Chapter 5

Varieties

The purpose of this chapter is to state some basic definitions and results from algebraic geometry that are required for the main part of the book. In particular, we define algebraic sets, irreducibility, function fields, rational maps and dimension. The chapter is not intended as a self-contained introduction to algebraic geometry. We make the following recommendations to the reader:

1. Readers who want a very elementary introduction to elliptic curves are advised to consult one or more of Koblitz [348], Silverman-Tate [567], Washington [626], Smart [572] or Stinson [592].

2. Readers who wish to learn algebraic geometry properly should first read a basic text such as Reid [497] or Fulton [216]. They can then skim this chapter and consult Stichtenoth [589], Moreno [439], Hartshorne [278], Lorenzini [394] or Shafarevich [543] for detailed proofs and discussion.

5.1 Affine algebraic sets

Let $\mathbb{k}$ be a perfect field contained in a fixed algebraic closure $\overline{\mathbb{k}}$. All algebraic extensions $\mathbb{k}'/\mathbb{k}$ are implicitly assumed to be subfields of $\overline{\mathbb{k}}$. We use the notation $\mathbb{k}[\underline{x}] = \mathbb{k}[x_1, \ldots, x_n]$ (in later sections we also use $\mathbb{k}[\underline{x}] = \mathbb{k}[x_0, \ldots, x_n]$). When $n = 2$ or 3 we often write $\mathbb{k}[x, y]$ or $\mathbb{k}[x, y, z]$.

Define **affine n-space over** $\mathbb{k}$ as $\mathbb{A}^n(\mathbb{k}) = \mathbb{k}^n$. We call $\mathbb{A}^1(\mathbb{k})$ the **affine line** and $\mathbb{A}^2(\mathbb{k})$ the **affine plane** over $\mathbb{k}$. If $\mathbb{k} \subseteq \mathbb{k}'$ then we have the natural inclusion $\mathbb{A}^n(\mathbb{k}) \subseteq \mathbb{A}^n(\mathbb{k}')$. We write $\mathbb{A}^n$ for $\mathbb{A}^n(\overline{\mathbb{k}})$ and so $\mathbb{A}^n(\mathbb{k}) \subseteq \mathbb{A}^n$.

Definition 5.1.1. Let $S \subseteq \mathbb{k}[\underline{x}]$. Define

$$V(S) = \{P \in \mathbb{A}^n(\overline{\mathbb{k}}) : f(P) = 0 \text{ for all } f \in S\}.$$

If $S = \{f_1, \ldots, f_m\}$ then we write $V(f_1, \ldots, f_m)$ for $V(S)$. An **affine algebraic set** is a set $X = V(S) \subset \mathbb{A}^n$ where $S \subset \Bbbk[\underline{x}]$.

Let $\Bbbk'/\Bbbk$ be an algebraic extension. The $\Bbbk'$**-rational points** of $X = V(S)$ are

$$X(\Bbbk') = X \cap \mathbb{A}^n(\Bbbk') = \{P \in \mathbb{A}^n(\Bbbk') : f(P) = 0 \text{ for all } f \in S\}.$$

An algebraic set $V(f)$, where $f \in \Bbbk[\underline{x}]$, is a **hypersurface**. If $f(\underline{x})$ is a polynomial of total degree 1 then $V(f)$ is a **hyperplane**.

Informally we often write "the algebraic set $f = 0$" instead of $V(f)$. For example, $y^2 = x^3$ instead of $V(y^2 - x^3)$. We stress that, as is standard, $V(S)$ is the set of solutions over an algebraically closed field.

When an algebraic set is defined as the vanishing of a set of polynomials with coefficients in $\Bbbk$ then it is called a $\Bbbk$-algebraic set. The phrase "defined over $\Bbbk$" has a different meaning and the relation between them will be explained in Remark 5.3.7.

Example 5.1.2. If $X = V(x_1^2 + x_2^2 + 1) \subseteq \mathbb{A}^2$ over $\mathbb{Q}$ then $X(\mathbb{Q}) = \varnothing$. Let $\Bbbk = \mathbb{F}_2$ and let $X = V(y^8 + x^6y + x^3 + 1) \subseteq \mathbb{A}^2$. Then $X(\mathbb{F}_2) = \{(0,1), (1,0), (1,1)\}$.

Exercise 5.1.3. Let $\Bbbk$ be a field. Show that $\{(t, t^2) : t \in \overline{\Bbbk}\} \subseteq \mathbb{A}^2$, $\{(t, \pm\sqrt{t}) : t \in \overline{\Bbbk}\} \subseteq \mathbb{A}^2$ and $\{(t^2 + 1, t^3) : t \in \overline{\Bbbk}\} \subseteq \mathbb{A}^2$ are affine algebraic sets.

Exercise 5.1.4. Let $f(x, y) \in \Bbbk[x, y]$ be a non-constant polynomial. Prove that $V(f(x, y)) \subset \mathbb{A}^2$ is an infinite set.

Example 5.1.5. Let $\Bbbk$ be a field. There is a one-to-one correspondence between the set $\Bbbk^*$ and the $\Bbbk$-rational points $X(\Bbbk)$ of the affine algebraic set $X = V(xy - 1) \subset \mathbb{A}^2$. Multiplication in the field $\Bbbk$ corresponds to the function mult : $X \times X \to X$ given by $\text{mult}((x_1, y_1), (x_2, y_2)) = (x_1x_2, y_1y_2)$. Similarly, inversion in $\Bbbk^*$ corresponds to the function $\text{inverse}(x, y) = (y, x)$. Hence we have represented $\Bbbk^*$ as an algebraic group, which we call $G_m(\Bbbk)$.

Example 5.1.6. Another elementary example of an algebraic group is the affine algebraic set $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2$ with the group operation $\text{mult}((x_1, y_1), (x_2, y_2)) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$. (These formulae are analogous to the angle addition rules for sine and cosine as, over $\mathbb{R}$, one can identify (x, y) with $(\cos(\theta), \sin(\theta))$.) The reader should verify that the image of mult is contained in X. The identity element is $(1, 0)$ and the inverse of (x, y) is $(x, -y)$. One can verify that the axioms of a group are satisfied. This group is sometimes called the **circle group**.

Exercise 5.1.7. Let $p \equiv 3 \pmod 4$ be prime and define $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ where $i^2 = -1$. Show that the group $X(\mathbb{F}_p)$, where X is the circle group from Example 5.1.6, is isomorphic as a group to the subgroup $G \subseteq \mathbb{F}_{p^2}^*$ of order $p + 1$.

Proposition 5.1.8. *Let $S \subseteq \Bbbk[x_1, \ldots, x_n]$.*

1. *$V(S) = V((S))$ where (S) is the $\Bbbk[\underline{x}]$-ideal generated by S.*
2. *$V(\Bbbk[\underline{x}]) = \varnothing$ and $V(\{0\}) = \mathbb{A}^n$ where $\varnothing$ denotes the empty set.*
3. *If $S_1 \subseteq S_2$ then $V(S_2) \subseteq V(S_1)$.*
4. *$V(fg) = V(f) \cup V(g)$.*
5. *$V(f) \cap V(g) = V(f, g)$.*

Exercise 5.1.9. Prove Proposition 5.1.8.

Exercise 5.1.10. Show that $V(S)(\Bbbk) = \mathbb{A}^n(\Bbbk)$ does not necessarily imply that $S = \{0\}$.

The following result assumes a knowledge of Galois theory. See Section A.7 for background.

Lemma 5.1.11. *Let $X = V(S)$ be an algebraic set with $S \subseteq \Bbbk[\underline{x}]$ (i.e., X is a $\Bbbk$-algebraic set). Let $\Bbbk'$ be an algebraic extension of $\Bbbk$. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk')$. For $P = (P_1, \ldots, P_n)$ define $\sigma(P) = (\sigma(P_1), \ldots, \sigma(P_n))$.*

1. *If $P \in X(\overline{\Bbbk})$ then $\sigma(P) \in X(\overline{\Bbbk})$.*
2. *$X(\Bbbk') = \{P \in X(\overline{\Bbbk}) : \sigma(P) = P$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk')\}$.*

Exercise 5.1.12. Prove Lemma 5.1.11.

Definition 5.1.13. The **ideal** over $\Bbbk$ of a set $X \subseteq \mathbb{A}^n(\overline{\Bbbk})$ is

$$I_\Bbbk(X) = \{f \in \Bbbk[\underline{x}] : f(P) = 0 \text{ for all } P \in X(\overline{\Bbbk})\}.$$

We define $I(X) = I_{\overline{\Bbbk}}(X)$.[1]

An algebraic set X is **defined over** $\Bbbk$ (sometimes abbreviated to "X over $\Bbbk$") if $I(X)$ can be generated by elements of $\Bbbk[\underline{x}]$.

Note that if X is an algebraic set defined over $\Bbbk$ then X is a $\Bbbk$-algebraic set. Perhaps surprisingly, it is not necessarily true that an algebraic set described by polynomials defined over $\Bbbk$ is an algebraic set defined over $\Bbbk$. In Remark 5.3.7 we will explain that these concepts are equivalent for the objects of interest in this book.

Exercise 5.1.14. Show that $I_\Bbbk(X) = I(X) \cap \Bbbk[\underline{x}]$.

The following example shows that $I_\Bbbk(X)$ is not necessarily the same as $I_\Bbbk(X(\Bbbk))$.

Example 5.1.15. Let $X = V(x^2 + y^2) \subset \mathbb{A}^2$ be an algebraic set over $\mathbb{R}$. Then $X(\mathbb{R}) = \{(0,0)\}$ while $X(\mathbb{C}) = \{(x, \pm ix) : x \in \mathbb{C}\}$. One has $I_\mathbb{R}(X) = (x^2 + y^2)$ where this denotes an $\mathbb{R}[x,y]$-ideal. Similarly, $I_\mathbb{C}(X)$ is the $\mathbb{C}[x,y]$-ideal $(x^2 + y^2)$. Indeed, $I_\mathbb{C}(X) = I_\mathbb{R}(X) \otimes_\mathbb{R} \mathbb{C}$. On the other hand, $I_\mathbb{R}(X(\mathbb{R}))$ is the $\mathbb{R}[x,y]$-ideal (x,y).

Proposition 5.1.16. *Let $X, Y \subseteq \mathbb{A}^n$ be sets and J a $\Bbbk[\underline{x}]$-ideal. Then*

1. *$I_\Bbbk(X)$ is a $\Bbbk[\underline{x}]$-ideal.*
2. *$X \subseteq V(I_\Bbbk(X))$.*
3. *If $X \subseteq Y$ then $I_\Bbbk(Y) \subseteq I_\Bbbk(X)$.*
4. *$I_\Bbbk(X \cup Y) = I_\Bbbk(X) \cap I_\Bbbk(Y)$.*
5. *If X is an algebraic set defined over $\Bbbk$ then $V(I_\Bbbk(X)) = X$.*
6. *If X and Y are algebraic sets defined over $\Bbbk$ and $I_\Bbbk(X) = I_\Bbbk(Y)$ then $X = Y$.*
7. *$J \subseteq I_\Bbbk(V(J))$.*
8. *$I_\Bbbk(\varnothing) = \Bbbk[\underline{x}]$.*

Exercise 5.1.17. Prove Proposition 5.1.16.

Definition 5.1.18. The **affine coordinate ring** over $\Bbbk$ of an affine algebraic set $X \subseteq \mathbb{A}^n$ defined over $\Bbbk$ is

$$\Bbbk[X] = \Bbbk[x_1, \ldots, x_n]/I_\Bbbk(X).$$

[1] The notation $I_\Bbbk(X)$ is not standard (Silverman [564] calls it $I(X/\Bbbk)$), but the notation $I(X)$ agrees with many elementary books on algebraic geometry, since they work over an algebraically closed field.

Warning: Here $\Bbbk[X]$ does not denote polynomials in the variable X. Hartshorne and Fulton write $A(X)$ and $\Gamma(X)$ respectively for the affine coordinate ring.

Exercise 5.1.19. Prove that $\Bbbk[X]$ is a commutative ring with an identity.

Note that $\Bbbk[X]$ is isomorphic to the ring of all functions $f : X \to \Bbbk$ given by polynomials defined over $\Bbbk$.

