An introduction to Algebraic Geometry - Varieties

Kieran G. O'Grady

22nd March 2024

Contents

Chapter 0

Introduction

Motivation

We will describe some problems and results in order to whet your appetite. Some (or most) of the statements below might leave you puzzled, do not worry, they will become clear later on. In fact one of the goals of reading the book is to be able to understand what is written in the paragraphs below.

We start from the following well known indefinite integral:

$$\int \frac{dx}{\sqrt{1-x^2}} = \arcsin x.$$

What if we ask

$$\int \frac{dx}{\sqrt{1-x^3}} =?$$

Note that one gets the first integral by writing out the formula for the length of arcs of a circle. Similarly, one gets the second integral, or more generally integrals of functions $p(x)^{-1/2}$, where p is a polynomial of degree 3 (or 4), if one sets out to compute the length of arcs of ellipses. There is no way to express the second integral starting from elementary functions. What Fagnano discovered for similar integrals, and what Euler amplified, is that, although we cannot express the integral via elementary functions, there is a rational addition formula, i.e. there exists a rational function F of four variables such that for fixed l_0 and varying a, b we have

$$\int_{l_0}^{a} \frac{dx}{\sqrt{1-x^3}} + \int_{l_0}^{b} \frac{dx}{\sqrt{1-x^3}} = \int_{l_0}^{c} \frac{dx}{\sqrt{1-x^3}} + \text{const},$$

where

$$c = F(a, b, \sqrt{1-a^3}, \sqrt{1-b^3}).$$

Let us sketch a geometric explanation of the addition formula. First of all it is convenient to allow x, y to be complex numbers. Since couples $(x, \sqrt{1-x^3})$ are solutions of the equation $x^3 + y^2 = 1$, we consider the curve $C_0 \subset \mathbb{A}^2(\mathbb{C})$ whose equation is $x^3 + y^2 = 1$, where $\mathbb{A}^2(\mathbb{C}) = \mathbb{C}^2$ is the standard complex affine plane. Now C_0 is a complex submanifold of $\mathbb{A}^2(\mathbb{C})$, hence a 1-dimensional complex manifold. Since it is not compact, we consider its closure $C \subset \mathbb{P}^2(\mathbb{C})$ in the projective complex plane. This means adding a single point "at infinity", namely $[0, 0, 1]$ (we let $[T, X, Y]$ be homogeneous coordinates, and $x = X/T$, $y = Y/T$). Note that by integrating the 1-form dx/y on C (as we will do) we do not have to pay attention to which of the two square roots of $1 - x^3$ we choose. A fundamental observation is that dx/y is holomorphic on all of C_0, including the points $(e^{2\pi mi/3}, 0)$ where the denominator vanishes), and moreover it extends to a holomorphic 1-form on all of C. In order to show that there is an addition formula we fix a line $R_0 \subset \mathbb{P}^2(\mathbb{C})$ intersecting C in 3 points $\overline{p}_1, \overline{p}_2, \overline{p}_3$ and, given another line R intersecting C in 3 points p_1, p_2, p_3, we let

$$\int_{R_0}^{R} \frac{dx}{y} := \int_{\overline{p}_1}^{p_1} \frac{dx}{y} + \int_{\overline{p}_2}^{p_2} \frac{dx}{y} + \int_{\overline{p}_3}^{p_3} \frac{dx}{y}.$$

Of course in order to make sense of the right hand side one needs to choose paths starting at $\overline{p}_i$ and ending at p_i for $i \in \{1, 2, 3\}$. By Goursat's Theorem the integrals do not vary if the paths are homotopically equivalent. Hence if we let R move in a small open subset of $\mathbb{P}^2(\mathbb{C})^\vee$ we may choose well defined homotopy classes of such paths and the integral above defines a well defined holomorphic function on the open set. There is no way to define a holomorphic function

$$R \overset{\Phi}{\mapsto} \int_{R_0}^{R} \frac{dx}{y}.$$

on all of $\mathbb{P}^2(\mathbb{C})^\vee$: if we define it locally and then we move around, when we come back the value of the function will change by an additive constant. Since it changes by an additive constant, the differential $d\Phi$ is a well defined holomorphic 1-form ω on all of $\mathbb{P}^2(\mathbb{C})^\vee$ although Φ is only well defined locally. Since every holomorphic 1-form on a complex projective space is zero, we get that $\omega = 0$, i.e. the (locally defined) function Φ is constant. Now notice that the given points $p_1, p_2 \in C$ there is a unique line R containing p_1, p_2 (if $p_1 = p_2$ we let R be the tangent to C at p_1), and that the coordinates of the third point of intersection of R and C, i.e. p_3, are rational functions of the coordinates of the first two points. This gives the validity of the formula

$$\int_{l_0}^{a} \frac{dx}{\sqrt{1-x^3}} + \int_{l_0}^{b} \frac{dx}{\sqrt{1-x^3}} = -\int_{l_0}^{c} \frac{dx}{\sqrt{1-x^3}} + \text{const},$$

where c is a rational function of $(a, b, \sqrt{1-a^3}, \sqrt{1-b^3})$. With a little more work one gets from this the addition formula as formulated above.

Next we ask more in general what can be said about integrals of the form

$$\int \frac{dx}{\sqrt{D(x)}}, \tag{0.0.1}$$

where $D(x)$ is a polynomial. For simplicity we assume that $D(x)$ has no multiple roots. If $D(x)$ has degree 3, then the arguments above apply verbatim to give an addition formula. In general, the first step is to consider the curve $C_0 \subset \mathbb{A}^2(\mathbb{C})$ whose equation is $y^2 = D(x)$. This is a 1-dimensional complex submanifold of $\mathbb{A}^2(\mathbb{C})$. Since it is not compact it is convenient to compactify. The closure of C_0 in $\mathbb{P}^2(\mathbb{C})$ is compact, but if the degree of $D(x)$ is greater than 3 then the closure of C_0 is not a submanifold of $\mathbb{P}^2(\mathbb{C})$ at its unique "point at infinity"(i.e. $[0, 0, 1]$). Nonetheless there is 1-dimensional complex manifold C containing C_0 as an open dense subset, in fact $C \backslash C_0$ consists of a single point if $D(x)$ has odd degree, and consists of two points if $D(x)$ has even degree. The qualitative behaviour of the integral that we set out to study is determined by the topology of C. The C^∞ manifold underlying C is connected, compact and orientable surface. By the classification compact surfaces it is homeomorphic to a connected sum of g tori. In fact one show that

$$g = \left\lfloor \frac{\deg D - 1}{2} \right\rfloor. \tag{0.0.2}$$

For example, if D has degree 3 then $g = 1$, i.e. C is a torus. Suppose that $g > 1$. Then there exists an addition formula, but it involves the addition of vectors in $\mathbb{C}^g$ obtained by integrating the g linearly independent holomorphic 1-forms

$$\frac{dx}{y}, \frac{xdx}{y}, \ldots, \frac{x^{g-1}dx}{y}. \tag{0.0.3}$$

Lastly we discuss how the topological quantity g (the genus of C) controls the arithmetic of C. Suppose that the polynomial $p(x)$ has integer coefficients. If p is a prime we let $\overline{D}(x) \in \mathbb{F}_p[x]$ be the polynomial whose coefficients are the equivalence classes of the coefficients of D - we say that $\overline{D}(x)$ is obtained from D reducing modulo p. We suppose that $\overline{D}(x)$ has the same degree as D (i.e. p does not divide the leading coefficient of D), and that $\overline{D}(x)$ does not have multiple roots in the algebraic closure of $\mathbb{F}_p$. We also assume that $p \neq 2$. For $n \geqslant 1$ let $\mathbb{F}_{p^n}$ be the finite field of cardinality p^n, and let $C(\mathbb{F}_{p^n})$ be the set of solutions in $\mathbb{F}_{p^n}$ of the equation $y^2 = \overline{D}(x)$. We view the points at infinity (there is one if $\deg D$ is odd and two if $\deg D$ is even) as solutions "in $\mathbb{F}_{p^n}$". A convenient generating function for the cardinalities $|C(\mathbb{F}_{p^n})|$ is given by Weil's zeta function

$$Z(C,T) \coloneqq \exp\left(\sum_{n=1}^{\infty} \frac{|C(\mathbb{F}_{p^n})|}{n} T^n\right). \tag{0.0.4}$$

A famous theorem of Weil states that

$$Z(C,T) = \frac{\prod_{i=1}^{2g}(1-a_iT)}{(1-T)(1-pT)}, \tag{0.0.5}$$

where each a_i is an algebraic integer of modulus $p^{1/2}$ (the last statement is an analogue of Riemann's hypothesis). This shows that the topological genus g can be extracted from the number of solutions $(x,y) \in \mathbb{A}^2(\mathbb{F}_{p^n})$ of the equation $y^2 = \overline{D}(x)$. We also see that there is an explicit formula giving the cardinality $|C(\mathbb{F}_{p^n})|$ for all n once we know the cardinalities $|C(\mathbb{F}_p)|, |C(\mathbb{F}_{p^2})|, \ldots, |C(\mathbb{F}_{p^{2g}})|$. The function of s obtained by making the substitution $T = p^{-s}$, i.e. $Z(C, p^{-s})$, is a precise analogue of Riemann's zeta function $\zeta(s)$, and the statement that each a_i has modulus $p^{1/2}$ is the analogue of the Riemann Hypothesis. It is very compelling evidence in favour of the validity of the Riemann Hypothesis.

Chapter 1

Quasi projective varieties

Throughout the book $\mathbb{K}$ is an algebraically closed field, e.g. $\mathbb{K} = \mathbb{C}$ or $\overline{\mathbb{Q}}$, the algebraic closure of the rational field $\mathbb{Q}$, or $\overline{\mathbb{F}_p}$, the algebraic closure of the finite field $\mathbb{F}_p$ where p is a prime. We are interested in understanding the set of solutions $(z_1, \ldots, z_n) \in \mathbb{K}^n$ of a family of polynomial equations

$$f_1(z_1, \ldots, z_n) = 0, \ldots, f_r(z_1, \ldots, z_n) = 0.$$

"Polynomial equations" means each f_i is an element of the polynomial ring $\mathbb{K}[z_1, \ldots, z_n]$.

In order to understand the geometry of a set of solutions of polynomial equations, it is convenient to replace affine space $\mathbb{A}^n(\mathbb{K})$ by projective space $\mathbb{P}^n(\mathbb{K})$, and consider the set of points in $\mathbb{P}^n(\mathbb{K})$ which are solutions of homogeneous polynomial equations in the homogeneous coordinates. As motivation for this step we recall that results in projective geometry are usually cleaner than in affine geometry - for example two distinct lines in a projective plane have exactly one point of intersection, while two distinct lines in an affine line may intersect in one point or be disjoint. If $\mathbb{K} = \mathbb{C}$ we may guess that passing to projective space makes life simpler because $\mathbb{P}^n(\mathbb{C})$ with the classical topology is compact, while $\mathbb{A}^n(\mathbb{C})$ is not (unless $n = 0$).

Whenever there is no possibility of a misunderstanding we omit $\mathbb{K}$ from the notation for affine and projective space, i.e. $\mathbb{A}^n$ is $\mathbb{A}^n(\mathbb{K})$ and $\mathbb{P}^n$ is $\mathbb{P}^n(\mathbb{K})$.

1.1 Zariski's topology on affine space

If $f_1, \ldots, f_r \in \mathbb{K}[z_1, \ldots, z_n]$, we let

$$V(f_1, \ldots, f_r) := \{z \in \mathbb{A}^n \mid f_i(z) = 0 \ \ \forall\, i \in \{1, \ldots, r\}\}. \tag{1.1.1}$$

More generally, if $I \subset \mathbb{K}[z_1, \ldots, z_n]$ is an ideal (note: the inclusion sign $\subset$ does not mean strict inclusion, and similarly for $\supset$) we let

$$V(I) := \{z \in \mathbb{A}^n \mid f(z) = 0 \ \ \forall\, f \in I\}. \tag{1.1.2}$$

Unless $n = 0$ or $I = 0$ an ideal I of $\mathbb{K}[z_1, \ldots, z_n]$ has an infinite number of elements so that $V(I)$ is the set of solutions of an infinite set of polynomial equations. However I has a finite set of generators $f_1, \ldots, f_r$ by Hilbert's basis Theorem A.3.6, and it follows that $V(I) = V(f_1, \ldots, f_r)$. In fact it is clear that $V(I) \subset V(f_1, \ldots, f_r)$. For the reverse inclusion $V(f_1, \ldots, f_r) \subset V(I)$ notice that if $z \in V(f_1, \ldots, f_r)$ and $f \in I$, then $f = \sum_{i=1}^r g_i f_i$ for suitable $g_1, \ldots, g_r \in \mathbb{K}[z_1, \ldots, z_n]$ and hence $f(z) = \sum_{i=1}^r g_i(z) f_i(z) = 0$.

An elementary observation is that passing from ideals to their zero sets reverses inclusion, i.e. if $I, J \subset \mathbb{K}[z_1, \ldots, z_n]$ are ideals then

$$I \subset J \text{ implies that } V(I) \supset V(J). \tag{1.1.3}$$

Proposition 1.1.1. *The collection of subsets $V(I) \subset \mathbb{A}^n$, where I runs through the collection of ideals of $\mathbb{K}[z_1, \ldots, z_n]$, satisfies the axioms for the closed subsets of a topological space.*

Proof. We have $\varnothing = V((1))$, $\mathbb{A}^n = V((0))$.

Let $I, J \subset \mathbb{K}[z_1, \ldots, z_n]$ be ideals. We claim that $V(I) \cup V(J) = V(I \cap J)$. We have $V(I), V(J) \subset V(I \cap J)$, because $I, J \supset I \cap J$. Thus $V(I) \cup V(J) \subset V(I \cap J)$. Hence it suffices to show that if $z \in V(I \cap J)$ and $z \notin V(I)$, then $z \in V(J)$. Since $x \notin V(I)$, there exists $f \in I$ such that $f(z) \neq 0$. If $g \in J$, then $f \cdot g \in I \cap J$, and thus $(f \cdot g)(z) = 0$ because $z \in V(I \cap J)$. Since $f(z) \neq 0$, it follows that $g(z) = 0$. This proves that $z \in V(J)$.

Lastly, let $\{I_t\}_{t \in T}$ be a family of ideals of $\mathbb{K}[z_1, \ldots, z_n]$. Then

$$\bigcap_{t \in T} V(I_t) = V(\langle \{I_t\}_{t \in T} \rangle),$$

where $\langle \{I_t\}_{t \in T} \rangle$ is the ideal generated by the collection of the I_t's. □

Definition 1.1.2. The *Zariski topology* of $\mathbb{A}^n$ is the topology whose closed sets are the sets $V(I)$, where I runs through the collection of ideals of $\mathbb{K}[z_1, \ldots, z_n]$. The Zariski topology of a subset $A \subset \mathbb{A}^n$ is the topology induced by the Zariski topology of $\mathbb{A}^n$.

Remark 1.1.3. If $\mathbb{K} = \mathbb{C}$, the Zariski topology is weaker than the classical topology of $\mathbb{A}^n$. In fact, unless $n = 0$, the Zariski is much weaker than the classical topology, in particular it is *not* Hausdorff.

Example 1.1.4. A subset $X \subset \mathbb{A}^n$ is a *hypersurface* if it is equal to $V(f)$, where f is a non constant homogeneous polynomial.

A picture of a hypersurface in $\mathbb{A}^2$ is in Figure 1.1. Notice that (x, y) are the affine coordinates - in general, whenever we consider affine or projective space of small dimension, we will denore affine or homogeneous coordinates by letters $x, y, z, \ldots$ and $X, Y, Z, \ldots$ respectively.

