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.0.7.

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.0.12.)

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.0.13. 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.

Chapter 2

Affine Varieties

In this chapter, we will assume that $\Bbbk$ is infinite, since when $\Bbbk$ is finite the only irreducible algebraic sets in $\mathbb{A}^n(\Bbbk)$ are singletons.

2.0.5 Definition. An irreducible affine algebraic set is called an *affine (algebraic) variety*, or simply a *variety* if the context is clear. Any variety X is endowed with the induced (Zariski) topology, whose open sets are of the form $X \bigcap U$ for some open subset $U \subseteq \mathbb{A}^n$.

2.1 Coordinate Rings

Since affine varieties are defined by polynomials over a field, the most natural functions to consider on an affine variety are those that come from evaluating polynomials over the base field.

2.1.1 Definition. Let $X \subseteq \mathbb{A}^n$ be an affine variety. A function $F : X \to \Bbbk$ is called a *polynomial function* if there is an $f \in \Bbbk[x_1, \ldots, x_n]$ such that $F(x) = f(x)$ for all $x \in X$.

If we wish to consider all polynomial functions on X, we can not simply take the entire polynomial ring $\Bbbk[x_1, \ldots, x_n]$, because two polynomials may give the same function when restricted to X. If $\Bbbk$ is finite, this is no surprise, because many polynomials in $\Bbbk[x_1, \ldots, x_n]$ determine the same function on $\mathbb{A}^n$. However, if $\Bbbk$ is infinite then polynomials in $\Bbbk[x_1, \ldots, x_n]$ determine unique functions on $\mathbb{A}^n$, so if $f, g \in \Bbbk[x_1, \ldots, x_n]$, then f and g determine the same polynomial function on X if and only if $f - g \in \mathrm{I}(X)$. Therefore, at least when $\Bbbk$ is infinite, we can identify the polynomial functions on X with the quotient ring $\Bbbk[x_1, \ldots, x_n]/\mathrm{I}(X)$.

2.1.2 Definition. Let $X \subseteq \mathbb{A}^n$ be an affine variety. The quotient ring $\Gamma(X) = \Bbbk[x_1, \ldots, x_n]/\mathrm{I}(X)$ is called the *coordinate ring* of X. Other common notations are $\Bbbk[X]$ and $A(X)$.

One can look at $\Bbbk[x_1, \ldots, x_n]/\operatorname{I}(X)$ to determine the irreducibility of X, since $\Bbbk[x_1, \ldots, x_n]/\operatorname{I}(X)$ is a domain if and only if $\operatorname{I}(X)$ is prime, which happens if and only if X is irreducible.

2.1.3 Examples.

(i) If $X = \mathbb{A}^n$ then $\operatorname{I}(X) = 0$, so $\Gamma(X) = \Bbbk[x_1, \ldots, x_n]$.

(ii) If X is a single point then $\Gamma(X) = \Bbbk$ since defining a function on a point is the same as fixing a value for that point.

(iii) If $X = \operatorname{V}(y - x^2) \subseteq \mathbb{A}^2$ then $\Gamma(X) = \Bbbk[x, y]/\langle y - x^2 \rangle \cong \Bbbk[\overline{x}]$, where $\overline{x}$ is the residue class of x in $\Gamma(X)$.

2.1.4 Theorem. *If X is an affine variety then $\Gamma(X)$ is Noetherian.*

PROOF: Suppose $X \subseteq \mathbb{A}^n$. Let $q : \Bbbk[x_1, \ldots, x_n] \to \Gamma(X)$ be the quotient map, and let I be an ideal of $\Gamma(X)$. Then $q^{-1}(I)$ is an ideal of $\Bbbk[x_1, \ldots, x_n]$, which is Noetherian, so $q^{-1}(I) = \langle f_1, \ldots, f_k \rangle$ for some $f_1, \ldots, f_k \in \Bbbk[x_1, \ldots, x_n]$. Therefore, $I = \langle q(f_1), \ldots, q(f_k) \rangle$, showing that $\Gamma(X)$ is Noetherian. □

The coordinate ring $\Gamma(X)$ has additional structure besides its ring structure. It is also a vector space over $\Bbbk$, where the vector space addition is the same as addition in the ring, and scalar multiplication coincides with multiplication in the ring. Such a ring is called a $\Bbbk$-*algebra*.

2.1.5 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.

2.2 Polynomial Maps

Continuing the theme of the previous section, we will now examine maps between two affine varieties. Since affine varieties are defined by the vanishing of polynomials, the natural functions between affine varieties are those whose components are polynomial functions.

2.2.1 Definition. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be two affine varieties. A function $\varphi : X \to Y$ is called a *polynomial map* if there are polynomials $f_1, \ldots, f_m \in \Bbbk[x_1, \ldots, x_n]$ such that $\varphi(x) = (f_1(x), \ldots, f_m(x))$ for every $x \in X$.

2.2.2 Examples.

(i) Polynomial functions $F : X \to \Bbbk \cong \mathbb{A}^1$ are polynomial maps.

(ii) Any linear map $\mathbb{A}^n \to \mathbb{A}^m$ is a polynomial map.

(iii) Affine maps $\mathbb{A}^n \to \mathbb{A}^m : x \mapsto Ax + b$, where A is an $m \times n$ matrix over $\Bbbk$ and $b \in \mathbb{A}^m$, are polynomial maps. If A is invertible then the map $x \mapsto Ax + b$ is called a *affine coordinate change*.
(iv) Projections and inclusions are polynomial maps.
(v) The map $\varphi : \mathbb{A}^1 \to \mathrm{V}(y^2 - x^3) \subseteq \mathbb{A}^2$ given by $\varphi(t) = (t^2, t^3)$ is a polynomial map.

Polynomial maps give the natural notion of equivalence for affine varieties.

2.2.3 Definition. Let X and Y be affine varieties. A polynomial map $\varphi : X \to Y$ is said to be an *isomorphism* if it is a bijection and its inverse is a polynomial map. We say that X and Y are *isomorphic* if there exists an isomorphism $\varphi : X \to Y$, in which case we write $X \cong Y$.

2.2.4 Examples.
(i) $\varphi : \mathrm{V}(y - x^2) \subseteq \mathbb{A}^2 \to \mathbb{A}^1 : (x, x^2) \mapsto x$ has a polynomial inverse $\varphi^{-1}(t) = (t, t^2)$, so $\mathrm{V}(y - x^2) \cong \mathbb{A}^1$.
(ii) $\varphi : \mathbb{A}^1 \to X = V(y^2 - x^3) \subseteq \mathbb{A}^2 : t \mapsto (t^2, t^3)$ is a bijective polynomial map. Indeed, in the metric topology over $\mathbb{C}$, φ is a homeomorphism. However, φ does not have a polynomial inverse. Suppose that $\varphi^{-1} : X \to \mathbb{A}^1$ is polynomial. Then φ^{-1} is a polynomial function on X, so it is an element of $\Gamma(X)$. Moreover, $\Gamma(X) = \Bbbk[x, y]/\langle y^2 - x^3 \rangle$. Since $\overline{y}^2 = \overline{x}^3$ in $\Gamma(X)$, any polynomial $f(x, y)$ can be written as $p(\overline{x}) + \overline{y}q(\overline{x})$ in $\Gamma(X)$. Therefore $\varphi^{-1}(x, y) = p(x) + yq(x)$ for some $p, q \in \Bbbk[x]$, and the composition $t \mapsto (t^2, t^3) \mapsto p(t^2) + t^3 q(t^2)$, an expression of degree at least 2 in t. In particular, $\varphi^{-1}(t^2, t^3) \neq t$, so φ does not have a polynomial inverse.
(iii) Any two varieties which are isomorphic via an affine coordinate change are said to be *affinely equivalent*. For example, any conic (a curve given by a polynomial of degree 2) is affinely equivalent to a parabola, a hyperbola, an ellipse, the union of two lines, or a double line.

2.2.5 Proposition. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties and $\varphi : X \to Y$ a polynomial map. Then:*

(i) *$\varphi^{-1}(Z) \subseteq X$ is an algebraic set for every algebraic set $Z \subseteq Y$.*
(ii) *If X is irreducible, then $\overline{\varphi(X)}$ is irreducible.*

Proof:
(i) This is simply that statement that φ is continuous in the Zariski topology. Indeed, if $Z = \mathrm{V}(g_1, \ldots, g_r)$ then $\varphi^{-1}(Z) = \mathrm{V}(g_1 \circ \varphi, \ldots, g_r \circ \varphi)$.
(ii) Let $Z = \overline{\varphi(X)}$. Suppose that $Z = Z_1 \cup Z_2$, where Z_1 and Z_2 are algebraic. Then $X = \varphi^{-1}(Z) = \varphi^{-1}(Z_1) \cup \varphi^{-1}(Z_2)$. By part (i), $\varphi^{-1}(Z_1)$ and $\varphi^{-1}(Z_2)$ are algebraic subsets of X. Therefore, by the irreducibility of X, either $X = \varphi^{-1}(Z_1)$ or $X = \varphi^{-1}(Z_2)$. Without loss of generality, assume that $X = \varphi^{-1}(Z_1)$. Then $\varphi(X) \subseteq Z_1$, so $\overline{\varphi(X)} \subseteq \overline{Z_1} = Z_1$, and $\overline{\varphi(X)} = Z_1$. Therefore, $\overline{\varphi(X)}$ is irreducible. □

So far we have three ways to test whether an algebraic set $X \subseteq \mathbb{A}^n$ is irreducible. We may ask:

(i) Is $\mathrm{I}(X)$ prime?
(ii) Is $\Bbbk[x_1, \ldots, x_n]/\mathrm{I}(X)$ an integral domain?
(iii) Is X the closure of the image of an irreducible algebraic set under a polynomial map?

2.2.6 Example. Consider $X = \mathrm{V}(y-x^2, z-x^3) \subseteq \mathbb{A}^3$, the twisted cubic. Note that $\mathrm{I}(X) = \langle y - x^2, z - x^3 \rangle$. One inclusion is obvious, and for any $f \in \mathrm{I}(X)$, by applying the division algorithm twice (once with respect to y and once with respect to z), we can write $f(x, y, z) = (y-x^2)g(x, y, z)+(z-x^3)h(x, z)+r(x)$. For all $x \in \Bbbk$, $(x, x^2, x^3) \in X$, so $r(x) = 0$ for all $x \in \Bbbk$, hence $r = 0$ and $f \in \langle y - x^2, z - x^3 \rangle$. In the quotient ring $\overline{y} = \overline{x}^2$ and $\overline{z} = \overline{x}^3$, so $\Bbbk[x, y, z]/I(X)$ is isomorphic to $\Bbbk[x]$, an integral domain. Therefore X is irreducible. On the other hand, $\varphi : \mathbb{A}^1 \to X, t \mapsto (t, t^2, t^3)$, is a surjective polynomial map. Therefore, since $\mathbb{A}^1$ is irreducible, so is $X = \varphi(\mathbb{A}^1)$.

A polynomial map between affine varieties acts naturally on their coordinate rings. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties and $\varphi : X \to Y$ a polynomial map. Pick $f_1, \ldots, f_m \in \Bbbk[x_1, \ldots, x_n]$ such that $\varphi(x) = (f_1(x), \ldots, f_m(x))$. If $g \in \Bbbk[x_1, \ldots, x_n]$ then $g \circ \varphi = g(f_1, \ldots, f_m)$ is a polynomial in $\Bbbk[x_1, \ldots, x_n]$. If $g \in \mathrm{I}(Y)$, then

$$(g \circ \varphi)(x) = g(f_1(x), \ldots, f_m(x)) = 0$$

for every $x \in X$ because $\varphi(x) \in Y$. Thus $g \circ \varphi \in \mathrm{I}(X)$. It follows that φ induces a well-defined map $\varphi^* : \Gamma(Y) \to \Gamma(X)$ given by

$$\varphi^*(g + \mathrm{I}(Y)) = (g \circ \varphi) + \mathrm{I}(X).$$

We call φ^* the *pullback* of φ. As is shown by the next proposition, the pullback completely determines the original polynomial map.

2.2.7 Proposition. *Let X and Y be affine varieties. If $\varphi : X \to Y$ and $\psi : X \to Y$ are polynomial maps such that $\varphi^* = \psi^*$, then $\varphi = \psi$.*

Proof: Consider $\Gamma(Y)$ as a quotient of $\Bbbk[y_1, \ldots, y_m]$. We have $\varphi^*(\overline{y_i}) = \psi^*(\overline{y_i})$, so $y_i \circ \varphi = y_i \circ \psi$. Let $\varphi = (f_1, \ldots, f_m)$ and $\psi = (g_1, \ldots, g_m)$ for some $f_1, \ldots, f_m, g_1, \ldots, g_m \in \Bbbk[x_1, \ldots, x_n]$. Then $y_i \circ \varphi = f_i$ and $y_i \circ \psi = g_i$, showing that $f_i = g_i$. Therefore, $\varphi = \psi$. □

Since coordinate rings naturally carry the additional structure of a $\Bbbk$-algebra, we would hope that the pullback of a polynomial map between affine varieties preserves this structure. Given $\Bbbk$-algebras A and B, we define a $\Bbbk$-*algebra homomorphism* from A to B to be a $\Bbbk$-linear ring homomorphism $\Phi : A \to B$, i.e. a ring homomorphism $\Phi : A \to B$ such that $\Phi(\alpha) = \alpha$ for every $\alpha \in \Bbbk$. Similarly, a $\Bbbk$-*algebra isomorphism* is a bijective $\Bbbk$-algebra homomorphism whose

inverse is also a $\Bbbk$-algebra homomorphism. If there exists a $\Bbbk$-algebra isomorphism $\Phi : A \to B$, we say that A and B are *isomorphic*, in which case we write $A \cong B$.

2.2.8 Examples.

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

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

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

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

One important property of $\Bbbk$-algebra homomorphisms is that they preserve the evaluation of polynomials. If A is a $\Bbbk$-algebra and $f \in \Bbbk[x_1, \ldots, x_n]$, then we can view f as a function from A^n to A, simply by substituting elements of A into the expression for f. If $\Phi : A \to B$ is a $\Bbbk$-algebra homomorphism and $f \in \Bbbk[x_1, \ldots, x_n]$, then $\Phi(f(a_1, \ldots, a_n)) = f(\Phi(a_1), \ldots, \Phi(a_n))$ for all $a_1, \ldots, a_n \in A$. Indeed, this property is equivalent to Φ being a $\Bbbk$-algebra homomorphism.

This next proposition shows that the association of a coordinate ring to an affine variety and the pullback of polynomial maps define a contravariant functor from the category of affine varieties with polynomial maps as morphisms to the category of $\Bbbk$-algebras with $\Bbbk$-algebra homorphisms as morphisms.

2.2.9 Proposition (Functorality). *Let X, Y, and Z be affine varieties. Then:*

(i) *if $\varphi = \mathrm{id}_X$ then $\varphi^* = \mathrm{id}_{\Gamma(X)}$;*

(ii) *if $\varphi : X \to Y$ and $\psi : Y \to Z$ are polynomial maps, $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$;*

(iii) *if $\varphi : X \to Y$ is a polynomial map, $\varphi^* : \Gamma(Y) \to \Gamma(X)$ is a $\Bbbk$-algebra homomorphism.*

Proof:

(i) For every $g \in \Gamma(Y)$, $\mathrm{id}_X^*(g) = g \circ \mathrm{id}_X = g$.

(ii) For every $g \in \Gamma(Z)$, $(\psi \circ \varphi)^*(g) = g \circ \psi \circ \varphi = \varphi^*(g \circ \psi) = \varphi^* \circ \psi^*(g)$.

(iii) Let $f, g \in \Gamma(Y)$ and $\alpha \in \Bbbk$. Then

$$\varphi^*(\alpha f + g) = (\alpha f + g) \circ \varphi = \alpha f \circ \varphi + g \circ \varphi = \alpha \varphi^*(f) + \varphi^*(g),$$

$$\varphi^*(fg) = (fg) \circ \varphi = (f \circ \varphi)(g \circ \varphi) = \varphi^*(f)\varphi^*(g),$$

and φ^* clearly sends the identity in $\Gamma(Y)$ to the identity in $\Gamma(X)$. □

What is the range of the functor that takes an affine variety to its coordinate ring and takes polynomial maps to $\Bbbk$-algebra homomorphisms of the coordinate rings? More precisely:

(i) If $\Gamma(X) \cong \Gamma(Y)$, is $X \cong Y$? More generally, which $\Bbbk$-algebra homomorphisms from $\Gamma(Y)$ to $\Gamma(X)$ are pullbacks of polynomial maps?

