A Curvy Introduction to Algebraic Geometry

Jeroen Sijsling

June 11, 2022

This is an incomplete version of the notes for the course *Einführung in die algebraische Geometrie* in the summer term 2022 at Ulm University. Remarks and criticism are highly welcome at jeroen.sijsling@uni-ulm.de.

Many thanks are due to Tim Evink, who provided copious corrections and important improvements to earlier versions of these notes.

Contents

Chapter 1

Syntax

What does it mean to "do geometry"? That is, what is the activity γεωμετρεῖν that Plotinus claims, at one further remove from the source, to be the activity that Plato describes as the everlasting occupancy of God? This is clearly a rather heady question. The modern answer is that there are many geometries, and that their most general form is that of a topological space X proved with an extra structure, namely the functions on the open subsets of X. Part of modern mathematics is that there are many ways to obtain such functions; one can think of smooth functions, but also of continuous functions, rational functions, and of much stranger and more abstract structures.
In all cases, the common notion that describes the structure of the provided functions on X is that of the structure sheaf $\mathscr{O}_X$ on X. In this chapter, we explain what a sheaf is, and use this concept to define locally ringed spaces. To develop the required formalism, we also indulge in some category theory, which is useful in many contexts.

1.1 Categories and universal constructions

Category theory is a kind of mathematical grammar. While it does not always contain deep mathematical results in itself, it helps to think of the structure underlying a given problem, and with it, to guide our minds in the right direction. Moreover, it shows the ubiquity of certain mathematical concepts and constructions, which allows for fruitful analogies and interactions between a priori disparate branches of mathematics.

It is easy to get lost in category theory. It is also very tempting and a lot of fun. There is a vast ocean of it, but for this course, we will only use category theory to express concisely what geometries and spaces are. Our categories serve a purpose, and we do not study them for their own sake. We see it more like one of Molière's bourgeois gentleman sees prose:

> Par ma foi ! il y a plus de quarante ans que je dis de la prose sans que j'en susse rien, et je vous suis le plus obligé du monde de m'avoir appris cela.

The main idea underlying category theory is that mathematics is best thought of as being not about about sets and the maps between them, but about structures called categories and the functors between them. Here is the formal definition.

Definition 1.1.1. A category $\mathcal{C}$ is given by the following data:

(i) a collection (set or class) $\mathrm{Obj}(\mathcal{C})$ of objects of $\mathcal{C}$;

(ii) for all X, Y in $\mathrm{Obj}(\mathcal{C})$, a collection $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ of morphisms (or arrows) from X to Y;

(iii) for all X, Y, Z in $\mathrm{Obj}(\mathcal{C})$, a composition map

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(X,Y) \times \mathrm{Hom}_{\mathcal{C}}(Y,Z) &\to \mathrm{Hom}_{\mathcal{C}}(X,Z) \\ (f,g) &\mapsto g \circ f \end{aligned} \tag{1.1.2}$$

We demand that the following properties be satisfied:

(C1) for all X there exists a morphism $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X,X)$ such that both $f \circ \mathrm{id}_X = f$ for all $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ and $\mathrm{id}_X \circ g = g$ for all $g \in \mathrm{Hom}_{\mathcal{C}}(Y,X)$.

(C2) for all f, g, h we have $h \circ (g \circ f) = (h \circ g) \circ f$ when these compositions make sense.

Definition 1.1.3. Let $\mathcal{C}$ be a category. Then a subcategory $\mathcal{D}$ of $\mathcal{C}$ is given by the following data:

(i) A subcollection $\mathrm{Obj}(\mathcal{D})$ of $\mathrm{Obj}(\mathcal{C})$;

(ii) For all X, Y in $\mathrm{Obj}(\mathcal{D})$, a subcollection $\mathrm{Hom}_{\mathcal{D}}(X,Y)$ of $\mathrm{Hom}_{\mathcal{C}}(X,Y)$.

We demand that the following properties be satisfied:

(SC1) for all $X \in \mathrm{Obj}(\mathcal{D})$ we have $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{D}}(X,X)$;

(SC2) if $X, Y, Z \in \mathrm{Obj}(\mathcal{D})$, then if $f \in \mathrm{Hom}_{\mathcal{D}}(X,Y)$ and $g \in \mathrm{Hom}_{\mathcal{D}}(Y,Z)$ we have $g \circ f \in \mathrm{Hom}_{\mathcal{D}}(X,Z)$.

A few important examples of categories are the following:

Example 1.1.4. (i) $\mathfrak{Set}$, the category with as objects all sets and with as morphisms the usual maps of sets.

(ii) $\mathfrak{Gp}$, the category with as objects all groups and with group homomorphisms as morphisms. It has the category $\mathfrak{Ab}$ of abelian groups as a subcategory.

(iii) $\mathfrak{Rng}$, the category with as objects all (unital) commutative rings and with ring homomorphisms as morphisms. It has the category $\mathfrak{Fld}$ of fields as a subcategory.

(iv) Given a field k, we can consider the category $\mathfrak{Vec}_k$ whose objects are vector spaces over k and whose morphisms are homomorphisms of vector spaces over k. It has the category $\mathfrak{FinVec}_k$ of finite-dimensional vector spaces over k as a subcategory.

(v) Given a field k, we can consider the category k-$\mathfrak{Alg}$ whose objects are k-algebras over k (that is, rings with a structure of vector space over k) and whose morphisms are ring homomorphisms that are also homomorphisms of vector spaces.

(vi) Given a commutative ring R, we can consider the category $\mathfrak{Mod}_R$ of left R-modules. Note that both $\mathfrak{Vec}_k$ and $\mathfrak{Ab}$ are instances of such a category, for $R = k$ and $R = \mathbb{Z}$ respectively.

It is the *arrows* that are the essence and life blood of category theory. A first categorical definition involving arrows, which you will already have encountered in many contexts, is the following.

Definition 1.1.5. Let $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$. Then f is called an isomorphism if there exists a $g \in \mathrm{Hom}_{\mathcal{C}}(Y,X)$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$.

Notation 1.1.6. Given X and Y in $\mathcal{C}$, the set of isomorphisms from X to Y is denoted by $\mathrm{Isom}(X,Y)$. We let $\mathrm{End}(X) = \mathrm{Hom}_{\mathcal{C}}(X,X)$ be the set of endomorphisms of X, and we let $\mathrm{Aut}(X) = \mathrm{Isom}(X,X)$ be the set of automorphisms of X.

Example 1.1.7. Let $X = \mathbb{Q}$ and let $Y = \mathbb{Q}^2$. Then we can consider X and Y both as objects of $\mathfrak{Set}$ and as objects of $\mathfrak{FinVec}_{\mathbb{Q}}$ in a natural way. In $\mathfrak{Set}$, the corresponding objects are isomorphic (why?), but in $\mathfrak{FinVec}_{\mathbb{Q}}$ they are not (why not?).

Often we will denote a composition $f \circ g$ of morphisms in a category by fg instead.

Universal constructions

Many important constructions in categories can be phrased without reference to elements, by means of so-called universal properties. An example of this is the following.

Definition 1.1.8. Let $\mathcal{C}$ be a category and let $X, Y \in \mathrm{Obj}(\mathcal{C})$. A product of X and Y is a triple (P, p_X, p_Y), where $P \in \mathrm{Obj}(\mathcal{C})$ and where $p_X : P \to X$ and $p_Y : P \to Y$ are morphisms, with the following property: given a triple $(Z, f_X : Z \to X, f_Y : Z \to Y)$, there exists a unique morphism $g : Z \to P$ such that $f_X = p_X g$ and $f_Y = p_Y g$. In a diagram:

$$\begin{tikzcd} & & X \\ Z \arrow[r, dashed, "g!"] \arrow[urr, bend left, "f_X"] \arrow[drr, bend right, "f_Y"'] & P \arrow[ur, "p_X"] \arrow[dr, "p_Y"'] & \\ & & Y \end{tikzcd} \tag{1.1.9}$$

Remark 1.1.10. We do not demand that the triple (P, p_X, p_Y) be unique. However, using its defining properties, you will show in the exercises that it is unique up to unique isomorphism, in the sense that if (P', p'_X, p'_Y) is another such triple, then there exists a unique isomorphism $f : P \to P'$ such that $p'_X = p_X f$ and $p'_Y = p_Y f$.

Because of this uniqueness up to unique isomorphism, we can still in good conscience speak of *the* product of X and Y, just like we speak of *the* group with two elements although there are infinitely many such groups sensu stricto. We denote this product by $(X \times Y, \pi_X, \pi_Y)$.

Example 1.1.11. (i) In $\mathfrak{Set}$, the product of two sets X and Y is the usual product of X and Y together with the projection morphisms sending (x,y) to x and y respectively.

(ii) In $\mathfrak{Ab}$ and $\mathfrak{Gp}$, the product of two objects X and Y is constructed in the same way; we consider $X \times Y$ as a group in the usual way.

An endless source of amusement in category theory is to reverse arrows. This makes products into so-called coproducts, which we will consider next. It also turns kernels into cokernels and mathematicians, who turn coffee into theorems, into comathematicians, who turn cotheorems into ffee.

Definition 1.1.12. Let $\mathcal{C}$ be a category, and let $X, Y \in \mathrm{Obj}(\mathcal{C})$. A coproduct of X and Y is a triple (C, i_X, i_Y), where $C \in \mathrm{Obj}(\mathcal{C})$ and where $i_X : X \to C$ and $i_Y : Y \to C$ are morphisms, with the following property: given a triple $(Z, f_X : X \to Z, f_Y : Y \to Z)$ there exists a unique morphism $g : C \to Z$ such that $f_X = g i_X$ and $f_Y = g i_Y$. In a diagram:

$$\begin{tikzcd}
X \arrow[dr, "i_X"'] \arrow[drr, bend left, "f_X"] & & \\
& C \arrow[r, dashed, "g!"] & Z \\
Y \arrow[ur, "i_Y"] \arrow[urr, bend right, "f_Y"'] & &
\end{tikzcd} \tag{1.1.13}$$

Once again, the coproduct of X and Y is unique up to unique isomorphism. We usually denote it by $(X \coprod Y, \iota_X, \iota_Y)$. It may seem innocuous to reverse arrows in this way, but it turns out that things get completely different.

Example 1.1.14. (i) In $\mathfrak{Set}$, the coproduct of X and Y is the *disjoint* union of X and Y, together with the inclusions of X and Y into it.

(ii) In $\mathfrak{Ab}$, the coproduct of X and Y is the product $X \times Y$, together with the maps i_X and i_Y that send $x \in X$ to $(x, 0)$ and $y \in Y$ to $(0, y)$, respectively.

(iii) In $\mathfrak{Gp}$, the coproduct of X and Y is the so-called free product of X and Y. We will not discuss this complicated construction further.

As you can see, the category $\mathfrak{Ab}$ is more well-behaved than $\mathfrak{Set}$ and $\mathfrak{Gp}$, in the sense that the product and the coproduct admit the same underlying object. The category $\mathfrak{Ab}$ is a special case of a so-called abelian category, which we will soon define. First we introduce some preliminary notions.

Definition 1.1.15. Let $\mathcal{C}$ be an category. A zero object of $\mathcal{C}$ is an object 0 of $\mathcal{C}$ such that for all objects X of $\mathcal{C}$ there exists unique morphisms $0 \to X$ and $X \to 0$.

Proposition 1.1.16. *Let $\mathcal{C}$ be a category, and suppose that* 0, $0'$ *are two zero objects of $\mathcal{C}$. Then there exists a unique isomorphism* $0 \to 0'$.

If a category $\mathcal{C}$ admits a zero object, then given two objects X and Y of $\mathcal{C}$, we define the zero morphism $X \to Y$ to be the composition $X \to 0 \to Y$.

Definition 1.1.17. Let $\mathcal{C}$ be an category with a zero object, and let $f : X \to Y$ be a morphism. A kernel of f is a pair (K, i), where $K \in \mathrm{Obj}(\mathcal{C})$ and where $i : K \to X$ is a morphism such that $fi = 0$ and such that for every other pair (Z, g) with $fg = 0$, there exists a unique morphism $h : Z \to K$ such that $g = ih$. In a diagram:

$$\begin{tikzcd}
K \arrow[r, "i"] \arrow[rr, bend left, "0"] & X \arrow[r, "f"] & Y \\
Z \arrow[u, dashed, "h!"] \arrow[ur, "g"] \arrow[urr, "0"'] & &
\end{tikzcd} \tag{1.1.18}$$

Reversing arrows, we get the dual notion.

Definition 1.1.19. Let $\mathcal{C}$ be an category with a zero object, and let $f : X \to Y$ be a morphism. A cokernel of f is a pair (C, q), where $C \in \mathrm{Obj}(\mathcal{C})$ and where $q : X \to K$ is a morphism such that $qf = 0$ and such that for every other pair (Z, g) with $qf = 0$, there exists a unique morphism $h : C \to Z$ such that $g = hq$. In a diagram:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[rr, bend left, "0"] \arrow[drr, "0"'] & Y \arrow[r, "q"] \arrow[dr, "g"] & C \arrow[d, dashed, "h!"] \\ & & Z \end{tikzcd} \tag{1.1.20}$$

Once again it turns out that the kernel and the cokernel of a morphism $f : X \to Y$ are unique up to unique isomorphism if they exist; we will often simply denote them by $(\ker(f), \iota)$ and $(\operatorname{coker}(f), \pi)$.

Example 1.1.21. Let $f : X \to Y$ be a morphism in $\mathfrak{Ab}$. Then a kernel of f is given by the pair $(\ker(f), \iota)$, where ι is the natural inclusion of $\ker(f)$ into X, and a cokernel of f is given by $(Y/f(X), \pi)$, where π is the canonical projection map $Y \to Y/f(X)$.

Definition 1.1.22. Let f be a morphism in a category. Then f is called a monomorphism if an equality $fg = fh$ implies $g = h$. The dual notion is that of an epimorphism, which is a morphism for which an equality $gf = hf$ implies $g = h$.

Example 1.1.23. (i) In the category $\mathfrak{Ab}$, monomorphisms are nothing but injective maps and epimorphisms are nothing but surjective maps.

(ii) In $\mathfrak{Rng}$, the morphism $\mathbb{Z} \to \mathbb{Q}$ is an epimorphism, though it is not surjective.

The nice thing about these definitions is that they do not refer to elements of X and Y in any way. Indeed, one of the great virtues of category theory is that it completely dispenses with using elements, even though the objects of many categories that one encounters in practice do have elements. The underlying philosophy is that morphisms, not elements, are what gives mathematics their structure.

Definition 1.1.24. An abelian category is a category $\mathcal{C}$ with the following properties:

(i) $\mathcal{C}$ admits a zero object;

(ii) for any two objects X and Y of $\mathcal{C}$, there exists both a product $(X \times Y, \pi_X, \pi_Y)$ and a coproduct $(X \coprod Y, \iota_X, \iota_Y)$;

(iii) for any morphisms $f : X \to Y$, there exists both a kernel $(\ker(f), \iota)$ and a cokernel $\operatorname{coker}(f), \pi)$;

(iv) any monomorphisms in $\mathcal{C}$ is the kernel of some morphism in $\mathcal{C}$, and similarly, any epimorphism in $\mathcal{C}$ is the cokernel of some morphism in $\mathcal{C}$.

Example 1.1.25. $\mathfrak{Ab}$, $\mathfrak{Vec}_K$ and $\mathfrak{Mod}_R$ are all abelian categories.

Remark 1.1.26. It turns out that for general abelian categories, the sets $\operatorname{Hom}_{\mathcal{C}}(X, Y)$ are abelian groups in a natural way. Note that this is clear in the concrete cases of the previous example.

An final important example of a category is $\mathfrak{Top}$, the category with as objects all topological spaces and with continuous maps as morphisms. We will now define it.

Definition 1.1.27. A topological space is a pair $(X, \mathcal{U}_X)$, where X is a set and where $\mathcal{U}_X$ is a set of subsets of X (called the open subsets of X for the given topology $\mathcal{U}_X$) that satisfies the following properties:

(i) We have $\emptyset \in \mathcal{U}_X$;

(ii) If $U_1, U_2 \in \mathcal{U}_X$, then $U_1 \cap U_2 \in \mathcal{U}_X$;

(iii) If I is a set, and $\{U_i\}_{i\in I}$ is a family of elements of $\mathcal{U}_X$ indexed by the elements of I, then $\cup_{i\in I} U_i \in \mathcal{U}_X$.

A morphism of topological spaces $f : (X,\mathcal{U}_X) \to (Y,\mathcal{U}_Y)$ is a map $f : X \to Y$ with the property that for all $V \in \mathcal{U}_Y$ we have $f^{-1}(V) \in \mathcal{U}_X$. We also say that f is a continuous map between the topological spaces $(X,\mathcal{U}_X)$ and $(Y,\mathcal{U}_Y)$.

It can be shown that the collection of topological spaces with continuous maps as morphisms is indeed a category.

Example 1.1.28. The set $\mathbb{R}$, provided with the set $\mathcal{U}_\mathbb{R}$ of open subsets in the sense of analysis, is a topological space. Using this topology, a map of sets $f : \mathbb{R} \to \mathbb{R}$ is a morphism of topological spaces if and only if it is continuous in the sense of analysis.

1.2 Functors and adjoints

Functors can be seen as operations or associations that preserve the structures that we encode in categories.

Definition 1.2.1. Let $\mathcal{C}, \mathcal{D}$ be two categories. A covariant functor $F : \mathcal{C} \to \mathcal{D}$ is the following collection of data:

(i) for all objects $X \in \mathcal{C}$, an object $F(X) \in \mathcal{D}$;

(ii) for all morphisms $f : X \to Y$ in $\mathcal{C}$, a morphism $F(f) : F(X) \to F(Y)$ in $\mathcal{D}$.

We demand that the following properties be satisfied:

(F1) for all X we have $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$;

(F2) when $f \circ g$ is defined, we have $F(f \circ g) = F(f) \circ F(g)$.

The definition of a contravariant functor is identical, except that the arrows are reversed: in (i), we demand that $F(f)$ be a morphism from $F(Y) \to F(X)$, and (ii) then becomes $F(f \circ g) = F(g) \circ F(f)$.

Example 1.2.2. (i) Given a group $G \in \mathfrak{Gp}$, we define its commutator subgroup $[G,G]$ to be the subgroup of G generated by the elements $g_1 g_2 g_1^{-1} g_2^{-1}$ with $g_1, g_2 \in G$. This is a normal subgroup of G, so we can define the abelianization G^{ab} of G to be the corresponding quotient:

$$G^{\mathrm{ab}} = G/[G,G]. \tag{1.2.3}$$

The group G^{ab} is abelian. Moreover, a morphism of groups $f : G \to H$ induces a morphism f^{ab} of abelian groups $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$. This means that abelianization is a functor $F : \mathfrak{Gp} \to \mathfrak{Ab}$, defined as follows:

$$\begin{cases} G \in \mathrm{Obj}(\mathfrak{Gp}) \mapsto F(G) = G^{\mathrm{ab}} \in \mathrm{Obj}(\mathfrak{Ab}), \\ f \in \mathrm{Hom}_{\mathfrak{Gp}}(G,H) \mapsto F(f) = f^{\mathrm{ab}} \in \mathrm{Hom}_{\mathfrak{Ab}}(G^{\mathrm{ab}}, H^{\mathrm{ab}}). \end{cases} \tag{1.2.4}$$

(ii) Given a group G, we can form its center

$$V(G) = \{z \in G : gz = zg \text{ for all } g \in G\}. \tag{1.2.5}$$

We again have that $V(G)$ is an abelian group. However, this construction does *not* give rise to a functor, since in general a map of groups $G \to H$ does not restrict in a natural way to a map $V(G) \to V(H)$. (Take a nontrivial map from $\mathbb{Z}/3\mathbb{Z}$ to S_3 to get a counterexample.) Note how this example again emphasizes the relevance of considering morphisms instead of only objects!

(iii) Any abelian group is a group, and any group is a set. Moreover, any homomorphism of abelian groups is a group homomorphism, and any group homomorphism is a map of sets. In this way, we obtain forgetful functors $\mathfrak{Ab} \to \mathfrak{Gp}$ and $\mathfrak{Gp} \to \mathfrak{Set}$.

Functors are quite well-structured; given two functors F, G between two categories, there is even a notion of a morphism between them (so that functors between two given categories actually form a category themselves!).

Definition 1.2.6. Let F, G be two functors $\mathcal{C} \to \mathcal{D}$. A natural transformation $\tau : F \to G$ is a collection of morphisms $\tau_X : F(X) \to G(X)$ in $\mathcal{D}$ for all $X \in \mathrm{Obj}(\mathcal{C})$ such that for any morphism $f : X_1 \to X_2$ in the category $\mathcal{C}$ we have a commutative diagram

$$\begin{array}{ccc} F(X_1) & \xrightarrow{\tau_{X_1}} & G(X_1) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(X_2) & \xrightarrow[\tau_{X_2}]{} & G(X_2) \end{array} \tag{1.2.7}$$

(Here and later, commutative means that the various possible compositions in a diagram coincide: For example, in (1.2.7) we have that $G(f)\tau_{X_1} = \tau_{X_2}F(f)$.)

A natural isomorphism is a natural transformation for which all τ_X are isomorphisms in the category $\mathcal{D}$.

This sounds and is rather abstract, but includes very natural constructions. Here is one example.

Example 1.2.8. Fix $n \in \mathbb{N}$. Let $\mathrm{GL}_n : \mathfrak{Rng} \to \mathfrak{Gp}$ be the functor that sends a ring R to the group $\mathrm{GL}_n(R)$ of invertible matrices over R, that is, the matrices over R whose determinant is a unit in R, and that sends a ring homomorphism $h : R \to S$ to the map $\mathrm{GL}_n(h) : \mathrm{GL}_n(R) \to \mathrm{GL}_n(S)$ obtained by applying h to the entries of a matrix in $\mathrm{GL}_n(R)$. Note that this is indeed a functor: given a ring homomorphism $R \to S$, we obtain a group homomorphism $\mathrm{GL}_n(R) \to \mathrm{GL}_n(S)$. Similarly, let $U : \mathfrak{Rng} \to \mathfrak{Gp}$ be the functor that sends R to the group of units R^* and that sends a ring homomorphism $h : R \to S$ to the map $U(h) : R^* \to S^*$ that is the restriction of h to the unit group of R.

Given a ring R, the determinant induces a group homomorphism $\det_R : \mathrm{GL}_n(R) \to R^* = U(R)$. Since this is defined by an integral expression in the coordinates of the matrix, we get a commutative diagram

$$\begin{array}{ccc} \mathrm{GL}_n(R) & \xrightarrow{\det_R} & U(R) \\ {\scriptstyle \mathrm{GL}_n(h)}\downarrow & & \downarrow{\scriptstyle U(h)} \\ \mathrm{GL}_n(S) & \xrightarrow[\det_S]{} & U(S) \end{array} \tag{1.2.9}$$

for any ring homomorphism $h : R \to S$. This means exactly that there is a natural transformation $\det : \mathrm{GL}_n \to U$.

Natural transformations also play an important role in defining so-called equivalences between categories. At first sight, it seems that there is a logical notion of categorical equivalence, namely the following.

Definition 1.2.10. Two categories $\mathcal{C}, \mathcal{D}$ are called isomorphic if there exist functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that FG and GF are the identity functors.

The problem is that this notion is far too restrictive for our purposes.

Example 1.2.11. Fix a field K and consider the category $\mathfrak{FinVec}_K$ of finite-dimensional vectors spaces over K. Moreover, define $\mathfrak{Mat}_K$ to be the categories whose set of objects is K^n, with $n \in \mathbb{N} = \{0, 1, \ldots\}$, and for which $\mathrm{Hom}(K^m, K^n) = \mathfrak{Mat}_{m,n}(K)$, with matrix multiplication as composition.

There is an obvious functor $\iota : \mathfrak{Mat}_K \to \mathfrak{FinVec}_K$. Moreover, if, as is common in mathematics, we are arrogant enough to assume that we pick out a basis B_V for every finite-dimensional vector space V over K, then there is also a functor $B : \mathfrak{FinVec}_K \to \mathfrak{Mat}_K$. Indeed, we can then send V to $K^{\dim(V)}$ and $f : V \to W$ to the matrix representation $B(f)$ of f in the bases B_V and B_W. You should check that B is indeed a functor before proceeding!

However, there are many, many more finite-dimensional vector space than there are powers K^n. This means that there is no chance of $\mathfrak{FinVec}_K$ and $\mathfrak{Mat}_K$ are isomorphic. They certainly are not isomorphic via the functors that we just defined, since in general V does not *equal* $K^{\dim(V)}$.

We weaken our notion of equivalence correspondingly.

Definition 1.2.12. Two categories $\mathcal{C}, \mathcal{D}$ are called equivalent if there exist functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that FG and GF are naturally isomorphic to the identity functors.

We now resume our previous example to show that while there may not exist an isomorphism of categories between $\mathfrak{Mat}_K$ and $\mathfrak{FinVec}_K$, we can still find an equivalence between these categories.

Example 1.2.13. If we take B_{K^n} to be the standard basis of K^n, then the composed functor $B\iota$ is the identity functor. Moreover, if we let $\tau_V : K^{\dim(V)} \to V$ be the isomorphism induced by our choice of basis for V, then for any morphism $f : V \to W$ in $\mathfrak{FinVec}_K$ the diagram

$$\begin{tikzcd} K^{\dim(V)} \arrow[r, "\tau_V"] \arrow[d, "\iota(B(f))"'] & V \arrow[d, "f"] \\ K^{\dim(W)} \arrow[r, "\tau_W"'] & W \end{tikzcd} \tag{1.2.14}$$

commutes. This means that τ defines a natural isomorphism $\iota B \to \mathrm{id}_{\mathfrak{FinVec}_K}$. Therefore B and ι do define an equivalence between $\mathfrak{FinVec}_K$ and $\mathfrak{Mat}_K$.

This is what we mean deep down when we say that matrices and maps between finite-dimensional vector spaces are “really” the same thing…

Example 1.2.15. Another nice example of an equivalence of categories is the Galois correspondence that figures in the main theorem of Galois theory. We do not take up this theme.

When equivalences are not available, there is still a very good second-best option. According to Saunders MacLane:

> The slogan is “Adjoint functors arise everywhere”.

They are certainly in the next definition.

Definition 1.2.16. Let $F: \mathcal{C} \to \mathcal{D}$ and $G: \mathcal{D} \to \mathcal{C}$ be functors. Then F is called left adjoint to G (which in turn is called right adjoint to G) if for all $X \in \mathcal{C}$ and $Y \in \mathcal{D}$ there is a bijection

$$\varphi_{X,Y} : \mathrm{Hom}_{\mathcal{D}}(F(X), Y) \to \mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \tag{1.2.17}$$

such that moreover these bijections vary naturally with X and Y in the sense that the diagrams

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{D}}(F(X), Y) & \xrightarrow{\varphi_{X,Y}} & \mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \\ \big\downarrow g \circ \_ \circ F(f) & & \big\downarrow G(g) \circ \_ \circ f \\ \mathrm{Hom}_{\mathcal{D}}(F(X'), Y') & \xrightarrow{\varphi_{X',Y'}} & \mathrm{Hom}_{\mathcal{C}}(X', G(Y')) \end{array} \tag{1.2.18}$$

commute for all $f: X' \to X$ and $g: Y \to Y'$.

This formal definition is not how one actually memorizes this definition, certainly not (1.2.18); concretely, all of this comes down to saying that giving a morphism from $F(X)$ to Y is "the same" as giving a morphism X to $G(Y)$. And this phenomenon does indeed show up everywhere. It is especially common for forgetful functors, which tend to admit left adjoints.

Example 1.2.19. (i) Consider the abelianization functor $\mathfrak{Gp} \to \mathfrak{Ab}$. This is in fact left adjoint to the forgetful functor $\mathfrak{Ab} \to \mathfrak{Gp}$. Indeed, the requested natural isomorphism

$$\mathrm{Hom}_{\mathfrak{Ab}}(G/[G,G], A) \to \mathrm{Hom}_{\mathfrak{Gp}}(G, A) \tag{1.2.20}$$

comes from the fact that given a group G and an abelian group A, any group homomorphism $G \to A$ factors uniquely through the projection $G \to G^{\mathrm{ab}}$ to the abelianization of G.

(ii) Let $\mathfrak{Fld} \to \mathfrak{Rng}$ be the forgetful functor. The formation of the quotient field of a ring is a left adjoint to this functor. Indeed, the natural isomorphism

$$\mathrm{Hom}_{\mathfrak{Fld}}(Q(R), K) \to \mathrm{Hom}_{\mathfrak{Rng}}(R, K) \tag{1.2.21}$$

comes from the fact that given a ring R and a field K, any ring homomorphism $R \to K$ extends uniquely to a homomorphism of fields $Q(R) \to K$. (If you have only seen the construction of $Q(R)$ for domains, do not worry; the construction for arbitrary rings is a generalization of it.)

(iii) Let $\mathfrak{Ab} \to \mathfrak{Set}$ be the forgetful functor. This functor again admits an adjoint, which sends a set S to the free abelian group

$$\mathbb{Z}[S] = \bigoplus_{s \in S} \mathbb{Z}s \tag{1.2.22}$$

over S, and which sends a map of sets $f: S \to T$ to the induced map

$$\begin{aligned} \mathbb{Z}[S] &\to \mathbb{Z}[T] \\ \sum_i n_i s_i &\mapsto \sum_i n_i f(s_i). \end{aligned} \tag{1.2.23}$$

You should check that these functors are indeed adjoint!

(iv) Intuitively, and as in the preceding examples, adjoints to a forgetful functor $\mathcal{D} \to \mathcal{C}$ are obtained by associating an "optimal" or "most universal" object of $\mathcal{D}$ to an object of $\mathcal{C}$.

(v) Finally, as a more advanced example, the tensor product functor $M \otimes_R \_ : \mathfrak{Mod}_R \to \mathfrak{Mod}_R$ is left adjoint to $\mathrm{Hom}_R(M, \_) : \mathfrak{Mod}_R \to \mathfrak{Mod}_R$. Indeed, in this case the isomorphism

$$\mathrm{Hom}(M \otimes_R N, L) \to \mathrm{Hom}(M, \mathrm{Hom}(N, L)) \tag{1.2.24}$$

comes from the property that both modules share, namely that they parametrize bilinear maps from $M \times N$ to L. For the tensor product, this is a matter of definition, whereas for the right-hand side we remark that giving a bilinear map $B : M \times N \to L$ gives rise to the morphism $M \to \mathrm{Hom}(N, L)$ given by $m \to B(m, \_)$.

1.3 Presheaves and sheaves

We now want to consider another category, namely that of "functions" on a given topological space. The first step towards formalizing this notion is provided by the following definition.

Definition 1.3.1. Let X be a topological space. We define the category $\mathfrak{Open}_X$ as follows: Its objects are the open subsets of X, and given $U, V \in \mathrm{Obj}(\mathfrak{Open}_X)$, the set of morphisms $\mathrm{Hom}_{\mathfrak{Open}_X}(U, V)$ consists of the inclusion of U into V if $U \subset V$; otherwise it is the empty set.

Example 1.3.2. Let X be an indiscrete topological space. By definition this means that $\mathrm{Obj}(\mathfrak{Open}_X) = \mathcal{U}_X$ has two elements, namely $\emptyset$ and X. The sets of morphisms $\mathrm{Hom}(\emptyset, \emptyset)$ and $\mathrm{Hom}(X, X)$ both have the identity morphism as their unique element. Beyond this, the only other morphism of $\mathfrak{Open}_X$ is that coming from the inclusion $\emptyset \to X$.

Definition 1.3.3. Let X be a topological space. A presheaf (of abelian groups) on X is a contravariant functor

$$\mathscr{F} : \mathfrak{Open}_X \to \mathfrak{Ab}. \tag{1.3.4}$$

This means that giving a presheaf on X amounts to giving the following data:

(i) for every open $U \subset X$ an abelian group $\mathscr{F}(U)$;

(ii) for every inclusion $V \subset U$ a restriction map $\rho_V^U : \mathscr{F}(U) \to \mathscr{F}(V)$.

Here the functoriality condition translates into the demand that ρ_U^U is the identity homomorphism for all open subsets U of X and that

$$\rho_W^U = \rho_W^V \circ \rho_V^U \tag{1.3.5}$$

for all inclusions $\rho_W^U = \rho_W^V \circ \rho_V^U$ of open subsets of X. Moreover, we impose $\mathscr{F}(\emptyset) = 0$.

The elements of the abelian group $\mathscr{F}(U)$ are called the sections of the presheaf $\mathscr{F}$ over the open set U.

Definition 1.3.6. Let $\mathscr{F}$ and $\mathscr{G}$ be two presheaves on the same topological space X. A morphism of presheaves from $\mathscr{F}$ to $\mathscr{G}$ is a natural transformation $\varphi : \mathscr{F} \to \mathscr{G}$. Here $\mathscr{F}$ and $\mathscr{G}$ are considered as contravariant functors on $\mathfrak{Open}_X$.

In other words, φ is a collection of homomorphisms of abelian groups $\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)$, one for every open subset U of X, such that for every inclusion $V \subset U$, the following diagram commutes:

$$\begin{tikzcd} \mathscr{F}(U) \arrow[r, "\varphi_U"] \arrow[d, "\rho^U_V"'] & \mathscr{G}(U) \arrow[d, "\sigma^U_V"] \\ \mathscr{F}(V) \arrow[r, "\varphi_V"'] & \mathscr{G}(V) \end{tikzcd} \tag{1.3.7}$$

We see that we can interpret φ as a collection of compatible maps φ_U between the sections of $\mathscr{F}$ and $\mathscr{G}$ over the various open subsets U of X.

The notion of morphism in Definition 1.3.6 above allows us to define the category $\mathfrak{PreSh}_X$ of presheaves on a given topological space X. Its objects are the presheaves on the topological space X, and given two such presheaves $\mathscr{F}$ and $\mathscr{G}$ we define $\mathrm{Hom}_{\mathfrak{PreSh}_X}$ to be the set of natural transformations $\mathscr{F} \to \mathscr{G}$. (In fact this set is even an abelian group in a natural way.)

Example 1.3.8.

(i) Let X be a topological space. Given an open set, we can consider

$$\mathscr{F}(U) = \mathrm{Hom}_{\mathfrak{Set}}(U, \mathbb{Z}), \tag{1.3.9}$$

the set of all functions on U with values in $\mathbb{Z}$. This set is an abelian group under pointwise addition of functions. There is the usual restriction map of functions $\rho^U_V : \mathscr{F}(U) \to \mathscr{F}(V)$ that sends a function $f \in \mathscr{F}(U)$ to its restriction $f|_V \in \mathscr{F}(V)$. It makes $\mathscr{F}$ into a presheaf on X.

(ii) Similarly, given an abelian group A we can define the presheaf of abelian groups

$$\mathscr{F}(U) = \mathrm{Hom}_{\mathfrak{Set}}(U, A) \tag{1.3.10}$$

on X: Given an open U of X, we get the abelian group of functions $U \to A$ as sections of $\mathscr{F}$ over U. Restriction again makes $\mathscr{F}$ into a presheaf on X.

(iii) Let us take $A = \mathbb{R}$ in (ii), with the usual topology. In (ii), we obtain quite a lot of functions, in fact usually a rather formless and unmanageable set. We can cut this down to size by using the topology of X and $\mathbb{R}$, in that we only consider the *continuous* functions $U \to \mathbb{R}$ on a given open subset U of X. That is, we instead consider

$$\mathscr{F}(U) = \mathrm{Hom}_{\mathfrak{Top}}(U, \mathbb{R}). \tag{1.3.11}$$

Since the restriction of a continuous function is again continuous, this construction is functorial and therefore does indeed give rise to a presheaf.

(iv) Finally, given a topological space X and an abelian group A, we can construct the constant presheaf $\underline{A}$ on X. This is the presheaf for which

$$\underline{A}(U) = A \tag{1.3.12}$$

for all non-empty $U \subset X$, which $\rho^U_V = \mathrm{id}_A$ if $V \subset U$ is non-empty and where $\rho^U_V = 0$ if V is empty.

(v) Let X be as in Example 1.3.2. Then giving a presheaf on X is the same as giving an abelian group A, in the following sense: Given A, the constant presheaf $\underline{A}$ is a presheaf on X, and conversely every presheaf on X is of the form $\underline{A}$ for some (uniquely determined) abelian group A, namely $A = \underline{A}(X)$.

Theorem 1.3.13. *Let X be a topological space. Then $\mathfrak{PreSh}_X$ is an abelian category.*

Proof. (Sketch) We verify parts (i)-(iv) of the definition.

(i): The zero object of $\mathfrak{PreSh}_X$ is the presheaf that sends all open sets U to the trivial abelian group 0, and for which all the restriction maps are the identity map $0 \to 0$.

(ii): Given $\mathscr{F}$ and $\mathscr{G}$, we define their product by $(\mathscr{F} \times \mathscr{G})(U) = \mathscr{F}(U) \times \mathscr{G}(U) = \mathscr{F}(U) \oplus \mathscr{G}(U)$. Given an inclusion $V \subset U$, we define the restriction map $(\mathscr{F} \oplus \mathscr{G})(U) \to (\mathscr{F} \oplus \mathscr{G})(V)$ to be the sum $\rho_V^U \oplus \sigma_V^U$, where ρ, σ are the restriction maps for $\mathscr{F}, \mathscr{G}$. This is indeed a presheaf, and one can show that it satisfies the relevant universal property, the proof being analogous to that of the next case.

(iii): Given a morphism $\varphi : \mathscr{F} \to \mathscr{G}$, we define $\ker(\varphi)(U) = \ker(\varphi_U)$ and $\operatorname{coker}(\varphi)(U) = \operatorname{coker}(\varphi_U)$ on objects. Using appropriate restriction maps, this gives rise to presheaves on X with the requested properties. Let us show this for $\operatorname{coker}(\varphi)$.

To start with, we show that the restriction map σ on $\mathscr{G}$ induces a well-defined restriction map

$$\operatorname{coker}(U) = \mathscr{G}(U)/\varphi_U(\mathscr{F}(U)) \to \mathscr{G}(V)/\varphi_V(\mathscr{F}(V)) = \operatorname{coker}(V). \tag{1.3.14}$$

For this, we consider the following diagram:

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r, "\varphi_U"] \arrow[d, "\rho_V^U"'] & \mathscr{G}(U) \arrow[r, "\pi_U"] \arrow[d, "\sigma_V^U"] & \mathscr{G}(U)/\varphi_U(\mathscr{F}(U)) \arrow[d, dashed, "\tau_V^U"] \\
\mathscr{F}(V) \arrow[r, "\varphi_V"] & \mathscr{G}(V) \arrow[r, "\pi_V"] & \mathscr{G}(V)/\varphi_V(\mathscr{F}(V))
\end{tikzcd} \tag{1.3.15}$$

Here π_U is the quotient map. The third isomorphism theorem shows that there is a unique map τ_V^U that makes this diagram commute; it exists because σ_V^U maps $\varphi_U(\mathscr{F}(U))$ to 0 in $\mathscr{G}(V)/\varphi_V(\mathscr{F}(V))$, or alternatively because σ_V^U maps $\varphi_U(\mathscr{F}(U))$ into $\varphi_V(\mathscr{F}(V))$. This, in turn, follows because φ is a natural transformation, showing that $\sigma_V^U \varphi_U = \varphi_V \rho_V^U$. A similar argument also shows that there is a natural transformation $\pi : \mathscr{G} \to \operatorname{coker}(\varphi)$ given by π_U on an open set U. In other words, at this point we have constructed the cokernel $\operatorname{coker}(\varphi)$ as a sheaf, along with a morphism of presheaves π from $\mathscr{G}$ to $\operatorname{coker}(\varphi)$.

We claim that the pair $(\operatorname{coker}(\varphi), \pi)$ indeed satisfies the universal property of a cokernel. For this, let H be another presheaf, and let $\psi : \mathscr{G} \to H$ be such that the composition $\psi\varphi$ is 0. This means that for any fixed U we get a diagram

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r, "\varphi_U"] \arrow[rr, bend left, "0"] \arrow[drr, "0"'] & \mathscr{G}(U) \arrow[r, "\pi_U"] \arrow[dr, "\psi_U"] & \mathscr{G}(U)/\varphi_U(\mathscr{F}(U)) \arrow[d, dashed, "\chi_U"] \\
& & H(U)
\end{tikzcd} \tag{1.3.16}$$

The existence and uniqueness of the map χ_U follows because $\mathscr{G}(U)/\psi_U(\mathscr{F}(U))$ is the cokernel in the category of abelian groups: we have defined it as such! The collection of these χ_U gives rise to a natural transformation $\chi : \operatorname{coker}(\varphi) \to H$ such that $\psi = \chi\pi$. Moreover, because the morphism χ_U is uniquely determined for all U, the morphism of presheaves χ is also unique. We have verified the universal property.

(iv): This is technical verification that is very similar to what went before and that we therefore do not write out here. $\square$

Presheaves form a very manageable category, because of the simplicity in the formation of their kernels and cokernels. This is of great help. However, recall that we want to think of presheaves as functions (vanilla, smooth, holomorphic or otherwise) on a space. Now functions on a space X have one very important intuitive property: If $(U_i)_{i\in I}$ is an open cover of X, and we are given functions f_i on the individual open sets U_i, then we can glue these together into a function f on all of X if and only if the restrictions of the f_i to the various intersections of the U_i all coincide. When we capture this in the language of presheaves, we get the following notion.

Definition 1.3.17. Let $\mathscr{F}$ be a presheaf (of abelian groups) on a topological space X. Then we call $\mathscr{F}$ a sheaf (of abelian groups) on X if the following condition is satisfied:

(Sh) Let U be an open subset of X, and let $(U_i)_{i\in I}$ be an open cover of U. Suppose that $f_i \in \mathscr{F}(U_i)$ are sections such that for all i, j in I we have

$$\rho^{U_i}_{U_i \cap U_j}(f_i) = \rho^{U_j}_{U_i \cap U_j}(f_j). \tag{1.3.18}$$

Then there exists a unique $f \in \mathscr{F}(U)$ such that for all i we have $\rho^U_{U_i}(f) = f_i$.

Remark 1.3.19. As a special case, we obtain that if $\mathscr{F}$ is a sheaf and $f \in \mathscr{F}(U)$ is such that $\rho^U_{U_i}(f) = 0$ for all open subsets U_i in a open cover $(U_i)_{i\in I}$ of U, then $f = 0$.

Sheaves turn out to be the "right" abstract formalization of functions on spaces, so we should study them in some detail.

Example 1.3.20. Let X be a topological space.

(i) For any abelian group A, the presheaf $\mathscr{F}(U) = \mathrm{Hom}_{\mathfrak{Set}}(U, A)$ is a sheaf, as a function on U is indeed uniquely determined by its restrictions to the elements of an open cover $(U_i)_{i\in I}$ of U.

(ii) The presheaf of continuous functions $\mathscr{F}(U) = \mathrm{Hom}_{\mathfrak{Top}}(U, \mathbb{R})$ is also a sheaf, because of Part (i) and the fact that a function on U is continuous if and only if its restrictions to the open subsets U_i of an open cover $(U_i)_{i\in I}$ of U are all continuous.

(iii) Let $X = \mathbb{C}$ with the usual topology. Then the constant presheaf $\underline{\mathbb{Z}}$ is *not* a sheaf on X. Indeed, let $U = U_1 \cup U_2$ be a disjoint union of two non-empty open subsets U_1 and U_2 of $\mathbb{C}$. Define $f_1 = 1 \in \mathbb{Z} = \underline{\mathbb{Z}}(U_1)$ and $f_2 = 2 \in \mathbb{Z} = \underline{\mathbb{Z}}(U_2)$.

The functions f_1 and f_2 satisfy the requested compatibility condition. Indeed, we have $\mathscr{F}(U_1 \cap U_2) = \mathscr{F}(\emptyset) = 0$. Therefore $\rho^{U_1}_{U_1 \cap U_2}(f_1) = 0 = \rho^{U_2}_{U_1 \cap U_2}(f_2)$. On the other hand, there is no $f \in \underline{\mathbb{Z}}(U_1 \cup U_2)$ such that $\rho^U_{U_1}(f) = f_1$ and $\rho^U_{U_2}(f) = f_2$. Indeed, since the restriction maps $\mathbb{Z} = \underline{\mathbb{Z}}(U_1 \cup U_2) \to \underline{\mathbb{Z}}(U_1) = \mathbb{Z}$ and $\mathbb{Z} = \underline{\mathbb{Z}}(U_1 \cup U_2) \to \underline{\mathbb{Z}}(U_2) = \mathbb{Z}$ are trivial, we would get $\rho^U_{U_1} f = 1$, so that $f = 1$, whereas $\rho^U_{U_1} f = 2$, so that $f = 2$. However, we know that $1 \neq 2$ in $\mathbb{Z}$.

We see that although the compatibility condition is satisfied, there does not exists a section in $\mathscr{F}(U)$ that "glues" f_1 and f_2 together. This implies that $\mathscr{F}$ is indeed not a sheaf on X.

This allows us to define the category $\mathfrak{Sh}_X$ of sheaves on X as a subcategory of $\mathfrak{PreSh}_X$. The objects of $\mathfrak{Sh}_X$ are the sheaves (of abelian groups) on X, and given $\mathscr{F},\mathscr{G} \in \mathrm{Obj}(\mathfrak{Sh}_X)$, we define a morphism of sheaves $\mathscr{F} \to \mathscr{G}$ to be a morphism from $\mathscr{F}$ to $\mathscr{G}$ considered as presheaves.

Remark 1.3.21. More formally, the previous paragraph states that we have constructed an inclusion functor (or alternatively, a forgetful functor)

$$\iota : \mathfrak{Sh}_X \to \mathfrak{PreSh}_X \tag{1.3.22}$$

that realizes $\mathfrak{Sh}_X$ as a full subcategory of $\mathfrak{PreSh}_X$. This means that there is a bijection

$$\mathrm{Hom}_{\mathfrak{Sh}_X}(\iota(\mathscr{F}),\iota(\mathscr{G})) \to \mathrm{Hom}_{\mathfrak{PreSh}_X}(\mathscr{F},\mathscr{G}) \tag{1.3.23}$$

for all sheaves $\mathscr{F},\mathscr{G}$ in $\mathfrak{Sh}_X$.

An important theorem on sheaves is the following:

Theorem 1.3.24. *Let X be a topological space. Then the category $\mathfrak{Sh}_X$ of sheaves on X is abelian.*

It may seem that this should be obvious. After all, to form cokernels, could we not proceed exactly as for presheaves? Unfortunately, this is not the case, as the next example shows. The problem is that the naive cokernel of a morphism of sheaves need no longer be a sheaf.

Example 1.3.25. Consider the topological space $X = \mathbb{C}^* = \mathbb{C} - \{0\}$, and let $\mathscr{O}_X^*$ be the sheaf of smooth non-zero functions with values in $\mathbb{C}$, so that

$$\mathscr{O}_X^*(U) = \mathscr{C}^\infty(U,\mathbb{C}^*). \tag{1.3.26}$$

Note that $\mathscr{O}_X^*$ is a sheaf of abelian groups via multiplication. Squaring induces a natural transformation $\mathscr{O}_X^* \to \mathscr{O}_X^*$.

Claim: The presheaf cokernel

$$\mathscr{O}_X^*/(\mathscr{O}_X^*)^2 : U \mapsto \mathscr{O}_X^*(U)/\mathscr{O}_X^*(U)^2 \tag{1.3.27}$$

is not a sheaf.

To see this, define

$$V_1 = \mathbb{C}^* - \mathbb{R}_-,\ V_2 = \mathbb{C}^* - \mathbb{R}_+. \tag{1.3.28}$$

On V_1, there is a well-defined smooth square root given by

$$w_1 : re^{i\vartheta} \mapsto r^{1/2}e^{i\vartheta/2} \tag{1.3.29}$$

for $\vartheta \in [-\pi,\pi]$. Similarly, on V_2 we have

$$w_2 : re^{i(\vartheta-\pi)} \mapsto r^{1/2}e^{i(\vartheta-\pi)/2}. \tag{1.3.30}$$

Consider a class in $\mathscr{O}_X^*(X)/(\mathscr{O}_X^*)^2(X)$ represented by some section $f \in \mathscr{O}_X^*(X)$. Given $P \in X$, we can always find an open $U_P \subset X$ such that $f|_{U_P}$ has image contained in either V_1 or V_2. Say that the image is in V_i. Then we can construct the smooth function

$$g_P = w_i \circ f|_{U_P}. \tag{1.3.31}$$

on U_P. We have $g_P^2 = f|_{U_P}$. In other words, for all $P \in X$ the restriction $f|_{U_P}$ is trivial in $\mathscr{O}_X^*(U_P)/(\mathscr{O}_X^*)^2(U_P)$.

