring, and will be denoted by A. Unless otherwise stated, addition and multiplication will be defined in the natural way.

Example 1.1. *Some basic examples of rings:*

- *The set of rational integers $\mathbb{Z}$*
- *The set of real numbers $\mathbb{R}$*
- *The set of complex numbers $\mathbb{C}$*
- *The set of rational numbers $\mathbb{Q}$*

It is important to note that $A = (0)$ is also a ring where 0 is both the additive identity and the multiplicative identity. We call this ring the **zero ring**. Furthermore, if A is a commutative ring, the set $A[x] = \{a_0 + a_1x + ... + a_nx^n : n \in \mathbb{N}, a_i \in \mathbb{R}\}$ is also a commutative ring. We call this ring the **ring of polynomials of a single variable**. If A is a commutative ring, $A[x_1, x_2, ..., x_n]$ is also a commutative ring. We call this ring the **ring of polynomials of multiple variables**. Note that in the cases of the polynomial rings, we assume that $x^0 = 1$. One final example worth mentioning is the set of functions that

map the elements from a given set to the real numbers. More precisely, let S be any set, and define $\mathcal{F}(S)$ by $\mathcal{F}(S) = \{f : S \longrightarrow \mathbb{R}\}$. Defining addition by $(f+g)(x) = f(x) + g(x)$ and multiplication by $(fg)(x) = f(x)g(x)$, the above set forms a commutative ring.

As is the case with groups, rings also have substructures called subrings.

Definition 2 (Subring)**.** *Let A be a ring. A subset $B \subseteq A$ is a subring of A if B itself is a ring with respect to the same binary operations on A.*

Example 2.1. *Some intuitive examples of subrings:*

- $\mathbb{Z}$ *is a subring of* $\mathbb{Q}$
- $\mathbb{Q}$ *is a subring of* $\mathbb{R}$
- $\mathbb{R}$ *is a subring of* $\mathbb{C}$
- A *is a subring of* $A[x]$
- $\{\bar{0}, \bar{3}\}$ *is a subring of* $\mathbb{Z}/6\mathbb{Z}$

Similar to groups, we can compare the structure of two rings using **ring homomorphisms**.

Definition 3 (Ring Homomorphism)**.** *Let A and B be rings. A map $f : A \longrightarrow B$ is a ring homomorphism if*

- $f(x+y) = f(x) + f(y)$ *for all* $x, y \in A$
- $f(xy) = f(x)f(y)$ *for all* $x, y \in A$
- $f(1_A) = 1_B$

Because ring homomorphisms preserve both addition and multiplication, we can observe that the image of f is a subring of B. Perhaps a more surprising fact is that the kernel of f is a subring of A.

Proposition 1. *Let $f : A \longrightarrow B$ be a ring homomorphism. Then, $ker(f) = \{a \in A : f(a) = 0\}$ is a subring of A.*

Proof. Let $f : A \longrightarrow B$ be a ring homomorphism. Observe that $(ker(f), +_A)$ is a subgroup of $(A, +_A)$. Let $x, y \in ker(f)$. Because f is a ring homomorphism, $f(x \cdot_A y) = f(x) \cdot_B f(y)$. By the definition of the kernel, $f(x) \cdot_B f(y) = 0_B \cdot_B 0_B = 0_B$. Hence, $x \cdot_A y \in ker(f)$. Thus, the conditions for a subring a fulfilled, so that $ker(f)$ is a subring of A.

□

Note that in the above proposition, the statement is true even though $ker(f)$ does not necessarily have an identity element.

We now define a substructure of a ring called an **ideal**. Ideals are to rings what normal subgroups are to groups. They allow for the formation of quotient rings, which bear a striking resemblances to quotient groups.

2.1 Ideals

Definition 4 (Ideal)**.** *A subset $I \subseteq A$ is an ideal of A if $(I, +)$ is an Abelian group and, for each $a \in A$ and each $x \in I$, $ax \in I$.*

Example 4.1. *Some examples of ideals:*

- *$n\mathbb{Z}$ is an ideal of $\mathbb{Z}$*
- *A is an ideal of A itself*
- *The set of polynomials with a constant term of zero is an ideal of $A[x]$*

Note that if $I \neq A$, then I is called a *proper ideal.*

Proposition 2. *If $f : A \longrightarrow B$ is a ring homomorphism, then $ker(f)$ is an ideal of A.*

