An introduction to Algebraic Geometry - Varieties

Kieran G. O'Grady

8th 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

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

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 notice that if $f \in I$ 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 $f(z) = 0$ for every $z \in V(f_1, \ldots, f_r)$.

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 $\emptyset = V((1))$, $\mathbb{A}^n = V((0))$.

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 $\overline{\mathbb{Q}}$.

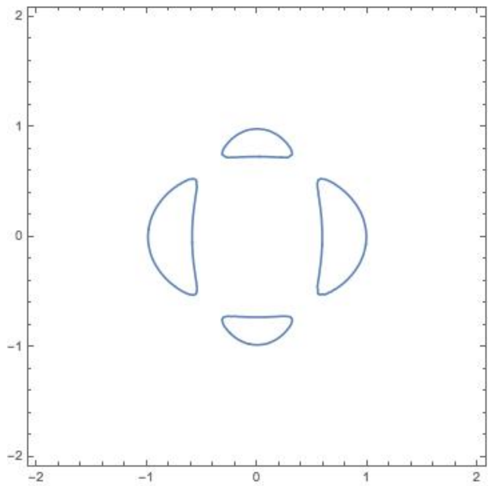

Figure 1.1: $(x^2 + 2y^2 - 1)(3x^2 + y^2 - 1) + \frac{3}{100} = 0$

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

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

Clearly $I(A)$ is an ideal of $\mathbb{K}[z_1, \ldots, z_n]$, and $V(I(A))$ is the closure of A in the Zariski topology.

Remark 1.1.5. If A is a finite dimensional affine space over $\mathbb{K}$, the Zariski topology on A may be defined by analogy with the case of $\mathbb{A}^n$, because the $\mathbb{K}$ algebra of polynomial functions on A is defined (and is ismorphic to $\mathbb{K}[z_1, \ldots, z_n]$ if n is the dimension of A). 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. From now on we identify $\mathbb{A}^n$ with the open subset $(\mathbb{P}^n \backslash V(Z_0)) \subset \mathbb{P}^n$ by mapping z to $[1, z]$. 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. $X = (\mathbb{P}^n \backslash V(Z_0)) \cap V(F_1, \ldots, F_r)$, 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 homogegenous polynomial of degree d_j and hence $V(F_1, \ldots, F_r) \subset \mathbb{P}^n$ is a closed subset. Since

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

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

$$I(A) := \langle F \in \mathbb{K}[Z_0, \ldots, Z_n] \mid F \text{ is homogeneous and } F(p) = 0 \text{ for all } p \in A\rangle, \tag{1.2.3}$$

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 $X = \emptyset$ 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 $X = \emptyset$, then $I(X) = \mathbb{K}[Z_0, \ldots, Z_n]$ and hence $I(X)$ is not prime. Thus we may assume that $X \neq \emptyset$, 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 $V(I) = \emptyset$ 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 $I = (1)$. $\square$

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 $f \in \sqrt{I}$. $\square$

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

Definition 1.5.1. Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be quasi projective varieties. A map $f\colon X \to Y$ is *regular at* $a \in X$ if there exist an open $U \subset X$ containing a and $F_0, \ldots, F_m \in \mathbb{K}[Z_0, \ldots, Z_n]_d$ such that for all $[Z] \in U$ $(F_0(Z), \ldots, F_m(Z)) \neq (0, \ldots, 0)$, and

$$f([Z]) = [F_0(Z), \ldots, F_m(Z)]. \tag{1.5.1}$$

The map f is *regular* if it is regular at each point of X.

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

Example 1.5.2. Let $X \subset \mathbb{A}^n$ be a locally closed subset (recall that $\mathbb{A}^n = \mathbb{P}^n_{Z_0}$). Then $f\colon X \to \mathbb{P}^m$ 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

$$f(z) = [f_0(z), \ldots, f_m(z)]. \tag{1.5.2}$$

(This includes the statement that $V(f_1, \ldots, f_m) \cap U = \emptyset$.) In fact, if f is regular there exist homogeneous $F_0, \ldots, F_m \in \mathbb{K}[Z_0, \ldots, Z_n]_d$ such that $f([1, z]) = [F_0(1, z), \ldots, F_m(1, z)]$, and it suffices to let $f_j(z) := F_j(1, z)$. Conversley, if (1.5.2) holds, then

$$f([Z_0, Z_1, \ldots, Z_n]) = [Z_0^d, Z_0^d f_1\left(\frac{Z_1}{Z_0}, \ldots, \frac{Z_n}{Z_0}\right), \ldots, Z_0^d f_m\left(\frac{Z_1}{Z_0}, \ldots, \frac{Z_n}{Z_0}\right)], \tag{1.5.3}$$

and for d is large enough, each of the rational functions appearing in (1.5.3) is actually a homogeneous polynomial of degree d.

