Abstract Algebra Review Notes

Will Huang
UW-Madison

Updated July 11, 2021

Contents

Part I
Introduction

These notes were compiled from the following classes during the following semesters to be used as a reference for future courses.

- Math 763: Introduction to Algebraic Geometry I (Fall 2021) - Basic concepts of algebraic geometry in the language of varieties
- Math 763: Introduction to Algebraic Geometry II (Fall 2021) -

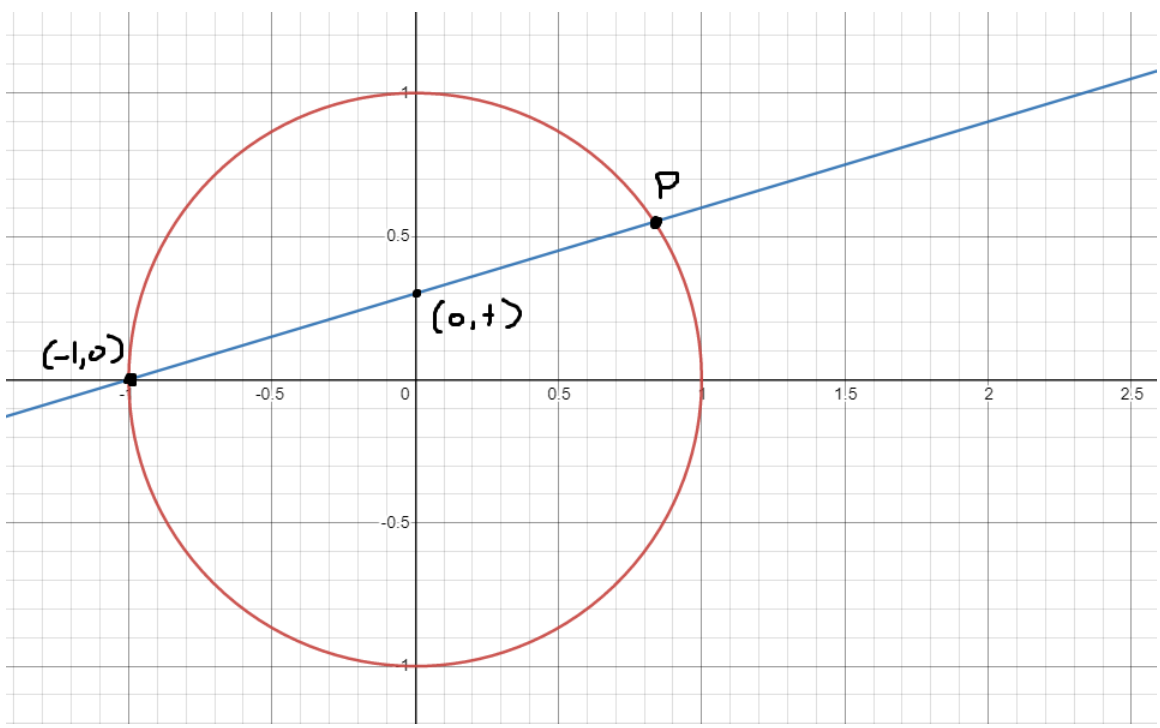
The primary textbook used in this course is Hartshorne's *Algebraic Geometry*, though sometimes Milne's (free) online notes are useful to consult.

1 Motivating Example: Projective Space

Before diving fully into algebraic geometry, we first present some classical geometrical examples which help us understand the motivations behind algebraic geometry. A classic question going all the way back to the Greek's is to parameterize the points on a circle using only rational functions.

$$x^2 + y^2 = 1$$

Of course any student with basic calculus experience can identify the canonical parameterization using sine and cosine, but to only use rational functions complicates things. Consider the picture below



By noting $(-1, 0)$ lies on the circle, we can choose any point t on the y-axis and draw a line through the two. The line will intersect the circle at another point P which has coordinates given by the system

$$\begin{cases} y = tx + t \\ x^2 + y^2 = 1 \end{cases}$$

For instance if we try to solve for x, we'll get the quadratic

$$x^2 + \frac{2t^2}{1+t^2}x + \frac{t^2-1}{1+t^2} = 0$$

and by noting $x = -1$ is already a solution, we find the roots and thus coordinates

$$x = \frac{1-t^2}{1+t^2} \qquad y = \frac{2t}{1+t^2}$$

However note that this expression will not generated the point $(-1, 0)$. Another interesting fact is that this argument works in any field (e.g. $\mathbb{Q}$ or even exotic fields like $\mathbb{F}_{49}$) since we've arrived at our solution through basic addition and multiplication (and since the original solution lies in the base field). This can be extended so that it also works for any quadric as long as there exists a solution for the quadric in the field we're working in.

