Chapter 1

Algebraic Sets

1.1 Affine Space

In elementary geometry, one considered figures with coordinates in some Cartesian power of the real numbers. As our starting point in algebraic geometry, we will consider figures with coordinates in the Cartesian power of some fixed field $\Bbbk$.

1.1.1 Definition. Let $\Bbbk$ be a field, and let $\mathbb{A}^n(\Bbbk) = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \Bbbk\}$. When the field is clear, we will shorten $\mathbb{A}^n(\Bbbk)$ to $\mathbb{A}^n$. We will refer to $\mathbb{A}^n$ as *affine n-space*. In particular, $\mathbb{A}^1$ is called the *affine line*, and $\mathbb{A}^2$ is called the *affine plane*.

From the algebraic point of view, the most natural functions to consider on $\mathbb{A}^n$ are those defined by evaluating a polynomial in $\Bbbk[x_1, \ldots, x_n]$ at a point. Analogously, the simplest geometric figures in $\mathbb{A}^n$ are the zero sets of a single polynomial.

1.1.2 Definition. If $f \in \Bbbk[x_1, \ldots, x_n]$, a point $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ such that $f(p) = f(a_1, \ldots, a_n) = 0$ is called a *zero of f* and

$$\mathrm{V}(f) = \{p \in \mathbb{A}^n \mid f(p) = 0\}$$

is called the *zero set* or *zero locus* of f. If f is non-constant, $\mathrm{V}(f)$ is called the *hypersurface* defined by f. A hypersurface in $\mathbb{A}^n$ is also called an *affine surface*, in order to distinguish it from hypersurfaces in other ambient spaces.

1.1.3 Examples.

(i) In $\mathbb{R}^1$, $\mathrm{V}(x^2+1) = \varnothing$, but in $\mathbb{C}^1$, $\mathrm{V}(x^2+1) = \{\pm i\}$. Generally, if $n = 1$ then $\mathrm{V}(F)$ is the set of roots of F in $\Bbbk$. If $\Bbbk$ is algebraically closed and F is non-constant then $\mathrm{V}(F)$ is non-empty.

(ii) In $\mathbb{Z}_p^1$, by Fermat's Little Theorem, $\mathrm{V}(x^p - x) = \mathbb{Z}_p^1$.

(iii) By Fermat's Last Theorem, if $n > 2$ then $\mathrm{V}(x^n + y^n - 1)$ is finite in $\mathbb{Q}^2$.

(iv) In $\mathbb{R}^2$, $\mathrm{V}(x^2+y^2-1) =$ the unit circle in $\mathbb{R}^2$, and in $\mathbb{Q}^2$ it gives the rational points on the unit circle. Notice the circle admits a parameterization by rational functions as follows:

$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right), t \in \mathbb{R}.$$

When $t \in \mathbb{Z}$ then we get a point in $\mathbb{Q}^2$.

Remark. A *rational curve* is a curve that admits a parameterization by rational functions. For example, the curve in the last example is rational.

1.2 Algebraic Sets and Ideals

1.2.1 Definition. If S is any set of polynomials in $\Bbbk[x_1, \ldots, x_n]$, we define

$$\mathrm{V}(S) = \{p \in \mathbb{A}^n \mid f(p) = 0 \text{ for all } f \in S\} = \bigcap_{f \in S} \mathrm{V}(f)$$

If $S = \{f_1, \ldots, f_n\}$ then we may write $\mathrm{V}(f_1, \ldots, f_n)$ for $\mathrm{V}(S)$. A subset $X \subseteq \mathbb{A}^n$ is an *(affine) algebraic set* if $X = \mathrm{V}(S)$ for some $S \subseteq \Bbbk[x_1, \ldots, x_n]$

1.2.2 Examples.

(i) For any $a, b \in \Bbbk$, $\{(a, b)\}$ is an algebraic set in $\Bbbk^2$ since $\{(a, b)\} = \mathrm{V}(x - a, y - b)$.

(ii) In $\mathbb{R}^2$, $\mathrm{V}(y-x^2, x-y^2)$ is only 2 points, but in $\mathbb{C}^2$ it is 4 points. Generally, Bézout's Theorem tells us that the number of intersection points of a curve of degree m with a curve of degree n is mn in projective space over an algebraically closed field.

(iii) The *twisted cubic* is the rational curve $\{(t, t^2, t^3) \mid t \in \mathbb{R}\} \subseteq \mathbb{R}^3$. It is an algebraic curve; indeed, it is easy to verify that it is $\mathrm{V}(y - x^2, z - x^3)$.

(iv) Not all curves in $\mathbb{R}^2$ are algebraic. For example, let

$$X = \{(x, y) \mid y - \sin x = 0\}$$

and suppose that X is algebraic, so that $X = \mathrm{V}(S)$ for some $S \subseteq \mathbb{R}[x, y]$. Then there is $F \in S$ such that $F \neq 0$ and so

$$X = \mathrm{V}(S) = \bigcap_{f \in S} \mathrm{V}(f) \subseteq \mathrm{V}(F).$$

Notice that the intersection of X with any horizontal line $y - c = 0$ is infinite for $-1 \leq c \leq 1$. Choose c such that $F(x, c)$ is not the zero polynomial and notice that the number of solutions to $F(x, c) = 0$ is finite, so X cannot be algebraic.

Remark. The method used in the last example works in more generality. Suppose that C is an algebraic affine plane curve and L is a line not contained C. Then $L \cap C$ is either $\varnothing$ or a finite set of points.

1.2.3 Proposition. *The algebraic sets in $\mathbb{A}^1$ are $\varnothing$, finite subsets of $\mathbb{A}^1$, and $\mathbb{A}^1$ itself.*

Proof: Clearly these sets are all algebraic. Conversely, the zero set of any non-zero polynomial is finite, so if S contains a non-zero polynomial F then $\mathrm{V}(S) \subseteq \mathrm{V}(F)$ is finite. If $S = \varnothing$ or $S = \{0\}$ then $\mathrm{V}(S) = \mathbb{A}^1$. $\square$

Before we continue, we recall some notation. If R is a ring and $S \subseteq R$, then $\langle S \rangle$ denotes the ideal generated by S[1]. If $S = \{s_1, \dots, s_n\}$, then we denote $\langle S \rangle$ by $\langle s_1, \dots, s_n \rangle$.