What is the field $\mathbb{K}$? The picture shows points with real coordinates. We can view the picture as a "slice" of the corresponding hypersurface over $\mathbb{C}$, or as the closure (either in the Zariski or the classical topology) of the corresponding hypersurface over the algebriac closure of the rationals $\overline{\mathbb{Q}}$.

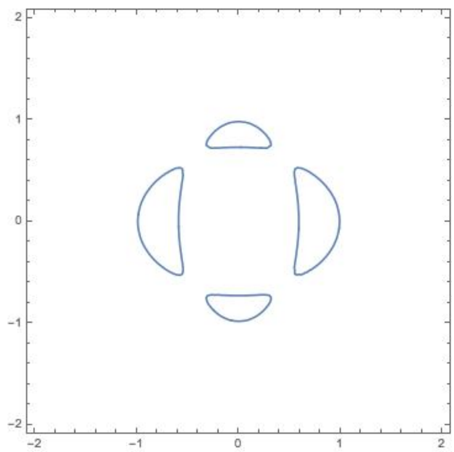

Figure 1.1: $(x^2 + 2y^2 - 1)(3x^2 + y^2 - 1) + \frac{3}{100} = 0$

Given a subset $X \subset \mathbb{A}^n$, let

$$I(X) := \{f \in \mathbb{K}[z_1, \ldots, z_n] \mid f(z) = 0 \text{ for all } z \in X\}. \tag{1.1.4}$$

Clearly $I(X)$ is an ideal of $\mathbb{K}[z_1, \ldots, z_n]$ and X is contained in the closed set $V(I(X))$. Moreover $V(I(X))$ is the closure of X in the Zariski topology. In fact suppose that $V(J) \subset \mathbb{A}^n$ is a closed subset containing X. Then $f(z) = 0$ for all $f \in J$ and $z \in X$, and hence $J \subset I(X)$. This shows that $V(J) \supset V(I(X))$ (recall (1.1.3)).

Remark 1.1.5. Let $\mathscr{A}$ be a finite dimensional affine space over $\mathbb{K}$ of dimension n. Then the Zariski topology on $\mathscr{A}$ may be defined by analogy with the case of $\mathbb{A}^n$, simply replacing $\mathbb{K}[z_1, \ldots, z_n]$ by the $\mathbb{K}$ algebra of polynomial functions on $\mathscr{A}$ (which is isomorphic to $\mathbb{K}[z_1, \ldots, z_n]$). Another way of putting it is that an affine transformation of $\mathbb{A}^n$ is a homemorphism for the Zariski topology.

1.2 Zariski's topology on projective space

Let $F \in \mathbb{K}[Z_0, \ldots, Z_n]_d$ be homogeneous of degree d (to be correct we should say that F belongs to the homogeneous summand of degree d, because the degree of 0 is $-\infty$). Let $x = [Z] \in \mathbb{P}^n$. Then $F(Z) = 0$ if and only if $F(\lambda Z) = 0$ for every $\lambda \in \mathbb{K}^*$, because $F(\lambda Z) = \lambda^d F(Z)$. Hence, although $F(x)$ is not defined, it makes to state that $F(x) = 0$ or $F(x) \neq 0$. Thus if $F_1, \ldots, F_r \in \mathbb{K}[Z_0, \ldots, Z_n]$ are homogeneous (of possibly different degrees) it makes sense to let

$$V(F_1, \ldots, F_r) := \{x \in \mathbb{P}^n \mid F_1(x) = \ldots = F_r(x) = 0\}. \tag{1.2.1}$$

As in the case of affine space, it is convenient to consider the zero locus of ideals, but we need to consider homogeneous ideals. An ideal $I \subset \mathbb{K}[Z_0, \ldots, Z_n]$ is *homogeneous* if

$$I = \bigoplus_{d=0}^{\infty} I \cap \mathbb{K}[Z_0, \ldots, Z_n]_d, \tag{1.2.2}$$

i.e. if it is generated by homogeneous elements. Let $I \subset \mathbb{K}[Z_0, \ldots, Z_n]$ be a homogeneous ideal; we let

$$V(I) := \{x \in \mathbb{P}^n \mid F(x) = 0 \;\; \forall \text{ homogeneous } F \in I\}.$$

By Hilbert's basis Theorem A.3.6 I is generated by a finite set of homogeneous polynomials $F_1, \ldots, F_r$, and hence $V(I) = V(F_1, \ldots, F_r)$. Notice that if $I \subset \mathbb{K}[Z_0, \ldots, Z_n]$ is a homogeneous ideal we have two different meanings for $V(I)$, namely the subset of $\mathbb{P}^n$ defined above and the subset of $\mathbb{A}^{n+1}$ defined in (1.1.2). The context will indicate which of the two we mean.

Proceeding as in the proof of Proposition 1.1.1 one gets the following result.

Proposition 1.2.1. *The collection of subsets $V(I) \subset \mathbb{P}^n$, where I runs through the collection of homogeneous ideals of $\mathbb{K}[Z_0, \ldots, Z_n]$, satisfies the axioms for the closed subsets of a topological space.*

Definition 1.2.2. The *Zariski topology* of $\mathbb{P}^n$ is the topology whose closed sets are the sets $V(I) \subset \mathbb{P}^n$, where I runs through the collection of homogeneous ideals of $\mathbb{K}[Z_0, \ldots, Z_n]$. The Zariski topology of a subset $A \subset \mathbb{P}^n$ is the topology induced by the Zariski topology of $\mathbb{P}^n$.

Remark 1.2.3. Let $\pi\colon (\mathbb{K}^{n+1}\backslash\{0\}) \longrightarrow \mathbb{P}^n$ be the map defined by $\pi(Z) = [Z]$, so that $\mathbb{P}^n$ is identified as the quotient of $\mathbb{K}^{n+1}\backslash\{0\}$ for the action by homotheties. The Zariski topology of $\mathbb{P}^n$ is the quotient of the Zariski topology on $\mathbb{K}^{n+1}\backslash\{0\}$.

Remark 1.2.4. If $F \in \mathbb{K}[Z_0, \ldots, Z_n]$ is homogeneous we let

$$\mathbb{P}^n_F := \mathbb{P}^n \backslash V(F). \tag{1.2.3}$$

Thus $\mathbb{P}^n_F$ is an open subset of $\mathbb{P}^n$.

From now on we make the identification

$$\begin{array}{ccc} \mathbb{A}^n & \longleftrightarrow & \mathbb{P}^n_{Z_0} \\ (z_1, \ldots, z_n) & \mapsto & [1, z_1, \ldots, z_n] \end{array}$$

The Zariski topology of $\mathbb{A}^n$ induced by the Zariski topology on $\mathbb{P}^n$ is the same as the Zariski topology of Definition 1.1.2. In fact let $X \subset \mathbb{A}^n$. Suppose first that X is closed for the topology induced from the Zariski topology of $\mathbb{P}^n$, i.e. $X = (\mathbb{P}^n_{Z_0}) \cap V(F_1, \ldots, F_r)$, where each $F_j \in \mathbb{K}[Z_0, Z_1, \ldots, Z_n]$ is homogeneous. Then $X = V(f_1, \ldots, f_r)$, where

$$f_j(z_1, \ldots, z_n) := F(1, z_1, \ldots, z_n).$$

Next suppose that X is closed for the Zariski topology of Definition 1.1.2, i.e. $X = V(f_1, \ldots, f_r)$ where $f_1, \ldots, f_r \in \mathbb{K}[z_1, \ldots, x_n]$. We may assume that all f_j are non zero because $\mathbb{A}^n$ is clearly closed for the induced topology, and hence each f_j has a well defined degree d_j . For $j \in \{1, \ldots, r\}$ let

$$F_j(Z_0, \ldots, Z_n) := Z_0^{d_j} f\left(\frac{Z_1}{Z_0}, \ldots, \frac{Z_n}{Z_0}\right).$$

Then F_j is a homogeneous polynomial of degree d_j and hence $V(F_1, \ldots, F_r) \subset \mathbb{P}^n$ is a closed subset. Since

$$V(f_1, \ldots, f_r) = (\mathbb{P}^n_{Z_0}) \cap V(F_1, \ldots, F_r),$$

we get that $V(f_1, \ldots, f_r)$ is closed for the induced topology.

Example 1.2.5. A subset $X \subset \mathbb{P}^n$ is a *hypersurface* if it is equal to $V(F)$, where F is a non constant homogeneous polynomial. Notice that $V(F) \cap \mathbb{A}^n$ is a hypersurface unless $F = cZ_0^d$ for some $c \in \mathbb{K}^*$.

Given a subset $A \subset \mathbb{P}^n$, let

$$I(A) := \langle F \in \mathbb{K}[Z_0, \ldots, Z_n] \mid F \text{ is homogeneous and } F(p) = 0 \text{ for all } p \in A\rangle, \tag{1.2.4}$$

where $\langle, \rangle$ means "the ideal generated by". Clearly $I(A)$ is a homogeneous ideal of $\mathbb{K}[Z_0, \ldots, Z_n]$, and $V(I(A))$ is the closure of A in the Zariski topology.

Definition 1.2.6. A *quasi-projective* variety is a Zariski locally closed subset of a projective space, i.e. $X \subset \mathbb{P}^n$ such that $X = U \cap Y$, where $U, Y \subset \mathbb{P}^n$ are Zariski open and Zariski closed respectively.

Example 1.2.7. By Remark 1.2.4, every closed subset of $\mathbb{A}^n$ is a quasi projective variety.

Remark 1.2.8. If V is a finite dimensional complex vector space, the Zariski topology on $\mathbb{P}(V)$ is defined by imitating what was done for $\mathbb{P}^n$: one associates to a homogeneous ideal $I \subset \operatorname{Sym} V^\vee$ the set of zeroes $V(I)$, etc. Everything that we do in the present chapter applies to this situation, but for the sake of concreteness we formulate it for $\mathbb{P}^n$.

1.3 Decomposition into irreducibles

A proper closed subset $X \subset \mathbb{P}^1$ (or $X \subset \mathbb{A}^1$) is a finite set of points. In general, a quasi projective variety is a finite union of closed subsets which are irreducible, i.e. are not the union of proper closed subsets. In order to formulate the relevant result, we give a few definitions.

Definition 1.3.1. Let X be a topological space. We say that X is *reducible* if either $X = \varnothing$ or there exist proper closed subsets $Y, W \subset X$ such that $X = Y \cup W$. We say that X is *irreducible* if it is not reducible.

Example 1.3.2. A subset $A \subset \mathbb{R}^n$ with the euclidean (classical) topology is irreducible if and only if it is a singleton.

Example 1.3.3. Projective space $\mathbb{P}^n$ with the Zariski topology is irreducible. In fact suppose that $\mathbb{P}^n = X \cup Y$ with X and Y proper closed subsets. Then there exist homogeneous $F \in I(X)$ and $G \in I(Y)$ such that $F(y) \neq 0$ for one (at least) $y \in Y$ and $G(x) \neq 0$ for one (at least) $x \in X$. In particular both F and G are non zero, and hence $FG \neq 0$ because $\mathbb{K}[Z_0, \ldots, Z_n]$ is an integral domain. On the other hand $FG = 0$ because $\mathbb{P}^n = Y \cup W$. This is a contradiction, and hence $\mathbb{P}^n$ is irreducible.

Remark 1.3.4. Since the field $\mathbb{K}$ is algebraically closed it is infinite, and hence there is no distinction between the polynomial ring $\mathbb{K}[z_1, \ldots, z_n]$ and the ring of polynomial functions in $z_1, \ldots, z_n$. That is implicit in the argument given in Example 1.3.3, and it will appear repeatedly.

Definition 1.3.5. Let X be a topological space. An *irreducible decomposition of* X consists of a decomposition (possibly empty)

$$X = X_1 \cup \cdots \cup X_r \tag{1.3.1}$$

where each X_i is a closed irreducible subset of X (irreducible with respect to the induced topology) and moreover $X_i \not\subset X_j$ for all $i \neq j$.

We will prove the following result.

Theorem 1.3.6. *Let $A \subset \mathbb{P}^n$ with the (induced) Zariski topology. Then A admits an irreducible decomposition, and such a decomposition is unique up to reordering of components.*

The key step in the proof of Theorem 1.3.6 is the following remarkable consequence of Hilbert's basis Theorem A.3.6.

Proposition 1.3.7. *Let $A \subset \mathbb{P}^n$, and let $A \supset X_0 \supset X_1 \supset \ldots \supset X_m \supset \ldots$ be a descending chain of Zariski closed subsets of A, i.e $X_m \supset X_{m+1}$ for all $m \in \mathbb{N}$. Then the chain is stationary, i.e. there exists $m_0 \in \mathbb{N}$ such that $X_m = X_{m_0}$ for $m \geqslant m_0$.*

Proof. Let $\overline{X}_i$ be the closure of X_i in $\mathbb{P}^n$. Then $X_i = A \cap \overline{X}_i$, because X_i is closed in A. Hence we may replace X_i by $\overline{X}_i$, or equivalently we may suppose that the X_i are closed in $\mathbb{P}^n$. Let $I_m = I(X_m)$. Then $I_0 \subset I_1 \subset \ldots \subset I_m \subset \ldots$ is an ascending chain of (homogeneous) ideals of $\mathbb{K}[Z_0, \ldots, Z_n]$. By Hilbert's basis Theorem and Lemma A.3.3 the ascending chain of ideals is stationary, i.e. there exists $m_0 \in \mathbb{N}$ such that $I_{m_0} = I_m$ for $m \geqslant m_0$. Thus $X_{m_0} = V(I_{m_0}) = V(I_m) = X_m$ for $m \geqslant m_0$. □

Proof of Theorem 1.3.6. If A is empty, then it is the empty union (of irreducibles). . Next, suppose that A is not empty and that it does not admit an irreducible decomposition; we will arrive at a contradiction. First A in reducible, i.e. $A = X_0 \cup W_0$ with $X_0, W_0 \subset A$ proper closed subsets. If both X_0 and W_0 have an irreducible decomposition, then A is the union of the irreducible components of X_0 and W_0, contradicting the assumption that A does not admit an irreducible decomposition. Hence one of X_0, W_0, say X_0, does *not* have an irreducible decomposition. In particular X_0 is reducible. Thus $X_0 = X_1 \cup W_1$ with $X_1, W_1 \subset X_0$ proper closed subsets, and arguing as above, one of X_1, W_1, say X_1, does not admit a decomposition into irredicbles. Iterating, we get a strictly descending chain of closed subsets

$$A \supsetneq X_0 \supsetneq X_1 \supsetneq \cdots \supsetneq X_m \supsetneq X_{m+1} \supsetneq \cdots$$

This contradicts Proposition 1.3.7. This proves that X has a decomposition into irreducibles $X = X_1 \cup \ldots \cup X_r$.

By discarding X_i's which are contained in X_j with $i \neq j$, we may assume that if $i \neq j$, then X_i is not contained in X_j.