If $\mathscr{O}_X^*/(\mathscr{O}_X^*)^2$ were a sheaf, then the above discussion would imply that f is trivial in $\mathscr{O}_X^*(X)/\mathscr{O}_X^*(X)^2$ by Remark 1.3.19, since the open sets $(U_P)_{P\in X}$ covers X. This would imply that $f = g^2$ for some function g on X. However, this is not always possible. For example, the non-zero function $f = x$ on X has no global square root. (Try defining one and see how the function behaves when you make a counterclockwise turn around 0.)

Remark 1.3.32. The example above also applies when considering the presheaf of holomorphic (instead of merely smooth) $\mathbb{C}^*$-valued functions on X.

Example 1.3.33. Here is another example that shows that presheaf cokernels of morphisms of sheaves may no longer be sheaves. Let X be a topological space with underlying set $\{O, C_1, C_2\}$ and open sets $\emptyset$, $\{O\}$, $\{O, C_1\}$, $\{O, C_2\}$ and X. (Intuitively, O is an open point of X, whereas C_1 and C_2 are closed points.)

In the exercises you will show that giving giving a presheaf $\mathscr{F}$ on X is nothing but giving a commutative diagram

$$\begin{tikzcd} & A_1 \arrow[dr, "g_1"] & \\ A \arrow[ur, "f_1"] \arrow[dr, "f_2"'] & & A_{12} \\ & A_2 \arrow[ur, "g_2"'] & \end{tikzcd} . \tag{1.3.34}$$

In fact we have $A = \mathscr{F}(X)$, $A_1 = \mathscr{F}(\{0, C_1\})$, $A_2 = \mathscr{F}(\{0, C_2\})$, and $A_{12} = \mathscr{F}(\{O\})$, while f_1, f_2, g_1, g_2 are the various restriction maps. You will also show that $\mathscr{F}$ is a sheaf if and only if the map

$$\begin{aligned} (f_1, f_2) : A &\to A_1 \oplus A_2 \\ a &\mapsto (f_1(a), f_2(a)) \end{aligned} \tag{1.3.35}$$

is injective and has image $\{(a_1, a_2) \in A_1 \oplus A_2 : g_1(a_1) = g_2(a_2)\}$. (Abstractly, this means that the triple (A, f_1, f_2) is the *equalizer* of the triple (A_{12}, g_1, g_2).

Now consider the diagram

$$\begin{tikzcd} & \mathbb{Z} \arrow[dr, "2"] & \\ \mathbb{Z} \arrow[ur, "1"] \arrow[dr, "-1"'] & & \mathbb{Z} \\ & \mathbb{Z} \arrow[ur, "2"'] & \end{tikzcd} , \tag{1.3.36}$$

with the integers denoting various multiplication maps. One verifies that this diagram defines a sheaf $\mathscr{F}$ on X. Multiplication by 2 on all sections defines a map $2 : \mathscr{F} \to \mathscr{F}$, and the resulting presheaf cokernel

$$\mathscr{F}/2\mathscr{F} : U \mapsto \mathscr{F}(U)/2\mathscr{F}(U) \tag{1.3.37}$$

is described by the following diagram:

$$\begin{tikzcd} & \mathbb{Z}/2\mathbb{Z} \arrow[dr, "2"] & \\ \mathbb{Z}/2\mathbb{Z} \arrow[ur, "1"] \arrow[dr, "-1"'] & & \mathbb{Z}/2\mathbb{Z} \\ & \mathbb{Z}\ 2\mathbb{Z} \arrow[ur, "2"'] & \end{tikzcd} . \tag{1.3.38}$$

This time, the sheaf property is not verified. In other words, once again the presheaf cokernel $\mathscr{F}/2\mathscr{F}$ is not a sheaf.

1.4 Sheaf cokernels

We want to make the sections of the presheaf cokernel glue in some way or other in order to define the sheaf cokernel. We will do this by "loosening up" the sections of arbitrary presheaves in such a way that they glue by default and by identifying sections that restrict to identical sections upon taking subcovers. In this way, the existence and uniqueness in the definition of a sheaf will hold essentially by default. Let us now perform these constructions on a technical level, where it can be considered as an adjoint to the forgetful functor from Remark 1.3.21.

You should *not* learn these constructions by heart! One of the important ideas behind algebraic geometry is that it is often sufficient to proof that certain objects (like sheafifications and cohomological functors) exist and can be constructed in principle: We do not always require their exact details when proceeding. And regardless, the material for the first chapter serves as motivation and inspiration rather than as direct learning material.

Definition 1.4.1. Let $\mathscr{F}$ be a presheaf on a topological space X, let U be an open subset of X.

A compatible tuple of sections of $\mathscr{F}$ over U is a tuple $(f_i)_{i\in I}$, where $f_i \in \mathscr{F}(U_i)$ are sections of $\mathscr{F}$ over an open cover of U such that

$$\rho^{U_i}_{U_i\cap U_j}(f_i) = \rho^{U_j}_{U_i\cap U_j}(f_j). \tag{1.4.2}$$

for all $i, j \in I$. (Note that unlike in Definition 1.3.17 we do not know whether the tuple $(f_i)_{i\in I}$ glues to an element f of $\mathscr{F}(U)$, since $\mathscr{F}$ is merely a presheaf this time!)

We say that two compatible tuples of sections $(f_i)_{i\in I}$ for an open cover $(U_i)_{i\in I}$ of U and $(g_j)_{j\in J}$ for a second open cover $(V_j)_{j\in J}$ are *equivalent* if all $i \in I$ and $j \in J$ there exists a cover $\{W_k\}_{k\in K}$ of $U_i \cap V_j$ such that

$$\rho^{U_i}_{W_k}(f_i) = \rho^{V_j}_{W_k}(g_j) \text{ for all } k \in K. \tag{1.4.3}$$

Given U, we let $C_{\mathscr{F}}(U)$ be the set of compatible tuples of sections $\{f_i\}_{i\in I}$ of $\mathscr{F}$ over U, and. Then $C_{\mathscr{F}}(U)$ is an abelian group via

$$\{f_i\}_{i\in I} + \{g_j\}_{j\in J} = \{h_{(i,j)}\}_{(i,j)\in I\times J}, \tag{1.4.4}$$

where

$$h_{i,j} = \rho^{U_i}_{U_i\cap V_j}(f_i) + \rho^{V_j}_{U_i\cap V_j}(g_j) \in \mathscr{F}(U_i \cap V_j). \tag{1.4.5}$$

Note that $(U_i \cap V_j)_{(i,j)\in I\times J}$ is indeed an open cover of U. Let

$$\mathscr{F}^+(U) = C(U)/\sim \tag{1.4.6}$$

be the set of equivalence classes of compatible tuples of sections under the equivalence from Definition 1.4.1. Then $\mathscr{F}(U)$ is again an abelian group, and in fact $\mathscr{F}(U)$ becomes a presheaf when using the restriction maps on compatible tuples of sections that is inherited from $\mathscr{F}$. (Some detail in these construction will be relegated to the exercises.)

In fact $\mathscr{F}^+$ is even a sheaf. Indeed, let $(U_i)_{i\in I}$ be an open cover of an open set $U \subset X$, and suppose that for all i we are given a section s_i of $\mathscr{F}^+$ over U_i. Such sections come from compatible tuples of sections $(f_{i,j})_{j\in J_i}$ of $\mathscr{F}$ for open covers $(U_{i,j})_{j\in J_i}$ of the individual U_i.

Now suppose that the restrictions of the s_i to the overlaps $U_i \cap U_{i'}$ are identical as sections of the presheaf $\mathscr{F}^+$. Then $s = (f_{i,j})_{i\in I, j\in J_i}$ is a section of $\mathscr{F}^+$ over U that restricts to the individual s_i. Indeed, the fact that the s_i are identical as sections of $\mathscr{F}^+$ when restricted to $U_i \cap U_{i'}$ means that the various restrictions of the $f_{i,j}$ to overlaps coincide (refining the open cover used if needed), so that s is a section of $\mathscr{F}^+$ over U by definition. The uniqueness of s follows from the very definition of $\mathscr{F}^+(U)$: indeed, quotienting out by the equivalence relation $\sim$ ensures that compatible tuples which have identical restrictions to open subcovers are in fact equal as sections of $\mathscr{F}^+(U)$. (Again: Some detail is omitted, since it becomes tortuous at some point.)

Definition 1.4.7. Let $\mathscr{F} \in \mathfrak{PreSh}_X$. We call the sheaf $\mathscr{F}^+ \in \mathfrak{Sh}_X$ defined above the sheaf associated to $\mathscr{F}$ or the sheafification of $\mathscr{F}$.

Example 1.4.8. Let X be a topological space, and let $\underline{A}$ be the constant presheaf on X with values in A. Then

$$\underline{A}^+(U) = \prod_{\pi_0(U)} A, \tag{1.4.9}$$

where $\pi_0(U)$ is the set of connected components of U.

Theorem 1.4.10. *Taking the associated presheaf is a left adjoint to the forgetful functor $\mathfrak{Sh}_X \to \mathfrak{PreSh}_X$ from Remark 1.3.21. More concretely, there are natural bijections*

$$\mathrm{Hom}_{\mathfrak{PreSh}_X}(\mathscr{F}, \mathscr{G}) \to \mathrm{Hom}_{\mathfrak{Sh}_X}(\mathscr{F}^+, \mathscr{G}). \tag{1.4.11}$$

Even more concretely: giving a morphism of presheaves $\mathscr{F} \to \mathscr{G}$, with $\mathscr{F}$ a presheaf and $\mathscr{G}$ a sheaf, is the same as giving a morphism of sheaves $\mathscr{F}^+ \to \mathscr{G}$.

Proof (sketch). There is a canonical morphism $\mathscr{F} \to \mathscr{F}^+$ given by interpreting a section $f \in \mathscr{F}(U)$ as a compatible tuple of sections (f) on the trivial cover (U) of U. This gives an arrow from the right hand side of (1.4.11) to the left hand side.

Conversely, given a map of presheaves $\varphi : \mathscr{F} \to \mathscr{G}$, consider a section over U of $\mathscr{F}^+$. It is represented by a compatible tuple of sections $(f_i)_{i\in I}$ over an open cover $(U_i)_{i\in I}$ of U. Consider the sections

$$g_i = \varphi_{U_i}(f_i) \in \mathscr{G}(U_i). \tag{1.4.12}$$

The fact that the f_i are compatible up to refinement implies that for all i, j in I we have

$$\rho^{U_i}_{U_i\cap U_j}(f_i) = \rho^{U_j}_{U_i\cap U_j}(f_j). \tag{1.4.13}$$

Because φ is a morphism of presheaves, this implies that

$$\rho^{U_i}_{U_i\cap U_j}(g_i) = \rho^{U_j}_{U_i\cap U_j}(g_j). \tag{1.4.14}$$

The sheaf property of $\mathscr{G}$, applied to the open cover $(V_j)_{j\in J}$, then gives us a well-defined section $g \in \mathscr{G}(U)$. Putting all maps $\mathscr{F}^+(U) \to \mathscr{G}(U)$ thus obtained together, we get a morphism of sheaves $\mathscr{F}^+ \to \mathscr{G}$. $\square$

The proof of Theorem 1.3.24 now proceeds as follows. All constructions are the same, except that of the cokernel. Given a morphism of sheaves $\varphi : \mathscr{F} \to \mathscr{G}$, let $\mathscr{G}/\varphi(\mathscr{F})$ be the presheaf cokernel, and consider the associated sheaf $(\mathscr{G}/\varphi(\mathscr{F}))^+$. Theorem 1.4.10 shows that if the composition of sheaf morphisms $\mathscr{F} \to \mathscr{G} \to H$ is 0, then the presheaf factorization

$$\begin{tikzcd} \mathscr{F} \arrow[r] \arrow[rr, bend left, "0"] \arrow[rrd, "0"'] & \mathscr{G} \arrow[r] \arrow[rd] & \mathscr{G}/\varphi(\mathscr{F}) \arrow[d, dashed, "!"] \\ & & H \end{tikzcd} \tag{1.4.15}$$

induces another unique factorization

$$\begin{tikzcd} \mathscr{F} \arrow[r] \arrow[rr, bend left, "0"] \arrow[rrd, "0"'] & \mathscr{G} \arrow[r] \arrow[rd] & \mathscr{G}/\varphi(\mathscr{F}) \arrow[r] \arrow[d, dashed, "!"] & (\mathscr{G}/\varphi(\mathscr{F}))^+ \arrow[ld, dashed, "!"] \\ & & H & \end{tikzcd} \tag{1.4.16}$$

This shows that $(\mathscr{G}/\varphi(\mathscr{F}))^+$ is the cokernel of φ in the category of sheaves.

Remark 1.4.17. We will usually denote the cokernel of a morphism of sheaves φ by $\operatorname{coker}(\varphi)$ again. A priori, this notation is ambiguous, since in the category of presheaves $\operatorname{coker}(\varphi)$ is something else entirely. However, we will mostly work in the context of sheaves, so unless otherwise stated, any cokernel mentioned will be a sheaf cokernel.

Definition 1.4.18. Let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism of sheaves. Then φ is called locally surjective if for any open set $U \subset X$ and any $g \in \mathscr{G}(U)$ there exists an open cover $(U_i)_{i\in I}$ of U and sections $f_i \in \mathscr{F}(U_i)$ such that $g_i = \varphi_{U_i}(f_i)$.

Proposition 1.4.19. *Let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism of sheaves. Then* $\operatorname{coker}(\varphi) = 0$ *if and only if φ is locally surjective.*

Proof. Suppose that $\operatorname{coker}(\varphi) = 0$. Let $g \in \mathscr{G}(U)$. Then we can map g into $\operatorname{coker}(\varphi)(U)$, where it becomes the zero section. By the very definition of the sheaf cokernel, this means that for the element $q = \varphi_U(g) \in \mathscr{G}(U)/\varphi_U(\mathscr{F}(U))$, there exists an open cover $(U_i)_{i\in I}$ of U on which the restrictions $q_i = \rho^U_{U_i}(q)$ are zero as sections of the presheaf cokernel over U_i. But this exactly that there exist $f_i \in \mathscr{F}(U_i)$ such that $g_i = \varphi_{U_i}(f_i)$.

Conversely, if φ is locally surjective, consider some open $U \subset X$ and let $q \in \operatorname{coker}(\varphi)(U)$. Then the section q of the sheaf cokernel is represented by a tuple of sections $q_i \in \operatorname{coker}(\varphi)(U_i)$ in the presheaf cokernel whose restrictions to the various intersections are compatible. We can represent q_i by $g_i \in \mathscr{G}(U_i)$. By local surjectivity, we may assume that $g_i = \varphi_{U_i}(f_i)$ with $f_i \in \mathscr{F}(U_i)$ after refining our cover further if necessary. But that means that $q_i = 0$ as a section of the presheaf cokernel over U_i, which in turn implies that q is trivial up to refinement and hence 0 in the sheaf cokernel. Since q and U were arbitrary, we see that $\operatorname{coker}(\varphi) = 0$. $\square$

Definition 1.4.20. Let $\mathcal{A}$ be an abelian category (like $\mathfrak{Sh}_X$ for a topological space X). We say that a sequence of morphisms

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0 \tag{1.4.21}$$

in $\mathcal{A}$ is a short exact sequence if the following holds:

(i) ι is a monomorphism;

(ii) π is an epimorphism;

(iii) We have $\mathrm{im}(\iota) = \ker(\pi)$.

More generally, we say that a sequence $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ is *exact (at B)* if we have $\mathrm{im}(\varphi) = \ker(\psi)$.

Remark 1.4.22. Note that given a morphism $\varphi : A \to B$ in an abelian category, we can define the image of φ without reference to elements of A as

$$\mathrm{im}(\varphi) = \ker(\mathrm{coker}(\varphi)). \tag{1.4.23}$$

Example 1.4.24. (i) The squaring map $\mathscr{O}_X^* \to \mathscr{O}_X^*$ has trivial cokernel in $\mathfrak{Sh}_X$. Its kernel is the constant sheaf $\underline{\{\pm 1\}}^+$. We obtain an exact sequence

$$1 \to \underline{\{\pm 1\}}^+ \to \mathscr{O}_X^* \to \mathscr{O}_X^* \to 1. \tag{1.4.25}$$

(ii) Similarly, exponentiation gives an exact sequence called the exponential sequence, given by

$$0 \to \underline{2\pi i \mathbb{Z}}^+ \to \mathscr{O}_X \to \mathscr{O}_X^* \to 1, \tag{1.4.26}$$

where now $\mathscr{O}_X$ is the sheaf of smooth (or holomorphic) functions on X, which we make into a sheaf of abelian groups under addition.

Example 1.4.27. Let us see what the sheafification of the cokernel $C = \mathscr{F}/2\mathscr{F}$ from Example 1.3.33 is. It turns out that we have $C^+(U) = C(U)$ for the open subsets $U \in \{\emptyset, \{O\}, \{O, C_1\}, \{O, C_2\}\}$. However, for $U = X$ something else happens.

This example is made easier by the fact that the set of non-trivial open subsets of X is fairly small: They are given by $U_{12} = \{O\}, U_1 = \{O, C_1\}$, and $U_2 = \{O, C_2\}$. So to describe compatible sections of C over X up to equivalence, we need only consider sections over these three sets: This obviates the need for using the refinement in the definition of the equivalence of compatible tuples of sections in Definition 1.4.1. Now giving compatible sections $a_1 \in C(U_1), a_2 \in C(U_2), a_{12} \in C(U_{12})$ is nothing but giving sections $a_1 \in C(U_1), a_2 \in C(U_2)$ that become equal under g_1 and g_2. This recovers the equalizer mentioned in Example 1.3.33. And indeed, since g_1 and g_2 are the zero maps, we see that we have

$$C^+(X) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \tag{1.4.28}$$

1.5 Locally ringed spaces

Definition 1.5.1. Let X be a topological space, and let $\mathscr{F}$ be a presheaf of abelian groups on X. Then the stalk of $\mathscr{F}$ at P is given by

$$\mathscr{F}_P = \{(U, f) : U \subset X \text{ open with } P \in U, f \in \mathscr{F}(U)\}/\sim, \tag{1.5.2}$$

where $(U_1, f_1) \sim (U_2, f_2)$ if there is some open V contained in $U_1 \cap U_2$ such that $\rho_V^{U_1}(f) = \rho_V^{U_2}(g)$.

The elements of the stalk $\mathscr{F}_P$, that is, the equivalence classes $[(U, f)]$ of the pairs (U, f) above, are called germs of sections of F around P. Given an element $f \in \mathscr{F}(U)$, we often denote the corresponding germ $[(U, f)]$ in $\mathscr{F}_P$ by f_P.

Let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism of sheaves. Then for all $P \in X$, we get an induced map on stalks:

$$\begin{aligned} \varphi_P : \mathscr{F}_P &\to \mathscr{G}_P \\ [(U, f)] &\mapsto [(U, \varphi_U(f)]. \end{aligned} \tag{1.5.3}$$

Proposition 1.5.4. *Let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism of sheaves on a topological space X.*

(i) φ has trivial kernel in $\mathfrak{Sh}_X$ if only if all φ_P are injective.

(ii) φ has trivial cokernel in $\mathfrak{Sh}_X$ if only if all φ_P are surjective.

(iii) φ is an isomorphism if only if all φ_P are.

Proof. We prove (i) and (ii): Part (iii) is very similar, and in fact a consequence of (i) and (ii). The exact proof is left as an exercise.

(i): Suppose that φ has trivial kernel. Let P be a point of X, and let $[(U_1, f_1)]$ and $[(U_2, f_2)]$ be two elements of $\mathscr{F}_P$ such that

$$\varphi_P([(U_1, f_1)]) = \varphi_P([(U_2, f_2)]). \tag{1.5.5}$$

This means that

$$[(U_1, \varphi_{U_1}(f_1))] = [(U_2, \varphi_{U_2}(f_2))]. \tag{1.5.6}$$

Then there is a $V \subset U_1 \cap U_2$ such that

$$\rho_V^{U_1}(\varphi_{U_1}(f_1)) = \rho_V^{U_2}(\varphi_{U_2}(f_2)). \tag{1.5.7}$$

Because φ is a morphism of sheaves, this implies that

$$\varphi_V(\rho_V^{U_1}(f_1)) = \varphi_V(\rho_V^{U_2}(f_2)). \tag{1.5.8}$$

Since the kernel of φ is trivial, the map φ_V is injective. So $\rho_V^{U_1}(f_1) = \rho_V^{U_2}(f_2)$ and therefore $[(U_1, f_1)] = [(U_2, f_2)]$, showing that φ_P is injective.

Conversely, suppose that φ_P is injective for all P in an open subset U of X. Let $f \in \mathscr{F}(U)$ be such that $\varphi_U(f) = 0$. Then for all P we have

$$\varphi_P([(U, f)]) = [(U, \varphi_U(f))] = 0 \in \mathscr{G}_P. \tag{1.5.9}$$

Since φ_P is injective, we get that $[(U, f)] = 0$. That is, f restricts to 0 in some neighborhood V_P of P. Since the neighborhoods V_P cover U, the sheaf property of $\mathscr{F}$ shows that $f = 0$. We have shown that φ_U is injective for all U, and therefore that φ is injective.

(ii): Suppose that φ has trivial cokernel. Then φ is locally surjective by Proposition 1.4.19. Let $[(U, g)] \in \mathscr{G}_P$, and let $(U_i)_{i \in I}$ be an open cover of U, with $f_i \in \mathscr{F}(U_i)$ such that $\rho_{U_i}^U(g) = \varphi_{U_i}(g_i)$. Since the U_i cover U, at least one of them, say U_1, contains P. Then $[(U_1, f_1)]$ is an element of $\mathscr{F}_P$ whose image under φ_P equals $[(U_1, g_1)] = [(U, g)]$ in $\mathscr{G}$.

Conversely, suppose that all φ_P are surjective. We will show that φ is locally surjective, which suffices by Theorem 1.4.10. Let (U, g) be given. Because the φ_P are surjective, we can for any point $P \in U$ find an open set U_P containing P and an $f_P \in \mathscr{F}(U_P)$ such that $\varphi_{U_P}(f_P)$ equals $\rho_{U_P}^U(g)$. Since the U_P cover U, this proves local surjectivity. □

Example 1.5.10. It is crucial for Proposition 1.5.4 that F and G be sheaves instead of mere presheaves. Indeed, consider the following example. Let X be the topological space from Example 1.3.33, and consider the sheaf F defined by the commutative diagram

$$\begin{tikzcd} & 0 \arrow[dr] & \\ \mathbb{Z} \arrow[ur, "1"] \arrow[dr, "1"'] & & 0 \\ & 0 \arrow[ur] & \end{tikzcd} \tag{1.5.11}$$

Then all stalks of F are trivial, so the zero map to the trivial sheaf $G = 0$ induces isomorphisms on stalks. However, this zero map $0 : F \to G$ is not an isomorphism, since the map $F(X) \to G(X) = 0$ is not an isomorphism in $\mathfrak{Ab}$. Note that F^+ is the trivial sheaf!

Example 1.5.12. Even if F and G are both sheaves, then $\mathscr{F}_P \cong \mathscr{G}_P$ for all P does not imply that $\mathscr{F} \cong \mathscr{G}$. We will see plenty of examples to the contrary when discussing line bundles later in these notes, but here is another example with the topological space X from Example 1.3.33.

For now, consider the topological space $X = \{O, C\}$ with open sets $\emptyset, U = \{O\}$, and $\{O, C\} = X$. Then giving a sheaf of abelian groups is the same as giving a homomorphism of abelian groups

$$A \to B \tag{1.5.13}$$

Indeed, given a sheaf F on X, we obtain a homomorphism (1.5.13), namely the restriction $F(X) \to F(U)$, and conversely, given a homomorphism (1.5.13), we can define a corresponding sheaf by defining $F(X) = A$, $F(U) = B$, and $F(\emptyset) = 0$, where all restriction maps are zero except for $F(X) \to F(U)$, which is the specified homomorphism $A \to B$.

Now given a homomorphism $A \to B$, the stalk of the corresponding stalks at the points O and C are both simply B, since for both points there is a smallest open set that contains them, to wit U. Therefore the two homomorphisms

$$\mathbb{Z}/2\mathbb{Z} \xrightarrow{1} \mathbb{Z}/2\mathbb{Z} \tag{1.5.14}$$

and

$$\mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \tag{1.5.15}$$

both define sheaves with stalk $\mathbb{Z}/2\mathbb{Z}$ at the points of X. Yet these sheaves are not isomorphic, since only one of them has the property that all its restriction maps are zero.

We now consider how to transport sheaves along continuous maps in both directions.

Definition 1.5.16. Let $\varphi : X \to Y$ be a continuous map of topological spaces, let $\mathscr{F} \in \mathfrak{Sh}_X$, and let $\mathscr{G} \in \mathfrak{Sh}_Y$. We define the pushforward of $\mathscr{F}$ along φ to be the sheaf $\varphi_*(\mathscr{F})$ on Y with

$$\varphi_*(\mathscr{F})(V) = \mathscr{F}(\varphi^{-1}(V)). \tag{1.5.17}$$

Moreover, given an inclusion $V_1 \subset V_2$, we define the corresponding restriction map of $\varphi_*(\mathscr{F})$ to be the map $\rho^{\varphi^{-1}(V_2)}_{\varphi^{-1}(V_1)} : \mathscr{F}(\varphi^{-1}(V_2)) \to \mathscr{F}(\varphi^{-1}(V_1))$ that comes from $\mathscr{F}$.

The pullback of $\mathscr{G}$ along φ is the sheaf $\varphi^{-1}(\mathscr{G})$ associated to the presheaf (!) that associates to an open $U \subset X$ the abelian group

$$\lim_{\varphi^{-1}(V) \subset U} \mathscr{G}(V) = \{(V, g) : \varphi^{-1}(V) \subset U, g \in \mathscr{G}(V)\}/\sim. \tag{1.5.18}$$

Here the equivalence relation $(V_1, g_1) \sim (V_2, g_2)$ is defined by the property that the restrictions of g_1 and g_2 to $V_1 \cap V_2$ coincide.

Remark 1.5.19. In fact $\varphi^{-1} : \mathfrak{Sh}_Y \to \mathfrak{Sh}_X$ is a functor, and so is $\varphi_* : \mathfrak{Sh}_X \to \mathfrak{Sh}_Y$, to which φ^{-1} is a left adjoint. This follows from the adjunction in Proposition 1.4.10 because the presheaf with sections (1.5.18) is a left adjoint to $\varphi_* : \mathfrak{PreSh}_X \to \mathfrak{PreSh}_Y$. However, it is completely safe to ignore this rather daunting technicality if you feel so inclined. In the future we will replace φ^{-1} by a much simpler adjoint in the context of line bundles.

Just like we can consider sheaves of abelian groups on a topological space X, we can consider sheaves of rings $\mathscr{F}$ on X; we simply demand that all $\mathscr{F}(U)$ are (commutative) rings and that all restriction maps are ring homomorphisms. In that case all stalks $\mathscr{F}_P$ are again rings in a natural way, as you will prove in the exercises.

Definition 1.5.20. Let R be a ring. Then R is called a local ring if it admits a unique maximal ideal. This is equivalent to demanding that the set of non-units $R \setminus R^*$ of R forms an ideal.

We now come to the fundamental definition of this first part of the notes.

Definition 1.5.21. A ringed space is a pair $(X, \mathscr{O}_X)$, where X is a topological space and where $\mathscr{O}_X$ is a sheaf of rings on X called the structure sheaf of the locally ringed space $(X, \mathscr{O}_X)$ (or, abusively, of X). A morphism of ringed spaces $(X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ is a pair $(\varphi, \varphi^\#)$, where $\varphi : X \to Y$ is a continuous map and where $\varphi^\# : \mathscr{O}_Y \to \varphi_* \mathscr{O}_X$ is a morphism of sheaves on Y.

The map $\varphi^\#$ induces maps on stalks

$$\begin{aligned} \varphi_P^\# : \mathscr{O}_{Y,\varphi(P)} &\to \mathscr{O}_{X,P} \\ [(V, g)] &\mapsto (\varphi^{-1}(V), \varphi^\#(g)). \end{aligned} \tag{1.5.22}$$

A locally ringed space is a ringed space $(X, \mathscr{O}_X)$ with the property that all stalks $\mathscr{O}_{X,P}$ are local rings, with unique maximal ideal $\mathfrak{m}_{X,P}$ say. A morphism of locally ringed spaces $(X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ is a morphism of locally ringed spaces $(\varphi, \varphi^\#)$ such that all maps $\varphi_P^\#$ are local homomorphisms, in the sense that

$$(\varphi_P^\#)^{-1}(\mathfrak{m}_{X,P}) = \mathfrak{m}_{Y,\varphi(P)} \tag{1.5.23}$$

for all $P \in X$.

Remark 1.5.24. The inclusion $(\varphi_P^\#)^{-1}(\mathfrak{m}_{X,P}) \subset \mathfrak{m}_{Y,\varphi(P)}$ is always satisfied; indeed, no element of $\mathfrak{m}_{X,P}$ can have preimage a unit, since the image of a unit under $\varphi_P^\#$ is again a unit and therefore not in $\mathfrak{m}_{Y,\varphi(P)}$. A formal argument shows that the reverse inclusion $(\varphi_P^\#)^{-1}(\mathfrak{m}_{X,P}) \supset \mathfrak{m}_{Y,\varphi(P)}$ is equivalent to $\varphi_P^\#(\mathfrak{m}_{Y,\varphi(P)}) \subset \mathfrak{m}_{X,P}$.

Intuitively, $\mathscr{O}_X$ is a sheaf of function on X of some kind; we will see concrete examples of this later. Given P, the stalk $\mathscr{O}_{X,P}$ can be thought of as germ of functions defined in some neighborhood of P, and the ideal $\mathfrak{m}_{X,P}$ as those germs of functions that vanish in P. So a locally ringed space is one in which any function $\varphi \in \mathscr{O}_X(U)$ that does not vanish in P admits a multiplicative inverse (V, g) for some open subset V of U that still contains P.

On the same intuitive level, the morphism of sheaves $\varphi^\#$ encodes the pullback of functions from opens of Y to opens of X obtained by composing with φ, and similarly the maps $\varphi_P^\#$ encode the pullback of function germs. The inclusion $(\varphi_P^\#)^{-1}(\mathfrak{m}_{X,P}) \subset \mathfrak{m}_{Y,\varphi(P)}$ comes down to the property that any function germ on Y around $\varphi(P)$ whose pullback to a function germ around P vanishes at P vanishes at $\varphi(P)$ itself, which is in line with our interpretation in terms of composing with φ. The converse inclusion amounts to stating that if a function germ on Y around $\varphi(P)$ vanishes at $\varphi(P)$, then the pullback of this germ to a germ on X around P vanishes at P as well. Of course this is mere intuition; the definitions allow for generalizations of sheaves beyond the functions that we are used to. Still, it is what motivates the definitions.

The next section will explain what all these constructions are good for.

1.6 Relation with classical constructions

In analysis, you will likely have seen the implicit function theorem. The context in which it is applied is as follows. Given a smooth function

$$F : \mathbb{R}^n \to \mathbb{R}^m \tag{1.6.1}$$

we can consider at the zero locus

$$X = V(F) := \{x \in \mathbb{R}^n : F(x) = 0\} \tag{1.6.2}$$

of F in $\mathbb{R}^n$. The implicit function theorem states a necessary and sufficient condition for X to be smooth at one of its points P, namely that the Jacobian matrix

$$DF(P) = \left(\frac{\partial F_i}{\partial x_j}(P)\right)_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} \tag{1.6.3}$$

has full rank m. If this condition holds, then we know more. Let us assume, without loss of generality, that the last m columns of $DF(P)$ are independent. Then there is a neighborhood U of P such that the projection

$$\pi : X \to \mathbb{R}^{n-m} \tag{1.6.4}$$

on the first $n-m$ coordinates is a smooth homeomorphism from U to an open set V in $\mathbb{R}^m$. Moreover, there is a function

$$g : V \to U \subset \mathbb{R}^m \tag{1.6.5}$$

such that the inverse of π on V is given by

$$y = (y_1, \ldots, y_{n-m}) \mapsto (y_1, \ldots, y_{n-m}, g_1(y), \ldots, g_m(y)). \tag{1.6.6}$$

We see that if the differential DF has full rank everywhere on X, then the functions π and g give us a way to parametrize the "patches" U of X. Such functions are also called charts. It allows us to generalize the smooth surfaces defined by a single function F. Yet perhaps we could more conveniently describe X by different equations on different patches! Heck, we might not even want to think of X as living in some larger ambient $\mathbb{R}^n$, but simply as an object by itself, obtained by smoothly "gluing" suitable patches. This leads to the following definition.

Definition 1.6.7. A *smooth manifold of dimension n* is a topological space X together with an open cover $(U_i)_{i\in I}$ of X and injective homeomorphisms $\varphi_i : U_i \to \mathbb{R}^n$ onto an open V_i in $\mathbb{R}^n$ with the property that for all i, j the map

$$\varphi_j \circ \varphi_i^{-1} : \varphi_i(U_i \cap U_j) \to \varphi_j(U_i \cap U_j) \tag{1.6.8}$$

is a smooth homeomorphism. The collection (U_i, φ_i) is called a smooth atlas on X.

This notion already gives us quite a bit of flexibility, essentially because we define smooth manifolds by local properties only. This allows them to have exotic global behavior. For example, there are smooth surfaces such as the Klein bottle that cannot be embedded into $\mathbb{R}^3$, although all of its local charts can be.

Note that we have not insisted on smoothness of the $\varphi_i : U_i \to V_i \subset \mathbb{R}^n$. In fact, that is part of the whole setup: We cannot make sense of this a priori because we do not assume X to be a subset of some $\mathbb{R}^n$, so we can only consider smoothness of the transition maps $\varphi_j \circ \varphi_i^{-1}$!

However, the presence of an atlas still allows us to unambiguously define the notion of a smooth function on X. Let $f : X \to \mathbb{R}$ be a function on X. In the classical case at the beginning of this section, one sees that f is smooth exactly if all $f \circ \varphi_i^{-1}$ are smooth. This is essentially because of the fact that smoothness of f at a point $P \in X$ is determined by the local behavior of f in a small subset containing P.

In the more general situation, we simply define a function $f : X \to \mathbb{R}$ to be smooth if and only if all compositions

$$f \circ \varphi_i^{-1} \tag{1.6.9}$$

This notion does not depend on the choice of i since on $U_i \circ U_j$ we have

$$(f \circ \varphi_j^{-1}) \circ (\varphi_j \circ \varphi_i^{-1}) = (f \circ \varphi_i^{-1}) \tag{1.6.10}$$

and $\varphi_j \circ \varphi_i^{-1}$ is smooth. In this way we get a well-defined subsheaf of the sheaf of all functions on X, equipped with which X becomes a locally ringed space of a certain special kind. Before formalizing this discovery, we need a definition.

Definition 1.6.11. Let X be a topological space and let $\mathscr{F} \in \mathfrak{Sh}_X$. Let U be an open subset of X. Then we can define the restriction $\mathscr{F}|_U \in \mathfrak{Sh}_U$ of $\mathscr{F}$ to U by

$$\mathscr{F}|_U(V) = \mathscr{F}(V) \tag{1.6.12}$$

for all $V \subset U$, with the same restriction maps as $\mathscr{F}$. (It is in fact nothing but the pullback (1.5.18) of $\mathscr{F}$ by the inclusion of U into X.)

We can now define a smooth manifold in terms of locally ringed spaces:

Definition 1.6.13. A smooth manifold of dimension n is a locally ringed space $(X, \mathscr{O}_X)$ with the property that there exists a cover $X = \bigcup_i U_i$ of X such that for all i we have

$$(U_i, \mathscr{O}_X|_{U_i}) \cong (V_i, \mathscr{C}^\infty_{\mathbb{R}^n}|_{V_i}) \tag{1.6.14}$$

for some open subset $V_i \in \mathbb{R}^n$. Here $\mathscr{C}^\infty_{\mathbb{R}^n}|_{V_i}$ is the sheaf of smooth functions on $V_i \subset \mathbb{R}^n$.

This definition of a smooth manifold is the more intrinsic of the two. After all, it does not depend on a privileged choice of open sets U_i and homeomorphisms φ_i. Of course we have to check that these definitions are essentially equivalent.

Proposition 1.6.15. *A smooth manifold in the sense of Definition 1.6.7 gives rise to a unique smooth manifold in the sense of Definition 1.6.13. Conversely, a manifold in the sense of Definition 1.6.13 gives rise to a smooth atlas in the sense of Definition 1.6.7.*

Proof. The discussion before the Proposition shows its first part: If we take the cover $(U_i)_{i \in I}$ defined by an atlas of X, then there is an isomorphism

$$(U_i, \mathscr{O}_X|_{U_i}) \cong (V_i, \mathscr{C}^\infty_{\mathbb{R}^n}|_{V_i}) \tag{1.6.16}$$

given by $(\varphi_i, \varphi_i^\#)$. Here we take

$$\begin{aligned} \varphi_i^\# : \mathscr{C}^\infty_{\mathbb{R}^n}|_{V_i}(W) &\to \mathscr{O}_X|_{U_i}(\varphi_i^{-1}(W)) \\ f &\mapsto f \circ \varphi_i \end{aligned} \tag{1.6.17}$$

which is well-defined by our very construction of $\mathscr{O}_X$.

Conversely, suppose that we are given a smooth manifold in the sense of Definition 1.6.13. Let $(U_i)_{i\in I}$ be an open cover of X. Then by taking compositions of the restriction of the maps in (1.6.14) we get isomorphisms

$$(\varphi_{i,j},\varphi_{i,j}^{\#}) = (\varphi_i(U_i\cap U_j),\mathscr{C}^\infty_{\mathbb{R}^n}|_{\varphi_i(U_i\cap U_j)}) \cong (\varphi_j(U_i\cap U_j),\mathscr{C}^\infty_{\mathbb{R}^n}|_{\varphi_j(U_i\cap U_j)}). \tag{1.6.18}$$

If we can show that the sheaf morphism $\varphi_{i,j}^{\#}$ is induced by composition with $\varphi_{i,j}=\varphi_j\circ\varphi_i^{-1}$, then this will in particular imply that the composition of the inclusion of $\varphi_i(U_i\cap U_j)$ into $\mathbb{R}^n$ with $\varphi_{i,j}$ is smooth. In turn, that will show the smoothness of the map $\varphi_{i,j}$, so that (U_i,φ_i) is indeed an atlas.

So we show that for any two subsets U,V of $\mathbb{R}^n$, an isomorphism

$$(\varphi,\varphi^{\#}) : (U,\mathscr{C}^\infty_{\mathbb{R}^n}|_U) \to (V,\mathscr{C}^\infty_{\mathbb{R}^n}|_V) \tag{1.6.19}$$

has the property that the sheaf map $\varphi^{\#}:\mathscr{O}_V\to\varphi^*(\mathscr{O}_U)$ is induced by composition with φ. We sketch the proof of this statement

(i) One first shows that the constant functions with values in $\mathbb{Q}$ are fixed because all $\varphi^{\#}$ are ring homomorphisms;

(ii) One then shows that $\varphi_U^{\#}(g-g(Q))$ is 0 in $P=\varphi^{-1}(Q)$ because $(\varphi,\varphi^{\#})$ is a morphism of locally ringed spaces, and conclude that $\varphi_U^{\#}(g)$ has value $g(Q)$ in P as well;

(iii) Finally, one shows the desired result by using denseness of $\mathbb{Q}$ in $\mathbb{R}$ and the fact that $\varphi^{\#}$ maps smooth functions to smooth functions.

We do not show that the constructions in the previous proposition are essentially inverse to one another. Suffice to state that they indeed are. □

Similarly, asking that $(X,\mathscr{O}_X)$ be locally isomorphic to $(V_i,\mathscr{C}^k_{\mathbb{R}^n}|_{V_i})$ gives us the category of k-fold differentiable manifolds of dimension n, while asking that it be locally isomorphic to $(V_i,\mathscr{C}^{\mathrm{hol}}_{\mathbb{C}^n}|_{V_i})$ for some $V_i\subset\mathbb{C}^n$ gives us the category of n-dimensional complex manifolds.

Remark 1.6.20. In contrast with the proof of Proposition 1.6.15, the sheaf of holomorphic functions

$$(\mathbb{C}^n,\mathscr{C}^{\mathrm{hol}}_{\mathbb{C}^n}) \tag{1.6.21}$$

has an automorphism that does *not* come from composition with holomorphic functions, namely the complex conjugation that sends a holomorphic function f with local power series development

$$f=\sum_{n=0}^{\infty}a_nz^n \tag{1.6.22}$$

to its conjugate

$$\overline{f}=\sum_{n=0}^{\infty}\overline{a}_nz^n. \tag{1.6.23}$$

This is possible because said conjugation is the unique non-trivial smooth field automorphism of the field of constants $\mathbb{C}$.

Our use for sheaves

Developing this theory is not just for fun. In algebraic geometry, the use of sheaves is especially important. The reason that we will not have simple building blocks as above (essentially one for any given dimension n) at our disposal. In a very imprecise nutshell, here is what goes wrong with the language of building blocks in an algebraic context.

Issue 1: We need larger open sets

Part of what makes algebraic geometry algebraic is that we only consider a very small sheaf of functions, namely the rational functions, which are functions that can be described locally as the quotient of polynomials. On $\mathbb{C}$, this means that we consider, given an open U, the ring

$$\mathscr{O}_X(U) = \{\text{simplified rational expressions } f(x) = p(x)/q(x) \text{ with } q(x) \neq 0 \text{ on } U\}. \quad (1.6.24)$$

This is a great presheaf on $\mathbb{C}$. Unfortunately, it is not a sheaf with respect to the usual analytic topology. Indeed, if we take two disjoint opens U_1 and U_2 and arbitrary functions f_1 and f_2 on U_1 and U_2, then it is very unlikely that f_1 and f_2 glue to give a rational function on $U_1 \cup U_2$. We already see this problem for the very simple case $f_1 = 1$, $f_2 = 2$. Another non-intuitive property for rational functions is the following.

Proposition 1.6.25. *Let f_1, f_2 be two rational functions on $\mathbb{C}$ that coincide on some non-empty open set. Then $f_1 = f_2$.*

Proof. Write $f_1 = p_1/q_1$, $f_2 = p_2/q_1$. Then $p_2 q_1 = p_1 q_2$ on an open. However, a polynomial over $\mathbb{C}$ has only finitely many zeros. This means that $p_2 q_1 = p_1 q_2$ as polynomials, and therefore $f_1 = f_2$. □

The first of these phenomena also shows the way out: If we simply introduce some topology in which there are no disjoint open sets, then the presheaf of rational functions may still be a sheaf after all! The right thing to do turns out to be to consider the cofinite topology, or in other words the Zariski topology, whose opens are given by

$$D(f) = \mathbb{C} - \{x : f(x) = 0\} \quad (1.6.26)$$

as f runs over the polynomials in one variable. With respect to this topology, $\mathscr{O}_X$ does form a sheaf, as we will show.

Issue 2: We need more building blocks

This tells us something about our sheaves of functions. But what will our spaces be? Well, instead of considering the zero loci of general smooth functions, we will considering the zero loci of polynomial functions, such as

$$X : y^2 = x^5 - x^2 + x. \quad (1.6.27)$$

A considerable complication is that although the derivative matrix of $y^2 - (x^5 - x^2 + x)$ has only non-zero entries in $(1,1)$, there is no *rational* function $y(x)$ defined in a neighborhood of $x = 1$ such that $y(x)^2 = x^5 - x^2 + x$. In particular, there is no way to *rationally* parametrize an open part of the solution set. In other words, the implicit function theorem does not apply in algebraic geometry, and we cannot get by with "standard" building blocks only.

The way out: commutative algebra

Because of the problems above, we have to spend some thought towards developing general machinery that delivers building blocks that are still flexible enough to get a decent building off the ground. Amazingly enough, theory from commutative algebra implies that such machinery does exist. With it, we can construct locally ringed spaces that locally look like sheaves of rational functions on sets defined by polynomial equations. These locally ringed space are called algebraic varieties, and they are the theme of the next chapter.

Chapter 2

Words

In line with the philosophy of the first chapter, we define what algebraic geometry is by means of the topological spaces and the functions that we consider. The topological spaces are algebraic varieties, that is, zero sets of polynomial equations that are "irreducible" in some precisely defined sense. The functions on these spaces are those that admit a local description as rational functions, that is, as quotients of polynomials. Finally, in line with the definition of a locally ringed space, we define morphisms between algebraic varieties to be maps that induce well-defined pullbacks for the aforementioned functions.
Unwinding all of these statements is far from trivial, and we spend some chapters on this. Some concepts simplify under this yoga; for example, it turns out that morphisms are functions between algebraic varieties whose coordinates can be described by means of rational functions.
We also define dimension and non-singularity in the algebraic-geometric context. This allows us to define algebraic curves (which are non-singular algebraic varieties of dimension 1) and their projective completions. These amazing geometric objects are the theme of the rest of these notes.

2.1 The Zariski topology

Let k be an algebraically closed field. Throughout this course, it is useful to think of $k = \mathbb{C}$, although the theory that we develop will apply more generally. We will start this chapter by defining the building blocks for algebraic varieties that we need. In analogy with the case of smooth and complex manifolds, these building blocks will be open subsets of k^n, but with respect to a new topology, which we introduce after first defining some general notions.

Definition 2.1.1. Let n be a strictly positive integer. We define affine n-space $\mathbb{A}^n_k$ over k (usually abbreviated to $\mathbb{A}^n$ when k is clear from the context) to be the set of n-tuples of elements of k, so

$$\mathbb{A}^n_k = \{(a_1, \ldots, a_n) : a_i \in k\}. \tag{2.1.2}$$

We usually denote a given tuple $(a_1, \ldots, a_n)$ by P.

We now consider special subsets of $\mathbb{A}^n$, namely those that are obtained as the common zeros of some subset of $k[x_1, \ldots, x_n]$. We also call the latter ring the coordinate ring of $\mathbb{A}^n$.

Definition 2.1.3. Let S be a subset of $k[x_1,\dots,x_n]$. We define the zero locus $V(S)$ of S in $\mathbb{A}^n$ to be the set of common zeros of the elements of S. In other words, we have

$$V(S) = \{P = (a_1,\dots,a_n) \in \mathbb{A}^n \mid f(P) := f(a_1,\dots,a_n) = 0 \text{ for all } f \in S\} \tag{2.1.4}$$

If Y is a subset of $\mathbb{A}^n$, then we say that Y is *algebraic* if we have $Y = V(S)$ for some subset S of $\mathbb{A}^n$.

We have studied such sets in our course on algebra, to which we will occasionally refer [4]. The first important observation is the following.

Proposition 2.1.5. *Let $S \subset k[x_1,\dots,x_n]$, and let $\mathfrak{a} = \langle S \rangle$ be the ideal of $k[x_1,\dots,x_n]$ generated by S. Then we have $V(S) = V(\mathfrak{a})$.*

Proof. Let $P \in V(\mathfrak{a})$. Then $f(P) = 0$ for all $f \in \mathfrak{a}$, so certainly $f(P) = 0$ for all $f \in S$. Therefore $P \in V(S)$. Since this holds for all points $P \in V(\mathfrak{a})$, we have shown the inclusion $V(\mathfrak{a}) \subset V(S)$. (In fact this argument shows equally well that $V(T) \subset V(S)$ whenever $S \subset T$.)

