ALGEBRAIC GEOMETRY

RITIK JAIN

1. INTRODUCTION

At its heart, algebraic geometry is the study of the vanishing of systems of polynomial equations

$$p_1(x_1, \cdots, x_n) = \cdots = p_m(x_1, \cdots, x_n) = 0.$$

Let us first consider the following classical problem in algebraic geometry: How many simultaneous solutions does a given system of polynomials have? That is, how many times do their graphs intersect?

For simple cases, i.e. when our polynomials have real coefficients and involve fewer than two variables, we can often answer this question by simple analytic methods. For instance, it is straightforward to show that the system

$$x^3 + 5x^2 + 8 - (x^2 + 2x + 1) = 0$$

has only one real solution simply by looking at the graphs of the functions and using a bit of calculus.

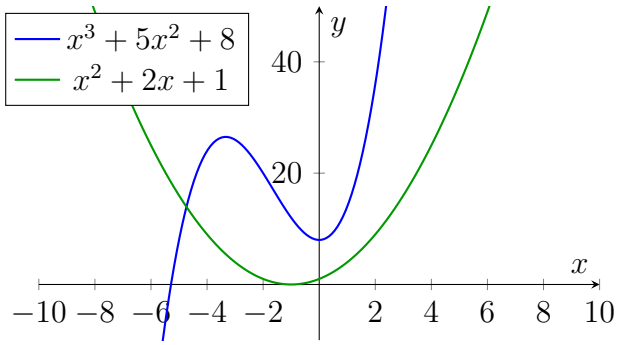


FIGURE 1. Graphs of $x^3 + 5x^2 + 8$ and $x^2 + 2x + 1$.

However, if we consider real polynomials in three or more variables, there is no way to see the graphs of the polynomials directly. Moreover, the graphs of such polynomials lie in $\mathbb{R}^n$ for $n > 1$, so the ordinary existence theorems in calculus (e.g. the Intermediate Value Theorem) no longer apply. More generally, if we wish to consider polynomials with coefficients in noncomplete fields, or in the extremal case, *finite fields*, the notion of

"geometry" in the ordinary sense totally breaks down, so we must rely on the algebraic data.

One fundamental piece of algebraic data that can be obtained from the set of polynomial equations p_i is their *total degrees* $\deg p_1, \cdots, \deg p_m$, which is the just the ordinary degree in the single-variable case.

In a certain special case, a landmark result dating back to the 18th century shows that the degrees indeed tell us quite a lot about the number of solutions of the p_i.

Theorem 1.1 (Bézout's Theorem)**.** *Let $f(x, y)$ and $g(x, y)$ be nonzero polynomials with complex coefficients of total degree m and n respectively with no common factors. Then, the system*

$$f(x, y) = g(x, y) = 0$$

has at most mn complex solutions. Moreover, if we count with multiplicity (and include points at infinity), then the total number of intersection points is exactly mn.

While solutions of polynomials systems is the basic starting point of algebraic geometry, it has grown far beyond these humble origins over the course of the 20th century.[1] In modern mathematics, it provides a complete, uniform framework for translating problems in abstract algebra, particularly those concerning *commutative rings*, to geometric problems, i.e. problems in topology and *scheme theory*, and vice versa.

Unfortunately, as algebraic geometry has advanced, it has become notorious for being fearsomely abstract and difficult to learn. In these notes, I hope to make clear the relatively simple constructions which form the backbone of the theory.

In Section 2, we will review some basic definitions and results from commutative algebra. Then, in Section 3, we will discuss the applications of algebraic geometry to the study of polynomial rings. Finally, in Section 4, we will introduce the prime spectrum of a ring as a first step towards scheme theory.

2. Preliminaries

2.1. Rings and Ideals.

We recall the definition of a ring:

Definition 2.1. A *ring* R is a set equipped with two operations

$$+ \colon R \times R \to R, \qquad \cdot \colon R \times R \to R,$$

called *addition* and *multiplication* satisfying the following axioms:

(i) Addition is associative and commutative, i.e. $(a+b)+c = a+(b+c)$ and $a+b = b+a$ for all $a, b, c \in R$.

[1] Today, the study of the solutions of polynomial systems is studied in *intersection theory*, an important subfield of modern algebraic geometry.

(ii) There exists an element $0_R \in R$ such that $a + 0_R = a$ for all $a \in R$. We call 0_R the *additive identity* of R.
(iii) For each $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0$.
(iv) Multiplication is associative and distributive, i.e. $(ab)c = a(bc)$, and

$$a(b+c) = ab + ac, \qquad (a+b)c = ac + bc$$

for all $a, b, c \in R$.
(v) There exists an element $1_R \in R$ such that $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$. We call 1_R the *multiplicative identity* of R.[2]

If a ring R also satisfies $ab = ba$ for all $a, b \in R$, it is called a *commutative ring*.

Example 2.2. The fundamental example of a ring is the set of integers $\mathbb{Z}$. Indeed, many familiar number systems are rings: for instance, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are all rings. For a noncommutative example, the set of $n \times n$ matrices over $\mathbb{R}$ is also a ring under addition and multiplication.

We can also form new rings from old rings.

Exercise 2.3. Show that for rings R, S, the Cartesian product

$$R \times S := \{(r, s) : r \in R, s \in S\}$$

is a ring under componentwise addition and multiplication.

Note that in the above definition of a ring, we do not require elements to have a *multiplicative inverse* in general. That is, for an element $a \in R$, there may not be an element a^{-1} such that $a \cdot a^{-1} = 1_R$. However, there is a special class of rings which satisfy this strong condition.

Definition 2.4. A *field* F is a commutative ring such that every nonzero element $a \in F$ has a multiplicative inverse; that is, there exists $a^{-1} \in F$ such that

$$aa^{-1} = 1.$$

Standard examples of fields include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. As is customary in algebraic geometry, we will henceforth use the symbol k rather than F to denote fields.

There is another important class of rings in which multiplication is nondegenerate, i.e. we cannot multiply nonzero elements and get zero.

Definition 2.5. A commutative ring R is called a *domain* if

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

[2]While some authors do not require rings to have 1, this axiom is essential in the vast majority of applications, including algebraic geometry. See [5].

We note that all fields are domains (why?), but an integral domain may not be a field. For instance, $\mathbb{Z}$ is clearly a domain, but no element in $\mathbb{Z} \setminus \{\pm 1\}$ has an inverse in $\mathbb{Z}$.

