Draft: March 9, 2014

# INTRODUCTION TO ALGEBRAIC GEOMETRY

MATTHEW EMERTON

Contents



## 1. Introduction and overview

Algebraic geometry is a continuation of what is sometimes called *analytic geometry*, or *coordinate geometry*, in high school, a subject which I guess goes back (at least) to Descartes, Fermat, and others of their era, who introduced algebraic methods and the use of coordinates into the study of geometric questions.

The basic objects of investigation in algebraic geometry are so-called *algebraic varieties*,[1] which are (roughly speaking) the geometric point-sets that can be cut out by systems of algebraic equations.

Despite its name, there are various approaches to algebraic geometry, some more algebraic than others. In what is perhaps the most algebraic approach, a large amount of commutative algebra is developed in advance, and this is then applied to deduce geometric facts. This approach is powerful, but can feel somewhat unmotivated for a beginner, since various simple geometric ideas can become hidden in the commutative algebra formalism.

There is also a more analytic approach, which focuses on the case of algebraic varieties over $\mathbb{C}$, and uses analytic as well as algebraic tools. Certainly the use of analytic tools (sometimes called *transcendental methods* in this context, to distinguish them from purely algebraic methods that, at least in principle, can work over arbitrary ground fields) adds power, and can be illuminating. (As one example of

[1]The word *variety* here is akin to the word *manifold*; it just indicates that we have a collection of points bound together in some geometric way. Note e.g. that in French, *variété* is in fact the word used for what is called a manifold in English.

such illumination, the use of formal completion methods in commutative algebra and its geometric applications is motivated by complex analytic ideas.)

Nevertheless, there is an appeal to using purely algebraic methods to investigate objects that are defined in purely algebraic terms (although probably one shouldn't be too doctrinaire on this point), and for a number theorist interested in using algebraic geometry to study Diophantine equations over number fields (or local fields, of finite fields), algebraic methods are indispensible in any case.

In these notes we use algebraic methods (with a few remarks in the context of algebraic varieties over the real and complex numbers indicating how the ideas we introduce interact with more analytic and topological ideas). However, we have tried to keep the presentation as geometric as possible, with an emphasis on simple ideas in projective geometry, such as projection to linear subspaces, dimension counting, and so on. One side-effect of this approach is that we don't develop terribly much commutative algebra; this can be regarded as either positive or negative, depending on one's predilections. Another is that we don't begin immediately with the Nullstellensatz for arbitrary algebraically closed fields, but only prove this after developing a reasonable amount of projective geometry. This necessitates the consideration of solutions in a universal domain in the meantime, which adds a layer of complication to our basic set-up which may not be of universal appeal.[2] Hopefully the advantages of our rather direct geometric perspecive provide some compensation for its short-comings.

1.1. **Conventions.** Unless otherwise stated, all rings are assumed to be commutative with 1. A *field* is a non-zero ring in which every non-zero element is invertible. An integral domain, or simply a domain, is a non-zero ring containing no non-zero zero-divisors; equivalently, an integral domain is a ring that may be embedded into a field. (One direction is clear; the other direction uses the construction of the field of fractions.)

An ideal $I$ in a ring $A$ is *prime* if $A/I$ is an integral domain, and *maximal* if $A/I$ is a field. Equivalently, a prime ideal in $A$ is the kernel of a homomorphism from $A$ to a field, and a maximal ideal is the kernel of a homomorphism from $A$ *onto* a field.

Note that, by definition, prime and maximal ideals are proper (i.e. not equal to all of $A$).

## 2. Affine space

If $k$ is a field, we let $\mathbb{A}^n(k)$ denote the set $k^n$. We typically label the coordinates by $x_1, \dots, x_n$.

All the concepts we study will be invariant under *affine linear* coordinate changes, i.e. coordinates changes of the form $x_i \mapsto \sum_{j=1}^n a_{ij}x_j + b_i$, where $(a_{ij})$ is an element of $\mathrm{GL}_n(k)$ (i.e. an invertible $n \times n$ matrix with entries in $k$) and $(b_1, \dots, b_n) \in k^n$.

2.1. **Polynomials as functions on affine space.** We let $k[x_1, \dots, x_n]$ denote the polynomial ring in the variables $x_1, \dots, x_n$. The elements of $k[x_1, \dots, x_n]$ induce functions on $\mathbb{A}^n(k)$ in the obvious way (substitute the coordinates of a point into the variables of the polynomial). In this way we can think of $k[x_1, \dots, x_n]$ as a ring of functions on $\mathbb{A}^n(k)$.

[2] In defense of this point of view, one can note that the idea of studying Diophantine equations over $\mathbb{Q}$ by first considering the space of solutions over $\mathbb{C}$ is a rather natural one.

Actually, we have to be a little careful on this point. A more precise statement is the evaluating polynomials on points gives a *homomorphism* from $k[x_1, \ldots, x_n]$ to the ring of $k$-valued functions on $\mathbb{A}^n(k)$, but this homomorphism is *not always* injective.

2.1.1. **Example.** If $k$ is finite of order $q$, then $x^q - x$ vanishes identically on $k$, and so each of the polynomials $x_i^q - x_i$ vanishes identically on $\mathbb{A}^n(k)$, although they are certainly a non-zero polynomials. Thus in this case the homomorphism from $k[x_1, \ldots, x_n]$ to functions on $\mathbb{A}^n$ is not injective.

We will see in Lemma 6.3.3 below that this homomorphism *is* injective if $k$ is infinite.

If $f \in k[x_1, \ldots, x_n]$ is non-zero, we define the degree of $f$ to be the maximal degree of all the monomials appearing with a non-zero coefficient in $f$.

Note that affine linear coordinate changes induces automorphisms of the $k$-algebra $k[x_1, \ldots, x_n]$, and leave the degree of a polynomial unchanged.

2.2. **Linear subspaces.** One of the basic structures we can consider in affine space is its collection of *linear subspaces*. A *linear subspace* of $\mathbb{A}^n(k) = k^n$ is a subset of $k^n$ that is a translate by some element of $k^n$ of a vector subspace of $k^n$, i.e. a subset of the form $V + x$ for some vector subspace $V$ and some element $x \in k^n$.

The collection of linear subspaces of $\mathbb{A}^n(k)$ is preserved under affine linear coordinate changes.

2.3. **Affine algebraic sets (first naive definition).** In naive terms, an algebraic subset of $\mathbb{A}^n$ is a locus of points cut out by a collection of polynomial equations. For example, the conic sections, or *conics*, cut out by equations of the form

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

are examples of algebraic sets.

We will postpone our formal definition of algebraic set, since we will first provide some motivation by remarking on the short-comings of this naive definition.

2.3.1. **Example.** If $k = \mathbb{R}$, and we consider the conic $x^2 + y^2 = 0$, then the only solutions in $\mathbb{R}^2$ are $(x, y) = (0, 0)$, although naively one might expect that a single equation in two variables should cut out a curve.

2.3.2. **Example.** If $k = \mathbb{R}$, and we consider the conic $x^2 + y^2 + 1 = 0$, then the set of solutions in $\mathbb{R}^2$ is empty.

Before introducing a formal definition of algebraic set in general, we will discuss a particular case which is concrete and requires little theory, but is nevertheless illustrative of many general feautres of the theory, namely the case of *plane curves*.

## 3. Affine plane curves

We focus on the case $n = 2$. Rather than writing $k[x_1, x_2]$, we will follow standard convention and write $k[x, y]$ for the polynomial ring in two variables.

## 3.1. **The basic definitions.**

3.1.1. **Definition.** *We define an* affine plane curve *to be a non-constant polynomial $f \in k[x, y]$, thought of modulo scaling by non-zero elements of $k^\times$.*

So an affine plane curve is given by a non-contant poylnomial $f(x, y)$, and we think of two polynomials as giving the same curve if they differ by a scalar.

We will often denote a curve (we will typically drop the adjectives *affine* and *plane* in this section, since they are always implied) by $C$, and refer to (one of) the equation(s) $f$ that gives rise to it as the, or an, equation of $C$.

3.1.2. **Remark.** This definition, notation, and terminology may seem a little odd, since according to our definition $C$ is *nothing but* $f$ (thought of up to non-zero scaling). However, we ulimately want to think of a curve as being something geometric, while the equation cutting it out is something algebraic, and so we introduce notation that emphasizes this. Of course, for this to have any content, we have to introduce more concepts related to curves, and we begin to do so.

3.1.3. **Definition.** If $f$ is an equation of the curve $C$, we write $C(k) := \{(x, y) \in \mathbb{A}^2(k) \,|\, f(x, y) = 0\}$, and call this the set of $k$-valued points (or sometimes simply the set of $k$-points) of the curve $C$. More generally, if $K$ is any extension field of $k$, we write $C(K) := \{(x, y) \in \mathbb{A}^2(K) \,|\, f(x, y) = 0\}$. (Note that these sets are well-defined independently of the non-zero scalar ambiguity that is inherent in the choice of $f$.)

This definition captures our intuition about what a plane curve should be: it should be the set of points cut out by an equation $f(x, y) = 0$ in the plane.

However, as we saw in the examples above, for some choices of $k$ and $C$, the set $C(k)$ can be a single point, or even empty! Thus we don't want to define the curve $C$ to be the set $C(k)$ itself. We want the curve to be something which exists and is interesting even if its set of $k$-points is very uninteresting (e.g. ). As the above definition suggests, we want to be able to consider the points of the curve not just over $k$, but over extensions of $k$. The most expedient way to achieve these aims is just to take the curve to be its equation (working modulo non-zero scalars, since obviosly multiplying $f$ by a scalar doesn't change its zero locus over any extension of $k$).

Later, we will prove the Nullstellensatz, which will show that the curve $C$ is essentially[3] determined by knowing the sets $C(K)$ for all extension $K$ of $C$ (or even just by knowing the set $C(K)$ for any one algebraically closed extension of $k$).

## 3.2. **Examples of plane curves — lines and conics.**

3.2.1. **Example.** Any linear (i.e. degree 1) polynomial is of the form $ax + by + c$, where $(a, b) \neq (0, 0)$. We call the corresponding degree 1 curves *lines*.

Note that then $C(k)$ is just a one-dimensional linear subspace of $\mathbb{A}^2(k)$. In this case, one easily verifies (just by choosing two distinct points on the line) that $C(k)$ determines $C$ (i.e. determines the polynomial $ax + by + c$ up to a non-zero scalar).

[3] I write "essentially" because in fact knowing $C(K)$ for all extensions $K$, or even one algebraically closed extension $K$, allows us to determine the irreducible factors of an equation for $C$, but not the powers with respect to which those factors appear in the equation.

3.2.2. **Example.** We call degree two plane curves *conics*.

Suppose that $k$ is algebraically closed, so that $C(k)$ contains a point. We may make an affine change of coordinates so that this point is the origin $(0,0)$, and then the equation for $C$ has the form $f(x,y) = l_1 + l_2 l_3$, where the $l_i$ are homogeneous linear polynomials in $x$ and $y$. (It is in obtaining the factorization of the quadratic terms that we use the assumption that $k$ is algebraically closed.)

Note that neither $l_2$ nor $l_3$ can vanish (otherwise $f$ wouldn't have degree 2), but $l_1$ may. Note also that we may find an affine change of coordinates that takes any two distinct lines to the standard coordinate lines ($x = 0$ and $y = 0$).

Using the preceding remarks, and considering the various possibilities for coincidences among the $l_i$, we find that (after an affine linear change of coordinates) $f(x,y)$ can be of five basic forms: $xy-1$, $x^2-y$, $xy$, $x(x-1)$, $x^2$. We refer to these as a *hyperbola*, a *parabola*, *two lines crossing*, *two parallel lines*, and a *double line*.

Thanks to Sachi Hashimoto for pointing out that the case of parallel lines was omitted from an earlier draft.

3.2.3. **Example.** If $k = \mathbb{R}$, then there are further possibilities for conics, because the quadratic term in $f$ may not be factorizable. In this case it can be reduced to $x^2 + y^2$ by a linear change of coordinates, and we find the following additional possible conics (up to affine change of coordinates): $x^2+y^2+1$ (whose real points are empty, as we've seen), $x^2+y^2$ (whose real points are a single point), and $x^2+y^2-1$ (whose real points are an *ellipse*[4]).

Note that if we consider the complex points of these real conics, then the empty case, and the case of the ellipse, both merge with the case of a hyperbola, while the case of a single point becomes that of two lines crossing (with the single point being the crossing point of the two lines).

3.3. **Tangents and smoothness.** Let $C$ be a plane curve with equation $f$, and suppose that $(0,0)$ lies in $C(k)$, i.e. that $f(0,0) = 0$. This just says that $f$ has no constant term, and so we may write $f = f_1 + \ldots + f_d$, where each $f_i$ a homogeneous polynomial of degree $i$, and $f_d \neq 0$ (so that $d$ equals the degree of $f$).

3.3.1. **Definition.** We say that $C$ is *non-singular*, or *smooth*, at $(0,0)$, or that $(0,0)$ is a *smooth point* of $C$, if $f_1 \neq 0$. In this case we say that the line with equation $f_1$ is the *tangent line* to $C$ at $(0,0)$.

If $f_1 = 0$ we say that $C$ is *singular* at $(0,0)$.

Since any point may be taken to the origin by an affine linear coordinate change (indeed, by a translation), this definition may be applied to any point $(x_0, y_0) \in C(k)$, by changing coordinates so that $(x,y)$ becomes the origin.

The following lemma gives another description of smoothness and the the tangent line, which doesn't require moving the point to the origin.

3.3.2. **Lemma.** *A point $(x_0,y_0) \in C(k)$ is a smooth point of $C$ if at least one of the partial derivatives $\dfrac{\partial f}{\partial x}$ or $\dfrac{\partial f}{\partial y}$ is non-zero at $(x_0,y_0)$. If this holds, then the equation for the tangent line to $C$ at $(x_0,y_0)$ is $ax + yb + c$, where*

$$a = \frac{\partial f}{\partial x}(x_0,y_0), \quad b = \frac{\partial f}{\partial y}(x_0,y_0), \text{ and } c = -\Big(\frac{\partial f}{\partial x}(x_0,y_0)x_0 + \frac{\partial f}{\partial y}(x_0,y_0)y_0\Big).$$

*Proof.* This is more-or-less immediate when $(x_0,y_0) = (0,0)$, and is easily checked in general just by making a translation that moves $(x_0,y_0)$ to $(0,0)$. □

[4]We say *ellipse*, rather than *circle*, because the former notion is invariant under affine linear coordinate changes, while the latter is not.

3.3.3. **Remark.** The lemma shows that the singular points on a plane curve $C$ with equation $f$ are the solutions to *three* simultaneous equations: $f = \dfrac{\partial f}{\partial x} = \dfrac{\partial f}{\partial y} = 0$. This allows one to compute them in practice; it also suggests that they should be fairly uncommon. (Morally, the plane has dimension two, and each equation typically cuts down the dimension by one; so typically we might expect every point to be non-singular. Later, we will make this kind of argument precise.)

The following discussion relates the tangent line to a plane curve at a smooth point, as we have defined it above, to traditional idea that a tangent line to a curve is one which should intersect the curve with "multiplicity $> 1$".

We begin by defining the intersection multiplicity of a curve and a line at a point that is common to both.

3.3.4. **Definition.** Let $C$ be a plane curve, and let $\ell$ be a line, and let $P \in C(k) \cap \ell(k)$ be a point of $\mathbb{A}^2(k)$ lying on both $C$ and $\ell$. Assume that $\ell \not\subseteq C$ (i.e. that the equation of $\ell$ does not divide the equation of $C$). Choose coordinates so that $\ell$ is cut out by $y = 0$, and that $P = (0, 0)$. If $\overline{f}(x)$ denotes the image of $f$ under the homomorphism $k[x, y] \to k[x]$ defined by $y \mapsto 0$, then we define the multiplicity of the intersection of $C$ and $\ell$ at $P$ to be the multiplicity of $x = 0$ as a root of $\overline{f}$.

3.3.5. **Remark.** Note that since $(0, 0)$ is a point on $C$ by assumption, it is the case that $x = 0$ is a root of $\overline{f}$. Since $\ell \not\subseteq C$, again by assumption, we see that $\overline{f} \neq 0$. Thus the multiplicity of intersection is finite and positive.

3.3.6. **Remark.** There is nothing important about our choosing coordinates so that $P = (0, 0)$ and $\ell = y$; this is just a convenient convention that allows us to give a concrete definition. One could make a more intrinsic definition as follows: if we let $\ell$ also denote an equation of $\ell$, and write $A := k[x, y]/(\ell)$ (the quotient of the polynomial ring by the principal ideal generated by $\ell$), and write $P = (a, b)$, then the $k$-algebra $A$ is isomorphic to a polynomial ring in one variable over $k$, and the image of $(x - a, y - b)$ in $A$ is a non-zero prime ideal, which we denote $\mathfrak{p}$. If we let $\overline{f}$ denote the image of $f$ in $A$ under the canonical surjection, then the multiplicity of intersection of $\ell$ and $C$ at $P$ is equal to the maximal power of $\mathfrak{p}$ that divides $(\overline{f})$. (This is easily verified. Indeed, the change of coordinates in that we imposed in Definition 3.3.4 just makes it easy to see that $A$ is a polynomial ring (we identify it with $k[x]$), and gives a concrete description of $\mathfrak{p}$ (as the ideal generated by $x$).)

3.3.7. **Lemma.** *If $C$ is a plane curve, and $P$ is a point in $C(k)$, then $C$ is smooth at $P$ if and only if there exists a line $\ell$ in $\mathbb{A}^2$ such that the intersection multiplicity of $\ell$ and $C$ at $P$ equals* 1. *In this case, the intersection multiplicity equals* 1 *for* every *line $\ell$ passing through $P$,* except *for the tangent line at $P$, whose intersection multiplicity with $C$ at $P$ is $\geq 2$.*

*Proof.* We may change coordinates so that $P = (0, 0)$ and $\ell$ is given by $y = 0$, and write $f = f_1 + \cdots + f_d$ as the sum of its homogeneous parts. Then, setting $y = 0$, we obtain $\overline{f} = \overline{f}_1 + \cdots + \overline{f}_d \in k[x]$, and we see that the intersection multiplicity is 1 precisely if $\overline{f}_1 \neq 0$.

If $f_1 = 0$ then of course this is not possible. Hence if $P$ is not a smooth point, the intersection multiplicity of *any* line with $P$ is $\geq 2$. On the other hand, if $f_1 \neq 0$, so that $C$ *is* smooth at $P$, then we see that $\overline{f}_1 \neq 0$ provided that $f_1$ is not a scalar multiple of $y$, that is (in coordinate free terms) if $\ell$ and the tangent line to $C$ at $P$ don't coincide. □

3.4. **Tangent cones.** We have seen in Lemma 3.3.7 that at a singular point $P$ of a curve $C$, *every* line through $P$ intersects $C$ with multiplicity $> 1$. Still, if one looks at some examples, it is clear that certain lines through $P$ are "more tangent" to $C$ at $P$ than others.

3.4.1. **Example.** Consider the graphs of $y^2 = x^3 + x^2$, $y^2 = x^3$, and also $y^2 = x^3 - x^2$.

Perhaps in a future iteration, when I learn how to add pictures, there will be pictures here ...

We capture this intuition with following definition.

3.4.2. **Definition.** Let $C$ be a curve and $P \in C(k)$. Choose coordinates so that $P = (0, 0)$, and write the equation $f$ of $C$ in the form $f = f_1 + \dots f_d$, where each $f_i$ is homogeneous of degree $i$. Let $m$ be the least value of $i$ such that $f_i \neq 0$ (so that $i = 1$ iff $C$ is smooth at $P$). Then we call the curve with equation $f_m$ the *tangent cone* to $C$ at $P$.

3.4.3. **Remark.** If $k$ is algebraically closed, then $f_m$ factors as a product of $m$ linear factors, and so the tangent cone is a union of lines through $(0, 0)$ (possibly with multiplicities). The reason we call it a *cone* is that such a union of lines is invariant under scaling, and such objects are called cones. (Think about the usual cone $x^2 + y^2 = z^2$ in space.)

## 4. Projective space

4.1. **Basic definitions.** For the moment, these are discussed in Subsection 8.2 below.

4.2. **Linear subspaces of $\mathbb{P}^n$.** Two points spane a uniquely determined line. Three points, not all colinear span a plane. Four points, not all coplanar, span a linear 3-space. Etc.

4.3. **Hyperplanes and the dual projective space.** A codimension one linear subspace of $\mathbb{P}^n$ is called a hyperplane. The equation for a hyperplane in $\mathbb{P}^n$ is of the form

$$a_0 x_0 + \cdots a_n x_n = 0,$$

where not all $a_i$ are zero, and the $a_i$ are determined up to a common non-zero scalar multiple.