Proof. Let $f : A \longrightarrow B$ be a ring homomorphism. Let $k \in ker(f)$ and let $x \in A$. Then, $f(xk) = f(x)f(k) = f(x) \cdot 0 = 0$. Thus, $xk \in ker(f)$. Therefore $ker(f)$ is an ideal of A. □

We can now use the concept of an ideal to define an equivalence relation $a \sim b \iff a - b \in I$. We denote the set of all equivalence classes by A/I. By defining addition by $(a + I) + (b + I) = (a + b) + I$ and multiplication by $(a+I)\cdot(b+I) = ab+I$, we give A/I a ring structure. We call this the **quotient ring**. Note that addition defined this way is well-defined because A is an Abelian group and I is a normal subgroup under addition. It it is straightforward to prove that the multiplication operation is also well-defined, and we omit the proof for the sake of brevity The operations above are identical to ones defined for modular arithmetic using the rational integers.

There exists a natural map $\varphi : A \longrightarrow A/I$ defined by $\varphi(a) = a + I$ for all $a \in A$. In fact, this map is a ring homomorphism, and is by its definition surjective.

Theorem 1 (Isomorphism Theorem)**.** *If $f : A \longrightarrow B$ is a ring homomorphism, then $im(f) \cong A/ker(f)$.*

Given how we have defined the notion of an ideal, it seems natural to ask what the ideals of A/I itself are. As we shall see, the ideals of A/I are precisely in one-to-one correspondence with the ideals of A containing I.

Throughout the rest of the paper, we will make use of the following elementary fact:

Proposition 3. *There is a one-to-one, order-preserving correspondence between the ideals J of A which contain I, and the ideals J' of A/I, given by $J = \varphi^{-1}(J')$.*

We now proceed to define the features of certain elements found in commutative rings.

Definition 5 (Zero-divisor)**.** *An element $x \in A$ is a zero-divisor if there exists a nonzero $y \in A$ such that $xy = 0$.*

Definition 6 (Nilpotent)**.** *An element $x \in A$ is nilpotent if there exists $n \geq 1$ such that $x^n = 0$.*

Definition 7 (Unit)**.** *An element $x \in A$ is a unit if there exists $y \in A$ such that $xy = 1$. Since x is uniquely determined by y, we denote y by x^{-1}.*

Note that if an element is nilpotent, it is always a zero-divisor. Furthermore, by definition, an element cannot be both a unit and a zero-divisor.

Definition 8 (Integral Domain)**.** *Let A be a commutative ring with identity. If the only zero-divisor of A is 0, then A is called an integral domain.*

Example 8.1. *Some examples of integral domains: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$.*

We denote the multiples of an element $x \in A$ by (x). These multiples form an ideal, which we call the ideal generated by x. For elements $x_1, ..., x_n \in A$, we denote by $(x_1, ..., x_n)$ the smallest ideal containing $x_1, ..., x_n$. We say this is the ideal generated by $x_1, ..., x_n$. Note that if x is a unit in A, then the ideal generated by x, is equal to the whole ring.

Proposition 4. *An ideal I of ring A is equal to A if and only if I contains a unit.*

Proof. The forward direction is trivial, because if $I = A$, then I contains all of the units in A. We seek to prove the backwards direction. Let I be an ideal of A, and let $u \in I$, where u is a unit. By definition, u^{-1} is also a unit. Let $x \in A$. Because A is closed, $x \cdot u^{-1} \in A$. By the definition of an ideal, $(x \cdot u^{-1}) \cdot u \in A$. Thus, $x \in I$. Therefore $A \subseteq I$. Since $I \subseteq A$ by definition, we get that $I = A$. $\square$

The notion of ideals allows us to write a characterization of fields.

Definition 9 (Field)**.** *A field is a ring A in which $1 \neq 0$ and every nonzero element is a unit.*

Proposition 5. *Let A be a ring. Then, the following are equivalent:*

- *A is a field*
- *The only ideals of A are (0) and A*
- *Any ring homomorphism from A to a nonzero ring B is injective*

Proof. $(i) \rightarrow (ii)$ Assume A is a field. Let I be a nonzero ideal. Then, I contains a unit (because all elements of a field have inverses), and therefore $I = A$.

$(ii) \rightarrow (iii)$ Assume the only ideals of A are (0) and A. Let $\varphi : A \longrightarrow B$ be a ring homomorphism. Then $ker(\varphi)$ is an ideal of A that does not equal A. Therefore $ker(\varphi) = 0$, and thus φ is injective.

