Basic algebraic geometry

Nigel Redding

March 2, 2026

1 Affine varieties

All rings, unless stated otherwise are commutative.

Recall that an *integral domain* or *domain* is a ring where $ab = 0$ implies $a = 0$ or $b = 0$. Moreover, if R is a domain and $a \neq 0$, then if $ab = ac$ then $b = c$, i.e. the *law of cancellation* holds in a domain. This is an equivalent definition. We say that the domain is a *principal ideal domain* or *PID* if every ideal is generated by one element.

As an example $\mathbb{Z}$ is a PID. Indeed, if I is a non-zero ideal, then we can choose elements a and b in I such that $b > a > 1$. Then we can write $b = qa + c$ for some integers q and c satisfying $q \geq 0$ and $0 \leq c < a$. As c is non-negative and a is the smallest positive integer in I, we see that $c = 0$, i.e. $b = qa$. This ring is also a *unique factorization domain*, which is a ring in which each non-zero element decomposes as a unique product of primes.

We call a non-zero element a of R a *unit* if there exists some b such that $ab = 1$. Ideals generated by units are the entire ring. A non-unit which is not the product of any two non-units is called an *irreducible element*. A *unique factorization domain* or *UFD* is a ring in which every non-zero, non-unit element is a unique product of irreducible elements. Hence, $\mathbb{Z}$ is a UFD. We also have the following well-known fact, which is easy to prove.

Theorem 1. *If R is a UFD then so is $R[X]$ and consequently so is $R[X_1, \ldots, X_n]$.*

We say R is *Noetherian* if every ideal is finitely generated. We have the following important theorem.

Theorem 2. *If R is Neotherian, then so is $R[X]$ and consequently so is $R[X_1, \ldots, X_n]$.*

We use the notation $R[\mathbf{X}]$ instead of $R[X_1, \ldots, X_n]$ when it is convenient and it does not cause confusion.

There are two proofs. We give a sketch of both. The first way is to take an ideal I in $R[X]$ and take the set of leading coefficients in I which is a finitely generated ideal in R. We call this ideal J. The idea of the proof is to decompose J into a sum which has a nice pre-image in $R[x]$.

The better way of approaching this is to use the concept of a *Grobner basis*. Unfortunately, I could not find a precise definition, but a Grobner basis is basically a finite generating set of I with "nice algorithmic properties". Thankfully, the exact definition does not matter for us. Basically, if $F = \sum a_i X_1^{i_i} \cdots X_k^{i_k}$, and $G_1, \ldots, G_m$ are a set of polynomials in $R[X]$, then we can write $F = \sum A_i G_i + C$, where $\deg C < \deg F$. This can be done by a sort of Euclidean algorithm using lexicographic ordering, called *Bucherberg's Algorithm*.

Given a subset X of R^n, we define its ideal $I(X)$ to be the set of polynomials $f \in R[\mathbf{X}]$ are zero on X. Similarly, for an ideal I of R, we define its *locus* to be the set of points $p \in R^n$ such that $fp = 0$ for all $f \in I$. In general, these maps are not inverses of each other, but we will get to their relationship quite soon. However, we can see some interesting properties. First, we say an algebraic set is *irreducible* if it is not a union of two non-empty algebraic sets, where the two sets in the union are unequal. It is easy to show that V is irreducible if and only if $I(V)$ is prime. Moreover, by Hilbert's basis theorem, we have

Proposition 1. *Every algebraic set is a finite intersection of irreducible algebraic sets.*

Proof. If I is minimally generated by irreducible polynomials $F_1, \ldots, F_k$, then $X = Z(F_1) \cap \cdots \cap Z(F_k)$. □

Example 1. *$\mathbb{A}^1$ is irreducible.*

Example 2. *Let $f \in k[x_1, \ldots, x_n]$. Then f is irreducible if and only if the ideal (f) is prime, if and only if $Z(f)$ is irreducible.*

Note that if f is reducible if and only if f has a non-trivial factorization $f = gh$. In this case, $Z(g)$ and $Z(h)$ would be proper subsets of $Z(f)$, and we would also have $Z(f) = Z(g) \cup Z(h)$. So we have shown that if f is reducible, then $Z(f)$ can be decomposed as two non-empty algebraic sets.