So we see that we may regard the hyperplanes in $\mathbb{P}^n$ themselves as the points $[a_0 : \cdots : a_n]$ of an $n$-dimensional projective space which we denote by $(\mathbb{P}^n)^*$, and call the *dual projective space* to $\mathbb{P}^n$.

If we work in a coordinate free fashion, so that $\mathbb{P}^n$ is obtained as the projectiviation of a vector space $V$, then $(\mathbb{P}^n)^*$ is obtained as the projectivization of the dual vector space $V^*$.

If $L \subset \mathbb{P}^n$ is a linear subspace of *dimension* $d$, then the collection of hyperplanes that contain $L$ form a linear subspace $L^*$ of $(\mathbb{P}^n)^*$ of *codimension* $d + 1$.

In invariant form, if $\mathbb{P}^n$ is the projectivization of $V$, and $L$ is obtained from the $d + 1$-dimensional subspace $W \subset V$, then $L^*$ is obtained as the projectivization of $W^\perp \subset V^*$ (the annihilator of $W$ in $V^*$).

## 5. Projective plane curves

5.1. **Lines in $\mathbb{P}^2$.** As a special case of the formation of dual spaces, we remark that the lines in $\mathbb{P}^2$ are parameterized by a space which is itself a projective plane, which we denote by $(\mathbb{P}^2)^*$, and refer to as the *dual projective plane* (to our original plane $\mathbb{P}^2$).

Concretely, the line with equation $aX+bY+cZ$ corresponds to the point $[a : b : c]$.

5.2. **The projective closure of an affine plane curve in $\mathbb{P}^2$.**

5.2.1. **Example.** Consider the parabola $y = x^2$ in $\mathbb{A}^2$. To compute points at infinity, we pass to homogeneous coordinates $x_1x_2 = x_0^2$ and set $x_2 = 0$. The only solution is $x_0 = 0$ (in which case necessarily $x_1 \neq 0$, and so can be scaled to be 1), and so we have a unique point at infinity, namely $[0 : 1 : 0]$.

Thanks to Oishee Banerjee for pointing out a typo here; $x_0$ and $x_1$ had been accidentally switched.

If we pass to the $\mathbb{A}^2$ which is the complement of $x_1 = 0$, with coordinates $u = x/y$ and $v = 1/y$ (so that the point $[0 : 1 : 0]$, which lies at infinity from the perspective of the $(x, y)$-plane, now lies at the origin), then the equation for our curve becomes (after clearing denominators in $v$) $v = u^2$.

In particular it is smooth at the point $(u, v) = (0, 0)$ (which remember is our point at infinity), with tangent line $v = 0$, which is precisely the line $x_2 = 0$, i.e. the line at infinity (from our original perspective).

In summary, the parabola $y = x^2$ has a single point at infinity, and it is tangent to the line at infinity at this point.

5.2.2. **Example.** Consider the hyperbola $xy = 1$ in $\mathbb{A}^2$. To compute points at infinity, we pass to the equation $x_0x_1 = x_2^2$, set $x_2 = 0$, and so find two points at infinity, namely $[0 : 1 : 0]$ and $[1 : 0 : 0]$.

Let's study what happens at the first of these. Just as in the previous example, we pass to the $(u, v)$ plane (the complement of $x_1 = 0$), where our curve becomes $u = v^2$. So again this is a smooth point, but now its tangent line is *not* the point at infinity, but rather is the line $u = 0$, i.e. $x_0 = 0$, which is the line $x = 0$ in our original affine coordinates.

Now $[0 : 1 : 0]$ is precisely the point lying at infinity on this the line $x = 0$, and, looking at the graph of $xy = 1$ we see that $xy = 1$ is asympotic to this line.

Add a picture of this graph some day...

A completely analogous computation shows that $[1 : 0 : 0]$ is also a smooth point, with tangent line $y = 0$, which is the other asymptote of the hyperbola.

In summary, the hyperbola $xy = 1$ has two points at infinity, it is smooth at each of them, and the tangent lines are precisely the two asymptotes of the hyperbola.

5.3. **Dual curves.** If $C$ is a smooth[5] projective plane curve, then at each point $P$ of $C$ (defined over some field $l \supset k$) we have the associated tangent line $t_p$ to $C$ at $P$, which is a point of the dual plane $(\mathbb{P}^2)^*$ (defined over the same field $l$).

If $C$ is a line $\ell$, then of course $t_P = \ell$ for all $P \in \ell(l)$ (and any $l \supset k$), so in this case the collection of $t_P$ in fact consists of a single point. We will exclude this somewhat degenerate case from now on.

5.3.1. **Proposition.** *Suppose that* $\deg C \geq 2$. *There is a curve $C^*$ in $(\mathbb{P}^2)^*$ with the property that, for any algebraically closed field extension $l \supset k$, the set of tangent*

[5]This means that $C$ is smooth at each of its points. More precisely, it is enough to check smoothness at all the points $C(l)$ for some algebraically closed field $l$ containing $k$, e.g. an algebraic closure of $k$; it then follows that $C$ is smooth at every point $P \in C(l)$ for *any* field extension $l$ of $k$. We haven't proved this yet, though.

*lines $t_P$, as $P$ ranges over the points of $C(l)$, is precisely the set $C^*(l)$ of $l$-valued points of $C^*$.*

*Proof.* We consider the affine chart of $(\mathbb{P}^2)^*$ consisting of lines of the form $y = mx + b$, and show that the set of $t_P$ lying in this chart is cut out by a polynomial equation in $m$ and $b$. There are analogous computations for the two other affine charts that, together with this one, cover $(\mathbb{P}^2)^*$.

We have to determine when $y = mx + b$ is of the form $t_P$ for some point $P$ of $C$. To this end, we substitute $Y = mX + bZ$ into the equation $F(X, Y, Z)$ for $C$, and ask whether it has a double root (which is the condition for it to be tangent to at least one of its points of intersection with $C$). The polynomial $f(X, mX + bZ, Z)$, which is homogeneous in the two variables $X$ and $Z$, has a discriminant $\Delta$, which is a polynomial in $m$ and $b$, and which vanishes precisely when $f(X, mX + bZ, Z)$ has a double root. Thus indeed the condition for a line to be of the form $t_P$ is cut out by a polynomial in the coefficients of the equation of the line. □

It's not so clear (to me, at least) how to compute the degree of $C^*$ from the description of its equation given in the preceding argument. However, we can use a slightly different approach to compute its degree.

5.3.2. **Proposition.** *If* $\deg C = d$, *then* $\deg C^* = d(d-1)$.

*Proof.* We will intersect $C^*$ with a typical line in $(\mathbb{P}^2)^*$, and count how many intersection points there are. A line in $(\mathbb{P}^2)^*$ corresponds to a point $P$ in $\mathbb{P}^2$; points on this line correspond to lines through $P$.

So we have to choose a point $P$ in $\mathbb{P}^2$, and count the lines through $P$ that are tangent to $C$. It will be easier if the points at which these lines are tangent do not lie at infinity, so we assume $P$ is chosen so that none of the tangent lines to the points at infinity of $C$ pass through $P$. (Since there are only finitely points at infinity on $C$, there are only finitely many such lines, and so as long as $k$ is infinite, so that $\mathbb{P}^2(k)$ is not the union of finitely many lines, this is possible.)

Now choose coordinates so that $P = (0, 0)$, let $f(x, y)$ be equation for (the affine part of) $C$, and write $f = f_d + f_{d-1} + \cdots + f_0$ as the sum of its homogeneous parts. The requirement that none of the tangent lines to the points through infinity pass through 0 is equivalent to the requirement that $f_{d-1}$ is coprime to $f_d$.

Now $(0, 0)$ lies on the tangent line through a point $(x_0, y_0)$ of $C$ if and only if $x_0 f_x(x_0, y_0) + y_0 f_y(x_0, y_0)$ vanishes, and so we must count the number of solutions to the simultaneous equations

$$f = 0, \qquad x f_x + y f_y = 0,$$

or equivalently

$$f_d + f_{d-1} + \cdots + f_0 = 0, \qquad d \cdot f_d + (d-1) \cdot f_{d-1} + \cdots + f_1 = 0.$$

Now subtracting $d$ times the first equation from the second, we may rewrite these as

$$f_d + f_{d-1} + \cdots + f_0 = 0, \qquad f_{d-1} + 2 \cdot f_{d-2} + \cdots (d-1) \cdot f_1 = 0.$$

Thus we are considering simultaneous equations of degree $d$ and $d-1$, which by Bézout's Theorem (to be proved later) have $d(d-1)$ common solutions. Furthermore, none of these common solutions lie at infinity (since $f_d$ and $f_{d-1}$ are

coprime).[6] Thus we find that there are $d(d-1)$ lines (counted with multiplicity) through $P = (0,0)$ that are tangent to $C$, and so $C^*$ has degree $d(d-1)$. □

5.3.3. **Remark.** If $C$ is a curve with singularities, then one can still define a "dual curve" $C^*$, as the collection of lines which meet $C$ at a point with multiplicity $> 1$. Provided that $C$ contains at least one smooth point (which is true if e.g. $k$ is perfect and $C$ is irreducible), this will in fact yield a curve, and its degree will be $d(d-1)$. However, the resulting curve won't be irreducible. The point is that if $P$ is a singular point on $C$, then *any* line passing through $C$ will have multiplicity $> 1$ at $P$, and so the entire line in $(\mathbb{P}^2)^*$ corresponding to $P$ will lie in $C^*$. In fact, this line will appear in the equation for $C^*$ to some power $> 1$. (For an ordinary node, it will appear with multiplicity two; for an ordinary cusp, with multiplicity three)

For this reason, the dual curve of a singular curve $C$ is usually defined to be the dual curve in the above sense, *but with all the extra multiple lines removed*. The degree of the dual curve is then called the *class* of $C$.

5.3.4. **Remark.** One can show that if $P$ is a point on $C$, and $t_P$ is the tangent line to $C$ at $P$, then the line in $(\mathbb{P}^2)^*$ corresponding to $P$ is tangent to $C^*$ at the point corresponding to $t_P$. Intuitively, this says that the dual curve to the dual curve is the original curve.

This may seem impossible, because the degree of $C^*$ is $d(d-1)$, so how could *its* dual have degree $d$? However, one has to be careful, because it will turn out that (once $d > 2$) that $C^*$ is quite singular. It turns out that the class of $C^*$ (in the sense of the preceding remark) is indeed $d$, and the dual of $C^*$ (again, in the sense of the preceding remark, i.e. after throwing away all extra lines) does coincide with $C$.

5.3.5. **Example.** If $C$ is a smooth cubic curve, then $C^*$ is a degree 6 curve with 9 cusps (corresponding to the 9 inflection points of $C$). The naive dual of $C^*$ (i.e. the set of points in $\mathbb{P}^2$ corresponding to lines in $(\mathbb{P}^2)^*$ that meet $C^*$ with multiplicity $> 1$) is then of degree $30 = 6(6-1)$. However, it contains 9 triple lines, corresponding to the 9 cusps of $C^*$. Once these are removed, we are left with the original cubic curve $C$. (Note that $30 - 9 \cdot 3 = 3$.)

5.4. **The genus of a smooth complex curve.** If $k = \mathbb{C}$ and $C$ is a smooth projective plane curve of degree $d$, then $C(\mathbb{C})$ is a compact connected Riemann surface.

To compute its genus, we can project $C$ from some point $P \notin C$ to a line. This is a degree $d$ morphism, which (by our computation of the degree of the dual curve) has $d(d-1)$ branch points. The Riemann–Hurwitz formula then shows that, if $g$ is the genus of $C(\mathbb{C})$, we have

$$2g - 2 = -2d + d(d-1) = d(d-3),$$

and thus that

$$g = \frac{(d-1)(d-2)}{2}.$$

[6] Incidentally, this shows why we didn't "cheat" when we eliminated the degree term from the second equation. If we had considered the simultaneous solutions of the two original degree $d$ equations (here we are assuming that $d \neq 0$ in $k$, so that $d \cdot f_d$ is a non-zero term), they would have had $d$ spurious common solutions at infinity, and so only $d^2 - d = d(d-1)$ of the solutions would have been meaningful — and these are the $d(d-1)$ solutions we have just introduced.

This is a famous formula, which can be derived in many different ways. If one knows this formula, then one can run the above argument backwards to determine that $\deg C^* = d(d-1)$. (This is the approach taken in *Hartshorne*, for example; see the exercises on pp. 304-5.)

5.5. **The complete linear system of conics.**

A projective plane conic has an equation of the form

$$a_0X^2 + a_1Y^2 + a_2Z^2 + a_3XY + a_4XZ + a_5YZ = 0. \tag{5.5.1}$$

It determines, and is determined by, the point

$$[a_0 : \cdots : a_5] \in \mathbb{P}^5.$$

In other words, the space of conics is a $\mathbb{P}^5$; we call it the *complete linear system* of conics.

Actually, below we will denote this space as $(\mathbb{P}^5)^*$, because we will see that is naturally identified with the dual space to a certain copy of $\mathbb{P}^5$ that contains $\mathbb{P}^2$.

5.5.2. *Base points.* If $P \in \mathbb{P}^2(k)$, we may consider the sublinear system consisting of conics that pass through $P$. An examination of (5.5.1) shows that this imposes a linear condition on the point of $(\mathbb{P}^5)^*$ corresponding to the conic. In other words, each point in $P$ determines a hyperplane on the space of conics; we get a map

$$\mathbb{P}^2(k) \to \mathbb{P}^5(k) \tag{5.5.3}$$

to the dual space of the space of conics. (Since we have taken the space of conics to be $(\mathbb{P}^5)^*$, its dual space is just $\mathbb{P}^5$ itself.) This is called the 2-uple embedding of $\mathbb{P}^2$. The following lemma shows that, among other things, it is an embedding.

5.5.4. **Lemma.** *The map* (5.5.3) *is an embedding.*

*Proof.* We have to show that given two distinct points $P$ and $Q$, we can find a conic passing through one, but not the other. Choose a line $\ell$ passing through $P$ but not through $Q$, and take the conic to be the double line $\ell^2$. □

Note that the hyperplanes in $\mathbb{P}^5$ are precisely the points of $(\mathbb{P}^5)^*$, i.e. the conics. If $H_C$ is the hyperplane corresponding to a conic $C$, then one checks (just chasing through the definitions) that the intersection of $H_C$ with the image of (5.5.3) is precisely (the image under (5.5.3) of) the set of points $C(k)$ of the conic $C$.

In other words, the 2-uple embedding allows us to realize conics in $\mathbb{P}^2$ as being obtained by intersecting (the image of) $\mathbb{P}^2$ with hyperplanes in a higher dimensional projective space (namely $\mathbb{P}^5$).

If $P$ and $Q$ are two distinct points in $\mathbb{P}^2$, then we can consider the sublinear system of conics with base-points at $P$ *and* $Q$, i.e. passing through both $P$ and $Q$. The lemma shows that this is the intersection of two distinct hyperplanes in $(\mathbb{P}^5)^*$, and so is a codimension two linear subspace of $(\mathbb{P}^5)^*$. It is dual, then, to a line in $\mathbb{P}^5$; this is precisely the line joining (the images under (5.5.3) of) $P$ and $Q$ in $\mathbb{P}^5$.

We can similarly impose base-points at three points (and so obtain a plane in $\mathbb{P}^5$ — actually we have to check that these three points can't be colinear; the following proposition does this), and so on. (Once we impose four or more base-points, there are non-trivial conditions to check to make sure that we actually cut down the dimension by one for each extra base-point.)

Write $S$ to denote the image of $\mathbb{P}^2$ under (5.5.3); it is a surface in $\mathbb{P}^5$.[7]

5.5.5. **Proposition.** (1) *If $P$ and $Q$ are distinct points in $S$, then the line joining $P$ and $Q$ contains no other points of $S$ besides $P$ and $Q$.*

(2) *If $P$, $Q$, and $R$ are three distinct points in $S$, let $\Pi$ denote the plane spanned by $P$, $Q$, and $R$. Either* (a) *thought of as a points in $\mathbb{P}^2$, these points are* not *colinear, in which case the plane $\Pi$ meets $S$ in no other point besides $P$, $Q$, and $R$; or* (b) *the points $P$, $Q$, and $R$ are colinear as points in $\mathbb{P}^2$, in which case the intersection of $\Pi$ with $S$ consists precisely of the image under* (5.5.3) *of this line, and this image is a conic in $\Pi$.*

*Proof.* To prove (1), we have to show that given three points, we can find a conic containing the first two but not the third. If the three points are not collinear, take the line through the first two and double it. If they are collinear, take the union of a line through the first not containing the second and a line through the second not containing the first.

To prove (2), we suppose given four points $P$, $Q$, $R$, and $S$, so that any conic containing the first three necessarily contains the fourth. Let $\ell$ be the line joining $P$ and $Q$. If $\ell_1$ is a line through $R$ that misses $S$, then $\ell\ell_1$ is a conic containing $P$, $Q$, and $R$, hence containing $S$. Thus $S$ lies on $\ell$. Interchanging the roles of $Q$ and $R$, we see that the line through $P$ and $R$ also contains $S$. Thus in fact all four points are collinear.

To check that the image of a line under (5.5.3) is a conic, make a direct computation. □

5.5.6. **Theorem.** (1) *If $P$, $Q$, $R$, and $S$ are four points, no three of which are collinear, then the space of conics passing through them forms a line in the $\mathbb{P}^5$ of conics.* (*It is called a* pencil *of conics.*) *It contains exactly three singular conics, each of which consists of two lines crossing.*

(2) *If $P$, $Q$, $R$, $S$, and $T$ are five points in $\mathbb{P}^2$, no three of which are collinear, then there is a unique conic containing them, which is necessarily irreducible* (*and hence smooth*).

*Proof.* Part (2) of the preceding proposition shows that we cut the dimension down by one for each extra base-point.

In the context of (1), we note that the only reducible (= singular) conics that contain the four points are the three different unions of lines that can be obtained by grouping the four points into pairs. □

5.5.7. **Example.** If we take $k = \mathbb{R}$, we see that circles are precisely the conics containing the points $[1 : i : 0]$ and $[1 : -i : 0]$ at infinity, and so we get the classical result that a cirle is uniquely determined by three non-colinear points lying on it.

5.5.8. **Remark.** *Any* pencil of conics arises by imposing four base-points; this follows from Bézout's Theorem (to be proved later). From the fact that there are three singular conics in a pencil, we deduce that the discriminant locus in $\mathbb{P}^5$ has degree 3.

[7]We haven't yet defined what we mean by a surface in $\mathbb{P}^5$, but in this case there are pretty easy explicit equations cutting out $S$, so this shouldn't be too confusing.

## 6. Affine algebraic sets

6.1. **Zeroes of equations and homomorphisms of $k$-algegras.** Let $k$ be a field. If $\Omega$ is an extension field of $k$, and if $a_1, \dots, a_n \in \Omega^n$, then we let

$$\varphi_{a_1,\dots,a_n} : k[x_1, \dots, x_n] \to \Omega$$

denote the homomorphism defined by mapping each $x_i$ to the corresponding $a_i$. Clearly any $k$-algebra homomorphism $\varphi : k[x_1, \dots, x_n] \to \Omega$ is of this form, for some uniquely determined $n$-tuple $a_1, \dots, a_n$. (One has $a_i = \varphi(x_i)$.)

If $f$ is a polynomial over $k$ in the variables $x_1, \dots, x_n$, then $f(a_1, \dots, a_n) = 0$ if and only if $\varphi_{a_1,\dots,a_n}(f) = 0$ if and only if $f \in \ker \varphi_{a_1,\dots,a_n}$. (Both assertions are obvious; indeed, the second is the very definition of the kernel.)

If $f_1, \dots, f_n$ is a collection of polynomials over $k$ in the variables $x_1, \dots, x_n$, and if $I \subseteq k[x_1, \dots, x_n]$ denotes the ideal generated by the $f_i$, then $a_1, \dots, a_n$ is a simultaneous solution of all the $f_i$ if and only if each $f_i \in \ker \varphi_{a_1,\dots,a_n}$ if and only if $I \subseteq \varphi_{a_1,\dots,a_n}$ if and only if $\varphi_{a_1,\dots,a_n}$ factors through $k[x_1, \dots, x_n]/I$, to induce a homomorphism $k[x_1, \dots, x_n]/I \to \Omega$. (Again, this is all obvious.)

Putting together these observations, we get the following lemma.

6.1.1. **Lemma.** *If, as above, $f_1, \dots, f_n$ is a collection of polynomials over $k$ in the variables $x_1, \dots, x_n$, and $I \subseteq k[x_1, \dots, x_n]$ denotes the ideal generated by the $f_i$, then the assignment $(a_1, \dots, a_n) \mapsto \varphi_{a_1,\dots,a_n}$ induces a bijection*

$$\{(a_1, \dots, a_n) \in \Omega^n \mid f_1(a_1, \dots, a_n) = \cdots = f_r(a_1, \dots, a_n) = 0\}$$
$$\leftrightarrow \{k\text{-algebra homomorphisms } \varphi : k[x_1, \dots, x_n]/I \to \Omega\}.$$

This lemma, simple but fundamental, is at the heart of the algebraic approach to algebraic geometry.