Lastly, let us prove that such a decomposition is unique up to reordering, by induction on r. The case $r = 1$ is trivially true. Let $r \geqslant 2$. Suppose that $X = Y_1 \cup \ldots \cup Y_s$, where each Y_j is Zariski closed irreducible, and $Y_j \not\subset Y_k$ if $j \neq k$. Since Y_s is irreducible, there exists i such that $Y_s \subset X_i$. We may assume that $i = r$. By the same argument, there exists j such that $X_r \subset Y_j$. Thus $Y_s \subset X_r \subset Y_j$. It follows that $j = s$, and hence $Y_s = X_r$. It follows that $X_1 \cup \ldots \cup X_{r-1} = Y_1 \cup \ldots \cup Y_{s-1}$, and hence the decomposition is unique up to reordering by the inductive hypothesis. □

Definition 1.3.8. Let X be a quasi projective variety, and let

$$X = X_1 \cup \ldots \cup X_r$$

be an irreducible decomposition of X. The X_i's are the *irreducible components of* X (this makes sense because, by Theorem 1.3.6, the collection of the X_i's is uniquely determined by X).

We notice the following consequence of Proposition 1.3.7.

Corollary 1.3.9. *A quasi projective variety X (with the Zariski topology) is quasi compact, i.e. every open covering of X has a finite subcover.*

The following result makes a connection between irreducibility and algebra.

Proposition 1.3.10. *A subset $X \subset \mathbb{P}^n$ is irreducible if and only if $I(X)$ is a prime ideal.*

Proof. The proof has essentially been given in Example 1.3.3. Suppose that X is irreducible. In particular $X \neq \varnothing$ (by definition), and hence $I(X)$ is a proper ideal of $\mathbb{K}[Z_0, \ldots, Z_n]$. We must prove that $\mathbb{K}[Z_0, \ldots, Z_n]/I(X)$ is an integral domain. Suppose the contrary. Then there exist

$$F, G \in \mathbb{K}[Z_0, \ldots, Z_n], \quad F \notin I(X),\ G \notin I(X), \tag{1.3.2}$$

such that

$$F \cdot G \in I(X). \tag{1.3.3}$$

By (1.3.2) both $X \cap V(F)$ and $X \cap V(G)$ are proper closed subsets of X, and by (1.3.3) we have $X = (X \cap V(F)) \cup (X \cap V(G))$. This is a contradiction, hence $I(X)$ is a prime ideal.

Next, assume that X is reducible; we must prove that $I(X)$ is not prime. If $X = \varnothing$, then $I(X) = \mathbb{K}[Z_0, \ldots, Z_n]$ and hence $I(X)$ is not prime. Thus we may assume that $X \neq \varnothing$, and hence there exist proper closed subset $Y, W \subset X$ such that $X = Y \cup W$. Since $Y \not\subset W$ and $W \not\subset Y$, there exist $F \in (I(Y) \backslash I(W))$ and $G \in (I(W) \backslash I(Y))$. It follows that both (1.3.2) and (1.3.3) hold, and hence $I(X)$ is not prime. □

Remark 1.3.11. Let $I := (Z_0^2) \subset \mathbb{K}[Z_0, Z_1]$. Then $V(I) = \{[0, 1]\}$ is irreducible although I is *not* prime. Of course $I(V(I))$ is prime, it equals (Z_0).

Remark 1.3.12. Let $X \subset \mathbb{A}^n$. Let $I(X) \subset \mathbb{K}[z_1, \ldots, z_n]$ be the ideal of polynomials vanishing on X. Then X is irreducible if and only if $I(X)$ is a prime ideal. The proof is analogous to the proof of Proposition 1.3.10. One may also directly relate $I(X)$ with the ideal $J \subset \mathbb{K}[Z_0, \ldots, Z_n]$ generated by homogeneous polynomials vanishing on X (as subset of $\mathbb{P}^n$), and argue that $I(X)$ is prime if and only if J is.

1.4 The Nullstellensatz

Let an ideal I in a ring R. The *radical* of I, denoted by $\sqrt{I}$, is the set of elements $a \in R$ such that $a^m \in I$ for some $m \in \mathbb{N}$. As is easily checked, $\sqrt{I}$ is an ideal. It is clear that $\sqrt{I} \subset I(V(I))$. The Nullstellensatz states that we have equality.

Theorem 1.4.1 (Hilbert's Nullstellensatz)**.** *Let $I \subset \mathbb{K}[z_1, \ldots, z_n]$ be an ideal. Then $I(V(I)) = \sqrt{I}$.*

Before discussing the proof of the Nullstellensatz, we introduce some notation. For $a = (a_1, \ldots, a_n)$ an element of $\mathbb{A}^n$, let

$$\mathfrak{m}_a := (z_1 - a_1, \ldots, z_n - a_n) = \{f \in \mathbb{K}[z_1, \ldots, z_n] \mid f(a_1, \ldots, a_n) = 0\}. \tag{1.4.1}$$

Notice that $\mathfrak{m}_a$ is the kernel of the surjective homomorphism

$$\begin{array}{ccc} \mathbb{K}[z_1, \ldots, z_n] & \xrightarrow{\phi} & \mathbb{K} \\ f & \mapsto & f(a_1, \ldots, a_n), \end{array}$$

and hence is a maximal ideal. The Nullstellensatz is a consequence of the following result.

Proposition 1.4.2. *An ideal $\mathfrak{m} \subset \mathbb{K}[z_1, \ldots, z_n]$ is maximal if and only if there exists $(a_1, \ldots, a_n) \in \mathbb{A}^n$ such that $\mathfrak{m} = \mathfrak{m}_a$.*

Proof. We have shown that $\mathfrak{m}_a$ is maximal. Now suppose that $\mathfrak{m} \subset \mathbb{K}[z_1, \ldots, z_n]$ is a maximal ideal. Let $F := \mathbb{K}[z_1, \ldots, z_n]/\mathfrak{m}$. Then F is an algebraic extension of $\mathbb{K}$ by Corollary A.5.2. Since $\mathbb{K}$ is algebraically closed $F = \mathbb{K}$, and hence the quotient map is

$$\mathbb{K}[z_1, \ldots, z_n] \xrightarrow{\phi} \mathbb{K}[z_1, \ldots, z_n]/\mathfrak{m} = \mathbb{K}.$$

For $i \in \{1, \ldots, n\}$ let $a_i := \phi(z_i)$. Then $(z_i - a_i) \in \ker \phi$. Since $\mathfrak{m}_a$ is generated by $(z_1 - a_1), \ldots, (z_n - a_n)$ it follows that $\mathfrak{m}_a \subset \mathfrak{m}$. Since both $\mathfrak{m}_a$ and $\mathfrak{m}$ are maximal it follows that $\mathfrak{m} = \mathfrak{m}_a$. □

Corollary 1.4.3 (Weak Nullstellensatz)**.** *Let $I \subset \mathbb{K}[z_1, \ldots, z_n]$ be an ideal. Then $V(I) = \varnothing$ if and only if $I = (1)$.*

Proof. If $I = (1)$, then $V(I) = \varnothing$. Assume that $V(I) = \varnothing$. Suppose that $I \neq (1)$. Then there exists a maximal ideal $\mathfrak{m} \subset \mathbb{K}[z_1, \ldots, z_n]$ containing I. Since $I \subset \mathfrak{m}$, $V(I) \supset V(\mathfrak{m})$. By Proposition 1.4.2 there exists $a \in \mathbb{K}^n$ such that $\mathfrak{m} = \mathfrak{m}_a$ and hence $V(\mathfrak{m}) = V(\mathfrak{m}_a) = \{(a_1, \ldots, a_n)\}$. Thus $a \in V(I)$ and hence $V(I) \neq \varnothing$. This is a contradiction, and hence $I = (1)$. □

Proof of Hilbert's Nullsetellensatz (Rabinowitz's trick). Let $f \in I(V(I))$. By Hilbert's basis theorem $I = (g_1, \ldots, g_s)$ for $g_1, \ldots, g_s \in \mathbb{K}[z_1, \ldots, z_n]$. Let $J \subset \mathbb{K}[z_1, \ldots, z_n, w]$ be the ideal

$$J := (g_1, \ldots, g_s, f \cdot w - 1).$$

Since $f \in I(V(I))$ we have $V(J) = \varnothing$ and hence by the Weak Nullstellensatz $J = (1)$. Thus there exist $h_1, \ldots, h_s, h \in \mathbb{K}[x_1, \ldots, x_n, y]$ such that

$$\sum_{i=1}^{s} h_i g_i + h\,(f \cdot w - 1) = 1.$$

Replacing w by $1/f(z)$ in the above equality we get

$$\sum_{i=1}^{s} h_i \left(z, \frac{1}{f(z)}\right) g_i(z) = 1. \tag{1.4.2}$$

Let $d >> 0$: multiplying both sides of (1.4.2) by f^d we get that

$$\sum_{i=1}^{s} \overline{h}_i\,(z)\, g_i(z) = f^d(z), \quad \overline{h}_i \in \mathbb{K}[z_1, \ldots, z_n].$$

Thus $f \in \sqrt{I}$. □

Example 1.4.4. Let $V(F) \subset \mathbb{P}^n$ be a hypersurface, and let $F_1, \ldots, F_r$ be the distinct prime factors of the decomposition of F into a products of primes (recall that $\mathbb{K}[Z_0, \ldots, Z_n]$ is a UFD, by Corollary A.2.2). The irreducible decomposition of $V(F)$ is

$$V(F) = V(F_1) \cup \ldots \cup V(F_r).$$

In fact, each $V(F_i)$ is irreducible by Proposition 1.3.10. What is not obvious is that $V(F_i) \not\subset V(F_j)$ if F_i, F_j are non associated primes. This follows from Hilbert's Nullstellensatz.

1.5 Regular maps

Let $U \subset \mathbb{P}^n$ be a locally closed subset. Suppose that $F_0, \ldots, F_m \in \mathbb{K}[Z_0, \ldots, Z_n]_d$ are homogeneous polynomials of the same degree, and that for all $[Z] \in U$ we have $(F_0(Z), \ldots, F_m(Z)) \neq (0, \ldots, 0)$. Let $[Z] \in U$. Then $[F_0(Z), \ldots, F_m(Z)] \in \mathbb{P}^m$ and if $\lambda \in \mathbb{K}^*$ we have

$$[F_0(\lambda Z), \ldots, F_m(\lambda Z)] = [\lambda^d F_0(Z), \ldots, \lambda^d F_m(Z)] = [F_0(Z), \ldots, F_m(Z)].$$

Hence we may define

$$\begin{array}{ccc} U & \longrightarrow & \mathbb{P}^m \\ [Z] & \to & [F_0(Z), \ldots, F_m(Z)] \end{array} \tag{1.5.1}$$

Maps as above are the local models for regular maps between quasi projective varieties.

Definition 1.5.1. Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be locally closed subsets (hence X and Y are quasi projective varieties), and let $\varphi\colon X \to Y$ be a map. Then φ is *regular at* $a \in X$ if there exist an open $U \subset X$ containing a such that the restriction of φ to U is described as in (1.5.1). (We assume that $(F_0(Z), \ldots, F_m(Z)) \neq (0, \ldots, 0)$ for all $[Z] \in U$.) The map φ is *regular* if it is regular at each point of X.

Remark 1.5.2. Let $\varphi\colon X \to Y$ be a map between quasi projective varieties. Suppose that $Y = \bigcup_{i\in I} U_i$ is an open cover, that $\varphi^{-1}U_i$ is open in X for each $i \in I$ and that the restriction

$$\begin{array}{ccc} \varphi^{-1}(U_i) & \longrightarrow & U_i \\ x & \mapsto & \varphi(x) \end{array}$$

is regular for each $i \in I$. Then φ is regular. In other words regularity of a map is a local notion.

Proposition 1.5.3. *A regular map of quasi projective varieties is Zariski continuous.*

Proof. Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be Zariski locally closed, and let $f\colon X \to Y$ be a regular map. We must prove that if $C \subset Y$ is Zariski closed, then $f^{-1}(C)$ is Zariski closed in X. Let $U \subset W$ be an open subset such that (1.5.1) holds. Let us show that $\phi^{-1}(C) \cap U$ is closed in U. Since C is closed $C = V(I) \cap Y$ where $I \subset \mathbb{K}[T_0, \ldots, T_m]$ is a homogeneous ideal. Thus

$$\phi^{-1}(C) \cap U = \{[Z] \in U \mid P(F_0(Z), \ldots, F_m(Z)) = 0\ \forall P \in I\}.$$

Since each $P(F_0(Z), \ldots, F_m(Z))$ is a homogeneous polynomial, we get that $\phi^{-1}(C) \cap U$ is closed in U.

By definition of regular map X can be covered by Zariski open sets U_α such that (1.5.1) holds with U replaced by U_α. We have proved that $C_\alpha := \phi^{-1}(C) \cap U_\alpha$ is closed in U_α for all α. It follows that $\phi^{-1}(C)$ is closed. In fact let $\overline{C}_\alpha \subset X$ be the closure of C_α and $D_\alpha := X \backslash U_\alpha$. Since C_α is closed in U_α we have

$$\overline{C}_\alpha \cap U_\alpha = C_\alpha = \phi^{-1}(C) \cap U_\alpha. \tag{1.5.2}$$

Moreover D_α is closed in X because U_α is open. By (1.5.2) we have

$$\phi^{-1}(C) = \bigcap_\alpha \left(\overline{C}_\alpha \cup D_\alpha\right).$$

Thus $\phi^{-1}(C)$ is an intersection of closed sets and hence is closed. □

It is convenient to unravel the condition of being regular for maps with domain a subset of an affine space or both domain and codomain subsets of an affine space.

Example 1.5.4. Let $X \subset \mathbb{A}^n$ $(= \mathbb{P}^n_{Z_0})$ and $Y \subset \mathbb{P}^m$ be locally closed subsets, and let $\varphi\colon X \to Y$ be a map. Then φ is a regular map if and only if, given any $a \in X$, there exist $f_0, \ldots, f_m \in \mathbb{K}[z_1, \ldots, z_n]$ (in general *not* homogeneous) such that on an open subset $U \subset X$ containing a we have

$$\varphi(z) = [f_0(z), \ldots, f_m(z)]. \tag{1.5.3}$$

(This includes the statement that $V(f_1, \ldots, f_m) \cap U = \emptyset$.) In fact, if φ is regular there exist homogeneous $F_0, \ldots, F_m \in \mathbb{K}[Z_0, \ldots, Z_n]_d$ such that $\varphi([1, z]) = [F_0(1, z), \ldots, F_m(1, z)]$, and it suffices to let $f_j(z) := F_j(1, z)$. Conversley, if (1.5.3) holds, then

$$\varphi([Z_0, Z_1, \ldots, Z_n]) = [Z_0^d, Z_0^d f_1\left(\frac{Z_1}{Z_0}, \ldots, \frac{Z_n}{Z_0}\right), \ldots, Z_0^d f_m\left(\frac{Z_1}{Z_0}, \ldots, \frac{Z_n}{Z_0}\right)], \tag{1.5.4}$$

and for d is large enough, each of the rational functions appearing in (1.5.4) is actually a homogeneous polynomial of degree d.

Example 1.5.5. Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be locally closed subsets and let $\varphi \colon X \to Y$ be a map. Recall that $\mathbb{A}^n = \mathbb{P}^n_{Z_0}$ and $\mathbb{A}^m = \mathbb{P}^m_{T_0}$. Then φ is regular if and only if locally there exist $f_0, \ldots, f_m \in \mathbb{K}[z_1, \ldots, z_n]$ (in general *not* homogeneous) such that

$$f(z) = \left(\frac{f_1(z)}{f_0(z)}, \ldots, \frac{f_m(z)}{f_0(z)}\right). \tag{1.5.5}$$

Here it is understood that $f_0(z) \neq 0$ for all z in the relevant open subset U of X. In fact this follows from (1.5.3) if we divide the homogeneous coordinates of $\varphi(z)$ by $f_0(z)$ (by hypothesis it does not vanish for $z \in U$).

