Scheme Theory & Weak Mordell–Weil for Elliptic Curves Over Number Fields

Carl-Fredrik Lidgren

Abstract

We provide an introduction to scheme-theoretic algebraic geometry, which studies spaces that are in essence locally solutions to systems of polynomial equations, and prove the weak Mordell–Weil theorem. The weak Mordell–Weil theorem states that for an elliptic curve E over a number field K, the quotient $E(K)/mE(K)$ is finite for all $m \geq 2$. The proof is adapted from a proof in the language of classical varieties, and uses some theorems from algebraic number theory (e.g. Hermite–Minkowski).

Acknowledgements

I would like to thank my advisor Oscar Marmon for his useful comments, providing good reference material, helping me understand the material, and helping me adjust statments of various things into the language used in the thesis. I would also like to thank my examiner Arne Meurman for reading and examining the thesis, and in doing so identifying errors that needed fixing, and for his overall comments on my work.

Populärvetenskaplig Sammanfattning

I många sammanhang är man intresserad av lösningar till ekvationer eller den geometriska strukturen av lösningarna till en mängd ekvationer, speciellt då det inte går att ange dem explicit. Även enkla exempel av detta finns: ekvationen $x^2 + y^2 = 1$ definierar en cirkel, men det går inte att beskriva alla reella tal som löser den utan att man använder transcendentala funktioner. Algebraisk geometri handlar då om att försöka lära sig om den geometriska strukturen av lösningarna till (system av) sådana ekvationer, nämligen de som ges av polynom, med hjälp av verktyg från modern abstrakt algebra. Inom modern algebraisk geometri studerar man objekt som heter *scheman*. Scheman är geometriska rum som i princip definieras "lokalt" av lösningar till polynomekvationer, vilket tillåter mycket flexibilitet inom de beteenden man kan fånga med dem.

Nära besläktat med algebraisk geometri är ett område som kallas aritmetisk geometri, vilket kan ses som korsningen mellan algebraisk geometri och talteori. Man är då främst intresserad av att lära sig om lösningar inom (generaliseringar av) heltalen eller rationella talen. Elliptiska kurvor (som har väldigt lite att göra med ellipser) är ofta bra exempel av scheman som är enkla nog att de går att studera men som är komplicerade nog att ha intressanta resultat. Ett mycket bemärkt sådant resultat är *Mordell–Weil* satsen, som angår *gruppstrukturen* av rationella punkterna på kurvan. En elliptisk kurva, vilket per definition ges av en ekvation $y^2 = x^3 + ax + b$, är speciell inom scheman eftersom den kommer med en regel, vilket man kallar en gruppregel, som låter en kombinera två punkter P och Q för att forma en punkt $P + Q$. Mordell–Weil satsen ger då en viss beskrivning av hur gruppstrukturen ser ut. Detta examensarbete angår en lite svagare version av Mordell–Weil satsen.

Contents

1 Introduction

Algebraic geometry is a field that studies (vast generalizations of) systems of polynomial equations using both tools adapted from geometric subjects, such as topology and differential geometry, and tools from commutative algebra. In essence, it acts as a method to turn certain geometric problems (so long as they can be stated in terms of polynomial equations) into algebraic ones, and vice-versa. One typical area of application is within number theory, where one is often interested in the structure of rational (or integer) solutions to diophantine equations, and potentially the most famous example of this is Fermat's last theorem regarding solutions to $x^p + y^p = z^p$ with p prime. Generally, one calls this hybrid of algebraic geometry and number theory "arithmetic geometry."

The purpose of this thesis is two-fold: to present the modern scheme-theoretic version of algebraic geometry, capturing as many of the essential details as possible, and then proving (or at least giving a very detailed sketch of a proof of) a partial version of a particularly celebrated theorem in arithmetic geometry, namely the *Mordell–Weil theorem for elliptic curves.* Elliptic curves are projective curves of a particular type, which can be shown to be given by equations of the form $y^2 = x^3 + ax + b$, and the Mordell–Weil theorem concerns the structure of the rational points on this curve. In particular, the rational points of an elliptic curve form an Abelian group, and the theorem states that this group is finitely generated. The secondary goal of this thesis is then to prove the *weak* Mordell–Weil theorem, which states that the quotient of the group of rational points by any integer greater than two is finite.

The structure of the thesis is as follows: Section 2 describes the scheme-theoretic language that makes up modern algebraic geometry (e.g. how schemes are defined, the relation to sheaves, intuition related to these objects, etc.), along with any major properties of schemes that will be needed for later sections. Section 3 covers what we will need to properly define and derive properties of elliptic curves, which includes divisors on schemes, sheaf cohomology, Riemann–Roch and how one uses it to define the genus of a curve, and how one reduces a scheme modulo p (or more general operations of that sort).

Section 4 gives the motivation for and proof of the weak Mordell–Weil theorem. In particular, we state and prove the *descent* theorem in Subsection 4.1, which explains why the weak Mordell–Weil theorem is of interest. In Subsection 4.2 we briefly go over some aspects of algebraic number theory that we need in the proof of weak Mordell–Weil, such as the notion of an *unramified* extension of number fields.

The content of the thesis is an amalgamation of information taken primarily from [Liu10], [Sil09], [Har77], [Stacks], [Vak17], and [Neu99], and so (unless otherwise specified) it should be assumed that any proof or statement is adapted from (or based on a statement from) one of these. In particular, the information of scheme-theoretic algebraic geometry came from [Liu10], [Har77], [Stacks], and [Vak17], roughly in order of proportion. The proof of Mordell–Weil is adapted from the more classically oriented one (i.e. based on classical algebraic varieties) provided in [Sil09], and a large part of the thesis is dedicated to translating the proofs and required concepts here to a more modern context (which was partially assisted by the supplementary lecture notes of Pete Clark, [Cla12]). Finally, the algebraic number theory used in a particular step of the proof of Mordell–Weil is sourced from [Neu99], and the information on homological algebra in Subsection 3.1 is based on [Wei95].

For space, time, and complexity reasons, a number of proofs of various lemmas, propositions, and theorems (particularly in Sections 2 & 3) are ommited (or, more accurately, are offloaded to one of the above sources). The ones considered to be worth keeping in (either for demonstrative purposes, for intuition, or some other reason) are still included. Similarly, many relatively advanced topics will simply be taken as prerequisites. In particular, this thesis assumes a fairly good understanding of and comfort with commutative algebra, knowledge of basic concepts and definitions in Galois theory and field theory, a working understanding of the language of category theory, knowledge of and understanding of basic notions of topology, as well as enough knowledge of surrounding areas (e.g. complex analysis, differential geometry, number theory, etc.) to derive intuition from them.

2 Schemes

This section introduces prerequisites in modern algebraic geometry, such as the definition of sheaves, schemes, functions between these, and various general theorems about them. The information is based on a combination of the information contained in [Liu10, Ch. 2, 3], [Vak17], and a little from [Stacks]. The structure is primarily based on that found in [Liu10], but we do not follow the exposition there too closely in all subsections. The subsections on projective schemes (Subsection 2.4) and on properties of schemes and morphisms (Subsections 2.5 & 2.6) are the most heavily based on [Liu10].

2.1 Sheaves

Sheaves are a crucial object of study for algebraic geometry, since they abstract a number of objects and behaviors from more classical geometric scenarios. Therefore, we will briefly summarize their main points.

Definition 2.1. Let X be a topological space. The *category of open sets* of X, $\mathrm{Open}(X)$, is the category whose objects are open sets of X, and where there is exactly one morphism $U \to V$ if and only if $U \subseteq V$.

Definition 2.2. Let X be a topological space. A *presheaf* $\mathcal{F}$ on X with values in a category $\mathcal{C}$ is a functor $\mathcal{F}\colon \mathrm{Open}(X)^{\mathrm{op}} \to \mathcal{C}$. Let $V \subseteq U$ be open sets of X. The induced map $\mathcal{F}(U) \to \mathcal{F}(V)$ is denoted by ρ_{UV} and is called the *restriction map* from U to V. Whenever $\mathcal{C}$ is a concrete category, we call an element $s \in \mathcal{F}(U)$ a *section* of $\mathcal{F}$ over U, and write $s|_V$ instead of $\rho_{UV}(s)$.

Definition 2.3. Let $\mathcal{F}$ be a presheaf on X, and $x \in X$ a point of X. The *stalk* of $\mathcal{F}$ at x, $\mathcal{F}_x$, is defined as

$$\mathcal{F}_x := \varinjlim_{U \ni x} \mathcal{F}(U).$$

For a section $s \in \mathcal{F}(U)$ where $x \in U$, we denote the image of s in $\mathcal{F}_x$ by $[s]_x$ and call it the *germ* of s at x.

Remark 2.4. Explicitly, this is the set of germs of sections of $\mathcal{F}$ at x, i.e. elements of $\mathcal{F}_x$ are pairs $[s, U]$ where $x \in U$, $s \in \mathcal{F}(U)$, and one sets $[s, U] = [t, V]$ if there exists some $W \subseteq U \cap V$ with $x \in W$ such that $s|_W = t|_W$. Hence, stalks model local behavior of sections of $\mathcal{F}$ around the point x.

Definition 2.5. Let $\mathcal{F}$ and $\mathcal{G}$ be presheaves on X. A *morphism of presheaves* $\sigma : \mathcal{F} \to \mathcal{G}$ is given by a collection of maps $\{\sigma_U : \mathcal{F}(U) \to \mathcal{G}(U)\}_{U \in \mathrm{Open}(X)}$ satisfying $\sigma_U \circ \rho_{UV} = \rho_{UV} \circ \sigma_V$, i.e. the following diagram commutes:

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\sigma_U"] \arrow[d, "\rho_{UV}"'] & \mathcal{G}(U) \arrow[d, "\rho_{UV}"] \\
\mathcal{F}(V) \arrow[r, "\sigma_V"] & \mathcal{G}(V)
\end{tikzcd}$$

A morphism of presheaves σ is an *isomorphism* if there exists some map $\sigma' : \mathcal{G} \to \mathcal{F}$ such that $\sigma' \circ \sigma = \mathrm{id}_{\mathcal{F}}$ and $\sigma \circ \sigma' = \mathrm{id}_{\mathcal{G}}$, i.e. if all the maps σ_U are isomorphisms. If such an isomorphism exists, one writes $\mathcal{F} \cong \mathcal{G}$.

Remark 2.6. From here on, we will take the value category $\mathcal{C}$ to be the category **Set** of sets. The theory remains the same if one replaces it with any other "familiar" category (i.e. at least concrete, so that one can talk about sections), most notably the category **CRng** of commutative rings with unit, which is what we will switch to using later.

Definition 2.7. Let $\mathcal{F}$ be a presheaf on X. We say $\mathcal{F}$ is a *sheaf* if it satisfies the following conditions for every open set U and every open cover $\{U_i\}_{i\in I}$ of U:

1. Let $s_i \in \mathcal{F}(U_i)$ be sections of $\mathcal{F}$ such that $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$ for all $i, j \in I$. Then there exists a section $s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$.
2. Let $s, t \in \mathcal{F}(U)$ be sections of $\mathcal{F}$ such that $s|_{U_i} = t|_{U_i}$ for all $i \in I$. Then $s = t$.

A morphism of sheaves is just a morphism of presheaves.

Remark 2.8. The above conditions can be combined into one condition stating that a particular sequence of maps is an equalizer diagram. In particular, a presheaf $\mathcal{F}$ is a sheaf if and only if for every cover $\{U_\lambda\}_{\lambda\in\Lambda}$ of an open set U the diagram

$$\begin{tikzcd} \mathcal{F}(U) \arrow[r] & \prod_{\lambda\in\Lambda}\mathcal{F}(U_\lambda) \arrow[r, shift left] \arrow[r, shift right] & \prod_{\lambda_1\lambda_2\in\Lambda}\mathcal{F}(U_{\lambda_1}\cap U_{\lambda_2}) \end{tikzcd}$$

is an equalizer diagram (see, e.g. [Stacks, Tag 006Z, Tag 00VL, Definition 7.7.1], [Liu10, p. 35, Lemma 2.7], or [Vak17, p. 75, 2.2.7]).

Remark 2.9. The purpose of the sheaf axioms is to ensure that sections behave essentially like functions and in a local manner. It is not hard to find presheaves which do not satisfy these axioms: consider the topological space with two points and the discrete topology, and let $\mathcal{F}$ be the sheaf which assigns to any open set the set $\mathbb{Z}$. Then this fails the first requirement of a sheaf. It should be noted that it is significantly harder to find presheaves that fail the second condition "in the wild." Preheaves that only satisfy the second condition have therefore been given their own name: *separated* presheaves.

It is useful to be able to construct sheaves on a topological space without having to specify exactly what it looks like explicitly. There are two main ways of doing this. The first is sheafification:

Proposition 2.10. *Let $\mathcal{F}$ be a presheaf on X. Then there exists a sheaf $\mathcal{F}^\dagger$ equipped with a morphism of presheaves $\theta\colon \mathcal{F} \to \mathcal{F}^\dagger$ such that for any sheaf $\mathcal{G}$ with a morphism of presheaves $\sigma\colon \mathcal{F} \to \mathcal{G}$ there exists a unique morphism of sheaves $\sigma'\colon \mathcal{F}^\dagger \to \mathcal{G}$ such that $\sigma = \sigma' \circ \theta$, i.e. which makes the following diagram commute:*

$$\begin{tikzcd} \mathcal{F} \arrow[r, "\theta"] \arrow[d, "\sigma"'] & \mathcal{F}^\dagger \arrow[dl, dashed, "\exists!\sigma'"] \\ \mathcal{G} & \end{tikzcd}$$

The sheaf $\mathcal{F}^\dagger$ is called the sheafification of $\mathcal{F}$ or the sheaf associated to $\mathcal{F}$. Furthermore, for all $x \in X$, we have $\mathcal{F}_x \cong \mathcal{F}^\dagger_x$.

Proof. See [Liu10, p. 36, Prop. 2.15], [Har77, p. 64, Prop.-Def. 1.2] or [Stacks, Tag 007X]. There are several constructions of this, but the one that I find the most enlightening is

$$\mathcal{F}^\dagger(U) = \left\{ ([s_x])_{x\in U} \in \prod_{x\in U} \mathcal{F}_x \,\middle|\, \forall x \in U,\, \exists V \subseteq U, s \in \mathcal{O}_X(V),\ \text{s.t. } x \in V \text{ and } \forall y \in V,\, [s_y] = [s]_y \right\}.$$

■

Proposition 2.11. *The sheafification $\mathcal{F}^\dagger$ of $\mathcal{F}$ is unique up to unique isomorphism.*

Proof. Suppose we have two sheaves $\mathcal{F}^\dagger_1$ and $\mathcal{F}^\dagger_2$ which satisfy the universal property given in Proposition 2.10, with structure morphisms θ_1 and θ_2. Then, by the given universal property, we have the commutative diagrams

$$\begin{tikzcd} \mathcal{F} \arrow[r, "\theta_1"] \arrow[d, "\theta_2"'] & \mathcal{F}_1^\dagger \arrow[dl, dashed, "\exists!"] \\ \mathcal{F}_2^\dagger & \end{tikzcd} \quad \begin{tikzcd} \mathcal{F} \arrow[r, "\theta_2"] \arrow[d, "\theta_1"'] & \mathcal{F}_2^\dagger \arrow[dl, dashed, "\exists!"] \\ \mathcal{F}_1^\dagger & \end{tikzcd} \quad \Longrightarrow \quad \begin{tikzcd} \mathcal{F}_1^\dagger & \mathcal{F} \arrow[l, "\theta_1"'] \arrow[r, "\theta_1"] \arrow[d, "\theta_2"'] & \mathcal{F}_1^\dagger \arrow[dl, dashed, "\exists!"] \\ & \mathcal{F}_2^\dagger \arrow[ul, dashed, "\exists!"] & \end{tikzcd}$$

which induces a map $\mathcal{F}_1^\dagger \to \mathcal{F}_1^\dagger$ (and similarly for $\mathcal{F}_2^\dagger$). Furthermore, by the given universal property, we have that the only morphism $\mathcal{F}_i^\dagger \to \mathcal{F}_i^\dagger$ which makes

$$\begin{tikzcd} \mathcal{F} \arrow[r, "\theta_i"] \arrow[d, "\theta_i"'] & \mathcal{F}_i^\dagger \arrow[dl, dashed] \\ \mathcal{F}_i^\dagger & \end{tikzcd}$$

commute is the identity on $\mathcal{F}_i^\dagger$ (since the morphism is unique, and the identity makes the diagram commute). Therefore, we see that the induced maps $\mathcal{F}_1^\dagger \to \mathcal{F}_2^\dagger$ and $\mathcal{F}_2^\dagger \to \mathcal{F}_1^\dagger$ must compose to the identity both ways, and therefore are isomorphisms. Hence $\mathcal{F}_1^\dagger \cong \mathcal{F}_2^\dagger$. Furthermore, this isomorphism is unique by the universal property. $\blacksquare$

Remark 2.12. Using a similar argument to the above, one can also show that if $\mathcal{F}$ is already a sheaf, then $\mathcal{F} \cong \mathcal{F}^\dagger$.

Remark 2.13. Sheafification functions by taking a presheaf and making its behavior "local" in a sense. This is adequately demonstrated by considering the presheaf $\mathcal{F}$ on X given by $\mathcal{F}(U) = \mathbb{Z}$ for all U. This can be thought of as sending U to the collection of constant integer maps on U. The sheafification $\mathcal{F}^\dagger$ then sends U to the collection of *locally* constant integer maps on U. Essentially, sheafification gives you the closest approximation of the given presheaf by a sheaf.

The other way of constructing a sheaf is by constructing it on a basis for the topology on X then extending it to the whole space.

Definition 2.14. Let $\mathcal{B}$ be a basis for the topology on X. A $\mathcal{B}$-sheaf on X is a sheaf except we replace Open(X) with $\mathcal{B}$ in the definition, i.e. it is a functor $\mathcal{B}^{\text{op}} \to \textbf{Set}$ which satisfies the sheaf axioms for open sets in $\mathcal{B}$. If $\mathcal{F}$ is a sheaf on X, denote by $\mathcal{F}|_{\mathcal{B}}$ the $\mathcal{B}$-sheaf given by restricting $\mathcal{F}$ to elements of $\mathcal{B}$.

Remark 2.15. Here we identify the collection $\mathcal{B}$ with the category formed by taking $U \in \mathcal{B}$ as objects and inclusions as morphisms.

Lemma 2.16. *Let $\mathcal{G}$ be a sheaf on X and $\mathcal{B}$ a basis for the topology on X. Then*

$$\mathcal{G}(U) \cong \varprojlim_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{G}(V).$$

Proof. There is an obvious map $f : \mathcal{G}(U) \to \varprojlim_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{G}(V)$ given by $s \mapsto (s|_V)_{V \in \mathcal{B}, V \subseteq U}$. Similarly, there is an obvious map $g \colon \varprojlim_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{G}(V) \to \mathcal{G}(U)$ given by taking a cover $\{V_i\}_{i \in I}$ of U by elements of $\mathcal{B}$ with $V_i \subseteq U$ for all $i \in I$, then sending $(s_V)_{V \subseteq U}$ to the gluing of the s_{V_i} (which exists and is unique by the sheaf axioms). We now just have to show that these compose to the identity. Let $s \in \mathcal{G}(U)$. Then $g(f(s)) = g((s|_V)_{V \subseteq U}) = s$ by the second sheaf axiom. Now let $s = (s_V)_{V \subseteq U} \in \varprojlim_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{G}(V)$. Then $f(g(s)) = (g(s)|_V)_{V \subseteq U} = (s_V)_{V \subseteq U}$. Hence $\mathcal{G}(U) \cong \varprojlim_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{G}(V)$. $\blacksquare$

Proposition 2.17. *Let $\mathcal{F}_0$ be a $\mathcal{B}$-sheaf on X. Then this extends to a sheaf $\mathcal{F}$ on X which is unique up to isomorphism. That is, $\mathcal{F}|_{\mathcal{B}} \cong \mathcal{F}_0$ and if $\mathcal{G}$ is a sheaf on X with $\mathcal{G}|_{\mathcal{B}} \cong \mathcal{F}_0$ then $\mathcal{G} \cong \mathcal{F}$.*

Proof. Define $\mathcal{F}$ by

$$\mathcal{F}(U) := \varprojlim_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{F}_0(V) = \left\{ (s_V) \in \prod_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{F}_0(V) \;\middle|\; \forall V, W \in \mathcal{B},\, W \subseteq V,\, s_V|_W = s_W \right\}.$$

Restriction maps $\mathcal{F}(U) \to \mathcal{F}(V)$ are given by throwing away basis sets not in V, that is $(s_W)_{W \subseteq U} \mapsto (s_W)_{W \subseteq V}$.

We begin by showing that this is a sheaf. Let $\{U_i\}_{i \in I}$ be a cover of an open set U, and let $s_i = (s_{i,V})_{V \subseteq U} \in \mathcal{F}(U_i)$ be sections that agree on intersection. Per definition, this says that for all $V \in \mathcal{B}$ with $V \subseteq U_i \cap U_j$, we have $s_{i,V} = s_{j,V}$. Hence, we can produce the desired section s on U by setting $s_V = s_{i,V}$ if $V \subseteq U_i$, $V \in \mathcal{B}$, and this is well-defined. Hence $\mathcal{F}$ satisfies the first sheaf axiom.

Now let $\{U_i\}_{i \in I}$ be a cover of an open set U, and let $s, t \in \mathcal{F}(U)$ be such that $s|_{U_i} = t|_{U_i}$ for all $i \in I$. Then we see that for all $V \in \mathcal{B}$ with $V \subseteq U$ we have $s_V = t_V$, which means that $s = t$. Hence $\mathcal{F}$ satisfies the second sheaf axiom. Therefore, $\mathcal{F}$ is a sheaf.

Now we want to show that $\mathcal{F}|_{\mathcal{B}} \cong \mathcal{F}_0$. Let $U \in \mathcal{B}$, $s \in \mathcal{F}(U)$. Then the component $s_U \in \mathcal{F}_0(U)$ of s completely determines s by definition, and for every section $t_0 \in \mathcal{F}_0(U)$ there exists an element $t \in \mathcal{F}(U)$ given by $t = (t_0|_V)_{V \subseteq U}$, so $\mathcal{F}(U) \cong \mathcal{F}_0(U)$. Hence we get isomorphisms $\phi_U : \mathcal{F}(U) \xrightarrow{\sim} \mathcal{F}_0(U)$ and $\psi_U : \mathcal{F}_0(U) \xrightarrow{\sim} \mathcal{F}(U)$ for all U given by the preceeding maps, i.e. $\phi_U(s) = s_U$ and $\psi_U(s) = (s|_V)_{V \subseteq U}$. Now we just show that these are compatible with restriction to get the desired isomorphism of $\mathcal{B}$-sheaves. Let $U, V \in \mathcal{B}$, $V \subseteq U$, and $s \in \mathcal{F}(U)$, $t \in \mathcal{F}_0(U)$. Then $\phi(s)|_V = s_U|_V = s_V = \phi(s|_V)$, and $\psi(t)|_V = (t|_W)_{W \subseteq U}|_V = (t|_W)_{W \subseteq V} = \psi(t|_V)$, so ϕ and ψ are morphisms. Hence $\mathcal{F}|_{\mathcal{B}} \cong \mathcal{F}_0$.

Now suppose we have a sheaf $\mathcal{G}$ on X such that $\mathcal{G}|_{\mathcal{B}} \cong \mathcal{F}_0$. Then by the above we also have $\mathcal{G}|_{\mathcal{B}} \cong \mathcal{F}|_{\mathcal{B}}$. By Lemma 2.16, for any open subset $U \subseteq X$, we have

$$\mathcal{G}(U) \cong \varprojlim_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{G}(V) \cong \varprojlim_{V \subseteq U,\, V \in \mathcal{B}} \mathcal{F}_0(V) = \mathcal{F}(U) \implies \mathcal{G} \cong \mathcal{F}.$$

■

Remark 2.18. The above proposition is extremely useful, since it allows us to specify a sheaf by specifying its values on a basis and be guaranteed that this extends in a sufficiently unique way to every open set. This is usually much easier than specifying the value in general, and we will be using it in the construction of affine schemes.

