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 $\mathrm{V}(S) = \mathbb{A}^1$. □

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 $S = \{s_1, \ldots, s_n\}$, then we denote $\langle S \rangle$ by $\langle s_1, \ldots, s_n \rangle$.

1.2.4 Proposition.

(i) *If $S \subseteq T \subseteq \Bbbk[x_1, \ldots, x_n]$ then $\mathrm{V}(T) \subseteq \mathrm{V}(S)$.*

(ii) *If $S \subseteq \Bbbk[x_1, \ldots, x_n]$ 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 $g_i \in \Bbbk[x_1, \ldots, x_n]$. Then

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

since $x \in \mathrm{V}(S)$. □

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,

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

[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.0.9.

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

PROOF: See Appendix A. □

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 $\langle S \rangle$. □

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 $\Bbbk[x_1, \ldots, x_n]$ by taking the common zeros of its members. We would now like to do the converse and associate an ideal in $\Bbbk[x_1, \ldots, x_n]$ 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,

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

1.2.11 Examples.

(i) The following ideals of $\Bbbk[x]$ correspond to the algebraic sets of $\mathbb{A}^1$: $\mathrm{I}(\varnothing) = \langle 1 \rangle$, $\mathrm{I}(\{a_1, \ldots, a_n\}) = \langle (x - a_1) \cdots (x - a_n) \rangle$, 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) $\mathrm{I}(\varnothing) = \Bbbk[x_1, \ldots, x_n]$.
$\mathrm{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ *for any point* $(a_1, \ldots, a_n) \in \mathbb{A}^n$.
$\mathrm{I}(\mathbb{A}^n) = 0$ *if* $\Bbbk$ *is infinite.*

(iii) $S \subseteq \mathrm{I}(\mathrm{V}(S))$ *for any set of polynomials* $S \subseteq \Bbbk[x_1, \ldots, x_n]$.
$X \subseteq \mathrm{V}(\mathrm{I}(X))$ *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* $S \subseteq \Bbbk[x_1, \ldots, x_n]$.
$\mathrm{I}(\mathrm{V}(\mathrm{I}(X))) = \mathrm{I}(X)$ *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. □

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 $I \subseteq \Bbbk[x_1, \ldots, x_n]$ 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 $\Bbbk[x_1, \ldots, x_n]$ 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.0.14.)

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.0.15. 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, $\sqrt{I} \subseteq \overline{I}$. □

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: See Appendix C. □

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. □

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.

1.5 Classification of Irreducible Algebraic Sets in $\mathbb{A}^2$

While the irreducible algebraic subsets of $\mathbb{A}^1(\Bbbk)$ are easy to determine, this is not the case for $\mathbb{A}^n(\Bbbk)$ in general. Nevertheless, such a classification exists for $\mathbb{A}^2(\Bbbk)$. If $\Bbbk$ is finite then so is $\mathbb{A}^2(\Bbbk)$, so the irreducible algebraic subsets of $\mathbb{A}^2(\Bbbk)$ are precisely the singletons. Therefore, we assume that $\Bbbk$ is infinite for the remainder of this section.

There are only a few possible candidates for irreducible subsets of $\mathbb{A}^2$. Since $\Bbbk$ is infinite, $\mathbb{A}^2$ itself is irreducible, and any singleton is irreducible. Moreover, it is natural to consider the zero set $\mathrm{V}(f)$ of an irreducible polynomial $f \in \Bbbk[x, y]$. However, if $\mathrm{V}(f)$ consists of a finite set of points other than a singleton, then $\mathrm{V}(f)$ is reducible. But we will show that if $\mathrm{V}(f)$ is infinite it is always irreducible, and that the sets listed are precisely the irreducible algebraic subsets of $\mathbb{A}^2$. First, we will prove a proposition that is also of independent interest.