Hilbert's Nullstellensatz is a powerful tool for understanding $I_{\overline{\Bbbk}}(X)$ and it has several other applications (for example, we use it in Section 7.5). We follow the presentation of Fulton [216]. Note that it is necessary to work over $\overline{\Bbbk}$.

Theorem 5.1.20. *(Weak Nullstellensatz) Let $X \subseteq \mathbb{A}^n$ be an affine algebraic set defined over $\overline{\Bbbk}$ and let $\mathfrak{m}$ be a maximal ideal of the affine coordinate ring $\overline{\Bbbk}[X]$. Then $V(\mathfrak{m}) = \{P\}$ for some $P = (P_1, \ldots, P_n) \in X(\overline{\Bbbk})$ and $\mathfrak{m} = (x_1 - P_1, \ldots, x_n - P_n)$.*

Proof: Consider the field $F = \overline{\Bbbk}[X]/\mathfrak{m}$, which contains $\overline{\Bbbk}$. Note that F is finitely generated as a ring over $\overline{\Bbbk}$ by the images of $x_1, \ldots, x_n$. By Theorem A.6.2, F is an algebraic extension of $\overline{\Bbbk}$ and so $F = \overline{\Bbbk}$.

It follows that, for $1 \leq i \leq n$, there is some $P_i \in \overline{\Bbbk}$ such that $x_i - P_i \in \mathfrak{m}$. Hence, $\mathfrak{n} = (x_1 - P_1, \ldots, x_n - P_n) \subseteq \mathfrak{m}$ and, since $\overline{\Bbbk}[X]/\mathfrak{n} = \overline{\Bbbk}$ it follows that $\mathfrak{m} = \mathfrak{n}$.

Finally, it is clear that $P \in V(\mathfrak{m})$ and if $Q = (Q_1, \ldots, Q_n) \in X(\overline{\Bbbk}) - \{P\}$ then there is some $1 \leq i \leq n$ such that $Q_i \neq P_i$ and so $(x - P_i)(Q_i) \neq 0$. Hence $V(\mathfrak{m}) = \{P\}$. □

Corollary 5.1.21. *If I is a proper ideal in $\overline{\Bbbk}[x_1, \ldots, x_n]$ then $V(I) \neq \varnothing$.*

Proof: There is some maximal ideal $\mathfrak{m}$ such that $I \subseteq \mathfrak{m}$. By Theorem 5.1.20, $\mathfrak{m} = (x_1 - P_1, \ldots, x_n - P_n)$ for some $P = (P_1, \ldots, P_n) \in \mathbb{A}^n(\overline{\Bbbk})$ and so $P \in V(I)$. □

Indeed, Corollary 5.1.21 is true when one starts with I a proper ideal in $\Bbbk[x_1, \ldots, x_n]$; see Lemma VIII.7.3 of [301].

We can now state the **Hilbert Nullstellensatz**. This form of the theorem (which applies to $I_{\Bbbk}(V(I))$ where $\Bbbk$ is not necessarily algebraically closed), appears as Proposition VIII.7.4 of [301].

Theorem 5.1.22. *Let I be an ideal in $R = \Bbbk[x_1, \ldots, x_n]$. Then $I_{\Bbbk}(V(I)) = \mathrm{rad}_R(I)$ (see Section A.9 for the definition of the radical ideal).*

Proof: One has $\mathrm{rad}_R(I) \subseteq I_{\Bbbk}(V(I))$ since $f^n \in I$ implies $f^n(P) = 0$ for all $P \in V(I)$ and so $f(P) = 0$ for all $P \in V(I)$. For the converse suppose $I = (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n))$ and $G(x_1, \ldots, x_n) \in I_{\Bbbk}(V(I))$. Define the $\Bbbk[x_1, \ldots, x_{n+1}]$-ideal

$$J = (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n), x_{n+1}G(x_1, \ldots, x_n) - 1).$$

Then $V(J) = \varnothing$ since if $P = (P_1, \ldots, P_{n+1}) \in \mathbb{A}^{n+1}(\overline{\Bbbk})$ is such that $F_i(P_1, \ldots, P_n) = 0$ for all $1 \leq i \leq m$ then $G(P_1, \ldots, P_n) = 0$ too and so one does not have $P_{n+1}G(P) = 1$. It follows from (the stronger form of) Corollary 5.1.21 that $J = (1)$ and so $1 \in J$. In other words, there are polynomials $a_i(x_1, \ldots, x_{n+1}) \in \Bbbk[x_1, \ldots, x_{n+1}]$ for $1 \leq i \leq m+1$ such that

$$1 = a_{m+1}(x_{n+1}G - 1) + \sum_{i=1}^{m} a_i F_i.$$

Write $y = 1/x_{n+1}$ and let $N = 1 + \max_{1 \leq i \leq m+1}\{\deg_{x_{n+1}}(a_i)\}$. One has

$$y^N = b_{m+1}(x_1, \ldots, x_n, y)(G - y) + \sum_{i=1}^{m} b_i(x_1, \ldots, x_n, y)F_i(x_1, \ldots, x_n)$$

for some polynomials $b_i \in \Bbbk[x_1, \ldots, x_n, y]$. Setting $y = G$ proves that $G^N \in I$ and so $G \in \mathrm{rad}_R(I)$. □

Corollary 5.1.23. *Let $f(x,y) \in \Bbbk[x,y]$ be irreducible over $\overline{\Bbbk}$ and let $X = V(f(x,y)) \subset \mathbb{A}^2(\overline{\Bbbk})$. Then $I(X) = (f(x,y))$, i.e., the ideal over $\overline{\Bbbk}[x,y]$ generated by $f(x,y)$.*

Proof: By Theorem 5.1.22 we have $I(X) = \mathrm{rad}_{\overline{\Bbbk}}((f(x,y)))$. Since $\overline{\Bbbk}[x,y]$ is a unique factorisation domain and $f(x,y)$ is irreducible, then $f(x,y)$ is prime. So $g(x,y) \in \mathrm{rad}_{\overline{\Bbbk}}((f(x,y)))$ implies $g(x,y)^n = f(x,y)h(x,y)$ for some $h(x,y) \in \overline{\Bbbk}[x,y]$ which implies $f(x,y) \mid g(x,y)$ and $g(x,y) \in (f(x,y))$. □

Theorem 5.1.24. *Every affine algebraic set X is the intersection of a finite number of hypersurfaces.*

Proof: By Hilbert's basis theorem (Corollary A.9.4) $\Bbbk[\underline{x}]$ is Noetherian. Hence $I_{\Bbbk}(X) = (f_1, \ldots, f_m)$ and $X = V(f_1) \cap \cdots \cap V(f_m)$. □

5.2 Projective Algebraic Sets

Studying affine algebraic sets is not sufficient for our applications. In particular, the set of affine points of the Weierstrass equation of an elliptic curve (see Section 7.2) does not form a group. Projective geometry is a way to "complete" the picture by adding certain "points at infinity".

For example, consider the hyperbola $xy = 1$ in $\mathbb{A}^2(\mathbb{R})$. Projective geometry allows an interpretation of the behaviour of the curve at $x = 0$ or $y = 0$; see Example 5.2.7.

Definition 5.2.1. Projective space over $\Bbbk$ of dimension n is

$$\mathbb{P}^n(\Bbbk) = \{\text{lines through } (0, \ldots, 0) \text{ in } \mathbb{A}^{n+1}(\Bbbk)\}.$$

A convenient way to represent points of $\mathbb{P}^n(\Bbbk)$ is using **homogeneous coordinates**: Let $a_0, a_1, \ldots, a_n \in \Bbbk$ with not all $a_j = 0$ and define $(a_0 : a_1 : \cdots : a_n)$ to be the equivalence class of $(n+1)$-tuples under the equivalence relation

$$(a_0, a_1, \cdots, a_n) \equiv (\lambda a_0, \lambda a_1, \cdots, \lambda a_n)$$

for any $\lambda \in \Bbbk^*$. Thus $\mathbb{P}^n(\Bbbk) = \{(a_0 : \cdots : a_n) : a_i \in \Bbbk \text{ for } 0 \leq i \leq n \text{ and } a_i \neq 0 \text{ for some } 0 \leq i \leq n\}$. Write $\mathbb{P}^n = \mathbb{P}^n(\overline{\Bbbk})$.

In other words, the equivalence class $(a_0 : \cdots : a_n)$ is the set of points on the line between $(0, \ldots, 0)$ and $(a_0, \ldots, a_n)$ with the point $(0, \ldots, 0)$ removed.

There is a map $\varphi : \mathbb{A}^n \to \mathbb{P}^n$ given by $\varphi(x_1, \ldots, x_n) = (x_1 : \cdots : x_n : 1)$. Hence $\mathbb{A}^n$ is identified with a subset of $\mathbb{P}^n$.

Example 5.2.2. The **projective line** $\mathbb{P}^1(\Bbbk)$ is in one-to-one correspondence with $\mathbb{A}^1(\Bbbk) \cup \{\infty\}$ since $\mathbb{P}^1(\Bbbk) = \{(a_0 : 1) : a_0 \in \Bbbk\} \cup \{(1 : 0)\}$. The **projective plane** $\mathbb{P}^2(\Bbbk)$ is in one-to-one correspondence with $\mathbb{A}^2(\Bbbk) \cup \mathbb{P}^1(\Bbbk)$.

Definition 5.2.3. A point $P = (P_0 : P_1 : \cdots : P_n) \in \mathbb{P}^n(\overline{\Bbbk})$ is **defined over** $\Bbbk$ if there is some $\lambda \in \overline{\Bbbk}^*$ such that $\lambda P_j \in \Bbbk$ for all $0 \leq j \leq n$. If $P \in \mathbb{P}^n$ and $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ then $\sigma(P) = (\sigma(P_0) : \cdots : \sigma(P_n))$.

Exercise 5.2.4. Show that P is defined over $\Bbbk$ if and only if there is some $0 \leq i \leq n$ such that $P_i \neq 0$ and $P_j/P_i \in \Bbbk$ for all $0 \leq j \leq n$. Show that $\mathbb{P}^n(\Bbbk)$ is equal to the set of points $P \in \mathbb{P}^n(\overline{\Bbbk})$ that are defined over $\Bbbk$. Show that $\sigma(P)$ in Definition 5.2.3 is well-defined (i.e., if $P = (P_0, \ldots, P_n) \equiv P' = (P'_0, \ldots, P'_n)$ then $\sigma(P) \equiv \sigma(P')$).

Lemma 5.2.5. *A point $P \in \mathbb{P}^n(\overline{\Bbbk})$ is defined over $\Bbbk$ if and only if $\sigma(P) = P$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$.*

Proof: Let $P = (P_0 : \cdots : P_n) \in \mathbb{P}^n(\overline{\Bbbk})$ and suppose $\sigma(P) \equiv P$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Then there is some $\xi : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \overline{\Bbbk}^*$ such that $\sigma(P_i) = \xi(\sigma)P_i$ for all $0 \leq i \leq n$. One can verify[2] that ξ is a 1-cocycle in $\overline{\Bbbk}^*$. It follows by Theorem A.7.2 (Hilbert 90) that $\xi(\sigma) = \sigma(\gamma)/\gamma$ for some $\gamma \in \overline{\Bbbk}^*$. Hence, $\sigma(P_i/\gamma) = P_i/\gamma$ for all $0 \leq i \leq n$ and all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Hence $P_i/\gamma \in \Bbbk$ for all $0 \leq i \leq n$ and the proof is complete. □

Recall that if f is a homogeneous polynomial of degree d then $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ for all $\lambda \in \Bbbk$ and all $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}(\Bbbk)$.

