Abstract and Explicit Constructions of Jacobian Varieties

by

David Urbanik

A thesis
presented to the University Of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2018.

Abstract

Abelian varieties, in particular Jacobian varieties, have long attracted interest in mathematics. Their influence pervades arithmetic geometry and number theory, and understanding their construction was a primary motivator for Weil in his work on developing new foundations for algebraic geometry in the 1930s and 1940s. Today, these exotic mathematical objects find applications in cryptography and computer science, where they can be used to secure confidential communications and factor integers in subexponential time.

Although in many respects well-studied, working in concrete, explicit ways with abelian varieties continues to be difficult. The issue is that, aside from the case of elliptic curves, it is often difficult to find ways of modelling and understanding these objects in ways amenable to computation. Often, the approach taken is to work “indirectly” with abelian varieties, in particular with Jacobians, by working instead with divisors on their associated curves to simplify computations. However, properly understanding the mathematics underlying the direct approach — why, for instance, one can view the degree zero divisor classes on a curve as being points of a variety — requires sophisticated mathematics beyond what is usually understood by algorithms designers and even experts in computational number theory. A direct approach, where explicit polynomial and rational functions are given that define both the abelian variety and its group law, cannot be found in the literature for dimensions greater than two.

In this thesis, we make two principal contributions. In the first, we survey the mathematics necessary to understand the construction of the Jacobian of a smooth algebraic curve as a group variety. In the second, we present original work with gives the first instance of explicit rational functions defining the group law of an abelian variety of dimension greater than two. In particular, we derive explicit formulas for the group addition on the Jacobians of hyperelliptic curves of every genus g, and so give examples of explicit rational formulas for the group law in every positive dimension.

Acknowledgements

I would like to thank my thesis advisors David Jao and Matt Satriano for their support.

Table of Contents

1 Introduction

If one were forced to pick a most influential mathematical object of the past 150 years, a certain candidate would be the elliptic curve. In many ways, elliptic curves lie at the center of mathematics: their points are described by polynomials, and so lie in the domain of number theory; they are groups, and so have abstract algebraic structure; and over the complex numbers they are complex tori, and so lie in the domain of geometry. Due to this rich abundance of structure, elliptic curves are not only fascinating in their own right — having lead to a proof of Fermat's Last Theorem and featuring in one of the Clay Mathematics Institute's Millennium Prize Problems — but also turn up as unexpected solutions to problems in cryptography and computational number theory.

The essential properties which make elliptic curves special — being specified by polynomial equations, possessing an algebraic group structure, and having geometric and topological properties — are not unique to elliptic curves. The general notion is that of an *abelian variety*: a projective algebraic variety with a group law given by algebraic maps. But unlike elliptic curves, general abelian varieties are much harder to describe. While elliptic curves can be characterized by their Weierstrass equations, describing higher-dimensional abelian varieties is typically only undertaken indirectly, where one proves that such objects and their defining equations must exist, but stops far short of writing any such equations down. Indeed, just to be able to properly discuss these varieties over non-algebraically closed fields, Weil was motivated to rewrite the foundations of algebraic geometry itself, work that was later superseded by Grothendieck's language of schemes.

But while developing the theory of these objects is probably best done indirectly, computational applications typically require explicit constructions. And while there has been increasing interest in work in this area, many basic operations lack efficient algorithms or formulas. One difficulty is that much of the work done by mathematicians is written in a language that requires years of serious study to understand properly, and so is inaccessible to algorithm designers. The goal of this thesis is to understand and explain both perspectives: we will show how to construct Jacobian varieties both in the modern formalism and using explicit equations in the hyperelliptic case, and discuss the connections between these two constructions. We also present some original results giving explicit equations for the group law on hyperelliptic Jacobians of any genus g.

1.1 What is a Jacobian Variety?

The Jacobian variety of a curve C takes many forms. Over the complex numbers, it can be viewed as arising from a quotient $\Omega^1(C)^*/H_1(C,\mathbb{Z})$, where $\Omega^1(C)^*$ is the dual space to the space of holomorphic one-forms on C, and $H_1(C,\mathbb{Z})$ embeds into $\Omega^1(C)^*$ by sending $[\gamma]$ to the integration functional $\omega \mapsto \int_{[\gamma]} \omega$. Over general fields, it can be regarded as a variety which parametrizes degree zero line bundles over C. Using the correspondence between divisors and line bundles, this can in turn be regarded as a variety parametrizing degree zero divisors modulo principal divisors.

Prior to the 1940s, varieties could be regarded as having two types: affine and projective. But in 1940 Weil announced a proof of the Riemann Hypothesis for function fields that required a theory of Jacobian varieties that did not exist at the time.[1] In 1941, he was unable to construct the Jacobian variety as a projective variety, and so was led to rewrite the foundations of algebraic geometry to allow him to work with so-called "abstract varieties"

[1] See the footnote on page 31 of [5]

— varieties without an embedding into affine or projective space — and completed his proof. His work was later superseded by Grothendieck, who developed new foundations for algebraic geometry which were broader and easier to work with than Weil's.

There are at least two possible views on what it can mean for a variety to be "abstract". One version, which we will see when we review Mumford's construction of hyperelliptic Jacobians, is that an abstract variety is kind of like an abstract manifold, in that it is described locally by charts satisfying certain compatibility conditions. This variant still requires one to consider the object as being given by explicit equations affine-locally, and so does not fully capture what, precisely, is meant when one refers to varieties for which no such equations are known. The second viewpoint, which requires the abstract language of category theory, will be the subject of the next section.

2 Universal Constructions and Representable Functors

The claim that the Jacobian of a curve C "is" a variety should already be regarded as quite curious. We have mentioned three realizations of Jacobians in passing — one involving holomorphic one-forms, one involving line bundles, and a third involving divisors — and none of these descriptions seem to resemble varieties. A related phenomenon is that one often hears that projective algebraic curves (say of degree d) form a variety, or that projective space is the variety of lines through the origin in some affine space. What is usually meant in these cases is that there is a bijection between the collection of objects being considered and the points of some algebraic variety, and in this sense the set under consideration is "realized" as a variety.

Of course, not any bijection will do; any two sets of the same cardinality are in bijection, and over an appropriate field a variety may be constructed of any desired cardinality, yet plainly not every set is a variety. The usual excuse is that some bijections are "natural" and some aren't, and the ones that are can be used to realize a class of objects as points in some space. But when one asks what exactly makes a map "natural" the answers received are often unclear; common explanations include that natural maps somehow "lack choices" or are "maps anyone else would choose".[2] In some ways, the notion is much like U.S. Supreme Court Justice Stewart's famous description of obscenity: it's difficult to describe, but you know it when you see it.

To understand just how category theory can make clear what it means for such a map to be natural, let us consider two descriptions of the ring of integers $\mathbb{Z}$. One way to describe $\mathbb{Z}$ is by explicit construction: we begin with $\mathbb{N}$, then consider equivalence classes of pairs of elements of $\mathbb{N}$ with the same difference, then define an operation $+$ and $\times$, and eventually construct an object which we may call $\mathbb{Z}$. A second description of $\mathbb{Z}$ is as follows: $\mathbb{Z}$ is a ring such that for any ring R, there is a unique morphism $\mathbb{Z} \to R$.

It is easy to see that $\mathbb{Z}$ satisfies the second property, but to what extent does this property determine $\mathbb{Z}$? Suppose we had a second ring $\mathbb{Z}'$ which satisfied the second property. Then we see that there is a unique map $f : \mathbb{Z} \to \mathbb{Z}'$ and a unique map $g : \mathbb{Z}' \to \mathbb{Z}$. The composition $g \circ f : \mathbb{Z} \to \mathbb{Z}$ is a map $\mathbb{Z} \to \mathbb{Z}$, and must be the unique such map also. But the identity map is such a map, so $g \circ f = \mathrm{id}_{\mathbb{Z}}$. Similarly, $f \circ g = \mathrm{id}_{\mathbb{Z}'}$. So we see that the given property determines $\mathbb{Z}$ up to isomorphism.

The isomorphisms f and g we have obtained in this way are in some ways very special. Not only do they give us an isomorphism between $\mathbb{Z}$ and $\mathbb{Z}'$, but they give us a way to translate between maps leading out of $\mathbb{Z}'$ and maps leading out of $\mathbb{Z}$. If we have any map $\mathbb{Z}' \to R$, where R is a ring, precomposing with f gives us a map $\mathbb{Z} \to R$ which satisfies the same uniqueness condition as the original map from $\mathbb{Z}' \to R$. In other words, the map f gives us not just a way to identify $\mathbb{Z}$ and $\mathbb{Z}'$, but a way to translate maps from $\mathbb{Z}'$ satisfying a certain characterizing property to maps from $\mathbb{Z}$ which satisfy the same property. In effect, the map f lets us replace $\mathbb{Z}'$ with $\mathbb{Z}$ in the category of rings, in the sense that we have a way of transforming any statement about $\mathbb{Z}'$ and its outward-pointing morphisms into an equivalent statement about $\mathbb{Z}$ and its outward-pointing morphisms.

The preceding example, although very straightforward, already contains several key ideas. It is first and foremost an example of a universal property — one of the simplest possible, since for a given "copy" of $\mathbb{Z}$ there is only one map $\mathbb{Z} \to R$ to describe for each ring R. The general idea of a universal property is that one can "define" objects up to a

[2] See for instance this MathOverflow discussion: `https://mathoverflow.net/questions/56938/what-does-the-adjective-natural-actually-mean`

certain flexibility in the underlying model being used; that is, provided we ensure that every statement we wish to make about $\mathbb{Z}$ is some statement about its ring-theoretic properties and its morphisms to other rings, it makes no difference which "version" of $\mathbb{Z}$ is chosen. Although this seems to vastly overcomplicate matters when it comes to working with integers, constructions in modern algebraic geometry can quickly grow very complicated, and it often helps to be able to have a general description of what properties the object of interest must satisfy, and then pick the most convenient model object for the situation of interest. The maps that then "translate" one model to another are called *natural isomorphisms.*

This sort of reasoning gives us the first outline for what it will mean to construct the Jacobian of a curve as a variety. The idea will be to find a universal-property-like description of what maps to the Jacobian ought to look like, and then prove that there does indeed exist an object (a variety) with maps matching the description. The description of those maps will take the form of a *functor*, and the object which satisfies the required properties will be said to *represent* the functor. The theory in this section develops these ideas.

2.1 Key Categorical Definitions

The following definitions are standard, so we present them without comment.

Definition 2.1. A *category* $\mathcal{C}$ consists of a collection of objects $\mathrm{Obj}(\mathcal{C})$ and a collection of morphisms $\mathrm{Mor}(\mathcal{C})$ satisfying the following properties:

(i) Each morphism f belonging to $\mathrm{Mor}(\mathcal{C})$ has a domain and a codomain, which are objects in $\mathrm{Obj}(\mathcal{C})$. We write $f : C \to C'$, where C is the domain of f and C' is the codomain of f.

(ii) If $f : C \to C'$ and $g : C' \to C''$ are morphisms in $\mathrm{Mor}(\mathcal{C})$, then there exists a morphism $g \circ f : C \to C''$, where the operation $- \circ -$ is called *composition.*

(iii) For each object C in $\mathrm{Obj}(\mathcal{C})$, there is an identity morphism $\mathrm{id}_C : C \to C$ which satisfies $f \circ \mathrm{id}_C = f$ and $\mathrm{id}_C \circ f = f$ whenever composition is defined.

Definition 2.2. If $\mathcal{C}$ and $\mathcal{D}$ are categories, then a functor $F : \mathcal{C} \to \mathcal{D}$ is a map defined on the objects and morphisms of $\mathcal{C}$, such that:

(i) For each $C \in \mathrm{Obj}(\mathcal{C})$ there is an object $F(C) \in \mathrm{Obj}(\mathcal{D})$.

(ii) For each $f \in \mathrm{Mor}(\mathcal{C})$ there is an morphism $F(f) \in \mathrm{Mor}(\mathcal{D})$.

(iii) If $\mathrm{id}_C \in \mathrm{Mor}(\mathcal{C})$ is an identity arrow, then $F(\mathrm{id}_C) = \mathrm{id}_{F(C)}$.

(iv) Functors which are *covariant* satisfy the following additional properties. If $f \in \mathrm{Mor}(\mathcal{C})$ takes the form $f : C \to C'$ then $F(f)$ takes the form $F(f) : F(C) \to F(C')$. If $f, g \in \mathrm{Mor}(\mathcal{C})$ then $F(g \circ f) = F(g) \circ F(f)$.

(v) Functors which are *contravariant* satisfy the following additional properties. If $f \in \mathrm{Mor}(\mathcal{C})$ takes the form $f : C \to C'$ then $F(f)$ takes the form $F(f) : F(C') \to F(C)$. If $f, g \in \mathrm{Mor}(\mathcal{C})$ then $F(g \circ f) = F(f) \circ F(g)$.

Every functor is either covariant or contravariant. Often this label will be omitted when the variance of the functor is understood from context. We will often (but not always) state definitions and theorems for functors of one particular variance, with the understanding that every definition, statement or theorem has a dual form for the other variance obtained by simply reversing the relevant arrows.

Notation 2.3. If $\mathcal{C}$ is a category and $C, C' \in \mathrm{Obj}(\mathcal{C})$ then we write $\mathrm{Hom}_{\mathcal{C}}(C, C')$ to denote all morphisms from C to C'.

Definition 2.4. A functor $F : \mathcal{C} \to \mathcal{D}$ is said to be *faithful* if for all $C, C' \in \mathrm{Obj}(\mathcal{C})$ the induced maps $\mathrm{Hom}_{\mathcal{C}}(C, C') \to \mathrm{Hom}_{\mathcal{D}}(F(C), F(C'))$ (or $\mathrm{Hom}_{\mathcal{C}}(C, C') \to \mathrm{Hom}_{\mathcal{D}}(F(C'), F(C))$ in the contravariant case) are injective.

Definition 2.5. A functor $F : \mathcal{C} \to \mathcal{D}$ is said to be *full* if for all $C, C' \in \mathrm{Obj}(\mathcal{C})$ the induced maps $\mathrm{Hom}_{\mathcal{C}}(C, C') \to \mathrm{Hom}_{\mathcal{D}}(F(C), F(C'))$ (or $\mathrm{Hom}_{\mathcal{C}}(C, C') \to \mathrm{Hom}_{\mathcal{D}}(F(C'), F(C))$ in the contravariant case) are surjective.

Definition 2.6. A functor $F : \mathcal{C} \to \mathcal{D}$ is said to be fully faithful if it is both full and faithful.

Definition 2.7. Suppose that $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{C} \to \mathcal{D}$ are functors. Then a natural transformation η between F and G is a collection of morphisms $\eta_C : F(C) \to G(C)$ such that for any morphism $f : C \to C'$ in $\mathrm{Mor}(\mathcal{C})$ the following diagram commutes:

$$\begin{tikzcd}
F(C) \arrow[r, "\eta_C"] \arrow[d, "F(f)"'] & G(C) \arrow[d, "G(f)"] \\
F(C') \arrow[r, "\eta_{C'}"] & G(C')
\end{tikzcd}$$

Note that we say a diagram *commutes* when any pair of compositions obtained by following any path of arrows between two objects are equal. We write $\eta : F \implies G$ to mean that η is a natural transformation from F to G.

Definition 2.8. If F, G and H are three functors from $\mathcal{C}$ to $\mathcal{D}$, $\eta : F \implies G$ and $\tau : G \implies H$ are two natural transformations, then we have a natural transformation $\tau \circ \eta : F \implies H$ defined via $(\tau \circ \eta)_C = \tau_C \circ \eta_C$.

Definition 2.9. We say that a natural transformation $\eta : F \implies G$ is a natural equivalence or an isomorphism of functors, if there exists a natural transformation $\eta^{-1} : G \implies F$ such that $\eta^{-1} \circ \eta$ and $\eta \circ \eta^{-1}$ are both equal to the identity natural transformations $\mathrm{id}_F : F \implies F$ and $\mathrm{id}_G : G \implies G$ respectively, which are the natural transformations where all the component maps are identity maps.

Definition 2.10. We have the following categories of interest:

(i) **Set** is the category whose objects are sets and whose morphisms are maps of sets with the obvious composition rule.

(ii) **Grp** is the category whose objects are groups and whose morphisms are group homomorphisms with the obvious composition rule.

(iii) **AbGrp** is the category whose objects are abelian groups and whose morphisms are group homomorphisms with the obvious composition rule.

(iv) **Ring** is the category whose objects are (commutative) rings and whose morphisms are ring homomorphisms with the obvious composition rule.

(v) Let R be a ring. Then **R-Mod** is a category whose objects are R-modules and whose morphisms are morphisms of R-modules with the obvious composition rule.

(vi) If $\mathcal{C}$ and $\mathcal{D}$ are categories, then $\mathcal{D}^{\mathcal{C}}$ is the category of (covariant) functors from $\mathcal{C}$ to $\mathcal{D}$ with morphisms being natural transformations between functors. Note that if $F : \mathcal{C} \to \mathcal{D}$ is a functor then there is a trivial natural transformation $\eta : F \implies F$ where each $\eta_C = \mathrm{id}_{F(C)}$ that serves as the identity morphism for the functor F in the category $\mathcal{D}^{\mathcal{C}}$.

(vii) Analogously, if $\mathcal{C}$ and $\mathcal{D}$ are two categories, there is a category of contravariant functors from $\mathcal{C}$ to $\mathcal{D}$. We will denote this $\mathcal{D}^{\mathcal{C}^{\mathrm{op}}}$. The notation is explained by the notion of *opposite category*, but we will not need this here.

2.2 Universality and Representability

A particular class of functors which plays a special role in category theory is the "Hom" functors. A Hom-functor on a category $\mathcal{C}$ is a functor $\mathrm{Hom}(C, -) : \mathcal{C} \to \mathbf{Set}$ (or $\mathrm{Hom}(-, C) : \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ in the contravariant case) associated to an object $C \in \mathrm{Obj}(\mathcal{C})$ which acts as follows:

(i) For any object $C' \in \mathrm{Obj}(\mathcal{C})$, we have $C' \mapsto \mathrm{Hom}(C, C')$.

(ii) For any morphism $f : C' \to C''$ we have a map f_* (respectively f^* in the contravariant case) where $f_* : \mathrm{Hom}(C, C') \to \mathrm{Hom}(C, C'')$ via $[g : C \to C'] \mapsto [f \circ g : C \to C'']$.

The importance of Hom-functors is tied to the same philosophy behind universal properties we described earlier: a Hom-functor associated to an object C effectively determines the object C up to a "natural isomorphism" between possible models of C, and the way in which this happens is closely related to the way in which universal properties determine objects up to "translating isomorphisms" as described earlier. To make this relationship precise we will consider some explicit cases of this phenomenon, for which the following definitions will prove useful.

Definition 2.11. Let $\mathcal{C}$ be a category, and X and Y objects in $\mathcal{C}$. A product of X and Y is an object $X \times Y$ whose properties are characterized by the following diagram:

$$\begin{tikzcd}
W \arrow[dr, "\exists!"] \arrow[drr, bend left, "\alpha_Y"] \arrow[ddr, bend right, "\alpha_X"'] & & \\
& X \times Y \arrow[r, "\pi_Y"] \arrow[d, "\pi_X"] & Y \\
& X &
\end{tikzcd}$$

That is, it is an object with two morphisms $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ such that for any other object $W \in \mathrm{Obj}(\mathcal{C})$ and any pair of morphisms $\alpha_X : W \to X$ and $\alpha_Y : W \to Y$ there exists a unique morphism $W \to X \times Y$ such that the above diagram commutes.

Definition 2.12. Let $\mathcal{C}$ be a category, X, Y and Z objects in $\mathcal{C}$, and $\alpha : X \to Z$ and $\beta : Y \to Z$ morphisms in $\mathcal{C}$. A fibre-product of X and Y over Z with respect to the morphisms α and β is an object $X \times_Z Y$ whose properties are characterized by the following diagram:

$$\begin{tikzcd}
W \arrow[dr, "\exists!"] \arrow[drr, bend left, "\gamma_Y"] \arrow[ddr, bend right, "\gamma_X"'] & & \\
& X \times_Z Y \arrow[r, "\pi_Y"] \arrow[d, "\pi_X"] & Y \arrow[d, "\beta"] \\
& X \arrow[r, "\alpha"] & Z
\end{tikzcd}$$

That is, it is an object with two morphisms $\pi_X : X \times_Z Y \to X$ and $\pi_Y : X \times_Z Y \to Y$ so that the bottom right square commutes. In addition, for any other object $W \in \mathrm{Obj}(\mathcal{C})$ and any pair of morphisms $\gamma_X : W \to X$ and $\gamma_Y : W \to Y$ such that the square involving X, Y, Z and W commutes, there exists a unique morphism $W \to X \times_Z Y$ such that the above diagram commutes.

Definition 2.13. Consider the specific case when $\mathcal{C} = \mathbf{Ring}$. Let A, B and C be objects in $\mathcal{C}$, and suppose that $\alpha : C \to A$ and $\beta : C \to B$ are morphisms of $\mathcal{C}$. Then a tensor product (of rings!) $A \otimes_C B$ of A and B over C with respect to the morphisms α and β is an object whose properties are characterized by the following diagram:

$$\begin{tikzcd}
D & & \\
& A \otimes_C B \arrow[ul, "\exists!"'] & B \arrow[l, "j_B"] \arrow[ull, bend right, "\gamma_B"'] \\
& A \arrow[u, "j_A"] \arrow[uul, bend left, "\gamma_A"] & C \arrow[l, "\alpha"] \arrow[u, "\beta"]
\end{tikzcd}$$

That is, it is an object with two morphisms $j_A : A \to A \otimes_C B$ and $j_B : B \to A \otimes_C B$ such that the bottom right square commutes. In addition, for any other object $D \in \mathrm{Obj}(\mathcal{C})$ and any pair of morphisms $\gamma_A : A \to D$ and $\gamma_B : B \to D$ such that the square involving A, B, C and D commutes, there exists a unique morphism $A \otimes_C B \to D$ such that the above diagram commutes.

The definitions 2.11, 2.12 and 2.13 are all examples of *universal properties*. A universal property is a description which characterizes an object in a category by describing either the morphisms out of it or the morphisms into it. Objects described by universal properties tend to have the interpretation of being the "simplest" or "most efficient" constructions satisfying a certain property. Another way to describe this phenomenon is that one describes a universal property in a category $\mathcal{C}$ by giving a functor $F : \mathcal{C} \to \mathbf{Set}$, and saying that an object C satisfies the universal property described by F if there exists an isomorphism of functors between F and one of the functors $\mathrm{Hom}(-, C)$ or $\mathrm{Hom}(C, -)$. This motivates the following definition:

Definition 2.14. We say that a functor $F : \mathcal{C} \to \mathbf{Set}$ is *representable* if there exists an object $C \in \mathrm{Obj}(\mathcal{C})$ and either an isomorphism of functors $\eta : F \implies \mathrm{Hom}(-, C)$ or an isomorphism of functors $\eta : F \implies \mathrm{Hom}(C, -)$. In such a situation, we say that C is a *representing object* for F.

The functor F which is being represented should be interpreted as a functor which sends objects of $\mathcal{C}$ to sets whose elements describe what the morphisms of a representing object "ought to look like", and which sends morphisms of $\mathcal{C}$ to sets whose elements describe what composing those morphisms with other morphisms in the category "ought to do". In some ways one can think of this as giving a kind of "axiomatic" description of an object — specifying how it should behave and what is relations to other objects in the category should be — and the task of deciding whether the functor is representable is the task of deciding whether there exists an object satisfying the axioms. The following lemmas give us some concrete examples of the connection between representability and universal properties.

Lemma 2.15. *Let $\mathcal{C}$ be a category, and X and Y objects in $\mathcal{C}$. Then W is a product of X and Y if and only if it (contravariantly) represents the functor $Hom(-,X) \times Hom(-,Y)$, defined as follows:*

(i) On objects U we have $U \mapsto Hom(U,X) \times Hom(U,Y)$.

(ii) If $f : V \to U$ is a morphism in $\mathcal{C}$, then the functor sends f to

$$f^* : Hom(U,X) \times Hom(U,Y) \to Hom(V,X) \times Hom(V,Y),$$

where f^* acts on a pair $(\alpha_X, \alpha_Y) \in Hom(U,X) \times Hom(U,Y)$ via

$$f^*(\alpha_X, \alpha_Y) = (\alpha_X \circ f, \alpha_Y \circ f).$$

Proof. Suppose first that W is a product of X and Y. Define the maps

$$\eta_U : \mathrm{Hom}(U,X) \times \mathrm{Hom}(U,Y) \to \mathrm{Hom}(U,W),$$

by sending a pair of maps (α_X, α_Y) to the unique map α_W induced by the universal property. Then suppose that $f : V \to U$ is a morphism in $\mathcal{C}$. Then

$$\eta_V(f^*(\alpha_X, \alpha_Y)) = \eta_V(\alpha_X \circ f, \alpha_Y \circ f) = f^*(\eta_U(\alpha_X, \alpha_Y)),$$

or alternatively, the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Hom}(U,X) \times \mathrm{Hom}(U,Y) \arrow[r, "\eta_U"] \arrow[d, "f^*"'] & \mathrm{Hom}(U,W) \arrow[d, "f^*"] \\
\mathrm{Hom}(V,X) \times \mathrm{Hom}(V,Y) \arrow[r, "\eta_V"] & \mathrm{Hom}(V,W).
\end{tikzcd}$$

Since all the maps η_U are invertible for all U, then the natural transformation η is invertible, hence an isomorphism of functors.