1.5.1 Proposition. *If $f, g \in \Bbbk[x, y]$ have no common factors then $\mathrm{V}(f, g) = \mathrm{V}(f) \cap \mathrm{V}(g)$ is at most a finite set of points.*

PROOF: Since f and g have no common factor in $\Bbbk[x, y] = \Bbbk[x][y]$, they have no common factors in $\Bbbk(x)[y]$. Therefore $\gcd(f, g)$ exists and is 1 in $\Bbbk(x)[y]$, so there are $s, t \in \Bbbk(x)[y]$ such that $sf + tg = 1$. Hence there is $d \in \Bbbk[x]$ such that $ds = a, dt = b$, where $a, b \in \Bbbk[x][y] = \Bbbk[x, y]$. Then $af + bg = d \in \Bbbk[x]$. Now if $(x_0, y_0) \in \mathrm{V}(f, g)$ then $d(x_0) = 0$, so there are at most finitely many possible values for x_0. Similarily, there are at most finitely many possible values for y_0, so $\mathrm{V}(f, g)$ is finite. □

Remark. Proposition 1.5.1 can be viewed as a weak form of Bézout's Theorem, which states 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.

1.5.2 Corollary. *If $f \in \Bbbk[x, y]$ is irreducible and X is an infinite algebraic set such that $X \subseteq \mathrm{V}(f)$, then $\mathrm{I}(X) = \langle f \rangle$. Therefore, $X = V(f)$ and $\mathrm{V}(f)$ is irreducible.*

PROOF: Clearly, $\langle f \rangle \subseteq \mathrm{I}(X)$. Suppose that there is $g \in \mathrm{I}(X)$ such that $g \notin \langle f \rangle$. Then f and g have no common factors, so $\mathrm{V}(f, g)$ is a finite set of points. But $X \subseteq \mathrm{V}(f, g)$ is infinite, so $\mathrm{I}(X) = \langle f \rangle$ and $X = \mathrm{V}(\mathrm{I}(X)) = \mathrm{V}(f)$. In particular, if $X = \mathrm{V}(f)$ then $\mathrm{I}(X) = \langle f \rangle$, which is prime given that f is irreducible, so $\mathrm{V}(f)$ is irreducible. □

1.5.3 Theorem. *Suppose $\Bbbk$ is infinite. Then the irreducible algebraic sets in $\mathbb{A}^2$ are*

(i) $\mathbb{A}^2$,
(ii) $\{(a, b)\}$, *for $a, b \in \Bbbk$,*
(iii) $\mathrm{V}(f)$ *where $f \in \Bbbk[x, y]$ is irreducible and $\mathrm{V}(f)$ is an infinite set.*

PROOF: We have already seen that all algebraic subsets of $\mathbb{A}^2$ of these forms are irreducible. Let $X \subseteq \mathbb{A}^2$ be an irreducible algebraic set. Assume that X is not $\mathbb{A}^2$ or a single point. Then $\mathrm{I}(X) \neq 0$, so there is at least on non-zero polynomial $f \in \mathrm{I}(X)$. Moreover, any irreducible factor of f is in the prime ideal $\mathrm{I}(X)$, since X is assumed to be irreducible. We may therefore assume that f is irreducible. Then Corollary 1.5.2 implies that $X = V(f)$ since X is infinite. □

1.5.4 Examples.

(i) In $\mathbb{R}^2$, $\mathrm{V}(y - x^2)$ is irreducible because $f = y - x^2$ is an irreducible polynomial and $\mathrm{V}(y - x^2)$ is infinite.
(ii) In $\mathbb{R}^2$, $\mathrm{V}(y^2 - x^2(x - 1))$ is also irreducible for the same reasons. Hence it is connected in the Zariski topology. However, it is not connected in the metric topology.

Appendix A

Some Ring Theory

A.0.5 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.0.6 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.0.7 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.0.8 Definition. We say that a ring R is *Noetherian* if every ideal of R is finitely generated.

A.0.9 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 $a_1, \ldots, a_m \in I$ such that $I = \langle a_1, \ldots, a_m \rangle$. Let $k \in \mathbb{N}$ be such that $a_1, \ldots, a_m \in I_k$. 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.0.10 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 $I \setminus \langle f_0, \ldots, f_k \rangle$. 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

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

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.0.11 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.0.12 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.0.13 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.0.14 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.0.15 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.0.14, I is radical. □

Appendix B

Transcendence Bases

B.0.16 Definition. Let K be a field, and let F be a subfield of K. A subset $U \subseteq K$ is said to be *algebraically independent* over F if for every $n \geq 1$, every non-zero $f \in F[x_1, \ldots, x_n]$, and all $u_1, \ldots, u_n \in U$, we have that $f(u_1, \ldots, u_n) \neq 0$. A *transcendence basis* of K over F is an algebraically independent subset of K that is maximal with respect to inclusion.