We can restate our result for any field by defining the circle and (any) line

$$C = \left\{(x, y) \mid x^2 + y^2 = 1\right\} \qquad L = \{(x, y) \mid x = 0\}$$

We've essentially demonstrated the isomorphism

$$C \setminus \{(-1, 0)\} \cong L$$

But having to remove a point from C is unpleasant, so instead suppose there is a point "at ∞" where all parallel lines meet, allowing us to instead write

$$C \cong L \cup \{\infty\}$$

The addition of a point ∞ defines the projective plane $\mathbb{P}^2$ where any two lines (parallel or not) will meet at one point (in $\mathbb{P}^2$). More formally, what we've (kinda) proved is the following theorem:

Theorem 1.1. Over any field, a smooth plane quadric with at least one point is isomorphic to $\mathbb{P}^1$

Part II
Varieties

2 Affine Varieties

Algebraic geometry originated as the study of varieties before being reformed into a theory of schemes. Still, we will start by studying varieties as it provides a nice introduction to algebraic geometry without much complicated machinery. For the rest of these notes we will assume $k = \overline{k}$ is an algebraically closed field (for instance $\mathbb{C}$ or $\overline{\mathbb{F}_p}$.

Definition. *For an algebraically closed field k, we define affine n-space as*

$$\mathbb{A}^n = \{(x_1, \dots, x_n) \mid x_i \in k\}$$

While this definition is very similar to that of a vector space, the difference between the two is that affine space has no distinguished origin. While $(0, \dots 0)$ certainly exists in affine space, there is no particular importance ascribed to it.

Definition. *An algebraic set $Y \subseteq \mathbb{A}^n$ is any set obtained as the zero locus of a set of polynomials*

$$Y = Z(f_1, \dots, f_k) \qquad f_i \in k[x_1, \dots, x_n]$$

where the zero locus is defined as

$$Z(f_1, \dots, f_k) = \{(x_1, \dots, x_n) \in \mathbb{A}^n \mid f_i(x_1, \dots, x_n) = 0 \ \forall i\}$$

In fact we can define the zero locus for any subset $S \subseteq k[x_1, \dots, x_n] = A$[1] as

$$Z(S) = \{P \in \mathbb{A}^n \mid f(P) = 0 \ \forall f \in S\} = \bigcap_{f \in S} Z(f)$$

Example. For $S = \varnothing$ (or $\{0\}$), the zero locus is $Z(S) = \mathbb{A}^n$, or all of affine space. For $S = \{1\}$, then the zero locus is nothing $Z(S) = \varnothing$.

Observe that for any subset $S \subseteq A$, $Z(S) = Z(\langle S \rangle)$ so there is no loss of generality in assuming that S is an ideal to begin with.

Definition. *Let $X \subseteq \mathbb{A}^n$ be any set, the ideal of X is the set*

$$I(X) = \{f \in A \mid f(P) = 0 \ \forall P \in X\} \subseteq A$$

Note the similarity between constructing I and Z, for the ideal we take a set of points and consider all the polynomials which vanish at those points. On the other hand for the zero locus we take a set of polynomials and consider the points that they all vanish at.

Example. If $P = (a_1, \dots, a_n)$, then we can take $I = (x_1 - a_1, \dots, x_n - a_n)$ and $Z(I) = \{P\}$.

[1] From here on out, we will refer to the polynomial ring as just A for notational convenience

Example. Let's completely characterize all algebraic sets of the affine line $\mathbb{A}^1$. Consider an ideal $\langle S\rangle \subseteq k[x]$ and note that ideals in $k[x]$ are principal $\langle S\rangle = \langle f\rangle$ for some polynomial f. Thus we have

$$Z(S) = Z(\langle S\rangle) = Z(f)$$

for any subset $S \subseteq k[x]$. In other words the algebraic sets of $\mathbb{A}^1$ are either a finite set of points in $\mathbb{A}^1$ or all of it.

This can be extended for any $\mathbb{A}^n$ by noting that A is Noetherian so that for any set $S \subseteq A$, we can derive

$$Z(S) = Z(\langle S\rangle) = Z(f_1, \ldots, f_n)$$

Theorem 2.1. The algebraic sets form the closed sets of a topology on $\mathbb{A}^n$, the Zariski topology.