Similarly, one may define maps on a basis:

Proposition 2.19. *Let X be a topological space, and let $\mathcal{F}, \mathcal{G}$ be sheaves on X. Let $\mathcal{B}$ be a basis on X, and let $\{\alpha_U\}_{U \in \mathcal{B}}$ be a collection of maps $\alpha_U : \mathcal{F}(U) \to \mathcal{G}(U)$ which are compatible with restriction maps. Then this extends to a map $\alpha\colon \mathcal{F} \to \mathcal{G}$ of sheaves which is an isomorphism if all the α_U are isomorphisms.*

Proof. By Lemma 2.16, if U is open then $\mathcal{F}(U) \cong \varprojlim_{V \in \mathcal{B}, V \subseteq U} \mathcal{F}(V)$. If $V \in \mathcal{B}$ with $V \subseteq U$, then we get a map $\mathcal{F}(V) \to \mathcal{G}(U)$ by noting that since we have maps $\mathcal{F}(V') \to \mathcal{G}(V')$ for all $V' \in \mathcal{B}$ with $V' \subseteq U$, the universal property of the limit gives that we get a map

$$\mathcal{F}(V) \to \varinjlim_{V' \in \mathcal{B}, V' \subseteq U} \mathcal{G}(V') \cong \mathcal{G}(U).$$

Since this happens in all cases, and since all maps involved commute by typical universal property arguments, we see that we get a well defined map

$$\mathcal{F}(U) \cong \varinjlim_{V\in\mathcal{B}, V\subseteq U} \mathcal{F}(V) \to \varinjlim_{V\in\mathcal{B}, V\subseteq U} \mathcal{G}(V) \cong \mathcal{G}(U)$$

which defines the required map α. If now all α_V are isomorphisms for $V \in \mathcal{B}$, then the middle map in the above is also an isomorphism, giving that α is an isomorphism. ■

Next, we describe two ways to transfer sheaves along continuous maps. To begin, we add that above we have seen that sheaves have morphisms between them with a clear composition law, so they form a category.

Definition 2.20. Let X be a topological space. We denote by $\mathbf{PShf}(X;\mathcal{C})$ the category of presheaves valued on $\mathcal{C}$ on X, and by $\mathbf{Shf}(X;\mathcal{C})$ the category of sheaves valued in $\mathcal{C}$ on X. When the category $\mathcal{C}$ is clear from context, we omit it.

Definition 2.21. Let $f : X \to Y$ be a continuous map, and let $\mathcal{F}$ be a sheaf on X. The *direct image sheaf*, $f_*\mathcal{F}$, is the sheaf on Y given by $f_*\mathcal{F}(U) := \mathcal{F}(f^{-1}(U))$. The induced functor $f_*\colon \mathbf{Shf}(X) \to \mathbf{Shf}(Y)$ is called the *direct image functor*.

The direct image functor transfers sheaves on X to sheaves on Y. Similarly, there is a way to transfer sheaves on Y to sheaves on X, however this is much more complicated. The only way to get open sets out of a continuous map is by taking inverse (i.e. $f^{-1}(U)$ for an open set U), which only allows us to produce the direct image functor. To get open set behavior in Y from X, the best we can do is approximate by taking a colimit over open sets containing $f(U)$ for an open set U of X. This also introduces a problem: the produced presheaf is rarely a sheaf, so we have to sheafify (see Proposition 2.10).

Definition 2.22. Let $f\colon X \to Y$ be a continuous map, and let $\mathcal{F}$ be a sheaf on Y. The *inverse image sheaf*, $f^{-1}\mathcal{F}$, is the sheaf on X given by

$$f^{-1}\mathcal{F} := (U \mapsto \varinjlim_{V\supseteq f(U)} \mathcal{F}(V))^{\dagger}.$$

The induced functor $f^{-1}\colon \mathbf{Shf}(Y) \to \mathbf{Shf}(X)$ is called the *inverse image functor*.

Remark 2.23. One can think of the colimit above as being essentially the same on that is used in the definition of the stalk: if $X = \{*\}$ is a single point with $i\colon X \to Y$ the inclusion of that point into Y (with image $y \in Y$), then $i^{-1}\mathcal{F}(\{*\}) = \mathcal{F}_y$. In fact, this can be taken further:

Proposition 2.24. *Let $f\colon X \to Y$ be a continuous map, let $\mathcal{F}$ be a sheaf on Y, and let $x \in X$. Then $(f^{-1}\mathcal{F})_x = \mathcal{F}_{f(x)}$.*

Proof. See [Stacks, Lemma 008H] or [Liu10, p. 37]. ■

The direct image and inverse image functors are related to each other by being adjoint, i.e. there is a natural isomorphism $\mathrm{Hom}_{\mathbf{Shf}(X)}(f^{-1}\mathcal{F}, \mathcal{G}) \cong \mathrm{Hom}_{\mathbf{Shf}(Y)}(\mathcal{F}, f_*\mathcal{G})$. This essentially states that instead of a "pullback" map $f^{-1}\mathcal{F}(U) \to \mathcal{G}(U)$, one can instead use a map $\mathcal{F}(U) \to f_*\mathcal{G}(U)$, which is useful since the latter is usually many times easier to work with.

The final subject of this subsection will be that of sheaves with values in other important categories, in particular Abelian groups (**Ab**), commutative rings with unit (**CRng**), and R-modules (R-**Mod**) for such a commutative ring R. Note that **Ab** is a special case of R-**Mod** with $R = \mathbb{Z}$.

Essentially, we must answer the question of how one lifts various important operations from these categories to the corresponding categories of sheaves. This question is actually answered, in some sense, by the existence of category theory, since it allows us to define e.g. products in very general situations, including here, using the notion of universal properties. There is a question of the existence of objects satisfying a given universal property (see, e.g., Proposition 2.10 for one such situation), but in general there is some "obvious" choice of object which should intuitively do so, and proving that it does is usually somewhat tedious and uninteresting but not hard. Hence, most of the following definitions should really be propositions, but for the sake of the exposition, they will not be marked as such nor proven. As always, a great resource for a detailed version of everything is given in [Stacks].

Definition 2.25. Let X be a topological space, and let $\mathcal{F}$ be a sheaf with values in one of the above categories or **Set**. A *subsheaf* of $\mathcal{F}$ is a sheaf $\mathcal{G}$ such that $\mathcal{G}(U) \subseteq \mathcal{F}(U)$ for all U.

Remark 2.26. This can be defined in greater generality, though it is entirely unnecessary in our situation.

Definition 2.27. Let X be a topological space, and let $\mathcal{F}$ be a sheaf of commutative rings on X. A *sheaf of ideals* of $\mathcal{F}$ is a sheaf $\mathcal{G}$ such that $\mathcal{G}(U)$ is an ideal of $\mathcal{F}(U)$.

Definition 2.28. Let X be a topological space, and let $\mathcal{F}, \mathcal{G}$ be sheaves with values in a category $\mathcal{C}$, which is one of the above categories. Then one defines

(a) $(\mathcal{F} \times \mathcal{G})(U) = \mathcal{F}(U) \times \mathcal{G}(U)$,
(b) $(\mathcal{F} \oplus \mathcal{G})(U) = \mathcal{F}(U) \oplus \mathcal{G}(U)$,
(c) if $\mathcal{C} = R\text{-}\mathbf{Mod}$, $\mathcal{F} \otimes_R \mathcal{G} = (U \mapsto \mathcal{F}(U) \otimes_R \mathcal{G}(U))^\dagger$,
(d) if $\sigma\colon \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves, $(\ker \sigma)(U) = \ker \sigma_U$,
(e) if $\sigma\colon \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves, $\operatorname{im} \sigma = (U \mapsto \operatorname{im} \sigma_U)^\dagger$,
(f) if $\mathcal{C} = \mathbf{CRng}$, $\mathcal{F}^\times(U) = \mathcal{F}(U)^\times$,
(g) if $\mathcal{C} \neq \mathbf{CRng}$ and $\mathcal{G}$ is a subsheaf of $\mathcal{F}$, or $\mathcal{C} = \mathbf{CRng}$ and $\mathcal{G}$ is a sheaf of ideals of $\mathcal{F}$, then $\mathcal{F}/\mathcal{G} = (U \mapsto \mathcal{F}(U)/\mathcal{G}(U))^\dagger$.

Remark 2.29. One may wonder why, in Definition 2.28, some things require the use of sheafification, and some things do not. The answer to this is actually rather deep, and has ties to some very general theorems in category theory, in particular to do with how limits interplay with other operations. The "general mantra," so to speak, is that "limits commute with limits and right adjoints" (this exact line is written down in [Vak17, p. 54, 1.6.12]). Essentially, the definition of sheafification is such that the functor $\mathcal{F} \mapsto \mathcal{F}^\dagger$ is left adjoint to the forgetful functor that sends a sheaf to itself as a presheaf, i.e. the forgetful functor is a right adjoint. Hence, if we have some diagram of sheaves $\mathcal{F}_i$, and take the limit $\varprojlim_i \mathcal{F}_i$, then the result is the same as if one performed the same limit computation in the category of presheaves. The kernel is an example of a limit construction, and so taking kernel is the same in the category of sheaves as it is in the category of presheaves. With this reasoning, it stands that one has "$(\varprojlim_i \mathcal{F}_i)(U) = \varprojlim_i(\mathcal{F}_i(U))$," though it should be noted that this is not a precise statement. Colimit constructions, however, do not in general behave in this way (they do always satisfy the dual condition, though), and so it makes sense that one has to sheafify. An extreme example of this is that one doesn't need to sheafify a subsheaf (where this is related to limits in the sense that "injectivity," i.e. being a monomorphism, is in some sense a limit-adjacent phenomenon), while one does need to sheafifiy a quotient (where being a quotient, i.e. there being some "surjection" or epimorphism, is related to colimits). One can look into Abelian categories to get more information on this.

Definition 2.30. Let X be a topological space and let $\mathcal{O}$ be a sheaf of commutative rings on X. An *$\mathcal{O}$-module* $\mathcal{F}$ is a sheaf of Abelian groups such that each $\mathcal{F}(U)$ is an $\mathcal{O}(U)$-module, and further, for $V \subseteq U$ open sets, the diagram

$$\begin{tikzcd}
\mathcal{O}(U) \times \mathcal{F}(U) \arrow[r] \arrow[d, "\rho_{UV} \times \rho_{UV}"'] & \mathcal{F}(U) \arrow[d, "\rho_{UV}"] \\
\mathcal{O}(V) \times \mathcal{F}(V) \arrow[r] & \mathcal{F}(V)
\end{tikzcd}$$

commutes, i.e. if $s \in \mathcal{F}(U), c \in \mathcal{O}(U)$, then $(cs)|_V = c|_V s|_V$.

Definition 2.31. Let X and $\mathcal{O}$ be as above, and let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}$-modules. A morphism of $\mathcal{O}$-modules is a morphism of sheaves $\sigma\colon \mathcal{F} \to \mathcal{G}$ such that the diagram

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

is commutative, i.e. if $s \in \mathcal{F}(U), c \in \mathcal{O}(U)$, then $\sigma_U(cs) = c\sigma_U(s)$.

Remark 2.32. Compare the above with how one usually defines R-modules for a (commutative) ring R. Indeed, $\mathcal{O}$-modules generalize sheaves of Abelian groups in the same way that R-modules generalize Abelian groups. One can show that every sheaf of Abelian groups is in a unique way a $\underline{\mathbb{Z}}$-module, where $\underline{\mathbb{Z}} := (U \mapsto \mathbb{Z})^\dagger$ is the sheafification of the constant $\mathbb{Z}$ presheaf.

Definition 2.33. Let X and $\mathcal{O}$ be as above, and let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}$-modules. One defines all operations in Definition 2.28 the same way, except for $\otimes$, which becomes

$$\mathcal{F} \otimes_{\mathcal{O}} \mathcal{G} := (U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}(U)} \mathcal{G}(U))^\dagger.$$

Remark 2.34. We will take a number of things for granted with regards to the operations described above. For example, one can check that if $\sigma\colon \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves, then $(\ker \sigma)_x = \ker \sigma_x$, and similarly for most of the other similar constructions. Another example that is good to highlight is that $(\mathcal{F} \otimes_{\mathcal{O}} \mathcal{G})_x = \mathcal{F}_x \otimes_{\mathcal{O}_x} \mathcal{G}_x$, which one can show using similar reasoning as that used in Remark 2.29, i.e. "colimits commute with colimits and left adjoints," where the stalk is a colimit construction, and $\otimes_{\mathcal{O}_x}$ is left adjoint to $\mathrm{Hom}_{\mathcal{O}_x}$. A last example of this that is important for later is that whenever $\mathcal{F}/\mathcal{G}$ makes sense, one has $(\mathcal{F}/\mathcal{G})_x = \mathcal{F}_x/\mathcal{G}_x$.

2.2 Affine Schemes

The main idea behind the construction of schemes is essentially the same as that of manifolds in topology: one defines some basic "template" spaces which one then glues together to make something more interesting. In the case of manifolds, the basic spaces are $\mathbb{R}^n$, while for schemes, the basic spaces are *affine schemes*. These are usually defined in several steps: first one specifies the underlying set of points, then a topology on it, then one gives a sheaf of commutative rings on it. We begin by specifying the points:

Definition 2.35. Let R be a commutative ring. The *spectrum* of R, $\operatorname{Spec} R$, is the set of prime ideals of R.

Remark 2.36. Why is this something we care about? The main realizations from classical algebraic geometry that allows this definition to make sense are that points in and irreducible subspaces (under a particular topology) of K^n (for K an algebraically closed field) correspond to maximal and prime ideals of $K[x_1, \dots, x_n]$, respectively. Essentially, points correspond to collections of functions which are zero at those points. Hence, one can, starting from $K[x_1, \dots, x_n]$ (i.e. polynomial functions on K^n), reconstruct K^n. Thus, to extend this to more general settings (i.e. where we can regard an element of any commutative ring R as a function on some space), it makes sense to construct a space from at least the maximal ideals of R. One includes the prime ideals because the points they introduce tend to provide quite useful information.

We will now endow $\operatorname{Spec} R$ with a topology. This requires a little bit of work.

Definition 2.37. Let R be a commutative ring, and $I \subseteq R$. The *zero-set* of I, $V(I)$, is the set of all prime ideals containing I. That is,

$$V(I) := \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subseteq \mathfrak{p}\} \subseteq \operatorname{Spec} R.$$

For $f \in R$, we will write $V(f)$ instead of $V((f))$.

Remark 2.38. The idea behind this definition is that if $f \in K[x]$ and $a \in K$, then $f(a) \equiv f(x) \pmod{x-a}$ by the division algorithm, so it is possible to determine the value of a polynomial by reducing modulo an ideal. Taking this to the general case, we can say that for $f \in R$ and $\mathfrak{p} \in \operatorname{Spec} R$, we have "$f(\mathfrak{p}) = 0$" (this notation will be justified later) if $f \in \mathfrak{p}$ since then $f \equiv 0 \pmod{\mathfrak{p}}$.

Proposition 2.39. *Let $I \subseteq R$, and let (I) be the ideal generated by I. Then $V(I) = V((I))$.*

Proof. Suppose $\mathfrak{p} \in V(I)$. Then, for all $f_1, \dots f_j \in I$ and $a_1, \dots, a_j \in R$, we have $f_i \in \mathfrak{p}$ for all $1 \leq i \leq j$, so $\sum_{i=1}^{j} a_i f_i \in \mathfrak{p}$ since $\mathfrak{p}$ is an ideal. Thus, since $(I) = \{c_1 g_1 + \cdots + c_n g_n \mid c_i \in R, g_i \in I\}$, we have that $(I) \subseteq \mathfrak{p}$ so $\mathfrak{p} \in V((I))$. Now suppose $\mathfrak{p} \in V((I))$. Then we have $I \subseteq (I) \subseteq \mathfrak{p}$ so $I \subseteq \mathfrak{p}$. Therefore $\mathfrak{p} \in V(I)$.

Since, from the above, $V(I) \subseteq V((I))$ and $V((I)) \subseteq V(I)$ we conclude that $V(I) = V((I))$. ■

Proposition 2.40. *(a) Let I_1, I_2 be ideals of R. Then $V(I_1) \cup V(I_2) = V(I_1 \cap I_2)$.*
(b) Let $\{I_\lambda\}_{\lambda \in \Lambda}$ be an arbitrary collection of ideals of R. Then $\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V(\sum_{\lambda \in \Lambda} I_\lambda)$.
(c) $V(0) = \operatorname{Spec} R$, and $V(R) = \emptyset$.

Proof. (a) Let $\mathfrak{p} \in V(I_1) \cup V(I_2)$. Then $I_1 \subseteq \mathfrak{p}$ and $I_2 \subseteq \mathfrak{p}$ so clearly $I_1 \cap I_2 \subseteq \mathfrak{p}$. Hence $\mathfrak{p} \in V(I_1 \cap V_2)$. Now let $\mathfrak{p} \in V(I_1 \cap I_2)$ and suppose $I_2 \not\subseteq \mathfrak{p}$. Then there is some $g \in I_2$ such that $g \notin \mathfrak{p}$, but for any $f \in I_1$, we have $fg \in I_1 \cap I_2 \subseteq \mathfrak{p}$, so $f \in \mathfrak{p}$. Hence $I_1 \subseteq \mathfrak{p}$, so $\mathfrak{p} \in V(I_1) \cup V(I_2)$.

(b) Suppose $\mathfrak{p} \in \bigcap_{\lambda \in \Lambda} V(I_\lambda)$. Then we have $I_\lambda \subseteq \mathfrak{p}$ for all $\lambda \in \Lambda$. Since $\mathfrak{p}$ is an ideal, we can take arbitrary sums to get that $\sum_{\lambda \in \Lambda} I_\lambda \subseteq \mathfrak{p}$ so that $\mathfrak{p} \in V(\sum_{\lambda \in \Lambda} I_\lambda)$. Now suppose $\mathfrak{p} \in V(\sum_{\lambda \in \Lambda} I_\lambda)$. Then, since $0 \in I_\lambda$ for each $\lambda \in \Lambda$, we have that $I_\lambda \subseteq \sum_{\lambda \in \Lambda} I_\lambda \subseteq \mathfrak{p}$ so $\mathfrak{p} \in V(I_\lambda)$ for all $\lambda \in \Lambda$. Hence $\mathfrak{p} \in \bigcap_{\lambda \in \Lambda} V(I_\lambda)$.

(c) $(0) = \{0\} \subseteq \mathfrak{p}$ for any prime ideal $\mathfrak{p}$, hence $V(0) = \operatorname{Spec} R$. Similarly, by definition a prime ideal $\mathfrak{p}$ is proper, so that $\mathfrak{p} \subsetneq R$. Therefore $V(R) = \emptyset$. ■

Definition 2.41. The *Zariski topology* on $\operatorname{Spec} R$ is the topology given by setting closed sets to be subsets of the form $V(I)$ for an ideal I of R.

Remark 2.42. Note that Proposition 2.40 says exactly that this is indeed a well defined topology. Furthermore, we will now always take $\operatorname{Spec} R$ to have the Zariski topology on it.

Working with the Zariski topology directly, while not at all impossible, is somewhat tedious. Therefore, we want a nice basis that allows us to easily work with open sets.

Definition 2.43. Let $f \in R$. Then the *distinguished open subset* given by f, $D(f)$, is defined by

$$D(f) := (\operatorname{Spec} R) \backslash V(f).$$

Proposition 2.44. *The distinguished open subsets $D(f)$ form a basis for the Zariski topology.*

Proof. Let $U \subseteq \operatorname{Spec} R$ be an open set. Since open sets are complements of closed sets, we see that $U = (\operatorname{Spec} R)\backslash V(I)$ for some ideal I of R. Since ideals are closed under addition, we have that $I = \sum_{f \in I}(f)$. Hence,

$$\begin{aligned} U = (\operatorname{Spec} R)\backslash V(I) = (\operatorname{Spec} R)\backslash V(\sum_{f\in I}(f)) &= (\operatorname{Spec} R)\backslash(\bigcap_{f\in I} V(f)) \\ &= \bigcup_{f\in I}((\operatorname{Spec} R)\backslash V(f)) = \bigcup_{f\in I} D(f). \end{aligned}$$

■

If we have a map of rings $R \to R'$, then it is sensible to ask whether this lifts to some relation between the spectra of these rings. The answer to this is that one indeed does get a map from this:

Definition 2.45. Let $\varphi\colon R \to R'$ be a homomorphism. Then we denote the map $\operatorname{Spec} R' \to \operatorname{Spec} R$ given by $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$ by $\operatorname{Spec} \varphi$.

Proposition 2.46. *Let $\varphi\colon R \to R'$ be a homomorphism. Then*

(a) $\operatorname{Spec}\varphi\colon \operatorname{Spec} R' \to \operatorname{Spec} R$ *is continuous.*
(b) If ϕ is surjective, then $\operatorname{Spec}\varphi$ *induces a homeomorphism* $\operatorname{Spec} R' \cong V(\ker\varphi) \subseteq \operatorname{Spec} R$.
(c) If $R' = S^{-1}R$ for some multiplicative subset S of R and ϕ is the map induced by localization, then $\operatorname{Spec}\varphi$ *induces a homeomorphism* $\operatorname{Spec} R' \cong \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \emptyset\}$.

Proof. (a) Let $I \subseteq R$ be an ideal. Then

$$\begin{aligned} (\operatorname{Spec}\varphi)^{-1}(V(I)) = \{\mathfrak{p} \in R' \mid \varphi^{-1}(\mathfrak{p}) \in V(I)\} &= \{\mathfrak{p} \in R' \mid I \subseteq \varphi^{-1}(\mathfrak{p})\} \\ &= \{\mathfrak{p} \in R' \mid \varphi(I) \subseteq \mathfrak{p}\} = V((\varphi(I))). \end{aligned}$$

Hence $\operatorname{Spec}\varphi$ sends closed sets to closed sets, and so is continuous.

(b) Since φ is surjective, we have an isomorphism $R/\ker\varphi \cong R'$. Hence, we have a correspondence between the ideals of R' and the ideals containing $\ker\varphi$. This immediately gives a bijective continuous map $\operatorname{Spec} R' \to V(\ker\varphi)$ given by $\operatorname{Spec}\varphi$. Furthermore, note that for an ideal J of R' we have $(\operatorname{Spec}\varphi)(V(J)) = V(\varphi^{-1}(J))$, so this map is closed. Hence we get the homeomorphism.

(c) Note that the prime ideals of $S^{-1}R$ are in correspondence with the primes $\mathfrak{p}$ of R that do not contain any elements of S, i.e. $\mathfrak{p} \cap S = \emptyset$, via the localization map. Hence, we get a continuous bijection $\operatorname{Spec} R' \to \{\mathfrak{p} \mid \mathfrak{p} \cap S = \emptyset\}$, and like the last segment of the proof, we just need to show that this is a closed map. Let $J \subseteq R'$ be an ideal of R'. Then

$$\begin{aligned} (\operatorname{Spec}\varphi)(V(J)) = \{\varphi^{-1}(\mathfrak{p}) \mid \mathfrak{p} \supseteq J\} &= \{\mathfrak{p} \in \operatorname{Spec} R \mid \phi^{-1}(J) \subseteq \mathfrak{p} \text{ and } \varphi(\mathfrak{p}) \in \operatorname{Spec} R'\} \\ &= V(\varphi^{-1}(J)) \cap \operatorname{im}(\operatorname{Spec}\varphi). \end{aligned}$$

Hence $\operatorname{Spec}\varphi$ is closed, and hence a homeomorphism onto its image. ■

Remark 2.47. A very useful special case of (c) in the above is that we get a canonical homeomorphism $\operatorname{Spec} R_f \cong D(f)$. A useful special case of (b) is that we get a canonical homeomorphism $V(I) \cong \operatorname{Spec} R/I$.

We will now endow $\operatorname{Spec} R$ with a sheaf of rings. Here, having the above basis will be helpful, since we will define the value of the sheaf on the distinguished open subsets, which then extends to every open set by Proposition 2.17.

Lemma 2.48. *Let R be a commutative ring. Then $\sqrt{(0)} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$.*

Proof. It is easy to see that if $f \in \sqrt{(0)}$ then $f \in \mathfrak{p}$ for every $\mathfrak{p} \in \operatorname{Spec} R$. This is because if $f^n = 0 \in \mathfrak{p}$ then $f \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Hence we see that $\sqrt{(0)} \subseteq \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$.

To show the converse, suppose we pick some $f \notin \sqrt{(0)}$. Then consider the set $F = \{1, f, f^2, \ldots\}$. The set S of ideals not containing F is non-empty, since $(0) \in S$ (since f is not nilpotent). Therefore, by Zorn's Lemma, there is some ideal $\mathfrak{m}$ maximal in this criterion. We now show that this ideal is prime. Suppose it is not: then there exists $g, h \notin \mathfrak{m}$ such that $gh \in \mathfrak{m}$. We therefore have that the set I_1 of elements $c \in R$ such that $cg \in \mathfrak{m}$ strictly contains $\mathfrak{m}$, i.e. $\mathfrak{m} \subsetneq I_1$, since all $m \in \mathfrak{m}$ are in I_1 and $h \in I_1$. Therefore, since $\mathfrak{m}$ was maximal with respect to not containing f^n for any n, we have that there is some n such that $f^n \in I_1$. This also shows that the set I_2 of elements $c \in R$ such that $cf^n \in \mathfrak{m}$ is an ideal strictly containing $\mathfrak{m}$, so $f^m \in I_2$ for some m. By the definition of I_1 and I_2, $f^n f^m = f^{n+m} \in \mathfrak{m}$, which contradicts the maximality of $\mathfrak{m}$. Hence $\mathfrak{m}$ must be prime, and so we have found a prime ideal not containing f. Hence $\bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p} \subseteq \sqrt{(0)}$.