B.0.17 Examples.

(i) The empty set is algebraically independent. If $K = F$, it is also a transcendence basis of K over F.

(ii) Let F a fixed field and let $K = F(x_1, \ldots, x_n)$ be the fraction field of the ring $F[x_1, \ldots, x_n]$. We claim that $\{x_1, \ldots, x_n\}$ is a transcendence basis of K over F. It is clearly algebraically independent, as if $f \in F[t_1, \ldots, t_n]$ is such that $f(x_1, \ldots, x_n) = 0$, we have that $f = f(t_1, \ldots, t_n) = 0$. To show that $\{x_1, \ldots, x_n\}$ is a maximal algebraically independent set, we will show that $\{x_1, \ldots, x_n, p/q\}$ is algebraically dependent over F for any $p, q \in F[x_1, \ldots, x_n]$, $q \neq 0$. Define $f \in F[t_1, \ldots, t_{n+1}]$ by

$$f(t_1, \ldots, t_{n+1}) = p(t_1, \ldots, t_n) - q(t_1, \ldots, t_n)t_{n+1}.$$

Then $f \neq 0$, but $f(x_1, \ldots, x_n, p/q) = 0$, showing that $\{x_1, \ldots, x_n, p/q\}$ is algebraically dependent over F. Therefore, $\{x_1, \ldots, x_n\}$ is a transcendence basis of K over F.

B.0.18 Theorem. *Let K be a field, and let F be a subfield of K. Then:*

(i) *Every algebraically independent subset U of K is contained in some transcendence basis. In particular, since the empty set is algebraically independent, K has a transcendence basis.*

(ii) *If B_1 and B_2 are both transcendence bases of K over F, then* $\mathrm{card}(B_1) = \mathrm{card}(B_2)$.

PROOF:

(i) Let P be the partial order of algebraically independent subsets of K that contain U, ordered by inclusion. If C is a chain in P, then $\bigcup C$ is clearly algebraically independent, as any possible algebraic dependence involves finitely many elements of $\bigcup C$, which could all be chosen to be in the same member of C. Therefore, by Zorn's Lemma, P has a maximal element. However, by definition, such a maximal element is a transcendence basis of K containing U.

(ii) For the sake of sanity, we will assume that B_1 is finite. In the infinite case, it is argued using either multiple applications of Zorn's Lemma or transfinite induction. Suppose $B_1 = \{x_1, \ldots, x_m\}$, where $m \geq 1$ is the minimal cardinality of any transcendence basis. It suffices to show that if $w_1, \ldots, w_n$ are algebraically independent elements of K then $n \leq m$, as we could then swap B_1 and B_2 to get the opposite inequality. If every w_i is an x_j, there is nothing to prove, so by possibly reordering the w_i's, we can assume that $w_1 \neq x_i$ for $i = 1, \ldots, m$. Since $\{x_1, \ldots, x_m\}$ is a transcendence basis, $\{w_1, x_1, \ldots, x_m\}$ is algebraically dependent, so there is a non-zero polynomial $f_1 \in F[t_1, \ldots, t_{m+1}]$, which can clearly be chosen to be irreducible, such that $f_1(w_1, x_1, \ldots, x_m) = 0$. After possibly renumbering the x_j's we may write

$$f_1 = \sum_{j=1}^{k} g_j(w_1, x_2, \ldots, x_m) x_1^j$$

for some $k \geq 1$ and $g_1, \ldots, g_k \in F[t_1, \ldots, t_{m+1}$. No irreducible factor of g_k vanishes on $(w_1, x_2, \ldots, x_n)$, otherwise w_1 would be a root of two distinct irreducible polynomials over $F(x_1, \ldots, x_m)$. Hence x_1 is algebraic over $F(w_1, x_2, \ldots, x_m)$ and $w_1, x_2, \ldots, x_m$ are algebraically independent over F, as otherwise the minimality of m would be contradicted. Continuing inductively, suppose that after a suitable renumbering of $x_1, \ldots, x_m$ we have found $w_1, \ldots, w_r$, $r < n$, sch that K is algebraiic over $F(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m)$. Then there exists a non-zero $f \in F[t_1, \ldots, t_{m+1}]$ such that