There are two types of subobjects in a given ring R: a *subring*, and an *ideal*. The former is simply a subset of R with a compatible ring structure, and the latter is defined as follows:

Definition 2.6. Let R be a ring. A subset $I \subseteq R$ is called an *ideal* if:

(i) $0_R \in I$,
(ii) $a, b \in I \implies a - b \in I$,
(iii) for all $r \in R$ and all $a \in I$, we have $ra \in I$.

In other words, ideals are additive subgroups of $(R, +)$ which are also closed under scalar multiplication by R.

Example 2.7. For a ring R and an element $x \in R$, the set

$$(x) := xR = \{xr \mid r \in R\}$$

is an ideal of R, called the *principal ideal generated by* x. One can show that every ideal of $\mathbb{Z}$ is of this form (n) for some integer $n \in \mathbb{Z}$. In any field k, the only ideals are (0) and $(1) = k$.

Some technicalities arise when one considers ideals in a noncommutative ring. For instance, in a noncommutative ring, we need to distinguish between *left ideals* and *right ideals*, and consequentially the algebra of ideals is more complex. Luckily for us, algebraic geometry deals almost exclusively with commutative rings, so we will henceforth assume all rings are commutative.

One application of ideals is their use in the construction of *quotient rings*.

Definition 2.8. Let R be a ring and $I \subseteq R$ an ideal. The *quotient ring* R/I is the set

$$R/I = \{a + I : a \in R\},$$

where

$$a + I = \{a + x : x \in I\}.$$

Addition and multiplication are defined by

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I)(b + I) = ab + I.$$

That is, R/I is R modulo the equivalence relation $a \sim b$ if and only if $a - b \in I$. One can verify that these operations are well-defined and make R/I into a ring.

Example 2.9. For an integer $n \geq 2$, the quotient ring $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \cdots, \overline{n-1}\}$ is called *the integers modulo* n. If p is prime, one can verify that $\mathbb{Z}/p\mathbb{Z}$ is indeed a field. That is, for every $a \in \mathbb{Z}$ there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{p}$.

We now define some important operations on ideals.

Proposition 2.10. *Let R be a commutative ring and let $I, J \subseteq R$ be ideals. Then:*

(i) The intersection $I \cap J$ is an ideal.
(ii) The sum *$I + J := \{x + y \mid x \in I, y \in J\}$ is also an ideal.*
(iii) The product *$IJ := \{x_1y_1 + \cdots + x_ny_n \mid n \geq 1,\ x_i \in I,\ y_i \in J\}$ is an ideal.*

Proof. Exercise. □

Remark 2.11. In general, the union $I \cup J$ of two ideals is not an ideal, since it may not be closed under addition. For the same reason, the set $\{xy \mid x \in I, y \in J\}$ is not an ideal in general, so as tempting as it may be to define IJ in this way, we cannot do so.

There are two types of ideals which are especially important.

Definition 2.12 (Prime and Maximal Ideals)**.** (i) A proper ideal $P \subsetneq R$ is called *prime* if

$$ab \in P \implies a \in P \text{ or } b \in P.$$

(ii) A proper ideal $M \subsetneq R$ is called *maximal* if there is no ideal I such that $M \subsetneq I \subsetneq R$.

The first condition generalizes the familiar property of prime numbers, namely, for any prime p, $p \mid ab$ implies $p|a$ or $p \mid b$. In terms of ideals, this means $ab \in p\mathbb{Z}$ implies $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

We can also define prime and maximal ideals in terms of the quotients they induce.

Exercise 2.13. For an ideal $I \subseteq R$, show that (i) I is prime if and only if R/I is an integral domain, and (ii) I is maximal if and only if R/I is a field.

In particular, this exercise shows that all maximal ideals are prime, but the converse does not hold in general.

2.2. **Ring homomorphisms.** In the same way that we can define functions of vector spaces which preserve linearity (namely, linear maps), we can define functions of rings which preserve ring structure.

Definition 2.14. A function $f : R \to S$ between rings is called a *ring homomorphism* if for all $a, b \in R$, we have

- $f(a + b) = f(a) + f(b)$,
- $f(ab) = f(a)f(b)$,
- $f(1_R) = 1_S$.

If f is bijective, it is called an *isomorphism*.

Definition 2.15. We call two rings R, S *isomorphic* if there exists an isomorphism $\phi : R \to S$. In this case, we write $R \cong S$.

One can easily verify that the inverse of an isomorphism is also an isomorphism, so the relation $\sim$ on the class of rings given by

$$R \sim S \iff R \cong S$$

is an equivalence relation. Therefore, if R and S are isomorphic, then they are essentially the same as rings.

As in linear algebra, we can also define kernels and images of ring homomorphisms.

Definition 2.16. For a ring homomorphism $f : R \to S$, we define the *kernel of* f as

$$\ker f := \{r \in R \mid f(r) = 0_S\},$$

and we define the *image of* R *under* f as

$$\operatorname{Im} f := \{f(r) \mid r \in R\}.$$

Exercise 2.17. Show that for a ring homomorphism $f : R \to S$, the kernel of f is an ideal of R, and the image of R under f is a subring of S.

Example 2.18. For an ideal I of a ring R, the *natural map*

$$\pi : R \to R/I, \qquad r \mapsto r + I$$

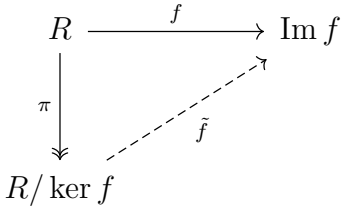
is a well-defined ring homomorphism. One can show that $\operatorname{Im} \pi = R/I$, i.e. π is surjective, and $\ker \pi = I$.

In the above example, we see that R can be made to be isomorphic to its image under a ring homomorphism by quotienting out the kernel. We conclude this subsection with the following useful result, which shows that this is true in general.

Theorem 2.19 (First Isomorphism Theorem)**.** *If $f : R \to S$ is a ring homomorphism, then*

$$R/\ker f \cong \operatorname{Im} f.$$

That is, there exists an isomorphism $\tilde{f}$ such that the following diagram commutes:



Proof. Exercise. Hint: Show that the map $\tilde{f} : r \mapsto f(r + \ker f)$ is a well-defined isomorphism $R/\ker f \to \operatorname{Im} f$. □

2.3. **Rings of Polynomials.** In this subsection, we will discuss rings of polynomials, which as alluded to in Section 1, are the basic starting point of algebraic geometry.