Secondly, we suppose that we have an isomorphism of functors

$$\eta : \mathrm{Hom}(-,X) \times \mathrm{Hom}(-,Y) \implies \mathrm{Hom}(-,W)$$

for some object W. Then we also have an inverse natural transformation η^{-1}. Define $(\pi_X, \pi_Y) = \eta_W^{-1}(\mathrm{id}_W)$. Then if U is an object in $\mathcal{C}$ equipped with two maps $(\alpha_X, \alpha_Y) \in \mathrm{Hom}(U,X) \times \mathrm{Hom}(U,Y)$, we may consider the map $f := \eta_U(\alpha_X, \alpha_Y) : U \to W$. Since η^{-1} is a natural transformation, we know that

$$\begin{tikzcd}
\mathrm{Hom}(W,W) \arrow[r, "\eta_W^{-1}"] \arrow[d, "f^*"'] & \mathrm{Hom}(W,X) \times \mathrm{Hom}(W,Y) \arrow[d, "f^*"] \\
\mathrm{Hom}(U,W) \arrow[r, "\eta_U^{-1}"] & \mathrm{Hom}(U,X) \times \mathrm{Hom}(U,Y)
\end{tikzcd}$$

commutes, and so tracing the path of id_W through the diagram we find that $(\alpha_X, \alpha_Y) = (\pi_X \circ f, \pi_Y \circ f)$, which is simply the commutativity of the product diagram. This relation also shows the uniqueness of the map f, since the definition of f means that f is determined by (α_X, α_Y), and the equation shows that f also determines this pair. □

Lemma 2.16. *Let $\mathcal{C}$ be a category, X, Y and Z objects in $\mathcal{C}$, and $\alpha : X \to Z$ and $\beta : Y \to Z$ maps in $\mathcal{C}$. Then W is a fibre product of X and Y over Z with respect to the maps α and β if and only if it (contravariantly) represents the functor*

$$F := Hom(-, X) \times_{Hom(-,Z)} Hom(-, Y),$$

defined via

(i) For any object U, the set $F(U)$ is equal to the collection of all pairs of morphisms $(\gamma_X, \gamma_Y) \in Hom(U, X) \times Hom(U, V)$ such that $\alpha \circ \gamma_X = \beta \circ \gamma_Y$ (i.e., the fibre product diagram commutes).

(ii) The image of F on a morphism $f : V \to U$ is the induced pullback map.

Proof. The proof is analogous to the argument in Lemma 2.15 above. Alternatively, it will follow from Lemma 2.18 below, with the understanding that the functor F is a fibre product object in the functor category $\mathbf{Set}^{\mathcal{C}^{op}}$ obtained by applying the map $\mathcal{C} \to \mathbf{Set}^{\mathcal{C}^{op}}$ described in Lemma 2.18 to the fibre product diagram in $\mathcal{C}$. □

Lemma 2.17. *Let $\mathcal{C} = \mathbf{Ring}$, A, B and C objects in $\mathcal{C}$, and $\alpha : C \to A$ and $\beta : C \to B$ maps in $\mathcal{C}$. Then D is a tensor product of A and B over C with respect to the maps α and β if and only if it represents the functor*

$$F := Hom(A, -) \times_{Hom(C,-)} Hom(B, -),$$

defined via

(i) For any object E, the set $F(E)$ is equal to the collection of all pairs of morphisms $(\gamma_A, \gamma_B) \in Hom(A, E) \times Hom(B, E)$ such that $\gamma_A \circ \alpha = \gamma_B \circ \beta$ (i.e., the tensor product diagram commutes).

(ii) The image of F on a morphism $f : E \to E'$ is the induced pushforward map (post composing with f).

Proof. This holds via an analogous argument as with 2.16, obtained by "reversing all the arrows". □

The preceding Lemmas can all be viewed as instances of the observation that to describe an object in a category $\mathcal{C}$, it suffices to describe (at least one of) its Hom-functors. The following Lemma makes this observation precise by showing that any category $\mathcal{C}$ is equivalent to a category formed from the collection of its Hom-functors and the natural transformations between them.

Lemma 2.18 (The Yoneda Lemma)**.** *Let $\mathcal{C}$ be a category. The map $C \mapsto Hom(-, C)$ is a functor[3], and it defines a full and faithful embedding $\mathcal{C} \to \mathbf{Set}^{\mathcal{C}^{op}}$. The analogous result is true in the contravariant case.*

[3] This really just gives the functor on objects, for its description on morphisms see part (i) of the proof.

Proof. The proof is essentially a series of "trivial" verifications, although what precisely is being said takes time to internalize.

(i) We first need to check that the given map is indeed a functor, which means we have to describe its action on morphisms. Suppose that $f : C \to C'$ is a morphism in $\mathcal{C}$. Then we obtain a collection of maps $(f_*)_A : \mathrm{Hom}(A, C) \to \mathrm{Hom}(A, C')$ for each $A \in \mathcal{C}$ sending $g : A \to C$ to $f \circ g : A \to C'$. We then have that if $A' \in \mathcal{C}$ and $\alpha : A \to A'$ is a morphism of C, then $(f_*)_A \circ \alpha^* = \alpha^* \circ (f_*)_{A'}$, i.e., the following diagram commutes

$$\begin{tikzcd}
\mathrm{Hom}(A', C) \arrow[r, "(f_*)_{A'}"] \arrow[d, "\alpha^*"'] & \mathrm{Hom}(A', C') \arrow[d, "\alpha^*"] \\
\mathrm{Hom}(A, C) \arrow[r, "(f_*)_{A'}"] & \mathrm{Hom}(A, C')
\end{tikzcd}$$

This shows that $f_* : \mathrm{Hom}(-, C) \implies \mathrm{Hom}(-, C')$ defines a natural transformation (note that α^* here is the image of the morphism α under the respective Hom-functors). It is clear that $(\mathrm{id}_C)_*$ gives the identity natural transformation, and that post composing respects composition (i.e., $(f_1 \circ f_2)_* = (f_1)_* \circ (f_2)_*$) so we see that the map $C \mapsto \mathrm{Hom}(-, C)$ is indeed a functor $\mathcal{C} \to \mathbf{Set}^{\mathcal{C}^{op}}$.

(ii) Suppose that $\gamma_1 : C \to C'$ and $\gamma_2 : C \to C'$ are morphisms which are sent to the same natural transformation, i.e., the natural transformations $(\gamma_1)_* : \mathrm{Hom}(-, C) \implies \mathrm{Hom}(-, C')$ and $(\gamma_2)_* : \mathrm{Hom}(-, C) \implies \mathrm{Hom}(-, C')$ are equal. Then in particular, we have that $((\gamma_1)_*)_C(\mathrm{id}_C) = ((\gamma_2)_*)_C(\mathrm{id}_C)$, i.e., that $\gamma_1 = \gamma_2$. So we see that the functor $C \mapsto \mathrm{Hom}(-, C)$ is faithful.

(iii) Suppose that $\eta : \mathrm{Hom}(-, C) \implies \mathrm{Hom}(-, C')$ is a natural transformation. We will show that $\eta = (\eta_C(\mathrm{id}_C))_*$. For any $A \in \mathrm{Obj}(\mathcal{C})$ and $\alpha : A \to C$, we have the commutativity of the diagram

$$\begin{tikzcd}
\mathrm{Hom}(C, C) \arrow[r, "\eta_C"] \arrow[d, "\alpha^*"'] & \mathrm{Hom}(A, C') \arrow[d, "\alpha^*"] \\
\mathrm{Hom}(A, C) \arrow[r, "\eta_A"] & \mathrm{Hom}(A, C')
\end{tikzcd}$$

and so

$$\begin{aligned}
((\eta_C(\mathrm{id}_C))_*)_A(\alpha) &= \eta_C(\mathrm{id}_C) \circ \alpha \\
&= \eta_A(\mathrm{id}_C \circ \alpha) \\
&= \eta_A(\alpha).
\end{aligned}$$

Hence we see that $\eta_A = ((\eta_C(\mathrm{id}_C))_*)_A$, and since A was arbitrary, that $\eta = (\eta_C(\mathrm{id}_C))_*$. This shows that the functor $C \mapsto \mathrm{Hom}(-, C)$ is full.

□

In section 4, we will want to construct the Jacobian as a certain object in the category of schemes. In order to ensure that the object we are constructing has the properties that we want, we will describe how it "ought to behave" by describing a certain functor which describes what its morphisms “ought to look like”. The question of constructing the Jacobian is then the question of constructing an object which can be shown to represent the desired functor. The Yoneda Lemma then tells us that, in many situations of interest, working with the functor we are representing is just as good as working with the object we have constructed, and so in many cases this lets us discard the explicit construction and work simply with the properties of the object determined by the functor.

3 Scheme Theory Background

In this section we introduce some necessary scheme theory background for the construction we will perform in Section 4. Since the background is somewhat extensive, most of the key definitions and theorems will be presented with minimal exposition. Readers interested in additional exposition of the basic material presented here can refer to the author's introductory article on schemes and sheaves[13].

3.1 Schemes and Sheaves

Definition 3.1. Let X be a topological space. The *category associated to* X is a category whose objects are the open sets $U \subseteq X$ and whose morphisms are inclusion maps $U \hookrightarrow U'$. We often use X and this category interchangeably when the context is clear.

Definition 3.2. Let X be a topological space. A *presheaf* on X with values in a category $\mathcal{C}$ is a contravariant functor $\mathcal{F} : X \to \mathcal{C}$. If $\iota : U \hookrightarrow U'$ is an inclusion of open sets in X, then we often refer to $\mathcal{F}(f)$ as a restriction map and label it $\mathrm{res}_U^{U'}$. We also require that $\mathcal{C}$ be a concrete category[4], so the objects in it can be thought of as having elements.

Notation 3.3. Let X be a topological space, and $\mathcal{F} : X \to \mathcal{C}$ a presheaf. If $U \subseteq X$ is open, we refer to the elements of $\mathcal{F}(U)$ as *sections over* U. We will sometimes use the notation $\Gamma(U, \mathcal{F}) := \mathcal{F}(U)$, which has the advantage that one can also consider varying the second argument.

Definition 3.4. Let $\mathcal{F}, \mathcal{G} : X \to \mathcal{C}$ be presheaves on X. A morphism of presheaves $\eta : \mathcal{F} \to \mathcal{G}$ is a collection of maps η_U such that for each inclusion map $\iota : U \hookrightarrow U'$, the following diagram commutes:

$$\begin{tikzcd}
F(U') \arrow[r, "\eta_{U'}"] \arrow[d, "\mathrm{res}_U^{U'}"'] & G(U') \arrow[d, "\mathrm{res}_U^{U'}"] \\
F(U) \arrow[r, "\eta_U"] & G(U)
\end{tikzcd}$$

This can also be viewed as a natural transformation between the functors $\mathcal{F}$ and $\mathcal{G}$.

Definition 3.5. Let X be a topological space. A *sheaf* on X with values in $\mathcal{C}$ is a presheaf $\mathcal{F} : X \to \mathcal{C}$ which satisfies the following two additional axioms:

(i) Suppose $s, s' \in \mathcal{F}(U)$ where $U \subset X$ is open and $\{U_\alpha\}_{\alpha \in I}$ is an open cover of U. Then if $\mathrm{res}_{U_\alpha}^U(s) = \mathrm{res}_{U_\alpha}^U(s')$ for all $\alpha \in I$ then $s = s'$.

(ii) Suppose that $\{s_\alpha\}_{\alpha \in I}$ is a collection of sections, where $s_\alpha \in \mathcal{F}(U_\alpha)$ and $\{U_\alpha\}_{\alpha \in I}$ is an open cover of an open set $U \subseteq X$. Then if $\mathrm{res}_{U_\alpha \cap U_{\alpha'}}^{U_\alpha}(s_\alpha) = \mathrm{res}_{U_\alpha \cap U_{\alpha'}}^{U_{\alpha'}}(s_{\alpha'})$ for all choices of indices α and α' such that $U_\alpha \cap U_{\alpha'} \neq \varnothing$, then there exists a section $s \in \mathcal{F}(U)$ such that $\mathrm{res}_{U_\alpha}^U(s) = s_\alpha$ for all $\alpha \in I$.

The first axiom is called the identity axiom, and the second the gluability axiom.

[4] Intuitively, this just means that the objects are sets and the morphisms are maps of sets satisfying some additional structural properties, e.g. the category of Rings, the category of Groups, etc.

Definition 3.6. Let $\mathcal{F}, \mathcal{G} : X \to \mathcal{C}$ be sheaves. A morphism of sheaves is simply a morphism between the underlying presheaves. In particular, this means that the category of sheaves on X is a full subcategory of the category of presheaves on X.

Definition 3.7. Let $\mathcal{F} : X \to \mathcal{C}$ where $\mathcal{C}$ is one of **AbGrp**, **Ring**, or **R-Mod** (in essence, we just need to be able to add things). Let $p \in X$ be a point of X. The *stalk above* p of $\mathcal{F}$ is an object $\mathcal{F}_p$ in $\mathcal{C}$ constructed as follows:

(i) As a set it is

$$\mathcal{F}_p := \{(s, U) : \ s \in \mathcal{F}(U), \ U \subseteq X \text{ open containing } p\} / \sim$$

where $(s, U) \sim (s', U')$ holds if and only if $\mathrm{res}^U_{U \cap U'}(s) = \mathrm{res}^{U'}_{U' \cap U}(s')$.

(ii) As an object in $\mathcal{C}$ it has the natural operations, where sections are added, scalar multiplied or multiplied by applying restriction maps to the domains if necessary.

Lemma 3.8. *Let $\mathcal{F} : X \to \mathcal{C}$ be a (pre)sheaf in one of* **AbGrp**, **Ring**, *or* **R-Mod**. *Then if $p \in X$, the stalk $\mathcal{F}_p$ can be characterized by the following universal property:*

(i) For all open sets U containing p, there exist maps $res^U_p : \mathcal{F}(U) \to \mathcal{F}_p$ such that if U and U' are two open sets containing p with $U' \subseteq U$, we have that $res^U_p = res^{U'}_p \circ res^U_{U'}$.

(ii) If S is any other object satisfying (i) with respect to the maps $\gamma^U_p : \mathcal{F}(U) \to S$, then there exists a unique map $\gamma : \mathcal{F}_p \to S$ such that $\gamma^U_p = \gamma \circ res^U_p$ for all open $U \subseteq X$.

Proof. We first show that the object $\mathcal{F}_p$ described in Definition 3.7 satisfies this property. We define the maps res^U_p via $s \mapsto (s, U)$. It is clear that when $U' \subseteq U$, both open sets containing p, we have $\mathrm{res}^U_p = \mathrm{res}^{U'}_p \circ \mathrm{res}^U_{U'}$ since this amounts to saying that $(s, U) \sim (\mathrm{res}^U_{U'}(s), U')$ for all $s \in \mathcal{F}(U)$.

Now suppose that we have an object S and maps $\gamma^U_p : \mathcal{F}(U) \to S$ as described. We define the map $\gamma : \mathcal{F}_p \to S$ by taking $(s, U) \mapsto \gamma^U_p(s)$. There are several things to check:

(1) This is well-defined. Indeed, if $(s, U) \sim (s', U')$, then $(s, U) \mapsto \gamma^U_p(s)$ and $(s', U') \mapsto \gamma^{U'}_p(s')$. But we know that $\mathrm{res}^U_{U \cap U'}(s) = \mathrm{res}^{U'}_{U \cap U'}(s')$, and so in particular that

$$\gamma^U_p(s) = \gamma^{U \cap U'}_p(\mathrm{res}^U_{U \cap U'}(s)) = \gamma^{U \cap U'}_p(\mathrm{res}^{U'}_{U \cap U'}(s')) = \gamma^{U'}_p(s').$$

(2) The map γ satisfies the desired condition; more precisely, we have that $\gamma^U_p = \gamma \circ \mathrm{res}^U_p$. This is because if $s \in \mathcal{F}(U)$, then $\gamma(\mathrm{res}^U_p(s)) = \gamma^U_p(s)$ by definition.

(3) The map γ is the unique such map. Indeed, for property (ii) to hold we must have that $\gamma^U_p = \gamma \circ \mathrm{res}^U_p$ and so we must have $(s, U) \mapsto \gamma^U_p(s)$.

(4) One may check that this map is a group homomorphism, a ring homomorphism or an R-module homomorphism as appropriate; this is simply a consequence of the fact that the maps γ^U_p have the appropriate properties.

The fact that this property determines the stalk up to isomorphism is simply the usual universal property argument. □

Definition 3.9. Let $\mathcal{F} : X \to \mathcal{C}$ be a (pre)sheaf. The *étalé space* of $\mathcal{F}$ is a topological space associated to $\mathcal{F}$. As a set it is defined as:

$$\mathrm{Et}(\mathcal{F}) := \bigcup_{p \in X} \mathcal{F}_p.$$

There is a natural projection map $\pi : \mathrm{Et}(\mathcal{F}) \to X$ given by $(s, U)_p \mapsto p$, where $(s, U)_p \in \mathcal{F}_p$. The topology on $\mathrm{Et}(\mathcal{F})$ is generated by sets $[s, U] := \{(s, U)_p\}_{p \in U}$; that is, it is the coarsest topology such that the maps $U \to \mathrm{Et}(\mathcal{F})$ given by $p \mapsto (s, U)_p$ are homeomorphisms onto their image for any fixed $s \in \mathcal{F}(U)$.

Suppose we have some base $\{U_\alpha\}_{\alpha \in I}$ for the topology on X, a collection of objects $\{\mathcal{F}(U_\alpha)\}_{\alpha \in I}$ in $\mathcal{C}$, and restriction maps $\mathrm{res}_{U_\alpha}^{U_{\alpha'}} : \mathcal{F}(U_{\alpha'}) \to \mathcal{F}(U_\alpha)$ whenever $U_\alpha \subset U_{\alpha'}$ that satisfy the usual axioms. Note that this information alone allows us to construct an étalé space $\mathrm{Et}(\mathcal{F})$, since the stalks are determined on a base, and since the topology on $\mathrm{Et}(\mathcal{F})$ is likewise determined on a base. Hence we may define a "completion" of $\mathcal{F}$ via

$$\overline{\mathcal{F}}(U) := \{\text{continuous maps } U \to \mathrm{Et}(F)\}.$$

If U_α is a basis set, we first observe that $\mathcal{F}(U_\alpha) \simeq \overline{\mathcal{F}}(U_\alpha)$. Indeed, there is a map $\varphi : \mathcal{F}(U_\alpha) \to \overline{\mathcal{F}}(U_\alpha)$ which sends s to the map $p \mapsto (s, U)_p$, which is clearly injective. To see that it is surjective, suppose have some $f \in \overline{\mathcal{F}}(U_\alpha)$. Then since f is continuous, there exists some basis open set $[s, V]$ such that $f^{-1}([s, V])$ is a non-empty open set. But this then means that f looks locally like a map $p \mapsto (s, V)_p$. All the sections s obtained in this way must agree on overlaps, and so must lift to some section of U_α; this shows surjectivity.

We have shown that one can construct a sheaf provided we know the values of the sheaf on a base and have restriction maps satisfying the sheaf axioms on that base. With more work, one can show that there is a unique (up to isomorphism) sheaf obtained in this way. We also have the following lemma:

Lemma 3.10. *Suppose that $\mathcal{F}, \mathcal{G} : X \to \mathcal{C}$ are sheaves, and that we have a collection of maps $\eta_{U_\alpha} : \mathcal{F}(U_\alpha) \to \mathcal{G}(U_\alpha)$ which commute with restrictions, where $\{U_\alpha\}_{\alpha \in I}$ is a base for the topology on X. Then there is a unique morphism of sheaves $\eta : \mathcal{F} \to \mathcal{G}$ which extends the maps η_{U_α}.*

Proof. We have just seen that we may identify $\mathcal{F}(U)$ with continuous maps $U \to \mathrm{Et}(\mathcal{F})$ and identify $\mathcal{G}(U)$ with continuous maps $U \to \mathrm{Et}(\mathcal{G})$. To define $\eta_U : \mathcal{F}(U) \to \mathcal{G}(U)$, we therefore need to describe a continuous map $\eta_U(f) : U \to \mathrm{Et}(\mathcal{G})$ determined by a continuous map $f : U \to \mathrm{Et}(\mathcal{F})$. The map f is determined by its restrictions to some open cover $\{U_\alpha\}_{\alpha \in A}$ of U by basis open sets, and so we may define $\eta_U(f)$ to be the unique map determined by the compatible sections $\{\eta_{U_\alpha}(f\big|_{U_\alpha})\}_{\alpha \in A}$.

If $\{V_\beta\}_{\beta \in B}$ is another open cover of U, we wish to show that the compatible sections $\{\eta_{U_\alpha}(f\big|_{U_\alpha})\}_{\alpha \in A}$ and $\{\eta_{V_\beta}(f\big|_{V_\beta})\}_{\beta \in B}$ determine the same map $\eta_U(f)$. Since $\eta_U(f)$ is a function, it suffices to show the two functions produced from the two different open covers agree at any $p \in U$. Since the value of $\eta_U(f)$ at p is equal to the value of any of its restrictions at p, then it suffices to show that if $p \in U_\alpha$ and $p \in V_\beta$, then $\eta_{U_\alpha}(f\big|_{U_\alpha})$ equals $\eta_{V_\beta}(f\big|_{V_\beta})$ at p. But by the compatibility conditions on the maps η_-, we know that the value of both of these maps at p is the value of $\eta_{U_\alpha \cap V_\beta}(f\big|_{U_\alpha \cap V_\beta})$ at p, so this shows that this definition is well-defined.

To see that the definition commutes with restriction maps, we note that in this case the restriction maps are merely restrictions maps of functions, and so the compatibility with restriction maps is easy to check from the fact that the sections $\eta_U(f)$ are defined so as to be determined by their restrictions to any open cover. The uniqueness claim follows from the fact that $\eta_U(f)$ must restrict to $\eta_{U_\alpha}(f|_{U_\alpha})$ whenever $U_\alpha \subseteq U$, and so this is the only possible definition. □

Definition 3.11. Let $\mathcal{F} : X \to \mathcal{C}$ be a (pre)sheaf. Then the *sheafification* of $\mathcal{F}$ is the sheaf $\mathcal{F}^{sh} : X \to \mathcal{C}$ defined via

$$\mathcal{F}^{sh}(U) = \{\text{continuous maps } U \to \mathrm{Et}(\mathcal{F})\},$$

and with the restriction morphisms being ordinary restrictions of functions.

Note that if a map $f : U \to \mathrm{Et}(F)$ is continuous, then $f^{-1}([s,V])$ is open for all open V with $s \in \mathcal{F}(V)$. Assuming $U' := f^{-1}([s,V])$ is non-empty, this means that on some open set $U' \subseteq U$ we have that $f(U') \subseteq [s,V]$, and so since $[s,V]$ contains at most one element in every stalk, that locally f looks like $p \mapsto (s,U')_p$ for some appropriate s. We have the following universal property characterizing the sheafification.

Lemma 3.12. *Let $\mathcal{F}$ be a (pre)sheaf. Then $\mathcal{F}^{sh}$ is a sheaf with a morphism of presheaves $\alpha : \mathcal{F} \to \mathcal{F}^{sh}$ such that for any sheaf $\mathcal{G}$ and any morphism of presheaves $\widetilde{\alpha} : \mathcal{F} \to \mathcal{G}$ there exists a unique morphism of sheaves $\gamma : \mathcal{F}^{sh} \to \mathcal{G}$ such that $\widetilde{\alpha} = \gamma \circ \alpha$.*

Proof. The map $\alpha : \mathcal{F} \to \mathcal{F}^{sh}$ consists of the maps $\alpha_U : \mathcal{F}(U) \to \mathcal{F}^{sh}(U)$ defined by $s \mapsto f_s$ where $f_s(p) = (s,U)_p \in \mathrm{Et}(\mathcal{F})$. It is clear that these maps commute with restrictions, since if $U' \subseteq U$ then

$$f_{\mathrm{res}^U_{U'}(s)}(p) = (\mathrm{res}^U_{U'}(s), U')_p = (s,U)_p = f_s(p) = f_s\big|_{U'}(p).$$

Now suppose that we have some presheaf map $\widetilde{\alpha} : \mathcal{F} \to \mathcal{G}$ where $\mathcal{G}$ is a sheaf. Define $\gamma : \mathcal{F}^{sh} \to \mathcal{G}$ via the maps $\gamma_U : \mathcal{F}^{sh}(U) \to \mathcal{G}(U)$, defined as follows:

(i) Given $f \in \mathcal{F}^{sh}(U)$, we know that f looks locally like the map $p \mapsto (s, V \cap U)_p$ for some $s \in \mathcal{F}(V \cap U)$. Define $\gamma_U(f)$ to be the unique element of $\mathcal{G}(U)$ such that $\gamma_U(f)\big|_{V \cap U} = \widetilde{\alpha}_{V \cap U}(s)$ for all choices of s and V which represent f in this way.

(ii) If near the point p, $f \in \mathcal{F}^{sh}(U)$ takes both the form $p \mapsto (s, V \cap U)_p$ and $p \mapsto (s', V' \cap U)_p$, then s and s' must agree on $V \cap V' \cap U$, and so the conditions that $\gamma_U(f)\big|_{V \cap U} = \widetilde{\alpha}_{V \cap U}(s)$ and $\gamma_U(f)\big|_{V' \cap U} = \alpha'_{V' \cap U}(s')$ are mutually consistent, in the sense that the sections $\widetilde{\alpha}_{V \cap U}(s)$ and $\widetilde{\alpha}_{V' \cap U}(s')$ have compatible restrictions and so the element $\gamma_U(f)$ is well-defined.