The identity map of a quasi projective variety is regular (choose $F_j(Z) = Z_j$). If $\varphi \colon X \to Y$ and $\psi \colon Y \to W$ are regular maps of quasi projective varieties, the composition $\psi \circ \varphi \colon X \to W$ is regular because the composition of homogeneous polynomial functions is a homogeneous polynomial function. Thus we have the *category of quasi projective varieties*. In particular we have the notion of isomorphism between quasi projective varieties.

Definition 1.5.6. A quasi projective variety is

- an *affine variety* if it is isomorphic to a closed subset of an affine space (as usual $\mathbb{A}^n = \mathbb{P}^n_{Z_0} \subset \mathbb{P}^n$),
- a *projective variety* if it is isomorphic to a closed subset of a projective space.

Remark 1.5.7. Let X be an affine variety. If $Y \subset X$ is closed then it is an affine variety. In fact by hypothesis there exist a closed subset $W \subset \mathbb{A}^n$ and an isomorphism $\varphi \colon X \xrightarrow{\sim} W$. Since φ is an isomorphism it is a homeomorphism (see Proposition 1.5.3), and hence $\varphi(Y)$ is a closed subset of W. Since W is closed in $\mathbb{A}^n$, it follows that $\varphi(Y)$ is a closed subset of $\mathbb{A}^n$. The isomorphism $Y \xrightarrow{\sim} \varphi(Y)$ shows that Y is an affine variety. Similarly one shows that if X is a projective variety and $Y \subset X$ is closed, then Y is a projective variety.

The example below gives open (and non closed) subsets of an affine space which are affine varieties.

Example 1.5.8. Let $f \in \mathbb{K}[z_1, \ldots, z_n]$. We let

$$\mathbb{A}^n_f := \mathbb{A}^n \backslash V(f). \tag{1.5.6}$$

Let $Y := V(f(z_1, \ldots, z_n) \cdot w - 1) \subset \mathbb{A}^{n+1}$. The regular map

$$\begin{array}{ccc} \mathbb{A}^n_f & \xrightarrow{\varphi} & Y \\ (z_1, \ldots, z_n) & \mapsto & (z_1, \ldots, z_n, \frac{1}{f(z_1, \ldots, z_n)}) \end{array}$$

is an isomorphism. In fact the inverse of φ is given by

$$\begin{array}{ccc} Y & \xrightarrow{\psi} & \mathbb{A}^n_f \\ (z_1, \ldots, z_n, w) & \mapsto & (z_1, \ldots, z_n) \end{array}$$

Example 1.5.9. Let

$$\mathcal{C}_d = \left\{[\xi_0, \ldots, \xi_d] \in \mathbb{P}^d \mid \operatorname{rk} \begin{pmatrix} \xi_0 & \xi_1 & \cdots & \xi_{d-1} \\ \xi_1 & \xi_2 & \cdots & \xi_d \end{pmatrix} \leqslant 1\right\}. \tag{1.5.7}$$

Since a matrix has rank at most 1 if and only if all the determinants of its 2×2 minors vanish it follows that $\mathcal{C}_d$ is closed. We have a regular map

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\varphi_d} & \mathcal{C}_d \\ [s, t] & \mapsto & [s^d, s^{d-1}t, \ldots, t^d] \end{array} \tag{1.5.8}$$

Let us prove that φ_d is an isomorphism. Let $\psi_d \colon \mathcal{C}_d \to \mathbb{P}^1$ be defined as follows:

$$\psi_d([\xi_0, \ldots, \xi_d]) = \begin{cases} [\xi_0, \xi_1] & \text{if } [\xi_0, \ldots, \xi_d] \in \mathcal{C}_d \cap \mathbb{P}^d_{\xi_0} \\ [\xi_{d-1}, \xi_d] & \text{if } [\xi_0, \ldots, \xi_d] \in \mathcal{C}_d \cap \mathbb{P}^d_{\xi_d} \end{cases}$$

Of course in order for this to make sense one has to check the following:

1. The subset $\mathscr{C}_d$ is the union of the open subsets $\mathcal{C}_d \cap \mathbb{P}^d_{\xi_0}$ and $\mathcal{C}_d \cap \mathbb{P}^d_{\xi_d}$.

2. The two expressions for ψ_d coincide for points in $\mathscr{C}_d \cap \mathbb{P}^d_{\xi_0} \cap \mathbb{P}^d_{\xi_d}$.

To prove (1) suppose that $[\xi] \in \mathscr{C}_d$ and $\xi_0 = 0$. By the equations defining $\mathscr{C}_d$ it follows that $\xi_1 = 0$, $\xi_2 = 0$, etc. up to $\ldots = \xi_{d-1}$. Hence if $\xi_0 = 0$ then $\xi_d \neq 0$, and this prove that Item (1) holds. To prove Item (2) suppose that $[\xi] \in \mathscr{C}_d \cap \mathbb{P}^d_{\xi_0} \cap \mathbb{P}^d_{\xi_d}$. By the equations defining $\mathscr{C}_d$ it follows that $\xi_0 \cdot \xi_n - \xi_1 \xi_{n-1} = 0$ and hence $[\xi_0, \xi_1] = [\xi_{d-1}, \xi_d]$. This prove that Item (2) holds.

One checks easily that $\psi_d \circ \varphi_d = \mathrm{Id}_{\mathbb{P}^1}$ and $\varphi_d \circ \psi_d = \mathrm{Id}_{\mathscr{C}_d}$. Thus φ_d is an isomorphism, as claimed.

Definition 1.5.10. The closed subset $\mathscr{C}_d \subset \mathbb{P}^d$ defined in (1.5.7) or any $X \subset \mathbb{P}^d$ projectively equivalent to $\mathscr{C}_d$ (i.e. given by $g(\mathscr{C}_d)$ where $g \in \mathrm{PGL}_n(\mathbb{K})$) is a *rational normal curve in* $\mathbb{P}^d$.

In the above definition "rational" refers to the fact that $\mathscr{C}_d$ (and hence also any X projectively equivalent to $\mathscr{C}_d$) is isomorphic to $\mathbb{P}^1$, "curve" refers to the fact that $\mathbb{P}^1$ (and hence also $\mathscr{C}_d$) has dimension 1 (we will define the dimension of a quasi projective variety later on), the attribute "normal" will be explained later in the book.

The remark below shows that, in the definition of regular map, we cannot require that φ is given globally by homogeneous polynomials.

Remark 1.5.11. Unless we are in the trivial case $d = 1$, it is *not* possible to define ψ_d *globally* as

$$\psi_d([\xi_0, \ldots, \xi_d]) = [P(\xi_0, \ldots, \xi_d), Q(\xi_0, \ldots, \xi_d)], \tag{1.5.9}$$

with $P, Q \in \mathbb{K}[\xi_0, \ldots, \xi_d]_e$ not vanishing simultaneously on $\mathscr{C}_d$. In fact suppose that (1.5.9) holds, and let

$$p(s,t) := P(s^d, \ldots, t^d), \quad q(s,t) := Q(s^d, \ldots, t^d).$$

The polynomials $p(s,t), q(s,t)$ are homogeneous of degree de, they do not vanish simultaneously on a non zero $(s_0, t_0) \in \mathbb{K}^2$, and for all $[s,t] \in \mathbb{P}^1$ we have $[p(s,t), q(s,t)] = [s,t]$. The last equality means that $tp(s,t) = sq(s,t)$. It follows that $p(s,t) = s \cdot r(s,t)$ and $q(s,t) = t \cdot r(s,t)$ where $r(s,t)$ has no non trivial zeroes. Thus $r(s,t)$ is constant. In particular $de = \deg p = \deg q = 1$, and hence $d = 1$.

The example below extends Example 1.5.9 to arbitrary dimension.

Example 1.5.12. We recall the formula

$$\dim \mathbb{K}[Z_0, \ldots, Z_n]_d = \binom{d+n}{n}. \tag{1.5.10}$$

(See Exercise 1.8.9 for a proof.) Let $N(n;d) := \binom{d+n}{n} - 1$. Let

$$\begin{array}{ccc} \mathbb{P}^n & \xrightarrow{\nu^n_d} & \mathbb{P}^{N(n;d)} \\ [Z] & \mapsto & [Z_0^d, Z_0^{d-1}Z_1, \ldots, Z_n^d] \end{array} \tag{1.5.11}$$

be defined by all homogeneous monomials of degree d - this is a *Veronese map.* Clearly ν^n_d is regular. Note that for $n = 1$ we get back the map φ_d in (1.5.8).

The homogeneous coordinates on $\mathbb{P}^{N(n;d)}$ appearing in (1.5.11) are indiced by length $n+1$ multiindices $I = (i_0, \ldots, i_n) \in \mathbb{N}^{n+1}$ such that $\deg I := i_0 + \ldots + i_n = d$; we denote them by $[\ldots, \xi_I, \ldots]$. Let $\mathscr{V}^n_d \subset \mathbb{P}^{N(n;d)}$ be the closed subset defined by

$$\mathscr{V}^n_d := V(\ldots, \xi_I \cdot \xi_J - \xi_K \cdot \xi_L, \ldots),$$

where I, J, L, K run through all multiindices such that $I + J = K + L$. Clearly $\nu^n_d(\mathbb{P}^n) \subset \mathscr{V}^n_d$. Let us show that ν^n_d is an isomorphism onto $\mathscr{V}^n_d$.

Let $s \in \{0,\ldots,n\}$, and let $H \in \mathbb{N}^{n+1}$ be a multiindex of degree $(d-1)$. We let $e_s \in \mathbb{N}^{n+1}$ be the element all of whose entries are equal to 0 except for the entry at place $s+1$, which is equal to 1, and $H_s := H + e_s$. Also let

$$\begin{array}{ccc} \mathscr{V}_d^n \backslash V(\xi_{H_0},\ldots,\xi_{H_n}) & \stackrel{\varphi_d^n(H)}{\longrightarrow} & \mathbb{P}^n \\ [\ldots,\xi_I,\ldots] & \mapsto & [\xi_{H_0},\ldots,\xi_{H_n}] \end{array}$$

Clearly $\varphi_d^n(H)$ is regular. Moreover if $[\ldots,\xi_I,\ldots] \in \mathscr{V}_d^n$ then there exist a multiindex $H \in \mathbb{N}^{n+1}$ of degree $(d-1)$ such that x belongs to $\mathscr{V}_d^n \backslash V(\xi_{H_0},\ldots,\xi_{H_n})$ for $H \in \mathbb{N}^{n+1}$ (there exists $I \in \mathbb{N}^{n+1}$ of degree d such that $\xi_I \neq 0$ and $I = H + e_s$ where s is such that $i_s \neq 0$). Moreover we claim that if $[\ldots,\xi_I,\ldots] \in \mathscr{V}_d^n$ belong both to the domain of $\varphi_d^n(H)$ and to the domain of $\varphi_d^n(H')$, then

$$\varphi_d^n(H)([\ldots,\xi_I,\ldots]) = [\xi_{H_0},\ldots,\xi_{H_n}] = [\xi_{H'_0},\ldots,\xi_{H'_n}] = \varphi_d^n(H')([z]). \tag{1.5.12}$$

In fact for $s,t \in \{0,\ldots,n\}$ we have $H_s + H'_t = H + H' + e_s + e_t = H_t + H'_s$, thus $\xi_{H_i} \cdot \xi_{H'_j} - \xi_{H_j} \cdot \xi_{H'_i} = 0$ by the equations defining $\mathscr{V}_d^n$, and this proves that the equality in (1.5.12) holds. This shows that the maps $\varphi_d^n(H)$'s define a regular map

$$\mathscr{V}_d^n \xrightarrow{\varphi_d^n} \mathbb{P}^n. \tag{1.5.13}$$

We claim that

$$\varphi_d^n \circ \nu_d^n = \mathrm{Id}_{\mathbb{P}^n} \tag{1.5.14}$$

$$\nu_d^n \circ \varphi_d^n = \mathrm{Id}_{\mathscr{V}_d^n}. \tag{1.5.15}$$

The first equality is easily checked. In order to check the second equality it suffices to show that ν_d^n is surjective. One may proceed as follows. Let $x = [\ldots,\xi_I,\ldots] \in \mathscr{V}_d^n$ be a point such that $\xi_{de_s} \neq 0$ for some $s \in \{0,\ldots,n\}$. Thus $x \in (\mathscr{V}_d^n \backslash V(\xi_{H_0},\ldots,\xi_{H_n}))$ where $H = (d-1)e_0$. It is not difficult to show that $x = \nu_d^n([\xi_{H_0},\ldots,\xi_{H_n}])$. Hence it suffices to prove that if $x = [\ldots,\xi_I,\ldots] \in \mathscr{V}_d^n$, then there exists $s \in \{0,\ldots,n\}$ such that $\xi_{de_s} \neq 0$. Equivalently, we must show that the following statement holds: if $\xi := (\ldots,\xi_I,\ldots)$ is such that $\xi_{de_s} = 0$ for all $s \in \{0,\ldots,n\}$ and $\xi_I \cdot \xi_J = \xi_K \cdot \xi_L$ whenever $I + J = K + L$, then $\xi_I = 0$ for all multiindices I. This is easily proved by "descending induction" on the maximum of $i_0,\ldots,i_n$. If the maximum is d, then $\xi_I = 0$ by hypothesis. Suppose that the maximum is at least $d/2$, i.e. that there exists $s \in \{0,\ldots,n\}$ be such that $2i_s \geqslant d$. Then $2I = de_s + J$ where $J \in \mathbb{N}^{n+1}$ is a multiindex of degree d and hence $\xi_I^2 = \xi_{de_s} \cdot \xi_J = 0$ by by the equations defining $\mathscr{V}_d^n$. Thus $\xi_I = 0$. This proves that if the maximum is at least $d/2$ then $\xi_I = 0$. Iterating the argument we get that if the maximum is at least $d/4$ then $\xi_I = 0$ etc.

The Veronese map allows us to show that the open affine subsets of a quasi projective variety form a basis for the Zariski topology. First we need a definition.

Definition 1.5.13. Let $X \subset \mathbb{P}^n$ be a closed subset. A *principal open subset* of X is an open $U \subset X$ which is equal to

$$X_F := X \backslash V(F),$$

where $F \in \mathbb{K}[Z_0,\ldots,Z_n]$ is a homogeneous polynomial of *strictly positive degree.*

Claim 1.5.14. *Let $X \subset \mathbb{P}^n$ be closed. A principal open subset of X is an affine variety.*

Proof. First we prove the claim for $X = \mathbb{P}^n$. Let $F \in \mathbb{K}[Z_0,\ldots,Z_n]$ be a homogeneous polynomial of strictly positive degree d. In order to prove that $\mathbb{P}^n_F$ is affine we consider the Veronese map $\nu_d^n\colon \mathbb{P}^n \longrightarrow \mathbb{P}^{N(n,d)}$, see (1.5.11). Let $\mathscr{V}_d^n := \mathrm{Im}(\nu_d^n)$ be the corresponding Veronese variety. As shown in Example 1.5.12 the map $\mathbb{P}^n \to \mathscr{V}_d^n$ defined by ν_d^n is an isomorphism. Let $F = \sum_I a_I Z^I$, and let $H \subset \mathbb{P}^{N(n,d)}$ be the hyperplane $H = V(\sum_I a_I \xi_I$. Then we have the isomorphism

$$\begin{array}{ccc} \mathbb{P}^n_F & \stackrel{\sim}{\longrightarrow} & (\mathscr{V}_d^n \backslash H) \\ x & \mapsto & \nu_d^n(x) \end{array} \tag{1.5.16}$$

But $\mathbb{P}^{N(n,d)}\backslash H$ is the affine space $\mathbb{A}^{N(n,d)}$, and hence $(\mathscr{V}_d^n\backslash H)$ is a closed subset of $\mathbb{A}^{N(n,d)}$. Hence the map in (1.5.16) is an isomorphism between $\mathbb{P}^n_F$ and closed subset of $\mathbb{A}^{N(n,d)}$, and therefore $\mathbb{P}^n_F$ is an affine variety.