Throughout this section, we take R to be a commutative ring.

Definition 2.20. The *ring of polynomials in one variable over* R, denoted $R[X]$, is the set of all formal expressions

$$f(X) = a_n X^n + \cdots + a_1 X + a_0, \qquad a_i \in R,$$

with addition and multiplication defined by the usual rules.

With these operations, $R[X]$ is a commutative ring, and R embeds into $R[X]$ as the subring of constant polynomials.

More generally, we may introduce several indeterminates.

Definition 2.21. For $n \geq 1$, the *polynomial ring in* n *variables over* R is

$$R[X_n] := R[X_1, \ldots, X_n],$$

whose elements are finite sums of monomials

$$a X_1^{\alpha_1} \cdots X_n^{\alpha_n}, \qquad a \in R,\ \alpha_i \in \mathbb{N}.$$

Polynomial rings preserve important algebraic properties.

Proposition 2.22. *If R is an integral domain, then $R[X]$ is an integral domain.*

Proof. If $f, g \in R[X]$ are nonzero, their leading coefficients are nonzero, and the leading coefficient of fg is the product of these coefficients. Since R has no zero divisors, this product is nonzero, so $fg \neq 0$. □

We will now study ideals of polynomial rings, specializing to the case where the coefficients lie in a field. We start with the following important result.

Theorem 2.23. *If k is a field, then every ideal of $k[X]$ is principal. That is, every ideal is of the form*

$$(f) = \{f(X)g(X) \mid g \in k[X]\}.$$

In fact, the above theorem holds if and only if k is a field. There is also a strikingly simple characterization of prime ideals over a field.

Proposition 2.24. *Let k be a field and let $f(X) \in k[X]$ be nonconstant. Then, the principal ideal (f) is maximal if and only if $f(X)$ is irreducible, i.e. f is nonconstant and does not factor as the product of two nonconstant polynomials.*

Thus, in $k[X]$, irreducible polynomials play the same role as prime numbers in $\mathbb{Z}$. Note that in both $k[X]$ and $\mathbb{Z}$, the prime ideals and maximal ideals are exactly the same. This is because both are examples of *principal ideal domains* (PIDs), which are a particularly nice sort of ring. However, we do not have this equivalence in general.

While the above characterization tells us that prime ideals in $k[X]$ are "simple" in the sense of being principal, it is not always obvious which polynomials are irreducible and which are not, so it may be nontrivial to check if an ideal is prime. For instance, who could tell *a priori* that the ideal

$$(7X^5 + 21X^4 - 42X^3 + 63X^2 + 105X - 21) \in \mathbb{Q}[X]$$

is prime?[3] In the case that k is particularly "nice," we have a very simple characterization of irreducible polynomials, and therefore of prime ideals.

Definition 2.25. A field k is called *algebraically closed* if every nonconstant polynomial

$$f(X) \in k[X]$$

has a root in k. Equivalently, k is algebraically closed if every polynomial of degree n in $k[X]$ has n roots, counted with multiplicity.

An important example is the complex numbers $\mathbb{C}$, which form an algebraically closed field by the Fundamental Theorem of Algebra.

Proposition 2.26. *Let k be algebraically closed. Then, a polynomial in $k[X]$ is irreducible if and only if it is linear. Equivalently, every prime ideal in $k[X]$ is of the form*

$$(X - a) = \{g(X)(X - a) \mid g \in k[X]\}.$$

Proof. Exercise. □

Thus, for an algebraically closed field k, prime/maximal ideals in $k[X]$ are precisely given by the linear polynomials $(X - a)$ for $a \in k$. In particular, the set of all prime ideals can be identified with k via the mapping $a \mapsto (X - a)$. As this observation suggests, algebraically closed fields are the simplest setting for algebraic geometry, and indeed, much of the classical theory takes place there.

3. Affine Varieties

As we mentioned in the introduction, modern algebraic geometry provides a comprehensive framework for studying rings geometrically, and for studying geometric objects using ring theory. The fundamental observation which set researchers in this direction was that many questions regarding systems of polynomial equations in n variables over a field k can be solved by studying the entire ring of polynomials $k[X_n]$ over k in n variables,

[3] The easiest way to verify that this polynomial is irreducible is by using *Eisenstein's Criterion*.

or, more generally, by studying quotients of this ring. In this section, we will describe this methodology precisely. We take k is a field throughout this section.

3.1. **Affine Algebraic Sets and Radical Ideals.** We begin with a fundamental definition.

Definition 3.1 (Affine Algebraic Sets)**.** A subset $V \subseteq k^n$ is called an *affine algebraic set* if V is the set of common zeros for some set of polynomials $S \subseteq k[X_n]$. In this case, we say that V is the *vanishing set*, or the *locus* of S, and we denote V by $V(S)$. If $S = \{f_1, \cdots, f_n\}$ has finitely many elements, we denote the vanishing set of S by $V(f_1, \cdots, f_n)$.

Example 3.2. The affine algebraic subsets of k are precisely the finite subsets of k, along with k. However, affine algebraic subsets are not always finite in k^n. For instance, the unit circle S^1 is an algebraic subset of $\mathbb{R}^2$, since it is the vanishing set of $x^2 + y^2 - 1$.

As the following proposition shows, the function $V(\cdot)$ satisfies some natural properties.

Proposition 3.3. *Let $A, B \subseteq k[X_n]$. The following properties hold.*

(1) If $A \subseteq B$, then

$$V(A) \subseteq V(B).$$

That is, $V(\cdot)$ is order-reversing *with respect to inclusion.*

(2) We have $V(A) \cap V(B) = V(A \cup B)$. More generally, for any index set J, we have

$$\bigcap_{j \in J} V(S_j) = V\left(\bigcup_{j \in J} S_j\right).$$

(3) For ideals I, J, we have $V(I) \cup V(J) = V(IJ)$.

(4) If $I = (A)$ is the ideal generated by A, then $V(A) = V(I)$.