Definition 5.2.6. Let $f \in \Bbbk[x_0, \ldots, x_n]$ be a homogeneous polynomial. A point $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\Bbbk)$ is a **zero** of f if $f(x_0, \ldots, x_n) = 0$ for some (hence, every) point $(x_0, \ldots, x_n)$ in the equivalence class $(x_0 : \cdots : x_n)$. We therefore write $f(P) = 0$. Let S be a set of polynomials and define

$$V(S) = \{P \in \mathbb{P}^n(\overline{\Bbbk}) : P \text{ is a zero of } f(\underline{x}) \text{ for all homogeneous } f(\underline{x}) \in S\}.$$

A **projective algebraic set** is a set $X = V(S) \subseteq \mathbb{P}^n(\overline{\Bbbk})$ for some $S \subseteq \Bbbk[\underline{x}]$. Such a set is also called a projective $\Bbbk$-algebraic set. For $X = V(S)$ and $\Bbbk'$ an algebraic extension of $\Bbbk$ define

$$X(\Bbbk') = \{P \in \mathbb{P}^n(\Bbbk') : f(P) = 0 \text{ for all homogeneous } f(\underline{x}) \in S\}.$$

Example 5.2.7. The hyperbola $y = 1/x$ can be described as the affine algebraic set $X = V(xy-1) \subset \mathbb{A}^2$ over $\mathbb{R}$. One can consider the corresponding projective algebraic set $V(xy - z^2) \subseteq \mathbb{P}^2$ over $\mathbb{R}$ whose points consist the points of X together with the points $(1 : 0 : 0)$ and $(0 : 1 : 0)$. These two points correspond to the asymptotes $x = 0$ and $y = 0$ of the hyperbola and they essentially "tie together" the disconnected components of the affine curve to make a single closed curve in projective space.

Exercise 5.2.8. Describe the sets $V(x^2+y^2-z^2)(\mathbb{R}) \subset \mathbb{P}^2(\mathbb{R})$ and $V(yz-x^2)(\mathbb{R}) \subseteq \mathbb{P}^2(\mathbb{R})$.

Exercise 5.2.9. What is $V(xz + y^2, xyz) \subseteq \mathbb{P}^2(\mathbb{C})$?

Exercise 5.2.10. What is $V(y^2 + x^2, x^2z - y^3) \subseteq \mathbb{P}^2(\mathbb{C})$?

A set of homogeneous polynomials does not in general form an ideal as one cannot simultaneously have closure under multiplication and addition. Hence it is necessary to introduce the following definition.

Definition 5.2.11. A $\Bbbk[x_0, \ldots, x_n]$-ideal $I \subseteq \Bbbk[x_0, \ldots, x_n]$ is a **homogeneous ideal** if for every $f \in I$ with homogeneous decomposition $f = \sum_i f_i$ we have $f_i \in I$.

Exercise 5.2.12. Let $S \subset \Bbbk[\underline{x}]$ be a set of homogeneous polynomials. Define (S) to be the $\Bbbk[\underline{x}]$-ideal generated by S in the usual way, i.e., $(S) = \{\sum_{j=1}^n f_j(\underline{x})s_j(\underline{x}) : n \in \mathbb{N}, f_j(\underline{x}) \in \Bbbk[x_0, \ldots, x_n], s_j(\underline{x}) \in S\}$. Prove that (S) is a homogeneous ideal. Prove that if I is a homogeneous ideal then $I = (S)$ for some set of homogeneous polynomials S.

Definition 5.2.13. For any set $X \subseteq \mathbb{P}^n(\overline{\Bbbk})$ define

$$I_{\Bbbk}(X) = \big(\{f \in \Bbbk[x_0, \ldots, x_n] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in X\}\big).$$

[2] At least, one can verify the formula $\xi(\sigma\tau) = \sigma(\xi(\tau))\xi(\sigma)$. The topological condition also holds, but we do not discuss this.

We stress that $I_{\Bbbk}(X)$ is not the stated set of homogeneous polynomials but the ideal generated by them. We write $I(X) = I_{\overline{\Bbbk}}(X)$.

An algebraic set $X \subseteq \mathbb{P}^n$ is **defined over** $\Bbbk$ if $I(X)$ can be generated by homogeneous polynomials in $\Bbbk[\underline{x}]$.

Proposition 5.2.14. *Let $\Bbbk$ be a field.*

1. *If $S_1 \subseteq S_2 \subseteq \Bbbk[x_0, \ldots, x_n]$ then $V(S_2) \subseteq V(S_1) \subseteq \mathbb{P}^n(\overline{\Bbbk})$.*
2. *If fg is a homogeneous polynomial then $V(fg) = V(f) \cup V(g)$ (recall from Lemma A.5.4 that f and g are both homogeneous).*
3. *$V(f) \cap V(g) = V(f, g)$.*
4. *If $X_1 \subseteq X_2 \subseteq \mathbb{P}^n(\Bbbk)$ then $I_{\Bbbk}(X_2) \subseteq I_{\Bbbk}(X_1) \subseteq \Bbbk[x_0, \ldots, x_n]$.*
5. *$I_{\Bbbk}(X_1 \cup X_2) = I_{\Bbbk}(X_1) \cap I_{\Bbbk}(X_2)$.*
6. *If J is a homogeneous ideal then $J \subseteq I_{\Bbbk}(V(J))$.*
7. *If X is a projective algebraic set defined over $\Bbbk$ then $V(I_{\Bbbk}(X)) = X$. If Y is another projective algebraic set defined over $\Bbbk$ and $I_{\Bbbk}(Y) = I_{\Bbbk}(X)$ then $Y = X$.*

Exercise 5.2.15. Prove Proposition 5.2.14.

Definition 5.2.16. If X is a projective algebraic set defined over $\Bbbk$ then the **homogenous coordinate ring** of X over $\Bbbk$ is $\Bbbk[X] = \Bbbk[x_0, \ldots, x_n]/I_{\Bbbk}(X)$.

Note that elements of $\Bbbk[X]$ are not necessarily homogeneous polynomials.

Definition 5.2.17. Let X be an algebraic set in $\mathbb{A}^n$ (respectively, $\mathbb{P}^n$) The **Zariski topology** is the topology on X defined as follows: The closed sets are $X \cap Y$ for every algebraic set $Y \subseteq \mathbb{A}^n$ (respectively, $Y \subseteq \mathbb{P}^n$).

Exercise 5.2.18. Show that the Zariski topology satisfies the axioms of a topology.

Definition 5.2.19. For $0 \leq i \leq n$ define $U_i = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n : x_i \neq 0\} = \mathbb{P}^n - V(x_i)$. (These are open sets in the Zariski topology.)

Exercise 5.2.20. Show that $\mathbb{P}^n = \cup_{i=0}^n U_i$ (not a disjoint union).

Exercise 5.2.21. What points of $\mathbb{P}^2(\Bbbk)$ do not lie in two of the three sets $U_0(\Bbbk), U_1(\Bbbk), U_2(\Bbbk)$?

Definition. Let $L \in \mathrm{GL}_{n+1}(\Bbbk)$ (i.e., L is an $(n+1) \times (n+1)$ matrix over $\Bbbk$ that is invertible). The map $L : \mathbb{P}^n \to \mathbb{P}^n$ given by

$$L(x_0 : \cdots : x_n) = (L_{0,0}x_0 + \cdots + L_{0,n}x_n : \cdots : L_{n,0}x_0 + \cdots + L_{n,n}x_n)$$

is called a **linear change of variables** on $\mathbb{P}^n$ over $\Bbbk$. The inverse change of variables is given by L^{-1}.

Example 5.2.22. The matrix

$$L = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

gives a linear change of variables $L : \mathbb{P}^2 \to \mathbb{P}^2$ of the form $L(x_0 : x_1 : x_2) = (y_0 : y_1 : y_2) = (x_0 - x_1 : x_1 : x_2)$. This maps the algebraic set $X = V(x_0^2 - x_1^2 + x_1x_2)$ to $Y = V(y_0^2 + 2y_0y_1 + y_1y_2)$. In other words, if $P \in X(\Bbbk)$ then $L(P) \in Y(\Bbbk)$.

A linear change of variable does not change the underlying geometry of an algebraic set, but can be useful for practical computation. For instance, sometimes we will use Exercise 5.2.23 to reduce any pair of points to affine space without changing the "shape" of the algebraic set.

Exercise 5.2.23. Show that if $P, Q \in \mathbb{P}^n(\Bbbk)$ then there is always a linear change of variables L on $\mathbb{P}^n$ over $\Bbbk$ such that $L(P), L(Q) \in U_n$.

We already mentioned the map $\varphi : \mathbb{A}^n \to \mathbb{P}^n$ given by $\varphi(x_1, \ldots, x_n) = (x_1 : \cdots : x_n : 1)$, which has image equal to U_n. A useful way to study a projective algebraic set X is to consider $X \cap U_i$ for $0 \leq i \leq n$ and interpret $X \cap U_i$ as an affine algebraic set. We now introduce the notation for this.

Definition 5.2.24. Let $\varphi_i : \mathbb{A}^n(\Bbbk) \to U_i$ be the one-to-one correspondence

$$\varphi_i(y_1, \ldots, y_n) = (y_1 : \cdots : y_i : 1 : y_{i+1} : \cdots : y_n).$$

We write φ for φ_n. Let

$$\varphi_i^{-1}(x_0 : \cdots : x_n) = (x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i).$$

be the map $\varphi_i^{-1} : \mathbb{P}^n(\Bbbk) \to \mathbb{A}^n(\Bbbk)$, which is defined only on U_i (i.e., $\varphi_i^{-1}(X) = \varphi_i^{-1}(X \cap U_i)$).[3]

We write $X \cap \mathbb{A}^n$ as an abbreviation for $\varphi_n^{-1}(X \cap U_n)$.

Let $\varphi_i^* : \Bbbk[x_0, \ldots, x_n] \to \Bbbk[y_1, \ldots, y_n]$ be the **de-homogenisation** map[4]

$$\varphi_i^*(f)(y_1, \ldots, y_n) = f \circ \varphi_i(y_1, \ldots, y_n) = f(y_1, \ldots, y_i, 1, y_{i+1}, \ldots, y_n).$$

We write φ^* for φ_n^*.

Let $\varphi_i^{-1*} : \Bbbk[y_1, \ldots, y_n] \to \Bbbk[x_0, \ldots, x_n]$ be the **homogenisation**

$$\varphi_i^{-1*}(f)(x_0, \ldots, x_n) = x_i^{\deg(f)} f(x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i)$$

where $\deg(f)$ is the total degree.

We write $\overline{f}$ as an abbreviation for $\varphi_n^{-1*}(f)$. For notational simplicity we often consider polynomials $f(x, y)$; in this case we define $\overline{f} = z^{\deg(f)} f(x/z, y/z)$.

We now state some elementary relations between projective algebraic sets X and their affine parts $X \cap U_i$.

Lemma 5.2.25. *Let the notation be as above.*

1. *$\varphi_i^* : \Bbbk[x_0, \ldots, x_n] \to \Bbbk[y_1, \ldots, y_n]$ is a $\Bbbk$-algebra homomorphism. The map $\varphi_i^{-1*} : \Bbbk[y_1, \ldots, y_n] \to \Bbbk[x_0, \ldots, x_n]$ satisfies most of the properties of a $\Bbbk$-algebra homomorphism, except that $\varphi_i^{-1*}(f+g) = \varphi_i^{-1*}(f) + \varphi_i^{-1*}(g)$ if and only if f and g have the same total degree.*
2. *Let $P = (P_0 : \cdots : P_n) \in \mathbb{P}^n(\Bbbk)$ with $P_i \neq 0$ and let $f \in \Bbbk[x_0, \ldots, x_n]$ be homogeneous. Then $f(P) = 0$ implies $\varphi_i^*(f)(\varphi_i^{-1}(P)) = 0$.*
3. *Let $f \in \Bbbk[x_0, \ldots, x_n]$ be homogeneous. Then $\varphi_i^{-1}(V(f)) = V(\varphi_i^*(f))$. In particular, $V(f) \cap \mathbb{A}^n = V(f \circ \varphi)$.*

[3] This notation does not seem to be standard. Our notation agrees with Silverman [564], but Hartshorne [278] has φ_i and φ_i^{-1} the other way around.

[4] The upper star notation is extended in Definition 5.5.23.

4. *Let $X \subseteq \mathbb{P}^n(\Bbbk)$. Then $f \in I_{\Bbbk}(X)$ implies $\varphi_i^*(f) \in I_{\Bbbk}(\varphi_i^{-1}(X))$. In particular, $f \in I_{\Bbbk}(X)$ implies $f \circ \varphi \in I_{\Bbbk}(X \cap \mathbb{A}^n)$.*
5. *If $P \in \mathbb{A}^n(\Bbbk)$ and $f \in \Bbbk[y_1, \ldots, y_n]$ then $f(P) = 0$ implies $\varphi_i^{-1*}(f)(\varphi_i(P)) = 0$. In particular, $f(P) = 0$ implies $\overline{f}(\varphi(P)) = 0$.*
6. *For homogeneous $f \in \Bbbk[x_0, \ldots, x_n]$ then $\varphi_i^{-1*}(\varphi_i^*(f)) \mid f$. Furthermore, if f has a monomial that does not include x_i then $\varphi_i^{-1*}(\varphi_i^*(f)) = f$ (in particular, $\overline{f \circ \varphi} = f$).*

Exercise 5.2.26. Prove Lemma 5.2.25.