Example 1.5.3. Let $X \subset \mathbb{A}^n$ be a locally closed subset and let $f\colon X \to \mathbb{P}^m$ be a map such that $f(X) \subset \mathbb{P}^m_{T_0}$ (we let $[T_0, \ldots, T_m]$ be homogeneous coordinates on $\mathbb{P}^m$). Then f 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, in affine coordinates $(\frac{T_1}{T_0}, \ldots, \frac{T_m}{T_0})$, we have

$$f(z) = \left(\frac{f_1(z)}{f_0(z)}, \ldots, \frac{f_m(z)}{f_0(z)}\right). \tag{1.5.4}$$

Example 1.5.4. Let $f \in \mathbb{K}[z_1, \ldots, z_n]$. Let $Y := V(f(z_1, \ldots, z_n) \cdot z_{n+1} - 1) \subset \mathbb{A}^{n+1}$. The map

$$\begin{array}{ccc} \mathbb{A}^n \backslash V(f) & \longrightarrow & Y \\ (z_1, \ldots, z_n) & \mapsto & (z_1, \ldots, z_n, \frac{1}{f(z_1, \ldots, z_n)}) \end{array}$$

is an isomorphism.

Example 1.5.5. Let

$$\mathcal{C}_n = \left\{[\xi_0, \ldots, \xi_n] \in \mathbb{P}^n \mid \operatorname{rk}\begin{pmatrix} \xi_0 & \xi_1 & \cdots & \xi_{n-1} \\ \xi_1 & \xi_2 & \cdots & \xi_n \end{pmatrix} \leqslant 1\right\}. \tag{1.5.5}$$

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

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\varphi_n} & \mathcal{C}_n \\ [s, t] & \mapsto & [s^n, s^{n-1}t, \ldots, t^n] \end{array} \tag{1.5.6}$$

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

$$\psi_n([\xi_0, \ldots, \xi_n]) = \begin{cases} [\xi_0, \xi_1] & \text{if } [\xi_0, \ldots, \xi_n] \in \mathcal{C}_n \cap \mathbb{P}^n_{\xi_0} \\ [\xi_{n-1}, \xi_n] & \text{if } [\xi_0, \ldots, \xi_n] \in \mathcal{C}_n \cap \mathbb{P}^n_{\xi_n} \end{cases}$$

Of course one has to check that the two expressions coincide for points in $\mathbb{K}_n \cap \mathbb{P}^n_{\xi_0} \cap \mathbb{P}^n_{\xi_n}$: from (1.5.5) we get that $\xi_0 \cdot \xi_n - \xi_1 \xi_{n-1}$ vanishes on $\mathbb{K}_n$ and this shows the required compatibility. One checks easily that $\psi_d \circ \varphi_n = \mathrm{Id}_{\mathbb{P}^1}$ and $\varphi_n \circ \psi_n = \mathrm{Id}_{\mathbb{K}_n}$; thus φ_n defines an isomorphism $\mathbb{P}^1 \xrightarrow{\sim} \mathbb{K}_n$.

Unless we are in the trivial case $n = 1$, it is *not* possible to define ψ_n *globally* as

$$\psi_n([\xi_0, \ldots, \xi_n]) = [P(\xi_0, \ldots, \xi_n), Q(\xi_0, \ldots, \xi_n)], \tag{1.5.7}$$

with $P, Q \in \mathbb{K}[\xi_0, \ldots, \xi_n]_e$ not vanishing simultaneously on $\mathbb{K}_n$. In fact suppose that (1.5.7) holds, and let

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

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), and forall $[s, t] \in \mathbb{P}^1$ we have $[p(s, t), q(s, t)] = [s, t]$. 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, i.e. $r(s, t)$ is constant. In particular $de = \deg p = \deg q = 1$, and hence $d = 1$.