By the last property, we have that all algebraic subsets of k^n are secretly the vanishing set of some ideal $I \subseteq k[X_n]$. That is, the mapping

$$V : \ \{\text{ideals } I \subseteq k[x_1, \ldots, x_n]\} \ \longrightarrow \ \{\text{algebraic subsets } V \subseteq k^n\}$$

is surjective. Note that the mapping $V : I \mapsto V(I)$, however, is not injective in general: there may be many ideals I which have the same vanishing set. For instance, the ideals $(x), (x^2), (x^3), \cdots$ all have the same vanishing set, namely, $\{0\}$. In order to make this mapping injective, we must restrict ourselves to *radical ideals*, which are defined as follows.

Definition 3.4 (Radical Ideals)**.** Let $I \subseteq R$ be an ideal in a commutative ring R. Then, the *radical* of I is defined as the set

$$\sqrt{I} := \{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}\}.$$

An ideal $I \subseteq R$ is called a *radical ideal* if $I = \sqrt{I}$.

That is, $\sqrt{I}$ is the set obtained by extending I to include all nth roots. One can check that this is an ideal in general. It also satisfies many nice properties.

Proposition 3.5. *(1) The arbitrary intersection of radical ideals is radical.*
(2) For any ideal I, we have $\sqrt{\sqrt{I}} = \sqrt{I}$.
(3) Prime ideals are radical. More generally, for any ideal $I \subseteq R$, we have

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$

That is, $\sqrt{I}$ is the intersection of all prime ideals containing I.

Proof. We will verify (3). First, for a prime ideal $\mathfrak{p}$ in a commutative ring R, we will show that $\sqrt{\mathfrak{p}} = \mathfrak{p}$. First, the inclusion $\mathfrak{p} \subseteq \sqrt{\mathfrak{p}}$ is clear from the definition of a radical ideal. Conversely, suppose $x \in \sqrt{\mathfrak{p}}$, so $x^n \in \mathfrak{p}$ for some $n \geq 1$. Then, since $\mathfrak{p}$ is prime, and

$$x^n = x \cdot x^{n-1} \in \mathfrak{p},$$

it follows that $x \in \mathfrak{p}$ or $x^{n-1} \in \mathfrak{p}$. Repeating this argument $n-1$ times yields $x \in \mathfrak{p}$, hence $\sqrt{\mathfrak{p}} = \mathfrak{p}$ as desired.

Now, we will show that for any ideal $I \subseteq R$, we have that $\sqrt{I}$ is the intersection of all prime ideals containing I. Let $x \in \sqrt{I}$, so that $x^n \in I$ for some $n \geq 1$. Then, if $\mathfrak{p}$ is any prime ideal containing I, it follows that $x^n \in \mathfrak{p}$, so by the previous argument, we obtain $x \in \mathfrak{p}$. As this holds for every $x \in \sqrt{I}$ and every prime ideal $\mathfrak{p} \supseteq I$, we conclude that

$$\sqrt{I} \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$

For the sake of brevity, we omit the proof of the reverse inclusion and refer the reader to [1, Ch. 15, Prop. 12]. □

Many common examples of radical ideals are in fact prime ideals, however, a radical ideal may not be prime. For instance, in $\mathbb{Z}$, an ideal (a) is radical if and only if $a = 0$ or a is squarefree. Thus, in particular, $(6) \subseteq \mathbb{Z}$ is a radical ideal, but since $\mathbb{Z}/6\mathbb{Z}$ is not a domain, it is not prime.

The following fundamental result in algebraic geometry, Hilbert's Nullstellensatz, shows that over algebraically closed fields, there is a rigid correspondence between affine algebraic sets and radical ideals.

Theorem 3.6 (Hilbert's Nullstellensatz)**.** *For an algebraic subset $V \subseteq k^n$, let $I(V) \subseteq k[X_n]$ denote the ideal of polynomials vanishing on V. Then, if k is algebraically closed, there is a bijective,*

order-reversing correspondence

(1)
$$\left\{ \text{ Radical ideals } J \subseteq k[X_n] \right\} \underset{I(V)\longleftarrow V}{\overset{J\longmapsto V(J)}{\rightleftarrows}} \left\{ \text{ Affine algebraic subsets } V \subseteq k^n \right\}$$

In particular, for any ideal $I \subseteq k[X_n]$ and any affine algebraic subset $V \subseteq k^n$, we have

$$I(V(I)) = \sqrt{I}, \qquad V(I(V)) = V,$$

and

(2)
$$I_1 \subseteq I_2 \implies V(I_2) \subseteq V(I_1), \qquad V_1 \subseteq V_2 \implies I(V_2) \subseteq I(V_1).$$

Remark 3.7. The order-reversing relation (2) is true over a general field. Indeed, if $I_1 \subseteq I_2$, then every common zero of the polynomials I_2 must also be a common zero of the polynomials in I_2, so $V(I_2) \subseteq V(I_1)$. On the other hand, if $V_1 \subseteq V_2$, then the ideal of polynomials $I(V_2)$ must be a subset of $I(V_1)$, since vanishing on V_2 is a stronger condition than vanishing on a smaller set V_1.

While the above formulation is very satisfying on an abstract level, we note that there is a more intuitive way to state the Nullstellensatz:

Proposition 3.8. *Theorem 3.6 is equivalent to the assertion that if k is algebraically closed, then every proper ideal $I \subset k[x_1, \ldots, x_n]$ has a common zero in k^n.*

Proof. First, assume Theorem 3.6. Then, for a proper ideal I, if $V(I) = \varnothing$, then

$$I(V(I)) = I(\varnothing) = k[x_1, \ldots, x_n],$$

hence $\sqrt{I} = k[x_1, \ldots, x_n]$, which implies $I = k[x_1, \ldots, x_n]$, a contradiction. Therefore $V(I) \neq \varnothing$, so every proper ideal has a zero.

Conversely, if every proper ideal $I \subset k[x_1, \ldots, x_n]$ has a common zero in k^n, one can show that

$$I(V(I)) = \sqrt{I}$$

using the technique of *localization*. However, since this lies beyond the scope of these notes, we omit the full proof. □

In these terms, the Nullstellensatz states that a set of polynomials $f_1, \cdots, f_m \in k[X_n]$ over an algebraically closed field is guaranteed to have a common zero under a very mild algebraic condition: namely, that the f_i do not generate the entire ring of polynomials. Indeed, this is how the Nullstellensatz (which translates to Zeros Theorem in English), earned its name.