1.2.4 Proposition.
(i) *If $S \subseteq T \subseteq \Bbbk[x_1, \dots, x_n]$ then $\mathrm{V}(T) \subseteq \mathrm{V}(S)$.*
(ii) *If $S \subseteq \Bbbk[x_1, \dots, x_n]$ then $\mathrm{V}(S) = \mathrm{V}(\langle S \rangle)$, so every algebraic set is equal to $\mathrm{V}(I)$ for some ideal I.*

Proof:
(i) Since $S \subseteq T$,

$$\mathrm{V}(T) = \bigcap_{f \in T} \mathrm{V}(f) \subseteq \bigcap_{f \in S} \mathrm{V}(f) = \mathrm{V}(S).$$

(ii) From (i), $\mathrm{V}(\langle S \rangle) \subseteq \mathrm{V}(S)$. If $x \in \mathrm{V}(S)$ and $f \in I$ then we can write f as

$$f = g_q f_1 + \cdots + g_m f_m,$$

where $f_i \in S$ and $g_i \in \Bbbk[x_1, \dots, x_n]$. Then

$$f(x) = g_1(x) f_1(x) + \cdots + g_m(x) f_m(x) = 0$$

since $x \in \mathrm{V}(S)$. $\square$

Since every algebraic set is the zero set of an ideal of polynomials, we now turn our attention to ideals in polynomial rings. If a ring R is such that all of its ideals are finitely generated it is said to be *Noetherian*[2]. For example, all fields are Noetherian. The Hilbert Basis Theorem states that all polynomial rings with coefficients in a Noetherian ring are Noetherian.

[1] The ideal generated by S is the intersection of all ideals containing S. More concretely,

$$\langle S \rangle = \left\{ \sum_{k=1}^{n} a_k s_k : a_1, \dots, a_n \in R \text{ and } s_1, \dots, s_n \in S \right\}.$$

[2] Some readers may be more familiar with a different definition of Noetherian in terms of ascending chains of ideals. This definition is equivalent to ours by Proposition A.0.12.

1.2.5 Theorem (Hilbert Basis Theorem). *If R is Noetherian, then $R[x_1, \ldots, x_n]$ is Noetherian.*

PROOF: See Appendix A. $\square$

An important geometric consequence of the Hilbert Basis Theorem is that every algebraic set is the zero set of a finite set of polynomials.

1.2.6 Corollary. *Every algebraic set X in $\mathbb{A}^n$ is the zero set of a finite set of polynomials.*

PROOF: $\Bbbk[x_1, \ldots, x_n]$ is Noetherian, so if $X = V(S)$, then $X = V(\langle S \rangle) = V(S')$, where S' is a finite subset of $\Bbbk[x_1, \ldots, x_n]$ that generates $\langle S \rangle$. $\square$

Remark. Since $\mathrm{V}(f_1, \ldots, f_n) = \bigcap_{k=1}^n \mathrm{V}(f_k)$, the preceding corollary shows that every algebraic set is the intersection of finitely many hypersurfaces.

1.2.7 Proposition.

(i) *If $\{I_\alpha\}$ is a collection of ideals then $\mathrm{V}(\bigcup_\alpha I_\alpha) = \bigcap_\alpha \mathrm{V}(I_\alpha)$, so the intersection of any collection of algebraic sets is an algebraic set.*

(ii) *If I and J are ideals then $\mathrm{V}(IJ) = V(I) \cup \mathrm{V}(J)$, so the finite union of algebraic sets is an algebraic set.*[3]

(iii) $\mathrm{V}(0) = \mathbb{A}^n$, $\mathrm{V}(1) = \varnothing$, *and* $\mathrm{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$, *so any finite set of points is algebraic.*

PROOF:

(i) We have

$$\mathrm{V}\left(\bigcup_\alpha I_\alpha\right) = \bigcap_{f \in \cup_\alpha I_\alpha} \mathrm{V}(f) = \bigcap_\alpha \bigcap_{f \in I_\alpha} \mathrm{V}(f) = \bigcap_\alpha \mathrm{V}(I_\alpha).$$

[3] Recall that the product of I and J is the ideal generated by products of an element from I and an element from J. More concretely,

$$IJ = \left\{ \sum_{k=1}^n a_k b_k : a_1, \ldots, a_n \in I \text{ and } b_1, \ldots, b_n \in J \right\}.$$

(ii) Since $(gh)(x) = 0$ if and only if $g(x) = 0$ or $h(x) = 0$,

$$
\begin{aligned}
\mathrm{V}(IJ) &= \bigcap_{f \in IJ} \mathrm{V}(f) \\
&= \bigcap_{g \in I, h \in J} \mathrm{V}(gh) \\
&= \bigcap_{g \in I, h \in J} \mathrm{V}(g) \cup \mathrm{V}(h) \\
&= \bigcap_{g \in I} \mathrm{V}(g) \cup \bigcap_{h \in J} \mathrm{V}(h) \\
&= \mathrm{V}(I) \cup \mathrm{V}(J).
\end{aligned}
$$

(iii) This is clear. □

Remark. Note that finiteness of the union in property (ii) is required; for example, consider $\mathbb{Z}$ in $\mathbb{R}$. It is not an algebraic set, because a polynomial over a field can only have finitely many roots, but it is the union of (infinitely many) algebraic sets, namely $\mathrm{V}(x - n)$ for $n \in \mathbb{Z}$.

The properties in Proposition 1.2.7 allow us to define a topology[4] on $\mathbb{A}^n$ whose closed sets are precisely the algebraic sets.

1.2.8 Definition. The topology on $\mathbb{A}^n$ whose closed sets are precisely the algebraic sets is called the *Zariski topology*.

Remark. When $\Bbbk$ is one of $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, the Zariski topology is weaker than the usual metric topology, as polynomial functions are continuous, so their zero sets are closed. However, in each of these cases, the Zariski topology is strictly weaker than the metric topology. For example, $\mathbb{Z}$ is closed in the usual topology of each of $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, but is not algebraic and thus is not closed in the Zariski topology.