Example 1.5.6. We recall the formula

$$\dim \mathbb{K}[Z_0,\dots,Z_n]_d = \binom{d+n}{n}. \tag{1.5.8}$$

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

$$\begin{array}{ccc} \mathbb{P}^n & \xrightarrow{\nu_d^n} & \mathbb{P}^{N(n;d)} \\ [Z] & \mapsto & [Z_0^d, Z_0^{d-1}Z_1, \dots, Z_n^d] \end{array} \tag{1.5.9}$$

be defined by all homogeneous monomials of degree d - this is a *Veronese map*. Clearly ν_d^n is regular.

The homogeneous coordinates on $\mathbb{P}^{N(n;d)}$ appearing in (1.5.9) are indiced by length $n+1$ multiindices $I = (i_0,\dots,i_n)$ such that $\deg I := i_0 + \dots + i_n = d$; we denote them by $[\dots,\xi_I,\dots]$. Let $\mathscr{V}_d^n \subset \mathbb{P}^{N(n;d)}$ be the closed subset defined by

$$\mathscr{V}_d^n := V(\dots,\xi_I \cdot \xi_J - \xi_K \cdot \xi_L,\dots),$$

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

Given a length $n+1$ multiindex H of degree $d-1$, we let $H_s := H + e_s$, where, for $e_0,\dots,e_n$ is the standard basis of $\mathbb{Z}^n$, i.e. e_s has alla entries equal to 0, except for the entry at place $s+1$, which is equal to 1. For $s \in \{0,\dots,n\}$, let

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

Let H, H' be length $n+1$ multiindices of degree $d-1$. It follows from the equations defining $\mathscr{V}_d^n$ that $\varphi_d^n(H)([z]) = \varphi_d^n(H')([z])$ for all $[Z]$ which is in the domain of $\varphi_d^n(H)$ and $\varphi_d^n(H')$. Thus the $\varphi_d^n(H)$'s define a regular map $\varphi_d^n \colon \mathscr{V}_d^n \to \mathbb{P}^n$. We claim that

$$\varphi_d^n \circ \nu_d^n = \mathrm{Id}_{\mathbb{P}^n} \tag{1.5.10}$$

$$\nu_d^n \circ \varphi_d^n = \mathrm{Id}_{\mathbb{P}^{N(n;d)}}. \tag{1.5.11}$$

The first equality is easily checked. In order to check the second equality, one may proceed as follows. Let $[\xi] = [\dots,\xi_I,\dots] \in \mathscr{V}_d^n$ be a point such that $\xi_{de_s} \neq 0$ for some $s \in \{0,\dots,n\}$. Then it is not difficult to show that there exists $[Z] \in \mathbb{P}^n$ such that $[\xi] = \nu_d^n([z])$. By (1.5.10), it follows that $\nu_d^n \circ \varphi_d^n([\xi]) = [\xi]$. Hence it suffices to prove that if $[\xi] \in \mathscr{V}_d^n$, then there exists $s \in \{0,\dots,n\}$ such that $\xi_{de_s} \neq 0$. Thus, we must show that if $\dots,\xi_I,\dots$ are such that $\xi_I \cdot \xi_J = \xi_K \cdot \xi_L$ whenever $I + J = K + L$, and $\xi_{de_s} = 0$ for all $s \in \{0,\dots,n\}$, then $\xi_I = 0$ for all multiindices I. This is easily proved by "descending induction" on the maximum of $i_0,\dots,i_n$, by using a suitable relation $\xi_I^2 = \xi_K \cdot \xi_L$ (if the maximum is d, then $\xi_I = 0$ by hypothesis).

Example 1.5.7. Assume that $\operatorname{char}\mathbb{K} = p > 0$. Let $X = V(G_1,\dots,G_r) \subset \mathbb{P}^n$ be a closed subset defined by homogeneous $G_1,\dots,G_r \in \mathbb{F}_p[Z_0,\dots,Z_n]$ (we require that the coefficients of the G_i's belong to the prime field $\mathbb{F}_p$). Then we may define the *Frobenius map* : $X \to X$ by setting

$$\begin{array}{ccc} X & \xrightarrow{F} & X \\ [Z] & \mapsto & [Z_0^p,\dots,Z_i^p,\dots,Z_n^p]. \end{array}$$

In fact, if $G_i = \sum_I a_J Z^J$, then

$$G_i(Z_0^p,\dots,Z_i^p,\dots,Z_n^p) = \sum_I a_J (Z^J)^p = \sum_I a_J^p (Z^J)^p = G_i(Z_0,\dots,Z_i,\dots,Z_n)^p = 0.$$

More generally, if all the coefficients of the G_i's are contained in $\mathbb{F}_{p^r}$ (e.g. if $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_p$), then we may define $F \colon X \to X$ replacing the exponent p by p^r. Notice that F is bijective, but it is not an isomorphism.