(ii) Which $\Bbbk$-algebras are coordinate rings of affine varieties defined over $\Bbbk$?

The answer to the first question very simple: *every* $\Bbbk$-algebra homomorphism between coordinate rings is the pullback of a unique polynomial map.

2.2.10 Proposition. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties, and let $\Phi : \Gamma(Y) \to \Gamma(X)$ be a $\Bbbk$-algebra homomorphism. Then there exists a unique polynomial map $\varphi : X \to Y$ such that $\varphi^* = \Phi$.*

Proof: Let $I = \mathrm{I}(X)$ and $J = \mathrm{I}(Y)$. Thus $\Gamma(X) = \Bbbk[x_1, \ldots, x_n]/I$ and $\Gamma(Y) = \Bbbk[y_1, \ldots, y_m]/J$. Let $\tilde{\Phi} : \Bbbk[y_1, \ldots, y_m] \to \Gamma(X)$ be the map defined by $\tilde{\Phi}(g) = \Phi(g + J)$, i.e. the lift of Φ to $\Bbbk[y_1, \ldots, y_m]$. Then $\tilde{\Phi}$ is a $\Bbbk$-algebra homomorphism, as it is the composition of two $\Bbbk$-algebra homomorphisms, Φ and the quotient map from $\Bbbk[y_1, \ldots, y_m]$ to $\Gamma(Y)$. For $i = 1, \ldots, m$, let f_i be a representative in $\Bbbk[x_1, \ldots, x_n]$ for $\Phi(y_i + J)$, so that $\tilde{\Phi}(y_i) = \Phi(y_i + J) = f_i + I$. Then for any $g \in \Bbbk[y_1, \ldots, y_m]$ we have

$$\begin{aligned} g(f_1, \ldots, f_m) + I &= g(\tilde{\Phi}(y_1), \ldots, \tilde{\Phi}(y_m)) \\ &= \tilde{\Phi}(g(y_1, \ldots, y_m)) \\ &= \tilde{\Phi}(g). \end{aligned}$$

Let $\varphi : X \to \mathbb{A}^m$ be the map defined by $\varphi(x) = (f_1(x), \ldots, f_m(x))$. In order to show that φ restricts to a polynomial map from X to Y, we only need to show that $\varphi(X) \subseteq Y$. Since $Y = \mathrm{V}(J)$, we want to show that every polynomial in J vanishes at $\varphi(x)$ for every $x \in X$. Fix $g \in J$. Then from the above,

$$\begin{aligned} g(f_1 + I, \ldots, f_m + I) &= g(f_1, \ldots, f_m) + I \\ &= \tilde{\Phi}(g) \\ &= 0 + I, \end{aligned}$$

since $g \in J$, so $g(f_1, \ldots, f_m) \in I$. It follows that $g(f_1(x), \ldots, f_m(x)) = 0$ for every $x \in X$. Therefore, $\varphi(X) \subseteq Y$, and φ defines a polynomial map from X to Y. It is clear that $\varphi^* = \Phi$, because for $g \in \Bbbk[y_1, \ldots, y_m]$,

$$\begin{aligned} \varphi^*(g + J) &= (g \circ \varphi) + I \\ &= g(f_1, \ldots, f_m) + I \\ &= \tilde{\Phi}(g) \\ &= \Phi(g + J). \end{aligned}$$

Finally, uniqueness follows from Proposition 2.2.7. □

2.2.11 Proposition. *Let $X \subseteq \mathbb{A}^m$ and $Y \subseteq \mathbb{A}^n$ be affine varieties, and let $\varphi : X \to Y$ be a polynomial map. Then φ is an isomorphism if and only if φ^* is an isomorphism, in which case $(\varphi^*)^{-1} = (\varphi^{-1})^*$.*

PROOF: Suppose that φ is an isomorphism. Then there exists a polynomial map $\varphi^{-1} : Y \to X$ such that $\varphi \circ \varphi^{-1} = \mathrm{id}_Y$ and $\varphi^{-1} \circ \varphi = \mathrm{id}_X$. Taking pullbacks, we get $(\varphi^{-1})^* \circ \varphi^* = \mathrm{id}_{\Gamma(Y)}$ and $\varphi^* \circ (\varphi^{-1})^* = \mathrm{id}_{\Gamma(X)}$, so φ^* is an isomorphism, and $(\varphi^{-1})^*$ is its inverse.

Conversely, suppose φ^* is an isomorphism. Then there exists a $\Bbbk$-algebra homomorphism $(\varphi^*)^{-1} : \Gamma(X) \to \Gamma(Y)$ such that $\varphi^* \circ (\varphi^*)^{-1} = \mathrm{id}_{\Gamma(X)}$ and $(\varphi^*)^{-1} \circ \varphi = \mathrm{id}_{\Gamma(Y)}$. By Proposition 2.2.10, there exists a polynomial map $\psi : Y \to X$ such that $(\varphi^*)^{-1} = \psi^*$. Then

$$(\varphi \circ \psi)^* = \varphi^* \circ \psi^* = \varphi \circ (\varphi^*)^{-1} = \mathrm{id}_{\Gamma(X)},$$

and

$$(\psi \circ \varphi)^* = \psi^* \circ \varphi^* = (\varphi^*)^{-1} \circ \varphi = \mathrm{id}_{\Gamma(Y)}.$$

Hence by the uniqueness in Proposition 2.2.10 we have $\varphi \circ \psi = \mathrm{id}_X$ and $\psi \circ \varphi = \mathrm{id}_Y$. Therefore, φ is an isomorphism. □

2.2.12 Corollary. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties. Then $X \cong Y$ if and only if $\Gamma(X) \cong \Gamma(Y)$.*

PROOF: Suppose $X \cong Y$. Then there exists an isomorphism $\varphi : X \to Y$. By Proposition 2.2.11, $\varphi^* : \Gamma(Y) \to \Gamma(X)$ is an isomorphism, so $\Gamma(X) \cong \Gamma(Y)$. Conversely, suppose $\Gamma(X) \cong \Gamma(Y)$. Then there exists a $\Bbbk$-algebra isomorphism $\Phi : \Gamma(Y) \to \Gamma(X)$. By Proposition 2.2.10, there exists a polynomial map $\varphi : X \to Y$ such that $\varphi^* = \Phi$. By Proposition 2.2.11, φ is an isomorphism, so $X \cong Y$. □

2.2.13 Example. Is $X = \mathrm{V}(yx - 1) \subseteq \mathbb{A}^2$ isomorphic to $\mathbb{A}^1$? No, since $\Gamma(\mathbb{A}^1) = \Bbbk[t]$ while $\Gamma(X)$ is the ring of Laurent polynomials, $\Bbbk[\overline{x}, \overline{x}^{-1}]$, and these $\Bbbk$-algebras are not isomorphic. To see this, suppose that $\Phi : \Bbbk[\overline{x}, \overline{x}^{-1}] \to \Bbbk[t]$ is an isomorphism. In particular, Φ is surjective, so $\Phi(1) = 1$ and $\Phi(\overline{x})\Phi(\overline{x}^{-1}) = \Phi(1) = 1$. Hence $\Phi(\overline{x})$ and $\Phi(\overline{x}^{-1})$ are units in $\Bbbk[t]$, so they must be scalars. But this implies that the entire range of Φ is contained in the scalars, a contradiction.

We now return to the question of which $\Bbbk$-algebras are isomorphic to coordinate rings of affine varieties. We will restrict ourselves to the case when $\Bbbk$ is algebraically closed, which is certainly reasonable, as when $\Bbbk$ is not algebraically closed we can not even describe the closed ideals $\Bbbk[x_1, \ldots, x_n]$ in any elementary manner.

We say that a $\Bbbk$-algebra A is *finitely generated* if there exist $a_1, \ldots, a_n \in A$ such that $A = \Bbbk[a_1, \ldots, a_n]$, or equivalently, if there exists a surjective homomorphism $\varphi : \Bbbk[x_1, \ldots, x_n] \to A$ for some $n \in \mathbb{N}$.

2.2.14 Examples.

(i) $\Bbbk[x_1, \ldots, x_n]$ is finitely generated.

(ii) Any quotient of a finitely generated $\Bbbk$-algebra is finitely generated. In particular, if X is an affine variety then $\Gamma(X)$ is finitely generated.

2.2.15 Proposition. *Suppose $\Bbbk$ is algebraically closed, and let A be a finitely generated $\Bbbk$-algebra that is an integral domain. Then there exists an affine variety X such that $A \cong \Gamma(X)$.*

PROOF: Since A is finitely generated, there exists an $n \in \mathbb{N}$ and a surjective $\Bbbk$-algebra homomorphism $\varphi : \Bbbk[x_1, \ldots, x_n] \to A$. Let $I = \ker(\varphi)$. By the First Isomorphism Theorem, $\Bbbk[x_1, \ldots, x_n]/I \cong A$. Hence $\Bbbk[x_1, \ldots, x_n]/I$ is an integral domain, and I is prime. Let $X = \mathrm{V}(I)$. Then X is an affine variety and

$$\Gamma(X) = \Bbbk[x_1, \ldots, x_n]/\,\mathrm{I}(X) = \Bbbk[x_1, \ldots, x_n]/I \cong A. \qquad \square$$

Therefore, when $\Bbbk$ is algebraically closed, the contravariant functor from the category of affine varieties with polynomial maps as morphisms to the category of finitely generated $\Bbbk$-algebras that are integral domains with $\Bbbk$-algebra homomorphisms as morphisms is an equivalence of categories. Indeed, we have the following correspondence:

Geometry	**Algebra**
affine variety X	finitely generated $\Bbbk$-algebra and integral domain $\Gamma(X)$
algebraic subset of X	radical ideal of $\Gamma(X)$
irreducible algebraic subset of X	prime ideal of $\Gamma(X)$
point of X	maximal ideal of $\Gamma(X)$
polynomial map $\varphi : X \to Y$	$\Bbbk$-algebra homomorphism $\varphi^* : \Gamma(Y) \to \Gamma(X)$

2.3 Rational Functions

2.3.1 Definition. Let $X \subseteq \mathbb{A}^n$ be a variety and $\Gamma(X)$ its coordinate ring. Since $\Gamma(X)$ is a domain, we may consider its field of fractions, which we will denote $\Bbbk(X)$. In this context, $\Bbbk(X)$ is called the *field of rational functions* on X, or the *function field* of X.

In contrast to polynomial functions, rational functions are not necessarily defined at every point in X, e.g. $f = 1/x$ is not defined at $x = 0$ on $\mathbb{A}^1$. However, at the same time, even though the expression $f = x^2/x$ is not defined at $x = 0$ on $\mathbb{A}^1$, by expressing f as $x/1$, we can extend it to all of $\mathbb{A}^1$.

2.3.2 Definition. A rational function F is said to be *regular* (or *defined*) at $p \in X$ if f can be written as a/b for some $a, b \in \Gamma(X)$ such that $b(p) \neq 0$. The *value of a rational function* f at p is defined to by $f(p) = a(p)/b(p)$. A point

where f is not defined is called a *pole* and the set of all such points is called the *pole set* of f.

Remark. There may be more than one way of writing f as a ratio of polynomial functions; f is defined at p if we can find a "denominator" for f that does not vanish at p. Nevertheleess, the value of f at p is independent of a and b. Indeed, if $f = a/b = a'/b'$ with $b(p), b'(p) \neq 0$, then $ab' = a'b$ if and only if $ab' - a'b \in \mathrm{I}(X)$, so

$$\frac{a(p)}{b(p)} = \frac{a'(p)}{b'(p)},$$

since $p \in X$.

2.3.3 Examples.

(i) Consider $f = x/y$ on $\mathbb{A}^2$. Then the pole set of f is $\{(x, y) \in \mathbb{A}^2 : y = 0\}$. But if one restricts f to $X = \mathrm{V}(x - y^2) \subseteq \mathbb{A}^2$ then $\overline{x}/\overline{y} = \overline{y^2}/\overline{y} = \overline{y}$ on X, so $\overline{f}$ is defined everywhere on X.

(ii) Consider $f = (1 - y)/x$ on $X = \mathrm{V}(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$. If $\mathrm{char}(\Bbbk) = 2$, then $x^2 + y^2 + 1 = (x + y - a)^2$, so $X = \mathrm{V}(x + y - 1)$. Therefore, on X, $1 - \overline{y} = \overline{x}$, so $f = 1$ is defined everywhere. If $\mathrm{char}(\Bbbk) \neq 2$, then f has pole set $\{(0, -1)\}$. Indeed, there are two points on X with x coordinate equal to 0, namely $(0, 1)$ and $(0, -1)$, but since we have

$$\frac{1 - \overline{y}}{\overline{x}} = \frac{(1 - \overline{y})(1 + \overline{y})}{\overline{x}(1 + \overline{y})} = \frac{\overline{x}^2}{\overline{x}(1 + \overline{y})} = \frac{\overline{x}}{1 + \overline{y}}$$

on X, the point $(0, 1)$ is not a pole of f. If $(0, -1)$ were not a pole then there would be $\overline{a}, \overline{b} \in \Gamma(X)$ such that $(1 - \overline{y})/\overline{x} = \overline{a}/\overline{b}$ with $b(0, -1) \neq 0$. Hence $(1 - \overline{y})\overline{b} - \overline{a}\overline{x} = 0$, so lifting to $\Bbbk[x, y]$ we get $(1 - y)b - ax = h$, where $h \in \mathrm{I}(X)$ and $b(0, -1) \neq 0$. But then at $(0, -1) \in X$ we have that $h(0, -1) = 0$ and $2b(0, -1) = 0$, a contradiction since $\mathrm{char}(\Bbbk) \neq 2$.

2.3.4 Proposition. *Let X be an affine variety. Then the pole set of a rational function on X is an algebraic subset of X.*

Proof: Suppose $f \in \Bbbk(X)$. The pole set of f is

$$X \cap \bigcap_{\substack{b \in \Bbbk[x_1, \ldots, x_n], \\ f = a/b}} \mathrm{V}(b),$$

which is clearly algebraic, as it is the intersection of algebraic sets. □

Therefore, the set of all points where $f \in \Bbbk(X)$ is defined is an open subset of X, called the *domain* of f. We denote the domain of f by $\mathrm{dom}(f)$.

Remark. If $f \in \Bbbk(X)$ is such that $\mathrm{dom}(f)$ is closed and non-empty, then $\mathrm{dom}(f) = X$. Indeed, if $\mathrm{dom}(f)$ is closed, then it is both open in closed in X. Thus $X = \mathrm{dom}(f) \cup (X \setminus \mathrm{dom}(f))$, where both $\mathrm{dom}(f)$ and $X \setminus \mathrm{dom}(f)$ are closed, implying that $\mathrm{dom}(f) = \varnothing$ or $\mathrm{dom}(f) = X$. But $\mathrm{dom}(f) \neq \varnothing$, so $\mathrm{dom}(f) = X$.

We have seen that polynomial functions are continuous with respect to the Zariski topology. Similarly, rational functions are continuous with respect to the induced Zariski topology on their domain.

2.3.5 Proposition. *Let $X \subseteq \mathbb{A}^n$ be an affine variety. If $f \in \Bbbk(X)$ then f is continuous with respect to the induced Zariski topology on* $\mathrm{dom}(f)$ *and the Zariski topology on $\mathbb{A}^1 \cong \Bbbk$.*

Proof: Exercise. □

2.3.6 Proposition. *Let $X \subseteq \mathbb{A}^n$ be an affine variety. If $f \in \Bbbk(X)$ is zero on a non-empty open set $U \subseteq X$, then f is zero on all of X.*

Proof: Choose $p \in U$ and $a, b \in \Gamma(X)$ such that $f = a/b$ and $b(p) \neq 0$. Note that although $b(p) \neq 0$, it may be zero at other points in U; let us then shrink the open set U. Consider $V = X \setminus \mathrm{V}(b)$. Then V is open in the induced Zariski topology on X, and $p \in U \cap V$, so $U \cap V$ is a non-empty open subset of X. Since $b(x) \neq 0$ for all $x \in U \cap V$ and $f(x) = 0$ for all $x \in U$, $a(x) = f(x)b(x) = 0$ for all $x \in U \cap V$. Moreover, since $U \cap V$ is a non-empty open subset of X with X is irreducible, $\overline{U \cap V} = X$. Hence $a(x) = 0$ for all $x \in X$ because polynomials are continuous with respect to the Zariski topology, so that $a^{-1}(0)$ is closed in X, implying that

$$X = \overline{U \cap V} \subseteq \overline{a^{-1}(0)} = a^{-1}(0) \subseteq X.$$

Therefore, $a = 0$, and $f = a/b = 0/b = 0$. □

2.3.7 Corollary (Identity Theorem). *Let X be an affine variety. If $f, g \in \Bbbk(X)$ agree on a non-empty open subset of X then $f = g$.*

Proof: Consider $f - g$ and apply the previous proposition. □

In particular, this corollary tells us that rational functions are completely determined by their restriction to some open set $U \subseteq X$.