Combining the two above paragraphs we obtain that $\sqrt{(0)} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$. ■

Lemma 2.49. *Let I be an ideal of R. Then $\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$.*

Proof. First, notice that $V(\sqrt{I}) = V(I)$ since if $f \in \sqrt{I}$, then $f^n \in I \subseteq \mathfrak{p}$, so $f \in \mathfrak{p}$, hence $\sqrt{I} \subseteq \mathfrak{p}$. We therefore also see that $\sqrt{I} \subseteq \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$.

To show the converse, it suffices to take modulo I by the correspondence theorem on ideals. But this is the same as showing that $\bigcap_{\mathfrak{p} \in \operatorname{Spec}(R/I)} \mathfrak{p} = \sqrt{(0)}$, which is the statement of Lemma 2.48. To be clear, let $\pi : R \to R/I$ be the canonical projection, then if $f \in R$ such that $\pi(f) \in \sqrt{(0)}$ then by definition $f^n \equiv 0 \pmod{I} \implies f^n \in I$, so $f \in \sqrt{I}$. ■

Lemma 2.50. *Let $f, g \in R$ such that $D(g) \subseteq D(f)$. Then $D(g) = D(fg)$.*

Proof. Using Proposition 2.40, we see that for any $h_1, h_2 \in R$, $D(h_1) \cap D(h_2) = D(h_1 h_2)$. Since $D(g) \subseteq D(f)$, we have

$$D(fg) = D(f) \cap D(g) = D(g),$$

yielding the desired result. ■

Proposition 2.51. *Let $X = \operatorname{Spec} R$, and let $\mathcal{B} = \{D(f)\}_{f \in R}$. Then $\mathcal{O}_X(D(f)) = R_f$ defines a $\mathcal{B}$-sheaf of commutative rings $\mathcal{O}_X$ on X.*

Proof. First we must show that we have restriction maps. Suppose we have $f, g \in R$ such that $D(g) \subseteq D(f)$. Then

$$D(g) \subseteq D(f) \implies X \backslash V(g) \subseteq X \backslash V(f) \implies V(f) \subseteq V(g).$$

By Lemma 2.49, $(g) \subseteq \bigcap_{\mathfrak{p} \in V(g)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{p} \in V(f)} \mathfrak{p} = \sqrt{(f)}$ so that there is some n such that $g^n = af$ for some $a \in R$. Therefore, we get a map $\rho_{fg} \colon R_f \to R_g$ given by $hf^{-k} \mapsto ha^k g^{-kn}$. Now suppose $D(g) = D(f)$. Then we also get that $f^m = bg$ for some m, and we get a map $\rho_{gf} : R_g \to R_f$. We will show that this is an isomorphism:

$$(\rho_{gf} \circ \rho_{fg})(hf^{-k}) = \rho_{gf}(ha^k g^{-kn}) = \frac{ha^k b^{kn}}{f^{kmn}} = h\frac{g^{kn} b^{kn}}{f^k f^{kmn}} = h\frac{f^{kmn}}{f^k f^{kmn}} = hf^{-n}.$$

An essentially identical calculation shows that the other composition is also the identity. Hence we see that $D(g) = D(f) \implies R_g \cong R_f$. As an aside, this also immediately gives (from Lemma

2.50) that $R_g \cong R_{fg} \cong (R_f)_g$ when $D(g) \subseteq D(f)$. This describes an alternative restriction, which sends $s \in R_f$ to $s/1 \in (R_f)_g$. This will be a useful characterization.

Now we must check that the sheaf axioms are satisfied. Let $U = D(f)$ be an open set, with a cover $\{U_\lambda = D(f_\lambda)\}_{\lambda\in\Lambda}$, and let $s = s_0/f^k \in R_f$ such that $s|_{U_\lambda} = 0$ for all $\lambda \in \Lambda$ (this will extend to the general case with two sections $t_1, t_2 \in R_f$ by setting $s = t_1 - t_2$). First, note that since $\bigcup_{\lambda\in\Lambda} U_\lambda = U$, we have $\sum_{\lambda\in\Lambda}(f_\lambda R_f) = R_f$, so in particular there is some finite subset $\Lambda' \subseteq \Lambda$ such that $1 \in \sum_{\lambda\in\Lambda'}(f_\lambda R_f)$. Now let $s = s_0/f^k \in R_f$ be such that $s|_{U_\lambda} = 0$. As stated above, Lemma 2.50 lets us restate this as saying that there is some $m_\lambda \geq 1$ such that $f_\lambda^{m_\lambda} s = 0$. Further unraveling this gives that there is some $n_\lambda \geq 1$ such that $f^{n_\lambda} f_\lambda^{m_\lambda} s_0 = 0$. By multiplying sufficiently, there is some *universal* choice of n and m such that $f^n f_\lambda^m s_0 = 0$ for all $\lambda \in \Lambda$. Since $V(I) = V(\sqrt{I})$, we have that $D(f_\lambda^m) = D(f_\lambda)$, so that $1 \in \sum_{\lambda\in\Lambda'} f_\lambda^m R_f$. But then $f^n s_0 \in \sum_{\lambda\in\Lambda'} f^n f_\lambda^m s_0 R_f = 0$, so $f_n s_0 = 0$, i.e. $s = 0$ in R_f.

Now we must show that sections can be glued. For now, assume Λ is finite, which we will then extend to the infinite case. Let $s_\lambda = a_\lambda / f_\lambda^{k_\lambda} \in R_{f_\lambda}$. Setting $g_\lambda = f_\lambda^{k_\lambda}$, we can equivalently consider $s_\lambda = a_\lambda/g_\lambda$ since $D(f_\lambda) = D(g_\lambda)$. We have that $s_\lambda|_{U_\lambda \cap U_\eta} = s_\eta|_{U_\lambda\cap U_\eta}$ for all $\lambda, \eta \in \Lambda$, which translates to the existence of some $m_{\lambda\gamma}$ such that

$$(g_\lambda g_\eta)^{m_{\lambda\eta}}(g_\eta a_\lambda - g_\lambda a_\eta) = 0.$$

Since Λ is finite, we can take the maximum of these. Set $m = \max_{\lambda,\eta\in\Lambda} m_{\lambda\eta}$. Then, for all $\lambda, \eta \in \Lambda$, we have $(g_\lambda g_\eta)^m (g_\eta a_\lambda - g_\lambda a_\eta) = 0$, that is

$$g_\lambda^m g_\eta^{m+1} a_\lambda = g_\lambda^{m+1} g_\eta^m a_\eta.$$

Set $h_\lambda = g_\lambda^{m+1}$. Again, $D(f_\lambda) = D(g_\lambda) = D(h_\lambda)$. As above, we have that $R_f = \sum_{\lambda\in\Lambda} h_\lambda R_f$, so that there are some $r_\lambda \in R_f$ such that $1 = \sum_{\lambda\in\Lambda} r_\lambda h_\lambda$. We finally set $s = \sum_{\lambda\in\Lambda} r_\lambda g_\lambda^m a_\lambda$. This is our desired gluing. To check this, note that

$$sh_\eta = \sum_{\lambda\in\Lambda} r_\lambda h_\eta g_\lambda^m a_\lambda = \sum_{\lambda\in\Lambda} r_\lambda h_\lambda g_\eta^m a_\eta = \left(\sum_{\lambda\in\Lambda} r_\lambda h_\lambda\right) g_\eta^m a_\eta = g_\eta^m a_\eta$$

hence $s g_\eta^{m+1} - g_\eta^m a_\eta = g_\eta^m(s g_\eta - a_\eta) = 0$, i.e. $s|_{U_\eta} = a_\eta/g_\eta = a_\eta/f_\eta^{k_\eta}$.

Now suppose that Λ is infinite. Pick some finite $\Lambda' \subseteq \Lambda$ such that $\sum_{\lambda\in\Lambda'} f_\lambda R_f = R_f$ and do the above procedure to produce some s. Now consider any $\eta \in \Lambda\backslash\Lambda'$, and apply the procedure to $\Lambda' \cup \{\eta\}$ to get some s'. Then, for all $\lambda \in \Lambda'$, $s|_{U_\lambda} = s'|_{U_\lambda}$ so, by the identity axiom (which we proved above), we must have $s = s'$, so that $s|_{U_\eta} = s'|_{U_\eta}$. This means that the s produced by the finite case is the right thing even for the infinite case, and so we are done. ■

Proposition 2.52. *Let $X = \operatorname{Spec} R$ and let $\mathfrak{p} \in X$. Then $\mathcal{O}_{X,\mathfrak{p}}$ is canonically isomorphic to $R_\mathfrak{p}$.*

Proof. Let $f \in R$ and $U = D(f)$. Then $\mathfrak{p} \in D(f)$ if and only if $f \notin \mathfrak{p}$. Hence,

$$\mathcal{O}_{X,\mathfrak{p}} = \varinjlim_{U\ni\mathfrak{p}} \mathcal{O}_X(U) = \varinjlim_{f\notin\mathfrak{p}} \mathcal{O}_X(D(f)) = \varinjlim_{f\notin\mathfrak{p}} R_f.$$

Now, if $f \notin \mathfrak{p}$, then the universal property of the localization gives us a canonical map $R_f \to R_\mathfrak{p}$ since we have a map $R \to R_\mathfrak{p}$ which maps f to a unit. Hence, by the universal property of the colimit, we get a map

$$\varphi\colon \varinjlim_{f\notin\mathfrak{p}} R_f \to R_\mathfrak{p}.$$

The map φ is surjective since every element $s \in R_{\mathfrak{p}}$ can be written as s_0/f with $f \notin \mathfrak{p}$, and is therefore in the image of the map $R_f \to R_{\mathfrak{p}}$, thus (by commutativity) in the image of the map $\varinjlim_{f \notin \mathfrak{p}} R_f \to R_{\mathfrak{p}}$. Injectivity follows from the following: if $s = s_0/f^n \in R_f$ is mapped to $0 \in R_{\mathfrak{p}}$, then necessarily there is some $g \notin \mathfrak{p}$ such that $gs_0 = 0$. From this we conclude that $s = 0$ in R_{fg}, and therefore is 0 in the colimit. Therefore, φ is an isomorphism, and is canonical by construction, i.e. since it is made out of a combination of canonical maps arising from universal properties. ■

Remark 2.53. There is a useful computational tool to mention here: to compute $R_{\mathfrak{p}}/\mathfrak{p}$ is the same as to compute $\operatorname{Frac}(R/\mathfrak{p})$.

Remark 2.54. Let R be an integral domain. Then if we let ξ be the point corresponding to $(0) \in X = \operatorname{Spec} R$, we see that $\mathcal{O}_{X,\xi} = R_{(0)} = \operatorname{Frac} R =: K$. Furthermore, we can view elements of $\mathcal{O}_X(U)$ as "actual" rational functions on X by noting that the map $\mathcal{O}_X(U) \to \mathcal{O}_{X,\xi} = K$ is injective. This follows from first considering a basis case: let $f \in R$. Then $\mathcal{O}_X(D(f)) = R_f$, and the map $R_f \to K$ is injective (i.e. $R_f \subseteq K$). In the general case, we set $U = \bigcup_{\lambda \in \Lambda} D(f_\lambda)$ and note that if $s \in \mathcal{O}_X(U)$ maps to $0 \in \mathcal{O}_{X,\xi}$ then $s|_{D(f_\lambda)} = 0$ for every $\lambda \in \Lambda$, and hence $s = 0$ by the identity sheaf axiom. Hence, we can think of sections on X as being rational functions, i.e. elements of $K = \operatorname{Frac} R$.

We end with a useful lemma:

Lemma 2.55. *Let $\mathfrak{p} \in \operatorname{Spec} R$. Then $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$.*

Proof. By definition, the closure of a set is the smallest closed set containing the set, i.e. the intersection of all closed sets larger than the set. Hence,

$$\overline{\{\mathfrak{p}\}} = \bigcap_{I \supseteq \mathfrak{p}} V(I).$$

Since $\mathfrak{p}$ is the smallest ideal containing itself, $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, since if $\mathfrak{p} \subseteq \mathfrak{q}$ and $\mathfrak{q} \subseteq \mathfrak{q}'$ then $\mathfrak{p} \subseteq \mathfrak{q}'$. ■

2.3 General Schemes

As mentioned in the beginning of the last subsection, schemes are made by "gluing together" affine schemes in a way similar to that of manifolds. The added difficulty with schemes is that they come equipped with some notion of what a "function" on the scheme is, which we saw in the previous subsection as the sheaf of regular functions defined for affine schemes. We therefore see that a scheme in general is more than just a space, and so we must make this precise.

Definition 2.56. A *ringed space* is a pair $(X, \mathcal{O}_X)$ of a topological space X and a sheaf of commutative rings on X. The sheaf $\mathcal{O}_X$ is called the *structure sheaf* of X. In abuse of notation, one often simply writes that X is a ringed space. A ringed space $(X, \mathcal{O}_X)$ is said to be a *locally* ringed space if for every $x \in X$ the stalk $\mathcal{O}_{X,x}$ is a local ring. The unique maximal ideal of $\mathcal{O}_{X,x}$ is denoted $\mathfrak{m}_x$, and one writes $k(x) := \mathcal{O}_{X,x}/\mathfrak{m}_x$ for the *residue field at x*.

Definition 2.57. Let X and Y be locally ringed spaces. A *morphism* of ringed spaces $(f, f^\sharp)\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a pair consisting of a continuous map $f\colon X \to Y$ and a "*pullback map*" $f^\sharp\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$ of sheaves (note that this map goes opposite the direction of f) such that for every $x \in X$ the induced map on stalks $f^\sharp_x\colon \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is a local map, i.e. $f^\sharp_x(\mathfrak{m}_{f(x)}) \subseteq \mathfrak{m}_x$. In abuse of notation, one usually simply denotes $(f, f^\sharp)$ by f.

Remark 2.58. These definitions make sense. In particular, one should think of a locally ringed space as being the "minimum sensible amount of structure" needed to have a precise notion of a "sheaf of functions" on a space, where the functions take values in some number of fields. The explanation for this is as follows: letting U be open in X, and $x \in U$, one should think of the composition of maps $\mathcal{O}_X(U) \to \mathcal{O}_{X,x} \to k(x)$ as a function which "evaluates" sections over U at x, where sections $s \in \mathcal{O}_X(U)$ with $[s]_x \in \mathfrak{m}_x$ are those that are zero at x. Note that the local condition here is important: without knowing that the stalks are local rings, we do not have a sensible notion of residue field. Thinking of things in this way is quite usefull, since it makes it obvious why this is important for algebraic geometry, i.e. we automatically get a notion of zero sets of functions.

Remark 2.59. The reasoning behind the reverse direction of $f^\sharp$ is again from analogies with manifolds. If one has a smooth real valued function ϕ on a manifold M and a smooth map $N \to M$ then one can pull back ϕ to a smooth real valued function on N, and this is a somewhat fundamental operation for differential geometry. We want to preserve such behavior in (locally) ringed spaces, except because the analogue of smooth real valued functions is stored in a sheaf, we must provide the map ourselves in the definition. Using the previous remark, we see that the requirement of being local maps on stalks translates to saying that if ϕ is zero at a point, then the pullback is also zero at the corresponding points in the fiber.

Remark 2.60. Note that an isomorphism of (locally) ringed spaces $X \xrightarrow{\sim} Y$ translates to essentially saying that X and Y are homeomorphic and that the structure sheaves are essentially the same (i.e. the only difference being that they work on different versions of the same underlying space).

Remark 2.61. Let R be a commutative ring. Then $(\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$ is a locally ringed space.

Definition 2.62. Let X be a locally ringed space, let $U \subseteq X$ be open, and let $x \in U$. We will denote by $\operatorname{ev}_{U,x} : \mathcal{O}_X(U) \to k(x)$ the composition of the maps $\mathcal{O}_X(U) \to \mathcal{O}_{X,x} \to k(x)$. Let $s \in \mathcal{O}_X(U)$. We write $s(x) := \operatorname{ev}_{U,x}(s)$ and call it the *value of s at x.*

Remark 2.63. The notation here is what justifies the notation in Remark 2.38. Furthermore, one sees that we can essentially treat the statement $s(x) = 0$ as a statement about a completely normal function.

We now come to the definition of a scheme.

Definition 2.64. A locally ringed space $(X, \mathcal{O}_X)$ is an *affine scheme* if there exists some ring R such that $(X, \mathcal{O}_X) \cong (\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$. We denote by **AffSch** the category of affine schemes.

Definition 2.65. A locally ringed space $(X, \mathcal{O}_X)$ is a *scheme* if for every $x \in X$ there is some open set U containing x such that $(U, \mathcal{O}_X|_U)$ is an affine scheme. A morphism of schemes is a morphism of locally ringed spaces. We denote by **Sch** the category of schemes. Let S be a scheme. An *S-scheme* X is a scheme X equiped with a map $X \to S$, called the *structure morphism* (equivalently, one says X is a *scheme over* S, i.e. $X \in \mathbf{Sch}/S$). A morphism of S-schemes $X \to Y$ is a morphism of schemes that is compatible with the structure morphisms, that is such that

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr] & & Y \arrow[dl] \\
& S &
\end{tikzcd}$$

is a commutative diagram. When $S = \operatorname{Spec} A$ for some ring A we say X is an A-scheme rather than a $\operatorname{Spec} A$-scheme. We will sometimes write "X/S" to mean that X is an S-scheme.

Remark 2.66. Note that one may slightly reword the definition of a scheme by saying that it is a locally ringed space with a cover of open sets $\{U_\lambda\}_{\lambda\in\Lambda}$ such that $(U_\lambda, \mathcal{O}_X|_{U_\lambda})$ is an affine scheme for all $\lambda \in \Lambda$. This is how the definition is worded in [Liu10, p. 44].

Definition 2.67. Let R be a commutative ring. *Affine n-space* (alt. *n-dimensional Affine space*) is defined as the (affine) scheme $\mathbb{A}^n_R := \operatorname{Spec} R[t_1, \dots, t_n]$.

Proposition 2.68. *Let X be a scheme, and let $U \subseteq X$ be an open set. Then $(U, \mathcal{O}_X|_U)$ is a scheme.*

Definition 2.69. Let X be a scheme, and let $U \subseteq X$ be an open set. We say that $(U, \mathcal{O}_X|_U)$ is an *open subscheme* of X.

Remark 2.70. Let $\pi : X \to \operatorname{Spec} k$ be a k-scheme with k a field. What requirements does this place on X? We get a map $\pi^\sharp : \mathcal{O}_{\operatorname{Spec} k} \to \pi_*\mathcal{O}_X$. However, since $\operatorname{Spec} k$ contains one point, we see that $\pi^\sharp$ only consists of one component map, namely $\pi^\sharp_{\{*\}} : k = \mathcal{O}_{\operatorname{Spec} k}(\{*\}) \to \mathcal{O}_X(X) = \pi_*\mathcal{O}_X(\{*\})$. In other words, this endows $\mathcal{O}_X(X)$ with the structure of a k-algebra. Furthermore, the restriction maps make all $\mathcal{O}_X(U)$'s into k-algebras for each open subset $U \subseteq X$ via composition of the maps $k \to \mathcal{O}_X(X) \to \mathcal{O}_X(U)$. In fact, with similar reasoning, one sees that putting a k-algebra structure on $\mathcal{O}_X(X)$ for an arbitrary scheme X is the same as endowing it with a k-scheme structure. This can be extended further.

Lemma 2.71. *Let X, Y be affine schemes. Then there is a natural isomorphism*

$$\operatorname{Hom}(X, Y) \cong \operatorname{Hom}(\mathcal{O}_Y(Y), \mathcal{O}_X(X)).$$

In other words, $\mathbf{AffSch} \cong \mathbf{CRng}^{\mathrm{op}}$.

Proof. See [Liu10, p. 48, Lemma 3.23]. ■

Proposition 2.72. *Let X be a scheme and Y an affine scheme. Then the map*

$$\rho \colon \operatorname{Hom}(X, Y) \to \operatorname{Hom}(\mathcal{O}_Y(Y), \mathcal{O}_X(X))$$

given by $\rho(f) = f^\sharp_Y$ is a bijection.

Proof. See [Liu10, p. 48, Prop. 3.25]. ■

Remark 2.73. We see from the above proposition that giving an A-scheme X for a ring A is the same as giving the structure sheaf $\mathcal{O}_X$ the structure of a sheaf of A-algebras.

Remark 2.74. Let X be a k-scheme. Since all of the $\mathcal{O}_X(U)$'s are k-algebras, we see also that necessarily $\mathcal{O}_{X,x}$ is a k-algebra for all $x \in X$. From this, one gets a map $k \to \mathcal{O}_{X,x} \to \mathcal{O}_{X,x}/\mathfrak{m}_x = k(x)$, so we see that $k(x)$ is a field extension of k.

Definition 2.75. A morphism $f : X \to Y$ of schemes is an *open* (resp. *closed*) *immersion* if $f(X)$ is open (resp. closed), a homeomorphism onto its image (i.e. the induced map $X \to f(X)$ is a homeomorphism), and for all $x \in X$ the pullback map $f^\sharp_x$ on stalks is an isomorphism (resp. a surjection).

Definition 2.76. Let X be a scheme. A *closed subscheme* of X is a closed set $Z \subseteq X$ endowed with the structure of a scheme $(Z, \mathcal{O}_Z)$ and a morphism $j^\sharp \colon \mathcal{O}_X \to j_*\mathcal{O}_Z$ where $j \colon Z \to X$ is the inclusion of Z into X, such that $(j, j^\sharp) \colon (Z, \mathcal{O}_Z) \to (X, \mathcal{O}_X)$ is a closed immersion.

Remark 2.77. If Z is a closed subset of a scheme X then there are several inequivalent closed subscheme structures one can put on X, unlike the case for open sets.

Proposition 2.78. *Let $X = \operatorname{Spec} R$ be an affine scheme, and let $g \in R$. Set $Y = \operatorname{Spec} A_g$. Then $(D(g), \mathcal{O}_X|_{D(g)}) \cong (Y, \mathcal{O}_Y)$.*

Proof. Recall that Proposition 2.46(c) essentially tells us that there is a canonical topological open immersion $i \colon Y \to X$ whose image is $D(g)$. Now let $h \in R$ be such that $D(h) \subseteq D(g)$, and let $\bar{h}$ be the image of $h \in A_g$. Then $\mathcal{O}_X(D(h)) = R_h = (R_g)_{\bar{h}} = \mathcal{O}_Y(D(\bar{h})) = i_*\mathcal{O}_Y(D(h))$. Therefore, we get an isomorphism $\mathcal{O}_X(D(h)) \cong i_*\mathcal{O}_Y(D(h))$ induced by i. By Proposition 2.19, this extends to an isomorphism $\mathcal{O}_X|_{D(g)} \cong i_*\mathcal{O}_Y$. Hence, we have that the topological open immersion i is an actual open immersion of ringed spaces, so that $(D(g), \mathcal{O}_X|_{D(g)}) \cong (Y, \mathcal{O}_Y)$. ■

Definition 2.79. Let X be a topological space, and let $x \in X$. We say that $y \in X$ *specializes* to x if $x \in \overline{\{y\}}$. One then also says that x *generalizes* to y.

Lemma 2.80. *Let X be a topological space, $x \in X$, and let $y \in X$ be a point that specializes to x. Then every open set that contains x also contains y.*

Proof. Suppose that we have some open set U with $x \in U$, but $y \notin U$. Then $y \in U^c$, which is also a closed set. Since the closure of a set is the intersection of all closed sets containing the set, we have that $\overline{\{y\}} \subseteq U^c$, so $x \in U^c$. But since $x \in U$, it cannot be that $x \in U^c$, so we have a contradiction. Hence, if $x \in U$ then $y \in U$. ■

Corollary 2.81. *Let R be a local ring, and let $\mathfrak{m}$ denote the maximal ideal of R. If $U \subseteq \operatorname{Spec} R$ is an open set containing $\mathfrak{m}$, then $U = \operatorname{Spec} R$.*

Proof. This follows from Lemma 2.80 and Lemma 2.55. ■

Proposition 2.82. *Let X be a scheme, and let $x \in X$. Then there is a canonical morphism of schemes $\operatorname{Spec} \mathcal{O}_{X,x} \to X$ whose image is the set of points that specialize to x.*

Proof. Let U be some affine open set containing x. Then we get a map $\mathcal{O}_X(U) \to \mathcal{O}_{X,x}$ which induces a map canonical map $\operatorname{Spec} \mathcal{O}_{X,x} \to U$, which in particular sends $\mathfrak{m}_x$ to x. Composing this with the inclusion $U \to X$ gives the map $f \colon \operatorname{Spec} \mathcal{O}_{X,x} \to X$. We want this to be independent of the choice of U. Suppose V is some open set containing x. Then $f^{-1}(V) \subseteq \operatorname{Spec} \mathcal{O}_{X,x}$ is an open subset of $\mathcal{O}_{X,x}$ containing $\mathfrak{m}_x$, and so by Corollary 2.81 we have that $f^{-1}(V) = \operatorname{Spec} \mathcal{O}_{X,x}$, i.e. $\operatorname{im} f \subseteq V$. Hence any open set containing x contains the image of f, so that the choice of open set doesn't matter. Now we will show that f has the right image.