In general, let $X \subset \mathbb{P}^n$ be closed, and let F be as above. Then X_F is a closed subset of the affine variety $\mathbb{P}^n_F$, and hence it is an affine variety, see Remark rmk:trapano. □

Proposition 1.5.15. *The open affine subsets of a quasi projective variety form a basis of the Zariski topology.*

Proof. Since a quasi-projective variety is an open subset of a projective variety, it suffices to prove the result for projective varieties. Let $X \subset \mathbb{P}^n$ be closed. Let $U \subset X$ be open. If $U = X$ then

$$U = X = X_{Z_0} \cup X_{Z_1} \cup \ldots \cup X_{Z_n}, \tag{1.5.17}$$

and each of the X_{Z_i}'s is an open affine subset by Claim 1.5.14.

Next asssume that $U \neq X$. Then $U = X\backslash V(F_1, \ldots, F_r)$, where each F_j is a non constant homogeneous polynomial, and $r \geqslant 1$. Then

$$U = X_{F_1} \cup \ldots \cup X_{F_r},$$

and each of the X_{F_j}'s is an open affine subset by Claim 1.5.14. □

1.6 Regular functions on affine varieties

Definition 1.6.1. A *regular function* on a quasi projective variety X is a regular map $X \to \mathbb{K}$.

Let X be a non empty quasi projective variety. The set of regular functions on X with pointwise addition and multiplication is a $\mathbb{K}$-algebra, named the *ring of regular functions* of X. We denote it by $\mathbb{K}[X]$.

If X is a projective variety, then it has few regular functions. In fact we will prove (see Corollary 2.4.6) that every regular function on X is locally constant. On the other hand, affine varieties have plenty of functions. In fact if $X \subset \mathbb{A}^n$ is closed we have an inclusion

$$\mathbb{K}[z_1, \ldots, z_n]/I(X) \hookrightarrow \mathbb{K}[X]. \tag{1.6.1}$$

Theorem 1.6.2. *Let $X \subset \mathbb{A}^n$ be closed. Then the homomorphism in* (1.6.1) *is an isomorphism, i.e. every regular function on X is the restriction of a polynomial function on $\mathbb{A}^n$.*

Theorem 1.6.2 follows from the Nullstellensatz. Before giving the proof we discusse a particular instance of Theorem 1.6.2, which shows the relation with the Nullstellensatz. Let $X \subset \mathbb{A}^n$ be closed. Suppose that $g \in \mathbb{K}[z_1, \ldots, z_n]$ and that $g(a) \neq 0$ for all $a \in Z$. Then $1/g \in \mathbb{K}[X]$ and hence Theorem 1.6.2 predicts the existence of $f \in \mathbb{K}[z_1, \ldots, z_n]$ such that $g^{-1} = f_{|X}$. Such an f exists by the Nullstellensatz. In fact let $X = V(g_1, \ldots, g_r)$ where $g_1, \ldots, g_r \in \mathbb{K}[z_1, \ldots, z_n]$. By our hypothesis on g we have $V(g_1, \ldots, g_r, g) = \emptyset$, and hence $(g_1, \ldots, g_r, g) = (1)$ by the Nullstellensatz. Hence there exist $f_1, \ldots, f_r, f \in \mathbb{K}[z_1, \ldots, z_n]$ such that

$$f_1 \cdot g_1 +, \ldots, f_r \cdot g_r + f \cdot g = 1.$$

Restricting to X we get that $f(x) = g(x)^{-1}$ for all $x \in X$, as claimed.

Before proving Theorem 1.6.2, we notice that, if $X \subset \mathbb{A}^n$ is closed, the Nullstellensatz for $\mathbb{K}[z_1, \ldots, z_n]$ implies a Nullstellensatz for $\mathbb{K}[z_1, \ldots, z_n]/I(X)$. First a definition: given an ideal $J \subset (\mathbb{K}[z_1, \ldots, z_n]/I(X))$ we let

$$V(J) := \{a \in X \mid f(a) = 0 \quad \forall f \in J\}.$$

The following result follows at once from the Nullstellensatz.

Proposition 1.6.3 (Nullstellensatz for a closed subset of $\mathbb{A}^n$)**.** *Let $X \subset \mathbb{A}^n$ be closed, and let $J \subset (\mathbb{K}[z_1, \ldots, z_n]/I(X))$ be an ideal. Then*

$$\left\{f \in (\mathbb{K}[z_1, \ldots, z_n]/I(X)) \mid f_{|V(J)} = 0\right\} = \sqrt{J}.$$

(The radical $\sqrt{J}$ is taken inside $\mathbb{K}[z_1, \ldots, z_n]/I(X)$.) In particular $V(J) = \varnothing$ if and only if $J = (1)$.

We introduce notation that is useful in the proof of Theorem 1.6.2. Given a quasi projective variety X, and $f \in \mathbb{K}[X]$, let

$$X_f := X \backslash V(f), \tag{1.6.2}$$

where $V(f) := \{x \in X \mid f(x) = 0\}$. Note the similarity with the notation for principal open subsets of projective varieties.

Remark 1.6.4. Assume that X is affine, hence we may assume that $X \subset \mathbb{A}^n$ is closed. The collection of open subsets $\{X_f\}$ is a basis for the Zariski topology of X. In fact let U be an open subset of X. Then $U = X\backslash V(g_1, \ldots, g_r)$ where $g_i \in \mathbb{K}[z_1, \ldots, z_n]$ for $i \in \{1, \ldots, r\}$. Let $f_i \coloneqq g_{i|X}$. Then $U = X_{g_1} \cup \ldots \cup X_{g_r}$.

Proof of Theorem 1.6.2. The proof is simpler if X is irreducible. We first give the proof under this hypothesis. Let $\varphi \in \mathbb{K}[X]$. We claim that there exist $f_i, g_i \in \mathbb{K}[z_1, \ldots, z_n]$ for $1 \leqslant i \leqslant d$ with $g_i \notin I(X)$ such that

(a) $X = \bigcup_{1 \leqslant i \leqslant d} X_{g_i}$, i.e. $V(g_1, \ldots, g_d) \cap X = \varnothing$,

(b) for all $x \in X_{g_i}$ we have $\varphi(x) = \frac{f_i(x)}{g_i(x)}$,

In fact by definition of regular function (see Example 1.5.5) there exist an open cover $X = \bigcup_{\alpha \in A} U_\alpha$ and $f_\alpha, g_\alpha \in \mathbb{K}[z_1, \ldots, z_n]$ for each $\alpha \in A$ such that $U_\alpha \subset X_{g_\alpha}$ and $\varphi(x) = \frac{f_\alpha(x)}{g_\alpha(x)}$ for each $x \in U_\alpha$. Since the Zariski topology is quasi compact (see Corollary 1.3.9) we may assume that index set A is finite, say $A = \{1, \ldots, d\}$. Of course we may asssume that $g_i \neq 0$ for all $i \in \{1, \ldots, d\}$. Since X is irreducible so is X_{g_i} and hence U_i is dense in X_{g_i}. This imples that $\varphi(x) = \frac{f_i(x)}{g_i(x)}$ on all of X_{g_i} because regular functions are Zariski continuous (see Proposition 1.5.3). This proves the claim.

In the rest of the proof we adopt the following notation: for $f \in \mathbb{K}[z_1, \ldots, z_n]$ we let $\overline{f} \coloneqq f_{|X}$.

For $i = 1, \ldots, d$ the equality $\overline{g}_i\varphi = \overline{f}_i$ holds on X_{g_i} by Item (2). Since X is irreducible and X_{g_i} is a non empty subset of X it is dense in X, and hence $\overline{g}_i\varphi = \overline{f}_i$ on all of X (this is where the hypothesis that X is irreducible simplifies the proof). By Proposition 1.6.3 we have that $(\overline{g}_1, \ldots, \overline{g}_d) = (1)$, i.e. there exist $h_1, \ldots, h_d \in \mathbb{K}[z_1, \ldots, z_n]$ such that

$$1 = \overline{h}_1\overline{g}_1 + \cdots + \overline{h}_d\overline{g}_d.$$

where $\overline{h}_i := h_{i|X}$. Multiplying by φ both sides of the above equality we get that

$$\varphi = \overline{h}_1\overline{g}_1\varphi + \cdots + \overline{h}_d\overline{g}_d\varphi = \overline{h}_1\overline{f}_1 + \ldots + \overline{h}_1\overline{f}_d = (h_1f_1 + \cdots + h_df_d)_{|X}. \tag{1.6.3}$$

This shows that φ is the restriction to X of a polynomial function on $\mathbb{A}^n$.

Now we give the proof for arbitrary (closed) X. Let $\varphi \in \mathbb{K}[X]$. This time we claim that there exist $f_i, g_i \in \mathbb{K}[z_1, \ldots, z_n]$ for $i \in \{1, \ldots, d\}$ such that

1. $X = \bigcup_{1 \leqslant i \leqslant d} X_{g_i}$, i.e. $V(g_1, \ldots, g_d) \cap X = \varnothing$,
2. for all $a \in X_{g_i}$ we have $\varphi(a) = \frac{f_i(a)}{g_i(a)}$,
3. for $1 \leqslant i \leqslant j$ we have $(g_jf_i - g_if_j)|_X = 0$.

We start proving the claim as in the case of X irreducible. There is a finite open cover $X = \bigcup_{\alpha \in A} U_\alpha$ and $f_\alpha, g_\alpha \in \mathbb{K}[z_1, \ldots, z_n]$ for each $\alpha \in A$ such that $U_\alpha \subset X_{g_\alpha}$ and $\varphi(x) = \frac{f_\alpha(x)}{g_\alpha(x)}$ for each $x \in U_\alpha$. We may cover U_α by open affine sets $X_{\gamma_{\alpha,1}}, \ldots, X_{\gamma_{\alpha,r}}$, see Remark 1.6.4. Since $V(\overline{g}_\alpha) \subset \bigcap_{j=1}^{r} V(\overline{\gamma}_{\alpha,j})$ (recall that $\overline{g}_\alpha$ and $\overline{\gamma}_{\alpha,j}$ are the restrictions to X of g_α and $\gamma_{\alpha,j}$ respectively), the Nullstellensatz for X gives that, for each α, j, there exist $N_{\alpha,j} > 0$ and $\mu_{\alpha,j} \in \mathbb{K}[z_1, \ldots, z_n]$ such that $\overline{\gamma}_{\alpha,j}^{N_{\alpha,j}} = \overline{\mu_{\alpha,j}} \cdot \overline{g}_\alpha$. Hence $\varphi(x) = \mu_{\alpha,j}(x) f_\alpha(x)/\gamma_{\alpha,j}(x)^{N_{\alpha,j}}$ for all $x \in X_{\gamma_{\alpha,j}}$. Since $V(\gamma_{\alpha,j}) = V(\gamma_{\alpha,j}^{N_{\alpha,j}})$ it follows that there exist $f_i', g_i' \in \mathbb{K}[z_1, \ldots, z_n]$ for $i \in \{1, \ldots, d\}$ such that $X = \bigcup_{i=1}^{d} X_{g_i'}$ and $\varphi(x) = f_i'(x)/g_i'(x)$ for all $x \in X_{g_i'}$. For $i \in \{1, \ldots, d\}$ let

$$f_i := f_i' g_i', \qquad g_i := (g_i')^2.$$

Clearly Items (1) and (2) hold. In order to check Item (3) we write

$$(g_j f_i - g_i f_j)|_X = ((g_j')^2 f_i' g_i' - (g_i')^2 f_j' g_j')|_X = ((g_i' g_j')(f_i' g_j' - f_j' g_i'))|_X.$$

Since $\varphi(z) = f_i'(x)/g_i'(x) = f_j'(x)/g_j'(x)$ for all $x \in X_{g_i'} \cap X_{g_j'}$ the last term vanishes on $X_{g_i'} \cap X_{g_j'}$. On the other hand the last term vanishes also on $(X \backslash X_{g_i'} \cap X_{g_j'}) = X \cap V(g_i' g_j')$ because of the factor $(g_i' g_j')$. This finishes the proof that there exist $f_i, g_i \in \mathbb{K}[z_1, \ldots, z_n]$ for $i \in \{1, \ldots, d\}$ such that (1), (2) and (3) hold.

Next, for $i = 1, \ldots, d$ let $\overline{g}_i := g_{i|X}$ and $\overline{f}_i := f_{i|X}$. Then

$$\overline{g}_i \varphi = \overline{f}_i. \tag{1.6.4}$$

In fact by Item (1) it suffices to check that (1.6.4) holds on X_{g_j} for $j = 1, \ldots, d$. For $j = i$ it holds by Item (2), for $j \neq i$ it holds by Item (3). Given the equalities in (1.6.4), one finishes the proof proceeding as in the case when X is irreducible. □

Example 1.6.5. Let X be an affine variety, thus we may assume that $X \subset \mathbb{A}^n$ is closed. If $f \in \mathbb{K}[X]$ then X_f is a principal open subset of $\overline{X}$. In fact by Theorem 1.6.2 there exists $g \in \mathbb{K}[z_1, \ldots, z_n]$ such that $f = g_{|X}$. If $d \gg 0$ then

$$G(Z_0, \ldots, Z_n) := Z_0^d g\left(\frac{Z_1}{Z_0}, \ldots, \frac{Z_1}{Z_0}\right)$$

is a homogeneous polynomial whose zero locus (in $\mathbb{P}^n$) is equal to the union of $V(Z_0)$ and $V(g)$ (which is contained in $\mathbb{A}^n$). Hence $\overline{X}_G = (\overline{X} \backslash V(G)) = (X \backslash V(g)) = X_f$. An explicit isomorphism between X_f and a closed subset of an affine space is obtained as follows. Let $Y := V(J) \subset \mathbb{A}^{n+1}$ where J is the ideal generated by $I(X)$ and the polynomial $g(z_1, \ldots, z_n) \cdot z_{n+1} - 1$. Then the map

$$\begin{array}{ccc} X_f & \longrightarrow & Y \\ (z_1, \ldots, z_n) & \mapsto & \left(z_1, \ldots, z_n, \frac{1}{f(z_1, \ldots, z_n)}\right) \end{array}$$

is an isomorphism (see Example 1.5.8). Note that by Theorem 1.6.2 every regular function on X_f is given by the restriction to X_f of $\frac{h}{f^m}$, where $h \in \mathbb{K}[X]$ and $m \in \mathbb{N}$.

Next, we give a few remarkable consequences of Theorem 1.6.2.

Proposition 1.6.6. *Let R be a finitely generated $\mathbb{K}$ algebra without nilpotents. There exists an affine variety X such that $\mathbb{K}[X] \cong R$ (as $\mathbb{K}$ algebras).*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be generators (over $\mathbb{K}$) of R, and let $\varphi\colon \mathbb{K}[z_1, \ldots, z_n] \to R$ be the surjection of algebras mapping z_i to α_i. The kernel of φ is an ideal $I \subset \mathbb{K}[z_1, \ldots, z_n]$, which is radical because R has no nilpotents. Let $X := V(I) \subset \mathbb{A}^n$. Then $\mathbb{K}[X] \cong R$ by Theorem 1.6.2. □

In order to introduce the next result we give a definition.