6.2. **Aside: the Hilbert Basis Theorem.** The Hilbet basis theorem asserts that any ideal in $k[x_1, \dots, x_n]$ (where, as before, $k$ is a field) is finitely generated. Thus there is nothing special about the ideal $I$ considered in Lemma 6.1.1; it could be *any* ideal in $k[x_1, \dots, x_n]$.

We recall the proof of Hilbert's theorem here, in the more general form that is usually considered, namely, that $A[x]$ is Noetherian if $A$ is. (This implies the Noetherianess of $k[x_1, \dots, x_n]$ by an obvious induction on $n$, starting with the fact that a field $k$ is certainly Noetherian, containing as it does only two ideals.)

6.2.1. **Theorem.** *If $A$ is Noetherian than so is $A[x]$.*

*Proof.* Let $I$ be an ideal in $A[x]$. Let $J_r \subseteq A$ be defined via

$$J_r := \{a \in A \mid a \text{ is the leading coefficient of an element of degree } r \text{ in } I\} \cup \{0\}.$$

One checks that $J_r$ is an ideal in $A$ (exercise), and that $J_r \subseteq J_{r+1}$ (exercise; hint: consider multiplication by $x$). Thus $J = \bigcup J_r$ is an ideal in $A$ (exercise), and so is finitely generated, by the hypothesis that $A$ is Noetherian. Thus for some sufficiently large $r$, we have

$$J_0 \subseteq J_1 \subseteq \cdots \subseteq J_r = J_{r+1} = J_{r+2} = \cdots .$$

Of course, each $J_i$ is also finitely generated (again using the Noetherianness of $A$).

We may and do choose, for each $i = 1, \dots, r$, a finite set $S_i = \{f_{i,1}, \dots, f_{i,s_i}\} \subseteq I$ of degree $i$ polynomials such that the leading coefficients of the elements of $S_i$ generate $J_i$.

One now checks that $S_0 \cup S_1 \cup \cdots \cup S_r$ generates $I$. To see this, let $I'$ denote the ideal generated by this union; certainly $I' \subseteq I$. If $i > r$, define $B_i := x^{i-r}B_r$; then each such $B_i$ lies in $I'$, and we see that $B_i$ is a set of degree $i$ polynomials whose leading coefficients generate $J_i$, for *every* $i \geq 0$ (taking into account the fact that $J_i = J_r$ when $i > r$). Recalling the definition of the $J_i$, we now see that $I = AB_0 + AB_1 + AB_2 + \cdots \subseteq I'$, and so $I = I'$, as claimed. In particular, the ideal $I$ is finitely generated. □

6.3. **Zero loci of ideals.** We make the following basic definition.

6.3.1. **Definition.** If $k$ is a field, $I$ is an ideal in $k[x_1, \ldots, x_n]$, and $\Omega$ is an extension of $k$, then we write

$$Z_I(\Omega) = \{(a_1, \ldots, a_n) \in \Omega^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\},$$

and refer to $Z_I(\Omega)$ as the zero locus of $I$ in $\Omega^n$ (or in $\mathbb{A}^n(\Omega)$; see Definition 6.3.2 below), or as the zero locus of $I$ with values in $\Omega$.

The notation we have chosen for $Z_I$ suggests that we regard $Z_I$ as a functor on the category of field extensions of $k$, and to this end, it is helpful to observe that $\Omega$ is indeed functorial in $\Omega$, in so far as if $\Omega \subseteq \Omega'$ is an extension (of extensions of $k$), then there is an evident inclusion $Z_I(\Omega) \subseteq Z_I(\Omega')$.

As was already noted in Subsection 6.1, if $I$ is generated by $f_1, \ldots, f_r$, then $Z_I(\Omega)$ is the subset of $\Omega^n$ consisting of simultaneous zeroes of each of the $f_i$. Lemma 6.1.1 shows that $Z_I(\Omega)$ may also be identified with the set of $n$-tuples $(a_1, \ldots, a_n)$ for which $\varphi_{a_1,\ldots,a_n}$ factors through $k[x_1, \ldots, x_n]/I$. Thus the functors $Z_I$ encode the concept of solving systems of polynomial equations.

6.3.2. **Definition.** When $I = 0$, we write $\mathbb{A}^n$ rather than $Z_0$. Thus

$$\mathbb{A}^n(\Omega) = \Omega^n.$$

The notation here stands for *$n$-dimensional affine space*.

It is natural to ask to what extent the functor $Z_I$ determines the ideal $I$. (If we know all the solutions to a collection of equations, can we recover the equations that have been solved?)

The precise answer to this question is the subject of the Nullstellensatz, which will take us some time to get to. However, we can at least say something about the special case of $\mathbb{A}^n$.

6.3.3. **Lemma.** *If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, and if $k$ is infinite, then $Z_I(k) = \mathbb{A}^n(k)$ if and only if $I = 0$.*

*Proof.* The if direction is clear (and holds without any hypothesis on $k$), and so we turn to proving the only if direction. More precisely, we will assume that $I \neq 0$, and prove that $Z_I(k) \neq \mathbb{A}^n(k)$. To this end, choose a non-zero element $f$ of $I$. Let $\ell$ be the equation for a hyperplane $Z_\ell(k)$ such that $\ell \nmid f$. (Such an $\ell$ exists because $k$ is infinite, and so there are infinitely many homogeneous linear polynomials $\ell$, while $f$ has only finitely many irreducible factors.) Then the restriction of $f$ to $Z_\ell(k)$ is not identically zero. This restriction is a polynomial in $n-1$ variables, and so by induction we may find a point of $Z_\ell(k)$ at which $f$ does not vanish. In other words, $Z_\ell(k) \not\subseteq Z_I(k)$, and so in particuar, $Z_I(k) \neq \mathbb{A}^n(k)$. □

6.3.4. **Corollary.** *If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, then $Z_I(\Omega) = \mathbb{A}^n(\Omega)$ for all extensions $\Omega$ of $k$ if and only if $I = 0$.*

*Proof.* The if direction being clear, we focus on proving the only if direction. Thus we assume that $Z_I(\Omega) = \mathbb{A}^n(\Omega)$ for all extensions $\Omega$ of $k$, with the aim of showing that $I = 0$. If $k$ is infinite, this follows immediately from Lemma 6.3.3 upon taking $\Omega = k$. In any case, $k$ always admits an extension $\Omega$ which is infinite. If we let $I_\Omega$ denote the ideal of $\Omega[x_1, \ldots, x_n]$ generated by $I$, then $Z_I(\Omega) = Z_{I_\Omega}(\Omega)$ (this is true for any choice of $I$), and so our assumption, together with Lemma 6.3.3, shows that $I_\Omega = 0$. Since $I \subseteq I_\Omega$, we find that $I = 0$ as well. □

6.4. **Finitely generated extensions of fields.** We need some facts and definitions from field theory.

If $\Omega/k$ is an extension of fields and $a_1, \ldots, a_n \in \Omega$, then we say that the $a_i$ are *mutually algebraic independent*, or simply *algebraically independent*, if the morphism $\varphi_{a_1,\ldots,a_n} : k[x_1, \ldots, x_n] \to \Omega$ is injective, i.e. has zero kernel. In this case, $\varphi_{a_1,\ldots,a_n}$ induces an isomorphism between $k[x_1, \ldots, x_n]$ and the $k$-subalgebra $k[a_1, \ldots, a_n]$ of $\Omega$ generated by the $a_i$, which then extends to an isomorphism between the field $k(x_1, \ldots, x_n)$ and the *subfield* $k(a_1, \ldots, a_n)$ of $\Omega$ generated by the $a_i$ over $k$.

6.4.1. **Lemma.** *If $l/k$ is a finitely generated extension of fields, then there exist $n$ mutually algebraically independent elements $a_1, \ldots, a_n \in l$ such that $l$ is a finite extension of $k(a_1, \ldots, a_n)$.*

*Proof.* Since $l$ is finitely generated over $k$, we may write $l = k(a_1, \ldots, a_{n'})$ for some collection of elements $a_1, \ldots, a_{n'} \in l$. Choose a maximal algebraically independent subset of these elements, which (after relabelling) we write as $a_1, \ldots, a_n$. Then, if $i > n$, the elements $a_1, \ldots, a_n, a_i$ are not algebraically independent, and so we may find a dependence non-zero polynomial $f$ in $n+1$-variables for which $f(a_1, \ldots, a_n, a_i) = 0$. Since $a_1, \ldots, a_n$ *are* algebraically independent, the polynomial $f(a_1, \ldots, a_n, x_{n+1}) \in k(a_1, \ldots, a_n)[x_{n+1}]$ is non-zero, and has $a_i$ as a zero. Thus $a_i$ is algebraic over $k(a_1, \ldots, a_n)$, and so $l = k(a_1, \ldots, a_n)[a_{n+1}, \ldots, a_{n'}]$ is finite over $k(a_1, \ldots, a_n)$. □

In the context of the preceding lemma, we say that elements $a_1, \ldots, a_n$ form a *transcendence basis* for $l$ over $k$. The size of a transcendence basis (the quanity $n$ of the preceding lemma) is an invariant of the extension $l/k$, and is called the *transcendence degree* of $l$ over $k$. We won't prove this till later.

6.5. **Universal domains.** We say that a field $\Omega$ is a *universal domain* if it is algebraically closed, and of infinite transcendence degree over its prime subfield (which we denote by $k_0$). Since we won't develop the theory of transcendence degree in the non-finitely generated context, we note the following equivalent, but more concrete, form of this definition: $\Omega$ is a univeral domain if and only if it is algebraically closed, and contains $n$ elements that are algebraically independent over $k_0$, for any $n \geq 0$.

6.5.1. **Example.**
(1) For any field $k$, an algebraic closure of $k(x_1, \ldots, x_n, \ldots)$ (where $x_1, \ldots, x_n, \ldots$ is a sequence of variables) is a universal domain containing $k$.
(2) The field $\mathbb{C}$ of complex numbers is a universal domain.

Example 6.5.1 (1) shows that any field may be embedded into a universal domain.

6.5.2. **Lemma.** *Let $\Omega$ be a universal domain with prime subfield $k_0$,*

(1) *If $k$ is any finitely generated field extension of $k_0$, then there is an embedding $k \hookrightarrow \Omega$.*
(2) *If $k \subseteq l$ is an extension of finitely generated field extensions of $k_0$, then any embedding $k \hookrightarrow \Omega$ may be extended to an embedding $l \hookrightarrow \Omega$.*

*Proof.* It suffices to prove (2); part (1) then follows as a special case, by replacing $k$ by $k_0$ and $l$ by $k$.

Since $l$ is finitely generated over $k$, by Lemma 6.4.1 we may find a finite number of elements $a_1, \dots, a_n \in l$ such that the $a_i$ are algebraically independent over $k$, and such that $l$ is algebraic over $k(a_1, \dots, a_n)$. Since $\Omega$ is a universal domain, and since $k$ is finitely generated over $k_0$, we may find elements $b_1, \dots, b_n \in \Omega$ which are algebraically independent over the image of $k$. We may then define an embedding $k(a_1, \dots, a_n) \hookrightarrow \Omega$, extending the given embedding $k \hookrightarrow \Omega$, by mapping $a_i$ to $b_i$. Since $\Omega$ is algebraically closed (being a univesal domain), while $l$ is algebraic over $k(a_1, \dots, a_n)$, this may be extended to an embedding $l \hookrightarrow \Omega$. □

We may bootstrap part (2) of the preceding lemma to an apparently stronger result. To this end, we recall a lemma from commutative algebra.

6.5.3. **Lemma.** *If $A$ is a non-zero ring, then $A$ contains a maximal ideal.*

*Proof.* An ideal $I$ in $A$ is proper if and only if $1 \notin I$. Thus if $\{I_i\}$ is any chain of proper ideals in $A$ (labelled by some totally ordered set), then the union $\bigcup_i I_i$ is also a proper ideal in $A$. (Since 1 does not lie in any of the $I_i$, it doesn't lie in their union either.) Zorn's Lemma now shows that the collection of all proper ideals in $A$ contains maximal elements. □

6.5.4. **Proposition.** *If $\Omega$ is a universal domain with prime subfield $k_0$, and if $A$ is a* non-zero *finitely generated algebra over a finitely generated field extension $k$ of $k_0$, then any embedding $k \hookrightarrow \Omega$ may be extended to a map of $k$-algebras $A \to \Omega$.*

*Proof.* Let $\mathfrak{m}$ be a maximal ideal of $A$ (which exists since $A$ is non-zero). The quotient $A/\mathfrak{m}$ is then a finitely generated field extension of $k$, and so part (2) of Lemma 6.5.2 shows that we may find an embedding $A/\mathfrak{m} \hookrightarrow \Omega$ extending the given embedding of $k$. Composing this with the canonical surjection $A \to A/\mathfrak{m}$ gives the desired map $A \to \Omega$. □

6.6. **The Nullstellensatz for universal domains.** We have shown above in Lemma 6.3.3 that the zero ideal in $k[x_1, \dots, x_n]$ is characterized by having every point of $\mathbb{A}^n(k)$ as a solution, for an infinite field $k$. Our goal now is to show that the unit ideal in $k[x_1, \dots, x_n]$ is characterized by having the empty set of solutions, provided that we consider solutions valued in a universal domain. (Below, in Subsection 11.1, we will prove the stronger result that the same remains true provided that we consider solutions valued in an algebraically closed extension of $k$. But we will need to develop more geometry before we can prove that result.)

6.6.1. **Theorem.** *If $I \subseteq k[x_1, \dots, x_n]$ is an ideal, and if $\Omega$ is a universal domain containing $k$, then $Z_I(\Omega) = \emptyset$ if and only if $I = k[x_1, \dots, x_n]$.*

*Proof.* The if direction is clear (for any choice of extension $\Omega$ of $k$, universal domain or not), so we focus on proving the only if direction. That is, we assume that $Z_I(\Omega) = \emptyset$, and we will show that $I$ is the unit ideal.

Let $k_0$ denote the prime subfield of $k$ (and hence of $\Omega$). By Hilbert's Basis Theorem we know that $I$ is finitely generated, say by $f_1, \ldots, f_r$, and so we may find a subfield $k'$ of $k$, finitely generated over $k_0$, such that $f_1, \ldots, f_r \in k'[x_1, \ldots, x_n]$. Let $I'$ denote the ideal in $k'[x_1, \ldots, x_n]$ generated by $f_1, \ldots, f_r$. Clearly $Z_{I'}(\Omega) = Z_I(\Omega)$ (just using that $I'$ and $I$ have the same set of generators), and hence $Z_{I'}(\Omega) = \emptyset$. Lemma 6.1.1 therefore implies that there are *no* $k'$-algebra homomorphisms $k'[x_1, \ldots, x_n]/I' \to \Omega$. It now follows from Proposition 6.5.4 that $k'[x_1, \ldots, x_n]/I'$ must be the zero $k'$-algebra, i.e. that $I'$ must be the unit ideal, and so in particular that $1 \in I'$. Since $I' \subseteq I$, we find that $1 \in I$, and thus that $I$ is also the unit ideal, as required. □

6.7. **Consequences of the Nullstellensatz.** We say that a field $\Omega$ *satisfies the Nullstellensatz* if the conclusion of Theorem 6.6.1 holds, for any subfield $k$ of $\Omega$, i.e. if for any subfield $k \subseteq \Omega$ and any ideal $I \subseteq k[x_1, \ldots, x_n]$ (with $n$ arbitrary), we have that $Z_I(\Omega) = \emptyset$ if and only if $I$ is the unit ideal. Clearly, it actually suffices to consider the case when $k = \Omega$ (since we may replace $I$ by the ideal in $\Omega[x_1, \ldots, x_n]$ that it generates, without changing the set $Z_I(\Omega)$).

As already remarked, we will prove later that a field satisfies the Nullstellensatz if (and only if) it is algebraically closed.

In this subsection, we describe the precise extent to which $Z_I(\Omega)$ determines the ideal $I$, under the assumption that $\Omega$ satisfies the Nullstellensatz.

6.7.1. **Definition.** If $I$ an ideal in a ring $A$, then $\mathrm{rad}(I)$ (the radical of $I$) is the ideal of $A$ defined by

$$\mathrm{rad}(I) := \{a \in A \mid a^N \in I \text{ for some } N\}.$$

Note that $I \subseteq \mathrm{rad}(I)$, and $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$.

Clearly for an ideal $I$ in $k[x_1, x_2, \ldots, x_n]$, we have $Z_{\mathrm{rad}(I)}(\Omega) = Z_I(\Omega)$.

6.7.2. **Theorem.** *If $k \subseteq \Omega$ is an extension of fields, and $\Omega$* satisfies the Nullstellensatz*, then, for any ideal $I \subseteq k[x_1, \ldots, x_n]$, a polynomial $f \in k[x_1, \ldots, x_n]$ vanishes identically on $Z_I(\Omega)$ if and only if $f \in \mathrm{rad}(I)$.*

*Proof.* We have already observed that if direction holds (without any assumption on $\Omega$). Thus we turn to proving the only if diretion, and, to this end, we suppose that $f$ vanishes identically on $Z_I(\Omega)$.

We define $J \subseteq k[x_1, \ldots, x_n, y]$ to be the ideal generated by $I$ together with the element $1 - fy$. The assumption that $f$ vanishes identically on $Z_I(\Omega)$ is immediately seen to imply that $Z_J(\Omega) = \emptyset$. Our assumption that $\Omega$ satisfies the Nullstellensatz then implies that $J$ is the unit ideal of $k[x_1, \ldots, x_n, y]$. If we set $A := k[x_1, \ldots, x_n]/I$, then we may rephrase this as saying that $1 - fy$ generates the unit ideal of $A[y]$. Lemma 6.7.3 below implies that $f$ is nilpotent in $A$, and thus that $f \in \mathrm{rad}(I)$, which is what we wanted. □

6.7.3. **Lemma.** *If $A$ is a ring and $a \in A$, then the polynomial $1 - ay$ is a unit in $A[y]$ if and only if $a$ is nilpotent in $A$.*

*Proof.* We may embed $A[y]$ in the power series ring $A[[y]]$, and the usual computation with geometric series shows that $1 - ay$ is a unit in $A[[y]]$, with

$$(1 - ay)^{-1} = 1 + ay + a^2y + \cdots + a^n y + \cdots .$$

Thus we see that $1 - ay$ is a unit in $A[y]$ if and only if this geometric series is in fact a polynomial if and only if $a$ is nilpotent, as claimed. □

6.7.4. **Remark.** The proof of Theorem 6.7.2 is known as *the Rabinowitz trick*.

The following result is an immediate corollary of Theorem 6.7.2.

6.7.5. **Corollary.** *If $k \subseteq \Omega$ is an extension of fields, and* $\Omega$ satisfies the Nullstellensatz*, then, for any ideals $I, J \subseteq k[x_1, \dots, x_n]$, we have that $Z_I(\Omega) \subseteq Z_J(\Omega)$ if and only if* $\mathrm{rad}(I) \supset \mathrm{rad}(J)$.

6.7.6. **Corollary.** *If $k$ is a field satisfying the Nullstellensatz, then the maximal ideals of $k[x_1, \dots, x_n]$ are precisely the ideals of the form $(x_1 - a_1, \dots, x_n - a_n)$, for some $n$-tuple $(a_1, \dots, a_n) \in k^n$.*

*Proof.* Clearly any such ideal is maximal. Conversely, if $\mathfrak{m}$ is a maximal ideal, write $\Omega = k[x_1, \dots, x_n]/\mathfrak{m}$. Since $Z_{\mathfrak{m}}(\Omega)$ is non-zero (tautologically), we conclude that $Z_{\mathfrak{m}}(k)$ is non-zero. If $(a_1, \dots, a_n)$ is a point of $Z_{\mathfrak{m}}(k)$, then we see that $(x_1 - a_1, \dots, x_n - a_n)$ (which is the kernel of $\varphi_{a_1,\dots,a_n}$) contains $\mathfrak{m}$, and thus these two ideals coincide (since $\mathfrak{m}$ is maximal by assumption). □

6.8. **The Zariski topology.** We suppose that $k \subseteq \Omega$ is an extension of fields, and that $\Omega$ satisfies the Nullstellensatz.

6.8.1. **Definition.** The Zariski topology on $\mathbb{A}^n(\Omega)$ over $k$ is defined by declaring the closed subsets to be those subsets of the form $Z_I(\Omega)$ for ideal $I \subseteq k[x_1, \dots, x_n]$. We write $\mathbb{A}^n_{/k}(\Omega)$ to denote $\mathbb{A}^n(\Omega)$ equipped with its Zariski topology over $k$.