Definition 5.2.27. Let $I \subseteq \Bbbk[y_1, \ldots, y_n]$. Define the **homogenisation** $\overline{I}$ to be the $\Bbbk[x_0, \ldots, x_n]$-ideal generated by the set $\{\overline{f}(x_0, \ldots, x_n) : f \in I\}$.

Exercise 5.2.28. Let $I \subseteq \Bbbk[y_1, \ldots, y_n]$. Show that $\overline{I}$ is a homogeneous ideal.

Definition 5.2.29. Let $X \subseteq \mathbb{A}^n(\overline{\Bbbk})$. Define the **projective closure** of X to be $\overline{X} = V\left(\overline{I(X)}\right) \subseteq \mathbb{P}^n$.

Lemma 5.2.30. *Let the notation be as above.*

1. *Let $X \subseteq \mathbb{A}^n$, then $\varphi(X) \subseteq \overline{X}$ and $\overline{X} \cap \mathbb{A}^n = X$.*
2. *Let $X \subseteq \mathbb{A}^n(\overline{\Bbbk})$ be non-empty. Then $I_{\Bbbk}\left(\overline{X}\right) = \overline{I_{\Bbbk}(X)}$.*

Proof: Part 1 follows directly from the definitions.

Part 2 is essentially that the homogenisation of a radical ideal is a radical ideal, we give a direct proof. Let $f \in \Bbbk[x_0, \ldots, x_n]$ be such that f is homogeneous and $f(\overline{X}) = 0$. Write $f = x_0^d g$ where $g \in \Bbbk[x_0, \ldots, x_n]$ has a monomial that does not include x_0. By part 1 and $X \neq \varnothing$, g is not constant. Then $g \circ \varphi \in I_{\Bbbk}(X)$ and so $g = \overline{g \circ \varphi} \in \overline{I_{\Bbbk}(X)}$. It follows from part 6 of Lemma 5.2.25 that $f \in \overline{I_{\Bbbk}(X)}$. Hence, $I_{\Bbbk}(\overline{X}) \subseteq \overline{I_{\Bbbk}(X)}$ and the result follows. □

Theorem 5.2.31. *Let $f(x_0, x_1, x_2) \in \Bbbk[x_0, x_1, x_2]$ be a $\overline{\Bbbk}$-irreducible homogeneous polynomial. Let*

$$X = V(f(x_0, x_1, x_2)) \subseteq \mathbb{P}^2.$$

Then $I_{\overline{\Bbbk}}(X) = (f(x_0, x_1, x_2))$.

Proof: Let $0 \leq i \leq 2$ be such that $f(x_0, x_1, x_2)$ has a monomial that does not feature x_i (such an i must exist since f is irreducible). Without loss of generality, suppose $i = 2$. Write $g(y_1, y_2) = \varphi^*(f) = f(y_1, y_2, 1)$. By part 6 of Lemma 5.2.25 the homogenisation of g is f.

Let $Y = X \cap \mathbb{A}^2 = V(g)$. Note that g is $\overline{\Bbbk}$-irreducible (since $g = g_1 g_2$ implies, by taking homogenisation, $f = \overline{g_1}\ \overline{g_2}$). Let $h \in I_{\overline{\Bbbk}}(X)$ then $h \circ \varphi \in I_{\overline{\Bbbk}}(Y)$ and so, by Corollary 5.1.23, $h \circ \varphi \in (g)$. In other words, there is some $h_1(y_1, y_2)$ such that $h \circ \varphi = g h_1$. Taking homogenisations gives $f \mid \overline{h_1}\, h$ and so $h \in (f)$. □

Corollary 5.2.32. *Let $f(x, y) \in \Bbbk[x, y]$ be a $\overline{\Bbbk}$-irreducible polynomial and let $X = V(f) \subseteq \mathbb{A}^2$. Then $\overline{X} = V(\overline{f}) \subseteq \mathbb{P}^2$.*

Exercise 5.2.33. Prove Corollary 5.2.32.

Example 5.2.34. The projective closure of $V(y^2 = x^3 + Ax + B) \subseteq \mathbb{A}^n$ is $V(y^2 z = x^3 + Axz^2 + Bz^3)$.

Exercise 5.2.35. Let $X = V(f(x_0, x_1)) \subseteq \mathbb{A}^2$ and let $\overline{X} \subseteq \mathbb{P}^2$ be the projective closure of X. Show that $\overline{X} - X$ is finite (in other words, there are only finitely many points at infinity).

A generalisation of projective space, called **weighted projective space**, is defined as follows: For $i_0, \ldots, i_n \in \mathbb{N}$ denote by $(a_0 : a_1 : \cdots : a_n)$ the equivalence class of elements in $\Bbbk^{n+1}$ under the equivalence relation

$$(a_0, a_1, \cdots, a_n) \equiv (\lambda^{i_0} a_0, \lambda^{i_1} a_1, \cdots, \lambda^{i_n} a_n)$$

for any $\lambda \in \Bbbk^*$. The set of equivalence classes is denoted $\mathbb{P}(i_0, \ldots, i_n)(\Bbbk)$. For example, it makes sense to consider the curve $y^2 = x^4 + ax^2z^2 + z^4$ as lying in $\mathbb{P}(1, 2, 1)$. We will not discuss this topic further in the book (we refer to Reid [498] for details), but it should be noted that certain coordinate systems used for efficient elliptic curve cryptography naturally live in weighted projective space.

5.3 Irreducibility

We have seen that $V(fg)$ decomposes as $V(f) \cup V(g)$ and it is natural to consider $V(f)$ and $V(g)$ as being 'components' of $V(fg)$. It is easier to deal with algebraic sets that cannot be decomposed in this way. This concept is most useful when working over an algebraically closed field, but we give some of the theory in greater generality.

Definition 5.3.1. An affine $\Bbbk$-algebraic set $X \subseteq \mathbb{A}^n$ is $\Bbbk$-**reducible** if $X = X_1 \cup X_2$ with X_1 and X_2 being $\Bbbk$-algebraic sets and $X_i \neq X$ for $i = 1, 2$. An affine algebraic set is $\Bbbk$-**irreducible** if there is no such decomposition. An affine algebraic set is **geometrically irreducible** if X is $\overline{\Bbbk}$-irreducible. An **affine variety** over $\Bbbk$ is a geometrically irreducible $\Bbbk$-algebraic set defined over $\Bbbk$.

A projective $\Bbbk$-algebraic set $X \subseteq \mathbb{P}^n$ is $\Bbbk$-**irreducible** (resp. **geometrically irreducible**) if X is not the union $X_1 \cup X_2$ of projective $\Bbbk$-algebraic sets $X_1, X_2 \subseteq \mathbb{P}^n$ (respectively, projective $\overline{\Bbbk}$-algebraic sets) such that $X_i \neq X$ for $i = 1, 2$. A **projective variety** over $\Bbbk$ is a geometrically irreducible projective $\Bbbk$-algebraic set defined over $\Bbbk$.

Let X be a variety (affine or projective). A **subvariety** of X over $\Bbbk$ is a subset $Y \subseteq X$ that is a variety (affine or projective) defined over $\Bbbk$.

This definition matches the usual topological definition of a set being irreducible if it is not a union of proper closed subsets.

Example 5.3.2. The algebraic set $X = V(x^2 + y^2) \subseteq \mathbb{A}^2$ over $\mathbb{R}$ is $\mathbb{R}$-irreducible. However, over $\mathbb{C}$ we have $X = V(x + iy) \cup V(x - iy)$ and so X is $\mathbb{C}$-reducible.

Exercise 5.3.3. Show that $X = V(wx - yz, x^2 - yz) \subseteq \mathbb{P}^3$ is not irreducible.

It is often easy to determine that a reducible algebraic set is reducible, just by exhibiting the non-trivial union. However, it is not necessarily easy to show that an irreducible algebraic set is irreducible. We now give an algebraic criterion for irreducibility and some applications of this result.

Theorem 5.3.4. *Let X be an algebraic set (affine or projective). Then X is $\Bbbk$-irreducible if and only if $I_\Bbbk(X)$ is a prime ideal.*

Proof: ($\Rightarrow$): Suppose $X = V(S)$ where $S \subseteq \Bbbk[\underline{x}]$ is $\Bbbk$-irreducible and that there are elements $f, g \in \Bbbk[\underline{x}]$ such that $fg \in I_\Bbbk(X)$. Then $X \subseteq V(fg) = V(f) \cup V(g)$, so $X = (X \cap V(f)) \cup (X \cap V(g))$. Since $X \cap V(f) = V(S, f)$ and $X \cap V(g) = V(S, g)$ are $\Bbbk$-algebraic sets it follows that either $X = X \cap V(f)$ or $X = X \cap V(g)$, and so $f \in I_\Bbbk(X)$ or $g \in I_\Bbbk(X)$.

($\Leftarrow$): Suppose $I = I_\Bbbk(X)$ is a prime ideal and that $X = X_1 \cup X_2$ where X_1 and X_2 are $\Bbbk$-algebraic sets. Let $I_1 = I_\Bbbk(X_1)$ and $I_2 = I_\Bbbk(X_2)$. By parts 3 and 4 of Proposition 5.1.16

or parts 4 and 5 of Proposition 5.2.14 we have $I \subseteq I_1$, $I \subseteq I_2$ and $I = I_1 \cap I_2$. Since $I_1 I_2 \subseteq I_1 \cap I_2 = I$ and I is a prime ideal, it follows that either $I_1 \subseteq I$ or $I_2 \subseteq I$. Hence either $I = I_1$ or $I = I_2$ and so, by part 6 of Proposition 5.1.16 or part 7 of Proposition 5.2.14, $X = X_1$ or $X = X_2$. □

Exercise 5.3.5. Show that $V(y - x^2)$ is irreducible in $\mathbb{A}^2(\Bbbk)$.

Exercise 5.3.6. Let $X \subset \mathbb{A}^n$ be an algebraic set over $\Bbbk$. Suppose there exist polynomials $f_1, \ldots, f_n \in \Bbbk[t]$ such that $X = \{(f_1(t), f_2(t), \ldots, f_n(t)) : t \in \overline{\Bbbk}\}$. Prove that X is geometrically irreducible.

Remark 5.3.7. A $\Bbbk$-algebraic set X is the vanishing of polynomials in $\Bbbk[x_1, \ldots, x_n]$. However, we say X is defined over $\Bbbk$ if $I_{\overline{\Bbbk}}(X)$ is generated by polynomials in $\Bbbk[x_1, \ldots, x_n]$. Hence, it is clear that an algebraic set defined over $\Bbbk$ is a $\Bbbk$-algebraic set. The converse does not hold in general. However, if X is absolutely irreducible and $\Bbbk$ is a perfect field then these notions are equivalent (see Corollary 10.2.2 of Fried and Jarden [214] and use the fact that when X is absolutely irreducible then the algebraic closure of $\Bbbk$ in $\Bbbk(X)$ is $\Bbbk$). Note that Corollary 5.1.23 proves a special case of this result.

The next few results use the notation of Definitions 5.2.24, 5.2.27 and 5.2.29.

Corollary 5.3.8. *Let $X \subseteq \mathbb{A}^n$ be a variety. Then $\overline{X}$ is geometrically irreducible. Let $X \subseteq \mathbb{P}^n$ be a variety. Then $X \cap \mathbb{A}^n$ is geometrically irreducible.*

Proof: The case where X is empty is trivial so suppose $X \neq \varnothing$. By Lemma 5.2.30, $I\left(\overline{X}\right) = \overline{I(X)}$. Hence, if $g, h \in \Bbbk[x_0, \ldots, x_n]$ are such that $gh \in I\left(\overline{X}\right)$ then $(g \circ \varphi)(h \circ \varphi) = (gh) \circ \varphi \in I(X)$ by part 4 of Lemma 5.2.25. Theorem 5.3.4 implies $I(X)$ is a prime ideal and so either $g \circ \varphi$ or $h \circ \varphi$ is in $I(X)$. Hence either g or h is in $I\left(\overline{X}\right)$.