Proof. To begin, the empty and full sets $S = \varnothing, \mathbb{A}^n$ are closed (from a previous example). Next we must show that arbitrary intersections remain closed, which follows from

$$\bigcap_{j\in J} Z(I_j) = Z(\bigcup_{j\in J} I_j)$$

The union of finitely many closed sets is also closed, so we just need to show that the union of two closed sets remains closed. In fact we will prove

$$Z(I) \cup Z(J) = Z(IJ)$$

Take some point $P \in Z(IJ)$ and suppose $P \notin Z(I)$ other wise we are done. This means that there exists some $f \in I$ such that $f(P) \neq 0$, but

$$P \in Z(IJ) \to (fg)(P) = f(P)g(P) = 0 \ \forall g \in J$$

So if $f(P) \neq 0$ then we must have $g(P) = 0$ for all $g \in J$, or in other words $P \in Z(J)$. Thus $Z(IJ) \subseteq Z(I) \cup Z(J)$, the other inclusion is trivial, thus we've established the equality. $\square$

Notably, $\mathbb{A}^n$ is not isomorphic to $\mathbb{A}^1 \times \mathbb{A}^1$ which is an issue we'll return to later. The Zariski topology is not Hausdorff, it is T1 but not T2. Points are closed but we cannot find always find disjoint neighborhoods for two distinct points. In fact any two open sets will intersect in the Zariski topology.

Lemma 2.2. 1)Z and I are inclusion reversing, that is

$$Z(S_1) \subseteq Z(S_2) \text{ if } S_1 \supseteq S_2$$
$$I(X_1) \supseteq I(X_2) \text{ if } X_1 \subseteq X_2$$

2) For some arbitrary set $X \subseteq \mathbb{A}^n$

$$Z(I(X)) = \overline{X}$$

3) For some ideal $J \subseteq A$

$$I(Z(J)) = \sqrt{J} = \{f \in A \mid \exists n > 0,\ f^n \in J\}$$

Proof. 1) Obvious from definitions

2) For some set $X \subseteq \mathbb{A}^n$, it's clear that $X \subseteq Z(I(X))$ and since $Z(I(X))$ is closed by definition, we have

$$\overline{X} \subseteq Z(I(X))$$

For the other direction, let W be closed and $W \supseteq X$, we must show that $W \supseteq Z(I(X))$. By definition, if W is closed then it is of the form $Z(\mathfrak{a})$ where $\mathfrak{a}$ is some ideal. Thus

$$W \supseteq X \to I(W) \supseteq I(X)$$

$$\therefore \mathfrak{a} \subseteq I(Z(\mathfrak{a})) \subseteq I(X)$$

$$\therefore Z(\mathfrak{a}) = W \supseteq Z(I(X))$$

Thus $Z(I(X))$ is the smallest closed set containing X, in other words it's the closure $\overline{X}$.

3) One inclusion can be seen since raising a polynomial to arbitrary powers does not change it's zeros, the other inclusion is a consequence of Hilbert's Nullstellensatz. □

Due to it's importance we will list but not prove (one form of) Hilbert's Nullstellensatz here.

Theorem 2.3. Let $\mathfrak{a} \subseteq A$ be an ideal and $f \in A$ a polynomial which vanishes at all the points of $Z(\mathfrak{a})$, then $f^n \in \mathfrak{a}$ for some integer $n > 0$.

Example. If $J = (x^2+1) \subseteq \mathbb{R}[x]$ an ideal, then $Z(J) = \varnothing$ and thus $I(Z(J)) = \mathbb{R}[x]$. However J is prime so $\sqrt{J} = J$ which does not satisfy the theorem. Thus it is crucial that we work over algebraically closed fields.

To recap what we've done thus far, we've defined two new operations, Z and I with

$$Z : \{\text{ideals in } A\} \mapsto \{\text{algebraic sets in } \mathbb{A}^n\}$$

$$I : \{\text{sets in } \mathbb{A}^n\} \mapsto \{\text{ideals in } A\}$$

As a consequence of the lemma, points are minimal closed subsets of $\mathbb{A}^n$. $I(P)$ are maximal ideals of A so all maximal ideals of A are of the form

$$(x_1 - a_1, \ldots, x_n - a_n)$$

Corollary 2.4. Z restricted to radical ideals and I restricted to algebraic sets are inverses

$$\{\text{radical ideals}\} \longleftrightarrow \{\text{algebraic sets}\}$$

Now we may ask what prime ideals correspond to under this given correspondence, but first we will need new technologies.