Definition 1.6.7. Let $\varphi\colon X \to Y$ be a regular map of non empty quasi projective varieties. The pull-back $\varphi^*\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ is the homomorphism of $\mathbb{K}$ algebras defined by

$$\begin{array}{ccc} \mathbb{K}[Y] & \xrightarrow{\varphi^*} & \mathbb{K}[X] \\ f & \mapsto & f \circ \varphi \end{array} \tag{1.6.5}$$

Proposition 1.6.8. *Let Y be an affine variety, and let X be a quasi projective variety. The map*

$$\begin{array}{ccc} \{X \xrightarrow{\varphi} Y \mid \varphi \text{ regular}\} & \longrightarrow & \{\mathbb{K}[Y] \xrightarrow{\alpha} \mathbb{K}[X] \mid \alpha \text{ homom. of } \mathbb{K}\text{-algebras}\} \\ \varphi & \mapsto & \varphi^* \end{array} \tag{1.6.6}$$

is a bijection.

Proof. We may assume that $Y \subset \mathbb{A}^n$ is closed; for $i \in \{1, \ldots, n\}$ let $\overline{z}_i := z_{i|X}$. Suppose that $f, g\colon X \to Y$ are regular maps, and that $f^* = g^*$. Then $f^*(\overline{z}_i) = g^*(\overline{z}_i)$ for $i \in \{1, \ldots, n\}$, and hence $f = g$. This proves injectivity of the map in (1.6.6).

In order to prove surjectivity, let $\alpha\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ be a homomorphism of $\mathbb{K}$ algebras. Let $f_i := \alpha(\overline{z}_i)$, and let $\varphi\colon X \to \mathbb{A}^n$ be the regular map defined by $\varphi(x) := (f_1(x), \ldots, f_n(x))$ for $x \in X$. We claim that $\varphi(x) \in Y$ for all $x \in X$. In fact, since Y is closed, it suffices to show that $g(\varphi(x)) = 0$ for all $g \in I(X)$. Now

$$g(\varphi(x)) = g(f_1(x), \ldots, f_n(x)) = g(\alpha(\overline{z}_1), \ldots, \alpha(\overline{z}_n)) = \alpha(g(\overline{z}_1), \ldots, \overline{z}_n) = \alpha(0) = 0.$$

(The third equality holds because α is a homomorphism of $\mathbb{K}$-algebras.) Thus φ is a regular map $f\colon X \to Y$ such that $\varphi^*(\overline{z}_i)) = \alpha(\overline{z}_i)$ for $i \in \{1, \ldots, n\}$. By Theorem 1.6.2 the $\mathbb{K}$-algebra $\mathbb{K}[Y]$ is generated by $\overline{z}_1, \ldots, \overline{z}_n$; it follows that $\varphi^* = \alpha$. □

Corollary 1.6.9. *In Proposition 1.6.6, the affine variety X such that $\mathbb{K}[X] \cong R$ is unique up to isomorphism.*

1.7 Quasi-projective varieties defined over a subfield of $\mathbb{K}$

Let $F \subset \mathbb{K}$ be a subfield. For example $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{C}$ or $\mathbb{F}_q \subset \overline{\mathbb{F}}_q$ where $q = p^r$ with p a prime.

Definition 1.7.1. A locally closed subset $X \subset \mathbb{P}^n(\mathbb{K})$ is *defined over F* if both the homogeneous ideals $I(\overline{X}) \subset \mathbb{K}[Z_0, \ldots, Z_n]$ and $I(\overline{X}\backslash X) \subset \mathbb{K}[Z_0, \ldots, Z_n]$ admit sets of generators belonging to $F[Z_0, \ldots, Z_n]$.

Trivially $\mathbb{P}^n(\mathbb{K})$ and $\mathbb{A}^n(\mathbb{K}) = \mathbb{P}^n(\mathbb{K})_{Z_0}$ are defined over the prime field, i.e. over $\mathbb{Q}$ if $\operatorname{char} \mathbb{K} = 0$ and over $\mathbb{F}_p$ if $\operatorname{char} \mathbb{K} = p$.

Remark 1.7.2. A locally closed subset $X \subset \mathbb{A}^n(\mathbb{K}) = \mathbb{P}^n(\mathbb{K})_{Z_0}$ is defined over F if both the ideals $I(\overline{X}) \subset \mathbb{K}[z_1, \ldots, z_n]$ and $I(\overline{X}\backslash X) \subset \mathbb{K}[z_1, \ldots, z_n]$ (in general non homogeneous) admit sets of generators which belong to $F[z_1, \ldots, z_n]$. This is so because a polynomial $p \in \mathbb{K}[z_1, \ldots, z_n]$ of degree d vanishes on X if and only if the homogeneous polynomial $P := Z_0^d \cdot f(Z_1/Z_0, \ldots, Z_n/Z_0)$ vanishes on $\overline{X}$, and conversely a homogeneous $P \in \mathbb{K}[Z_0, \ldots, Z_n]$ vanishes on $\overline{X}$ if and only if $P(1, z_1, \ldots, z_n) \in \mathbb{K}[z_1, \ldots, z_n]$ vanishes on X.

Example 1.7.3. Let $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$. If a_i belongs to F for all $i \in \{1, \ldots, n\}$ then $\{a\}$ is defined over F because its ideal is generated by $(z_1 - a_1, \ldots, z_n - a_n)$. The converse is true if we make a hypothesis on the field extension $F \subset \mathbb{K}$. Let $\operatorname{Aut}(\mathbb{K}, F)$ be the group of automorphisms of $\mathbb{K}$ fixing every element of F. Assume that the field of elements of $\mathbb{K}$ fixed by $\operatorname{Aut}(\mathbb{K}, F)$ is equal to F. (Since $\mathbb{K}$ is algebraically closed this holds if $\operatorname{char} \mathbb{K} = 0$ or, in case $\operatorname{char} \mathbb{K} = p$ if F is perfect, i.e. every element of F has a p-th root in F (necessarily unique).) With this hypothesis, suppose that $\{a\}$ is defined over

F, and let $p_1, \ldots, p_r \in F[z_1, \ldots, z_n]$ be generators of $I(\{a\}) \subset \mathbb{K}[z_1, \ldots, z_n]$. For $j \in \{1, \ldots, r\}$ let $p_j = \sum_I c_{j,I} z^I$ where $c_{j,I} \in F$ for each multiindex I. If $\sigma \in \mathrm{Aut}(\mathbb{K}, F)$ we have

$$0 = \sigma(0) = \sigma(p_j(a)) = p_j(\sigma(a_1), \ldots, \sigma(a_n)) = \sum_I c_{j,I}\sigma(a_1)^{i_1} \ldots \sigma(a_n)^{i_n} = p_j(\sigma(a)). \tag{1.7.1}$$

(The second to last equality holds because p_j has coefficients in F.) Since the above equality holds for generators of the ideal of $\{a\}$, we get that $(\sigma(a_1), \ldots, \sigma(a_n)) = (a_1, \ldots, a_n)$ for all $\sigma \in \mathrm{Aut}(\mathbb{K}, F)$. By our hypothesis on $\mathrm{Aut}(\mathbb{K}, F)$ it follows that $a_i \in F$ for all i.

Example 1.7.4. Let $Q \in \mathbb{R}[Z_0, \ldots, Z_n]_2$ be a non zero quadratic form. Then $Z := V(Q) \subset \mathbb{P}^n(\mathbb{C})$ is a projective variety defined over $\mathbb{R}$. In fact if Q has rank at least 2 then Q generates $I(Z)$, and if Q has rank 1, i.e. $Q = L^2$ for $L \in \mathbb{C}[Z_0, \ldots, Z_n]_1$ then either $L \in \mathbb{R}[Z_0, \ldots, Z_n]_1$ or $\sqrt{-1}L \in \mathbb{R}[Z_0, \ldots, Z_n]_1$.

Example 1.7.5. The Fermat hypersurface $X := V(\sum_{i=0}^n Z_i^d)$ is defined over the prime field. In order to check this one must show that $I(X)$, i.e. the radical of $(\sum_{i=0}^n Z_i^d)$ is generated by a polynomial with coefficients in the prime field. If $\mathrm{char}\,\mathbb{K}$ does not divide d then the polynomial $\sum_{i=0}^n Z_i^d$ generates a radical ideal in $\mathbb{K}[Z_0, \ldots, Z_n]$ (to see this take the formal partial derivative with respect to one of its variables), and hence it generates $I(X)$. Since the coefficients of $\sum_{i=0}^n Z_i^d$ belong to the prime field we are done. If $\mathrm{char}\,\mathbb{K} = p > 0$ write $d = p^r d_0$ where p does not divide d_0. Then $\sum_{i=0}^n Z_i^d = (\sum_{i=0}^n Z_i^{d_0})^{p^r}$ and hence $I(X)$ is generated by $\sum_{i=0}^n Z_i^{d_0}$ (see above). Since the coefficients of $\sum_{i=0}^n Z_i^{d_0}$ belong to the prime field we are done.

Remark 1.7.6. Let $F \subset F' \subset \mathbb{K}$ be an inclusion of fields, and let $X \subset \mathbb{P}^n(\mathbb{K})$ be a locally closed subset defined over F. Then X is also defined over F'. In particular if X is defined over the prime field it is defined over every subfield of $\mathbb{K}$.

Definition 1.7.7. Let $X \subset \mathbb{P}^n(\mathbb{K})$ be a locally closed subset defined over F. We let $X(F) \subset X$ be the set of points represented by $(n+1)$-tuples $(Z_0, Z_1, \ldots, Z_n) \in F^{n+1} \backslash \{(0, \ldots, 0)\}$.

Remark 1.7.8. Let $X \subset \mathbb{A}^n(\mathbb{K})$ be a locally closed subset defined over F. Then $X(F) \subset X$ is equal to $X \cap \mathbb{A}^n(F)$.

Remark 1.7.9. Let $F \subset F' \subset \mathbb{K}$ be an inclusion of fields, and let $X \subset \mathbb{P}^n(\mathbb{K})$ be a locally closed subset defined over F. Then X is also defined over F' and hence $X(F')$ is also defined. In particular $X(\mathbb{K})$ is defined and equals X.

Remark 1.7.10. Let p be a prime, and suppose that $\mathbb{F}_q \subset \mathbb{K}$ where $q = p^r$. Let $X \subset \mathbb{P}^n(\overline{\mathbb{F}}_p)$ be a locally closed subset defined over F_q. For each $m \in \mathbb{N}_+$ there is a unique inclusion $\mathbb{F}_q \subset \mathbb{F}_{q^m} \subset \mathbb{K}$, and hence we have $X(\mathbb{F}_{q^m})$. Clearly $X(\mathbb{F}_{q^m})$ is a finite set.

Definition 1.7.11. Let $X \subset \mathbb{P}^n(\overline{\mathbb{F}}_p)$ be a locally closed subset defined over F_q, where $q = p^r$. The *Weil Zeta function of* X is defined to be formal power series in the variable T given by

$$Z(X, T) := \exp\left(\sum_{m=1}^{\infty} \frac{|X(\mathbb{F}_{q^m})|}{m} T^m\right) \tag{1.7.2}$$

Definition 1.7.12. Let $X \subset \mathbb{P}^n(\mathbb{K})$ and $Y \subset \mathbb{P}^m(\mathbb{K})$ be locally closed subset, both defined over a subfield $F \subset \mathbb{K}$. A map $\varphi := X \to Y$ is *defined over* F if for each $a \in X$ there exist an open $U \subset X$ containing a and $P_j \in F[Z_0, \ldots, Z_n]_d$ for $j \in \{0, \ldots, m\}$ (d depends on U), such that the restriction of φ to U is

$$\begin{array}{ccc} U & \longrightarrow & \mathbb{P}^m \\ [Z] & \to & [P_0(Z), \ldots, P_m(Z)] \end{array} \tag{1.7.3}$$

(of course $(P_0(Z), \ldots, P_m(Z)) \neq (0, \ldots, 0)$ for all $[Z] \in U$).

Let $F \subset \mathbb{K}$ be a subfield. If $X \subset \mathbb{P}^n(\mathbb{K})$ is a locally closed subset defined over F then the identity map $\mathrm{Id}_X : X \to X$ is clearly defined over F. If $X \subset \mathbb{P}^n(\mathbb{K})$, and $Y \subset \mathbb{P}^m(\mathbb{K})$, $W \subset \mathbb{P}^l(\mathbb{K})$ are locally closed subsets defined over F and $\varphi\colon X \to Y$, $\psi\colon Y \to W$ are regular maps defined over F then the composition $\psi \circ \varphi\colon X \to W$ is also defined over F. In fact this holds because if $P \in F[Z_0, \ldots, Z_m]_d$ and $Q_0, \ldots, Q_m \in F[T_0, \ldots, T_n]_e$ then $P(Q_0, \ldots, Q_m) \in F[T_0, \ldots, T_n]_{de}$.

Hence we have the category of quasi projective varieties defined over F. In particular we have the notion of isomorphism over F of varieties defined over F.

Remark 1.7.13. Let $X \subset \mathbb{P}^n(\mathbb{K})$ and $Y \subset \mathbb{P}^m(\mathbb{K})$ be locally closed subsets defined over F. If $\varphi\colon X \to Y$ is a regular map defined over F then $\varphi(X(F)) \subset Y(F)$ because the value of a polynomial with coefficients in F at $(A_0, \ldots, A_n) \in F^{n+1}$ belongs to F.

Example 1.7.14. Let $Q_1, Q_2 \in \mathbb{R}[Z_0, \ldots, Z_n]_2$ be non degenerate quadratic forms, and let $X_i := V(Q_i)$ for $i \in \{1, 2\}$. Then $X_i \subset \mathbb{P}^n(\mathbb{C})$ is a projective variety defined over $\mathbb{R}$. Since Q_i is diagonalizable in suitable coordinates, there exists a projectivity $\varphi\colon \mathbb{P}^n(\mathbb{C}) \to \mathbb{P}^n(\mathbb{C})$ whose restriction to X_1 defines an isomorphism $X_1 \xrightarrow{\sim} X_2$. In particular X_1 is isomorphic to X_2 (over $\mathbb{C}$). On the other hand X_1 is not necessarily isomorphic to X_2 over $\mathbb{R}$. In fact let $Q_1 := \sum_{j=0}^{n} Z_j^2$ and $Q_2 := Z_0^2 - \sum_{j=1}^{n} Z_j^2$. Thus $X_1(\mathbb{R})$ is empty while $X_2(\mathbb{R})$ is not empty. Since a regular map $\varphi\colon X_1 \to X_2$ defined over $\mathbb{R}$ maps $X_1(\mathbb{R})$ to $X_2(\mathbb{R})$ it follows that X_1 is not isomorphic to X_2 over $\mathbb{R}$ (we assume that $n \geqslant 1$).

Under a suitable hypothesis we can avoid computing the radical of ideals if we wish to decide whether a locally closed subset $X \subset \mathbb{P}^n(\mathbb{K})$ is defined over a subfield $F \subset \mathbb{K}$. Let $\mathrm{Aut}(\mathbb{K}/F)$ be the group of automorphisms of K which are the identity on F.

Proposition 1.7.15. *Suppose that the fixed field of* $\mathrm{Aut}(\mathbb{K}/F)$ *is equal to* F. *Let* $X \subset \mathbb{P}^n(\mathbb{K})$ *be a locally closed subset given by* $V(I) \backslash V(J)$ *where* $I, J \subset \mathbb{K}[Z_0, \ldots, Z_n]$ *are homogeneous ideals which admit sets of generators belonging to* $F[Z_0, \ldots, Z_n]$. *Then* X *is defined over* F.