$$f(w_{r+1}, w_1, \ldots, w_r, x_{r+1}, \ldots, x_m) = 0.$$

Since the w_i's are algebraically independent over F, it follows by the same argument as in the case above that some x_j, which we can assume to be x_{r+1}, is algebraic over $F(w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m)$. Since a tower of algebraic extensions is algebraic, it follows that K is algebraic over $F(w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m)$. If $n \geq m$, we can continue inductively and replace all of the x_j's by w_i's to see that K is algebraic over $F(w_1, \ldots, w_m)$, showing that $n = m$, as desired. □

B.0.19 Definition. Let K be a field, and let F be a subfield of K. The *transcendence degree* of K over F is the cardinality of any transcendence basis of K over F.

Appendix C

A Proof of the Nullstellensatz

We begin by examining extensions of rings that are analogous to algebraic extensions of fields, where an arbitrary polynomial with coefficients in the base field is replaced with a monic polynomial with coefficients in the base ring.

C.0.20 Definition. Let S be a ring and R be a subring of S.

(i) An element $s \in S$ is *integral over* R if s is the root of a monic polynomial in $R[x]$.

(ii) The ring S is an *integral extension* of R, or just *integral over* R, if every $s \in S$ is integral over R.

(iii) The *integral closure* of R in S is the set of elements of S that are integral over R.

One fundamental fact about integral extensions is that they are transitive, i.e. the composition of integral extensions is also an integral extension. In the proof we use a special case of a notion from the theory of modules. If R and S are rings and $R \subseteq S$, we say that S is a finitely generated R-module if there exists a finite set $A \subseteq S$ such that $S = RA$.

C.0.21 Proposition. *Let T be a ring and R be a subring of T. If $t \in T$, then the following are equivalent:*

(i) *t is integral over R;*

(ii) *$R[t]$ is a finitely generated R-module;*

(iii) *there exists a subring S of T such that $t \in S$ and S is a finitely generated R-module.*

Proof: Suppose that t is integral over R. There then exist $r_0, ..., r_{n-1} \in R$ such that

$$t^n + r_{n-1}t^{n-1} + \cdots + r_1 t + r_0 = 0,$$

or

$$t^n = -(r_{n-1}t^{n-1} + \cdots + r_1 t + r_0),$$

so t^n and all higher powers of t can be expressed as R-linear combinations of $t^{n-1}, \ldots, t, 1$. Then $R[t] = R\{t^{n-1}, \ldots, t, 1\}$ is a finitely generated R-module.

Suppose $R[t]$ is a finitely generated R-module. Since $t \in R[t]$ and $R[t] \subseteq T$, this means that $S = R[t]$ satisfies the conditions of (iii).

Suppose there exists a subring S of T such that $t \in S$ and S is a finitely generated R-module. Let $A \subseteq S$ be a finite set such that $S = RA$. Enumerate the elements of A by $A = \{a_1, \ldots, a_n\}$. For $i = 1, \ldots, n$, the element ta_i is an element of S and can thus be written as R-linear combinations of $a_1, \ldots, a_n$, i.e. for some coefficients $c_{ij} \in R$,

$$ta_i = \sum_{j=1}^{n} c_{ij} a_j.$$

By rearranging terms, we obtain

$$\sum_{j=1}^{n} (\delta_{ij} t - c_{ij}) a_j = 0,$$

where δ_{ij} is the Kronecker delta. Let B be the $n \times n$ matrix whose i, j entry is $\delta_{ij} t - c_{ij}$, and let v be the $n \times 1$ column vector whose entries are $a_1, \ldots, a_n$. These equations then simply amount to saying that $Bv = 0$; it follows from Cramer's Rule that $(\det B)a_i = 0$ for $i = 1, \ldots, n$. Since $1 \in S$ is an R-linear combination of $a_1, \ldots, a_n$, it follows that $\det B = 0$. But $B = tI - C$, where C is the matrix whose i, j entry is c_{ij}. Thus, t is a root of the monic polynomial $\det(xI - C) \in R[x]$, i.e. t is integral over R. □