2.4 Rational Maps

2.4.1 Definition. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be varieties. A map $\varphi : X \to Y$ such that

$$\varphi(x) = (f_1(x), \ldots, f_m(x))$$

for some $f_1, \ldots, f_m \in \Bbbk(X)$ is called a *rational map*. If $p \in X$, we say that φ is *regular* (or *defined*) at p if each f_i is regular at p. The set of all points where φ is defined is called the *domain* of φ, and is denoted by $\mathrm{dom}(f)$.

Note that the domain of φ is an open subset of X, since it is the intersection of the domains of the rational functions f_i, which are each open sets.

2.4.2 Examples.

(i) Rational functions $f : X \to \Bbbk \cong \mathbb{A}^1$ are rational maps.

(ii) Any polynomial map is a rational map.

(iii) Suppose $\mathrm{char}(\Bbbk) \neq 2$, and let $X = \mathrm{V}(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$. The parameterization $\varphi : \mathbb{A}^1 \to X$ of X given by

$$\varphi(t) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right)$$

is a rational map. Its domain is $\mathbb{A}^1 \setminus \{i, -i\}$, and its range is $X \setminus \{(0,1)\}$.

2.4.3 Definition. A rational map $\varphi : X \to Y$ is called *dominant* if $\overline{\varphi(X)} = Y$.

2.4.4 Examples.

(i) Suppose $\mathrm{char}(\Bbbk) \neq 2$, and let $X = \mathrm{V}(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$. The rational map $\varphi : \mathbb{A}^1 \to X$ given by

$$\varphi(t) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right)$$

is dominant, because $\overline{\varphi(\mathbb{A}^1)} = \overline{X \setminus \{(0,1)\}} = X$.

(ii) A proper inclusion between affine varieties is not a dominant map.

Given two rational maps $\varphi : X \to Y$ and $\psi : Y \to Z$, the composition of ψ and φ is not defined if $\varphi(X) \cap (\text{domain } \psi)$ is empty. This problem can be bypassed if we assume that φ is dominant. Indeed, if $\overline{\varphi(X)} = Y$, then if $\varphi(X) \cap \mathrm{dom}(\psi) = \varnothing$, this would imply that $\varphi(X) \subseteq (X \setminus \mathrm{dom}(\psi))$ is a proper closed subset of Y (since $\mathrm{dom}(\psi)$ is open), and thus $\overline{\varphi(X)} \subseteq X \setminus \mathrm{dom}(\psi)$, contradicting the assumption that φ is dominant. Therefore, if φ is dominant there is a well-defined composition $\psi \circ \varphi : X \to Z$.

2.4.5 Definition. A dominant rational map $\varphi : X \to Y$ is *birational* or a *birational equivalence* if φ has an inverse rational map that is also dominant. In this case, X and Y are said to be *birational* or *birationally equivalent*, denoted $X \sim Y$.

2.4.6 Examples.

(i) Every isomorphism is a birational equivalence.

(ii) Let $X = \mathrm{V}(xy-1) \subseteq \mathbb{A}^2$. The map $\varphi : X \to \mathbb{A}^1$ defined by $\varphi(x,y) = x$ is a polynomial map that is injective but not surjective, because $0 \notin \varphi(X)$. However, it is a dominant rational map, and it has a rational inverse on the open subset $U = \mathbb{A}^1 \setminus \{(0,0)\}$ of $\mathbb{A}^1$, given by $\varphi^{-1}(t) = (t, 1/t)$. This inverse is dominant because φ is defined on all of X, so X is birationally equivalent to $\mathbb{A}^1$, even though X is not isomorphic to $\mathbb{A}^1$.

(iii) Let $X = \mathrm{V}(y^2 - x^3) \subseteq \mathbb{A}^2$. The rational map $\varphi : \mathbb{A}^1 \to X$ defined by $\varphi(t) = (t^2, t^3)$ is bijective, and thus dominant, but not an isomorphism. Nevertheless, it has a rational inverse $\varphi^{-1} : X \to \mathbb{A}^1$, defined on the open subset $U = X \setminus \{(0,0)\}$ and given by $\varphi^{-1}(x,y) = y/x$. Since the domain of φ is all of X, φ^{-1} is dominant. Thus X is birational to $\mathbb{A}^1$.

2.4.7 Definition. A variety $X \subseteq \mathbb{A}^n$ that is birationally equivalent to $\mathbb{A}^m$, for some m, is said to be *rational*.

The last two examples above are both rational. We will later see that there are curves that are not rational.

How do rational maps act on rational functions? That is, given a rational map $\varphi : X \subseteq \mathbb{A}^n \to Y \subseteq \mathbb{A}^m$, can we define a pullback $\varphi^* : \Bbbk(Y) \to \Bbbk(X)$ that is well-defined as a $\Bbbk$-algebra homomorphism? This imposes the following two conditions on φ:

(i) φ must be dominant to ensure that one can compose φ with any rational function on Y;

(ii) φ^* must be a non-zero field homomorphism and would therefore be injective (as units are mapped to units).

For any rational function $g \in \Bbbk(Y)$, let $\varphi^*(g) = g \circ \varphi \in \Bbbk(X)$. Clearly, $\varphi^* : \Gamma(Y) \to \Bbbk(X)$ is a well-defined ring homomorphism. Moreover, φ^* is injective. Indeed, suppose on the contrary that there exists a non-zero $f \in \Gamma(Y)$ such that $\varphi * (f) = 0$. Then $\varphi(X) \subseteq \mathrm{V}(f) \subsetneq Y$, so $\overline{\varphi(X)} \subseteq \overline{\mathrm{V}(f)}$, contradicting the fact that $\varphi(X)$ is dense in Y. Hence φ^* is injective on $\Gamma(Y)$ so that it extends in the obvious way to a $\Bbbk$-algebra homomorphism $\varphi^* : \Bbbk(Y) \to \Bbbk(X)$, i.e. $\varphi^*(a/b) = \varphi^*(a)\varphi^*(b)^{-1}$.

As in the case of the pullback of a polynomial map, the next proposition shows that the association of a function field to an affine variety and the pullback of dominant rational maps defines a contravariant functor from the category of affine varieties with dominant rational maps as morphisms to the category of field extensions of $\Bbbk$ with $\Bbbk$-algebra homomorphisms as morphisms.

2.4.8 Proposition (Functoriality). *Let X, Y, and Z be affine varieties. Then:*

(i) *if $\varphi : X \to Y$ and $\psi : X \to Y$ are dominant rational maps such that $\varphi^* = \psi^*$ then $\varphi = \psi$;*

(ii) $\mathrm{id}_X^* = \mathrm{id}_{\Bbbk(X)}$;
(iii) *if* $\varphi : X \to Y$ *and* $\psi : Y \to Z$ *are both dominant rational maps then* $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$;
(iv) φ^* *is an injective* $\Bbbk$*-algebra homomorphism.*

PROOF:
(i) Choose $f_1, \ldots, f_m, g_1, \ldots, g_m \in \Bbbk(X)$ such that $\varphi = (f_1, \ldots, f_m)$ and $\psi = (g_1, \ldots, g_m)$. Then $y_i \circ \varphi = f_i$ and $y_i \circ \psi = g_i$, showing that $f_i = g_i$. Therefore, $\varphi = \psi$.
(ii) For every $g \in \Bbbk(Y)$, $\mathrm{id}_X^*(g) = g \circ \mathrm{id}_X = g$.
(iii) For every $g \in \Bbbk(Z)$, $(\psi \circ \varphi)^*(g) = g \circ \psi \circ \varphi = \varphi^*(g \circ \psi) = \varphi^* \circ \psi^*(g)$.
(iv) We showed that it is injective above, and it is clearly a $\Bbbk$-algebra homomorphism. □

As in the case of the pullback of a polynomial map, every $\Bbbk$-algebra homomorphism between function fields is the pullback of a dominant rational map.

2.4.9 Proposition. *Let* $X \subseteq \mathbb{A}^n$ *and* $Y \subseteq \mathbb{A}^m$ *be affine varieties, and let* $\Phi : \Bbbk(Y) \to \Bbbk(X)$ *be a* $\Bbbk$*-algebra homomorphism. Then there exists a unique dominant rational map* $\varphi : X \to Y$ *such that* $\varphi^* = \Phi$.

PROOF: Let $I = \mathrm{I}(X)$ and $J = \mathrm{I}(Y)$. Thus $\Gamma(X) = \Bbbk[x_1, \ldots, x_n]/I$ and $\Gamma(Y) = \Bbbk[y_1, \ldots, y_m]/J$. Since $\Phi : \Bbbk(Y) \to \Bbbk(X)$ is an injective $\Bbbk$-algebra homomorphism, it restricts to an injective $\Bbbk$-algebra homomorphism from $\Gamma(Y)$ to $\Bbbk(X)$. Let $\tilde{\Phi} : \Bbbk[y_1, \ldots, y_m] \to \Bbbk(X)$ be the map defined by $\tilde{\Phi}(g) = \theta(g + J)$, i.e. the lift of $\Phi_{|\Gamma(Y)}$ to $\Bbbk[y_1, \ldots, y_m]$. Then $\tilde{\Phi}$ is a $\Bbbk$-algebra homomorphism, as it is the composition of two $\Bbbk$-algebra homomorphisms, Φ and the quotient map from $\Bbbk[y_1, \ldots, y_m]$ to $\Gamma(Y)$. For $i = 1, \ldots, m$, let $f_i = \tilde{\Phi}(y_i)$. Then for any $g \in \Bbbk[y_1, \ldots, y_m]$ we have

$$\begin{aligned} g(f_1, \ldots, f_m) &= g(\tilde{\Phi}(y_1), \ldots, \tilde{\Phi}(y_m)) \\ &= \tilde{\Phi}(g(y_1, \ldots, y_m)) \\ &= \tilde{\Phi}(g). \end{aligned}$$

Let $\varphi : X \to \mathbb{A}^m$ be the rational map defined by $\varphi(x) = (f_1(x), \ldots, f_m(x))$. In order to show that φ is a dominant rational map from X to Y, we need to show that $\varphi(X) \subseteq Y$ and $\overline{\varphi(X)} = \varphi(Y)$. Fix $g \in J$. Then from the above,

$$g(f_1, \ldots, f_m) = \tilde{\Phi}(g) = \Phi(g + J) = \Phi(0) = 0,$$

so $g(f_1(x), \ldots, f_m(x)) = g(f_1, \ldots, f_m)(x) = 0$ for every $x \in X$. Therefore, $\varphi(X) \subseteq Y$, and φ defines a rational map from X to Y. Since Y is closed, $\overline{\varphi(X)} \subseteq Y$. We need to show that

$$Y \subseteq \overline{\varphi(X)} = \mathrm{V}(\mathrm{I}(\varphi(X))).$$

Fix $p \in Y$ and $g \in \mathrm{I}(\varphi(X))$. Since Φ is a $\Bbbk$-algebra homomorphism, we have that for all $x \in X$, $\Phi(g)(x) = g(\varphi(x)) = 0$. Thus $\Phi(g) = 0$, and $g = 0$ since Φ is injective. In particular, $g(p) = 0$. Since the choice of g was arbitrary, $p \in \mathrm{V}(\mathrm{I}(\varphi(X))) = \overline{\varphi(X)}$, showing that $\overline{\varphi(X)} = Y$. It is clear that $\varphi^* = \Phi$, because for $g \in \Bbbk[y_1, \ldots, y_m]$,

$$\varphi^*(g + J) = g(f_1, \ldots, f_m) = \tilde{\Phi}(g).$$

Finally, uniqueness follows from Proposition 2.4.8 (i). □

2.4.10 Proposition. *Let $X \subseteq \mathbb{A}^m$ and $Y \subseteq \mathbb{A}^n$ be affine varieties, and let $\varphi : X \to Y$ be a dominant rational map. Then φ is birational if and only if φ^* is an isomorphism, in which case $(\varphi^*)^{-1} = (\varphi^{-1})^*$.*

Proof: Analogous to the proof of Proposition 2.2.11. □

2.4.11 Corollary. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be varieties. Then $X \sim Y$ if and only if $\Bbbk(X) \cong \Bbbk(Y)$.*

Proof: Analogous to the proof of Corollary 2.2.12. □

2.5 Dimension

There are two natural ways to define dimension for affine varieties varieties, which are both very similar to the case of linear algebra, where the dimension of a finite-dimensional vector space V is equal to the maximum size of a linearly independent family of linear maps to the scalar field. In the case of of an affine variety X, it would make sense to consider instead algebraically independent rational functions on X. Thus we arrive at a definition of the dimension of X as the transcendence degree of $\Bbbk(X)$ over $\Bbbk$ (for the definition of transcendence degree, see Appendix B).

The dimension of V can also be characterized as the maximum length of a descending chain of proper subspaces. We will see that the dimension of a variety can be described in a similar fashion as the maximum length of a descending chain of proper subvarieties, and that this notion of dimension agrees with the transcendence degree of the function field of the variety.

2.5.1 Definition. Let X be an affine variety. The *dimension* of X is the transcendence degree of the function field $\Bbbk(X)$ over $\Bbbk$, and is denoted by $\dim X$. If $Y \subseteq X$ is a subvariety of X then the *codimension* of Y in X is $\operatorname{codim}_X Y = \dim X - \dim Y$. A variety of dimension 1 is a *curve*, a variety of dimension 2 is a *surface*, and a variety of dimension n is called an *n-fold*.

By Corollary 2.4.11, dimension is invariant under birational equivalence.

2.5.2 Examples.

(i) $\mathbb{A}^n$ has dimension n since in $\Bbbk(x_1, \ldots, x_n) \cong \Bbbk(\mathbb{A}^n)$ the coordinate functions $x_1, \ldots, x_n$ are algebraically independent. It follows that $\mathbb{A}^n$ and $\mathbb{A}^m$ cannot be birational if $m \neq n$.

(ii) If X consists of a single point then $\Bbbk(X) = \Bbbk$, so $\dim X = 0$.

The dimension of a variety has the particularly strong property that any proper subvariety must have strictly smaller dimension. This is certainly not the case if one considers manifolds instead of varieties.

2.5.3 Theorem. *If Y is a proper subvariety of $X \subseteq \mathbb{A}^m$ then* $\dim Y < \dim X$.

PROOF: Let $n = \dim X$. Then any $n+1$ of the coordinate functions $x_1, \ldots, x_m$ are algebraically dependent as elements of $\Bbbk(X)$, and also as elements of $\Bbbk(Y)$. Therefore $\dim Y \leq \dim X$.

Assume that $\dim Y = \dim X$. We will derive the contradiction $Y = X$ by showing that $\mathrm{I}(Y) \subseteq \mathrm{I}(X)$. Since $\dim Y = n$ there are coordinate functions $x_{i_1}, \ldots, x_{i_n}$ whose images are algebraically independent in $\Bbbk(Y)$. Then $x_{i_1}, \ldots, x_{i_n}$ must be algebraically independent in $\Bbbk(X)$. Let $u \in \Gamma(X)$ be non-zero. Then u depends algebraically on $x_{i_1}, \ldots, x_{i_n}$, i.e. there is a polynomial $a \in \Bbbk[t_1, \ldots, t_{n+1}]$ such that

$$\begin{aligned} &a(u, x_{i_1}, \ldots, x_{i_n}) \\ &\qquad = a_k(x_{i_1}, \ldots, x_{i_n})u^k + \cdots + a_1(x_{i_1}, \ldots, x_{i_n})u + a_0(x_{i_1}, \ldots, x_{i_n}) = 0 \end{aligned}$$

on X. Since $\Gamma(X)$ is a domain we may assume a is irreducible and $a_0(x_{i_1}, \ldots, x_{i_n})$ is non-zero on X. Then $a(u, x_{i_1}, \ldots, x_{i_n}) = 0$ on Y since $Y \subseteq X$ so if $u = 0$ on Y then $a_0(x_{i_1}, \ldots, x_{i_n}) = 0$ on Y, a contradiction since $x_{i_1}, \ldots, x_{i_n}$ are algebraically independent in $\Bbbk(Y)$. Since $u \neq 0$ on X implies $u \neq 0$ on Y we have that $\mathrm{I}(Y) \subseteq \mathrm{I}(X)$. □

2.5.4 Corollary. *Let X be an affine variety. Then* $\dim X = 0$ *if and only if X is a single point.*

PROOF: Clearly, if X is a single point, then $\Bbbk(X) \cong \Bbbk$, so $\dim X = 0$. Conversely, suppose that $\dim X = 0$, but X has more than one point. Then there exists a $p \in X$ such that $\{p\} \subsetneq X$. Then $0 = \dim\{p\} < \dim X = 0$, contradicting to the previous theorem. □

2.5.5 Example. Plane curves given by irreducible polynomials have dimension 1. Suppose $X = \mathrm{V}(f)$ for some irreducible polynomial $f \in \Bbbk[x, y]$. The algebraically independent elements x and y of $\Bbbk[x, y]$ descend to algebraically dependent elements $\overline{x}$ and $\overline{y}$ in $\Bbbk(X)$. Indeed, $f(\overline{x}, \overline{y}) = 0$.