The bijection between algebraic subsets in k^n and radical ideals in $k[X_n]$ given in Theorem 3.6 is but one manifestation of the more general *algebra-geometry* correspondence. As we will see, there are other such bijections between algebraic objects in $k[X_n]$ and geometric objects in k^n, particularly when k is algebraically closed. Another salient example is the following corollary of the Nullstellensatz:

Theorem 3.9 (Weak Nullstellensatz)**.** *If k is algebraically closed, there is a bijective, order-reversing correspondence*

$$\text{(3)} \qquad \left\{ \textit{ Maximal ideals } \mathfrak{m} \subseteq k[X_n] \right\} \underset{I(x) \longleftarrow x}{\overset{\mathfrak{m} \longmapsto V(\mathfrak{m})}{\rightleftarrows}} \left\{ \textit{ Points } x \in k^n \right\}$$

Proof. First, since maximal ideals $\mathfrak{m}$ are radical, Theorem 3.6 implies

$$I(V(\mathfrak{m})) = \mathfrak{m}.$$

Moreover, since $\mathfrak{m}$ is proper and maximal, $V(\mathfrak{m})$ is nonempty and cannot contain more than one point. Indeed, if $a, b \in V(\mathfrak{m})$ with $a \neq b$, then

$$\mathfrak{m} \subseteq I(\{a\}) = (x_1 - a_1, \ldots, x_n - a_n),$$

and since $I(\{a\})$ is maximal, this forces $\mathfrak{m} = I(\{a\})$, contradicting $b \in V(\mathfrak{m})$. Thus, $V(\mathfrak{m}) = \{a\}$ for some $a \in k^n$, and

$$\mathfrak{m} = I(\{a\}) = (x_1 - a_1, \ldots, x_n - a_n).$$

Conversely, for $a = (a_1, \ldots, a_n) \in k^n$, the ideal

$$I(a) = (x_1 - a_1, \ldots, x_n - a_n)$$

is the kernel of the evaluation map $k[X_n] \to k,\ f \mapsto f(a)$, so by the First Isomorphism Theorem, $k[X_n]/I(a) \cong k$. That is, $I(a)$ is maximal, so we obtain the result. □

In the next section, we will see even more correspondences between algebraic and geometric objects.

3.2. **The Zariski Topology and Coordinate Rings.** In this section, we will construct the *Zariski topology*, which turns out to be the correct topological structure on k^n for algebraic geometry. It is defined, quite naturally, as follows.

Definition 3.10 (Zariski Topology)**.** The *Zariski topology* on k^n is the topology τ in which the closed sets are precisely the affine algebraic sets. We call the topological space (k^n, τ) the *affine n-space over k*, and denote it by $\mathbb{A}^n_k$ or $\mathbb{A}^n$ when there is no ambiguity.

Example 3.11. The closed sets in the Zariski topology on k are precisely the finite sets, so in this case, the Zariski topology is the *cofinite topology* on k.

In general, the Zariski topology on k^n is T_1, meaning that points are closed, but unlike most commonly encountered topological spaces, it is not Hausdorff in general.

Remark 3.12. Many algebraic properties of $k[X_n]$ are naturally encoded in the geometry/topology of $\mathbb{A}^n_k$. For instance, Hilbert's Basis Theorem in commutative algebra [4, Thm. 2.7] states that every ideal in $k[X_n]$ is finitely generated. Using the Nullstellensatz, this implies that every algebraic subset of k^n is of the form $V(f_1, \cdots, f_n)$ for finitely many polynomials $f_1, \cdots, f_n \in k[X_n]$. Put another way, every closed subset in $\mathbb{A}^n_k$ is the intersection of finitely many sets of the form $V(f_i)$.

Now that we have seen the Zariski topology on k^n and its subsets, it is natural to ask, what do the Zariski-continuous functions look like? However, unlike in analysis, continuity in the Zariski topology is too weak of a condition to be meaningful. For instance, any injective function $f : \mathbb{A}^1_k \to \mathbb{A}^1_k$ is automatically continuous, since the preimage of any point under such a map is either a point or the empty set. More precisely, the Zariski topology is very *coarse*, meaning there are few open sets, so it is easy for a map to be Zariski-continuous.

As it turns out, the correct morphisms in the Zariski topology are the *regular maps*. In addition to being continuous, they satisfy a certain natural correspondence (Theorem 3.17). First, we define the *coordinate ring* of an affine algebraic set V, which is exactly the ring of regular maps on V.

Definition 3.13 (Coordinate ring)**.** Let $V \subseteq k^n$ be an affine algebraic set. The *coordinate ring* of V is the quotient ring

$$k[V] := k[X_n]/I(V),$$

where $I(V)$ denotes the ideal of polynomials in $k[x_1, \ldots, x_n]$ that vanish on V.

From the above definition, it is not immediately obvious why each $[f] \in k[V]$ can be interpreted as a function on V. The reason is as follows: two polynomials $f, g : k^n \to k$ define the same function on V precisely when $f - g \equiv 0$ on V: that is, when $f - g \in I(V)$. Therefore, each

$$[f] \in k[x_1, \ldots, x_n]/I(V)$$

represents a unique function on V. For instance, for $V = \mathbb{A}^n$, we have

$$k[\mathbb{A}^n] = k[X_n]/I(\mathbb{A}^n) = k[X_n]/(0) \cong k[X_n],$$

so the coordinate ring construction agrees with our intuition.

Note that coordinate rings are k-algebras (k-vector spaces with multiplication), so we may consider k-algebra homomorphisms $k[W] \to k[V]$ between coordinate rings. We

will now define *morphisms* $V \to W$ of affine algebraic sets, and as we will see, these will correspond naturally to k-algebra homomorphisms $k[W] \to k[V]$.

Definition 3.14. Let $V \subseteq \mathbb{A}_k^n$ and $W \subseteq \mathbb{A}_k^m$ be affine algebraic sets. A map $\varphi : V \to W$ is called a *morphism* (or *regular map*) if there exist polynomials $f_1, \ldots, f_m \in k[X_n]$ such that

$$\varphi(\alpha) = \big(f_1(\alpha), \ldots, f_m(\alpha)\big)$$

for all $\alpha \in V$. Equivalently, φ is a morphism if for all $f \in k[W]$, we have $f \circ \varphi \in k[V]$. We say that φ is an *isomorphism* $V \to W$ if there exists an inverse morphism $\psi : W \to V$ of φ.

We now show that the ring of regular functions on an affine algebraic set is given precisely by its coordinate ring.