Definition. *A nonempty topological space X is irreducible if $X = X_1 \cup X_2$ with X_1, X_2 closed implies $X_1 = X$ or $X_2 = X$.*

In other words, a topological space is irreducible if it cannot be written as the intersection of two proper closed (nonempty) subsets.

Example. The only irreducible sets of $\mathbb{R}^n$ are points.

Example. $\mathbb{A}^1$ is irreducible because all its proper closed subsets are finite.

There is a corollary from this definition.

Corollary 2.5. If X is irreducible and $U_1, U_2 \subseteq X$ are open and nonempty, then $U_1 \cap U_2 \neq \varnothing$

Proof. This follows directly from De Morgan's laws, since

$$U_1 \cap U_2 = \varnothing \to U_1^c \cup U_2^c = X$$

a contradiction, since X is irreducible. □

Note that nonempty open subsets of an irreducible space will also be irreducible (and furthermore dense). As a consequence, it's closure will be the entire space.

Proposition 2.6. Let $X \subseteq \mathbb{A}^n$ be irreducible and closed and $\mathfrak{a} \subseteq A$ be prime. Then

1. $I(X)$ is prime
2. $Z(\mathfrak{a})$ is irreducible

Proof. 1) Suppose $fg \in I(X)$, then

$$Z(fg) \supseteq Z(I(X)) = X \quad \longrightarrow \quad Z(F) \cup Z(g) \supseteq X$$
$$\therefore (X \cap Z(f)) \cup (X \cap Z(g)) = X$$

and since both those sets on the left are closed, we must have either $X = X \cap Z(f)$ or $X = X \cap Z(g)$, which is equivalent to the statement $X \subseteq Z(f)$ or $X \subseteq Z(g)$. Thus $f \in I(X)$ or $g \in I(X)$, which means $I(X)$ is a prime ideal.

2) Suppose we can write $Z(\mathfrak{a}) = Y_1 \cup Y_2$, then

$$I(Z(\mathfrak{a})) = \mathfrak{a} = Z(Y_1 \cup Y_2) = Z(Y_1) \cap Z(Y_2)$$

which means $\mathfrak{a} = Z(Y_1)$ or $=Z(Y_2)$ which subsequently implies $Z(\mathfrak{a}) = Y_1$ or $Z(\mathfrak{a}) = Y_2$, thus $Z(\mathfrak{a})$ is irreducible. □

Now we can define the main topic of study for this chapter.

Definition. *An affine variety is an irreducible closed subset of $\mathbb{A}^n$. The associated affine coordinate ring of a variety $X \subseteq \mathbb{A}^n$ is the quotient*

$$A(X) = A/I(X)$$

An open subset of an affine variety is a quasi-affine variety.

Note that for a prime ideal $\mathfrak{p}$, the zero locus $Z(\mathfrak{p})$ is an affine variety and for an affine variety X, $I(X)$ is prime. In particular, the zero locus for a set of irreducible polynomials will be an affine variety.

For an affine variety $X \subseteq \mathbb{A}^n$, the coordinate ring $A(X)$ is an integral domain, furthermore it is finitely generated as a k-algebra. The converse is also true, if B is a finitely generated k-algebra which also happens to be an integral domain, then it is possible to write

$$B = A/\mathfrak{a}$$

for some ideal $\mathfrak{a} \subseteq A$ and let $Y = Z(\mathfrak{a})$ be the corresponding variety.

Example. Since the zero ideal is prime, $Z(0) = \mathbb{A}^n$ is irreducible and closed and thus an affine variety.

Note that since $\mathbb{A}^n$ is a variety, any open subset of it will automatically be irreducible and thus are quasi-affine variety. However we cannot say the same for closed subsets since they may not be irreducible by default.

Example. Let $f \in k[x, y]$ be irreducible so that it generates a prime ideal (since $k[x, y]$ is a UFD). The zero locus $Z(f)$ will be irreducible and thus an affine variety

In the situation above, $Z(f)$ is known as an affine curve, defined by the equation $f(x, y) = 0$. If the polynomial f is of degree d, then we say that $Z(f)$ is a curve of degree d. This can be generalized to higher orders by taking some irreducible $f \in \mathbb{A}^n$ to get an affine variety $Z(f)$. For $n = 3$ this is known as a surface and for $n > 3$ as a hypersurface.

To study varieties, we must also study their topology, which belong to an important class of topologies.