Let $R = \mathcal{O}_X(U)$, so that $U = \operatorname{Spec} R$ is the open neighbourhood around x from above, and let $y \in \operatorname{im} f$. Denote by $\mathfrak{p}$ (resp. $\mathfrak{q}$) the image of x (resp. y) in $\operatorname{Spec} R$. Then $\mathcal{O}_{X,x} \cong R_{\mathfrak{p}}$, so that points of $\mathcal{O}_{X,x}$ are ideals contained in $\mathfrak{p}$, and the map $\operatorname{Spec} \mathcal{O}_{X,x} \to U$ is identified with the map $\operatorname{Spec} R_{\mathfrak{p}} \to \operatorname{Spec} R$, and has image those points that are contained in $\mathfrak{p}$. Hence $\mathfrak{q} \subseteq \mathfrak{p}$, so that $\mathfrak{p} \in V(\mathfrak{q}) = \overline{\{\mathfrak{q}\}}$ so that y specializes to x.

Now suppose that y specializes to x. Then, by Lemma 2.80, every open neighbourhood of x contains y, so y is in the above mentioned affine neighbourhood U of x. Hence, we may again denote y by $\mathfrak{q} \in R$. Since $\mathfrak{q}$ specializes to $\mathfrak{p}$ (using the same names as above), we conclude that $\mathfrak{q} \subseteq \mathfrak{p}$, and so can be identified with an element of $\operatorname{Spec} R_{\mathfrak{p}} = \operatorname{Spec} \mathcal{O}_{X,x}$, i.e. $y \in \operatorname{im} f$. ■

Definition 2.83. Let X and Y be schemes. The Y*-rational points* of X are defined as $X(Y) := \operatorname{Hom}_{\mathbf{Sch}}(Y, X)$. If X and Y are S-schemes, then one takes this over S instead, i.e. $X(Y) := \operatorname{Hom}_{\mathbf{Sch}/S}(Y, X)$. When $Y = \operatorname{Spec} R$ for a ring R, one writes $X(R)$ instead of $X(\operatorname{Spec} R)$.

It is good to ask whether we can concretely describe what the k-rational points of a k-scheme look like. This is answered by the following:

Lemma 2.84. *Let R be a commutative ring, $I \subseteq R$ an ideal. Then the map*

$$\operatorname{Spec} R/I \to \operatorname{Spec} R$$

induced by the surjection $R \to R/I$ is a closed immersion with image $V(I)$.

Proof. This follows immediately from Proposition 2.46. ■

Lemma 2.85. *Let $x \in X$. Then there is a canonical map* $\operatorname{Spec} k(x) \to X$ *with image x.*

Proof. From Proposition 2.82 we get a canonical map $\operatorname{Spec} \mathcal{O}_{X,x} \to X$. Furthermore, since $k(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x$, Lemma 2.84 gives a canonical closed immersion $\operatorname{Spec} k(x) \to \operatorname{Spec} \mathcal{O}_{X,x}$ with image $\{x\} = V(\mathfrak{m}_x)$. Composing these gives the desired canonical map $\operatorname{Spec} k(x) \to X$. ■

Proposition 2.86. *Let X be a k-scheme. Then $X(k)$ can be identified with the points $x \in X$ such that $k(x) = k$.*

Proof. Let $x \in X$ be a point such that $k(x) = k$. From Lemma 2.85, this immediately gives a unique map $\operatorname{Spec} k \to X$ with image x which commutes with the structure map $X \to \operatorname{Spec} k$, i.e. it gives an element of $X(k)$.

Now suppose $\bar{x} \in X(k)$, i.e. $\bar{x}$ is a map $\operatorname{Spec} k \to X$. Let $x = \bar{x}(*)$ denote the image of the unique element in $\operatorname{Spec} k$. Since $\bar{x}$ is a map of schemes, we get a map $\bar{x}^\sharp : \mathcal{O}_X \to \bar{x}_* \mathcal{O}_{\operatorname{Spec} k}$. Since $\bar{x}^{-1}(U) = \{*\}$ if and only if $x \in U$, we see that this is the same as being given maps $\bar{x}^\sharp_U : \mathcal{O}_X(U) \to k$ with $x \in U$. By the universal property of the colimit, we then get a map $\bar{x}^\sharp_x \mathcal{O}_{X,x} \to k$. Since $\bar{x}^\sharp_x$ is a map of local rings, and the maximal ideal of a field is the zero ideal, we have that $\bar{x}^\sharp_x(\mathfrak{m}_x) = 0$, so that $\mathfrak{m}_x \subseteq \ker \bar{x}^\sharp_x$. Since $\mathfrak{m}_x$ is maximal, this is also an equality. Hence, the image of $\bar{x}^\sharp_x$ is a field containing (see Remark 2.74) and contained in k, i.e. equal to k, so that $k(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x = \mathcal{O}_{X,x}/\ker \bar{x}^\sharp_x = \operatorname{im} \bar{x}^\sharp_x = k$. ■

Remark 2.87. Note that the above proposition does not generalize to extensions K/k, i.e. it is not in general true that if X is a k-scheme, then $X(K)$ is in bijection with points $x \in X$ such that $k(x) = K$ or $k(x) \subseteq K$. There is, however, a characterization of $X(K)$ which is fairly similar to this, which will be the subject of a later proposition, and will involve *base change*, replacing X with a K-scheme X_K.

Remark 2.88. Let X be a k-scheme, and identify $X(k)$ with the points of X with residue field k. Then if we are given some global section $s \in \mathcal{O}_X(X)$, observe that this produces a "genuine" function $X(k) \to k$, given by $x \mapsto s(x)$ (recall Definition 2.62). In other words, we are justified in thinking of sections of $\mathcal{O}_X$ as functions in a way similar to the traditional sense, even if they are defined in a totally abstract way.

There is a second, more specialized, characterization of the k-rational points of a k-scheme, which confirms the intuition implied by the name, and provides a more direct geometric interpretation.

Proposition 2.89. *Let $X = \operatorname{Spec} k[t_1, \ldots, t_n]/I$ be an affine k-scheme, with k a field. Let $Z = \{(a_1, \ldots, a_n) \in k^n \mid \forall f \in I,\ f(a_1, \ldots, a_n) = 0\}$. Then there is a canonical bijection $Z \xrightarrow{\sim} X(k)$.*

Proof. Let $a = (a_1, \ldots, a_n) \in Z$, and set $\mathfrak{m}_a = (t_1 - a_1, \ldots, t_n - a_n)$. This ideal is maximal, and $I \subseteq \mathfrak{m}_a$, since if $f \in I$ then $f \pmod{\mathfrak{m}_a} \equiv f(a) = 0$. Hence, $\mathfrak{m}_\mathfrak{a}$ determines a point x_a of X, which has $k(x_a) = k[t_1, \ldots, t_n]/\mathfrak{m}_a = k$ (identifying X with $V(I) \subseteq \mathbb{A}^n_k$), so that x_a is a k-rational point of X.

Now suppose we are given a k-rational point $x \in X(k)$. Let a_i be the image of t_i in $k(x) = k$, and set $\mathfrak{m} = (t_1 - a_1, \dots, t_n - a_n)$. Then $f \in \mathfrak{m}$ if and only if $f(a) = 0$. Furthermore, $x \subseteq \mathfrak{m}$ and $I \subseteq x$ so $I \subseteq \mathfrak{m}$, hence if $f \in I$ then $f(a) = 0$ so that $a \in Z$. ■

Remark 2.90. This tells us essentially that the theory of schemes actually is an extension of the classical theory of algebraic geometry, in the sense that schemes manage to encode the same kind of information (and more), just in a different way. In other words, the problem of solving systems of polynomial equations is the same as finding rational points on schemes.

2.4 Projective Schemes

Projective schemes form a large class of examples of schemes that are not affine, and are also usually the schemes that are of most interest. Classically speaking, they can be seen as the prototype for schemes: projective n-space is covered by $n+1$ copies of affine n-space. Generally, the way to think about projective space is to imagine that one is adjoining some points "at infinity" so that geometric objects behave better (i.e. many theorems about projective space have affine analogues, but for which the statements require many caveats and exceptions; a notable example of this is Bézout's theorem). The way we define projective schemes is somewhat analogous to how one defines affine schemes, in that one does an operation on a ring to produce a geometric space. However, rather than using Spec, one uses something called Proj, which only accepts *graded* rings as input.

For the time being, fix a commutative ring R.

Definition 2.91. A commutative ring B is *graded* if B decomposes as a direct sum $\bigoplus_{d \geq 0} B_d$ of Abelian groups (called the *grading*) such that $B_d B_c \subseteq B_{d+c}$. If, furthermore, B is an R-algebra, we say that it is a *graded R-algebra* if the image of R in B is contained in B_0. Elements of B_d are called *homogeneous elements of degree d*. An ideal $I \subseteq B$ is called a *homogeneous ideal* if it is generated by homogeneous elements. A homomorphism of graded rings $\phi : C \to B$ is a homomorphism of rings such that there exists some $r \geq 1$ satisfying $\phi(C_d) \subseteq B_{rd}$ for all $d \geq 0$.

Definition 2.92. Let B be a graded ring. Then we call the ideal $B_+ = \bigoplus_{d>0} B_d$ the *irrelevant ideal.*

Definition 2.93. Let B be a graded R-algebra. Then we define

$$\operatorname{Proj} B = \{\mathfrak{p} \subset B \mid \mathfrak{p} \text{ is prime, homogeneous, and } \mathfrak{p} \not\supseteq B_+\}.$$

Definition 2.94. Let B be a graded R-algebra, and let $I \subseteq B$ be a homogeneous ideal. Then the set $V_+(I) = \{\mathfrak{p} \in \operatorname{Proj} B \mid I \subseteq \mathfrak{p}\}$.

Proposition 2.95. *Let B be a graded R-algebra.*

(a) Let I, J be homogeneous ideals of B. Then $V_+(I) \cup V_+(J) = V_+(I \cap J)$.
(b) Let $\{I_\lambda\}_{\lambda \in \Lambda}$ be a collection of homogeneous ideals of B. Then $\bigcap_{\lambda \in \Lambda} V_+(I_\lambda) = V_+(\sum_{\lambda \in \Lambda} I_\lambda)$.
(c) $V(0) = \operatorname{Proj} B$, and $V(B) = \emptyset$.

Proof. The proof of this is identical to that of Proposition 2.40. ■

Hence, we see that we can endow $\operatorname{Proj} B$ with a topology similar to that of Spec.

Definition 2.96. The *Zariski topology* on $\operatorname{Proj} B$ is the topology determined by setting the closed sets to be of the form $V_+(I)$ for homogeneous ideals $I \subseteq B$.

Definition 2.97. Let B be a graded ring, and let $I \subseteq B$ be an ideal. Then define the *homogenization* of I to be $I^h := \bigoplus_{d \geq 0}(B_d \cap I)$.

Lemma 2.98. *Let B be a graded ring, and let I, J be ideals of B.*

(a) If I is prime, then the associated homogeneous ideal I^h is prime.
(b) If I, J are homogeneous, then $V_+(I) \subseteq V_+(J)$ if and only if $J \cap B_+ \subseteq \sqrt{I}$.
(c) $\operatorname{Proj} B = \emptyset$ *if and only if B_+ is nilpotent.*

Proof. (a) Suppose we have $a, b \in B$ with $ab \in I^h$ but $a, b \notin I^h$. Write a and b in terms of their homogeneous components

$$a = \sum_{i=0}^{n} a_i, \quad b = \sum_{j=0}^{m} b_j$$

where $a_d, b_d \in B_d$. Then note that $ab = a_n b_m + \sum c_i$, where c_i are elements of degree strictly less than $n+m$. Hence, the degree $n+m$ component of ab is $a_n b_m$, so that $a_n b_m \in I^h \subseteq I$. Since $a, b \notin I^h$, we can assume that $a_n, b_m \notin I^h$, but since $a_n b_m \in I^h$ is a strictly homogeneous element, we see that the primality of I gives that $a_n \in I^h$ or $b_m \in I^h$, giving a contradiction. Hence we conclude that I^h is prime.

(b) For proving ($\Longleftarrow$), begin by assuming that $J \cap B_+ \subseteq \sqrt{I}$. Since $\mathfrak{p} \supseteq I$ if and only if $\mathfrak{o} \supseteq \sqrt{I}$, we see that any $\mathfrak{p} \in V_+(I)$ satisfies $\mathfrak{p} \supseteq J \cap B_+ \supseteq JB_+$. Since $\mathfrak{p} \not\supseteq B_+$ and is prime, it must be that $\mathfrak{p} \supseteq J$, so that $\mathfrak{p} \in V_+(J)$, i.e. $V_+(I) \subseteq V_+(J)$. For the ($\Longrightarrow$) direction, suppose $V_+(I) \subseteq V_+(J)$. For any $\mathfrak{p} \in V(I)$, the homogenization $\mathfrak{p}^h$ is prime (by part (a)) and contains I (since I is homogeneous). If $\mathfrak{p}^h$ does not contain B_+, then $\mathfrak{p}^h \in V_+(I)$ so that $\mathfrak{p} \supseteq \mathfrak{p}^h \supseteq J \supseteq J \cap B_+$ (since $\mathfrak{p}^h \in V_+(I) \implies \mathfrak{p} \in V_+(J)$). If $\mathfrak{p}^h$ does contain B_+, then still one has $\mathfrak{p} \supseteq \mathfrak{p}^h \supseteq J \cap B_+$, so that $J \cap B_+ \subseteq \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \sqrt{I}$ (by Lemma 2.49).

(c) This follows from the above two parts, since $\operatorname{Proj} B = \emptyset$ if and only if $V_+(0) \subseteq V_+(B_+)$, which by (b) is equivalent to $B_+ \subseteq \sqrt{(0)}$, i.e. B_+ is nilpotent. ■

We will want an analogue of the isomorphism $D(f) \cong \operatorname{Spec} R_f$ from the subsection on affine schemes (Subsection 2.2). To do this, we have to replace "pure" localization with only looking at those elements that have degree 0.

Definition 2.99. Let B be a graded ring, and let $f \in B$ be a homogeneous element. The *distinguished open set defined by f* is $D_+(f) := \operatorname{Proj} B \backslash V_+(f)$.

Remark 2.100. These form a basis for the zariski topology on $\operatorname{Proj} B$, which can be proven in the exact same way as in the Spec case. Furthermore, we may actually restrict ourselves to $f \in B_+$, since $\emptyset = V_+(B_+) = \bigcap_i V_+(f_i)$, where the f_i are homogeneous elements that generate B_+, so that $\operatorname{Proj} B = \bigcup_i D_+(f_i)$. Similarly, one may conclude that for homogeneous $g \in B$, one has $D_+(g) = \bigcup_i D_+(gf_i)$ with $gf_i \in B_+$.

Definition 2.101. Let B be a graded ring, and let $f \in B$ be a homogeneous element. The *elements of degree zero* of B_f, denoted $B_{(f)}$, is the subring of B_f made up of elements of the form a/f^n, $n \geq 0$, with $\deg a = n \deg f$.

Proposition 2.102. *Let B be a graded ring, and let $f \in B_+$ be a homogeneous element of degree r. Then*

(a) There exists a canonical homeomorphism $\theta \colon D_+(f) \to \operatorname{Spec} B_{(f)}$.
(b) If $D_+(g) \subseteq D_+(f)$ and $a = g^r f^{-\deg g}$, then $\theta(D_+(g)) = D(a)$.
(c) We have a canonical homomorphism $B_{(f)} \to B_{(g)}$ which induces an isomorphism $(B_{(f)})_a \cong B_{(g)}$.
(d) If I is a homogeneous ideal of B, then $\theta(V_+(I) \cap D_+(f)) = V(I_{(f)})$, where $I_{(f)} := IB_f \cap B_{(f)}$.
(e) If I is an ideal of B generated by homogeneous elements $h_1, \ldots h_n$, then for any homogeneous $f \in B$ with $\deg f = 1$, the ideal $I_{(f)}$ is generated by $h_i/f^{\deg h_i}$, $1 \leq i \leq n$.

Proof. See [Liu10, p. 51–52, Lemma 3.36]. ■

With the above in mind, we are now equipped to turn $\operatorname{Proj} B$ into a scheme. In particular, one sets $\mathcal{O}_{\operatorname{Proj} B}(D_+(f)) = B_{(f)}$ to define the structure sheaf.

Proposition 2.103. *Let R be a commutative ring, and let B be a graded R-algebra. Then $\operatorname{Proj} B$ can be endowed with a unique R-scheme structure such that for any $f \in B_+$, the open set $D_+(f)$ is affine and isomorphic to $\operatorname{Spec} B_{(f)}$.*

Proof. Set $X = \operatorname{Proj} B$ and let $\mathcal{B}$ be the basis of the Zariski topology on X given by $D_+(f)$ with $f \in B_+$. Then, as specified above, set $\mathcal{O}_X(D_+(f)) = B_{(f)}$, and note that Proposition 2.102 gives that if $D_+(f) = D_+(g)$ then $B_{(f)}$ is canonically isomorphic to $B_{(g)}$, and if $D_+(g) \subseteq D_+(f)$ then we have a canonical restriction $\mathcal{O}_X(D_+(f)) \to \mathcal{O}_X(D_+(g))$. Hence $\mathcal{O}_X$ is a $\mathcal{B}$-presheaf, and furthermore the map θ from Proposition 2.102 shows that $\mathcal{O}_X$ is a $\mathcal{B}$-sheaf. Hence, $\mathcal{O}_X$ extends to a sheaf on X, which gives X the structure of a scheme, and the statement about $D_+(f)$ being affine is immediate. Finally, this determines an R-algebra structure on X, since each $B_{(f)}$ is an R-algebra (due to the image of R being degree zero), and so we have a cover of X by affine R-schemes. ■

This finally gives us a way to define projective n-space, like we defined affine n-space before.

Definition 2.104. Let R be a commutative ring, and let $R[t_0, \dots, t_n]$ be endowed with the structure of a graded R-algebra by degree. Then we define *projective n-space* over R to be $\mathbb{P}^n_R := \operatorname{Proj} R[t_0, \dots, t_n]$.

Remark 2.105. Contrast this with the definition of affine n-space. In particular, note that indexing starts with zero in the projective case, and with one in the affine case.

Remark 2.106. This looks basically the same as one expects from classical projective geometry (e.g. over the complex numbers). In particular, setting $B = R[t_0, \dots, t_n]$, one has $B_{(t_i)} = R[t_0/t_i, \dots, t_n/t_i]$, which corresponds to the classical case in the sense that the affine open subset $D_+(t_i) \cong \operatorname{Spec} B_{(t_i)}$ is analogous to the typical coordinate chart of projective space given by supposing that the ith homogeneous coordinate is non-zero.

In the case of classical algebraic geometry, one usually defines a projective variety (essentially) as a closed set in projective space. Now, in the case of scheme-theoretic algebraic geometry, one does something similar. Recall from the last subsection that one can define closed subschemes of a scheme.

Definition 2.107. Let R be a commutative ring. A *projective scheme* over R is an R-scheme which is isomorphic to some closed subscheme of $\mathbb{P}^n_R$ for some $n \geq 0$.

In other words, projective R-schemes are schemes that can be made to sit in $\mathbb{P}^n_R$, which is a very similar definition to the classical one.

Proposition 2.108. *Let $\phi \colon C \to B$ be a homomorphism of graded R-algebras, and let $M = \phi(C_+)B$. Then ϕ induces a morphism of R-schemes $f : \operatorname{Proj} B \backslash V_+(M) \to \operatorname{Proj} C$ such that for all homogeneous $h \in C_+$, $f^{-1}(D_+(h)) = D_+(\phi(h))$, and such that $f|_{D_+(\phi(h))}$ is the same as the morphism of affine schemes induced by the map $C_{(h)} \to B_{(\phi(h))}$. In particular, if I is a homogeneous ideal of $R[t_0, \dots, t_n]$, then $\operatorname{Proj} R[t_0, \dots, t_n]/I$ is isomorphic to a closed subscheme of $\mathbb{P}^n_R$ with underlying topological space $V_+(I)$, i.e. it is a projective scheme.*

Proof. Let $\mathfrak{p} \in \operatorname{Proj} B$. Then $\mathfrak{q} := \phi^{-1}(\mathfrak{p})$ is a homogeneous ideal of C, and $\mathfrak{q}$ does not contain C_+ if and only if $\mathfrak{p}$ does not contain M. Hence, $f = \phi^{-1}$ gives a map $\operatorname{Proj} B \backslash V_+(M) \to \operatorname{Proj} C$. Now we must verify the properties specified above. Let $h \in C_+$ be homogeneous, i.e. $h \in C_d$ for some $d \geq 1$. Then

$$f^{-1}(D_+(h)) = f^{-1}(\operatorname{Proj} C \backslash V_+(h)) = \operatorname{Proj} B \backslash f^{-1}(V_+(h)) = \operatorname{Proj} B \backslash V_+(\phi(h)) = D_+(\phi(h))$$

which verifies the first property. To check the second property, note that $f|_{D_+(\phi(h))}$ does indeed give a map $\operatorname{Spec} B_{(\phi(h))} \to \operatorname{Spec} C_{(h)}$, due to Proposition 2.102, which then corresponds to a homomorphism $C_{(h)} \to B_{(\phi(h))}$ induced by ϕ.

The last statement of the proposition follows from the preceeding ones by setting $C = R[t_0, \dots, t_n]$ and $B = R[t_0, \dots, t_n]/I$, with ϕ being the canonical projection map. Then $\phi(C_+) = B_+$ so that we get a morphism of R-schemes $f : \operatorname{Proj} B \to \mathbb{P}^n_R$, which has image $V_+(I)$, and furthermore the map $\operatorname{Proj} B \to (V_+(I), f_*\mathcal{O}_{\operatorname{Proj} B})$ is an isomorphism of R-schemes, so that $\operatorname{Proj} B$ is isomorphic to a closed subscheme of $\mathbb{P}^n_R$. ■

Remark 2.109. Observe that the above tells us that (at least some) projective schemes look like zero-sets of homogeneous polynomials. In fact, it is possible to prove that *all* projective schemes are off this form. See, for example, [Liu10, p. 168–169].

In the previous subsection, we saw that k-rational points of certain affine k-schemes corresponded exactly to what one wants them to, i.e. to points in classical affine space satisfying some defining polynomial equations. We want a similar result for projective schemes of the type seen above (or, going by the remark, indeed *all* projective schemes) over fields. To do this, we will first describe what classical projective space looks like.

Definition 2.110. Let k be a field, and let V be a vector space over k. Let $\sim$ be the equivalence relation on $V \backslash \{0\}$ given by $u \sim v$ if there is some $\lambda \in k^\times$ such that $u = \lambda v$. Then define $\mathbb{P}(V) := (V \backslash \{0\}) / \sim$. If V is finite dimensional, then fixing some isomorphism $V \cong k^n$ one denotes the equivalence class of $a = (a_1, \dots, a_n) \in k^n \backslash \{0\}$ in $\mathbb{P}(V)$ as $[a_1 : \dots : a_n]$, and one calls the a_i *homogeneous coordinates.*

This is projective space in the sense of classical projective geometry, i.e. the space of lines passing through the origin of V. In particular, we want rational points of $\mathbb{P}^n_k$ to be points of $\mathbb{P}(k^{n+1})$.

Lemma 2.111. *Let $a = [a_0 : \dots : a_n] \in \mathbb{P}(k^{n+1})$, and set $\rho(a)$ to be the ideal of $k[t_0, \dots, t_n]$ generated by $a_j t_i - a_i t_j$, $0 \leq i, j \leq n$. Then $\rho(a) \in \mathbb{P}^n_k$, and the map $\rho\colon \mathbb{P}(k^{n+1}) \to \mathbb{P}^n_k$ induces a bijection between $\mathbb{P}(k^{n+1})$ and the set of rational points $\mathbb{P}^n_k(k)$.*

Proof. First of all, the map ρ is well defined since k is a field, and that if $[a'_0 : \dots : a'_n]$ are another set of homogeneous coordinates of a, then there is some $c \in k^\times$ such that $a_i = c a'_i$. Then, since ideals allow us to multiply by arbitrary constants, we can just multiply $a'_j t_i - a_i t_j$ by c to get $a_j t_i - a_i t_j$, and similarly one can go the opposite direction using $1/c$.

Since at least one homogeneous coordinate of a is non-zero, we may assume without loss of generality that this coordinate is a_0. Since $\rho(a)$ is generated by homogeneous elements, it is homogeneous. Furthermore, $k[t_0, \dots, t_n]/\rho(a) \cong k[t_0]$ is an integral domain, so $\rho(a)$ is prime. Finally, the irrelevant ideal of $k[t_0, \dots, t_n]$ is the maximal ideal $(t_0, \dots, t_n)$, which $\rho(a)$ clearly does not contain (since then $\rho(a)$ would be equal to it, by maximality, and the quotient would be k, not $k[t_0]$). Hence, $\rho(a) \in \mathbb{P}^n_k$, so we have a map $\mathbb{P}(k^{n+1}) \to \mathbb{P}^n_k$. Now we just need to show that $\rho(a)$ is a rational point.