(iii) Suppose $U \subseteq U'$, and that $f \in \mathcal{F}(U')$. Then the map $\gamma_{U'}(f)$ is defined by the property that $\gamma_{U'}(f)\big|_{V \cap U'} = \widetilde{\alpha}_{V \cap U'}(s)$ for all choices of s and V which represent f in the sense described in (i). The restriction of $\gamma_{U'}(f)$ to U, therefore, is defined by the property that its restriction to $V \cap U$ equals $\widetilde{\alpha}_{V \cap U}(s)$ for these same choices of s and V since $U \subseteq U'$. But this is simply the definition of $\gamma_U(f)$, so we see that γ commutes with restrictions, and is a well-defined sheaf morphism.

(iv) The uniqueness of γ follows from the fact that property (i) must be satisfied for any such γ, since a section $s \in \mathcal{F}(U)$ is sent to the map $f_s : U \to \mathrm{Et}(\mathcal{F})$ by α, and the condition that $\widetilde{\alpha} = \gamma \circ \alpha$ tells us that we must have $\gamma_U(f_s) = \tilde{\alpha}_U(s)$.

□

We will have two main uses for sheaves in this article. The first will be to construct the structure sheaf of a scheme, and the second will be to construct "invertible sheaves", which are objects that more-or-less take the role of line bundles in algebraic geometry (and are often simply referred to as such). For now, we have done enough work to proceed with the basic definitions and properties of schemes, so we postpone a further discussion of sheaves until it is needed.

Definition 3.13. A *ringed space* is a pair $(X, \mathcal{O}_X)$ consisting of a topological space X and a sheaf of rings $\mathcal{O}_X$.

Definition 3.14. A *locally ringed space* is a ringed space $(X, \mathcal{O}_X)$ such that all the stalks of $\mathcal{O}_X$ are local rings.

Definition 3.15. Suppose that $\varphi : X \to Y$ is a continuous map, and $\mathcal{F}$ is a sheaf on X. Then we may define a sheaf $\varphi_*\mathcal{F}$ on Y, called the *pushforward* of $\mathcal{F}$ along φ, on open sets U via:

$$(\varphi_*\mathcal{F})(U) := \mathcal{F}(\varphi^{-1}(U)).$$

The restriction maps are those of $\mathcal{F}$.

Definition 3.16. A *morphism of locally ringed spaces* $\varphi : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ consists of:

(i) A continuous maps $\varphi : X \to Y$ (written with the same symbol by abuse of notation).

(ii) A morphism of sheaves $\widetilde{\varphi} : \mathcal{O}_Y \to (\varphi_*\mathcal{O}_X)$ (thought of as a "pullback" map).

(iii) The morphism of sheaves in (ii) is *local on stalks*, which means that the induced maps on stalks map the maximal ideal $\mathfrak{m}_q$ of the stalk at $q = f(p)$ into the maximal ideal $\mathfrak{m}_p$ in the stalk at p.

Definition 3.17. Two locally ringed spaces $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are isomorphic if there is a pair of mutually inverse morphisms of locally ringed spaces between them, where the identity morphisms on $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are given by the identity maps on the topological spaces and the identity sheaf morphisms.

Definition 3.18. Let R be a ring. We define the *affine scheme* $X = \operatorname{Spec} R$ to be a locally ringed space $(X, \mathcal{O}_X)$ constructed as follows:

(i) As a set, $X = \operatorname{Spec} R$ is the collection of all prime ideals in R.

(ii) As a topological space, its open sets are generated by the sets, associated to each $f \in R$,

$$D(f) := \{\mathfrak{p} \in \operatorname{Spec} R : f \notin \mathfrak{p}\}.$$

We often refer to this as the set of points where f does not vanish, in light of the fact that these are precisely the ideals such that f is non-zero under the quotient map $R \mapsto R/\mathfrak{p}$.

(iii) The sheaf $\mathcal{O}_X$ is specified on the base $D(f)$ by $\mathcal{O}_X(D(f)) = R_f$, where R_f is the localization of R by f, and the restriction maps are the natural localization maps. Note that if $D(f) \subset D(g)$, then we have that

$$f \in \bigcap_{\substack{\mathfrak{p}\text{ prime} \\ g \in \mathfrak{p}}} \mathfrak{p} = \sqrt{\langle g \rangle},$$

where the equality holds by a theorem from commutative algebra. Hence $1/g$ is of the form r/f^k for $k \in \mathbb{Z}_{\geq 0}$ and $r \in R$, and so the map $R_g \to R_f$ does exist.

Notation 3.19. If R is a ring and $I \subset R$ is an ideal, we denote by $V(I)$ the subset of $\operatorname{Spec} R$ consisting of all prime ideals containing I; i.e., all points at which the functions in I are zero. If $f \in R$, we write $V(f)$ for $V(\langle f \rangle)$. Note that the closed sets on $\operatorname{Spec} R$ are generated by the sets $V(f)$ for $f \in R$, and these sets are the complements of the sets $D(f)$.

Lemma 3.20. *Consider the affine scheme Spec$R$ constructed in Definition 3.18. Then if $\mathfrak{p} \in$ Spec$R$, the local ring at $\mathfrak{p}$ is $R_{\mathfrak{p}}$, which is the localization of R at the prime ideal $\mathfrak{p}$.*

Proof. Using the fact that the stalks of sheaves are determined on a base, we simply observe that $R_{\mathfrak{p}}$ satisfies the universal property described in Lemma 3.8. □

Definition 3.21. An *affine scheme* is a locally ringed space isomorphic to the locally ringed space $\operatorname{Spec} R$ for some ring R.

The association between affine schemes and schemes is actually much stronger than simply the statement that an affine scheme is built out of a ring. For instance, if $\pi : R \to S$ is a ring morphism, then we have natural maps $\pi_f : R_f \to (\pi_* \mathcal{O}_{\operatorname{Spec} S})(D(f))$ defined as the unique maps such that the diagrams

$$\begin{tikzcd}
R \arrow[r, "\pi"] \arrow[d] & S \arrow[d] \\
R_f \arrow[r, "\pi_f"] & (\pi_* \mathcal{O}_{\operatorname{Spec} S})(D(f))
\end{tikzcd}$$

commute (i.e., where $\pi_f(1/f) = 1/\pi(f)$). One can check that this gives a morphism of sheaves $\mathcal{O}_{\operatorname{Spec} R} \to \pi_* \mathcal{O}_{\operatorname{Spec} S}$ and hence a morphism of schemes $\operatorname{Spec} S \to \operatorname{Spec} R$ (as a map of topological spaces it is $\mathfrak{p} \mapsto \pi^{-1}(\mathfrak{p})$). For a full discussion of this we refer to the author's expository article on schemes and sheaves[13]. We have the following result:

Proposition 3.22. *The functors Spec* : **Ring** $\to$ **AffSch** *and* $\Gamma(-, \mathcal{O}_-)$: **AffSch** $\to$ **Ring** *give an equivalence of categories between* **Ring** *and* **AffSch**. □

Definition 3.23. Suppose that $(X, \mathcal{O}_X)$ is a ringed space. Then if $U \subset X$ is open, $(U, \mathcal{O}_X\big|_U)$ is a ringed space where U has the subspace topology and the sheaf is defined in the natural way.

Definition 3.24. A *scheme* is a locally ringed space $(X, \mathcal{O}_X)$ such that every point $\mathfrak{p} \in X$ has an open neighbourhood U such that the locally ringed space $(U, \mathcal{O}_X\big|_U)$ is isomorphic as a locally ringed space to an affine scheme.

When working with schemes, we will often make a temporary identification between an open set $U \subseteq X$ and some affine spectrum $\operatorname{Spec} R$. Thus, the points of X can be thought of as collections of prime ideals which are identified by the various restriction maps in the structure sheaf, where we use the usual correspondence between prime ideals in a ring R and prime ideals in a localization R_f or $R_{\mathfrak{p}}$. The sections of the structure sheaf $\mathcal{O}_X$ are to be thought of as functions on the points of X, and we may evaluate such a function $f \in \mathcal{O}_X(U)$ at $\mathfrak{p} \in U$ by considering the image of f modulo $\mathfrak{p}$ in the stalk $(\mathcal{O}_X)_{\mathfrak{p}}$. We will sometimes use the notation $\kappa(\mathfrak{p})$ for the field $(\mathcal{O}_X)_{\mathfrak{p}}/\mathfrak{p}$.

The equivalence in Proposition 3.22 may be extended as follows. Suppose that $\pi : X \to \operatorname{Spec} R$ is a morphism of schemes. Then the associated morphism of structure sheaves gives us a morphism $\pi^\sharp : R \to \Gamma(X, \mathcal{O}_X)$. If R_f is the coordinate ring of $\operatorname{Spec} R$ on the set $D(f)$, then we have associated morphisms (by abuse of notation) $\pi^\sharp : R_f \to \mathcal{O}_X(\pi^{-1}(D(f)))$ which commute with the restriction maps. Note that the value of $\pi^\sharp(f)$ is determined by the map $R \to \Gamma(X, \mathcal{O}_X)$ and the requirement that the maps commute with restrictions, and so there is only one choice for the map $R_f \to \mathcal{O}_X(\pi^{-1}(D(f))$: the one which satisfies $\pi^\sharp(1/f) = 1/\pi^\sharp(f)$. Hence we see that the sheaf morphism $\mathcal{O}_{\operatorname{Spec} R} \to \pi_*\mathcal{O}_X$ is uniquely determined by the ring morphism $\pi^\sharp : R \to \Gamma(X, \mathcal{O}_X)$, and it is easy to see that given such a morphism we may define a scheme morphism $\pi : X \to \operatorname{Spec} R$ by making the only possible choices for the associated maps.

The preceding argument exhibits a bijection $\operatorname{Hom}_{\mathbf{Ring}}(R, \Gamma(X, \mathcal{O}_X)) \simeq \operatorname{Hom}_{\mathbf{Sch}}(X, \operatorname{Spec} R)$. It is easy to show that this bijection is natural in both X and Y, i.e., that we have natural isomorphisms

$$\begin{aligned} \operatorname{Hom}_{\mathbf{Ring}}(-, \Gamma(X, \mathcal{O}_X)) &\simeq \operatorname{Hom}_{\mathbf{Sch}}(X, \operatorname{Spec} -) \qquad\qquad \text{and} \\ \operatorname{Hom}_{\mathbf{Ring}}(R, \Gamma(-, \mathcal{O}_-)) &\simeq \operatorname{Hom}_{\mathbf{Sch}}(-, \operatorname{Spec} R). \end{aligned}$$

We say that the functors $\Gamma(-, \mathcal{O}_-)$ and Spec form an *adjoint pair.* This correspondence is useful for understanding fibre products, which we now discuss.

Lemma 3.25. *Suppose that $\alpha : \mathit{Spec} A \to \mathit{Spec} C$ and $\beta : \mathit{Spec} B \to \mathit{Spec} C$ are morphisms of schemes. Then the fibre product $\mathit{Spec} A \times_{\mathit{Spec} C} \mathit{Spec} B$ is equal to $\mathit{Spec} A \otimes_C B$, where the morphisms associated to the tensor product are the ring morphisms associated to α and β (see also Definition 2.13).*

Proof. We have

$$\begin{aligned} \operatorname{Hom}_{\mathbf{Sch}}(-, \operatorname{Spec} A \otimes_C B) &\simeq \operatorname{Hom}_{\mathbf{Ring}}(A \otimes_C B, \Gamma(-, \mathcal{O}_-)) \\ &\simeq \operatorname{Hom}_{\mathbf{Ring}}(A, \Gamma(-, \mathcal{O}_-)) \times_{\operatorname{Hom}_{\mathbf{Ring}}(C, \Gamma(-, \mathcal{O}_-))} \operatorname{Hom}_{\mathbf{Ring}}(B, \Gamma(-, \mathcal{O}_-)) \\ &\simeq \operatorname{Hom}_{\mathbf{Sch}}(-, \operatorname{Spec} A) \times_{\operatorname{Hom}_{\mathbf{Sch}}(-, \operatorname{Spec} C)} \operatorname{Hom}_{\mathbf{Sch}}(-, \operatorname{Spec} B). \end{aligned}$$

The identifications are to be interpreted in the sense of natural isomorphism of functors, where the natural isomorphisms exist due to the adjoint property just discussed and Lemma 2.17. The fact that $\operatorname{Spec} A \otimes_C B$ is a fibre product then follows by Lemma 2.16. □

We will use the fact that general fibre products exists in the category of schemes without proof. In general, it is common in specific concrete situations to find a scheme that satisfies the universal property rather than use a general construction, and so there is little sense in proving an existence theorem (and it is too much of a distraction).

Although the language of schemes will be convenient for constructing the Jacobian variety, general schemes can be quite unwieldy, and what we will want in many cases is something that more closely resembles classical affine and projective varieties. For this reason, we introduce several properties of schemes which will be useful. Note that although a scheme is a pair consisting of a topological space and its structure sheaf, we often refer to it as just the topological space with the structure sheaf implicit.

Definition 3.26. We say a scheme X is *Noetherian* if it admits a finite covering by affine open sets $U \cong \operatorname{Spec} R_i$ where each R_i is a Noetherian ring.

Definition 3.27. We say that a scheme X is *irreducible* if it is irreducible as a topological space.

Lemma 3.28. *A scheme X is irreducible if and only if every affine open set is irreducible.*

Proof. If $X = D \cup E$ is a non-trivial decomposition of X as a union of two closed sets, and U is an affine open, then $U = (U \cap D) \cup (E \cap U)$ is a decomposition of U as a union of two relatively closed sets which is non-trivial provided that U is not contained in either D or E. Since the affine opens form a base for the topology on X, we may find an affine open U_1 in $X \setminus D$ and an affine open U_2 in $X \setminus E$. The intersection $U_1 \cap U_2$ contains neither points from D or E and so is empty, hence the union $U_1 \sqcup U_2$ is disjoint. If $U_1 = \operatorname{Spec} R_1$ and $U_2 = \operatorname{Spec} R_2$, then $U_1 \sqcup U_2 = \operatorname{Spec}(R_1 \times R_2)$ and so $U_1 \sqcup U_2$ is affine and not contained in either D or E. Hence if X is reducible then so must be this affine open, which means that if the affine opens are irreducible then so is X.

Alternatively, suppose that X is irreducible, and let $U \subseteq X$ be an affine open. Since U has the subspace topology, if it is reducible then it is of the form $U = (D \cap U) \cup (E \cap U)$ where D and E are closed in X and U is not contained in either D or E. Then $D \cup (E \cup (X \setminus U))$ is a non-trivial decomposition of X, and so if X is irreducible so must be U. □

Definition 3.29. We say that a scheme X is *reduced* if all of the rings $\mathcal{O}_X(U)$ for open $U \subseteq X$ are reduced, i.e., have no non-zero nilpotent elements. Equivalently, X is reduced if all its stalks are reduced.

Definition 3.30. We say that a scheme X is *integral* if all of the rings $\mathcal{O}_X(U)$ are integral domains for all open $U \subseteq X$.

The concepts in definitions 3.30, 3.29 and 3.30 are related by the following Lemma.

Lemma 3.31. *A scheme X is integral if and only if it is both irreducible and reduced.*

Proof. If X is integral then it is reduced, since if $\mathcal{O}_X(U)$ is integral for $U \subseteq X$ open then it is reduced. Moreover, if $\operatorname{Spec} R = U \subseteq X$ is an affine open which is reducible, then it is of the form $U = V(f) \cup V(g)$ for $f, g \in R$. We have $V(f) \cup V(g) = V(fg)$. But then $fg = 0$ as the ideal $\langle fg \rangle$ is contained in every prime ideal, contradicting the integrality of R. Thus if X is integral every affine open is irreducible, hence X is irreducible by Lemma 3.28.

Suppose X is both reduced and irreducible, and let $\mathcal{O}_X(U) = R$ be some coordinate ring of an affine open $U = \operatorname{Spec} R$. Then if $f, g \in R$ are non-zero and $fg = 0$ we see that $U = V(f) \cup V(g)$. If $V(f) = \operatorname{Spec} R$ then $\langle f \rangle$ is contained in every prime ideal, and so is contained in their intersection, the nilradical ideal. But since R is reduced, this ideal is zero, and so $V(f)$ is a non-trivial closed set; the same argument works for $V(g)$. But since X is irreducible such a decomposition can't exist, and therefore there is no product fg of non-zero elements f and g which equals zero, i.e., R is integral. The result follows as integrality can be checked on affine opens, since a non-trivial product $fg = 0$ in some coordinate ring would give another such product in some affine coordinate ring. □

Lemma 3.32. *Suppose that X is integral. Then there is a unique point, called the* generic point *of X, which corresponds to the ideal $\langle 0 \rangle$ in any affine coordinate ring.*

Proof. If U and V are two affine opens in X then $U \cap V$ is non-trivial since X is irreducible. The restriction maps $\operatorname{res}^U_{U \cap V}$ and $\operatorname{res}^V_{U \cap V}$ identify the generic points of U and V, and so they must both correspond to the same point in X. □

Definition 3.33. If X is integral then the *fraction field* of X, written $K(X)$, is defined to be the stalk at the generic point of $\mathcal{O}_X$.

Remark. We could actually define the fraction field to be the fraction field of any affine open, but we prefer this definition since we wish to emphasize that there are natural restriction-compatible inclusions into the fraction field from all the coordinate rings of X.

Definition 3.34. If R is a ring, then the *Krull dimension* of R is the maximum (if it exists) of the lengths of chains $\langle 0\rangle \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_k$ of prime ideals where each inclusion is strict. Note the length of the chain is the number of strict inclusions, or one less than the number of prime ideals in the chain.

Definition 3.35. Let X be a scheme. Then the *dimension* of X is the maximum (if it exists) of the lengths of chains $X = D_0 \supset D_1 \supset D_2 \supset \cdots \supset D_k = \{p\}$ of irreducible closed sets where each inclusion is strict and where D_k is a one-point space. Note that the length of the chain is the number of strict inclusions, or one less than the number of closed sets involved in the chain.

Lemma 3.36. *If R is a ring, the Krull dimension of R is equal to the dimension of $\operatorname{Spec} R$.*

Proof. We claim that the map $\operatorname{Spec} R \to \mathcal{P}(X)$ given by $\mathfrak{p} \mapsto \overline{\{\mathfrak{p}\}}$ gives an inclusion-reversing bijection between points of $\operatorname{Spec} R$ and irreducible closed subsets of $\operatorname{Spec} R$. Note that $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, so it suffices to show that any irreducible closed set is the vanishing set of some prime ideal. To see this, suppose that $V(J)$ is a closed irreducible subset where $J \subset R$ is an ideal. If J is not prime, then there is $ab \in J$ such that neither $a \in J$ nor $b \in J$. Hence $V(J) = V(\langle J, a\rangle) \cup V(\langle J, b\rangle)$ and $V(J)$ is not irreducible. Hence if $V(J)$ is irreducible then J must be prime.

The inclusion-reversing property is straightforward. □

Definition 3.37. We say that a scheme X is *regular* if the Krull-dimension of every stalk is equal to the minimal number of generators for its maximal ideal.

Definition 3.38. We say that a scheme X is *factorial* if all stalks are unique factorization domains.

3.2 Line Bundles

To discuss invertible sheaves (line bundles), we will need the notion of an $\mathcal{O}_X$-module. We begin by motivating this notion.

In algebraic geometry, many objects of interest can be viewed as algebraic analogues of notions one finds in manifold theory. In manifold theory, a bundle over a space X is a space E (called the "total space") equipped with a projection map $\pi : E \to X$ which satisfies certain properties appropriate for the category of interest (continuous, smooth, etc.). The bundle map associates to each point $p \in X$ a fibre $\pi^{-1}(p)$ above p, and the fibres are typically required to satisfy some regularity conditions. For instance, when dealing with *fibre bundles*, there is typically some "standard" fibre F such that around any point $p \in X$, there is an open neighbourhood U of p such that $\pi^{-1}(U) \cong U \times F$. The canonical example is that of a vector bundle such as the tangent bundle of a manifold, where F is chosen to be some standard vector space such as $\mathbb{R}^n$ or $\mathbb{C}^n$, and then the fibre above p is a collection of vectors located "above" p.

The main use of such a construction is that one can define many objects of interest as "sections" of such a bundle. A section of a bundle $\pi : E \to X$ is an appropriate (continuous, smooth, etc.) map $\alpha : X \to E$ such that $\pi \circ \alpha = \mathrm{id}_X$. That is, it assigns to each point $p \in X$ a single object in the fibre $\pi^{-1}(p)$ in an appropriately varying way. Sections can then be used to define vector fields (a collection of vectors, one for each point of X, which varies accordingly with the manifold structure), differentials (an object which associates a dual vector to each point and can be used to define integrals), and higher-order tensors.

One can imagine transporting such a construction to algebraic geometry as follows: define E to be a scheme equipped with a morphism $\pi : E \to X$ of schemes together with an open cover $\{U_i\}_{i \in I}$ of X such that we have isomorphisms $\varphi_i : \pi^{-1}(U_i) \cong U_i \times F$ (for some appropriate F) and the "chart transition maps" $\varphi_j \circ \varphi_i^{-1} : U_i \times F \to U_j \times F$ restrict to isomorphisms between the copies of F at each point $p \in U_i$ where the map is defined (i.e., the transition maps preserve the fibres above each point). This would be a direct translation of the conventional manifold theory, and it works, but the difficulty is that the spaces E and its associated maps are often very difficult to construct.

A simpler idea is to work simply with the sections themselves, and ignore the concrete construction of the bundle object. In the case of vector bundles, in particular, where each fibre F is in fact a vector space, sections can be added and scaled point-wise. This makes the space of sections of the bundle into a module over space of functions on X. The idea in algebraic geometry is to interpret an R-module M in this manner: since every ring R corresponds to the functions on some algebraic space (the scheme $\operatorname{Spec} R$) then we hope to be able to interpret an R-module M as being sections of some bundle over the space $\operatorname{Spec} R$. This motivates the following definitions.

Definition 3.39. Let $(X, \mathcal{O}_X)$ be a ringed space. An *$\mathcal{O}_X$-module* is a sheaf $\mathcal{F}$ of abelian groups such that for every open $U \subseteq X$, the space of sections $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module. We also require that the module action commutes with restriction, i.e., if $U \subseteq U'$, the following diagram commutes:

$$\begin{tikzcd}
\mathcal{O}_X(U') \times \mathcal{F}(U') \arrow[r, "\text{action}"] \arrow[d, "\mathrm{res}_U^{U'} \times \mathrm{res}_U^{U'}"'] & \mathcal{F}(U') \arrow[d, "\mathrm{res}_U^{U'}"] \\
\mathcal{O}_X(U) \times \mathcal{F}(U) \arrow[r, "\text{action}"] & \mathcal{F}(U)
\end{tikzcd}$$

Useful examples include $\mathcal{O}_X$ acting on itself, and the sheaf of functions on a manifold acting on the sheaf associated to a vector bundle.

Definition 3.40. If $\mathcal{F}$ and $\mathcal{G}$ are $\mathcal{O}_X$-modules, then a morphism between $\mathcal{F}$ and $\mathcal{G}$ is a sheaf map $\alpha : \mathcal{F} \to \mathcal{G}$ such that for each open set $U \subseteq X$ the following diagram commutes:

$$\begin{tikzcd}
\mathcal{O}_X(U) \times \mathcal{F}(U) \arrow[r, "\text{action}"] \arrow[d, "\mathrm{id}_{\mathcal{O}_X(U)} \times \alpha_U"'] & \mathcal{F}(U) \arrow[d, "\alpha_U"] \\
\mathcal{O}_X(U) \times \mathcal{G}(U) \arrow[r, "\text{action}"] & \mathcal{G}(U)
\end{tikzcd}$$

Definition 3.41. If $\mathcal{F}$ is a $\mathcal{O}_X$-module and X is integral, then a *rational section* of $\mathcal{F}$ is an element of the stalk at the generic point.

Definition 3.42. Let M be an R-module. We may construct a sheaf on $\operatorname{Spec} R$ associated to M, denoted $\widetilde{M}$, as follows:

(i) On the open set $D(f)$, we define $\widetilde{M}(D(f)) = M_f$, where M_f is a module defined by

$$M_f := \left\{ \frac{m}{f^k} : m \in M, k \in \mathbb{Z}_{\geq 0} \right\},$$

with the obvious addition rule, equivalences, and with R_f action defined by

$$\frac{r}{f^\ell} \cdot \frac{m}{f^k} := \frac{r \cdot m}{f^{\ell+k}}.$$

(ii) If $D(f) \subset D(g)$, then we may map $M_g \to M_f$ in the natural way, noting as we did in the construction of the affine scheme $\operatorname{Spec} R$ that $D(f) \subset D(g)$ implies that $1/g$ is of the form r/f^k for $r \in R$ and $k \in \mathbb{Z}_{\geq 0}$. This gives us the restriction maps.

One may verify both the sheaf axioms and that the construction gives the sheaf $\widetilde{M}$ an $\mathcal{O}_{\operatorname{Spec} R}$-module structure.

Lemma 3.43. *Given a morphism $\varphi : M \to N$ of R modules, we obtain a unique morphism $\widetilde{\phi} : \widetilde{M} \to \widetilde{N}$ of $\mathcal{O}_{Spec\, R}$-modules, and every morphism of $\mathcal{O}_{Spec\, R}$-modules between $\widetilde{M}$ and $\widetilde{N}$ arises in this way. In particular, we have a functor $\widetilde{(-)}$:* **R-Mod** $\to$ **Sh**(*Spec$R$*)*, where the latter is the category of sheaves on Spec$R$.*

Proof. If we have a morphism $\varphi : M \to N$, then this induces a morphism $\varphi_f : M_f \to N_f$ defined by $\frac{m}{f^k} \mapsto \frac{\varphi(m)}{f^k}$ such that the diagram

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[d, "\text{res}"'] & N \arrow[d, "\text{res}"] \\
M_f \arrow[r, "\varphi_f"] & N_f
\end{tikzcd}$$

commutes. The map φ_f is the uniquely determined, since we must have $\frac{m}{1} \mapsto \frac{\varphi(m)}{1}$ by the commutativity of the square, and the behaviour on the denominators is forced on us by the fact that φ_f must be a homomorphism of R_f-modules. This gives us one possible choice for the morphism of $\mathcal{O}_{\operatorname{Spec} R}$ modules $\widetilde{\varphi} : \widetilde{M} \to \widetilde{N}$, namely the one determined by the maps φ_f on the open base $\{D(f)\}_{f \in R}$, and it is easy to see that this does in fact give such a morphism.