1.2.9 Example. The non-empty open sets in the Zariski topology on the affine line $\mathbb{A}^1$ are precisely the complements of finite sets of points. However, this is not true for $\mathbb{A}^n$ when $\Bbbk$ is infinite and $n > 1$. For example, $\mathrm{V}(x^2 + y^2 - 1)$, the unit circle in $\mathbb{R}^2$, is closed but is not finite. Moreover, note that the Zariski topology on $\mathbb{A}^n$ is Hausdorff[5] if and only if $\Bbbk$ is finite, in which case it is identical to the discrete topology.

---

[4] A *topology* on a set X is a collection τ of subsets of X that satisfies the following properties:

(i) $\varnothing, X \in \tau$,
(ii) if $G_i \in \tau$ for every $i \in I$ then $\bigcup_{i \in I} G_i \in \tau$,
(iii) if $G_1, G_2 \in \tau$ then $G_1 \cap G_2 \in \tau$.

The sets in τ are said to be *open*, and their complements are said to be *closed*.

[5] Recall that a topology is said to be Hausdorff if distinct points always have disjoint open neighbourhoods.

We have associated an algebraic subset of $\mathbb{A}^n$ to any ideal in $\Bbbk[x_1, \dots, x_n]$ by taking the common zeros of its members. We would now like to do the converse and associate an ideal in $\Bbbk[x_1, \dots, x_n]$ to any subset of $\mathbb{A}^n$.

1.2.10 Definition. Given any subset $X \subseteq \mathbb{A}^n$ we define $\mathrm{I}(X)$ to be the *ideal of* X,

$$\mathrm{I}(X) = \{f \in \Bbbk[x_1, \dots, x_n] \mid f(p) = 0 \text{ for all } p \in X\}.$$

1.2.11 Examples.

(i) The following ideals of $\Bbbk[x]$ correspond to the algebraic sets of $\mathbb{A}^1$: $\mathrm{I}(\varnothing) = \langle 1 \rangle$, $\mathrm{I}(\{a_1, \dots, a_n\}) = \langle (x - a_1) \cdots (x - a_n) \rangle$, and

$$\mathrm{I}(\mathbb{A}^1) = \begin{cases} 0 & \text{if } \Bbbk \text{ is infinite,} \\ \langle x^{p^n} - x \rangle & \text{if } \Bbbk \text{ has } p^n \text{ elements.} \end{cases}$$

Note that if $X \subseteq \mathbb{A}^1$ is infinite then $\Bbbk$ is infinite and $\mathrm{I}(X) = 0$.

(ii) In $\mathbb{A}^2$, $\mathrm{I}(\{(a, b)\}) = \langle x - a, y - b \rangle$. Clearly

$$\langle x - a, y - b \rangle \subseteq \mathrm{I}(\{(a, b)\}),$$

so we need only prove the reverse inequality. Assume that $f \in \mathrm{I}(\{(a, b)\})$. By the division algorithm, there is $g(x, y) \in \Bbbk[x, y]$ and $r(y) \in \Bbbk[y]$ such that

$$f(x, y) = (x - a)g(x, y) + r(y).$$

But $0 = f(a, b) = r(b)$, so $y - b$ divides $r(y)$ and we can write we can write $r(y) = (y - b)h(y)$, and hence

$$f = (x - a)g + (y - b)h \in \langle x - a, y - b \rangle.$$

1.2.12 Proposition.

(i) *If* $X \subseteq Y \subseteq \mathbb{A}^n$ *then* $\mathrm{I}(Y) \subseteq \mathrm{I}(X)$.

(ii) $\mathrm{I}(\varnothing) = \Bbbk[x_1, \dots, x_n]$.
$\mathrm{I}(\{(a_1, \dots, a_n)\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ *for any point* $(a_1, \dots, a_n) \in \mathbb{A}^n$.
$\mathrm{I}(\mathbb{A}^n) = 0$ *if* $\Bbbk$ *is infinite.*

(iii) $S \subseteq \mathrm{I}(\mathrm{V}(S))$ *for any set of polynomials* $S \subseteq \Bbbk[x_1, \dots, x_n]$.
$X \subseteq \mathrm{V}(\mathrm{I}(X))$ *for any set of points* $X \subseteq \mathbb{A}^n$.

(iv) $\mathrm{V}(\mathrm{I}(\mathrm{V}(S))) = \mathrm{V}(S)$ *for any set of polynomials* $S \subseteq \Bbbk[x_1, \dots, x_n]$.
$\mathrm{I}(\mathrm{V}(\mathrm{I}(X))) = \mathrm{I}(X)$ *for any set of points* $X \subseteq \mathbb{A}^n$.

PROOF:

(i) If f is zero on every point of Y then it is certainly zero on every point of X.

(ii) That $\mathrm{I}(\varnothing) = \Bbbk[x_1, \ldots, x_n]$ and $\mathrm{I}(\mathbb{A}^n) = 0$ if $\Bbbk$ is infinite are clear. Fix $(a_1, \ldots, a_n) \in \mathbb{A}^n$, and define $\varphi : \Bbbk[x_1, \ldots, x_n] \to \Bbbk$ by $\varphi(f) = f(a_1, \ldots, a_n)$. Clearly, φ is a surjective homomorphism, and

$$\ker(\varphi) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$

We have

$$\Bbbk[x_1, \ldots, x_n]/\langle x_1 - a_1, \ldots, x_n - a_n \rangle \cong \Bbbk,$$

so $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is a maximal ideal. The ideal $\mathrm{I}(\{(a_1, \ldots, a_n)\})$ is proper and contains $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$, a maximal ideal, so it must be equal to that maximal ideal.

(iii) These follow from the definitions of I and V.