Proposition 3.15. *Let $V \subseteq \mathbb{A}_k^n$ be an affine algebraic set. Then the ring of regular functions $V \to \mathbb{A}_k^1$ is naturally isomorphic to*

$$k[V] = k[X_n]/I(V).$$

Proof. First, by the definition of a morphism, a regular function $f : V \to \mathbb{A}_k^1$ is given by a polynomial $g \in k[X_n]$ such that

$$f(x) = g(x) \quad \text{for all } x \in V.$$

On the other hand, every polynomial defines a regular function on V by restriction, giving a ring homomorphism

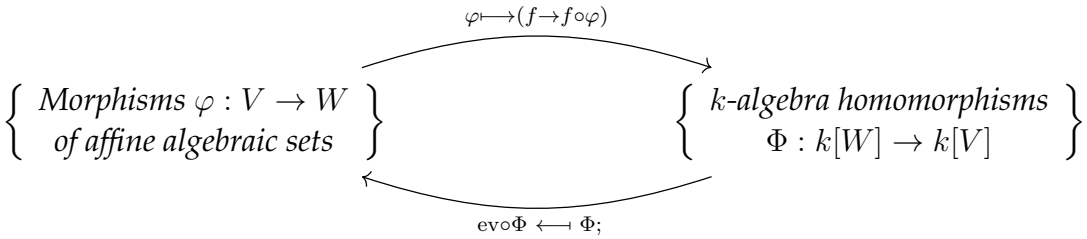
$$\Phi : k[X_n] \longrightarrow \mathrm{Reg}(V, \mathbb{A}_k^1), \qquad F \mapsto F|_V,$$

where $\mathrm{Reg}(V, \mathbb{A}_k^1)$ is the ring of regular functions $V \to \mathbb{A}_k^1$. But here, two polynomials define the same function on V exactly when their difference vanishes on V, so $\ker \Phi = I(V)$, and the result follows from the First Isomorphism Theorem. □

Remark 3.16. Regular maps of affine algebraic sets are naturally analogous to *smooth maps* in differential geometry. In particular, for smooth manifolds M, N with open subsets $U \subseteq M$, $V \subseteq N$, a map $\varphi : U \to V$ is smooth if and only if for all smooth functions $f \in C^\infty(V)$, we have that $f \circ \varphi \in C^\infty(U)$. Similarly, a map $\varphi : V \to W$ of affine algebraic sets is regular if and only if we can pull back every polynomial function $f \in k[W]$ to a polynomial function $f \circ \varphi \in k[V]$.

As it turns out, there is a bijective correspondence between regular maps $V \to W$ and k-algebra homomorphisms $k[W] \to k[V]$.

Theorem 3.17. *Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine algebraic sets. Then there is a bijective correspondence*



More precisely:

(1) Every morphism $\varphi : V \to W$ induces a k-algebra homomorphism

$$\varphi^* : k[W] \to k[V], \qquad \varphi^*(f) = f \circ \varphi.$$

(2) Every k-algebra homomorphism $\Phi : k[W] \to k[V]$ is of the form $\Phi = \varphi^* = f \circ \varphi$ for a unique morphism

$$\varphi : V \to W, \qquad \varphi(a) = \big((\Phi y_1)(a), \ldots, (\Phi y_m)(a)\big),$$

where $y_1, \ldots, y_m$ are the coordinate functions on W.

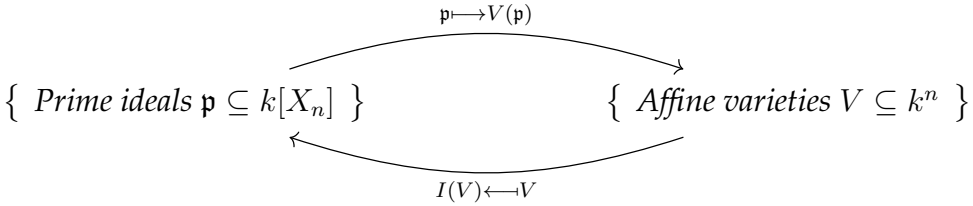
In particular, this correspondence allows us to construct regular maps $V \to W$ between affine algebraic subsets by solely considering k-algebra homomorphisms $k[W] \to k[V]$. Since it is often easier to work with $k-$algebras, this correspondence is often useful.

3.3. **Affine Varieties.** We conclude this section by discussing a particularly important class of affine algebraic sets called *affine varieties*.

Definition 3.18 (Affine Varieties)**.** An algebraic set $V \subseteq k^n$ is called an *affine variety* if it cannot be written as the union $V = V_1 \cup V_2$ of two proper affine algebraic subsets of V.

That is, affine varieties are the irreducible "building blocks" of more general affine algebraic sets, in exactly the same way that prime ideals are the building blocks of more general ideals. In particular, the bijection (1) given by the Nullstellensatz restricts to the following equivalence:

Theorem 3.19. *If k is algebraically closed, there is a bijective, order-reversing correspondence*



Proof. First, suppose $\mathfrak{p} \subset k[X_n]$ is prime, and let

$$V(\mathfrak{p}) = V_1 \cup V_2$$

for affine algebraic subsets $V_i = V(I_i)$. Then, by Proposition 3.3,

$$V(\mathfrak{p}) = V(I_1) \cup V(I_2) = V(I_1 I_2).$$

Then, by the Nullstellensatz,

$$\mathfrak{p} = I(V(\mathfrak{p})) = I(V(I_1 I_2)) = \sqrt{I_1 I_2},$$

hence $I_1 I_2 \subseteq \mathfrak{p}$. Now, since $\mathfrak{p}$ is prime, this implies $I_1 \subseteq \mathfrak{p}$ or $I_2 \subseteq \mathfrak{p}$, hence $V(\mathfrak{p}) = V_1$ or $V(\mathfrak{p}) = V_2$. Thus, $V(\mathfrak{p})$ is irreducible.

Conversely, suppose that V is an affine variety. Then, if $f \cdot g \in I(V)$, we have $V \subseteq V(f) \cup V(g)$. But since V is irreducible, this implies $V \subseteq V(f)$ or $V \subseteq V(g)$, hence $f \in I(V)$ or $g \in I(V)$. That is $I(V)$ is prime as desired.