Conversely, suppose that $P \in S$, so that $f(P) = 0$ for all $f \in S$. Let $g \in \mathfrak{a}$. Then by definition of $\langle S \rangle$ there exists a finite subset S' of S such that

$$g = \sum_{f \in S'} c_f f, \tag{2.1.6}$$

where $c_f \in k[x_1,\dots,x_n]$ for all $f \in S'$. Therefore

$$g(P) = \sum_{f \in S'} c_f(P) f(P) = \sum_{f \in S'} c_f(P) \cdot 0 = 0. \tag{2.1.7}$$

Since this argument applies for all elements $g \in \mathfrak{a}$, we see that $P \in V(\mathfrak{a})$. And in turn, since this holds for all points $P \in V(\mathfrak{a})$, we have shown the inclusion $V(S) \subset V(\mathfrak{a})$. The proposition is proved. $\square$

Proposition 2.1.5 implies that every algebraic subset $\mathbb{A}^n$ in fact admits a description $Z = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $\mathbb{A}^n$. We will often still use descriptions $Z = V(S)$ for more general subset S of $k[x_1,\dots,x_n]$, in particular when $Z = V(f)$ is a principal closed set, that is, when Z is the zero locus of a single polynomial $f \in k[x_1,\dots,x_n]$. In fact, Proposition 2.1.5 can be combined with the Hilbert Nullstellensatz to show the following strong (and far from obvious) statement on algebraic sets:

Proposition 2.1.8. *Let $Z \subset \mathbb{A}^n$ be an algebraic set. Then there exists a* finite *set $S = \{f_1,\dots,f_r\}$ of elements of $k[x_1,\dots,x_n]$ such that we have*

$$Z = V(S) = V(f_1,\dots,f_r). \tag{2.1.9}$$

Proof. By definition, we have $Z = V(T)$ for some subset T of $k[x_1,\dots,x_n]$, and Proposition 2.1.5 shows that $Z = V(\mathfrak{a})$ for the ideal $\mathfrak{a}$ of $k[x_1,\dots,x_n]$ generated by T. The Hilbert Basis Theorem [4, Theorem 6.1.11] shows that there exists a finite subset S of $k[x_1,\dots,x_n]$ such that $\mathfrak{a} = \langle S \rangle$. Another application of Proposition 2.1.5 then shows that $Z = V(S)$. $\square$

We see that the Hilbert Basis Theorem is an algebraic result with a very concrete interpretation; it shows that the algebraic subsets of $\mathbb{A}^n$ are exactly those subsets Y that admit a description as the set of solutions $(a_1,\dots a_n)$ of a finite system of multivariate equations in the n variables $x_1,\dots,x_n$:

$$Y:\begin{cases} f_1(x_1,\dots,x_n) & = & 0,\\ \quad\vdots & & \vdots\\ f_r(x_1,\dots,x_n) & = & 0.\end{cases} \tag{2.1.10}$$

The following properties of algebraic subsets of $\mathbb{A}^n$ are proved as in [2, Proposition I.1.1]:

Proposition 2.1.11.

(i) The empty set $\emptyset$ and $\mathbb{A}^n$ itself are algebraic subsets of $\mathbb{A}^n$.

(ii) If Z_1 and Z_2 are algebraic subsets of $\mathbb{A}^n$, then so is their union $Z_1 \cup Z_2$.

(iii) If $(Z_i)_{i\in I}$ is a family of algebraic subsets of $\mathbb{A}^n$, then their intersection $\bigcap_{i\in I} Z_i$ is an algebraic subset of $\mathbb{A}^n$ as well.

Proof. (i): We have $\emptyset = V(1)$ and $\mathbb{A}^n = V(0)$.

(ii): By hypothesis, we can write $Z_1 = V(S_1)$ and $Z_2 = V(S_2)$, where S_1 and S_2 are subsets of $k[x_1,\dots,x_n]$. Define

$$T = S_1S_2 = \{f_1f_2 \,|\, f_1 \in S_1, f_2 \in S_2\}. \tag{2.1.12}$$

Then we have $Z_1\cup Z_2 = V(T)$. Indeed, suppose that $P \in Z_1\cup Z_2$. We may then assume $P \in Z_1$ by symmetry. Then $f_1(P) = 0$ for all $f_1 \in S_1$, so we also have $(f_1f_2)(P) = f_1(P)f_2(P) = 0f_2(P) = 0$ for all $f_1 \in S_1$ and $f_2 \in S_2$, which shows that $P \in V(T)$. Conversely, suppose that $P \in V(T)$. If $P \in Z_1 = V(S_1)$, then we are done. If not, then there exists an element g_1 of S with $g_1(P) \neq 0$. On the other hand, we have $f_1(P)f_2(P) = (f_1f_2)(P) = 0$ for all $f_1 \in S_1$ and $f_2 \in S_2$ by our assumption that $P \in V(T)$, so in particular we have $g_1(P)f_2(P) = 0$ for all $f_2 \in S$. Since $g_1(P) \neq 0$, this shows that $f_2(P) = 0$ for all $f_2 \in S_2$. This shows that $P \in V(S_2) = Z_2$, as desired.

(iii): By hypothesis, we can write $Z_i = V(S_i)$ for all $i \in I$ as in Part (ii). Given $i \in I$, let us write the elements of S_i as $f_{i,j}$, where j runs through some index set J_i that depends on $i \in I$. We show that we can write $Z = \bigcap_{i\in I} Z_i$ as $V(T)$, where

$$T = \bigcup_{i\in I} S_i. \tag{2.1.13}$$

Indeed, suppose that $P \in Z$. Then $T \in Z_i$ for all $i \in I$, so that $f_{i,j}(P) = 0$ for all $j \in J_i$. Since the elements of T are exactly the polynomials $f_{i,j}$ with $i \in I$ and $j \in J_i$, we see that $P \in V(T)$. Conversely, if $P \in V(T)$, then by definition $f(P) = 0$ for all $f \in T$, which means that $f_{i,j}(P) = 0$ for all $i \in I$ and all $j \in J_i$. Combining these statements for a fixed $i \in I$, we see that $P \in V(S_i)$ for all $i \in I$. This implies $P \in V(T)$. □

Example 2.1.14. Consider the affine plane $\mathbb{A}^2_k$, which has the three lines

$$\begin{aligned} Z_1 &= V(x_1),\\ Z_2 &= V(x_2),\\ Z_3 &= V(x_2-1)\end{aligned} \tag{2.1.15}$$

as algebraic subsets. The union $Z_1\cup Z_2$ of the two lines Z_1 and Z_2 is again algebraic, because it is the zero locus of the function x_1x_2, in line with the proof of Proposition 2.1.11. The intersection $Z_1\cap Z_2$ is also algebraic, because it is the common zero locus of the two functions x_1 and x_2. In other words, we have

$$Z_1\cap Z_2 = V(x_1,x_2) = \{(0,0)\}, \tag{2.1.16}$$

where we slightly abuse notation by writing $V(x_1,x_2)$ where actually $V(\{x_1,x_2\})$ is meant. (We also did then when we defined the principal closed subset $V(f)$, which strictly speaking should be written as $V(\{f\}$. It can be shown that we cannot write $Z_1 \cap Z_2 = V(f)$ for a single polynomial $f \in k[x_1,x_2]$.

Now consider the set

$$Z = (Z_1 \cap Z_2) \cup (Z_1 \cap Z_3) = \{(0,0),(1,0)\}. \tag{2.1.17}$$

The proof of Proposition shows how to write Z as an algebraic subset of $\mathbb{A}^n$: We have $(Z_1 \cap Z_2) = V(x_1,x_2)$ and $(Z_1 \cap Z_3) = V(x_1,x_3)$, so that Z is the zero locus of the set T_1 of mutual products of the elements of the sets $S_1 = (x_1,x_2)$ and $S_2 = (x_1,x_3)$. That is, we have

$$T_1 = V(x_1^2, x_1x_2, x_1(x_2-x_1), x_2(x_2-1)). \tag{2.1.18}$$

Alternatively, we can write $Z = Z_1 \cap (Z_2 \cup Z_3)$. Since $Z_1 = V(x_1)$ an $Z_2 \cup Z_3 = V(x_2(x_2-1))$, this leads to the alternative presentation $Z = V(T_2)$, where this time

$$T_2 = V(x_1, x_2(x_2-x_1)). \tag{2.1.19}$$

This concrete example shows that there are in general multiple ways to describe a given subset of $\mathbb{A}_k^2$ as an algebraic subset (if it indeed is one), and that some of these descriptions are simpler than others.

Proposition 2.1.11 is reminiscent of the properties of open sets. This is no coincidence:

Proposition 2.1.20. *Let $\mathcal{U}$ be the set of subsets U of $\mathbb{A}^n$ that are of the form*

$$U = \mathbb{A}^n - V(S) \tag{2.1.21}$$

for some subset S of $k[x_1,\dots,x_n]$. Then $\mathcal{U}$ is a topology on $\mathbb{A}^n$.

Proof. This is a direct consequence of applying De Morgan's laws to the statements of Proposition 2.1.11: Part (i) shows that $\emptyset, \mathbb{A}^n \in \mathcal{U}$, Part (ii) shows that a finite intersection of elements of $\mathcal{U}$ is again in $\mathcal{U}$, and Part (iii) shows that arbitrary unions of elements of $\mathcal{U}$ are in $\mathcal{U}$. □

Definition 2.1.22. We call the topology on $\mathbb{A}^n$ from Proposition 2.1.11 the Zariski topology.

Example 2.1.23. Let us consider the Zariski topology on $\mathbb{A}^1$. Suppose first that $Z = V(S) \subset \mathbb{A}^n$ is an algebraic set that. If $S \subset \{0\}$, then we have that $V(S) = \mathbb{A}^1$. So suppose that $V(S)$ contains a non-zero element $f \in k[x_1]$. Then $V(S)$ is contained in $V(f)$, as we saw in the proof of Proposition 2.1.5. Now note that a non-zero univariate polynomial has at most finitely many zeros. This implies that a non-trivial algebraic subset of $\mathbb{A}^1$ is finite.

Conversely, if $Y = \{a_1,\dots,a_r\} \subset \mathbb{A}^n$ is a finite subset of $\mathbb{A}^1$, then we have $Y = V(f)$ for $f = (x_1-a_1)\cdots(x_1-a_r)$. This shows that the proper algebraic subsets of $\mathbb{A}^1$ are exactly the finite subsets of $\mathbb{A}^1$. Taking complements, we see that the Zariski topology on $\mathbb{A}^1$ is the cofinite topology, that is, the topology of $\mathbb{A}^1$ whose open subsets are $\emptyset, \mathbb{A}^1$, and the subsets of $\mathbb{A}^1$ whose complement is finite.

For general affine n-space $\mathbb{A}^n$, the topology does not admit as compact a description as in the previous example. However, there is still one useful observation to make. For this, we define the principal open subset $D(f)$ of $\mathbb{A}^n$ corresponding to an element $f \in k[x_1,\dots,x_n]$ as

$$D(f) = \mathbb{A}^n - V(f). \tag{2.1.24}$$

Lemma 2.1.25. *The principal open sets $D(f)$ form a basis of the topology of $\mathbb{A}^n$. That is, every open subset of $\mathbb{A}^n$ is a union of principal open subsets.*

Proof. Let $U = \mathbb{A}^n - V(S)$ be an algebraic subset. Proposition 2.1.8 shows that we may assume $S = \{f_1, \dots, f_r\}$ to be finite. Then

$$V(S) = V(f_1) \cap \ldots \cap V(f_s) \tag{2.1.26}$$

so that De Morgan's laws show that

$$U = \mathbb{A}^n - V(S) = (\mathbb{A}^n - V(f_1)) \cup \ldots \cup (\mathbb{A}^n - V(f_r)) = D(f_1) \cup \ldots \cup D(f_r). \tag{2.1.27}$$

Since U was arbitrary, the proposition is proved. In fact we have even shown that every open subset of $\mathbb{A}^n$ is a *finite* union of principal open subsets. □

Example 2.1.28. The cofinite Zariski topology on $\mathbb{A}^1$ considered in Example 2.1.23 is likely coarser than topologies to which you are used so far, in that it contains only very large open subsets. In fact, this topology is not even Hausdorff. That is, given points P_1 and P_2 of $\mathbb{A}^1$, we cannot find open subsets U_1 and U_2 with $P_1 \in U_1$ and $P_2 \in U_2$ such that $U_1 \cap U_2 = \emptyset$. Indeed, *any* two non-empty open subsets U_1, U_2 of $\mathbb{A}^1$ intersect!

To see this, choose non-empty principal open subsets $D(f_1)$ and $D(f_2)$ that are contained in U_1 and U_2, respectively. Then as in the proof of Lemma 2.1.25 we see that $D(f_1) \cap D(f_2) = D(f_1 f_2)$. Since the open subsets $D(f_1)$ and $D(f_2)$ of $\mathbb{A}^1$ are non-empty, we have $f_1 \neq 0$ and $f_2 \neq 0$. Therefore the intersection $D(f_1 f_2)$ is non-empty because the non-zero polynomial $f_1 f_2$ only has finitely many zeros and the base field k, which we supposed to be algebraically closed, is infinite.

Remark 2.1.29. As in the case of $\mathbb{A}^1$, the topology on $\mathbb{A}^n$ is not Hausdorff. The proof of this statement requires the Nullstellensatz, which we prove in the next section.

2.2 Varieties and the Nullstellensatz

In order to define the building blocks that we mentioned in Section 1.6, we introduce one more topological notion.

Definition 2.2.1. Let X be a topological space, and let Y be a subset of X. Then we say that Y is irreducible if for any decomposition

$$Y = Z_1 \cup Z_2 \tag{2.2.2}$$

with Z_1 and Z_2 closed in Y we either have that $Z_1 = Y$ or $Z_2 = Y$. (Recall that a subset Z of Y is said to be closed if it is closed for the subspace topology on Y, that is, if we can write $Z = Y \cap C$ with C closed in X.)

We say that the topological space X is irreducible if it is irreducible as a subset of itself.

Example 2.2.3. Consider the Zariski topology on $\mathbb{A}^1$. Then Example 2.1.23 implies that the irreducible subsets of $\mathbb{A}^1$ are exactly the points of $\mathbb{A}^1$.

Proposition 2.2.4. *Suppose that U and V are two non-empty open subsets of an irreducible topological space X. Then their intersection $U \cap V$ is non-empty as well.*

Proof. Taking complements of the closed Z_1 and Z_2 in Definition 2.2.1, we obtain the following statement for the irreducible space X: If $\emptyset = U_1 \cap U_2$ with U_1 and U_2 open in X, then either $U_1 = \emptyset$ or $U_2 = \emptyset$. Taking the contrapositive, we obtain the statement of the proposition. □

Proposition 2.2.5. *Let Y be a subset of a topological space X. Then Y is irreducible if and only if the closure $\overline{Y}$ of Y in X is irreducible.*

Proof. Suppose that Y is irreducible. Consider a decomposition

$$\overline{Y} = Z_1 \cup Z_2 \tag{2.2.6}$$

with Z_1 and Z_2 closed in $\overline{Y}$. We may assume that Z_1 and Z_2 are closed subsets of $\overline{Y}$, since replacing them by $\overline{Y} \cap Z_1$ and $\overline{Y} \cap Z_2$ gives another such decomposition of $\overline{Y}$. Suppose that the decomposition is proper in the sense that neither of Z_1 and Z_2 equals $\overline{Y}$. Then we can define closed subsets $Y_1 = Y \cap Z_1$ and $Y_2 = Y \cap Z_2$ of Y. We show that Y_1 and Y_2 are proper subsets of Y. Once this is done, we obtain a contradiction with the assumption that Y is irreducible and the proposition is proved.

By symmetry, it suffices to show that Y_1 is a proper subset of Y. Suppose instead that $Y_1 = Y \cap Z_1 = Y$. Then we would have that Y is a subset of the closed subset Z_1 of X. By definition of the closure, this implies that $\overline{Y}$ is a subset of Z_1. But then we would have $\overline{Y} = Z_1$, in contradiction with the hypothesis that the decomposition in (2.2.6) is proper. This shows that $\overline{Y}$ is irreducible if Y is; the converse is left as an exercise. □

Lemma 2.2.7. *Suppose that the topological space X is irreducible. Then every open subset of U is irreducible and dense in X.*

Proof. The statement is clear if U is empty or all of X. Otherwise, suppose that there exists a decomposition

$$U = Y_1 \cup Y_2 \tag{2.2.8}$$

with Y_1 and Y_2 closed in U. Write $Y_1 = U \cap Z_1$ and $Y_2 = U \cap Z_2$ for closed subsets Z_1 and Z_2 of X, which we may assume to be proper and non-empty, since otherwise the decomposition in (2.2.8) would not be proper. Furthermore, define $Z_3 = X - U$, which is again a proper non-empty subset of X. Then since $Z_1 \cup Z_2$ contains $Y_1 \cup Y_2 = U$ we have that $Z_1 \cup Z_2 \cup Z_3$ contains $U \cup Z_3 = X$, so that in fact

$$X = Z_1 \cup Z_2 \cup Z_3 = (Z_1 \cup Z_2) \cup Z_3 \tag{2.2.9}$$

Since Z_3 is a proper subset of X and X is irreducible, we get

$$X = Z_1 \cup Z_2. \tag{2.2.10}$$

But as was mentioned above, the closed subsets Z_1 and Z_2 of X are proper. We see that the existence of a proper decomposition (2.2.8) leads to a contradiction with the assumption that X is irreducible, so that we can conclude that U is indeed irreducible.

We now show that U is dense. Once again this is clear when U is empty or all of X. Otherwise, let $Y = \overline{U}$ be the closure of U in X. Then we can write

$$X = \overline{U} \cup (X - U), \tag{2.2.11}$$

where both subsets $\overline{U}$ and $X - U$ of X are closed. Since $X - U$ is a proper subset of X, we see that we must have $\overline{U} = X$, because X is irreducible, so that indeed U is dense. □

Remark 2.2.12. Alternatively, and far easier, one can prove the first part of Lemma 2.2.7 by using the second part in combination with Proposition 2.2.5.

The proof of the following proposition will be given later:

Theorem 2.2.13. *Let $X = \mathbb{A}^n$, equipped with the Zariski topology. Then X is irreducible.*

Combining Lemma 2.2.7 and Theorem 2.2.13, we again see that the open subsets of $\mathbb{A}^n$ with respect to the Zariski topology with respect to the Zariski topology are "large" in the sense that they are irreducible and dense in $\mathbb{A}^n$.

Example 2.2.14. The irreducibility of $\mathbb{A}^n$ is particularly clear when $n = 1$, so that the Zariski topology is the cofinite topology on the infinite set $\mathbb{A}^1$ (cf. Example 2.1.28). In this case the proper closed subsets of $\mathbb{A}^1$ are the finite subsets, and we cannot write the infinite set $\mathbb{A}^1$ as a union of two such sets. Similarly, a non-empty open subset of $\mathbb{A}^1$ is of infinite cardinality, so that its closure cannot be contained in any proper closed subset of $\mathbb{A}^1$ and therefore equals $\mathbb{A}^1$ itself. The irreducibility of such an open subset can be shown in a similar fashion, since it cannot be written as a union of two subsets of finite cardinality.

Example 2.2.15. Consider the subset $U = D(x_1x_2) = \mathbb{A}^2_k - V(x_1x_2)$ of $\mathbb{A}^2_k$. Although $V(x_1x_2)$ is not irreducible, Lemma 2.2.7 shows that U is irreducible and dense in $\mathbb{A}^2_k$.

Remark 2.2.16. As is shown in [2, Proposition I.1.5], a general closed subset Z of $\mathbb{A}^n$ can be written as a union

$$Z = Z_1 \cup \ldots \cup Z_r \tag{2.2.17}$$

where the Z_i are irreducible closed subsets of $\mathbb{A}^n$. Moreover, if we demand that there are no mutual inclusions among the Z_i, then these sets are even uniquely determined up to renumbering. They are called the irreducible components of Z.

Example 2.2.18. Consider the closed subsets of $\mathbb{A}^2_k$ from Example 2.1.14. Then $Z_1 \cap Z_2$ has the single irreducible component $\{(0,0)\}$, whereas the irreducible components of $Z_1 \cap (Z_2 \cup Z_3)$ are $\{(0,0)\}$ and $\{(0,1)\}$.

Note that irreducibility can also be lost when only taking intersections: If we define

$$Z_4 = V(x_2 - x_1^2), \tag{2.2.19}$$

then the irreducible components of $Z_3 \cap Z_4$ are the singleton sets corresponding to the two points $(1,1)$ and $(-1,1)$.

Definition 2.2.20. An affine variety is a closed algebraic subset X of $\mathbb{A}^n$, equipped with the subspace topology induced by the Zariski topology on $\mathbb{A}^n$.

Remark 2.2.21. Using the definition of the induced topology and the fact that X is closed in $\mathbb{A}^n$, we see that a subset Y of X is closed if and only if Y itself is an algebraic subset of $\mathbb{A}^n$.

Remark 2.2.22. More intuitively, the Hilbert Basis Theorem shows that an affine variety $X \subset \mathbb{A}^n$ is the zero locus

$$X : \begin{cases} f_1(x_1, \ldots, x_n) & = & 0, \\ \vdots & & \vdots \\ f_r(x_1, \ldots, x_n) & = & 0. \end{cases} \tag{2.2.23}$$

of a finite set of polynomial equations in $k[x_1, \ldots, x_n]$ that is irreducible with respect to the Zariski topology. We will later see how the additional condition that X be irreducible can be verified in practice. A closed subset of X is nothing but a subset of X obtained by adjoining another finite amount of algebraic equations to the $f_i(x_1, \ldots, x_n) = 0$ that define X.

Note that conversely, not every system (2.2.23) defines an algebraic variety, because the corresponding zero locus X may not be irreducible. Proposition 2.2.37 will give us a criterion for X to be irreducible.

It remains to prove Theorem 2.2.13. We will prove this as a corollary of a general statement that has many more useful consequences, but first we need another definition. Given a subset S of $k[x_1, \ldots, x_n]$, we have associated a subset $Y = V(S)$ of $\mathbb{A}^n$ to it in the previous section. There is also an association in the other direction.

Definition 2.2.24. Let Y be a subset of $\mathbb{A}^n$. We define the ideal of vanishing $I(Y) \subset k[x_1,\ldots,x_n]$ as

$$I(Y) = \{f \in k[x_1,\ldots,x_n] \mid f(P) = 0 \text{ for all } P \in Y\}. \tag{2.2.25}$$

Remark 2.2.26. The proof of Proposition 2.1.11 shows that that if $Z_1 = V(S_1)$ and $Z_2 = V(S_2)$, then

$$Z_1 \cup Z_2 = V(S_1 S_2). \tag{2.2.27}$$

This statement has a pendant in terms of ideals of vanishing, namely that for any two subsets Y_1 and Y_2 (not necessarily algebraic) we have

$$I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2). \tag{2.2.28}$$

The proof of (2.2.28) is left as an exercise.

Recall that given an ideal $\mathfrak{a}$ of a ring R, the radical $\sqrt{\mathfrak{a}}$ of $\mathfrak{a}$ is defined as

$$\sqrt{\mathfrak{a}} = \{f \in R \mid f^n \in R \text{ for some } n > 0\}. \tag{2.2.29}$$

Proposition 2.2.30. *Let S, S_1, S_2 be subsets of $k[x_1,\ldots,x_n]$, and let Y, Y_1, Y_2 be subsets of $\mathbb{A}^n$.*

(i) If $S_1 \subset S_2$, then $V(S_1) \supset V(S_2)$.

(ii) If $Y_1 \subset Y_2$, then $I(Y_1) \supset I(Y_2)$.

(iii) We have $V(I(V(S))) = V(S)$.

(iv) We have $I(V(I(Y))) = I(Y)$.

Proof. The first two statements are formal consequences of the definitions. As for Part (iii), the definition of the ideal of vanishing implies that $S \supset I(V(S))$ for any subset S of $k[x_1,\ldots,x_n]$, which in turn implies $V(S) \subset V(I(V(S)))$ by Part (i). On the other hand, we also have that $V(I(Y))$ contains Y for all Y, again by the definition of the ideal of vanishing. Applying this to the case $Y = V(S)$, we get that $V(I(V(S))) \subset V(S)$, so that in fact we have $V(I(V(S))) = V(S)$, which proves our claim. The proof of Part (iv) is similar. □

Example 2.2.31. The converse of the implication in Part (i) of Proposition 2.2.30 is not true. For example, let $n = 1$, and let $S_1 = \{x_1^2(x_1 - 1)\}$ and $S_2 = \{x_1(x_1 - 1)^2\}$. Then we have $V(S_1) = \{0, 1\} = V(S_2)$ although neither of S_1 and S_2 is contained in the other. This problem is not even resolved when passing to ideals instead of subsets of $k[x_1,\ldots,x_n]$: In our example the ideals

$$\begin{aligned} \mathfrak{a}_1 &= (x_1^2(x_1 - 1)), \\ \mathfrak{a}_2 &= (x_1(x_1 - 1)^2) \end{aligned} \tag{2.2.32}$$

of $k[x_1]$ have the same zero locus $\{0, 1\}$, but there is not even an inclusion in any direction between $\mathfrak{a}_1$ and $\mathfrak{a}_2$.

Neither is the converse of Part (ii) of Proposition 2.2.30 true. For example, let $n = 1$, and let $Y_1 = \mathbb{A}^1 - \{0\}$ and $Y_2 = \mathbb{A}^1 - \{1\}$. Then we have $I(Y_1) = 0 = I(Y_2)$ since any univariate polynomial with an infinite number of zeros is in fact the zero polynomial, but there is not even an inclusion in any direction between Y_1 and Y_2.

Theorem 2.2.33. *We Y be a subset of $\mathbb{A}^n$, and let S be a subset of $k[x_1,\ldots,x_n]$.*

(i) We have $V(I(Y)) = \overline{Y}$, where $\overline{Y}$ is the closure of Y in X.

(ii) We have $I(V(S)) = \sqrt{\langle S \rangle}$, where $\langle S \rangle$ is the ideal of $k[x_1,\ldots,x_n]$ generated by S.

Proof. For Part (i), we first again note that the definition of the ideal of vanishing implies that the closed subset $V(I(Y))$ indeed contains Y. Conversely, suppose that Z is a closed subset of $\mathbb{A}^n$ that contains Y. Then we can write $Z = V(T)$ for some subset T of $k[x_1,\dots,x_n]$, and we have $Y \subset V(T)$. Proposition 2.2.30 then shows that $I(Y) \supset I(V(T))$ and $V(I(Y)) \subset V(I(V(T))) = V(T)$. We see that $V(I(Y))$ contains $V(T) = Z$. Since Z was arbitrary, this shows that $V(I(Y))$ is indeed the closure of Y in $\mathbb{A}^n$.

Part (ii) is the famous Hilbert Nullstellensatz [4, Theorem 6.4.10], for whose proof we refer to *loc. cit.* □

Proposition 2.2.33(ii) shows that given Y, the ideal $I(Y)$ is that largest ideal of $k[x_1,\dots,x_n]$ with respect to inclusion whose zero locus equals Y. It has the following important corollary, of which it is in fact itself a consequence and which is far from trivial (the hypothesis that k is algebraically closed is crucial, and a direct proof requires the Noether normalization lemma).

Corollary 2.2.34. *Let S be a subset of $k[x_1,\dots,x_n]$. Then the zero locus $V(S)$ is non-empty if and only if S does not generate the unit ideal of $k[x_1,\dots,x_n]$.*

Proof. If S generates the unit ideal of $k[x_1,\dots,x_n]$, then we have $V(S) = V(\langle S\rangle) = V(1) = \emptyset$ by Proposition 2.1.5. Conversely, if $V(S) = \emptyset$, then $I(V(S)) = I(\emptyset) = k[x_1,\dots,x_n]$, so that $\langle S\rangle = I(V(S))$ contains 1. Using the definition of the radical $\sqrt{\langle S\rangle}$ then shows that $\langle S\rangle$ itself also contains 1 so that it is the unit ideal of $k[x_1,\dots,x_n]$. □

Remark 2.2.35. In fact [4, §6.3] shows that the points of $V(S)$ are in bijective correspondence with the maximal ideals that contain the ideal $\langle S\rangle$. Indeed, if $P = (a_1,\dots,a_n) \in V(S)$, then

$$\mathfrak{m}_P = (x_1 - a_1,\dots,x_n - a_n) \tag{2.2.36}$$

is an ideal of $k[x_1,\dots,x_n]$ that contains $\langle S\rangle$, and conversely all such ideals are of the form $\mathfrak{m}_P$ for some uniquely determined point $P \in V(S)$.

The following Proposition is [2, Corollary I.1.4].

Proposition 2.2.37. *Let Y be a closed subset of $\mathbb{A}^n$. Then Y is irreducible if and only if $I(Y)$ is a prime ideal of $k[x_1,\dots,x_n]$.*

This proves Theorem 2.2.13, since $I(\mathbb{A}^n) = 0$ is a prime ideal of $k[x_1,\dots,x_n]$.

Example 2.2.38. Consider the algebraic subset $Z = V(x_3 - x_1^2)$ of $k[x_1,x_2]$. Then Z is irreducible. Indeed, $I(Z)$ contains the ideal $J = (x_2 - x_1^2)$, and moreover the quotient $k[x_1,x_2]/J \cong k[x_1]$ is an integral domain, which implies that its nilradical $\sqrt{0}$ is trivial. Using the correspondence between ideals of a quotient ring and those of the original ring, we obtain that $J = \sqrt{J}$. Therefore Proposition 2.2.33(ii) implies that

$$I(Z) = \sqrt{J} = J = (x_2 - x_1^2). \tag{2.2.39}$$

Since $k[x_1,x_2]/J$ is a prime ideal, Proposition 2.2.37 implies that Z is irreducible.

Example 2.2.40. Consider the ideal

$$\mathfrak{a} = (x_1^2(x_1 - 1)^3) \tag{2.2.41}$$

of $k[x_1]$. Then $V(\mathfrak{a}) = \{0,1\}$, so that $I(V(\mathfrak{a})) = (x_1(x_1 - 1))$. We conclude from Theorem 2.2.33 that

$$\sqrt{\mathfrak{a}} = (x_1(x_1 - 1)). \tag{2.2.42}$$

Definition 2.2.43. Let X be an affine variety. We define the coordinate ring $k[X]$ of X to be the quotient

$$k[X] = k[x_1,\dots,x_n]/I(X). \tag{2.2.44}$$

Remark 2.2.45. Since $I(X)$ is a prime ideal by Proposition 2.2.37, the coordinate ring $k[X]$ is an integral domain. Taking $S = I(X)$ in Remark 2.2.35, we see that the points of $X = V(I(X))$ are in bijection with the maximal ideals of $k[x_1,\dots,x_n]$ that contain $I(X)$. In turn, the third isomorphism theorem for rings shows that these maximal ideals are in bijective correspondence with the maximal ideals of $k[X]$. Concretely, a point $P = (a_1,\dots,a_n) \in X$ once again gives rise to the maximal ideal

$$\mathfrak{m}_P = (x_1 - a_1,\dots,x_n - a_n) + I(X) \tag{2.2.46}$$

of $k[X]$.

2.3 Regular functions

We now come to the definition of the functions that we want to consider on affine varieties. As was discussed in the first chapter, it is these functions that make the variety into an algebraic-geometric object instead of merely a topological space. To do this, we will use the formalism of sheaves. Throughout this section, we consider an affine variety $X \subset \mathbb{A}_k^n$, and we often use the notation $\mathfrak{a}$ for its ideal of vanishing $I(X)$.

We will consider those functions on X that are algebraic in the sense that they admit a local description as rational functions, that is, as a quotient of polynomials.

Definition 2.3.1. Let U be an open subset of X. A regular function on U is a function $f : U \to \mathbb{A}^1$ such that the following property is satisfied: For all $P \in U$ there exists an open subset U_P of U and polynomials $r,s \in k[x_1,\dots,x_n]$ such that

(i) $P \in U_P$;

(ii) $s(Q) \neq 0$ for all $Q \in U_P$;

(iii) $f(Q) = r(Q)/s(Q)$ for all $Q \in U_P$.

The definition is somewhat cumbersome, but this has an important motivation, namely that we do not immediately want to impose that f admits a description as a quotient r/s on all of U. This is the whole point of using sheaves. As in the case of (for example) smooth functions, we do not impose a special global form for the regular functions f on all of U, but we only demand f to have certain local behavior. It is a priori very well possible that by patching together functions on an open cover of U with such correct local behavior, or even with a certain special local canonical form, we obtain a function on the larger open set U that no longer allows a simple description or normal form on all of U simultaneously. Let us consider an example of this phenomenon in the context of regular functions.

Example 2.3.2. Consider the algebraic curve

$$X : x_2^2 - 1 = x_1^3 - x_1 \subset \mathbb{A}_k^2. \tag{2.3.3}$$

On the principal open subset $D(x_1) = X - \{(0,1),(0,-1)\}$ of X, we have the regular function $f_1 = (x_2+1)/x_1$, whereas the principal open subset $D(x_2-1) = X - \{(0,1),(-1,1),(1,1)\}$ admits the regular function $f_2 = (x^2-1)/(x_2-1)$. By the defining equation of X, we have that f_1 and f_2 coincide on the intersection $D(x_1) \cap D(x_2-1)$. This means that they glue to a function f on $U = D(x_1) \cup D(x_2 - 1) = X - \{(0,1)\}$. The function f is regular on U definition, although it turns out that it is impossible to describe f on U by means of a *single* quotient of polynomials r/s.

We see that the function f from Example 2.3.2 Fortunately, as we shall see, we can still give a simple global descriptions of the regular functions on U whenever U is a principal open subset of an affine variety X. But to show that, we need to put in some work.

As in [2, Lemma I.3.1], one first shows the following:

Lemma 2.3.4. *Let f be a regular function on an open subset U of X. Then f is continuous with respect to the Zariski topology.*

Given an open subset U of X, the set $\mathscr{O}_X(U)$ of regular functions on U is a ring in a natural way: As usual, given two functions $f, g \in \mathscr{O}_X(U)$, we define $f + g$ and fg by

$$\begin{aligned} (f+g)(P) &= f(P) + g(P) \quad \text{and} \\ (fg)(P) &= f(P)g(P). \end{aligned} \tag{2.3.5}$$

Proposition 2.3.6. *The ring structure on $\mathscr{O}_X(U)$ is well-defined. With the usual restriction of functions, this makes $\mathscr{O}_X$ into a sheaf of rings on X.*

Proof. Let $f_1, f_2 \in \mathscr{O}_X(U)$. Given $P \in U$, we can find an open subset $U_P \subset U$ that contains P on which f_1 can be described as a quotient r_1/s_1 with $s_1(Q) \neq 0$ for all $Q \in U_P$. Similarly, we can find a subset $V_P \subset U$ that contains P on which f_2 can be described as a quotient r_2/s_2 with $s_2(Q) \neq 0$ for all $Q \in U_P$. But then on $U_P \cap V_P$ the function $f_1 + f_2$ admits the description

$$f_1 + f_2 = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \tag{2.3.7}$$

and $f_1 f_2$ admits the description

$$f_1 f_2 = \frac{r_1 r_2}{s_1 s_2}. \tag{2.3.8}$$

In either case, the denominator $s_1 s_2$ does not vanish in any point Q of U_P. We see that $f_1 + f_2$ and $f_1 f_2$ both admit a local description as a rational function. Since P was arbitrary, we see that both $f_1 + f_2$ and $f_1 f_2$ are again regular functions, that is, elements of $\mathscr{O}_X(U)$.

Let $f \in \mathscr{O}_X(U)$, and let $\rho_V^U(f)$ be its restriction to V. Consider a point $P \in V$. Then there exists a neighborhood $U_P \subset U$ such that we can write f as a quotient of polynomials r/s on U_P, with s nowhere zero. Then on $V_P = U_P \cap V$ the same holds for $\rho_V^U(f)$. Since V_P is once again a neighborhood of P and P was arbitrary, this shows that $\rho_V^U(f)$ is again in $\mathscr{O}_X(V)$, so that the restriction maps are well-defined. As in Example 1.3.8, we see that these restriction maps make $\mathscr{O}_X(U)$ into a presheaf.

Now suppose that regular functions $(f_i)_{i \in I}$ are given on an open cover $(U_i)_{i \in I}$ of U. Suppose moreover that these functions are compatible in the sense that their restrictions agree on overlaps. To show that $\mathscr{O}_X(U)$ is a sheaf, we have to find a regular function $f \in \mathscr{O}_X(U)$ of which all the f_i are restrictions. As in Example 1.3.20, we see that there exists a function f on U of which all the f_i are restrictions. The point is that we have to show that f is regular. For this, let $P \in U$. Choose $i \in I$ such that $P \in U_i$. Then because f_i is regular on U_i there is a subset V_P of U_i that contains P and on which f_i admits a description as a rational functions r/s with s nowhere zero. But this means that the same holds for the function f on V_P, since f restricts to f_i on U_i, and hence on V_P as well. Since P was arbitrary, we have shown that f is indeed a regular function on U. $\square$

Remark 2.3.9. In the final part of Proposition 2.3.6, we have made crucial use of the fact that Definition 2.3.1 only imposes a *local* description of a regular function f as a rational function on subsets of U, instead of a global description of this form all of U. Proving the sheaf property would have been impossible otherwise, as Example 2.3.2 shows.

Given a regular function $f \in \mathscr{O}_X(U)$ and an open subset V of U, we will often denote the restriction of f to V by the more concise $f|_V$ instead of $\rho_V^U(f)$.

Proposition 2.3.10. *The pair $(X, \mathscr{O}_X)$ is a locally ringed space.*

Proof. Proposition 2.3.6 shows that $(X, \mathscr{O}_X)$ is a ringed space. Given $P \in X$, let us consider the stalk $\mathscr{O}_{X,P}$ of $\mathscr{O}_X$ at P. An element of $\mathscr{O}_{X,P}$ is nothing but an equivalence class $[(U, f)]$, where U is an open subset of X that contains P and where f is a regular function on U.

Let us first show that $[(U, f)]$ is a unit in $\mathscr{O}_{X,P}$ if and only if $f(P) \neq 0$. On the one hand, if $f(P) = 0$, then there cannot exist an element $[(V, g)] \in \mathscr{O}_{X,P}$ such that $1 = [(U, f)][(V, g)] = [(U \cap V, f|_{U\cap V} g|_{U\cap V})]$, because the product $f|_{U\cap V} g|_{U\cap V}$ evaluates to 0 in P. On the other hand, suppose that $f(P) \neq 0$. Given an open subset $V \subset U$ with $P \in V$, we have $[(U, f)] = [(V, f|_V)]$. After a suitable such restriction, we may assume that $f = r/s$ admits a description by means of a rational function on all of U, with s nowhere zero on U. Consider the principal open subset $D(r)$ of X. Then $P \in D(r)$, since the fact that $f(P) \neq 0$ implies that $r(P) \neq 0$. On the neighborhood $U \cap D(r)$, the numerator of the rational function $g = s/r$ is everywhere non-zero. Now $[(U, f)][(U \cap D(r), g)] = 1$ by construction, so our claim is proved.

These considerations show that $\mathscr{O}_{X,P}$ is a local ring. Indeed, the non-units of $\mathscr{O}_{X,P}$ are exactly the elements $[(U, f)]$ with $f(P) = 0$, and these indeed form an ideal, for example because they are the kernel of the evaluation homomorphism

$$\begin{aligned} \mathscr{O}_{X,P} &\to k \\ f &\mapsto f(P). \end{aligned} \tag{2.3.11}$$

□

We can simplify our consideration of rational functions on X by means of the following observation.

Lemma 2.3.12. *Let f and g be two rational functions on an open subset $U \subset X$. If $f|_V = g|_V$ for some non-empty open subset $V \subset U$, then in fact $f = g$.*

Proof. The open subset V is dense in U by Proposition 2.2.5 and Lemma 2.2.7. The conclusion then follows from Lemma 2.3.4. □

Remark 2.3.13. Lemma 2.3.12 is what makes the regular functions in algebraic geometry different from the usual continuous or smooth functions. For example, there exist non-zero functions on $\mathbb{R}$ that are non-zero, yet are zero on a prescribed open subset of $\mathbb{R}$, for example the "bump functions" considered in functional analysis.

Definition 2.3.14. We define the function field $k(X)$ of X to be the set of equivalence classes pairs $[(U, f)]$ with $U \subset X$ a non-empty open subset and with $f \in \mathscr{O}_X(U)$. As before, two such pairs (U, f) and (V, g) are considered equivalent if and only if $f|_{U\cap V} = g|_{U\cap V}$. The ring structure on $k(X)$ is defined by

$$\begin{aligned} [(U, f)] + [(V, g)] &= [(U \cap V, f|_{U\cap V} + g|_{U\cap V})] \\ [(U, f)] \cdot [(V, g)] &= [(U \cap V, f|_{U\cap V} \cdot g|_{U\cap V})]. \end{aligned} \tag{2.3.15}$$

Proposition 2.3.16. *The ring structure on $k(X)$ is well-defined, and with it, $k(X)$ is a field.*

Proof. To show that the ring structure is well-defined, it suffices to show that $U \cap V$ is non-empty for any two non-empty open subset U, V of X, but this is nothing but Proposition 2.2.4. Now let $[(U, f)] \in k(X)$ with $f \neq 0$ be given. Restricting as in the proof of Proposition 2.3.10, we may assume that $f = r/s$ is a rational function with s nowhere zero on U, and as in said proof, we see that $[(U \cap D(r), s/r)]$ is an inverse of $[(U, f)]$ in $k(X)$. □

Proposition 2.3.17. *Let $P \in X$, and let $U \subset X$ be an open subset that contains P. Then there are canonical injections*

$$\mathcal{O}_X(U) \hookrightarrow \mathcal{O}_{X,P} \hookrightarrow k(X) \tag{2.3.18}$$

Proof. The first canonical map is

$$\begin{aligned} \mathcal{O}_X(U) &\to \mathcal{O}_{X,P} \\ f &\mapsto (U, f). \end{aligned} \tag{2.3.19}$$

Suppose that $f_1, f_2 \in \mathcal{O}_X(U)$ are such that $[(U, f_1)] = [(U, f_2)]$. Then by definition there is open subset $V \subset U$ such that $f_1|_V = f_2|_V$. Lemma 2.3.12 shows that $f_1 = f_2$, so that (2.3.19) is injective.

The second canonical map is

$$\begin{aligned} \mathcal{O}_{X,P} &\to k(X) \\ [(U, f)] &\mapsto [(U, f)]. \end{aligned} \tag{2.3.20}$$

Suppose that $[(U_1, f_1)], [(U_2, f_2)] \in \mathcal{O}_{X,P}$ are such that $[(U_1, f_1)] = [(U_2, f_2)]$ in $k(X)$. Then by definition there is open subset $V \subset U_1 \cap U_2$ such that $f_1|_V = f_2|_V$. Lemma 2.3.12 shows that $f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}$. Since $P \in U_1 \cap U_2$, we see that $[(U_1, f_1)] = [(U_2, f_2)]$ in $\mathcal{O}_{X,P}$, so that the map (2.3.19) is indeed injective as well. □

We are about to give simple descriptions of the ring of global sections $\mathcal{O}_X(X)$ and the stalk $\mathcal{O}_{X,P}$. For this, we need a useful algebraic notion.

Definition 2.3.21. Let R be a domain, and let S be a subset of R that is multiplicatively closed in the sense that if $s_1, s_2 \in S$, then also $s_1 s_2 \in S$. We define the localization R_S of R at S to be the subring

$$R_S = \{r/s : r \in R, s \in S\} \subset Q(R) \tag{2.3.22}$$

of the field of fractions $Q(R)$ of R.

An important special case it that where $S = R \setminus \mathfrak{p}$ is the complement of prime ideal, which is multiplicatively closed by the defining property of such an ideal. In this case, we will write $R_{\mathfrak{p}}$ for R_S.

Proposition 2.3.23. *Let R be a domain. Then we have $R = \bigcap_{\mathfrak{m} \subset R} R_{\mathfrak{m}}$ as a subset of $Q(R)$. Here $\mathfrak{m}$ runs through the set of maximal ideals of R.*

Proof. The inclusion $R \subset \bigcap_{\mathfrak{m} \subset R} R_{\mathfrak{m}}$ is clear. Conversely, suppose that $x \in \bigcap_{\mathfrak{m} \subset R} R_{\mathfrak{m}}$, and consider the denominator ideal

$$\mathfrak{d}_x = \{r \in R : rx \in R\}. \tag{2.3.24}$$

If $x \notin R$, then $\mathfrak{d}_a$ is a proper ideal of R, so that it is contained in a maximal ideal $\mathfrak{m}$ of R. By assumption, we have $x \in R_{\mathfrak{m}}$, so that we can write $x = r/s$ for $r \in R$ and $s \in R \setminus \mathfrak{m}$. Now $sx = r \in R$. But then $s \in \mathfrak{d}_x \subset \mathfrak{m}$, a contradiction. We conclude $x \in R$, so that the converse inclusion also holds. □

For the following theorem, also see [2, Theorem I.3.2].

Theorem 2.3.25. *Let X be an affine variety, and let $P \in X$ be a point. Let $\mathfrak{m}$ be the maximal ideal of $k[X]$ that corresponds to P, as in Remark 2.2.45.*

(i) There is a canonical isomorphism $\mathscr{O}_{X,P} \cong k[X]_{\mathfrak{m}}$;

(ii) There is a canonical isomorphism $k(X) \cong Q(k[X])$;

(iii) There is a canonical isomorphism $\mathscr{O}_X(X) \cong k[X]$.

Proof. (i) There is a canonical map

$$\begin{aligned} k[X]_{\mathfrak{m}} &\to \mathscr{O}_{X,P} \\ r/s &\to [(D(s), r/s)]. \end{aligned} \tag{2.3.26}$$

Note that this map is indeed well-defined because if $s \in \mathfrak{m}$, then $D(s)$ contains P. The map (2.3.26) is surjective. Indeed, the definition of a regular functions implies that after restricting if necessary, a class in $\mathscr{O}_{X,P}$ is represented by a pair $([U, f])$, where f admits an expression as a regular function r/s with s non-zero on all of U. The definition of the equivalence relation on $\mathscr{O}_{X,P}$ implies that $[(U, f)] = [(D(s), r/s)]$, so that $[(U, f)]$ is the image of $r/s \in k[X]_{\mathfrak{m}}$.

On the other hand, if r_1/s_1 and r_2/s_2 have the same image in $\mathscr{O}_{X,P}$, then the rational functions r_1/s_1 and r_2/s_2 coincide on the open set $D(s_1) \cap D(s_2) = D(s_1 s_2)$. This means that there is an equality of regular functions $r_1 s_2 = r_2 s_1$ on $D(s_1, s_2)$, so that Lemma 2.3.12 implies that $r_1 s_2 = r_2 s_1$ on all of X and therefore $r_1/s_1 = r_2/s_2$ as elements of $k[X]_{\mathfrak{m}} \subset k(X)$. This shows injectivity of (2.3.26), which, along with the previously proved surjectivity, shows that this map is surjective.

(ii) The proof of this statement is similar to that of Part (i) and is left to the reader.

(iii) There is certainly a homomorphism

$$\begin{aligned} k[X] &\to \mathscr{O}_X(X) \\ f &\to [(X, f)]. \end{aligned} \tag{2.3.27}$$

Arguing as in the proof of (i), one shows that (2.3.27) is injective. Conversely, let $f \in \mathscr{O}_X(X)$ be a regular function. Then using Part (i) and the inclusions from Proposition 2.3.17, we see from Proposition 2.3.23 that

$$f \in \bigcap_{P \in X} \mathscr{O}_{X,P} = \bigcap_{\mathfrak{m} \subset k[X]} k[X]_{\mathfrak{m}} = k[X]. \tag{2.3.28}$$

Here the intersection is taking inside the function field $k(X)$, which again makes sense because of Proposition 2.3.17. The theorem is proved. □

Remark 2.3.29. Because of Part (ii), we will often denote an element of $k(X)$ by f instead of by $[(U, f)]$.

Remark 2.3.30. In the next section, we will see an analog of Part (ii) of Theorem 2.3.25 for principal open subsets $D(f)$ of X. For general open subsets U of X, there is no simple algebraic way of describing $\mathscr{O}_X(U)$.

2.4 Morphisms between affine varieties

We now consider the "right" notion of maps between affine varieties, motivated by our description of maps between locally ringed spaces at the end of Section 1.5.

Definition 2.4.1. Let X and Y be two affine varieties over k. A morphism from X to Y is a map $\varphi : X \to Y$ that is continuous with respect to the Zariski topology and that furthermore satisfies the property that for every regular function on a subset $V \subset Y$, the composition $\varphi^*(f) := f \circ \varphi : \varphi^{-1}(V) \to V$ is regular on the open subset $\varphi^{-1}(V)$ of X.

Remark 2.4.2. Definition 2.4.1 still makes sense for quasi-affine varieties, that is, for non-empty open subsets of affine varieties. We will need this when proving Theorem 2.4.30.

With this notion of morphisms, we obtain the category of varieties over k, which we will denote by $\mathfrak{Var}_k$.

Remark 2.4.3. It can in fact be shown that Definition 2.4.1 furnishes the same morphisms as does the more general Definition 1.5.21 of morphisms between locally ringed spaces if we additionally insist that the second map $\varphi^\#$ in the latter definition preserve the k-algebra structure, in the sense that

$$\varphi^\#_V : \mathscr{O}_Y(V) \to \varphi_*(\mathscr{O}_X(V)) = \mathscr{O}_X(\varphi^{-1}(V)) \tag{2.4.4}$$

be a homomorphism of k-algebras for all open subsets V of Y. In another form, this was alluded to in Remark 1.6.20, which shows that can go wrong if we do not impose this condition. We do not go into this matter in more detail in these notes.

See [2, Proposition I.3.6] for another proof of the following lemma.

Lemma 2.4.5. *Suppose that $\varphi : X \to Y$ is a map of sets between affine varieties, where $Y \subset \mathbb{A}^n$. Then φ is a morphism if and only if $\varphi^*(x_i) = x_i \circ \varphi$ is a regular function on X for all $i = 1, \dots, n$.*

Proof. The definition of a morphism implies that $\varphi^*(x_i)$ is regular whenever φ is a morphism. Conversely, if all $\varphi^*(x_i)$ are regular, then also $\varphi^*(g)$ is regular for all polynomials $g \in k[x_1, \dots, x_n]$, since sums, products, and scalar multiples of regular functions are regular.