(iv) From (iii), $\mathrm{V}(S) \subseteq \mathrm{V}(\mathrm{I}(\mathrm{V}(S)))$, and by Proposition 1.2.4 (i), $\mathrm{V}(\mathrm{I}(\mathrm{V}(S))) \subseteq \mathrm{V}(S)$ since $S \subseteq \mathrm{V}(\mathrm{I}(S))$. Therefore $\mathrm{V}(S) = \mathrm{V}(\mathrm{I}(\mathrm{V}(S)))$. The proof of the second part is similar. $\square$

Remarks.

(i) As is shown in the proof of part (ii) of the last proposition, the ideal $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ of any point $(a_1, ..., a_n) \in \mathbb{A}^n$ is maximal.

(ii) Equality does not always hold in part (iii) of the last proposition, as shown by the following examples:

(a) Consider $I = \langle x^2 + 1 \rangle \subseteq \mathbb{R}[x]$. Then $1 \notin I$, so $I \neq \mathbb{R}[x]$. But $\mathrm{V}(I) = \varnothing$, so $\mathrm{I}(\mathrm{V}(I)) = \mathbb{R}[x] \supsetneq I$.

(b) Consider $X = [0, 1] \subseteq \mathbb{R}$. Then $\mathrm{I}(X) = 0$ and $\mathrm{V}(\mathrm{I}(X)) = \mathbb{R} \supsetneq X$.

These examples also show that not every ideal of $\Bbbk[x_1, \ldots, x_n]$ is the ideal of a set of points and that not every subset of $\mathbb{A}^n$ is algebraic.

We have a correspondence between subsets of $\mathbb{A}^n$ and ideals of $\Bbbk[x_1, \ldots, x_n]$ given by

$$X \mapsto I(X) \qquad \text{and} \qquad I \mapsto V(I).$$

By part (iv) of the last proposition, this correspondence is one-to-one when restricted to algebraic sets and ideals of sets of points. Given that not every subset of $\mathbb{A}^n$ is algebraic and not every ideal of $\Bbbk[x_1, \ldots, x_n]$ is the ideal of a set of points, we would like to examine the smallest algebraic set containing an arbitary subset of $\mathbb{A}^n$ and the smallest ideal of a set of points containing an arbitrary ideal of $\Bbbk[x_1, \ldots, x_n]$.

1.2.13 Definition. Let $X \subseteq \mathbb{A}^n$ and $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. The *closure of* X (in the Zariski topology) is the smallest algebraic set containing X (i.e. the smallest closed set containing X), and is denoted $\overline{X}$. The *closure of* I is the smallest ideal of a set of points that contains I, and is denoted $\overline{I}$. If $I = \overline{I}$, we say that I is *closed*.

Remark. Note that I is the ideal of a set of points if and only if $I = \overline{I}$.

1.2.14 Proposition.

(i) *If* $X \subseteq \mathbb{A}^n$*, then* $\overline{X} = \mathrm{V}(\mathrm{I}(X))$.

(ii) *If* $I \subseteq \Bbbk[x_1, \dots, x_n]$ *is an ideal, then* $\overline{I} = \mathrm{I}(\mathrm{V}(I))$.

PROOF: We will only prove (i), as the proof of (ii) is very similar. By part (iii) of Proposition 1.2.12, we have $X \subseteq \mathrm{V}(\mathrm{I}(X))$ Since $\mathrm{V}(\mathrm{I}(X))$ is an algebraic set, $\overline{X} \subseteq \mathrm{V}(\mathrm{I}(X))$. Conversely, since $X \subseteq \overline{X}$, $\mathrm{V}(\mathrm{I}(X)) \subseteq \mathrm{V}(\mathrm{I}(\overline{X}))$. By part (ii) of Proposition 1.2.7, we have $\mathrm{V}(\mathrm{I}(\overline{X})) = \overline{X}$, because $\overline{X}$ is an algebraic set. Therefore, $\mathrm{V}(\mathrm{I}(X)) \subseteq \overline{X}$, showing that $\overline{X} = \mathrm{V}(\mathrm{I}(X))$. □

1.2.15 Examples.

(i) If $X = (0, 1) \subseteq \mathbb{R}$, then the closure of X in the metric topology is $[0, 1]$, whereas the closure of X in the Zariski topology is $\mathbb{R}$.

(ii) If $\Bbbk$ is infinite and $X \subseteq \mathbb{A}^1$ is any infinite set of points then $\overline{X} = \mathbb{A}^1$. In particular, the Zariski closure of any non-empty open set is the whole line, or every non-empty open set is Zariski dense in the affine line.

(iii) Let $I = \langle x^2 \rangle$. Then $\overline{I} = \mathrm{I}(\mathrm{V}(I)) = \langle x \rangle$, so that $I \neq \overline{I}$ and I is not an ideal of a set of points.

1.3 Radical Ideals and the Nullstellensatz

In the previous section, we examined algebraic sets and ideals of sets of points. We saw that every algebraic set is the zero set of a finite set of polynomials. In this section, we will look for an intrinsic description of ideals of sets of points. We have already seen that not every ideal is the ideal of a set of points. Intuitively, an ideal I of $\Bbbk[x_1, \dots, x_n]$ is the ideal of a set of points whenever its generators intersect with the smallest possible multiplicity. However, since the multiplicity of any intersection is lost when we take the zero set of an ideal, as sets do not have any way of keeping track of multiplicity, we should not expect to get it back when we again take the ideal of that zero set.

1.3.1 Examples.

(i) Let $I = \langle x^2 + y^2 - 1, x \rangle \subseteq \mathbb{R}[x, y]$. The set $\mathrm{V}(x^2 + y^2 - 1)$ is the unit circle, and $\mathrm{V}(x)$ is the vertical line through the origin. The line intersects the circle twice, each time with “multiplicity one”. Therefore, our intuition would lead us to think that I is a closed ideal. This is correct, as

$$\overline{I} = \mathrm{I}(\mathrm{V}(I)) = \mathrm{I}(\{(0, -1), (0, 1)\}) = \langle x, y^2 - 1 \rangle = I.$$

(ii) Let $I = \langle x^2 + y^2 - 1, x - 1 \rangle \subseteq \mathbb{R}[x, y]$. The set $\mathrm{V}(x^2 + y^2 - 1)$ is the unit circle, and $\mathrm{V}(x - 1)$ is the vertical line that is tangent to the circle at $(1, 0)$. Because it only intersects the circle at one point, the intersection is with “multiplicity two”. Therefore, our intuition would lead us to think that I is not a closed ideal. This is indeed the case, as

$$\overline{I} = \mathrm{I}(\mathrm{V}(I)) = \mathrm{I}(\{(1, 0)\}) = \langle x - 1, y \rangle \neq I.$$

The zero sets of the generators of $\overline{I}$ are a vertical line through $(1,0)$ and a horizontal line through the origin, which intersect once at the point $(1,0)$ with "multiplicity one", again confirming our intuition.