6.8.2. **Remark.** We note that

(1) $Z_I(\Omega) \cup Z_J(\Omega) = Z_{IJ}(\Omega)$.
(2) $\bigcap_i Z_{I_i}(\Omega) = Z_{\sum_i I_i}(\Omega)$.
(3) $Z_{k[x_1,\dots,x_n]}(\Omega) = \emptyset$.
(4) $Z_0(\Omega) = \mathbb{A}^n(\Omega)$.

Thus the Zariski topology is indeed a topology.

6.8.3. **Remark.** The Zariski topology on $\mathbb{A}^n_{/k}(\Omega)$ depends on the choice of $k$ (which is why we include $k$ in the notation). For example, the singleton $\{i\}$ is closed in $\mathbb{A}^1_{/\mathbb{C}}(\mathbb{C})$ (it is the zero locus of the polynomial $x - i \in \mathbb{C}[x]$), but is not closed in $\mathbb{A}^1_{/\mathbb{R}}(\mathbb{C})$; its closure in $\mathbb{A}^1_{/\mathbb{R}}(\mathbb{C})$ is equal to $\{i, -i\}$ (this set being the zero locus of the polynomial $x^2 + 1 \in \mathbb{R}[x]$).

The Zariski topology on $\mathbb{A}^n_{/k}(\Omega)$ induces a topology on each $Z_I(\Omega)$, which we refer to as the Zariski topology on $Z_I(\Omega)$. Corollary 6.7.5 shows that the closed subsets of $Z_I(\Omega)$ are precisely the subsets $Z_J(\Omega)$, as $J$ ranges over ideals $J \subseteq \mathrm{rad}(I)$.

6.8.4. **Definition.** We refer to the sets $Z_I(\Omega)$, endowed with their Zariski topology, as affine algebraic sets

## 7. Interlude on topology

Here we will discuss irreducibility, dimension, etc..

## 8. Projective algebraic sets

8.1. **The incompleteness of affine algebraic sets.** A technical difficulty with affine algebraic sets is that (when they are not just a finite union of points) they are not complete, in a sense that the following example should convey.

8.1.1. **Example.** Consider the intersection of the locus $xy = 1$ and the locus $y = tx$ (where $t$ is, to begin with, a non-zero parameter). Clearly, the intersection is equal to the set $\{(x, tx) \,|\, x^2 = 1/t\}$, and so consists of two points. However, if we consider what happens as $t \to 0$ (in an informal sense, for the moment), we see that these two points of intersection disappear: the loci $xy = 1$ and $y = 0$ do not intersect.

There is another way to phrase the incompleteness described in the preceding example which is technically more precise (it doesn't appeal to notions of convergence and limit which make little or no sense when $k$ and $\Omega$ are not equal to $\mathbb{C}$), if slightly less intuitive. Namely, rather than thinking of $t$ as a parameter, in some slightly unspecified sense, just regard $y = tx$ as an equation in three variables $x$, $y$, and $t$. Then we can consider the affine algebraic set $Z_{(xy-1,y-tx)}(\Omega) \subseteq \mathbb{A}^3_{/k}(\Omega)$.

Projection onto the third variable (i.e. projecting onto the $t$-line) gives a map $\mathbb{A}^3_{/k}(\Omega) \to \mathbb{A}^1_{/k}(\Omega)$, and the fibre of this projection over any particular value of $t$ is then equal to the intersection of the loci cut out by the equations $xy = 1$ and $y = tx$ (with $t$ now taken to be the particular value under consideration). Our previous vague remarks about a limit of intersections disappearing as $t \to 0$ can now be made precise in the following way: the image of $Z_{(xy-1,y-tx)}(\Omega)$ under this projection, which is equal to $\{t \in \mathbb{A}^1(\Omega) \,|\, t \neq 0\}$, is *not* Zariski closed. (Its Zariski closure is equal to all of $\mathbb{A}^1(\Omega)$, but it does not contain the point $t = 0$ of this closure.)

Our goal in introducing projective space and projective algebraic sets, first and foremost, is to find a setting in which the incompleteness problems of the type just described are eliminated. The technical expression of the completeness of projective space will be given in Theorem 8.6.1 below; a quick glance at the statement of that theorem will show that it is phrased in terms of certain projections being closed maps in the Zariski topology. (It then becomes a bit of an art to learn how to apply the completeness property for projective spaces, described in such terms, to deal with problems of "limits" (intuitively understood) such as the one described in the above example.)

8.2. **Projective space.** We begin by introducting projective space, and to motivate this, we consider perhaps the simplest situation of "missing limits", namely missing points at infinity in affine space. To this end, consider affine space $\mathbb{A}^n(\Omega)$ (with coordinates $x_1, \ldots, x_n$), but regard it as the hyperplane $H$ in $\Omega^{n+1}$ (with coordinates $x_0, \ldots, x_n$) cut out by the equation $x_0 = 1$.

If we consider any line $\ell$ through the origin in $\Omega^{n+1}$ which does not lie in the plane $x_0 = 0$, then $\ell$ intersects $H$ in precisely one point, and in this way we identify $\mathbb{A}^n(\Omega)$ with a subset of the set of all lines through the origin in $\Omega^{n+1}$. Now imagine varying $\ell$, and in particular, rotating it so that it ultimately lies in the plane $x_0 = 0$. The point of intersection with $H$ will then run off "to infinity" and disappear as the line $\ell$ comes to rest in the plane $x_0 = 0$.

If we want this limiting point of intersection to exist, we have no choice but to add points to $\mathbb{A}^n(\Omega)$. We do this in the simplest (and most tautological!) way

possible, namely, beginning with the identification of $\mathbb{A}^n(\Omega)$ with the set of lines $\ell$ through the origin of $\Omega^{n+1}$ which do not lie in the hyperplane $x_0 = 0$, we simply define $\mathbb{P}^n(\Omega)$ to be the set of all lines through the origin of $\Omega^{n+1}$.

8.2.1. **Definition.** If $\Omega$ is a field, we let $\mathbb{P}^n(\Omega)$ denote the set of lines through the origin of $\Omega^{n+1}$.

A line through the origin, which is to say a point in $\mathbb{P}^n(\Omega)$, is determined by any non-zero point $(x_0, x_1, \dots, x_n)$ lying on it, and we write $(x_0 : x_1 : \dots : x_n)$ to denote the line through the origin that passes through such a non-zero point. Two non-zero points $(x_0, x_1, \dots, x_n)$ and $(x'_0, x'_1, \dots, x'_n)$ lie on the same line through the origin if and only if $(x_0, x_1, \dots, x_n) = \lambda(x'_0, x'_1, \dots, x'_n)$ for some $\lambda \in \Omega^\times$, and so $(x_0 : x_1 : \dots : x_n) = (x'_0 : x'_1 : \dots : x'_n)$ if and only if $(x_0, x_1, \dots, x_n) = \lambda(x'_0, x'_1, \dots, x'_n)$ for some $\lambda \in \Omega^\times$. We refer to the numbers $x_0, x_1, \dots, x_n$ as the homogeneous coordinates of the point $(x_0 : x_1 : \dots : x_n) \in \mathbb{P}^n(\Omega)$; they are thus well-determined up to simultaneous multiplication by a non-zero scalar.

8.3. **Zero loci of homogeneous ideals.** Since points in $\mathbb{P}^n(\Omega)$ are described not by well-defined coordinates, but only by coordinates that are well-defined up to a simultaneous non-zero scalar multiple, it doesn't make sense to evaluate an arbitrary element $f \in k[x_0, \dots, x_n]$ at a point of $\mathbb{P}^n(\Omega)$.

However, if $f \in k[x_0, \dots, x_n]$ is homogeneous, say of degree $d$, then

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n)$$

for any $\lambda \in \Omega^\times$, and so the vanishing or not of $f$ at a point of $\mathbb{P}^n(\Omega)$ is well-defined, independently of the choice of homogeneous coordinates.

8.3.1. **Definition.** For each $d \geq 0$, we write $k[x_0, \dots, x_n]_d$ to denote the $k$-vector subspace of $k[x_0, \dots, x_n]$ consisting of homogenous polynomials of degree $d$. (The dimension of $k[x_0, \dots, x_n]$ is equal to $\binom{n+d}{n}$.)

We regard $k[x_0, \dots, x_n]$ as a graded ring via the decomposition

$$k[x_0, \dots, x_n] = k[x_0, \dots, x_n]_0 \oplus k[x_0, \dots, x_n]_1 \oplus \dots \oplus k[x_0, \dots, x_n]_d \oplus \dots .$$

8.3.2. **Definition.** We say that an ideal $I \subseteq k[x_0, \dots, x_n]$ is homogeneous if the inclusion $\bigoplus_{d=0}^{\infty} \big(I \cap k[x_0, \dots, x_n]_d\big) \subseteq I$ is an equality, or, equivalently, if $I$ can be generated by homogenous polynomials.

Studying the simultaneous zero loci of collections of homogeneous polynomials is evidently the same as studying the zero loci of homogeneous ideals.

The following result gives the analogue of Theorem 6.6.1 in the context of homogeneous ideals and projective algebraic sets.

8.3.3. **Proposition.** *Suppose that $\Omega$ satisfies the Nullstellensatz. Then for a homogeneous ideal $I \subset k[x_0, \dots, x_n]$, the zero locus of $I$ in $\mathbb{P}^n(\Omega)$ is empty if and only if $I_d = k[x_0, \dots, x_n]_d$ for some $d$ (and hence for all sufficiently large $d$).*

*Proof.* The zero locus of $I$ in $\mathbb{P}^n(\Omega)$ is empty if and only if the zero locus of $I$ in $\mathbb{A}^{n+1}$ is either empty or equal to $(0, \dots, 0)$. In the former case, Theorem 6.6.1 implies that $I = k[x_0, \dots, x_n]$, and so $I_d = k[x_0, \dots, x_n]_d$ for every $d \geq 0$. In the latter case, since $\{(0, \dots, 0)\}$ is the zero locus of the ideal $(x_0, \dots, x_n)$, it follows from Corollary 6.7.5 that $I$ contains some power of the ideal $(x_0, \dots, x_n)$, and elementary manipulations show that this is equivalence to showing that $I$ contains

$k[x_0, \ldots, x_n]_{d_0}$ for some $d_0 \geq 0$, and hence for all $d \geq d_0$ (since $I$ is an ideal). Since $I$ is homogeneous, this in turn is equivalent to having $I_d = k[x_0, \ldots, x_n]_d$ for all $d \geq d_0$, as required. □

8.4. **Zariski topology and projective closure.**

8.5. **The products $\mathbb{A}^m \times \mathbb{P}^n$.** Let $x_1, \ldots, x_m$ be coordinates for $\mathbb{A}^m$, and let $x_0, \ldots, x_n$ be homogeneous coordinates for $\mathbb{P}^n$. We can define Zariski closed subsets of $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ using polynomials that are of arbitrary nature in the $x$ variables, and homogeneous in the $y$ variables.

Equivalently, we may may use ideals $I \subset k[x_1, \ldots, x_m, y_0, \ldots, y_n]$ that are homogenous with the respect to the $y$ variables.

8.6. **Elimination theory.** The following result, known as the *main theorem of elimination theory*, although it may seem technical, is the key result which formulates the "completeness" of projective space.

8.6.1. **Theorem.** *Suppose that the field $\Omega$ satisfies the Nullstellensatz, and let $I \subseteq k[x_1, \ldots, x_m, y_0, \ldots, y_n]$ be an ideal, homogeneous in the $y_i$. If $Z_I(\Omega)$ denotes the zero locus of $I$ in $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$, then the image of $Z_I(\Omega)$ under the projection*

$$\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega) \to \mathbb{A}^m(\Omega)$$

*is Zariski closed over $k$.*

*Proof.* Let $\pi : \mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega) \to \mathbb{A}^m(\Omega)$ denote the projection onto the first factor. To show that $\pi\big(Z_I(\Omega)\big)$ is closed, we have to show that if $(a_1, \ldots, a_m) \notin \pi\big(Z_I(\Omega)\big)$, then there exists a polynomial $f$ such that $f(a_1, \ldots, a_m) \neq 0$, and such that if $f(b_1, \ldots, b_m) \neq 0$, then $(b_1, \ldots, b_m) \notin \pi\big(Z_I(\Omega)\big)$.

Since $(a_1, \ldots, a_m) \notin \pi\big(Z_I(\Omega)\big)$, it follows from Proposition 8.3.3 that

$$\varphi_{a_1,\ldots,a_m}(I_d) = k[y_0, \ldots, y_n]_d$$

for some sufficiently large value of $d$. Thus, if we let $\{f_i\}$ be a basis for $k[y_0, \ldots, y_d]$, then we may find elements $\{g_i\}$ of $I_d$ for which $\varphi_{a_1,\ldots,a_m}(g_i) = f_i$, and we may further write

$$\begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix} = M \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix},$$

for some matrix $M$ with entries in $k[x_1, \ldots, x_m]$. If we set $f := \det M$, then $f$ is an element of $k[x_1, \ldots, x_m]$, whose value at $(a_1, \ldots, a_m)$ is non-zero (indeed, $\varphi_{a_1,\ldots,a_m}(M)$ is the identity matrix, and so $f(a_1, \ldots, a_m) = 1$), and with the property that $f(b_1, \ldots, b_m) \neq 0$ implies that $\varphi_{b_1,\ldots,b_m}(I_d) = k[y_0, \ldots, y_n]_d$, and hence that $b_1, \ldots, b_m \notin \pi\big(Z_I(\Omega)\big)$. This completes the proof. □

Here is one way to phrase this result (which in fact reflects that way the we proved it). Namely, if $X \subseteq \mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ is a closed subset, and $\varphi : X \to \mathbb{A}^m(\Omega)$ denotes the natural projection (i.e. projection from $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ onto the first factor), then if $P \in \mathbb{A}^m(\Omega)$ is such that $\varphi^{-1}(P)$ is empty, then there is an open subset $U \subset \mathbb{A}^m(\Omega)$ such that $\varphi^{-1}(U)$ is empty. (Indeed, the theorem assures us that $\varphi(X)$ is closed, and the assumption that $\varphi^{-1}(P) = \emptyset$ is just another way of saying that $P \notin \varphi(X)$. Thus we can take $U$ to be the complement of $\varphi(X)$ in $\mathbb{A}^m(\Omega)$.)

We now give an application of elimination theory to prove a strengthening of this result, with the condition of being *empty* replaced by that of being *finite*.

8.6.2. **Corollary.** *Suppose, as in the above discussion, that we are given a closed subset $X \subset \mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$, and let $\varphi : X \to \mathbb{A}^m(\Omega)$ denote the natural projection. If $P \in \mathbb{A}^m(\Omega)$ has the property that its preimage $\varphi^{-1}(P)$ is finite, then we may find an open neighbourhood $U$ of $P$ in $\mathbb{A}^m(\Omega)$ such that for each point $Q \in U$, its preimage $\varphi^{-1}(Q)$ is finite.*

*Proof.* We may as well assume that $k = \Omega$, and in particular that $k$ is infinite.

Observe that $\varphi^{-1}(P)$ is equal to the intersection $X \cap \big(\{P\} \times \mathbb{P}^n(\Omega)\big)$. Since this set is finite, and since $k$ is infinite, we may find a hyperplane $H \subset \mathbb{P}^n(\Omega)$ such that $\varphi^{-1}(P)$ is disjoint from $\{P\} \times H$.

Now consider the intersection $X \cap (\mathbb{A}^m(\Omega) \times H)$. This is a closed subset of $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ (being the intersection of two closed subsets), and so by Theorem 8.6.1 its image under $\varphi$ is closed. By the choice of $H$, this image doesn't contain $P$, and so its complement $U$ is an open neighbourhood of $P$. If $Q \in U$, then we see that $\varphi^{-1}(Q) = X \cap \big(\{Q\} \times \mathbb{P}^n(\Omega)\big)$ is closed in $\{Q\} \times \mathbb{P}^n(\Omega)$ (being the intersection of the latter with the closed set $X$), and is contained in $\{Q\} \times \big(\mathbb{P}^n(\Omega) \setminus H\big)$.

Note that, for an appropriate choice of coordinates, $\mathbb{P}^n(\Omega) \setminus H = \mathbb{A}^n(\Omega)$, and so we are left with following problem: to show that a closed subset of $\mathbb{P}^n(\Omega)$, which is contained in $\mathbb{A}^n(\Omega)$, is finite. We leave this as an exercise. (Later we will prove a more general version of this statement.) □

8.6.3. **Remark.** The analogues of Theorem 8.6.1 and Corollary 8.6.2, in which $\mathbb{P}^n(\Omega)$ is replaced by $\mathbb{A}^n(\Omega)$, are false.

We already gave a counterexample to Theorem 8.6.1 for affine space in the discussion of Subsection 8.1. Here we give another, simpler one. Namely, if we consider the projection

$$\mathbb{A}^2(\Omega) = \mathbb{A}^1(\Omega) \times \mathbb{A}^1(\Omega) \to \mathbb{A}^1(\Omega)$$

(projection onto the first coordinates), and let $Z = \{(x, y)\, xy = 1\}$, then $Z$ is a closed subset of $\mathbb{A}^2(\Omega)$, but its image in $\mathbb{A}^1(\Omega)$ is equal to the subset $\{x \,|\, x \neq 0\}$, which is not Zariski closed. Thus the main theorem of elimination theory doesn't hold when projective space is replaced by affine space.

If we consider a slight variation of this, namely the projection

$$\mathbb{A}^3(\Omega) = \mathbb{A}^1(\Omega) \times \mathbb{A}^2(\Omega) \to \mathbb{A}^1(\Omega),$$

and let $X = \{(x, y, z)\, xy = 1\}$, then, letting $\varphi : X \to \mathbb{A}^1(\Omega)$ denote the projection (as above), we see that $\varphi^{-1}(0)$ is empty (and hence finite), while for any $x \neq 0$, we have $\varphi^{-1}(x) = \{(x, 1/x, z)\, z \in \Omega\}$, which is infinite. Thus the analogue of Corollary 8.6.2 is also false if we replace projective space by affine space.

## 9. Morphisms and the category of quasi-projective algebraic sets

Already in the previous section, in the discussion of elimination theory, we found ourselves discussing products, and certain natural maps that arise when thinking about products (such as projections). It is convenient to introduce some categorical language for discussing these sorts of things.

9.1. **Quasi-projective algebraic sets.** So far, we have introduced three kinds of algebraic sets: affine algebraic sets (Zariski closed subsets of $\mathbb{A}^n(\Omega)$), projective algebraic sets (Zariski closed subsets of $\mathbb{P}^n(\Omega)$), and a kind of hybrid object, namely Zariski closed subsets of $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$.

Note that $\mathbb{A}^n(\Omega)$ is a Zariski *open* subset of $\mathbb{P}^n(\Omega)$ (it is the complement of the hyperplane at infinity), and so any affine algebraic set is an open subset of its projective closure (i.e. its Zariski closure in $\mathbb{P}^n(\Omega)$).

We will see soon (in Subsection 10.1 below) that $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ may also be regarded as an open subset of a projective algebraic set.

Thus the following definition incorporates, and extends, all our previous notations of algebraic set.

9.1.1. **Definition.** We say that a subset $X \subset \mathbb{P}^n(\Omega)$ is a *quasi-projective* algebraic set over $k$ if there is a Zariski closed subset (i.e. a projective algebraic set) over $k$, say $Z \subset \mathbb{P}^n(\Omega)$, such that $X$ is a Zariski open subset of $Z$.

9.1.2. **Remark.** If $S$ is any topological space, then we say that a subset $X$ of $S$ is *locally closed* if there is a closed subset $Z \subset S$ such at $X$ is an open subset of $Z$ (when $Z$ is given its induced topology). One easily checks that we may take $Z$ to be the closure of $X$, i.e. that $X$ is locally closed in $S$ if and only if it is an open subset of its closure in $S$.

The preceding definition may then be rephrased as follows: the quasi-projective algebraic sets are precisely the subsets of $\mathbb{P}^n(\Omega)$ that are locally closed in the Zariski topology.

9.1.3. **Remark.** If $X$ is any quasi-projective variety, and $P \in X$, then we choose coordinates so that $P \in X \cap \mathbb{A}^n(\Omega) \subset X$. (Just choose coordinates so that the hyperplane at infinity doesn't contain $P$.) Since $\mathbb{A}^n(\Omega)$ is an open subset of $\mathbb{P}^n(\Omega)$, we see that $U := X \cap \mathbb{A}^n(\Omega)$ is an open subset of $X$. Thus any point of a quasi-projective algebraic set has an open neighbourhood which is contained in $\mathbb{A}^n(\Omega)$ (for some appropriate choice of coordinates on projective space).

We always endow a quasi-projective algebraic set with its Zariski topology, i.e. the topology induced on it by the Zariski topology on the projective space that contains it.

We also remark that an easy argument shows that if $X$ is a locally closed subset of a topological space $S$, and $Y$ is a locally closed subset of $X$ (when $X$ is endowed with its induced topology), then $Y$ is a locally closed subset of $S$. Thus locally closed subsets of quasi-projective varieties are again quasi-projective varieties.