Since $a_0 \neq 0$, we have that $t_i - a_0^{-1}a_it_0 \in \rho(a)$ for all i, so that $(t_0) \not\subseteq \rho(a)$, i.e. $\rho(a) \in D_+(t_0)$, and so, by Proposition 2.102, corresponds to the ideal of $k[t_0^{-1}t_1, \dots, t_0^{-1}t_n]$ generated by $t_0^{-1}t_i - a_0^{-1}a_i$, $1 \leq i \leq n$. The residue field $k(\rho(a))$ can then be calculated as

$$k(\rho(a)) = \operatorname{Frac}(k[t_0^{-1}t_1, \dots, t_0t_n^{-1}]/(t_0^{-1}t_1 - a_0^{-1}a_1, \dots, t_0^{-1}t_n - a_0^{-1}a_n)) = \operatorname{Frac} k = k$$

so that $\rho(a)$ is a rational point, which gives us that ρ is a map $\mathbb{P}(k^{n+1}) \to \mathbb{P}^n_k(k)$. We now just need to show that it is injective and surjective.

Let $a, b \in \mathbb{P}(k^{n+1})$ be points with homogeneous coordinates $[a_0 : \dots : a_n]$ and $[b_0 : \dots : b_n]$ be such that $\rho(a) = \rho(b)$. We can, as before, assume that $a_0 \neq 0$. Then, one also gets that $b_0 \neq 0$ since otherwise $t_0 \in \rho(b) = \rho(a)$, which cannot happen. Additionally, using the same reasoning as above, $\rho(a)$ corresponds to the ideal generated by the $t_0^{-1}t_i - a_0^{-1}a_i$, and $\rho(b)$ corresponds to the ideal generated by the $t_0^{-1}t_i - b_0^{-1}b_i$, so that $a_i/a_0 = b_i/b_0$ for every i. But then $b_i = (b_0/a_0)a_i$, so that $b = a$ in $\mathbb{P}(k^{n+1})$. From this, the injectivity of ρ follows.

Let $x \in \mathbb{P}^n_k(k)$ be a rational point. We wish to find some $a \in \mathbb{P}(k^{n+1})$ such that $\rho(a) = x$. There is some t_i such that $x \in D_+(t_i)$, and without loss of generality, we may assume that $i = 0$ so that $x \in D_+(t_0)$. Let a_i be the image of $t_0^{-1}t_i \in \mathcal{O}_{\mathbb{P}^n_k}(D_+(t_0))$ in the residue field $k = k(x)$. Then, setting $a = [a_0 : \dots : a_n]$, we clearly have that $\rho(a) = x$. Hence ρ is surjective.

From the above, we conclude that we get a bijection $\rho\colon \mathbb{P}(k^{n+1}) \xrightarrow{\sim} \mathbb{P}^n_k(k)$. ■

The above lemma gives us a partial case of what we want. In general, we will now want points of solutions to systems of polynomial equations in $\mathbb{P}(k^{n+1})$ to correspond to rational points of corresponding projective schemes given by some $\operatorname{Proj} k[t_0, \dots, t_n]/I$.

Definition 2.112. Let $P_1, \dots, P_m \in k[t_0, \dots, t_n]$ be homogeneous polynomials. Let $Z_+(P_1, \dots, P_m)$ denote the set of points $a = [a_0 : \dots : a_n]$ in $\mathbb{P}(k^{n+1})$ such that $P_i(a_0, \dots, a_n) = 0$ for all i.

Remark 2.113. This is well-defined, since if $a = [a_0 : \dots : a_n]$ is a solution, then for any $\lambda \in k^\times$, $\lambda a := [\lambda a_0 : \dots : \lambda a_n]$ is also a solution since the P_i are homogeneous, which implies that $P_i(\lambda a) = \lambda^r P_i(a)$ for some r, i.e. $P_i(a) = 0 \implies P_i(\lambda a) = 0$.

This finally allows us to precisely state what we want:

Proposition 2.114. *Let k be a field, let $P_1, \dots, P_m \in k[t_0, \dots, t_n]$ be homogeneous polynomials, and let $I = (P_1, \dots, P_m)$. Then there is a bijection between $Z_+(P_1, \dots, P_m)$ and the k-rational points of* $\operatorname{Proj} k[t_0, \dots, t_n]/I$.

Proof. Set $B = k[t_0, \dots, t_n]$ and $Z_+ = Z_+(P_1, \dots, P_m)$. By Proposition 2.108, $\operatorname{Proj} B/I$ is isomorphic to a closed subscheme of $\mathbb{P}^n_k$, in particular with image $V_+(I)$. Hence, the rational points of $\operatorname{Proj} B/I$ are in bijection with $V_+(I) \cap \mathbb{P}^n_k(k)$. Now let ρ be the bijection $\mathbb{P}(k^{n+1}) \xrightarrow{\sim} \mathbb{P}^n_k$ from above. The proposition will follow from showing that $\rho(Z_+) = V_+(I) \cap \mathbb{P}^n_k$.

Fix some $0 \leq i \leq n$ and let $U_i = \rho^{-1}(D_+(t_i)(k)) \subseteq \mathbb{P}(k^{n+1})$. Note that U_i consists of those $a = [a_0 : \dots : a_n] \in \mathbb{P}(k^{n+1})$ such that $a_i \neq 0$. We then just have to show that $\rho(Z_+ \cap U_i) = V_+(I) \cap D_+(t_i)(k)$. Letting $p\colon U_i \to k^n$ be the bijection given by

$$[a_0 : \dots : a_n] \mapsto (a_0/a_i, \dots, a_{i-1}/a_i, a_{i+1}/a_i, \dots a_n/a_i),$$

θ be the bijection $D_+(t_i)(k) \xrightarrow{\sim} (\operatorname{Spec} B_{(t_i)})(k)$, and λ be the bijection $k^n \xrightarrow{\sim} (\operatorname{Spec} B_{(t_i)})(k)$ given by the fact that $B_{(t_i)} \cong k[t_0/t_i, \dots, t_n/t_i] \cong k[T_1, \dots, T_n]$, we get a commutative diagram

$$\begin{tikzcd}
U_i \arrow[r, "\rho|_{U_i}"] \arrow[d, "p"] & D_+(t_i)(k) \arrow[d, "\theta"] \\
k^n \arrow[r, "\lambda"] & (\operatorname{Spec} B_{(t_i)})(k)
\end{tikzcd}$$

For a homogeneous polynomial $P \in k[t_0, \dots, t_n]$, set

$$P_{(i)} := P(t_0/t_i, \dots, t_n/t_i) \in B_{(t_i)}.$$

Then, by Proposition 2.89, we have that $(\lambda \circ p)(Z_+ \cap U_i) = V(P_{1(i)}, \dots, P_{m(i)})$, and by Proposition 2.102 we have that

$$\theta(V_+(I) \cap D_+(t_i)(k)) = V(I_{(t_i)})(k) \subseteq \operatorname{Spec} B_{(t_i)}.$$

Finally, $I_{(t_i)}$ is the ideal generated by the $P_{1(i)}, \dots, P_{m(i)}$, so that $\theta(V_+(I) \cap D_+(t_i)(k)) = V(P_{1(i)}, \dots, P_{m(i)}) = (\lambda \circ p)(Z_+ \cap U_i) = (\theta \circ \rho|_{U_i})(Z_+ \cap U_i)$. Since everything is a bijection, we see that $\rho(Z_+ \cap U_i) = V_+(I) \cap D_+(t_i)(k)$, which implies that $\rho(Z_+) = V_+(I) \cap \mathbb{P}^n_k(k)$, which completes the proof. ■

The above proposition justifies why we want to study Proj, why $\mathbb{P}^n_k$ is called projective space, and why projective schemes are in analogy with classical projective varieties. This essentially concludes this subsection on the basic behavior of projective schemes.

2.5 Properties of Schemes

We now want to study some properties of the objects defined in the subsections prior to this, and in particular the behavior of a certain operation that can be defined for them: the fiber product. The fiber product is a powerful tool for studying schemes, since it happens to preserve many of the features of interest that a scheme may have (e.g. there are a number of theorems on cohomology regarding its behavior under certain fiber products). Fiber products also allow us to get a generalization of the characterization of rational points on a nice scheme, i.e. of similar types as in Proposition 2.89 and in Proposition 2.114.

The way one defines the fiber product is perhaps somewhat different from how one usually conceptualizes a product in many mathematical disciplines. For example, in many cases, one may simply give an explicit description of the product (e.g. the product $A \times B$ of two sets A, B being the pairs of elements (a, b) with $a \in A$, $b \in B$). In the case of schemes, however, one begins by defining the (fiber) product in the categorical sense, and then showing that there exists an object which satisfies the required property, without ever specifying what it explicitly looks like in the general case.

Definition 2.115. Let $\mathcal{C}$ be a category, let $S \in \mathcal{C}$, and let $(f : X \to S), (g : Y \to S) \in \mathcal{C}/S$. The *fiber product* of X and Y over S, is an object $X \times_S Y$ equipped with S-morphisms (i.e. morphisms in $\mathcal{C}/S$) $\pi_X : X \times_S Y \to X$ and $\pi_Y : X \times_S Y \to Y$ (called the *projections*) such that if Z is any other object with S-morphisms $p\colon Z \to X$, $q\colon Z \to Y$ then there exists a unique map $p \times_S q\colon Z \to X \times_S Y$ making the following diagram commute:

$$\begin{tikzcd}
 & Z \arrow[dl, "p"'] \arrow[d, dashed, "p \times_S q"] \arrow[dr, "q"] & \\
X & X \times_S Y \arrow[l, "\pi_X"] \arrow[r, "\pi_Y"'] & Y
\end{tikzcd}$$

Remark 2.116. Note that, while it isn't usually included in the notation, the maps f, g specifying the S-object structure of X and Y are very significant in the structure of $X \times_S Y$.

Remark 2.117. There is another way to characterize this construction. Here, we essentially define the fiber product $X \times_S Y$ as the product in $\mathcal{C}/S$, but we can equivalently define it within the category $\mathcal{C}$ as the limit of the diagram

$$\begin{tikzcd} & Y \arrow[d, "g"] \\ X \arrow[r, "f"] & S \end{tikzcd}$$

which also gives an important mental image of what one can use the fiber product for: if X and Y are S-objects, then we can construct from this a Y-object $X \times_S Y$, which arises in the diagram

$$\begin{tikzcd} X \times_S Y \arrow[r, "\pi_Y"] \arrow[d, "\pi_X"] & Y \arrow[d, "g"] \\ X \arrow[r, "f"] & S \end{tikzcd}$$

with π_Y giving the structure morphism as a Y-object. This is one of the reasons fiber products are also called *pullbacks*, since in a sense one is "pulling back" the object X along the map g to get $X \times_S Y$. Note that if S is a terminal object, then the fiber product $X \times_S Y$ coincides with the regular categorical product $X \times Y$.

Having defined what a fiber product should be in a general category (and hence in the cateogry **Sch** of schemes), we now turn our attention to if it actually exists, and how to compute it in special cases. Recall from an earlier comment that we cannot directly compute it in general; we can, however, compute it in the affine case, then glue these together in the general case to show existence.

We begin with lemmas showing that we can, in fact, glue compatible schemes and morphisms together:

Lemma 2.118. *Let X, Y be schemes, let $\{U_i\}_{i\in I}$ be a covering of X, and let $f_i \colon U_i \to Y$ be morphisms such that $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$. Then there exists a unique morphism $f \colon X \to Y$ such that $f|_{U_i} = f_i$.*

Proof. On the topological space level, the map f is simply given by setting $f(x) = f_i(x)$ if $x \in U_i$, and this is well defined since the f_i agree on intersections. To get the required map $f^\sharp \colon \mathcal{O}_Y \to f_*\mathcal{O}_X$, note that (setting h_i to be the inclusion $U_i \to X$) we have maps

$$f_i^\sharp \colon \mathcal{O}_Y \to f_{i,*}\mathcal{O}_{U_i} = f_{i,*}h_i^{-1}\mathcal{O}_X$$

and that we can specify the map $f^\sharp$ by specifying it for all open sets $V \subseteq Y$. In particular, letting V be such an open set, we consider $s_i = f_{i,V}^\sharp(s) \in \mathcal{O}_{U_i}(f^{-1}(V)) = \mathcal{O}_X(f^{-1}(V) \cap U_i) = \mathcal{O}_X(f_i^{-1}(V))$. We want to show that $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$ so that we can glue these together to get a section $s \in \mathcal{O}_X(f^{-1}(V))$. Set $f_{ij} = f_i|_{U_i\cap U_j}$, so that $f_{ij} = f_{ji}$. Then note that $s_i|_{U_i\cap U_j} = f_{ij,V}^\sharp(s) = f_{ji,V}^\sharp(s) = s_j|_{U_i\cap U_j}$ so we are done since this defines a map $\mathcal{O}_Y \to f_*\mathcal{O}_X$. Uniqueness follows from the fact that morphisms are determined by their constituent parts. ■

Lemma 2.119. *Let S be a scheme, and let $\{X_i\}_{i\in I}$ be a family of S-schemes. Suppose there exists open subschemes X_{ij} of X_i and isomorphisms of S-schemes $f_{ij} : X_{ij} \xrightarrow{\sim} X_{ji}$ such that $f_{ii} = \mathrm{id}_{X_i}$, $f_{ij}(X_{ij} \cap X_{ik}) = X_{ji} \cap X_{jk}$, and $f_{ik} = f_{jk} \circ f_{ij}$ on $X_{ij} \cap X_{ik}$. Then there exists an S-scheme X, which is unique up to isomorphism, along with open immersions $g_i \colon X_i \to X$ such that $g_i = g_j \circ f_{ij}$ on X_{ij}, and $X = \bigcup_{i\in I} g_i(X_i)$.*

Proof. The underlying topological space is constructed as follows: $X = (\coprod_{i\in I} X_i) / \sim$, where $x \sim y$ if $x \in X_i$, $y \in X_j$, and $y = f_{ij}(x)$. Endow this with the quotient topology. This immediately gives topological open immersions $g_i : X_i \hookrightarrow X$ such that $g_i = g_j \circ f_{ij}$. Set

$U_i = g_i(X_i)$, and set $\mathcal{O}_{U_i} := g_{i,*}\mathcal{O}_{X_i}$. If $V \subseteq U_i \cap U_j$ is some open set, then $\mathcal{O}_{U_i}(V) = \mathcal{O}_{X_i}(g_i^{-1}(V)) = \mathcal{O}_{X_i}((f_{ji} \circ g_j^{-1})(V)) = \mathcal{O}_{X_j}(g_j^{-1}(V)) = \mathcal{O}_{U_j}(V)$, so that $\mathcal{O}_{U_i}|_{U_i \cap U_j} = \mathcal{O}_{U_j}|_{U_i \cap U_j}$. Hence we can define the sheaf $\mathcal{O}_X$ on X to be such that $\mathcal{O}_X|_{U_i} = \mathcal{O}_{U_i}$. Then $(X, \mathcal{O}_X)$ is a scheme, and the g_i determine isomorphisms $X_i \cong U_i$. Now we just need to construct the structure morphism $X \to S$, which we do by utilizing Lemma 2.118. In particular, let $h_i : U_i \to S$ be the composition of g_i^{-1} and the structure morphism $X_i \to S$. Then $h_i|_{U_i \cap U_j} = h_j|_{U_i \cap U_j}$, so we may glue these to a unique morphism $h \colon X \to S$ which is by construction compatible with the S-scheme structures on the X_i. The uniqueness follows from the fact that if there were any other "gluing" of the X_i's, the induced isomorphisms would glue to an isomorphism with X. ■

Proposition 2.120. *Let S be a scheme, and let X, Y be S-schemes. Then the fiber product $X \times_S Y$ exists and is unique up to unique isomorphism. If S, X and Y are affine, then $X \times_S Y = \operatorname{Spec}(\mathcal{O}_X(X) \otimes_{\mathcal{O}_S(S)} \mathcal{O}_Y(Y))$, with the projection maps induced by the canonical morphisms $\mathcal{O}_X(X) \to \mathcal{O}_X(X) \otimes_{\mathcal{O}_S(S)} \mathcal{O}_Y(Y)$ and $\mathcal{O}_Y(Y) \to \mathcal{O}_X(X) \otimes_{\mathcal{O}_S(S)} \mathcal{O}_Y(Y)$.*

Proof. First of all, supposing the fiber product exists, the uniqueness up to unique isomorphism follows directly from the universal property, and this is easy (though somewhat notationally tedious) to check. The proof is in essence identical to that of Proposition 2.11, whereby one constructs maps that must be unique and must compose to the identity in both directions, i.e. are isomorphisms. Second, note that if the fiber product $X \times_S Y$ exist, then it also satisfies the universal property of $Y \times_S X$, and so that too exists, and furthermore they are uniquely isomorphic. Third, if $X \times_S Y$ exists and U is an open subscheme of X, then $U \times_S Y$ also exists, since $(\pi_X^{-1}(U), \pi_X|_{\pi_X^{-1}(U)}, \pi_Y|_{\pi_X^{-1}(U)})$ satisfies the required universal property.

We now consider showing existence in the completely affine case, i.e. $S = \operatorname{Spec} A$, $X = \operatorname{Spec} B$ and $Y = \operatorname{Spec} C$. Setting $W = \operatorname{Spec}(B \otimes_A C)$, we get (from the maps $B \to B \otimes_A C$ and $C \to B \otimes_A C$) maps $p \colon W \to X$ and $q \colon W \to Y$. Now, to check the universal property, consider an S-scheme (i.e. an A-scheme) Z with maps $f : Z \to X$ and $g \colon Z \to Y$. By Proposition 2.72, this corresponds to maps $B \to \mathcal{O}_Z(Z)$ and $C \to \mathcal{O}_Z(Z)$. The universal property of the tensor product (more accurately, this is an direct but not immediate consequence of it), there then exists a unique map $B \otimes_A C \to \mathcal{O}_X(Z)$ commuting with the maps of B, C to Z, so that we get the required map $Z \to W$.

Now consider the case when X is not affine. Choose an affine open cover $\{U_i\}_{i \in I}$ of X. Then the fiber products $U_i \times_S Y$ exist. Let $p_i \colon U_i \times_S Y \to U_i$ and $q_i \colon U_i \times_S Y \to Y$ denote the projections of these. Then for all i, j, by the third point above, we have that $(U_i \cap U_j) \times_S Y = p_i^{-1}(U_i \cap U_j) = p_j^{-1}(U_i \cap U_j)$ which determines a unique isomorphism $f_{ij} : p_i^{-1}(U_i \cap U_j) \xrightarrow{\sim} p_j^{-1}(U_i \cap U_j)$. If $i, j, k \in I$ then $f_{ik} = f_{jk} \circ f_{ij}$ due to the uniqueness of the isomorphism

$$p_i^{-1}(U_i \cap U_j \cap U_k) \xrightarrow{\sim} p_k^{-1}(U_i \cap U_j \cap U_k).$$

Therefore, by Lemma 2.119, we can glue these schemes together to form a scheme W. Since all the f_{ij} are compatible with the X-scheme and Y-scheme structures of the $U_i \times_S Y$, this combines to give projections $p \colon W \to X$ and $q \colon W \to Y$ by Lemma 2.118. Let Z be a scheme with maps $f \colon Z \to X$ and $g \colon Z \to Y$, let $Z_i := f^{-1}(U_i)$, and let $f_i := f|_{Z_i}, g_i := g|_{Z_i}$. Note that $\{Z_i\}_{i \in I}$ gives a cover of Z. Now, this gives us maps $f_i \times_S g_i \colon Z_i \to U_i \times_S Y$, which further gives us maps $h_i \colon Z_i \to W$ (with h_i being the composition of $f_i \times_S g_i$ with the open immersion $U_i \times_S Y \to W$) which agree on overlapping sets, so again by Lemma 2.118 we may glue these to a unique map $h \colon Z \to W$, which by definition makes the desired diagram commute, so that $W = X \times_S Y$.

Now consider the case when X and Y are arbitrary, and S is affine. Choosing an affine open cover $\{U_i\}_{i \in I}$ of Y, we see (by the symmetry mentioned in the second point discussed at the start) that $X \times_S U_i$ exists for all $i \in I$. Following the same proceedure as in the above paragraph, we glue these together to get the fiber product $X \times_S Y$.

Finally, consider the case when S is not affine. Let $\{S_i\}_{i\in I}$ be an affine open cover of S, let f (resp. g) denote the structure morphism of X (resp. Y), and let $X_i = f^{-1}(S_i)$, $Y_i = g^{-1}(S_i)$. Now note that X_i and Y_i are S_i-schemes, so that we may take the fiber product $X_i \times_{S_i} Y_i$ (and this exists since S_i is affine). Since every S_i scheme is in a natural way an S-scheme (by composing with the open immersion $S_i \to S$), we have that $X_i \times_S Y_i = X_i \times_{S_i} Y_i$. Set $W_i = X_i \times_S Y_i$, and set $W_{ij} = (X_i \cap X_j) \times_S (Y_i \cap Y_j) \subseteq W_i, W_j$. Then clearly $W_{ij} \cong W_{ji}$ (via the identity), and so the requirements of Lemma 2.119 follow trivially, giving that we can glue these together to get a scheme W. Following similar reasoning as the above paragraphs, this is the fiber product $X \times_S Y$. ■

Remark 2.121. For notational purposes, when $S = \operatorname{Spec} R$ one usually writes $X \times_R Y$ instead of $X \times_{\operatorname{Spec} R} Y$.

Example 2.122. A good example of an easy application of the above is that $\mathbb{A}^n_k \times \mathbb{A}^m_k \cong \mathbb{A}^{n+m}_k$. This follows from the affine part of the above proposition, and from the fact that

$$k[x_1, \dots, x_n] \otimes_k k[t_1, \dots, t_m] = k[x_1, \dots, x_n, t_1, \dots, t_m] = k[x_1, \dots, x_{n+m}].$$

Remark 2.123. From the complexity of the above proof, it should be relatively clear that (denoting the underlying space by $\operatorname{sp}(\cdot)$) $X \times_S Y$ in general does not have the underlying space $\operatorname{sp}(X) \times_{\operatorname{sp}(S)} \operatorname{sp}(Y)$. However, this is where there is some magical interaction with rational points: by the universal property, the map $\operatorname{Hom}_{\mathbf{Sch}/S}(Z, X \times_S Y) \to \operatorname{Hom}_{\mathbf{Sch}/S}(Z, X) \times \operatorname{Hom}_{\mathbf{Sch}/S}(Z, Y)$, induced by the maps

$$\operatorname{Hom}_{\mathbf{Sch}/S}(Z, X \times_S Y) \to \operatorname{Hom}_{\mathbf{Sch}/S}(Z, X) \quad \text{and} \quad \operatorname{Hom}_{\mathbf{Sch}/S}(Z, X \times_S Y) \to \operatorname{Hom}_{\mathbf{Sch}/S}(Z, Y)$$

given by composition with the projections, is a bijection. Recall in other notation that this says that $(X \times_S Y)(Z) \cong X(Z) \times Y(Z)$. Furthermore, if we set $Z = Y$ then we get that $(X \times_S Y)(Y) \cong X(Y) \times Y(Y)$. If we then recognize that $X \times_S Y$ is also a Y-scheme, then we can consider what happens when we restrict to the subset of $(X \times_S Y)(Y)$ which consists of only those morphisms that are also Y-morphisms, which gives that $\operatorname{Hom}_{\mathbf{Sch}/Y}(Y, X \times_S Y) \cong X(Y)$. This leads well into the next topic, namely that of *base change*.

Definition 2.124. Let S be a scheme, and let X, Y be S-schemes. The scheme $X \times_S Y$ when endowed with the structure of a Y-scheme using the second projection is called the *base change* by $Y \to S$, and is usually denoted X_Y. If $f : X \to Z$ is a morphism of schemes, then we sometimes denote the induced morphism $f \times \mathrm{id}_Y : X_Y \to Z_Y$ by f_Y.

Remark 2.125. As with the general fiber product, one usually alters the notation to write X_R and f_R when $Y = \operatorname{Spec} R$ for convenience.

Remark 2.126. Note that we can rephrase $\operatorname{Hom}_{\mathbf{Sch}/Y}(Y, X \times_S Y) = X(Y)$ as $X_Y(Y) = X(Y)$, stating essentially that Y-rational points are invariant under base change by Y. This immediately gives us a route towards a generalization of Proposition 2.89 and Proposition 2.114.

Lemma 2.127. *Let R be a ring, let B be a graded R-algebra, and let C be an R-algebra. Then there is a canonical isomorphism*

$$\operatorname{Proj}(B \otimes_R C) \cong \operatorname{Proj} B \times_R \operatorname{Spec} C.$$

Proof. See [Liu10, p. 82, Prop. 1.9]. ■

Remark 2.128. As an aside, this lemma leads to a fun consequence. While it is not true that $\mathbb{P}^1_k \times_k \mathbb{P}^1_k$ gives us $\mathbb{P}^2_k$, it *is* true that $\mathbb{P}^2_k = \mathbb{P}^1_k \times_k \mathbb{A}^1_k$. In fact, one gets that $\mathbb{P}^n_k = \mathbb{P}^1_k \times \mathbb{A}^{n-1}_k$.