Before proving Proposition 1.7.15 we go through a few preliminaries. The group $\mathrm{Aut}(\mathbb{K})$ of field automorphisms of $\mathbb{K}$ acts on $\mathbb{P}^n$ as follows: for $\sigma \in \mathrm{Aut}(\mathbb{K})$

$$\begin{array}{ccc} \mathrm{Aut}(\mathbb{K}) \times \mathbb{P}^n & \longrightarrow & \mathbb{P}^n \\ (\sigma, [Z_0, \ldots, Z_n]) & \mapsto & [\sigma(Z_0), \ldots, \sigma(Z_n)] \end{array} \tag{1.7.4}$$

Note that if $X \subset \mathbb{A}^n$ $(= \mathbb{P}^n_{Z_0})$ then $\sigma(z_1, \ldots, z_n) = (\sigma(z_1), \ldots, \sigma(z_n))$.

Remark 1.7.16. In general the map $\mathbb{P}^n \to \mathbb{P}^n$ that one gets by fixing a non trivial $\sigma \in \mathrm{Aut}(\mathbb{K})$ in (1.7.4) is not regular. For example if $F = \mathbb{R} \subset \mathbb{C}$ and σ is complex conjugation the map is not regular.

Proposition 1.7.17. *Let* $X \subset \mathbb{P}^n(\mathbb{K})$ *be a locally closed subset defined over* F. *If* $\sigma \in \mathrm{Aut}(\mathbb{K}/F)$ *then* $\sigma(X) = X$.

Proof. It suffices to prove that $\sigma(X) = X$ for every closed subset $X \subset \mathbb{P}^n(\mathbb{K})$ defined over F. Let $P \in F[Z_0, \ldots, Z_n] \cap I(X)$ be homogeneous. Thus $P = \sum_I c_I Z^I$ where each c_I belongs to F. If $[A_0, \ldots, A_n] \in X$ then $P(A_0, \ldots, A_n) = 0$ and hence

$$0 = \sigma(P(A_0, \ldots, A_n)) = \sum_I \sigma(c_I)\sigma(A_0)^{i_0} \ldots \sigma(A_n)^{i_n} = \sum_I c_I \sigma(A_0)^{i_0} \ldots \sigma(A_n)^{i_n} = P(\sigma(A_0), \ldots, \sigma(A_n)).$$

This proves that $\sigma(X) \subset X$ because the ideal $I(X) \subset \mathbb{K}[Z_0, \ldots, Z_n]$ is generated by homogeneous elements of $F[Z_0, \ldots, Z_n] \cap I(X)$. Thus we also have $\sigma^{-1}(X) \subset X$ and hence $X \subset \sigma(X)$. ☐

Proof of Proposition 1.7.15. The group $\mathrm{Aut}(\mathbb{K}/F)$ acts on $\mathbb{K}[Z_0, \ldots, Z_n]$ by acting on the coefficients of polynomials. We claim that $\mathrm{Aut}(\mathbb{K}/F)$ maps $I(X)$ to itself. In fact let $\sigma \in \mathrm{Aut}(\mathbb{K}/F)$ and let $P \in I(X)$ be a homogeneous polynomial, $P = \sum_I c_I Z^I$. By Proposition 1.7.17 we have $\sigma^{-1}(X) = X$, hence

$$\sigma(P)(A) = \sum_I \sigma(c_I) A^I = \sigma\left(\sum_I c_I \sigma^{-1}(A_0)^{i_0} \ldots \sigma^{-1}(A_n)^{i_n}\right) = \sigma(P(\sigma^{-1}(A)) = 0.$$

We have an obvious isomorphism $\mathbb{K}[Z_0,\ldots,Z_n] \cong \mathbb{K}_F F[Z_0,\ldots,Z_n]$ which is equivariant for the action of $\mathrm{Aut}(\mathbb{K}/F)$ that we have just defined and the action considered in Section A.6. By Proposition A.6.3 it follows that $I(X)$ is generated (as $\mathbb{K}$ vector space by its intersection with $F[Z_0,\ldots,Z_n]$. This proves Proposition 1.7.15. □

Example 1.7.18. Assume that $\mathrm{char}\,\mathbb{K} = p > 0$. Let $F\colon \mathbb{K} \to \mathbb{K}$ be the Frobenius automorphism: $F(a) := a^p$. Let r be a positive natural number. Of course F^r is also an automorphism of $\mathbb{K}$. Note that $F^r(a) = a^q$ and that $F^r \in \mathrm{Aut}(\mathbb{K}/\mathbb{F}_q)$. There exists a unique embedding $\mathbb{F}_q \subset \mathbb{K}$. Suppose that $X \subset \mathbb{P}^n$ is a closed subset defined over $\mathbb{F}_q$. Proposition 1.7.17 gives that we have the bijective map

$$\begin{array}{ccc} X & \xrightarrow{\pi} & X \\ [Z] & \mapsto & [Z_0^q,\ldots,Z_n^q]. \end{array}$$

This is the *Frobenius map of* X. Note the exceptional feature of the Frobenius map: it is regular (see remark 1.7.16) and even defined over the prime field. Let $X \subset \mathbb{P}^n$ be a locally closed subset defined over $\mathbb{F}_q$. Since π is a bijection (but not an isomorphism) then the same formula gives a Frobenius map from X to itself.

1.8 Exercises

Exercise 1.8.1. Which of the following subsets of $\mathbb{A}^2$ are locally closed? Which are closed?

(a) $X := \left\{(x,y) \mid \exp\left(2\pi\sqrt{-1}x\right) = 1\right\} \subset \mathbb{A}^2(\mathbb{C})$.

(b) $Y := \left\{\left(t,t^2\right) \mid t \in \mathbb{K}\right\} \subset \mathbb{A}^2(\mathbb{K})$.

(c) $W := \left\{\left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right) \mid t \in \mathbb{C}\backslash\left\{\pm\sqrt{-1}\right\}\right\} \subset \mathbb{A}^2(\mathbb{C})$.

(d) $V := \left\{(t,tu) \mid (t,u) \in \mathbb{K}^2\right\} \subset \mathbb{A}^2(\mathbb{K})$.

Exercise 1.8.2. Compute $I(Z)$ for

1. $Z = V\left(x^2+1\right) \subset \mathbb{A}^1(\mathbb{K})$,
2. $Z = \mathbb{Z}^2 \subset \mathbb{A}^2(\mathbb{C})$,
3. $Z = V\left(x^2-y^2, x^2-xy\right) \subset \mathbb{A}^2(\mathbb{K})$.

Exercise 1.8.3. Let $M_{2,2}(\mathbb{C})$ be the complex vector-space of 2×2 complex matrices. Let $n>0$ and let $U_n \subset M_{2,2}(\mathbb{C})$ be the set of matrices T such that $T^n = 1$ (here $1 \in M_{2,2}(\mathbb{C})$ is the unit matrix).

1. Prove that U_n is a closed subset (for the Zariski Topology) of $M_{2,2}(\mathbb{C})$.
2. Describe the irreducible components of U_n and show that there are $\binom{n+1}{2}$ of them.

Exercise 1.8.4. Let $f_1,\ldots,f_r \in \mathbb{K}[x,y]$ and suppose that

$$\gcd\{f_1,\ldots,f_r\} = 1.$$

Show that $V(f_1,\ldots,f_r) \subset \mathbb{A}^2(\mathbb{K})$ is finite.

Exercise 1.8.5. Let $X \subset \mathbb{A}^2(\mathbb{K})$ be a proper closed irreducible subset. Show that Z is either a singleton or an irreducible hypersurface.

Exercise 1.8.6. Let $M_n(\mathbb{K})$ be the vector-space of $n \times n$ matrices with entries in $\mathbb{K}$, and let $M_n(\mathbb{K})_- \subset M_n(\mathbb{K})$ be the subspace of skew-symmetric matrices. Let $X \in M_n(\mathbb{K})_-$: then

$$X = \begin{bmatrix} 0 & x_{1,2} & \dots & \dots & x_{1,n} \\ -x_{1,2} & 0 & x_{2,3} & \dots & x_{2,n} \\ -x_{1,3} & -x_{1,3} & 0 & \dots & x_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -x_{1,n} & -x_{2,n} & \dots & \dots & 0 \end{bmatrix}$$

Thus $\{x_{1,2}, \ldots, x_{1,n}, x_{2,3}, \ldots, x_{n-1,n}\}$ is a basis of the dual of $M_n(\mathbb{K})_-$, and hence $\mathbb{K}[x_{1,2}, \ldots, x_{1,n}, x_{2,3}, \ldots, x_{n-1,n}]$ is the $\mathbb{K}$ algebra of. polynomial functions on $M_n(\mathbb{K})_-$. Let $\Delta_n \subset M_n(\mathbb{K})_-$ be the set of $n \times n$ singular skew-symmetric matrices, and let δ_n be the polynomial on $M_n(\mathbb{K})_-$ given by $\delta_n(X) := \det X$. Then Δ_n is closed in $M_n(\mathbb{K})_-$ because $\Delta_n = V(\delta_n)$. Prove the following:

(1.8.6a) If n is odd then $\Delta_n = M_n(\mathbb{K})_-$.

(1.8.6b) If n is even then Δ_n is a hypersurface and $I(\Delta_n) \neq (\delta_n)$.

Exercise 1.8.7. An affine map

$$\begin{array}{ccc} \mathbb{A}^n & \longrightarrow & \mathbb{A}^n \\ Z & \mapsto & A \cdot Z + B \end{array}$$

(here Z, B are column vectors with n entries and $A \in \mathrm{GL}_n(\mathbb{K})$) is an automorphism of $\mathbb{A}^n$.

(1.8.7a) Show that *every* automorphism of $\mathbb{A}^1$ is an affine map.

(1.8.7b) Let $n \geqslant 2$. Show that if $f \in \mathbb{K}[z_1, \ldots, z_{n-1}]$ then

$$\begin{array}{ccc} \mathbb{A}^n & \xrightarrow{\Phi_f} & \mathbb{A}^n \\ z & \mapsto & (z_1, \ldots, x_{n-1}, z_n + f(z_1, \ldots, z_{n-1}) \end{array} \tag{1.8.5}$$

is an automorphism. Prove that Φ_f is an affine map if and only if $\deg f \leqslant 1$.

Exercise 1.8.8. Show that one can prove the validity of Theorem 1.6.2 for $\mathbb{A}^n$ by invoking unique factorization in $\mathbb{K}[z_1, \ldots, z_n]$, without using the Nullstellensatz.

Exercise 1.8.9. Let K be a field. Given a finite-dimensional K-vector space V define the formal power series $p_V \in \mathbb{Z}[[t]]$ as

$$P_V := \sum_{d=0}^{\infty} (\dim_k \mathrm{Sym}^d V) t^d$$

where $\mathrm{Sym}^d V$ is the symmetric product of V. Thus if $V = K[x_1, \ldots, x_n]_1$ then $S^d(K[x_1, \ldots, x_n]_1) = K[x_1, \ldots, x_n]_d$.

1. Prove that if $V = U \oplus W$ then $P_V = P_U \cdot P_W$.
2. Prove that if $\dim_K V = n$ then $P_V = (1-t)^{-n}$ and hence the equality in (1.5.10) holds.

Exercise 1.8.10. The purpose of the present exercise is to give a different proof of the properties of the Veronese map ν_d^n discussed in Example 1.5.12, *valid if* $\mathrm{char}\,\mathbb{K} = 0$, *or more generally* $\mathrm{char}\,\mathbb{K}$ *does not divide* $d!$. Let

$$\begin{array}{ccc} \mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_1) & \xrightarrow{\mu_d^n} & \mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_d) \\ [L] & \mapsto & [L^d] \end{array} \tag{1.8.6}$$

and let $\mathscr{W}_d^n = \mathrm{Im}(\mu_d^n)$. The above map can be identified with the Veronese map ν_d^n. In fact, writing $L \in \mathbb{K}[T_0, \ldots, T_n]_1$ as $L = \sum_{i=0}^n \alpha_i T_i$, we see that $[\alpha_0, \ldots, \alpha_n]$ are coordinates on $\mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_1)$, and they give an identification $\mathbb{P}^n \xrightarrow{\sim} \mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_1)$. Moreover, let

$$\begin{array}{ccc} \mathbb{P}^{\binom{d+n}{n}-1} & \xrightarrow{\sim} & \mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_d), \\ [\ldots, \xi_I, \ldots] & \mapsto & \sum_{\substack{I=(i_0,\ldots,i_n) \\ i_0+\ldots+i_n=d}} \frac{d!}{i_0! \cdot \ldots \cdot i_n!} \xi_I T^I \end{array}$$

where $T^I = T_0^{i_0} \cdot \ldots \cdot T_n^{i_n}$. By Newton's formula $(\sum_{i=0}^n \alpha_i T_i)^d = \sum_I \frac{d!}{i_0! \cdot \ldots \cdot i_n!} \alpha^I T^I$, we see that, modulo the above isomorphisms, the Veronese map ν_d^n is identified with μ_d^n, and hence $\mathscr{V}_d^n$ is identified with $\mathscr{W}_d^n$.

Now let us show that $\mathscr{W}_d^n$ is closed. The key observation is that $[F] \in \mathscr{W}_d^n$ if and only if $\frac{\partial F}{\partial Z_0}, \ldots, \frac{\partial F}{\partial Z_n}$ span a 1-dimensional subspace of $\mathbb{K}[Z_0, \ldots, Z_n]$. This may be proved by induction on $\deg F$ and *Euler's identity*

$$\sum_{j=0}^n Z_j \frac{\partial F}{\partial Z_j} = (\deg F) \cdot F, \tag{1.8.7}$$

valid for F *homogeneous*. Now, the condition that $\frac{\partial F}{\partial Z_0}, \ldots, \frac{\partial F}{\partial Z_n}$ span a 1-dimensional subspace of $\mathbb{K}[Z_0, \ldots, Z_n]$ is equivalent to the vanishing of determinants of all 2×2 minors of the matrix whose entries are the coordinates of $\frac{\partial F}{\partial Z_0}, \ldots, \frac{\partial F}{\partial Z_n}$; thus $\mathscr{W}_d^n$ is closed.