Moreover, note that the maps $I(-)$ and $V(-)$ are inverse, since for prime $\mathfrak{p}$,

$$I(V(\mathfrak{p})) = \sqrt{\mathfrak{p}} = \mathfrak{p},$$

and for an affine variety V,

$$I(V(I(V))) = \sqrt{I(V)} = I(V),$$

hence $V(I(V)) = V$. Finally, the correspondence is order-reversing by Proposition 3.3, so the result is obtained. □

Like prime ideals, affine varieties enjoy some special properties which their more general counterparts do not. For instance, their coordinate rings are integral domains. Indeed, affine varieties may be defined by this property:

Proposition 3.20. *An affine algebraic subset $V \subseteq k^n$ is an affine variety if and only if its coordinate ring*

$$k[V] = k[X_n]/I(V)$$

is an integral domain.

Proof. First, suppose that V is an affine variety. Then, by Theorem 3.19, $I(V)$ is a prime ideal, so clearly, $k[V] = k[X_n]/I(V)$. Conversely, suppose that V is not an affine variety, so there exists proper algebraic subsets V_1, V_2 of V such that $V = V_1 \cup V_2$. Then, we can find f_1, f_2 such that $f_i \equiv 0$ on V_i, but f_1 does not vanish on all of V_2 and f_2 does not vanish on all of V_1. Then, $f_1, f_2 \notin I(V)$, but their product $f_1 \cdot f_2$ vanishes on all of V. Then, $f_1 \cdot f_2 \in I(V)$, hence $I(V)$ is not a prime ideal. □

One application of Proposition 3.20 is that we can consider rational functions f/g on affine varieties.

Definition 3.21. For an affine variety V, we call the field of fractions

$$k(V) := \mathrm{Frac}(k[V])$$

the *function field* of V.

The function field of a variety is an important invariant for several reasons. For one, it allows us to define the *dimension* of a variety V, which is defined to be the transcendence degree of $k(V)$ over k. For example, if $V = \mathbb{A}^n_k$, we have that $k[\mathbb{A}^n_k] = k[X_n]$, thus

$$k(V) = \mathrm{Frac}(k[X_n]) = k(x_1, \cdots, x_n),$$

which has transcendence degree n over k. Therefore, $\dim \mathbb{A}^n_k = n$.

One can also classify varieties via function fields. We call two varieties V, W *birationally equivalent* if they have isomorphic function fields, which guarantees that V and W are isomorphic "almost everywhere." This perspective is useful since, by *Chow's lemma*, every variety V has a nice birationally equivalent counterpart W, so it essentially suffices to only work with nice varieties.[4]

In this section, we have studied the correspondence between the ring structure of $k[X_n]$ and the topology of $\mathbb{A}^n_k$. A highlight of our investigation was the Nullstellensatz (Theorem 3.6) which establishes a strong connection between radical ideals and affine algebraic subsets. In the next section, we generalize the relationship between ideals and algebraic subsets by associating a geometric space to an arbitrary commutative ring.

4. The Prime Spectrum of a Ring

In Section 3, we saw that the ring structure of $k[X_n]$ for a field k encodes a lot of important geometric data of the underlying space $\mathbb{A}^n_k$. Conversely, the geometric data of $\mathbb{A}^n_k$ tells us about the structure of $k[X_n]$. One may ask, is there a way to generalize this? That is:

Question 4.1. For a given commutative ring R, can we always find a "geometric" space X_R such that R can be realized as the ring of functions on X_R?

It is a very surprising fact that the answer to Question 4.1 is true in general. That is, we can always realize a commutative ring R as a ring of functions. The space on which R acts is called its *prime spectrum* $\mathrm{Spec}\, R$, or simply its *spectrum* where there is no ambiguity.

Definition 4.2 (Prime Spectrum)**.** For a ring R, we define the *spectrum* of R to be the set

$$\mathrm{Spec}\, R := \{\, \mathfrak{p} \mid \mathfrak{p} \subset R \text{ is a prime ideal} \,\}.$$

Example 4.3. Some examples are as follows:

(1) $\mathrm{Spec}\, \mathbb{Z} = \{(0), (2), (3), \ldots, (p), \ldots\}$,

[4]More precisely, Chow's Lemma states that every variety is birationally equivalent to a *projective variety*.

(2) $\operatorname{Spec} \mathbb{Z}/4\mathbb{Z} = \{(2)\}$,
(3) $\operatorname{Spec} \mathbb{C}[X] = \{0\} \cup \{\, (X-a) \mid a \in \mathbb{C} \,\}$.

To see why a commutative ring R can be seen as the ring of functions on $\operatorname{Spec} R$, we will first consider the classical case of $R = k[X]$ for an algebraically closed field k, e.g. $k = \mathbb{C}$. First, we observe that there is a 1–1 correspondence

$$k \longrightarrow \operatorname{Spec} k[X] \setminus \{(0)\}, \qquad a \longmapsto (X-a),$$

Therefore, as a set, $\operatorname{Spec} k[X] \setminus \{(0)\}$ is equivalent to the space k on which $k[X]$ acts as the ring of functions.

Moreover, for each $f \in k[X]$, we can define an action of f on $\operatorname{Spec} k[X]$ as follows. For each $\mathfrak{p} \in \operatorname{Spec} k[X]$, let $f(\mathfrak{p})$ to be the image of f under the canonical map

$$\pi_{\mathfrak{p}} : k[X] \longrightarrow k[X]/\mathfrak{p},$$

so $f(\mathfrak{p}) = \pi_{\mathfrak{p}}(f)$ is defined at every point $\mathfrak{p}$ in $\operatorname{Spec} k[X]$. Note that this is not a well-defined function in the usual sense, since for each prime $\mathfrak{p}$, $f(\mathfrak{p})$ takes values in different quotient rings. However, we claim that this construction has a natural interpretation.

Let $\mathfrak{p} = (X-a)$ for $a \in k$. Then for $f_1, f_2 \in k[X]$, we have by definition that

$$\pi_{\mathfrak{p}}(f_1 - f_2) = 0$$

if and only if $f_1(a) = f_2(a)$. In particular, for any $f \in k[X]$, we have

$$f \equiv f(a) \pmod{(X-a)},$$

therefore $f(\mathfrak{p}) = f(a)$ in $k[X]/(X-a)$. That is, for any prime $\mathfrak{p} = (X-a) \in k[X]$, the assigment $f \mapsto f(\mathfrak{p})$ agrees with the evaluation map $f \to f(a)$.