$(iii) \rightarrow (i)$ Assume that any ring homomorphism from A to a nonzero ring B is injective. Let x be a nonzero element in A. If x is not a unit, then (x) is

a proper ideal of A. Now, let $\varphi : A \longrightarrow A/(x)$ be the natural map. Since φ is injective, $ker(\varphi) = (x) = (0)$, which is a contradiction. Thus, x is a unit. Therefore, A is a field. $\square$

We now introduce the fundamental concepts of prime ideals and maximal ideals.

2.2 Prime and Maximal Ideals

Definition 10 (Prime Ideals)**.** *Let A be a ring. A proper ideal I of A is a prime ideal if for all $a, b \in A$ where $ab \in I$, either $a \in I$ or $b \in I$.*

Example 10.1. *Some examples of prime ideals.*

- $p\mathbb{Z} \subseteq \mathbb{Z}$
- $(0) \subseteq$ *any integral domain*
- $(x) \subseteq \mathbb{R}[x]$

Definition 11 (Maximal Ideals)**.** *An ideal I is a maximal ideal if there does not exist an ideal $J \subset A$ such that $I \subseteq J$.*

Equivalently, an ideal p is prime if and only if A/p is an integral domain, and an ideal m is maximal if and only if A/m is a field. [3] Thus, a maximal ideal is always a prime ideal, though the converse is not necessarily true. Another fairly straightforward property is that if $\varphi : A \longrightarrow B$ is a surjective homomorphism and $p \subseteq A$ is a prime ideal, then $\varphi(p)$ is a prime ideal.

Theorem 2. *Every nonzero ring A has at least one maximal ideal.*

Proof. Let Σ be the set of all proper ideals of nonzero ring A. Since $(0) \in \Sigma$, Σ is nonempty. Let $I_1 \subseteq I_2 \subseteq ...$ be a chain in Σ. Because $I_1 \subseteq I_2 \subseteq ...$ is an increasing chain, $\bigcup_{i=1}^{\infty} I_n$ is an ideal. If $\bigcup_{i=1}^{\infty} I_n = A$, then $1 \in \bigcup_{i=1}^{\infty} I_n$ so that $1 \in I_j$ for some j. Then $I_j = A$, which contradicts the assumption that I_j is proper. Thus, $\bigcup_{i=1}^{\infty} I_n \in \Sigma$ and is an upper bound for the chain $I_1 \subseteq I_2 \subseteq ....$ Therefore, by Zorn's Lemma, Σ has a maximal element m. If m is not a maximal ideal, then there exists a proper ideal J such that $m \subset J$. Then, $J \in \Sigma$ and $m \subset J$, which contradicts the maximality of m. Thus, m is a maximal ideal. $\square$

Corollary 2.1. *If A is a ring and I is a proper ideal of A, then there exists a maximal ideal of A containing I.*

Corollary 2.2. *Let $x \in A$ be a nonunit. Then, there exists a maximal ideal containing x.*

Proposition 6. *Let A be a ring and let $I \neq A$ be an ideal of A such that every $x \in A - I$ is a unit in A. Then I is the unique maximal ideal of A.*

Proof. Let A be a ring and let $I \neq A$ be an ideal of A such that every $x \in A - I$ is a unit in A. By definition, I is the set of all nonunits in A. Every ideal which is not equal to the ring itself consists of nonunits, and is thus contained in I. Therefore, I is the only maximal ideal of A. □

The proof of the proposition above implies that there are some rings with multiple maximal ideals, and some rings with only one. We say that rings that only have one maximal ideal are local rings.

Definition 12 (Local Ring)**.** *A ring is said to be a local ring if it has only one maximal ideal.*

Example 12.1. *Examples of local rings:*

- *every field is a local ring with maximal ideal* (0)
- $\mathbb{Z}/p^n\mathbb{Z}$ *where* p *is prime is a local ring whose maximal ideal contains all multiples of* p

We can further characterize unique maximal ideals with the following proposition:

Proposition 7. *Let A be a ring and let m be a maximal ideal of A. If $1+x \in m$ is a unit for all $x \in m$, then m is the unique maximal ideal of A.*

Proof. Let x be a nonunit. If $x \notin m$, then $m + (x) = A$. Then, there exists $u \in m$ and $r \in A$ such that $u + rx = 1$. Thus, $1 - u = rx$. Thus, $1 - u$ is a unit which means rx is a unit. This in turn means x is a unit, which is a contradiction. Therefore $x \in m$. Thus, m contains all nonunits of A. By Proposition 6, m is the unique maximal ideal of A. □