C.0.22 Proposition. *Let R, S, and T be rings such that $R \subseteq S \subseteq T$. If T is integral over S and S is integral over R, then T is integral over R.*

Proof: Fix $t \in T$. Since T is integral over S, there exist $s_0, ..., s_{n-1} \in S$ with

$$t^n + s_{n-1} t^{n-1} + \cdots + s_1 t + s_0 = 0.$$

Since each $s_i \in S$ is integral over R, by Proposition C.0.21, each ring $R[s_i]$ is a finitely generated R-module, implying that $R[s_0, \ldots, s_{n-1}]$ is a finitely generated R-module as well. In addition, since the monic polynomial displayed above has coefficients in $R[s_0, \ldots, s_{n-1}]$, t is integral over $R[s_0, \ldots, s_{n-1}]$, so $R[s_0, \ldots, s_{n-1}, t]$ is a finitely generated R-module. Hence, t is integral over R by Proposition C.0.21. □

If either ring in an integral extension is a field, then the integral extension is simply a field extension.

C.0.23 Proposition. *Let R be a ring and S be an integral domain that is integral over R. Then, R is a field if and only if S is a field.*

PROOF: Suppose R is a field and fix a non-zero $s \in S$. Then, s is integral over R, so there exist $a_0, a_1, \ldots, a_{n-1} \in R$ such that

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0.$$

Since S is an integral domain, we may assume $a_0 \neq 0$, as otherwise s factors out of the left-hand side of the equation, implying that s is a zero divisor. Then

$$s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1) = -a_0,$$

and since $(-1/a_0) \in R$, this shows that

$$s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1)(-1/a_0) = -a_0(-1/a_0) = 1,$$

so s is invertible. Therefore, S is a field.

Conversely, suppose that S is a field and fix a non-zero $r \in R$. Since $r^{-1} \in S$ is integral over R, there exist $a_0, a_1, \ldots, a_{n-1} \in R$ such that

$$r^{-m} + a_{m-1}r^{-m+1} + \cdots + a_1 r^{-1} + a_0 = 0.$$

Then

$$r^{-1} = -(a_{m-1} + \cdots + a_1 r^{m-2} + a_0 r^{m-1}) \in R.$$

Therefore, R is a field. □

Most rings we deal with in these notes are also vector spaces over some field $\Bbbk$, where the vector space addition is the same as addition in the ring, and the scalar multiplication coincides with multiplication in the ring, after identifying the scalar $\alpha \in \Bbbk$ with the element $\alpha \cdot 1$ of the ring. Such rings are called $\Bbbk$-*algebras*. We deal with $\Bbbk$-algebras elsewhere in these notes, but repeat some basic facts about them here.

C.0.24 Examples.

(i) $\Bbbk[x_1, \ldots, x_n]$ is a $\Bbbk$-algebra.

(ii) Let A be a $\Bbbk$-algebra and I an ideal of A. Then I is also a vector subspace of A, and the ring quotient of A by I agrees with the vector space quotient of A by I. Hence A/I is also a $\Bbbk$-algebra.

Given $\Bbbk$-algebras A and B, we define a $\Bbbk$-*algebra homomorphism* from A to B to be a ring homomorphism $\varphi : A \to B$ such that $\varphi(\alpha) = \alpha$ for every $\alpha \in \Bbbk$.

C.0.25 Examples.

(i) Let A be a $\Bbbk$-algebra and I be an ideal of A. The quotient map $\varphi : A \to A/I$ is then a $\Bbbk$-algebra homomorphism.

(ii) The map $\varphi : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n]$ defined by

$$\varphi(a_n x^n + \cdots + a_1 x + a_0) = \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0}$$

is a ring homomorphism that is not a $\mathbb{C}$-algebra homomorphism.

Let A be a $\Bbbk$-algebra. We say that A is *finitely generated* if $A = \Bbbk[a_1, \ldots, a_n]$ for some $a_1, \ldots, a_n \in A$. Moreover, $y_1, \ldots, y_n \in A$ are said to be *algebraically independent* if there is no non-zero $f \in \Bbbk[x_1, \ldots, x_n]$ such that $f(y_1, \ldots, y_n) = 0$, or equivalently, if the $\Bbbk$-algebra homomorphism

$$\varphi : \Bbbk[x_1, \ldots, x_n] \to \Bbbk[y_1, \ldots, y_n]$$

defined by $\varphi(x_i) = y_i$ is an isomorphism.