On the other hand, suppose $Z(f) = X \cup Y$ for non-empty algebraic sets X and Y.

Observation 1. *X is irreducible if and only if $I(X)$ is prime.*

We continue to get more interesting properties of algebraic sets. Suppose $I \subset J$ are ideals. Then $V(J) \subset V(I)$. The situation is simple when k is algebraically closed. If I is a proper ideal of $k[\mathbf{X}]$, then there is some maximal ideal J containing I. But we know J is generated by $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$. So $a = (a_1, \ldots, a_n) \in V(I)$. Hence

Proposition 2. *If k is algebraically closed and I is a proper ideal of $k[\mathbf{X}]$ then $V(I) \neq 0$.*

Next we define the radical of an ideal I as

$$\mathrm{rad}(I) = \{f \in R[\mathbf{X}] : f^r \in I \text{ for some } r > 0\}.$$

When k is an algebraically closed field, I claim that $I(V(I)) = \mathrm{rad}(I)$. If we had this, then this would allow us to reduce a generating ideal of an algebraic set to a minimal one. Showing that $\mathrm{rad}(I) \subset I(V(I))$ is straightforward. For the other direction, suppose $f \in I(V(I))$. Let $f_1, \ldots, f_k$ be the generators of I. We wish to find some r such that $f^r = \sum a_i f_i$ where a_i are members of $k[X_1, \ldots, X_n]$. Then the ideal J generated by $f_1, \ldots, f_k$ and $1 - x_{n+1}f$ is the entire ring, since if it were not, then $V(J)$ would have at least one element, which it does not, because f vanishes whenever each f_i does. Thus one can write

$$1 = g_1 f_1 + \cdots + g_k f_k + h(1 - x_{n+1}f)$$

for some g_i and h in $k[x_1, \ldots, x_{n+1}]$. Substituting $1/f(x_1, \ldots, x_n)$ for x_{n+1} results in the equation

$$1 = \sum g_i(x_1, \ldots, x_n, \frac{1}{f(x_1, \ldots, x_n)}) f_i(x_1, \ldots, x_n).$$

We can multiply both sides by a high enough power of f to remove f from the denominator of the rational expression on the right hand side, yielding

$$f^r = \sum c_i f_i$$

for some c_i in I. Thus we have the following theorem

Theorem 3. *(Hilbert's Nullstellensats) $I(V(I)) = rad(I)$.*

This important theorem characterizes gives us a one-to-one correspondence between the radical ideals of $\mathfrak{r}$ and the algebraic sets in $\mathbb{A}^n$. We can go even further. We say $\mathfrak{r}$ is *reduced* if it contains no non-zero nilpotent elements.

Proposition 3. *$\mathfrak{r}/\mathfrak{i}$ is reduced if and only if $\mathfrak{i}$ is a radical ideal.*

Proof. Suppose $\mathfrak{r}/\mathfrak{i}$ is reduced. To show that $\mathfrak{i}$ is radical, suppose $x \in \mathfrak{r}$ is such that $x^n \in \mathfrak{i}$ for some $n \geq 1$. We aim to show that $x \in \mathfrak{i}$. We can safely assume $n > 1$. Then let m be the smallest positive integer such that $2m > n$. Then $y = x^m$ is a nonzero nilpotent element in $\mathfrak{r}$, which is impossible.
Secondly, if $\mathfrak{i}$ is radical, then if $x \in \mathfrak{r}/\mathfrak{i}$ is nilpotent, then $x^2 \in \mathfrak{i}$, so $x \in \mathfrak{i}$. □

Thus we have a one-to-one correspondence between the following sets

$$\text{radical ideals of } \mathfrak{r} \longleftrightarrow \text{ reduced quotients of } \mathfrak{r} \longleftrightarrow \text{ alg. sets}$$

The reader may have noticed, or already knows that the "reduced quotient" is just a ring $k[x_1, \ldots, x_n]/I(X)$ where X is an algebraic set. We call this the coordinate ring, and delay a full study to the next section.