For the converse, suppose $X \cap \mathbb{A}^n \neq \varnothing$. If $gh \in I(X \cap \mathbb{A}^n)$ then $\overline{g}\,\overline{h} = \overline{gh} \in \overline{I(X \cap \mathbb{A}^n)} \subseteq I(X)$. Hence $\overline{g}$ or $\overline{h}$ is in $I(X)$ and so, by part 4 of Lemma 5.2.25, g or h is in $I(X \cap \mathbb{A}^n)$. □

Theorem 5.3.9. *Let $X \subseteq \mathbb{P}^n$ be an algebraic set such that $X \cap \mathbb{A}^n \neq \varnothing$. Then $\overline{X \cap \mathbb{A}^n} \subseteq X$. If X is a variety then $\overline{X \cap \mathbb{A}^n} = X$.*

Proof: If $f \in I(X)$ then $f \circ \varphi \in I(X \cap \mathbb{A}^n)$ and so $\overline{f \circ \varphi} \in \overline{I(X \cap \mathbb{A}^n)}$. Hence, $f \in \overline{I(X \cap \mathbb{A}^n)}$. In other words, $I(X) \subseteq I\left(\overline{X \cap \mathbb{A}^n}\right)$ and so $\overline{X \cap \mathbb{A}^n} \subseteq X$.

Let $X_1 = \overline{X \cap \mathbb{A}^n} \subseteq X$ and $X_2 = X \cap V(x_0)$. Then $X = X_1 \cup X_2$ and so, if X is irreducible and $X \cap \mathbb{A}^n \neq \varnothing$ then $X = X_1$. □

Theorem 5.3.10. *Let $\Bbbk$ be a field and let $f(x, y) \in \Bbbk[x, y]$ (or $f(x, y, z) \in \Bbbk[x, y, z]$ homogeneous) have no repeated factors over $\overline{\Bbbk}$. Let $X = V(f(x, y)) \subset \mathbb{A}^2(\Bbbk)$ or $X = V(f(x, y, z)) \subseteq \mathbb{P}^2(\Bbbk)$. Then X is geometrically irreducible if and only if f is irreducible over $\overline{\Bbbk}$.*

Proof: Suppose $X = V(f)$ is geometrically irreducible but that $f = gh$ is a factorization in $\overline{\Bbbk}[x, y]$ or $\overline{\Bbbk}[x, y, z]$ with both g and h having degree ≥ 1. Since f has no repeated factors we have that g and h have no irreducible factors in common. Now, $V(f) = V(gh) = V(g) \cup V(h)$. Since $V(f)$ is irreducible either $V(g) = V(f)$ or $V(h) = V(f)$. Without loss of generality we may assume $V(g) = V(f)$. By Hilbert's Nullstellensatz (Theorem 5.1.22) it follows that $g^m \in \langle f \rangle$ for some integer m, which means that $f \mid g^m$. Now, let q be an irreducible factor of h. Then $q \mid f$ and so $q \mid g^m$ and so $q \mid g$. But g and h are supposed to have no common irreducible factors, so this is a contradiction. Hence, if X is geometrically irreducible then f is $\overline{\Bbbk}$-irreducible.

Conversely, by Corollary 5.1.23 (respectively, Theorem 5.2.31) we have $I_{\overline{\Bbbk}}(V(f)) = (f)$. Since f is irreducible it follows that (f) is a prime ideal and so X is irreducible. □

Example 5.3.11. It is necessary to work over $\overline{\Bbbk}$ for Theorem 5.3.10. For example, let $f(x,y) = y^2 + x^2(x-1)^2$. Then $V(f(x,y)) \subseteq \mathbb{A}^2(\mathbb{R})$ consists of two points and so is reducible, even though $f(x,y)$ is $\mathbb{R}$-irreducible.

Lemma 5.3.12. *Let X be a variety and $U \subset X$ a non-empty set. If U is open (in the Zariski topology) in X then U is **dense** in X (i.e., the topological closure of U in X in the Zariski topology is X).*

Proof: Let X_1 be the closure of U in X and $X_2 = X - U$. Then $X = X_1 \cup X_2$ and X_1, X_2 are closed sets. Since X is irreducible and $X_2 \neq X$ it follows that $X_1 = X$. □

Lemma 5.3.13. *Let X be a variety and U a non-empty open subset of X. Then $I_{\Bbbk}(U) = I_{\Bbbk}(X)$.*

Proof: Since $U \subseteq X$ we have $I_{\Bbbk}(X) \subseteq I_{\Bbbk}(U)$. Now let $f \in I_{\Bbbk}(U)$. Then $U \subseteq V(f) \cap X$. Write $X_1 = V(f) \cap X$, which is an algebraic set, and $X_2 = X - U$, which is also an algebraic set. Then $X = X_1 \cup X_2$ and, since X is irreducible and $X_2 \neq X$, $X = X_1$. In other words, $f \in I_{\Bbbk}(X)$. □

Exercise 5.3.14. Let X be an irreducible variety. Prove that if $U_1, U_2 \subseteq X$ are non-empty open sets then $U_1 \cap U_2 \neq \varnothing$.

5.4 Function Fields

If X is a variety defined over $\Bbbk$ then $I_{\Bbbk}(X)$ is a prime ideal and so the affine or homogeneous coordinate ring is an integral domain. One can therefore consider its field of fractions. If X is affine then the field of fractions has a natural interpretation as a set of maps $X \to \Bbbk$. When X is projective then a ratio f/g of polynomials does not give a well-defined function on X unless f and g are homogeneous of the same degree.

Definition 5.4.1. Let X be an affine variety defined over $\Bbbk$. The **function field** $\Bbbk(X)$ is the set

$$\Bbbk(X) = \{f_1/f_2 : f_1, f_2 \in \Bbbk[X], f_2 \notin I_{\Bbbk}(X)\}$$

of classes under the equivalence relation $f_1/f_2 \equiv f_3/f_4$ if and only if $f_1 f_4 - f_2 f_3 \in I_{\Bbbk}(X)$. In other words, $\Bbbk(X)$ is the field of fractions of the affine coordinate ring $\Bbbk[X]$ over $\Bbbk$.

Let X be a projective variety. The **function field** is

$$\Bbbk(X) = \{f_1/f_2 : f_1, f_2 \in \Bbbk[X] \text{ homogeneous of the same degree}, f_2 \notin I_{\Bbbk}(X)\}$$

with the equivalence relation $f_1/f_2 \equiv f_3/f_4$ if and only if $f_1 f_4 - f_2 f_3 \in I_{\Bbbk}(X)$.

Elements of $\Bbbk(X)$ are called **rational functions**. For $a \in \Bbbk$ the rational function $f : X \to \Bbbk$ given by $f(P) = a$ is called a **constant function**.

Exercise 5.4.2. Prove that the field of fractions of an integral domain is a field. Hence, deduce that if X is an affine variety then $\Bbbk(X)$ is a field. Prove also that if X is a projective variety then $\Bbbk(X)$ is a field.

We stress that, when X is projective, $\Bbbk(X)$ is not the field of fractions of $\Bbbk[X]$ and that $\Bbbk[X] \not\subseteq \Bbbk(X)$. Also note that elements of the function field are not functions $X \to \Bbbk$ but maps $X \to \Bbbk$ (i.e., they are not necessarily defined everywhere).

Example 5.4.3. One has $\Bbbk(\mathbb{A}^2) \cong \Bbbk(x,y)$ and $\Bbbk(\mathbb{P}^2) \cong \Bbbk(x,y)$.

Definition 5.4.4. Let X be a variety and let $f_1, f_2 \in \Bbbk[X]$. Then f_1/f_2 is **defined** or **regular** at P if $f_2(P) \neq 0$. An equivalence class $f \in \Bbbk(X)$ is **regular** at P if it contains some f_1/f_2 with $f_1, f_2 \in \Bbbk[X]$ (if X is projective then necessarily $\deg(f_1) = \deg(f_2)$) such that f_1/f_2 is regular at P.

Note that there may be many choices of representative for the equivalence class of f, and only some of them may be defined at P.

Example 5.4.5. Let $\Bbbk$ be a field of characteristic not equal to 2. Let X be the algebraic set $V(y^2 - x(x-1)(x+1)) \subset \mathbb{A}^2(\Bbbk)$. Consider the functions

$$f_1 = \frac{x(x-1)}{y} \qquad \text{and} \qquad f_2 = \frac{y}{x+1}.$$

One can check that f_1 is equivalent to f_2. Note that f_1 is not defined at $(0,0), (1,0)$ or $(-1,0)$ while f_2 is defined at $(0,0)$ and $(1,0)$ but not at $(-1,0)$. The equivalence class of f_1 is therefore regular at $(0,0)$ and $(1,0)$. Section 7.3 gives techniques to deal with these issues for curves, from which one can deduce that no function in the equivalence class of f_1 is defined at $(-1,0)$.

Exercise 5.4.6. Let X be a variety over $\Bbbk$. Suppose f_1/f_2 and f_3/f_4 are equivalent functions on X that are both defined at $P \in X(\Bbbk)$. Show that $(f_1/f_2)(P) = (f_3/f_4)(P)$.

Hence, if f is a function that is defined at a point P then it makes sense to speak of the **value** of the function at P. If the value of f at P is zero then P is called a **zero** of f.[5]

Exercise 5.4.7. Let $X = V(w^2x^2 - w^2z^2 - y^2z^2 + x^2z^2) \subseteq \mathbb{P}^3(\Bbbk)$. Show that $(x^2 + yz)/(x^2 - w^2) \equiv (x^2 - z^2)/(x^2 - yz)$ in $\Bbbk(X)$. Hence find the value of $(x^2 - z^2)/(x^2 - yz)$ at the point $(w : x : y : z) = (0 : 1 : 1 : 1)$. Show that both representations of the function have the same value on the point $(w : x : y : z) = (2 : 1 : -1 : 1)$.

Theorem 5.4.8. *Let X be a variety and let f be a rational function. Then there is a non-empty open set $U \subset X$ such that f is regular on U. Conversely, if $U \subset X$ is non-empty and open and $f : U \to \Bbbk$ is a function given by a ratio f_1/f_2 of polynomials (homogeneous polynomials of the same degree if X is projective) that is defined for all $P \in U$ then f extends uniquely to a rational function $f : X \to \Bbbk$.*

Proof: Let $f = f_1/f_2$ where $f_1, f_2 \in \Bbbk[X]$. Define $U = X - V(f_2)$. Since $f_2 \neq 0$ in $\Bbbk[X]$ we have U a non-empty open set, and f is regular on U.

For the converse, Let $f = f_1/f_2$ be a function on U given as a ratio of polynomials. Then one can consider f_1 and f_2 as elements of $\Bbbk[X]$ and f_2 non-zero on U implies $f_2 \neq 0$ in $\Bbbk[X]$. Hence f_1/f_2 corresponds to an element of $\Bbbk(X)$. Finally, suppose f_1/f_2 and f_3/f_4 are functions on X (where f_1, f_2, f_3, f_4 are polynomials) such that the restrictions $(f_1/f_2)|_U$ and $(f_3/f_4)|_U$ are equal. Then $f_1f_4 - f_2f_3$ is zero on U and, by Lemma 5.3.13, $(f_1f_4 - f_2f_3) \in I_{\Bbbk}(X)$ and $f_1/f_2 \equiv f_3/f_4$ on X. □

Corollary 5.4.9. *If X is a projective variety and $X \cap \mathbb{A}^n \neq \varnothing$ then $\Bbbk(X) \cong \Bbbk(X \cap \mathbb{A}^n)$. If X is non-empty affine variety then $\Bbbk(X) \cong \Bbbk(\overline{X})$.*

Proof: The result follows since $X \cap \mathbb{A}^n = X - V(x_n)$ is open in X and X is open in $\overline{X}$. □

[5] For curves we will later define the notion of a function f having a pole at a point P. This notion does not make sense for general varieties, as shown by the function x/y on $\mathbb{A}^2$ at $(0,0)$ for example.

Definition 5.4.10. Let X be a variety and $U \subseteq X$. Define $\mathcal{O}(U)$ to be the elements of $\overline{\Bbbk}(X)$ that are regular on all $P \in U(\overline{\Bbbk})$.