To see that every morphism $\widetilde{\phi} : \widetilde{M} \to \widetilde{N}$ arises in this way, we simply observe that any such map of $\mathcal{O}_{\operatorname{Spec} R}$ modules gives a map $M = \widetilde{M}(\operatorname{Spec} R) \to \widetilde{N}(\operatorname{Spec} R) = N$ which must determine the rest of the map $\widetilde{\phi}$ in the manner just described. The claim of functoriality amounts to checking that an identity map of R-modules induces an identity map of sheaves, and that the construction respects composition, and both of these facts are straightforward. □

Much like the affine schemes $\operatorname{Spec} R$ serve as a kind of "standard local model" for schemes, the sheaves $\widetilde{M}$ often serve as a kind of "standard local model" for sheaves associated to schemes. Sheaves for which this holds (in some precise sense) are called quasi-coherent. We won't need this notion, although all sheaves we consider will in fact be of this type. In the case we are most interested in, in fact, the sheaves will "look locally" like $\mathcal{O}_{\operatorname{Spec} R}$ acting on itself by left-multiplication, for some appropriate choice of R. The reason for this is because we are interested in line bundles, and a section of a line bundle "looks locally" like a single function from the base space into the total space, but where these functions can be scaled pointwise by functions on the space. Defining this concept directly however is somewhat unintuitive, so we first define general vector bundles and then consider these "line bundles" as a special case.

Definition 3.44. Let $\mathcal{F}$ and $\mathcal{G}$ be $\mathcal{O}_X$-modules. Then $\mathcal{F} \oplus \mathcal{G}$ is a $\mathcal{O}_X$ module, where on $U \subset X$ we have $(\mathcal{F} \oplus \mathcal{G})(U) := \mathcal{F}(U) \oplus \mathcal{G}(U)$, where the right-hand side is a $\mathcal{O}_X(U)$-module. The restriction maps are the natural ones.

Definition 3.45. A *free sheaf* of rank n is an $\mathcal{O}_X$ module $\mathcal{F}$ such that $\mathcal{F} \cong \mathcal{O}_X^{\oplus n}$ where the exponent denotes an n-fold direct sum.

Definition 3.46. Let X be a scheme. A locally free sheaf on X is a sheaf $\mathcal{F}$ such that around every point $p \in X$ there exists an open neighbourhood U such that the scheme $(U, \mathcal{F}\big|_U)$ is isomorphic to a free sheaf of rank n. Note that n does not vary with the choice of point p or open set U.

The idea behind Definition 3.46 is that it mimics the definition of a vector bundle in that it says that all points of X must have a neighbourhood on which the sheaf is "trivializable". In the ordinary bundle-based definition, where $\pi : E \to X$ is a vector bundle over X, this means we have some open set U on which $\pi^{-1}(U) \cong U \times K^n$ for some appropriate vector space K^n (or alternatively, an n-dimensional affine space). When one uses this isomorphism to describe E, then with respect to this trivialization sections of E must look like maps $p \mapsto (p, f_1(p), \ldots, f_n(p))$, where the f_i's are functions on U. Thus we may regard the sections of a vector bundle as things which are locally n-tuples of functions on U, or in other words, the sheaf $\mathcal{F}$ associated to a vector bundle should be locally free.

Definition 3.47. Let X be a scheme. An *invertible sheaf* is a locally free sheaf of rank 1. We will frequently refer to this as a line bundle.

Definition 3.48. Let $\mathcal{F}$ and $\mathcal{G}$ be two $\mathcal{O}_X$-modules. The *tensor product* of $\mathcal{F}$ and $\mathcal{G}$, denoted $\mathcal{F} \otimes \mathcal{G}$, is the sheaf associated to the sheafification of the presheaf

$$(\mathcal{F} \otimes \mathcal{G})^{\text{pre}}(U) := \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U),$$

with the natural restriction maps.

Lemma 3.49. *Suppose that M and N are R-modules. Then $\widetilde{M} \otimes \widetilde{N}$ is equal to $\widetilde{M \otimes N}$.*

Proof. It suffices to exhibit a map from the presheaf $\mathcal{F} := (\widetilde{M} \otimes \widetilde{N})^{\text{pre}}$ to the sheaf $\widetilde{M \otimes N}$ which satisfies the universal property of sheafification. This means that, for each standard open $D(f) \subset \operatorname{Spec} R$, we need maps $\alpha_{D(f)} : M_f \otimes N_f \to (M \otimes N)_f$ which commute with restrictions. Note that tensor products commute with localizations, so there are natural maps that do this; in particular, the maps defined on pure tensors by $\frac{m}{f^k} \otimes \frac{n}{f^\ell} \to \frac{m \otimes n}{f^{k+\ell}}$ will work. These maps are isomorphisms, hence the map of presheaves thus induced is an isomorphism, and so satisfies the required universal property. In particular, we see that sheafification is not needed in this case. □

The two preceding definitions of "invertible sheaf" and "tensor product of sheaves" are each confusing in their own way. First of all, the term "invertible sheaf" needs explaining. Secondly, the tensor product construction can be unintuitive. These two things are in fact closely related: the tensor product can be used to define an operation on isomorphism classes of sheaves for which the invertible sheaves are precisely the "invertible" elements. To understand these two phenomena, we consider a classic example from algebraic number theory.

Let K be a number field, and $\mathcal{O}_K$ its ring of integers. As $\mathcal{O}_K$ is a Dedekind domain, we may define a *fractional ideal* of $\mathcal{O}_K$ to be an $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K such that there exists another $\mathcal{O}_K$-submodule $\mathfrak{b}$ of K such that the ideal product satisfies $\mathfrak{a} \cdot \mathfrak{b} = \mathcal{O}_K$. In this case, both $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals, and $\mathfrak{b}$ is the inverse of $\mathfrak{a}$ (and vice versa). The collection of all fractional ideals of K with the ideal product operation form an abelian group with identity element $\mathcal{O}_K$. An important subgroup is the group of principal fractional ideals — those fractional ideals generated over $\mathcal{O}_K$ by a single element of K. The quotient by this subgroup is called the class group of K, denoted $\mathrm{Cl}(K)$.

We may in fact interpret the above group in terms of the language of invertible sheaves and tensor products of sheaves we have just defined. For this we need the following lemma.

Lemma 3.50. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be $\mathcal{O}_K$-submodules of K. Then the product $\mathfrak{a} \cdot \mathfrak{b}$ is isomorphic to the tensor product of $\mathcal{O}_K$ modules $\mathfrak{a} \otimes_{\mathcal{O}_K} \mathfrak{b}$.*

Proof. For ease of notation, we will omit the subscript on all tensor products, which we assume to be over $\mathcal{O}_K$. We begin by establishing some properties of the $\mathcal{O}_K$-modules $\mathfrak{a}$. Suppose in particular that $\mathcal{O}_K \subseteq \mathfrak{a}$. Since there exists some $\mathfrak{c} \subseteq \mathcal{O}_K$ such that $\mathfrak{a} \cdot \mathfrak{c} = \mathcal{O}_K$, we may in particular find elements $a_1, \ldots, a_n \in \mathfrak{a}$ and $c_1, \ldots, c_n \in \mathfrak{c}$ such that $\sum_{i=1}^n a_i c_i = 1$. This lets us define two maps, one a map $\iota : \mathfrak{a} \to \mathcal{O}_K^n$ and another a map $\rho : \mathcal{O}_K^n \to \mathfrak{a}$, where $\iota(a) = (ac_1, \ldots, ac_n)$ and ρ is defined on the standard basis vector e_i by $\rho(e_i) = a_i$. Note that $\rho \circ \iota = \mathrm{id}_{\mathfrak{a}}$. With these definitions, we have the following split exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{a} \arrow[r, "\iota"] & \mathcal{O}_K^n \arrow[r] \arrow[l, bend left, "\rho"] & \mathcal{O}_K^n/\iota(\mathfrak{a}) \arrow[r] & 0,
\end{tikzcd}$$

and so we see that $\mathfrak{a}$ is a direct summand of $\mathcal{O}_K^n$. In this case, one says that $\mathfrak{a}$ is *projective* (i.e., it is the direct summand of a free module). An analogous argument (where the exact sequence splits on the other side) shows that $\mathfrak{c}$ is projective.

Now suppose we consider the injective map $\mathfrak{b} \to K$. If we were to tensor both sides of the arrow on the left with $\mathcal{O}_K^n$, we would obtain an injection $\alpha : \mathfrak{b}^{\oplus n} \to K^{\oplus n}$. Writing $\mathcal{O}_K^n \cong \mathfrak{a} \oplus \mathfrak{s}$, we obtain the commuting diagram

$$\begin{tikzcd}
(\mathfrak{a} \oplus \mathfrak{s}) \otimes \mathfrak{b} \arrow[r, "\alpha"] \arrow[d, equal] & (\mathfrak{a} \oplus \mathfrak{s}) \otimes K \arrow[d, equal] \\
(\mathfrak{a} \otimes \mathfrak{b}) \oplus (\mathfrak{s} \otimes \mathfrak{b}) \arrow[r, "\alpha_1 \times \alpha_2"] & (\mathfrak{a} \otimes K) \oplus (\mathfrak{s} \otimes K),
\end{tikzcd}$$

where the maps α_1 and α_2 are the natural ones. Using the fact that $\mathfrak{a} \otimes K \cong K$ via the $m : \mathfrak{a} \otimes K \to K$ given by $a \otimes r \mapsto a \cdot r$, we thus see that the map $m \circ \alpha_1 : \mathfrak{a} \otimes \mathfrak{b} \to K$ is injective (as α is injective), and so gives an isomorphism between $\mathfrak{a} \otimes \mathfrak{b}$ and its image $\mathfrak{a} \cdot \mathfrak{b}$. □

Using this lemma, we may reinterpret the equivalence relation we have imposed on the fractional ideals of K as specifying isomorphism classes of $\mathcal{O}_K$-modules, and hence by

Lemma 3.43, isomorphism classes of invertible sheaves on $\operatorname{Spec}\mathcal{O}_K$. For instance, if $\mathfrak{a}$ and $\mathfrak{a}'$ are isomorphic as $\mathcal{O}_K$-modules, then we see that

$$\mathfrak{a}'\mathfrak{a}^{-1} \cong \mathfrak{a}' \otimes \mathfrak{a}^{-1} \cong \mathfrak{a} \otimes \mathfrak{a}^{-1} \cong \mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathcal{O}_K,$$

and so $\mathfrak{a}'\mathfrak{a}^{-1}$ is principal, and hence $\mathfrak{a}$ and $\mathfrak{a}'$ are related by a principal ideal. Alternatively, if $\mathfrak{a}' = (r\mathcal{O}_K) \cdot \mathfrak{a}$, then the map $a \mapsto r \cdot a$ gives an isomorphism $\mathfrak{a} \xrightarrow{\sim} \mathfrak{a}'$. Thus we see that the group $\mathrm{Cl}(K)$ embeds naturally into the commutative monoid consisting of isomorphism classes of sheaves on $\operatorname{Spec}\mathcal{O}_K$ with the tensor product operation. To characterize the image of this embedding, we prove the following lemmas.

Lemma 3.51. *Let X be a scheme and $\mathcal{F}$ and $\mathcal{G}$ two invertible sheaves. Then $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ is also invertible.*

Proof. Let $p \in X$ be a point, and let U and V be neighbourhoods of p such that $\mathcal{F}\big|_U \cong \mathcal{O}_X\big|_U$ and $\mathcal{G}\big|_V \cong \mathcal{O}_X\big|_V$ we then have that $\mathcal{F}\big|_{U\cap V} \cong \mathcal{G}\big|_{U\cap V} \cong \mathcal{O}_X\big|_{U\cap V}$, and so

$$\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}\big|_{U\cap V} = \mathcal{F}\big|_{U\cap V} \otimes_{\mathcal{O}_X\big|_{U\cap V}} \mathcal{G}\big|_{U\cap V} \cong \mathcal{O}_X\big|_{U\cap V} \otimes_{\mathcal{O}_X\big|_{U\cap V}} \mathcal{O}_X\big|_{U\cap V} \cong \mathcal{O}_X\big|_{U\cap V}.$$

□

Definition 3.52. Let X be a scheme and $\mathcal{F}$ and an $\mathcal{O}_X$-module. We will define an $\mathcal{O}_X$-module $\mathcal{H}om(\mathcal{F}, \mathcal{O}_X)$ in a series of steps. Note that this is *not* the same as the object $\mathrm{Hom}_{\mathcal{C}}(\mathcal{F}, \mathcal{O}_X)$, which is a collection of morphisms in the category $\mathcal{C}$ (written without a subscript when no ambiguity is possible), and we distinguish between the two cases by the calligraphic font in use when referring to the $\mathcal{O}_X$-module.

(i) On the open set $U \subseteq X$, define (as a set)

$$\mathcal{H}om(\mathcal{F}, \mathcal{O}_X)(U) := \left\{\text{morphisms } \mathcal{F}\big|_U \to \mathcal{O}_X\big|_U \text{ of } \mathcal{O}_X\big|_U \text{ modules.}\right\}.$$

(ii) For each open $U \subseteq X$, we turn $\mathcal{H}om(\mathcal{F}, \mathcal{O}_X)(U)$ into an abelian group by the addition law that takes two morphisms of $\mathcal{O}_X$-modules $\alpha, \alpha' : \mathcal{F}\big|_U \to \mathcal{O}_X\big|_U$ and produces the morphism of $\mathcal{O}_X$-modules $\alpha + \alpha'$ defined on open sets $V \subseteq U$ by

$$(\alpha + \alpha')_V(f) := \alpha_V(f) + \alpha'_V(f).$$

It is clear that these maps are morphisms of $\mathcal{O}_X(V)$-modules (as they are defined as the sum of two such maps), and that they commute with restrictions since this is true for both α_V and α'_V. Hence $\alpha + \alpha'$ is a well-defined morphism of $\mathcal{O}_X$-modules. It is clear that this operation is commutative, associative, has additive inverses (since we may negate morphisms), and a zero element (the zero morphism).

(iii) We turn $\mathcal{H}om(\mathcal{F}, \mathcal{O}_X)(U)$ into an $\mathcal{O}_X(U)$-module by adding an $\mathcal{O}_X(U)$-action to the addition law. If $\alpha : \mathcal{F}\big|_U \to \mathcal{O}_X\big|_U$ and $a \in \mathcal{O}_X$, then we may define a map $(a \cdot \alpha) : \mathcal{F}\big|_U \to \mathcal{O}_X\big|_U$ on open sets $V \subseteq U$ via as $(a \cdot \alpha)_V(f) = a\big|_V \cdot \alpha_V(f)$. To see that this is a morphism of sheaves, it suffices to observe that both the $\mathcal{O}_X$-module action and the maps α_V commute with restrictions. Furthermore, each map $(a \cdot \alpha)_V$ is clearly a $\mathcal{O}_X(V)$-module homomorphism since α_V is, and so this gives a morphism of $\mathcal{O}_X$-modules. If α and α' are two morphisms of $\mathcal{O}_X$-modules, then we clearly have $a \cdot (\alpha + \alpha') = a \cdot \alpha + a \cdot \alpha'$ since this is true for each of the "component maps" α_V, α'_V, etc.

(iv) The restriction maps for the sheaf $\mathcal{H}om(\mathcal{F}, \mathcal{O}_X)$ are defined by restriction of morphisms, i.e., by taking a map $\alpha : \mathcal{F}\big|_U \to \mathcal{O}_X\big|_U$ and obtaining the map $\alpha\big|_V : \mathcal{F}\big|_V \to \mathcal{O}_X\big|_V$ where $V \subseteq U$ by keeping only the maps α_W where $W \subseteq V$. These restrictions commute with addition and scalar multiplication of morphisms since those definitions are all done "component-wise", i.e., they are defined in terms of the maps $\alpha_U : \mathcal{F}(U) \to \mathcal{O}_X(U)$.

(v) Supose that $\{U_i\}_{i\in I}$ is an open cover of the open set U, and that we have some $\alpha \in \mathcal{H}om(\mathcal{F}, \mathcal{O}_X)(U)$ such that $\alpha\big|_{U_i} = 0$ for all i. Then given some α_V for any open $V \subseteq U$, we know that α_V is determined by the maps $\alpha_{V\cap U_i}$ as i ranges over all values in I. But we know that $\alpha_{V\cap U_i} = (\alpha\big|_{U_i})_{V\cap U_i} = 0$ for all $i \in I$, hence $\alpha_V = 0$. Since V was an arbitrary open subset of U, we see that $\alpha = 0$. This verifies the identity axiom.

(vi) Suppose that $\{U_i\}_{i\in I}$ is an open cover of the open set U, and we have a collection of sheaf maps $\beta_i \in \mathcal{H}om(\mathcal{F}, \mathcal{O}_X)(U_i)$ with compatible restrictions. We define an element $\alpha \in \mathcal{H}om(\mathcal{F}, \mathcal{O}_X)(U)$ by requiring that for any open $V \subseteq U$, the map α_V restricts on $V \cap U_i$ to $(\beta_i)_{V\cap U_i}$. The fact that the β_i's are compatible ensures this requirement is consistent, and if $f_i = f\big|_{V\cap U_i}$ where $f \in \mathcal{F}(V)$, applying the gluability axiom to the collection of compatible sections $(\beta_i)_{V\cap U_i}(f_i)$ determines a unique section in $\mathcal{O}_X(V)$ which is the image of α_V on f. This verifies the gluability axiom.

Lemma 3.53. *Let $\mathcal{F}$ be an invertible sheaf on a scheme X. Then $\mathcal{H}om(\mathcal{F}, \mathcal{O}_X)$ is an invertible sheaf and $\mathcal{H}om(\mathcal{F}, \mathcal{O}_X) \otimes_{\mathcal{O}_X} \mathcal{F} \cong \mathcal{O}_X$.*

Remark. This does not work for locally free sheaves of rank greater than one; in fact, for reasonable classes of $\mathcal{O}_X$-modules, invertible sheaves can be characterized by this property.

Remark. A useful example to keep in mind is the case of one-dimensional (say smooth) manifolds M. In that case, we have two natural line bundles, namely the tangent and cotangent bundles TM and T^*M respectively. If X is a vector field on $U \subseteq M$ (a section of TM over U) and ω is a one-form on $U \subseteq M$ (a section of T^*M over U) then there is a natural pairing $(X, \omega) \mapsto \omega(X) \in C^\infty(U)$. This is a collection of bilinear maps, and produces a map $\Gamma(-, TM) \otimes \Gamma(-, T^*M) \to C^\infty(-)$. The fact that this map is an isomorphism is due to the fact that "$1 \cdot 1 = 1$", namely, that the vector spaces $T_pM \otimes T_p^*M$ are $1 \cdot 1$ dimensional since both T_pM and T_p^*M are one-dimensional.

Proof. In the spirit of the above remark, we define a map $\eta : \mathcal{H}om(\mathcal{F}, \mathcal{O}_X) \otimes_{\mathcal{O}_X} \mathcal{F} \to \mathcal{O}_X$ and show it is an isomorphism. If $U \subseteq X$ is open, we define $(\eta^{\text{pre}})_U$ on pure tensors $\alpha \otimes s$ in $\mathcal{H}om(\mathcal{F}, \mathcal{O}_X)(U) \otimes_{\mathcal{O}_X(U)} \mathcal{O}_X(U)$ by $\alpha \otimes s \mapsto \alpha_U(s) \in \mathcal{O}_X(U)$. This gives us a presheaf morphism η^{pre} from $\big(\mathcal{H}om(\mathcal{F}, \mathcal{O}_X)(U) \otimes_{\mathcal{O}_X(U)} \mathcal{O}_X(U)\big)^{\text{pre}}$ to $\mathcal{O}_X$, and thus gives us a morphism of sheaves η in accordance with the universal property. We will show this morphism is an isomorphism.

Since $\mathcal{F}$ is invertible, around each point p there is some affine open neighbourhood U such that $\mathcal{F}\big|_U \cong \mathcal{O}_X\big|_U$. Using this isomorphism, we may express the map $\eta\big|_U$ as being determined by the maps, $\mathcal{H}om\ \big(\mathcal{O}_X\big|_U, \mathcal{O}_X\big|_U\big)\,(V) \otimes_{\mathcal{O}_X(V)} \mathcal{O}_X(V) \to \mathcal{O}_X(V)$. Using Lemma 3.43, and the obvious naturality of the addition and multiplication law on $\mathcal{H}om\ \big(\mathcal{O}_X\big|_U, \mathcal{O}_X\big|_U\big)\,(V)$, we may view these as being maps $\operatorname{Hom}_{\mathcal{O}_X(V)}(\mathcal{O}_X(V), \mathcal{O}_X(V)) \otimes_{\mathcal{O}_X(V)} \mathcal{O}_X(V) \to \mathcal{O}_X(V)$ of modules given on pure tensors by $\alpha \otimes s \mapsto \alpha(s)$. Taking $\alpha = \operatorname{id}_{\mathcal{O}_X(V)}$ we see this map is surjective; if $\alpha(s) = 0$, and then since $\alpha(s) = s\alpha(1)$ we find that $\alpha \otimes s = s\alpha \otimes 1 = 0$ since the map $s\alpha$ is identically zero. Note that every element in the tensor product is a pure tensor in this case, so this shows that the map is also injective, and hence an isomorphism. This shows that the maps $\eta\big|_U$ are isomorphisms for all U, and so η is an isomorphism. □

Using Lemma 3.53, we may (finally) define:

Definition 3.54. Let X be a scheme. The group $\operatorname{Pic}(X)$ is the collection of all isomorphism classes of invertible sheaves on X with the operation of tensor product. Lemma 3.53 shows that inverses exist, and the isomorphism class of $\mathcal{O}_X$ is the identity element. If R is a ring, we sometimes write $\operatorname{Pic}(R)$ for $\operatorname{Pic}(\operatorname{Spec} R)$.

Returning to our class group example, we see that we have an embedding of groups $\operatorname{Cl}(K) \hookrightarrow \operatorname{Pic}(\mathcal{O}_K)$. To see that this is an isomorphism, we need to show that any line bundle on $\operatorname{Spec}\mathcal{O}_K$ comes from a fractional ideal of K. If $\mathcal{L}$ is such a line bundle, then $M := \mathcal{L}(\operatorname{Spec}\mathcal{O}_K)$ is an $\mathcal{O}_K$-module which satisfies the property that for each prime $\mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K$ we have $M_{\mathfrak{p}} \cong (\mathcal{O}_K)_{\mathfrak{p}}$. Using an argument similar to the one in Lemma 3.50, which we omit, one can again show that M must be *projective*, and in particular that we may tensor the injective map $\mathcal{O}_X \hookrightarrow K$ on the left with M to get an injective map $M \to M \otimes_{\mathcal{O}_K} K \cong K$ which exhibits M as a fractional ideal in K. Hence we see that $\operatorname{Cl}(K) \cong \operatorname{Pic}(\mathcal{O}_K)$.

This may seem like a tedious and unnecessary way to interpret a concept that is much more straightforward in its original formulation (and it is!), but it has the advantage that the same language can also be used to formulate the theory of line bundles and divisors. In particular, we will see that, with reasonable restrictions on X, the group $\operatorname{Pic}(X)$ is closely related to the group of divisors on X, and a subgroup of $\operatorname{Pic}(X)$ will be our model for the Jacobian variety of X.

3.3 Weil Divisors

In this section, we restrict our level of generality considerably and assume that every scheme X is integral, Noetherian, regular, and finite dimensional. We do this both because it's true for the cases we are interested in (algebraic curves), and because it considerably simplifies the exposition. In particular, it lets us speak of the function field $K(X)$ of X, and lets us use the tools of valuation theory in the codimension-one stalks of X.

Some results we will need here require prerequisite material which would lead us astray, so we will omit some proofs. We begin with the following definition.

Definition 3.55. Define the group $\operatorname{Weil} X$ to be the free abelian group generated by irreducible codimension 1 subschemes of X. Note that a subscheme has codimension 1 if the (non-negative) difference between the dimension of X and its dimension is 1.

Definition 3.56. A *divisor* D is an element of $\operatorname{Weil} X$, that is, a formal $\mathbb{Z}$-linear combination of irreducible codimension one subschemes of X. We write this as

$$D = \sum n_Y[Y],$$

where the sum is over all irreducible codimension one subschemes of X and only finitely many of the coefficients $n_Y \in \mathbb{Z}$ are non-zero.

Definition 3.57. If D and D' are two divisors on X with coefficients n_Y and n'_Y respectively (as Y ranges over all irreducible codimension one subschemes) then we say $D \geq D'$ if $n_Y \geq n'_Y$ for all Y.

Definition 3.58. If D is a divisor on X we say D is *effective* if $D \geq 0$, where we regard 0 as the zero element of the group $\operatorname{Weil} X$.

Definition 3.59. If D is a divisor on X and $U \subseteq X$, then $D\big|_U$ is a divisor on U obtained from D by keeping only those non-zero terms whose points lie in U.