Let $V(T) \subset Y$ be a closed subset, where $T \subset k[x_1, \dots, x_n]$. Let us define

$$S = \{\varphi^*(g) : g \in S\}. \tag{2.4.6}$$

Then by the first part of the proof, the elements of S are regular functions on all of X, and can therefore be represented by polynomials. This shows that $V(S)$ is a closed subset of X. We claim that in fact

$$\varphi^{-1}(V(T)) = V(S). \tag{2.4.7}$$

Indeed, given $P \in X$ we have that $P \in \varphi^{-1}(V(T))$ if and only if $\varphi(P) \in V(T)$ if and only if $g(\varphi(P)) = 0$ for all $g \in T$ if and only if $f(P) = 0$ for all $s \in S$, where the last statement follows because the elements of S are the elements $\varphi^*(g)$ with $g \in T$ by definition. Equality (2.4.7) shows that the inverse image of every closed set of Y under φ is closed in X. Taking complements, we see that the inverse image of every open set of Y under φ is open in X, or in other words that φ is continuous. Since the observation from the first part of the proof shows that a composition $\varphi^*(g)$ are regular whenever g is, we see that φ is indeed a morphism of varieties. $\square$

The following result is a special case of [2, Proposition I.3.5].

Theorem 2.4.8. *Let X and Y be two affine varieties over k. Then there is a natural bijection*

$$\mathrm{Hom}_{\mathfrak{Var}_k}(X,Y) \leftrightarrow \mathrm{Hom}_{k\text{-}\mathfrak{Alg}}(k[Y],k[X]). \tag{2.4.9}$$

Proof. If $\varphi : X \to Y$ is a morphism of varieties, then we obtain the following homomorphism of k-algebras:

$$\begin{aligned} h = \varphi^* : k[Y] &\to k[X] \\ g &\mapsto \varphi^*(g) := g \circ \varphi. \end{aligned} \tag{2.4.10}$$

Indeed, we can interpret $g \in k[Y]$ as a global section in $\mathscr{O}_Y(Y)$ by Theorem 2.3.25. Since φ is a morphism, the composition $\varphi^*(g) = g \circ \varphi$ is in $\mathscr{O}_X(\varphi^{-1}(Y)) = \mathscr{O}_X(X) = k[X]$, again by Theorem 2.3.25.

Conversely, suppose that we are given a homomorphism of k-algebras $h : k[Y] \to k[X]$. Suppose that $Y \subset \mathbb{A}^n$, so that its ring of global regular functions $k[Y]$ admits the description $k[Y] = k[x_1,\ldots,x_n]/I(Y)$. For $i = 1,\ldots,n$, we define

$$\varphi_i = h(\overline{x}_i) \in k[X]. \tag{2.4.11}$$

We claim that the map

$$\begin{aligned} \varphi : X &\to Y \\ P &\mapsto (\varphi_1(P),\ldots,\varphi_n(P)) \end{aligned} \tag{2.4.12}$$

is well-defined and a morphism of varieties. First note that for all $P \in X$ and for all $g \in I(Y)$ we have

$$\begin{aligned} g(\varphi(P)) &= g(\varphi_1(P),\ldots,\varphi_n(P)) \\ &= g(h(\overline{x}_1)(P),\ldots,h(\overline{x}_n)(P)) \\ &= h(g(\overline{x}_1(P),\ldots,\overline{x}_n(P))) \\ &= h(\overline{g}(P_1,\ldots,P_n)) \\ &= (h \circ \overline{g})(P_1,\ldots,P_n) \\ &= 0(P_1,\ldots,P_n) \\ &= 0. \end{aligned} \tag{2.4.13}$$

Here the third equality follows because g can be represented by a polynomial in $k[x_1,\ldots,x_n]$, which is another consequence of Theorem 2.3.25. We have therefore shown that φ is well-defined: It is a morphism because of Lemma 2.4.5, since the compositions $\varphi^*(x_i) = \varphi_i$ are indeed regular functions.

It is left as an exercise to prove that the above two associations furnish mutually inverse bijections. □

This translates questions about varieties and morphisms into questions about homomorphisms between quotients of polynomial rings, which are more easily understood.

Remark 2.4.14. If X is merely quasi-affine, then Theorem 2.4.8 generalizes to yield a one-to-one correspondence between the morphisms $X \to Y$ and the k-algebra homomorphisms from $k[Y] \to \mathscr{O}_X(X)$. The proof is identical.

Example 2.4.15. Let $X = \mathbb{A}^1$ and let $Y = V(x_1^2 + x_2^2 - 1)$. Then we have

$$\begin{aligned} k[X] &= k[t] \\ k[Y] &= k[x_1,x_2]/(x_1^2 + x_2^2 - 1). \end{aligned} \tag{2.4.16}$$

Theorem 2.4.8 shows that the set of morphisms of varieties $\varphi : Y \to X$ is in correspondence with the set of k-algebra homomorphisms $h : k[t] \to k[x_1, x_2]/(x_1^2 + x_2^2 - 1)$. More precisely, if $\varphi : Y \to X$ is a morphism, then the corresponding homomorphism

$$h_\varphi = \varphi^* : k[t] = k[X] = \mathscr{O}_X(X) \to \mathscr{O}_Y(Y) = k[Y] = k[x_1, x_2]/(x_1^2 + x_2^2 - 1) \tag{2.4.17}$$

is characterized by

$$h_\varphi : t \mapsto \varphi^*(t) = t \circ \varphi \in \mathscr{O}_Y(Y) = k[x_1, x_2]/(x_1^2 + x_2^2 - 1). \tag{2.4.18}$$

Since the value of $\varphi^*(t)$ at a point $Q = (Q_1, Q_2)$ of Y is $t(\varphi(Q))$, we see that $h_\varphi(t)$ is the "general expression" of φ at a point in Y. Conversely, if a homomorphism $h : k[x_1, x_2]/(x_1^2 + x_2^2 - 1) \to k[t]$ is provided, then the corresponding morphism of varieties φ_h is defined by

$$\varphi_h(Q) = h(t)(Q). \tag{2.4.19}$$

An example of a morphism $Y \to X$ is

$$\begin{aligned} \varphi : Y &\to X \\ (Q_1, Q_2) &\mapsto Q_1. \end{aligned} \tag{2.4.20}$$

We have that $h_\varphi = \varphi^*$ sends t to $\varphi^*(t)$. Since

$$\varphi^*(t)(Q_1, Q_2) = (t \circ \varphi)(Q_1, Q_2) = t(\varphi(Q_1, Q_2)) = t(Q_1) = Q_1, \tag{2.4.21}$$

we see that

$$h_\varphi(t) = x_1. \tag{2.4.22}$$

Now let us consider the morphisms of varieties $\varphi : X \to Y$. These are in bijective correspondence with the k-algebra homomorphisms $h : k[x_1, x_2]/(x_1^2 + x_2^2 - 1) \to k[t]$. More precisely, if $\varphi : X \to Y$ is a morphism, then the corresponding homomorphism h_φ is obtained by pullback. That is, $h_\varphi : \mathscr{O}_Y(Y) \to \mathscr{O}_X(X)$ is characterized by

$$\begin{aligned} h_\varphi = \varphi^* : x_1 &\mapsto \varphi^*(x_1) = x_1 \circ \varphi \in \mathscr{O}_X(X) = k[t], \\ x_2 &\mapsto \varphi^*(x_2) = x_2 \circ \varphi \in \mathscr{O}_X(X) = k[t]. \end{aligned} \tag{2.4.23}$$

Note that indeed $h_\varphi(x_1^2 + x_2^2 - 1) = 0$: Since $\varphi(P) = (Q_1, Q_2)$ lies in Y for all $P \in X$, we see that indeed

$$h_\varphi(x_1^2 + x_2^2 - 1)(P) = x_1(\varphi(P))^2 + x_2(\varphi(P))^2 - 1 = Q_1^2 + Q_2^2 - 1 = 0 \tag{2.4.24}$$

for all $P \in X$, so that $h_\varphi(x_1^2 + x_2^2 - 1)$ is the zero polynomial by Lemma 2.3.12. Conversely, a map $h : k[x_1, x_2]/(x_1^2 + x_2^2 - 1) \to k[t]$ gives rise to a morphism of varieties

$$\begin{aligned} \varphi_h : X &\to Y \\ P &\mapsto (h(x_1)(P), h(x_2)(P)). \end{aligned} \tag{2.4.25}$$

The map φ_h is well-defined because $h(x_1)(P)^2 + h(x_2)(P)^2 - 1 = h(x_1^2 + x_2^2 - 1)(P) = h(0)(P) = 0$.

In fact these considerations show that there does not exist a non-constant morphism of varieties $X \to Y$, as there do not exist univariate polynomials $f_1, f_2 \in k[t]$ such that $f_1^2 + f_2^2 = 1$. It turns out that we can define more morphisms from suitable open subsets of X to those of Y, as we will see later.

Remark 2.4.26. We have been quite pedantic in Example 2.4.15 in that we have not written (2.4.20) in the form $(x_1, x_2) \mapsto x_1$. When one is very careful about these matters, then the components Q_1 and Q_2 of a given point $Q \in Y$ are elements of k, that is, coordinate values (or ordinates), whereas x_1 and x_2 are coordinate functions instead. The morphisms φ involve coordinate values, whereas the homomorphisms h involve coordinate functions instead. In the rest of these notes, we will not be as careful in this regard.

Theorem 2.4.8 enables us to determine the ring of regular functions $\mathscr{O}_X(U)$ on principal open subsets U of affine varieties X by means of a very neat trick. Let us first fix some notation: We assume that $X \subset \mathbb{A}^n$ is defined by a finite system of equations

$$X : \begin{cases} f_1(x_1, \ldots, x_n) & = & 0, \\ \vdots & & \vdots \\ f_r(x_1, \ldots, x_n) & = & 0, \end{cases} \tag{2.4.27}$$

and we consider a polynomial $g \in k[x_1, \ldots, x_n]$ that has non-zero image $\overline{g}$ in the coordinate ring $k[X] = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ of X. We now consider the principal open subset

$$U = D(\overline{g}) = D(g) \cap X \subset X. \tag{2.4.28}$$

Since $\overline{g}$ is non-zero in $k[X]$, this is a non-empty subset of X.

Now consider the affine variety $X_g \subset \mathbb{A}_k^{n+1}$ defined by the following equations:

$$X_g : \begin{cases} f_1(x_1, \ldots, x_n) & = & 0, \\ \vdots & & \vdots \\ f_r(x_1, \ldots, x_n) & = & 0, \\ x_{n+1} g(x_1, \ldots, x_n) - 1 & = & 0. \end{cases} \tag{2.4.29}$$

Theorem 2.4.30. *With notation as above, there are mutually inverse morphisms*

$$\begin{aligned} D(g) &\to X_g \\ (a_1, \ldots, a_n) &\mapsto (a_1, \ldots, a_n, 1/g(a_1, \ldots, a_n)) \\ (a_1, \ldots, a_n) &\leftarrow\!\shortmid (a_1, \ldots, a_n, a_{n+1}). \end{aligned} \tag{2.4.31}$$

Proof. The maps are indeed well-defined because $g(a_1, \ldots, a_n) \neq 0$ for all points $P = (a_1, \ldots, a_n)$ in $D(g)$, and they are also mutually inverse. To show that they are regular, we use Lemma 2.4.5. Since the coordinate functions x_i are certainly regular, we see that the map $X_g \to D(g)$ is a morphism. To show this for the map $D(g) \to X_g$, it suffices to remark that $1/g$ is indeed a rational function with non-zero denominator on $D(g)$, so that it is regular. □

Corollary 2.4.32. *With notation as in Theorem 2.4.30, there is a canonical isomorphism*

$$\begin{aligned} \mathscr{O}_X(D(g)) &= \mathscr{O}_{X_g}(X_g) \\ &= k[x_1, \ldots, x_n, x_{n+1}]/(f_1, \ldots, f_r, x_{n+1} g - 1) \\ &= k[X][x_{n+1}]/(x_{n+1} \overline{g} - 1) \\ &= k[X]_{\overline{g}}. \end{aligned} \tag{2.4.33}$$

In other words, the elements of $\mathscr{O}_X(D(g))$ are represented by rational functions of the form r/g^i, with $r \in k[x_1, \ldots, x_n]$ and with i a positive integer.

Proof. It follows from the definition of an isomorphism of varieties that it induces an isomorphism of coordinate rings. The remaining part of the statement is a consequence of the definition of $k[X]_{\overline{g}}$. □

Example 2.4.34. We again put ourselves in the situation of Example 2.4.15, except that we remove the points $\pm\sqrt{-1}$ from X and replace it by its open subset

$$U = X - \{\pm\sqrt{-1}\} = X \cap D(t^2+1). \tag{2.4.35}$$

Similarly, we remove one point from the circle Y and replace it by its open subset

$$V = Y - \{1,0\} = Y \cap D(x_1 - 1). \tag{2.4.36}$$

Theorem 2.4.30 and Corollary 2.4.32 show that U is isomorphic to an affine variety with coordinate ring

$$k[U] = k[t,(t^2+1)^{-1}] \tag{2.4.37}$$

and that V is isomorphic to an affine variety with coordinate ring

$$k[V] = k[x_1,x_2,(x_1-1)^{-1}]/(x_1^2+x_2^2-1). \tag{2.4.38}$$

Now there are more morphisms $U \to V$ and $V \to U$, as can be seen using Theorem 2.4.8. One interesting example of a morphism $\psi : V \to U$ is

$$\begin{aligned} \psi : V &\to U \\ (Q_1,Q_2) &\mapsto \frac{Q_2}{Q_1-1}. \end{aligned} \tag{2.4.39}$$

It has an inverse $\varphi : U \to V$ which is given by

$$\begin{aligned} \varphi : U &\to V \\ P &\mapsto \left(\frac{P^2-1}{P^2+1}, \frac{-2P}{P^2+1}\right). \end{aligned} \tag{2.4.40}$$

We see that the affine circle with one point removed is isomorphism to the projective line with three points removed. There is a deeper reason behind for this result, which we will consider later.

Remark 2.4.41. The reason that there is no simple description of the ring of regular functions $\mathscr{O}_X(U)$ on the open subset $U \subset X$ from Example 2.3.2 is that there is no description of U as an open subset of the form $D(f)$. To prove that this is indeed the case is a more complicated matter, which we will take up later.

Note that for the curve X from Example 2.3.2 Theorem 2.4.30 still shows that

$$\mathscr{O}_X(X - \{(0,1),(0,-1)\}) = k[X]_{x_1} = k[x_1,x_2,x_3]/(x_2^2 - x_1^3 + x_1 - 1, x_3x_1 - 1) \tag{2.4.42}$$

and

$$\mathscr{O}_X(X - \{(-1,0),(0,0),(1,0)\}) = k[X]_{x_2} = k[x_1,x_2,x_3]/(x_2^2 - x_1^3 + x_1 - 1, x_3x_2 - 1) \tag{2.4.43}$$

since $X - \{(0,1),(0,-1)\} = D(x)$ and $X - \{(-1,0),(0,0),(1,0)\} = D(y)$.

Remark 2.4.44. Consider the open subset $U = \mathbb{A}_k^2 - \{(0,0)\}$ of $\mathbb{A}_k^2$. Then since $U = D(x_1) \cup D(x_2)$ we have

$$\mathscr{O}_X(U) = \mathscr{O}_X(D(x_1)) \cap \mathscr{O}_X(D(x_2)) = k[x_1,x_2]_{x_1} \cap k[x_1,x_2]_{x_2} = k[x_1,x_2]. \tag{2.4.45}$$

2.5 Projective varieties

We will now define certain closures of affine algebraic varieties in a larger space obtained by adding points "at infinity". Such a closure can be seen as a compactification of the original variety, and using them will be necessary for many later results.

Definition 2.5.1. The n-dimensional projective space $\mathbb{P}^n_k$ over k (usually abbreviated to $\mathbb{P}^k$ when k is clear from the context) is defined as

$$\mathbb{P}^n_k = \left\{(a_0,\dots,a_n) \in k^{n+1} \mid (a_0,\dots,a_n) \neq (0,\dots,0)\right\}/\sim, \tag{2.5.2}$$

where the equivalence relation $\sim$ is defined by

$$(a_0,\dots,a_n) \sim (b_0,\dots,b_n) \quad \Leftrightarrow \quad \exists \lambda \in k^* : a_i = \lambda b_i \text{ for all } i = 0,\dots,n. \tag{2.5.3}$$

We will denote the point in $\mathbb{P}^n$ given by the equivalence class of a non-zero element $(a_0,\dots,a_n) \in k^{n+1}$ by

$$(a_0 : \dots : a_n) \in \mathbb{P}^n. \tag{2.5.4}$$

If $(a_0 : \dots : a_n) \in \mathbb{P}^n$, then by definition one of the a_i is non-zero. (Note that the property that the i-th coordinate of $(a_0 : \dots : a_n)$ is non-zero is independent of the chosen representative, even though the actual value of said coordinate is not.) In other words: $\mathbb{P}^n$ is covered by the standard open subsets $U_0,\dots,U_n$ defined by

$$U_i = \{(a_0 : \dots : a_n) \in \mathbb{P}^n \mid a_i \neq 0\}. \tag{2.5.5}$$

Proposition 2.5.6. *The map*

$$\begin{aligned} \varphi_i : U_i &\to \mathbb{A}^n \\ (a_0/a_i,\dots,a_n/a_i) &\leftarrow\!\shortmid (a_0,\dots,a_n) \qquad \textit{(fraction } a_i/a_i \textit{ removed on the left hand side)} \end{aligned} \tag{2.5.7}$$

is a bijection. Its inverse is given by

$$\begin{aligned} \mathbb{A}^k_n &\to U_i \\ (b_1,\dots,b_n) &\mapsto (b_1,\dots,1,\dots,b_n) \qquad \textit{(1 at the } i\textit{-the coordinate on the right hand side).} \end{aligned} \tag{2.5.8}$$

Proof. The composed map $\mathbb{A}^n \to \mathbb{A}^n$ is the identity because the i-th coordinate of $(b_1,\dots,1,\dots,b_n)$ equals 1 by construction, and the composed map $U_i \to U_i$ is the identity because if $a_i \neq 0$ then indeed

$$(a_0 : \dots, a_n) = (a_0/a_i : \dots : a_n/a_i) \tag{2.5.9}$$

as the representatives on both sides of this equation are transformed into each other by multiplication with the non-zero scalar a_i. □

When seeing Proposition 2.5.6 the reader may be reminded of an atlas. And indeed these bijections enable us to give $\mathbb{P}^n$ a structure of locally ringed space. The maps φ already enable us to define a structure of locally ringed space $(U_i, \mathscr{O}_{U_i})$ on the open sets U_i by transferring that structure from $(\mathbb{A}^n, \mathscr{O}_{\mathbb{A}^n})$. That is, we impose that a subset $V \subset U_i$ is open if and only if $\varphi_i(V)$ is open with respect to the Zariski topology on $\mathbb{A}^k_n$, and that for such an open set $V \subset U_i$, a function $f : V \to \mathbb{A}^1$ is regular (that is, an element of $\mathscr{O}_{U_i}(V)$) if and only if the composition $f\varphi_i^{-1}$ is regular as a function on $\varphi_i(V) \subset \mathbb{A}^n$.

Remark 2.5.10. Note that a function $f : U_i \cap U_j \to \mathbb{A}^1$ can be considered both as a function f_i on $U_i \cap U_j$ considered as an open subset of U_i and as a function f_j on $U_i \cap U_j$ considered as an open subset of U_j. We claim that using the definitions above, f_i is regular if and only if f_j is. In other words: the composition $f\varphi_i^{-1}$ is regular on $\varphi_i(U_i \cap U_j) \subset \mathbb{A}^n$ if and only if $f\varphi_j^{-1}$ is regular on $\varphi_j(U_i \cap U_j) \subset \mathbb{A}^n$. This observation is a consequence of the fact that the composed map

$$\begin{aligned} \varphi_j\varphi_i^{-1} : \varphi_i(U_i \cap U_j) &\to \varphi_j(U_i \cap U_j) \\ (b_1, \dots, b_n) &\mapsto (b_1/b_j, \dots, 1/b_j, \dots, b_n/b_j) \end{aligned} \tag{2.5.11}$$

(where $1/b_j$ occurs at the i-th entry) an isomorphism of quasi-affine varieties, with inverse morphism

$$\begin{aligned} \varphi_i\varphi_j^{-1} : \varphi_j(U_i \cap U_j) &\to \varphi_i(U_i \cap U_j) \\ (b_1, \dots, b_n) &\mapsto (b_1/b_i, \dots, 1/b_i, \dots, b_n/b_i) \end{aligned} \tag{2.5.12}$$

(where $1/b_i$ occurs at the j-th entry). This implies that composition with $\varphi_j\varphi_i^{-1}$ preserves regularity by definition, and of course $f\varphi_i^{-1} = (f\varphi_j^{-1})(\varphi_j\varphi_i^{-1})$. The same remark applies to functions defined on open subsets V of $U_i \cap U_j$.

Now let $V \subset \mathbb{P}^n$ be a general open subset. We define a topology on $\mathbb{P}^n$ by decreeing that V is open if and only if $V \cap U_i$ is open in U_i for all $i = 0, \dots, n$. Moreover, given such an open subset $V \subset \mathbb{P}^n$, a function $f : V \to \mathbb{A}^1$ is decreed to be regular (that is, an element of $\mathscr{O}_{\mathbb{P}^n}(V)$) if and only if the restriction $f|_{V \cap U_i} : V \cap U_i \to \mathbb{A}^k_1$ is regular for all $i = 0, \dots, n$.

Theorem 2.5.13. *The above topology on $\mathbb{P}^n$ and the sheaf $\mathscr{O}_{\mathbb{P}^n}$ are well-defined, and with them, $(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n})$ is a locally ringed space. Finally, we have*

$$(U_i, \mathscr{O}_{\mathbb{P}^n}|_{U_i}) = (U_i, \mathscr{O}_{U_i}) \cong (\mathbb{A}^n, \mathscr{O}_{\mathbb{A}^n}). \tag{2.5.14}$$

Proof. The verification that the set of subsets of $\mathbb{P}^n$ obtained by the decrees above is indeed a topology is left to the reader as an exercise, as is the fact that $\mathscr{O}_{\mathbb{P}^n}$ is a sheaf.

The fact that the ringed space $(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n})$ is a locally ringed space is a formal verification. Indeed, the sets U_i are open, so by our definition of regularity on $\mathbb{P}^n$ by means of restriction, the stalk of $\mathscr{O}_{\mathbb{P}^n}$ at a point $P \in U_i$ can be identified with the stalk of $\mathbb{A}^n$ at the point $\varphi_i^{-1}(P)$, which is known to be a local ring by Proposition 2.3.10.

As for the final statement, let $V \subset U_i$. Then a regular function in $\mathscr{O}_{\mathbb{P}^n}(V)$ has to be an element of $\mathscr{O}_{U_i}(V)$ by definition of the sheaf $\mathscr{O}_{\mathbb{P}^n}$. The converse, that any element f of $\mathscr{O}_{U_i}(V)$ is in fact also an element of $\mathscr{O}_{\mathbb{P}^n}(V)$, is a priori less clear. For this, we use Remark 2.5.10, which shows that for all $j = 0, \dots, n$, the restriction $f|_{U_j \cap V} = f_{U_i \cap U_j \cap V}$ is regular considered as a function on $U_j \cap V$ as an open subset of U_j, since by assumption it is regular as a function on $U_j \cap V$ as a subset of $U_i \cap V$. □

Example 2.5.15. We consider the projective line $\mathbb{P}^1$. In this case, the sets U_i become especially concrete. There are two of them, namely

$$\begin{aligned} U_0 &= \left\{(a_0 : a_1) \in \mathbb{P}^1 : a_0 \neq 0\right\} = \{(1 : t) : t \in k\} \quad \text{and} \\ U_1 &= \left\{(a_0 : a_1) \in \mathbb{P}^1 : a_1 \neq 0\right\} = \{(t : 1) : t \in k\}. \end{aligned} \tag{2.5.16}$$

The trivializations are given by

$$\begin{aligned} \varphi_0 : U_0 &\to \mathbb{A}^1 \\ (a_0 : a_1) &\mapsto a_1/a_0 \\ (1 : t) &\hookleftarrow t \end{aligned} \tag{2.5.17}$$

and

$$\begin{aligned} \varphi_1 : U_1 &\to \mathbb{A}^1 \\ (a_0 : a_1) &\mapsto a_0/a_1 \\ (t : 1) &\leftarrow\!\shortmid t \end{aligned} \tag{2.5.18}$$

and the compositions $\varphi_0\varphi_1^{-1}$ and $\varphi_1\varphi_0^{-1}$, both defined on

$$\varphi_0(U_0 \cap U_1) = \varphi_1(U_1 \cap U_0) = \mathbb{A}^1 - \{0\}, \tag{2.5.19}$$

are given by

$$\varphi_0\varphi_1^{-1} = \varphi_1\varphi_0^{-1} : t \mapsto t^{-1}. \tag{2.5.20}$$

More concretely, that means that if $(a_0 : a_1)$ is a point with $a_0 \neq 0$ and $a_1 \neq 0$, then the corresponding parameters

$$\varphi_0(a_0 : a_1) = a_1/a_0 \tag{2.5.21}$$

and

$$\varphi_1(a_0 : a_1) = a_0/a_1 \tag{2.5.22}$$

are each other's multiplicative inverses. The open set U_0 contains the further point $(1 : 0)$, whereas U_1 contains the further point $(0 : 1)$.

The function

$$\begin{aligned} f : U_1 &\to \mathbb{A}^1 \\ (a_0 : a_1) &\mapsto (a_0^2 + a_0a_1)/a_1^2 \end{aligned} \tag{2.5.23}$$

is well-defined, as it is invariant under scaling a_0 and a_1 simultaneously. It is also regular: Under the isomorphism φ_1 it corresponds to the function

$$\begin{aligned} \mathbb{A}^1 &\to \mathbb{A}^1 \\ t &\mapsto f(\varphi_1^{-1}(t)) = f(t : 1) = t^2 + t. \end{aligned} \tag{2.5.24}$$

Via the other chart φ_0, we can consider the restriction of f to the overlap $U_0 \cap U_1$ as a function on $\varphi_0(U_0 \cap U_1) = \mathbb{A}^1 - \{0\}$. Using this alternative trivialization, the function is given by

$$\begin{aligned} \mathbb{A}^1 - \{0\} &\to \mathbb{A}^1 \\ t &\mapsto f(\varphi_0^{-1}(t)) = f(1 : t) = (1+t)/t^2 \end{aligned} \tag{2.5.25}$$

which is indeed a regular function on $\mathbb{A}^1 - \{0\}$ Note that the functions (2.5.24) and (2.5.25) are indeed obtained from each other by composition with $\varphi_0\varphi_1^{-1} = \varphi_1\varphi_0^{-1}$, that is, by substituting t^{-1} for t.

While this is a satisfactory description of projective n-space, there is a far more elegant one that uses homogeneous polynomials, that is, polynomials in $k[x_0, \dots, x_n]$ the total degree of all of whose monomials is identical. For example (and this is no coincidence, as we shall see) the numerator and denominator of the regular function from Equation (2.5.23) are homogeneous polynomials. We will now define another topology, which is at least a priori different from that obtained in Theorem 2.5.13. It is motivated by the following observations, which we do not prove.

Proposition 2.5.26. *Let $F \in k[x_0, \dots, x_n]$. Then the following statements are equivalent:*

(i) If $F(a_0, \dots, a_n) = 0$, then also $F(\lambda a_0, \dots, \lambda a_n) = 0$ for all $\lambda \in k^*$;

(ii) F is homogeneous.

Proposition 2.5.27. *Let $\mathfrak{a} \subset k[x_0, \ldots, x_n]$ be an ideal, and for $d \in Z$ define*

$$\mathfrak{a}_d = \{f \in I : f \text{ homogeneous of degree } d\} \cup \{0\}. \tag{2.5.28}$$

Then the following statements are equivalent:

(i) If $F(x_0, \ldots, x_n) \in \mathfrak{a}$, then also $F(\lambda x_0, \ldots, \lambda x_n \in \mathfrak{a})$ for all $\lambda \in k^*$;

(ii) $\mathfrak{a}$ is generated by a set of homogeneous polynomials;

(iii) $\mathfrak{a}$ is homogeneous, that is, we have $\mathfrak{a} = \bigoplus_d \mathfrak{a}_d$.

In other words: the homogeneous polynomials and ideals in $k[x_0, \ldots, x_n]$ are exactly those whose zero locus is invariant under scaling by elements of k^*, and therefore well-defined as a subset of $\mathbb{P}^n$ (instead of merely $\mathbb{A}_k^{n+1}$). Given a homogeneous ideal $\mathfrak{a}$, we define its zero locus $V(\mathfrak{a})$ in $\mathbb{P}^n$ by

$$V(\mathfrak{a}) = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n \mid F(a_0, \ldots, a_n) = 0 \text{ for all } F \in \mathfrak{a}\}. \tag{2.5.29}$$

Definition 2.5.30. We define the Zariski topology on $\mathbb{P}^1$ to be the topology whose closed subsets are the zero loci $V(\mathfrak{a})$ of homogeneous ideals defined above.

In fact, this is exactly the topology that we considered in Theorem 2.5.13, as the following Proposition shows. (See also [2, Proposition I.2.2].)

Proposition 2.5.31. *The map $\varphi_i : U_i \to \mathbb{A}^n$ from Proposition 2.5.6 is a homeomorphism from U_i (equipped with the induced topology) to $\mathbb{A}^n$ (equipped with the Zariski topology).*

Proof. We first set up our construction: Given a homogeneous polynomial $F \in k[x_0, \ldots, x_n]$ we define the corresponding dehomogenized polynomial $\operatorname{dehom}(F) \in k[y_1, \ldots, y_n]$ by

$$\operatorname{dehom}(F) = f(y_1, \ldots, 1, \ldots, y_n) \tag{2.5.32}$$

where the 1 occurs in the i-th place. Conversely, given $f \in k[y_1, \ldots, y_n]$, we define the corresponding homogenized polynomial $\hom(f) \in k[x_0, \ldots, x_n]$ by

$$x_i^{\deg(f)} f(x_0/x_i, \ldots, x_n/x_i), \tag{2.5.33}$$

where the fraction x_i/x_i is omitted.

Now suppose that $Y \subset U_i$ is closed. Consider its closure $\overline{Y} \subset \mathbb{P}^n$. By definition, we have $\overline{Y} = V(T)$ for some subset $T \subset k[x_0, \ldots, x_n]$. Let us show that $\varphi_i(Y) = V(\operatorname{dehom}(T))$. Suppose $Q = (b_1, \ldots, b_n) \in \varphi_i(Y)$. Then $P = \varphi_i^{-1}(Q) = (b_1 : \ldots : 1 : \ldots : b_n)$ is in $Y \subset \overline{Y}$, so $F(P) = 0$ for all $F \in T$. But then in particular $0 = F(b_1, \ldots, 1, \ldots, b_n) = \operatorname{dehom}(F)(Q)$ for all $F \in T$, so that $Q \in V(\operatorname{dehom}(T))$. On the other hand, if $Q \in V(\operatorname{dehom}(T))$, then the same argument shows that $\varphi_i^{-1}(Q) \in V(T) = \overline{Y}$. We also know that $\varphi_i^{-1}(Q) \in U_i$, and since Y is closed in U_i, we conclude that $\varphi_i^{-1}(Q) \in U_i \cap \overline{Y} = Y$.

Conversely, suppose that $Y \subset \mathbb{A}^n$ is closed. Then $Y = V(S)$ for some subset $S \subset k[y_1, \ldots, y_n]$. Let us show that $\varphi_i^{-1}(Y) = V(\hom(S)) \cap U_i$. If $Q \in Y = V(S) \subset \mathbb{A}^n$, then certainly $\varphi_i^{-1}(Q) \in \varphi^{-1}(\mathbb{A}^n) = U_i$. In addition, we have that $f(b_1, \ldots, b_n) = 0$ for all $f \in S$. With $P = \varphi_i^{-1}(Q) = (b_1, \ldots, 1, \ldots b_n) = (a_0, \ldots, a_n)$ as above, we also see that $\operatorname{dehom}(f)(P) = a_i^{\deg(f)} f(a_0/a_i, \ldots, a_n/a_i) = f(b_1, \ldots, b_n) = 0$ for all $f \in S$, so that indeed $P = \varphi^{-1}(Q) \in V(\operatorname{dehom}(S))$. On the other hand, suppose that $P \in V(\hom(S)) \cap U_i$. Then we can write $P = (b_1 : \ldots : 1 : \ldots :$

b_n). Since $P \in V(\hom(S))$, we have that $0 = \hom(f)(P) = 1^{\deg(f)} f(b_1/1, \ldots, b_n/1) = f(b_1, \ldots, b_n)$ for all $f \in S$. But this means that $Q = \varphi_i(P) = (b_1, \ldots, b_n)$ is in $V(S) = Y$.

We have shown that the bijections φ_i and φ_i^{-1} maps closed subsets to closed subsets. Taking complements, we see that they map open subsets to open subsets, which proves the proposition. □

Definition 2.5.34. A projective variety is a closed subset of $\mathbb{P}^n$, equipped with the induced Zariski topology. A quasi-projective variety is an open subset of a projective variety.

Definition 2.5.35. Let $Y \subset \mathbb{A}^n$ be a subset. We can consider $\mathbb{A}^n$ as the open subset U_0 of $\mathbb{P}^n$ via the map

$$\iota = \varphi_0^{-1} : (t_1, \ldots, t_n) \mapsto (1, t_1, \ldots, t_n). \tag{2.5.36}$$

We define the projective closure of Y to be the closure of $\iota(Y)$ with respect to the Zariski topology on $\mathbb{P}^n$.

As in the case of affine varieties, we can construct a converse to the construction of the zero locus.

Definition 2.5.37. Let $Y \subset \mathbb{P}^n$. The homogeneous ideal of vanishing $I(Y)$ of Y is defined by

$$I(Y) = \{F \in k[x_0, \ldots, x_n] \mid F(P) = 0 \text{ for all } P \in Y\} \subset k[x_0, \ldots, x_n]. \tag{2.5.38}$$

Note that this ideal is homogeneous by Proposition 2.5.27.

Remark 2.5.39. It turns out that once again we have

$$V(I(Y)) = \overline{Y} \tag{2.5.40}$$

for all subsets $Y \subset \mathbb{P}^n$.

Moreover, a version of the Nullstellensatz holds: We have

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}} \tag{2.5.41}$$

for all homogeneous ideals $\mathfrak{a} \subset k[x_0, \ldots, x_n]$, provided that $V(\mathfrak{a}) \neq \emptyset$.

Finally, as for $\mathbb{A}^n$ one can show that $\mathbb{P}^n$ is irreducible as a topological space. We skip the proof of these statements; they are obtained by adapting the arguments from the affine case.

Proposition 2.5.42. *Suppose that $Y \subset \mathbb{A}^n$, with projective closure $\overline{Y} \subset \mathbb{P}^n$. Then*

$$I(\overline{Y}) = \langle \hom(I(Y)) \rangle. \tag{2.5.43}$$

Proof. Since both sides of (2.5.43) are homogeneous, we may assume that F is homogeneous. Moreover, we may assume that Y is closed, since $I(Y) = I(V(I(Y))) = I(Z)$ for the affine closure $Z \subset \mathbb{A}^n$ of Y by Proposition 2.2.30 and Theorem 2.2.33, and similarly $I(V(I(\overline{Y}))) = I(\overline{Y}) = I(\overline{Z})$ by Remark 2.5.39, so that neither side of (2.5.43) changed when Y is replaced by Z.

Suppose first that $F \in I(\overline{Y}) \subset k[x_0, \ldots, x_n]$. Then in particular $F(P) = 0$ for all $P = (1 : b_1 : \ldots : b_n)$ in $\overline{Y} \cap \mathbb{A}^n = Y$. Therefore $\operatorname{dehom}(F) \in I(Y)$. Now we have $\hom(\operatorname{dehom}(F)) = x_0^{-d} F$ for some positive integer d. Since F is in the ideal $I(\overline{Y})$ if and only $x_0 F$ is, we may in fact assume that $d = 0$, which shows that indeed $F = \hom(\operatorname{dehom}(F)) \in \hom(I(Y))$.

For the converse, it suffices to show that if $f \in I(Y)$, then $F = \hom(f) \in I(\overline{Y})$. So consider such an $f \in I(Y) \subset k[y_1, \ldots, y_n]$. Then arguing as in the proof of Proposition 2.5.31, we see that $V(F) \cap \mathbb{A}^n = V(f)$. This implies that F is everywhere zero on Y, but then it is everywhere 0 on the closure $\overline{Y}$ as well, since $V(F)$ is after all closed in $\mathbb{P}^n$. We have shown the reverse inclusion, and with it, the proposition. □

Example 2.5.44. Suppose that $Y \subset \mathbb{A}^2_k$ is an affine curve with $I(Y) = (f)$ for an irreducible polynomial $f \in \mathbb{A}^2_k$. Then Proposition 2.5.42 shows that the projective closure $\overline{Y}$ of Y is defined by the homogenization $F = \mathrm{hom}(f)$ of f, that is,

$$\overline{Y} = V(F) = V(\mathrm{hom}(f)). \tag{2.5.45}$$

Remark 2.5.46. In general, it is *not* true that if $Y \subset \mathbb{A}^n$ is such that $Y = V(T)$, then the projective closure $\overline{Y}$ of Y is given by $V(\mathrm{hom}(T))$. An example is given by the twisted cubic curve

$$Y = V(x_2 - x_1^2, x_3 - x_1^3) \subset \mathbb{A}^k_3. \tag{2.5.47}$$

This example is considered in more detail in the exercises.

Let $X \subset \mathbb{P}^n$ be a projective variety. To define the notion of regular functions on X, we reduce our considerations to the standard affine subsets of X.

Definition 2.5.48. Let $U \subset X$ be an open subset, and let $P \in U$. Suppose that a function $f : U \to \mathbb{A}^1$ is given. Then we say that f is regular at P if $f|_{U \cap U_i}$ is regular at P for some standard open subset U_i that contains P. We say that f is regular if it is regular at all $P \in U$.

Remark 2.5.49. As in the proof of Theorem 2.5.13, one can apply Remark 2.5.10 to show that Definition 2.5.48 makes sense, in that it is independent of the choice of standard open subset U_i that contains P.

As before, we obtain a sheaf of regular functions $\mathscr{O}_X$ on X, and $(X, \mathscr{O}_X)$ is a locally ringed space. We have now in principle defined everything that we need to understand regular functions on projective varieties. Once again, however, there is an elegant rephrasing in terms of homogeneous polynomials, to which we now turn.

Definition 2.5.50. Let $X \subset \mathbb{P}^n$ be a projective variety with homogeneous ideal of vanishing $I(X) \subset k[x_0, \dots, x_n]$. We define the homogeneous coordinate ring $S(X)$ of X by

$$S(X) = k[x_0, \dots, x_n]/I(X). \tag{2.5.51}$$

Since X is a homogeneous ideal, we have a graded decomposition

$$S(X) = \bigoplus_{d=0}^{\infty} S_d \tag{2.5.52}$$

of $S(X)$ by total degree d. In general, given a ring S with such a grading along with a homogeneous prime ideal $\mathfrak{p} \subset S$, we denote the elements of the localization $S_\mathfrak{p}$ that are of degree 0 by $S_{(\mathfrak{p})}$. Also see [2, Theorem I.3.4] for the upcoming results.

Proposition 2.5.53. *Let X be a projective variety X, and let $P \in X$.*

(i) We have $\mathscr{O}_{X,P} = S(X)_{(\mathfrak{m}_P)}$, where $\mathfrak{m}_P \subset S(X)$ is the ideal of homogeneous polynomials that vanish in P;

(ii) We have $k(X) = S(X)_{((0))}$.

Proof (sketch). Choose i such that $P \in U_i$, and let $X_i = X \cap U_i$. We know from Theorem 2.3.25 that

$$\mathscr{O}_{X,P} = k[X_i]_{\mathfrak{m}_P}. \tag{2.5.54}$$

Our previous considerations show that $k[X_i]$ is a quotient of

$$k[U_i] = k[x_1/x_i, \dots, x_n/x_i]. \tag{2.5.55}$$

This means that the elements of $\mathcal{O}_{X,P}$ are represented by the quotients r/s with $r,s \in k[x_1/x_i,\ldots,x_n/x_i]$ with $s(P) \neq 0$). Rewriting these as homogeneous functions in the x_i we obtain Part (i), and Part (ii) is proved similarly. Note that we need the numerator and denominator of the homogeneous involved to be of equal homogeneous degree for f to be well-defined. □

Example 2.5.56. We reverse-engineer Example 2.5.15. There we considered the element of the function field of $X = \mathbb{P}^1$ represented by the rational function $t \mapsto (1+t)/t^2$ on a subset of the standard open subset U_0 of $\mathbb{A}^k_1$ with parameter $t = a_1/a_0$. Substituting, we obtain the homogeneous expression

$$\frac{1+(a_1/a_0)}{(a_1/a_0)^2} = (a_0^2 + a_0a_1)/a_1^2 \tag{2.5.57}$$

which is in fact the expression that we started with.

Example 2.5.58. Let us consider the projective curve

$$E : y^2z = x^3 - 2xz^2 + 5z^3. \tag{2.5.59}$$

which admits the points $P = (1:2:1)$ and $O = (0:1:0)$. Since yz and x^2 are both monomials of homogeneous degree 2 and x^2 does not vanish identically on E, we have that $f = yz/x^2 \in S(E)_{((0))}$, so that Proposition 2.5.53 shows that f is a rational function on E. Moreover, since x^2 does not vanish in P, we obtain that $f \in S(E)_{(\mathfrak{m}_P)} = O_{E,P}$.

It is not immediately obvious what we can say about f as a function in a neighborhood of O, since direct substitution of f in O leads to $0/0$. Instead, we can rewrite f

$$f = \frac{yz}{x^2} = \frac{xy}{y^2 + 2xz - 5z^2} \in k(E) \tag{2.5.60}$$

since

$$(yz)(y^2 + 2xz - 5z^2) = x^2(xy) \tag{2.5.61}$$

in the homogeneous coordinate ring $S(E) = k[x,y,z]/(y^2z - x^3 + 2xz^2 - 5z^3)$. Indeed, the difference between the two sides of (2.5.61) equals

$$y^3 + 2xyz^2 - 5yz^3 - x^3y = y(y^2z - x^3 + 2xz^2 - 5z^3) = 0 \in S(E). \tag{2.5.62}$$

The new expression on the right hand side of (2.5.60) shows that f can be extended to a function that is well-defined in O, where it then has value $0/1 = 0$.

Note that using Proposition 2.5.6, we see that the standard affine patch $U = E \cap D(z)$ is described by the defining equation

$$U : y^2 = x^3 - 2x + 5 \tag{2.5.63}$$

and that if $(x:y:z) \in E$ with $z \neq 0$, then $(x/z, y/z) \in U$. On U, the rational function f restricts to y/x^2, which is no longer homogeneous of degree 0. (Even the fact that it is homogeneous is a more coincidence.

To conclude this section, we show a remarkable result on everywhere regular functions on projective varieties.

Theorem 2.5.64. *Let X be a projective variety. Then the everywhere regular functions on X are exactly the constant functions. That is, we have*

$$\mathcal{O}_X(X) = k. \tag{2.5.65}$$

The proof of this fundamental fact, as given in [2, Theorem I.3.4] using the notion of integral extensions, is very elegant.

Remark 2.5.66. Theorem 2.5.64 does not hold for general quasi-projective varieties, as this would allow for poles at the points that are omitted.

2.6 Dimension and regularity

Having considered both affine and projective varieties, we come to the following unifying notion.

Definition 2.6.1. From now on, we will simply call all of the locally ringed spaces defined so far, namely (quasi-)affine varieties and (quasi-)projective varieties over k, an (algebraic) variety over k.

As for smooth manifolds, one can define the dimension of an algebraic variety. To develop this theory in general requires quite a bit of difficult commutative algebra to link the topological and algebraic notions, so instead we limit ourselves to stating the most important results.

Definition 2.6.2. Let X be an irreducible topological space. We define the dimension $\dim(X)$ of X to be the supremum of the set of integers n for which there exists a non-trivial chain of inclusions

$$Z_1 \subsetneq Z_2 \subsetneq \ldots \subsetneq Z_n \subsetneq X \tag{2.6.3}$$

with the Z_i irreducible subsets of X.

The following analogous definition for domains will not be surprising in light of Proposition 2.2.37.

Definition 2.6.4. Let R be a domain. We define the dimension $\dim(R)$ of R to be the supremum of the set of integers n for which there exists a non-trivial chain of inclusions

$$(0) \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n \tag{2.6.5}$$

with the $\mathfrak{p}_i$ prime ideals of R.

The main results on dimension are the following:

Theorem 2.6.6. *Let X be an algebraic variety with function field $k(X)$. Then the following statements hold.*

(i) $\dim(X)$ *equals the transcendence degree of* $k(X)$ *over* k.

(ii) *If X is an affine or quasi-affine variety, then* $\dim(X)$ *also equals* $\dim k[X]$.

(iii) *We have* $\dim \mathscr{O}_{X,P} = \dim(X)$ *for all points* $P \in X$.

Proposition 2.6.7. *Let X be an algebraic variety with affine or projective closure $\overline{X}$. Then* $\dim(X) = \dim(\overline{X})$.

Proposition 2.6.8. *Let $X \subset \mathbb{A}^n$. Then X is an affine variety of dimension $n-1$ if and only if $X = V(f)$ for a non-constant irreducible polynomial $f \in k[x_1, \ldots, x_n]$. Conversely, if $X = V(g)$ for another such polynomial, then $g = \lambda f$ for some $\lambda \in k^*$.*

Proposition 2.6.9. *Let $X \subset \mathbb{P}^n$. Then X is a projective variety of dimension $n-1$ if and only if $X = V(F)$ for a non-constant irreducible homogeneous polynomial $f \in k[x_0, x_1, \ldots, x_n]$. Conversely, if $X = V(G)$ for another such polynomial, then $G = \lambda F$ for some $\lambda \in k^*$.*

Example 2.6.10. Suppose that f is a non-constant irreducible polynomial in $k[x_1,\dots,x_n]$. Then $X = V(f) \subset \mathbb{A}_n^k$ is an algebraic variety. Indeed, since the multivariate polynomial ring $k[x_1,\dots,x_n]$ is a unique factorization domain [4, §2.8], its irreducible element f is prime [4, §2.7], so that X is an algebraic variety by Proposition 2.2.37. It has dimension $n-1$ by Proposition 2.6.8.

Since (f) is a prime ideal, we have that

$$I(X) = I(V(f)) = \sqrt{(f)} = (f). \tag{2.6.11}$$

Proposition 2.5.42 and Example 2.5.44 now show that the projective closure $\overline{X}$ of X is given by

$$\overline{X} = V(\mathrm{hom}(f)) \tag{2.6.12}$$

Both Proposition 2.5.42 and Proposition 2.6.7 now show that $\dim(\overline{X}) = \dim(X) = n-1$.

The notion of dimension plays a role when defining the analog of smoothness for algebraic varieties, which is motivated by the implicit function theorem:

Definition 2.6.13. Let $X \subset \mathbb{A}^n$ be a variety, and let $P \in X$ be a point. Write $X = V(f_1,\dots,f_r)$ for a finite set of polynomials $f_1,\dots,f_r \in k[x_1,\dots,x_n]$ (note that this is possible by Proposition 2.1.8). The Jacobian matrix $J_X(P)$ of X at P (for the given choice of generators f_i) is the matrix defined by

$$J_X(P) = \left(\frac{\partial f_i}{\partial x_j}(P)\right)_{\substack{1\le i\le r,\\ 1\ \le j\le n}} \tag{2.6.14}$$

We say that P is a regular point of X if we have

$$\mathrm{rk}(J_X(P)) = n - \dim(X). \tag{2.6.15}$$

If P is not a regular point of X, then we also say that it is a singular point of X.

Definition 2.6.13 may look convincing, but it is actually quite unsatisfactory. For example, suppose that X is a projective variety, and that the point $P \in X$ belongs to multiple standard affine subset. Then a priori it is possible that Definition 2.6.13 gives different results for the regularity of P depending on the standard affine subset that is used. Moreover, Definition 2.6.13 might depend on our choice of the generators $f_1,\dots,f_r$. To show that this is not the case, we find a criterion for regularity that is intrinsic, in the sense that it only depends on X itself and not on any embedding of X into $\mathbb{A}^n$ (or $\mathbb{P}^n$).