2.3 Nilradical

Definition 13 (Nilradical)**.** *The nilradical N of a ring A is the set of all nilpotent elements in A.*

Proposition 8. *The nilradical N of a ring A is an ideal of A.*

Proof. Let N be the nilradical of A. If $x, y \in N$, then there exist $n, m \in \mathbb{N}$ such that $x^n = 0$ and $y^m = 0$. Then, $(x + y)^{n+m} = 0$ so that $x + y \in N$. If $x \in N$ and $r \in A$, then because $x^n = 0$, $(rx)^n = 0$ so that $rx \in N$. Therefore, N forms an ideal. □

Proposition 9. *The nilradical of a ring A is the intersection of all the prime ideals of A.*

Proof. Let $\bigcap p$ denote the intersection of all the prime ideals of A. Let $x \in A$ be nilpotent, and let p be a prime ideal. Then, $x^n \in p$ for some $n > 0$ and hence $x \in p$ (because p is prime). Therefore $x \in \bigcap p$. Conversely, suppose x is not nilpotent. Let Σ be the set of ideals with the property $x^n \notin I$ for each ideal I

and for all $n > 0$. Because $0 \in \Sigma$, Σ is nonempty. Let $I_1 \subseteq I_2 \subseteq ...$ be a chain in Σ. Thus, $\bigcup_{i=1}^{\infty} I_n$ is a proper ideal and $I \in \Sigma$. Thus, $\bigcup_{i=1}^{\infty} I_n$ is an upper bound for the chain. By Zorn's Lemma, Σ has a maximal element p. Let $xy \in p$. If $x \notin p$ and $y \notin p$, then $p + (x) \notin \Sigma$ and $p + (y) \notin \Sigma$. Thus, there exist n, m so that $x^n \in p + (x)$ and $x^m \in p + (y)$. It follows that $x^{n+m} \in p + (xy)$, hence the ideal $p + (xy) \notin \Sigma$ and therefore $xy \notin p$. Thus, there exists a prime ideal p such that $x \notin p$, so that $x \notin \bigcap p$. Therefore, the nilradical $N = \bigcap p$. □

2.4 Jacobson Radical

Now that we know that the intersection of a ring's prime ideals is its nilradical, a natural question is what can we say about the intersection of all its maximal ideals? We call this intersection the Jacobson radical, and we characterize it as follows.

Definition 14 (Jacobson Radical)**.** *The intersection of all maximal ideals $J = \bigcap m$ is an ideal and is called the Jacobson Radical*

Proposition 10. *$x \in J$ if and only if $1 - xy$ is a unit in A for all $y \in A$.*

Proof. ($\Longrightarrow$) Let $x \in J$. Then $x \in m$ for all maximal ideals m. For any $y \in A$, $1 - xy \notin m$ for all m. Thus, $1 - xy$ is a unit in A.

($\Longleftarrow$) Let $1 - xy$ be a unit in A for all $y \in A$. Suppose $x \notin m$ for some maximal ideal m. Then, $m + (x) = A$. Then, there exist, $u \in m$ and $y \in A$ such that $u + xy = 1$. Therefore $u = 1 - xy$ so that u is a unit, which is a contradiction. Thus x is in all maximal ideals. Therefore, $x \in J$. □

Corollary 2.3. *Let m be a maximal ideal and let $1 + x$ be a unit for all $x \in m$. Then, A is a local ring.*

Proof. Let $1 + x$ be a unit for all $x \in m$. Let y be a nonunit in A. Then $xy \in m$ so that $1 + xy$ is a unit. Then, $x \in J$ so that $m = J$. Thus, A is a local ring. □

Note: $1 \notin p$ for any prime ideal p.

2.5 Properties of Ideals

Now that we have investigated the properties of various ideals, we can perform operations on them. For the sake of brevity, we omit the proofs of these properties. [6]

Proposition 11. *Let I and J be ideals of ring A.*

- *$I \cup J$ is an ideal if and only if $I \subseteq J$ or $J \subseteq I$*
- *$I + J = \{x + y : x \in I, y \in J\}$ is an ideal of A*
- *$I \cap J = \{x \in A : x \in I, x \in J\}$ is an ideal of A*
- *IJ is defined to be the smallest ideal containing the set $\{xy : x \in I, y \in J\}$*

Examples of operations on two ideals:

- $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$
- $(m\mathbb{Z} + n\mathbb{Z})(m\mathbb{Z} \cap n\mathbb{Z}) = mn\mathbb{Z}$

Definition 15 (Coprime Ideals)**.** *Let I and J be ideals of ring A. If $I + J = A$, then I and J are called coprime.*

Definition 16 (Direct Product)**.** *Let A_1,...,A_n be rings. Their direct product $\prod_{i=1}^{n} A_i$ is the set of all sequences $x = (x_1, ..., x_n)$ with $x_i \in A_i$ and componentwise addition and multiplication. The direct product forms a commutative ring.*

Let A be a ring and let I_1,...,I_n be ideals of A. We will define a homomorphism $\phi : A \longrightarrow \prod_{j=1}^{n} A/I_j$ by the rule $\phi(x) = (x + I_1, ..., x + I_n)$.