Proposition 1.5.8. *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

$$\overline{C}_\alpha \cap U_\alpha = C_\alpha = \phi^{-1}C \cap U_\alpha. \tag{1.5.12}$$

Moreover D_α is closed in X because U_α is open. By (1.5.12) 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. □

The following lemma will be useful later on. The easy proof is left to the reader.

Lemma 1.5.9. *Let $f\colon X \to Y$ be a map between quasi projective varieties. Suppose that $Y = \bigcup_{i \in I} U_i$ is an open cover, that $f^{-1}U_i$ is open in X for each $i \in I$ and that the restriction*

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

is regular for each $i \in I$. Then f is regular.

Definition 1.5.10. A quasi projective variety is

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

We will give some remarkable examples of locally closed subsets of a projective space which are affine varieties. First a definition.

Definition 1.5.11. 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 1.5.12. *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 $\nu^n_d\colon \mathbb{P}^n \longrightarrow \mathbb{P}^{N(n,d)}$, see (1.5.9). Let $\mathscr{V}^n_d := \operatorname{Im} \nu^n_d$ be the corresponding Veronese variety. As shown in Example 1.5.6 the map $\mathbb{P}^n \to \mathscr{V}^n_d$ defined by ν^n_d is an isomorphism. It follows that the restriction of ν^n_d to $\mathbb{P}^n_F$ defines an isomorphism between $\mathbb{P}^n_F$ and $\mathscr{V}^n_d \backslash H$, where $H \subset \mathbb{P}^{N(n,d)}$ is a suitable hyperplane section (if $F = \sum_I a_I Z^I$ then $H = V(\sum_I a_I \xi_I)$. Equivalently, $\mathbb{P}^n_F$ is isomorphic to the intersection of the affine space $\mathbb{P}^{N(n,d)} \backslash H$ and the closed set $\mathscr{V}^n_d$, and hence is an affine variety.

In general, let $X \subset \mathbb{P}^n$ be closed, and let F be as above. Since ν^n_d is an isomorphism $\nu^n_d(X_F)$ is closed in the affine variety $\mathscr{V}^n_d \backslash H$, and hence is itself affine. Moreover, the restriction of ν^n_d to X_F defines an isomorphism between X_F and the affine variety $\nu^n_d(X_F)$. □

The result below is a remarkable consequence of Claim 1.5.12.

Proposition 1.5.13. *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 is the emptyset, it is clearly affine, hence we may assume that $U = X \backslash W$, where $W \subsetneq X$ is closed. Let $W = V(I)$, where $I \subset \mathbb{K}[Z_0, \ldots, Z_n]$ is a homogeneous ideal, not the zero ideal because $W \neq X$. Let $J \subset \mathbb{K}[Z_0, \ldots, Z_n]$ be the homogeneous ideal generated by all products $F \cdot Z_i$, where $F \in I$, and $i \in \{0, \ldots, n\}$. Then $V(J) = V(I) = W$, and J is generated by a non empty finite set of non costant homogeneous polynomials $F_1, \ldots, F_r$. Then

$$U = X \backslash V(F_1, \ldots, F_r) = X_{F_1} \cup X_{F_2} \cup \ldots \cup X_{F_r}.$$

□

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* (1.6.1) *is an equality, i.e. every regular function on X is the restriction of a polynomial function on $\mathbb{A}^n$.*

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 $V(J) = \emptyset$ if and only if $J = (1)$.

The following example makes it clear that Proposition 1.6.3 must play a rôle in the proof of Theorem 1.6.2. 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 $g^{-1} = f_{|X}$. By Proposition 1.6.3, $(g) = (1)$ in $\mathbb{K}[z_1, \ldots, z_n]/I(X)$, because $V(\overline{g}) = \emptyset$, where $\overline{g} := g_{|X}$. hence there exists $f \in \mathbb{K}[z_1, \ldots, z_n]$ such that $\overline{f} \cdot \overline{g} = 1$, where $\overline{f} := f_{|X}$, i.e. $g^{-1} = f_{|X}$

Proof of Theorem 1.6.2. Let $\varphi \in \mathbb{K}[X]$. We claim that there exist $f_i, g_i \in \mathbb{K}[z_1, \ldots, z_n]$ for $1 \leqslant i \leqslant d$ such that

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

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 $(g_j f_i - g_i f_j)|_X = 0$.