For this, we look more closely at the local ring $\mathcal{O}_{X,P}$ of X at P. Let $\mathfrak{m}_{X,P}$ be its unique maximal ideal. First note that there is an isomorphism

$$\begin{aligned} \mathcal{O}_{X,P}/\mathfrak{m}_{X,P} &\to k \\ f + \mathfrak{m}_{X,P} &\mapsto f(P) \end{aligned} \tag{2.6.16}$$

which is well-defined because Proposition 2.3.10 shows that $\mathfrak{m}_{X,P}$ is exactly the ideal of elements of $\mathcal{O}_{X,P}$ that vanish at P. This implies that the abelian group $\mathfrak{m}_{X,P}/\mathfrak{m}_{X,P}^2$ is a k-module: It is certainly an $\mathcal{O}_{X,P}$-module under multiplication, and the action of $\mathfrak{m}_{X,P}$ on $\mathfrak{m}_{X,P}/\mathfrak{m}_{X,P}^2$ is trivial, since $\mathfrak{m}_{X,P}$ maps $\mathfrak{m}_{X,P}$ to $\mathfrak{m}_{X,P}^2$ under multiplication. In other words, $\mathfrak{m}_{X,P}/\mathfrak{m}_{X,P}^2$ is an $\mathcal{O}_{X,P}/\mathfrak{m}_{X,P}$-module in a natural way, and Equation (2.6.16) then shows that it is also k-module, that is, a k-vector space.

Definition 2.6.17. We say that the local ring $\mathcal{O}_{X,P}$ is regular if

$$\dim(\mathcal{O}_{X,P}) = \dim_k(\mathfrak{m}_{X,P}/\mathfrak{m}_{X,P}^2). \tag{2.6.18}$$

Theorem 2.6.19. *With notation as in Definitions 2.6.13 and 2.6.17, we have that X is non-singular at P if and only if $\mathscr{O}_{X,P}$ is a regular local ring.*

Proof. In order to prove the Theorem, we investigate the k-vector space $\mathfrak{m}_{X,P}/\mathfrak{m}_{X,P}^2$ more closely. First write $P = (a_1, \ldots, a_n)$ and let

$$\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) \subset k[X] \tag{2.6.20}$$

be the corresponding maximal ideal of $k[X] = k[x_1, \ldots, x_n]/I(X)$. We claim that

$$\mathfrak{m}_{X,P} = \mathfrak{m}\mathscr{O}_{X,P}, \tag{2.6.21}$$

or in other words, that the ideal $\mathfrak{m}_{X,P}$ is also generated by the affine functions $x_i - a_i$. This follows because $\mathscr{O}_{X,P} = k[X]_{\mathfrak{m}}$ by Theorem 2.3.25, which implies that every element of $\mathfrak{m}_{X,P}$ is of the form r/s with $r, s \in k[X]$ such that $r(P) = 0$ and $s(P) \neq 0$. This means that $r \in \mathfrak{m}$ and $s \in \mathscr{O}_{X,P}^*$, so that indeed $r/s = rs^{-1} \in \mathfrak{m}\mathscr{O}_{X,P}$.

Equation (2.6.21) implies that the canonical map

$$\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}_{X,P}/\mathfrak{m}_{X,P}^2 \tag{2.6.22}$$

that sends the coset of a function in $\mathfrak{m}$ to the image of its stalk in $\mathfrak{m}_{X,P}/\mathfrak{m}_{X,P}^2$, is a well-defined isomorphism of k-vector spaces. So we study the "global" quotient $\mathfrak{m}/\mathfrak{m}^2$ instead in the rest of the proof. To this end, we will in turn use the ideal

$$\mathfrak{n} = (x_1 - a_1, \ldots, x_n - a_n) \subset k[x_1, \ldots, x_n] \tag{2.6.23}$$

of $k[x_1, \ldots, x_n]$ to study $\mathfrak{m}$, which is the image of $\mathfrak{n}$ in $k[X]$. Once again we obtain a canonical surjective map of k-vector spaces

$$\mathfrak{n}/\mathfrak{n}^2 \to \mathfrak{m}/\mathfrak{m}^2. \tag{2.6.24}$$

Now as a k-vector spaces, we have that

$$\mathfrak{n}/\mathfrak{n}^2 = k(x_1 - a_1) \oplus \ldots \oplus k(x_n - a_n) \tag{2.6.25}$$

since $\mathfrak{n}^2$ is nothing but the ideal of polynomials in the multivariate polynomial ring $k[x_1, \ldots, x_n]$ that are monomials of order ≥ 2 in the $x_i - a_i$. In particular, we see that

$$\dim_k(\mathfrak{n}/\mathfrak{n}^2) = n. \tag{2.6.26}$$

Since $k[X] = k[x_1, \ldots, x_n]$ and $\mathfrak{n}^2$ is the image of $(x_1, \ldots, x_n)$, we have that

$$\begin{aligned} k[X]/\mathfrak{m}^2 &= (k[x_1, \ldots, x_n]/I(X))/(\text{image of } \mathfrak{n}^2\ ) \\ &= k[x_1, \ldots, x_n]/(I(X) + \mathfrak{n}^2) \\ &= (k[x_1, \ldots, x_n]/\mathfrak{n}^2)/(\text{image of } I(X)). \end{aligned} \tag{2.6.27}$$

To obtain $\mathfrak{m}/\mathfrak{m}^2$, we therefore have to quotient out the image of $I(X)$ in $\mathfrak{n}/\mathfrak{n}^2$. But since the action of $\mathscr{O}_{X,P}$ on $\mathfrak{n}/\mathfrak{n}^2$ factors through k, as we have seen, this is nothing but the k-span of the image of a set of generators of the ideal $I(X)$ in $\mathfrak{n}/\mathfrak{n}^2$. Now the Theorem is proved by the observation that given $f \in I(X)$, its expression in terms of the basis used in (2.6.25) is given by

$$\left(\frac{\partial f}{\partial x_1}(P), \ldots, \frac{\partial f}{\partial x_n}(P) \right). \tag{2.6.28}$$

(The proof of this statement is part of an exercise this week.) Indeed, once (2.6.28) is shown, we conclude that in terms of the basis used in (2.6.25), the image of $I(X)$ in $\mathfrak{n}/\mathfrak{n}^2$ is the span of the rows of the Jacobian matrix $J_X(P)$, so that $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = n - \mathrm{rk}(J_X(P))$, which equals $\dim(X)$ as requested if and only if $\mathrm{rk}(J_X(P)) = n - \dim(X)$. $\square$

Remark 2.6.29. One can show that the set of singular points of a variety form a proper closed subset, as one expects intuitively; see [2, Theorem I.5.3].

Example 2.6.30. Consider an affine curve X given by an irreducible polynomial of the form

$$X : y^2 = x^3 + c_4 x + c_6, \tag{2.6.31}$$

where $c_4, c_6 \in k$. Note that X is indeed a curve by Example 2.6.10. We determine the singular points on X.

Given a point $P = (a, b) \in X$, the Jacobian matrix is given by

$$J_X(P) = \left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P) \right) \tag{2.6.32}$$

where $f = y^2 - x^3 - c_4 x - c_6$ is the polynomial for which $X = V(f)$. A calculation shows that

$$J_X(P) = \left(-3a^2 - c_4, 2b \right). \tag{2.6.33}$$

The point P is regular if and only if $J_X(P)$ has rank $2 - \dim(X) = 2 - 1 = 1$, which is the case if and only if said matrix is non-zero. Taking the contrapositive, we see that $P = (a, b)$ is a singular point of X if and only if the system of equations

$$\begin{aligned} b^2 &= a^3 + c_4 a + c_6, \\ 3a^2 + c_4 &= 0, \\ 2b &= 0 \end{aligned} \tag{2.6.34}$$

has a solution.

Let us first suppose that $\mathrm{char}(k) \neq 0$. Then (2.6.34) implies that $b = 0$, and it remains to find the solutions of the system of equations

$$\begin{aligned} a^3 + c_4 a + c_6 &= 0, \\ 3a^2 + c_4 &= 0. \end{aligned} \tag{2.6.35}$$

Let $g = x^3 + c_4 x + c_6$. Then finding solutions to (2.6.35) is the same as finding common zeros of g and $g' = 3x^2 + c_4$. By [4, §3.5], such solutions exist if and only the discriminant

$$D_g = -4c_4^3 - 27c_6^2 \tag{2.6.36}$$

is zero.

An example of a curve for which this happens is

$$X : y^2 = x^3 - 3x + 2. \tag{2.6.37}$$

In this particular case, (2.6.35) becomes

$$\begin{aligned} a^3 - 3a + 2 &= 0, \\ 3a^2 - 3 &= 0, \end{aligned} \tag{2.6.38}$$

which has the unique solution $a = 1$. This gives rise to the singular point $P = (1, 0)$ on X. Note that

$$X : y^2 = (x-1)^2 (x+2), \tag{2.6.39}$$

which explains why X is singular at P: Since y and $x-1$ are elements of the maximal ideal $\mathfrak{n} = (x-1, y) \subset k[x,y]$, we obtain that $y^2 - (x-1)^2(x+2) \in \mathfrak{n}^2$, so that

$$\begin{aligned} \mathfrak{m}/\mathfrak{m}^2 &= (\mathfrak{n}/\mathfrak{n}^2)/(\text{image of } I(X)) \\ &= (\mathfrak{n}/\mathfrak{n}^2)/(y^2 - (x-1)^2(x+2)) \\ &= \mathfrak{n}/\mathfrak{n}^2 \end{aligned} \tag{2.6.40}$$

and

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\mathfrak{n}/\mathfrak{n}^2) = 2 \neq 1. \tag{2.6.41}$$

If $\mathrm{char}(k) = 2$, then the system of equations (2.6.34) becomes

$$\begin{aligned} b^2 &= a^3 + c_4 a + c_6, \\ a^2 + c_4 &= 0. \end{aligned} \tag{2.6.42}$$

Let w_1 be the (unique) square root of c_4 in k, and let w_2 be the (unique) square root of $w_1^3 + c_4 w_1 + c_6$ in k. Then (2.6.42) has the unique solution $P = (w_1, w_2)$.

Finally, let us consider the projective closure E of X. As we have seen in Example 2.5.44, the curve E is defined by the homogenized equation

$$E : y^2 z = x^3 + c_4 x z^2 + c_6 z^3 \tag{2.6.43}$$

The standard open subset $D(z)$ of E equals X (note that we can scale to ensure that $z = 1$, which recovers the original equation (2.6.31) for X). If we put $z = 0$, then we obtain the single new point at infinity

$$O = (0 : 1 : 0) \in E. \tag{2.6.44}$$

We have already determined when the points of $E - \{O\} = X$ are regular. Let us do the same for O. To this end, we use the standard affine subset $D(y)$. Dehomogenizing by putting $y = 1$, we obtain the affine equation

$$z = x^3 + c_4 x z^2 + c_6 z^3, \tag{2.6.45}$$

for which $O = (0, 0)$. Now the Jacobian matrix in O becomes

$$\left(\frac{\partial(z - x^3 - c_4 x z^2 - c_6 z^3)}{\partial x}(0,0), \frac{\partial(z - x^3 - c_4 x z^2 - c_6 z^3)}{\partial z}(0,0) \right) = (0,1). \tag{2.6.46}$$

Since this matrix has rank $1 = 2 - 1 = 2 - \dim(E)$, we see that E is regular at O (independent of the characteristic. Intuitively, the reason for this is that the defining equation (2.6.45) is, up to terms of higher order, approximated by that of its tangent line $z = 0$ at P that corresponds to the vector $(0, 1)$ in (2.6.46) under the isomorphism (2.6.25).

(Note that we have already shown that all other points of the affine patch (2.6.45) are regular when $D_g \neq 0$. Indeed, these points belong to the affine patch X, and we showed in the first part of this example that these points are regular, even though we used a completely different equation. To drive home the point: This is a consequence, perhaps a somewhat surprising one, of the fact that regularity is intrinsic to the point P and X and does not depend on a particular embedding of X into an affine space, as we showed in Theorem 2.6.19.)

2.7 Curves and discrete valuation rings

Definition 2.7.1. An algebraic curve is an algebraic variety of dimension 1.

Remark 2.7.2. It will be shown in an exercise that the Zariski topology on an algebraic curve X is the cofinite topology. This is a direct consequence of the fact that X is of dimension 1.

Local rings of varieties have an especially nice structure when we consider algebraic curves. Before we can state the result, we need an important definition.

Definition 2.7.3. Let K be a field. A discrete valuation on K is a function

$$v : K \to \mathbb{Z} \cap \{\infty\} \tag{2.7.4}$$

with the following properties:

(DV1) We have $v(x) = \infty$ if and only if $x = 0$;

(DV2) For all $x, y \in K$ we have

$$v(xy) = v(x) + v(y); \tag{2.7.5}$$

(DV3) For all x, y in K we have

$$v(x+y) \geq \min\{v(x), v(y)\}. \tag{2.7.6}$$

Remark 2.7.7. One can show that the inequality (2.7.6) is in fact an equality if $v(x) \neq v(y)$.

Example 2.7.8. Let $K = k(x)$ be a rational function field over k, and consider the function

$$\begin{aligned} v_\infty &: K \to \mathbb{Z} \cup \{\infty\} \\ f &= r/s \mapsto \deg(s) - \deg(r). \end{aligned} \tag{2.7.9}$$

where $r, s2 \in k[x]$ are such that $f = r/s$. Then v_∞ is a valuation. Indeed, (DV1) follows from the definition of the degree. Now consider $f_1 = r_1/s_1$ and $f_2 = r_2/s_2$. Then $f_1 f_2 = (r_1 r_2)/(s_1 s_2)$, so that

$$\begin{aligned} v_\infty(f_1 f_2) &= v_\infty((r_1 r_2)/(s_1 s_2)) \\ &= \deg(s_1 s_2) - \deg(r_1 r_2) \\ &= \deg(s_1) + \deg(s_2) - \deg(r_1) + \deg(r_2) \\ &= \deg(s_1) - \deg(r_1) + \deg(s_2) - \deg(r_2) \\ &= v_\infty(f_1) + v_\infty(f_2). \end{aligned} \tag{2.7.10}$$

which shows (DV2). Let us first prove (DV3) for polynomials f_1, f_2. In that case we now that $\deg(f_1 + f_2) \leq \max\{\deg(f_1), \deg(f_2)\}$, so that

$$\begin{aligned} v_\infty(f_1 + f_2) &= -\deg(f_1 + f_2) \\ &\geq -\max\{\deg(f_1), \deg(f_2)\} \\ &= \min\{-\deg(f_1), -\deg(f_2)\} \\ &= \min\{v_\infty(f_1), v_\infty(f_2)\}. \end{aligned} \tag{2.7.11}$$

In general, given rational functions $f_1, f_2 \in k[x]$, we can choose $s \in k[x]$ such that $s f_1 = r_1$ and $s f_2 = r_2$ are both in $k[x]$. Then by (DV2), which we already proved for v_∞, along with (DV3) for polynomials, we get

$$\begin{aligned} v_\infty(f_1+f_2) &= v_\infty((r_1+r_2)/s) \\ &= v_\infty(r_1+r_2) - v_\infty(s) \\ &\geq \min\{v_\infty(r_1), v_\infty(r_2)\} - v_\infty(s) \\ &= \min\{v_\infty(r_1) - v_\infty(s), v_\infty(r_2) - v_\infty(s)\} \\ &= \min\{v_\infty(r_1/s), v_\infty(r_2/s)\} \\ &= \min\{v_\infty(f_1), v_\infty(f_2)\}. \end{aligned} \tag{2.7.12}$$

Note that the degree of a polynomial measures its pole order at infinity, so one might $v_\infty = -\deg$ to measure the zero order of a rational function at the point ∞ of $\mathbb{P}^1$ at infinity. This will indeed turns out to be the case.

Another example of a valuation on $k(X)$ is given by

$$v_0(f) = \begin{cases} n & \text{if } f = x^n(r/s) \text{ with } r,s \in k[x] \text{ non-zero at } 0 \\ \infty & \text{if } f = 0. \end{cases} \tag{2.7.13}$$

This time it is clear from the definition that v_0 measures the zero order of a rational function at $0 \in \mathbb{P}^1$. Let us check that it is indeed a discrete valuation of K. Property (DV1) is clearly fulfilled. For (DV2), write $f_1 = x^{n_1}(r_1/s_1)$ and $f_2 = x^{n_2}(r_2/s_2)$ with r_1, s_1, r_2, s_2 non-zero at 0. Then

$$f_1 f_2 = x^{n_1+n_2}\frac{r_1 r_2}{s_1 s_2} \tag{2.7.14}$$

with $r_1 r_2$ and $s_1 s_2$ non-zero at 0, so that indeed

$$v_0(f_1 f_2) = n_1 + n_2 = v_0(f_1) + v_0(f_2), \tag{2.7.15}$$

which shows (DV2). Let us first prove (DV3) for polynomials f_1, f_2. We can write $f_1 = x^{n_1} r_1$ and $f_2 = x^{n_2} r_2$ with $n_1, n_2 \geq 0$, and we may suppose that $n_1 \leq n_2$. Then we can write

$$f_1 + f_2 = x^{n_1}(f_1 + x^{n_2 - n_1} f_2) \tag{2.7.16}$$

with $f_1 + x^{n_2-n_1} f_2$ a polynomial, so that $v_0(f_1 + x^{n_2-n_1} f_2) \geq 0$. Using (DVR2), we see that

$$\begin{aligned} v_0(f_1+f_2) &= v_0(x^{n_1}(f_1 + x^{n_2-n_1} f_2)) \\ &= v_0(x^{n_1}) + v_0(f_1 + x^{n_2-n_1} f_2) \\ &= n_1 + v_0(f_1 + x^{n_2-n_1} f_2) \\ &\geq n_1 = \min\{n_1, n_2\} = \min\{v_0(f_1), v_0(f_2)\}. \end{aligned} \tag{2.7.17}$$

This shows (DV3) for polynomials f_1, f_2; the general case follows as for v_∞ above.

Note that the discrete valuations v_∞ and v_0 are both trivial on k^*. In the exercises, you will classify the other discrete valuations of K with this property; they will turn out to measure the zero order of a rational function at the other points of $\mathbb{P}^1$.

Proposition 2.7.18. *Let v be a discrete valuation on a field K. Then the valuation ring $\mathcal{O}_v$ of v defined by*

$$\mathcal{O}_v = \{x \in K : v(x) \geq 0\} \tag{2.7.19}$$

is a local ring with maximal ideal

$$\mathfrak{m}_v = \{x \in K : v(x) > 0\}. \tag{2.7.20}$$

Proof. The fact that $\mathscr{O}_v$ is a ring follows by Parts (ii) and (iii) of Definition 2.7.3, and this can also be used to show that $\mathfrak{m}_v$ is a maximal ideal. To show the remainder of the proposition, it suffices to show that $x \in K^*$ has valuation 0 if and only if $x \in \mathscr{O}_v^*$. To this end, first observe that

$$v(1) = v(1^2) = 2v(1), \tag{2.7.21}$$

so that $v(1) = 0$. Now for $x \in K^*$ we have

$$xx^{-1} = 1. \tag{2.7.22}$$

Considering valuations on both sides and using that $v(1) = 0$, we see that $v(x^{-1}) = -v(x)$. On the other hand, we have that x is in $\mathscr{O}_v^*$ if and only if both elements on the left hand side are in $\mathscr{O}_v$. This is equivalent to $v(x) \geq 0$ and $-v(x) = v(x^{-1}) \geq 0$, that is, with $v(x) = 0$. This finishes the proof. □

Example 2.7.23. In the situation of Example 2.7.8, we have

$$\mathscr{O}_{v_\infty} = \{f = r/s \in k(x) \mid \deg(r) \leq \deg(s)\} \tag{2.7.24}$$

and

$$\mathfrak{m}_{v_\infty} = \{f = r/s \in k(x) \mid \deg(r) < \deg(s)\}, \tag{2.7.25}$$

whereas

$$\mathscr{O}_{v_0} = \{f = r/s \in k(x) \mid x \nmid s\} \tag{2.7.26}$$

and

$$\mathfrak{m}_{v_0} = \{f = r/s \in k(x) \mid x \nmid s, x \mid r\}. \tag{2.7.27}$$

Definition 2.7.28. A discrete valuation ring is a ring that is isomorphic to a ring of the form (2.7.19).

For our main theorem, we need one result that is important in its own right. It is a version of Nakayama's famous lemma.

Lemma 2.7.29. *Let M be a finitely generated module over a local ring R with maximal ideal $\mathfrak{m}$. If $\mathfrak{m}M = M$, or in other words if $M/\mathfrak{m}M = 0$, then $M = 0$.*

Proof. Let $m_1, \ldots, m_r$ be a set of generators of M, with r minimal. By hypothesis we can write

$$m_r = \sum_{i=1}^{r} a_i m_i \tag{2.7.30}$$

for certain $a_i \in \mathfrak{m}$. This means that

$$(1 - a_r)m_r = a_1 m_1 + \ldots + a_{r-1} m_{r-1} \tag{2.7.31}$$

But since $a_r \in \mathfrak{m}$ and $1 \notin \mathfrak{m}$, we see that $1 - a_r \notin \mathfrak{m}$, which means $(1 - a_r) \in R^*$ since R is a local ring. Multiplying by its inverse, we see that we can express m_r by means of the other generators, a contradiction with the minimality of r. □

The proof of the upcoming theorem follows [3].

Theorem 2.7.32. *Let X be an algebraic curve, let $P \in X$ be a point, and let $\mathscr{O}_{X,P}$ be the local ring of X at P. Then the following statements are equivalent:*

(i) P is regular;

(ii) $\mathscr{O}_{X,P}$ *is a discrete valuation ring;*

(iii) $\mathscr{O}_{X,P}$ *is integrally closed;*

(iv) *The maximal ideal* $\mathfrak{m}_{X,P} \subset \mathscr{O}_{X,P}$ *is principal;*

(v) *Every proper non-zero ideal of* $\mathscr{O}_{X,P}$ *is a power of* $\mathfrak{m}_{X,P}$.

Proof. Before we start the proof proper, we abbreviate notation by writing $\mathscr{O} = \mathscr{O}_{X,P}$ and $\mathfrak{m} = \mathfrak{m}_{X,P}$. Now observe the following:

(OBS1) The powers $\mathfrak{m}^n$ are distinct for all $n \in \mathbb{N}$;

(OBS2) Every non-zero ideal $\mathfrak{a}$ of $\mathscr{O}$ contains some power $\mathfrak{m}^n$.

Property (OBS1) is a direct consequence of Lemma 2.7.29 for $M = \mathfrak{m}$. Property (OBS2) is a consequence of Theorem 2.2.33; if $\mathfrak{a}$ is a proper non-zero ideal of $\mathscr{O}$, as we may assume, then the radical $\sqrt{\mathfrak{a}}$ corresponds to the closed point corresponding to $\mathscr{O} \subset k(X)$, so that it equals the single maximal ideal of $\mathscr{O}$. Now $\mathscr{O}$ is noetherian, since it is a localization of a quotient of a multivariate ring polynomial ring, so that we can write $\mathfrak{m} = (\gamma_1, \dots, \gamma_r)$ for certain $\gamma_i \in \mathscr{O}$. Because $\sqrt{\mathfrak{a}} = \mathfrak{m}$, there exist positive integers e_i such that $e_i^{n_i} \in \mathfrak{a}$. But then $\mathfrak{m}^N \subset \mathfrak{a}$ for $N = e_1 + \dots + e_r$, since every element of

$$\mathfrak{m}^N = \langle \gamma_1^{N_1} \cdots \gamma_r^{N^r} \ : \ \sum_{i=1}^r N_i \rangle \tag{2.7.33}$$

is a multiple of some element $\gamma_i^{e_i} \in \mathfrak{a}$, as not every N_i on the right hand side of (2.7.33) can be strictly smaller than e_i.

(ii) $\Rightarrow$ (iii): Suppose that $\mathscr{O} = \mathscr{O}_v$ for a valuation v on $k(X)$, and let $\alpha \in k(X) \setminus \mathscr{O}_v$, so that $e = v(\alpha) < 0$. We have to show that α is not integral over $\mathscr{O}_v$. In the contrary case, there would exist $a_{n-1}, \dots, a_0 \in \mathscr{O}_v$ such that

$$\alpha^n = a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0. \tag{2.7.34}$$

Since $v(a_i) \geq 0$ for all i, the valuations of the terms on the right hand side of (2.7.34) are all at most $(n-1)e$. Hence the same holds for their sum by (DV3). This is a contradiction, because the valuation of the left hand side of (2.7.34) equals ne, which is strictly smaller than $(n-1)e$ because $e < 0$.

(iii) $\Rightarrow$ (iv): Consider a non-zero element $a \in \mathfrak{m}$, and choose n minimal such that $\mathfrak{m}^n \subset (a)$ (and therefore $(1/a)\mathfrak{m} \subset \mathscr{O}$). Since $\mathfrak{m} \subsetneq \mathfrak{m}^{n-1}$ by (OBS1), there exists an element $b \in \mathfrak{m}^{(n-1)} \setminus (a)$. If we let $\pi = a/b$, then $\pi^{-1} \notin \mathscr{O}$ since $b \notin (a)$. Moreover, we have

$$\pi^{-1}\mathfrak{m} = (b/a)\mathfrak{m} = (1/a)(b\mathfrak{m}) \in (1/a)\mathfrak{m}^n \subset \mathscr{O} \tag{2.7.35}$$

Suppose that $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$. Choosing generators $\gamma_1, \dots, \gamma_r$ of the finitely generated $\mathscr{O}$-module $\mathfrak{m}$ as above, we see that we can write

$$\pi^{-1}\gamma_i = \sum_{j=1}^r a_{ij}\gamma_j \tag{2.7.36}$$

for certain $a_{ij} \in \mathscr{O}$. Applying Cramer's rule to this system of equations, we see that $\det((a_{ij} - \delta_{ij}\pi^{-1})_{i,j})$ is zero, which implies that π^{-1} is integral over $\mathscr{O}$. But this is nonsense, because $\mathscr{O}$

is integrally closed by hypothesis and we saw above that $\pi^{-1} \notin \mathscr{O}$. The only other possibility besides $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$ is $\pi^{-1}\mathfrak{m} = R$, that is, $\mathfrak{m} = (\pi)$ is a principal ideal.

(iv) $\Rightarrow$ (i): If $\mathfrak{m} = (\alpha)$ as an $\mathscr{O}$-module, then $\mathfrak{m}/\mathfrak{m}^2 = (\alpha)$ as an $\mathscr{O}/\mathfrak{m}$-module, that is, as a k-vector space, so that $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$ by (OBS1).

(i) $\Rightarrow$ (v): If $\pi \in \mathscr{O}$ generates the 1-dimensional k-vector space $\mathfrak{m}/\mathfrak{m}^2$, then $(\pi) = \mathfrak{m}$ by Nakayama's Lemma applied to $M = \mathfrak{m}/(\pi)$. Given another non-zero ideal $\mathfrak{a}$ of $\mathscr{O}$, we can use (OBS2) to find a maximal integer $n \geq 1$ such that $\mathfrak{a} \subset \mathfrak{m}^n$. By definition of n, there exists $\alpha \in \mathfrak{a} \setminus \mathfrak{m}^{n+1}$. Since $\alpha \in \mathfrak{a}$, we can write $\alpha = u\pi^n$ for some $u \in \mathscr{O}$, and since $\alpha \notin \mathfrak{m}^{n+1}$, we have $u \notin \mathfrak{m}$, so that $u \in \mathscr{O} \setminus \mathfrak{m}$ is a unit. We see that

$$(\alpha) = (u\pi^n) = (u)(\pi)^n = \mathfrak{m}^n. \tag{2.7.37}$$

Since $\alpha \in \mathfrak{a}$, we have $\mathfrak{m}^n = (\alpha) \subset \mathfrak{a}$. Since we already knew that $\mathfrak{a} \subset \mathfrak{m}^n$, we see that $\mathfrak{a} = \mathfrak{m}^n$, which was to be shown.

(v) $\Rightarrow$ (ii): Given an element $\alpha \in \mathscr{O}$, we define $v(\alpha)$ to be the integer n such that $\alpha = \mathfrak{m}^n$. Note that n is unique by (OBS2). We extend v to $k(X) = Q(\mathscr{O})$ by $v(\alpha/\beta) = v(\alpha) - v(\beta)$. The proof that v is indeed a valuation is then analogous to the methods used in Example 2.7.8. It is left as an exercise. □

Remark 2.7.38. The proof of Theorem 2.7.32 in fact shows that $\mathfrak{m}_{X,P}$ is generated by any element of $\mathfrak{m}_{X,P} \setminus \mathfrak{m}_{X,P}^2$. Such an element, typically denoted by $\pi_{X,P}$, π_P, or π, is called a uniformizer of the ring $\mathscr{O}_{X,P}$ (or of the curve X at the point P). Moreover, our construction of the valuation v_P of $k(X)$ that corresponds to a point X shows that v_P is trivial on k^*.

Example 2.7.39. Consider the affine curve

$$X : y^2 = x^5 - 2x + 1. \tag{2.7.40}$$

over the base field $k = \overline{\mathbb{Q}}$. Using the Jacobian criterion, it can be verified that X is indeed a non-singular curve, since the polynomial $x^5 - 2x + 1$ does not have multiple roots. We determine generators for the maximal ideal of some points of X.

We first take $P = (0,1)$. Since $\mathfrak{m}_{X,P}$ is the image in $k[X]$ of the maximal ideal $\mathfrak{n} = (x, y-1)$ of $k[x,y]$, we see that $\mathfrak{m}_{X,P}$ is generated by x and $y - 1$. We already know a priori that one of x and $y - 1$ is in $\mathfrak{m}_{X,P} \setminus \mathfrak{m}_{X,P}^2$ (and perhaps both are) since otherwise we would have $\mathfrak{m}_{X,P} = \mathfrak{m}_{X,P}^2$, hence $\mathfrak{m}_{X,P} = 0$ by Nakayama's Lemma, which is absurd. To find which of x and $y - 1$ is in $\mathfrak{m}_{X,P}$, we define $\widetilde{y} = y - 1$ and rewrite the equation of X as

$$X : \widetilde{y}^2 - 2\widetilde{y} = x^5 - 2x \tag{2.7.41}$$

Now recall from (2.6.27) that

$$\begin{aligned} \mathfrak{m}_{X,P}/\mathfrak{m}_{X,P}^2 &= (\mathfrak{n}/\mathfrak{n}^2)/\text{image of } I(X) \\ &= (kx \oplus k\widetilde{y})/\text{image of } \widetilde{y}^2 - 2\widetilde{y} - x^5 + 2x \\ &= (kx \oplus k\widetilde{y})/k(2x - 2\widetilde{y}) \\ &= (kx \oplus k\widetilde{y})/k(x - \widetilde{y}). \end{aligned} \tag{2.7.42}$$

Since both x and $\widetilde{y}$ have non-trivial image in $kx \oplus k\widetilde{y}/k(x - \widetilde{y})$, we see that either is a uniformizer at P, so that

$$\mathfrak{m}_{X,P} = x\mathscr{O}_{X,P} = \widetilde{y}\mathscr{O}_{X,P}. \tag{2.7.43}$$

Indeed, we can express either of x and $\widetilde{y} - 1$ in terms of the other up to a unit: We have

$$\widetilde{y} = \frac{x^4 - 2}{\widetilde{y} - 2} x \tag{2.7.44}$$

and conversely

$$x = \frac{\widetilde{y} - 2}{x^4 - 2}\widetilde{y} \tag{2.7.45}$$

Next, we take $Q = (1, 0)$. We now define $\widetilde{x} = x - 1$ and rewrite the equation of X as

$$X : y^2 = \widetilde{x}^5 + 5\widetilde{x}^4 + 10\widetilde{x}^3 + 10\widetilde{x}^2 + 3\widetilde{x}. \tag{2.7.46}$$

In this case, $\mathfrak{m}_{X,Q}$ is the image of $\mathfrak{n} = (\widetilde{x}, y)$ and we have

$$\begin{aligned} \mathfrak{m}_{X,Q}/\mathfrak{m}_{X,Q}^2 &= (\mathfrak{n}/\mathfrak{n}^2)/\text{image of } I(X) \\ &= (k\widetilde{x} \oplus ky)/k(-3\widetilde{x}) \\ &= (k\widetilde{x} \oplus ky)/k\widetilde{x}. \end{aligned} \tag{2.7.47}$$

Since $\widetilde{x}$ has trivial image in this quotient, it is not a uniformizer at Q, but y still is, so that

$$\mathfrak{m}_{X,Q} = y\mathscr{O}_{X,Q}. \tag{2.7.48}$$

And indeed we can write $\widetilde{x}$ as a power of y times a unit, because

$$\widetilde{x} = \frac{\widetilde{x}^5 + 5\widetilde{x}^4 + 10\widetilde{x}^3 + 10\widetilde{x}^2 + 3\widetilde{x}}{3} y^2. \tag{2.7.49}$$

The local structure of non-singular curves allows us to prove many useful properties that often no longer hold for varieties of higher dimension. One of them is the following.

Proposition 2.7.50. *Let X be a non-singular curve, let $P \in X$ be a point, and let Y be a projective variety. If $\varphi : X \setminus \{P\} \to Y$ is a morphism, then there exists a unique morphism $X \to Y$ that extends φ.*

Proof. We do not attempt to improve the exposition in [2, Proposition I.6.8]. □

In particular, this implies that any morphism $\varphi : U \to Y$ whose domain is an open (and therefore cofinite) subset U of a curve X and whose codomain is a projective curve Y extends to all of X. We combine this with a second observation: It turns out that a point on a non-singular algebraic curve X is uniquely determined by the corresponding valuation on the function field $k(X)$. These observations together imply that non-singular algebraic curves can essentially be described purely in terms of their function fields and discrete valuation rings. For more details, we refer to [2, §1.6] for the technical details and only summarize the main results.

Proposition 2.7.51. *Let $\varphi : X \to Y$ be morphism of algebraic curves. Then either φ is constant or it is* dominant*, meaning that $\varphi(X)$ is an open subset of Y.*

Theorem 2.7.52. *Associating to a X its function field $k(X)$ and to a morphism $\varphi : X \to Y$ the corresponding pullback map*

$$\begin{aligned} \varphi^* : k(Y) &\to k(X) \\ f &\mapsto \varphi^*(f) = f \circ \varphi \end{aligned} \tag{2.7.53}$$

gives rise to an equivalence of categories between

(i) The category of non-singular projective algebraic curves over k, with dominant morphisms of algebraic curves;

(ii) *The category of function fields over k (that is, finitely generated extensions of k of transcendence degree 1), with homomorphisms that fix k.*

If X is projective, then the set of points of X is in bijective correspondence with set the discrete valuations of $k(X)$ that are trivial on k.

The reason that Theorem 2.7.52 considers only projective curves is that a given curve has the same function field as its open subsets. A crucial part of the proof of Theorem 2.7.52 is that for every non-singular algebraic curve U there exists a projective curve X that contains U. The curve X is in turn uniquely determined by U. It is the "largest" curve that contains U and corresponds to the function field $k(U)$, in the sense that it is the unique curve for which *every* discrete valuation on $k(U)$ that is trivial on k^* corresponds to an actual point on X. The projective curve X is called the projective completion of the non-singular curve U.

Example 2.7.54. Consider the case $U = \mathbb{A}^1$, so that $k(U) = k(x)$. Every point $a \in U$ gives rise to a discrete valuation v_a of $k(x)$, namely

$$v_a(f) = \begin{cases} n & \text{if } f = (x-a)^n (r/s) \text{ with } r, s \in k[x] \text{ non-zero at } 0 \\ \infty & \text{if } f = 0. \end{cases} \tag{2.7.55}$$

However, the valuation v_∞ from Example 2.7.8 does not correspond to a point of U, but only to the point ∞ of the projective completion $X = \mathbb{P}^1$ of $U = \mathbb{A}^1$.

Remark 2.7.56. As we will later see concretely, the projective completion of a given quasi-projective curve $U \subset \mathbb{P}^n$ may *not* be given by the projective closure of U. Indeed, said closure may very well be non-singular. We will instead determine the projective completion by applying Theorem 2.7.60 below.

In terms of (inverse) images of points, the correspondence between points of curves and discrete valuations of their function fields has the following properties. Let X and Y be algebraic curves over k with function fields $k(X)$ and $k(Y)$, and let $\varphi : X \to Y$ be a morphism. Then using Theorem 2.7.52 we can consider $k(Y)$ as a subfield of $k(X)$.

Proposition 2.7.57. *Let $P \in X$. Then we have*

$$\mathcal{O}_{Y,\varphi(P)} = \mathcal{O}_{X,P} \cap k(Y). \tag{2.7.58}$$

Proposition 2.7.59. *Let $Q \in Y$. Then the fiber $\varphi^{-1}(Q)$ is in natural bijection with the set of discrete valuation rings of $k(X)$ that contain $\mathcal{O}_{Y,Q} \subset k(Y)$.*

Along with Theorem 2.7.32(iii), these propositions can be used to show the final result of this section, namely:

Theorem 2.7.60. *Let X and Y be non-singular projective algebraic curves, let $\varphi : X \to Y$ be a non-constant morphism, and let $V \subset Y$ be an affine open subset. Then the inverse image $U = \varphi^{-1}(V) \subset X$ is affine as well, and its coordinate ring $k[U]$ is the integral closure of $k[V] \subset k(Y)$ in the field extension $k(Y) \subset k(X)$ induced by φ as in Theorem 2.7.52.*

Proof (sketch). We have that

$$k[U] = k[\varphi^{-1}(U)] = \bigcap_{P \in U} \mathcal{O}_{X,P} = \bigcap_{Q \in V} \bigcap_{P \in \varphi^{-1}(Q)} \mathcal{O}_{Y,Q}. \tag{2.7.61}$$

Now in light of Proposition 2.7.59 and since $k[V] = \bigcap_{Q \in V} \mathcal{O}_{Y,Q}$, the final intersection is exactly the intersection of all discrete valuation rings that contain $k[V]$. Since these discrete valuation rings are integrally closed by Theorem 2.7.32(iii), this intersection equals the integral closure of $k[V]$ by local-global results on the integral closure that are obtained using commutative algebra. □

Chapter 3

Spell components

Divisors, or translating the same notion into a different language, line bundles are a fundamental tool in algebraic geometry. They will allow us to understand the various maps from a given non-singular projective curve to and into projective spaces. Particularly important are the divisors that come from differential forms on a curve; these are called canonical divisors. We study these divisors, their properties under pullback, and the corresponding maps to projective spaces. This leads to the fundamental theorems of Riemann–Hurwitz and Riemann–Roch, and therefore to the magic that they make happen in the final chapter of these notes.

For the rest of these notes, we make the following assumption:

The curves that we consider are non-singular and projective, and the morphisms that we consider are non-constant, unless explicitly mentioned otherwise.

3.1 Divisors, pullbacks, and pushforwards

We now introduce a fundamental tool in the study of curves. There are various ways of looking at it, but the following definition is arguably the most intuitive.

Definition 3.1.1. Let X be an algebraic curve. A Weil divisor (often simply called a divisor) on X is an element D of the free abelian group $\mathrm{Div}(X)$ generated by the points of X. Concretely, this means that

$$D = \sum_{P \in X} n_P [P] \tag{3.1.2}$$

where $[P]$ is the image of the point P in $\mathrm{Div}(X)$ and where $n_P = 0$ for all but finitely many P. A Weil divisor (3.1.2) is called effective if $n_P \geq 0$ for all P. We denote this by writing $D \geq 0$. The support of an effective Weil divisor is the set of points $P \in X$ such that $n_P > 0$ in (3.1.2).

Given a non-zero element f of the function field $k(X)$ of X, we define the corresponding principal divisor to be

$$(f) = \sum_{P \in X} v_P(f)[P] \tag{3.1.3}$$

where v_P is the valuation of $k(X)$ corresponding to the point P. The point P is called a zero of f if $v_P(f) > 0$, in which case we call $v_P(f)$ the zero order of f at P. It is called a pole of f

if $v_P(f) < 0$, in which case we call $-v_P(f)$ the pole order of f at P. Similarly, we will use the notation $v_P(D) := n_P$ for a Weil divisor D as in (3.1.2) and $P \in X$ to denote the order of D at P.

Proposition 3.1.4. *The principal divisor of a non-zero element $f \in k(X)^*$ is well-defined. In other words, we have $v_P(f) = 0$ for almost all $P \in X$.*

Proof. The rational function f is a regular function on some non-empty open subset U of X. Because of the very definition of a regular function, this means that $f = r/s$ is a rational function on a further non-empty open subset V of U, with the property that $s(P) \neq 0$ for all $P \in V$. Since f is non-zero, the set of zeros of r in V is not all of V, and therefore $V \cap D(r)$ is a non-empty open subset of X on which f has neither poles nor zeros. However, you have shown in the exercises that because $\dim(X) = 1$, the open subsets of X are exactly the cofinite subsets. This implies the proposition. □

The following proposition will be an exercise.

Proposition 3.1.5. *Let* $\mathrm{Princ}(X) \subset \mathrm{Div}(X)$ *be the subset of* $\mathrm{Div}(X)$ *given by the divisors of rational functions $f \in k(X)^*$. Then* $\mathrm{Princ}(X)$ *is a subgroup of* $\mathrm{Div}(X)$.

Definition 3.1.6. We define the divisor class group $\mathrm{Cl}(X)$ of X to be the quotient

$$\mathrm{Cl}(X) = \mathrm{Div}(X)/\mathrm{Princ}(X) \tag{3.1.7}$$

Given $D_1, D_2 \in \mathrm{Div}(X)$, we say that D_1 and D_2 are linearly equivalent (notation: $D_1 \sim D_2$) if they define the same element of $\mathrm{Cl}(X)$, that is, if

$$D_1 = D_2 + (f) \tag{3.1.8}$$

for some $f \in k(X)^*$.

For affine curves, the class group is related to an algebraic notion.

Proposition 3.1.9. *Let $X \subset \mathbb{A}^n$ be an* affine *curve with coordinate ring $k[X]$. Then $\mathrm{Cl}(X) = 0$ if and only if $k[X]$ is a unique factorization domain if and only if $k[X]$ is a principal ideal domain.*

Proof. We only show one direction, as the other requires more commutative algebra (see [2, Proposition II.6.2]). Suppose that $k[X]$ is a principal ideal domain. We will show that for every $P \in X$, the divisor $[P]$ is zero in $\mathrm{Cl}(X)$. Since the classes $[P]$ generate $\mathrm{Div}(X)$ and therefore also its quotient $\mathrm{Cl}(X)$, this will show that $\mathrm{Cl}(X) = 0$.

So let $P \in X$, and let $\mathfrak{m}_P \subset k[X]$ be the maximal ideal corresponding to P. Since $k[X]$ is a principal ideal domain, there exists an element f of $k[X]$ such that $(f) = \mathfrak{m}_P$. This means in particular that $v_P(f) = 1$. We claim that $v_Q(f) = 0$ for all $Q \neq P$. If not, then we would have $f \in \mathfrak{m}_Q$ and therefore $\mathfrak{m}_P \subset \mathfrak{m}_Q$, which is impossible since $\mathfrak{m}_P$ and $\mathfrak{m}_Q$ are distinct maximal ideals. Therefore $(f) = [P]$ and $[P]$ is indeed zero in $\mathrm{Cl}(X)$. □

Example 3.1.10. Let $X = \mathbb{A}^1$. Then $k[\mathbb{A}^1] = k[t]$ is a principal ideal domain. We conclude that $\mathrm{Cl}(\mathbb{A}^1) = 0$. The same is true for all open subsets of $\mathbb{A}^1$. Geometrically, this follows from the general principle that if $P \in U$ is given and $f \in k(X)^*$ is such that $(f) = [P]$, then also $f \in k(U)^*$, which has the same principal divisor $[P]$. Algebraically, this follows because since $X = \mathbb{A}^1$ there exists a $g \in k[X]$ such $X - U = V(g)$, which by Theorem 2.4.30 is affine with coordinate ring $k[X]_g = k[t]_g$, and a localization of a principal ideal domain is still a principal ideal domain.

Definition 3.1.11. Let $D = \sum_{P \in X} n_P[P]$ be a divisor on an algebraic curve X. We define the degree $\deg(D)$ of D by

$$\deg(D) = \sum_{P \in X} n_P. \tag{3.1.12}$$

Remark 3.1.13. Note that the degree is once again well-defined on $\mathrm{Div}(X)$ by Proposition 3.1.4.

For the projective line $\mathbb{P}^1$, we can describe the class group is as follows.

Proposition 3.1.14. *Let $H \subset \mathbb{P}^1$ be the hyperplane $H : x_0 = 0$.*

(i) Given $D \in \mathrm{Div}(X)$, we have $D \equiv \deg(D)H$;

(ii) Given $f \in k(X)^*$, we have $\deg(f) = 0$ and $(f) \sim 0$.

Proof. As we have seen in Proposition 2.5.53, a rational function on $\mathbb{P}^1$ can be represented by a quotient r/s, where $r, s \in k[x_0, x_1]$ are homogeneous polynomials of equal degree. For the first result in Part (ii) it therefore suffices to show that if $r \in k[x_0, x_1]$ is a homogeneous polynomial of degree n, then its zero locus, counted with multiplicities, is of degree n. Now we can write r as

$$r = x_0^i(a_0 x_0^{n-i} + a_1 x_0^{n-i-1} x_1 + \ldots + a_{n-i-1} x_0 x_1^{n-i-1} + a_n x_1^{n-i}) \tag{3.1.15}$$

with $a_0 \neq 0$. On the affine subset $D(x_0)$, we obtain the zero divisor of the polynomial

$$a_0 + a_1 t + \ldots + a_{n-i-1} t^{n-i-1} + a_n t^{n-i} \tag{3.1.16}$$

which indeed has degree $n - i$ be the fundamental theorem of algebra (you should prove this as an exercise!). At the remaining point $(0:1)$, we obtain a zero of multiplicity i, so that indeed the zero divisor of the homogeneous function r has degree n and $\deg(r/s) = \deg(r) - \deg(s) = n - n = 0$.

Now suppose that D is a divisor of degree 0 on $\mathbb{P}^1$. Then we can write $D = D_1 - D_2$ with D_1, D_2 effective of equal degree n say. Suppose that D_1 contains $(0:1)$ with multiplicity $i \leq n$. Then $D_i \cap D(x_0)$ is a divisor on $\mathbb{A}^1$ of degree $n - i$, and by Proposition 3.1.9, we can find a polynomial $f \in k[t] = k[x_1/x_0]$ with divisor $D_i \cap D(x_0)$. The argumentation in the first part of the proof shows that $\deg(f) = n - i$. We see that we have

$$D_1 = i[(0:1)]^i + (D_i \cap D(x_0)) = (x_0)^i + (f) = (x_0)^i + (\mathrm{hom}(f)) = (r) \tag{3.1.17}$$

where

$$r = x_0^i \,\mathrm{hom}(f) = x_0^i f(x_1/x_0) \in k[x_0, x_1] \tag{3.1.18}$$

is homogeneous of degree $n - i + i = n$. Similarly, we find $s \in k[x_0, x_1]$ of homogeneous degree n such that $D_2 = (s)$. This means that the quotient $f = r/s$ is a well-defined rational function on $\mathbb{P}^1$ such that $(f) = (r/s) = (r) - (s) = D_1 - D_2$. This shows Part (i) and the remainder of Part (ii). $\square$

As always, it is crucial to study how divisors behave with respect to morphisms of curves.

Definition 3.1.19. Let $\varphi : X \to Y$ be a morphism of curves, and let

$$D = \sum_{Q \in Y} n_Q[Q] \in \mathrm{Div}(Y). \tag{3.1.20}$$

We define the pullback $\varphi^*(D)$ of D along φ by

$$\varphi^*(D) = \sum_{P\in X} e_\varphi(P) n_{\varphi(P)}[P] \in \mathrm{Div}(X). \tag{3.1.21}$$

where $e_\varphi(P)$ is the ramification index of φ at P, that is, the valuation

$$e_\varphi(P) = v_P(\pi_{\varphi(P)}) := v_P(\varphi^*(\pi_{\varphi(P)})) \tag{3.1.22}$$

at $P \in X$ of a uniformizer $\pi_{\varphi(P)} \in \mathscr{O}_{Y,\varphi P} \subset k(Y)$ (which we consider as an element of $\subset k(X)$ after composing with φ).

Remark 3.1.23. Alternatively and equivalently, as in [2, §II.6], one defines

$$\varphi^*(D) = \sum_{Q\in Y} f^*(Q), \tag{3.1.24}$$

where

$$\varphi^*(Q) = \sum_{\substack{P\in X\\ \varphi(P)=Q}} v_P(\pi_Q)[P] \tag{3.1.25}$$

where $\pi_Q \in \mathscr{O}_{Y,Q} \subset k(Y) \subset k(X)$ is a uniformizer at $Q \in Y$.