C.0.26 Theorem (Noether Normalization Lemma). *Let A be an integral domain that is a finitely generated $\Bbbk$-algebra, and let d be the transcendence degree of the fraction field of A over $\Bbbk$. There exist elements $y_1, \ldots, y_d \in A$ which are algebraically independent over $\Bbbk$ and are such that A is integral over $\Bbbk[y_1, \ldots, y_d]$.*

Proof: Suppose that $A = \Bbbk[r_1, \ldots, r_n]$. If $r_1, \ldots, r_n$ are already algebraically independent over $\Bbbk$, then we are done. If not, there is a non-trivial polynomial relation amongst the r_i's, i.e. there exists a finite family $\mathcal{F}$ of distinct tuples $j = (j_1, \ldots, j_n)$ of non-negative integers and corresponding non-zero cofficients $a_j \in \Bbbk$ such that

$$\sum_{j \in \mathcal{F}} a_j r_1^{j_1} \ldots r_n^{j_n} = 0.$$

Let $m = (1, m_2, \ldots, m_n)$ be a vector of positive integers, and let

$$y_2 = r_2 - r_1^{m_2}, \ldots, y_n = r_n - r_1^{m_n}.$$

We use the dot product $j \cdot m$ to denote $j_1 + m_2 j_2 + \cdots + m_n j_n$. Substituting $r_i = y_i + r_1^{m_i}$ into the above relation, we get

$$\sum_{j \in \mathcal{F}} a_j r_1^{j \cdot m} + f(r_1, y_2, \ldots, y_n) = 0,$$

where f is a polynomial in which no pure power of r_1 appears. Let l be an integer greater than any component of a vector in $\mathcal{F}$, and let $m = (1, l, l^2, \ldots, l^{n-1})$. Then, all $j \cdot m$ are distinct for those j such that $a_j \neq 0$. In this way, we obtain an integral equation for r_1 over $\Bbbk[y_2, \ldots, y_n]$, implying that $\Bbbk[y_2, \ldots, y_n][r_1]$ is integral over $\Bbbk[y_2, \ldots, y_n]$ by Proposition C.0.21. However, $A = \Bbbk[r_1, y_2, \ldots, y_n]$ by the definition of the y_i's; it follows that A is integral over $\Bbbk[y_2, \ldots, y_n]$.

We now proceed inductively, applying the same construction to $\Bbbk[y_2, \ldots, y_n]$ and using the transitivity of integral extensions, to shrink the number of y's down to an algebraically independent set. Thus, there exist algebraically independent elements $y_1, \ldots, y_k \in A$ such that A is integral over $\Bbbk[y_1, \ldots, y_k]$. Since $y_1, \ldots, y_k$ are still algebraically independent in the fraction field of A, and since A is integral over $\Bbbk[y_1, \ldots, y_k]$, they generate the fraction field of A over $\Bbbk$. Therefore, $y_1, \ldots, y_k$ form a transcendence basis of the fraction field of A over $\Bbbk$, and $k = d$ as desired. □

In the particular case of fields, the Noether Normalization Lemma can be restated more naturally in the language of field extensions.

C.0.27 Corollary. *Let L be a field extension of $\Bbbk$ that is finitely generated as a $\Bbbk$-algebra. Then L is algebraic over $\Bbbk$.*

PROOF: By the Noether Normalization Lemma, there exist algebraically independent $y_1, \ldots, y_n \in L$ such that L is integral over $\Bbbk[y_1, \ldots, y_n]$. Since L is a field, by Proposition C.0.23, $\Bbbk[y_1, \ldots, y_n]$ is also a field. But this implies $\Bbbk[y_1, \ldots, y_n] = \Bbbk$, as no polynomial ring over a field is a field. Therefore, L is integral over $\Bbbk$, i.e. L is algebraic over $\Bbbk$. □