The preceding definitions suggest two natural questions: what's so special about codimension one, and why are we "adding" schemes? The reason is that codimension one schemes tend to naturally have "additive" (or multiplicative, depending on your point of view) structure! To understand why, suppose that R is an integral domain, and consider two elements $f, g \in R$. Then f and g each define closed codimension one subschemes $V(f)$ and $V(g)$ of $\operatorname{Spec} R$ respectively. We then have that $V(fg) = V(f) \cup V(g)$, and so to consider both $V(f)$ and $V(g)$ simultaneously we may multiply f and g. This is not quite true, because $V(f)$ and $V(g)$ may share some common components (i.e., they may have some non-trivial intersection), and so we really should count these with multiplicity. The idea is then to associate to $V(f)$ a divisor which is the sum of its irreducible components, and likewise for $V(g)$, and to represent the "sum" $V(f) + V(g)$ by adding these components keeping track of how many times each component occurs.

Now if f or g are rational functions on X (i.e., defined only on a dense open set), then their behaviour at certain points of X may have a cancellative effect when attempting to add subschemes in this way. For instance, if $f = rs$ and $g = t/r$, where r, s and t are all defined on all of X, then $V(fg) = V(st)$, and so the portion of $V(f)$ corresponding to $V(r)$ was in effect "cancelled" by the denominator of g. This suggests that the divisor associated to g should be the divisor associated to t minus the divisor associated to r. More specifically, we will construct a group homomorphism $\operatorname{div} : K(X)^\times \to \operatorname{Weil} X$ which sends $f \in K(X)^\times$ to a divisor $\operatorname{div}(f) = \sum_Y \operatorname{ord}_Y(f)[Y]$, where $\operatorname{ord}_Y(f)$ is the "order of vanishing" of f at Y. The image of this map gives an important subgroup of $\operatorname{Weil} X$ called the subgroup of *principal divisors*.

Another source of additive (or multiplicative) structure on codimension one subschemes comes from sections of line bundles. If s is a rational section on $\mathcal{L}$, then s need not be a function, and may not have a well-defined value at points $p \in X$. However, we may still determine when s is zero by saying that s vanishes at $p \in X$ if it vanishes at p under any trivialization. That is, if we have a map $\mathcal{L}\big|_U \xrightarrow{\sim} \mathcal{O}_X\big|_U$ which assigns s the function f on U, then we say that s is zero at $p \in U$ if $f = 0$ in $\kappa(p)$. This is well-defined, since if we have another map $\mathcal{L}\big|_V \xrightarrow{\sim} \mathcal{O}_X\big|_V$ corresponding to the open set $V \subset X$ which assigns s to g, then the induced map $\mathcal{O}_X\big|_{U\cap V} \xrightarrow{\sim} \mathcal{O}_X\big|_{U\cap V}$ induces an isomorphism between the stalks at $\mathfrak{p}$ that sends the image of f in $\kappa(\mathfrak{p})$ to the image of g in $\kappa(\mathfrak{p})$, and so f is zero in $\kappa(\mathfrak{p})$ if and only if g is.

If we then have a rational section s of the line bundle $\mathcal{L}$ and a rational section t of the line bundle $\mathcal{L}'$, then we may view the expression st (or more carefully, $s \otimes t$) as a rational section of the line bundle $\mathcal{L} \otimes \mathcal{L}'$. Note that since the stalks of $\mathcal{L} \otimes \mathcal{L}'$ are the tensor products of the corresponding stalks of $\mathcal{L}$ and $\mathcal{L}'$, we see that the $K(X)$-module of rational sections of $\mathcal{L} \otimes \mathcal{L}'$ is the tensor product over $K(X)$ of the $K(X)$-modules of rational sections of $\mathcal{L}$ and $\mathcal{L}'$. We will see that we can extend our group homomorphism div in such way that $\operatorname{div}(st) = \operatorname{div}(s) + \operatorname{div}(t)$, and in doing so we will have a map from the commutative monoid of pairs $(\mathcal{L}, s)$ consisting of line bundles on s and rational sections into the group $\operatorname{Weil} X$. We will then be interested in identifying these pairs up to isomorphism, and understanding the image of div in $\operatorname{Weil} X$ which results. In good situations we will see that this gives an isomorphism of groups, and that one really can view codimension one subschemes of X as corresponding to a certain additive group structure in a natural way.

Notation 3.60. Let $Y \subset X$ is an irreducible codimension one subscheme corresponding to the point $p \in X$. Then $(\mathcal{O}_X)_p$ is a discrete-valuation ring (recall that X is regular). We denote the valuation at p either by val_Y or val_p.

Definition 3.61. If $\mathcal{L}$ is a line bundle on X and s is a rational section, we define

$$\mathrm{div}(s) = \sum_Y \mathrm{val}_Y(s)[Y] \in \mathrm{Weil}(X),$$

where the sum is understood to be over irreducible codimension one closed subschemes of Y (we will adopt the convention that Y is always understood to be a codimension one irreducible closed subscheme).

Lemma 3.62. *The sum in definition 3.61 is well-defined, in the sense that there are only finitely many non-zero terms.*

Proof. Since X is Noetherian, it has a finite open cover by affine open sets corresponding to Noetherian rings, and so it suffices to consider the case where $X = \operatorname{Spec} R$ is affine and R is Noetherian. Note that any open cover of an affine scheme $\operatorname{Spec} R$ admits a finite subcover; this is true in particular for a subcover of the open cover $\{D(f)\}_{f \in R}$ since

$$\bigcup_{i\in I} D(f_i) = \operatorname{Spec} R \iff \bigcap_{i \in I} V(f_i) = \varnothing \iff \sum_{i\in I}\langle f_i \rangle = R,$$

and the right-hand side equality indicates there is a sum $f_{i_1} + \cdots + f_{i_k} = 1$, and thus $\operatorname{Spec} R = D(f_{i_1}) \cup \cdots \cup D(f_{i_k})$. Thus, by considering a finite open subcover of $\{D(f)\}_{f\in R}$ where $\mathcal{L}$ is trivalizable on each open set in the cover, we may reduce further to the case where $\mathcal{L} \cong \mathcal{O}_X$. A rational section may then be viewed as an element of the fraction field $\mathrm{Frac}(R)$. We may therefore write this section as a/b where $a, b \in R$, and as $\mathrm{val}_Y(a/b) = \mathrm{val}_Y(a) - \mathrm{val}_Y(b)$, it suffices to show that $\mathrm{val}_Y(a)$ is only non-zero for finitely many $Y \subset X$ (the same argument works for $\mathrm{val}_Y(b)$ by symmetry).

Let $\mathfrak{p}_Y$ be the prime ideal corresponding to Y. If $\mathrm{val}_Y(a) = 0$, then $a \in \mathfrak{p}_Y$. In particular, $\langle a \rangle \subseteq \mathfrak{p}_Y$. In a Noetherian ring, there are only finitely minimal prime ideals containing any given ideal (a fact that comes from primary decomposition), and so we see that there are only finitely many such ideals $\mathfrak{p}_Y$. □

Definition 3.63. We define the group

$$\mathrm{Sec}(X) = \{(\mathcal{L}, s) : \mathcal{L} \text{ a line bundle on } X,\ s \text{ a rational section}\}/\sim,$$

where the equivalence relation is defined by $(\mathcal{L}, s) \sim (\mathcal{L}', t)$ if there is some isomorphism $\mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ which sends s to t. The group operation is tensor product (of both line bundles and sections). The identity element is $(\mathcal{O}_X, 1)$.

Lemma 3.64. *The map div* : *Sec*$(X) \to$ *Weil*(X) *is a group homomorphism.*

Proof. It suffices to show that $\mathrm{val}_p(st) = \mathrm{val}_p(s) + \mathrm{val}_p(t)$. Note that the first valuation is the valuation corresponding to the stalk $S_p := (\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}')_p = \mathcal{L}_p \otimes_{\mathcal{O}_{X,p}} \mathcal{L}'_p$. Recall that these stalks are (non-canonically) isomorphic to $(\mathcal{O}_{X,p} \otimes_{\mathcal{O}_{X,p}} \mathcal{O}_{X,p})$, and so in particular every element of the stalk is a pure tensor. The unique maximal ideal in S_p can be characterized as the set of all non-invertible elements, hence it contains exactly the elements of the form $x \otimes y$ where either x is in the maximal ideal $\mathfrak{m}_p$ of $\mathcal{L}_p$ or y is in the maximal ideal $\mathfrak{m}'_p$ of $\mathcal{L}'_p$ (or both). If x is a generator for $\mathfrak{m}_p$, then $x \otimes 1$ cannot be written as a product of two non-invertible elements in S_p and hence must be a generator for its maximal ideal; the same is true of $1 \otimes y$ when y is a generator for $\mathfrak{m}'_p$. Factoring $s \otimes t = (s \otimes 1)(1 \otimes t)$ we may thus compute that

$$\mathrm{val}_p(s \otimes t) = \mathrm{val}_p(s \otimes 1) + \mathrm{val}_p(1 \otimes t) = \mathrm{val}_p(s) + \mathrm{val}_p(t).$$

□

We would next like to show that div is injective, which means characterizing its kernel. In particular, we wish to understand what it means for a section s of a line bundle $\mathcal{L}$ to have "no zeros or poles" in codimension one. The main tool is the following lemma from commutative algebra, which effectively shows that a function having no poles in codimension one extends over the entire set.

Lemma 3.65. *If R is a regular integral domain, then*

$$R = \bigcap_{codim\,\mathfrak{p}=1} R_{\mathfrak{p}},$$

where the intersection takes place in the fraction field.

Proof. Omitted. □

Using this lemma, we may prove the following.

Lemma 3.66. *Suppose that s is a rational section of the line bundle $\mathcal{L}$ on X, and that s has no poles (i.e., $val_p(s) \geq 0$ for all codimension one points $p \in X$). Then s is a regular (global) section of $\mathcal{L}$.*

Proof. Let $U = \operatorname{Spec} R$ be an affine open subset of X and $\varphi : \mathcal{L}\big|_U \xrightarrow{\sim} \mathcal{O}_X\big|_U$ a trivialization. Then $\varphi(s)$ satisfies $\mathrm{val}_{\mathfrak{p}}(\varphi(s)) \geq 0$ for each codimension one point $\mathfrak{p} \in \operatorname{Spec} R$, and so belongs to $R_{\mathfrak{p}}$ for all such points. By Lemma 3.65, we see that $\varphi(s) \in R$, and hence is regular on U. Since the affine opens cover X, s is a globally regular section. □

Lemma 3.67. *The map $div : Sec(X) \to Weil(X)$ is injective.*

Proof. Suppose that $\mathcal{L}$ is a line bundle on X and s is a rational section of $\mathcal{L}$ such that $\mathrm{div}(s) = 0$. Then s has no poles, hence is regular. We may thus define a map $\varphi : \mathcal{O}_X \to \mathcal{L}$ given by $f \in \mathcal{O}_X(U) \mapsto f \cdot s\big|_U$. If we can show this is an isomorphism, we will have shown that the pair $(\mathcal{L}, s)$ corresponds to the pair $(\mathcal{O}_X, 1)$ and hence is the identity element in $\mathrm{Sec}(X)$.

To show the morphism φ of sheaves is an isomorphism it suffices to show that it induces isomorphisms over any open set U. Thus it suffices to show that for a trivialization $\psi : \mathcal{L}\big|_U \xrightarrow{\sim} \mathcal{O}_X\big|_U$ the map $\psi \circ \varphi\big|_U : \mathcal{O}_X\big|_U \to \mathcal{O}_X\big|_U$ is an isomorphism. If $f \in \mathcal{O}_X(V)$ for $V \subseteq U$ open, then this map acts as $f \mapsto f \cdot \psi(s\big|_V)$. The element $\psi(s\big|_U)$ has no no zeros and no poles (since $\mathrm{div}(s) = 0$) so in particular it is invertible, and we may define a map $\mathcal{O}_X\big|_U \to \mathcal{O}_X\big|_U$ given on $V \subseteq U$ open by $g \mapsto g \cdot \psi(s\big|_V)^{-1}$, which gives an inverse to $\psi \circ \varphi\big|_U$. □

The above lemma tells us that there is a subgroup of the group $\operatorname{Weil} X$ whose behaviour corresponds to that of multiplying sections on various line bundles of X. The utility of such a statement, however, would be very little if we could not identify any non-trivial line bundles. The next definition gives a family of sheaves which, it turns out, exhausts all line bundles on X.

Definition 3.68. Let $D \in \operatorname{Weil} X$ be a Weil divisor. We define the sheaf $\mathcal{O}_X[D]$ on the open set $U \subseteq X$ by

$$\mathcal{O}_X[D](U) := \{f \in K(X)^\times : \operatorname{div}\big|_U(f) + D\big|_U \geq 0\} \cup \{0\}$$

with the obvious $\mathcal{O}_X(U)$ action and with the restriction maps being the obvious inclusions. Note that $\operatorname{div}\big|_U(f)$ means the function div corresponding to the subscheme U acting on $f\big|_U$ and $D\big|_U$ means the divisor obtained from D by ignoring any points of X which do not lie in U.

Lemma 3.69. *Suppose that $\mathcal{L}$ is an invertible sheaf, and that s is a rational section of $\mathcal{L}$. Then $\mathcal{O}_X[div(s)] \cong \mathcal{L}$.*

Proof. Omitted.

□

Lemma 3.70. *If $\mathcal{L} := \mathcal{O}_X[D]$ is an invertible sheaf, then there exists a canonical rational section s of $\mathcal{L}$ such that $div(s) = D$ corresponding to the element $1 \in K(X)^\times$.*

Proof. To eliminate possible confusion, we use the notation $1_{\mathcal{L}}$ to denote the rational section of $\mathcal{L}$ corresponding to $1 \in K(X)$. Let $p \in X$ be of codimension one. Since $\mathcal{L}$ is invertible, we can find an affine open set U containing p such that $\mathcal{L}\big|_U \cong \mathcal{O}_X\big|_U$. In particular, if p is not in the *support* of D (the set of points whose coefficients in D are non-zero), then this isomorphism arises simply from observing that $\mathcal{L}(U) = \mathcal{O}_X(U)$ for U small enough. Since this isomorphism induces a correspondence between the valuation at p on $\mathcal{L}$ and the valuation at p on $\mathcal{O}_X$, we see that $\operatorname{val}_p(1_{\mathcal{L}}) = 0$ if p is not in the support of D.

If p is in the support of D, then the isomorphism must send $1_{\mathcal{L}}$ to a function f regular over U, with inverse map division by f. Hence for $g \in \mathcal{L}(U)$ with $\operatorname{div}(g) + D\big|_U \geq 0$, we must have $\operatorname{div}(fg) \geq 0$ for all choices of g, and therefore $\operatorname{div}(g) = D\big|_U$. This in particular means that $\operatorname{div}\big|_U(1_{\mathcal{L}}) = D\big|_U$. □

Lemma 3.71. *By the preceding two lemmas, we may represent any element of $Sec(X)$ in the form $(\mathcal{O}_X[div(s)], s)$. In this case, its inverse is given by $(\mathcal{O}_X[-div(s)], 1/s)$.*

Proof. Applying the div homomorphism to the product we get $\operatorname{div}(s(1/s)) = 0$, which completes the proof by the injectivity of div. □

The preceding Lemmas show that any line bundle takes the form described in Definition 3.68, but it need not be the case that every sheaf of the form in Definition 3.68 is a line bundle. We do not dwell on this point here, but instead introduce a condition that will give us a family of objects X for which this correspondence does hold.

Lemma 3.72. *If X is factorial, then $\mathcal{O}_X[D]$ is an invertible sheaf for any divisor D. Consequently, the map $div : Sec(X) \to Weil(X)$ is an isomorphism.*

Proof. To show that $\mathcal{L} := \mathcal{O}_X[D]$ is an invertible sheaf, it suffices to show that there is a covering by affine open sets U such that $\mathcal{L}\big|_U \cong \mathcal{O}_X\big|_U$. Note that if $g \in \mathcal{O}_X(U)$ satisfies $D\big|_U = \operatorname{div}\big|_U(g)$, then the map $\mathcal{O}_X(U) \to \mathcal{L}(U)$ given by $f \mapsto f/g$ induces an isomorphism between $\mathcal{O}_X(U)$ and $\mathcal{L}(U)$ with inverse $s \mapsto sg$. Thus it suffices to show that for each point $p \in X$ there is an affine open neighbourhood U and a rational function g on U such that $D\big|_U = \operatorname{div}\big|_U(g)$. This is clearly true for the case when $D\big|_U = 0$, so we consider the case when $D\big|_U = np$ for $p \in U$. In this case, we note that since $\mathcal{O}_{X,p}$ is a UFD, we may take a generator x for the principal prime ideal corresponding to p. Then $\mathrm{val}_p(x^n) = n$, and so by restricting to a small enough open set U we may take $g = x^n$ as desired.

We have already shown the map div is injective, and this Lemma, in conjunction with Lemma 3.70, shows that the map is surjective. □

The preceding results in some sense "justify" the consideration of the group $\mathrm{Weil}(X)$, in that we see that it corresponds naturally to structures associated with X. A second question of interest is the relationship between $\mathrm{Weil}(X)$ (or $\mathrm{Sec}(X)$) and $\mathrm{Pic}(X)$. Intuitively, $\mathrm{Pic}(X)$ is a group that we get when we "forget" about the rational section s in the pair $(\mathcal{L}, s)$ and only worry about the line bundle. We will see that $\mathrm{Pic}(X)$ in fact corresponds naturally to a quotient subgroup of $\mathrm{Weil}(X)$.

Definition 3.73. A divisor D is called *principal* if it is the image of a rational function $f \in K(X)$ under $(\mathcal{O}_X, f) \mapsto \mathrm{div}(f)$. Note that the set $\{(\mathcal{O}_X, f) : f \in K(X)\}$ forms a subgroup of $\mathrm{Sec}(X)$. We denote the image of this subgroup by $\mathrm{Prin}(X)$.

Definition 3.74. Define the *class group* $\mathrm{Cl}(X)$ to be the group $\mathrm{Weil}(X)/\mathrm{Prin}(X)$.

Lemma 3.75. *We have an commuting diagram of groups*

$$\begin{tikzcd}
Sec(X) \arrow[r, hook, "div"] \arrow[d] & Weil(X) \arrow[d, "/Prin(X)"] \\
Pic(X) \arrow[r, hook] & Cl(X)
\end{tikzcd}$$

where the map $Sec(X) \to Pic(X)$ is the map that "forgets" the section, and the bottom arrow will be described over the course of the lemma. If X is factorial, the two horizontal arrows are isomorphisms.

Proof. We first describe the bottom arrow. Suppose that $\mathcal{L}$ is a representative of an element in $\mathrm{Pic}(X)$. Then we may find a rational section s of $\mathcal{L}$ and send $\mathcal{L} \mapsto \mathrm{div}(s) + \mathrm{Prin}(X)$. If $\mathcal{L}' \cong \mathcal{L}$ and t is a rational section of $\mathcal{L}'$, then $\mathcal{L} \otimes \mathcal{L}'^{\vee} \cong \mathcal{O}_X$ and so $\mathrm{div}(s) - \mathrm{div}(t) \in \mathrm{Prin}(X)$, so this map is well-defined. It is injective since if $(\mathcal{L}, s)$ and $(\mathcal{L}', t)$ are two elements of $\mathrm{Sec}(X)$ such that $\mathrm{div}(s) - \mathrm{div}(t) \in \mathrm{Prin}(X)$, then we must have that $\mathcal{L} \otimes \mathcal{L}'^{\vee} \cong \mathcal{O}_X$.

If X is factorial then the top arrow is an isomorphism. Hence every divisor D is of the form $D = \mathrm{div}(s)$ for some section s of $\mathcal{L}$, hence every equivalence class $D + \mathrm{Prin}(X)$ is of the form $\mathrm{div}(s) + \mathrm{Prin}(X)$ and the image of some $\mathcal{L}$. □

The use of the factoriality assumption in the preceding Lemmas may seem somewhat ad-hoc, but it is justified by the fact that it holds for the important case of algebraic curves which we will need to understand the idea of the Jacobian variety of a curve. We introduce some basic terminology in the next section for this purpose.

3.4 Algebraic Curves

Throughout this section, we assume that $\Bbbk$ is an algebraically closed field.

Definition 3.76. An irreducible topological space X is said to be an *curve* if it is of dimension one.

Definition 3.77. A morphism $\pi : X \to Y$ of schemes is said to be *affine* if inverse images of affine sets are affine.

Definition 3.78. A morphism $\pi : X \to Y$ is said to be a *closed embedding* if it is affine and each induced map $\Gamma(U, \mathcal{O}_Y) \to \Gamma(\pi^{-1}(U), \mathcal{O}_X)$ is surjective.

Definition 3.79. A scheme X is said to be *projective over* $\Bbbk$ if there is a closed embedding $X \hookrightarrow \mathbb{P}^n_{\Bbbk}$ for some n, where $\mathbb{P}^n_{\Bbbk}$ is n-dimensional projective space. Note that we have not constructed $\mathbb{P}^n_{\Bbbk}$ as a scheme here, but a construction can be found in the author's article on schemes and sheaves[13].

Throughout the rest of the thesis, we use the term *algebraic curve* to mean a projective, integral, regular scheme over a field $\Bbbk$ whose topological space is a curve. Over the complex numbers, we will also view this curve as a complex manifold, which technically requires that one exhibit a correspondence between curves in the sense we have defined them and their so-called "analytification" (which has, for instance, a Hausdorff topology and a complex manifold structure), but we will ignore this detail. We also introduce some additional ideas regarding line bundles on algebraic curves.

Definition 3.80. If C is an algebraic curve and $D \in Weil(C)$ is a divisor, where $D = \sum_p n_p p$, the *degree* of D is defined to be the sum

$$\sum_p n_p \in \mathbb{Z}.$$

This gives a group homomorphism $\deg : \mathrm{Weil}(C) \to \mathbb{Z}$.

Definition 3.81. Let $\pi : C \to C'$ be a morphism between algebraic curves, and $\pi^* : K(C') \to K(C)$ be the induced morphism between the underlying function fields. If $p \in C$ is a closed point (i.e., not the generic point), then we define the *ramification* of π at p by

$$e_\pi(p) := \mathrm{val}_p(\pi^* t_q),$$

where t_q is any generator of the maximal ideal corresponding to $q = \pi(p)$ (i.e., a *uniformizer* at q).

Definition 3.82. Let $\pi : C \to C'$ be a morphism between algebraic curves, and $D = \sum_{q \in C} n_q q$ a divisor on C'. Then we define the *pullback* of D by

$$\pi^*(q) = \sum_{p \in \pi^{-1}(q)} e_\pi(p) p,$$

and extending linearly.

Definition 3.83. Let $\pi : C \to C'$ be a morphism between algebraic curves. The *degree* of the map π is the degree of the field extension induced by π^*, i.e., $[K(C) : \pi^*(K(C'))]$.

The various notions of *degree* will let us better characterize the elements of $\mathrm{Pic}(C)$. In particular, we will see that line bundles have a well-defined degree (the degree of any rational section), and that the degree of the divisor associated to any rational function is zero. The following proposition is of crucial importance. We omit the proof.

Proposition 3.84. *Let $\pi : C \to C'$ be a morphism of algebraic curves. Then for each closed point p of C', we have*

$$\deg \pi^*(p) = \deg \pi.$$

Note that on the LHS we interpret $\pi^*(p)$ as a divisor on C'.

Using this proposition, we may establish some crucial facts about divisors on algebraic curves.

Lemma 3.85. *Let C be an algebraic curve. There is a natural one-to-one correspondence between elements of $K(C)$ and morphisms $C \to \mathbb{P}^1$.*

Proof. The function field of $\mathbb{P}^1$ is $\Bbbk(x)$. Any morphism $C \to \mathbb{P}^1$ induces a morphism $K(\mathbb{P}^1) \to K(C)$ on function fields, and any such morphism on function fields is determined by the image of x. Conversely, given such a morphism on function fields (i.e., the image of the element x) we have the natural morphisms of the corresponding structure sheaves (identifying the function spaces with subrings of the function fields as usual), and this induces a morphism $C \to \mathbb{P}^1$. □

Lemma 3.86. *If C is an algebraic curve and $f \in K(C)$ is non-zero, then $div(f) = f^*(0) - f^*(\infty)$ where f is regarded as a map $f : C \to \mathbb{P}^1$.*

Proof. Let $t_0 \in K(\mathbb{P}^1)$ be a uniformizer at $0 \in \mathbb{P}^1$. Then

$$f^*(0) = \sum_{p \in f^{-1}(0)} \mathrm{val}_p(f^*t_0)p.$$

Note that $\mathrm{val}_p(f^*t_0) \leq 0$ means that f^*t_0 does not belong to the maximal ideal at p. Moreover, if $\mathrm{val}_p(f^*t_0) > 0$ then f^*t_0 belongs to the maximal ideal at p, hence the maximal ideal at $0 \in \mathbb{P}^1$ is mapped into the maximal ideal at $p \in C$ by f^*, and so $f(p) = 0$. The above sum is therefore just the divisor of zeros of f, and the analogous fact holds for the point $\infty \in \mathbb{P}^1$. This completes the proof. □

Lemma 3.87. *If C is an algebraic curve and $f \in K(C)$ is non-zero, then* $\deg div(f) = 0$.

Proof. Using Proposition 3.84 with $\pi = f$ and $p = 0$ (respectively $\pi = f$ and $p = \infty$) in conjunction with Lemma 3.86 we see that

$$\deg \mathrm{div}(f) = \deg f^*(0) - \deg f^*(\infty) = \deg f - \deg f = 0.$$

□

Definition 3.88. If $\mathcal{L}$ is a line bundle on an algebraic curve C, then we define the degree of $\mathcal{L}$ to be the degree of any rational section of $\mathcal{L}$.