9.2. **Morphisms.** To define a category, one must define a collection of objects, and one must define the morphisms between them. The objects of our category will the quasi-projective algebraic setse. In this subsection we define the morphisms, and establish their basic properties.

9.2.1. **Definition.** Let $X$ and $Y$ be quasi-projective algebraic sets, say with $X$ being locally closed in $\mathbb{P}^m(\Omega)$ and $Y$ being locally closed in $\mathbb{P}^n(\Omega)$. We say that a function $\varphi : X \to Y$ is a *morphism* from $X$ to $Y$ if it satisfies the following condition: for each point $P \in X$, there exists an open neighbourhood $U$ of $P$ in $X$ which is contained in $\mathbb{A}^m(\Omega)$ (for some suitable choice of coordinates on $\mathbb{P}^m(\Omega)$ — see Remark 9.1.3) and an open neighbourhood $V$ of $\varphi(P)$ in $Y$ which is contained in $\mathbb{A}^n(\Omega)$ (for some suitable choice of coordinates on $\mathbb{P}^n(\Omega)$ — again, see Remark 9.1.3), such that

$\varphi(U) \subset V$, and such that the restriction $\varphi_{|U} : U \to V$ (which is now a function from a subset of $\mathbb{A}^m(\Omega)$ to a subset of $\mathbb{A}^n(\Omega)$) admits a formula of the form

$$\varphi(x_1, \dots, x_m) = \Big(\frac{f_1(x_1, \dots, x_m)}{g_1(x_1, \dots, x_m)}, \dots, \frac{f_n(x_1, \dots, x_m)}{g_n(x_1, \dots, x_m)}\Big), \tag{9.2.2}$$

where the $f_i$ and $g_i$ are elements of $k[x_1, \dots, x_m]$, and furthermore the polynomials $g_i$ are nowhere zero on $U$ (so that the preceding formula makes sense as a function from $U$ to $\mathbb{A}^n(\Omega)$).

9.2.3. **Remark.** In the context of the preceding definition, we have to choose coordinates on $\mathbb{P}^m(\Omega)$ and $\mathbb{P}^n(\Omega)$, and open neighbourhoods $U$ of $P$ and $V$ of $\varphi(P)$, such that $\varphi(U) \subset V$ and such that $U \subset \mathbb{A}^m(\Omega)$ and $V \subset \mathbb{A}^n(\Omega)$. The condition for $\varphi$ to be a morphism is then expressed in terms of the coordinates on $\mathbb{A}^m(\Omega)$ and $\mathbb{A}^n(\Omega)$; namely, $\varphi_{|U}$ has to be expressible in terms of rational functions in these coordinates whose denominators are nowhere zero on $U$.

Now, if $U$ and $V$ have been chosen, it might be that there is another choice of coordinates on $\mathbb{P}^m(\Omega)$, or on $\mathbb{P}^n(\Omega)$, so that $U$ also lies in $\mathbb{A}^m(\Omega)$, or $V$ also lies in $\mathbb{A}^n(\Omega)$, with respect to these new coordinates. Our goal in this remark is to observe that if we change coordinates in this way in either the source or target of $\varphi$, then it is still given by a formula of the form (9.2.2).

We begin by supposing that the open set $U$ lies in more than one copy of affine space; i.e. that there is more than one hyperplane that is disjoint from $U$. Suppose that $H$ is the hyperplane at infinity, so that $U \subset \mathbb{A}^m(\Omega) = \mathbb{P}^m(\Omega) \setminus H$. Suppose now that $H'$ is another hyperplane (defined over $k$) disjoint from $U$, so that $\mathbb{P}^m(\Omega) \setminus H'$ is another copy of $\mathbb{A}^m(\Omega)$ containing $U$.

We may choose coordinates $x_1, \dots, x_m$ for (the first copy of) $\mathbb{A}^m(\Omega)$ so that $H' \cap \mathbb{A}^m(\Omega)$ is cut out by $x_1 = 0$. Then $y_1 = 1/x_1, y_2 = x_2/x_1, \dots, y_m = x_m/x_1$ will be (the restriction to $\mathbb{P}^m \setminus (H \cup H')$ of) affine coordinates on $\mathbb{P}^m(\Omega) \setminus H'$.

Now suppose that

$$\varphi(x_1, \dots, x_m) = \Big(\frac{f_1(x_1, \dots, x_m)}{g_1(x_1, \dots, x_m)}, \dots, \frac{f_n(x_1, \dots, x_m)}{g_n(x_1, \dots, x_m)}\Big)$$

is a formula for $\varphi_{|U}$ in terms of the coordiantes $x_1, \dots, x_m$. (Note that the condition of being expressible in this manner is invariant under affine linear changes of coordinates on the source, so $\varphi_{|U}$ is indeed expressible in this manner.) Then substituting $x_1 = 1/y_1, x_2 = y_2/y_1, \dots, x_m = y_m/y_1$, we find the formula

$$\varphi(y_1, \dots, y_m) = \Big(\frac{f_1(1/y_1, y_2/y_1, \dots, y_m/y_1)}{g_1(1/y_1, y_2/y_1, \dots, y_m/y_1)}, \dots, \frac{f_n(1/y_1, y_2/y_1, \dots, y_m/y_1)}{g_n(1/y_1, y_2/y_1, \dots, y_m/y_1)}\Big)$$

for $\varphi_{|U}$ in terms of the coordinates $y_1, \dots, y_m$. Since $y_1$ is nowhere vanishing on $U$, we see that we may rewrite this formula as

$$\varphi(y_1, \dots, y_m) = \Big(\frac{f_1'(y_1, \dots, y_m)}{g_1'(y_1, \dots, y_m)}, \dots, \frac{f_n'(y_1, \dots, y_m)}{g_n'(y_1, \dots, y_m)}\Big),$$

where $f_i', g_i' \in k[y_1, \dots, y_m]$, and the $g_i'$ are nowhere vanishing on $U$.

The conclusion of this analysis is that if $\varphi : X \to Y$ is a morphism, and $U$ is an open subset of $X$, contained in $\mathbb{A}^m(\Omega)$, on which $\varphi$ is given by a formula involving rational functions in the coordinates on $\mathbb{A}^m(\Omega)$ as in Definition 9.2.1, then if we can embed $U$ into any other copy of $\mathbb{A}^m(\Omega)$ contained in $\mathbb{P}^m(\Omega)$ (by choosing a different

hyperplane at infinity) then $\varphi_{|U}$ will be equally well given by a formula involving rational functions of these new coordinates.

A similar analysis applies if the neighbourhood $V$ of $\varphi(P)$ is contained in two different copies of affine space inside $\mathbb{P}^n(\Omega)$ (given by making two different choices of the hyperplane at infinity). Certainly, if we compose a formula of the form (9.2.2) with an affine linear change of coordinates on the target, we obtain another formula of the same form (whose denominators are again nowhere vanishing on $U$). Now, after making such a linear change of coordinates, we may assume that the affine coordinates, say $u_1, \dots, u_n$, in the first copy of $\mathbb{A}^n(\Omega)$ are related to the affine coordinates in the second copy, say $v_1, \dots, v_n$, via the formula

$$v_1 = 1/u_1, v_2 = u_2/u_1, \dots, v_n = u_n/u_1.$$

Then in the new coordinates, $\varphi$ will be given by the formula

$$\begin{aligned}\varphi(x_1, \dots, x_m) \\ = \Big(\frac{g_1(x_1, \dots, x_m)}{f_1(x_1, \dots, x_m)}, \frac{f_2(x_1, \dots, x_m)g_1(x_1, \dots, x_m)}{f_1(x_1, \dots, x_m)g_2(x_1, \dots, x_m)}, \\ \dots, \frac{f_n(x_1, \dots, x_m)g_1(x_1, \dots, x_m)}{f_1(x_1, \dots, x_m)g_n(x_1, \dots, x_m)}\Big).\end{aligned}$$

Our assumption that $V$ is not contained in the hyperplane $u_1 = 0$, together with the assumption that $\varphi(U) \subset V$, ensures that $f_1$ is nowhere vanishing on $U$. Thus this is again an expression for $\varphi$ in terms of rational functions whose denominators are nowhere vanishing on $U$.

The preceding remark will be useful in proving part (2) of our next result, which records some basic properties of morphisms.

9.2.4. **Proposition.** (1) *If $\varphi : X \to Y$ is a morphism of quasi-projective varieties, then $\varphi$ is continuous.*

(2) *If $\varphi : X \to Y$ and $\psi : Y \to Z$ are morphisms of quasi-projective varieties, then the composite $\psi\varphi : X \to Z$ is again a morphism of quasi-projective varieties.*

*Proof.* □

The following result follows essentially by definition. It expresses the fact that being a morphism is a *local* property.

9.2.5. **Lemma.** *If $\varphi : X \to Y$ is a function between quasi-projective algebraic sets, and each point $P \in X$ has an open neighbourhood $U$ such that $\varphi_{|U}$ is a morphism, then $\varphi$ itself is a morphism.*

To motivate our next lemma, recall first the following easy fact from topology: if $S$ and $T$ are topological spaces, and $T'$ is a subset of $T$ endowed with the induced topology, and $\varphi : S \to T'$ is a function, then $\varphi$ is continuous if and only if the composite $\iota\varphi$ is continuous, where $\iota : T' \hookrightarrow T$ is the inclusion. Less formally, the function $\varphi$ is continuous as a map to $T'$ if and only if it is continuous when regarded as a map to $T$. (This is immediately verified just from the definition of the induced topology.)

In general, an arbitrary subset of a quasi-projective algebraic set is not a quasi-projective algebraic set, and we won't be able to prove a perfect analogue of the

preceding result. However, we have observed that a locally closed subset of a quasi-projective algebraic set *is* again a quasi-algebraic set, and the following result then gives an analogue of the preceding topological result in the context of such locally closed subsets.

9.2.6. **Lemma.** *Let $X$ be a quasi-projective algebraic set, let $Y$ be a locally closed subset of $X$ (so that $Y$ is also a quasi-projective algebraic set), and let $\iota : Y \to X$ denote the inclusion.*

(1) *$\iota$ is a morphism.*
(2) *If $Z$ is any quasi-projective algebraic set and $\varphi : Z \to Y$ is a function, then $\varphi$ is a morphism if and only if the composite $\iota\varphi : Z \to X$ is a morphism.*

*Proof.* Claim (1) is immediate, since if $P$ is any point of $Y$, and $U$ is any neighbourhood of $P$ contained in an affine space of $\mathbb{P}^n(\Omega)$ (this being the projetive space containing $X$ and $Y$), then $\iota$ is given on $U$ by the formula $\iota(x_1, \dots, x_n) = (x_1, \dots, x_n)$.

If $\varphi : Z \to Y$ is a morphism, we then see that $\iota\varphi$ is a composite of morphisms, hence is a morphism by the preceding lemma, and so one direction of claim (2) is also proved. Finally, suppose that $\varphi : Z \to Y$ is a function for which the composite $\iota\varphi$ is a morphism. Then, by definition, for any point $P \in Z$ there are open neighbourhoods $U$ of $P$ and $V$ of $\iota\varphi(P) = \varphi(P)$ in $Z$ and $X$, each which is contained in an affine space, so that $\iota\varphi(P)$ is given by a formula

$$\iota\varphi(x_1, \dots, x_m) = \Big(\frac{f_1(x_1, \dots, x_m)}{g_1(x_1, \dots, x_m)}, \dots, \frac{f_n(x_1, \dots, x_m)}{g_n(x_1, \dots, x_n)}\Big),$$

as in Definition 9.2.1.

But if we now define $V' = V \cap Y$, then $V'$ is a neighbourhood of $P$ in $Y$ which is contained in an affine space, and $\varphi$ is of course given by exactly the same formula as $\iota\varphi$. Thus $\varphi$ is itself a morphism. □

## 10. Products of algebraic sets

There is an obvious identification $\mathbb{A}^m(\Omega) \times \mathbb{A}^n(\Omega) \xrightarrow{\sim} \mathbb{A}^{m+n}(\Omega)$, and it is clear that via this identification, the product of two affine algebraic sets becomes identified with an affine algeraic set in $\mathbb{A}^{m+n}(\Omega)$. For more general quasi-projective algebraic sets, it is less obvious how to regard their product as an algebraic set.

In Subsection 8.5 we considered the products $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$, and described how to cut out algebraic subsets of these products: namely, via polynomials (or ideasl) that were arbitrary in the coordinates on $\mathbb{A}^m$, but homogeneous in the coordinates on $\mathbb{P}^n$. It is easy to see, then, that the product of an affine algebraic set and a projective algebraic set forms an algebraic set in $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ (for the appropriate choice of $m$ and $n$).

We could use the same idea to cut out algebraic subsets of $\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega)$, namely via polynomials (or ideals) that are bihomogeneous in the two sets of homogeneous coordinates. A product of two projective algebraic sets could then be regarded as an algebraic set in $\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega)$ (again, for the appropriate choices of $m$ and $n$).

However, this is not a very convenient way to think about products, for example because it means that we leave the worlds of quasi-projective algebraic sets; to get a complete theory that allowed us to form arbitrary products we would have to consider locally subsets of $\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega)$, and then (to form products of those with quasi-projective algebraic sets) $\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega) \times \mathbb{P}^p(\Omega)$, and so on.

To avoid having to work with this proliferation of products of projective spaces, it is convenient to once and for all identify the product $\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega)$ with a projective algebraic set in $\mathbb{P}^{mn+n+n}(\Omega)$, via the so-called *Segre embedding*. We discuss this next.

## 10.1. **Products of projective spaces and the Segre embedding.**

10.1.1. **Definition.** Let $x_0, \ldots, x_m$ denote homogeneous coordinates on $\mathbb{P}^m$, and let $y_0, \ldots, y_n$ denote homogeneous coordinates on $\mathbb{P}^n$. The Segre embedding

$$\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega) \hookrightarrow \mathbb{P}^{mn+m+n}(\Omega)$$

is defined via

$$\begin{aligned}\big([x_0 : \ldots : x_m], [y_0 : y_1 : \ldots : y_n]\big) \\ \mapsto [x_0y_0 : x_0y_1 : \ldots : x_0y_n : x_1y_0 : \ldots : x_1y_n : \ldots : x_my_0 : \ldots : x_my_n].\end{aligned}$$

10.1.2. **Remark.** A little more abstractly (and a little more canonically), if $V$ is an $m+1$-dimensional vector space, with associated projective space $\mathbb{P}(V)$, and $W$ is an $n+1$-dimensional vector space, with associated projective space $\mathbb{P}(W)$, then the Segre embedding is the morphism

$$\mathbb{P}(V) \times \mathbb{P}(W) \to \mathbb{P}(V \otimes W)$$

associated to the universal bilinear map

$$V \times W \to V \otimes W.$$

The following lemma records the basic properties of the Segre embedding.

10.1.3. **Lemma.** *The Segre embedding is well-defined and injective (jusitfying its description as an* embedding*), and its image is a Zariski closed subset of* $\mathbb{P}^{mn+m+n}(\Omega)$.

*Proof.* We consider just the case $m = n = 1$, leaving the general case as an exercise.

Suppose that $([x_0 : x_1], [y_0 : y_1])$ is a point of $\mathbb{P}^1(\Omega)$. Then at least one of $x_0, x_1$ and at least one of $y_0, y_1$ is non-zero. and we may as well assume (after relabelling if necessary) that $x_0$ and $y_0$ are non-zero. The product $x_0y_0$ is then non-zero, and hence $[x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1]$ is a well-defined point of $\mathbb{P}^3(\Omega)$. Note that if we multiply either $(x_0, x_1)$ or $(y_0, y_1)$ by a non-zero scalar, then all the products $x_iy_j$ are multiplied by this same non-zero scalar, so that the point $[x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1]$ only depends on the points $[x_0 : x_1]$ and $[y_0 : y_1]$ of $\mathbb{P}^1(\Omega)$, and the Segre embedding is well-defined.

Suppose now that $\big([x_0 : x_1], [y_0 : y_1]\big)$ and $\big([x_0' : x_1'], [y_0' : y_1']\big)$ are two points in $\mathbb{P}^1(\Omega) \times \mathbb{P}^1(\Omega)$ with the same image in $\mathbb{P}^3(\Omega)$. Then, again, at least one of $x_0, x_1$ and at least one of $y_0, y_1$ is non-zero. and as before we may as well assume (after relabelling if necessary) that $x_0$ and $y_0$ are non-zero.

By assumption the points $[x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1]$ and $[x_0'y_0' : x_0'y_1' : x_1'y_0' : x_1'y_1']$ coincide, meaning that there is a non-zero scalar $\lambda \in \Omega$ such that

$$(x_0'y_0', x_0'y_1', x_1'y_0', x_1'y_1') = \lambda(x_0y_0, x_0y_1, x_1y_0, x_1y_1). \tag{10.1.4}$$

In particular, we see that $x_0'y_0' = \lambda x_0y_0$ is non-zero, so that both $x_0'$ and $y_0'$ are also non-zero. Then, we find that

$$x_1'/x_0' = x_1'y_1'/x_0'y_1' = x_1y_1/x_0y_1 = x_1/x_0,$$

and hence $[x_0 : x_1]$ and $[x'_0 : x'_1]$ are the same point of $\mathbb{P}^1(\Omega)$. A similar calculation shows that $[y_0 : y_1]$ and $[y'_0 : y'_1]$ are the same point of $\mathbb{P}^1(\Omega)$. Thus the Segre embedding is injective, as claimed.

(Another way to phrase this last computation, which makes it even more transparent — and which can help when extending it to the general case — is to note that since $x_0, y_0$, $x'_0$, and $y'_0$ are all non-zero, we may as well assume — by rescaling — that they are all equal to 1, so that our points have the form $([1 : x_1], [1 : y_1])$ and $([1 : x'_1], [1 : y'_1])$. In this case the equation (10.1.4) simplifies to

$$(1, x'_1, y'_1, x'_1 y'_1) = \lambda(1, x_1, y_1, x_1 y_1).$$

Obviously, then, we must have $\lambda = 1$, yielding $x'_1 = x_1$, $y'_1 = y_1$, as required.)

Let $x, y, z, w$ denote the homogeneous coordinates on $\mathbb{P}^3(\Omega)$. Then one immediately verifies that the image of the Segre embedding is contained in the zero locus of $xw - yz$. Conversely, suppose that $[x : y : z : w] \in \mathbb{P}^3(\Omega)$ satisfies $xw = yz$; we will show that this point lies in the image of the Segre embedding. At least one of $x, y, z$, or $w$ is non-zero; an obvious consideration of the symmetry of the situation shows that it suffices to treat the case where $x \neq 0$. Then one checks that

$$\big([x : z], [x : y]\big) \mapsto [x^2 : xy : xz : yz] = [x^2 : xy : xz : xw] = [x : y : z : w]$$

(the second-to-last equality using our assumption that $xw = yz$, and the final equality applying a rescaling of the homogeneous coordinates by $x^{-1}$) under the Segre embedding. Thus the image of the Segre embedding precisely the zero locus of $xw - yz$, and so we've proved that the image of the Segre embedding is Zariski closed, as required. □

Our next lemma confirms that we have achieved our goal, namely that we can take products of quasi-projective algebraic sets without leaving the category of quasi-projective algebraic sets.

10.1.5. **Lemma.** *If $X$ and $Y$ are (quasi-)projective algbraic sets, say contained as (locally) closed subsets in $\mathbb{P}^m(\Omega)$ and $\mathbb{P}^n(\Omega)$, then the image of $X \times Y$ under the Segre embedding $\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega) \hookrightarrow \mathbb{P}^{mn+m+n}(\Omega)$ is a (locally) closed subset of $\mathbb{P}^{mn+m+n}(\Omega)$.*

*Proof.* We first reduce the quasi-projective case to the projective case. If $X$ is locally closed, and we let $Z$ denote its closure, than the complement $W$ of $X$ in $Z$ is closed, and so $X = Z \setminus W$ is expressed as a difference of closed subsets of $\mathbb{P}^m(\Omega)$. Similarly, we may write $Y = S \setminus T$ as the difference of closed subsets of $\mathbb{P}^n(\Omega)$. The product $X \times Y$ is then equal to the difference $Z \times S \setminus (Z \times T \cup W \times S)$. If we have proved that the product of closed sets maps to a closed set under the Segre embedding, then we see that this does indeed express $X \times Y$ as a difference of closed sets, and hence that $X \times Y$ has locally closed image under the Segre embedding.