Proposition 2.129. *Let X be a k-scheme, and let K/k be a field extension. Then:*

(a) if X is a closed subscheme $V(I)$ of $\mathbb{A}^n_k$, then $X(K)$ can be identified with

$$\{p \in K^n \mid \forall f \in I,\ f(p) = 0\};$$

(b) if X is a closed subscheme $V_+(I)$ of $\mathbb{P}^n_k$, then $X(K)$ can be identified with

$$\{p \in \mathbb{P}(K^{n+1}) \mid \forall f \in I,\ f(p) = 0\}.$$

Proof. This follows by applying Proposition 2.89 and Proposition 2.114 together with Lemma 2.127 to X_K, and noting that $X_K(K) \cong X(K)$. ■

This gives us a good geometric characterization of the K-rational points of suitable k-schemes. There is one further characterization that may be of interest, which is more similar to that of Proposition 2.86. Recall, however, that identifying the K-rational points of a scheme is not as simple as identifying the points with residue field lying in K. Instead, we have the following:

Proposition 2.130. *Let K/k be a field extension, let X be a k-scheme, and let $s \in X(K)$. Then s is uniquely determined by a point $x \in X$ with a homomorphism of k-algebras $k(x) \to K$. Furthermore, if K'/K is a field extension, then there is a natural inclusion $X(K) \subseteq X(K')$.*

Proof. Let $s \in X(K)$, and let $x \in X$ be the image of s. Then we get an induced morphism $s^\sharp_x : \mathcal{O}_{X,x} \to K$, which further induces a morphism of k-algebras $\mathcal{O}_{X,x}/\mathfrak{m}_x = k(x) \to K$. Now, if $x \in X$ and we are given a map $k(x) \to K$ of k-algebras, then this induces a morphism of affine schemes $\operatorname{Spec} K \to \operatorname{Spec} k(x)$, which we can then compose with the canonical morphism $\operatorname{Spec} k(x) \to X$ to get a K-rational point $\operatorname{Spec} K \to X$ (this, in particular, is because the map $k(x) \to K$ is a morphism of k-algebras, not just of fields). This has image x and clearly produces the given map $k(x) \to K$, so that the two operations described are inverses of each other.

Now, if K'/K is another extension, we get an induced morphism $\operatorname{Spec} K' \to \operatorname{Spec} K$, which by composition induces a map $X(K) \to X(K')$. This map is injective by the above. ■

Remark 2.131. This tells us why it isn't enough to find points $x \in X$ with $k(x) \subseteq K$: it is possible for several K-rational points to be "glued" to the same point $x \in X$. The ambiguity then arises from the Galois group $\operatorname{Gal}(K/k)$ generally being non-trivial. A good example of this is to consider the real affine line $\mathbb{A}^1_\mathbb{R}$ and the complex affine line $\mathbb{A}^1_\mathbb{C}$. The Galois group $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ consists of exactly one non-trivial automorphism, namely complex conjugation, and a point in $\mathbb{A}^1_\mathbb{R}$ generally looks like either $(t - r)$, for $r \in \mathbb{R}$, or like some quadratic $(t^2 + at + b)$, which then determines *two* complex numbers. In other words, geometrically the real affine line looks like the complex plane folded in half, i.e. with complex conjugates glued together. This also follows from the above proposition, since we then see that if we pick any non-real point $x = (t^2 + at + b) \in \mathbb{A}^1_\mathbb{R}$, then $k(x) = \mathbb{C}$ and $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ allows us two ways to automorphically map $\mathbb{C}$ to $\mathbb{C}$.

When we move to the complex affine line, however, we somehow "unglue" the conjugate-identified points, so that points of $\mathbb{A}^1_\mathbb{C}$ are essentially in bijection with points of $\mathbb{C}$ (excluding the generic point). It should be further noted that $(\mathbb{A}^1_\mathbb{R})_\mathbb{C} = \mathbb{A}^1_\mathbb{C}$ since $\mathbb{R}[t] \otimes \mathbb{C} = \mathbb{C}[t]$, so that this observation ties in with Proposition 2.129.

Since the above proposition tells us that $X(k) \subseteq X(K)$ when K/k is a field extension, there is a reasonable question if we can somehow identify which K-rational points are also k-rational. There is some precedent for this: consider the natural action of $G = \operatorname{Gal}(K/k)$ (with K/k being some reasonably nice field extension) on K. We can identify the field k as the field that is fixed by every element of G. Similarly, if we consider the natural action of G on K^n, then we see that we can identify k^n with the subset of K^n fixed by G. Hence, there should be some analogous action of G on $X(K)$ (induced by an action on X) whose fixed points are given by $X(k)$. First of all, what do we mean by a group G acting on a scheme?

Definition 2.132. Let S be a scheme, and let X be an S-scheme. The *automorphism group* of X is the group of S-automorphisms of X, i.e. the subset $\operatorname{Aut}_S(X) \subseteq \operatorname{Hom}_{\mathbf{Sch}/S}(X, X)$ of isomorphisms equipped with the group structure given by composition. When the scheme S is obvious, we simply denote this by $\operatorname{Aut}(X)$ rather than $\operatorname{Aut}_S(X)$, and when $S = \operatorname{Spec} R$ we write $\operatorname{Aut}_R(X)$ instead of $\operatorname{Aut}_{\operatorname{Spec} R}(X)$.

Definition 2.133. Let S be a scheme, let X be an S-scheme, and let G be a group. An *action* of G on X is a group homomorphism $G \to \operatorname{Aut}_S(X)$.

Remark 2.134. Let K/k be a galois extension. Then $G = \operatorname{Gal}(K/k)$ acts on $\operatorname{Spec} K$ in a natural way: each $\sigma\colon K \to K$ induces an automorphism of k-schemes $\operatorname{Spec}\sigma\colon \operatorname{Spec} K \to \operatorname{Spec} K$, i.e. an element of $\operatorname{Aut}_k(\operatorname{Spec} K)$, so we get a map $G \to \operatorname{Aut}(\operatorname{Spec} K)$. Furthermore, if X is a k-scheme, then we get an action $G \to \operatorname{Aut}_k(X_K)$ given by $\sigma \mapsto \operatorname{id}_X \times_k (\operatorname{Spec}\sigma)$. Using the fact that $X_K(K) = X(K)$, this then gives an action of G on $X(K)$. When X is, for example, a closed subscheme $V(I)$ of $\mathbb{A}^n_k$, then the action of $\sigma \in G$ on a point $x = (x_1, \ldots, x_n) \in X(K)$ (using the identification from Proposition 2.129) is given by $\sigma(x) = (\sigma(x_1), \ldots, \sigma(x_n))$, i.e. coincides with the natural action on K^n.

Proposition 2.135. *Let K/k be a Galois extension, let X be a k-scheme, and let $G = \operatorname{Gal}(K/k)$. Then, letting G act on $X(K)$ as above, we have that the fixed points of the action are the k-rational points of X, i.e. $X(K)^G = X(k)$.*

Proof. Let $\rho \in X(K)$, and let x be the image of ρ in X. Then by Proposition 2.130, ρ is uniquely determined by an associated morphism of k-algebras $\alpha\colon k(x) \to K$. If $\sigma \in G$, then the action on ρ is given by composing σ with α, i.e. it sends ρ to the point determined by x and $\sigma \circ \alpha$. If we then want $\sigma(\rho) = \rho$, it must be that the map α is left unchanged, i.e. the image of α is an invariant subfield of K. Hence, it must be that if $\rho \in X(K)^G$ (i.e. ρ is fixed by *every* $\sigma \in G$) then $\rho \in X(k)$. ■

As we saw in Remark 2.131, the action of base change can provide finer information of a scheme by ungluing points and such. This tells us that we should be interested not only in the scheme itself, but how it looks under base change by various extensions of the base field. In particular, we will be interested in properties that appear when one base changes by the algebraic closure.

Definition 2.136. Let k be a field, $\bar{k}$ its algebraic closure, and let X be a k-scheme. Let $\mathcal{P}$ be some property that a (k-)scheme can have (e.g. being connected as a topological space). We say the the property $\mathcal{P}$ holds *geometrically* if $\mathcal{P}$ holds for $X_{\bar{k}}$ (e.g. X is *geometrically connected* if $X_{\bar{k}}$ is connected).

The example of being geometrically connected will be of particular interest later when we discuss genus with regards to Riemann–Roch.

For the next part, we will begin with an example (which will also serve as motivation for models and reduction later). In particular, this will demonstrate how schemes can in some sense "parametrize" families of schemes in a natural way.

Example 2.137. Consider the $\mathbb{Z}$-scheme $\mathbb{A}^1_{\mathbb{Z}} = \operatorname{Spec}\mathbb{Z}[t]$ with structure morphism π induced by the unique homomorphism $\mathbb{Z} \to \mathbb{Z}[t]$. What does $\mathbb{A}^1_{\mathbb{Z}}$ actually "look like"? We should think of it as lying "over" $\operatorname{Spec}\mathbb{Z}$, which itself can be thought of as a line consisting of the prime numbers $p \in \mathbb{Z}$ and some kind of "point at infinity" which really lies everywhere, i.e. the generic point determined by the ideal (0). So we can then restrict ourselves to determining what $\mathbb{A}^1_{\mathbb{Z}}$ looks like "above" a given prime number $p \in \mathbb{Z}$, i.e. computing what $\pi^{-1}(p)$ is. A prime ideal of $\mathbb{Z}[t]$ is either of the form $(f(t))$ for an irreducible polynomial $f \in \mathbb{Z}[t]$, or of the form $(p, f(t))$. In particular, $\pi((p, f(t))) = (p)$, so that $\pi^{-1}(p)$ consists of the points of $\mathbb{A}^1_{\mathbb{Z}}$ that are of that form. Further, note that if $g \in (p, f(t))$ then $pg \in (p, f(t))$, i.e. $\mathbb{Z}[t]/(p, f(t)) = \mathbb{F}_p[t]/(f(t))$. In other words, in some sense we can think of $(p, f(t))$ as encoding the polynomial $f(t)$ modulo p, so that $\pi^{-1}(p) = \{\text{irreducible polynomials}/\mathbb{F}_p\} = \mathbb{A}^1_{\mathbb{F}_p}$. The part of $\mathbb{A}^1_{\mathbb{Z}}$ that lies over the generic point can also be characterized like this: if $g \in \mathbb{Q}[t]$ is irreducible, then we get an irreducible polynomial $h \in \mathbb{Z}[t]$ given by clearing the denominators of g, and further we get that $(h) = (g)$ in $\mathbb{Q}[t]$. In other words, the set of ideals $(f(t))$ generated by irreducible polynomials $f \in \mathbb{Z}[t]$ is the same as the set of ideals generated by irreducible polynomials of $\mathbb{Q}[t]$, i.e. $\pi^{-1}(0) = \mathbb{A}^1_{\mathbb{Q}}$.

This tells us that $\mathbb{A}^1_{\mathbb{Z}}$ can be thought of as a combination of the affine lines $\mathbb{A}^1_{\mathbb{Q}}$, and $\mathbb{A}^1_{\mathbb{F}_p}$ with $p \in \mathbb{Z}$ prime, i.e. the structure morphism $\mathbb{A}^1_{\mathbb{Z}} \to \operatorname{Spec}\mathbb{Z}$ parametrizes these schemes. The only difficulty here is that we have not yet ensured that the inverse images of π can actually be given structures of schemes, but this is solved using the fiber product.

Definition 2.138. Let $f\colon X \to Y$ be a morphism of schemes. For a point $y \in Y$, the *fiber of f over y* is

$$X_y := X \times_Y \operatorname{Spec} k(y).$$

X_y is a $k(y)$-scheme via the second projection map.

Proposition 2.139. *Let X, Y be schemes, let $f : X \to Y$ be a morphism of schemes, and let $y \in Y$. Then the first projection map $X \times_Y \operatorname{Spec} k(y) \to X$ induces a homeomorphism $X_y \cong f^{-1}(y)$, and we can endow $f^{-1}(y)$ with a natural scheme structure so that this is an isomorphism of schemes.*

Proof. In general, this is hard, so we want to reduce to an easier case. For notation, denote by $\pi_X\colon X_y \to X$ and $\pi_y\colon X_y \to \operatorname{Spec} k(y)$ the projections.

First, note for $V = \operatorname{Spec} A$ an affine open neighbourhood of y that $X \times_Y \operatorname{Spec} k(y) = (X \times_Y V) \times_V \operatorname{Spec} k(y)$. Furthermore, from the proof of the existence of the fiber product, we have that $X \times_Y V = f^{-1}(V)$, so that $X_y = f^{-1}(V)_y$. Hence, we can restrict our interest to this affine neighbourhood, i.e. we can assume that $Y = V = \operatorname{Spec} A$ is affine. Actually, one may reduce one more step, since again by the proof of the existence of the fiber product, we have that if $U \subseteq X$ is any open subset of X, then $\pi_X^{-1}(U) = U \times_Y \operatorname{Spec} k(y)$. Because $f^{-1}(V)$ is an open subscheme of X, it can be covered by affine open subsets $\{U_i\}$ of X so that $X_y = f^{-1}(V)_y$ is the union of the $U_{i,y} = \pi_X^{-1}(U_i)$'s, i.e. we may assume that $X = \operatorname{Spec} B$ too is affine.

Having made these reductions we are left with a morphism $f : \operatorname{Spec} B \to \operatorname{Spec} A$. Let $\mathfrak{p} \in \operatorname{Spec} A$ be the prime ideal associated to y, let $p_1 : X \times_Y \operatorname{Spec} A_{\mathfrak{p}} \to X$ be the morphism associated to the canonical homomorphism $B \to B \otimes_A A_{\mathfrak{p}} = B_{\mathfrak{p}}$, and let $p_2\colon X_y \to X \times_Y \operatorname{Spec} A_{\mathfrak{p}}$ be the morphism associated to the canonical surjection $B \otimes_A A_{\mathfrak{p}} \to B \otimes_A k(\mathfrak{p})$ (induced by $k(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$). Then $\pi_X = p_1 \circ p_2$. By Proposition 2.46, since p_1 is a localization, we have that π_X gives a homeomorphism $X_y \xrightarrow{\sim} \{\mathfrak{q} \in X = \operatorname{Spec} B \mid \mathfrak{q} \supseteq \mathfrak{p}B \text{ and } \mathfrak{q} \cap f_Y^{\sharp}(A \backslash \mathfrak{p}) = \emptyset\}$, i.e. $(f_Y^{\sharp})^{-1}(\mathfrak{q}) = \mathfrak{p}$, so that $f(\mathfrak{q}) = \mathfrak{p} = y$. Hence $X_y \cong f^{-1}(y)$.

Let $i : X_y \xrightarrow{\sim} f^{-1}(y)$ be the above isomorphism. The last statement of the proposition follows immediately from giving $f^{-1}(y)$ the structure sheaf $i_*\mathcal{O}_{X_y}$, and this also immediately gives that the induced morphism $X_y \to (f^{-1}(y), i_*\mathcal{O}_{X_y})$ (given by $(i, \mathrm{id}_{i_*\mathcal{O}_{X_y}})$) of schemes is an isomorphism. ■

Remark 2.140. This proposition clarifies how one can regard a morphism $X \to Y$ of schemes as a "parametrization" of a family of $k(y)$-schemes X_y, $y \in Y$. In the above example, taking $X = \mathbb{A}^1_{\mathbb{Z}}$, the morphism $X \to \operatorname{Spec}\mathbb{Z}$ does exactly this, since for a prime $p \in \operatorname{Spec}\mathbb{Z}$, the fiber over p is $X_p = \operatorname{Spec}\mathbb{Z}[t] \times_{\mathbb{Z}} \operatorname{Spec}\mathbb{F}_p = \operatorname{Spec}(\mathbb{Z}[t] \otimes_{\mathbb{Z}} \mathbb{F}_p) = \operatorname{Spec}\mathbb{F}_p[t] = \mathbb{A}^1_{\mathbb{F}_p}$, and similarly the fiber over the generic point (since $\mathbb{Z}_{(0)} = \mathbb{Q}$) is given by $X_{(0)} = \operatorname{Spec}(\mathbb{Z}[t] \otimes_{\mathbb{Z}} \mathbb{Q}) = \mathbb{A}^1_{\mathbb{Q}}$. This last fiber has a name in general:

Definition 2.141. Let X be a topological space. X is said to be *irreducible* if whenever U, V are closed sets of X with $X = U \cup V$, then $U = X$ or $V = X$. A scheme X is said to be irreducible if it is irreducible as a topological space. Any irreducible topological space X has a point $\xi \in X$ such that $X = \overline{\{\xi\}}$, called a *generic point*.

Definition 2.142. Let $f \colon X \to Y$ be a morphism of schemes with Y irreducible, and let $\xi \in Y$ be the generic point. The fiber X_ξ over ξ is called the *generic fiber*.

Example 2.143. As we saw above, if we let $X = \mathbb{A}^1_{\mathbb{Z}}$, $Y = \operatorname{Spec}\mathbb{Z}$ and let f be the unique structure morphism, then the generic fiber X_ξ is given by $\mathbb{A}^1_{\mathbb{Q}}$.

Remark 2.144. All of the above has a natural generalization to $X = \mathbb{A}^n_{\mathbb{Z}}$. In particular, if $y \in \operatorname{Spec}\mathbb{Z}$ is any point, then $X_y = X \times_{\mathbb{Z}} \operatorname{Spec} k(y) = \operatorname{Spec}(\mathbb{Z}[t_1, \dots, t_n] \otimes k(y)) = \mathbb{A}^n_{k(y)}$. In fact, this computation always works: let S be any scheme, let $\mathbb{A}^n_S := \mathbb{A}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S$, and consider this as an S-scheme. Then if $y \in S$ we have

$$\mathbb{A}^n_{S,y} = (\mathbb{A}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S) \times_S \operatorname{Spec} k(y) = \mathbb{A}^n_{\mathbb{Z}} \times_{\mathbb{Z}} \operatorname{Spec} k(y) = \mathbb{A}^n_{k(y)},$$

and note that this generalizes the previous statement since if $S = \operatorname{Spec} R$ then $\mathbb{A}^n_S = \mathbb{A}^n_R$. Furthermore, one can even do this with projective space: let $\mathbb{P}^n_S := \mathbb{P}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S$. Then one has, by Lemma 2.127, that

$$\mathbb{P}^n_{S,y} = (\mathbb{P}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S) \times_S \operatorname{Spec} k(y) = \mathbb{P}^n_{\mathbb{Z}} \times_{\mathbb{Z}} \operatorname{Spec} k(y) = \operatorname{Proj}(\mathbb{Z}[t_1, \dots, t_n] \otimes k(y)) = \mathbb{P}^n_{k(y)},$$

so that, for example, if $X = \mathbb{P}^1_{\mathbb{Z}}$ with canonical morphism $X \to \operatorname{Spec}\mathbb{Z}$, we have that the generic fiber is $X_\xi = \mathbb{P}^1_{\mathbb{Q}}$.

For a good part of the later sections, we will be interested in *curves*. This requires that we should be able to talk about the dimension of a scheme. The idea here is similar to how one defines the dimension of a vector space: one can think of the dimension of a vector space V as being the supremum of the lengths of chains of linearly independent elements, i.e. chains of subsets of V of the form $\emptyset \subset \{e_1\} \subset \{e_1, e_2\} \subset \cdots \subset \{e_1, \dots, e_n\}$ with the e_i's linearly independent, where one defines the length of such a chain to be n. One can think of this as representing chains of subspaces $0 \subset \operatorname{Span}(e_1) \subset \cdots \subset \operatorname{Span}(e_1, \dots, e_n)$, i.e. "irreducible" parts of V. This is also how one defines the *Krull* dimension of a topological space.

Definition 2.145. Let X be a topological space. A *chain of irreducibles* in X is a strictly increasing sequence of irreducible closed subsets of X

$$\emptyset \subset Z_1 \subset \cdots \subset Z_n \subseteq X.$$

The length of such a sequence is defined to be n.

Definition 2.146. Let X be a topological space. The *Krull dimension* (or, for convenience, sometimes just the *dimension*) of X is the supremum of lengths of chains of irreducibles in X, and we denote this by $\dim X$. The dimension of a scheme is the dimension of the underlying topological space.

How do we know that this will behave the way we want? We will, for example, certainly want $\dim \mathbb{A}_k^1$ to be one. There is a related notion, namely the Krull dimension of a ring, which is of interest for this.

Definition 2.147. Let R be a commutative ring, and let $\mathfrak{p}$ be a prime ideal. The *height* of $\mathfrak{p}$, $\operatorname{ht}(\mathfrak{p})$, is the supremum of the lengths of strictly increasing chains of prime ideals contained in $\mathfrak{p}$.

Definition 2.148. Let R be a commutative ring. The *Krull dimension* of R is $\dim R := \sup_{\mathfrak{p}\in \operatorname{Spec} R} \operatorname{ht}(\mathfrak{p})$.

Proposition 2.149. *Let R be a commutative ring. Then*

$$\dim R = \dim \operatorname{Spec} R = \sup\{\dim R_{\mathfrak{m}} \mid \mathfrak{m} \textit{ maximal}\}.$$

Proof. See [Liu10, p. 69, Prop. 5.8]. ■

Example 2.150. If k is a field, then $\dim k = 0$. Hence we also see that $\dim \operatorname{Spec} k = 0$, which is intuitively correct since $\operatorname{Spec} k$ consists of a point. One also has $\dim \mathbb{Z} = 1$, and indeed if R is any principal ideal domain then $\dim R = 1$, so, for example, we also have $\dim k[t] = 1$, i.e. $\dim \mathbb{A}_k^1 = 1$. Furthermore, it can also be shown that $\dim k[t_1, \dots, t_n] = n$ (by considering the chain $(0) \subset (t_1) \subset (t_1, t_2) \subset \cdots \subset (t_1, \dots, t_{n-1}) \subset k[t_1, \dots, t_n]$) so that $\dim \mathbb{A}_k^n = n$.

Remark 2.151. Note, however, that $\mathbb{A}_R^n$ is not generally of dimension n for all commutative rings R. It can be shown that $\dim \mathbb{A}_R^n = \dim R + n$ (see, for example, [Liu10, p. 72]) so that $\dim \mathbb{A}_{\mathbb{Z}}^1 = 2$.

Definition 2.152. A scheme is said to be of *pure (Krull) dimension n* if all its irreducible components are of dimension n.

Definition 2.153. A *curve* is a scheme of pure dimension one. Let S be a scheme. A *curve over S* is an S-scheme such that the fibers over $y \in S$ are all curves (i.e. of pure dimension one).

Example 2.154. As seen above, $\operatorname{Spec} \mathbb{Z}$ is a curve since $\dim \operatorname{Spec} \mathbb{Z} = \dim \mathbb{Z} = 1$. Similarly, for a field k, $\mathbb{A}_k^1$ and $\mathbb{P}_k^1$ are curves over k. Note, however, that $\operatorname{Spec} \mathbb{Z}$ is *not* a curve over $\mathbb{Z}$, since the fibers are of dimension zero.

Remark 2.155. Note that if S is a scheme and X is an S-curve, then it is not generally true that X is also a curve indpendent of S. Indeed, since the fibers of $X \to S$ are of dimension one, generically one should think of X as being of Krull dimension $1 + \dim S$. Hence, for example, curves over $\mathbb{Z}$ will topologically look more like surfaces than curves, which is confirmed by examining the $\mathbb{Z}$-curve $\mathbb{A}_{\mathbb{Z}}^1 \to \mathbb{Z}$.

We will in general not be interested in *all* curves, but only those that are in some sense analogous to classical algebraic varieties.

Definition 2.156. Let k be a field. An *affine algebraic variety* over k is an affine scheme associated to a finitely generated k-algebra. An *algebraic variety* over k is a k-scheme which has a covering by a finite number of affine algebraic varieties. A *projective variety* over k is a projective k-scheme.

Remark 2.157. Note that projective varieties are automatically algebraic varieties, since they sit inside some $\mathbb{P}_k^n$, which is an algebraic variety on account of being covered by $n+1$ copies of $\mathbb{A}_k^n$.

Definition 2.158. Let k be a field. An *algebraic curve* over k is an algebraic variety over k that is a curve.

There is something of an analogy between schemes and manifolds, as mentioned when they were defined earlier. As a result, there is also a degree to which algebraic geometry can be compared to differential geometry, which suggests that we should be interested in distinguishing schemes that are "smoother" than other schemes, much like how one works (almost) exclusively with smooth manifolds in differential geometry. For this, we will require several things, but primarily the notion of *regularity*. The motivation from this also comes from differential geometry, in particular through a certain description of the (co)tangent space at a point.

Suppose we have a local ring R, and we set $k = R/\mathfrak{m}$ to be the residue field. Note that $\mathfrak{m}/\mathfrak{m}^2$ is a k-vector space: let $a \in R$, let $v \in \mathfrak{m}$, and let $[a]$ (resp. $[v]$) denote the image of a (resp. v) in the quotient by $\mathfrak{m}$ (resp. $\mathfrak{m}^2$). Then if $a' \in [a]$ we see that $a - a' \in \mathfrak{m}$ so that $a'v - av = (a - a')v \in \mathfrak{m}^2$, so that $a[v] - a'[v] = 0$ and $[a][v]$ is well-defined.