Proposition 12. *Let A be a ring and let I_1,...,I_n be ideals of A.*

- *If I_i and I_j are coprime whenever $i \neq j$, then $\prod I_i = \bigcap I_i$*
- *ϕ is surjective $\iff$ I_i, I_j are coprime whenever $i \neq j$*
- *ϕ is injective $\iff \bigcap I_i = (0)$*

Proof. Let A be a ring and let I_1,...,I_n be ideals of A.

(i) We proceed by induction n. The statement is clearly true for $n = 2$. Suppose $n > 2$ and the result is true for I_1,...,I_{n-1}, and let $J = \prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$. Since $I_i + I_n = A = (1)$, we have equations $x_i + y_i = 1$ for $x_i \in I_i, y_i \in I_n$. Therefore, $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} 1 - y_i \equiv 1 \mod I_n$. Hence, $I_n + J = (1)$ and so $\prod_{i=1}^{n} I_i = J \cdot I_n = J \cap I_n = \cap_{i=1}^{n} I_i$.

(ii) ($\Longrightarrow$) Let us show that I_1 and I_2 are coprime. Assume ϕ is surjective. There exists $x \in A$ such that $\phi(x) = (1, 0, ..., 0)$. Thus $x \equiv 1 \mod I_1$ and $x \equiv 0 \mod I_2$ so that $1 = (1 - x) + x \in I_1 + I_2$.

($\Longleftarrow$) Assume I_i and I_j are coprime whenever $i \neq j$. It is enough to show that there exists an element $x \in A$ such that $\phi(x) = (1, 0, ..., 0)$. Since $I_1 + I_j = A = (1)$ for $j > 1$, we have equations $u_i + v_i = 1$, where $u_i \in I_1, v_i \in I_j$. Take $x = \prod_{i=2}^{n} v_i$. Then, $x = \prod 1 - u_i \equiv 1 \mod I_1$ and $x \equiv 0 \mod I_j$. Thus, $\phi = (1, 0, ..., 0)$.

(iii) The proof is trivial, since $\bigcap I_i$ is the kernel of ϕ. □

2.6 Properties of Prime Ideals

We now investigate two interesting properties of prime ideals.

Proposition 13. *Let P_1 and P_2 be prime ideals of ring A. If I is an ideal such that $I \subseteq P_1 \cup P_2$, then $I \subseteq P_1$ or $I \subseteq P_2$.*

Proof. Let $x \in I$. Assume I is an ideal such that $I \subseteq P_1 \cup P_2$. Suppose $I \nsubseteq P_1$. Then, there exists, $y \in I \setminus P_1$. Since $I \subseteq P_1 \cup P_2$, then $y \in P_2$. Consider the element $x+y \in I$. Suppose $x+y \in P_1$. If $x \in P_1$, then $(x+y)-x \in P_1$ so that $y \in P_1$, which is a contradiction. Thus $x \notin P_1$ and therefore $x \in P_2$. Therefore $I \subseteq P_2$. Suppose that $x+y \notin P_1$. Then $x+y \in P_2 \implies (x+y)-y \in P_2 \implies x \in P_2$. Therefore $I \subseteq P_2$. Thus, $I \subseteq P_1$ or $I \subseteq P_2$. □

This proof can be extended to n prime ideals using induction on n, which we leave as an exercise to the reader.

Proposition 14. *Let I_1,...,I_n be ideals of a ring A, and let P be a prime ideal containing $\cap_{j=1}^{n} I_j$. Then $P \supseteq I_j$ for some j.*

Proof. Suppose $P \not\supseteq I_j$ for all j. Then, there exists $x_i \in I_j$ so that $x_i \notin P$. Therefore $\prod x_i \in \prod I_j \subseteq \bigcap I_j$. But, because P is prime, $P \not\supseteq \bigcap I_j$, which is a contradiction. Therefore, $P \supseteq I_j$ for some j. □

Definition 17 (Ideal Quotient)**.** *Let I be an ideal and let S be any set in A. The ideal quotient is defined by $I : S = \{x \in A : xS \subseteq I\}$.*

In less formal terms, the ideal quotient takes an ideal I and "divides" it by the set S. Below are some properties of ideal quotients. We once again omit the proofs for brevity.