Since $\dim \mathbb{A}^2 = 2$, the previous example shows that plane curves have codimension 1 in $\mathbb{A}^2$. Similarly, any hypersurface defined by a non-constant irreducible polynomial has codimension 1.

2.5.6 Theorem. *Let $f \in \Bbbk[x_1, \ldots, x_n]$ be a non-constant irreducible polynomial. Then $\mathrm{V}(f) \subseteq \mathbb{A}^n$ has codimension 1.*

PROOF: Let $X = \mathrm{V}(f)$. Suppose that x_n appears in the expression of f. Then $\overline{x}_1, \ldots, \overline{x}_{n-1}$ are algebraically independent in $\Bbbk(X)$. Indeed, if they are not then there is a polynomial g involving only the variables $x_1, \ldots, x_{n-1}$ that is zero on X. Then $g \in \mathrm{I}(X) = \langle f \rangle$, so $f \mid g$ and x_n appears in the expression for g, a contradiction. Therefore $\dim X \geq n-1$, and Theorem 2.5.3 implies that $\dim X = n-1$, so $\operatorname{codim} X = 1$. □

2.5.7 Example. Consider $X = \mathrm{V}(y^2 - x^3)$. By Example 2.4 (ii), $f = \overline{x} - 1 \in \Gamma(X)$ is irreducible, but $\mathrm{V}(f) \cap X = \{(1,1), (1,-1)\}$ is reducible. However, both of the irreducible components of $\mathrm{V}(f) \cap X$, $\{\ (1,\ 1)\ \}$ and $\{(1,-1)\}$ have codimension 1 in X.

In fact, the following general result holds, but its proof uses more complicated algebraic techniques.

2.5.8 Theorem. *Let $X \subseteq \mathbb{A}^n$ be a affine variety, and let $f \in \Bbbk[x_1, \ldots, x_n]$ be a polynomial such that $\mathrm{V}(f) \cap X \neq X$. Then each of the irreducible components of $\mathrm{V}(f) \cap X$ has codimension 1 in X.*

PROOF: See Theorem 2 on p. 41 in Chapter 1 of Mumford's "Red Book on Varieties and Schemes". □

2.5.9 Corollary. *If $Y \subsetneq X \subseteq \mathbb{A}^n$ has codimension r in X then there exist irreducible closed subsets $Y_0, \ldots, Y_r$ of X of codimension $0, \ldots, r$, respectively, such that*

$$Y = Y_r \subsetneq Y_{r-1} \subsetneq \cdots \subsetneq Y_0 = X.$$

PROOF: We prove the statement by induction on r. If $r = 1$, then there is nothing to prove. Suppose $r > 1$. Since $Y \subsetneq X$, there exists a non-zero $f \in \mathrm{I}(Y)$ such that f does not vanish on X, i.e. such that $f \neq \mathrm{I}(X)$. Moreover, since $\mathrm{I}(Y)$ is prime, we can assume that f is irreducible. Then $Y_i = \mathrm{V}(f)$ is a subvariety of X of codimension 1 that contains Y. Then $Y \subsetneq Y_I \subsetneq X$. Repeat the construction with $Y \subsetneq Y_1$ to get a subvariety Y_2 of Y_1 of codimension 1 and such that $Y \subsetneq Y_2 \subsetneq Y_1 \subsetneq X$, and continue inductively to prove the statement.□

The last corollary suggests the following characterization of the dimension of a variety, which could be called topological, as it involves only the Zariski topology of the variety and no additional structure.

2.5.10 Corollary. *The dimension of an affine variety X is the largest integer d for which there exists a chain of irreducible closed subsets*

$$X_1 \subsetneq \cdots \subsetneq X_d = X.$$

PROOF: If $X = \{p\}$, then this is clear from Theorem 2.5.3. Otherwise, this follows from the previous corollary with $Y = \{p\}$ for some $p \in X$. $\square$

The *Krull dimension* of a ring R is defined as the length of the longest chain of prime ideals in R. Let $X \subseteq \mathbb{A}^n$ be an affine variety. Since prime ideals of $\Gamma(X)$ correspond to prime ideals of $\Bbbk[x_1, \ldots, x_n]$ that contain $\mathrm{I}(X)$, the chains of prime ideals

$$I_1 \subsetneq \cdots \subsetneq I_d$$

in $\Gamma(X)$ correspond to chains of prime ideals

$$\mathrm{I}(X) \subseteq J_1 \subsetneq \cdots \subsetneq J_d$$

of $\Bbbk[x_1, \ldots, x_n]$. In turn, such chains of prime ideals of $\Bbbk[x_1, \ldots, x_n]$ correspond to chains of irreducible closed sets

$$\mathrm{V}(J_d) \subsetneq \mathrm{V}(J_{d-1}) \subsetneq \cdots \subsetneq \mathrm{V}(J_1) \subseteq X.$$

Therefore, by Corollary 2.5.10, we see that the Krull dimension of $\Gamma(X)$ is equal to the dimension of X.

Chapter 3

Local Properties of Affine Varieties

Throughout the remainder of these notes, we assume that $\Bbbk$ is algebraically closed.

3.1 Local Rings

3.1.1 Definition. Let X be an affine variety. If $p \in X$, the *local ring of X at p*, denoted by $\mathcal{O}_p(X)$, is the subring of $\Bbbk(X)$ consisting of those rational functions that are defined at p. The *maximal ideal of p* is

$$\mathrm{M}_p(X) = \{f \in \mathcal{O}_p(X) \mid f(p) = 0\}.$$

Consider the evaluation homomorphism from $\mathcal{O}_p(X)$ to $\Bbbk$. It is surjective with kernel $\mathrm{M}_p(X)$. By the First Isomorphism Theorem, $\mathcal{O}_p(X)/\mathrm{M}_p(X) \cong \Bbbk$, implying that $\mathrm{M}_p(X)$ is a maximal ideal. To justify calling $\mathrm{M}_p(X)$ *the* maximal ideal of p, note that an element $f \in \mathcal{O}_p(X)$ is a unit if and only if $f(p) \neq 0$, so $\mathrm{M}_p(X)$ is the entire set of non-units, and hence is the *unique* maximal ideal of $\mathcal{O}_p(X)$.

Remark. The local ring captures the local properties of a variety at a point p, i.e. those that depend only on behaviour in neighbourhoods of p.

3.1.2 Theorem. *Let X be an affine variety, and let p be a point of X. Then $\mathcal{O}_p(X)$ is Noetherian.*

Proof: Consider an ideal $J \subseteq \mathcal{O}_p(X)$. Then, $J \cap \Gamma(X)$ is an ideal of $\Gamma(X)$ and is therefore finitely generated, say by $f_1, \ldots, f_r$. We shall show that these elements also generate J in $\mathcal{O}_p(X)$, thus proving that $\mathcal{O}_p(X)$ is Noetherian. Let $f \in J$. Since f is regular at p, there is a polynomial $b \in \Gamma(X)$ such that $b(p) \neq 0$ and $bf \in \Gamma(X)$. In fact, $bf \in J \cap \Gamma(X)$, and so can be expressed as

a linear combination of $f_1, \ldots, f_r$. Therefore f can be expressed as a linear combination of rational functions regular at p (this is seen by dividing by b).$\square$

3.1.3 Definition. The *ring of regular functions* on X, denoted $\mathcal{O}(X)$, is the set of rational functions that are defined for all $p \in X$, i.e.

$$\mathcal{O}(X) = \bigcap_{p \in X} \mathcal{O}_p(X).$$

An element of $\mathcal{O}(X)$ is called a *regular function*.

Clearly $\Gamma(X) \subseteq \mathcal{O}(X)$. In fact, we will see that $\Gamma(X) = \mathcal{O}(X)$, essentially because $\Bbbk$ is algebraically closed, but if we were to consider the same definitions in the case where $\Bbbk$ is not algebraically closed, equality could fail.

3.1.4 Theorem. *Let $X \subseteq \mathbb{A}^n$ be an affine variety. Then $\mathcal{O}(X) = \Gamma(X)$.*

Proof: We need only show that $\mathcal{O}(X) \subseteq \Gamma(X)$. If $f \in \mathcal{O}(X)$, define

$$J_f = \{g \in \Bbbk[x_1, \ldots, x_n] \mid \overline{g} f \in \Gamma(X)\}.$$

Clearly, J_f is an ideal of $\Bbbk[x_1, \ldots, x_n]$. Moreover, since $\overline{g} = 0$ for all $g \in \mathrm{I}(X)$, we have that $\mathrm{I}(X) \subseteq J_f$. Hence $\mathrm{V}(J_f) \subseteq X$ is the pole set of f. However, since $f \in \mathcal{O}(X)$, the pole set $\mathrm{V}(J_f)$ of f is empty. Therefore, by the Nullstellensatz,

$$\Bbbk[x_1, \ldots, x_n] = \mathrm{I}(\mathrm{V}(J_f)) = \sqrt{J_f}.$$

But then $1 \in \sqrt{J_f}$, so $1 \in J_f$, which implies that $f \in \Gamma(X)$. $\square$

Before we proceed, we will introduce some notation. Let $R \subseteq S$ be two rings with identity and let $I \subseteq R$ be an ideal. Then IS denotes the ideal in S generated by I. Note that $I \subseteq IS$, but the inclusion may be strict.

Since $\Gamma(X) \subseteq \mathcal{O}_p(X)$, we have the following correspondence between ideals of $\Gamma(X)$ and $\mathcal{O}_p(X)$, given by

$$I \mapsto I\mathcal{O}_p(X) \qquad \text{and} \qquad J \mapsto \Gamma(X) \cap J.$$

In general, this correspondence is not one-to-one. For example, if I is a proper ideal of $\Gamma(X)$ and $f \in I$ is such that $f(p) \neq 0$, then f is a unit in $\mathcal{O}_p(X)$. Therefore, $I\mathcal{O}_p(X) = \mathcal{O}_p(X)$ and $I\mathcal{O}_p(X) \cap \Gamma(X) = \Gamma(X) \neq I$. However, if I is a prime ideal of $\Gamma(X)$ contained in the ideal M_p of p in $\Gamma(X)$, then we leave it as an exercise to show that $I\mathcal{O}_p(X) \cap \Gamma(X) = I$. Moreover, these maps give a one-to-one correspondence between prime ideals of $\Gamma(X)$ contained in M_p and prime ideals of $\mathcal{O}_p(X)$.

Using this ideal correspondence, one can show that the Krull dimension of $\mathcal{O}_p(X)$ is equal to the dimension of X.

3.2 Smooth Points on Affine Varieties

In this section, we introduce the notion of a smooth point on an affine variety.

3.2.1 Definition. Let X be an r-dimensional variety in $\mathbb{A}^n$ whose ideal is generated by $f_1, \ldots, f_s$. The *Jacobian matrix* of $f_1, \ldots, f_s$ at $p \in X$ is

$$\mathrm{Jac}(f_1, \ldots, f_s)(p) = \left[\frac{\partial f_i}{\partial x_j}(p)\right]_{s \times n}.$$

The *Zariski tangent space* to X at p is

$$\mathrm{T}_p(X) = \ker(\mathrm{Jac}(f_1, \ldots, f_s)(p)) \subset \Bbbk^n.$$

We say that p is a *smooth or non-singular point* of X if $\dim_{\Bbbk}(T_p(X)) = \dim X$, which happens if and only if the rank of $\mathrm{Jac}(f_1, \ldots, f_s)(p)$ is $n - r$. Otherwise, p is a *singular point* of X. Moreover, X is called *smooth* if it is smooth at every point; if not, it is said to be *singular*.

Note that

$$\mathrm{Jac}(f_1, \ldots, f_s)(p) = \begin{bmatrix} \nabla f_1(p) \\ \vdots \\ \nabla f_s(p) \end{bmatrix},$$

where

$$\nabla g(p) := \left(\frac{\partial g}{\partial x_1}(p), \ldots, \frac{\partial g}{\partial x_n}(p)\right)$$

is the gradient of g for any $g \in \Bbbk[x_1, \ldots, x_n]$. Therefore,

$$\mathrm{T}_p(X) = \{\vec{v} \in \Bbbk^n \mid \nabla f_i(p) \cdot \vec{v} = 0, \text{ for all } i = 1, \ldots, s\} \subset \Bbbk^n.$$

Furthermore, if we translate $T_p(X)$ by p in $\mathbb{A}^n$, we obtain the 'physical' tangent space to X at p in $\mathbb{A}^n$.

3.2.2 Proposition. *The definitions of smoothness and Zariski tangent space are independent of the choice of generators of $I(X)$.*

Proof: Suppose that $I(X) = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. Let us verify that $\mathrm{Jac}(f_1, \ldots, f_s)(p)$ and $\mathrm{Jac}(g_1, \ldots, g_t)(p)$ have the same rank at every $p \in X$. Since $f_i \in \langle g_1, \ldots, g_t \rangle$, for all $i = 1, \ldots, s$, there exist $a_{il} \in k[x_1 \ldots, x_n]$ such that $f_i = \sum_{l=1}^{t} a_{il} g_l$. Therefore,

$$\frac{\partial f_i}{\partial x_j}(p) = \sum_{l=1}^{t} \left[\frac{\partial a_{il}}{\partial x_j}(p) g_l(p) + a_{il}(p) \frac{\partial g_l}{\partial x_j}(p)\right] = \sum_{l=1}^{t} a_{il}(p) \frac{\partial g_l}{\partial x_j}(p),$$

where the second equality follows from the fact that $g_l(p) = 0$, for all $l = 1, \ldots, t$. Consequently,

$$\nabla f_i(p) = \left(\sum_{l=1}^{t} a_{il}(p) \frac{\partial g_l}{\partial x_1}(p), \ldots, \sum_{l=1}^{t} a_{il}(p) \frac{\partial g_l}{\partial x_n}(p)\right) = \sum_{l=1}^{t} a_{il}(p) \nabla g_l(p),$$

and $\nabla f_i(p) \in \text{span}_k\{\nabla g_1(p), \ldots, \nabla g_t(p)\}$ for all $i = 1, \ldots, s$.

Similarly, $g_l = \sum_{i=1}^{t} b_{li} f_i$ for some $b_{li} \in \Bbbk[x_1, \ldots, x_n]$, implying that $\nabla g_l(p) \in \text{span}_{\Bbbk}\{\nabla f_1(p), \ldots, \nabla f_s(p)\}$, for all $l = 1, \ldots, t$. Thus,

$$\begin{aligned} \text{rk}(\text{Jac}(f_1, \ldots, f_s)(p)) &= \dim_k(\text{span}_k\{\nabla f_1(p), \ldots, \nabla f_s(p)\}) \\ &= \dim_k(\text{span}_k\{\nabla g_1(p), \ldots, \nabla g_t(p)\}) \\ &= \text{rk}(\text{Jac}(g_1, \ldots, g_t)(p)). \end{aligned}$$

Furthermore, $\ker(\text{Jac}(f_1, \ldots, f_s)(p)) = \ker(\text{Jac}(g_1, \ldots, g_t)(p))$. □

3.2.3 Examples.

(i) $\mathbb{A}^n$ is smooth. Indeed, $\text{I}(\mathbb{A}^n) = \langle 0 \rangle$, so that $\text{T}_p(\mathbb{A}^n) = \Bbbk^n \simeq \mathbb{A}^n$ for all $p \in \mathbb{A}^n$; hence, $\dim_{\Bbbk}(\text{T}_p(\mathbb{A}^n)) = \dim \mathbb{A}^n$ for all $p \in \mathbb{A}^n$.