Algebraically, if $I = \mathrm{I}(X)$ for some $X \subseteq \mathbb{A}^n$ then I is radical. Recall that an ideal I is *radical* if I is equal to its radical ideal $\sqrt{I}$,

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n > 0\}.$$

Equivalently, I is radical if the following condition holds:

$$a^n \in I \text{ implies that } a \in I \text{ for all } a \in R \text{ and } n > 0.$$

(See Proposition A.0.17.)

1.3.2 Examples.

(i) If $X \subseteq \mathbb{A}^n$ then $\mathrm{I}(X)$ is radical, because $f(x) = 0$ whenever $f^n(x) = 0$.

(ii) Every prime ideal is radical. For a proof, see Proposition A.0.18. However, not every proper radical ideal is prime. For example, the ideal

$$\langle x(x-1)\rangle = \mathrm{I}(\{0,1\})$$

of $\Bbbk[x]$ is radical, but it is not prime.

(iii) Let $I = \langle x^2 + y^2 - 1, x - 1\rangle \subseteq \mathbb{R}[x,y]$. Then $y^2 \in I$, because

$$y^2 = (x^2 + y^2 - 1) - (x+1)(x-1),$$

but $y \notin I$, simply because of the degrees of the y terms in the generators. Hence I is not radical. We already examined this example geometrically above.

(iv) Let $I = \langle y - x^2, y - x^3\rangle$. If $u = x(x-1)$, then

$$u^2 = [(y - x^2) - (y - x^3)](x-1) \in I,$$

but $u \notin I$, because of the degrees of the x terms in the generators. Hence I is not radical. Geometrically, $\mathrm{V}(y - x^2)$ is an upwards parabola through the origin, and $\mathrm{V}(y - x^3)$ intersects it twice, at the origin and at the point $(1,1)$. There are only two points of intersection, yet the degrees of the polynomials involved imply that there should be three, including multiplicity. Thus one of the points of intersection (in fact, the origin) has "multiplicity two".

We saw in the first of the above examples that if I is the ideal of a set of points then I is radical. Is the converse true? That is, if I is radical is it true that $I = \overline{I}$?

1.3.3 Proposition. *If I is an ideal of $\Bbbk[x_1, \ldots, x_n]$, then $I \subseteq \sqrt{I} \subseteq \overline{I}$. In particular, a closed ideal is radical.*

Proof: Clearly, $I \subseteq \sqrt{I}$. Suppose $f \in \sqrt{I}$. Then $f^n \in I$ for some $n \geq 1$. Since $f^n(x) = 0$ if and only if $f(x) = 0$, we have $f \in \mathrm{I}(\mathrm{V}(I))$. By Proposition 1.2.14, $\overline{I} = \mathrm{I}(\mathrm{V}(I))$, so $f \in \overline{I}$. Therefore, $\sqrt{I} \subseteq \overline{I}$. $\square$

It follows from the previous proposition that if $I = \sqrt{I}$ then $I = \overline{I}$ if and only if $\sqrt{I} = \mathrm{I}(\mathrm{V}(I))$. However, if $\Bbbk$ is not algebraically closed, it often happens that $\sqrt{I} \neq \mathrm{I}(\mathrm{V}(I))$:

1.3.4 Example. The polynomial $x^2 + 1 \in \mathbb{R}[x]$ is irreducible, so the ideal $\langle x^2 + 1 \rangle$ is maximal. Hence it is radical, and it is obviously proper. However,

$$\mathrm{I}(\mathrm{V}(x^2 + 1)) = \mathrm{I}(\varnothing) = \Bbbk[x]$$

so $\langle x^2 + 1 \rangle$ is not an ideal of a set of points. Clearly, $x^2 + 1$ can be replaced by any irreducible polynomial of degree at least 2 in any non-algebraically closed field.

However, the lack of algebraic closure in the base field is actually necessary for a counterexample. If the base field is algebraically closed, $\overline{I} = \sqrt{I}$. This result is due to Hilbert and is known as the Nullstellensatz, which is German for "zero points theorem".

1.3.5 Theorem (Nullstellensatz). *Suppose $\Bbbk$ is algebraically closed, and let $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. Then $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$, so $\overline{I} = \sqrt{I}$ and I is the ideal of a set of points if and only if $I = \sqrt{I}$.*

Proof: To come. $\square$

A related question is the characterization of maximal ideals of $\Bbbk[x_1, \ldots, x_n]$. We have seen that the ideal of a single point $(a_1, \ldots, a_n) \in \mathbb{A}^n$ is the maximal ideal $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Are all maximal ideals of $\Bbbk[x_1, \ldots, x_n]$ of this form? Again, the example of $\langle x^2 + 1 \rangle$ in $\mathbb{R}[x]$ shows this to be false in general. However, this is true when $\Bbbk$ is algebraically closed. Indeed, if I is a maximal ideal of $\Bbbk[x_1, \ldots, x_n]$ then I is radical, so by the Nullstellensatz I is the ideal of a set of points. Since I is a maximal ideal and taking zero sets reverses inclusions, $\mathrm{V}(I)$ is a non-empty minimal algebraic set, which must consist of a single point $(a_1, \ldots, a_n) \in \mathbb{A}^n$.

1.4 Irreducible Algebraic Sets

1.4.1 Definition. An algebraic set $X \subseteq \mathbb{A}^n$ is *irreducible* if $X \neq \varnothing$ and X cannot be expressed at $X = X_1 \cup X_2$, where X_1 and X_2 are algebraic sets not equal to X.