(Notice: the last item implies that on $X_{g_i} \cap X_{g_j}$ we have $f_i/g_i = f_j/g_j$.) For $i = 1, \ldots, d$ let $\overline{g}_i := g_{i|X}$ and $\overline{f}_i := f_{i|X}$. Then

$$\overline{g}_i \varphi = \overline{f}_i. \tag{1.6.2}$$

In fact by Item (1) it suffices to check that (1.6.2) holds on X_{f_j} for $j = 1, \ldots, d$. For $j = i$ it holds by Item (2), for $j \neq i$ it holds by Item (3). (Notice: if we do not assume that Item (3) holds we only know that (1.6.2) holds on $U_j \cap U_i$.) 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 and remembering (1.6.2) we get that

$$\varphi = \overline{h}_1 \overline{g}_1 \varphi + \cdots + \overline{h}_d \overline{g}_d \varphi = \overline{h}_1 \overline{f}_1 + \ldots + \overline{h}_1 \overline{f}_d = (h_1 f_1 + \cdots + h_d f_d)_{|X}. \tag{1.6.3}$$

It remains to prove that there exist $f_i, g_i \in \mathbb{K}[z_1, \ldots, z_n]$ with the properties stated above. By definition of regular function there exist an open covering of X, and for each set U of the open cover a couple $\alpha, \beta \in \mathbb{K}[z_1, \ldots, z_n]$ such that $\varphi(x) = \alpha(x)/\beta(x)$ for all $x \in U$ (it is understood that $\beta(x) \neq 0$ for all $x \in U$). By Remark 1.6.4 we may cover U by open affine sets $X_{\gamma_1}, \ldots, X_{\gamma_r}$. Since $V(\beta) \subset \bigcap_{i=1}^{r} V(\gamma_i)$ the Nullstellensatz gives that, for each i, there exist $N_i > 0$ and $\mu_i \in \mathbb{K}[z_1, \ldots, z_n]$ such that $\gamma_i^{N_i} = \mu_i \beta$ and hence $\varphi(x) = \mu_i(x)\alpha(x)/\gamma_i(x)^N$ for all $x \in X_{\gamma_i}$. Since $X_{\gamma_i} = X_{\gamma_i^N}$ we get that we have covered X by principal open sets $X_{g'}$ such that $\varphi = f'/g'$ for all $x \in X_{g'}$, where $f' \in \mathbb{K}[z_1, \ldots, z_n]$ (of course f' depends on g'). By Corollary 1.3.9, the open covering has a finite subcovering, corresponding to $f_1', g_1', \ldots, f_d', g_d'$. Now 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 $\varphi(z) = f_i'(z)/g_i'(z) = f_j'(z)/g_j'(z)$ for all $z \in X_{g_i'} \cap X_{g_j'}$ the last term vanishes on $X_{g_i'} \cap X_{g_j'}$, on the other hand it vanishes also on $(X \backslash X_{g_i'} \cap X_{g_j'}) = X \cap V(g_i' g_j')$ because of the factor $(g_i' g_j')$. □

We end the present section with a couple of consequences of Theorem 1.6.2.

First we give a more explicit version of Proposition 1.5.13 in the case that the quasi projective variety itself is affine. Given a quasi projective variety X, and $f \in \mathbb{K}[X]$, let

$$X_f := X \backslash V(f), \tag{1.6.4}$$

where $V(f) := \{x \in X \mid f(x) = 0\}$. The following remark is easily verified.

Remark 1.6.4. Let $X \subset \mathbb{A}^n$ be closed (and hence an affine variety). Let $f \in \mathbb{K}[X]$, and hence by Theorem 1.6.2 there exists $\tilde{f} \in \mathbb{K}[z_1, \ldots, z_n]$ such that $\tilde{f}_{|X} = f$. Let $Y \subset \mathbb{A}^{n+1}$ be the subset of solutions of $g(z_1, \ldots, z_n) = 0$ for all $g \in I(X)$, and the extra equation $f(z_1, \ldots, z_n) \cdot z_{n+1} - 1 = 0$. Then the map

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

is an isomorphism. In particular X_f is an open affine subset of X. Moreover, the open affine subset X_f, for $f \in \mathbb{K}[X]$ form a basis for the Zariski topology of X.