(ii) Let $X = \text{V}(f) \subset \mathbb{A}^n$ be an irreducible hypersurface, with $f \in \Bbbk[x_1, \ldots, x_n]$ an irreducible polynomial. Then X is non-singular at $p \in X$ if $\nabla f(p) \neq 0$. Equivalently, X is non-singular at p if and only if there exists a well-defined normal direction to X at p, in which case the tangent space to X at p is given by

$$\text{T}_p(X) = \{\vec{v} \in \Bbbk^n \mid \nabla f(p) \cdot \vec{v} = 0\} \subsetneq \Bbbk^n$$

and $\dim_{\Bbbk}(\text{T}_p(X)) = \dim(X) = n - 1$. Otherwise, $\text{T}_p(X) = \Bbbk^n \simeq \mathbb{A}^n$.

For example:

- The irreducible hypersurface $X = \text{V}(x^2 + x^3 - y^2) \subset \mathbb{A}^3$ has a double line of singularities along the z-axis.
- The double cone $\text{V}(x^2 + y^2 - z^2) \subset \mathbb{A}^3$ has a singularity at $(0, 0, 0)$.

(iii) More general varieties are intersections of hypersurfaces. For instance, consider a variety in $\mathbb{A}^3$ of the form

$$X = \text{V}(f, g) = \text{V}(f) \cap \text{V}(g) \subset \mathbb{A}^3,$$

where $f, g \in \Bbbk[x, y, z]$ are irreducible polynomials with distinct zero sets. Then, X is smooth at p if and only if

$$\text{Jac}(f, g)(p) = \begin{bmatrix} \nabla f(p) \\ \nabla g(p) \end{bmatrix}$$

has rank 2 if and only if $\nabla f(p), \nabla g(p) \neq 0$ and $\nabla f(p) \nparallel \nabla g(p)$ if and only if $\text{V}(f)$ and $\text{V}(g)$ have distinct tangent planes at p whose intersection is the tangent line

$$\begin{aligned} \text{T}_p(X) &= \text{T}_p(\text{V}(f)) \cap \text{T}_p(\text{V}(g)) \\ &= \{\vec{v} \in \mathbb{A}^n \mid \nabla f(p) \cdot \vec{v} = \nabla g(p) \cdot \vec{v} = 0\} \subset \mathbb{A}^3 \end{aligned}$$

to X at p.

For example, let $X = \mathrm{V}(y - x^2, z - x^3) \subset \mathbb{A}^3$ be the twisted cubic. Then

$$\mathrm{Jac}(y - x^2, z - x^3) = \begin{bmatrix} -2x & 1 & 0 \\ -3x^2 & 0 & 1 \end{bmatrix},$$

which has rank 2 for every point $(x, y, z) \in \mathbb{A}^3$, and the tangent line to X at $p = (x_0, y_0, z_0)$ is $\mathrm{T}_p(X) = \mathrm{V}(-2x_0x + y, -3x_0^2x + z)$.

At every point $p \in X$, we define the *Zariski cotangent space* of X at p to be $\mathrm{T}_p(X)^*$. The following theorem tells us that the cotangent space of X at p can be completely described in terms of the maximal ideal $\mathrm{M}_p(X)$ of X at p.

3.2.4 Theorem. *Let $X \subset \mathbb{A}^n$ be an affine variety and $p = (a_1, \ldots, a_n) \in X$. Then*

$$\mathrm{M}_p(X)/(\mathrm{M}_p(X))^2 \simeq (\mathrm{T}_p(X))^*,$$

where the k-vector space isomorphism is induced by the differential map

$$d_p : \Bbbk[x_1, \ldots, x_n] \to (\mathbb{A}^n)^*, f \mapsto \frac{\partial f}{\partial x_1}(p)(x_1 - a_1) + \cdots + \frac{\partial f}{\partial x_n}(p)(x_n - a_n).$$

Proof: Let M be the ideal of p in $\Bbbk[x_1, \ldots, x_n]$. The differential map is linear, surjective, and its kernel consists of all polynomials with no constant or linear terms (i.e. the ideal $M^2 = \langle (x_i - a_i)(x_j - a_j), i, j = 1, \ldots, n \rangle$), implying that $(\mathbb{A}^n)^* \cong M/M^2$.

Now d_p descends properly to a map $\Gamma(X) \to (\mathrm{T}_p(X))^*$. Suppose that $\mathrm{I}(X)$ is generated by $f_1, \ldots, f_s \in \Bbbk[x_1, \ldots, x_n]$. If $\overline{g} = \overline{g'}$ in $\Gamma(X)$, then $g' = g + h$ for some $h \in \mathrm{I}(X)$. In particular, $h = \sum_{i=1}^s h_i f_i$ with $h_i \in \Bbbk[x_1, \ldots, x_n]$ and

$$d_p g' = d_p g + \sum_{i=1}^n \left(d_p h_i \cdot f_i(p) + h_i(p) \cdot d_p f_i \right).$$

Since $f_i(p) = 0$ for all $i = 1, \ldots, s$, this reduces to $d_p g' = d_p g + \sum_{i=1}^n h_i(p) \cdot d_p f_i$.

Recall that, as a subset of $\mathbb{A}^n$, the tangent space to X at p is the translate of

$$\mathrm{T}_p(X) = \{ \vec{v} \in \Bbbk^n \mid \nabla f_i(p) \cdot \vec{v} = 0, \text{ for all } i = 1, \ldots, s \} \subset \Bbbk^n$$

by p. Moreover, for any such vector $\vec{v} + p$, we have $d_p f_i(\vec{v} + p) = \nabla f_i(p) \cdot \vec{v} = 0$ for all $i = 1, \ldots, s$. Consequently, if we restrict ourselves to $T_p(X)$, we obtain

$$d_p g'|_{\mathrm{T}_p(X)} = d_p g|_{\mathrm{T}_p(X)},$$

implying that

$$d_p \overline{g} := d_p g|_{\mathrm{T}_p(X)}$$

is a well-defined linear functional on $\mathrm{T}_p(X)$ for any $\overline{g} \in \Gamma(X)$. Note that $\overline{M} = \langle \overline{x}_1 - a_1, \ldots, \overline{x}_n - a_n \rangle \subset \Gamma(X)$ is the set of elements of $\Gamma(X)$ that are zero at p, and $\overline{M}^2$ is the kernel of d_p.

Further, d_p extends properly to a map $\mathrm{M}_p(X) \to (\mathrm{T}_p(X))^*$. Indeed, suppose a rational function is given by $\overline{g}_1/\overline{g}_2$ in a neighbourhood of p, for some $g_1, g_2 \in \Bbbk[x_1, \ldots, x_n]$, where $g_2(p) \neq 0$ and $g_1(p) = 0$. Then

$$d_p\left(\frac{\overline{g}_1}{\overline{g}_2}\right) := \frac{(d_p g_1)g_2(p) - g_1(p)(d_p g_2)}{g_2(p)^2}|_{\mathrm{T}_p(X)} = \frac{d_p g_1}{g_2(p)}|_{\mathrm{T}_p(X)},$$

where the second equality follows from the fact that $g_1(p) = 0$. Finally, since $\mathrm{M}_p(X) = \overline{M}\mathcal{O}_p(X)$, we see that $(\mathrm{M}_p(X))^2 = \overline{M}^2\mathcal{O}_p(X)$ is the kernel of d_p, so $(\mathrm{T}_p(X))^* \simeq \mathrm{M}_p(X)/(\mathrm{M}_p(X))^2$. □

3.2.5 Examples.

(i) Let X be the parabola $\mathrm{V}(y - x^2) \subset \mathbb{A}^2$. Then, X is smooth and $\Gamma(X) = \Bbbk[t]$. At $p = (0,0)$, $\mathrm{M}_p(X) = \langle \overline{x} \rangle$ and $\mathrm{M}_p(X)/(\mathrm{M}_p(X))^2 = \{\lambda\overline{x} \mid \lambda \in \Bbbk\}$.

(ii) Let X be the cusp curve $\mathrm{V}(y^2 - x^3)$, which is singular at $p = (0,0)$. Here $\Gamma(X) = \Bbbk[x,y]/\langle y^2 - x^3 \rangle$ and $\mathrm{M}_{(0,0)}(X) = \langle \overline{x}, \overline{y} \rangle \subseteq \Bbbk(X)$. We have

$$(\mathrm{M}_{(0,0)}(X))^2 = \langle \overline{x}^2, \overline{xy}, \overline{y}^2 \rangle = \langle \overline{x}^2, \overline{xy} \rangle,$$

so $\mathrm{M}_{(0,0)}(X)/(\mathrm{M}_{(0,0)}(X))^2 = \{a\overline{x} + b\overline{y} \mid a, b \in \Bbbk\}$, which has dimension two, confirming that $(0,0)$ is a singular point.

3.2.6 Theorem. *Let X be a variety of dimension r and $p \in X$. The minimal number generators of $M_p(X)$ is equal to* $\dim_k(M_p(X)/M_p^2(X))$.

Proof: Let $M = M_p(X)$. Suppose that $\{\overline{m}_1, \ldots, \overline{m}_s\}$ is a basis of the k-vector space M/M^2, for some $m_i \in M$. Let us show that $M = < m_1, \ldots, m_s >$. Set $M' = < m_1, \ldots, m_s >$. Clearly, $M' \subseteq M$ so that M/M' is well-defined, and we need to show that $M = M'$ or, equivalently, that $M/M' = 0$. Suppose that $M = < a_1, \ldots, a_t >$. Now, in M/M^2, $\overline{a}_i = \alpha_{i1}\overline{m}_1 + \cdots + \alpha_{is}\overline{m}_s$ for some $\alpha_{i1}, \ldots, \alpha_{is} \in k$, so that

$$a_i = (\alpha_{i1}m_1 + \cdots + \alpha_{is}m_s) + b_i$$

with $b_i \in M^2$. Since $(\alpha_{i1}m_1 + \cdots + \alpha_{is}m_s) \in M'$, we have $a_i \equiv b_i$ in M/M'. However, $b_i = \sum_j \mu_{ij}a_j$ for some $\mu_{ij} \in M$. Note that $\mu_{ij}(p) = 0$ for all i, j. Thus, $a_i \equiv \sum_j \mu_{ij}a_j$ in M/M' or, equivalently, the $a_1, \ldots, a_t$ are solutions of the homogeneous system

$$\sum_{j=1}^{t}(\delta_{ij} - \mu_{ij})a_j \equiv 0 \qquad (***)$$

in M/M', where δ_{ij} is the Kronecker delta. But $\det(\delta_{ij} - \mu_{ij})$ is a unit in $\mathcal{O}_p(X)$ since $\det(\delta_{ij} - \mu_{ij})(p) = \det(\delta_{ij}) = 1$. Therefore, the homogeneous system (***) only has the trivial solution and $a_1, \ldots, a_t \equiv 0$ in M/M', proving that $M = M'$. □

A local ring R is called *regular* if the minimum number of generators of its maximal ideal M is equal to the Krull dimension $\dim R$ of R. We therefore have:

3.2.7 Theorem. *Let X be a variety and $p \in X$. Then, p is smooth if and only if $\mathcal{O}_p(X)$ is regular.*

PROOF: By definition, the point p is smooth if and only if $\dim_k T_p(X) = \dim X$. Moreover, we have seen that $\dim X = \dim \mathcal{O}_p(X)$. Consequently, since $T_p(X)$ is isomorphic to $(M_p(X)/M_p^2(X))^*$ as a k-vector space and the minimal number of generators of $M_p(X)$ is $\dim_k(M_p(X)/M_p^2(X))$, we obtain that p is smooth if and only if the minimal number of generators of $M_p(X)$ is $\dim \mathcal{O}_p(X)$. □

A local Noetherian ring with Krull dimension 1 whose maximal ideal is principal is called a *discrete valuation ring (DVR)*. Note that $\mathcal{O}_p(X)$ is a local Noetherian ring of Krull dimension 1 whenever $\dim X$, in which case, $M_p(X)$ is principal at smooth points p of X. We therefore have:

3.2.8 Corollary. *If X is a curve and $p \in X$, then p is smooth if and only if $\mathcal{O}_p(X)$ is a DVR.*

In fact, Hartshorne defines a smooth curve as being a collection of DVRs (the idea being that if you are given the local ring at every point, you can recover the tangent line at every point and "integrate" the tangent directions to get the curve).

Another consequence of Theorem 3.2.7 is the the following:

3.2.9 Corollary. *Smoothness is invariant under isomorphism.*

PROOF: Exercise. □

Remark: Note however that smoothness may not be invariant under birational equivalence. For example, $X = V(y - x^2) \subset \mathbb{A}^2$ is smooth at every point, while $X' = V(y^2 - x^3) \subset \mathbb{A}^2$ is smooth everywhere except at $(0, 0)$. By Corollary 3.2.9, this means that $X \not\sim X'$. Nonetheless, $X \sim \mathbb{A}^1 \sim X'$.

3.2.10 Proposition. *Let X be an affine variety. Then, $\dim_k(T_p(X)) \geq r$, for all $p \in X$.*

PROOF: This proof is similar to the proof of Corollary 2.5.9 in the lecture notes. Let f_1 be a non-zero element in $\Gamma(X)$ such that $f_1(p) = 0$. Then the irreducible components of $Y = X \cap V(f_1)$ have codimension one in X and at least one of them contains p. Let Y_1 be one of the irreducible components containing p. Now, let f_2 be a non-zero element in $\Gamma(Y_1)$ such that $f_2(p) = 0$. Then the irreducible components of $Y_1 \cap V(f_2)$ have codimension one in Y_1 and

at least one of them contains p. Proceeding inductively we obtain a chain of subvarieties of X containing p

$$\{p\} \subsetneq Y_{r-1} \subsetneq \cdots \subsetneq Y_1 \subsetneq X,$$

which must have length r since $\dim X = r$. Moreover, $\{p\} = V(f_1, \ldots, f_r)$ and r is the minimal number of functions whose common zero set is p. Then, since $< f_1, \ldots, f_r > \subset M_p(X)$, this means that $M_p(X)$ is generated by at least r elements, so that

$$\dim_k(T_p(X)) = \dim_k(M_p(X)/M_p^2(X)) \geq r = \dim X. \qquad \square$$

Remark: Suppose that $I(X)$ is generated by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Since $T_p(X) = \ker(\mathrm{Jac}(f_1, \ldots, f_s)(p))$, the proposition implies that

$$\mathrm{rk}(\mathrm{Jac}(f_1, \ldots, f_s)(p)) \leq n - r$$

with equality holding if and only if p is a smooth point of X.

We can then use Proposition 3.2.10 to prove that the set of singular points of a variety is algebraic.

3.2.11 Proposition. *The set of singular points of a variety X is a proper algebraic subset of X.*

Proof: To come. $\square$

The generators of $M_p(X)$ are called *local parameters of* $\mathcal{O}_p(X)$. How does one find them?

3.2.12 Examples.

(i) We saw in example 3.2.3(i) that $\mathbb{A}^n$ is smooth at every point $p = (a_1, \ldots, a_n)$. Consequently, $M_p(\mathbb{A}^n)$ must have at least $n = \dim \mathbb{A}^n$ generators. Indeed, $M_p(\mathbb{A}^n) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, so that $\{t_1 = x_1 - a_1, \ldots, t_n = x_n - a_n\}$ is a set of local parameters for $\mathcal{O}_p(\mathbb{A}^n)$.

(ii) Suppose that $X = V(f) \subset \mathbb{A}^n$ is a hypersurface with $I(X) = \langle f \rangle$ for some irreducible polynomial $f \in k[x_1, \ldots, x_n]$. Referring to example 3.2.3(ii), X is smooth at the point p if and only if $\nabla f(p) \neq \vec{0}$, in which case the Zariski tangent space of X at p is given by

$$\mathrm{T}_p(X) = \{\vec{v} \in \Bbbk^n \mid \nabla f(p) \cdot \vec{v} = 0\} \subsetneq \Bbbk^n$$

and $\dim_{\Bbbk}(\mathrm{T}_p(X)) = \dim(X) = n - 1$. After an appropriate affine transformation taking p to the origin, we can assume without loss of generality that $p = (0, \ldots, 0)$. In this case, $f(p) = f(0, \ldots, 0) = 0$ since $p \in X$, implying that f does not have a constant term. Moreover, if we write

$$f = a_1 x_1 + \cdots + a_n x_n + (\text{terms of order} \geq 2),$$

then

$$\nabla f(p) = (a_1, \ldots, a_n)$$

because the partial derivatives of the higher order terms in f vanish at $p = (0, \ldots, 0)$. Hence,

$$\begin{aligned} \mathrm{T}_p(X) &= \{(x_1, \ldots, x_n) \in \Bbbk^n \mid \nabla f(p) \cdot (x_1, \ldots, x_n) = 0\} \\ &= \{(x_1, \ldots, x_n) \in \Bbbk^n \mid a_1 x_1 + \cdots + a_n x_n = 0\}. \end{aligned}$$

In other words, the Zariski tangent space to X at $p = (0, \ldots, 0)$ is the zero set of the linear part of f. Moreover, since $\nabla f(p) \neq \vec{0}$, at least one of the a_i's is non-zero, say a_{i_0}, we see that X is smooth at $p = (0, \ldots, 0)$ if and only if the linear part of f is non-zero. Let us show the following:

Claim. If $a_{i_0} \neq 0$, then $M_p(X) = \langle x_1, \ldots, \hat{x}_{i_0}, \ldots, x_n \rangle$, where $\hat{x}_{i_0}$ indicates that x_{i_0} does not appear as a generator.