C.0.28 Theorem (Weak Nullstellensatz). *Suppose $\Bbbk$ is algebraically closed. Then every maximal ideal in $\Bbbk[x_1, \ldots, x_n]$ is of the form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $(a_1, \ldots, a_n) \in \mathbb{A}^n$. Moreover, if I is a proper ideal of $\Bbbk[x_1, \ldots, x_n]$ then $\mathrm{V}(I) \neq \varnothing$.*

PROOF: Let $R = \Bbbk[x_1, \ldots, x_n]$ and let I be a maximal ideal of R. Then R/I is a field extension of $\Bbbk$ and finitely generated as a $\Bbbk$-algebra. By Corollary C.0.27, it is an algebraic extension of $\Bbbk$. Since $\Bbbk$ is algebraically closed, $R/I = \Bbbk$. Let $\varphi : R \to \Bbbk$ be the quotient map, and let $a_i = \varphi(x_i)$ for $i = 1, \ldots, n$. Let $I' = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. For $i = 1, \ldots, n$, we have

$$\varphi(x_i - a_i) = \varphi(x_i) - \varphi(a_i) = a_i - \varphi(a_i) = a_i - a_i = 0,$$

so $\varphi(f) = 0$ for every $f \in I'$. Hence $I' \subseteq I$. However, I' is maximal, so $I = I'$.

Let I be a proper ideal of $\Bbbk[x_1, \ldots, x_n]$. Then I is contained in a maximal ideal, so there exist $a_1, \ldots, a_n \in \Bbbk$ such that

$$I \subseteq \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$

Thus

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

so $(a_1, \ldots, a_n) \in \mathrm{V}(I)$, and $\mathrm{V}(I) \neq \varnothing$. □

C.0.29 Theorem (Strong Nullstellensatz). *Suppose $\Bbbk$ is algebraically closed, and let $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. Then $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$, or $\overline{I} = \sqrt{I}$, so I is the ideal of a set of points if and only if $I = \sqrt{I}$.*

PROOF: Since $\sqrt{I} \subseteq \mathrm{I}(\mathrm{V}(I))$, we only need to prove the reverse inclusion. Fix $g \in \mathrm{I}(\mathrm{V}(I))$. By the Hilbert Basis Theorem, we have $I = \langle f_1, \ldots, f_m \rangle$ for some $f_1, \ldots, f_m \in \Bbbk[x_1, \ldots, x_n]$. Let us introduce a new variable x_{n+1} and consider the ideal $I' = \langle f_1, \ldots, f_m, 1 - x_{n+1} g \rangle$ of $\Bbbk[x_1, \ldots, x_n, x_{n+1}]$. If $f_1, \ldots, f_m$ vanish at $(a_1, \ldots, a_{n+1}) \in \mathbb{A}^{n+1}$, then g also vanishes at $(a_1, \ldots, a_{n+1})$, as $g \in \mathrm{I}(\mathrm{V}(I))$, so $1 - x_{n+1} g$ is non-zero. Hence $\mathrm{V}(I') = \varnothing$. By the Weak Nullstellensatz, I'

is not proper, i.e. $1 \in I'$. Therefore, there exist $h_1, \ldots, h_{n+1} \in \Bbbk[x_1, \ldots, x_{n+1}]$ such that

$$1 = h_1 f_1 + \cdots + h_n f_n + h_{n+1}(1 - x_{n+1} g).$$

Working in the field of fractions of $\Bbbk[x_1, \ldots, x_{n+1}]$, substitute g^{-1} for x_{n+1} and multiply both sides by an appropriate power g^k of g to clear denominators on the right-hand side and give

$$g^k = \tilde{h}_1 f_1 + \cdots + \tilde{h}_n f_n + \tilde{h}_{n+1}(1 - g^{-1} g) = \tilde{h}_1 f_1 + \cdots + \tilde{h}_n f_n \in I,$$

where $\tilde{h}_i(x_1, \ldots, x_n) := g^k h_i(x_1, \ldots, x_n, g^{-1}) \in \Bbbk[x_1, \ldots, x_n]$ for all $i = 1, \ldots, n$. Hence $g \in \sqrt{I}$. Therefore, $\mathrm{I}(\mathrm{V}(I)) \subseteq \sqrt{I}$ and $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$. $\square$