Let us sketch out some more properties of algebraic sets before we finish this section. We will finish with giving $\mathbb{A}^n$ a topology, and we will introduce the notion of dimension of algebraic sets.

Proposition 4. *1. The union of two algebraic sets is algebraic.*

2. The intersection of two algebraic sets is algebraic.

3. $\emptyset$ and $\mathbb{A}^n$ are algebraic.

Proof. For 1. and 2., we let X and Y be algebraic sets generated by $I_X = (F_1, \ldots, F_n)$ and $I_Y = (G_1, \ldots, G_m)$. Then note that $X \cup Y$ is generated by the product of the ideals $I_X \cdot I_Y$ and $X \cap Y$ is generated by the sum $I_X + I_Y$. Finally, the ideal of $\emptyset$ is the ring $\mathfrak{r}$ and the ideal of $\mathbb{A}^n$ is $\{0\}$. □

Definition 1. *We give $\mathbb{A}^n$ the* Zariski topology*, which defines the open sets as complements of algebraic sets in $\mathbb{A}^n$. We call open sets* quasi-algebraic sets.

As an example, note that the Zariski-closed sets of $\mathbb{A}^1$ are the finite subsets of $\mathbb{A}^1$. The closed sets in $\mathbb{A}^2$ consist of finite sets, lines and curves.

Definition 2. *An* affine variety *is an irreducible affine algebraic set. A* quasi-affine variety *is a an open subset of an affine variety.*

Remark 1. *The Zariski topology is Hausdorff if and only if k is a finite field...*

We define the *Krull dimension* of a ring to be the supremum of lengths of proper chains of prime ideals, and we denote this by $\dim \mathfrak{r}$. For a prime ideal $\mathfrak{p} \subset \mathfrak{r}$, we define its height to be the supremum of its proper chains of prime ideals.

Proposition 5. *If $\mathfrak{r}$ is Noetherian and $\mathfrak{p}$ is a prime ideal of $\mathfrak{r}$, then*

$$\dim \mathfrak{r} = \dim \mathfrak{r}/\mathfrak{p} + \mathrm{ht}(\mathfrak{p}).$$

Proof. Left to the reader. □

Definition 3. *If X is a topological space, we define its* dimension *to be the supremum of lengths of strictly descending chains of closed sets in X.*

Proposition 6. *Let X be an algebraic set in $\mathbb{A}^n(k)$. Then the topological dimension of X is equal to the Krull dimension of $A(X)$.*

Proof. Let $X \supset Y_0 \supset Y_1 \supset \cdots$ be a descending chain of closed sets in X, where $Y_i \neq Y_{i+1}$. As each Y_i is closed in X, we have $Y_i = Z(\tilde{I}_i)$ where $\tilde{I}_i = I_i/I(X)$ for some prime ideal I_i in $k[x_1, \ldots, x_n]$. We thus get an ascending chain of ideals $I_i \subset \cdots$ which terminates at the Krull dimension of $A(X)$ □

For example, the dimension of $\mathbb{A}^n$ is n.

Proposition 7. *If X is a quasi-affine variety, then* $\dim X = \dim \overline{X}$.

We leave the proof as an exercise to the reader.

Proposition 8. *A variety X in $\mathbb{A}^n$ has dimension $n-1$ if and only if X is generated by a single irreducible polynomial.*

Proof. Suppose X has dimension 1, and let $\mathfrak{p}$ denote its prime ideal. Then by a proposition above, $\mathfrak{p}$ has height 1. By another theorem, this is principle.

Conversely, if X is generated by a principal prime ideal $\mathfrak{p}$, then this ideal has height 1 and proves the theorem. □