Proof: We first note that $M_p(X) = \langle \bar{x}_1, \ldots, \bar{x}_n \rangle$. But X is smooth at p and $\dim X = n - 1$, so $M_p(X)$ only requires $n - 1$ generators. Grouping terms with x_{i_0}, we get

$f = a_{i_0} x_{i_0}$(1+higher order terms involving x_{i_0})

$$+(a_1 x_1 + \cdots + \widehat{a_{i_0} x_{i_0}} + \cdots + a_n x_n) + h(x_i, \ldots, x_{i_0}, \ldots, x_n)$$

with h a polynomial in $x_1, \ldots, \hat{x}_{i_0}, \ldots, x_n$ that only involves monomials of degree ≥ 2. This means in particular that $\bar{h} \in M_p(X)$ in $\mathcal{O}_p(X)$. Let $g := (1 + \text{higher order terms involving } x_{i_0})$ in the expression of f. Then, $g(0, \ldots, 0) = 1 \neq 0$, implying that $\bar{g}$ is a unit in $\mathcal{O}_p(X)$. Thus, in $\mathcal{O}_p(X)$, we have

$$0 = \bar{f} = a_{i_0} \bar{x}_{i_0} \bar{g} + \bar{h}$$

or, equivalently,

$$\bar{x}_{i_0} = -a_{i_0}^{-1} \bar{g}^{-1} \bar{h},$$

implying that $x_{i_0} \in \langle x_1, \ldots, \hat{x}_{i_0}, \ldots, x_n \rangle$ and $M_p(X) = \langle x_1, \ldots, \hat{x}_{i_0}, \ldots, x_n \rangle$.□

Putting it all together, we obtain:

3.2.13 Proposition. *Let $X = V(f) \subset \mathbb{A}^n$ be a hypersurface with $I(X) = \langle f \rangle$ for some irreducible polynomial $f \in k[x_1, \ldots, x_n]$. Let $p = (0, \ldots, 0)$. Suppose that $p \in X$ so that f has no constant term. Then, X is smooth at p if and only if the linear part*

$$a_1 x_1 + \cdots + a_n x_n$$

of f is non-zero, in which case

$$\mathrm{T}_p(X) = V(a_1 x_1 + \cdots + a_n x_n) \subset \mathbb{A}^n.$$

Moreover, if $a_{i_0} \neq 0$, then

$$M_p(X) = \langle x_1, \ldots, \hat{x}_{i_0}, \ldots, x_n \rangle,$$

where $\hat{x}_{i_0}$ indicates that x_{i_0} does not appear as a generator of $M_p(X)$.

To illustrate the proposition with a concrete example, consider the paraboloid $X = V(z - x^2 - y^2) \subset \mathbb{A}^3$, so that $f = z - x^2 - y^2$. Then, $(0,0,0) \in X$ and f has non-zero linear part z. Therefore, X is smooth at $(0,0,0)$ with tangent plane $z = 0$. Moreover, $M_p(X) = \langle \bar{x}, \bar{y} \rangle$. Note that $\bar{z} = \bar{x}^2 + \bar{y}^2 \in M_p^2(X)$.

Remarks. (i) Suppose that $f = f_1 + f_m + \cdots + f_d$, where each f_i is a homogeneous polynomial of degree i and f_m is the first homogeneous component of f, other than the linear part f_1, that is non-zero. Then, in $\mathcal{O}_p(X)$, we have

$$\bar{f}_1 = -\bar{f}_m - \cdots - \bar{f}_d \in M_p^m(X)$$

with $m \geq 2$ This shows, in particular, that the residue class of any linear polynomial whose zero set is $T_p(X)$ cannot be a generator of $M_p(X)$. We are, of course, assuming here that $p = (0, \ldots, 0)$.

(ii) When considering a point p other than the origin, first translate it to the origin, then carry out the above analysis.

For example, consider the hyperbola $X = V(xy - 1) \subset \mathbb{A}^2$ and $p = (1,1) \in X$. Set $v = x - 1$ and $w = y - 1$ so that p corresponds to $(0,0)$ in the (v,w)-plane. Then, $f(v,w) = (v+1)(w+1) = v + w + vw$ has non-zero linear part $v+w$, implying in particular that X is smooth at p with tangent line $v+w = 0$. Moreover, since the coefficients of both v and w are non-zero in $v + w$, either $\bar{v}$ or $\bar{w}$ can generate $M_p(X)$. Hence, $M_p(X) = \langle \bar{v} \rangle = \langle \bar{w} \rangle$. Going back to the coordinates x and y, we see that the tangent line to X at p is $x + y = 2$ and $M_p(X) = \langle \bar{x} - 1 \rangle = \langle \bar{y} - 1 \rangle$.

(iii) When $X = V(f) \subset \mathbb{A}^2$ is a plane curve and p is a smooth point of X, we know that $M_p(X)$ is principal. In fact, one can show that $M_p(X)$ can be generated by the residue class in $\mathcal{O}_p(X)$ of any linear polynomial $h \in k[x,y]$ such that $h = 0$ is a line passing through p that is *not* tangent to X at p. In other words, $M_p(X) = \langle \bar{h} \rangle$. (Exercise.)

3.3 Smooth Points on Affine Plane Curves

In this section, we consider affine plane curves, that is, 1-dimensional varieties in $\mathbb{A}^2$:

$$C = V(f) \subset \mathbb{A}^2$$

with $f \in k[x,y]$ irreducible (and $V(f)$ infinite). We have seen that, in this case, a point $p \in C$ is smooth if and only if $\mathcal{O}_p(C)$ is DVR. In fact, if $p = (0,0)$, then $M_p(C)$ is generated by a local parameter of the form $t = \bar{h}$ for any homogeneous linear polynomial such that $h = 0$ is a line through p that is *not* tangent to C at p.

Why is $\mathcal{O}_p(C)$ called a DVR?

3.3.1 Proposition. *Suppose that $\mathcal{O}_p(C)$ is a DVR with maximal ideal $M_p(C) = \langle t \rangle$. For every $0 \neq z \in \mathcal{O}_p(C)$, we have*

$$z = t^n u$$

for some $n \in \mathbb{Z}^{\geq 0}$ and unit u in $\mathcal{O}_p(C)$. Moreover, this decomposition is unique.

PROOF: If z is a unit then there is nothing to prove (take $n = 0$ and $u = z$). If z is not a unit then $z \in M_p(C)$, so $z = z_1 t$ for some $z_1 \in \mathcal{O}_p(C)$, and $z_1 \neq 0$. Repeating this process, by induction we get a sequence $z = z_0, z_1, z_2, \ldots$ such that $z_i = z_{i+1} t$ for all $i \geq 0$. The sequence must eventually terminate with $z_n = u$, a unit, giving $z = ut^n$. Indeed, suppose the sequence is infinite. The chain of ideals $\langle z_0 \rangle \subseteq \langle z_1 \rangle \subseteq \langle z_2 \rangle \subseteq \cdots$ must eventually be stationary since $\mathcal{O}_p(C)$ is Noetherian. Therefore there is $n \geq 0$ such that $\langle z_{n-1} \rangle \subsetneqq \langle z_n \rangle = \langle z_{n+1} \rangle = \cdots$. Then z_n and z_{n+1} differ by a factor of a unit, a contradiction since $z_n = z_{n+1} t$ and t is not a unit.

Finally, suppose $t^n u = t^m v$ for some $n \geq m \geq 0$ and u, v units in $\mathcal{O}_p(C)$. In PIDs we may cancel terms, hence $t^{n-m} = vu^{-1}$ is a unit, which implies that $n = m$ and $u = v$. □

Remark. Local parameters are unique up to a unit in $\mathcal{O}_p(C)$.

Given a non-zero element $z \in \mathcal{O}_p(C)$ such that $z = t^n u$ for a unit $u \in \mathcal{O}_p(C)$, we let $\operatorname{ord}_p^C(z) = n$ to be the *valuation of z*. Note that $t(p) = 0$ and $u(p) \neq 0$, so that we can think of n as the order of vanishing of z at $p \in C$. We also let $\operatorname{ord}_p^C(0) = \infty$. We thus have a *(discrete) valuation map* (also called the *order map*) $\operatorname{ord}_p^C : \mathcal{O}_p(C) \to \mathbb{N} \cup \{\infty\}$. Note that ord_p^C has the following important properties:

(i) ord_p^C is independent of the choice of local parameter,
(ii) $\operatorname{ord}_p^C(z) = \infty$ if and only if z is identically zero on C,
(iii) $\operatorname{ord}_p^C(z) = 0$ if and only if z is a unit in $\mathcal{O}_p(C)$,
(iv) $\operatorname{ord}_p^C(zz') = \operatorname{ord}_p^C(z) + \operatorname{ord}_p^C(z')$,
(v) $\operatorname{ord}_p^C(z + z') \geq \min(\operatorname{ord}_p^C(z), \operatorname{ord}_p^C(z'))$.

PROOF: Exercise. □

This valuation map extends uniquely to a well-defined map $\operatorname{ord}_p^C : \Bbbk(C) \to \mathbb{Z} \cup \{\infty\}$ by letting $\operatorname{ord}_p^C(\overline{a}/\overline{b}) = \operatorname{ord}_p^C(\overline{a}) - \operatorname{ord}_p^C(\overline{b})$. Then

$$\mathcal{O}_p(C) = \{f \in \Bbbk(C) \mid \operatorname{ord}_p^C(f) \geq 0\}$$

is the (discrete) valuation ring of $\Bbbk(C)$ and

$$\mathrm{M}_p(C) = \{f \in \Bbbk(C) \mid \operatorname{ord}_p^C(f) > 0\}.$$

Remark. More generally, given a field K and an ordered abelian group, a map $v : K \setminus \{0\} \to G$ that satisfies the properties

(i) $v(xy) = v(x) + v(y)$,
(ii) $v(x + y) \geq \min(v(x), v(y))$

is called a *valuation of* K. Then,

$$R = \{x \in K \mid v(x) \geq 0\} \cup \{0\}$$

is the *valuation ring of* K, and

$$M = \{x \in K \mid v(x) > 0\} \cup \{0\}$$

is the unique maximal ideal of R. If $G = \mathbb{Z}$, then v is said to be a *discrete valuation* and R can easily be shown to be a discrete valuation ring in the sense that we defined earlier.

Let us compute the valuation of some examples.

3.3.2 Example. Let $C = V(y - x^2) \subset \mathbb{A}^2$ so that $I(C) = \langle f \rangle$ with $f = y - x^2 \in k[x, y]$. Note that $\bar{y} = \bar{x}^2$ in $k(C)$.

At $(0, 0) \in C$, since f has non-zero linear term y, C is smooth with tangent line $y = 0$. Therefore, $t = \bar{x}$ generates $M_{(0,0)}(C)$ because $x = 0$ is *not* tangent to C at $(0, 0)$. Consider the polynomial function $z = \bar{y} \in k(C)$. It is defined at $(0, 0)$ and $z = \bar{x}^2 = t^2 \cdot 1$ in $\mathcal{O}_{(0,0)}(C)$, implying that $\mathrm{ord}_{(0,0)}(C)(z) = 2$. In other words, x vanishes at order 2 at the origin.

Consider instead the polynomial function $z' = \bar{x} + \bar{y} \in k(C)$. It is of course defined at every point in C. Let us compute its order of vanishing at $(0, 0)$ and $(-1, 1)$ on C. At $(0, 0)$, $z' = \bar{x} + \bar{x}^2 = \bar{x}(\bar{x} + 1) = t^1 \cdot u$ with $u = \bar{x} + 1$ a unit in $\mathcal{O}_{(0,0)}(C)$ since $u(0, 0) = 1 \neq 0$. Thus, $\mathrm{ord}^C_{(0,0)}(z') = 1$. We should remark that, although z and z' both are linear polynomial functions, the reason z vanishes at order 2 at the origin and z' only at order 1 is because z corresponds to the tangent line to C at the origin.

Let us now compute $\mathrm{ord}^C_{(-1,1)}(z')$. We first translate to the origin by setting $v = x+1$ and $w = y-1$ so that $p = (x, y) = (-1, 1)$ become $p = (v, w) = (0, 0)$. Then, $f(v, w) = (w + 1) - (v - 1)^2 = (w - 2v) + v^2$ and $\bar{w} = 2\bar{v} + \bar{v}^2$ in $k(C)$. Moreover, we see that the tangent line to C at p is $w - 2v = 0$. This means in particular that $s = \bar{v}$ generates $M_p(C)$ because $v = 0$ is not tangent to C at p. Hence,

$$z' = \bar{x} + \bar{y} = (\bar{v} - 1) + (\bar{w} + 1) = \bar{v} + \bar{w} = \bar{v} + (2\bar{v} + \bar{v}^2) = \bar{v}(3 + \bar{v}) = s^1 \cdot u'$$

with $u' = 3 + \bar{v}$ a unit in $\mathcal{O}_p(C)$ since $u(p) = 3 \neq 0$. Therefore, $\mathrm{ord}^C_p(z') = 1$.

We finishing the example by noting that z' vanishes with order 1 at both $(0, 0)$ and $(-1, 1)$ on C. This is not very surprising because the zeroes of z' correspond to the intersection points of the line $x+y = 0$ with C and $x+y = 0$ is not tangent to C at either point.

3.3.3 Proposition. *Let C be an affine plane curve, and let p be a smooth point of C. Fix a local parameter $t \in \mathcal{O}_p(C)$, so that $\mathrm{M}_p(C) = \langle t \rangle$. Then any element $f \in \mathcal{O}_p(C)$ can be expressed as a unique formal power series*

$$f = \sum_{i=0}^{\infty} a_i t^i$$

such that $[f - (a_0 + a_1 t + \cdots + a_m t^m)] \in \mathrm{M}_p^{m+1}(C)$ for all m.

PROOF: Note that $\mathrm{M}_p^m(C) = \langle t^m \rangle$ for all m. Also, since each unit $u \in \mathcal{O}_p(C)$ can be written as $u = a_0 + f$, with $a_0 = u(0)$ and $f_1 = u - u(0) \in \mathrm{M}_p(C)$, the $\Bbbk$-vector space $\mathcal{O}_p(C)/\mathrm{M}_p(C)$ is isomorphic to $\{f(0) \mid f \in \mathcal{O}_p(C)\} \cong \Bbbk$. Similarly,

$$\mathrm{M}_p(C)/\mathrm{M}_p^{m+1}(C) \cong \{a_m t^m \mid a_m \in \Bbbk\} \cong \Bbbk.$$

Indeed, let $f in \mathrm{M}_p^m(C)$ be such that $f \notin \mathrm{M}_p^{m+1}(C)$. Then $f \neq 0$ and $f = t^m z$ for some $z \neq 0$. If z is not a unit, then $z = t^r u$, with $r \geq$ and u a unit. Thus $f = t^{m+r} u$, with $m + r \geq m + 1$, which contradicts the fact that $f \notin \mathrm{M}_p^{m+1}(C)$. Therefore, z is a unit and $z = a_m + f_1$, with $a_m \in \Bbbk$ and $f_1 \in \mathrm{M}_p(C)$, so that $f = a_m t^m + t^m f_1$. Since $t^m f_1 \in \mathrm{M}_p^{m+1}(C)$, $f \equiv a_m t^m (\mathrm{mod}\, \mathrm{M}_p^{m+1}(C))$.

We will now show the existence of the power series expansion. If $f \in \mathcal{O}_p(C)$ is non-zero, then $f = t^m u$, where u is a unit. Thus $f = t^m(a_m + f_1) = a_m t^m + t^m f_1$ for some $f_1 \in \mathrm{M}_p(C)$, and $f - a^m t^m = t^m f_1 \in \mathrm{M}_p^{m+1}(C)$. If $f_1 = 0$, we are done. Otherwise, since $f_1 \in \mathrm{M}_p$, $f_1 = t f_2$ for some $f_2 \in \mathcal{O}_p(C)$. Repeating the same process as above, we get a formal power series expansion

$$f = \sum_{i=0}^{\infty} a_i t^i,$$

with each $a_i \in \Bbbk$ and $[f - (a_0 + a_1 t + \cdots + a_m t^m)] \in \mathrm{M}_p^{m+1}(C)$ for all m.