1.4.2 Proposition. *An algebraic set $X \subseteq \mathbb{A}^n$ is irreducible if and only if $\mathrm{I}(X)$ is prime.*

Proof: If X is irreducible then suppose that $f, g \in \Bbbk[x_1, \ldots, x_n]$ are such that $fg \in \mathrm{I}(X)$. Then $\langle fg \rangle \subseteq \mathrm{I}(X)$, so $X = \mathrm{V}(\mathrm{I}(X)) \subseteq \mathrm{V}(fg) = \mathrm{V}(f) \cup \mathrm{V}(g)$. Hence $X = (X \cap \mathrm{V}(f)) \cup (X \cap \mathrm{V}(g))$, so without loss of generality, $X = X \cap \mathrm{V}(f) \subseteq \mathrm{V}(f)$. Therefore $f \in \mathrm{I}(X)$ and $\mathrm{I}(X)$ is prime.

Suppose that $\mathrm{I}(X)$ is prime but is reducible, with $X = X_1 \cup X_2$. Then $\mathrm{I}(X) = \mathrm{I}(X_1) \cap \mathrm{I}(X_2)$. If $\mathrm{I}(X) = \mathrm{I}(X_1)$ then $X = X_1$, which is not allowed. Hence there is $f \in \mathrm{I}(X_1) \setminus \mathrm{I}(X)$. But for any $g \in \mathrm{I}(X_2)$, $fg \in \mathrm{I}(X_1) \cap \mathrm{I}(X_2) = \mathrm{I}(X)$, so since $f \notin \mathrm{I}(X)$ and $\mathrm{I}(X)$ is prime, $g \in \mathrm{I}(X)$. This implies that $\mathrm{I}(X) = \mathrm{I}(X_2)$ (and hence $X = X_2$), a contradiction. □

1.4.3 Examples.

(i) $\mathbb{A}^n$ is irreducible for all $n \geq 1$, because $\mathrm{I}(\mathbb{A}^n) = \{0\}$, which is a prime ideal.

(ii) If $(a_1, \ldots, a_n) \in \mathbb{A}^n$, then $\{x\}$ is irreducible, because

$$\mathrm{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$

which is a maximal ideal and therefore prime.

(iii) Since $\Bbbk[x_1, \ldots, x_n]$ is a UFD, any ideal generated by an irreducible polynomial is prime. If $\Bbbk$ is algebraically closed then $\mathrm{V}(p)$ is irreducible for every irreducible polynomial $p \in \Bbbk[x_1, \ldots, x_n]$ by the Nullstellensatz. Hence when $\Bbbk$ is algebraically closed there is a one to one correspondence between irreducible polynomials in $\Bbbk[x_1, \ldots, x_n]$ and irreducible hypersurfaces in $\mathbb{A}^n$.

Remark. If $X \subseteq \mathbb{A}^n$ is an irreducible algebraic set, then X is connected in the Zariski topology. Recall that a closed subset of a topological space is connected if and only if it is not the union of two disjoint closed proper subsets. However, if $X = X_1 \cup X_2$ where $X_1, X_2 \subseteq \mathbb{A}^n$ are closed, $X = X_1$ or $X = X_2$ by the irreducibility of X, showing that X is connected.

The correspondence between algebraic sets and ideals of sets of points takes irreducible algebraic sets to prime ideals, and prime ideals that are ideals of sets of points to irreducible algebraic sets. If $\Bbbk$ is algebraically closed, by combining the results of this chapter we have the following correspondence:

Geometry	**Algebra**
affine space $\mathbb{A}^n$	polynomial ring $\Bbbk[x_1, \ldots, x_n]$
algebraic set	radical ideal
irreducible algebraic set	prime ideal
point	maximal ideal

Remark. If $\Bbbk$ is not algebraically closed then there are more prime ideals than irreducible algebraic sets.

(i) distinct prime ideals may give the same algebraic set, e.g. $\mathrm{V}(\langle x^2+y^2\rangle) = \{(0,0)\} = \mathrm{V}(\langle x,y\rangle)$ in $\mathbb{R}^2$;

(ii) a prime ideal may have a reducible zero set, e.g. $\mathrm{V}(\langle x^2+y^2(y-1)^2\rangle) = \{(0,0),(0,1)\}$ in $\mathbb{R}^2$.

Mirroring the decomposition of an integer as the product of primes, every algebraic set decomposes as the union of finitely many irreducible algebraic sets.

1.4.4 Proposition. *Every algebraic set X is a finite union of irreducible algebraic sets.*

PROOF: Suppose that X is not the union of a finite number of irreducibles. Then, in particular, X itself is not irreducible, so $X = X_1 \cup X_1'$, where $X_1, X_1' \subsetneqq X$. Without loss of generality, we can assume that X_1 is not the union of a finite number of irreducibles. Repeating this we get an infinite strictly descending chain of algebraic sets $X \supsetneqq X_1 \supsetneqq \cdots$. But then $\mathrm{I}(X) \subsetneqq \mathrm{I}(X_1) \subsetneqq \cdots$ is an infinite strictly ascending chain of ideals in $\Bbbk[x_1,\ldots,x_n]$, a contradiction since $\Bbbk[x_1,\ldots,x_n]$ is Noetherian. □

Suppose that $X = X_1 \cup \cdots \cup X_r$, where each X_i is an irreducible algebraic set. In what sense is this decomposition unique? It can not literally be unique, as we could include any irreducible algebraic subset of X. However, this is the only obstruction to the uniqueness of the decomposition, since any irreducible algebraic subset of X must in fact already be contained in some X_j, as implied by the following lemma.