Proposition 15. *Let I be an ideal and let S be any set in A.*

- *If $S \subseteq I$, then $I : S = A$*
- *If $x, y \in I : S$, then $x + y \in I : S$*
- *If $x, y \in I : S$, then $xy \in I : S$*
- *If $x \in I : S$ and $a \in A$, then $xa \in I : S$*
- $I \subseteq I : S$
- $(I : J) : K = I : JK$
- $I(I : S) \subseteq I$
- $(I_1 \cap I_2) : S = (I_1 : S) \cap (I_2 : S)$

By the third and fourth properties above, we can conclude that $I : S$ forms a subring of A and that $I : S$ is an ideal of A.

Definition 18 (Radical of an Ideal)**.** *Let I be an ideal of ring A. The radical of I is defined by $r(x) = \{x \in A : x^n \in I, n \in N\}$*

The radical of an ideal is itself an ideal of A.

Proposition 16. *Some properties of the radical of an ideal:*

- $I \subseteq r(I)$

- *If $I \subseteq J$, then $r(I) \subseteq r(J)$*
- $r(r(I)) = r(I)$
- $r(I) = A$ *if and only if* $I = A$
- $r(IJ) = r(I \cap J) = r(I) \cap r(J)$
- $r(I + J) = r(r(I) + r(J))$
- *if P is prime, $r(P^n) = P$ for all $n > 0$*

Let $f : A \longrightarrow B$ be a ring homomorphism. Let I be an ideal A. $f(I)$ is not always an ideal of B. To solve this dilemma, we use a tool known as extension, which we define as follows:

2.7 Extension and Contraction of Ideals

Definition 19 (Extension)**.** *Let I be an ideal of A. We define the extension of I by $I^e = \{\Sigma_{i=1}^{n}(a_i \cdot f(x_i)) : a_i \in B, x_i \in I, n \in \mathbb{N}\}$*

In other words, the extension of ideal I is the ideal generated by $f(I)$ in B.

We have already seen that if $J \subseteq B$ is an ideal in B, then $f^{-1}(J)$ is an ideal in A. We call $f^{-1}(J)$ the **contraction** of ideal J, and denote it by J^c.

Proposition 17. *Let $f : A \longrightarrow B$ be a ring homomorphism. Let I be an ideal in A and J be an ideal in B. Then,*

- $(I^e)^c \supseteq I$
- $(J^c)^e \subseteq J$
- $I^{ece} = I^e$
- $J^{cec} = J^c$
- *If C is the set of all contracted ideals of A and E is the set of all extended ideals of B, then $C = \{I : I^{ec} = I\}$ and $E = \{J : J^{ce} = J\}$*

Proof. The first two facts are trivial, and the third and fourth follow from them. For the fifth statement, let $I \in C$. Then $I = J^c = J^{cec} = I^{ec}$. Conversely, if $I = I^{ec}$, then I is the contraction of I^e. The proof is similar for elements in E. □

3 Applications of Rings in Algebraic Geometry

Having studied the properties of rings and their various ideals, we will now present an application of this information in algebraic geometry. First we will cover some useful topological definitions which allow us to reach the desired applications. A knowledge of basic definitions in topology is assumed. [5]

Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E.

Proposition 18. *If I is the ideal generated by E, then $V(E) = V(I) = V(r(I))$*

Proof. By definition, $I = (E)$, so that any prime ideal containing E also contains I and vice versa. Thus, $V(E) = V(I)$. Any prime ideal containing $r(I)$ also contains I, so it suffices to show that $V(I) \supseteq V(r(I))$. Let $p \in V(I)$. If $x \in r(I)$, then $x^n \in I \subseteq p$ for some n. Because p is prime, $x \in p$, which completes the proof. □

Proposition 19. *$V(0) = X$ and $V(1) = \varnothing$.*

Proof. $V(0) = X$ is clear, as every ideal contains (0) as a subideal. Since no prime ideal contains 1 as an element, $V(1) = \varnothing$ is also clear. □

Consider the ideal generated by E_i, where $i \in I$ is any family of subsets of A. From the definitions of E and V, we can conclude that the set of all prime ideals of A which contain the union of all such E_i is in fact equal to the intersection of the sets of all prime ideals of A which contain E_i. More formally, $V(\bigcup_{i\in I} E_i) = \bigcap_{i\in I} V(E_i)$.