To show uniqueness, it is enough to show that if $f = 0$, then every power series expansion of f must be identically zero. Suppose

$$f = \sum_{i=0}^{\infty} a_i t^i.$$

Then $a_0 = f(p) = 0$. Since $a_1 t = -(f - (a_0 + a_1 t)) \in \mathrm{M}_p^2(C)$ and $\mathrm{M}_p(C)/\mathrm{M}_p^2(C) \cong \{\alpha t \mid \alpha \in \Bbbk$, we must have $a_1 = 0$. In general, if $i > 0$, then

$$a_i t^i = -(f - (a_0 + a_t + \cdots + a_i t^i)) \in \mathrm{M}_p^{i+1}(C),$$

and $\mathrm{M}_p^i / \mathrm{M}_p^{i+1} \cong \{\alpha t^i \mid \alpha \in \Bbbk\}$, so $a_i = 0$. □

The power series in the above is called the *Taylor series expansion of f*.

Remark. If p is not smooth on C then one can still describe regular functions at p in terms of power series, except that in this case the power series expression may not be unique.

3.3.4 Definition. A polynomial $f \in \Bbbk[x_1, \ldots, x_n]$ is said to be homogeneous if each of its terms has the same degree, which we call the *degree* of f. A homogeneous polynomial of degree m is called an *m-form*.

Clearly, every polynomial is a sum of forms. Consider an affine plane curve $C = \mathrm{V}(f)$, and suppose $p = (0,0) \in C$, so that $f(0,0) = 0$. Let

$$f = f_m + f_{m+1} + \cdots + f_d,$$

where each f_i is an i-form and $f_m \neq 0$. Since $f(0,0) = 0$, $m \geq 0$. Thus, if $m \geq 2$, then C singular at p and the Zariski tangent space to C at p is 2-dimensional. However, there are always "preferred" tangent lines to C at p corresponding to the linear factors of f_m. More precisely, if $f_m = h_1 \cdots h_m$ with every h_j a 1-form, then $V(h_1), \ldots, V(h_m)$ are the *tangent directions* of C at p.

3.3.5 Definition. Let $f \in \Bbbk[x, y]$ and

$$f = f_m + \cdots + f_d,$$

where each f_i is an i-form and $f_m \neq 0$. If $p = (0,0)$, we define the *multiplicity* of $C = \mathrm{V}(f)$ at p to be m, and denote it by $\mathrm{m}_p(f)$.

Remark. If $\mathrm{m}_p(C) = 1$, then $C = \mathrm{V}(f)$ is smooth at p. Otherwise, it is singular.

3.4 Intersection Multiplicity

3.4.1 Definition. Let C and D be affine plane curves C and D. If $p \in \mathbb{A}^2$, we say that C and D *intersect properly* at p if C and D have no common component that passes through p, and that C and D *intersect transversally* if they are both smooth at p and have distinct tangent lines at p.

3.4.2 Examples.

(i) The curves given by $y - x$ and $y - x^2$ intersect transversally at $(0,0)$.
(ii) The curves given by $y - x^2$ and $y + x^2$ do not intersect transversally at $(0,0)$, since both curves have $y = 0$ as their tangent line at $(0,0)$.

3.4.3 Definition. Let $C = \mathrm{V}(f)$ and $D = \mathrm{V}(g)$ be affine plane curves, and let $p \in C$. We define the *intersection multiplicity* of C and D at p, denoted $\mathrm{I}(p, C \cap D)$, to be the order of vanishing of g at p on C, or the order of vanishing of f at p on D.

Let us suppose that C is smooth at p, so that we can assume, without loss of generality, that C is irreducible. Then $\mathcal{O}_p(C)$ is a DVR with $\mathrm{M}_p(C) = \langle t \rangle$ for some $t \in \mathcal{O}_p(C)$, and every element of $\mathcal{O}_p(C)$ can be expressed uniquely as a power series in t. If g has f as a factor, so that C is a component of D, then

$\overline{g} = 0 \in \mathcal{O}_p(C)$ and we define $\mathrm{I}(p, C \cap D) = \infty$. If $p \notin D$, so that C and D do not intersect at p, then $\overline{g}$ is a unit in $\mathcal{O}_p(C)$, and its order is zero. Otherwise, if f and g do not have a common factor (so that C and D intersect properly at p) then $\overline{g} = ut^m$, for some $1 \leq m < \infty$ and some unit u in $\mathcal{O}_p(C)$. In this case

$$\mathrm{I}(p, C \cap D) = \mathrm{ord}_p^C(\overline{g}) = m.$$

3.4.4 Examples.

(i) If $C = \mathrm{V}(y^2 - x^3 - x)$ and $D = \mathrm{V}(x+y)$ then C and D are both smooth at $(0,0)$. They have distinct tangent lines $\mathrm{V}(x)$ and $\mathrm{V}(x+y)$, respectively, so they intersect transversely at $(0,0)$ with intersection multiplicity 1.

(ii) If $C = \mathrm{V}(y^2 - x^3 - x^2)$ and $D = \mathrm{V}(x+y)$ then D is smooth at $(0,0)$ but C is not. C has tangent directions $\mathrm{V}(y+x)$ and $\mathrm{V}(y-x)$. Note that $f = -x^3 + (y-x)g$, so $\overline{f} = -\overline{x}^3$ in $\mathcal{O}_p(D)$. Since $\mathrm{V}(x)$ is not the tangent line to D at $(0,0)$, we set $t = \overline{x}$, so that $\overline{f} = -t^3 \in \mathcal{O}_p(D)$, giving $I(p, C \cap D) = \mathrm{ord}_p^D(\overline{f}) = 3$.

We will now investigate the properties of intersection multiplicity in this case where one of the curves is smooth at the point of intersection, and we will use these properties to define an intersection multiplicity for possibly non-singular curves.

3.4.5 Proposition. *Let $C = \mathrm{V}(f)$, where C is an irreducible affine plane curve smooth at $p \in \mathbb{A}^2$, and let $D = \mathrm{V}(g)$. Then:*

(i) *$\mathrm{I}(p, C \cap D)$ is invariant under affine coordinate changes;*

(ii) *$\mathrm{I}(p, C \cap D) = \infty$ if and only if C is a component of D;*

(iii) *if C and D intersect properly, then $\mathrm{I}(p, C \cap D) < \infty$. Also, $\mathrm{I}(p, C \cap D) = 0$ if and only if $p \notin C \cap D$;*

(iv) *if $g = g_1 g_2$, then $D = \mathrm{V}(g_1) \cup \mathrm{V}(g_2)$, and*

$$\mathrm{I}(p, C \cap D) = \mathrm{I}(p, C \cap \mathrm{V}(g_1)) + \mathrm{I}(p, C \cap \mathrm{V}(g_2));$$

(v) *$\mathrm{I}(p, C \cap D) = \mathrm{I}(p, C \cap E)$ for any curve $E = \mathrm{V}(g + f \cdot h)$;*

(vi) *$\mathrm{I}(p, C \cap D) = 1$ if and only if C and D intersect transversely at p, otherwise $\mathrm{I}(p, C \cap D) \geq m_p(C) m_p(D)$ with equality holding if they do not have common tangent directions at p;*

(vii) *if C and D are smooth at p, then $\mathrm{I}(p, C \cap D) = \mathrm{I}(p, D \cap C)$.*

Proof:

(i) Since $\Bbbk(C)$ is invariant under affine coordinate changes, the local $\mathcal{O}_p(C)$ is invariant under affine coordinate changes, so the order of vanishing is also invariant.

(ii) We have that

$$\begin{aligned} \mathrm{I}(p, C \cap D) = \infty &\iff \overline{g} = 0 \text{ in } \mathcal{O}_p(C) \\ &\iff g \in \mathrm{I}(C) = \langle f \rangle, \text{ where } f \text{ is irreducible} \\ &\iff f \text{ is a factor of } g \\ &\iff C \text{ is a component of } D. \end{aligned}$$

(iii) If C and D intersect properly at p, then $\overline{g} \neq 0$ in $\mathcal{O}_p(C)$ and $\overline{g}$ is not a unit (since it must have at least one zero on C). Thus, $\mathrm{ord}_p^C(\overline{g})$ is neither 0 nor ∞. Also, if $p \notin C \cap D$, then $\overline{g}$ is a unit in $\mathcal{O}_P(C)$, which implies that $\mathrm{ord}_p^C(\overline{g}) = 0$.

(iv) We have that

$$\mathrm{ord}_p^C(\overline{g}) = \mathrm{ord}_p^C(\overline{g_1} \cdot \overline{g_2}) = \mathrm{ord}_p^C(\overline{g_1}) + \mathrm{ord}_p^C(\overline{g_2}).$$

(v) If $h \in \Bbbk[x, y]$, let $g_0 = g + f \cdot h$. Then $\mathrm{V}(g_0) \cap C = \mathrm{V}(g) \cap C = D \cap C$ and $\mathrm{ord}_p^C(\overline{g_0}) = \mathrm{ord}_p^C(\overline{g})$ for any $p \in C \cap D$.

(vi) First note that $\mathrm{m}_p(C) = 1$ as C is smooth at p. Let t be a local parameter in $\mathcal{O}_p(C)$. Then, $\overline{g} = t^k u$, with $k \geq m = \mathrm{m}_p(D)$ and u a unit. Let

$$g = g_m + g_{m+1} + \cdots + g_d,$$

where each g_i is an i-form and $g_m \neq 0$. Since $\Bbbk$ is algebraically closed, every form of degree m splits into m linear factors, so $g_m = h_1 \dots h_m$, where each h_i is a tangent direction of D. If none of the tangent directions of D at p are tangent to C, then for each i, $h_i = tu_i$ for some unit u_i, so that $g_m = t^m u_1 \dots u_m$ and $g = t^m(u_1 \dots u_m + \dots)$, so $k = m$, and thus $\mathrm{ord}_p^C(\overline{g}) = k = m = \mathrm{m}_p(D)$. Otheriwse, for some i, $h_i = t^{k_i} u_i$ for some $k_i \geq 2$ and unit u_i. Thus, $k > m = \mathrm{m}_p(g)$. Finally, if C and D meet transversally, then they have distinct tangent lines and $\mathrm{m}_p(C) = \mathrm{m}_p(D) = 1$, so $\mathrm{I}(p, C \cap D) = 1$.

(vii) Let t be a local parameter in $\mathcal{O}_p(C)$. If $\mathrm{ord}_p^C(\overline{g}) = m$, then $\overline{g} = t^m u$ for some unit u, so that $\dim_{\Bbbk}(\mathcal{O}_p(C)/\langle \overline{g} \rangle) = \mathrm{ord}_p^C(\overline{g})$. But $\mathcal{O}_p(C)/\langle g \rangle \cong \mathcal{O}_p(\mathbb{A}^2)/\langle f, g \rangle$, so $\mathrm{ord}_p^C(\overline{g}) = \dim_{\Bbbk}(\mathcal{O}_p(\mathbb{A}^2)/\langle f, g \rangle)$. This argument is symmetric in f and g, so we have $\mathrm{ord}_p^C(\overline{g}) = \mathrm{ord}_p^D(\overline{f})$. □

3.4.6 Example. Let $C = \mathrm{V}(f)$, where $f = y + (x^2 + y^2)$, let $D = \mathrm{V}(g)$, where $g = xy + (x^2+y^2)^2$, and let $p = (0, 0)$. Note that $g = y(x - (x^2+y^2)) + (x^2+y^2)f$. Let $E = \mathrm{V}(y(x - (x^2 + y^2)))$. Then by property (v), $\mathrm{I}(p, C \cap D) = \mathrm{I}(p, C \cap E)$. Also, $E = E_1 \cup E_2$, with $E_1 = \mathrm{V}(y)$ and $E_2 = \mathrm{V}(x - (x^2 + y^2))$, so by property (iv),

$$\mathrm{I}(p, C \cap E) = \mathrm{I}(p, C \cap E_1) + \mathrm{I}(p, C \cap E_2).$$

Since E_1 is smooth at p, by property (vii) we have $\mathrm{I}(p, C \cap E_1) = \mathrm{I}(p, E_1 \cap C)$. Since $x = 0$ is not the tangent line to E_1 at p, $t = \overline{x}$ is a local parameter in $\mathcal{O}_p(E_1)$. Since $\overline{y} = 0$ in $\Gamma(E_1) = \Gamma(\mathrm{V}(y))$, we have

$$\mathrm{I}(p, E_1 \cap C) = \mathrm{ord}_p^{E_1}(\overline{f}) = \mathrm{ord}_p^{E_1}(\overline{y} + (\overline{x}^2 + \overline{y}^2)) = \mathrm{ord}_p^{E_1}(\overline{x}^2) = 2.$$

Since C and E_2 have distinct tangent lines (namely $y = 0$ and $x = 0$ respectively) at p, they intersect transversally, so by property (vi), $\mathrm{I}(p, C \cap E_2) = 1$. Therefore,

$$\mathrm{I}(p, C \cap E) = \mathrm{I}(p, C \cap E_1) + \mathrm{I}(p, C \cap E_2) = 2 + 1 = 3.$$

In the proof of the last of the above properties, we showed that if $C = \mathrm{V}(f)$ is smooth, then

$$\mathcal{O}_p(C)/\langle g\rangle \cong \mathcal{O}_p(\mathbb{A}^2)/\langle f, g\rangle,$$

and

$$\mathrm{I}(p, C \cap D) = \mathrm{ord}_p^C(g) = \dim_{\Bbbk} \mathcal{O}_p(C)/\langle g\rangle = \dim_{\Bbbk} \mathcal{O}_p(\mathbb{A}^2)/\langle f, g\rangle.$$

The expression in the right-hand side of the last equality does not involve any smoothness assumptions on either C or D, so it is reasonable to adopt it as our definition of the generalized intersection multiplicity of two affine plane curves C and D at a point $p \in \mathbb{A}^2$. However, to show that the properties of intersection multiplicity from the smooth case hold in this new setting, we require the following technical result.

3.4.7 Proposition. *If $I \subseteq \Bbbk[x, y]$ is such that $I = \langle f, g\rangle$ and $\mathrm{V}(I) = \{p_1, \ldots, p_m\}$ then*

(i) $\dim_{\Bbbk}(\Bbbk[x, y]/I) < \infty$;
(ii) *as a $\Bbbk$-vector space,*

$$\Bbbk[x, y]/I \cong \mathcal{O}_{p_1}(\mathbb{A}^2)/I\mathcal{O}_{p_1}(\mathbb{A}^2) \times \cdots \times \mathcal{O}_{p_m}(\mathbb{A}^2)/I\mathcal{O}_{p_m}(\mathbb{A}^2).$$

Proof:

(i) Let $pi_i = (a_i, b_i)$ for $i = 1, \ldots, m$. Let $h_0 = (x - a_1) \ldots (x - a_m)$ and $h_1 = (y - b_1) \ldots (y - b_m)$. Then $h_0, h_1 \in \mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$ so that $h_0^N, h_1^N \in I$ for some N. Thus, $\overline{h_0}^N = \overline{h_1}^N = 0$ in $\Bbbk[x, y]/I$, so $\overline{x}^{mN}$ is a linear combination of $\overline{x}^{mN-1}, \ldots, \overline{x}, 1$. But then, $\overline{x}^r$ is a linear combination of $\overline{x}^{mN-1}, \ldots, \overline{x}, 1$, for all $r \in \mathbb{N}$. By an identical argument, $\overline{y}^t$ is a linear combination of $1, \overline{y}, \ldots, \overline{y}^{mN-1}$ for every $t \in \mathbb{N}$. Therefore,

$$\Bbbk[x, y]/I = \mathrm{span}_{\Bbbk}\{\overline{x}^{\ell_1}\overline{y}^{\ell_2} \mid \ell_1, \ell_2 \leq mN - 1\}.$$

(ii) For this proof we write $\mathcal{O}_{p_i}$ for $\mathcal{O}_{p_i}(\mathbb{A}^2)$ and $\overline{h}$ for the image of a polynomial h in the ring $\Bbbk[x, y]/I$. Since $\Bbbk[x, y] \subseteq \mathcal{O}_{p_i}$ for each i and $I \subseteq I\mathcal{O}_{p_i}$, there is a well-defined homomorphism

$$\varphi_i : \Bbbk[x, y]/I \to \mathcal{O}_{p_i}/I\mathcal{O}_{p_i} : \overline{h} \mapsto h + I\mathcal{O}_{p_i}.$$

These maps induce a homomorphism

$$\varphi : \Bbbk[x, y]/I \to \prod_{i=1}^{m} \mathcal{O}_{p_i}/I\mathcal{O}_{p_i} : \overline{h} \mapsto (\varphi_1(h), \ldots, \varphi_m(h)),$$

which we will show is an isomorphism. We need only to prove that φ is bijective. For simplicity we assume that I is radical (so that $I = \mathrm{I}(\mathrm{V}(I))$).