In order to show that μ_d^n is an isomorphism, we notice that if $F = L^d$, where $L \in \mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_1$ is non zero, then for each $i \in \{0, \ldots, n\}$ the partial derivative $\frac{\partial^{n-1} F}{\partial Z_i^{n-1}}$ is a multiple of L (eventually equal to 0 if $\frac{\partial L}{\partial Z_i} = 0$), and that one at least of such $(n-1)$-th partial derivative is non zero. Thus, the inverse of μ_d^n is the regular map $\theta_d^n \colon \mathscr{W}_d^n \longrightarrow \mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_1)$ defined by

$$\theta_d^n([F]) := \begin{cases} [\frac{\partial^{n-1} F}{\partial Z_0^{n-1}}] & \text{if } \frac{\partial^{n-1} F}{\partial Z_0^{n-1}} \neq 0, \\ \cdots\cdots & \cdots\cdots \\ [\frac{\partial^{n-1} F}{\partial Z_n^{n-1}}] & \text{if } \frac{\partial^{n-1} F}{\partial Z_n^{n-1}} \neq 0. \end{cases} \tag{1.8.8}$$

Exercise 1.8.11. Let R be an integral domain, and let $(m, n) \in (\mathbb{N}^2 \backslash \{0\})$. Let $F \in R[X, Y]_m$ and $G \in R[X, Y]_n$. The *resultant* $\mathscr{R}(F, G)$ is the element of R defined as follows. Consider the map of free R-modules

$$\begin{array}{ccc} R[X,Y]_{n-1} \oplus R[X,Y]_{m-1} & \stackrel{L(F,G)}{\longrightarrow} & R[X,Y]_{m+n-1} \\ (\Phi, \Psi) & \mapsto & \Phi \cdot F + \Psi \cdot G \end{array} \tag{1.8.9}$$

and let $S(F, G)$ be the matrix of $L(F, G)$ relative to the basis

$$(X^{n-1}, 0),\ (X^{n-2}Y, 0),\ \ldots\ ,\ (Y^{n-1}, 0),\ (0, X^{m-1}),\ (0, X^{m-2}Y),\ \ldots\ ,\ (0, Y^{m-1}) \tag{1.8.10}$$

of the domain and the basis

$$X^{m+n-1},\ X^{m+n-2}Y,\ \ldots\ ,\ XY^{m+n-2},\ Y^{m+n-1} \tag{1.8.11}$$

of the codomain. Then $\mathscr{R}(F, G)$ is defined by

$$\mathscr{R}(F, G) := \det S(F, G). \tag{1.8.12}$$

Explicitly: if

$$F = \sum_{i=0}^m a_i X^{m-i} Y^i, \quad G = \sum_{j=0}^n b_j X^{n-j} Y^j \tag{1.8.13}$$

then

$$\mathscr{R}(F,G) = \det \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \cdots & a_0 & \vdots & \vdots & \cdots & b_0 \\ a_m & a_{m-1} & \cdots & \vdots & b_n & b_{n-1} & \cdots & \vdots \\ 0 & a_m & \cdots & \vdots & 0 & b_n & \cdots & \vdots \\ 0 & 0 & \cdots & \vdots & 0 & 0 & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a_m & 0 & 0 & \cdots & b_n \end{pmatrix}. \tag{1.8.14}$$

Now let K be a field and $K \subset \overline{K}$ be an algebraic closure of K. Let $F \in K[X, Y]_m$ and $G \in K[X, Y]_n$.

(a) Prove that $\mathscr{R}(F,G)=0$ if and only if there exists $H\in K[X,Y]_d$ with $d>0$ which divides both F and G (in $K[X,Y]$).

(b) Prove that $\mathscr{R}_{m,n}(F,G)=0$ if and only if there exists a common non-trivial root of F and G in $\overline{k}^2$, i.e. $[X_0,Y_0]\in\mathbb{P}^1_{\overline{k}}$ such that $F(X_0,Y_0)=G(X_0,Y_0)=0$.

(c) Let $f(t,x)\in K[t_1,\ldots,t_m][x]$ and $g(t,x)\in K[t_1,\ldots,t_m][x]$ (here $t=t_1,\ldots,t_m$) be polynomials of degrees m and n in x respectively, i.e.

$$f(t,x)=\sum_{i=1}^{m}a_i(t)x^{m-i},\quad g(t,x)=\sum_{j=1}^{n}b_j(t)x^{n-j}\quad a_i(t),b_j(t)\in K[t_1,\ldots,t_m],\quad a_0(t)\neq 0\neq b_0(t).$$

We let

$$D(f,g):=\{\overline{t}\in\mathbb{A}^m(\overline{K})\mid \exists x\in\overline{K}\text{ such that }f(\overline{t},x)=g(\overline{t};x)=0\}.$$

Using the properties of the resultant proved above show that if f,g are both monic, i.e. $a_0(t)=b_0(t)=1$, then there exists $\varphi\in K[t_1,\ldots,t_m]$ such that $D(f,g)=V(\varphi)$.

(d) Give examples of $f(t,x)\in K[t_1,\ldots,t_m][x]$ and $g(t,x)\in K[t_1,\ldots,t_m][x]$ for which there exists no $\varphi\in K[t_1,\ldots,t_m]$ such that $D(f,g)=V(\varphi)$.

Exercise 1.8.12. Let V be a $\mathbb{K}$ vector space of finite dimension, and let $0\leqslant h\leqslant\dim V$. The *Grassmannian*

$$\operatorname{Gr}(h,V):=\{W\subset V\mid \dim W=h\}.$$

is the set of subvector spaces of V of dimension h. Note that if $h\in\{0,\dim V\}$, then $\operatorname{Gr}(h,V)$ is a singleton, that $\operatorname{Gr}(1,V)=\mathbb{P}(V)$, and that we have a bijection

$$\begin{array}{ccc}\mathbb{P}(V^\vee) & \longrightarrow & \operatorname{Gr}(\dim V-1,V)\\ [f] & \mapsto & \ker(f)\end{array}$$

The goal of the present exercise is to identify (in a reasonable way) the elements of $\operatorname{Gr}(h,V)$ with the points of a projective variety.

1. Let $v_1,\ldots,v_a\in V$ be linearly independent, and let $\alpha\in\bigwedge^h V$. Prove that

$$v_i\wedge\alpha=0\quad\forall i\in\{1,\ldots,a\}$$

if and only if $\alpha=v_1\wedge\ldots\wedge v_a\wedge\beta$ for a suitable $\beta\in\bigwedge^{h-a}V$.

2. For $\alpha\in\bigwedge^h V$, let m_α be the linear map

$$\begin{array}{ccc}V & \xrightarrow{m_\alpha} & \bigwedge^{h+1}V\\ v & \mapsto & v\wedge\alpha\end{array}$$

Using the result of Item (1) show that if $\alpha\neq 0$ then the kernel of m_α has dimension at most h, and that it has dimension equal to h if and only if α is *decomposable*, i.e. $\alpha=w_1\wedge\ldots\wedge w_h$ for suitable linearly independent $w_1\wedge\ldots\wedge w_h\in V$.

3. The *Plücker map* is given by

$$\begin{array}{ccc}\operatorname{Gr}(h,V) & \xrightarrow{\mathcal{P}} & \mathbb{P}\left(\bigwedge^h V\right)\\ W & \mapsto & \bigwedge^h W.\end{array}$$

Note that this makes sense because $\bigwedge^h W$ is a 1-dimensional subspace of $\bigwedge^h V$. Using the result of Item (2) prove that $\mathscr{P}$ is injective, and that $\operatorname{Im}\mathscr{P}$ is a closed subset of $\mathbb{P}\left(\bigwedge^h V\right)$. Thus we have identified $\operatorname{Gr}(h,V)$ with a projective variety.

Note that we have a bijection

$$\begin{array}{ccc}\operatorname{Gr}(k+1,V) & \longrightarrow & \operatorname{Gr}(k,\mathbb{P}(V)):=\{L\subset\mathbb{P}(V)\mid L\text{ linear subspace, }\dim L=k\}\\ W & \mapsto & \mathbb{P}(W).\end{array}$$

Thus we may also identify $\operatorname{Gr}(k,\mathbb{P}(V))$ with a projective variety.

Let $v_1, \ldots, v_m$ be a basis of V. If $I = \{i_1, \ldots, i_h\}$ with $1 \leqslant i_1 < \ldots < i_h \leqslant \dim V$ we let $v_I := v_{i_1} \wedge \ldots \wedge v_{i_h}$. Then $\mathscr{B} := \{\ldots, v_I, \ldots\}$, for I running through subsets of $\{1, \ldots, m\}$ of cardinality h, is a basis of $\bigwedge^h V$. Associated to $\mathscr{B}$ we have homogeneous coordinates $[\ldots, T_I, \ldots]$ on $\mathbb{P}(\bigwedge^h V)$. By associating to linearly independent vectors $w_1, \ldots, w_h \in V$ the matrix with rows the coordinates of the w_i's in the chosen basis, we get a matrix

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{h1} & \cdots & a_{hm} \end{pmatrix}$$

of rank h. The homogeneous coordinates $[\ldots, T_I, \ldots]$ of $\mathscr{P}(\langle w_1, \ldots, w_h \rangle)$ are given by

$$T_I = \det \begin{pmatrix} a_{1,i_1} & \cdots & a_{1,i_h} \\ \vdots & \ddots & \vdots \\ a_{h,i_1} & \cdots & a_{h,i_h} \end{pmatrix}.$$

Exercise 1.8.13. The goal of the present exercise is to show that the Grassmannian $\mathrm{Gr}(h, V)$ (identified with its image by the Plücker embedding) has an open covering by pairwise intersecting open subsets isomorphic to an affine space of dimension $h \cdot (\dim V - h)$, and that it is irreducible.

1. Let $m := \dim V$, and let $\{v_1, \ldots, v_m\}$ be a basis of V. Let $[\ldots, T_I, \ldots]$ be the associated homogeneous coordinates on $\mathbb{P}(\bigwedge^h V)$, where I runs through subsets of $\{1, \ldots, m\}$ of cardinality h. Thus we have the open covering
$$\mathrm{Gr}(h, V) = \bigcup_{|I|=h} \mathrm{Gr}(h, V)_I, \tag{1.8.15}$$
where $\mathrm{Gr}(h, V)_I \subset \mathrm{Gr}(h, V)$ is the open subset of points such that $T_I \neq 0$. Let $I = \{1, \ldots, h\}$. Show that the map
$$\begin{array}{ccc} \mathscr{M}_{h,m-h}(\mathbb{K}) & \longrightarrow & \mathrm{Gr}(h, V)_I \\ \begin{pmatrix} a_{1,1} & \cdots & a_{1,m-h} \\ \vdots & \ddots & \vdots \\ a_{h,1} & \cdots & a_{h,m-h} \end{pmatrix} & \mapsto & \langle \ldots, v_i + \sum_{j=1}^{m-h} a_{i,j} v_{h+j}, \ldots \rangle_{1 \leqslant i \leqslant h} \end{array} \tag{1.8.16}$$
is an isomorphism. Show that for any other multiindex J we have an analogous isomorphisms
$$\mathbb{A}^{h(m-k)} \cong \mathscr{M}_{h,m-h}(\mathbb{K}) \xrightarrow{\sim} \mathrm{Gr}\,(h, V)_J\,.$$
2. Show that for all subsets $I, J \subset \{1, \ldots, m\}$ of cardinality h the interesection $\mathrm{Gr}\,(h, V)_I \cap \mathrm{Gr}\,(h, V)_J$ is non empty.
3. Show that the Grassmannian $\mathrm{Gr}(h, V)$ is irreducible.

Exercise 1.8.14. We recall that if $\phi\colon B \to A$ is a homomorphism of rings, and $I \subset A$, $J \subset B$ are ideals, the *contraction* $I^c \subset B$ and the *extension* $J^e \subset A$ are the ideals defined as follows:

$$I^c := \phi^{-1} I, \quad J^e := \left\{ \sum_{i=1}^{r} \lambda_i \phi(b_i) \mid \lambda_i \in A,\ b_i \in J\ \forall i = 1, \ldots, r \right\} \tag{1.8.17}$$

(In other words, J^e is the ideal of A generated by $\phi(J)$.)

Let $f\colon X \to Y$ be a regular map between affine varieties and suppose that $f^*\colon \mathbb{K}[Y] \longrightarrow \mathbb{K}[X]$ is injective.

1. Let $p \in X$. Prove that $\mathfrak{m}_p^c = \mathfrak{m}_{f(p)}$, in particular it is maximal.
2. Let $q \in Y$. Prove that
$$f^{-1}(q) = \{p \in X \mid \mathfrak{m}_p \supset \mathfrak{m}_q^e\},$$
and conclude, by the Nulstellensatz, that $f^{-1}(q)$ is not empty if and only if $\mathfrak{m}_q^e \neq \mathbb{K}[X]$.

Exercise 1.8.15. The left action of $\mathrm{GL}_n(\mathbb{K})$ on $\mathbb{A}^n$ defines a left action of $\mathrm{GL}_n(\mathbb{K})$ on $\mathbb{K}[z_1, \ldots, z_n]$ as follows. Let $\phi \in \mathbb{K}[z_1, \ldots, z_n]$ and $g \in \mathrm{GL}_n(\mathbb{K})$. Let z be the column vector with entries $z_1, \ldots, z_n$: we define $g\phi \in \mathbb{K}[z_1, \ldots, z_n]$ by letting

$$g\phi(X) := \phi(g^{-1} \cdot z).$$

Now let $G < \mathrm{GL}_n(\mathbb{K})$ be a subgroup. The *algebra of G-invariant polynomials* is

$$\mathbb{K}[z_1,\ldots,z_n]^G := \{\phi\mathbb{K}[z_1,\ldots,z_n] \in \mid g\phi = \phi \;\forall g \in G\}.$$

(it is clearly a $\mathbb{K}$-algebra). Now suppose that G is finite. One identifies $\mathbb{A}^n/G$ with an affine variety proceeding as follows.

1. Define the *Reynolds operator* as

$$\begin{array}{ccc} \mathbb{K}[z_1,\ldots,z_n] & \longrightarrow & \mathbb{K}[z_1,\ldots,z_n]^G \\ \phi & \mapsto & \frac{1}{|G|}\sum_{g\in G} g\phi. \end{array}$$

   Prove the *Reynolds identity*

$$R(\phi\psi) = \phi R(\psi) \quad \forall \phi \in \mathbb{K}[z_1,\ldots,z_n]^G.$$

2. Let $I \subset \mathbb{K}[z_1,\ldots,z_n]$ be the ideal generated by *homogeneous* $\phi \in \mathbb{K}[z_1,\ldots,z_n]^G$ of strictly positive degree (i.e. non-constant). By Hilbert's basis theorem there exists a finite basis $\{\phi_1,\ldots,\phi_d\}$ of I; we may assume that each ϕ_i is homogeneous and G-invariant. Prove that $\mathbb{K}[z_1,\ldots,z_n]^G$ is generated *as* $\mathbb{K}$*-algebra* by $\phi_1,\ldots,\phi_d$. Since $\mathbb{K}[z_1,\ldots,z_n]^G$ is an integral domain with no nilpotents it follows that there exist an affine variety X (well-defined up to isomorphism) such that $\mathbb{K}[X] \xrightarrow{\sim} \mathbb{K}[z_1,\ldots,z_n]^G$. One sets $\mathbb{A}^n/G =: X$.
3. Let $\iota\colon \mathbb{K}[z_1,\ldots,z_n]^G \hookrightarrow \mathbb{K}[z_1,\ldots,z_n]$ be the inclusion map. By Proposition 1.6.8, there exist a unique regular map

$$\mathbb{A}^n \xrightarrow{\pi} X = \mathbb{A}^n/G. \tag{1.8.18}$$

   such that $\iota = \pi^*$. Prove that

$$\pi(p) = \pi(q) \quad \text{if and only if} \quad q = gp \text{ for some } g \in G,$$

   and that π is surjective. [*Hint:* Let $J \subset \mathbb{K}[z_1,\ldots,z_n]^G$ be an ideal. Show that $J^e \cap \mathbb{K}[z_1,\ldots,z_n]^G = J$ where J^e is the extension relative to the inclusion ι.]

Exercise 1.8.16. Keep notation and hypotheses as in Exercise 1.8.15. Describe explicitly $\mathbb{A}^n/G$ and the quotient map $\pi\colon \mathbb{A}^n \to \mathbb{A}^n/G$ for the following groups $G < \mathrm{GL}_n(\mathbb{K})$:

1. $n = 2$, $G = \{\pm 1_2\}$.
2. $n = 2$, $G = \left\langle \begin{pmatrix} \omega_k & 0 \\ 0 & \omega_k^{-1} \end{pmatrix} \right\rangle$ where ω_k is a primitive k-th rooth of 1.
3. $G = \mathcal{S}_n$, the group of permutation of n elements viewed in the obvious way as a subgroup of $\mathrm{GL}_n(\mathbb{K})$ (group of permutations of coordinates).