1.4.5 Lemma. *Let $X \subseteq \mathbb{A}^n$ be an irreducible algebraic set. If $X \subseteq X_1 \cup \cdots \cup X_r$, where $X_1,\ldots,X_r \subseteq \mathbb{A}^n$ are algebraic, then $X \subseteq X_j$ for some j.*

PROOF: Since $X \subseteq \bigcup_{i=1}^n X_i$, $X = \bigcup_{i=1}^n X \cap X_i$. By the irreducibility of X, we have $X = X \cap X_j$ for some j, so $X \subseteq X_j$. □

By successively discarding the X_i's that are included in one of the other X_j's, we therefore obtain a description of X as

$$X = X_1 \cup \cdots \cup X_m,$$

where each X_i is an irreducible algebraic set and $X_i \subsetneq X_j$ when $i \neq j$. We call such a decomposition an *irredundant decomposition* of X. Since the following proposition shows that an algebraic set has a unique irredundant decomposition, we will usually refer to an irredundant decomposition of X simply as the *decomposition* of X.

1.4.6 Proposition. *Every algebraic set X has a unique irredundant decomposition into irreducible algebraic sets.*

Proof: By Proposition 1.4.4, X is the finite union of irreducible algebraic sets. By possibly removing some constituents of this union, we have an irredundant decomposition $X = X_1 \cup \cdots \cup X_m$. Suppose that X also has an irredundant decompostion $X = Y_1 \cup \cdots \cup Y_n$. Then for any i, X_i is contained in some Y_{j_0} by Lemma 1.4.5. Similarly, $Y_{j_0} \subseteq X_{i_0}$ for some i_0, but this implies that $X_i \subseteq Y_{j_0} \subseteq X_{i_0}$, and since the decomposition is irredundant, $X_i = X_{i_0} = Y_{j_0}$. Therefore every X_i corresponds to a Y_j, and vice-versa. $\square$

1.4.7 Examples.

(i) Suppose that $f \in \Bbbk[x_1, \ldots, x_n]$ and $f = f_1^{r_1} \ldots f_m^{r_m}$ then

$$\mathrm{V}(f) = \mathrm{V}(f_1) \cup \cdots \cup \mathrm{V}(f_m).$$

If $\Bbbk$ is algebraically closed then this is a decomposition and $\mathrm{I}(\mathrm{V}(f)) = \langle f_1 \cdots f_m \rangle$.

(ii) Consider $X = \mathrm{V}(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) \subseteq \mathbb{C}^2$. Notice that

$$y^4 - x^2 = (y^2 - x)(y^2 + x),$$

and

$$y^4 - x^2y^2 + xy^2 - x^3 = (y^2 + x)(y - x)(y + x),$$

so $\mathrm{V}(y^2 + x)$ is an irreducible component of X. The other 3 points in X are $(0, 0)$, $(1, 1)$ and $(1, -1)$. But $(0, 0) \in \mathrm{V}(y^2 + x)$, so the decomposition of X is $\mathrm{V}(y^2 + x) \cup \{(1, 1)\} \cup \{(1, -1)\}$.

(iii) Consider $X = \mathrm{V}(x^2 + y^2(y - 1)^2) \subseteq \mathbb{R}^2$. $X = \{(0, 0), (0, 1)\}$, so X is reducible. But $f(x, y) = x^2 + y^2(y - 1)^2$ is irreducible in $\mathbb{R}[x, y]$. Indeed,

$$f(x, y) = (x + iy(y - 1))(x - iy(y - 1)).$$

Since $\mathbb{R}[x, y] \subseteq \mathbb{C}[x, y]$ are UFDs, if f factors in $\mathbb{R}[x, y]$ the decompostion must agree with the decomposition we have, up to constant multiple, but this is impossible.

Appendix A

Some Ring Theory

A.0.8 Definition. A *principal ring* is a ring for which every ideal is generated by a single element. A principal integral domain is called a *principal ideal domain*, or *PID* for short.

A.0.9 Proposition. $\Bbbk[x]$ *is a PID.*

PROOF: Since $\Bbbk[x]$ is clearly an integral domain, we only need to show that it is principal. Let I be an ideal of $\Bbbk[x]$, and let f be a monic polynomial of minimum degree in I. First, we show that f is unique, i.e. if g is another monic polynomial in I such that $\deg(g) = \deg(f)$, then $f = g$. Let $h = f - g$. Then $h \in I$, and since $\deg(h) < \deg(f)$ we must have $h = 0$, so $g = f$.

We now show that $I = \langle f \rangle$. Since $f \in I$, we have $\langle f \rangle \subseteq I$. To establish the reverse inclusion, fix $g \in I$. By the division algorithm, there exist $q, r \in \Bbbk[x]$ such that r is monic, $g = qf + r$, and either $r = 0$ or $\deg(r) < \deg(f)$. Since I is an ideal, $r = g - qf \in I$. By the minimality of the degree of f, we can not have $\deg(r) < \deg(f)$, so $r = 0$. Therefore, $g = qf$ and $g \in \langle f \rangle$. Since $g \in I$ was arbitrary, this shows that $I \subseteq \langle f \rangle$, and thus $I = \langle f \rangle$. □

A.0.10 Proposition. *If* $n > 1$, $\Bbbk[x_1, \ldots, x_n]$ *is not principal.*

PROOF: Suppose that I is principal. Let $I = \langle x_1, \ldots, x_n \rangle$. Then $I = \langle p \rangle$ for some $p \in \Bbbk[x_1, \ldots, x_n]$. Hence $p|q$ for every $q \in I$. In particular, $q|x_i$ for $1 \leq i \leq n$. Since the only elements in $\Bbbk[x_1, \ldots, x_n]$ that divide every indeterminate are the non-zero scalars, p must be a scalar. However, this a contradiction, as there are no non-zero scalars in I. Therefore, our assumption that I is principal is false, and $\Bbbk[x_1, \ldots, x_n]$ is not principal. □

A.0.11 Definition. We say that a ring R is *Noetherian* if every ideal of R is finitely generated.