Thus, $k[X]$ acts on $\operatorname{Spec} k[X]$ in the same way that it acts on the affine space k.

We can generalize this construction to any commutative ring R. For $r \in R$ and $\mathfrak{p} \in \operatorname{Spec} R$, we define $r(\mathfrak{p})$ to be the image $\pi_{\mathfrak{p}}(r)$ of r under the canonical map $R \to R/\mathfrak{p}$, so each $r \in R$ acts as a function on $\operatorname{Spec} R$. Accordingly, we call R the ring of *regular functions* on $\operatorname{Spec} R$.

Example 4.4. Let $R = \mathbb{Z}$. Then, for $f = 17 \in \mathbb{Z}$, we have

$$f((p)) = 17 \pmod{p}$$

for all prime ideals $(p) \in \operatorname{Spec} \mathbb{Z}$. For instance,

$$f((2)) \equiv 1 \pmod 2, \quad f((3)) \equiv 2 \pmod 3, \quad \dots$$

In this way, we can view $\mathbb{Z}$ as a space of functions.

We now claim that the correspondence between R and $\operatorname{Spec} R$ lifts to the level of topology. Recall that in Section 3, we defined the *Zariski topology* on k^n to be the topology generated by declaring the *algebraic subsets*

$$V(I) := \{x \in k^n \mid I \text{ an ideal in } k[X_n],\, f(x) = 0 \text{ for all } f \in I\}$$

to be closed. We can also define the *Zariski topology on* $\operatorname{Spec} R$ as follows:

Definition 4.5 (Zariski Topology)**.** For a commutative ring R and all ideals $I \subseteq R$, define

$$V(I) := \{\, \mathfrak{p} \in \operatorname{Spec} R \mid I \subset \mathfrak{p} \,\}$$

to be the *vanishing of* I. Then, we define a topology on $\operatorname{Spec} R$ by taking all subsets of the form $V(I) \subseteq \operatorname{Spec} R$ to be closed. This is called the *Zariski topology* on $\operatorname{Spec} R$.

Exercise 4.6. Show that this indeed defines a topology.

Remark 4.7. In the case $R = k[X_n]$ for an algebraically closed field k, closed subsets of $\operatorname{Spec} k[X_n]$ correspond to vanishing sets of polynomials by Hilbert's Nullstellensatz, thus the identification

$$(a_1, \ldots, a_n) \mapsto (X_1 - a_1, \ldots, X_n - a_n)$$

is a homeomorphism $\mathbb{A}^n_k \to \operatorname{Spec} k[X_n] \setminus \{(0)\}$ when k is equipped with the Zariski topology. In particular, k and $\operatorname{Spec} k[X] \setminus \{(0)\}$ are homeomorphic in the Zariski topology so Definition 4.5 generalizes Definition 3.10.

Intuitively, the Zariski topology on a ring declares a set of prime ideals to be "close" if they all contain a common ideal I. For instance, in $\mathbb{Z}$, we have

$$V((2)) = \{(2)\}, \quad V((12)) = \{(2), (3)\},$$

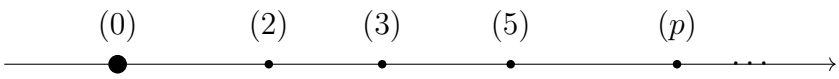
and in $\mathbb{C}[x]$,

$$V((x^2 + 1)) = \{(x + i), (x - i)\}.$$

In this way, the Zariski topology is quite natural algebraically. However, as a topological space, it has many pathological properties: for instance, it is almost never Hausdorff, and points are not in general closed.

Exercise 4.8. Show that $\{\mathfrak{p}\} \subset \operatorname{Spec} R$ is closed if and only if $\mathfrak{p} \subset R$ is maximal.

Indeed, a point can even be dense in the Zariski topology! Consider $(0) \in \operatorname{Spec} \mathbb{Z}$. Then the smallest closed set containing (0) is $V(0) = \operatorname{Spec} \mathbb{Z}$, so $\{(0)\}$ is dense in $\operatorname{Spec} \mathbb{Z}$. Moreover, every other point in $\operatorname{Spec} \mathbb{Z}$ is closed, since for all primes p we have that $\mathbb{Z}/(p)$ is a field. We can illustrate this with the picture



The "affine line" of $\operatorname{Spec} \mathbb{Z}$.

Indeed, in any PID, every nonzero prime ideal is maximal (why?), so we can draw a similar picture for $\mathbb{C}[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}_p$, etc.

The Zariski topology interacts naturally with many classic constructions in commutative algebra. For instance, for a ring homomorphism $f\colon R \to S$ of rings R, S, it is well-known that the preimage $f^{-1}(I)$ of an ideal $I \subseteq S$ is also an ideal in R. This is called the *contraction* of I under f. Moreover, if I is prime in S, then $f^{-1}(I)$ is prime in R.

Proposition 4.9. *Let $f : R \to S$ be a homomorphism of commutative rings. Then contraction by f induces a Zariski-continuous map*

$$f^* : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$$

given by

$$f^*(\mathfrak{q}) = f^{-1}(\mathfrak{q}),$$

so the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \xleftarrow[f^*]{} & \operatorname{Spec} S \end{array}$$

In fancier terms, Spec is a contravariant functor

$$\operatorname{Spec} : \mathbf{CRing} \to \mathbf{Top}$$

between the category of commutative rings and the category of topological spaces.

This functor can be extended to an *equivalence of categories* from **CRing** to the category **Aff** of *affine schemes*, which are, informally, topological spaces which are locally isomorphic to the spectrum of a ring. Led by Grothendieck, the reformulation of algebraic geometry in terms of schemes led to many great advancements in mathematics, for instance, the resolution of Fermat's Last Theorem by Andrew Wiles. To learn more about schemes, interested readers may wish to consult [2, 3], preferably after studying an introductory text such as [4].

References

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, Hoboken, NJ, 2003. 10
[2] D. Eisenbud and J. Harris, *The Geometry of Schemes*, Graduate Texts in Mathematics 197, Springer, New York, 2000. 20
[3] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics 52, Springer, New York, 1977. 20
[4] J. S. Milne, *Algebraic Geometry*, available at `https://www.jmilne.org/math/`, course notes. 13, 20
[5] B. Poonen, Why all rings should have a 1, *Mathematics Magazine* **92** (2019), no. 1, 58–62.