Proposition 3.1.26. *The ramification index $e_\varphi(P)$ defined in (3.1.22) does not depend on the choice of uniformizer $\pi_{\varphi(P)}$.*

Proof. Suppose that $\pi_1, \pi_2 \in \mathscr{O}_{Y,\varphi(P)}$ are both uniformizers. Then $v_{\varphi(P)}(\pi_1/\pi_2) = 1 - 1 = 0$, so that $\pi_1/\pi_2 \in O^*_{Y,\varphi(P)}$. This means that the rational π_1/π_2 is well-defined and non-zero at $\varphi(P)$, which in turn implies that the composition $\varphi^*(\pi_1/\pi_2) = (\pi_1/\pi_2)\circ\varphi$ is well-defined and non-zero at P. Since

$$\varphi^*(\pi_1/\pi_2) = (\pi_1/\pi_2)\circ\varphi = (\pi_1\circ\varphi)/(\pi_2\circ\varphi) = \varphi^*(\pi_1)/\varphi^*(\pi_2), \tag{3.1.27}$$

we see that

$$0 = v_P(\varphi^*(\pi_1)/\varphi^*(\pi_2)) = v_P(\varphi^*(\pi_1))/v_P(\varphi^*(\pi_2)) \tag{3.1.28}$$

so that indeed $v_P(\varphi^*(\pi_1)) = v_P(\varphi^*(\pi_2))$. □

We now have two pullback maps φ^*, one from $k(Y) \to k(X)$ that sends $f \in k(Y)$ to $\varphi^*(f) := f\circ\varphi$, and another one from $\mathrm{Div}(Y)$ to $\mathrm{Div}(X)$ defined in Definition 3.1.19. These maps are compatible in the following way:

Proposition 3.1.29. *Suppose that $\varphi : X \to Y$ is a morphism of curves. If $f \in k(Y)^*$, then we have*

$$\varphi^*((f)) = (\varphi^*(f)) \in \mathrm{Div}(X). \tag{3.1.30}$$

Proof. We have to show that

$$v_P(\varphi^*(f) = e_\varphi(P) v_{\varphi(P)}(f) \tag{3.1.31}$$

for all $P \in X$. To this end, use the fact that $\mathscr{O}_{Y,\varphi(P)}$ is a discrete valuation ring to write

$$f = u\pi^n \tag{3.1.32}$$

where $u \in \mathscr{O}_{Y,\varphi(P)}$ and where $\pi \in \mathfrak{m}_{Y,\varphi(P)}$ is a uniformizer. Note that then $v_{\varphi(P)}(f) = n$. Since u is well-defined and non-zero at $\varphi(P)$, the same holds for $\varphi^*(u) = u\circ\varphi$ at P, which is therefore a unit in $\mathscr{O}_{X,P}$. Therefore by definition of $e_\varphi(P)$ we have

$$v_P(f) = v_P(u\pi^n) = v_P(u) + n v_P(\pi) = n e_{\varphi(P)} = e_\varphi(P) v_{\varphi(P)}(f). \tag{3.1.33}$$

□

We define yet another map denoted by φ^*, this time between divisor class groups.

Remark 3.1.34. Proposition 3.1.29 implies that the pullback map $\varphi^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$ induces a map $\mathrm{Cl}(Y) \to \mathrm{Cl}(X)$, also denoted by φ^*, such that

$$\varphi^*([D]) = [\varphi^*(D)]. \tag{3.1.35}$$

With more effort, one can also show the following result on the multiplicativity of the degree. Although some of the constructions and results in this section also apply to more general curves, it is here that we must definitely restrict to the non-singular projective case.

Proposition 3.1.36. *Let $\varphi : X \to Y$ be a morphism of non-singular projective curves, and let $D \in \mathrm{Div}(Y)$. Then we have*

$$\deg(\varphi^*(D)) = \deg(\varphi)\deg(D) \tag{3.1.37}$$

where $\deg(\varphi) = [k(X) : k(Y)]$.

Proof. We refer to the excellent exposition in [2, Proposition II.6.9]. □

Corollary 3.1.38. *Suppose that X is a non-singular projective curve. Then $\deg(f) = 0$ for all $f \in k(X)^*$.*

Proof. If f is constant, then certainly $\deg(f) = 0$. Otherwise Proposition 2.7.50 shows that the rational function f can be extended to a morphism $\overline{f} : X \to \mathbb{P}^1$, and as you will show in an exercise, our definitions imply that

$$(f) = \overline{f}^{-1}([0] - [\infty]). \tag{3.1.39}$$

We conclude using Proposition 3.1.36. □

Corollary 3.1.40. *The degree map $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ induces a degree map on $\mathrm{Cl}(X) \to \mathbb{Z}$, also denoted by $\deg$, with*

$$\deg([D]) = \deg(D). \tag{3.1.41}$$

Definition 3.1.42. Let $X \subset \mathbb{P}^k_2$ be a non-singular projective curve. Then by Proposition 2.6.9 we have $X = V(F)$ for an irreducible homogeneous polynomial $F \in k[x_0, x_1, x_2]$ that is well-defined up to a non-zero scalar. We define the degree $\deg(X)$ of X in $\mathbb{P}^k_2$ by

$$\deg(X) = \deg(F). \tag{3.1.43}$$

Corollary 3.1.44 (Bézout's Theorem)**.** *Let $X, Y \subset \mathbb{P}^k_2$ be two projective curves. Then counting with multiplicities, we have that*

$$\#(X \cap Y) = \deg(X)\deg(Y). \tag{3.1.45}$$

In particular, if H is a hyperplane, that is, a curve in $\mathbb{P}^2_k$ defined by a homogeneous linear equation, then counting with multiplicities we have

$$\#(X \cap H) = \deg(X). \tag{3.1.46}$$

Proof (sketch). We can only sketch the proof of this statement, since it depends on the meaning of the qualification "with multiplicities". However, we take it to mean the following: If we write $Y = V(G)$ for a homogeneous polynomial $G \in k[x_0, x_1, x_2]$, then the zero divisor of G on X has degree $\deg(X)\deg(G)$. Now note that for all homogeneous polynomials G_1, G_2 that are non-zero on X we have

$$\deg(G_1 G_2) = \deg(G_1) + \deg(G_2), \tag{3.1.47}$$

Moreover, as in Proposition 3.1.14 one shows that homogeneous functions of the same degree define linearly equivalent divisors. Since the degree only depends on the linear equivalence class by Corollary 3.1.38, we may replace G with $\ell^{\deg(G)}$, where $\ell \in k[x_0, x_1, x_2]$ is linear and defines a hyperplane H, say $x_1 = 0$. Now $\varphi : x_1/x_0$ defines a rational function $X \to \mathbb{P}^1$ whose divisor of zeros $\varphi^*([0])$ is given by $X \cap H$ counted with multiplicities. We are done by Proposition 3.1.36 if we can show that $\deg(\varphi) = \deg(F)$. To this end, take $t = x_1/x_0$. Then the extension of $k(\mathbb{P}^1) = k(t)$ corresponding to X is defined by the dehomogenized polynomial $F(1, t, s)$, which has degree $\deg(F)$. □

Example 3.1.48. Consider the curve

$$X : y^2 = x^3 - 3x + 3. \tag{3.1.49}$$

We determine the principal divisor $D = (y-1)$. This divisor has no poles, since y is everywhere regular on X. Determining the zeros $P = (a, b) = (a, 1)$ of $y - 1$ requires us to solve the equation

$$1 = a^3 - 3a + 3, \tag{3.1.50}$$

which has the two solutions $a = 1$ and $a = 2$.

We first determine the multiplicity of $P_1 = (1, 1)$ in D. For this, we determine a uniformizer of the local ring $\mathscr{O}_{X,P_1}$. Since the corresponding Jacobian matrix is given by

$$\left(\frac{\partial(y^2 - x^3 + 3x - 3)}{\partial x}(P_1), \frac{\partial(y^2 - x^3 + 3x - 3)}{\partial y}(P_1) \right) = \left(3a^2 - 3, 2b\right) = (0, 2), \tag{3.1.51}$$

we see that we can use the function x as a uniformizer at P_1. Since

$$y - 1 = \frac{x^3 - 3x + 2}{y + 1} = (x-1)^2 \frac{x+2}{y+1}, \tag{3.1.52}$$

with $(x+2)/(y+1) \in \mathscr{O}^*_{X,P_1}$, we see that

$$v_{P_1}(D) = v_{P_1}(f) = 2. \tag{3.1.53}$$

The valuation of f at the second point $P_2 = (2, 1)$ can be determined analogously. However, we can also use Proposition 3.1.36. Indeed, we have that D is the divisor of zeros of the function $y - 1$, or in other words the pullback of the divisor $[0] \in \mathbb{A}^1$ under the map

$$\begin{aligned} \varphi = y - 1 : X &\to \mathbb{A}^1 \\ (a, b) &\mapsto b - 1 \end{aligned} \tag{3.1.54}$$

Now φ has degree 3, since the polynomial $y^2 - x^3 - 3x + 3$ that defines X has degree 3 when considered as an element of $k[y-1][x]$. Therefore we know that

$$\deg(D) = \deg(\varphi^*([0])) = \deg(\varphi)\deg([0]) = 3 \cdot 1 = 3. \tag{3.1.55}$$

Since D has a double zero at P_1 and a zero of some non-trivial order at P_2, we see that we must have

$$D = 2[P_1] + [P_2]. \tag{3.1.56}$$

Example 3.1.57. We now consider the projective closure

$$E : y^2 z = x^3 - 3xz^3 + 3z^3 \tag{3.1.58}$$

of the curve from the previous Example 3.1.48. Note first that X can be identified with the standard affine open $D(z)$ of E. There is only one other point on E, namely

$$O = (0 : 1 : 0). \tag{3.1.59}$$

Since $y-z$ is not zero in O, Example 3.1.48 shows that the principal divisor of the homogeneous form (but not function) $y-z$ is still given by

$$(y - z) = 2[P_1] + [P_2]. \tag{3.1.60}$$

We now instead consider the rational function

$$\frac{y - z}{z} = (y/z) - 1 \tag{3.1.61}$$

that is nothing but the function from Example 3.1.48 written in projective coordinates, and ask what its divisor D is this time around. Note that we have already determine its intersection with (or more precisely its pullback to) the affine patch X, namely $2[P_1]+[P_2]$.

There are multiple ways to determine D. First, one can determine the multiplicity of D at O by hand. To this end, we consider the affine patch $D(y)$ of E, which leads to the defining equation

$$z = x^3 - 3xz^2 + 3z^3 \tag{3.1.62}$$

We have to determine the valuation of D at $O = (0, 0)$. On this patch, the function (3.1.61) dehomogenizes to $(1/z) - 1 = (z - 1)/z$. Since $z - 1$ has neither a pole nor a zero at O, the requested valuation is simply $v_O(1/z) = -v_O(z)$. Now using the Jacobian matrix or inspecting (3.1.62), we see that x is a uniformizer at O. Using that $z \in \mathfrak{m}_{E,O}$, or alternatively that $z(1 - 3xz + 3z^2) = x^3$ with $1 - 3xz + 3z^2 \in \mathscr{O}_{E,O}$, we see that $v_P(z) = 3$, so that in the end

$$D = 2[P_1] + [P_2] - 3[O]. \tag{3.1.63}$$

Alternatively, one shows that $(z) = 3[O]$ for the *homogeneous* coordinate z; this result can be obtained without calculation from Proposition 3.1.36, the observation that the only zero of z is O, and the fact that $(z) = \varphi^*([0])$ for the morphism $\varphi = z : E \to \mathbb{P}^1$ induced by z, which again has degree 3. Finally, one can apply Corollary 3.1.38 to the function (3.1.61), which can only have a pole at the single point O in $X \setminus E$.

Given a morphism of curves $\varphi : X \to Y$, it is easier to define a map in the converse direction to that in Definition 3.1.19.

Definition 3.1.64. Let $\varphi : X \to Y$ be a morphism of curves, and let

$$D = \sum_{P \in X} n_P [P] \in \mathrm{Div}(X). \tag{3.1.65}$$

We define the pushforward $\varphi_*(D)$ of D along φ by

$$\varphi_*(D) = \sum_{P \in X} n_P [\varphi(P)] \in \mathrm{Div}(X). \tag{3.1.66}$$

Remark 3.1.67. Using results from commutative algebra one can show that if $D = (f)$ for $f \in k(X)$, then $\varphi_*(f) = (g)$, where

$$g = \mathrm{Nm}_{k(X)\,|\,k(Y)}(f) \in k(Y). \tag{3.1.68}$$

This again implies that φ_* induces a map on divisor class groups $\mathrm{Div}(X) \to \mathrm{Div}(Y)$, also denoted by φ_*, with

$$\varphi_*([D]) = [\varphi_*(D)]. \tag{3.1.69}$$

3.2 Cartier divisors and invertible sheaves

In this section, we introduce some formalism to relate Weil divisors with the notion of a line bundle, which is omnipresent in modern algebraic geometric. Our assumptions on curves and morphisms are as at the start of Section 3.1. We start on this road with a simple observation.

Proposition 3.2.1. *Let X be a curve, and let $D \in \mathrm{Div}(X)$ be a Weil divisor on X. Then D is locally principal; in other words, there exists an open cover $(U_i)_{i\in I}$ of X such that for all $i \in I$ the restriction*

$$D|_{U_i} = \sum_{P\in U} v_P(D)[P] \tag{3.2.2}$$

is a principal divisor on U_i.

Proof. It suffices to show that given $P \in X$ we can find an open subset U of X that contains P such that $D|_U$ is principal. To this end, consider a uniformizer π of the maximal ideal $\mathfrak{m}_{X,P}$ of the local ring $\mathscr{O}_{X,P}$. Then since π is germ at P, there exists an open set V such that π is given by a non-zero rational function r/s on V with $s(Q) \neq 0$ for all $Q \in V$.

The set of points Q in V at which $r(Q) = 0$ is finite, since the proper closed subsets of X are finite. Similarly, we have seen in Proposition 3.1.4 that the support $\mathrm{Supp}(D)$ of D, that is, the points Q of X for which $v_Q(D) \neq 0$, is finite. This means that the set V obtained by removing the zeros of r except for P and the points in $\mathrm{Supp}(D)$ except for P, is cofinite and contains P. It is therefore an open subset of X, on which the Zariski topology is the cofinite topology since X is an algebraic curve.

Let us show that $D|_U$ equals the principal divisor (f) for $f = \pi^{v_P(D)}$. Let $Q \in U$. If $Q \neq P$, then $v_Q(D) = 0$ and $v_Q(f)$ by out construction of U from V above. On the other hand, at P we have

$$v_P(f) = v_P(\pi^{v_P(D)}) = v_P(D)v_P(\pi) = v_P(D) \tag{3.2.3}$$

so that our claim is proved. □

Our first abstraction of the notion of a divisor is the following.

Definition 3.2.4. A Cartier divisor on X is a global section of the quotient sheaf $Q = k(X)^*/\mathscr{O}_X^*$. A Cartier divisor is called principal if it is in the image of the map $k(X)^* \to Q(X)$. The Cartier divisor class group $\mathrm{CaCl}(X)$ is defined as the quotient

$$\mathrm{CaCl}(X) = Q(X)/\mathrm{im}(k(X)^*). \tag{3.2.5}$$

Remark 3.2.6. Note that the constant presheaf $k(X)^*$ is indeed a sheaf on the algebraic curve X, in spite of Example 1.4.8. The reason for this is that if X is an algebraic curve (or an open subset of an algebraic curve) then X is connected, because X is irreducible.

Unwinding the definitions (and observing that irreducible spaces are connected), we see that a Cartier divisor is described by a tuple $(U_i, f_i)_{i\in I}$, where

(i) $(U_i)_{i\in I}$ is an open cover of X, and

(ii) $f_i \in k(X)^*$ are rational functions such that the restriction of f_i/f_j ton $U_i \cap U_j$ is an element of $\mathscr{O}_X(U_i \cap U_j)^*$.

Let D be a Weil divisor on X. Then we can associate a Cartier divisor to D in the following way. Choose an open cover $(U_i)_{i\in I}$ such that the restrictions $D|_{U_i}$ are all locally principal, and choose $f_i \in k(U_i)^* = k(X)^*$ such that $D_{U_i} = (f_i)$. Then $(U_i, f_i)_{i\in I}$ is a Cartier divisor. Indeed, $f_i|_{U_i\cap U_j}$ and $f_j|_{U_i\cap U_j}$ on $U_i\cap U_j$ both have associated divisor $D|_{U_i\cap U_j}$, so that on this subset f_i/f_j has associated divisor $D|_{U_i\cap U_j} - D|_{U_i\cap U_j} = 0$; it is therefore an element of $\mathscr{O}_X(U_i\cap U_j)^*$ (with inverse f_j/f_i).

Conversely, let $(U_i, f_i)_{i\in I}$ be a Cartier divisor on X. Then we can associate a Weil divisor to $(U_i, f_i)_{i\in I}$ in the following way. On the open subsets U_i, we consider the divisor $D_i = (f_i)$. Then we claim that $D_i|_{U_i\cap U_j} = D_j|_{U_i\cap U_j}$, or in other words that given $P\in U_i\cap U_j$ we have $v_P(D_i) = v_P(D_j)$. This implies that the given Weil divisors D_i glue to a global Weil divisor D on X whose multiplicity at a point P equals the common value of $v_P(D_i)$ for the various U_i such that $P\in U_i$. To prove the claim, it suffices to observe that on $U_i\cap U_j$ we have that

$$v_P(D_i) - v_P(D_j) = v_P(D_i - D_j) = v_P((f_i) - (f_j)) = v_P(f_i/f_j) = 0 \tag{3.2.7}$$

since $f_i/f_j \in \mathscr{O}_X(U_i\cap U_j)^*$.

Proposition 3.2.8. *The associations above send principal Weil divisors on X to principal Cartier divisors on X and conversely. Moreover, they give rise to mutually inverse isomorphisms between the group of Weil divisors* $\mathrm{Div}(X)$ *on X and the group of Cartier divisors on X, as well as to mutually inverse isomorphisms*

$$\mathrm{Cl}(X) \leftrightarrow \mathrm{CaCl}(X). \tag{3.2.9}$$

Proof. The proof is a formal argument which is left as an exercise. □

The second and final abstraction is the following.

Definition 3.2.10. A sheaf of $\mathscr{O}_X$-modules on X is a sheaf F on X with the property that

(i) $F(U)$ is provided with a structure of $\mathscr{O}_X(U)$-module $\cdot$ for all open $U\subset X$, and

(ii) for every inclusion $V\subset U$ of open subsets of X, the restriction maps ρ^U_V of F satisfy

$$\rho^U_V(f\cdot s) = f_V\cdot \rho^U_V(s) \tag{3.2.11}$$

for all $f\in\mathscr{O}_X(U)$ and for all $s\in F(U)$.

A morphism of sheaves of $\mathscr{O}_X$-modules $F\to G$ is a morphism of sheaves $\varphi: F\to G$ such that the component maps $\varphi_U : F(U)\to G(U)$ are all homomorphisms of $\mathscr{O}_X$-modules.

Definition 3.2.12. An invertible sheaf (of $\mathscr{O}_X$-modules) on X is a sheaf of $\mathscr{O}_X$-modules $\mathscr{L}$ on X for which there exists a cover $(U_i)_{i\in I}$ with the property that there is an isomorphism $\mathscr{L}|_{U_i}\cong\mathscr{O}_{U_i}$ of $\mathscr{O}_{U_i}$-modules for all $i\in I$.

Let $D = (U_i, f_i)_{i\in I}$ be a Cartier divisor on X. Then we can associate an invertible sheaf $\mathscr{L}(D)$ to $(U_i, f_i)_{i\in I}$ in the following way. Given $U\subset X$, we let

$$\mathscr{L}(D)(U) = \Big\{f\in k(X) \mid f\in f_i^{-1}\mathscr{O}_X(U_i\cap U) \text{ for all } i\in I \tag{3.2.13}$$

Note that the demands in (3.2.13) are compatible in the sense that if $f\in k(X)$, then $f\in f_i^{-1}\mathscr{O}_X(U_i\cap U_j)$ if and only if $f\in f_j^{-1}\mathscr{O}_X(U_i\cap U_j)$, since f_i/f_j is in $\mathscr{O}_X(U_i\cap U_j)^*$. This is an invertible sheaf on X by construction.

Conversely, if $\mathscr{L}$ is an invertible sheaf, then we can realize it as a subsheaf of $k(X)$ via a choice of isomorphism of $\mathscr{O}_X$-modules

$$\mathscr{L}\otimes_{\mathscr{O}_X} k(X)\cong k(X). \tag{3.2.14}$$

(If you do not know what the tensor product is, fret not and simply assume that $\mathscr{L}$ is isomorphic to a subsheaf of $k(X)$.) Given an open subset U, the $\mathscr{O}_X(U)$-submodules of $k(X)$ that are isomorphic to $\mathscr{O}_X(U)$ are generated by a single element and therefore of the form $f^{-1}\mathscr{O}_X(U)$ for some $f \in k(X)^*$. We can therefore find an open cover $(U_i)_{i\in I}$ and $f_i \in k(X)^*$ such that $\mathscr{L}|_{U_i} = f_i^{-1}\mathscr{O}_X(U_i)$ as a subsheaf of $k(X)$. Since

$$(\mathscr{L}|_{U_i})|_{U_j} = \mathscr{L}|_{U_i \cap U_j} = (\mathscr{L}|_{U_j})|_{U_i} \qquad \text{for all } i, j \in I, \tag{3.2.15}$$

we get

$$f_i^{-1}\mathscr{O}_X(U_i \cap U_j) = f_j^{-1}\mathscr{O}_X(U_i \cap U_j), \tag{3.2.16}$$

which implies that $f_i/f_j \in \mathscr{O}_X(U_i \cap U_j)^*$, so that we have associated a Cartier divisor $(U_i, f_i)_{i\in I}$ to $\mathscr{L}$.

Proposition 3.2.17. *The associations above give mutually inverse isomorphisms between the group of Cartier divisors on X and the group of line bundles on X that are subsheaves of the constant sheaf $k(X)$. Moreover, two Cartier divisors D_1 and D_2 are equivalent if and only if the associated line bundles $\mathscr{L}(D_1)$ and $\mathscr{L}(D_2)$ are isomorphic.*

Proof. The first part of the proof is a formal argument that is left to the reader. As for the second part, if $D_1 - D_2 = (f)$, then multiplication with f yields an isomorphism $\mathscr{L}(D_1) \to \mathscr{L}(D_2)$. Indeed, locally D_1, resp. D_2, is described by f_1 resp. f_2. The condition $D_1 - D_2 = (f)$ shows that $f_1 = f_2 f$ up to a unit of $\mathscr{O}_X(U)$, so that the map

$$\begin{aligned} f_1^{-1}\mathscr{O}_X(U) &\to f_2^{-1}\mathscr{O}_X(U) \\ g &\mapsto fg \end{aligned} \tag{3.2.18}$$

is an isomorphism. Conversely, if U is an open where both $\mathscr{L}(D_1)$ and $\mathscr{L}(D_2)$ are isomorphic to $\mathscr{O}_X(U)$, then the isomorphism is defined by multiplication by some element $f \in k(X)^*$. Indeed, if $\mathscr{L}(D_1)|_U = f_1^{-1}\mathscr{O}_U$ and $\mathscr{L}(D_2)|_U = f_2^{-1}\mathscr{O}_U$, and the isomorphism of $\mathscr{O}_U$-modules maps f_1^{-1} to g say, then we can take $f = gf_1$. But if this holds on an open, then it holds on all of X, essentially because of Lemma 2.3.12. Reversing the argument above, we see that $\mathscr{L}(D_2) = f\mathscr{L}(D_1)$ implies that $D_1 - D_2 = (f)$. □

Example 3.2.19. Consider the affine curve

$$X : y^2 = x^5 - 2x + 1 \tag{3.2.20}$$

and let D be the Weil divisor $[P]$ with $P = (0, 1)$. We determine a Cartier divisor corresponding to P. In Example 2.7.39, we have seen that x and $y - 1$ are both uniformizers at P. So let $U_1 = D(x) \cup \{P\}$ and $f_1 = x$. Then by construction $D_{U_1} = (f_1)$, since f_1 has a single zero at P and no zeros elsewhere on U_1. Similarly, if we take $U_2 = D(y-1) \cup \{P\}$, then $D_{U_2} = (f_2)$. Since $V(x) \cap V(y-1) = V(x, y-1) = \{P\}$, we have that $D(x) \cup D(y-1) = X - \{P\}$ and therefore $D(x) \cup D(y-1) \cup \{P\} = X$. Therefore we see that $((U_1, f_1), (U_2, f_2))$ is a Cartier divisor that represents D. (Note that this is indeed a Cartier divisor because x and $y-1$ are both units on $D(x) \cap D(y-1)$ and they both have valuation 1 at P, so that $x/(y-1)$ is a unit everywhere on $(D(x) \cup \{P\}) \cap (D(y-1) \cup \{P\})$.)

Similarly, if E is the Weil divisor $[Q]$ with $Q = (1, 0)$, then a similar argument shows that $((V_1, g_1), (V_2, g_2))$ is a corresponding Cartier divisor, where $(V_1, g_1) = (D(x+y-1) \cup \{Q\}, x+y-1)$ and $(V_2, g_2) = (D(y-1) \cup \{Q\}, y-1)$. Once more this works because $x + y - 1$ and $y - 1$ both have a single zero at Q. This time cannot replace (V_1, g_1) by $((D(x) \cup \{Q\}, x)$ since x has a double zero at Q instead.

It turns out that neither of the divisors D and E are principal, so in both cases we really need two patches and two rational functions to describe the corresponding Cartier divisors.

Remark 3.2.21. Pullbacks and pushforwards can also be described in terms of Cartier divisors and line bundles. Given a morphism $\varphi : X \to Y$ and a Cartier divisor $D = (U_i, f_i)_{i\in I}$, the pullback of D is described by $(U_i, \varphi^*(f_i))_{i\in I}$. The pullback of a line bundle is more complicated to describe, as it requires the tensor product. More precisely, given a line bundle $\mathscr{L}$ we have

$$\varphi^*(\mathscr{L}) = \varphi^{-1}(\mathscr{L}) \otimes_{\varphi^{-1}(\mathscr{O}_Y)} \mathscr{O}_X \tag{3.2.22}$$

Here the map $\varphi_{-1}(\mathscr{O}_Y) \to \mathscr{O}_X$ required to form the tensor product is the adjoint, in the sense of Remark 1.5.19, of the map $\mathscr{O}_Y \to \varphi_*(\mathscr{O}_X)$ given by pullback (this maps a regular function $f \in \mathscr{O}_Y(V)$ to the composition $\varphi^*(f) = f \circ \varphi \in \mathscr{O}_X(\varphi^{-1}(V)) = \varphi_*(\mathscr{O}_X)(V)$). The pushforwards on the level of Cartier divisor and line bundles are yet more adjoints, namely of the given pullbacks φ^*.

As you can see, pullbacks and pushforwards of Weil divisors are easier to comprehend. The adjoints φ_* and φ^* is the simpler pair of adjoints that you were promised in Remark 1.5.19.

Remark 3.2.23. Given a Weil divisor D, we will often denote the k-vector space of global sections $\mathscr{L}(D)(X)$ of the corresponding line bundle $\mathscr{L}(D)$ by $L(D)$. The space $L(D)$ can be described as follows. Take $(U_i, f_i)_{i\in I}$ to be a Cartier divisor corresponding to D. Then we have

$$L(D) = \left\{ f \in k(X) \mid f \in f_i^{-1} \mathscr{O}_X(U_i) \text{ for all } i \in I \right\}. \tag{3.2.24}$$

Now a rational function f is in $f_i^{-1}\mathscr{O}_X(U_i)$ if and only if $f_i f \in \mathscr{O}_X(U_i)$. Since $\mathscr{O}_X(U_i) = \cap_{P\in U_i} \mathscr{O}_{X,P}$, this is equivalent to demanding $v_P(f_i f) \geq 0$ for all $P \in U_i$, or in other words that $v_P(f) \geq -v_P(f_i) = v_P(D)$ for all $P \in U_i$. Combining these conditions for all elements of the cover $(U_i)_{i\in I}$, we obtain that

$$L(D) = \{ f \in k(X) \mid v_P(f) \geq -v_P(D) \text{ for all } P \in X \}. \tag{3.2.25}$$

In other words, we can see the elements of $L(X)$ as the elements of $k(X)^*$ whose poles are bounded by the divisor D. This makes the spaces $L(X) = \mathscr{L}(D)(X)$ far more concrete, and the same holds more generally for the spaces

$$\mathscr{L}(D)(U) = \{ f \in k(X) \mid v_P(f) \geq -v_P(D) \text{ for all } P \in U \}. \tag{3.2.26}$$

obtained by considering open subset $U \subset X$.

Remark 3.2.27. Let $\varphi : X \to Y$ be a morphism of non-singular curves, and let $\mathscr{L}$ be an invertible sheaf on Y. Then we have already defined the pullback $\varphi^*(\mathscr{L})$. We will now show that we can pull back global sections of $\mathscr{L}$ to global sections if $\varphi^*(\mathscr{L})$ as well. Once again, this is easier when we restrict to invertible sheaves of the form $\mathscr{L}(D)$ on Y. So consider a global section $f \in L(D)$ of such a sheaf. In Remark 3.2.23, we have seen that this is the same as a rational function $f \in k(Y)$ with the property that $v_Q(f) \geq -v_Q(D)$ for all $Q \in Y$. We claim that

$$\varphi^*(f) \in \varphi^*(\mathscr{L}(D))(X) = \mathscr{L}(\varphi^*(D))(X) = L(\varphi^*(D)). \tag{3.2.28}$$

Indeed, let $P \in X$. Then as in the proof of Proposition 3.1.29 we see that

$$v_P(\varphi^*(f)) = e_\varphi(P) v_{\varphi(P)}(f). \tag{3.2.29}$$

On the other hand, we have that

$$v_P(\varphi^*(D)) = e_\varphi(P) v_{\varphi(P)}(D) \tag{3.2.30}$$

by definition. Since $v_{\varphi(P)}(f) \geq -v_{\varphi(P)}(D)$, we see that indeed $v_P(\varphi^*(f)) \geq v_P(\varphi^*(D))$ for all P, so that (3.2.28) indeed holds. In fact the pullback map

$$\begin{aligned} \varphi^* : L(D) &\to L(\varphi^*(D)) \\ f &\mapsto \varphi^*(f) \end{aligned} \tag{3.2.31}$$

thus obtained is a k-linear map.

The final important results on spaces of global sections $L(D)$ is the following. Given the vector space $L(D)$, we can construct a corresponding projective space

$$\mathbb{P}L(D) = (L(D) \setminus \{0\})/\sim \tag{3.2.32}$$

where the equivalence relation $\sim$ on $L(D) \setminus \{0\}$ is defined by

$$f \sim g \quad \Leftrightarrow \quad f = \lambda g \text{ for } \lambda \in k^*. \tag{3.2.33}$$

Proposition 3.2.34. *Let D be a Weil divisor on a curve X, and let $|D| \subset \mathrm{Div}(X)$ be the subset of effective divisors on X that are linearly equivalent to D. Then the map*

$$\begin{aligned} \mathbb{P}L(D) &\to |D| \\ [f] &\mapsto D + (f) \end{aligned} \tag{3.2.35}$$

is bijective.

Proof. The map is well-defined because $(\lambda f) = (f)$ for all $\lambda \in k^*$, and it is well-defined because $D + (f) \geq 0$ in light of (3.2.25). Conversely, if E is effective and linearly equivalent to D, then we have $E = D + (f)$ for some $f \in k(X)^*$ with $D + (f) \geq 0$, so that $f \in L(D) \setminus \{0\}$ by (3.2.25). □

Remark 3.2.36. The set $|D|$ from Proposition 3.2.34 is also called the linear system of effective divisors defined by D.

3.3 Morphisms induced by line bundles

In this section, we will occasionally have to consider more general varieties. Anyway... once upon a time there was a projective space $\mathbb{P}^n$, and on that projective space there lived the following sheaf, which was virtuous and helped in many constructions.

Definition 3.3.1. Consider the homogeneous coordinate ring $S = k[x_0, \ldots, x_n]$ of $\mathbb{P}^n$. We define Serre's twisting sheaf on $\mathbb{P}^n$ (notation: $\mathscr{O}_{\mathbb{P}^n}(1)$ or $\mathscr{O}(1)$) to be the sheaf of $\mathscr{O}_{\mathbb{P}^n}$-modules that corresponds to the S-module $M = \bigoplus_{d \in \mathbb{Z}} M_d$ that is obtained by shifting the grading on S, so that

$$M_d = S_{d+1}. \tag{3.3.2}$$

More concretely, this means that if $D(F) \subset \mathbb{P}^n$ is an open set defined by a homogeneous polynomial $F \in k[x_0, \ldots, x_n]$, then

$$\mathscr{O}(1)(D(F)) = \left\{ G/F^d \ : \ d \geq 0,\, G \text{ homogeneous of degree } \deg(G) = d\deg(F) + 1 \right\}, \tag{3.3.3}$$

which is indeed a module for the ring of regular functions

$$\mathscr{O}(D(F)) = \left\{ G/F^d \ : \ d \geq 0,\, G \text{ homogeneous of degree } \deg(G) = d\deg(F) \right\}. \tag{3.3.4}$$

In particular, we see that on the principal open subsets $U_0,\dots,U_n \subset \mathbb{P}^n$ we have

$$\mathcal{O}(1)(U_i) = \left\{G/x_i^d \ : \ d \geq 0, G \text{ homogeneous of degree } \deg(G) = d+1\right\}. \tag{3.3.5}$$

which is a module for

$$\mathcal{O}(U_i) = k[x_0/x_i,\dots,x_n/x_i]. \tag{3.3.6}$$

Example 3.3.7. Consider the twisting sheaf $\mathcal{O}(1)$ on $\mathbb{P}^1$. Then we have

$$x_1^2/x_0 \in \mathcal{O}(1)(U_0) \tag{3.3.8}$$

but

$$x_1^2/x_0 \notin \mathcal{O}(1)(U_1) \tag{3.3.9}$$

since the denominator of x_1^2/x_0 is not a power of x_1. On the other hand, we have

$$x_0 + 2x_1 = (x_0+2x_1)/x_0 = (x_0+2x_1)/x_1 \in \mathcal{O}(1)(U_0) \cap \mathcal{O}(1)(U_1) = \mathcal{O}(1)(\mathbb{P}^1). \tag{3.3.10}$$

Note that x_1/x_0 is not even a section in $\mathcal{O}(1)(U_0)$ since the degree the condition in (3.3.5) on the degree of homogeneity is not satisfied. Also note that the global section $x_0 + 2x_1 \in \mathcal{O}(1)(\mathbb{P}^1)$ from (3.3.10) is not an actual function on $\mathbb{P}^1$, since the x_i-coordinate of a point in $\mathbb{P}^1$ is not well-defined! The linear form $x_0 + 2x_1$ is *only* well-defined as a global section of $\mathcal{O}(1)$.

Proposition 3.3.11. *We have*

$$\mathcal{O}(1)(\mathbb{P}^n) = S_1 = kx_0 \oplus \ldots \oplus kx_n. \tag{3.3.12}$$

Proof. The proof is analogous to that of Theorem 2.5.64. Intuitively, since we consider sections that are regular on *all* of $\mathbb{P}^n$, no denominators can occur in the expressions (3.3.5), as in Example 3.3.7, and we only obtain the homogeneous polynomials of degree 1 in S, that is, the linear forms in the variables $x_0,\dots,x_n$. □

Proposition 3.3.11 shows that $\mathcal{O}(1)$ has quite a few global sections. Given $P \in P^n$, the stalk

$$\mathcal{O}(1)_P = \{F/G \ : \ F, G \text{ homogeneous with } G(P) \neq 0 \text{ and } \deg(F) = \deg(G)+1\}. \tag{3.3.13}$$

is generated by the global sections $x_i \in \mathcal{O}(1)(\mathbb{P}^n)$ as a module over the local ring

$$\mathcal{O}_{\mathbb{P}^n,P} = \{F/G \ : \ F, G \text{ homogeneous with } G(P) \neq 0 \text{ and } \deg(F) = \deg(G)\}. \tag{3.3.14}$$

The corresponding general notion is the following.

Definition 3.3.15. Let X be a projective variety, and let $\mathcal{L}$ be an invertible sheaf of $\mathcal{O}_X$. We say that $\mathcal{L}$ is generated by global sections if the elements of the space of global sections $\mathcal{L}(X)$ generate the stalk $\mathcal{L}_P$ as an $\mathcal{O}_{X,P}$-module for every $P \in X$.

If D is a Weil divisor, then we say that D is base-point free if the invertible sheaf $\mathcal{L}(D)$ is generated by global sections. Note that this implies that whether D is base-point free only depends on the linear equivalence class of D, since linearly equivalent divisors give rise to isomorphism invertible sheaves.

Remark 3.3.16. Definition 3.3.15 also makes sense for affine varieties, but for those it is always trivially fulfilled. The situation is more difficult in the projective case, where there is often a dearth of global sections.

Proposition 3.3.17. *Let $\varphi : X \to Y$ be a morphism of projective varieties, and let $\mathscr{L}$ be a sheaf on Y that is generated by global sections. Then the sheaf $\varphi^*(\mathscr{L})$ is generated by global sections as well.*

Proof (sketch). This follows from (3.2.22) since the pullbacks $\varphi^*(s)$ of the sections s of $\mathscr{L}$ generate $\varphi^{-1}(\mathscr{L})$ as a module over $\varphi^{-1}(\mathscr{O}_X)$. (As usual, this is perhaps clearest when $\mathscr{L} = \mathscr{L}(D)$; see Remark 3.2.27.) □

The proof of Proposition 3.3.17 also shows the following.

Corollary 3.3.18. *Let X be a projective curve, and let $\varphi : X \to \mathbb{P}^n$ be a morphism. Then $\varphi^*(\mathscr{O}(1))$ is an invertible sheaf on X, which is generated by the pullbacks $s_i = \varphi^*(x_i)$ of the global sections x_i of* (1).

Remarkably, Corollary 3.3.18 admits the following converse, which is fundamental for the study of projective curves over fields.

Theorem 3.3.19. *Let X be a projective curve, and let $\mathscr{L}$ be an invertible sheaf on X that is generated by global sections. Choose global sections $s_0, \dots, s_n$ such that*

$$\mathscr{L}(X) = kx_0 \oplus \ldots \oplus kx_n. \tag{3.3.20}$$

Then there exists a unique morphism $\varphi : X \to \mathbb{P}^n_k$ such that $\mathscr{L} \cong \varphi^*(\mathscr{O}(1))$ and $s_i = \varphi^*(x_i)$. If $\mathscr{L}$ is a subsheaf of $k(X)$, as happens for example when $\mathscr{L} = \mathscr{L}(D)$ for some Weil divisor D on X, then given a point $P = (a_0 : \dots, a_n) \in X$ we have

$$\varphi(P) = (s_0(P) : \ldots : s_n(P)). \tag{3.3.21}$$

Proof. We define the subsets $X_0, \dots, X_n \subset \mathbb{P}^n$ by

$$X_i = \{P \in X \mid s_i \notin \mathfrak{m}_{X,P}\mathscr{L}_P\}. \tag{3.3.22}$$

As you will show in the exercises, the sets X_i are open in $\mathbb{P}^n$, and they cover $\mathbb{P}^n$ because $\mathscr{L}$ is generated by the global sections $s_0, \dots, s_n$. Let $U_i = D(x_i) \subset \mathbb{P}^n$. Then we can define a morphism

$$\begin{aligned} \varphi_i : X_i &\to U_i \\ y_j = x_j/x_i &\mapsto s_j/s_i \end{aligned} \tag{3.3.23}$$

as in Remark 2.4.14, since the corresponding ring homomorphism

$$\begin{aligned} k[U_i] &\to \mathscr{O}_X(X_i) \\ y_i &\mapsto s_j/s_i \end{aligned} \tag{3.3.24}$$

is well-defined. Indeed, s_j and s_i are sections of the same invertible sheaf $\mathscr{L}$ over the open set X_i. Choosing a further open subset $U_i \subset X_i$ such that $\mathscr{L}|_{U_i} \cong \mathscr{O}_{U_i}$, we see that s_j/s_i defines an element of $k(X)$. (It is this observation that also shows that the description (3.3.21) makes sense.) Moreover, since $s_i(P) \neq 0$ for $P \in U_i$, we see that $s_j/s_i \in \mathscr{O}_X(X_i)$, from which we can conclude by observing that $k[U_i]$ is a polynomial ring.

This shows that the restrictions φ_i of φ are morphisms. This implies that φ is a morphism as well, since the property of being a morphism is local on the base. Indeed, suppose that f is a regular function on an open subset U of X. Then the restrictions $f|_{U_i}$ are regular for all i, and so therefore are the pullbacks $\varphi_i^*(f_| U_i)$ since all φ_i are morphisms. However, we have

$$\varphi_i^*(f_| U_i) = (\varphi^*(f))|_{\varphi^{-1}(U_i)}, \tag{3.3.25}$$

which implies that $\varphi^*(f)$ is regular because the regular functions form a sheaf and the sets $\varphi^{-1}(U_i)$ cover X. □

Example 3.3.26. Consider the Weil divisor $D = 2[\infty]$ on $\mathbb{P}^1$ with $\infty = (0:1)$, and let $\mathscr{L} = \mathscr{L}(D)$ be the corresponding sheaf. Then the description (3.2.25) shows that the functions in $f \in \mathscr{L}(X)$ are everywhere regular on $\mathbb{A}^1 = \mathbb{P}^1 \setminus \{\infty\}$, so that they are elements of $k[t] = k[x_1/x_0]$. As in the proof of Corollary 3.1.38, we consider f as a function $\mathbb{P}^1 \to \mathbb{P}^1$, and then we see that $\deg(f) \leq 2$, since by definition of $\mathscr{L}(X)$ the number of poles of f, counted with multiplicity, is at most 2. These considerations imply that

$$\mathscr{L}(X) = k1 \oplus kt \oplus kt^2. \tag{3.3.27}$$

Choosing the basis of $\mathscr{L}(X)$ accordingly, we obtain the morphism

$$\begin{aligned} \varphi : X &\to \mathbb{P}^2 \\ t &\mapsto (1 : t : t^2). \end{aligned} \tag{3.3.28}$$

which extends projectively to

$$\begin{aligned} \varphi : X &\to \mathbb{A}^3 \\ (x_0 : x_1) &\mapsto (x_0^2 : x_0 x_1 : x_1^2). \end{aligned} \tag{3.3.29}$$

The image of φ is given by

$$\varphi(X) = V(x_1^2 - x_0 x_2). \tag{3.3.30}$$

Remark 3.3.31. For another example, see Example [2, II.7.1.1], which shows that the automorphisms of the projective space $\mathbb{P}^n$ are given by the projective linear maps

$$(x_0 : \ldots : x_n) \mapsto \left(\sum_j a_{0,j} x_j, \ldots, \sum_j a_{n,j} \right) \tag{3.3.32}$$

induced by invertible $(n+1) \times (n+1)$-matrices $(a_{i,j})$.

Consider a morphism φ as constructed in Theorem 3.3.19, and let $H \subset \mathbb{P}^n$ be a hyperplane. Then H is the zero locus of a non-zero linear form

$$\ell = \alpha_0 x_0 + \ldots + \alpha_n x_n. \tag{3.3.33}$$

In other words, H is the zero locus of the section $\ell \in \mathscr{O}(1)(\mathbb{P}^n)$. The pullback of $H \cap X$ under φ is therefore the zero locus $V(s)$ of the non-zero section $s = \varphi^*(\ell)$, that is, the set of points where s is in the submodule obtained by multiplying with the maximal ideal $\mathfrak{m}_{X,P}$:

$$V(s) = \{ P \in X \mid s \in \mathfrak{m}_{X,P} \mathscr{L}_P \} \subset X. \tag{3.3.34}$$

We see that

$$\varphi^*(V(\ell)) = V(\varphi^*(s)) \tag{3.3.35}$$

or phrased in another way:

Let $\varphi : X \to \mathbb{P}^n$ be a morphism defined by a sheaf $\mathscr{L}$ that is generated by global sections. Then the intersections of $\varphi(X)$ with the various hyperplane sections in $\mathbb{P}^n$ pull back to the zero loci of the non-zero global sections of $\mathscr{L}$.

In the special case where $s = f \in k(X)^*$ is a non-zero section of the invertible sheaf $\mathscr{L} = \mathscr{L}(D)$, we have

$$\mathscr{L}(D)_P = \mathfrak{m}_{X,P}^{-v_P(D)} \tag{3.3.36}$$

so that the points P where f has a zero are exactly the points where $v_P(f) > -v_P(D)$. These are exactly the points in the support of the effective divisor $D+(f) \in |D|$ considered in 3.2.34. In fact, we see that if we take multiplicities into account we have

$$\varphi^*(V(\ell)) = V(\varphi^*(f)) = D + (f) \in |D|. \tag{3.3.37}$$

Remark 3.3.38. Note the subtlety: We do not consider the divisor defined by f as a rational function, but as a section of the sheaf $\mathscr{L}(D)$. This is what makes D appear in the final equality in (3.3.37).

Summarizing, in the special case $\mathscr{L} = \mathscr{L}(D)$, we see the following.

Let $\varphi : X \to \mathbb{P}^n$ be a morphism defined by a base-point free divisor D. Then the intersections of $\varphi(X)$ with the various hyperplane sections in $\mathbb{P}^n$ pull back to the elements of the linear system $|D|$.

What is the use of this? One important application is that we can understand when the map φ furnishes an embedding of X into projective space. For this, we need first of all that given two distinct points $P_1, P_2 \in X$, their images $\varphi(P_1), \varphi(P_2) \in \mathbb{P}^n$ are distinct. This is the case if and only if there exists a hyperplane H that contains P_1 but not P_2. Let ℓ by a linear form defining H. Then $s = \varphi^*(s)$ is a global section of $\mathscr{L}$ with $s \in \mathfrak{m}_{X,P_1}\mathscr{L}_{P_1}$ but $s \notin \mathfrak{m}_{X,P_2}\mathscr{L}_{P_2}$. We therefore see that injectivity of the morphism φ translates into the following condition:

$$\forall P_1, P_2 \in X \text{ with } P_1 \neq P_2 \;\; \exists s \in \mathscr{L}(X) : s \in \mathfrak{m}_{X,P_1}\mathscr{L}_{P_1}, s \notin \mathfrak{m}_{X,P_2}\mathscr{L}_{P_2}. \tag{3.3.39}$$

It turns out that this is not quite enough. For example, the map

$$\begin{aligned} \varphi : \mathbb{A}^1 &\to \mathbb{A}^2 \\ t &\mapsto (t^2, t^3) \end{aligned} \tag{3.3.40}$$

is injective, but its image $V(y^2 - x^3)$ has a singular point at $(0,0)$, so that we do not obtain a smooth embedding. To this end, we need that there is a well-defined tangent line at every point $\varphi(P) \in \varphi(X)$. This happens if and only if there is a hyperplane $H \subset \mathbb{P}^n$ that intersects P with multiplicity one. Translating this in terms of global sections of $\mathscr{L}$, we see that for the embedding to have non-singular image we additionally need the following condition:

$$\forall P \in X \;\; \exists s \in \mathscr{L}(X) : s \in \mathfrak{m}_{X,P}\mathscr{L}_P, s \notin \mathfrak{m}_{X,P}^2\mathscr{L}_P. \tag{3.3.41}$$

One can show, although we do not prove it here, that (3.3.39) and (3.3.41) are enough to ensure that φ is an embedding of X into $\mathbb{P}^n$ whose image is a non-singular curve.

Definition 3.3.42. An invertible sheaf on a projective curve X that is generated by global sections and that satisfies the conditions (3.3.39) and (3.3.41) is called very ample.

Example 3.3.43. The sheaf $\mathscr{L}(2D)$ from Example 3.3.26 is very ample.

We will see a useful rephrasing of the condition for a sheaf to be very ample when we discuss the Riemann–Roch theorem.

3.4 Sheaves of differentials

In this section, we will define one of the most important line bundles on a non-singular algebraic curve.

Definition 3.4.1. Let X be a non-singular algebraic curve. A differential on X is an expression ω of the form

$$\omega = \sum_{i=1}^{r} f_i d(g_i), \tag{3.4.2}$$

where $f_i, g_i \in k(X)$. Moreover, the symbol d satisfies the following rules:

(i) d is k-linear;

(ii) $d(\lambda) = 0$ for all $\lambda \in k$;

(iii) $d(fg) = fdg + gdf$.