Lemma 3.89. *The degree of $\mathcal{L}$ in definition 3.88 is well-defined.*

Proof. Suppose that s and s' are both rational sections of $\mathcal{L}$. By Lemma 3.69 we have that $\mathcal{L} \cong \mathcal{O}_C[\mathrm{div}(s)] \cong \mathcal{O}_C[\mathrm{div}(s')]$, hence

$$\mathcal{O}_C \cong \mathcal{L} \otimes \mathcal{L}^\vee \cong \mathcal{O}_C[\mathrm{div}(s)] \otimes \mathcal{O}_C[\mathrm{div}(1/s')].$$

Since s/s' corresponds to a rational section of $\mathcal{O}_C$ under this isomorphism, we have $\mathrm{div}(s) = \mathrm{div}(s')$. □

3.5 Final Digression: Pullbacks of Line Bundles

We need one final tool before discussing the construction of the Jacobian variety, and due to lack of a more opportune moment to discuss it we are forced to place it here. The notion is that of the pullback of a line bundle; we will need it when describing the functor which the Jacobian variety is meant to represent, and given a morphism $f : X \to Y$ and a line bundle $\mathcal{L}$ on Y it will give us a line bundle $f^*\mathcal{L}$ on X. The version of this concept for manifolds or even more general topological spaces is more intuitive, so we describe that first.

Recall that sheaves are objects typically associated to some sort of fibre bundle. If Y is (say) a smooth manifold, then a fibre bundle over Y is an object E together with a map $\pi : E \to Y$ such that above every point $p \in Y$ the fibre $\pi^{-1}(p)$ is isomorphic to some "standard fibre" F. In particular, every point $p \in Y$ has a neighbourhood $U \subseteq Y$ such that $\pi^{-1}(U) \cong U \times F$.

Now suppose that $f : X \to Y$ is a map. We wish to define a "pullback bundle" f^*E which is in some sense the pullback of $\pi : E \to Y$ along f. A nice example of what we want is the case where $f : X \hookrightarrow Y$ is an inclusion, in which case we wish that $f^*E = \pi^{-1}(X)$ holds. This in particular is true if we define the pullback bundle via the fibre product, i.e., we define the pullback f^*E to be an object with two maps $\pi^* : f^*E \to X$ and $g : f^*E \to E$ such that the diagram

$$\begin{tikzcd}
f^*E \arrow[r, "g"] \arrow[d, "\pi^*"] & E \arrow[d, "\pi"] \\
X \arrow[r, "f"] & Y
\end{tikzcd}$$

commutes and such that f^*E is universal with respect to this property.

Now when working with schemes, it is often easier to work with sheaves instead of bundles, so we first reinterpret this definition in the language of sheaves. We have two sheaves, $\mathcal{F}$ on Y and $f^*\mathcal{F}$ on X, defined by

$$\begin{aligned}
\mathcal{F}(U) &= \{U \xrightarrow{s} E : \pi \circ s = \mathrm{id}_U\}, \qquad\qquad \text{and} \\
(f^*\mathcal{F})(V) &= \{V \xrightarrow{s} f^*E : \pi^* \circ s = \mathrm{id}_V\}.
\end{aligned}$$

To describe $f^*\mathcal{F}$ via a universal property, we need to describe one of its functors of morphisms in the category of sheaves on X. This functor of morphisms should itself be determined by the sheaf $\mathcal{F}$ and the map f alone.

To see how we can do this, suppose for the moment that $\mathcal{G}$ is another sheaf on X, and it corresponds to a bundle $\pi' : E' \to X$. Then a morphism of sheaves $f^*\mathcal{F} \to \mathcal{G}$ corresponds to a bundle morphism $E' \to f^*E$, which is a fibre preserving map $g' : E' \to f^*E$, i.e., a map g' such that $\pi^* \circ g' = \pi'$. We then have the following commuting diagram:

$$\begin{tikzcd}
E' \arrow[dr, "g'"] \arrow[drr, dotted, bend left] \arrow[ddr, bend right, "\pi'"'] & & \\
& f^*E \arrow[r, "g"] \arrow[d, "\pi^*"] & E \arrow[d, "\pi"] \\
& X \arrow[r, "f"] & Y
\end{tikzcd}$$

The question of whether the map g' exists is then a question of whether the dotted arrow exists satisfying the fibre product universal property: if the dotted arrow does exist, then the universal property of the fibre product guarantees the existence of g', and if g' exists then we may take the dotted arrow to be $g \circ g'$. The dotted arrow can itself be interpreted as a bundle morphism between the bundle f_*E' with projection map $f \circ \pi' : E' \to Y$ and the bundle E. Hence we have a bijection

$$\{\text{bundle maps } E' \to f^*E\} \longleftrightarrow \{\text{bundle maps } f_*E' \to E\}.$$

Since the correspondence between sheaves and bundles is a contravariant one, this in turn induces a bijection

$$\{\text{sheaf maps } f^*\mathcal{F} \to \mathcal{G}\} \longleftrightarrow \{\text{sheaf maps } \mathcal{F} \to f_*\mathcal{G}\}.$$

Turning back to the categories of schemes and sheaves on schemes, this motivates the following definition:

Definition 3.90. Let X, Y be schemes, $f : X \to Y$ a morphism of schemes, and $\mathcal{F}$ a $\mathcal{O}_Y$-module. Then the *pullback* $f^*\mathcal{F}$ is a $\mathcal{O}_X$-module such that we have an isomorphism of functors

$$\operatorname{Hom}_{\mathcal{O}_X}(f^*\mathcal{F}, -) \simeq \operatorname{Hom}_{\mathcal{O}_Y}(\mathcal{F}, f_*-).$$

We will use the fact that pullbacks exist without proof. The following lemmas are also important.

Lemma 3.91. *Suppose that $\iota : U \hookrightarrow X$ is an inclusion which realizes U as an open subscheme of the scheme X. Then if $\mathcal{F}$ is an $\mathcal{O}_X$-module, then $\iota^*\mathcal{F} = \mathcal{F}\big|_U$.*

Proof. If $\mathcal{G}$ is a $\mathcal{O}_U$-module then $\iota_*\mathcal{G}$ is a $\mathcal{O}_X$-module. Any morphism $\alpha : \mathcal{F} \to \iota_*\mathcal{G}$ corresponds to a collection of restriction-respecting maps $\alpha_V : \mathcal{F}(V) \to \mathcal{G}(\iota^{-1}(V))$. We have the commutativity of the diagram

$$\begin{tikzcd}
\mathcal{F}(V) \arrow[r, "\alpha_V"] \arrow[d, "\mathrm{res}^V_{U\cap V}"] & \mathcal{G}(\iota^{-1}(V)) = \mathcal{G}(U \cap V) \arrow[d, "\mathrm{res}^{U\cap V}_{U\cap V}"] \\
\mathcal{F}(U \cap V) \arrow[r, "\alpha_{U\cap V}"] & \mathcal{G}(U \cap V)
\end{tikzcd}$$

Since the right downward arrow is the identity map, the map α_V is uniquely determined by $\alpha_{U\cap V}$, and so the morphism $\alpha : \mathcal{F} \to \iota_*\mathcal{G}$ is determined by the morphism $\alpha\big|_U : \mathcal{F}\big|_U \to \mathcal{G}$. We thus have a bijection $\operatorname{Hom}_{\mathcal{O}_U}(\mathcal{F}\big|_U, \mathcal{G}) \simeq \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{F}, \iota_*\mathcal{G})$.

To check that this bijection is natural in $\mathcal{G}$, we consider an arbitrary morphism of $\mathcal{O}_U$-modules $\beta : \mathcal{G} \to \mathcal{G}'$. Then the component maps of the morphism $\beta \circ \alpha\big|_U$ over the open set $V \subseteq U$ are given by $\beta_V \circ \alpha_V$. We denote the map $\iota_*\beta : \iota_*\mathcal{G} \to \iota_*\mathcal{G}'$ to be the map induced by β via the functor ι_*, i.e., the one whose component maps $(\iota_*\beta)_V : \mathcal{G}(\iota^{-1}(V)) \to \mathcal{G}'(\iota^{-1}(V))$ are just the maps $\beta_{U\cap V}$. Then if $V \subseteq U$, the component maps of $(\iota_*\beta) \circ \alpha$ are $\beta_{U\cap V} \circ \alpha_V = \beta_V \circ \alpha_V$, and in particular we have $((\iota_*\beta) \circ \alpha)\big|_U = \beta \circ \alpha\big|_U$. Thus we see that the unique extension to X of the sheaf morphism $\beta \circ \alpha\big|_U$ is in fact $(\iota_*\beta) \circ \alpha$, and so the bijection $\operatorname{Hom}_{\mathcal{O}_U}(\mathcal{F}\big|_U, \mathcal{G}) \simeq \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{F}, \iota_*\mathcal{G})$ is natural in $\mathcal{G}$. □

Lemma 3.92. *If $f : X \to Y$ is a morphism of schemes, then $f^*\mathcal{O}_Y = \mathcal{O}_X$.*

Proof. It suffices to exhibit a bijection $\operatorname{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{G}) \simeq \operatorname{Hom}_{\mathcal{O}_Y}(\mathcal{O}_Y, f_*\mathcal{G})$ which is natural in $\mathcal{G}$. We omit the proof. □

Lemma 3.93. *If $f : X \to Y$ and $g : Y \to Z$ are morphisms of schemes, and $\mathcal{F}$ is an $\mathcal{O}_Z$-module, then $(g \circ f)^*\mathcal{F} = g^*(f^*\mathcal{F})$.*

Proof.

$$\begin{aligned}\mathrm{Hom}_{\mathcal{O}_X}((g \circ f)^*\mathcal{F}, -) &\simeq \mathrm{Hom}_{\mathcal{O}_Z}(\mathcal{F}, (g \circ f)_* -)\\ &\simeq \mathrm{Hom}_{\mathcal{O}_Z}(\mathcal{F}, f_*(g_* -))\\ &\simeq \mathrm{Hom}_{\mathcal{O}_Y}(f^*\mathcal{F}, g_* -)\\ &\simeq \mathrm{Hom}_{\mathcal{O}_X}(g^*(f^*\mathcal{F}), -)\end{aligned}$$

□

Lemma 3.94. *If $f : X \to Y$ is a morphism of schemes and $\mathcal{F}$ and $\mathcal{G}$ are $\mathcal{O}_Y$-modules, then*

$$f^*(\mathcal{F} \otimes_{\mathcal{O}_Y} \mathcal{G}) = (f^*\mathcal{F}) \otimes_{\mathcal{O}_X} (f^*\mathcal{G}).$$

Proof. Omitted. □

Lemma 3.95. *If $f : X \to Y$ is a morphism of schemes and $\mathcal{L}$ is an invertible sheaf on Y, then $f^*\mathcal{L}$ is an invertible sheaf on X.*

Proof. Since $\mathcal{L}$ is an invertible sheaf, around any $p \in Y$ there is an open neighbourhood U such that $\mathcal{L}\big|_U \cong \mathcal{O}_X\big|_U$. Denote by ι the morphism $\iota : f^{-1}(U) \hookrightarrow X$. Then by Lemmas 3.91, 3.92 and 3.93 we have

$$\begin{aligned}(f^*\mathcal{L})\big|_{f^{-1}(U)} &= \iota^*(f^*\mathcal{L})\\ &= (f \circ \iota)^*\mathcal{L}\\ &= (f\big|_{f^{-1}(U)})^*\mathcal{L}\big|_U\\ &\cong (f\big|_{f^{-1}(U)})^*\mathcal{O}_X\big|_U\\ &\cong \mathcal{O}_Y\big|_{f^{-1}(U)}\end{aligned}$$

which shows that $f^*\mathcal{L}$ is also invertible. □

All of this amounts to saying that

Lemma 3.96. *If $f : X \to Y$ is a morphism of schemes, then $f^* : Pic(Y) \to Pic(X)$ is a group homomorphism. In particular, Pic is a functor* **Sch** $\to$ **Grp**. □

4 Abstract Construction of the Jacobian Variety

In this section we describe how one goes about constructing the Jacobian variety of a curve C. The idea will be along the lines we sketched in our exposition of category theory, in that we will describe a particular functor in an appropriate category and argue that it can be represented. To justify this as being a construction of "the" Jacobian variety, it is important that the functor we describe has an interpretation where the points of the representing object are in fact the things we wish to view as points of the Jacobian. Moreover, we need to understand what we are to expect of a functor that corresponds to a "group object". The next section develops these ideas.

4.1 The Functorial Viewpoint on Group Schemes

When working with, say, manifolds, one can view a point p in a space X as a map $\bullet \to X$ from the one point space $\bullet$ whose image is $\{p\}$. An advantage of this viewpoint is that it allows us to interpret the sets $\mathrm{Hom}(\bullet, X)$ as being a collection of points of X, and thus if a functor F is contravariantly representable by X, we are justified in thinking of the points of X as being the set $F(\bullet)$.

With schemes the situation is more complicated, because there is not just one "type" of point by many: a scheme can have points over $\mathbb{Z}$, over $\mathbb{Q}$, over an arbitrary ring or field, or even over another scheme. In general, we have the following definition:

Definition 4.1. Let X be a scheme. Then a Y-valued point of X, where Y is also a scheme, is an element of the set $\mathrm{Hom}_{\mathbf{Sch}}(Y, X)$.

The usual case is when $Y = \mathrm{Spec}\, R$ is affine, which we will often refer to being the R-valued case. One can see that this generalizes the usual notion of the field of definition of a point from classical algebraic geometry, since a map $\mathrm{Spec}\, \Bbbk \to X$ corresponds to a collection of compatible morphisms $\mathcal{O}_X(U) \to \Bbbk$ for each open set $U \subseteq X$, and the kernel of each such morphism is a maximal ideal of the ring $\mathcal{O}_X(U)$ corresponding to the point of interest. If $\mathcal{O}_X(U)$ is a $\Bbbk$-algebra, then this is just the usual notion of $\Bbbk$-valued point.

In general, we would like to be able to ensure that all the rings $\mathcal{O}_X(U)$ are $\Bbbk$-algebras over some field $\Bbbk$, since our construction of the Jacobian of a curve C will generally have the curve C defined over some field $\Bbbk$. The next definition will ensure this is the case.

Definition 4.2. Let $\Bbbk$ be a field. We define a $\Bbbk$-scheme to be a scheme X with a morphism $X \to \mathrm{Spec}\, \Bbbk$. Note that because the topological space of $\mathrm{Spec}\, \Bbbk$ consists of a single point, this is essentially just a collection of maps $\Bbbk \hookrightarrow \mathcal{O}_X(U)$ which commute with restrictions, or another way of saying that the elements of $\Bbbk$ are (constant) functions on X.

Definition 4.3. A morphism of $\Bbbk$-schemes X and Y is defined to be a morphism $\pi : X \to Y$ of schemes such that the following triangle commutes:

$$\begin{tikzcd}
X \arrow[rr, "\pi"] \arrow[dr] & & Y \arrow[dl] \\
& \mathrm{Spec}\, \Bbbk &
\end{tikzcd}$$

We refer to the category of $\Bbbk$-schemes by **k-Sch**. The morphism into $\mathrm{Spec}\, \Bbbk$ is called the *structure morphism* of the scheme. Note the important difference between a map $X \to$

$\operatorname{Spec}\Bbbk$ and a map $\operatorname{Spec}\Bbbk \to X$: while the former ensures that the functions on X include the constant functions in $\Bbbk$, the latter picks out a so-called "$\Bbbk$-valued point" of X. This idea will be important later, when we will want to ensure that the object X we are using to represent the functor has the "right $\Bbbk$-valued points", which will simply mean that the representing natural transformation associates the right set to $\mathrm{Hom}_{\mathbf{k\text{-}Sch}}(\operatorname{Spec}\Bbbk, X)$. Note also that products in **k-Sch** are simply fibre products over the structure morphisms; we will often write this as simply a product when the underlying category is understood.

To construct the Jacobian variety of a curve C over a field $\Bbbk$, we will want it to be a $\Bbbk$-scheme with a group structure given by morphisms of $\Bbbk$-schemes. An easy way to express this idea is with the notion of a *group object* in the category **k-Sch**, which we now define.

Definition 4.4. A *group object* in **k-Sch** consists of the following data:

(i) A map $m : G \times_{\Bbbk} G \to G$ called the multiplication map.

(ii) A map $i : G \to G$ called the inversion map.

(iii) A map $e : \operatorname{Spec}\Bbbk \to G$.

These maps satisfy the following commutative diagrams:

(i) Associativity:

$$\begin{tikzcd}
G \times_{\Bbbk} G \times_{\Bbbk} G \arrow[r, "\mathrm{id}\times m"] \arrow[d, "m\times\mathrm{id}"'] & G \times_{\Bbbk} G \arrow[d, "m"] \\
G \times_{\Bbbk} G \arrow[r, "m"] & G
\end{tikzcd}$$

(ii) Identity:

$$\begin{tikzcd}
G \times_{\Bbbk} \operatorname{Spec}\Bbbk \arrow[r, "\mathrm{id}\times e"] \arrow[d, "e\times\mathrm{id}"'] \arrow[dr, "\mathrm{id}"] & G \times_{\Bbbk} G \arrow[d, "m"] \\
G \times_{\Bbbk} G \arrow[r, "m"] & G
\end{tikzcd}$$

(iii) Inverse:

$$\begin{tikzcd}
G \arrow[r, "\mathrm{id}\times i"] \arrow[d, "i\times\mathrm{id}"'] \arrow[dr] & G \times_{\Bbbk} G \arrow[ddr, "m"] & \\
G \times_{\Bbbk} G \arrow[drr, "m"] & \operatorname{Spec}\Bbbk \arrow[dr, "e"] & \\
 & & G
\end{tikzcd}$$

The maps $a \times b$ are all obtained from the universal property of the target products, where we suppress some compositions with associated projection maps (as in the case of the associativity diagram, where the source is also a product). We note that $G \times_{\Bbbk} \operatorname{Spec}\Bbbk \simeq G$, which is why we have a diagonal identity arrow in the second diagram.

If one applies the Yoneda Lemma to the diagrams in Definition 4.4, then one obtains the same diagrams with G replaced by $\mathrm{Hom}_{\textbf{k-Sch}}(-, G)$ and the various morphisms replaced by pushforward maps. If we evaluate these diagrams on some $\Bbbk$-scheme X, then the diagrams reduce to telling us that $\mathrm{Hom}_{\textbf{k-Sch}}(X, G)$ forms a group. The Yoneda embedding is functorial in the first argument, and each induced pushforward morphism m_*, i_*, etc. commutes with any pullback morphism induced by a map of $\Bbbk$-schemes $\pi : X \to X'$. In fact, we have the following:

Lemma 4.5. *An object G in* **k-Sch** *is a group object if and only if $Hom_{\textbf{k-Sch}}(X, G)$ is a group functorially in X.*[5]

Proof. We omit the proof because it is really nothing more than a tedious verification. □

A functor satisfying the characterization of Lemma 4.5 is called a *group functor*. The idea is that the points of the group scheme G should form a group over any field, ring, or even scheme, and that the group operation should be natural in the sense that if one were to perform a "base change" then the base change would commute with the group operation. So for instance, if a group operation is given by polynomial or rational functions which describes a group law in the sense that the *algebraic expressions themselves* satisfy the properties of a group law (as opposed to just coincidentally giving maps of points that happen to satisfy the group axioms), then one can freely extend the field or ring of definition of the points of the space and still have a group law. Moreover, the process of extending the field of definition commutes with the group operation itself: if one computes the sum of two points on an elliptic curve defined over $\mathbb{Q}$, and then views those points as lying in $\mathbb{C}$, one gets the same result as if one had first viewed those points as lying in $\mathbb{C}$ and then computed their sum. This is exactly the intuition that the group functor language encodes, where we keep in mind the interpretation of $\mathrm{Hom}_{\textbf{k-Sch}}(X, G)$ as the X-valued points of G as described above.

4.2 Finding the Right Functor

We now turn to the question of where it is that Jacobian varieties come from, and how we can find an appropriate functor to describe their points in the category **k-Sch** over some field $\Bbbk$. Like with many things in algebraic geometry, the picture is clearest over the complex numbers. There, one can show the existence of a one dimensional abelian variety as follows: if $\Lambda \subset \mathbb{C}$ is a lattice, then $\mathbb{C}/\Lambda$ is a compact Riemann Surface. The addition law on $\mathbb{C}$ descends to an addition law on $\mathbb{C}/\Lambda$ which turns $\mathbb{C}/\Lambda$ into a group in the category of compact Riemann Surfaces. The category of compact Riemann Surfaces is known to be equivalent to the category of smooth, projective, algebraic curves over $\mathbb{C}$, hence each such lattice under this correspondence gives rise to an algebraic curve with an algebraic group law. These curves are called *elliptic curves*.

This argument makes crucial use of the fact that every compact one dimensional complex manifold (compact Riemann Surface) is an algebraic curve; this correspondence does not extend to dimensions greater than one, and so establishing the existence of higher dimensional abelian varieties is not as simple. What is true, however, is that every complex abelian variety is isomorphic to a complex manifold of the form $\mathbb{C}^g/\Lambda$ where $\Lambda \subset \mathbb{C}^g$ has

[5] The terminology "functorially in X" simply means that as we vary X all the natural diagrams (i.e., the ones that encode the group law) induced by pullbacks of morphisms $\pi : X \to X'$ commute. This is standard terminology.

the structure of a lattice (this fact follows from some basic Lie Group theory, but we do not prove it here). The issue is that not every lattice $\Lambda \subset \mathbb{C}^g$ gives rise to an abelian variety, as in general the space of meromorphic functions on these lattices might be sufficiently meagre so as to not possess enough algebraic relations among them to give it a variety structure.

If C is a one-dimensional compact Riemann Surface of genus g, then the *Jacobian* of C is a particular complex torus $X \cong \mathbb{C}^g/\Lambda$ associated to C for which the space of meromorphic functions on $\mathrm{Jac}(C)$ has "enough" algebraic relations to give it the structure of a variety. To construct it we consider the vector space $\Gamma(C, \Omega^1_C)^*$, where Ω^1_C is the sheaf of holomorphic one-forms on C. This vector space is isomorphic to $\mathbb{C}^g$, and there is a natural embedding of $H_1(C, \mathbb{Z})$ into this vector space via the map $[\gamma] \mapsto \int_\gamma -$, where the notation on the right-hand side denotes the integration functional that integrates a one-form along the curve γ. The map is well-defined since any such integral is zero on closed curves homologous to a point. This map is injective, and the embedding of $H_1(C, \mathbb{Z}) \cong \mathbb{Z}^{2g}$ defines a lattice Λ in $\Gamma(C, \Omega^1_C)^*$. We then have $\mathrm{Jac}(C) = \Gamma(C, \Omega^1_C)^*/\Lambda$.

In the theory of complex abelian varieties, which we do not develop here, there is a natural notion of duality. The idea can be interpreted as coming from a certain point of view regarding complex abelian varieties and their lattices. On one hand, we can imagine studying complex abelian varieties of dimension g by simply studying those lattices $\Lambda \subset \mathbb{C}^g$ such that $\mathbb{C}^g/\Lambda$ has the structure of a variety. But another, equivalent, perspective is to imagine fixing a lattice $\Lambda \cong \mathbb{Z}^{2g}$ and instead studying the different complex structures on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^{2g}$ (i.e., $\mathbb{R}$-algebra homomorphisms $\mathbb{C} \to \mathrm{End}_{\mathbb{R}}\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$)[11][12]. This second perspective gives rise to a natural duality, where the dual lattice is $\Lambda^\vee = \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$ and there is a natural map $\mathbb{C} \to \mathrm{End}_{\mathbb{R}}\Lambda^\vee \otimes_{\mathbb{Z}} \mathbb{R}$ which we omit. Under this duality, the complex torus $\Gamma(C, \Omega^1_C)^*/\Lambda$ satisfies the correspondence

$$\Gamma(C, \Omega^1_C)^*/\Lambda = \mathrm{Pic}^0(C)^\vee,$$

where we denote by $\mathrm{Pic}^0(C)$ the group of isomorphism classes of degree 0 line bundles[6] on C. The Abel-Jacobi theorem gives a natural bijection between $\Gamma(C, \Omega^1_C)^*/\Lambda$ and $\mathrm{Pic}^0(C)$ (they are dual, but need not be isomorphic, when C is not an algebraic curve), and so both are called "the" Jacobian in this case.

Based on this motivating digression, we need to describe a functor **k-Sch** $\to$ **Set** so that the $\Bbbk$-valued points of the functor (i.e., $\Bbbk$-valued points of any representing scheme) are the elements of $\mathrm{Pic}^0(C)$. For a $\Bbbk$-scheme T, we define

$$\mathrm{P}^0_C(T) = \mathrm{Pic}^0(C \times T)/q^*\mathrm{Pic}^0(T),$$

where $q : C \times T \to T$ is the standard projection. We have not defined what it means for a general line bundle on a scheme X to be degree zero, but for our purposes we may say that this is true when the pullback of the line bundle to any curve contained in X has degree zero. The functor is then defined on morphisms via the natural pullback maps, where one can show that the pullback of a degree zero line bundle is again degree zero.

It is easy to see that $\mathrm{P}^0_C(\mathrm{Spec}\, \Bbbk) = \mathrm{Pic}^0(C)$, and so this functor (assuming it in fact is a functor) is a good candidate. It is also clear that $\mathrm{P}^0_C(T)$ forms a group for each T, and the properties of the pullback show that this group operation is natural in T. We omit a proof of the following proposition.

[6] We are sweeping the difference between holomorphic and algebraic line bundles under the rug here.

Proposition 4.6. *P^0_C is a functor* **k-Sch** $\to$ **Set***.*

Proof. Omitted. $\square$

The above proposition along with Lemma 4.5 shows that to construct $\mathrm{Jac}(C)$ as a group scheme, it suffices to represent P^0_C. To go on to show that $\mathrm{Jac}(C)$ is an abelian variety one needs to demonstrate some additional properties of the $\Bbbk$-scheme representing P^0_C, which we omit.