Since $X \times Y = \big(X \times \mathbb{P}^n(\Omega)\big) \cap \big(\mathbb{P}^m(\Omega) \times Y\big)$, we further reduce to the case where one of $X$ or $Y$ is all of projective space. It obviously suffices to consider the case when $Y = \mathbb{P}^n(\Omega)$, since the other case will be handled identically. Now we may write $X = Z_I(\Omega)$ for some homogeneous ideal $I$. Since then $X = \cap_{F \in I} Z_{(F)}(\Omega)$, where $F$ runs over all the homogeneous ideals in $I$, and since a product of intersections is equal to the intersection of the products, we reduce to the case where $X$ is the zero locus of a single homogeneous polynomial $F(x_0, \ldots, x_m)$.

As before, we now restrict to the case $m = n = 1$ (basically so as to simplifty the indices), leaving the general case as an exercise. As in the proof of the previous

lemma, let $x, y, z, w$ denote the homogeneous coordinates on $\mathbb{P}^3(\Omega)$, so that the Segre embedding is defined by

$$x = x_0y_0, y = x_0y_1, z = x_1y_0, w = x_1y_1.$$

Let $d$ denote the degree of $F$. Then we can find homogeneous polynomials of degree $d$, say $F_0(x, z)$ and $F_1(y, w)$, so that $F_0(x_0y_0, x_1y_0) = y_0^d F(x_0, x_1)$, and $F_1(x_0y_1, x_1y_1) = y_1^d F(x_0, x_1)$. Since at least one of $y_0$ and $y_1$ is non-zero at any point of $\mathbb{P}^1(\Omega)$, we then see that the image of $X \times \mathbb{P}^1(\Omega)$ is equal to the intersection of the image of $\mathbb{P}^1(\Omega) \times \mathbb{P}^1(\Omega)$ with zero locus of the homogeneous ideal $\big(F_0(x, z), F_1(y, w)\big)$; in particular, it is Zariski closed. □

The following definition records the key application of the Segre embedding that is provided by the preceding lemma.

10.1.6. **Definition.** If $X$ and $Y$ are two quasi-projective algebraic sets, then we regard $X \times Y$ as a quasi-projective algebraic set by identifying with its image under the Segre embedding.

The next result follows directly from what we have proved, but it is important, and so is worth recording.

10.1.7. **Lemma.** *If $X$ and $Y$ are quasi-projective algebraic sets.*

(1) *If $Z$ and $W$ are closed subsets of $X$ and $Y$ respectively, then $Z \times W$ is a closed subset of $X \times Y$.*
(2) *If $U$ and $V$ are open subsets of $X$ and $Y$ respectively, then $U \times V$ is an open subset of $X \times Y$.*

*Proof.* Suppose that $X$ is locally closed in $\mathbb{P}^m(\Omega)$, and that $Y$ is locally closed in $\mathbb{P}^n(\Omega)$. We may write $Z = X \cap Z'$ for some closed subset $Z'$ of $\mathbb{P}^m(\Omega)$ (by definition of the induced topology), and may similarly write $W = Y \cap W'$ for some closed subset $W'$ of $\mathbb{P}^n(\Omega)$.

Then $Z \times W = (X \times Y) \cap (Z' \times W')$. Lemma 10.1.5 shows that $Z' \times W'$ is closed in $\mathbb{P}^{mn+m+n}$, and thus that $Z \times W$ is closed in $X \times Y$.

Note that claim (2) follows formally from claim (1), since

$$U \times V = X \times Y \setminus \big(X \times (Y \setminus V) \cup (X \setminus V) \times Y\big).$$

□

One way to state the preceding result is that the Zariski topology on $X \times Y$ is stronger than the product topology. (Note that typically it is genuinely stronger than the product topology; indeed it will be so unless one of $X$ or $Y$ is a finite set.)

10.2. **Products of affine spaces.** We now have two ways to think about a product of affine spaces $\mathbb{A}^m(\Omega) \times \mathbb{A}^n(\Omega)$ as a quasi-projective variety: there is the obvious identification $\mathbb{A}^m(\Omega) \times \mathbb{A}^n(\Omega) \xrightarrow{\sim} \mathbb{A}^{m+n}(\Omega)$, and there is the quasi-projective algebraic set struture it obtains via our general construction in terms of the Segre embedding. The next lemma shows that these coincide.

10.2.1. **Lemma.** *The natural identification $\mathbb{A}^m(\Omega) \times \mathbb{A}^n(\Omega) \xrightarrow{\sim} \mathbb{A}^{m+n}(\Omega)$ is an isomorphism of quasi-projective varieties, if we endow the source with its quasi-projective algebraic set structure via Definition* 10.1.6 *and we endow the target with its natural affine algebraic set structure.*

*Proof.* This is just a matter of showing that this identification, and its inverse, are both morphisms. As usual, we treat the case $m = n = 1$ here, leaving the general case an an exercise.

We use the coordiantes $[x_0 : x_1]$ and $[y_0 : y_1]$ on our two copies of $\mathbb{P}^1(\Omega)$, and corresponding affine coordinates $x_1/x_0$ and $y_1/y_0$ on our two copies of $\mathbb{A}^1(\Omega)$. We use the coordinates $x, y, z, w$ on $\mathbb{P}^3(\Omega)$, and we recall that the Segre embedding is given by

$$x = x_0y_0, y = x_0y_1, z = x_1y_0, w = x_1y_1.$$

The image of $\mathbb{A}^1(\Omega) \times \mathbb{A}^1(\Omega)$ lies in the copy of $\mathbb{A}^3(\Omega) \subset \mathbb{P}^3(\Omega)$ given by $x \neq 0$, whose affine coordinates are $y/x, z/x, w/x$.

In terms of these coordiantes, the map $\mathbb{A}^1(\Omega) \times \mathbb{A}^1(\Omega) \to \mathbb{A}^2(\Omega)$ is given by the formula

$$(\frac{y}{x}, \frac{z}{x}, \frac{w}{x}) \mapsto (\frac{z}{x}, \frac{y}{x}),$$

and its inverse is given by

$$(\frac{x_1}{x_0}, \frac{y_1}{y_0}) \mapsto (\frac{y_1}{y_0}, \frac{x_1}{x_0}, \frac{x_1}{x_0}\frac{y_1}{y_0}).$$

These are polynomial formulas in the various affine coordiantes, and so are indeed morphisms. □

10.3. **Products of algebraic sets as categorical products.** If $X$ and $Y$ are quasi-projective algebraic sets, then we have seen that $X \times Y$ is again a quasi-projective algebraic set. Our goal in this subsection is to show that $X \times Y$ is equal to the *categorical product* of $X$ and $Y$.

We begin with the following lemma, showing that the projections from a product to its factors are morphisms.

10.3.1. **Lemma.** *If $X$ and $Y$ are quasi-projective algebraic sets (so that $X \times Y$ is also a quasi-projective algebraic set), then the projection morphisms $X \times Y \to X$ and $X \times Y \to Y$ (defined by $(P, Q) \mapsto P$ and $(P, Q) \mapsto Q$) are morphisms*

*Proof.* Obviously it suffices to prove the lemma for the projection onto $X$; the case of the projection onto $Y$ will proceed in a completely analogous manner.

Suppose that $X$ is locally closed in $\mathbb{P}^m(\Omega)$ and that $Y$ is locally closed in $\mathbb{P}^n(\Omega)$, so that $X \times Y$ is locally closed in $\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega)$. Then applying Lemma 9.2.6 to these various locally closed embeddings, we see that it suffices to prove the lemma in the particular case when $X = \mathbb{P}^m(\Omega)$ and $Y = \mathbb{P}^n(\Omega)$.

Let $(P, Q)$ be a point of $\mathbb{P}^m(\Omega) \times \mathbb{P}^n(\Omega)$. Choosing coordinates appropriately, we may assume that $(P, Q) \in \mathbb{A}^m(\Omega) \times \mathbb{A}^n(\Omega)$. Lemma 10.2.1 then allows us to identify $\mathbb{A}^m(\Omega) \times \mathbb{A}^n(\Omega)$ with $\mathbb{A}^{m+n}(\Omega)$, and it suffices to show that the projection $\mathbb{A}^{m+n}(\Omega) \to A^m(\Omega)$ given by mapping to the first $m$ coordinates is a morphism. But this is obvious. □

The following lemma now shows that the product of quasi-projective varieties, as we have defined it, serves as a categorical product.

10.3.2. **Lemma.** *Let $X, Y$, and $Z$ be quasi-projective algebraic sets, and let $\varphi : Z \to X$ and $\psi : Z \to Y$ be functions. Then $\varphi$ and $\psi$ are morphisms if and only if their product $(\varphi, \psi) : Z \to X \times Y$, defined by $P \mapsto (\varphi(P), \psi(P))$, is a morphism.*

*Proof.* If $(\varphi, \psi)$ is a morphism, then so are of $\varphi$ and $\psi$, since these are obtained by composing $(\varphi, \psi)$ with the projections onto $X$ and $Y$ respectively, and Lemma 10.3.1 shows that each of these projections is a morphism (and the composite of morphisms is a morphism).

Conversely, suppose that each of $\varphi$ and $\psi$ is a morphism. Suppose that $X$ is locally closed in $\mathbb{P}^m(\Omega)$ and $Y$ is locally closed in $\mathbb{P}^n(\Omega)$. Let $\mathbb{P}^N(\Omega)$ be the projective space containing $Z$. Let $P$ be a point of $Z$, and consider $\varphi(P)$. Since $\varphi$ is a morphism, we may find a neighbourhood of $U$ of $P$, contained in a copy of $\mathbb{A}^N(\Omega)$ contained in $\mathbb{P}^N(\Omega)$, and a neighbourhood $V$ of $\varphi(P)$, contained in a copy of $\mathbb{A}^m(\Omega)$ inside $\mathbb{P}^n(\Omega)$, so that $\varphi_{|U}$ is given by a formula involving rational functions in the coordinates $u_1, \ldots, u_N$ on $\mathbb{A}^N(\Omega)$. We may find neighbourhoods $U'$ of $P$ and $V'$ of $\psi(P)$ satisfying the analogous condition for $\psi$.

Now replacing $U$ and $U'$ by $U \cap U'$, and taking into account Remark 9.2.3, we may assume that $U = U'$, both contained in $\mathbb{A}^N(\Omega)$. We will show that $(\varphi_{|U}, \psi_{|U}) : U \to X \times Y$ is a morphism. It will follow by Lemma 9.2.5 that $(\varphi, \psi)$ itself is a morphism. Now $\varphi_{|U}$ factors through $V$ and $\psi_{|U}$ factors through $V'$, and $V \times V'$ is open in $X \times Y$ and locally closed in $\mathbb{A}^m(\Omega) \times \mathbb{A}^n(\Omega)$ (by Lemma 10.1.7). Thus by Lemma 9.2.6, it suffices to prove that the function $U \to \mathbb{A}^m(\Omega) \times \mathbb{A}^n(\Omega)$ induced by $(\varphi_{|U}, \psi_{|U})$ is a morphism. By Lemma 10.2.1, it in fact suffices to show that this function is a morphism, when regarded as taking values in $\mathbb{A}^{m+n}(\Omega)$. But since each of $\varphi_{|U}$ and $\psi_{|U}$ is given by a formula in terms of rational functions whose denominators are nowhere vanishing on $U$, the same is true of this map $U \to \mathbb{A}^{m+n}(\Omega)$, and thus it is also a morphism, as required. □

As one consequence of the preceding results, we can show that a product of morphisms is a morphism. (This is just a specialization to our particular context of a general argument about categorical products.)

10.3.3. **Lemma.** *Suppose that $X, Y, Z,$ and $W$ are algebraic sets, and that $\varphi : X \to Y$ and $\psi : Z \to W$ are morphisms. Then the product map $\varphi \times \psi : X \times Z \to Y \times W$ is a morphism.*

*Proof.* To check this, it suffices, by the preceding lemma, to check that each of the momorphisms $X \times Z \to Y$ (given by projecting to $X$, and then applying $\varphi$) and $X \times Z \to W$ (given by projecting to $Z$, and then applying $\psi$) is a morphism. But Lemma 10.3.1 shows that each of these maps is a composite of morphisms, and hence is indeed a morphism. □

10.4. **Diagonals and graphs.** Let $\varphi : X \to Y$ be a morphism of quasi-projective algebraic sets. Applying Lemma 10.3.2 to the pair of morphisms consisting of $\mathrm{id}_X : X \to X$ and $\varphi : X \to Y$, we obtain a morphism $X \to X \times Y$ given by $P \mapsto \big(P, \varphi(P)\big)$. For obvious reasons, we refer to this morphism as the *graph* of $\varphi$, and denote it by $\Gamma_\varphi$.

A special case is given by taking $\varphi = \mathrm{id}_X$ as well. In this case, we write $\Delta_X : X \to X \times X$ rather than $\Gamma_{\mathrm{id}_X}$, since this is simply the diagonal map $P \mapsto (P, P)$.

10.4.1. **Lemma.** *If $\varphi : X \to Y$ is a morphism, then $\Gamma_\varphi : X \to X \times Y$ has closed image, and induces an isomorphism from $X$ to its image.*

*Proof.* Lemma 10.3.1 shows that $X \to X \times Y$ is a morphism, and obviously, when restricted to the image $\Gamma_f(X)$, it provides an inverse to $\Gamma_f$. Thus all that remains to show is that $\Gamma_f(X)$ is closed.

Morally, this is true because

$$\Gamma_f(X) = \{(P, Q) \in X \times Y \,|\, \varphi(P) = Q\},$$

and since $\varphi$ is a morphism, this equation cuts out a Zariski closed set. However, writing this out directly is slightly messy, and we can argue in a slightly less direct way.

Namely, observe that $\Gamma_f(X)$ is the preimage under the morphism $\varphi \times \mathrm{id}_Y$ of $\Delta_Y(Y) \subset Y \times Y$. Since $\varphi \times \mathrm{id}_Y$ is a morphism (by Lemma 10.3.3) is it continuous for the Zariski topologies on its source and target, and so it suffices to show that $\Delta_Y(Y)$ is a closed subset of $Y \times Y$. If $Y$ is locally closed in $\mathbb{P}^n(\Omega)$, then $\Delta_Y(Y) = \Delta_{\mathbb{P}^n(\Omega)} \cap (Y \times Y)$, and so it suffices to show that $\Delta_{\mathbb{P}^n(\Omega)}\big(\mathbb{P}^n(\Omega)\big)$ is closed in $\mathbb{P}^n(\Omega) \times \mathbb{P}^n(\Omega)$.

We check this in the case $n = 1$, leaving the case of general $n$ as an exercise. In this case, we recall that $\mathbb{P}^1(\Omega) \times \mathbb{P}^1(\Omega)$ is identified with the zero locus of $xw - yz$ in $\mathbb{P}^3(\Omega)$ via the embedding

$$x = x_0y_0, y = x_0y_1, z = x_1y_0, w = x_1y_1,$$

We then see that $\Delta_{\mathbb{P}^1(\Omega)}\big(\mathbb{P}^1(\Omega)\big)$ is cut out by the additional equation $y = z$; in particular, it is Zariski closed. □

By construction, we may factor any morphism $\varphi : X \to Y$ through its graph: $\varphi$ is given as the composite

$$X \overset{\Gamma_\varphi}{\hookrightarrow} X \times Y \to Y.$$

This is is often useful, since it factors the arbitrary morphism $\varphi$ as the composite of a closed embedding and a projection.

10.5. **Elimination theory, revisited.** There is one more important detail that we have to check with regard to the Segre embedding. Namely, we may restrict the Segre embedding to $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$, and we now have two ways to impose a Zariski topology on this product: using the approach of Subsection 8.5 above, or by regarding it as a subset of $\mathbb{P}^{mn+m+n}(\Omega)$ via the (restriction of) the Segre embedding.

10.5.1. **Lemma.** *The restriction of the Segre embedding to $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ embeds it as a locally closed subset of $\mathbb{P}^{mn+m+n}(\Omega)$, and the Zariski topology defined on $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ in Subsection 8.5 coincides with the Zariski topology induced on it by regarding it as a locally closed subset of $\mathbb{P}^{mn+m+n}(\Omega)$ via the Segre embedding.*

*Proof.* Again, we treat just the case $m = n = 1$, leaving the general case as an exercise. We may identify $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ as the subset of points of the form $\big([x_0 : x_1], [y_0 : y_1])\big)$ in $\mathbb{P}^1(\Omega)$ for which $x_0 \neq 0$.

Since $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ is a product of quasi-projective varieties, the first claim of the lemma is a special case of the Lemma 10.1.5. However, it won't hurt to prove this special case explicitly. As in the proof of Lemma 10.1.3, let $x, y, z, w$ be the homogeneous coordiantes on $\mathbb{P}^3(\Omega)$. The Segre embedding is defined by

$$x = x_0y_0, y = x_0y_1, z = x_1y_0, w = x_1y_1.$$

Since $x_0 \neq 0$, and at least one of $y_0$ or $y_1$ is non-zero, we see that the image of $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ coincides precisely with the complement in the zero locus of $xw - yz$ (which we recall from the proof of Lemma 10.1.3 coincides with the image of the Segre embedding on $\mathbb{P}^1(\Omega) \times \mathbb{P}^1(\Omega)$) of the zero locus of the homogeneous ideal $(x, y)$. Thus this image is locally closed in $\mathbb{P}^3(\Omega)$, as claimed.

If we write $t = x_1/x_0$, so that $t$ is a coordinate on $\mathbb{A}^1(\Omega)$, then we see that for any homogeneous polynomial $F(x, y, z, w)$, the intersection of the zero locus of $F$ with the image of $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ is equal to the zero locus of the polynomial $F(y_0, y_1, ty_0, ty_1)$, which is then homogeneous in the $y$ variables. This shows that the preimage, under the Segre embedding, of any Zariski closed subset of $\mathbb{P}^3(\Omega)$ is a Zariski closed subset of $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$, in the sense of Subsection 8.5.

Conversely, suppose that $f(t, y_0, y_1)$ is a polynomial that is homogeneous in the $y$ variables. We wish to show that the image of its zero locus in $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ under the Segre embedding is the intersection of the image of $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ with a Zariski closed subset of $\mathbb{P}^3(\Omega)$.

Let $d$ denote the degree of $f(t, y_0, y_1)$ with respect to $t$ (i.e. the largest power of $t$ appearing in $f$), and define $f_0(t, y_0, y_1) = y_0^d f_0(t, y_0, y_1)$ and $f_1(t, y_0, y_1) = y_1^d f(t, y_0, y_1)$. Note that since at any point of $\mathbb{P}^1(\Omega)$ at least one of $y_0$ or $y_1$ is non-zero, the zero locus of $f$ in $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ coincides with the common zero locus of $f_0$ and $f_1$. Note also that we may then find homogeneous polynomials $F_0(x, y, z)$ and $F_1(x, y, w)$ such that $f_0 = F_0(y_0, y_1, y_0 t)$ and $f_1 = F_1(y_0, y_1, y_1 t)$. Thus we see that the image of the zero locus of $f$ in $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ under the Segre embedding is equal to the intersection of the image of $\mathbb{A}^1(\Omega) \times \mathbb{P}^1(\Omega)$ with the zero locus of the ideal $(F_0, F_1)$. This completes the proof of the lemma. □

With the previous lemma in hand, we are now able to extend Theomem 8.6.1 (the main theorem of elimination theory) in the following manner.

10.5.2. **Theorem.** *Suppose that $\Omega$ satisfies the Nullstellensatz. If $X$ is any quasi-projective algebraic set, and $Y$ is any projective algebraic set, then the projection morphism $X \times Y \to X$ is a closed map.*

*Proof.* If we choose $n$ so that $Y$ is a closed subset of $\mathbb{P}^n(\Omega)$, then $X \times Y$ is a closed subset of $X \times \mathbb{P}^n(\Omega)$ (by Lemma 10.1.7), and so it suffices to consider the case when $Y = \mathbb{P}^n(\Omega)$.

A simple topological argument shows that it suffices to find a cover of $X$ by open sets $U$ such that the projection $U \times \mathbb{P}^n \to U$ is closed. (This uses the fact that the sets $U \times \mathbb{P}^n$ then provide an open cover of $X \times \mathbb{P}^n$, by Lemma 10.1.7.)

As already noted in Remark 9.1.3, if $X$ is locally closed in $\mathbb{P}^m(\Omega)$, then each point $P \in X$ has an open neighbourhood $U$ contained in a copy of $\mathbb{A}^m(\Omega)$ inside $\mathbb{P}^m(\Omega)$.

Now the morphism $\mathbb{A}^m(\Omega) \to \mathbb{P}^n(\Omega) \to \mathbb{A}^m(\Omega)$ is closed, by Theorem 8.6.1 (and here we apply Lemma 10.5.1 to see that there is no ambiguity in the topology on $\mathbb{A}^m(\Omega) \times \mathbb{P}^n(\Omega)$ for which this holds), and hence its restriction $U \times \mathbb{P}^n(\Omega) \to U$ is closed as well. This proves the theorem. □

We have the following important corollary.