Notice that, by Theorem 1.6.2 and the above isomorphism, every regular function on X_f is given by the restriction to X_f of $\frac{g}{f^m}$, where $g \in \mathbb{K}[X]$ and $m \in \mathbb{N}$.

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

Proposition 1.6.5. *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, consider a regular map $f\colon X \to Y$ of (non empty) quasi projective varieties. The pull-back $f^*\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ is the homomorphism of $\mathbb{K}$-algebras defined by $f^*(\varphi) := \varphi \circ f$.

Proposition 1.6.6. *Let Y be an affine variety, and let X be a quasi projective variety. The map*

$$\begin{array}{ccc} \{f\colon X \to Y \mid f \text{ regular}\} & \longrightarrow & \{\varphi\colon \mathbb{K}[Y] \to \mathbb{K}[X] \mid \varphi \text{ homomorphism of } \mathbb{K}\text{-algebras}\} \\ f & \mapsto & f^* \end{array} \tag{1.6.5}$$

is a bijection.

Proof. We may assume that $Y \subset \mathbb{A}^n$ is closed; let $\iota\colon Y \hookrightarrow \mathbb{A}^n$ be the inclusion map. Suppose that $f, g\colon X \to Y$ are regular maps, and that $f^* = g^*$. Then $f^*(\iota^*(z_i)) = g^*(\iota^*(z_i))$ for $i \in \{1, \ldots, n\}$, and hence $f = g$. This proves injectivity of the map in (1.6.5). In order to prove surjectivity, let $\varphi\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ be a homomorphism of $\mathbb{K}$ algebras. Let $f_i := \varphi(\iota^*(z_i))$, and let $f\colon X \to \mathbb{A}^n$ be the regular map defined by $f(x) := (f_1(x), \ldots, f_n(x))$ for $x \in X$. Then $f(x) \in Y$ for all $x \in X$. In fact, since Y is closed, it suffices to show that $g(f(x)) = 0$ for all $g \in I(X)$. Now

$$g(f_1(x), \ldots, f_n(x)) = g(\varphi(\iota^*(z_1)), \ldots, \varphi(\iota^*(z_n)) = \varphi(g(\iota^*(z_1)), \ldots, \iota^*(z_n)) = \varphi(0) = 0.$$

(The second and last equality hold because φ is a homomorphism of $\mathbb{K}$-algebras.) Thus f is a regular map $f\colon X \to Y$ such that $f^*(\iota^*(z_i)) = \varphi(\iota^*(z_i))$ for $i \in \{1, \ldots, n\}$. By Theorem 1.6.2 the $\mathbb{K}$-algebra $\mathbb{K}[Y]$ is generated by $\iota^*(z_1), \ldots, \iota^*(z_n)$; it follows that $f^* = \varphi$. □

Corollary 1.6.7. *In Proposition 1.6.5, 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 $\mathbb{K}$

1.8 Exercises

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

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

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

(c) $W \coloneqq \left\{\left(\dfrac{2t}{t^2+1}, \dfrac{t^2-1}{t^2+1}\right) \mid t \in \mathbb{C}\setminus\left\{\pm\sqrt{-1}\right\}\right\} \subset \mathbb{A}^2(\mathbb{C})$.

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

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 $Z \subset \mathbb{A}^2_{\mathbb{C}}$ be a proper closed irreducible subset. Show that Z is either a singleton or an irreducible hypersurface.

Exercise 1.8.6. 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

$$\begin{array}{ccc} R[X,Y]_{n-1} \oplus R[X,Y]_{m-1} & \xrightarrow{L(F,G)} & R[X,Y]_{m+n-1} \\ (\Phi, \Psi) & \mapsto & \Phi \cdot F + \Psi \cdot G \end{array} \tag{1.8.1}$$