Proposition 20. *If $(E_i)_{i\in I}$ is any family of subsets of A, then $V(\bigcup_{i\in I} E_i) = \bigcap_{i\in I} V(E_i)$.*

Proof. Let prime ideal p contain $\bigcup_{i\in I} E_i$. Then, p contains E_i for all I, and thus $p \in \bigcap_{i\in I} V(E_i)$. Conversely, let $p \in \bigcap_{i\in I} V(E_i)$. Then p contains E_i for all I, which completes the proof. □

Proposition 21. *Let I and J be ideals of A. Then, $V(I \cap J) = V(IJ) = V(I) \cup V(J)$.*

Proof. The result follows immediately from the property of radicals $r(IJ) = r(I \cap J) = r(I) \cap r(J)$. □

From propositions 18-21, we have shown that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. This topology is known as the **Zariski topology**. [7] The topolocial space X is called the **prime spectrum** of A and is denoted by **Spec(A)**.

Let A be a ring. We will now consider the subspace of Spec(A) consisting of the maximal ideals of A, which with the induced topology, is called the **maximal spectrum** of A and is denoted by **Max(A)**.

Having covered the topological definitions above, we will round out the paper by looking by applying the concept of rings to elementary algebraic geometry. Once again, we assume some basic familiarity with the subject on the part of the reader. [4]

Let k be an algebraically closed field and let $\{f_\alpha(t_1, ..., t_n) = 0 : \alpha \in I\}$, where I is an index set, be a set of polynomial equations in n variables with coefficients in k. The set X of all points $x = (x_1, ..., x_n) \in k^n$ which satisfy these equations is called an **affine algebraic variety**. Consider the set of all polynomials $g \in k[t_1, ..., t_n]$ with the property that $g(x) = 0$ for all $x \in X$. This set is actually an ideal in the polynomial ring, called the **ideal of the**

variety X, and is denoted by $I(X)$. We can also observe that the quotient ring $P(X) = k[t_1, ..., t_n]/I(X)$ is the ring of polynomials functions on X. This is because two polynomials g, h define the same polynomial function on X if and only if $g - h \in I(X)$ (i.e. $g - h$ *vanishes* at every point of X). Let ϵ_i be the image of t_i in $P(X)$. The ϵ_i are called the **coordinate functions on X**. That is, if $x \in X$, then $\epsilon_i(x)$ is the ith coordinate of x. $P(X)$ is thus generated as a k-algebra by the coordinate function, and is referred to as the **coordinate ring**. With this information, we will first prove a version of Hilbert's Nullstellensatz, which is given below.

Theorem 3 (Hilbert's Nullstellentsatz)**.** *For each $x \in X$, let m_x be the ideal of all $f \in P(X)$ such that $f(x) = 0$, which is a maximal ideal of $P(X)$. There exists a bijective map $\mu : X \longrightarrow Y$, where Y equals Max($P(X)$) and $x \mapsto m_x$.*

Proof. We first show that μ is injective. If $x \neq y$, then there must exist $x_i \neq y_i$ for some i. Thus, $\epsilon_i - x_i$ is in m_x but not in m_y. Thus, $m_x \neq m_y$ so that μ is injective. To prove μ is surjective, we note that if k is an algebraically closed field, and an ideal I of $k[t_1, ..., t_n]$ is not the whole ring, then $Z(I) \neq \varnothing$. Thus, for a given maximal ideal m, there exists $x \in Z(m)$, which means $m_x \supseteq m$. By the maximality of m, we can see that $m_x \subseteq m$ is also true, so that $m_x = m$. Now we let m be the maximal ideal of $P(X)$. Notice that m is a maximal ideal of $k[t_1, ..., t_n]$ containing $I(X)$. By the above result, we can say this maximal ideal is m_x for some $x \in k^n$. Since $I(X) \subseteq m_x$, that means $x \in X$. Thus, any maximal ideal in $P(X)$ is given by m_x for some $x \in X$. Hence, μ is surjective, which completes the proof. □

The above version of Hilbert's Nullstellantz is mainly used for the purposes of commutative algebra. The more common form of the theorem is stated below for reference.