Let P be a point of X, and let $U \subset \mathbb{A}^n$ be an affine patch of X that contains P. After a translation, we may assume that $P = (0,\ldots,0)$. On U, every rational function g can be written as a rational expression in $x_1,\ldots,x_n$, so that the rules in Definition 3.4.1 enable us to express dg as

$$dg = \frac{\partial g}{\partial x_1} dx_1 + \ldots + \frac{\partial g}{\partial x_n} dx_n. \tag{3.4.3}$$

Suppose that x_1 is a uniformizer at P, as we may after changing coordinates. Applying this to the defining equations of U, we can express all differentials $dx_2,\ldots,dx_n$ in terms of dx_1. This is most easily seen when $n = 2$, and indeed it is the case (though this is far from obvious, see [1, Exercise 7.21]) that every point on P non-singular curve X admits an affine patch U in $\mathbb{A}^2$ for which P is regular. By Proposition 2.6.8, U is defined by a single equation $g(x_1,x_2) = 0$. Deriving this relation, we see that

$$\frac{\partial g}{\partial x_1} dx_1 + \frac{\partial g}{\partial x_2} dx_2 = 0 \tag{3.4.4}$$

so that

$$dx_2 = -(\frac{\partial g}{\partial x_1} / \frac{\partial g}{\partial x_2}) dx_1. \tag{3.4.5}$$

Eliminating the differentials of the other variables in this way, we see that if $P \in X$ is a point of X with uniformizer π_P, we can express any differential ω on X in the form

$$\omega = f d\pi_P \tag{3.4.6}$$

where $f \in k(X)$.

Definition 3.4.7. Let ω be a differential form on X, and let P be a point of X. We define the valuation $v_P(\omega)$ of ω at P to be the valuation $v_P(f)$, where f is as in (3.4.6).

Remark 3.4.8. The valuation from Definition 3.4.7 does not depend on the choice of uniformizer. Indeed, suppose that u,v are two uniformizers of X at P. Since u and v are functions on a curve X, they satisfy a relation

$$g(u,v) = 0. \tag{3.4.9}$$

Moreover, since u and v are both uniformizers of X at P, which in the equation above has coordinates $(0,0)$, both partial derivatives $\frac{\partial g}{\partial u}$ and $\frac{\partial g}{\partial v}$ are non-zero. Since

$$\begin{aligned} du &= -(\frac{\partial g}{\partial u} / \frac{\partial g}{\partial v}) du, \\ dv &= -(\frac{\partial g}{\partial v} / \frac{\partial g}{\partial u}) du, \end{aligned} \tag{3.4.10}$$

we see that by changing uniformizers, the rational function f in (3.4.6) is multiplied by a non-zero rational function, so that its valuation does not change.

Definition 3.4.11. Given a non-zero differential form ω on X, we define the corresponding canonical divisor (ω) by

$$(\omega) = \sum_{P \in X} v_P(\omega)[P]. \tag{3.4.12}$$

Remark 3.4.13. Let us shows that the canonical divisor is well-defined, that is, that given a non-zero differential ω we have $v_P(\omega) = 0$ for almost all $P \in X$. To this end, we again choose an affine open part U of X which is described by a single equation in two variables

$$U : g(x_1, x_2) = 0. \tag{3.4.14}$$

Since U is open in X, it is cofinite, so it suffices to show that $v_P(\omega)$ for all $P \in U$. To this end, use (3.4.5) to write

$$\omega = f\,dx_1 = f\,d(x_1 - P_1). \tag{3.4.15}$$

An inspection of the Jacobian matrix

$$J_U(P) = \left(\frac{\partial g}{\partial x_1}(P), \frac{\partial g}{\partial x_2}(P)\right) \tag{3.4.16}$$

shows that $x_1 - a_1$ is a uniformizer at P as long as $\frac{\partial g}{\partial x_2}(P) \neq 0$. Now the definition of $v_P(\omega)$ shows that $v_P(\omega) = 0$ as long as $\frac{\partial g}{\partial x_2}(P) \neq 0$ and moreover $v_P(f) = 0$ for f as in (3.4.15). The former condition holds on a cofinite set because the non-trivial equation $\frac{\partial g}{\partial x_2}(P) = 0$ defines a proper closed subset of U which is therefore finite. The latter condition is also satisfied for a cofinite subset of U by Proposition 3.1.4.

Proposition 3.4.17. *Let K_1, K_2 be two canonical divisors on X. Then K_1 and K_2 are linearly equivalent.*

Proof. Suppose that ω_1, ω_2 are such that $K_1 = (\omega_1)$ and $K_2 = (\omega_2)$. Choose a rational function x on X and write $\omega_i = f_i dx$ for $i = 1, 2$. Then

$$K_1 - K_2 = (\omega_1) - (\omega_2) = (f_1 dx) - (f_2 dx) = (f_1) + (dx) - (f_2) - (dx) = (f_1) - (f_2) = (f_1/f_2) \tag{3.4.18}$$

which finishes the proof. □

Definition 3.4.19. We define the line bundle Ω^1 defined by a canonical divisor K the *canonical line bundle* of X. The space of global sections of Ω_1 is denoted by $H^0(X, \Omega_X)$.

Proposition 3.4.17 implies that the canonical line bundle is well-defined up to isomorphism. Alternatively, one can work with the differentials (3.4.6) directly; since such a form is regular in an open neighborhood of P if and only if $f \in \mathscr{O}_{X,P}$, we see that they indeed form an invertible sheaf.

Definition 3.4.20. We define the genus $g(X)$ of X by

$$g(X) = H^0(X, \Omega_X). \tag{3.4.21}$$

Proposition 3.4.22. *Suppose that X_1, X_2 are isomorphic non-singular projective curves. Then $g(X_1) = g(X_2)$.*

Proof. Let $\varphi : X_1 \to X_2$ be an isomorphism. Given a differential form $\omega_2 = f_2 d\pi_2$ on X_2, with π_2 a uniformizer at $P_2 \in X_2$, its pullback

$$\varphi^*(\omega_2) = \varphi^*(f_2)\varphi^*(d\pi_2) = (f_2 \circ \varphi)d(\pi_2 \circ \varphi) \tag{3.4.23}$$

is a differential form on X_1. Since φ is an isomorphism, $\pi_2 \circ \varphi$ is a uniformizer at $P_1 = \varphi^{-1}(P_2)$. Therefore the valuation of $\varphi^*(\omega_2)$ at the point P_1 coincides with that of $\varphi^*(f_2)$, which, again because φ is an isomorphism, coincides with that of $\varphi^*(f_2)$ and therefore with that of the pullback $\varphi^*(\omega_2)$. This implies that

$$(\varphi^*(\omega)) = \varphi^*((\omega)) \tag{3.4.24}$$

In other words, φ^* maps a canonical divisor on X_2 to a canonical divisor on X_1. This means that the resulting spaces of global sections are isomorphic (again under pullback with φ) and therefore so are the dimensions of these spaces, which are $g(X_1)$ and $g(X_2)$ by definition. □

Remark 3.4.25. The equality (3.4.24) does not hold for general morphisms of curves; this is explored further in the Riemann–Hurwitz theorem (Theorem 3.8.8).

Remark 3.4.26. One construction that is highly useful when discussing valuations of functions and differentials is the following. The discrete valuation v_P on $\mathscr{O}_{X,P}$ gives rise to a norm $x \mapsto e^{-v_P(x)}$ on $\mathscr{O}_{X,P}$, and we denote the completion of $\mathscr{O}_{X,P}$ with respect to this norm by $\widehat{\mathscr{O}}_{X,P}$. It turns then turns out that there is an isomorphism of this completion with the power series ring $k[[t]]$, given by

$$\begin{aligned} \widehat{\mathscr{O}}_{X,P} &\to k[[t]] \\ \pi_P &\mapsto t \end{aligned} \tag{3.4.27}$$

where π_P is a uniformizer of X at P. We will often express this by writing $\mathscr{O}_{X,P} = k[[\pi_P]]$.

Given an element $f \in \mathscr{O}_{X,P}$, we can consider it as an element of $k[[\pi_P]]$ via (3.4.27), so that

$$f = c_e \pi_P^e + \text{terms of higher order.} \tag{3.4.28}$$

with $c_e \neq 0$. The valuation of f is then nothing but the order e of f considered as a power series. Moreover, taking derivations, we can write

$$df = (ec_e\pi_P^{e-1} + \text{terms of higher order})d\pi_P \tag{3.4.29}$$

and df is then the order of the power series between parentheses, which (nota bene!) may be strictly larger than $e-1$ if $\mathrm{char}(k) \mid e$. We consider these issues in Section 3.8.

Remark 3.4.30. The treatment in this section, while correct in all essentials, is not completely rigorous, which means that we have resorted to dubious steps and hand-waving here and there. A more complete treatment would involve the technical tool called Kähler differentials [2, Section II.8]. However, let it be stated explicitly here that the constructions in this section are still completely up to the task of working with differentials on algebraic curve in practice.

3.5 Examples of sheaves of differentials

Example 3.5.1. Consider the projective line $\mathbb{P}^1$ with homogeneous coordinates $(x_0 : x_1)$, and let $x = x_1/x_0$ be one of the affine coordinates on $\mathbb{P}^1$. We consider the differential

$$\omega = dx \in H^0(\mathbb{P}^1, \Omega_{\mathbb{P}^1}). \tag{3.5.2}$$

Since $\omega = 1 \cdot dx = 1 \cdot d(x-a)$ for all $a \in \mathbb{A}^1$, we see that ω has no zeros or poles on the affine part $D(x_0)$ corresponding to the coordinate x. It remains to determine the order of ω at the point at infinity $\infty = (0:1)$. For this, we change the affine coordinate x to $u = x_0/x_1 = 1/x$. On the level of differentials, we have that

$$dx = d(1/u) = u^{-2} du. \tag{3.5.3}$$

Since u is a uniformizer at ∞, we see that $\mathrm{ord}_\infty(dx) = -2$ and therefore

$$(\omega) = -2[\infty]. \tag{3.5.4}$$

Let $K = -2[\infty]$. Then $\ell(K) = 0$. Indeed, suppose that $f \in L(K)$. Then $v_P(f) \geq -v_P(K)$ for all P, so that in particular $v_P(f) \geq 0$ for all P, which implies that f is everywhere regular on $\mathbb{P}^1$. Theorem 2.5.64 then shows that f is constant. However, since $v_\infty(f) \geq -v_P(K) = 2$, we see that in fact f is zero, and we conclude that

$$H^0(\mathbb{P}^1, \Omega_{\mathbb{P}^1}) = 0. \tag{3.5.5}$$

In other words, $\mathbb{P}^1$ does not admit any non-zero global differentials, so that $g(\mathbb{P}^1) = 0$.

Example 3.5.6. Let $\mathrm{char}(k) \neq 2$, and let E be the projective closure of an affine curve

$$U : y^2 = x^3 + c_4 x + c_6 \tag{3.5.7}$$

with $4c_4^3 + 27c_6^2 \neq 0$. Then we have seen in Example 2.6.30 that E is a non-singular curve. Let us consider the differential ω_1 on E whose restriction to the affine part U is given by

$$\omega_1 = dx \tag{3.5.8}$$

We determine the canonical divisor K_1 of ω_1. To this end, recall that the Jacobian matrix $J_U(P)$ in a point $P = (a,b)$ of U is given by

$$J_U(P) = \left(-3a^2 - c_4, 2b\right). \tag{3.5.9}$$

This implies that $x-a$ is a uniformizer at all points $P = (a,b)$ of U with $b \neq 0$. For such points we can write $\omega_1 = d(x-a)$, so that $v_P(\omega_1) = 0$ for such points.

Now suppose that $b = 0$. Then $x-a$ is not a uniformizer at P, but since U is non-singular, we have that $y - b = y$ is a uniformizer. Since $g = x^3 + c_4 x + c_6$ has a simple zero in a, as we saw in Example 2.6.30, we can write $g = (x-a)h$ with $h(a) \neq 0$. The equation for U then becomes $y^2 = (x-a)h$. Since $v_P(y) = 1$ and since $v_P(h) = 0$ because h is a non-zero regular function in P, we see that $v_P(x-a) = 2$. Moreover, taking differentials we see that

$$2y\,dy = (3x^2 + c_4)dx \tag{3.5.10}$$

so that

$$dx = (2y/(3x^2 + c_4))dy. \tag{3.5.11}$$

Since $3x^2 + c_4$ is non-zero, again because g has a simple zero in a, we see that again $v_P(\omega_1) = v_P(y) = 0$.

Finally, we consider the point $O = (0:1:0)$ at infinity for the homogenized equation

$$E : y^2 z = x^3 + c_4 x z^2 + c_6 z^3. \tag{3.5.12}$$

We dehomogenize by setting $(x:y:z) = (u:1:v)$. The definition equation for the corresponding affine patch Y of E is given by

$$Y : v = u^3 + c_4uv^2 + c_6v^3. \tag{3.5.13}$$

so that u is a uniformizer at the point at infinity $O = (0:0) \in Y$. If $(a:b)$ is a point on the affine part U, then it corresponds to the point $(a:b:1)$ of E and therefore to the point $(a/b : 1/b)$ of Y if $b \neq 0$. In terms of coordinates, this means that we have $u = x/y$ and $v = 1/y$. We can accordingly rewrite the differential ω_1 as

$$\omega_1 = dx = d(u/v) = (vdu - udv)/v^2. \tag{3.5.14}$$

Also note that that (3.5.13) implies that $e = v_O(v) = 3$. Indeed, we have $e \geq 1$ since e is zero in O, so that the right hand side of (3.5.13) contains only terms of valuation ≥ 3 and therefore $e \geq 3$ by the properties of a discrete valuation. On the other hand, the terms on the right hand side have valuation $3, 1+2e, 3e$ respectively, and these values are distinct since $e \geq 3$, so that $e = 3$ by Remark 2.7.7.

The differential (3.5.14) is rather unwieldy to simplify directly, so we take another approach. If we define $w = v/u$, then the defining equation (3.5.13) of Y can be rewritten as

$$w = u^2 + c_4u^2u^2 + c_6u^2w^3. \tag{3.5.15}$$

From this, we see that

$$dw = 2udu + 2c_4uw^2du + 2c_4u^2wdw + 2c_6uw^3du + 3c_6u^2w^2dw. \tag{3.5.16}$$

Therefore

$$(1 - 2c_4u^2w - 3c_6u^2w^2)dw = (2u + 2c_4uw^2 + 2c_6uw^3)du \tag{3.5.17}$$

Now $(1 - 2c_4u^2w - 3c_6u^2w^2)$ is a local unit at O and du has trivial valuation because u is a uniformizer at O. Moreover, the valuation of $2u + 2c_4uw^2 + 2c_6uw^3$ equals 2, since u and w have valuation 1 and $3-1 = 2$ respectively, so that the terms in the given sum have distinct valuations $1,5,7$, which implies the claim by Remark 2.7.7. We conclude that

$$v_O(d(v/u)) = v_O(dw) = 1. \tag{3.5.18}$$

Now observe that

$$d(u/v) = d(1/w) = (1/w^2)dw \tag{3.5.19}$$

has valuation $-2v_O(w) + v_O(dw) = -2\cdot 2 + 2 = -3$. This implies that

$$v_O(\omega_1) = -3. \tag{3.5.20}$$

and

$$K_1 = (\omega_1) = P_1 + P_2 + P_3 - 3[O]. \tag{3.5.21}$$

where the points $P_i = (a_i, 0) \in U$ correspond to the simple roots a_i of g.

(Another way to obtain the valuation (3.5.21) is to use the fact that $\omega_1 = d(u/v)$ along with the fact that $v_O(u/v) = 1 - 3 = -2$. This means that under the injection of the field of fractions of $\mathscr{O}_{Y,O}$ into $k((u))$, the element u/v has a Laurent series expansion that starts with a non-zero multiple of u^{-2}. The Laurent expansion of the corresponding differential therefore starts with a non-zero multiple of u^{-3} since $\mathrm{char}(k) \neq 0$, which implies that its valuation equals -3.)

Observe that (ω_1) equals the principal divisor (y). Indeed, we have seen above that y has simple zeros at the points P_i, and it is non-zero and regular elsewhere on the affine part U. Since $E \setminus U = \{O\}$, we get $v_P(y) = -3$ either by a direct calculation or by Corollary 3.1.38. We see that if we consider $\omega_2 = dx/y$ instead of ω_1, then

$$K_2 = (\omega_2) = (\omega_1) - (f) = 0. \tag{3.5.22}$$

In this case $L(K_2)$ is nothing but the space of everywhere regular functions on U, which we know to be the constant functions by Theorem 2.5.64. We conclude that

$$H^0(E, \Omega_E) = k\frac{dx}{y} \tag{3.5.23}$$

is a space of dimension 1, so that $g(E) = 1$.

Example 3.5.24. Again suppose that $\mathrm{char}(k) \neq 2$, and consider the curve

$$U : y^2 = x^5 + x + 1 \tag{3.5.25}$$

As in the previous example, one shows that U is non-singular because the polynomial $g = x^5 + x + 1$ has simple roots. Let X be a projective curve that contains U as an affine subset, which exists by Theorem 2.7.52. As in the previous example, one shows that the canonical divisor $K_1 = (\omega_1)$ of the differential $\omega_1 = dx$ on X satisfies

$$(K_1)|_U = P_1 + P_2 + P_3 + P_4 + P_5 \tag{3.5.26}$$

where $P_i = (a_i, 0)$ are the five points corresponding to the roots of g.

It remains to analyze the valuations of K_1 at the remaining points in $X \setminus U$. This is more subtle than before, since we cannot take X to be the projective closure of U in $\mathbb{P}^2$, the reason being that this closure is singular. Indeed, this closure is defined by the homogeneous equation

$$y^2z^3 = x^5 + xz^4 + z^5. \tag{3.5.27}$$

This leads to the single new point $(0:1:0)$, which after dehomogenizing becomes the point $(0,0)$ on the affine curve

$$z^3 = x^5 + xz^4 + z^5. \tag{3.5.28}$$

Since the expansion around $(0,0)$ only contains terms of higher order, we see that this point is singular. (Alternatively, one can calculate the Jacobian matrix directly.)

To construct a second affine patch for X, we employ a useful trick based on Theorem 2.7.60. First we note that the affine patch U is the integral closure of $k[x]$ in $k(U)$. Indeed, since U is non-singular, the local rings $O_{U,P}$ are all regular and therefore discrete valuation rings, which are integrally closed in their field of fractions $k(U)$. Hence so is their intersection $k[U]$, which is therefore the integral closure of $k[x]$ in $k(U)$.

To obtain a second affine patch, we use the new coordinate $u = 1/x$ on the projective line corresponding to $k(U)$. If we then also define $v = y/x^3$, then we can rewrite (3.5.25) as

$$0 = (y^2 - x^5 - x - 1)/(x^6) = (y^2/x^6) - (1/x) - (1/x^5) - (1/x^6) = v^2 - u^6 - u^5 - u. \tag{3.5.29}$$

One checks that the new affine patch

$$V : v^2 = u^6 + u^5 + u \tag{3.5.30}$$

thus obtained is indeed regular. Indeed, outside of the new point at infinity $\infty = (0:0)$, we can consider V as a subset of U via the mutually inverse morphisms

$$\begin{aligned} U \setminus V(x) &\longleftrightarrow V \setminus V(u) = V \setminus \{\infty\} \\ (x,y) &\longmapsto (1/x, y/x^3) \\ (1/u, v/u^3) &\longleftarrow (u,v). \end{aligned} \tag{3.5.31}$$

Therefore we only have to check regularity of V at ∞. This can be done can be done using the corresponding Jacobian matrix

$$J_V(\infty) = \left(\frac{\partial(v^2 - u^6 - u^5 - u)}{\partial u}(\infty), \frac{\partial(v^2 - u^6 - u^5 - u)}{\partial v}(\infty) \right) = (-1, 0). \tag{3.5.32}$$

which shows that v is a uniformizer at ∞.

We claim that the affine curve V has the property that its coordinate ring $k[V] = k[u,v]/(v^2 - u^6 - u^5 - u)$ is the integral closure of $k[u] = k[1/x]$ in $k(U)$. Indeed, as above we see that $k[V]$ is integrally closed in $k(V) = k(U)$ because V is non-singular, and therefore it is the integral closure of $k[u]$ in $k(U)$ since it contains $k[u]$. Theorem 2.7.60 shows that V is the remaining affine part of X that we need.

To determine K on X, we rewrite $\omega_1 = dx$ as

$$\omega_1 = d(1/u) = u^{-2} du. \tag{3.5.33}$$

Equation (3.5.30) and the fact that u is a uniformizer at ∞ shows that $v_\infty(u) = 2$, so it remains to determine $v_\infty(du)$. The power series argument from Example 3.5.6 can be modified to show that $v_\infty(du)$, but there is also a direct argument: Taking derivations on both sides of (3.5.30), we obtain

$$2v dv = (6u^5 + 5u^4 + 1) du. \tag{3.5.34}$$

The valuation of dv at ∞ equals 0 since v is a uniformizer there. Since $6u^5+5u^4+1$ is a regular function on V that is non-zero in ∞, it has valuation. Therefore $v_\infty(du) = v_\infty(2v) = v_\infty(v) = 1$, which shows that

$$v_\infty(\omega_1) = v_\infty(u^{-2} du) = -2 v_\infty(u) + v_\infty(du) = -2 \cdot 2 + 1 = -3 \tag{3.5.35}$$

and

$$K_1 = (\omega_1) = P_1 + P_2 + P_3 + P_4 + P_5 - 3\infty \tag{3.5.36}$$

If we again divide by y to consider $\omega_2 = dx/y$ instead, we get that

$$K_2 = (\omega_2) = 2\infty. \tag{3.5.37}$$

We see that determining the space of global sections $H^0(X, \Omega_X)$ is isomorphic to $L(2\infty)$ via

$$\begin{aligned} L(2\infty) &\to H^0(X, \Omega_X) \\ f &\mapsto f\omega_2 = f(dx/y) \end{aligned} \tag{3.5.38}$$

Now $L(2\infty)$ is a subspace of the space of functions that are everywhere regular on $X \subset X$, and the latter space admits the k-basis of monomials

$$\left(1, x, x^2, \dots, y, yx, yx^2, \dots\right). \tag{3.5.39}$$

The valuation of $x = 1/u$ in ∞ equals $-v_\infty(u) = -2$, and the valuation of $y = v/u^3$ equals $v_\infty(v) - 3v_\infty(u) = 1 - 3 \cdot 2 = -5$. Therefore the valuations of the monomials above are

$$(0, -2, -4, \ldots, -5, -7, -9 \ldots). \tag{3.5.40}$$

The discrete valuation properties of v_∞ imply that $L(2\infty)$ is spanned by the first two monomials $1, x$, so that applying the bijection (3.5.38) yields

$$H^0(X, \Omega_X) = k(dx/y) \oplus k(xdx/y). \tag{3.5.41}$$

We will generalize this example in Sections 4.3 and 4.4.

3.6 The Riemann–Roch Theorem

Let D be a Weil divisor on a non-singular projective curve X. As in Remark 3.2.23, we consider its space of global sections

$$L(D) = \{f \in k(X) \mid v_P(f) \geq -v_P(D) \text{ for all } P \in X\}. \tag{3.6.1}$$

In what follows, we study the dimension

$$\ell(D) = \dim_k L(D). \tag{3.6.2}$$

Proposition 3.6.3. *Suppose that* $\deg(D) < 0$. *Then* $\ell(D) = 0$.

Proof. Suppose that $f \in L(D)$ is non-zero. Then for all $P \in X$ we have $v_P(f) \geq -v_P(D)$, so that by Corollary 3.1.38 we have

$$0 = \deg((f)) = \sum_{P \in X} v_P(f) \geq \sum_{P \in X} -v_P(D) = -\deg(D) > 0, \tag{3.6.4}$$

a contradiction. We conclude that $L(D) = 0$, so that $\ell(D) = 0$. □

Proposition 3.6.5. *Let* $P \in X$. *Then* $\ell(D + P) \leq \ell(D) + 1$.

Proof. Let $e = v_P(D)$. Given $n \in \mathbb{Z}$, we define the k-vector subspace $W_P(n) \subset \mathscr{O}_{X,P}$ by

$$W_P(n) = \{f \in \mathscr{O}_{X,P} : v_P(f) \geq n\} \tag{3.6.6}$$

We have that $L(D) \subset L(D + P) \subset W_P(-e - 1)$, and an element f of $L(D + P)$ is in $L(D)$ if and only if $v_P(f) \geq -v_P(D)$, that is, if and only if f is in $W_P(-e)$. We see that $L(D)$ is the kernel of the map

$$\begin{aligned} L(D + P) &\to W_P(e - 1)/W_P(-e) \\ f &\mapsto [f]. \end{aligned} \tag{3.6.7}$$

Now it suffices to note that $\mathscr{O}_{X,P}$ is a discrete valuation ring, so that $W_P(n) = \mathfrak{m}_{X,P}^n$. This means that if $\pi_P \in \mathscr{O}_{X,P}$ is a uniformizer of X at P, then there is an isomorphism

$$\begin{aligned} k = \mathscr{O}_{X,P}/\mathfrak{m}_{X,P} &\to \mathfrak{m}_{X,P}^{-e-1}/\mathfrak{m}_{X,P}^{-e} = W_P(-e - 1)/W_P(-e) \\ f &\mapsto \pi_P^{-e-1} f. \end{aligned} \tag{3.6.8}$$

Therefore the quotient $W_P(-e - 1)/W_P(e)$ is of dimension at most 1, so that the kernel $L(D)$ of (3.6.7) is of codimension at most 1 in $L(D + P)$. □

Corollary 3.6.9. *We have $\ell(D) \leq 1 + \deg(D)$.*

Proof. We have $\ell(D - (\deg(D) + 1)) = 0$ by Proposition 3.6.3. The result then follows by applying Proposition 3.6.5 $\deg(D) + 1$ times. □

The definitive statement on dimensions of spaces of global sections is the Riemann–Roch theorem. We do not give its proof here; its proof is based on certain cohomological considerations around the sheaf of differentials, which are collectively called Poincaré duality.

Theorem 3.6.10. *Let X be a non-singular projective curve, and let K be a canonical divisor on X. Then for any divisor D on X we have*

$$\ell(D) - \ell(K - D) = 1 - g + \deg(D). \tag{3.6.11}$$

Remark 3.6.12. Note that the statement of the Riemann–Roch theorem is independent of the choice of canonical divisor K. Indeed, if K_1 and K_2 are two canonical divisors, then we have seen that K_1 and K_2 are linearly equivalent. The same then holds for $K_1 - D$ and $K_2 - D$. Now in general, if E_1 and E_2 are linearly equivalent divisors, with $E_1 = E_2 + (f)$ say, then there are mutually inverse isomorphisms of k-vector spaces

$$\begin{aligned} L(E_1) &\to L(E_2) \\ g &\mapsto fg \\ f^{-1}g &\leftarrow\!\shortmid g. \end{aligned} \tag{3.6.13}$$

In particular, this implies that $\ell(E_1) = \ell(E_2)$. Similarly, we note that $\deg(E_1) = \deg(E_2)$ by 3.1.38.

Example 3.6.14. We can check the Riemann–Roch theorem when $X = \mathbb{P}^1$. To this end, let D be a divisor on X. Then Proposition 3.1.14 implies that

$$D \sim n[\infty] \tag{3.6.15}$$

for $n = \deg(D)$. If $n < 0$, then Proposition 3.6.3 shows that $\ell(D) = 0$. Otherwise $L(D)$ is a subspace of the functions that are everywhere regular outside ∞, that is, a subspace of the polynomial ring $k[x] = k[x_1/x_0]$. A k-basis of this space is given by the monomials

$$\left(1, x, x^2, \ldots\ldots\right) \tag{3.6.16}$$

whose valuations at ∞ are given by

$$(0, -1, -2, \ldots). \tag{3.6.17}$$

The properties of the discrete valuation v_∞ now imply that

$$L(n[\infty]) = \{f \in k[X] \mid v_\infty(f) \geq n\} = k \oplus kx \oplus kx^n. \tag{3.6.18}$$

This shows that

$$\ell(D) = \begin{cases} n+1 & \text{if } n \geq 0 \\ 0 & \text{otherwise.} \end{cases} \tag{3.6.19}$$

Now let us see if these results are indeed consistent with Riemann–Roch, which states that

$$\ell(D) - \ell(K - D) = 1 - g + \deg(D). \tag{3.6.20}$$

We consider only the case $n = \deg(D) \geq 0$. Then (3.5.4) implies that

$$\deg(K - D) = \deg(K) - \deg(D) = -2 - \deg(D) < 0. \tag{3.6.21}$$

(As in Remark 3.6.12, note that the degree of the canonical divisor is well-defined.) We see that $\ell(K - D) = 0$ by Proposition 3.6.3, and we have already seen that $g(\mathbb{P}^1) = 0$, so that we obtain

$$\ell(D) = 1 + \deg(D) \tag{3.6.22}$$

when $\deg(D) \geq 0$, in line with (3.6.19) .

The Riemann–Roch theorem is not only interesting in itself. Indeed, being able to compute the dimensions of spaces $\ell(D)$ is very useful when determining whether a given divisor is very ample.

Proposition 3.6.23. *Let X be a non-singular projective curve, and let D be a divisor on X. Then D is base-point free if and only if*

$$\ell(D - P) = \ell(D) - 1 \tag{3.6.24}$$

for all $P \in X$, and X is very ample if and only if

$$\ell(D - P - Q) = \ell(D) - 2 \tag{3.6.25}$$

for every pair of points (P, Q) on X (not necessarily distinct).

Proof. Suppose first that D is base-point free, and let $P \in X$. Because of our hypothesis, we can can choose a section f in $L(D)$ that is not in $\mathfrak{m}_{X,P}\mathscr{L}(D)_P$. In terms of valuations, this means that $v_P(f) = -v_P(D)$. Indeed, we have $v_P(f) \geq -v_P(D)$ because $f \in L(D)$. Moreover, if we let π_P be a uniformizer at P, then $\mathfrak{m}_{X,P}(u)$ and $\mathscr{L}(D)_P = u^{-v_P(D)}\mathscr{O}_{X,P}$ by the definition of the Cartier divisor $L(D)$. This means that $f \in \mathfrak{m}_{X,P}\mathscr{L}(D)_P$ if and only if f is in $u^{-v_P(D)+1}\mathscr{O}_{X,P}$, that is, if and only if $v_P(f_D) \geq -v_P(D) + 1$. Since f is not in fact in $\mathfrak{m}_{X,P}\mathscr{L}(D)_P$, we get the requested equality of valuations. Proceeding as in the proof of Proposition 3.6.5, we see that existence of f implies that the map

$$L(D) \to W_P(-v_P(D))/W_P(-v_P(D) + 1) \cong k \tag{3.6.26}$$

is surjective. Since its kernel equals $L(D - P)$, we obtain that $\ell(D - P) = \ell(D) - 1$ for all $P \in X$. Conversely, if this criterion is satisfied, then the argument can be run in reverse to show that for all $P \in X$ there exists a section $f \in L(D)$ that is not in $\mathfrak{m}_{X,P}\mathscr{L}(D)_P$, which means that D is base-point free.

If X is very ample, then it is generated by global sections by definition. We rephrase the further conditions (3.3.39) and (3.3.41) in terms of (3.6.1). If the first condition (3.3.39) is satisfied, then given $Q \neq P$ we can choose $g \in L(D)$ such that $g \in \mathfrak{m}_{X,P}\mathscr{L}(D)_P$ but $g \notin \mathfrak{m}_{X,Q}\mathscr{L}(D)_Q$. As we have seen, this means that $g \in L(D - P)$ and that the map

$$L(D - P) \to W_Q(v_Q(D))/W_Q(-v_Q(D) + 1) \cong k \tag{3.6.27}$$

is surjective, so that its kernel $L(D - P - Q)$ is of codimension 1 in $L(D - P)$ and therefore $\ell(D - P - Q) = \ell(D) - 2$ for P and Q distinct. Similarly, if condition (3.3.39) is satisfied, we obtain that $\ell(D - 2P) = \ell(D) - 2$ for all P. (Please check this for yourself!) This means that the conditions in the proposition are necessary, and since this argument can again be run in reverse, they are sufficient as well. □

3.7 Consequences of the Riemann–Roch Theorem

Here are some general theoretic consequences of the Riemann–Roch theorem that are often useful.

Proposition 3.7.1. *Let K be a canonical divisor on a non-singular projective curve X of genus g. Then* $\deg(K) = 2g - 2$.

Proof. Take $D = K$ in the Riemann–Roch theorem to obtain

$$\ell(K) - \ell(0) = 1 - g + \deg(K). \tag{3.7.2}$$

We have $\ell(K) = g$ by definition, and $\ell(0)$ is nothing but the dimension of the space of everywhere regular rational functions on X, which equals 1 by Theorem 2.5.64. The result follows. □

Proposition 3.7.3. *Let X be a non-singular projective curve of genus g, and let D be a divisor on X. If* $\deg(D) \geq 2g - 1$, *then* $\ell(D) = 1 - g + \deg(D)$.

Proof. By Proposition 3.7.1 we have $\deg(K - D) = 2g - 2 - \deg(D) \leq 2g - 2 - (2g - 1) = -1$, so that $\ell(K - D)$ by Proposition 3.6.3. A direct application of Riemann–Roch now yields the result. □

Remark 3.7.4. Proposition 3.7.3 shows that if P is a point of X, then $\ell((2g + 1)[P]) = 1 - g + 2g + 1 = g + 2 > 1$. This implies that there exists a non-zero $f \in k(X)^*$ that has no poles outside P. This gives a more precise and more effective form of Remark 2.5.66: Any quasi-projective curve U with projective completion $X \neq U$ admits an everywhere regular non-constant function, which we can take to be the function f that we just constructed for a point $P \in X \setminus U$. (Note that f is indeed not constant on U, since otherwise it would be constant on X by Lemma 2.3.12.)

Corollary 3.7.5. *Let X be a non-singular projective curve of genus g, and let D be a divisor on X. If* $\deg(D) \geq 2g$, *then D is base-point free.*

Proof. We apply the criterion from Proposition 3.6.23. Since $\deg(D)$ and $\deg(D) - 1$ are both greater than or equal to $2g - 1$, Proposition 3.7.3 shows that indeed

$$\ell(D - P) = 1 - g + \deg(D - P) = 1 - g + \deg(D) - 1 = \ell(D) - 1 \tag{3.7.6}$$

for all $P \in X$. □

Corollary 3.7.7. *Let X be a non-singular projective curve of genus g, and let D be a divisor on X. If* $\deg(D) \geq 2g + 1$, *then D is very ample.*

Proof. The proof is similar to that of Corollary 3.7.5. □

Example 3.7.8. Consider the divisor $D = [\infty]$ on $\mathbb{P}^1$. Since $g(\mathbb{P}^1) = 0$ by Example 3.5.1, Corollary 3.7.7 shows that D is very ample. We can also see this using Proposition 3.6.23 directly. Indeed, we have $\deg(D) = 2$, so that $\deg(D - P - Q) = 0$ for all $P, Q \in X$, so that indeed Example 3.6.14 shows that

$$\ell(D - P - Q) = \deg(D - P - Q) = \deg(D) - 2 = \ell(D) - 2. \tag{3.7.9}$$

Note that D gives rise to the identity morphism $\mathbb{P}^1 \to \mathbb{P}^1$.

Remark 3.7.10. As we will see later, the converse statements to Corollary 3.7.5 and 3.7.7 do not hold. For a counterexample to the converse of Corollary 3.7.5, consider the curve $\overline{X}$ from Example 3.5.24 and let $D = K = 2[\infty]$. Then D is base-point free, although its degree is smaller than $2g = 4$. Indeed, arguing as in Example 3.5.24 shows that we have

$$L(D) = k1 \oplus kx. \tag{3.7.11}$$

so that $\ell(D) = 2$. We also have $\ell(D - P) = 1 = \ell(D) - 1$ for all $P \in X$. Indeed, otherwise we would have $\ell(D - P) = 2$ for some P. If this happens for $P = \infty$, then we get $\ell([\infty]) = 2$. This means that there exists a non-constant rational function f which is everywhere regular on $\overline{X}$ and which has a pole at ∞ only. Such a function f gives rise to an omorphism $X \to \mathbb{P}^1$ that is an isomorphism because of Proposition 3.1.36 and Theorem 2.7.52, which is impossible because $g(X) = 2$ and $g(\mathbb{P}^1) = 0$.

On the other hand, suppose that $P = (a, b) \in X$. Then the function $g = (x - a)$ has divisor $[P] + [Q] - 2[\infty]$, where $Q = (a, -b)$. Since the value of $\ell(D)$ does not change under taking linearly equivalent divisors, we see that

$$\ell(D - P) = \ell(D + (g) - [P]) = \ell([Q]). \tag{3.7.12}$$

The same argument as above shows that we cannot have $\ell([Q]) = 2$. Combining this with the previous case, we see that $2[\infty]$ is indeed a base-point free divisor on X.

Note that $3[\infty]$ is no longer base-point free, even though it is a "larger" divisor than D. Indeed, we have $L(3[\infty]) = L(2[\infty])$, so that the criterion for $3[\infty]$ to be base-point free fails for $P = \infty$.

We will see a counterexample to the converse of Corollary 3.7.7 in Section 4.4, where we will encounter curves X that admit a very ample divisor D of degree $2g - 2$. Indeed, in these examples we can take $D = K$ to be the canonical divisor.

Remark 3.7.13. As in Remark 3.7.10, given a point P on a non-singular projective curve X of genus g, we can ask what the dimensions $\ell(n[P])$ are. It turns out that for all but finitely many points P, we have

$$\ell(n[P] = \begin{cases} 0 & \text{if } n < 0 \\ 1 & \text{if } 0 \le n \le 2g - 2 \\ 1 - g + n & \text{if } n > 2g - 2. \end{cases} \tag{3.7.14}$$

Points P where this property does not hold are called Weierstrass points of X. Note that the point $\infty \in \overline{X}$ from Example 3.7.10 is a Weierstrass point, since for $n = 2$ we have $\ell(n[\infty]) = 2$ even though n is in the interval $[0, 2g - 2] = [0, 2]$.

We will see further, more explicit consequences of the Riemann–Roch for curves of low genus in the final chapters of these notes.

3.8 The Riemann–Hurwitz Theorem

Recall that given a non-constant morphism $\varphi : X \to Y$ of non-singular curves and a point $P \in X$, we have defined the ramification index of φ at P in Definition 3.1.19.

Definition 3.8.1. We say that φ is tamely ramified at P if the ramification index $e_\varphi(P)$ is coprime to the characteristic of the ground field k. If φ is not tamely ramified, then we will also call it wildly ramified.

The morphism φ is called separable if the induced map of function fields $\varphi^* : k(Y) \to k(X)$ is separable.

Given a point $P \in X$, we can consider a uniformizer $\pi_{\varphi(P)} \in \mathcal{O}_{X,P}$ of Y at $\varphi(P)$, as well as its pullback $\varphi^*(\pi_{\varphi(P)}) = \pi_{\varphi(P)} \circ \varphi$. It can be shown that if φ is separable, then $v_P(d(\varphi^*(\pi_{\varphi(P)}))) = 0$ for all but finitely many points of P of X. This makes the following notion well-defined.

Definition 3.8.2. Let $\varphi : X \to Y$ be non-constant separable morphism of non-singular curves. We define the ramification divisor R_φ of φ to be

$$R_\varphi = \sum_{P \in X} v_P(d(\varphi^*(\pi_{\varphi(P)})))[P] \tag{3.8.3}$$

The branch divisor is the pushforward of R_φ to Y.

Equation (3.8.3) involves quite a stack of parentheses, but it often simplifies:

Lemma 3.8.4. *Suppose that φ is tamely ramified in P. Then we have*

$$v_P(R_\varphi) = v_P(d(\varphi^*(\pi_{\varphi(P)}))) = e_\varphi(P) - 1. \tag{3.8.5}$$

Proof. The first equality is part of the definition of R_φ. For the second part, we choose a uniformizer π_Q at the point $Q = \varphi(P)$ as well. We then consider the two resulting embeddings $k(Y) \hookrightarrow k((\pi_Q))$ and $k(X) \hookrightarrow k((\pi_P))$. By the definition of the ramification index, after modifying π_Q by a non-zero scalar if needed, we can write

$$\varphi^*(\pi_Q) = \pi_Q \circ \varphi = \pi_P^e + \text{terms of higher order} \in k((\pi_P)) \tag{3.8.6}$$

where $e = e_\varphi(P)$. By deriving this equation, we obtain

$$d(\varphi^*(\pi_Q)) = (e\pi_P^{e-1} + \text{terms of higher order})d\pi_P \in k((\pi_P))d\pi_P. \tag{3.8.7}$$

Our hypothesis that the ramification of φ is tame implies that $e \neq 0$ in k, so that we indeed obtain $v_P(d(\varphi^*(\pi_Q))) = e - 1$. □

Theorem 3.8.8 (Riemann–Hurwitz)**.** *Let $\varphi : X \to Y$ be a non-constant morphism of non-singular curves of degree n, and let ω_Y be a differential form on Y, with pullback $\varphi^*(\omega_Y)$ to X. Then we have*

$$(\varphi^*(\omega_Y)) = \varphi^*((\omega_Y)) + R_\varphi \tag{3.8.9}$$

and

$$2g(X) - 2 = n(2g(Y) - 2) + \deg(R_\varphi). \tag{3.8.10}$$

In particular, if φ is everywhere tamely ramified, then we have

$$(\varphi^*(\omega_Y)) = \varphi^*((\omega_Y)) + \sum_{P \in X} (e_\varphi(P) - 1)[P]. \tag{3.8.11}$$

and

$$2g(X) - 2 = n(2g(Y) - 2) + \sum_{P \in X} (e_\varphi(P) - 1). \tag{3.8.12}$$

Proof. Consider a point P of X with image $Q = \varphi(P)$ in Y. If we choose a uniformizer π_Q at Q, then we can locally write

$$\omega_Y = f\, d\pi_Q \tag{3.8.13}$$

with $f \in k(Y)$, so that the valuation $w := v_Q(\omega_Y)$ equals $v_Q(f)$. We now consider the pullback

$$\omega_X = \varphi^*(\omega_Y) = \varphi^*(f)\varphi^*(d\pi_Q)) = (f \circ \varphi)d(\pi_Q \circ \varphi) \tag{3.8.14}$$

obtained by pulling back ω_Y, and determine its valuation at P. We have

$$v_P(\omega_X) = v_P(\varphi^*(f)) + v_P(d(\varphi^*(\pi_Q))). \tag{3.8.15}$$

Let us analyze the two terms in (3.8.15). To this end, we once again choose a uniformizer π_P at P and consider the two embeddings $\mathscr{O}_{Y,Q} \hookrightarrow k[[\pi_Q]]$ and $\mathscr{O}_{X,P} \hookrightarrow k[[\pi_P]]$. Then we can write

$$f = c\pi_Q^w + \text{terms of higher order}, \tag{3.8.16}$$

so that by substitution we obtain

$$\varphi^*(f) = f \circ \varphi = c\pi_P^{ew} + \text{terms of higher order} \tag{3.8.17}$$

and therefore $v_P(\varphi^*(f)) = ew$. We see that

$$v_P(\omega_X) = ew + v_P(d(\varphi^*(\pi_Q))) = e_\varphi(P)v_Q(\omega_Y) + v_P(d(\varphi^*(\pi_Q))). \tag{3.8.18}$$

We now form divisors on X whose valuations at points $P \in X$ coincide with the terms in (3.8.18). The left hand side then becomes

$$\sum_{P \in X} v_P(\omega_X)[P] = (\omega_X). \tag{3.8.19}$$

Second, the divisor

$$\sum_{P \in X} e_\varphi(P)v_Q(\omega_Y)[P] \tag{3.8.20}$$

is nothing but the pullback $\varphi^*(\omega_Y)$. Finally, the divisor

$$\sum_{P \in X} v_P(d(\varphi^*(\pi_Q)))[P] \tag{3.8.21}$$

equals R_φ by definition.

The statements on degrees follow because

$$\deg(\varphi^*(\omega_Y)) = \deg(\varphi)\deg(\omega_Y) \tag{3.8.22}$$

by Proposition 3.1.36 and moreover $\deg(\omega_X) = 2g(X) - 2$ as well as $\deg(\omega_Y) = 2g(Y) - 2$ by Proposition 3.7.1. □

Remark 3.8.23. In essence, the Riemann–Hurwitz theorem compares the divisor of the pullback of a differential form with the pullback of the divisor of that differential form. The final summand R_φ in (3.8.9) is a "defect" incurred by ramification.

This statement admits a sheaf-theoretic generalization that can also be used for varieties of higher dimension. For this, one introduces the sheaf of relative differentials $\Omega_{X|Y}$ with respect to a morphism $\varphi : X \to Y$; these are differentials on X that are trivial on the pullbacks of functions from Y. Moreover, one sets $\omega_{X|Y}$ to be the e-th exterior power of $\Omega_{X|Y}$, where e is the codimension of X with respect to Y. One then shows that if $f : X \to Y$ and $g : Y \to Z$ are morphism that satisfy a weak condition (more precisely, that they are quasi-projective local intersections) then we have

$$\omega_{X|Z} \cong \omega_{X|Y} \otimes_{\mathscr{O}_X} f^*(\omega_{Y|Z}). \tag{3.8.24}$$

This formula is called the adjunction formula. The Riemann–Hurwitz formula is the case where Z is simply a point and where X and Y are curves. The left hand side of (3.8.9) then corresponds to $\omega_{X|Z}$, the first term on the right hand side corresponds to $f^*(\omega_{Y|Z})$, and the second term on the right hand side corresponds to the relative sheaf of differentials $\omega_{X|Y}$. This is only one example of a classical result that has been made abstract to an incredible extent by Alexander Grothendieck in the language of schemes and dualizing sheaves; it leads to the Grothendieck–Riemann–Roch theorem.

3.9 Consequences of the Riemann–Hurwitz Theorem

Example 3.9.1. We consider the map

$$\begin{aligned} \varphi : \mathbb{P}^1 &\to \mathbb{P}^1 \\ x &\mapsto x^2(x-1). \end{aligned} \tag{3.9.2}$$

Then $\deg(\varphi) = 3$, and since φ has no poles outside $[\infty]$, we see that

$$\varphi^*([\infty]) = 3[\infty] \tag{3.9.3}$$

by Proposition 3.1.36, which means that φ ramifies at $x = \infty$. To analyze the other ramification of this map, we consider the equation

$$x^2(x-1) = t \tag{3.9.4}$$

as $t \in k$ varies. There is no ramification in the fiber of φ over t if and only if (3.9.4) has three distinct solutions. This is the case if and only the discriminant $\Delta(t)$ of the polynomial $x^2(x-1) - t$ is zero in t. We calculate

$$\Delta(t) = -27t^2 - 4t \tag{3.9.5}$$

and distinguish an number of cases.

Suppose first that $\mathrm{char}(k) \notin \{2, 3\}$. Then the equation $\Delta(t) = 0$ has the distinct solutions $t = 0$ and $t = -4/27$. For $t = 0$ we get the solution $x = 0$ with multiplicity 2, and for $t = -4/27$ we also get a solution of multiplicity 2 since

$$x^2(x-1) + 4/27 = (x - 2/3)^2(x + 1/3) \tag{3.9.6}$$

which means that $x = 2/3$ is a ramification point of φ of index 2. In this case we have

$$R_\varphi = [0] + [2/3] + 2[\infty]. \tag{3.9.7}$$

which is of degree 4. This is in accordance with (3.8.10), which states in this case that

$$-2 = 3 \cdot (-2) + \deg(R_\varphi). \tag{3.9.8}$$

Now suppose that $\mathrm{char}(k) = 3$. Then $\Delta(t) = -t$, so that we only obtain the double solution for $t = 0$. Taking into account (3.8.10), we see that we must have

$$R_\varphi = [0] + 3[\infty] \tag{3.9.9}$$

and we have wild ramification at $x = \infty$. To check the valuation 3 of $x = \infty$ in R_φ by hand, we use the local uniformizers $u = 1/t$ and $v = 1/x$ at infinity. Equation (3.9.4) then transforms to

$$\frac{1}{v^2}\left(\frac{1}{v} - 1\right) = \frac{1}{t} \tag{3.9.10}$$

which can be rewritten as

$$t = v^3/(1-v) = v^3 + v^4 + v^5 + \ldots \in k[[v]]. \tag{3.9.11}$$

We see that

$$dt = (v^3 + 2v^4 + v^6 + \ldots)dv \in k[[v]]dv \tag{3.9.12}$$

which indeed has valuation 3.