Lemma 5.4.11. *If X is an affine variety over $\Bbbk$ then $\mathcal{O}(X) = \overline{\Bbbk}[X]$.*

Proof: (Sketch) Clearly $\overline{\Bbbk}[X] \subseteq \mathcal{O}(X)$. The converse follows since $\mathcal{O}(X)$ is the intersection of the local rings (see Definition 7.1.1) at all $P \in X(\overline{\Bbbk})$. We refer to Proposition 2 on page 43, Chapter 2 of [216] or Theorem I.3.2(a) of [278] for the details. □

Definition 5.4.12. Let X be a variety over $\Bbbk$ and $f \in \overline{\Bbbk}(X)$. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. If $f = f_1/f_2$ where $f_1, f_2 \in \overline{\Bbbk}[\underline{x}]$ define $\sigma(f) = \sigma(f_1)/\sigma(f_2)$ where $\sigma(f_1)$ and $\sigma(f_2)$ denote the natural Galois action on polynomials (i.e., $\sigma(\sum_i a_i x^i) = \sum_i \sigma(a_i) x^i$). Some authors write this as f^σ.

Exercise 5.4.13. Prove that $\sigma(f)$ is well-defined (i.e., if $f \equiv f'$ then $\sigma(f) \equiv \sigma(f')$). Let $P \in X(\overline{\Bbbk})$. Prove that $f(P) = 0$ if and only if $\sigma(f)(\sigma(P)) = 0$.

Remark 5.4.14. Having defined an action of $G = \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ on $\overline{\Bbbk}(X)$ it is natural to ask whether $\overline{\Bbbk}(X)^G = \{f \in \overline{\Bbbk}(X) : \sigma(f) = f \ \forall \sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)\}$ is the same as $\Bbbk(X)$. The issue is whether a function being "defined over $\Bbbk$" is the same as "can be written with coefficients in $\Bbbk$". Indeed, this is true but not completely trivial.

A sketch of the argument is given in Exercise 1.12 of Silverman [564] and we give a few extra hints here. Let X be a projective variety. One first shows that if X is defined over $\Bbbk$ and if $\Bbbk'$ is a finite Galois extension of $\Bbbk$ then $I_{\Bbbk'}(X)$ is an induced Galois module (see page 110 of Serre [542]) for $\mathrm{Gal}(\Bbbk'/\Bbbk)$. It follows from Section VII.1 of [542] that the Galois cohomology group $H^1(\mathrm{Gal}(\Bbbk'/\Bbbk), I_{\Bbbk'}(X))$ is trivial and hence, by Section X.3 of [542], that $H^1(G, I_{\Bbbk'}(X)) = 0$. One can therefore deduce, as in Exercise 1.12(a) of [564], that $\overline{\Bbbk}[X]^G = \Bbbk[X]$.

To show that $\overline{\Bbbk}(X)^G = \Bbbk(X)$ let $(f_0 : f_1) : X \to \mathbb{P}^1$ and let $\sigma \in G$. Then $\sigma(f_0) = \lambda_\sigma f_0 + G_{0,\sigma}$ and $\sigma(f_1) = \lambda_\sigma f_1 + G_{1,\sigma}$ where $\lambda_\sigma \in \overline{\Bbbk}^*$ and $G_{0,\sigma}, G_{1,\sigma} \in I_{\overline{\Bbbk}}(X)$. One shows first that $\lambda_\sigma \in H^1(G, \overline{\Bbbk}^*)$, which is trivial by Hilbert 90, and so $\lambda_\sigma = \sigma(\alpha)/\alpha$ for some $\alpha \in \overline{\Bbbk}$. Replacing f_0 by αf_0 and f_1 by αf_1 gives $\lambda_\sigma = 1$ and one can proceed to showing that $G_{0,\sigma}, G_{1,\sigma} \in H^1(G, I_{\overline{\Bbbk}}(X)) = 0$ as above. The result follows.

For a different approach see Theorem 7.8.3 and Remark 8.4.11 below, or Corollary 2 of Section VI.5 (page 178) of Lang [364].

5.5 Rational Maps and Morphisms

Definition 5.5.1. Let X be an affine or projective variety over a field $\Bbbk$ and Y an affine variety in $\mathbb{A}^n$ over $\Bbbk$. Let $\phi_1, \ldots, \phi_n \in \Bbbk(X)$. A map $\phi : X \to \mathbb{A}^n$ of the form

$$\phi(P) = (\phi_1(P), \ldots, \phi_n(P)) \tag{5.1}$$

is **regular** at a point $P \in X(\overline{\Bbbk})$ if all ϕ_i, for $1 \leq i \leq n$, are regular at P. A **rational map** $\phi : X \to Y$ defined over $\Bbbk$ is a map of the form (5.1) such that, for all $P \in X(\overline{\Bbbk})$ for which ϕ is regular at P then $\phi(P) \in Y(\overline{\Bbbk})$.

Let X be an affine or projective variety over a field $\Bbbk$ and Y a projective variety in $\mathbb{P}^n$ over $\Bbbk$. Let $\phi_0, \ldots, \phi_n \in \Bbbk(X)$. A map $\phi : X \to \mathbb{P}^n$ of the form

$$\phi(P) = (\phi_0(P) : \cdots : \phi_n(P)) \tag{5.2}$$

is **regular** at a point $P \in X(\overline{\Bbbk})$ if there is some function $g \in \Bbbk(X)$ such that all $g\phi_i$, for $0 \leq i \leq n$, are regular at P and, for some $0 \leq i \leq n$, one has $(g\phi_i)(P) \neq 0$.[6] A **rational**

[6] This last condition is to prevent ϕ mapping to $(0 : \cdots : 0)$, which is not a point in $\mathbb{P}^n$.

map $\phi : X \to Y$ defined over $\Bbbk$ is a map of the form (5.2) such that, for all $P \in X(\overline{\Bbbk})$ for which ϕ is regular at P, then $\phi(P) \in Y(\overline{\Bbbk})$.

We stress that a rational map is not necessarily defined at every point of the domain. In other words, it is not necessarily a function.

Exercise 5.5.2. Let X and Y be projective varieties. Show that one can write a rational map in the form $\phi(P) = (\phi_0(P) : \cdots : \phi_n(P))$ where the $\phi_i(\underline{x}) \in \Bbbk[\underline{x}]$ are all homogeneous polynomials of the same degree, not all $\phi_i(\underline{x}) \in I_\Bbbk(X)$, and for every $f \in I_\Bbbk(Y)$ we have $f(\phi_0(\underline{x}), \ldots, \phi_n(\underline{x})) \in I_\Bbbk(X)$.

Example 5.5.3. Let $X = V(x - y) \subseteq \mathbb{A}^2$ and $Y = V(x - z) \subseteq \mathbb{P}^2$. Then

$$\phi(x, y) = (x : xy : y)$$

is a rational map from X to Y. Note that this formula for ϕ is not defined at $(0, 0)$. However, ϕ is regular at $(0, 0)$ since taking $g = x^{-1}$ gives the equivalent form $\phi(x, y) = (x^{-1}x : x^{-1}xy : x^{-1}y) = (1 : y : y/x)$ and $y/x \equiv 1$ in $\Bbbk(X)$. Also note that the image of ϕ is not equal to $Y(\Bbbk)$ as it misses the point $(0 : 1 : 0)$.

Similarly, $\psi(x : y : z) = (x/y, z/y)$ is a rational map from Y to X. This map is not regular at $(1 : 0 : 1)$ but it is surjective to X. The composition $\psi \circ \phi$ maps (x, y) to $(1/y, 1/x)$.

Example 5.5.4. Let $X = V(y^2z - (x^3 + Axz^2)) \subseteq \mathbb{P}^2$ and $Y = \mathbb{P}^1$. Consider the rational map

$$\phi(x : y : z) = (x/z : 1).$$

Note that this formula for ϕ is defined at all points of X except $P_0 = (0 : 1 : 0)$. Let $g(x : y : z) = (x^2 + Az^2)/y^2 \in \Bbbk(X)$. Then the map $(x : y : z) \mapsto (gx/z : g)$ can be written as $(x : y : z) \mapsto (1 : g)$ and this is defined at $(0 : 1 : 0)$. It follows that ϕ is regular at P_0 and that $\phi(P_0) = (1 : 0)$.

Lemma 5.5.5. *Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a rational map. Then there is an open set $U \subseteq X$ such that ϕ is regular on U.*

Proof: Write ϕ as $(\phi_1, \ldots, \phi_n)$ if Y is affine or $(\phi_0 : \cdots : \phi_n)$ if Y is projective. By Theorem 5.4.8 for each ϕ_i for $1 \leq \phi_i \leq n$ (respectively, $0 \leq \phi_i \leq n$) there is a non-empty open set $U_i \subset X$ such that ϕ_i is regular. Taking $U = \cap_i U_i$ gives the result. □

It immediately follows that Theorem 5.4.8 generalises to rational maps.

Theorem 5.5.6. *Let X and Y be varieties. Suppose $\phi_1, \phi_2 : X \to Y$ are rational maps that are regular on non-empty open sets $U_1, U_2 \subseteq X$. Suppose further that $\phi_1|_{U_1 \cap U_2} = \phi_2|_{U_1 \cap U_2}$. Then $\phi_1 = \phi_2$.*

Exercise 5.5.7. Prove Theorem 5.5.6.

Definition 5.5.8. Let X and Y be algebraic varieties over $\Bbbk$. A rational map $\phi : X \to Y$ defined over $\Bbbk$ is a **birational equivalence** over $\Bbbk$ if there exists a rational map $\psi : Y \to X$ over $\Bbbk$ such that:

1. $\psi \circ \phi(P) = P$ for all points $P \in X(\overline{\Bbbk})$ such that $\psi \circ \phi(P)$ is defined;
2. $\phi \circ \psi(Q) = Q$ for all points $Q \in Y(\overline{\Bbbk})$ such that $\phi \circ \psi(Q) = Q$ is defined.

Varieties X and Y are **birationally equivalent** if there is a birational equivalence $\phi : X \to Y$ between them.

Exercise 5.5.9. Show that $X = V(xy-1) \subseteq \mathbb{A}^2$ and $Y = V(x_1-x_2) \subseteq \mathbb{P}^2$ are birationally equivalent.

Exercise 5.5.10. Verify that birational equivalence is an equivalence relation.

Example 5.5.11. The maps $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ and $\varphi_i^{-1} : \mathbb{P}^n \to \mathbb{A}^n$ from Definition 5.2.24 are rational maps. Hence $\mathbb{A}^n$ and $\mathbb{P}^n$ are birationally equivalent.

Definition 5.5.12. Let X and Y be varieties over $\Bbbk$ and let $U \subseteq X$ be open. A rational map $\phi : U \to Y$ over $\Bbbk$ which is regular at every point $P \in U(\overline{\Bbbk})$ is called a **morphism** over $\Bbbk$.

Let $U \subseteq X$ and $V \subseteq Y$ be open. If $\phi : U \to Y$ is a morphism over $\Bbbk$ and $\psi : V \to X$ is a morphism over $\Bbbk$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity on V and U respectively then we say that U and V are **isomorphic** over $\Bbbk$. If U and V are isomorphic we write $U \cong V$.

Example 5.5.13. Let X be $V(xy - z^2) \subseteq \mathbb{P}^2$ and let $\phi : X \to \mathbb{P}^1$ be given by $\phi(x : y : z) = (x/z : 1)$. Then ϕ is a morphism (for $(1 : 0 : 0)$ replace ϕ by the equivalent form $\phi(x : y : z) = (1 : z/x)$ and for $(0 : 1 : 0)$ use $\phi(x : y : z) = (z/y : 1)$). Indeed, ϕ is an isomorphism with inverse $\psi(x : z) = (x/z : z/x : 1)$.

Lemma 5.5.5 shows that every rational map $\phi : X \to Y$ restricts to a morphism $\phi : U \to Y$ on some open set $U \subseteq X$.

Exercise 5.5.14. Let $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2$ over $\Bbbk$. By taking a line of slope $t \in \Bbbk$ through $(-1, 0)$ give a formula for a rational map $\phi : \mathbb{A}^1 \to X$. Explain how to extend this to a morphism from $\mathbb{P}^1$ to $V(x^2 + y^2 - 1)$. Show that this is an isomorphism.

We now give the notion of a dominant rational map (or morphism). This is the appropriate analogue of surjectivity for maps between varieties. Essentially, a rational map from X to Y is dominant if its image is not contained in a proper subvariety of Y. For example, the map $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ is dominant. Birational maps are also dominant.