Theorem 4. *Let I be an ideal of the polynomial ring $k[x_1, ..., x_n]$. Let the algebraic set $V(I)$ of this ideal be defined by all n-tuples $x = (x_1, ..., x_n) \in k^n$ such that $f(x) = 0$ for all $f \in I$. If p is a polynomial in $k[x_1, ..., x_n]$ that vanishes on the algebraic set $V(I)$, then there exists $n \in \mathbb{N}$ such that $p^n \in I$.*

Let $f_1, ..., f_m$ be elements of $k[t_1, ..., t_n]$. These elements determine a **polynomial mapping** $\phi : k^n \longrightarrow k^m$ given by the following: if $x \in k^n$, then the coordinates of $\phi(x)$ are $f_1(x), ..., f_m(x)$. Let X and Y be affine algebraic varieties in k^n, k^m respectively. A map $\phi : X \longrightarrow Y$ is said to be *regular* if ϕ is the restriction to X of a polynomial mapping from k^n to k^m. If ς is a polynomial function on Y, then $\varsigma \circ \phi$ is a polynomial function on X. Thus, ϕ induces a k-algebra homomorphism $P(Y) \longrightarrow P(X)$, namely $\varsigma \mapsto \varsigma \circ \phi$.

Proposition 22. *There is a one-to-one correspondence between the regular mappings $X \longrightarrow Y$ and the k-algebra homomorphisms $P(Y) \longrightarrow P(X)$.*

Proof. Let $\phi : X \longrightarrow Y$ be a regular mapping. Then, $\phi = (\phi_1, ..., \phi_m)$, where $\phi_i \in k[t_1, ..., t_n]$. This is turn defines a mapping $P(Y) = k[t_1, ..., t_m] \longrightarrow$

$k[t_1, ..., t_m] = P(X)$ given by $g \mapsto g(\phi_1, ..., \phi_m)$. Let $\varphi : P(Y) \longrightarrow P(X)$ be a k-algebra homomorphism. We can now construct a regular map $\phi : X \longrightarrow Y$ given by $\phi = (\varphi(t_1), ..., \varphi(t_n))$. We now claim that these two maps are inverses, and thus there is a one-to-one correspondence between regular maps and k-algebra homomorphisms.

Observe that the image of the regular map ϕ is of the form $g \mapsto g(\phi_1, ..., \phi_m)$. In particular, t_i is mapped to ϕ_i. Thus, if we use the definition $\phi = (\varphi(t_1), ..., \varphi(t_n))$ to get a regular map $X \longrightarrow Y$, then the map will be ϕ itself. Now, if we are given $\varphi : P(Y) \longrightarrow P(X)$, then we get the regular map $(\varphi(t_1), ..., \varphi(t_n))$, which when composed with ϕ, is mapped to $g \mapsto g(\varphi(t_1), ..., \varphi(t_n)) = \varphi(g)$. Hence, the maps are inverses of one another, and therefore there is a one-to-one correspondence. □

This proposition, though simple in its statement, demonstrates a profound relationship between algebra and geometry. Given that there is a one-to-one correspondence between the regular mappings and k-algebra homomorphisms, we can conclude that there is a bijection that maps k-algebra homomorphisms to regular mappings, and vice versa. Though this is just a set-theoretic bijection so far, a remarkable result from algebraic geometry is that this statement can be extended so that finitely generated k-algebras and affine algebraic varieties are in fact categorically equivalent. This equivalence links algebraic operations on rings to the geometric properties of varieties, and thus is a powerful bridge between algebra and geometry themselves. Though the proof of this equivalence is outside the scope of this paper [2], it demonstrates a link between algebraic structures and geometric spaces which is fundamental for the field of algebraic geometry.

4 Acknowledgements

I would like to thank my mentor, Pranjal Warade, for her guidance and support throughout the REU program, and for helping me understand many of the concepts present in this paper (especially those regarding the applications of rings). I would also like to thank Peter May and everyone involved with the UChicago REU program for creating an excellent research experience.

References

[1] M.F. Atiyah and I.G. MacDonald. *Introduction to commutative algebra*. Westview Press, 1969.

[2] Mitchell Faulk. Equivalence of categories for affine varieties. *Columbia University*, 2014.

[3] David Harari. M1 algebra 2020-2021: Commutative rings. *Université Paris-Saclay*, 2020.

[4] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[5] J Peter May. Finite spaces and larger contexts. *Unpublished book*, 2016.

[6] Neal H McCoy. *Rings and ideals*, volume 8. American Mathematical Soc., 1948.

[7] James R Munkres. *Topology; a first course [by] james r. munkres*. Prentice-Hall, 1974.