Choose polynomials f_i such that

$$f_i(p_i) \neq 0 \qquad \text{and} \qquad f_i(p_j) = 0$$

for $i \neq j$. Set $e_i = 1/f_i(p_i)f_i$. Then e_ie_j vanishes at every point of $\mathrm{V}(I)$ if $i \neq j$, so $\overline{e}_i\overline{e}_j = 0$. Furthermore, $\sum_i e_i$ evaluates to 1 at every point of $\mathrm{V}(I)$, so $\sum_i \overline{e}_i = 1$. Now $e_i(p_i) \neq 0$, so $\varphi(\overline{e}_i)$ is a unit in $\mathcal{O}_{p_i}/I\mathcal{O}_{p_i}$ for each i. Therefore, since

$$\varphi_i(e_i)\varphi_i(e_j) = \varphi_i(e_ie_j) = 0,$$

we have $\varphi_i(e_j) = 0$ in $\mathcal{O}_{p_i}/I\mathcal{O}_{p_i}$ for all $j \neq i$. Therefore

$$\varphi(e_i) = (0, \ldots, 0, 1, 0, \ldots, 0),$$

where the one is in the i^{th} position. Notice that if $g \in \Bbbk[x, y]$ is such that $g(p_i) \neq 0$ then there is $h \in \Bbbk[x, y]$ such that $\overline{h}\overline{g} = \overline{e}_i$. Indeed, we set $h = 1/g(p_i)e_i$; this works since $(g(p_i) - g)e_i \in I$. Now if $\varphi(\overline{g}) = 0$ then $\varphi_i(\overline{g}) = 0$ for every i, so $g \in I\mathcal{O}_{p_i}$ for all i. In particular, this means that for each i there is $s_i \in \Bbbk[x, y]$ such that $s_i(p_i) \neq 0$ and $s_ig \in I$. Moreover, there are $h_i \in \Bbbk[x, y]$ such that $\overline{h}_i\overline{s}_i = \overline{e}_i$. Thus

$$\overline{g} = \left(\sum_i \overline{e}_i\right)\overline{g} = \sum_i \overline{h}_i\overline{s}_i\overline{g} = 0.$$

Therefore φ is injective. An element of $\prod_{i=1}^m \mathcal{O}_{p_i}/I\mathcal{O}_{p_i}$ has the form

$$\left(\frac{a_1}{s_1} + I\mathcal{O}_{p_i}, \ldots, \frac{a_m}{s_m} + I\mathcal{O}_{p_i}\right),$$

for some $a_i, s_i \in \Bbbk[x, y]$, where $s_i(p_i) \neq 0$. Take h_i as above, and note that

$$\varphi\left(\sum_i a_ih_ie_i\right) = \left(\frac{a_1}{s_1} + I\mathcal{O}_{p_i}, \ldots, \frac{a_m}{s_m} + I\mathcal{O}_{p_i}\right)$$

Therefore φ is surjective. □

Given the above analysis of the smooth case, we see that the intersection multiplicity $\mathrm{I}(p, C \cap D)$ of any two affine plane curves C and D at a point $p \in \mathbb{A}^2$ should satisfy the following properties:

3.4.8 Properties of Intersection Multiplicity.

(i) $\mathrm{I}(p, C \cap D)$ *is a non-negative integer if* C *and* D *intersect properly, and it is* ∞ *if* C *and* D *have a common component passing through* p.

(ii) $p \notin C \cap D$ *if and only if* $\mathrm{I}(p, C \cap D) = 0$.

(iii) $\mathrm{I}(p, C \cap D)$ *is invariant under affine corrdinate change.*

(iv) *It is symmetric, i.e.* $\mathrm{I}(p, C \cap D) = \mathrm{I}(p, D \cap C)$

(v) $\mathrm{I}(p, C \cap D) = 1$ *if and only if* C *and* D *intersect transversely at* p*, otherwise* $\mathrm{I}(p, C \cap D) \geq m_p(C)m_p(D)$ *with equality holding if they do not have common tangent directions at* p.

(vi) *It is additive, i.e.* $\mathrm{I}(p, (C_1 \cup C_2) \cap D) = \mathrm{I}(p, C_1 \cap D) + \mathrm{I}(p, C_2 \cap D)$.

(vii) $\mathrm{I}(p, C \cap D) = \mathrm{I}(p, C \cap E)$ *for any curve* E *such that* $E = \mathrm{V}(g + f \cdot h)$ *for some* $h \in \Bbbk[x, y]$.

3.4.9 Theorem. *Let* C *and* D *be affine plane curves. There exists a unique intersection number* $\mathrm{I}(p, C \cap D)$*, defined for all plane curves and all points* $a \in \mathbb{A}^2$*, satisfying the above properties. It is given by*

$$\mathrm{I}(p, C \cap D) = \dim_{\Bbbk}(\mathcal{O}_p(\mathbb{A}^2)/\langle f, g\rangle),$$

where $C = \mathrm{V}(f)$ *and* $D = \mathrm{V}(g)$.

Proof: Uniqueness follows from the construction. One therefore only has to show that $\dim_{\Bbbk}(\mathcal{O}_p(\mathbb{A}^2)/\langle f, g\rangle)$ satisfies the above properties. Properties (ii), (iii), (iv), and (vii) are clear, and properties (v) and (vi) are difficult to prove in general. We therefore only check property (i). Given property (ii), we may assume that every component of C and D passes through p.

If C and D have a common component given by $\mathrm{V}(h)$, where $h \in \Bbbk[x, y]$ is irreducible, then $\langle f, g\rangle \subseteq \langle h\rangle$, so that we have a surjective $\Bbbk$-linear map from $\mathcal{O}_p(\mathbb{A}^2)/\langle f, g\rangle\mathcal{O}_p(\mathbb{A}^2)$ to $\mathcal{O}_p(\mathbb{A}^2)/\langle h\rangle\mathcal{O}_p(\mathbb{A}^2)$, which is isomorphic as a $\Bbbk$-algebra to $\mathcal{O}_p(\mathrm{V}(h))$. Since $\mathcal{O}_p(\mathrm{V}(h))$ is an infinite $\Bbbk$-vector space, this implies that $\mathrm{I}(p, C \cap D) = \infty$. Let us now assume that C and D intersect properly at p. Given Proposition 3.4.7, we have

$$\begin{aligned}
\mathrm{I}(p, C \cap D) &\leq \sum_{p \in C \cap D} \mathrm{I}(p, C \cap D) \\
&= \sum_{p \in C \cap D} \dim_{\Bbbk}(\mathcal{O}_p(\mathbb{A}^2)/I\mathcal{O}_p(\mathbb{A}^2)) \\
&= \dim_{\Bbbk}(\Bbbk[x, y]/I) \\
&< \infty.
\end{aligned}$$

□

3.4.10 Examples.

(i) Let $C = \mathrm{V}(y^2 - x^3)$ and $D = \mathrm{V}(y - x^2)$. In this case D is smooth and $C \cap D = \{(0, 0), (1, 1)\}$. C is not smooth at the origin. C and D do not intersect transversely at the origin and have common tangent direction $\mathrm{V}(y)$. They do intersect transversely at $(1, 1)$, so $\mathrm{I}((1, 1), C \cap D) = 1$. Since D is smooth at the origin, let us express f modulo g.

$$f = y^2 - x^3 \equiv \overline{x}^3(\overline{x} - 1)$$

in $\mathcal{O}_{(0,0)}(D)$, so we will take $\mathrm{V}(x)$ to be the generator of $\mathrm{M}_{(0,0)}(D)$. Then $\overline{f} = \overline{x}^3 u$, so $I((0, 0), C \cap D) = \mathrm{ord}^D_{(0,0)}(\overline{f}) = 3$. Note that the sum of the intersection multiplicities is less than the product of the degrees. This is because C and D are in $\mathbb{A}^2$ and would intersect at ∞ in $\mathbb{P}^2$. Let

$I = \langle f, g\rangle \subseteq \Bbbk[x, y]$ and notice that $\mathrm{I}(p, C\cap D) = \dim_{\Bbbk}(\mathcal{O}_p(\mathbb{A}^2)/I\mathcal{O}_p(\mathbb{A}^2))$. Globally,

$$\Bbbk[x, y]/I = \Bbbk[x, y]/\langle y - x^2, y^2 - x^3\rangle = \{a_0 + a_1\overline{x} + a_2\overline{x}^2 + a_3\overline{x}^3 \mid a_i \in \Bbbk\}$$

a $\Bbbk$-vector space of dimension $4 = 3+1$.

(ii) Let $C = \mathrm{V}((x^2 + y^2)^2 + 3x^2y - y^3)$ and $D = \mathrm{V}((x^2 + y^2)^3 - 4x^2y^2)$. The tangent directions at the origin are $\mathrm{V}(y)$ and $\mathrm{V}(y \pm \sqrt{3}x)$ for C and $\mathrm{V}(x)$ and $\mathrm{V}(y)$ for D. Therefore we have to rewrite the equations in such a way as to obtain distinct tangent directions. Notice that

$$g = (x^2 + y^2 - 3y)f + y^2q,$$

where $q = 5x^2 - 3y^2 + 4y^3 + 4x^2y$, which does not have $\mathrm{V}(y)$ as a tangent direction. Thus $\overline{g} = \overline{y}^2\overline{q}$ in $\mathcal{O}_p(C)$, so that $\mathrm{V}(g)$ has at least 3 components $\mathrm{V}(y)$, $\mathrm{V}(y)$, and $\mathrm{V}(q)$. It can be shown that

$$\mathrm{I}((0, 0), C \cap D) = 2\,\mathrm{I}((0, 0), C \cap \mathrm{V}(y)) + \mathrm{I}((0, 0), C \cap \mathrm{V}(q)) = 14.$$

3.5 Blow-ups

The set $\widetilde{\mathbb{A}^2} = \mathrm{V}(y - xu) \subseteq \mathbb{A}^3$ is called the *(local) blow-up* of $\mathbb{A}^2$ at the origin. Consider the projection $\pi : \widetilde{\mathbb{A}^2} = \mathrm{V}(y - xu) \to \mathbb{A}^2$ given by $\pi(x, y, u) = (x, y)$. Then we call

$$\pi^{-1}(0, 0) = \{(0, 0, u) \mid u \in \Bbbk\} = \mathrm{V}(x, y) \subseteq \mathbb{A}^3$$

the *exceptional curve*. If $x \neq 0$ and u is the slope of the line joining (x_0, y_0) and $(0, 0)$, then

$$\pi^{-1}(0, 0) = \left\{(x_0, y_0, \frac{y_0}{x_0} \mid x_0 \neq 0, \frac{y_0}{x_0} = u\right\},$$

and $\pi^{-1}(0, y_0) = \varnothing$ if $y_0 \neq 0$. Therefore

$$\mathrm{Im}(\pi) = (\mathbb{A}^2 \setminus \mathrm{V}(y)) \cup \{(0, 0)\},$$

and $\mathbb{A}^2 \setminus \mathrm{V}(y)$ is a non-empty open set of $\mathbb{A}^2$, so it is dense. Therefore, π is a dominant polynomial map, which is one-to-one awya from the exceptional curve. The map π also has a rational inverse $\pi^{-1} : \mathbb{A}^2 \to \widetilde{\mathbb{A}^2}$, given by $\pi^{-1}(x, y) = (x, y, yx)$. Then, since $\mathrm{dom}(()\pi^{-1}) = \mathbb{A}^2 \setminus \mathrm{V}(x)$, and

$$\mathrm{Im}(\pi) = (\widetilde{\mathbb{A}^2} \setminus \mathrm{V}(x, y)) \cup \{(0, 0, u) \mid u \in \Bbbk\},$$

and $\widetilde{\mathbb{A}^2} \setminus \mathrm{V}(x, y)$ is a non-empty open set of $\widetilde{\mathbb{A}^2}$, so it is dense. Therefore, π^{-1} is a dominant rational map, showing that π is a birational equiovalence and that $\widetilde{\mathbb{A}^2} \sim \mathbb{A}^2$.

What happens to curves under the map π^{-1}?

3.5.1 Example. Let $X = \mathrm{V}(y^2 - x^3) \subset \mathbb{A}^2$, which is singular at $(0,0)$. Consider

$$\pi^{-1}(X) \subseteq \widetilde{\mathbb{A}^2} = \mathrm{V}(y - xu) \subseteq \mathbb{A}^3.$$

Then

$$\pi^{-1}(X) = \mathrm{V}(y^2 - x^3, y - xu) = \mathrm{V}(x,y) \cup \mathrm{V}(x - u^2, y - u^3).$$

Ignoring the exceptional curve, let $\widetilde{X} = \mathrm{V}(x - u^2, y - u^3) = \overline{\pi^{-1}(X \setminus \{(0,0)\}}$. We call $\widetilde{X}$ the proper transform, or blow-up, of X. Note that $\widetilde{X}$ is the twisted cubic, which we know to be non-singular.

3.5.2 Definition. Let $X \subset \mathbb{A}^2$ be an affine plane curve. We call

$$\widetilde{X} = \overline{\pi^{-1}(X \setminus \{(0,0)\}}$$

the *(local) blow-up* of X at $p = (0,0)$.

Remark. The (local) blow-up $\widetilde{\mathbb{A}^2} = \mathrm{V}(y - xu) \subset \mathbb{A}^3$ of $\mathbb{A}^2$ is in fact the closure in $\mathbb{A}^3$ of the graph of the projection map $\varphi : \mathbb{A}^2 \to \mathrm{V}(x-1) \cong \Bbbk$ given by $\varphi(x,y) = y/x$ from 0 onto $\mathrm{V}(x-1)$ in $\mathbb{A}^2$.

One can also construct a blow-up of $\mathbb{A}^2$ at 0 by using the projection from 0 onto $\mathrm{V}(y-1)$ in $\mathbb{A}^2$, which will then give us $\widetilde{\mathbb{A}^2} = \mathrm{V}(x - uy) \subset \mathbb{A}^3$. Note that $\mathrm{V}(y - xu) \cong \mathrm{V}(x - uy)$ since they are related by the affine coordinate change $(x,y) \mapsto (y,x)$.

In general, one constructs the (local) blow-up $\widetilde{\mathbb{A}^n}$ of $\mathbb{A}^n$ at 0 by considering the projection of $\mathbb{A}^n$ onto any plane $\mathrm{V}(x_i - 1)$ in $\mathbb{A}^n$. We then get that

$$\widetilde{\mathbb{A}^n} = \mathrm{V}(x_1 - u_1 x_i, \ldots, x_{i-1} - u_{i-1}x_i, x_{i+1} - u_{i+1}x_i, \ldots, x_n - u_n x_i) \subset \mathbb{A}^n \times \mathbb{A}^{n-1},$$

where $(u_1, u_2, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n)$ are coordinates in $\mathbb{A}^{n-1}$. Again, the projection $\pi : \widetilde{\mathbb{A}^n} \to \mathbb{A}^n, (x_1, \ldots, x_n, u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n) \mapsto (x_1, \ldots, x_n)$ is a birational equivalence, so that $\widetilde{\mathbb{A}^n} \sim \mathbb{A}^n$. Moreover, if $X \subset \mathbb{A}^n$, we let

$$\widetilde{X} = \overline{\pi^{-1}(X) \setminus \{(0,0)\}}$$

be the *(local) blow-up* of X at 0.

Appendix A

Some Ring Theory

A.0.3 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.0.4 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.0.5 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.0.6 Definition. We say that a ring R is *Noetherian* if every ideal of R is finitely generated.

A.0.7 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.0.8 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.0.9 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.0.10 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.0.11 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.0.12 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.0.13 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.0.12, I is radical. □

Appendix B

Transcendence Bases

B.0.14 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.0.15 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.0.16 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.0.17 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.0.18 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.0.19 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.0.20 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.0.19, 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.0.19. □

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

C.0.21 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.0.22 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.0.23 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.0.24 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.0.19. 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.0.25 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.0.21, $\Bbbk[y_1, \ldots, y_n]$ 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.0.26 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.0.25, 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.0.27 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 $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$. $\square$