Definition 5.5.15. Let X and Y be varieties over $\Bbbk$. A set $U \subseteq Y(\overline{\Bbbk})$ is **dense** if its closure in the Zariski topology in $Y(\overline{\Bbbk})$ is equal to $Y(\overline{\Bbbk})$. A rational map $\phi : X \to Y$ is **dominant** if $\phi(X(\overline{\Bbbk}))$ is **dense** in $Y(\overline{\Bbbk})$.

Example 5.5.16. Let $\phi : \mathbb{A}^2 \to \mathbb{A}^2$ be given by $\phi(x, y) = (x, x)$. Then ϕ is not dominant (though it is dominant to $V(x-y) \subseteq \mathbb{A}^2$). Let $\phi : \mathbb{A}^2 \to \mathbb{A}^2$ be given by $\phi(x, y) = (x, xy)$. Then ϕ is dominant, even though it is not surjective.

We now show that a morphism is a continuous map for the Zariski topology.

Lemma 5.5.17. *Let X and Y be varieties over $\Bbbk$. Let $\phi : X \to Y$ be a morphism. Let $V \subseteq Y$ be an open set such that $\phi(X) \cap V \neq \varnothing$. Then $\phi^{-1}(V)$ is an open set in X. Similarly, let $Z \subseteq Y$ be a closed set such that $\phi(X) \cap Z \neq \varnothing$. Then $\phi^{-1}(Z)$ is closed in X.*

Exercise 5.5.18.★ Prove Lemma 5.5.17.

Exercise 5.5.19. Let X and Y be varieties and let $\phi : X \to Y$ be a morphism. Show that the Zariski closure of $\phi(X)$ in Y is irreducible.

Lemma 5.5.20. *Let X and Y be affine varieties over $\Bbbk$, let $U \subseteq X$ be open, and let $\phi : U \to Y$ be a morphism. Then the composition $f \circ \phi$ induces a well-defined ring homomorphism from $\overline{\Bbbk}[Y]$ to $\mathcal{O}(U)$.*

Proof: If $f \in \overline{\Bbbk}[Y]$ then f is regular on Y and, since ϕ is regular on U, $f \circ \phi$ is regular on U. Hence, $f \circ \phi \in \mathcal{O}(U)$.

We now show that the map is well-defined. Suppose $f \equiv 0$ in $\overline{\Bbbk}[Y]$. Since f vanishes on Y it follows that, for all $P \in U(\overline{\Bbbk})$, $f(\phi(P)) = 0$. Write $f \circ \phi = f_1/f_2$ where f_1 and f_2 are polynomials. It follows that $f_1 \in I(U) = I(X)$ (using Lemma 5.3.13). Hence, $f \circ \phi \equiv 0$ in $\mathcal{O}(U)$. Finally, the map is a ring homomorphism since $(f_1 + f_2) \circ \phi = (f_1 \circ \phi) + (f_2 \circ \phi)$ and similarly for multiplication. □

Definition 5.5.21. Let X and Y be affine varieties over $\Bbbk$, let $U \subseteq X$ be open, and let $\phi : U \to Y$ be a morphism. The **pullback**[7] is the ring homomorphism $\phi^* : \overline{\Bbbk}[Y] \to \mathcal{O}(U)$ defined by $\phi^*(f) = f \circ \phi$.

Lemma 5.5.22. *Let X and Y be affine varieties over $\Bbbk$, let $U \subseteq X$ be open, and let $\phi : U \to Y$ be a morphism. Then ϕ is dominant if and only if ϕ^* is injective.*

Proof: Let $f \in \overline{\Bbbk}[Y]$ be in the kernel of ϕ^*. Now $\phi^*(f) = 0$ is the same as $f \circ \phi = 0$ on U, which implies $\phi(U) \subseteq V(f) \cap Y$. If $\phi(U)$ is dense in Y then $Y \subseteq V(f)$ and so $f \in I(Y)$ and ϕ^* is injective. Conversely, if $\phi(U)$ is not dense in Y then there is some polynomial $f \notin I(Y)$ such that $\phi(U) \subseteq Y \cap V(f)$. It follows that $\phi^*(f) = 0$ and ϕ^* is not injective. □

Note that if X and ϕ are defined over $\Bbbk$ then $\phi^* : \overline{\Bbbk}[Y] \to \mathcal{O}(U)$ restricts to $\phi^* : \Bbbk[Y] \to \Bbbk(X)$. If ϕ^* is injective then one can extend it to get a homomorphism of the field of fractions of $\Bbbk[Y]$ to $\Bbbk(X)$.

Definition 5.5.23. Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a dominant rational map defined over $\Bbbk$. Define the **pullback** $\phi^* : \Bbbk(Y) \to \Bbbk(X)$ by $\phi^*(f) = f \circ \phi$.

We will now sketch a proof that ϕ^* is a $\Bbbk$-algebra homomorphism. Recall that a $\Bbbk$-algebra homomorphism of fields is a field homomorphism that is the identity map on $\Bbbk$.

Theorem 5.5.24. *Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a dominant rational map defined over $\Bbbk$. Then the pullback $\phi^* : \Bbbk(Y) \to \Bbbk(X)$ is an injective $\Bbbk$-algebra homomorphism.*

Proof: Without loss of generality we may assume that X and Y are affine. The rational map ϕ is therefore given by $\phi(\underline{x}) = (\phi_1(\underline{x}), \ldots, \phi_n(\underline{x}))$. Let $U \subseteq X$ be an open set on which ϕ is regular. Then $\phi : U \to Y$ is a morphism and we know $\phi^* : \overline{\Bbbk}[Y] \to \mathcal{O}(U)$ is a ring homomorphism by Lemma 5.5.20. The field of fractions of $\overline{\Bbbk}[Y]$ is $\overline{\Bbbk}(Y)$ and the field of fractions of $\mathcal{O}(U)$ is $\overline{\Bbbk}(X)$. The natural extension of ϕ^* to $\phi^* : \overline{\Bbbk}(Y) \to \overline{\Bbbk}(X)$ is well-defined.

It immediately follows that ϕ^* is a ring homomorphism and that ϕ^* is the identity on $\overline{\Bbbk}$. Hence, ϕ^* is a $\overline{\Bbbk}$-algebra homomorphism. Furthermore, ϕ^* is injective by Lemma 5.5.22. Finally, since ϕ is defined over $\Bbbk$ it restricts to an injective homomorphism from $\Bbbk(Y)$ to $\Bbbk(X)$. □

Example 5.5.25. Consider the rational maps from Example 5.5.16. The map $\phi(x, y) = (x, x)$ is not dominant and does not induce a well-defined function from $\Bbbk(x, y)$ to $\Bbbk(x, y)$ since, for example, $\phi^*(1/(x - y)) = 1/(x - x) = 1/0$.

The map $\phi(x, y) = (x, xy)$ is dominant and $\phi^*(f(x, y)) = f(x, xy)$ is a field isomorphism.

[7] Pullback is just a fancy name for "composition"; but we think of it as "pulling" a structure from the image of ϕ back to the domain.

Exercise 5.5.26. Let K_1, K_2 be fields containing a field $\Bbbk$. Let $\theta : K_1 \to K_2$ be a $\Bbbk$-algebra homomorphism. Show that θ is injective.

Theorem 5.5.27. *Let X and Y be varieties over $\Bbbk$ and let $\theta : \Bbbk(Y) \to \Bbbk(X)$ be a $\Bbbk$-algebra homomorphism. Then θ induces a dominant rational map $\phi : X \to Y$ defined over $\Bbbk$.*

Proof: If Y is projective it suffices to construct a rational map to an affine part, say $Y \cap \mathbb{A}^n$. Hence, we assume that $Y \subseteq \mathbb{A}^n$ is affine and described by coordinates $(y_1, \ldots, y_n)$.

The homomorphism θ maps each y_i to some $\phi_i(\underline{x}) \in \Bbbk(X)$ for $1 \leq i \leq n$. Define $\phi : X \to \mathbb{A}^n$ by

$$\phi(P) = (\phi_1(P), \ldots, \phi_n(P)).$$

We now show that if $P \in X(\overline{\Bbbk})$ and if ϕ is regular at P then $\phi(P) \in Y(\overline{\Bbbk})$. Let $f \in I(Y)$. Then

$$f(\phi(P)) = f(\phi_1(P), \ldots, \phi_n(P)) = f(\theta(y_1)(P), \ldots, \theta(y_n)(P)).$$

Now, θ is a $\Bbbk$-algebra homomorphism and f is a polynomial in $\Bbbk[y_1, \ldots, y_n]$. Hence

$$f(\theta(y_1), \ldots, \theta(y_n)) = \theta(f(y_1, \ldots, y_n)).$$

Since $f(y_1, \ldots, y_n) \in I(Y)$ it follows that $f(y_1, \ldots, y_n) = 0$ in $\Bbbk(Y)$ and so $\theta(f) = 0$. It follows that $f(\phi(P)) = \theta(f)(P) = \theta(0)(P) = 0$ for all $f \in I(Y)$ and so $P \in Y(\overline{\Bbbk})$ by part 5 of Proposition 5.1.16.

Finally, by Exercise 5.5.26, θ is injective. Also, ϕ^* equals θ and so ϕ^* is injective. Hence, Lemma 5.5.22 implies that ϕ is dominant. □

Theorem 5.5.28. *Let X and Y be varieties over $\Bbbk$. Then X and Y are birationally equivalent over $\Bbbk$ if and only if $\Bbbk(X) \cong \Bbbk(Y)$ (isomorphic as fields).*

Proof: Let $\phi : X \to Y$ and $\psi : Y \to X$ be the birational equivalence. First we must deduce that ϕ and ψ are dominating. There are subsets $U \subseteq X$ and $V \subseteq Y$ such that ϕ is regular on U, ψ is regular on V and $\psi \circ \phi$ is the identity on U (in other words, $\phi : U \to V$ is an isomorphism). The maps $\phi^* : \overline{\Bbbk}[V] \to \mathcal{O}(U)$ and $\psi^* : \overline{\Bbbk}[X] \to \mathcal{O}(V)$ therefore satisfy $\phi^*\psi^*(f) = f \circ (\psi \circ \psi) = f$ (at least, they are equal on $U \cap \phi^{-1}(V)$, which can be shown to be open) and so are injective. It follows from Lemma 5.5.22 that ϕ and ψ are dominant.

Hence, ϕ induces a $\Bbbk$-algebra homomorphism $\phi^* : \Bbbk(Y) \to \Bbbk(X)$ and ψ induces a $\Bbbk$-algebra homomorphism $\phi^* : \Bbbk(X) \to \Bbbk(Y)$. Finally, $\psi \circ \phi$ induces a $\Bbbk$-algebra homomorphism $\phi^*\psi^* : \Bbbk(X) \to \Bbbk(X)$ that is the identity (since it is the identity on a dense open set). It follows that ψ^* and ϕ^* are isomorphisms.

For the converse, if $\theta : \Bbbk(Y) \to \Bbbk(X)$ is an isomorphism then we associate a dominant rational map $\phi : X \to Y$ to θ and $\psi : Y \to X$ to θ^{-1}. Since $\theta^{-1}\theta$ is the identity it follows that $\psi \circ \phi$ is the identity whenever it is regular. □

Some authors prefer to study function fields rather than varieties, especially in the case of dimension 1 (there are notable classical texts that take this point of view by Chevalley and Deuring; see Stichtenoth [589] for a more recent version). By Theorem 5.5.28 (and other results) the study of function fields up to isomorphism is the study of varieties up to birational equivalence. A specific set of equations to describe a variety is called a **model**.

Definition 5.5.29. Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a rational map over $\overline{\Bbbk}$ given by $\phi(P) = (\phi_1(P), \ldots, \phi_n(P))$ if Y is affine and $(\phi_0(P) : \cdots : \phi_n(P))$ if Y is projective. Let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Define $\sigma(\phi) : X \to Y$ by $\sigma(\phi)(P) = (\sigma(\phi_1)(P), \ldots, \sigma(\phi_n(P)))$ if Y is affine and $\sigma(\phi)(P) = (\sigma(\phi_0)(P) : \cdots : \sigma(\phi_n(P)))$ if Y is projective. Many authors act by Galois on the right and so write the action as ϕ^σ.