We now give a brief sketch, following Milne[5][6], of how one shows that P^0_C is representable. Noting the correspondence between $\mathrm{Pic}^0(C)$ and degree zero divisors modulo principal divisors, we endeavour to construct a variety whose points correspond to a divisor from each equivalence class in $\mathrm{Pic}^0(C)$. To represent a formal sum of r points, it is natural to consider the symmetric product

$$C^{(r)} := \underbrace{C \times C \times \cdots \times C}_{r \text{ times}}/S_r,$$

where the group action is given by permuting elements. The $\Bbbk$-points of $C^{(r)}$ then can be thought of as representing effective divisors (divisors with non-negative coefficients) of degree r. Denote by $\mathrm{Pic}^r(C)$ the set of equivalence classes of degree r divisors. If $P \in C$ is some $\Bbbk$-point, then we have a bijective map $\mathrm{Pic}^0(C) \to \mathrm{Pic}^r(C)$ sending $[D] \mapsto [D+rP]$. By defining a functor P^r_C analogous to P^0_C one can extend this to an isomorphism of functors, and so it suffices to represent P^r_C.

It is not in general true that every equivalence class in $\mathrm{Pic}^r(C)$ contains a unique representative which is an effective degree r divisor; in general there may be many representatives to choose from, and so we might instead hope to be able to choose these representatives in some canonical way and describe $\mathrm{Jac}(C)$ as a subvariety derived from $C^{(r)}$. Via the Riemann-Roch Theorem, one can show that for $r > 2g-2$ the natural map $\varphi : C^{(r)} \to \mathrm{Pic}^r(C)$ sending an effective degree r divisor D to $[D]$ is surjective, and so selecting a representative of $\mathrm{Pic}^r(C)$ is just a matter of defining a map $s : \mathrm{Pic}^r(C) \to C^{(r)}$ such that $\varphi \circ s = \mathrm{id}$.

The points p of $C^{(r)}$ of interest are then the ones in the image of s, or the ones that satisfy $p = (s \circ \varphi)(p)$. If we can interpret both s and φ functorially, then map $s \circ \varphi$ will be a morphism, and we may form the fibre product

$$\begin{tikzcd}
J \arrow[r] \arrow[d] & C^{(r)} \arrow[d, "(\mathrm{id}, s\circ\varphi)"] \\
C^{(r)} \arrow[r, "\Delta"] & C^{(r)} \times C^{(r)}
\end{tikzcd}$$

where Δ is the diagonal map. The $\Bbbk$-points of J will then be those pairs $(a, b) \in C^{(r)} \times C^{(r)}$ such that $a = b$ and $a = (s\circ\varphi)(b)$, and so correspond bijectively (and, hopefully, functorially) to $\mathrm{Pic}^r(C)$.

Unfortunately, it is not always possible to find a map s which can be given a functorial interpretation, but fortunately, this can be done “locally” on open subsets of $C^{(r)}$. The full Jacobian can then be constructed as a union of subvarieties by gluing of charts. For details on this construction please see the exposition by Milne[5][6].

5 Concrete Equations for Hyperelliptic Jacobians and their Group Law

In this section we present some original work which gives explicit equations for the group law on hyperelliptic Jacobians on an affine dense open set. It can be read independently of the rest of the thesis, and in fact should be, as it is essentially the rough draft of a paper that will soon be submitted to a mathematical journal.

5.1 Introduction

Abelian varieties and their equations have long attracted interest in arithmetic geometry. Although it is known that equations describing these varieties must exist, and their nature has received some study[7–9], it is in general believed to be impractical or infeasible to write such equations down. This attitude is perhaps best summarized in Milne's notes[5] on the subject, where he writes "In general, it is not possible to write down explicit equations for an abelian variety of dimension > 1, and if one could, they would be too complicated to be of use."

A brief look at the literature on the matter seems to justify this outlook. For instance, the paper of Flynn[16] gives a general set of equations for genus two Jacobians over an arbitrary ground field; there are 72 equations in total, listed in an appendix, which describe these Jacobians as projective subvarieties of a 15-dimensional projective space. A follow-up paper from Flynn[15] describes the group law, the equations of which he describes as "too large to be written down," and instead focuses on methods to compute specializations of the group law for tasks such as point-doubling or the addition of fixed points of low order. Related work by Grant[3] gives a simpler set of defining equations in 8-dimensional projective space, but at the cost of some generality.[7] In both cases, the authors remark that portions of their exposition required computer verification, as the algebraic expressions involved are too complicated to be reliably manipulated by hand.

One of the difficulties that arises in these approaches is that the usual methods for embedding genus g Jacobians into n-dimensional projective spaces tend to result in an exponential dependence of n on g, with $n = 3^g - 1$ and $n = 4^g - 1$ being common (as in the case for $g = 2$ above). This ensures that finding explicit equations via this strategy must necessarily be impractical for large g. An alternative approach, which we pursue in this paper, is to give explicit equations for Jacobians and their group law affine-locally, and construct the full Jacobian by gluing of charts. For hyperelliptic curves, the Jacobian variety itself is described in this manner by Mumford[10], with the affine-local pieces utilizing affine spaces of dimension $3g+1$, and hence with the number of parameters depending only linearly on g. In this paper, we show how to extend this construction to give explicit equations for the group law.

Our work is inspired by the paper of Leitenberger[4] and the paper of Costello and Lauter[1], both of which essentially carry out this approach in the case $g = 2$. Our methods can be viewed as a substantial generalization of their work.

5.2 Algebraic Construction of Hyperelliptic Jacobians

In this section, we review the construction of hyperelliptic Jacobians that appears in Mumford's Lectures on Theta[10] and set notation. We consider hyperelliptic curves C defined

[7] Although, in fairness to Grant, our work makes similar assumptions.

over an algebraically closed field $\Bbbk$ with $\operatorname{char}\Bbbk \neq 2$ by two equations of the form

$$C_1 : y^2 = f(x) = f_{2g+1}x^{2g+1} + f_{2g}x^{2g} + \cdots + f_0$$
$$C_2 : s^2 = h(t) = t(h_{2g+1}t^{2g+1} + h_{2g}t^{2g} + \cdots + h_0)$$

glued along the morphism which makes the identifications $x = 1/t$ and $y = s/t^{g+1}$. We require that $f(x)$ has non-vanishing discriminant, and that f is monic.[8] Note that the equation C_2 completes the curve defined by C_1 by adding a single "infinite" point corresponding to $(t, s) = (0, 0)$. Note also that $h_i = f_{(2g+1)-i}$. We will work with the equation C_1, and refer to the point $(t, s) = (0, 0)$ by the symbol ∞. We define the *hyperelliptic involution* to be the map $\iota : C \to C$ determined by $(x, y) \mapsto (x, -y)$. If P is a point on C, then $\iota(P)$ is deemed its *conjugate*.

One may check that the curve C is smooth, and that all divisor classes in $\operatorname{Jac}(C) = \operatorname{Pic}^0(C)$ have a unique representative of the form $P_1 + \cdots + P_g - g\infty$, where each P_i is a point on C. To introduce coordinates into $\operatorname{Jac}(C)$, Mumford describes how to parametrize unordered g-tuples of points on C_1. Given $P_i = (x_i, y_i)$, where $1 \leq i \leq g$ and $P_i \neq \iota(P_j)$ for $i \neq j$, we define two polynomials describing the divisor $P_1 + \cdots + P_g$. The first is defined as

$$u(x) = \prod_{i=1}^{n}(x - x_i) = u_g x^g + u_{g-1}x^{g-1} + \cdots + u_0;$$

that is, it is the monic polynomial whose roots are the x-coordinates of the P_i's counted with their multiplicity $\operatorname{mult}(P_i)$. The second polynomial $v(x) = \sum_{i=0}^{g-1} v_i x^i$ is defined to be the unique polynomial of degree $g - 1$ which approximates the function y up to order $\operatorname{mult}(P_i)$ at P_i; that is, where $\operatorname{val}_{P_i}(v - y) = \operatorname{mult}(P_i)$ for all $1 \leq i \leq g$, and val_{P_i} is the valuation at P_i. Note that for each i, the coordinate function $z_i = x - x_i$ is a uniformizer at P_i, and re-expressing the polynomial v in terms of z_i the condition $\operatorname{val}_{P_i}(v - y) = \operatorname{mult}(P_i)$ amounts to imposing $\operatorname{mult}(P_i)$ linear relations on the coefficients v_i. Since there are g such conditions total a polynomial v satisfying these conditions must exist. To see the uniqueness claim, observe that if v_1 and v_2 are any two such polynomials their difference $v_1 - v_2$ satisfies

$$\operatorname{val}_{P_i}(v_1 - v_2) \geq \min\{\operatorname{val}_{P_i}(v_1 - y), \operatorname{val}_{P_i}(y - v_2)\} = \operatorname{mult}(P_i).$$

But then $v_1 - v_2$ is a polynomial of degree at most $g - 1$ and has g roots with multiplicity, hence must be zero.

The pairs (u, v) are in one-to-one correspondence with degree g effective divisors on C_1 not containing any pair of conjugate points: the roots of u give the x-coordinates x_i of the g points, the value $v(x_i)$ gives their y-coordinates y_i, and as we have seen the pair (u, v) is uniquely determined. Moreover, we have

$$\operatorname{val}_{P_i}(f - v^2) = \operatorname{val}_{P_i}(y^2 - v^2) = \operatorname{mult}(P_i) + \operatorname{val}_{P_i}(y + v) = \operatorname{mult}(P_i),$$

where we have used the fact that $y + v$ is non-vanishing at P_i since $\operatorname{char}\Bbbk \neq 2$. Hence $f - v^2$ is a polynomial in x of degree $2g + 1$ which vanishes to order $\operatorname{mult}(P_i)$ at each point P_i, and so we have that $u|(f - v^2)$. Writing $w = \sum_{i=0}^{g+1} w_i x^i$ for the unique monic degree $g + 1$

[8] For the formulas we will develop, it will be useful to consider all the coefficients of f on "equal footing," which is why we give the x^{2g+1} coefficient a distinct label despite the fact that we will always assume it is equal to 1.

polynomial which satisfies $f - v^2 = uw$, we get the following relations by examining the x^i coefficient:

$$f_i - \sum_{j=0}^{i} v_j v_{i-j} = \sum_{j=0}^{i} u_j w_{i-j} \qquad\qquad 0 \leq i \leq 2g+1. \tag{1}$$

Here we have adopted a convention which will be in use throughout the paper, which is that polynomials may be regarded as formal power series in which all but finitely many coefficients, all of which have non-negative index, are zero. Thus we have that each of the sets of coefficients f_i, u_i, v_i and w_i are defined for all $i \in \mathbb{Z}_{\geq 0}$ (or, when it will be convenient, all $i \in \mathbb{Z}$), and so the equation (1) holds for all $i \in \mathbb{Z}_{\geq 0}$, although it is only non-trivial when $0 \leq i \leq 2g+1$.

The polynomials u, v and w have $g + g + (g+1) = 3g+1$ undetermined coefficients among them, and as i ranges from 0 to $2g$ we obtain $2g+1$ relations from (1), where we note that the relation obtained in the case $i = 2g+1$ is redundant. We have the following result from Mumford[10]:

Theorem 5.1 (Mumford)**.** *The equations (1) for $0 \leq i \leq 2g$ define a g-dimensional affine variety $Z \subset \mathbb{A}_{\Bbbk}^{3g+1}$ whose points are in bijection with divisors of the form*

$$\left\{ D = \sum_{i=1}^{g} P_i : \;\; P_i \neq \infty \textit{ for all } i, \;\; P_i \neq \iota(P_j) \textit{ for } i \neq j \right\}.$$

If $\Bbbk = \mathbb{C}$ then the variety is smooth.

The equations (1) therefore parametrize the points of $\mathrm{Jac}(C) \setminus \Theta$, where

$$\Theta := \left\{ [D] \in \mathrm{Jac}(C) : D \sim \sum_{i=1}^{g-1} P_i - (g-1)\infty, \quad P_i \in C(\Bbbk) \text{ for } 1 \leq i \leq g-1 \right\}.$$

Mumford then shows that one can cover $\mathrm{Jac}(C)$ by an atlas of charts isomorphic to Z. He does this by studying sets of the form $[e_T] + (\mathrm{Jac}(C) \setminus \Theta)$, where e_T is a 2-torsion divisor associated to a certain subset T of the branch points of C (those points P satisfying $\iota(P) = P$), and showing that they cover $\mathrm{Jac}(C)$. He then shows that the translation map $[D] \mapsto [e_T] + [D]$ is algebraic, and that gluing a translate of Z for each set $[e_T] + (\mathrm{Jac}(C) \setminus \Theta)$ gives an atlas of charts for $\mathrm{Jac}(C)$.

To describe an explicit group law on $\mathrm{Jac}(C)$, therefore, it suffices to describe it on Z. This is first and foremost because Z defines a dense open set of $\mathrm{Jac}(C)$, and so knowing the group law on Z allows one to compute it for almost all points of $\mathrm{Jac}(C)$ (i.e., apart from on a set of measure zero when $\Bbbk = \mathbb{C}$), and secondly because if one wants to add points belonging to Θ, one can pre- and post-compose with algebraic translations by $[e_T]$ and $-[e_T]$ to bring both summands into a chart isomorphic to Z. In principle, one has to deal with numerous edge cases corresponding to the various situations in which the translation and group-law maps may not be defined, which can occur for instance when a group addition or translation has its result in a different chart. The number and complexity of such edge cases appears to grow with g, and the author is unaware of an easy way to resolve them in general. For this reason, we will restrict our attention to describing the group law for divisor classes belonging to a dense open subset of Z, and leave a discussion of these special cases to future work.

5.3 Special Classes of Polynomials

The derivation of the group law equations will involve two operations of interest: reduction of one polynomial by another polynomial, and equating coefficients of various polynomial expressions. The process of solving equations arising from these operations has a few general features, which we develop here for use in the next section. In this section we work mainly with formal power series for simplicity, although we emphasize that in the applications that follow we will deal exclusively with polynomials. If L is a Laurent series, then $[L]_i$ denotes its i'th coefficient.

For each $n \geq 1$, denote by

$$S_n := \left\{ \sigma = (\sigma_1, \ldots, \sigma_k) \in \mathbb{Z}^k_{\geq 1} : \quad \sum_{i=1}^{k} \sigma_i = n, \quad k \in \mathbb{Z}_{\geq 0} \right\}$$

the set of compositions of the integer n. When $n = 0$ we adopt the usual convention that S_0 contains a single empty composition. If $\sigma \in S_n$ we denote by $|\sigma|$ the length of σ, which is the number of elements in the corresponding sum, or zero if $n = 0$. We have the following Lemma:

Lemma 5.2. Suppose $\alpha = \sum_i \alpha_i x^i$ and $\beta = \sum_i \beta_i x^i$ are Laurent series over $\Bbbk$. Define the *nth iterate of the dth order reduction of α by β at index k* to be the Laurent series A_n defined inductively as follows:

$$\begin{aligned} A_{-1} &= \alpha \\ A_n &= A_{n-1} - x^{d-n} \left[A_{n-1} \right]_{k-n} B \end{aligned}$$

Then

$$[A_n]_i = \alpha_i - \sum_{0 \leq \ell \leq m \leq n} \alpha_{k-\ell} \beta_{i-d+m} \left(\sum_{\sigma \in S_{m-\ell}} (-1)^{|\sigma|} \prod_{r=1}^{|\sigma|} \beta_{k-d-\sigma_r} \right).$$

Remark. The special case of Lemma 5.2 which will be of interest is when $d \geq 0$, α is a polynomial of degree k, and β is a monic polynomial of degree $k - d$, in which case A_d will be the polynomial obtained by reducing α modulo β.

Proof. For the case $n = 0$, we have

$$[A_0]_i = [\alpha - x^d \alpha_k B]_i = \alpha_i - \sum_{0 \leq \ell \leq m \leq 0} \alpha_{k-\ell} \beta_{i-d+m} \cdot 1,$$

where the factor of 1 can be viewed as coming from the empty product $\prod_{r=1}^{|\sigma|} \beta_{k-d-\sigma_r}$ where σ is the unique element of S_0. For the inductive case, we first observe that when $\ell \leq m \leq n-1$, the elements of $S_{n-\ell}$ are in bijection with the elements of $\bigcup_{m=\ell}^{n-1} S_{m-\ell}$, where the bijection is obtained in the natural way by adding in the last summand of $(n - m)$. We thus compute that

$$\begin{aligned}
[A_n]_i &= [A_{n-1}]_i - [x^{d-n}[A_{n-1}]_{k-n}B]_i \\
&= \left[\alpha_i - \sum_{0\le\ell\le m\le n-1} \alpha_{k-\ell}\beta_{i-d+m}\left(\sum_{\sigma\in S_{m-\ell}} (-1)^{|\sigma|}\prod_{r=1}^{|\sigma|}\beta_{k-d-\sigma_r}\right)\right] \\
&\quad - \left[\alpha_{k-n} - \sum_{0\le\ell\le m\le n-1} \alpha_{k-\ell}\beta_{k-d-(n-m)}\left(\sum_{\sigma\in S_{m-\ell}} (-1)^{|\sigma|}\prod_{r=1}^{|\sigma|}\beta_{k-d-\sigma_r}\right)\right]\beta_{i-d+n} \\
&= \left[\alpha_i - \sum_{0\le\ell\le m\le n-1} \alpha_{k-\ell}\beta_{i-d+m}\left(\sum_{\sigma\in S_{m-\ell}} (-1)^{|\sigma|}\prod_{r=1}^{|\sigma|}\beta_{k-d-\sigma_r}\right)\right] \\
&\quad - \left[\alpha_{k-n}\beta_{i-d+n} + \sum_{0\le\ell\le n-1} \alpha_{k-\ell}\beta_{i-d+n}\left(\sum_{\ell\le m\le n-1}\sum_{\sigma\in S_{m-\ell}} (-1)^{|\sigma|+1}\beta_{k-d-(n-m)}\prod_{r=1}^{|\sigma|}\beta_{k-d-\sigma_r}\right)\right] \\
&= \left[\alpha_i - \sum_{0\le\ell\le m\le n-1} \alpha_{k-\ell}\beta_{i-d+m}\left(\sum_{\sigma\in S_{m-\ell}} (-1)^{|\sigma|}\prod_{r=1}^{|\sigma|}\beta_{k-d-\sigma_r}\right)\right] \\
&\quad - \left[\alpha_{k-n}\beta_{i-d+n} + \sum_{0\le\ell\le n-1} \alpha_{k-\ell}\beta_{i-d+n}\left(\sum_{\sigma\in S_{n-\ell}} (-1)^{|\sigma|}\prod_{r=1}^{|\sigma|}\beta_{k-d-\sigma_r}\right)\right] \\
&= \alpha_i - \sum_{0\le\ell\le m\le n} \alpha_{k-\ell}\beta_{i-d+m}\left(\sum_{\sigma\in S_{m-\ell}} (-1)^{|\sigma|}\prod_{r=1}^{|\sigma|}\beta_{k-d-\sigma_r}\right).
\end{aligned}$$

□

The next special situation of interest arises when equating coefficients of two polynomials, one of which arises from a product. We again work in the language of formal power series for convenience.

Lemma 5.3. *Suppose that $\alpha = \sum_{i\ge0}\alpha_i x^i$, $\beta = \sum_{i\ge0}\beta_i x^i$ and $\gamma = \sum_{i\ge0}\gamma_i x^i$ are formal power series over $\Bbbk$, and that $\alpha = \beta\gamma$. Suppose also that $\gamma_0 \neq 0$. Then we are in the situation that $\alpha_k = \sum_{j=0}^{k}\beta_j\gamma_{k-j}$, and so*

$$\beta_k = \sum_{j=0}^{k}\frac{\alpha_j}{\gamma_0}\sum_{\sigma\in S_{k-j}}\frac{(-1)^{|\sigma|}}{\gamma_0^{|\sigma|}}\prod_{r=1}^{|\sigma|}\gamma_{\sigma_r}.$$

Proof. For $k = 0$ we have $\alpha_0 = \beta_0\gamma_0$, and so we may invert γ_0 to get the desired equation.

Considering the inductive case, we have that $\alpha_k = \sum_{i=0}^{k-1} \beta_i \gamma_{k-i} + \beta_k \gamma_0$, and so

$$\begin{aligned}
\beta_k &= \frac{\alpha_k}{\gamma_0} + \sum_{i=0}^{k-1} \frac{(-1)}{\gamma_0} \beta_i \gamma_{k-i} \\
&= \frac{\alpha_k}{\gamma_0} + \sum_{i=0}^{k-1} \frac{(-1)}{\gamma_0} \left(\sum_{j=0}^{i} \frac{\alpha_j}{\gamma_0} \sum_{\sigma \in S_{i-j}} \frac{(-1)^{|\sigma|}}{\gamma_0^{|\sigma|}} \prod_{r=1}^{|\sigma|} \gamma_{\sigma_r} \right) \gamma_{k-i} \\
&= \frac{\alpha_k}{\gamma_0} + \sum_{j=0}^{k-1} \frac{\alpha_j}{\gamma_0} \sum_{j \le i \le k-1} \sum_{\sigma \in S_{i-j}} \frac{(-1)^{|\sigma|+1}}{\gamma_0^{|\sigma|+1}} \gamma_{k-i} \prod_{r=1}^{|\sigma|} \gamma_{\sigma_r} \\
&= \sum_{j=0}^{k} \frac{\alpha_j}{\gamma_0} \sum_{\sigma \in S_{k-j}} \frac{(-1)^{|\sigma|}}{\gamma_0^{|\sigma|}} \prod_{r=1}^{|\sigma|} \gamma_{\sigma_r},
\end{aligned}$$

where we have used the natural bijection between S_{k-j} and $\bigcup_{i=j}^{k-1} S_{i-j}$ obtained by adding $(k-i)$. □

5.4 The Group Law

To compute the sum of two distinct points P and Q (representing the divisor classes $[P-\infty]$ and $[Q-\infty]$) on an elliptic curve, one intersects the curve C with a line ℓ through P and Q which intersects the curve C at a third point R. The sum $[P-\infty]+[Q-\infty]$ is then the divisor class $[\iota(R)-\infty]$, and equations for the group law may be computed by explicitly solving the curve equation for the coordinates of the point $\iota(R)$.

To generalize this strategy to a hyperelliptic curve of genus g, it is natural to try adding $[D_1] = [P_1 + \cdots + P_g - g\infty]$ to $[D_2] = [Q_1 + \cdots + Q_g - g\infty]$ by constructing an interpolating function $\ell(x)$ through the points $P_1, \ldots, P_g, Q_1, \ldots, Q_g$ which intersects the curve at g other points $R_1, \ldots, R_g$. The sum $[D_1]+[D_2]$ is then the divisor class $[\iota(R_1) + \cdots + \iota(R_g) - g\infty]$. If one then attempts to solve for the coordinates of the points $\iota(R_1), \ldots, \iota(R_g)$, however, this seems to require extracting roots, and so this strategy does not produce rational formulas for the group law.

An alternative strategy, employed in the work of Costello and Lauter[1], is to instead represent the divisors D_1 and D_2 using two pairs (u_1, v_1) and (u_2, v_2) as in Section 5.2. If one does this, then the condition that the interpolation function ℓ intersect the curve C with appropriate multiplicity at the various points P_i and Q_i for $1 \le i \le g$ becomes equivalent to the two modular conditions $v_1 \equiv \ell \pmod{u_1}$ and $v_2 \equiv \ell \pmod{u_2}$. Performing a modular reduction, one gets a linear system of equations for the coefficients of ℓ, and solves them to find the interpolation function ℓ in terms of the coefficients of u_1, v_1, u_2 and v_2. Noting that the function $f - \ell^2$ vanishes on all the points P_i, Q_i and any additional intersections R_j, one can then derive linear relations for the coefficients of a polynomial u_3 whose roots give the x-coordinates of the points R_j by noting that $u_3 | (f - \ell^2)$; it is then a simple matter to find an appropriate v_3 to describe the sum.

Costello and Lauter carry out this strategy explicitly for $g = 2$, and sketch how it might work in general, but their approach has an important drawback. Namely, the interpolation functions they use are simply polynomials in x, and for $g > 2$ they do not give g additional intersections $R_1, \ldots, R_g$ but instead some number of intersections strictly between g and $2g$. Therefore, their strategy requires carrying out multiple stages of calculations, the number of which depends on g, and appropriate formulas must be derived for each choice of g

independently. Ideally, it would be possible to carry out a similar strategy with an interpolation function for which exactly g additional intersections $R_1, \dots, R_g$ are guaranteed in the general case, and so do the computation "all at once".

To achieve such an interpolation of the points $P_1, \dots, P_g, Q_1, \dots, Q_g$, we use rational functions of the form

$$\frac{p(x)}{q(x)} = \frac{p_a x^a + \cdots + p_1 x + p_0}{q_b x^b + \cdots + q_1 x + q_0}, \tag{2}$$

where $a = (3g - \varepsilon)/2$, $b = (g - 2 + \varepsilon)/2$, and ε is the parity of g. Since we have $\deg p + \deg q + 2 = 2g + 1$ coefficients and only $2g$ points to interpolate, we have one additional degree of freedom. The interpolation function is a polynomial of degree 1 (respectively 3) for the cases $g = 1$ (respectively $g = 2$). Such interpolation functions are considered by Leitenberger in his paper[4], and were first considered by Jacobi[2] in connection with Abel's Theorem. Leitenberger uses these interpolation functions to derive equations for the group law in the $g = 2$ case, but his methods do not appear to generalize. Our derivation, which will be more in line with the polynomial division techniques used in the paper [1] of Costello and Lauter, will achieve explicit formulas for all positive integers g.