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

$$(X^{n-1}, 0),\ (X^{n-2}Y, 0),\ \ldots\ ,\ (Y^{n-1}, 0),\ (0, X^{m-1}),\ (0, X^{m-2}Y),\ \ \ldots\ ,\ (0, Y^{m-1}) \tag{1.8.2}$$

of the domain and the basis

$$X^{m+n-1},\ X^{m+n-2}Y,\ \ldots\ ,\ XY^{m+n-2},\ Y^{m+n-1} \tag{1.8.3}$$

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

$$\mathscr{R}(F, G) := \det S(F, G). \tag{1.8.4}$$

Explicitly: if

$$F = \sum_{i=0}^{m} a_i X^{m-i} Y^i, \quad G = \sum_{j=0}^{n} b_j X^{n-j} Y^j \tag{1.8.5}$$

then

$$\mathscr{R}(F, G) = \det \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \cdots & a_0 & \vdots & \vdots & \cdots & b_0 \\ a_m & a_{m-1} & \cdots & \vdots & b_n & b_{n-1} & \cdots & \vdots \\ 0 & a_m & \cdots & \vdots & 0 & b_n & \cdots & \vdots \\ 0 & 0 & \cdots & \vdots & 0 & 0 & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a_m & 0 & 0 & \cdots & b_n \end{pmatrix}. \tag{1.8.6}$$

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

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

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

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

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

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

The goal of the present exercise is to identify (in a reasonable way) the elements of $\mathrm{Gr}\,(h,V)$ 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

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

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 $\mathrm{Im}\,\mathscr{P}$ is a closed subset of $\mathbb{P}\left(\bigwedge^h V\right)$. Thus we have identified $\mathrm{Gr}\,(h,V)$ with a projective variety.

Note that we have a bijection

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

Thus we may also identify $\mathrm{Gr}\,(k,\mathbb{P}(V))$ 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 1.8.8. 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
$$\mathrm{Gr}(h, V) = \bigcup_{|I|=h} \mathrm{Gr}(h, V)_I, \tag{1.8.7}$$
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
$$\begin{array}{ccc} \mathscr{M}_{h,m-h}(\mathbb{K}) & \longrightarrow & \mathrm{Gr}(h, V)_I \\ \begin{pmatrix} a_{1,1} & \cdots & a_{1,m-h} \\ \vdots & \ddots & \vdots \\ a_{h,1} & \cdots & a_{h,m-h} \end{pmatrix} & \mapsto & \langle \ldots, v_i + \sum_{j=1}^{m-h} a_{i,j} v_{h+j}, \ldots \rangle_{1 \leqslant i \leqslant h} \end{array} \tag{1.8.8}$$
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 1.8.9. 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 (1.5.8) 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 1.5.6, *valid if* $\mathrm{char}\, \mathbb{K} = 0$, *or more generally* $\mathrm{char}\, \mathbb{K}$ *does not divide* $d!$. Let

$$\begin{array}{ccc} \mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_1) & \xrightarrow{\mu_d^n} & \mathbb{P}(\mathbb{K}[T_0, \ldots, T_n]_d) \\ [L] & \mapsto & [L^d] \end{array} \tag{1.8.9}$$

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

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

where $T^I = T_0^{i_0} \cdot \ldots \cdot T_n^{i_n}$. By Newton's formula $(\sum_{i=0}^n \alpha_i T_i)^d = \sum\limits_I \frac{d!}{i_0! \cdot \ldots \cdot i_n!} \alpha^I T^I$, 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*

$$\sum_{j=0}^{n} Z_j \frac{\partial F}{\partial Z_j} = (\deg F) \cdot F, \tag{1.8.10}$$

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

$$\theta_d^n([F]) := \begin{cases} [\frac{\partial^{n-1} F}{\partial Z_0^{n-1}}] & \text{if } \frac{\partial^{n-1} F}{\partial Z_0^{n-1}} \neq 0, \\ \cdots\cdots & \cdots\cdots \\ [\frac{\partial^{n-1} F}{\partial Z_n^{n-1}}] & \text{if } \frac{\partial^{n-1} F}{\partial Z_n^{n-1}} \neq 0. \end{cases} \tag{1.8.11}$$

Exercise 1.8.11. 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:

$$I^c := \phi^{-1} I, \quad J^e := \left\{ \sum_{i=1}^{r} \lambda_i \phi(b_i) \mid \lambda_i \in A,\ b_i \in J\ \forall i = 1, \ldots, r \right\} \tag{1.8.12}$$

(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
$$f^{-1}(q) = \left\{ p \in X \mid \mathfrak{m}_p \supset \mathfrak{m}_q^e \right\},$$
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 1.8.12. 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 1.6.6, there exist a unique regular map
$$\mathbb{A}^n \xrightarrow{\pi} X = \mathbb{A}^n/G. \tag{1.8.13}$$
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 1.8.13. Keep notation and hypotheses as in Exercise 1.8.12. 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).