Lemma 5.5.30. *Let X and Y be varieties over $\Bbbk$ and let $\phi : X \to Y$ be a rational map over $\overline{\Bbbk}$. If $\sigma(\phi) = \phi$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ then ϕ is defined over $\Bbbk$.*

Proof: If Y is affine then $\phi(P) = (\phi_1(P), \ldots, \phi_n(P))$ where $\phi_i \in \overline{\Bbbk}(X)$. If $\sigma(\phi) = \phi$ then $\sigma(\phi_i) = \phi_i$ for all $1 \leq i \leq n$. Remark 5.4.14 therefore implies that $\phi_i \in \Bbbk(X)$ for all i and so ϕ is defined over $\Bbbk$.

If Y is projective then $\phi(P) = (\phi_0(P) : \cdots : \phi_n(P))$ where $\phi_i \in \overline{\Bbbk}(X)$ for $0 \leq i \leq n$. If $\phi(P) = \sigma(\phi)(P)$ then, for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$, there is some $xi(\sigma) \in \overline{\Bbbk}^*$ such that $\sigma(\phi_i) = \xi(\sigma)\phi_i$ for all $0 \leq i \leq n$. As in Lemma 5.2.5, $\xi : \mathrm{Gal}(\overline{\Bbbk}/\Bbbk) \to \overline{\Bbbk}^*$ is a 1-cocycle and so by Hilbert 90 is a co-boundary. It follows that one can choose the ϕ_i so that $\sigma(\phi_i) = \phi_i$ and hence, by Remark 5.4.14, $\phi_i \in \Bbbk(X)$ for $0 \leq i \leq n$. □

5.6 Dimension

The natural notion of dimension (a point has dimension 0, a line has dimension 1, a plane has dimension 2, etc) generalises to algebraic varieties. There are algebraic and topological ways to define dimension. We use an algebraic approach.[8]

We stress that the notion of dimension only applies to irreducible algebraic sets. For example $X = V(x, y) \cup V(x-1) = V(x(x-1), y(x-1)) \subseteq \mathbb{A}^2$ is the union of a point and a line so has components of different dimension.

Recall the notion of transcendence degree of an extension $\Bbbk(X)$ over $\Bbbk$ from Definition A.6.3.

Definition 5.6.1. Let X be a variety over $\Bbbk$. The **dimension** of X, denoted $\dim(X)$, is the transcendence degree of $\Bbbk(X)$ over $\Bbbk$.

Example 5.6.2. The dimension of $\mathbb{A}^n$ is n. The dimension of $\mathbb{P}^n$ is n.

Theorem 5.6.3. *Let X and Y be varieties. If X and Y are birationally equivalent then $\dim(X) = \dim(Y)$.*

Proof: Immediate from Theorem 5.5.28. □

Corollary 5.6.4. *Let X be a projective variety such that $X \cap \mathbb{A}^n$ is non-empty. Then $\dim(X) = \dim(X \cap \mathbb{A}^n)$. Let X be an affine variety. Then $\dim(X) = \dim\left(\overline{X}\right)$.*

Exercise 5.6.5. Let f be a non-constant polynomial and let $X = V(f)$ be a variety in $\mathbb{A}^n$. Show that $\dim(X) = n - 1$.

Exercise 5.6.6. Show that if X is a non-empty variety of dimension zero then $X = \{P\}$ is a single point.

An useful alternative formulation of dimension is as follows.

Definition 5.6.7. Let R be a ring. The **Krull dimension** of R is the supremum of $n \in \mathbb{Z}_{\geq 0}$ such that there exists a chain $I_0 \subset I_1 \subset \cdots \subset I_n$ of prime R-ideals such that $I_{j-1} \neq I_j$ for $1 \leq j \leq n$.

Theorem 5.6.8. *Let X be an affine variety over $\Bbbk$. Then $\dim(X)$ is equal to the Krull dimension of the affine coordinate ring $\Bbbk[X]$.*

Proof: See Proposition I.1.7 and Theorem I.1.8A of [278]. □

[8] See Chapter 8 of Eisenbud [191] for a clear criticism of this approach.

Corollary 5.6.9. *Let X and Y be affine varieties over $\Bbbk$ such that Y is a proper subset of X. Then* $\dim(Y) < \dim(X)$.

Proof: Since $Y \neq X$ we have $I_{\Bbbk}(X) \subsetneq I_{\Bbbk}(Y)$ and both ideals are prime since X and Y are irreducible. It follows that the Krull dimension of $\Bbbk[X]$ is at least one more than the Krull dimension of $\Bbbk[Y]$. □

Exercise 5.6.10. Show that a proper closed subset of a variety of dimension 1 is finite.

5.7 Weil Restriction of Scalars

Weil restriction of scalars is simply the process of re-writing a system of polynomial equations over a finite algebraic extension $\Bbbk'/\Bbbk$ as a system of equations in more variables over $\Bbbk$. The canonical example is identifying the complex numbers $\mathbb{A}^1(\mathbb{C})$ with $\mathbb{A}^2(\mathbb{R})$ via $z = x + iy \in \mathbb{A}^1(\mathbb{C}) \mapsto (x, y) \in \mathbb{A}^2(\mathbb{R})$. We only need to introduce this concept in the special case of affine algebraic sets over finite fields.

Lemma 5.7.1. *Let q be a prime power, $m \in \mathbb{N}$ and fix a vector space basis $\{\theta_1, \ldots, \theta_m\}$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $x_1, \ldots, x_n$ be coordinates for $\mathbb{A}^n$ and let $y_{1,1}, \ldots, y_{1,m}, \ldots, y_{n,1}, \ldots, y_{n,m}$ be coordinates for $\mathbb{A}^{nm}$. The map $\phi : \mathbb{A}^{nm} \to \mathbb{A}^n$ given by*

$$\phi(y_{1,1}, \ldots, y_{n,m}) = (y_{1,1}\theta_1 + \cdots + y_{1,m}\theta_m, y_{2,1}\theta_1 + \cdots + y_{2,m}\theta_m, \ldots, y_{n,1}\theta_1 + \cdots + y_{n,m}\theta_m)$$

gives a bijection between $\mathbb{A}^{nm}(\mathbb{F}_q)$ and $\mathbb{A}^n(\mathbb{F}_{q^m})$.

Exercise 5.7.2. Prove Lemma 5.7.1.

Definition 5.7.3. Let $X = V(S) \subseteq \mathbb{A}^n$ be an affine algebraic set over $\mathbb{F}_{q^m}$. Let ϕ be as in Lemma 5.7.1. For each polynomial $f(x_1, \ldots, x_n) \in S \subseteq \mathbb{F}_{q^m}[x_1, \ldots, x_n]$ write

$$\phi^*(f) = f \circ \phi = f(y_{1,1}\theta_1 + \cdots + y_{1,m}\theta_m, y_{2,1}\theta_1 + \cdots + y_{2,m}\theta_m, \ldots, y_{n,1}\theta_1 + \cdots + y_{n,m}\theta_m) \tag{5.3}$$

as

$$f_1(y_{1,1}, \ldots, y_{n,m})\theta_1 + f_2(y_{1,1}, \ldots, y_{n,m})\theta_2 + \cdots + f_m(y_{1,1}, \ldots, y_{n,m})\theta_m \tag{5.4}$$

where each $f_j \in \mathbb{F}_q[y_{1,1}, \ldots, y_{n,m}]$. Define $S' \subseteq \mathbb{F}_q[y_{1,1}, \ldots, y_{n,m}]$ to be the set of all such polynomials f_j over all $f \in S$. The **Weil restriction of scalars** of X with respect to $\mathbb{F}_{q^m}/\mathbb{F}_q$ is the affine algebraic set $Y \subseteq \mathbb{A}^{mn}$ defined by

$$Y = V(S').$$

Example 5.7.4. Let $p \equiv 3 \pmod 4$ and define $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ where $i^2 = -1$. Consider the algebraic set $X = V(x_1x_2 - 1) \subseteq \mathbb{A}^2$. The Weil restriction of scalars of X with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$ with basis $\{1, i\}$ is

$$Y = V(y_{1,1}y_{2,1} - y_{1,2}y_{2,2} - 1, y_{1,1}y_{2,2} + y_{1,2}y_{2,1}) \subseteq \mathbb{A}^4.$$

Recall from Example 5.1.5 that X is an algebraic group. The multiplication operation $\text{mult}((x_1, x_2), (x_1', x_2')) = (x_1x_1', x_2x_2')$ on X corresponds to the operation

$$\begin{gathered}\text{mult}((y_{1,1}, y_{1,2}, y_{2,1}, y_{2,2}), (y_{1,1}', y_{1,2}', y_{2,1}', y_{2,2}')) \\ = (y_{1,1}y_{1,1}' - y_{1,2}y_{1,2}', y_{1,1}y_{1,2}' + y_{1,2}y_{1,1}', y_{2,1}y_{2,1}' - y_{2,2}y_{2,2}', y_{2,1}y_{2,2}' + y_{2,2}y_{2,1}')\end{gathered}$$

on Y.

Exercise 5.7.5. Let $p \equiv 3 \pmod 4$. Write down the Weil restriction of scalars of $X = V(x^2 - 2i) \subset \mathbb{A}^1$ with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$.

Exercise 5.7.6. Let $p \equiv 3 \pmod 4$. Write down the Weil restriction of scalars of $V(x_1^2 + x_2^2 - (1 + 2i)) \subset \mathbb{A}^2$ with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$.

Theorem 5.7.7. *Let $X \subseteq \mathbb{A}^n$ be an affine algebraic set over $\mathbb{F}_{q^m}$. Let $Y \subseteq \mathbb{A}^{mn}$ be the Weil restriction of X. Let $k \in \mathbb{N}$ be coprime to m. Then there is a bijection between $X(\mathbb{F}_{q^{mk}})$ and $Y(\mathbb{F}_{q^k})$.*

Proof: When $\gcd(k, m) = 1$ it is easily checked that the map ϕ of Lemma 5.7.1 gives a a one-to-one correspondence between $\mathbb{A}^{nm}(\mathbb{F}_{q^k})$ and $\mathbb{A}^n(\mathbb{F}_{q^{mk}})$.

Now, let $P = (x_1, \ldots, x_n) \in X$ and write $Q = (y_{1,1} \ldots, y_{n,m})$ for the corresponding point in $\mathbb{A}^{mn}$. For any $f \in S$ we have $f(P) = 0$. Writing $f_1, \ldots, f_m$ for the polynomials in equation (5.4) we have

$$f_1(Q)\theta_1 + f_2(Q)\theta_2 + \cdots + f_m(Q)\theta_m = 0.$$

Since $\{\theta_1, \ldots, \theta_m\}$ is also a vector space basis for $\mathbb{F}_{q^{mk}}$ over $\mathbb{F}_{q^k}$ we have

$$f_1(Q) = f_2(Q) = \cdots = f_m(Q) = 0.$$

Hence $f(Q) = 0$ for all $f \in S'$ and so $Q \in Y$. Similarly, if $Q \in Y$ then $f_j(Q) = 0$ for all such f_j and so $f(P) = 0$ for all $f \in S$. □

Note that, as the following example indicates, when k is not coprime to m then $X(\mathbb{F}_{q^{mk}})$ is not usually in one-to-one correspondence with $Y(\mathbb{F}_{q^k})$.

Exercise 5.7.8. Consider the algebraic set X from Exercise 5.7.5. Show that $X(\mathbb{F}_{p^4}) = \{1 + i, -1 - i\}$. Let Y be the Weil restriction of X with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$. Show that $Y(\mathbb{F}_{p^2}) = \{(1, 1), (-1, -1), (i, -i), (-i, i)\}$.

Note that the Weil restriction of $\mathbb{P}^n$ with respect to $\mathbb{F}_{q^m}/\mathbb{F}_q$ is not the projective closure of $\mathbb{A}^{mn}$. For example, considering the case $n = 1$, $\mathbb{P}^1$ has one point not contained in $\mathbb{A}^1$, whereas the projective closure of $\mathbb{A}^m$ has an $(m - 1)$-dimensional algebraic set of points at infinity.

Exercise 5.7.9. Recall from Exercise 5.5.14 that there is a morphism from $\mathbb{P}^1$ to $Y = V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$. Determine the Weil restriction of scalars of Y with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$. It makes sense to call this algebraic set the Weil restriction of $\mathbb{P}^1$ with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$.