Definition 2.159. Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. We say R is *regular* if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim R$.

Definition 2.160. Let X be a scheme, and $x \in X$ be a point. We say X is *regular at x* (or that x is a *regular point*) if the local ring $\mathcal{O}_{X,x}$ is regular. If x is not a regular point, then it is called *singular*. We say X itself is regular if all points of X are regular, and call it singular otherwise.

There is some further intuition that can be had here: suppose we have a scheme whose local rings are all Noetherian (as an aside, such schemes are called *locally Noetherian*). Then we know that $\dim_{k(x)} \mathfrak{m}_x/\mathfrak{m}_x^2$ is finite, and so the dual $T_{X,x} := (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$ has the same dimension and therefore is isomorphic to $\mathfrak{m}_x/\mathfrak{m}_x^2$. There is a reason for the choice of name for $T_{X,x}$. If M is a smooth manifold, and we denote by $\mathcal{O}_M$ the sheaf of smooth functions to $\mathbb{R}$, then one can check that $\mathfrak{m}_{M,x}/\mathfrak{m}_{M,x}^2$ is the *co*tangent space at $x \in M$, so that the dual is the tangent space $T_{M,x}$ at the point x.

So we see that a locally Noetherian scheme X is regular at $x \in X$ if $\dim \mathcal{O}_{X,x} = \dim_{k(x)} T_{X,x}$, i.e. if the "local dimension" of the scheme at x, given by the dimension of the local ring at x, is the same as the dimension of the tangent space at x. This then coincides with how one defines, for example, a surface in Gaussian geometry, that is: it is a topological space that is locally $\mathbb{R}^2$, and at all points has a two-dimensional tangent space.

Definition 2.161. Let X be an algebraic variety over a field k, let $x \in X$, and let $\bar{k}$ be the algebraic closure of k. We say X is *smooth at x* if the fiber $X_{\bar{k},x}$ is regular. We say X itself is smooth if it is smooth at every point, i.e. if it is geometrically regular.

Remark 2.162. There is a more general notion of a *smooth morphism* of schemes, which we include in the next subsection, and is harder to define. This then allows one to define a general smooth S-scheme X as smooth if the structure morphism $X \to S$ is smooth.

Finally, we will define three important properties a scheme can have: reducedness, integrality, and being Noetherian. Roughly speaking, a scheme is reduced if it has no "infinitesimal" parts, represented by the lack of nilpotents. The analogy comes from the notion of *dual numbers*, i.e. the ring $R[\epsilon] := R[x]/(x^2)$, where one usually denotes the indeterminate x as ϵ to suggest that it is somehow an infinitesimal. Essentially, one adjoins an element to R which is "sufficiently small" such that when you square it, it is zero, i.e. it is infinitesimally small. One can then check that, for example, if $f \in R[x]$ then $f(x + \epsilon) = f(x) + \epsilon f'(x)$. In other words, nilpotents tell us about infinitesimal behavior, and a reduced scheme should be one that doesn't have any such behavior.

Definition 2.163. Let R be a commutative ring. We say R is *reduced* if R has no non-trivial nilpotent elements, i.e. if $\sqrt{(0)} = (0)$.

Definition 2.164. Let X be a scheme, and let $x \in X$. We say X is *reduced at* x if $\mathcal{O}_{X,x}$ is a reduced ring. We say X itself is reduced if every point of X is reduced.

Lemma 2.165. *Let* X *be a scheme. Then* X *is reduced if and only if* $\mathcal{O}_X(U)$ *is a reduced ring for every open set* $U \subseteq X$.

Proof. Suppose X is reduced, and let $f \in \mathcal{O}_X(U)$ be such that $f^n = 0$ for some $n > 1$. Then for every $x \in U$, $[f]_x = 0$ since $\mathcal{O}_{X,x}$ is reduced. From the sheaf axioms we then conclude that $f = 0$. Now suppose $\mathcal{O}_X(U)$ is a reduced ring for all open sets U, let $x \in X$ and let $f_x \in \mathcal{O}_{X,x}$ be non-zero. Then there is some open set V with $x \in V$ such that $[f, V] = f_x$ where f is non-zero and therefore not nilpotent, so f_x is not nilpotent in $\mathcal{O}_{X,x}$. ■

Definition 2.166. Let X be a scheme. We say X is *integral at* x if $\mathcal{O}_{X,x}$ is an integral domain. We say the scheme X is integral if it is reduced and irreducible.

Lemma 2.167. *Let* X *be a scheme, and let* $x \in X$. *Then the irreducible components of* X *containing* x *correspond to the irreducible components of* $\operatorname{Spec} \mathcal{O}_{X,x}$.

Proof. See [Liu10, p. 64, Prop. 4.12]. ■

Lemma 2.168. *Let* X *be a scheme. Then* X *is integral if and only if* $\mathcal{O}_X(U)$ *is an integral domain for every open set* $U \subseteq X$.

Proof. See [Liu10, p. 65, Prop. 4.17]. ■

Proposition 2.169. *Let* X *be an integral scheme. Then* X *is integral at every point.*

Proof. This follows from the above lemmas. In particular, suppose $f_x, g_x \in \mathcal{O}_{X,x}$ such that $f_x g_x = 0$. We can then pick a neighbourhood V of x and representatives $[f, V]$, $[g, V]$ of f_x and g_x, such that $fg = 0$ in $\mathcal{O}_X(V)$, i.e. $f = 0$ or $g = 0$, giving that $f_x = 0$ or $g_x = 0$. Hence $\mathcal{O}_{X,x}$ is an integral domain. ■

Definition 2.170. A scheme is called *Noetherian* if it is locally Noetherian (i.e. the local rings are all Noetherian) and quasicompact.

2.6 Properties of Morphisms

A number of properties in modern algebraic geometry are phrased in terms of morphisms of schemes, mostly due to the *relative* perspective introduced by Grothendieck. This is also why one considers schemes X lying over other schemes S, since this is essentially studying morphisms $X \to S$. There are a great number of possible interesting properties to study throughout the literature, but we will concern ourselves primarily with what is required for properly defining properness, smoothness, étale-ness, and the degree of a morphism.

We will begin by describing proper morphisms, which consist of a combination of three criteria: being universally closed, being separated, and being of finite type. The first is essentially a topological property.

Definition 2.171. Let $f\colon X \to Y$ be a morphism of schemes. We say f is *closed* if for every closed set V, the image $f(V)$ is closed. We say that f is *universally closed* if for every morphism $Y' \to Y$ the induced morphism $X \times_Y Y' \to Y'$ is closed.

Remark 2.172. In other words, a universally closed morphism is one which is stable under base change (that is, remains closed after one performs a base change).

The other properties are a little harder to characterize, but have fairly intuitive origins. Schemes are very rarely Hausdorff topological spaces, due to the Zariski topology being too sparse, and this is something of a problem. Consider the scheme formed by gluing two affine lines together everywhere but the origin (this can be done using the gluing lemma, Lemma 2.119, of the previous subsection). This obviously is something of a strange space to study, and so we want to exclude it (and its affiliates) in many cases. However, while one would usually use the Hausdorff condition to remove these kinds of pathologies, this can no longer be done due to the natural topology on a scheme. Hence, we replace it with an analogous condition, namely separatedness.

Definition 2.173. Let $f\colon X \to Y$ be a morphism of schemes. The *diagonal morphism* $\Delta_{X/Y}$ associated to f is the induced morphism $(\mathrm{id}_X, \mathrm{id}_X)\colon X \to X \times_Y X$.

Definition 2.174. Let $f : X \to Y$ be a morphism of schemes. We say that f is a *separated morphism*, or that X is *separated over* Y, if $\Delta_{X/Y}$ is a closed immersion. We say X is *separated* if it separated over $\mathbb{Z}$.

Remark 2.175*.* This is a particularly strange condition if provided without good justification. The definition comes from a condition that, in the case of topological spaces, happens to be equivalent to being Hausdorff. In particular, a topological space X is Hausdorff if and only if the diagonal morphism $\Delta\colon X \to X \times X$, given by $x \mapsto (x, x)$, satisfies that $\Delta(X)$ is closed.

This is generally a hard condition to check, so we have the following:

Proposition 2.176. *Let X be a scheme. Then X is separated (over $\mathbb{Z}$) if and only if for every pair U, V of affine open subsets of X, the intersection $U \cap V$ is affine and the canonical homomorphism $\mathcal{O}_X(U) \otimes_{\mathbb{Z}} \mathcal{O}_X(V) \to \mathcal{O}_X(U \cap V)$ is surjective.*

Proof. See [Liu10, p. 100, Prop. 3.6]. ∎

Remark 2.177*.* One can now check that reasonable things are separated (e.g. the projective space $\mathbb{P}^n_{\mathbb{Z}}$) and that unreasonable things are not (like the affine line with a double origin). This observation actually covers a lot of ground, practically speaking, since we have the following:

Proposition 2.178. *Open and closed immersions are separated, the composition of separated morphisms is separated, separated morphisms are stable under base change, and if $X \to Z$, $Y \to Z$ are separated, then so is $X \times_Z Y \to Z$.*

Proof. See [Liu10, p. 101, Prop. 3.9]. ∎

Remark 2.179*.* From this, we immediately get that all notable projective spaces are separated. In particular, let S be a scheme. Then $\mathbb{P}^n_S = \mathbb{P}^n_{\mathbb{Z}} \times S$ is separated over S since $\mathbb{P}^n_{\mathbb{Z}}$ is separated. Hence one also gets that all projective schemes are separated (since they are closed subschemes of projective spaces).

The final ingredient we need, then, is what it means for a morphism to be of finite type.

Remark 2.180*.* In the following, we will refer to what is sometimes called “compact” as “quasicompact.” This is essentially to reduce confusion, since in some places “compact” means “compact and Hausdorff.” Hence, by quasicompact, we mean that every cover has a finite subcover.

Definition 2.181. Let $f\colon X \to Y$ be a morphism of schemes. We say that f is *quasicompact* if for every affine open subset $V \subseteq Y$, the inverse image $f^{-1}(V)$ is quasicompact.

Definition 2.182. Let $f\colon X \to Y$ be a morphism of schemes. We say f is of *finite type* if f is quasicompact, and if for every affine open subset $V \subseteq Y$ and every affine subset $U \subseteq f^{-1}(V)$, the induced morphism $\mathcal{O}_Y(V) \to \mathcal{O}_X(U)$ makes $\mathcal{O}_X(U)$ into a finitely generated $\mathcal{O}_Y(V)$-algebra. We say that a Y-scheme X is of finite type if the structure morphism is of finite type.

Example 2.183. We have already come across a fairly rich class of schemes of finite type. Let k be a field. Then k-schemes of finite type are precisely the same as algebraic varieties over k.

We also have a similar set of statements as for separated morphisms that apply to morphisms of finite type.

Proposition 2.184. *Closed immersions are of finite type, the composition of two morphisms of finite type is of finite type, morphisms of finite type are stable under base change, and if $X \to Z$, $Y \to Z$ are of finite type, then so is $X \times_Z Y \to Z$.*

Proof. See [Liu10, p. 88, Prop. 2.4]. ■

Remark 2.185. As with before, this gives us that a number of other things are of finite type. For example, if $X \to Y$ is of finite type, then we immediately get that for $y \in Y$, the fiber X_y is an algebraic variety over $k(y)$.

We are now ready to define what a proper morphism is.

Definition 2.186. Let $f : X \to Y$ be a morphism of schemes. We say f is *proper* if it is universally closed, separated, and of finite type. We say that a Y-scheme is proper if the structure morphism is proper.

Remark 2.187. In other words, a proper morphism is one that is extraordinarily well behaved. It ensures a Hausdorff-like condition, it ensures that closed sets are sent to closed sets, and it ensures that the domain behaves like a variety over the codomain.

Proposition 2.188. *Closed immersions are proper, the composition of proper morphisms is proper, proper morphisms are stable under base change, and if $X \to Z$, $Y \to Z$ are proper, then so is $X \times_Z Y \to Z$.*

Proof. See [Liu10, p. 104, 3.16]. ■

Smooth morphisms are defined by combining the notion of a *flat* morphism with the easier definition over a field. A flat morphism somehow guarantees that the fibers of the morphism are "continuous."

Definition 2.189. A morphism $f : X \to Y$ of schemes is said to be *flat* at $x \in X$ if the homomorphism $f_x^\sharp\colon \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is flat (i.e. gives $\mathcal{O}_{X,x}$ the structure of a flat $\mathcal{O}_{Y,f(x)}$ module).

Proposition 2.190. *Open immersions are flat, flat morphisms are stable under base change, the composition of flat morphisms is flat, the fiber product of two flat morphisms is flat, and a morphism* $\operatorname{Spec} A \to \operatorname{Spec} B$ *is flat if and only if the induced map $B \to A$ is flat.*

Proof. See [Liu10, p. 136, Prop. 3.3]. ■

Definition 2.191. Let Y be a locally Noetherian scheme. A morphism $f\colon X \to Y$ of finite type is said to be *smooth* at $x \in X$ if it is flat at x, and if the induced fiber $X_{f(x)} \to \operatorname{Spec} k(f(x))$ is smooth (according to Definition 2.161).

Smooth morphisms will be important when we discuss reduction in Section 3, which are integral to the proof of weak Mordell–Weil. A property which will provide us with interesting structural information about elliptic curves is that of a morphism being *étale*. Roughly speaking, these are analogous to local isomorphism in differential geometry. They are based on two notions: flatness, which we recall from smoothness, and being unramified.

Definition 2.192. Let X and Y be locally Noetherian schemes, and let $f : X \to Y$ be a morphism of schemes. We will say f is *unramified* at $x \in X$ if the morphism $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ satisfies $\mathfrak{m}_{f(x)}\mathcal{O}_{X,x} = \mathfrak{m}_x$ and if the extension $k(f(x)) \to k(x)$ is separable. We say f is unramified if it is unramified for all $x \in X$.

Definition 2.193. A morphism $X \to Y$ is *étale* at $x \in X$ if it is flat and unramified at x. We say it is étale if it is étale for all $x \in X$.

The property of these that we will primarily care about in this thesis is actually the "unramified" part. This is due to the following proposition:

Proposition 2.194. *Let $f : X \to Y$ be a morphism of finite type between locally Noetherian schemes. Then f is unramified if and only if for all $y \in Y$, the fiber X_y is finite, reduced, and $k(x)$ is separable over $k(y)$ for all $x \in X_y$. In particular, if f is unramified, then X_y is finite as a set.*

Proof. See [Liu10, p. 139, Lemma 3.20]. In particular, note that the proof shows X_y is of dimension zero, and hence quasicompactness shows that X_y as a set is finite (and furthermore, is discrete as a topological space). ■

It is generally of interest to want to be able to talk about the degree of a morphism. One also wants the notion to be roughly analogous to , for example, a map $\mathbb{R} \to \mathbb{R}$ given by $x \mapsto x^2$ being of degree two. The inspiration here will come from looking at the residue field at a generic point of an irreducible scheme. For an example, we will begin by considering the map $\mathbb{A}^1_k \to \mathbb{A}^1_k$ induced by the map $k[t] \to k[t]$ given by $t \mapsto t^2$. Intuitively speaking, we want this to be a degree two map, so the question is how we can extract this from the map $\mathbb{A}^1_k \to \mathbb{A}^1_k$. Note that the generic point $\xi = (0)$ is mapped to itself, so that we get a map $\mathcal{O}_{\mathbb{A}^1_k,\xi} \to \mathcal{O}_{\mathbb{A}^1_k,\xi}$, which in turns gives us a map $k(\xi) \to k(\xi)$, i.e. a map $k(t) \to k(t)$, given by $t \mapsto t^2$. This allows us to regard $k(t)$ as a field extension of itself, in particular as an extension of degree two. One can further check that if we instead had a map given by $t \mapsto t^3$, this extension would be of degree three. This is telling us that this is the property we want to calculate to get the degree of a map.

Definition 2.195. We say that a morphism $f : X \to Y$ is *dominant* if $f(X)$ is dense in Y.

Proposition 2.196. *Let X and Y be integral schemes with generic points ξ_X and ξ_Y, respectively. Then a morphism $f : X \to Y$ is dominant if and only if $f(\xi_X) = \xi_Y$.*

Definition 2.197. Let X be an irreducible scheme with generic point ξ. The *function field* of X is $K(X) := k(\xi)$.

Remark 2.198. In other words, a dominant map is exactly what one needs to get a map $K(Y) \to K(X)$ of the function fields of integral schemes.

Definition 2.199. Let $f : X \to Y$ be a dominant morphism of integral schemes. The *degree* of f, denoted $\deg f$, is the degree of the induced extension $K(X)/K(Y)$, i.e. we set $\deg f := [K(X) : K(Y)]$. This does not need to be finite.

This then gives that if we set $f\colon \mathbb{A}^1_k \to \mathbb{A}^1_k$ to be the morphism induced by $t \mapsto t^2$ as above, then $\deg f = 2$ as desired. This, however, leaves us with a problem: we also want the morphism $g\colon \mathbb{A}^1_k \to \mathbb{A}^2_k$ induced by $k[t_1, t_2] \to k[t]$ given by $(t_1, t_2) \mapsto (t, t^2)$ to be considered a degree two map, but clearly $g(\xi) = (t_2 - t_1^2) \neq (0)$, so g is not dominant. Note however that $(t_2 - t_1^2)$ is the generic point of the irreducible open subscheme $Y = \operatorname{Spec} k[t_1, t_2]/(t_2 - t_1^2)$ and the induced map $\mathbb{A}^1_k \to Y$ actually *is* dominant and has degree two. This suggests the following definition:

Definition 2.200. Let X be an integral scheme, let Y be a scheme, and let $i : Z \to Y$ be an integral closed subscheme of Y. Let $f : X \to Y$ be a morphism of schemes that factors as $f = i \circ \tilde{f}$ where $\tilde{f}\colon X \to Z$ is a dominant morphism. Then we define the degree of f to be the degree of $\tilde{f}$, i.e. $\deg f := \deg \tilde{f}$.

We then see that, following this definition, the map $\mathbb{A}^1_k \to \mathbb{A}^2_k$ given above is a degree two map, as desired. Computing the degree above does come with the difficulty of computing the field of rational functions, however, and so we want an easy way to do this. This is provided by the following:

Proposition 2.201. *Let X be an integral scheme with generic point ξ, and let $V \subseteq X$ be an affine open subset of X. Then $\operatorname{Frac}(\mathcal{O}_X(V)) \cong \mathcal{O}_{X,\xi}$.*

Proof. The point ξ is also a generic point of V when we view V as its own topological space, and we have that $\mathcal{O}_{X,\xi} = \mathcal{O}_{V,\xi}$. We can compute $\mathcal{O}_{V,\xi}$ as $\operatorname{Frac}(\mathcal{O}_V(V)) = \operatorname{Frac}(\mathcal{O}_X(V))$, and so we get the desired equality $\mathcal{O}_{X,\xi} = \operatorname{Frac}(\mathcal{O}_X(V))$. ■

Example 2.202. Let us compute $K(\mathbb{P}^n_k)$ for k a field. We can pick the affine open subset $V = \operatorname{Spec} k[t_0/t_i, \ldots, t_n/t_i]$ for some $0 \leq i \leq n$, which has (by definition) global sections $\mathcal{O}_X(V) = k[t_0/t_i, \ldots, t_n/t_i]$, and from this we get $K(\mathbb{P}^n_k) = \operatorname{Frac}(\mathcal{O}_X(V)) = k(t_0/t_i, \ldots, t_n/t_i)$.

We will now apply this to computing the degree of a particular kind of morphism as an example of its utility.

Lemma 2.203. *Let k be a field, let C_1 be a proper smooth curve over k, let C_2 be any curve over k, and let $f : C_1 \to C_2$ be a morphism. Then $f(C_1) = pt$ or f is surjective, and in the second case we have that $K(C_1)$ is a finite extension of $K(C_2)$, and for all affine open subsets $V \subseteq C_2$, the preimage $f^{-1}(V)$ is affine and $\mathcal{O}_{C_1}(f^{-1}(V))$ is finitely generated over $\mathcal{O}_{C_2}(V)$.*

Proof. See [Har77, p. 137, Prop. II.6.8]. ■

Example 2.204. Let $f_0, f_1 \in k[t_0, t_1]$ be homogeneous polynomials of degree d with no common zeros, and set $X = \operatorname{Proj}(k[t_0, t_1])$, $Y = \operatorname{Proj}(k[T_0, T_1])$ (i.e. $X \cong Y \cong \mathbb{P}^1_k$). Let $\phi\colon X \to Y$ be the morphism given by $T_i \mapsto f_i$. The above lemma gives that we may compute the degree of this map. The map ϕ induces the map

$$K(Y) \to K(X), \quad T_1/T_0 \mapsto f_1/f_0.$$

This exhibits $K(Y)$ as a subfield of $K(X)$. We then get $\deg \phi = [K(X) : K(Y)] = d$ since $K(Y)$ occupies all the rational functions whose degree is a multiple of d.

In other words, we get the expected result that a morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$ induced by polynomials of degree d is itself of degree d. One should take care, however, with generalizing this: it is not true that an analogous morphism $\mathbb{P}^n_k \to \mathbb{P}^m_k$ is of degree d, though there is a strongly similar result regarding this.

3 Elliptic Curves

The purpose of this section is to describe elliptic curves as particular kinds of schemes, prove that they satisfy a Weierstrass-type equation (i.e. $y^2 = x^3 + ax + b$), and describe how one can reduce a scheme (most importantly for us, an elliptic curve) modulo p, which will be necessary for proving the weak Mordell–Weil theorem. To do these things, we introduce sheaf cohomology, divisors on schemes, cohomological duality, and the Riemann–Roch theorem. The information here is based primarily on [Liu10], [Har77], and [Cla12] (for the subsection on reduction), though mostly the former.

3.1 Sheaf Cohomology

Cohomology is a tool used primarily for detecting certain obstructions in a topological space X which prevents one from, for example, extending a section on an open set $U \neq X$ to a global section on X. Classically, the motivation for this comes from singular (co)homology, which is a topological invariant that provides information about the number of (and structure of) "holes" in the space X. Another classical example of a cohomology theory is de Rham cohomology, which measures the amount by which the fundamental theorem of calculus fails on a given smooth manifold. Somewhat remarkably, one can show that in most cases, de Rham cohomology and singular cohomology actually coincide, so that differential information can be used to detect holes in a space (a simple demonstration of this is given by Cauchy's residue theorem).

Sheaf cohomology is, in a sense, closer to de Rham cohomology than to singular cohomology, though these are all related. In essence, we are interested in the following fact: if

$$0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$$

is a short exact sequence of sheaves of Abelian groups on a topological space X, then this in general only induces an exact sequence of the form

$$0 \to \Gamma(X, \mathcal{F}) \to \Gamma(X, \mathcal{G}) \to \Gamma(X, \mathcal{H}).$$

That is, one cannot conclude from a surjective morphism $\mathcal{G} \to \mathcal{H}$ that global sections of $\mathcal{H}$ extend to global sections of $\mathcal{G}$. Sheaf cohomology seeks to measure the obstruction preventing this from happening. The cohomology theory of sheaves is a special case of general homological algebra, a brief description of which can be found in [Har77, III.1]. A more extensive description can be found in, for example, [Wei95].

We define cohomology as the *right derived functor* of the global section functor $\Gamma(X, -) : \mathbf{Shf}(X; \mathbf{Ab}) \to \mathbf{Ab}$. In particular, we have the following definitions:

Definition 3.1. Let F be a functor $\mathbf{Shf}(X; \mathbf{Ab}) \to \mathbf{Ab}$. We say F is *exact* if whenever $0 \to \mathcal{G}_1 \to \mathcal{G}_2 \to \mathcal{G}_3 \to 0$ is exact, the induced sequence of maps $0 \to F(\mathcal{G}_1) \to F(\mathcal{G}_2) \to F(\mathcal{G}_3) \to 0$ is also exact. We say F is *left exact* if the statement is true with "$\to 0$" removed.

Example 3.2. The statement above is essentially saying that $\Gamma(X, -)$ is a left exact functor.

Definition 3.3. A sheaf $\mathcal{I}$ of Abelian groups is called *injective* if $\mathrm{Hom}(-, \mathcal{I})$ is an exact functor. Let $\mathcal{F}$ be a sheaf of Abelian groups. An *injective resolution* of $\mathcal{F}$ is a collection of injective sheaves $\mathcal{I}^n$, $n \geq 0$, with maps $\mathcal{I}^n \to \mathcal{I}^{n+1}$ and a map $\epsilon \colon \mathcal{F} \to \mathcal{I}^0$ such that the sequence

$$0 \to \mathcal{F} \xrightarrow{\epsilon} \mathcal{I}^0 \to \mathcal{I}^1 \to \cdots$$

is exact.