10.5.3. **Corollary.** *Suppose that $\Omega$ satisfies the Nullstellensatz. If $X$ is a projective algebraic set, then any morphism $\varphi : X \to Y$ to a quasi-projective algebraic set is closed.*

*Proof.* We factor $\varphi$ as

$$X \overset{\Gamma_\varphi}{\hookrightarrow} X \times Y \to Y.$$

The first morphism is a closed embedding, and the second morphism is closed, by the preceding theorem. Thus the composite of these two morphisms, which is to say $\varphi$, is closed. □

## 11. The Nullstellensatz

11.1. **The Nullstellensatz for algebraically closed fields.** Let $\overline{k}$ be an algebraic closure of $k$.

11.1.1. **Theorem.** *If $I \subseteq k[x_1, \dots, x_n]$ is an ideal, and if $Z_I(\Omega) \neq \emptyset$ for some field extension $\Omega$ of $k$, then $Z_I(\overline{k}) \neq \emptyset$.*

*Proof.* Evidently, replacing $I$ by the ideal it generates in $\overline{k}[x_1, \dots, x_n]$, we may suppose that $k = \overline{k}$. Also, replacing $\Omega$ by a universal domain which contains it, we may assume that $\Omega$ is a universal domain, and hence satisfies the Nullstellensatz. (This will allow us to apply the main theorem of elimination theory, and its corollaries.)

We proceed by induction on $n$, the result being clear if $n = 0$. If $I$ is zero, then there is nothing to prove. Thus we may assume that $I \neq 0$, and hence that $Z_I(\Omega) \neq \mathbb{A}^n(\Omega)$. Write $Z := Z_I(\Omega)$, and consider the projective closure $\overline{Z}$ of $Z$ in $\mathbb{P}^n$. Since $Z \neq \mathbb{A}^n(\Omega)$, we have that $\overline{Z}$ does not contain the entire hyperplane $H$ at infinity, and thus by Lemma 6.3.3 we may find a $k$-valued point $P$ of $H$ (the hyperplane at infinity) that does not lie in $\overline{Z}$.

Let $H'$ be a hyperplane in $\mathbb{P}^n(\Omega)$ defined over $k$ which does not contain $P$. Consider the "projection from a point" $\mathbb{P}^n(\Omega) \setminus \{P\} \to H'$. This is a morphism (check!), and so its restriction to $\overline{Z}$ is a morphism.

Corollary 10.5.3 implies that the image of $\overline{Z}$ in $H'$ (which is a copy of $\mathbb{P}^{n-1}(\Omega)$) is closed. Since $P$ lies in the hyperplane at infinity, a point in the image of $\overline{Z}$ lies at infinity if and only if it is the image of a point at infinity in $\overline{Z}$ if and only if its entire preimage in $\overline{Z}$ lies at infinity. Thus the image of $Z$ under projection from $P$ consists precisely of those points in the image of $\overline{Z}$ which do not lie at infinity; thus this image is a closed subspace of $H' \setminus H$ (which is a copy of $\mathbb{A}^{n-1}(\Omega)$). It is non-empty, since $Z$ is, and hence by induction we may assume that it contains a $k$-valued point $Q$.

Now consider the line $\ell$ joining $P$ and $Q$. This line is defined over $k$ (since it joins two points with coordinates in $k$), and its intersection with $\overline{Z}$ is a Zariski closed subset. It is non-empty (since $Q$ is in the image of $\overline{Z}$ under the projection from $P$ to $H'$). Now a Zariksi closed subset of a line over $k$ consists of either the entire line (in fact, this is not the case in our situation, since $P \notin \overline{Z}$) or of a finite number of points defined over $k$ (since it is obtained by solving a polynomial in one variable with coefficients in $k$, and $k$ is algebraically closed). Thus $\ell \cap \overline{Z}$ contains a point defined over $k$. Since $Q$ does not lie on $H$, neither does this point, and so in fact we have constructed a point of $Z$ defined over $k$, as required. □

11.1.2. **Corollary.** *If $I \subseteq k[x_1, \dots, x_n]$ is an ideal, then $Z_I(\overline{k}) = \emptyset$ if and only if $I = k[x_1, \dots, x_n]$.*

*Proof.* Since $k$ can be embedded into a universal domain $\Omega$, this follows immediately from Theorems 6.6.1 and 11.1.1. □

11.1.3. **Corollary.** *A field* satisfies the Nullstellensatz (*in the sense of Subsection* 6.7) *if and only if it is algebraically closed.*

*Proof.* The preceding corollary precisely shows that algebraically closed fields satisfy the Nullstellensatz. Conversely, if a field satisfies the Nullstellensatz, then any non-constant element of $k[x]$ must have a zero in $k$, and thus $k$ must be algebraically closed. □

Thus all our results on fields that satisfy the Nullstellensatz apply to arbitrary algebraically closed fields.

## 12. Regular functions on affine algebraic sets

12.1. **Affine neighbourhoods.** As we noted in Remark 9.1.3, if $X$ is a quasi-projective algebraic set, contained in $\mathbb{P}^n(\Omega)$, then each point $P \in X$ has an open neighbourhood $U$ which is contained in $\mathbb{A}^n(\Omega)$ (for an appropriate choice of coordinates on $\mathbb{P}^n(\Omega)$).

In this section we record a much more precise result, which is a consequence of the Rabinowitz trick, and is extremely useful in many situations.

12.1.1. **Proposition.** *If $X$ is a quasi-projective algebraic set, then each point of $X$ has a neighbourhood basis consisting of open subsets that are isomorphic to affine algebraic sets.*

*Proof.* Let $P \in X \subset \mathbb{P}^n(\Omega)$, and (as in Remark 9.1.3) choose coordinates on $\mathbb{P}^n(\Omega)$ so that $P \in \mathbb{A}^n(\Omega)$. Replacing $X$ by $U := X \cap \mathbb{A}^n(\Omega)$ (which is an open subset of $X$ containing $P$), we may assume that $X$ is in fact locally closed in $\mathbb{A}^n(\Omega)$. We may thus write $X = Z \setminus W$, for some closed subsets $Z$ and $W$ of $\mathbb{A}^n(\Omega)$ (with $P \in Z$ and $P \notin W$).

Now any open neighbourhood $V$ of $P$ is (by definition of the induced topology) of the form $X \setminus Y$, for some closed subset $Y$ of $\mathbb{A}^n(\Omega)$. We may thus write $V = Z \setminus (W \cup Y)$. Now the closed set $W \cup Y$ is the zero locus of some ideal $I \in k[x_1, \dots, x_n]$ (where the $x_i$ are coordinates on $\mathbb{A}^n(\Omega)$). Since $P \in V$, there is some element $f \in I$ such that $f(P) \neq 0$, and so if we let $T$ denote the zero locus of $f$, then $P \notin T$, while $T \supset W \cup Y$, and so $Z \setminus T$ is an open neighbourhood of $P$ in $X$ which is contained in $V$.

The Rabinowitz trick shows that $\mathbb{A}^n(\Omega) \setminus T$ is isomorphic to a closed subset of $\mathbb{A}^{n+1}(\Omega)$, and so $Z \setminus T$, which is a closed subset of $\mathbb{A}^n(\Omega) \setminus T$, is also isomorphic to a closed subset of $\mathbb{A}^{n+1}(\Omega)$. Thus we have shown that $V$, which was an arbitrary neighbourhood of $P$, contains an open neighbourhood of $P$ which is isomorphic to an affine algebraic set. □

12.1.2. **Remark.** We will frequently engage in a common abuse of language, and say that a quasi-projective algebraic set is *affine* provided that it is *isomorphic* to an affine algebraic set. Admitting this abuse of language, the preceding theorem is usually stated in the form "each point of a quasi-projective algebraic set admits a basis of open affine neighbourhoods".

12.2. **Rings of regular functions, and an equivalence of categories.**

12.2.1. **Definition.** If $X$ is an affine algebraic set, then we let $k[X]$ denote the set of morphisms from $X$ to $\mathbb{A}^1$. The set $k[X]$ is naturally a $k$-algebra under pointwise addition and multiplication, and we refer to it as the *ring of regular functions* on $X$*, or sometimes as the* affine ring *of* $X$*.*

12.2.2. **Theorem.** *If $X = Z_I(\Omega) \subset \mathbb{A}^n(\Omega)$, for an ideal $I \subset k[x_1, \dots, x_n]$, then there is a natural isomorphism $k[x_1, \dots, x_n]/\mathrm{rad}(I) \xrightarrow{\sim} k[X]$.*

12.2.3. **Theorem.** *The passage from $X$ to $k[X]$ induces an anti-equivalence of categories between the category of affine algebraic sets and the category of reduced, finitely generated $k$-algebras.*

## 13. Proper, projective, and finite morphisms, and Chevalley's theorem

### 13.1. **Projective and proper morphisms.**

13.1.1. **Definition.** A morphism $\varphi : X \to Y$ of quasi-projective algebraic sets is called *projective* if it may be factored as

$$X \hookrightarrow Y \times \mathbb{P}^n(\Omega) \to Y,$$

where the first morphism is a closed embedding (i.e. has closed image, and induces an isomorphism of $X$ onto its image), and the second morphism is simply the projection onto $Y$.

13.1.2. **Definition.** A morphism $\varphi : X \to Y$ of quasi-projective algebraic sets is called *proper* if for any quasi-projective algebraic set $Z$, the induced morphism $\varphi \times \mathrm{id}_Z : X \times Z \to Y \times Z$ is *closed*.

13.1.3. **Theorem.** *A morphism is projective if and only if it is proper.*

*Proof.* Suppose first that $\varphi$ is projective, and choose a corresponding factorization

$$X \hookrightarrow Y \times \mathbb{P}^n(\Omega) \to Y$$

of $\varphi$. Taking the product with $Z$, we obtain a corresponding factorization of $\varphi \times \mathrm{id}_Z$, namely

$$X \times Z \hookrightarrow Y \times Z \times \mathbb{P}^n(\Omega) \to Y \times Z.$$

The first arrow comes from taking the product with a closed embedding, and so (by Lemma 10.1.7) is again a closed embedding, while the second arrow is simply the projection onto $Y \times Z$, and so is closed by Theorem 10.5.2. Thus $\varphi \times \mathrm{id}_Z$ is closed, and so $\varphi$ is proper.

Conversely, suppose that $\varphi$ is proper. Since $X$ is a quasi-projective variety, it is a locally closed subset of $\mathbb{P}^n(\Omega)$ for some $n$; let $\iota : X \to \mathbb{P}^n(\Omega)$ denote the inclusion. Then $\varphi$ admits the factorization

$$X \overset{(\varphi,\iota)}{\hookrightarrow} Y \times \mathbb{P}^n(\Omega) \to Y.$$

We will show that the first of these maps is a closed embedding, and thus that $\varphi$ is projective.

Firstly, consider the factorization

$$X \overset{\Gamma_\iota}{\hookrightarrow} X \times \mathbb{P}^n(\Omega) \overset{\varphi \times \mathrm{id}_{\mathbb{P}^n(\Omega)}}{\longrightarrow} Y \times \mathbb{P}^n(\Omega)$$

of $(\varphi, \iota)$. The first arrow is the graph of $\iota$, and so is closed by Lemma 10.4.1. The second arrow is the product of $\varphi$ with $\mathbb{P}^n(\Omega)$, and so is closed, since by assumption $\varphi$ is proper. Thus the composite of these morphisms (i.e. $(\varphi, \iota)$) is closed.

The morphism $(\varphi, \iota)$ admits an alternate factorization, namely as

$$X \overset{\Gamma_\varphi}{\hookrightarrow} X \times Y \overset{\iota \times \mathrm{id}_Y}{\longrightarrow} \mathbb{P}^n(\Omega) \times Y \cong Y \times \mathbb{P}^n(\Omega)$$

(where the last isomorphism just switches the two factors). The first of these arrows is a graph, hence is a closed embedding (by Lemma 10.4.1), and the second arrow is the product of the locally closed embedding $\iota$ with $\mathbb{P}^n(\Omega)$, and so is again a locally closed embedding (by Lemma 10.1.7); thus their composite (i.e. $(\varphi, \iota)$) is a locally closed embedding. We have already seen that $(\varphi, \iota)$ is closed, and so in fact it is a closed embedding, as required. □

13.2. **Finite morphisms and Chevalley's theorem.**

13.2.1. **Definition.** A morphism of rings $A \to B$ is said to be *finite* if it makes $B$ a finitely generated $A$-module.

13.2.2. **Remark.** The condition that $B$ be finitely generated over $A$ as a *module* is much stronger than the condition that it be finitely generated over $A$ as an algebra. For example, if $A = k$ is a field, then $k[x_1, \ldots, x_n]$ is certainly finitely generated as a $k$-algebra, but it is infinite-dimensional as a $k$-vector space.

13.2.3. **Definition.** We say that a morphism $\varphi : X \to Y$ of quasi-projective algebraic sets is *finite* if each point $P \in Y$ admits an open affine neighbourhood $U$ whose preimage $V := \varphi^{-1}(U)$ is again affine (in the sense that it is isomorphic to an affine algebraic set), and such that the induced morphism $\varphi^* : k[U] \to k[V]$ on affine rings (given by pull-back via $\varphi$) is a *finite* morphism.

13.2.4. **Example.** If $X$ is the zero locus of $y^2 - x$ in $\mathbb{A}^2(\Omega)$, and $Y = \mathbb{A}^1(\Omega)$, then the morphism $\varphi$ given by $(x, y) \mapsto x$ is finite. Indeed, we take $U = Y$ and $V = X$. The morphism $\varphi^*$ is then the inclusion $k[x] \hookrightarrow k[x, y]/(y^2 - x)$, and we note that

$$k[x, y]/(y^2 - x) = k[x]\langle 1, y\rangle$$

is free of rank two (and in particular finitely generated) as a $k[x]$-module.

13.2.5. **Example.** If $X$ is the zero locus of $xy - 1$ in $\mathbb{A}^2(\Omega)$, and $Y = \mathbb{A}^1(\Omega)$, then the morphism $\varphi$ given by $(x, y) \mapsto x$ is not finite.

Indeed, take $P$ to be the point $0 \in \mathbb{A}^1(\Omega)$. The open neighbourhood $U$ of $P$ are given by taking the complement of the zeroes of a polynomial $f(x)$ with non-constant term. (This last condition ensures that 0 is not a root of $f(x)$.) Such a neighbourhood $U$ is affine, with affine ring given by $k[x, 1/f]$. (This is a special case of the Rabinowitz trick.) The preimage of $U$ is then again affine, with affine ring given by $k[x, 1/f, y]/(xy - 1) = k[x, x^{-1}, 1/f]$. Since $f$ has non-zero constant term, it is easy to verify that $k[x, x^{-1}, 1/f]$ is not finitely generated as a module over $k[x, 1/f]$.

The preceding counterexample involves our favourite, and standard, illustration of the incompleteness of affine space, namely a hyperbola. Thus it will likely come as no surprise that finiteness of a morphism is related to projectivity of a morphism. The precise statement is given in the following theorem, which is due to Chevalley. It connects the algebraic concept of finiteness to the more geometric concepts of projectivity and finiteness of fibres.

13.2.6. **Theorem.** *A morphism of quasi-projective algebraic sets is finite if and only if it is projective with finite fibres.*

*Proof.* Suppose, to begin with, that $\varphi : X \to Y$ is a projective morphism of quasi-projective algebraic sets with finite fibres. We will show that $\varphi$ is finite.

By definition of projectivity, we may factor $\varphi$ as

$$X \hookrightarrow Y \times \mathbb{P}^n(\Omega) \to Y,$$

where the first arrow is a closed embedding, and the second arrow is the projection.

Let $P$ be a point of $Y$. By assumption $\varphi^{-1}(P)$ is finite, and so we may find a hyperplane $H \subset \mathbb{P}^n(\Omega)$ disjoint from $\varphi^{-1}(P)$.[8] Since $H$ is closed in $\mathbb{P}^n(\Omega)$, we see

[8]We want this hyperplane to be defined over $k$, so that we can choose coordinates on $\mathbb{P}^n$ so that it becomes the hyperplane at infinity, and so at this point we are tacitly assuming that $k$ is

that $Y \times H$ is closed in $Y \times \mathbb{P}^n(\Omega)$ (Lemma 10.1.7), and hence so is $X \cap (Y \times H)$. Theorem 10.5.2 then shows that the image of $X \cap (Y \times H)$ under the projection $Y \times \mathbb{P}^n(\Omega) \to Y$ is closed; denote its complement by $U'$. Our choise of $H$ ensures that $P \in U'$, and by construction we have that

$$\varphi^{-1}(U') \subset Y \times (\mathbb{P}^n(\Omega) \setminus H).$$

Let $U$ be an affine open neighbourhood of $P$ contained in $U'$. (We can find such a neighbourhood, by Proposition 12.1.1.) Then

$$\varphi^{-1}(U) = X \cap \big(U \times \mathbb{P}^n(\Omega)\big),$$

and so $\varphi^{-1}(U)$ is closed in $U \times \mathbb{P}^n(\Omega)$. On the other hand, since $U \subset U'$, we have that

$$\varphi^{-1}(U) \subset U \times \big(\mathbb{P}^n(\Omega) \setminus H\big),$$

and so in fact $\varphi^{-1}(U)$ is closed in $U \times \big(\mathbb{P}^n(\Omega) \setminus H\big)$. This latter set is a product of affine algebraic sets, and so is itself an affine algebraic set. Thus $\varphi^{-1}(U)$, being closed in an affine algebraic set, is itself an affine algebraic set.

Writing $V := \varphi^{-1}(U)$, it suffices to show that the morphism $k[U] \to k[V]$, induced by pull-back via $\varphi$, is a finite morphism of rings. To do this, we use the description of closed subsets of affine times projective space given in Subsection 8.5. We see that $V$, being a closed subset of $U \times \mathbb{P}^n(\Omega)$, is the zero locus of a homogeneous ideal $I \subset k[U][y_0, \dots, y_n]$, where the $y_i$ are homogeneous coordinates on $\mathbb{P}^n(\Omega)$.

Let's choose coordinates so that $H$ is cut out by $y_0 = 0$. Then, since in fact

$$V \subset U \times \big(\mathbb{P}^n(\Omega) \setminus H\big), \tag{13.2.7}$$

we find that the zero locus of the homogeneous ideal $(I, y_0)$ is empty. We deduce from Proposition 8.3.3 that $(I, y_0)_d = k[U][y_0, \dots, y_n]_d$ for some $d$. Thus, if $m_d$ is monomial of degree $d$ in the $y_i$, we may write

$$m_d = y_0 f_{d-1} + f_d, \tag{13.2.8}$$

where $f_d \in I$ and $f_{d-1}$ is homogeneous of degree $d-1$.

Now, again taking into account (13.2.7), we see that the affine ring $k[V]$ is obtained as the quotient $k[U][y_1/y_0, \dots, y_n/y_0]/\widetilde{I}$, where $\widetilde{I}$ is the ideal obtained by "dehomogenizing" $I$ with respect to $y_0$; i.e., it is the ideal generated by the polynomials $y_0^{-i} f_i$, where $f_i$ is a(n arbitrary) homogeneous element of $I$ of degree $i$.

Dehomogenizing the relation (13.2.8) in this way, we find that

$$y_0^{-d} m_d = y_0^{-(d-1)} f_{d-1} + y_0^{-d} f_d \equiv y_0^{-(d-1)} f_{d-1} \bmod \widetilde{I}.$$

Thus any element of $k[U][y_1/y_0, \dots, y_n/y_0]$ of degree $\geq d$ in the variables $y_i/y_0$ is congruent modulo $\widetilde{I}$ to an element of degree $\leq d-1$. Thus $k[U][y_1/y_0, \dots, y_n/y_0]/\widetilde{I}$ (which, as we have already noted, is just $k[V]$) is generated as a $k[U]$-module by the images of the monomials of degree $\leq d-1$ in the variables $y_i/y_0$. In particular, it is finitely generated as a $k[U]$-module. This completes the proof of the "if" direction of the theorem. □

To be continued ...

infinite. The theorem remains true when $k$ is finite, but a little extra argument is required, which we omit.

## 14. Localization

Localization is the process in commutative algebra that corresponds to the geometric/topological idea of restricting attention to an open subset of some given algebraic set.

14.1. **Distinguished open subsets of an affine algebraic set.** We begin with a recapitulation and slight reformulation of the results we have already deduced from the Rabinowitz trick.

If $V$ is an affine algebraic set, let $A := k[V]$ denote the ring of regular functions on $V$. If $f \in A$, and $Z := \{P \in V \mid f(P) = 0\}$, then $Z$ is a closed subset of $f$ (e.g. because $f$ is Zariski continuous, and $Z$ is the preimage of the closed subset $\{0\} \subset \mathbb{A}^1$), and so $D(f) := V \setminus Z$ is an open subset of $V$.