5.4.1 Group Law on a Dense Open Set

Recall that, by the discussion in Section 5.2, we are working to describe the group law on the open dense set Z described in Theorem 5.1. The points of Z are in bijection with unordered tuples of g points on C_1, none of which are conjugates of each other. The variety Z is described by $2g + 1$ equations in the coefficients of three polynomials u, v and w, however the coefficients of w are entirely determined by those of u and v so we may ignore w and simply use the polynomials u and v.

The derivation takes the form of a series of three lemmas. The first of these, Lemma 5.4, derives equations for the interpolation function p/q in terms of the coefficients of two pairs (u, v) and (u', v') representing divisors D and D'. The second lemma, Lemma 5.5, uses the relationship between p/q and f to find formulas for the coefficients of a degree g monic polynomial u'' representing the x-coordinates of a divisor D'' which corresponds to the sum $[D] + [D']$. The third and final lemma solves for the coefficients of the polynomial v'' in terms of the coefficients of u'' and p/q.

Lemma 5.4. *Suppose that (u, v) and (u', v') describe divisors $D = \sum_{i=1}^{g} P_i$ and $D' = \sum_{i=1}^{g} P_i'$ respectively, such that the $2g$ summands in $D + D'$ have distinct x-coordinates. Let $a = (3g - \varepsilon)/2$ and $b = (g - 2 + \varepsilon)/2$ as before, and define $d = (g - \varepsilon)/2$. Define the quantities:*

$$\kappa_{i,\ell} = \sum_{\ell \le m \le d} u_{i-d+m} \left(\sum_{\sigma \in S_{m-\ell}} (-1)^{|\sigma|} \prod_{r=1}^{|\sigma|} u_{g-\sigma_r} \right)$$

$$\kappa'_{i,\ell} = \sum_{\ell \le m \le d} u'_{i-d+m} \left(\sum_{\sigma \in S_{m-\ell}} (-1)^{|\sigma|} \prod_{r=1}^{|\sigma|} u'_{g-\sigma_r} \right)$$

$$\lambda_{i,j} = -v_{i-j} + \sum_{0 \le \ell \le d} v_{(a-j)-\ell} \kappa_{i,\ell}$$

$$\lambda'_{i,j} = -v'_{i-j} + \sum_{0 \le \ell \le d} v'_{(a-j)-\ell} \kappa'_{i,\ell}$$

Then the requirement that a rational function of the form in (2) interpolates the divisors D and D' induces the following system of linear relations on the coefficients of p/q:

$$\left(\begin{array}{ccc|ccc} \kappa_{0,d}-\kappa'_{0,d} & \cdots & \kappa_{0,0}-\kappa'_{0,0} & \lambda'_{0,1}-\lambda_{0,1} & \cdots & \lambda'_{0,b}-\lambda_{0,b} \\ \kappa_{1,d}-\kappa'_{1,d} & \cdots & \kappa_{1,0}-\kappa'_{1,0} & \lambda'_{1,1}-\lambda_{1,1} & \cdots & \lambda'_{1,b}-\lambda_{1,b} \\ \kappa_{2,d}-\kappa'_{2,d} & \cdots & \kappa_{2,0}-\kappa'_{2,0} & \lambda'_{2,1}-\lambda_{2,1} & \cdots & \lambda'_{2,b}-\lambda_{2,b} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \kappa_{g-2,d}-\kappa'_{g-2,d} & \cdots & \kappa_{g-2,0}-\kappa'_{g-2,0} & \lambda'_{g-2,1}-\lambda_{g-2,1} & \cdots & \lambda'_{g-2,b}-\lambda_{g-2,b} \\ \kappa_{g-1,d}-\kappa'_{g-1,d} & \cdots & \kappa_{g-1,0}-\kappa'_{g-1,0} & \lambda'_{g-1,1}-\lambda_{g-1,1} & \cdots & \lambda'_{g-1,b}-\lambda_{g-1,b} \end{array}\right) \left(\begin{array}{c} p_g/q_0 \\ \vdots \\ p_a/q_0 \\ \hline q_1/q_0 \\ \vdots \\ q_b/q_0 \end{array}\right) = \left(\begin{array}{c} \lambda_{0,0}-\lambda'_{0,0} \\ \lambda_{1,0}-\lambda'_{1,0} \\ \lambda_{2,0}-\lambda'_{2,0} \\ \vdots \\ \lambda_{g-2,0}-\lambda'_{g-2,0} \\ \lambda_{g-1,0}-\lambda'_{g-1,0} \end{array}\right)$$

$$p_i = \sum_{\ell=0}^{d} p_{a-\ell}\kappa_{i,\ell} - \sum_{j=1}^{b} q_j\lambda_{i,j} - q_0\lambda_{i,0} \qquad\qquad 0 \le i \le g-1$$

Label the $g \times g$ matrix M, and let M_j denote the matrix obtained from M by replacing the jth column with the solution vector on the right. Then on a dense open set of $Z \times Z$ these relations determine an interpolation function p/q with the desired properties via the equations

$$\begin{aligned} p_{g+i} &= \det(M_{1+i}) && 0 \le i \le d+1 \\ q_0 &= \det(M) \\ q_i &= \det(M_{1+d+i}) && 1 \le i \le b \\ p_i &= \sum_{\ell=0}^{d} \det(M_{1+(d-\ell)})\kappa_{i,\ell} - \sum_{j=1}^{b} \det(M_{1+d+j})\lambda_{i,j} - \det(M)\lambda_{i,0} && 0 \le i \le g-1 \end{aligned}$$

Proof. Label the points $P_i = (x_i, y_i)$ and $P'_i = (x'_i, y'_i)$. The requirement that p/q interpolates the points of D is equivalent to the condition that $p/q \equiv v \pmod{u}$, and since we require that q does not vanish at any x_i, to the condition that $p - qv \equiv 0 \pmod{u}$. By expanding this relation, we see that this condition is equivalent to

$$\sum_{i\ge 0} \alpha_i x^i := \sum_{i \ge 0} \left(p_i - \sum_{j=0}^{b} q_j v_{i-j} \right) x^i \equiv 0 \pmod{u}.$$

To find appropriate linear relations for the coefficients of p/q, we apply Lemma 5.2 with $\beta_i = u_i$, $n = d = a - g = (g - \varepsilon)/2$ and $k = a$. We therefore get for $0 \le i \le g-1$ the relations

$$\begin{aligned} 0 &= \alpha_i - \sum_{\ell=0}^{d} \alpha_{a-\ell}\kappa_{i,\ell} \\ &= \left(p_i - \sum_{j=0}^{b} q_j v_{i-j} \right) - \sum_{\ell=0}^{d} \left(p_{a-\ell} - \sum_{j=0}^{b} q_j v_{a-\ell-j} \right) \kappa_{i,\ell} \\ &= p_i - \sum_{\ell=0}^{d} p_{a-\ell}\kappa_{i,\ell} + \sum_{j=1}^{b} q_j \left(-v_{i-j} + \sum_{\ell=0}^{d} v_{(a-j)-\ell}\kappa_{i,\ell} \right) + q_0 \left(-v_i + \sum_{\ell=0}^{d} v_{a-\ell}\kappa_{i,\ell} \right) \end{aligned}$$

Using the notation defined in the statement of the Lemma, this reads

$$0 = p_i - \sum_{\ell=0}^{d} p_{a-\ell}\kappa_{i,\ell} + \sum_{j=1}^{b} q_j\lambda_{i,j} + q_0\lambda_{i,0} \qquad 0 \le i \le g-1. \tag{3}$$

The analogous process for the primed variables gives us the same equations with $\kappa'_{i,\ell}$ replacing $\kappa_{i,\ell}$ and $\lambda'_{i,j}$ replacing $\lambda_{i,j}$. Therefore, taking differences we see that in order for p/q to have the desired form, we must have

$$0 = \sum_{\ell=0}^{d} p_{a-\ell}(\kappa_{i,\ell} - \kappa'_{i,\ell}) + \sum_{j=1}^{b} q_j(\lambda'_{i,j} - \lambda_{i,j}) + q_0(\lambda'_{i,0} - \lambda_{i,0}) \qquad 0 \le i \le g-1. \tag{4}$$

Equation (4) gives the matrix equation after dividing through by q_0, and equation (3) gives the desired relation for p_i for $0 \le i \le g-1$. The formulas for the coefficients of p/q then follow by Cramer's rule, assuming that the linear system is non-degenerate.

We now show that the matrix M is non-degenerate on a dense open set of $Z \times Z$. Note that because $Z \times Z$ is irreducible and $\det(M) \ne 0$ is an open condition, it suffices to show that the set of points for which M is non-degenerate is non-empty. Note that the conditions $p/q \equiv v \pmod{u}$ and $p/q \equiv v' \pmod{u'}$ uniquely determine p/q up to a projective rescaling, since if $\widetilde{p}/\widetilde{q}$ is another interpolation function satisfying the same conditions we have $p\widetilde{q} \equiv \widetilde{p}q \pmod{uu'}$ and hence $p\widetilde{q} = \widetilde{p}q$ since $\deg(p\widetilde{q} - \widetilde{p}q) = 2g-1 < 2g = \deg(uu')$. Since the derived linear system is equivalent to the condition that p/q is an interpolation function, the statement that the system is solvable on an open dense set of $Z \times Z$ amounts to the statement that at least one such interpolation function exists, which is clearly true.

□

Lemma 5.5. *Continue with the notation and assumptions of Lemma 5.4. Define the quantities:*

$$\begin{aligned}
\rho &= p_a^2(1-\varepsilon) - f_{2g+1}q_b^2\varepsilon \\
\omega_j &= \sum_{i=0}^{j} u_i u'_{j-i} \\
\eta_k &= \sum_{j=0}^{k}\left(p_j p_{k-j} - f_{k-j}\sum_{i=0}^{j} q_i q_{j-i}\right)
\end{aligned}$$

Suppose the sum $[D - g\infty] + [D' - g\infty]$ is represented by a divisor $D'' - g\infty$ with $D'' = \sum_{i=1}^{g} P''_i$ and P''_i a point on C_1 for $1 \le i \le g$. Then if (u'', v'') is the pair of polynomials representing D'', the coordinates of u'' are given by:

$$u''_j = \sum_{i=0}^{j} \frac{\eta_i}{\rho\omega_0} \sum_{\sigma \in S_{j-i}} \frac{(-1)^{|\sigma|}}{\omega_0^{|\sigma|}} \prod_{r=1}^{|\sigma|} \omega_{\sigma_r}.$$

Proof. The polynomials p and q in Lemma 5.4 were computed to satisfy $p - qv \equiv 0 \pmod{u}$. Furthermore, the pair (u, v) satisfies $f - v^2 \equiv 0 \pmod{u}$. Together these two facts imply that

$$p^2 - fq^2 \equiv p^2 - v^2q^2 \equiv (p-qv)^2 - 2qv(p-qv) \equiv 0 + 0 \equiv 0 \pmod{u}.$$

The analogous fact is true for u'. Since u and u' have distinct roots, we see that $uu'|(p^2-fq^2)$. The polynomial $p^2 - fq^2$ has degree $\max\{2a, 2(b+g)+1\} = 3g$ with leading coefficient ρ, and so we may write $p^2 - fq^2 = \rho uu'u''$ where u'' is monic of degree g and the roots x''_i of u'' are such that there exists $Q''_i = (x''_i, y''_i)$ on C_1 satisfying $p(x''_i) - y''_i q(x''_i) = 0$.

Viewing $p - yq$ as a function on C, it has zeros precisely at the roots of the polynomial $p^2 - fq^2$, and so has $3g$ of them (with multiplicity) corresponding to the roots of the polynomials u, u' and u''. As the number of zeros on C must equal the number of poles, the function $p - yq$ must then have a pole of order $3g$ at ∞, and so we find that

$$(D - g\infty) + (D' - g\infty) \sim -\sum_{i=1}^{g} Q_i + g\infty.$$

The relations $Q_i + \iota(Q_i) \sim 2\infty$ then give us that

$$(D - g\infty) + (D' - g\infty) \sim \sum_{i=1}^{g} \iota(Q_i) - g\infty.$$

So we see that if we take $P''_i = (x''_i, -y''_i)$, then u'' satisfies the hypotheses of the theorem.

To solve for the coefficients u''_j, we expand the relation $p^2 - fq^2 = \rho uu'u''$ and equate coefficients. This gives us:

$$\sum_{j=0}^{k} \left(p_j p_{k-j} - f_{k-j} \sum_{i=0}^{j} q_i q_{j-i} \right) = \rho \sum_{j=0}^{k} u''_j \left(\sum_{i=0}^{k-j} u_i u'_{(k-j)-i} \right),$$

or simply $\eta_k/\rho = \sum_{j=0}^{k} u''_j \omega_{k-j}$. Applying Lemma 5.3 gives the result. □

Remark. The formulas in Lemma 5.5 are defined provided that $\omega_0 \neq 0$ and $\rho \neq 0$. The first condition reduces to the statement that $x_i \neq 0$ and $x'_i \neq 0$ for all $1 \leq i \leq g$, and the second says that either $p_a \neq 0$ or $q_b \neq 0$ depending on the parity of g. This latter case again reduces to the non-vanishing of a certain matrix determinant as defined in Lemma 5.4, which again defines a dense open subset of $Z \times Z$ for similar reasons as before.

Lemma 5.6. *Continue with the notation and assumptions in Lemmas 5.4 and 5.5. Define the quantities:*

$$\begin{aligned}
\kappa''_{i,\ell} &= \sum_{\ell \leq m \leq d} u''_{i-d+m} \left(\sum_{\sigma \in S_{m-\ell}} (-1)^{|\sigma|} \prod_{r=1}^{|\sigma|} u''_{g-\sigma_r} \right) \\
\tau_{i,s} &= -\sum_{m=g+1-\varepsilon}^{d+s} q_{a-m} \kappa''_{i,m-s} \\
\mu_i &= -p_i + \sum_{0 \leq \ell \leq d} p_{a-\ell} \kappa''_{i,\ell}
\end{aligned}$$

Then we have

$$\left[\begin{pmatrix} q_0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ q_1 & q_0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ q_b & q_{b-1} & \cdots & q_0 & 0 & \cdots & 0 \\ 0 & q_b & \cdots & q_1 & q_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & q_b & q_{b-1} & \cdots & q_0 \end{pmatrix} + \begin{pmatrix} 0 & \cdots & 0 & \tau_{0,d+1} & \cdots & \tau_{0,g-1} \\ 0 & \cdots & 0 & \tau_{1,d+1} & \cdots & \tau_{1,g-1} \\ 0 & \cdots & 0 & \tau_{2,d+1} & \cdots & \tau_{2,g-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \tau_{g-2,d+1} & \cdots & \tau_{g-2,g-1} \\ 0 & \cdots & 0 & \tau_{g-1,d+1} & \cdots & \tau_{g-1,g-1} \end{pmatrix}\right] \begin{pmatrix} v''_0 \\ v''_1 \\ v''_2 \\ \vdots \\ \vdots \\ v''_{g-2} \\ v''_{g-1} \end{pmatrix} = \begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \vdots \\ \vdots \\ \mu_{g-2} \\ \mu_{g-1} \end{pmatrix}$$

and so

$$v''_i = \frac{\det(Q+T)_{1+i}}{\det(Q+T)},$$

where $Q+T$ is the sum of the two matrices between the square brackets, with Q denoting the first matrix and T the second, and $(Q+T)_j$ is the matrix obtained by replacing the jth column of $Q+T$ with the solution vector on the right.

Proof. As with the pairs (u,v) and (u',v') we have a relation $p+qv'' \equiv 0 \pmod{u''}$, this time with a sign change to account for the sign of the y-coordinate in the points P''_i. Proceeding as in Lemma 5.4, we have the equations

$$\begin{aligned} 0 &= p_i - \sum_{\ell=0}^{d} p_{a-\ell}\kappa''_{i,\ell} + \sum_{j=0}^{b} q_j \left(v''_{i-j} - \sum_{\ell=0}^{d} v''_{(a-j)-\ell}\kappa''_{i,\ell} \right) \\ &= -\mu_i + \left(\sum_{j=0}^{g-1} v''_j q_{i-j} \right) - \left(\sum_{j=0}^{b}\sum_{\ell=0}^{d} v''_{(a-j)-\ell} q_j \kappa''_{i,\ell} \right) \end{aligned}$$

To extract the coefficient of $v''_{(a-j)-\ell}$ in the second summation on the last line, we use the change of indices $s=(a-j)-\ell$ and $m=a-j=s+\ell$. As s is the index of v'' we have the bound $s \le g-1$, and from the equality $s=(a-j)-\ell$ we get $s \ge a-b-d = d+1$. Then for fixed s, we have $m \le s+d$ and $m \ge a-b = g+1-\varepsilon$. This gives us the equality

$$\sum_{j=0}^{g-1} v''_j q_{i-j} + \sum_{s=d+1}^{g-1} v''_s \left(- \sum_{m=g+1-\varepsilon}^{s+d} q_{a-m}\kappa''_{i,m-s} \right) = \mu_i,$$

from which the matrix equation follows. The formula for v''_i then follows from Cramer's rule. □

Remark. To understand when the above formulas successfully determine v'' (in particular, when $\det(Q+T)$ does not vanish), note that if the roots of u'' are distinct and do not coincide with the roots of q, then the relationship $p+qv'' \equiv 0 \pmod{u''}$ determines the value of the degree $g-1$ polynomial v'' at g distinct points, which suffices to determine it. These conditions on u'' and q may be expressed by asserting the non-vanishing of certain discriminant and resultant polynomials, so we once again see that the desired relations hold on some dense open set of $Z \times Z$.

Theorem 5.7. *There exist explicit polynomial and rational functions describing the group law on an open dense set of Jac(C).*

Proof. This is merely a summary of Lemmas 5.4, 5.5 and 5.6 and their associated remarks. □

5.5 Conclusion

The formulas we have described have some drawbacks compared to the usual methods for computing the group law. For one, the use of inversions and the requirements on both Z and the divisors represented by (u, v) and (u', v') limit the scope of the formulas somewhat, and one might suspect that handling the various edge cases would make them difficult to use. In fact, this is generally not so serious, since most applications of abelian variety arithmetic in cryptography or computer science require the use of finite fields of exponentially large prime characteristic r, and if one heuristically models each inequality defining the validity of the group law as holding with probability $(r-1)/r$, then one concludes that encountering most such edge cases is exponentially unlikely in practice.

Another objection is that the formulas do not extend to the important case of doubling. This is already the case when $g = 1$, which as shown in Appendix A is really just a case of the usual elliptic curve group law, where the chord-based addition formula only holds when adding two distinct points and one must instead use a tangent line in the degenerate case. A similar phenomenon holds here, in that when doubling points the relations in Lemma 5.4 are always dependent, and one must use additional relations which enforce a higher-order agreement between the interpolation function p/q and the function y on C to determine p/q. This is done for the case $g = 2$ in the work of Costello and Lauter, but we do not pursue it here as the approach grows considerably in complexity with g. However we may simply observe that one can circumvent this issue entirely by simply computing a scaling of the form $2[D]$ as a sum of the form $(([D] + [E]) + [D]) - [E]$, where $[E]$ is an appropriate "dummy" divisor class chosen at random.

Another objection is that the formulas use expressions that grow quickly in complexity, requiring sums over compositions and matrix determinants, and so are unlikely to be competitive with reduction-based approaches for large g. While this is certain to be true asymptotically, the $g = 1$ and $g = 2$ cases (that of the elliptic curve group law and the work of Costello and Lauter respectively) are quite efficient, and a heavily unoptimized implementation by the author[14] was able to use the formulas for Jacobian arithmetic up to $g = 8$ without much difficulty. We note that the general expressions that appear in Lemmas 5.4 and 5.6 obscure the fact that many of the terms that appear in these expressions are often zero (either due to an abundance of zeros in the coefficients of f or because the indices fall out of range), and so in practice the complexity may be overstated. The case where $g = 3$ in particular may benefit from some hand-optimization.

We also wish to emphasize the inherent value in explicit constructions. The usual approach to constructing the Jacobian of a curve as an abelian variety uses the language of schemes and representable functors, which is convenient for many theoretical purposes, but carries with it associated baggage that can make it difficult to apply. For this reason, the use of higher-dimensional abelian varieties in cryptography and computer science can often be traced back to either the hyperelliptic Jacobian construction appearing in Mumford's Lectures on Theta, or the work of Flynn, even though it is unlikely those authors had any particular computational application in mind. These constructions are messy, but they can be made practical, whereas the author is unaware of any computational applications of the usual scheme-theoretic approach.

6 References

[1] Craig Costello and Kristin Lauter. Group Law Computations on Jacobians of Hyperelliptic Curves. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography*, pages 92–117, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[2] C G. J. Jacobi. Über die Darstellung einer Reihe gegebner Werthe durch eine gebrochne rationale Function. 1846:127–156, 01 1846.

[3] David Grant. Formal groups in genus two. *Journal für die reine und angewandte Mathematik*, 411:96–121, 1990.

[4] Frank Leitenberger. About the group law for the Jacobi variety of a hyperelliptic curve. *Beitrage zur Algebra und Geometrie*, 10 2005.

[5] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[6] James S. Milne. Jacobian varieties (january 4, 2018), 2018. Available at www.jmilne.org/math/.

[7] David Mumford. On the Equations Defining Abelian Varieties. I. *Inventiones Mathematicae*, 1, 12 1966.

[8] David Mumford. On the Equations Defining Abelian Varieties. II. *Inventiones Mathematicae*, 3, 01 1967.

[9] David Mumford. On the Equations Defining Abelian Varieties. III. *Inventiones Mathematicae*, 3, 01 1967.

[10] David Mumford. *Tata Lectures on Theta II.* 1984.

[11] Martin Orr. Hodge Structures and Abelian Varieties, 2010. Retrieved from the blog at www.martinorr.name.

[12] Martin Orr. Dual Abelian Varieties Over The Complex Numbers, 2011. Retrieved from the blog at www.martinorr.name.

[13] David Urbanik. A Brief Introduction to Schemes and Sheaves (July, 2018), 2018. Available at csclub.uwaterloo.ca/ dburbani/.

[14] David Urbanik. Explicit Jacobian Arithmetic in any Genus g (Source Code). `https://csclub.uwaterloo.ca/~dburbani/work/jacarith_dburbani_August2018.zip`, 2018.

[15] E V Flynn. The group law on the Jacobian of a curve of genus 2. 1993, 01 1993.

[16] Eugene Victor Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. 107:425 – 441, 05 1990.

A The Elliptic Curve Case

As an illustrative example, we demonstrate that the above derivation gives the usual group law in the case $g = 1$. The equation defining C_1 is

$$y^2 = f(x) = x^3 + f_2x^2 + f_1x + f_0.$$

A pair representing the divisor $D = P$ looks like $(u, v) = (x + u_0, v_0)$. The open set Z is then described by the equations (1), which are

$$\begin{aligned} f_0 - v_0^2 &= u_0w_0 \\ f_1 &= u_0w_1 + w_0 \\ f_2 &= u_0 + w_1. \end{aligned}$$

Using the second equation we may eliminate w_0, and using the third equation we may further eliminate w_1, resulting in a curve defined by

$$\begin{aligned} f_0 - v_0^2 &= u_0(f_1 - u_0(f_2 - u_0)) \\ f_0 - v_0^2 &= u_0f_1 - u_0^2f_2 + u_0^3 \\ v_0^2 &= (-u_0)^3 + f_2(-u_0)^2 + f_1(-u_0) + f_0, \end{aligned}$$

which is evidently isomorphic to C_1.

Now let $D = P$, $D' = P'$, $(u, v) = (x + u_0, v_0)$ and $(u', v') = (x + u_0', v_0')$. Following the notation in Lemma 3 we have $\varepsilon = 1$ and so $a = 1$ and $b = 0$. Hence the interpolation function p/q is of the form $(p_1/q_0)x + (p_0/q_0)$. The matrix in Lemma 3 is 1×1 with a single entry

$$\kappa_{0,0} - \kappa'_{0,0} = u_0 - u_0',$$

and the solution vector is also 1×1 with a single entry

$$\lambda_{0,0} - \lambda'_{0,0} = v_0' - v_0.$$

We therefore get, from the formulas in Lemma 5.4, that

$$\begin{aligned} p_1 &= v_0' - v_0 \\ q_0 &= u_0 - u_0' \\ p_0 &= (v_0' - v_0)u_0 - (u_0 - u_0')(-v_0), \end{aligned}$$

and hence

$$\frac{p(x)}{q(x)} = \frac{v_0' - v_0}{u_0 - u_0'}x + \frac{v_0' - v_0}{u_0 - u_0'}u_0 + v_0.$$

One easily checks that p/q is a line through the points $(-u_0, v_0)$ and $(-u_0', v_0')$.

Continuing with Lemma 5.5, we see that

$$u_0'' = \frac{p_0^2 - f_0q_0^2}{-q_0^2u_0u_0'}$$

A long but straightforward calculation shows that $u_0'' = -\lambda^2 + f_2 - u_0 - u_1$, where $\lambda = (v_0' - v_0)/(u_0 - u_0')$. This agrees with the usual formulas for the elliptic curve group law for a Weirstrass form elliptic curve. Note that u_0'' is the negative of the usual x-coordinate here. Then, applying Lemma 5.6 we get that

$$\begin{aligned} v_0'' &= \frac{\mu_0}{q_0} \\ &= \frac{-p_0 + p_1 \kappa_{0,0}''}{q_0} \\ &= -\lambda u_0 + \lambda u_0'' - v_0, \end{aligned}$$

which also agrees with the usual formulas.