Definition. *A topological space X is Noetherian if it satisfies the descending chain condition (DCC) on closed sets: if we have a sequence of closed subsets*

$$X_1 \supseteq X_2 \supseteq \cdots$$

then there exists some integer n such that

$$X_n = X_{n+1} = \cdots$$

In other words any descending chain must terminate.[2]

We care about Noetherian topologies because $\mathbb{A}^n$ is Noetherian under the Zariski topology. If we have a chain

$$X_1 \supseteq X_2 \supseteq \cdots$$

then the corresponding ideals form another chain

$$I(X_1) \subseteq I(X_2) \subseteq \cdots$$

[2] This is equivalent to the ascending chain condition (ACC) on open sets, which some might be more used to seeing. Indeed a ring is Noetherian if it satisfies ACC on its ideals

which must terminate since A is Noetherian. This means the chain $X_i = Z(I(X_i))$ will also terminate, thus $\mathbb{A}^n$ is Noetherian. Recall that all proper ideals in a Noetherian ring have a decomposition in term of irreducible and thus primary ideals. An analogous statement holds for topological spaces.

Proposition 2.7. Every nonempty closed subsets Y of a Noetherian topological space X can be written as

$$Y = Y_1 \cup \cdots \cup Y_n$$

where Y_i are irreducible and closed (variety). If we require that the subsets not contain each other

$$Y_i \not\subseteq Y_j \qquad i \neq j$$

then the Y_i are unique and are called the irreducible components of Y.

Proof. □

There is a direct consequence of this in the language of varieties.

Corollary 2.8. Every algebraic set in $\mathbb{A}^n$ can be uniquely expressed as a union of varieties, no one containing the other.

Chains of closed subsets provide important information for how "large" a topological space is. We will use their size to quantify the "size" of topological spaces and rings.

Definition. *For a topological space X, define the dimension* $\dim X = n$ *to be the size of the largest chain*

$$Z_0 \supset Z_1 \supset \cdots \supset Z_n$$

of distinct irreducible closed subsets of X. The dimension of an affine or quasi-affine variety is its dimension as a topological space.

Since we will primarily be talking about $\mathbb{A}^n$ as the topological space in question, all dimensions will be finite since infinitely large chains cannot exist in Noetherian spaces.

Example. Since the only (proper) irreducible closed subsets of $\mathbb{A}^1$ are single points, its dimension is 1.

This concept can be applied to rings in general. Recall that if $\mathfrak{p}$ is prime, then $Z(\mathfrak{p})$ will be irreducible.

Definition. *For a ring A, then height of a prime ideal ht $\mathfrak{p} = n$ is the maximum length of a (distinct) prime ideal chain*

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n = \mathfrak{p}$$

The maximum possible height of all prime ideals (supremum) in A is called its Krull dimension (or simply dimension) of the ring A.

Given the connection between prime ideals and irreducible closed subsets, we expect there to be some connection between the dimension of a topological space and the Krull dimension of a ring. In fact there is and that is part of why affine coordinate rings are so useful.

Proposition 2.9. If X is an affine algebraic set, then

$$\underbrace{\dim X}_{\text{as a topological space}} = \underbrace{\dim A(X)}_{\text{as a ring}}$$

Proof. The closed irreducible subsets of X correspond to prime ideals of A which contain $I(X)$. In turn these are just prime ideals of $A(X)$ so a chain of closed irreducible subsets of X corresponds to a chain of prime ideals of $A(X)$, thus the two will have equivalent length so the dimensions are equal. □

Note that this result is slightly more general than we actually need. An affine algebraic set is any closed subset of $\mathbb{A}^n$, note necessarily irreducible. We can make this into a theorem about affine varieties and their coordinate rings by imposing the condition that X be irreducible, at the cost of losing some generality.

Given this relationship between dimensions, we can use what we know about Noetherian rings to study affine varieties. In particular, recall the following theorem

Theorem 2.10. Let B be an integral domain which is finitely generated as a k-algebra. Then for every prime $\mathfrak{p} \subseteq B$

$$\text{ht } \mathfrak{p} + \dim B/\mathfrak{p} = \dim B$$

Furthermore, the dimension of B is equal to the transcendence degree of the quotient field $K(B)$ (field of fractions) over k, i.e. the size of the largest algebraically independent subset of $K(B)$ over k.

Proof. □

Proposition 2.11. $\dim \mathbb{A}^n = n$

Proof. We have the following relationships between dimensions:

$$\dim \mathbb{A}^n = \dim A(\mathbb{A}^n) = \dim A/(0) = \dim A = n$$

□

3 Projective Varieties

4 Morphisms