14.1.1. **Proposition.** *The quasi-projective algebraic set $D(f)$ is isomorphic to an affine algebraic set, and its ring of regular functions is naturally isomorphic to $A[y]/(1-fy)$. Furthermore, the open sets $D(f)$ (for $f \in k[V]$) form a basis of open sets for the Zariski topology of $V$.*

*Proof.* The first claim is a restatement of the Rabinowitz trick, namely: the map $P \mapsto \big(P, f(P)^{-1}\big)$ induces an isomorphism between $D(f)$ and the closed subset

$$\{(P, y) \in V \times \mathbb{A}^1 \mid 1 - f(P)y = 0\}.$$

Theorem 12.2.2 then shows that $k[D(f)] \cong A[y]/I$, where $I$ denotes the radical of $(1 - fy)$. We will see in Corollary 14.3.7 below (since $A$ is reduced, being the ring of regular functions on $V$) that $(1-fy)$ is already a radical ideal, and hence indeed $k[D(f)] \cong A[y]/(1 - fy)$.

The fact that every point of $V$ has a neighbourhood basis consisting of open sets of the form $D(f)$ was proved in the course of proving Proposition 12.1.1. The following lemma shows that the intersection of two sets of the form $D(f)$ is again of this form, □

14.1.2. **Lemma.** *If $f_1, f_2 \in k[V]$, then $D(f_1) \cap D(f_2) = D(f_1 f_2)$.*

*Proof.* This is just a restatement of the fact that $(f_1 f_2)(P) \neq 0$ if and only if both $f_1(P) \neq 0$ and $f_2(P) \neq 0$. □

14.1.3. **Definition.** For an affine algebraic set $V$, the open subsets of the form $D(f)$ (for some $f \in k[V]$) are called *distinguished open subsets* of $V$.

Slightly informally, in the above context one might write $A[1/f]$ rather than $A[y]/(1 - fy)$, since adjoining an element $y$ for which $fy = 1$ amounts precisely to adjoining a multiplicative inverse for $f$ to $A$.

The algebraic process of passing from $A$ to $A[1/f]$ is called localization.

14.2. **Localizing rings.** Let $A$ be a ring, and let $S$ be any subset of $A$.

14.2.1. **Definition.** We write

$$A_S := A[\{x_a\}_{a \in A}]/(\{1 - ax_a\}_{a \in S}).$$

In words: we adjoin one variable, which we've denoted $x_a$, to $A$ for each element $a \in S$, and for each such element we impose the relation $ax_a = 1$. We refer to $A_S$ as the *localization* of $A$ at $S$.

Slightly informally, one could write $A[\{a^{-1}\}]_{a\in S}$ for $A_S$, since we form $A_S$ precisely by adjoining an inverse for each $a \in S$. One way that this can be expressed more formally is by the following universal property of $A_S$.

14.2.2. **Proposition.** *If $B$ is an $A$-algebra, say with structural morphism $\varphi : A \to B$, then $\mathrm{Hom}_{A-\mathrm{alg}}(A_S, B)$ is either empty or consists of a single element, and it is non-empty precisely if the element $\varphi(a) \in B$ is invertible for each $a \in S$.*

*Proof.* To give a ring homomorphism $\psi : A_S \to B$ compatible with $\varphi$, we have to give elements $\psi(x_a) \in B$ for each $a \in S$, and these have to satisfy the relations $\varphi(a)\psi(x_a) = 1$. Thus we can define such a $\psi$ precisely if $\varphi(a)$ is invertible for each $a \in S$, in which case the value of $\psi(x_a)$ is uniquely determined, namely as $\varphi(a)^{-1}$. □

Sometimes it is convenient to suppose that the set $S$ is closed under multiplication.

14.2.3. **Definition.** We say that a subset $S$ of $A$ is *multiplicative* if it is closed under multiplication.

14.2.4. **Lemma.** *If $S$ is a subset of $A$, and $T$ is the multiplicative subset of $A$ that $S$ generates (i.e. $T$ consists of all finite products of elements of $S$), then there is a natural (indeed, a unique) isomorphism of $A$-algebras $A_S \cong A_T$.*

*Proof.* Since the set of units of a ring is closed under multiplication, one sees from Proposition 14.2.2 that $A_S$ and $A_T$ satisfy the same universal property, and hence are naturally isomorphic.

Concretely, taking $B$ to be $A_T$ in that proposition, we find that there is an (indeed, a unique) $A$-algebra homomorphism $A_S \to A_T$, and similarly, taking $B$ to be $A_S$ and applying the proposition to $A_T$ (and noting that since all the elements of $S$ map to units in $A_S$, so do all the elements of $T$), we obtain an $A$-algebra homomorphism $A_T \to A_S$ (which is again unique). These homomorphisms are mutually inverse, and so induce the required isomorphism. (To see that they are inverse, one can work with the explicit description given in the proof of Proposition 14.2.2, or one can note that the composite $A_S \to A_T \to A_S$ is an $A$-algebra endomorphism of $A_S$, and similarly $A_T \to A_S \to A_T$ is an $A$-algebra endomorphism of $A_T$, and Proposition 14.2.2 shows that the only endomorphism of either $A_S$ or $A_T$ is the identity.) □

14.2.5. **Remark.** If $S$ consists of a single element $a \in A$, then we usually write $A_a$ rather than $A_{\{a\}}$ for the localization of $A$ at the singleton set $a$.

14.2.6. **Lemma.** *If $S$ is a finite set, and $a$ denotes the product of the finitely many elements of $S$, then there is a natural (indeed, a unique) isomorphism of $A$-algebras $A_S \cong A_a$.*

*Proof.* This is proved similarly to Lemma 14.2.4, noting for any finite set of elements of a ring, each element of the set is invertible if and only if their product is (and hence, all the elements of $S$ have invertible images in a given $A$-algebra $B$ if and only if the image of their product $a$ is invertible in $B$). □

14.3. **Localizing modules.**

14.3.1. **Definition.** If $A$ is a ring, $S$ is a subset of $A$, and $M$ is an $A$-module, then we write

$$M_S := A_S \otimes_A M,$$

and refer to $M_S$ as the *localization* of $M$ at $S$.

The following lemma shows that localization at $S$ is an exact functor (for any set $S$), or equivalently, that $A_S$ is a *flat* $A$-algebra.

14.3.2. **Lemma.** *The functor $M \mapsto M_S$ is exact, i.e. if $0 \to M \to N \to P \to 0$ is an exact sequence of $A$-modules, then the induced exact sequence $0 \to M_S \to N_S \to P_S \to 0$ is again exact.*

*Proof.* Since tensoring is always right exact, the only thing we have to check is that if $M \hookrightarrow N$ is an injective homomorphism of $A$-modules, then the induced homomorphism $M_S \to N_S$ is again injective.

Going back to the definition of $A_S$ as $A[\{x_a\}_{a\in S}]/(\{1-ax_a)_{a\in S})$, we see that we may write

$$M_S = M[\{x_a\}_{a\in S}]/\sum_{a\in S}(1-ax_a)M[\{x_a\}_{a\in S}],$$

and similarly

$$N_S = N[\{x_a\}_{a\in S}]/\sum_{a\in S}(1-ax_a)N[\{x_a\}_{a\in S}].$$

(Here we write $M[\{x_a\}_{a\in S}]$ to denote the module over $A[\{x_a\}_{a\in S}]$ consisting of polynomials with coefficients in $M$, and similarly for $N[\{x_a\}_{a\in S}]$.)

Suppose that $m \in M_S$ lies in the kernel of $M_S \to N_S$. Let $m' \in M[\{x_a\}_{a\in S}]$ be a polynomial (with coefficients in $M$) that maps to $m'$ in $M_S$. The assumption that $m'$ lies in the kernel of $M_S \to N_S$ implies that the image of $m'$ in $N[\{x_a\}_{a\in S}]$ lies in $\sum_{a\in S}(1-ax_a)N[\{x_a\}_{a\in S}]$. Now $m'$ is a polynomial, so it only actually involves finitely many of the variables $x_a$. (Put another way, the coefficient in $m'$ of all but finitely many of the monomials in the $x_a$'s are zero.) Similarly, if its image lies in $\sum_{a\in S}(1-ax_a)N[\{x_a\}_{a\in S}]$, then in fact its image lies in $\sum_{a\in S'}(1-ax_a)N[\{x_a\}_{a\in S'}]$ for some finite subset $S'$ of $S$.

In other words, we may find a finite subset $S'$ of $S$ so that $m' \in M[\{x_a\}_{a\in S'}]$, and such that its image in $N[\{x_a\}_{a\in S'}]$ lies in $\sum_{a\in S'}(1-ax_a)N[\{x_a\}_{a\in S'}]$. If we can show that $m'$ then lies in $\sum_{a\in S'}(1-ax_a)M[\{x_a\}_{a\in S'}]$, then in particular we will know that it lies in $\sum_{a\in S}(1-ax_a)M[\{x_a\}_{a\in S}]$, and thus that its image $m$ in $M_S$ vanishes. Thus we will have proved that $M_S \to N_S$ is injective, as required.

To summarize: the discussion of the preceding paragraph shows (replacing $S$ with $S'$) that we may assume that $S$ is finite. Lemma 14.2.6 then shows that we may assume that $S = \{a\}$ is a singleton. Thus we are reduced to showing that if $M \hookrightarrow N$ is injective, then the induced homomorphism

$$M[x]/(1-ax)M[x] \to N[x]/(1-ax)N[x]$$

is injective.

Suppose that $m'$ is a polynomial in $M[x]$ whose image in $N[x]$ is divisible by $(1-ax)$, say $m' = (1-ax)n'$, for some $n' \in N[x]$. (Since $M[x] \to N[x]$ is an embedding, we use the same notation to denote $m'$ and its image in $N[x]$.) Note that $N[x]$ embeds into $N[[x]]$ (power-series in $x$ with coefficients in $M$) and that

$1 - ax$ is invertible in $A[[x]]$ (its inverse is $1 + ax + a^2x^2 + \cdots$). Thus, working in $N[[x]]$, we find that $n' = (1 - ax)^{-1}m' \in M[[x]]$. Thus $n' \in N[x] \cap M[[x]] = M[x]$, and so in fact $(1-ax)$ divides $m'$ in $M[x]$. This implies that $M[x]/(1-ax)M[x] \to N[x]/(1 - ax)N[x]$ is injective, as required. □

14.3.3. **Remark.** (1) The part of the preceding proof in which we reduce to a finite set $S'$ may be expressed more succinctly in terms of direct limits. More precisely, we have a natural isomorphism

$$A[\{x_a\}_S] \xrightarrow{\sim} \varinjlim_{S'} A[\{x_a\}_{a \in S'}]$$

(where $S'$ runs over the finite subsets of $S$), and thus a natural isomorphism

$$A_S \xrightarrow{\sim} \varinjlim_{S'} A_{S'},$$

where $S'$ runs over all the finite subsets of $S$. Since tensor products commute with direct limits, we then obtain a natural isomorphism

$$M_S \xrightarrow{\sim} \varinjlim_{S'} M_{S'}.$$

Finally, since passing to direct limits is exact, we find that the kernel of $M_S \to N_S$ is the direct limit of the kernels of the homomorphisms $M_{S'} \to N_{S'}$.

(2) The proof of exactness in the case $S = \{a\}$ may also be expressed more succinctly, via the snake lemma. Namely, from the exact sequence $0 \to M \to N \to P \to 0$ we obtain an exact sequence $0 \to M[x] \to N[x] \to P[x] \to 0$, and we may then form the morphism of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M[x] & \longrightarrow & N[x] & \longrightarrow & P[x] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1-ax} & & \downarrow{\scriptstyle 1-ax} & & \downarrow{\scriptstyle 1-ax} & & \\ 0 & \longrightarrow & M[x] & \longrightarrow & N[x] & \longrightarrow & P[x] & \longrightarrow & 0 \end{array}$$

Now multiplication by $(1-ax)$ is invertible on $M[[x]]$, $N[[x]]$, and $P[[x]]$, and hence injective on $M[x]$, $N[x]$, and $P[x]$. The snake lemma thus implies that we obtain a short exact sequence

$$0 \to M[x]/(1 - ax)M[x] \to N[x]/(1 - ax)N[x] \to P[x]/(1 - ax)P[x] \to 0,$$

as required.

The preceding lemma implies in particular that if $M$ is a submodule of an $A$-module $N$, then we $M_S$ embeds as a submodule of $N_S$. The next lemma gives a kind of converse to this fact.

14.3.4. **Lemma.** *If $N$ is an $A$-modules, and if $M'$ is an $A_S$-submodule of $N_S$, then there is an $A$-submodule $M$ of $N$ so that $M'$ is the image of $M_S$ under its natural embedding into $N_S$. More precisely, if $\varphi : N \to N_S$ denotes the natural map, and if we write $M := \varphi^{-1}(M')$, then the embedding $M_S \hookrightarrow N_S$ identifies $M_S$ with $M'$.*

*Proof.* By Lemma 14.2.4, it is no loss of generality to assume that $S$ is multiplicative, and we do so. Now, if $a' \in A_S$, then we may find $a'' \in S$ so that $a'a''$ lies in the image of the natural map $A \to A_S$. (Just "clear denominators"; it is to simplify the statement of this step that we assume $S$ multiplicative.)

Let $m' \in M' \subset N_S$. Since $N_S := A_S \otimes N$, we may write $m'$ as a finite sum $m' = \sum_i a'_i \otimes n_i$, for some $a'_i \in A_S$ and $n_i \in N$. Choose $a''_i \in S$ so that $a'_i a''_i \in A$ for each $i$, and write $a := \prod_i a''_i$. Then $aa'_i \in A$ for all $i$, and so $am' = \sum_i aa'_i \otimes n_i$ is the image in $N_S$ of the element $\sum_i (aa'_i)n_i$ of $N$. It is also an element of $M'$ (since $M'$ is an $A_S$-submodule of $N_S$).

Thus, if we let $\varphi : N \to N_S$ denote the natural map, we find that $am' \in \varphi\big(\varphi^{-1}(M')\big)$. Since $a \in S$, it is invertible in $A_S$, and thus we find that $m' \in A_S\varphi\big(\varphi^{-1}(M')\big)$. Thus, if we write $M = \varphi^{-1}(M')$, then $M$ is an $A$-submodule of $N$, and $M'$ is the image of $M_S := A_S \otimes M$ in $N_S$. □

The following lemma describes the kernel of the natural map $M \to M_S$.

14.3.5. **Lemma.** *If $T$ denotes the multiplicative set generated by $S$, then the kernel of $M \to M_S$ consists precisely of those $m \in M$ such that $tm = 0$ for some $t \in T$.*

*Proof.* As in the proof of Lemma 14.3.2, we write

$$M_S = M[\{x_a\}_{a\in S}]/\sum_{a\in S}(1 - ax_a)M[\{x_a\}_{a\in S}].$$

If $m \in M$ lies in the kernel of the map $M \to M_S$, then we see that $m$ (thought of as a constant polynomial) lies in $\sum_{a\in S}(1 - ax_a)M[\{x_a\}_{a\in S}]$. Thus in fact

$$m \in \sum_{a\in S'}(1 - ax_a)M[\{x_a\}_{a\in S'}]$$

for some finite subset $S'$ of $S$, and so $m$ lies in the kernel of the natural homomorphism $M \to M_{S'}$. Thus, replacing $S$ by $S'$, we may assume that $S'$ is finite, and then, by applying Lemma 14.2.6, that $S' = \{a\}$ is a singleton.

Suppose now that $m = (1 - ax)m'$ for some $m' \in M[x]$. Working in $M[[x]]$, we find that

$$m' = (1 + ax + a^2x^2 + \cdots + a^nx^n + \cdots)m = m + amx + a^2mx^2 + \cdots + a^nmx^n + \cdots .$$

Since $m'$ is a polynomial by assumption, we find that necessarily $a^nm = 0$ for some $n$, and thus that the lemma holds when $S = \{a\}$. As we already observed, this implies the lemma in general. □

14.3.6. **Remark.** (1) As with the proof of Lemma 14.3.2, the first part of the proof of the preceding lemma could be rephrased in the language of direct limits.

(2) Note the similarity of the second part of the argument with the proof of Lemma 6.7.3. Indeed, that lemma is a special case of the preding lemma; namely, it treats the case when $A_a = 0$, i.e. the case when all of $A$ is in the kernel of the natural homomorphism $A \to A_a$, or equivalently, the case when 1 lies in this kernel. The previous lemma shows that this is the case precisely when $a^n = 0$ for some $n$, and this is also precisely the conclusion of Lemma 6.7.3.

We note the following consequence of the preceding lemma.

14.3.7. **Corollary.** *If $A$ is reduced, then so is $A_S$, for any subset $S$ of $A$.*

*Proof.* By Lemma 14.2.4, it is no loss of generality to assume that $S$ is multiplicative, and we do so.

If $I'$ denotes the nilradical of $A_S$ (i.e. the ideal of nilpotent elements in $A_S$), and $I$ denotes its preimage under the natural map $A \to A_S$, then Lemma 14.3.4 shows that $I'$ is generated by the image of $I$ in $A_S$. Thus, in order to show that $A_S$ is

reduced, it suffices to show that if an element of $A$ has nilpotent image in $A_S$, then it actually has zero image in $A_S$.

Suppose that $a \in A$ has nilpotent image in $A_S$, so that $a^n$ lies in the kernel of $A \to A_S$. Then the preceding lemma shows that $a'''a^n = 0$ for some $a''' \in S$. Thus $a'''a$ is a nilpotent element of $A$, and so $a'''a = 0$. The preceding lemma then applies again to show that the image of $a$ in $A_S$ vanishes, as required. □

14.4. **Localization at a prime ideal.**

14.4.1. **Definition.** If $\mathfrak{p}$ is a prime ideal in the ring $A$, then we write $A_\mathfrak{p}$ to denote the localization of $A$ at the multiplicative subset $S = A \setminus \mathfrak{p}$.

14.4.2. **Remark.** (1) The fact that $A \setminus \mathfrak{p}$ is multiplicative is a rephrasing of the fact that $\mathfrak{p}$ is a *prime* ideal.

(2) The notation $A_\mathfrak{p}$ is completely at odds with our general notation $A_S$ for localizations, since it *does not* mean that we take $S$ to be the set $\mathfrak{p}$! (Rather, we take $S$ to be the *complement* of $\mathfrak{p}$ in $A$.) This is an unfortunate but completely standard convention, which doesn't cause confusion in practice (once you get used to it), since prime ideals will always have fairly distinctive notation, usually involving the letter '$p$' in some way (such as $\mathfrak{p}$), which will alert you to which convention is being used at any given moment.

The key feature of $A_\mathfrak{p}$ is that it has only one maximal ideal, the ideal generated by $\mathfrak{p}$.

14.4.3. **Proposition.** *If $\mathfrak{p}$ is a prime ideal in $A$, then the ideal $\mathfrak{p}A_\mathfrak{p}$ of $A_\mathfrak{p}$ is maximal, and is in fact the unique maximal ideal of $A_\mathfrak{p}$. The quotient field $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is naturally isomorphic to the fraction field of the integral domain $A/\mathfrak{p}$.*

*Proof.* If $I'$ is an ideal in $A_\mathfrak{p}$, then Lemma 14.3.4 shows that $I'$ is generated as an ideal by the image (under the natural map $A \to A_\mathfrak{p}$) of an ideal $I \subset A$. Now if $I$ is not contained in $\mathfrak{p}$, then it contains some element $a \in A \setminus \mathfrak{p}$, whose image in $A_\mathfrak{p}$ is a unit. Thus $I'$ contains a unit, and hence is the unit ideal.

Thus any *proper* ideal of $A_\mathfrak{p}$ is generated by the image of an ideal in $A_\mathfrak{p}$ *that is contained in* $\mathfrak{p}$, and hence any proper ideal of $A_\mathfrak{p}$ is contained in $\mathfrak{p}A_\mathfrak{p}$. This shows that $\mathfrak{p}A_\mathfrak{p}$ is a maximal ideal in $A_\mathfrak{p}$, and is the unique such maximal ideal.

Proposition 14.2.2 shows that $A_\mathfrak{p}$ is universal for morphisms to $A$-algebras in which the image of $A \setminus \mathfrak{p}$ consists of units. Thus $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is universal for morphisms to $A$-algebras in which $\mathfrak{p}$ maps to zero, and the image of $A \setminus \mathfrak{p}$ consists of units. We can reformulate this to say that $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is universal for morphisms to $A/\mathfrak{p}$-algebras in which the image of the non-zero elements of $A/\mathfrak{p}$ consists of units. But these latter algebras are precisely the algebras over the fraction field $\kappa(\mathfrak{p})$ of $A/\mathfrak{p}$. Thus $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is universal for morphisms to $\kappa(\mathfrak{p})$-algebras. But obviously $\kappa(\mathfrak{p})$ is universal for morphisms to $\kappa(\mathfrak{p})$-algebras, and so there is a natural isomorphism $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong \kappa(\mathfrak{p})$, as claimed. □

Mathematics Department, University of Chicago, 5734 University Ave., Chicago, IL 60637

*E-mail address*: emerton@math.uchicago.edu