A.0.12 Proposition. *Let R be a ring. Then the following are equivalent:*

(i) *R is Noetherian,*

(ii) *R satisfies the ascending chain condition on ideals, i.e. if*

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

is a chain of ideals of R, there exists a $k \in \mathbb{N}$ such that

$$I_k = I_{k+1} = \cdots = I_{k+n} = \cdots .$$

PROOF: Suppose R is Noetherian, and let

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

be a chain of ideals of R. Let

$$I = \bigcup_{k \in \mathbb{N}} I_k.$$

In general, the union of ideals is not an ideal, but the union of an increasing chain of ideals can easily be seen to be an ideal. Thus I is an ideal. Since R is Noetherian, I is finitely generated, i.e. there exist $a_1, \dots, a_m \in I$ such that $I = \langle a_1, \dots, a_m \rangle$. Let $k \in \mathbb{N}$ be such that $a_1, \dots, a_m \in I_k$. Then

$$I = I_k = I_{k+1} = \cdots = I_{k+n} = \cdots .$$

Conversely, suppose R satisfies the ascending chain condition but is not Noetherian, and let I be an ideal of R that is not finitely generated. Pick $a_0 \in I$, and let $I_0 = \langle a_0 \rangle$. Since I is not finitely generated, $I_0 \neq I$. Pick $a_1 \in I \setminus I_0$, and let $I_1 = \langle a_0, a_1 \rangle$. Since I is not finitely generated, $I_0 \subsetneq I_1 \neq I$. Continuing by induction, we get an increasing chain of ideals

$$I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots ,$$

in contradiction to the ascending condition on R. Therefore, our assumption that R is not Noetherian is false. □

We now establish that polynomial rings over an arbitrary Noetherian ring are Noetherian.

A.0.13 Theorem (Hilbert Basis Theorem). *If R is a Noetherian ring, then $R[x]$ is Noetherian.*

PROOF: Suppose $R[x]$ is not Noetherian, and let I is an ideal of $R[x]$ that is not finitely generated. Let f_0 be a polynomial of minimum degree in I. Continuing by induction, let f_{k+1} be a polynomial of minimum degree in $I \setminus \langle f_0, \dots, f_k \rangle$. For every $k \in \mathbb{N}$, let $d_k = \deg(f_k)$, and let a_k be the leading coefficient of f_k, and let $J = \langle \{a_k : k \in \mathbb{N}\} \rangle$. Since R is Noetherian and

$$\langle a_0 \rangle \subseteq \langle a_0, a_1 \rangle \subseteq \cdots \langle a_0, \dots, a_n \rangle \subseteq \cdots$$

is an increasing chain of ideals whose union is J, there exists an $n \in \mathbb{N}$ such that $J = \langle a_0, \ldots, a_n \rangle$.

Let $I_0 = \langle f_0, \ldots, f_n \rangle$. By construction, $f_{n+1} \notin I_0$. Since $J = \langle a_0, \ldots, a_n \rangle$ and $a_{n+1} \in J$, there exist $b_0, \ldots, b_n \in R$ such that $a_{n+1} = b_0 a_0 + \cdots + b_n a_n$. Then, as $f_{n+1} \in I \setminus I_0$, we have

$$g = m_{n+1} - x^{d_{n+1}-d_0} b_0 f_0 - \cdots - x^{d_{n+1}-d_n} b_n f_n \in I,$$

so $\deg(g) < \deg(f_{n+1})$. However, $g \notin I_0$, as $f_{n+1} \notin I_0$, contradicting the minimality of $\deg(f_{n+1})$. Therefore, our assumption that $R[x]$ is not Noetherian is false. □

A.0.14 Corollary. *If R is a Noetherian ring, then $R[x_1, \ldots, x_n]$ is Noetherian.*

PROOF: Since $R[x_1, \ldots, x_{n+1}] \cong R[x_1, \ldots, x_n][x_{n+1}]$, the result follows by induction from the Hilbert Basis Theorem. □

A.0.15 Definition. Let R be a ring, and I an ideal in R. The *radical* of I is the ideal

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n > 0\}.$$

If $I = \sqrt{I}$, we say that I is *radical*.

A.0.16 Proposition. *Let R be a ring, and I an ideal of R. Then $\sqrt{I}$ is an ideal of R.*

PROOF: If $a \in R$ and $b \in \sqrt{I}$, then $b^n \in I$ for some $n > 0$, so

$$(ab)^n = a^n b^n \in I,$$

and $ab \in \sqrt{I}$. If $a, b \in \sqrt{I}$, $a^m \in I$ and $b^n \in I$ for some $m, n > 0$. Therefore, by the Binomial Theorem,

$$(a+b)^{m+n+1} = \sum_{k=0}^{m+n+1} \binom{m+n-1}{k} a^k b^{m+n-1-k}.$$

For every $k \in \mathbb{N}$, either $k \geq m$, or $m-1 \geq k$ and $m+n-1-k \geq n$. This implies that for any $k \in \mathbb{N}$, either $a^k \in I$ or $b^{m+n-1-k} \in I$. Therefore, every term of the series expansion of $(a+b)^{m+n+1}$ is in I, showing that $(a+b)^{m+n+1} \in I$, or $a + b \in \sqrt{I}$. Therefore, $\sqrt{I}$ is an ideal. □

A.0.17 Proposition. *Let R be a ring, and I an ideal of R. Then I is radical if and only if $a^n \in I$ implies that $a \in I$ for all $a \in R$ and $n > 0$.*

PROOF: Suppose I is radical and $a^n \in I$. Then $a \in \sqrt{I} = I$. Conversely, suppose that $a^n \in I$ implies that $a \in I$ for all $a \in R$ and $n > 0$. Clearly, $I \subseteq \sqrt{I}$, so we only need to show that $\sqrt{I} \subseteq I$. If $a \in \sqrt{I}$ then $a^n \in I$ for some $n > 0$. Thus $a \in I$, showing that $\sqrt{I} \subseteq I$ and that I is radical. □

A.0.18 Proposition. *Let R be a ring, and I a prime ideal of R. Then I is radical.*

PROOF: Given $a \in R$ and $n > 0$ such that $a^n \in I$, we will show that $a \in I$ by induction on the n such that $a^n \in I$. If $n = 1$ and $a^n \in I$, then clearly $a \in I$. Suppose that $b^n \in I$ implies $b \in I$, and that $a^{n+1} \in I$. Since I is prime, either $a \in I$ or $a^n \in I$, in which case we also have $a \in I$ by our induction hypothesis. Therefore, by Proposition A.0.17, I is radical. $\square$