Finally, suppose that $\mathrm{char}(k) = 2$. Then $\Delta(t) = t^2$, so that we again only obtain the double solution for $t = 0$. This time the derivative of t in (3.9.4) is

$$dt = (v^2 + v^4 + v^6 + \ldots)dv \in k[[v]]dv \tag{3.9.13}$$

so that the multiplicity of $x = \infty$ in $\mathbb{R}_\varphi$ equals 2. For $x = 0$ and $t = 0$ we can use (3.9.4) to determine the multiplicity: We have

$$t = x^2(x-1) = x^2 + x^3 \tag{3.9.14}$$

so that

$$dt = x^2 dx \tag{3.9.15}$$

from which we see that the requested valuation at $x = 0$ equals 2. This time we obtain

$$R_\varphi = 2[0] + 2[\infty], \tag{3.9.16}$$

and as before, we see that $\deg(R_\varphi) = 4$.

Example 3.9.17. We study tamely ramified covers of $\mathbb{P}^1$ in more detail. Suppose that $\varphi : X \to \mathbb{P}^1$ is such a cover, ramified over ∞ and of degree n. Since no ramification occurs over the finite points of $\mathbb{P}^1$, we can use Proposition 3.1.36 to express the degree of the ramification divisor of φ as

$$\deg(R_\varphi) = \sum_{\substack{P \in X \\ \varphi(P)=\infty}} e_\varphi(P) - 1 = \sum_{\substack{P \in X \\ \varphi(P)=\infty}} e_\varphi(P) - \sum_{\substack{P \in X \\ \varphi(P)=\infty}} 1 = n - \#\varphi^{-1}(\infty). \tag{3.9.18}$$

If φ has degree 1, then it is an isomorphism, a case that does not interest us overmuch. But this is in fact the only possibility: Equations (3.8.10) and (3.9.18) imply that

$$-2 \le 2g(X) - 2 = -2n + \deg(R_\varphi) \le -2n + (n-1) = -n - 1 \tag{3.9.19}$$

so that $n \le 1$.

What if we admit two branch points instead, say 0 and ∞? Then a similar estimate shows that

$$-2 \le 2g(X) - 2 = -2n + \deg(R_\varphi) \le -2n + 2(n-1) = -2 \tag{3.9.20}$$

where equality is attained if and only if $g(X) = 0$ and both fibers $\varphi^{-1}(\infty)$ and $\varphi^{-1}(0)$ are of cardinality 1. In the next section we will show that this implies that $X = \mathbb{P}^1$. Moreover, by applying an automorphism of X, we can ensure that the ramification points above ∞ and 0 are ∞ and 0, respectively. This means that φ can be interpreted as an everywhere regular function on $\mathbb{P}^1$ that has a zero of multiplicity n at at 0. The only such functions are

$$\begin{aligned} \varphi : \mathbb{P}^1 &\to \mathbb{P}^1 \\ x &\mapsto x^n. \end{aligned} \tag{3.9.21}$$

By contrast, if we allow wild ramification, then there are far more covers with one or two branch points. Indeed, Example 3.9.1 gives a morphism that in characteristic 2 and 3 has only two ramification, and therefore in particular only two branch points. Moreover, it turns out that for every curve X over $\overline{F}_p$ there exists a morphism $\varphi : X \to \mathbb{P}^1$ that is ramified over 1 point only, which is in stark contrast to the affine case at the beginning of this example.

Example 3.9.22. Over the ground field $k = \overline{\mathbb{Q}}$, maps $\varphi : X \to \mathbb{P}^1$ that ramify over at most three points are known as Belyi maps. An example with $g(X) = 1$ is given by

$$\begin{aligned} \varphi : E : y^2 = x^3 + 1 &\longrightarrow \mathbb{P}^1 \\ (x, y) &\longmapsto \frac{1}{2}(-y+1). \end{aligned} \tag{3.9.23}$$

A famous result of Belyi states every curve X over $\overline{\mathbb{Q}}$ admits a Belyi map, and moreover that every curve over $\mathbb{C}$ that admits a Belyi map can be defined over $\overline{\mathbb{Q}}$ (in the sense that it can be defined by equations with coefficients in $\overline{\mathbb{Q}}$). This leads to the theme of dessins d'enfant, which are the graphs obtained as the preimages $\varphi^{-1}([0,1])$ of the unit interval. They can be studied group-theoretically by means of the

Example 3.9.24. We now consider maps $\varphi : X \to \mathbb{P}^1$ of degree 2 when $\mathrm{char}(k) \neq 2$. Such maps are automatically tamely ramified, and the Riemann–Hurwitz formula states

$$2g(X) - 2 = -2 \cdot 2 + \sum_{P \in X} (e_P - 1). \tag{3.9.25}$$

Now since $\deg(\varphi)$ we can only have $e_P = 1$ or $e_P = 2$. So if we let d be the number of points of $\mathbb{P}^1$ with ramification index 2, then we get

$$2g(X) - 2 = -4 + d \tag{3.9.26}$$

or in other words

$$g(X) = (d-2)/2. \tag{3.9.27}$$

This implies in particular that d is even.

In this special case, an equation for the curve X can be obtained without too much trouble. Since $k(Y)$ is an extension of $k(\mathbb{P}^1) = k(x)$ of degree 2, it is defined by an equation of degree 2 in y. Completing the square, which is possibly since $\mathrm{char}(k) \neq 2$ we obtain an affine defining equation of the form

$$U : y^2 = f(x). \tag{3.9.28}$$

If f contains a multiple linear factor $(x-a)$, then we can absorb this by replacing y by $(x-a)y$, so we may assume that f is separable, in which case one can argue as in Example 2.6.30 to show that U is non-singular. Conversely, given any separable polynomial $f \in k[x]$, the curve (3.9.28) is non-singular and defines a tamely ramified cover of $\mathbb{P}^1$ of degree 2. We call such curves hyperelliptic.

One thing may seem strange. What if f has odd degree? Then we seem to get an odd number of branch points, namely the zeros of f, which lead to the value $y = 0$ with multiplicity 2 when solving for y. Certainly this contradicts our statement above that d is even? In point of fact we have to consider the projective closure of U, which maps to $\mathbb{P}^1$, and as we shall see in Section 4.3, the point ∞ ramifies for this map if and only if $\deg(f)$ is odd. So if $\deg(f)$ is even, then we get $d = \deg(f)$ and $g(X) = (d-2)/2 = \deg(f)/2 - 1$, whereas if $\deg(f)$ is odd, we get $d = \deg(f)+1$ and $g(X) = (d-2)/2 = (\deg(f)-1)/2$. Or stated differently: If $f \in k[x]$ is a separable polynomial, and if X the hyperelliptic curve obtained as the projective completion of the affine patch $U : y^2 = f$, then we have

$$g(X) = \lfloor \frac{\deg(f) - 1}{2} \rfloor. \tag{3.9.29}$$

Remark 3.9.30. Tamely ramified covers of the projective line also exist in characteristic 2, but in this case the affine patches of hyperelliptic curves are defined by equations of the form

$$U : y^2 + h(x)y = f(x) \tag{3.9.31}$$

since we cannot complete the square as in the previous example.

Chapter 4

Magic

We apply the results of the previous chapter. Rather astonishingly, it is now possible to describe what a (non-singular, projective) curve of given genus over an algebraically closed base field looks like. We do this for curves of genus 0 up to 3, and treat hyperelliptic curves on the way.
In a nutshell, our results are as follows:

(i) A curve of genus 0 is isomorphic to the projective line $\mathbb{P}^1$.

(ii) A curve of genus 1 is isomorphic to a so-called elliptic curve, defined by a homogeneous equation

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

of degree 3 in $\mathbb{P}^2$. Moreover, such curves admits a group law, characterized by the fact that three points on a line sum to 0.

(iii) A curve of genus 2 is isomorphic to a so-called hyperelliptic curve, which is the projective completion of a non-singular affine curve of the form

$$U : y^2 + h(x)y = f(x)$$

where $g(x) = f(x) + 4h(x)^2$ is of degree either 5 or 6.

(iv) A curve of genus 3 is either a hyperelliptic curve as above where this time $g(x) = f(x) + 4h(x)^2$ of degree either 7 or 8 instead, or it is a plane quartic, that is, a projective curve $X = V(F) \subset \mathbb{P}^2$ defined by a homogeneous polynomial $F(x_0, x_1, x_2)$ of degree 4.

4.1 Curves of genus 0

We have seen that $\mathbb{P}^1$ is a non-singular projective curve of genus 0. Up to isomorphism, it is the only such curve:

Proposition 4.1.1. *Let X be a non-singular curve of genus $g = 0$. Then $X \cong \mathbb{P}^1$.*

Proof. Since the base field k is algebraically closed, the Nullstellensatz shows that X has a point P. The Riemann–Roch theorem applied to the divisor $D = [P]$ shows that

$$\ell([P]) - \ell(K - [P]) = 1 - g + \deg([P]) = 1 + \deg([P]) = 2. \tag{4.1.2}$$

Since $g = 0$, Proposition 3.7.1 shows that $\deg(K) = 2g - 2 = -2$, so that $\deg(K - [P]) = -3$. Proposition 3.6.3 then implies that $\ell(K - [P]) = 0$. We see that

$$\ell([P]) = 2. \tag{4.1.3}$$

This implies that $L([P])$ contains a non-constant function f. Because of the defining property of $L([P])$, we see that f can only have a pole at P, of pole order at most 1. Therefore the pole order of f must equal 1, since otherwise Theorem 2.5.64 shows that f is constant. As in the proof of Corollary 3.1.38, we see that f defines a morphism $X \to \mathbb{P}^1$. One the other hand, since f has a single pole, Proposition 3.1.36 shows that f has degree 1, which means that it is an isomorphism. □

It is possible to develop the theory of algebraic curves over non-algebraically closed fields as well. In this situation Proposition 4.1.1 no longer holds. However, it turns out that because the canonical sheaf is intrinsically defined, we can always find a canonical divisor K over the base field. We can then apply the analog of the following result:

Proposition 4.1.4. *Let X be a non-singular curve of genus* 0*, and let K be a canonical divisor on X. Then $\mathscr{L}(-K)$ defines an embedding of X into $\mathbb{P}^2$ whose image is a* conic*, that is, a projective curve in $\mathbb{P}^2$ defined by a homogeneous equation of degree* 2*.*

Proof. Since $\deg(-K) = 2 \geq 2g + 1$, Corollary 3.7.7 shows that $-K$ is very ample. Since $\ell(-K) = 1 + 2 = 3$, Theorem 3.3.19 states that after choosing a basis of $L(-K)$ we obtain an embedding

$$\varphi : X \to \mathbb{P}^{3-1} = \mathbb{P}^2 \tag{4.1.5}$$

such that $\mathscr{L}(-K) = \varphi^*(\mathscr{O}(1))$. Now the global sections of $\mathscr{O}(1)$ are given by linear forms ℓ that define hyperplanes in $\mathbb{P}^2$. Theorem 3.3.19 shows that these pull back to global sections s of $\mathscr{L}(-K)$. This means that under the embedding φ, the intersection of H with X corresponds to the zero locus of a global section $s \in L(-K)$ on X. If s corresponds to a rational function $f \in k(X)$, then by definition of the invertible sheaf $\mathscr{L}(-K)$ its zeros (counted with multiplicities) are described by the effective divisor $(f) - K$ that is linearly equivalent to $-K$. Conversely, any effective divisor linearly equivalent to $-K$ is obtained in this way.

Let $(f) - K$ be a hyperplane section of X thus obtained. Then $\deg((f) - K) = \deg((f)) - \deg(K) = 0 - (-2) = 2$ by Corollary 3.1.38. Now Proposition 2.6.9 shows that $\varphi(X) \subset \mathbb{P}^2$ is defined by a single homogeneous equation, and Bézout's Theorem (Corollary 3.1.44) shows that this equation is of degree 2. □

Remark 4.1.6. The discussion in the proof of Proposition 4.1.4 applies more generally: If D is a divisor on a curve X, then the zero divisors of the elements of $L(D)$ run through the effective divisors on X that are linearly equivalent to D. Moreover, if D is base-point free, then the pullbacks of hyperplane sections of $\varphi(X)$ under the morphism φ are exactly these effective divisors.

There are many conics over $\mathbb{Q}$ that do not admit a rational point. For example, this is the case for

$$X : x^2 + y^2 + z^2 = 0 \subset \mathbb{P}^2 \tag{4.1.7}$$

since X does not even have real points. Another example is

$$X : x^2 + y^2 - 3z^2 = 0 \subset \mathbb{P}^2 \tag{4.1.8}$$

which does have real points. Determining whether a given conic has a point is an arithmetic question related to Hilbert symbols and quaternion algebras. We do not go into this matter further, but illustrate how a conic with a point can be explicitly parametrized by $\mathbb{P}^1$.

Example 4.1.9. Consider the conic

$$X : x^2 + y^2 - z^2 = 0. \tag{4.1.10}$$

It admits the rational point $P = (1 : 0 : 1)$. To find an isomorphism of X with $\mathbb{P}^1$, we have to find a rational function $f \in k(X)$ that has a single pole in P and no poles elsewhere. We try to construct f as a quotient of suitable homogeneous linear forms. First note that the linear form $x - z$ vanishes in P. In fact Bézout's theorem (Corollary 3.1.44) shows that counting multiplicities, the zero locus of $x - z$ has two points of intersection with X. And so it turns out: In fact $x - z$ has a double zero at P, since it has no zeroes elsewhere.

We try to find a linear form ℓ such that we can take $f = \ell/(x - z)$. For this, we need to cancel the double zero of $x - z$ at P, so that we obtain a single pole in the end. This works as long as ℓ also has a zero at P. To this end, we can take $\ell = y$. We see that y has another zero at $Q = (1 : 0 : -1)$, so that

$$(f) = (y/(x - z)) = (y) - (x - z) = [P] + [Q] - 2[P] = [Q] - [P]. \tag{4.1.11}$$

We see that f defines an isomorphism $f : X \to \mathbb{P}^1$ that sends Q to 0 and P to infinity.

Of course f is nothing but the projective pendant of the map that we encountered in Example 2.4.34. Note how much easier our construction of morphisms has become as we need no longer worry about poles because of the extension property in Proposition 2.7.50.

The construction of the inverse of f can be understood as follows. The affine version

$$\begin{aligned} f : X &\to \mathbb{P}^1 \\ (x, y) &\mapsto y/(x - 1) \end{aligned} \tag{4.1.12}$$

of the map that we constructed associates to a given point (x, y) of X the slope of the line through (x, y) and $(1, 0)$. Conversely, let such a slope t be given. The corresponding line is parametrized by

$$\lambda \mapsto (\lambda + 1, t\lambda). \tag{4.1.13}$$

Substituting this expression in the affine equation $x^2 + y^2 = 1$, we obtain the equation

$$(\lambda + 1)^2 + t^2\lambda^2 = 1 \tag{4.1.14}$$

which can be rewritten as

$$(t^2 + 1)\lambda^2 + 2\lambda = 0. \tag{4.1.15}$$

Besides the solution $\lambda = 0$ that corresponds to the base point $P = (1, 0)$ in affine coordinates, we get $\lambda = -2/(t^2 + 1)$. Substituting this into (4.1.13), we obtain the inverse from Example 2.4.34.

In Example 2.4.34 we constructed an isomorphism of $\mathbb{P}^1$ with three given points removed with the circle with three given points removed. Such an isomorphism exists for any conic X with three points removed in our usual situation where the base field k is algebraically closed. Indeed, Theorem 4.1.1 shows that there exists an isomorphism $X \to \mathbb{P}^1$, so that the given points map to *some* subset of three points of $\mathbb{P}^1$. This may not be the specified subset, but one can then apply the following useful result, which is often summarized by stating that the automorphism group of $\mathbb{P}^1$ is three-transitive.

Proposition 4.1.16. *Let $S = \{s_1, s_2, s_3\}$ and $T = \{t_1, t_2, t_3\}$ be two subsets of $\mathbb{P}^1$ of cardinality 3. Then there exists an automorphism φ of $\mathbb{P}^1$ such that $\varphi(s_i) = t_i$ for $i = 1, 2, 3$.*

Proof. Since we can compose automorphisms, we may assume that $S = \{\infty, 0, 1\}$ and $T = \{t_1, t_2, t_3\}$. Then we can take

$$\begin{aligned} \varphi : \mathbb{P}^1 &\to \mathbb{P}^1 \\ x &\mapsto \frac{t_1(t_3 - t_2)x + t_2(t_1 - t_3)}{(t_3 - t_2)x + (t_1 - t_3)}, \end{aligned} \tag{4.1.17}$$

which has inverse

$$\begin{aligned} \varphi^{-1} : \mathbb{P}^1 &\to \mathbb{P}^1 \\ x &\mapsto \frac{(t_3 - t_1)(x - t_2)}{(t_3 - t_2)(x - t_1)}. \end{aligned} \tag{4.1.18}$$

□

Remark 4.1.19. The proof of Proposition 4.1.16 in fact does not deal with the case where one of the points t_i is ∞. This case is left to the reader as an exercise. (Hint: Reduce the question to the construction of a linear system of equations.)

4.2 Curves of genus 1

We have seen curves of genus 1 in Example 2.6.30 and Example 3.5.6. It turns out that if $\mathrm{char}(k) \neq 2, 3$, then these are essentially all examples of curves of genus 1.

Theorem 4.2.1. *Suppose that $\mathrm{char}(k) \neq 2, 3$. Let E be a curve of genus 1 over k. Then E admits a defining equation*

$$E : y^2 z = x^3 + c_4 x z^2 + c_6 z^3. \tag{4.2.2}$$

with $4c_4^3 + 27c_6^2 \neq 0$.

Proof. Choose a point O on E. We consider the spaces of global sections $L(n[O])$ for n positive. If $n = 0$, then $L(0)$ is the space of everywhere regular functions on E, which is of dimension 1 because it is the space of constant functions k, as Theorem 2.5.64 shows. If $n > 0$, then the Riemann–Roch theorem tells us that

$$\ell(n[O]) - \ell(K - n[O]) = 1 - g + n = n, \tag{4.2.3}$$

where K is a canonical divisor on E. Note that $\deg(K) = 2g - 2$ because of Proposition 3.7.1, so that $\deg(K - n[O]) < 0$, which implies $\ell(K - n[D]) = 0$ by Proposition 3.6.3. We see that

$$\ell(n[D]) = n \quad \text{for } n > 0. \tag{4.2.4}$$

For $n = 1$, we see that $L([O])$ is the old space of constant functions. For $n = 2$, we have $\ell(2[O]) = 2$, and we get a second rational function x with $v_O(x) = -2$. For $n = 3$, we get yet another function y with $v_O(y) = -3$. Note also that $L(3[O])$ is very ample because of Corollary 3.7.7, so that it gives rise to an embedding

$$\varphi : E \to \mathbb{P}^2. \tag{4.2.5}$$

It remains to describe the defining equation of E. Because of Proposition 2.6.9 we need only find a homogeneous equation of smallest degree that relates x and y. To this end, we consider the spaces $L(n[O])$ further.

For $n = 4$ we have that $L(4[O]) = 4$, and the functions $1, x, y, x^2$ are in this spaces. Since their valuations $0, -2, -3, -4$ are distinct, they do not satisfy a linear relation. The same holds when considering the space $L(5[O])$, which is spanned by the functions $1, x, y, x^2, xy$ with distinct valuations $0, -2, -3, -4, -5$ at O. However, we have $L(6[O]) = 6$, but this space contiains the 7 monomials $1, x, y, x^2, xy, x^3, y^2$. We see that there exists a linear dependence between these monomials, and since the respective valuations are $0, -2, -3, -4, -5, -6, -6$, this relation must involve both x^2 and y^3. Since 2 and y are coprime, a suitable scaling ensures that x and y both occur with coefficient 1 in this relation, which is therefore of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{4.2.6}$$

Since $\mathrm{char}(k) \neq 2, 3$, we can apply Tschirnhausen transformations to rewrite this equation in the form

$$y^2 = x^3 + c_4 x + c_6. \tag{4.2.7}$$

The homogenization (4.2.2) of this equation is therefore the equation that defines E. Since E is a non-singular projective curve, we see that $4c_4^3 + 27c_6^2 \neq 0$ by Example 2.6.30. □

Remark 4.2.8. Theorem 4.2.1 shows that also if $\mathrm{char}(k) = 2, 3$, the elliptic curve still admits a non-singular equation

$$E : y^2 + a_1 xyz + a_3 yz^3 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3. \tag{4.2.9}$$

Definition 4.2.10. An elliptic curve is a pair (E, O), where E is a curve of genus 1 and where O is a point on E.

Theorem 4.2.11. *Let (E, O) be an elliptic curve, and let $\mathrm{Pic}(E) = \mathrm{Cl}^0(E)$ be the Picard group of E, that is, the subgroup of the class group of E generated by the image of divisors of degree 0. Then the map*

$$\begin{aligned} i : E &\to \mathrm{Pic}(E) \\ P &\mapsto [P] - [O] \end{aligned} \tag{4.2.12}$$

is an isomorphism.

Proof. We first show that i is injective. Suppose that $[P] - [O]$ and $[Q] - [O]$ have the same image in $\mathrm{Pic}(E)$ for distinct points P and Q of E. Then $[P] - [O] \sim [Q] - [O]$ by definition of the class group. But this means that $[P] - [Q] \cong 0$, which implies that there exists a rational function f on E with divisor $[P] - [Q]$. As we have seen in the proof of Corollary 3.1.38, such a rational function f defines an isomorphism $E \to \mathbb{P}^1$, which is nonsense since $g(E) = 1$ and $g(\mathbb{P}^1) = 0$.

Now to show that i is surjective. Let D be a divisor on E of degree 0. Then $D + [O]$ has degree 1. As in the proof of Theorem 4.2.1, we see that $\ell(D + [O]) = 1$. This means that there exists a non-trivial rational function $f \in D + [O]$, which means that $D + [O] + (f) \geq 0$ is effective. But this divisor is again of degree 1 by Corollary 3.1.38. We see that $D + [O] + (f) = [P]$ for some $P \in E$, which means that $D \cong [P] - [O]$. This shows surjectivity. □

We can use Theorem 4.2.1 to embed E into $\mathbb{P}^2$ using the invertible sheaf $\mathscr{L}(3[O])$, so that O becomes the point $(0 : 1 : 0)$ of E. Moreover, we can use Theorem 4.2.11 to define a group law on E. This group law has the following property. Suppose that $P + Q + R = 0$. Then this means that

$$([P] - [O]) + ([Q] - [O]) + ([R] - [0]) \sim 0, \tag{4.2.13}$$

that is,

$$[P] + [Q] + [R] \sim 3[O] \tag{4.2.14}$$

Note that $3[O]$ is a hyperplane section of E, namely the intersection with the hyperplane $z = 0$. Now as Remark 4.1.6 shows, because the embedding φ from (4.2.5) comes from the divisor $3[O]$, the hyperplane sections of E are exactly the divisors on E that are linearly equivalent to $3[O]$. Since $[P]+[Q]+[R]$ is such a divisor, and this argument can be run in reverse, we see the following,

Proposition 4.2.15. *If (E, O) is an elliptic curve defined by an equation*

$$E : y^2 z = x^3 + c_4 x z^2 + c_6 z^3 \tag{4.2.16}$$

and if $O = (0 : 1 : 0)$, then the group law from Theorem 4.2.11 is characterized by the following property:

Three points $P, Q, R \in E$ sum to zero if and only if they are collinear.

This makes it possible to make the abelian group structure on E completely explicit. First of all, using the isomorphism (4.2.12), we see that O is the identity element of E. Now note that if $P \neq Q$ are distinct points on E, then we can draw a line ℓ through P and Q, which by Bézout's theorem (Corollary 3.1.44) has a third point of intersection R with E. Then $R = -P - Q$. If $R = O = (0 : 1 : 0)$, then $P + Q = -R = O$. Otherwise we have $R = (a : b : 1)$ for some $a, b \in k$. The line $x = az$ then has three points of intersection with E, one of which is O and the other of which is $(a : -b : 1)$. Note that this implies that $(a : b : 1) + (a : -b : 1) + O = 0$, or in other words, since $O = 0$, that

$$-(a : b : 1) = (a : -b : 1). \tag{4.2.17}$$

We see that $-R = P + Q$ is the point $(a : -b : 1)$ obtained by mirroring R in the y-axis.

If $P = Q$, then the argument can be run with a tangent line ℓ of E at P. This satisfies $\ell \cap E = 2[P] + [R]$ for some R, and again we have that $2[P] = -R$ can be obtained by reflecting the third point R in the y-axis.

Example 4.2.18. Let E be the elliptic curve with affine equation

$$E : y^2 = x^3 - 2x + 5. \tag{4.2.19}$$

and consider the points $P = (1, 2)$ and $Q = (2, 3)$. A line through these points is given by $y = x + 1$. Let us parametrize this so that P corresponds to the parameter value $t = 0$ and such that Q corresponds to the parameter value $t = 1$. This is achieved by the function

$$\ell(t) = (t + 1, t + 2). \tag{4.2.20}$$

We now determine the third point on the corresponding line. By substituting (4.2.20) into (4.2.19) we obtain

$$t^2 + 4t + 4 = (t + 2)^2 = (t + 1)^3 - 2(t + 1) + 5 = t^3 + 3t^2 + t + 4, \tag{4.2.21}$$

that is,

$$t^3 + 2t^2 - 3t = 0. \tag{4.2.22}$$

Counting multiplicities, the cubic equation (4.2.22) has three solutions. By construction already know two parameter values that correspond to solutions, namely $t = 0$ and $t = 1$, so we divide with remainder by $t(t - 1)$ to obtain the polynomial $t + 3$, which shows that the third parameter value that corresponds to a solution is $t = -3$. Alternatively, we can use that the sum of the roots of the monic polynomial (4.2.22) equals minus the second highest coefficient, that is, −2; this leads to the same parameter value, and with it, to the third point

$$R = (-2,-1) \in E \cap \ell \tag{4.2.23}$$

We now see that

$$P + Q = -R = (-2, 1). \tag{4.2.24}$$

We now calculate the point $2P = P + P$. For this, we calculate the tangent line to E at P. To this end, let $f = y^2 - x^3 + 2x - 5$ be the polynomial equation whose vanishing defines E. Then we have

$$J_E(P) = \left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) = \left(-3x^2 + 2, 2y\right)(P) = (-1, 4). \tag{4.2.25}$$

This means that up to higher order terms, the equation for E in P is given by $x-1-4(y-2) = 0$. A parametrization of the corresponding line for which P corresponds to the parameter value $t = 0$ is given by

$$\ell(t) = (t+1, (1/4)t + 2). \tag{4.2.26}$$

This time, substitution of (4.2.26) into (4.2.19) gives

$$(1/16)t^2 + t + 4 = ((1/4)t + 2)^2 = (t+1)^3 - 2(t+1) + 5 = t^3 + 3t^2 + t + 4, \tag{4.2.27}$$

that is,

$$t^3 + (47/16)t^2 = 0 \tag{4.2.28}$$

Besides the solution of double multiplicity $t = 0$ we obtain the third solution $t = -47/16$. This leads to the third point

$$R = (-31/16, 81/64). \tag{4.2.29}$$

We see that

$$2P = -R = (-31/16, -81/64). \tag{4.2.30}$$

Remark 4.2.31. It can be shown that elliptic curves are the only non-singular curves that admit a group law. Their higher-dimensional analogs, that is, non-singular projective group varieties, are called abelian varieties. It turns out that if X is a general non-singular projective curve, then $\mathrm{Pic}(X)$ is an abelian variety of dimension $g(X)$.

Remark 4.2.32. Over non-algebraically closed fields, there may not exists a rational point O of E. In this case, not every curve X of genus 1 admits the structure of an elliptic curve. More astonishingly, it turns out that the embeddings of such curves X into projective spaces $\mathbb{P}^n$ can be very complicated, in the sense that they may only exist for large n.

The theory of elliptic curve is a vast area of mathematics, and a subject of a course of its own. Let us only mention here that these curves arose when determining the arc length of ellipses (hence their name), and that over $\mathbb{C}$, they can be described as complex tori ("doughnuts") of dimension 1. That is, there exists a lattice $\Lambda \subset \mathbb{C}$ such that there is an isomorphism of holomorphic Riemann surfaces

$$E \cong \mathbb{C}/\Lambda. \tag{4.2.33}$$

4.3 Hyperelliptic curves

Definition 4.3.1. Let X be a non-singular projective curve over k. Then we say that X is hyperelliptic if it is of genus ≥ 2 and it admits a tamely ramified map $\pi : X \to \mathbb{P}^1$ of degree 2.

We have seen hyperelliptic curves in Example 3.9.24. The current section will study them in more detail.

For simplification, we assume throughout that $\mathrm{char}(k) \neq 2$, so that, as we have seen, X admits an affine patch U with defining equation

$$U : y^2 = f(x) = a_n x^n + \ldots + a_1 x + a_0 \tag{4.3.2}$$

with f separable. We will construct the projective completion X of U by adapting the argument in Example 3.5.24. As in Example 3.9.24, define

$$g = \lfloor \frac{n-1}{2} \rfloor. \tag{4.3.3}$$

Moreover, let us define the reciprocal polynomial $\widetilde{f}$ of f by

$$\widetilde{f} = a_0 x^n + \ldots + a_{n-1} x + a_n. \tag{4.3.4}$$

We introduce the new coordinates

$$u = 1/x, \qquad v = y/x^{g+1} \tag{4.3.5}$$

Then (4.3.2) can be rewritten as

$$V : v^2 = \widetilde{f}(u) \tag{4.3.6}$$

if n is even, and as

$$V : v^2 = u\widetilde{f}(u) \tag{4.3.7}$$

if n is odd. Moreover, there are mutually inverse isomorphisms

$$\begin{aligned} X \setminus V(x) &\longleftrightarrow Y \setminus V(u) = Y \setminus \{\infty\} \\ (x,y) &\longmapsto (1/x, y/x^{g+1}) \\ (1/u, v/u^{g+1}) &\longleftarrow (u,v). \end{aligned} \tag{4.3.8}$$

Let us check that V is non-singular. Because of (4.3.8), we need only check this for the points in $V(u)$. If n is odd, then the only such point is $\infty = (0,0)$, where v is a local uniformizer. If n is even, we get two new points ∞_1, ∞_2, which in the coordinates (u,v) on V are given by $(u,v) = (0, \pm\sqrt{a_n})$. These points are singular because $\widetilde{f}$ is separable; indeed, its roots are of the form $1/r$, where r runs through the roots of f.

As in Example 3.9.24, we claim that the affine curve V has the property that its coordinate ring $k[V]$ is the integral closure of $k[u] = k[1/x]$ in $k(U)$. The proof is identical: We again see that $k[V]$ is integrally closed in $k(V) = k(U)$ because V is non-singular, and therefore it is the integral closure of $k[u]$ in $k(U)$ since it contains $k[u]$. Theorem 2.7.60 shows that V is the remaining affine part of the projective completion X that we need.

In terms of the coordinates (u,v) on U, the map $\pi : X \to \mathbb{P}^1$ is given by

$$\begin{aligned} (\pi)|_U : U &\to \mathbb{P}^1 \\ (u,v) &\mapsto u. \end{aligned} \tag{4.3.9}$$

The considerations above therefore show that π ramifies over $u = 0$ if and only if the degree of f is odd. With this, the remark at the end of Example 3.9.24 is now fully explained.

Proposition 4.3.10. *Let X be a hyperelliptic curve of genus g with affine defining equation*

$$U : y^2 = f(x) \tag{4.3.11}$$

where f is separable of degree either $2g+1$ or $2g+2$. Then

$$H^0(X,\Omega_X) = k\frac{dx}{y} \oplus kx\frac{dx}{y} \oplus \ldots \oplus kx^{g-1}\frac{dx}{y}. \tag{4.3.12}$$

Proof. Let $K = (\omega)$ for $\omega = dx/y$. As in Example 3.5.24, we see that $K|_U$ is trivial. Since $\deg(K) = 2g-2$, we see that

$$K = (2g-2)[\infty] \tag{4.3.13}$$

if $n = \deg(f)$ is odd. If n is even, then the fact that ω is mapped to a scalar multiple when applying the map $(x,y) \mapsto (x,-y)$ shows that $v_{\infty_1}(\omega) = v_{\infty_2}(\omega)$, so that in fact

$$K = (g-1)[\infty_1] + (g-1)[\infty_2]. \tag{4.3.14}$$

Similarly, if n is odd we have

$$v_\infty(x) = -2 \tag{4.3.15}$$

whereas if n is even we have

$$v_{\infty_1}(x) = v_{\infty_1} = -1. \tag{4.3.16}$$

Since x is regular on U, we see that indeed the differential $x_i\omega = x^i(dx/y)$ are everywhere regular for $i = 0,\ldots.g-1$. The statement of the proposition follows since the regular functions $1,\ldots,x^{g-1}$ are linearly independent. □

Proposition 4.3.17. *Let K be a canonical divisor on a non-singular projective curve X of genus ≥ 1. Then K is base-point free.*

Proof. This is a direct consequence of the fact that X admits global differentials at all when $g \geq 1$. Indeed, let ω be a global differential on X. Then by definition of the canonical divisor $K = (\omega)$, the section ω generates $\mathscr{L}(K)_P$ as an $\mathscr{O}_{X,P}$-module, since the valuation of ω at P coincides with that of $K = (\omega)$. Alternatively, we let $\ell(K) = g$ by definition, and the Riemann–Roch theorem shows that for all $P \in X$ we have

$$\ell([P]) - \ell(K-[P]) = 1 - g + 1 = -g + 2. \tag{4.3.18}$$

Now we have $\ell([P]) = 1$ by a familiar argument: The constants are in $L([P])$, but any other rational function in this space would give rise to an isomorphism of $g(X)$ with $\mathbb{P}^1$, which is absurd. Therefore

$$1 - \ell(K-[P]) = -g + 2, \tag{4.3.19}$$

which shows that $\ell(K-[P])$ for all $P \in X$. This implies that K is base-point free by Proposition 3.6.23. □

The following result gives an intrinsic characterization of hyperelliptic curves.

Proposition 4.3.20. *Let K be a canonical divisor on a non-singular projective curve X of genus ≥ 2. Then K is very ample if and only if X is not hyperelliptic.*

Proof. By Proposition 3.6.23, we have that K is very ample if and only if

$$\ell(K-[P]-[Q]) = \ell(K) - 2 = g - 2 \tag{4.3.21}$$

for all pairs of points (P,Q) on X. Riemann–Roch shows that

$$\ell([P]+[Q[) - \ell(K-[P]-[Q]) = 1 - g + 2, \tag{4.3.22}$$

so that (4.3.21) is satisfied if and only if

$$\ell([P]+[Q]) = 1 \qquad \text{for all } P,Q \in X. \tag{4.3.23}$$

Suppose that X is hyperelliptic, so that there exists a rational map $\pi : X \to \mathbb{P}^1$ of degree 2. Then if we interpret π as a rational function f on X, we have $(f) = D - E$ with E an effective divisor of degree 2. This means that $E = P + Q$ for some points $P,Q \in X$, but then $\ell([P]+[Q]) = 2$ and (4.3.23) implies that K is not very ample. This also follows directly from the description in 4.3.10, since the morphism

$$\begin{aligned} \varphi_K : X &\to \mathbb{P}^{g-1} \\ (x,y) &\mapsto (1 : x : \ldots : x^{g-1}) \end{aligned} \tag{4.3.24}$$

that K gives rise to is not injective.

Conversely, if $\ell([P]+[Q])$, the we can run the argument above in reverse: As in the proof of Corollary 3.1.38, a non-constant global section $f \in L([P]+[Q])$ gives rise to a map $\varphi = \overline{f}$ of degree 2. ☐

Proposition 4.3.25. *Let X be a non-singular projective hyperelliptic curve, and let D_1, D_2 be two divisors on X of degree 2 such that $\ell(D_1) = \ell(D_2) = 2$. Then D_1 and D_2 are linearly equivalent.*

Proof. Since $\ell(D_1)$ and $\ell(D_2)$ are both non-trivial, we may assume that they are both effective. Moreover, we have $\ell(D_i - [P]) = 1$ for all $P \in X$. Indeed, we can find a non-zero $f \in k(X)$ such that $D_i - [P] + (f) \geq 0$ is effective of degree 1, say of the form $[Q_i]$, but if $\ell(D_i - [P]) = 2$, then also $\ell([Q_i]) = 2$ and we get the usual contradiction via the construction of an isomorphism $X \to \mathbb{P}^1$ from $\mathscr{L}([Q_i])$. Now the fact that $\ell(D_i - [P]) = 1$ means that $D_i - [P] \cong [Q_i]$ for a *unique* point $Q_i \in X$.

Now consider the canonical morphism φ_K from (4.3.24). Then the proof of Proposition 4.3.20 and the discussion in Section 3.3 imply that φ_K has the property that

$$\varphi_K(P) = \varphi_K(Q_1) = \varphi_K(Q_2). \tag{4.3.26}$$

Since φ_K is of degree 2, this can only hold if $Q_1 = Q_2$. But then the effective divisors $[P]+[Q_i]$ that are equivalent to D_i coincide, and hence D_1 and D_2 are linearly equivalent. ☐

Proposition 4.3.27. *Let $\varphi : X_1 \to X_2$ be an isomorphism of hyperelliptic curves. Then there exists an isomorphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ that makes the following diagram commute:*

$$\begin{tikzcd} X_1 \arrow[r, "\varphi"] \arrow[d, "\pi_1"] & X_2 \arrow[d, "\pi_2"] \\ \mathbb{P}^1 \arrow[r, "\psi"] & \mathbb{P}^1 \end{tikzcd} \tag{4.3.28}$$

Proof. In the language of morphisms to projective spaces, Proposition 4.3.25 states that given a hyperelliptic curve X, there exists a unique morphism $p : X \to \mathbb{P}^1$ of degree 2 up to an automorphism of $\mathbb{P}^1$. Indeed, if $p : X \to \mathbb{P}^1$ is a map of degree 2, then $D = p^*([\infty])$ is a divisor of degree 2, and since the divisor $p^*([a])$ for $a \in \mathbb{P}^1$ varying give rise to linearly equivalent divisors, we have $\ell(D) = 2$. Conversely, Theorem 3.3.19 describes how a divisor D of degree 2 with $\ell(D) = 2$ gives rise to a map $p : X \to \mathbb{P}^1$. The uniqueness of the divisor D up to linear equivalence means that the associated line bundle is well-defined up to isomorphism, which in turn means that p is essentially unique. Only the choice of basis of $L(D)$ changes the map p by an automorphism of $\mathbb{P}^1$.

Now the map $\pi_2 \circ \varphi$ is a degree 2 map from X_1 to $\mathbb{P}^1$. We have just shown that this means $\pi_2 \circ \varphi = \psi \circ \pi_1$ for some automorphism ψ of $\mathbb{P}^1$. The statement of the proposition is proved. □

Proposition 4.3.29. *Let X_1, X_2 be non-singular hyperelliptic curves obtained as the projective completions of the affine patches*

$$U_i : y^2 = f_i(x) \tag{4.3.30}$$

with f_1, f_2 separable. Write $g = g(X_1) = g(X_2)$. Then any isomorphism $X_1 \to X_2$ is the projective extension of a map in affine coordinates of the following form:

$$(x, y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^{g+1}} \right). \tag{4.3.31}$$

Here a, b, c, d are such that $ad - bc \neq 0$, and $e \in k^*$ is a non-zero scalar.

Proof (sketch). The fact that x is mapped to a fractional linear transformation in x is a translation of Proposition 4.3.27. The statement on the y-coordinate then follows by performing the substitution in x and seeing what power of $(cx + d)$ is needed to end up with a multiple of the defining equation of X_1 when substituting. Note that $ad - bc \neq 0$ and $e \in k^*$ because otherwise the map (4.3.31) would not be an isomorphism. □

Remark 4.3.32. As for curves of 1, subtleties occur when trying to generalize hyperelliptic curves to arbitrary base fields. In odd genus, this gives rise to so-called generalized hyperelliptic curves, which are covers of non-trivial conics of degree 2. Such curves admit a hyperelliptic equation $U : y^2 = f(x)$ over the algebraic closure, but not over the base field.

4.4 Curves of genus 2 and 3

We conclude these notes by analyzing curves of genus 2 and 3.

Proposition 4.4.1. *Let X be a non-singular projective curve of genus 2. Then X is hyperelliptic, and if $\mathrm{char}(k) \neq 2$, then X admits an affine part U with defining equation*

$$U : y^2 = f(x), \tag{4.4.2}$$

where $f \in k[x]$ is a separable polynomial of degree 5 or 6.

Proof. Consider a canonical divisor K on X. Then $\deg(K) = 2$ by Proposition 3.7.1, and $\ell(K) = 2$ because $g(X) = 2$. We have that K is base-point free by Proposition 4.3.17, so it defines a map

$$\varphi_K : X \to \mathbb{P}^{2-1} = \mathbb{P}^1 \tag{4.4.3}$$

by Theorem 3.3.19. Remark 4.1.6 also shows that the hyperplane section $[\infty]$ on $\mathbb{P}^1$ pulls back to an effective divisor on that is linearly equivalent to K and therefore has degree

$\deg(K) = 2$ by Corollary 3.1.38. Therefore Proposition 3.1.36 shows that $\deg(\varphi_K) = 2$, and since the codomain of φ_K is $\mathbb{P}^1$, we see that X is indeed hyperelliptic. The statement on the degree follows from the discussion in Example 3.9.24. □

Similarly, one shows the following.

Proposition 4.4.4. *Let X be a non-singular projective hyperelliptic curve of genus 3. Then if $char(k) \neq 2$, then the curve X admits an affine part U with defining equation*

$$U : y^2 = f(x), \tag{4.4.5}$$

where $f \in k[x]$ is a separable polynomial of degree 7 or 8.

Now for the remaining case in genus 3, namely that of non-hyperelliptic curves. In genus 3, such curves turn out to exist.

Proposition 4.4.6. *Suppose that X is a non-singular projective non-hyperelliptic curve of genus 3. Then X is isomorphic to a non-singular plane quartic; that is, we have*

$$X \cong V(F) \subset \mathbb{P}^2, \tag{4.4.7}$$

where $F \in k[x,y,z]$ is a homogeneous quartic polynomial.

Proof. Consider a canonical divisor K on X Proposition 4.3.20 shows that K defines an embedding φ_K of X into $\mathbb{P}^2$. Proposition 2.6.9 shows that $\varphi(X) = V(F)$ for some homogeneous polynomial $F \in k[x,y,z]$. Moreover, Remark 4.1.6 shows that the pullbacks along φ of the hyperplane sections of $\varphi(X)$ are effective divisors that are linearly equivalent to K. Since these divisors are of degree $\deg(K) = 2g - 2 = 4$ by Proposition 3.7.1, which implies that the homogeneous degree of F equals 4. □

We have studied the isomorphisms of hyperelliptic curves in the previous section. The isomorphisms of plane quartic curves also admit a simple description:

Proposition 4.4.8. *Let $\varphi : X_1 \to X_2$ be an isomorphism of plane quartic curves. If we use canonical divisors K_1 and K_2 to embed X_1 and X_2 into $\mathbb{P}^2$, then φ is the restriction of an invertible linear transformation of $\mathbb{P}^2$ defined by a non-singular matrix $T \in \mathrm{GL}_3(k)$.*

Proof. As in the proof of Proposition 3.4.22, the isomorphism $\varphi : X_1 \to X_2$ gives rise to a pullback on the level of differentials. More precisely, suppose that $B_2 = (\omega_1, \omega_2, \omega_3)$ is a basis of global differentials on X_2. Then $B_1 = (\varphi^*(\omega_1), \varphi^*(\omega_2), \varphi^*(\omega_3))$ is a basis of global differential on X_1. Since K_1 and K_2 are canonical divisors, the corresponding embeddings i_1 and i_2 into $\mathbb{P}^2$ are obtained by choosing a basis of the corresponding global sections, that is, of the global differential forms on X_1 and X_2. Let us choose i_1 and i_2 to correspond to the bases B_1 and B_2. Now let $P \in X_1$. Then

$$i_2(\varphi(P)) = (\omega_1(\varphi(P)) : \omega_2(\varphi(P)) : \omega_3(\varphi(P))) = (\varphi^*(\omega_1)(P) : \varphi^*(\omega_2)(P) : \varphi^*(\omega_3)(P)) = i_1(P). \tag{4.4.9}$$

We see that with the choices of embeddings i_1 and i_2, the isomorphism φ even corresponds to the identity map on $\mathbb{P}^2$. The statement of the Proposition follows. (Note that the invertible T intervenes because of the different possible choices of bases of global differentials used to define i_1 and i_2.) □

It turns out that a converse to Proposition 4.4.6 holds: Any non-singular curve of the form (4.4.7) with F a homogeneous quartic polynomial is of genus 3. More generally, we have the following result:

Theorem 4.4.10. *Suppose that $X = V(F)$ is a non-singular plane curve with F homogeneous of degree d. Then we have*

$$g(X) = \frac{(d-1)(d-2)}{2} \in \{0,1,3,6,\ldots\}. \tag{4.4.11}$$

The (sketch of a) proof of this theorem uses the aforementioned adjunction formula

$$\omega_{X|Z} \cong \omega_{X|Y} \otimes_{\mathscr{O}_X} f^*(\omega_{Y|Z}). \tag{4.4.12}$$

For a smooth embedding $i : X \to S$ of a curve into a surface S followed by a projection to a point, this formula turns out to reduce to

$$\omega_X = i^*(\mathscr{L}(X) \otimes_{\mathscr{O}_S} \omega_S) \tag{4.4.13}$$

We have $S = \mathbb{P}^2$, so we have to determine the canonical divisor $\omega_{\mathbb{P}^1}$. Recall that this is the second exterior power of the sheaf of differentials $\Omega_{\mathbb{P}^1}$. So let us determine the divisor of poles of the differential ω that on $D(x_0) \subset \mathbb{P}^2$ is given by

$$\omega = dx_1 \wedge dx_2 \tag{4.4.14}$$

and has neither poles nor zeros. We now consider this differential on the hyperplane $V(x_0) \subset \mathbb{P}^2$. Setting $x_2 = 1$ instead, the form ω transforms to

$$\omega = d(x_1/x_0) \wedge d(1/x_0) = x_0^{-4}((x_0 dx_1 - x_1 dx_0) \wedge dx_0) = -x_0^{-3} dx_0 \wedge dx_1. \tag{4.4.15}$$

As in Proposition 3.1.14, the isomorphism classes of invertible sheaves on $\mathbb{P}^2$ are described by the Serre twists $\mathscr{O}(n)$. In other words, if we let $H = V(x_0) \subset \mathbb{P}^2$, then all divisors D on $\mathbb{P}^2$ are linearly equivalent to $n[H]$ for some uniquely determined value of n. The calculation (4.4.15) shows that

$$(\omega) \sim 3H \quad \text{on } \mathbb{P}^2. \tag{4.4.16}$$

Moreover, since X is defined by a linear homogeneous form of degree d, we have that

$$\mathscr{L}(X) \sim \mathscr{O}(d). \tag{4.4.17}$$

The adjunction formula therefore shows that

$$\omega_X = i^*(\mathscr{O}(d-3)). \tag{4.4.18}$$

But since X is defined by a homogeneous form of degree d, the pullback $i^*(\mathscr{O}(d-3))$, which on the level of divisors corresponding to the intersection of a form in $\mathscr{O}(d-3)$ with X, is of degree $d(d-3)$ by Bézout's theorem (Corollary 3.1.44). We see that

$$\deg(\omega_X) = d(d-3). \tag{4.4.19}$$

On the other hand, Proposition 3.7.1 tells us that $\deg(\omega_X) = g - 2$. This implies Theorem 4.4.10 after a short calculation.

Remark 4.4.20. Theorem 4.4.10 implies that for example a hyperelliptic curve of genus 4 does not admit any non-singular plane model. But neither is this the case for a hyperelliptic curve of genus 3 (as we have seen) or, for that matter, for one of genus 6. In fact the situation is even more remarkable, in that if X is a hyperelliptic curve, then X is not a (global) complete intersection, meaning that it is impossible to define X as the zero locus of $n-1$ homogeneous polynomials in $\mathbb{P}^n$. The proof of this statement is another (more complicated) application of the adjunction formula.

Glossary

English word	German word
adjoint functors	adjungierte Funktoren
category	Kategorie
coincide	übereinstimmen
dense	dicht
forgetful functor	Vergessfunktor
ideal of vanishing	Verschwindungsideal
localization	Lokalisierung
locally ringed space	lokal geringter Raum
manifold	Mannigfaltigkeit
presheaf	Prägarbe
principal open subset	standard offene Teilmenge
restriction map	Einschränkung
sheaf	Garbe
stalk	Halm
subcategory	Teilkategorie
zero locus	Nullstellenmenge
zero object	Nullobjekt

Bibliography

[1] William Fulton. *Algebraic Curves; An Introduction to Algebraic Geometry*. Lecture notes, University of Michigan, 2008.

[2] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[3] Nomen Nescio. *Characterizing discrete valuation rings*. Lecture notes, New Mexico State University, Fall 2001.

[4] Stefan Wewers. *Algebra*. Lecture notes, Ulm University, winter semester 2021-2022.