Proposition 3.4. *The category* $\mathbf{Shf}(X;\mathbf{Ab})$ *has enough injectives, i.e. every sheaf* $\mathcal{F} \in \mathbf{Shf}(X;\mathbf{Ab})$ *has at least one injective resolution.*

Proof. See [Har77, III, Prop. 2.2 & Cor. 2.3]. ■

If we let $\mathcal{F}$ be a sheaf with an injective resolution $\mathcal{I}^\bullet$, then one gets an induced sequence

$$0 \to \Gamma(X,\mathcal{I}^0) \to \Gamma(X,\mathcal{I}^1) \to \Gamma(X,\mathcal{I}^2) \to \cdots$$

(where $0 \to \Gamma(X,\mathcal{I}^0)$ is the composition $0 \to \Gamma(X,\mathcal{F}) \to \Gamma(X,\mathcal{I}^0)$) which is no longer exact, but it is instead a *chain complex.* What this means is that the composition of any two consequtive maps in the sequence is zero, i.e. if $d^n : \Gamma(X,\mathcal{I}^{n-1}) \to \Gamma(X,\mathcal{I}^n)$ are the induced maps, then $d^{n+1} \circ d^n = 0$. One often writes this as "$d^2 = 0$" for simplicity. Now, an important property of a chain complex is that $\operatorname{im} d^n \subseteq \ker d^{n+1}$. This is what we use to define cohomology:

Definition 3.5. Let $\mathcal{F}$ be a sheaf of Abelian groups on a topological space X, with an injective resolution $\mathcal{I}^\bullet$, and let d^n be the maps as above. The *cohomology groups* of X with *coefficients in* $\mathcal{F}$ are defined as

$$\mathrm{H}^n(X,\mathcal{F}) := \ker d^{n+1} / \operatorname{im} d^n.$$

This gives a functor $\mathrm{H}^n(X,-)\colon \mathbf{Shf}(X;\mathbf{Ab}) \to \mathbf{Ab}$. Furthermore, $\mathrm{H}^0(X,\mathcal{F}) = \Gamma(X,\mathcal{F})$.

Remark 3.6. For a proof of the last statement, note that $\Gamma(X,\mathcal{F}) = \ker d^1$ since $\Gamma(X,-)$ is left exact, so that $\mathrm{H}^0(X,\mathcal{F}) = \ker d^1 / \operatorname{im} d^0 = \ker d^1 = \Gamma(X,\mathcal{F})$.

Remark 3.7. The definition above is dependent on a choice of injective resolution. One can show that the result is actually independent of this choice, see [Wei95, p. 44, Lemma 2.4.1].

In what way do these groups measure the failure of $\Gamma(X,-)$ to be exact? This is answered by the following:

Proposition 3.8. *Let* $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$ *be an exact sequence of sheaves of Abelian groups on a topological space* X*. Then we have an induced long exact sequence*

$$0 \to \mathrm{H}^0(X,\mathcal{F}) \to \mathrm{H}^0(X,\mathcal{G}) \to \mathrm{H}^0(X,\mathcal{H}) \to \mathrm{H}^1(X,\mathcal{F}) \to \mathrm{H}^1(X,\mathcal{G}) \to \mathrm{H}^1(X,\mathcal{H}) \to \cdots$$

Proof. See [Wei95, p. 45, Thm. 2.4.6]. ■

The above groups are generally quite hard to calculate, but there are certain theorems about their vanishing that make it somewhat easier. In particular, there is a theorem of Grothendieck which describes what the cohomology groups of certain spaces with specified dimension look like.

Definition 3.9. Let X be a topological space. We say X is *Noetherian* if every descending chain of closed subsets stabilizes, i.e. if $Z_1 \supseteq Z_2 \supseteq \cdots \supseteq Z_n \supseteq \cdots$ are closed subsets of X then there is some $r \geq 1$ such that $Z_r = Z_{r+1}$.

Remark 3.10. Note that while Noetherian schemes are also Noetherian as topological spaces, the converse is not true. There are schemes X whose underlying topological space $\mathrm{sp}(X)$ is Noetherian while X itself is not Noetherian.

Theorem 3.11 (Grothendieck's vanishing theorem)**.** *Let* X *be a Noetherian topological space, let* $\mathcal{F}$ *be a sheaf of Abelian groups on* X*, and let* $n = \dim X$*. Then, for all* $i > n$*, we have* $\mathrm{H}^i(X,\mathcal{F}) = 0$.

Proof. See [Har77, p. 208–211, Thm. III.2.7]. ■

Remark 3.12. This should be thought of as analogous to saying that in an n-dimensional space, you can't have holes that are of larger dimension than n.

Corollary 3.13. *Let C be a Noetherian algebraic curve over a field k. Then, for every sheaf of Abelian groups $\mathcal{F}$ on C, the only cohomology groups that are non-trivial are $\mathrm{H}^0(C, \mathcal{F})$ and $\mathrm{H}^1(C, \mathcal{F})$.*

Remark 3.14. Inserting this into the statement about long exact sequences in cohomology, we see that if C is a Noetherian curve as above, and $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$ is an exact sequence of sheaves of Abelian groups, then we get the long exact sequence

$$0 \to \mathrm{H}^0(C, \mathcal{F}) \to \mathrm{H}^0(C, \mathcal{G}) \to \mathrm{H}^0(C, \mathcal{H}) \to \mathrm{H}^1(C, \mathcal{F}) \to \mathrm{H}^1(C, \mathcal{G}) \to \mathrm{H}^1(C, \mathcal{H}) \to 0.$$

Remark 3.15. If the coeffiecient sheaf $\mathcal{F}$ has more structure, then often this structure can be transported to the cohomology groups. For example, if X is a scheme over a ring R, and $\mathcal{F}$ is an $\mathcal{O}_X$-module, then the cohomology groups $\mathrm{H}^n(X, \mathcal{F})$ are R-modules. As a consequence, we see that if $R = k$ is a field, then the cohomology groups become k-vector spaces.

In practice, the above defintion of cohomology is generally very difficult to actually compute, so one tends to use an "approximation" of it which can be shown to be accurate in most cases one cares about. This is called Čech cohomology, and [Liu10] contains a good account of it. In this thesis however, we will primarily only need what has been presented so far (e.g. that $\mathrm{H}^0(X, \mathcal{F}) = \Gamma(X, \mathcal{F})$) along with the intuition that comes along with a comparison to singular cohomology in algebraic topology (i.e. that $\mathrm{H}^1(X, \mathcal{F})$ should somehow measure one-dimensional "holes").

Finally, we will now define two invariants of a projective curve that are based on the cohomology, namely the *arithmetic genus* and the *geometric genus*. The first of these is defined in terms of the *Euler characteristic*.

Definition 3.16. Let X be a projective variety over a field k, and let $\mathcal{F}$ be an $\mathcal{O}_X$-module. Then the *Euler–Poincaré characteristic* (or just *Euler characteristic*) of $\mathcal{F}$ is

$$\chi_k(\mathcal{F}) := \sum_{i \geq 0} (-1)^i \dim_k \mathrm{H}^i(X, \mathcal{F}).$$

Remark 3.17. The intuition for this is from algebraic topology, where one can show that this type of alternating sum does indeed give the Euler characteristic. Note also that the above can be "poorly defined" since some sheaves may have infinite-dimensional cohomology groups, so that the differences don't make sense. This can be resolved by restricting to a smaller class of $\mathcal{O}_X$-modules. One can also weaken X being a projective variety/k to simply being a proper scheme/k (it is easy to check that all projective varieties over k are proper over k).

Definition 3.18. Let X be a projective curve over a field k. Then the *arithmetic genus* $p_a(X)$ is given by

$$p_a(X) := 1 - \chi_k(\mathcal{O}_X).$$

Remark 3.19. This definition is essentially designed to mimic $\chi = 2g - 2$ from classical algebraic topology and geometry. Note also that it expands, in the case of curves as above, as

$$p_a(X) = 1 - \dim_k \mathrm{H}^0(X, \mathcal{O}_X) + \dim_k \mathrm{H}^1(X, \mathcal{O}_X)$$

by Grothendieck's vanishing theorem, and so we see that if $p_a(X) = 1$, then $\dim_k \mathrm{H}^0(X, \mathcal{O}_X) = \dim_k \mathrm{H}^1(X, \mathcal{O}_X)$, which is of interest in the case of elliptic curves.

The geometric genus is a little harder to define. It relies upon a particular object called the *dualizing sheaf*, which one can associate to any morphism of schemes, and is vastly outside the scope of this thesis. What we will need is the following:

Definition 3.20. Let $(X, \mathcal{O}_X)$ be a ringed space, and let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules. We define *sheaf-hom*, $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$, to be the sheaf $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})(U) = \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{F}|_U, \mathcal{G}|_U)$. We define the *sheaf dual* of an $\mathcal{O}_X$-module $\mathcal{F}$ to be $\mathcal{F}^\vee := \mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{O}_X)$.

Remark 3.21. This satisfies certain "obvious" properties analogous to those of $\operatorname{Hom}_R(M, N)$ for M, N modules over a ring R. In particular, $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{F}) = \mathcal{F}$, so that $\mathcal{O}_X^\vee = \mathcal{O}_X$.

Definition 3.22. Let $(X, \mathcal{O}_X)$ be a ringed space. An $\mathcal{O}_X$-module $\mathcal{F}$ is *quasi-coherent* if for every $x \in X$ there is some open neighbourhood U of x and an exact sequence

$$\mathcal{O}_X^{(J)}|_U \to \mathcal{O}_X^{(I)} \to \mathcal{F} \to 0,$$

where I, J are sets, and $\mathcal{O}_X^{(I)}$ (resp. $\mathcal{O}_X^{(J)}$) denotes the direct sum $\bigoplus_{i \in I} \mathcal{O}_X$ (resp. $\bigoplus_{j \in J} \mathcal{O}_X$).

Proposition-Definition 3.23. *Let X be a projective scheme over a field k, and suppose* $\dim X \leq r$ *for some $r \in \mathbb{N}$. Then there exists an $\mathcal{O}_X$-module $\omega_{X/k,r}$, called the r-*dualizing sheaf *of X, such that for any quasi-coherent sheaf $\mathcal{F}$ we have*

$$\mathrm{H}^0(X, \mathcal{F}^\vee \otimes \omega_{X/k,r}) \cong \mathrm{H}^r(X, \mathcal{F})^\vee,$$

where on the right-hand-side, one takes the dual as a k-vector space. If $\dim X = r$*, then we will write $\omega_{X/k}$ for $\omega_{X/k,r}$.*

Proof. See [Liu10, p. 246, Cor. 4.29 & Remark 4.30], or in general the entire section in [Liu10] on duality theory, and in particular the part on Grothendieck duality. ■

This then gives us the definition of the geometric genus:

Definition 3.24. Let X be a smooth projective variety over a field k. Then we define the *geometric genus* $p_g(X)$ as

$$p_g(X) := \dim_k \mathrm{H}^0(X, \omega_{X/k}).$$

Remark 3.25. If we suppose X is a projective curve, then we get that $\mathrm{H}^0(X, \omega_{X/k}) = \mathrm{H}^1(X, \mathcal{O}_X)^\vee$, so that $p_g(X) = \dim \mathrm{H}^1(X, \mathcal{O}_X)$.

In some cases, the arithmetic genus and geometric genus will coincide, so one can combine them into one invariant.

Proposition-Definition 3.26. *Let X be a smooth, geometrically connected, projective curve over a field k. Then $p_a(X) = p_g(X)$, and we simply refer to this common value as the genus $g(X)$ (or, sometimes, just g).*

Proof. We use [Liu10, p. 105, Cor. 3.21] to see that $\mathrm{H}^0(X, \mathcal{O}_X) = \Gamma(X, \mathcal{O}_X) = \mathcal{O}_X(X) = k$ when X is as described in the proposition. We then use Remark 3.19 to compute $p_a(X) = 1 - 1 + \dim_k \mathrm{H}^1(X, \mathcal{O}_X) = \dim_k \mathrm{H}^1(X, \mathcal{O}_X)$. Combining this with the above remark, we get that $p_a(X) = \dim_k \mathrm{H}^1(X, \mathcal{O}_X) = p_g(X)$. ■

3.2 Divisors & Riemann–Roch

In this subsection we are going to concern ourselves primarily with describing enough language that we can state the Riemann-Roch theorem and later use it to show that elliptic curves satisfy certain equations. For this, we will describe two definitions of divisors on schemes: Cartier divisors, and Weil divisors. The first of these is the most general, but due to this is also more lacking in intuition. The latter is distinctly more geometrically intuitive, but is also restrictive in the sense that one only considers Weil divisors on sufficiently nice schemes.

We begin with Cartier divisors. The motivation for divisors in general came from trying to prove the Riemann-Roch theorem, which in some sense was trying to answer the question of whether it was always possible to describe functions with given poles and zeros. To this end, it makes sense that divisors should somehow locally be represented by rational functions, potentially modulo extraneous parts. This is indeed what Cartier divisors essentially are. For now, let $R(A)$ denote the regular elements of a ring A, i.e. the elements of A that are not zero-divisors. Then:

Proposition 3.27. *Let X be a scheme, and for any open subset $U \subseteq X$ set*

$$\mathcal{R}_X(U) := \{s \in \mathcal{O}_X(U) \mid \forall x \in U,\ [s]_x \in R(\mathcal{O}_{X,x})\}.$$

Then $\mathcal{R}_X$ is a sheaf, with $\mathcal{R}_X(U) = R(\mathcal{O}_X(U))$ if U is affine. Furthermore, there is a unique presheaf $\mathcal{K}'_X$ on X, containing $\mathcal{O}_X$, such that

(a) For any $U \subseteq X$ open, we have $\mathcal{K}'_X(U) = \mathcal{R}_X(U)^{-1}\mathcal{O}_X(U)$.
(b) For any $U \subseteq X$ open, the canonical morphism $\mathcal{K}'_X(U) \to \prod_{x \in U} \mathcal{K}'_{X,x}$ is injective (i.e. $\mathcal{K}'_X$ is a separated presheaf).
(c) If X is locally Noetherian, then for any $x \in X$ we have that $\mathcal{K}'_{X,x} \cong \operatorname{Frac}(\mathcal{O}_{X,x})$.

Proof. See [Liu10, p. 255, Lemma 1.12]. ■

Definition 3.28. Let X be a scheme. The *sheaf of stalks of meromorphic functions* on X, denoted $\mathcal{K}_X$, is $(\mathcal{K}'_X)^\dagger$, i.e. the sheaf associated to the presheaf $\mathcal{K}'_X$ described above. An element $s \in \mathcal{K}_X(X)$ is called a *meromorphic function* on X. The subsheaf of $\mathcal{K}_X$ given by the invertible elements is denoted, as usual, by $\mathcal{K}_X^\times$.

Remark 3.29. Since $\mathcal{O}_X$ is a subpresheaf of $\mathcal{K}'_X$, we see that it is also a subsheaf of $\mathcal{K}_X$. Recall also that sheafification turns "global" properties to "local" properties, so that since an element of $\mathcal{K}'_X(U)$ is a quotient s/r with $s \in \mathcal{O}_X(U)$ and $r \in \mathcal{R}_X(U)$ (roughly speaking, r is a "regular" element of $\mathcal{O}_X(U)$), an element of $\mathcal{K}_X(U)$ is locally of this form, i.e. is locally a quotient of a section $s \in \mathcal{O}_X(U)$, and some kind of "regular" section r of $\mathcal{O}_X(U)$. Note, further, that if X is locally Noetherian, then by the properties of sheafification, we have that $\mathcal{K}_{X,x} = \mathcal{K}'_{X,x} = \operatorname{Frac}(\mathcal{O}_{X,x})$.

Remark 3.30. The above sheaf is a generalization of the function field of an integral scheme. Note that if X is integral, then the sheaf $\mathcal{K}_X$ is just the constant sheaf $\underline{K(X)}$ associated to $K(X)$.

Definition 3.31. Let X be a scheme. The *group of Cartier divisors* on X, denoted $\operatorname{Div}_{\mathrm{C}}(X)$, is given by the group $\mathrm{H}^0(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times) = (\mathcal{K}_X^\times/\mathcal{O}_X^\times)(X)$, and elements of $\operatorname{Div}_{\mathrm{C}}(X)$ are called *Cartier divisors*. If $U \subseteq X$ is an open set, denote by $D|_U$ the restriction of a Cartier divisor D to U as a section of $\mathcal{K}_X^\times/\mathcal{O}_X^\times$. Let $\operatorname{div} : \Gamma(X, \mathcal{K}_X^\times) \to \operatorname{Div}_{\mathrm{C}}(X)$ denote the projection map induced by the quotient $\mathcal{K}_X^\times \to \mathcal{K}_X^\times/\mathcal{O}_X^\times$. An element of $\operatorname{Div}_{\mathrm{C}}(X)$ of the form $\operatorname{div}(f)$, $f \in \mathcal{K}_X^\times(X)$, is called a *principal* Cartier divisor. We say a Cartier divisor is *effective* if it is in the image of the canonical map $\Gamma(X, \mathcal{O}_X \cap \mathcal{K}_X^\times) \to \mathrm{Div}_\mathrm{C}(X)$, and write $\mathrm{Div}_\mathrm{C}^+(X)$ for the set of effective Cartier divisors. One usually writes $D \geq 0$ to say $D \in \mathrm{Div}_\mathrm{C}^+(X)$. The group law on $\mathrm{Div}_\mathrm{C}(X)$ is notated additively.

Definition 3.32. Let $D_1, D_2 \in \mathrm{Div}_\mathrm{C}(X)$. We say D_1 and D_2 are *linearly equivalent*, and write $D_1 \sim D_2$, if their difference $D_1 - D_2$ is principal.

Remark 3.33. A Cartier divisor D on a scheme X can be represented via a collection of pairs $\{(U_i, f_i)\}_i$, where $\bigcup_i U_i = X$, $f_i \in \mathcal{K}_X^\times(U_i)$ (i.e. f_i is the quotient of two regular elements in $\mathcal{O}_X(U_i)$), and $f_i|_{U_i \cap U_j} \in f_j|_{U_i \cap U_j} \mathcal{O}_X(U_i \cap U_j)^\times$ for all i, j. One then sees that, if D_1 and D_2 are Cartier divisors represented by $\{(U_i, f_i)\}_i$ and $\{(V_j, g_j)\}_j$ then $D_1 + D_2$ is represented by $\{(U_i \cap V_j, f_i g_j)\}_{i,j}$. A Cartier divisor D is then effective if it is represented by $\{(U_i, f_i)\}_i$ with $f_i \in \mathcal{O}_X(U_i)$ for all i, and principal if it is represented by $\{(X, f)\}$ for some $f \in \mathcal{K}_X^\times(X)$.

Definition 3.34. Let D be a Cartier divisor on a scheme X, represented by some collection $\{(U_i, f_i)\}_i$. The *sheaf associated to D*, denoted $\mathcal{O}_X(D)$, is defined by setting $\mathcal{O}_X(D)|_{U_i} = f_i^{-1}\mathcal{O}_X|_{U_i}$. (Note that, here, we do not mean the inverse image functor).

Remark 3.35. The above definition is independent of the choice of representation. Furthermore, a Cartier divisor D is effective if and only if $\mathcal{O}_X(-D) \subseteq \mathcal{O}_X$, and we also have $\mathcal{O}_X(D)|_U = \mathcal{O}_U(D|_U)$ for any open set U. One further sees that $\mathcal{O}_X(D_1 + D_2) = \mathcal{O}_X(D_1) \otimes_{\mathcal{O}_X} \mathcal{O}_X(D_2)$. This gives us a group law on the collection of $\mathcal{O}_X$-modules of the form $\mathcal{O}_X(D)$.

We now move on to the more geometrically friendly concept of Weil divisors. These only make sense on Noetherian schemes. In one phrase, Weil divisors are *cycles of codimension one.* This is made up of the following concepts:

Definition 3.36. Let X be a topological space, and let V be an irreducible closed subset of X. The *codimension* of V in X, denoted $\mathrm{codim}(V, X)$, is the supremum of the lengths of chains of irreducibles in X of the form

$$Y \subseteq Z_0 \subset Z_1 \subset \cdots \subset Z_n.$$

If Z is a closed set in X, then one sets $\mathrm{codim}(Z, X)$ to be the infinimum of the codimensions of the irreducible components of Z. We say Z is *pure* of codimension n if all irreducible subsets of Z are of codimension n.

Definition 3.37. A *cycle* on a Noetherian scheme X is an element of the direct sum $\bigoplus_{x \in X} \mathbb{Z}$. That is, a cycle is a formal finite sum $\sum_{x \in X} n_x[x]$. If $Z = \sum_{x \in X} n_x[x]$ is a cycle, then we write $\mathrm{mult}_x(Z) := n_x$. If $\mathrm{mult}_x(Z) \geq 0$ for all $x \in X$, then we say Z is *positive* and write $Z \geq 0$. If $\mathrm{mult}_x(Z) = n > 0$ then we say Z has a *zero* of order n_x at x, and similarly if $\mathrm{mult}_x(Z) = n < 0$ then we say Z has a *pole* of order n at x.

Remark 3.38. Since there is a bijection between the points of X and the irreducible components of X (given by $x \mapsto \overline{\{x\}}$), we can reformulate this as a cycle being a formal sum $\sum_{x \in X} n_x[\overline{\{x\}}]$. Additionally, any cycle Z can be written as a difference $Z = Z_0 - Z_\infty$ of two positive divisors (by moving all zeros into Z_0 and all poles into $-Z_\infty$).

Definition 3.39. A prime cycle is a cycle $\sum_{x \in X} n_x[\overline{\{x\}}]$ such that there exists some $y \in X$ with $n_x = 0$ for all $x \in X \backslash \{y\}$.

Definition 3.40. Let Z be a cycle. The *support* of Z is

$$\mathrm{Supp}\, Z := \bigcup_{\substack{x \in X \\ \mathrm{mult}_x(Z) \neq 0}} \overline{\{x\}}.$$

Definition 3.41. A cycle Z on a Noetherian scheme X is said to be of *codimension n* if $\operatorname{Supp} Z$ is pure of codimension n. A cycle of codimension one is called a *Weil divisor*, and we denote the group of such divisors by $\operatorname{Div}_{\mathrm{W}}(X)$. If U is an open subscheme of X, then one can restrict a Weil divisor Z to U in an obvious way (by removing unused terms in the formal sum), and one denotes this by $Z|_U$.

Remark 3.42. It can be shown that $\operatorname{codim}(\overline{\{x\}}, X) = \dim \mathcal{O}_{X,x}$, so that a cycle $\sum_{x\in X} n_x[\overline{\{x\}}]$ is a Weil divisor if and only if $\dim \mathcal{O}_{X,x} = 1$ for all $x \in X$ such that $n_x \neq 0$.

Example 3.43. If X is an algebraic curve over a field k, then the cycles of codimension one are just formal sums of closed points on X.

Proposition 3.44. *Let X be a regular, integral, and Noetherian scheme. Then the notions of Cartier divisors and Weil divisors coincide, i.e. there exists an isomorphism $[-]\colon \operatorname{Div}_W(X) \xrightarrow{\sim} \operatorname{Div}_C(X)$, such that a Cartier divisor D is effective if and only if $[D]$ is positive.*

Proof. See [Liu10, p. 271, Prop. 2.16]. ■

Remark 3.45. Although this is not how [Liu10] does it, the above proposition allows us to introduce the notions of principal Weil divisor and linear equivalence of Weil divisors by porting them from Cartier divisors. In fact, [Liu10, p. 270, Prop. 2.14] provides proof that this does not lead to errors. Similarly, this lets us speak of the multiplicity of a Cartier divisor at a point $x \in X$, by setting $\operatorname{mult}_X(D) := \operatorname{mult}_x([D])$.

Definition 3.46. Let D be (Weil or Cartier) divisor on a regular, integral, and Noetherian curve X over a field k. Then the *degree* of D is the integer

$$\deg_k D = \sum_{x\in X} \operatorname{mult}_x(D)[k(x) : k].$$

Definition 3.47. Let D be a (Weil or Cartier) divisor. Then define $L(D) := \mathrm{H}^0(X, \mathcal{O}_X(D))$, and $\ell(D) := \dim_k L(D)$.

Remark 3.48. If X is an integral projective curve over k, then one gets that $L(D) = \{f \in K(X)^\times \mid \operatorname{div}(f) + D \geq 0\} \cup \{0\}$.

We now state the Riemman–Roch theorem.

Theorem 3.49 (Riemann–Roch)**.** *Let $f\colon X \to \operatorname{Spec} k$ be a projective curve over a field k, and let $D \in \operatorname{Div}_C(X)$. Then*

$$\dim_k \mathrm{H}^0(X, \mathcal{O}_X(D)) - \dim_k \mathrm{H}^0(X, \omega_f \otimes \mathcal{O}_X(-D)) = \deg_k D - p_a(X) + 1.$$

Proof. See [Liu10, p. 281, Thm. 3.26]. It is essentially a consequence of cohomological duality and a more classical theorem about the degree of a divisor (see [Liu10, p. 279, Thm. 3.17]), which follows essentially from the flatness of $\mathcal{O}_X(E)$ for certain divisors E. ■

Remark 3.50. Primarily, we will be interested in Weil divisors for computation in the next subsection, and we need the above proposition to show that we may later apply Riemann-Roch to both Cartier divisors *and* Weil divisors.

3.3 Elliptic Curves as Schemes

In this subsection, we will sketch a proof that elliptic curves have a defining equation of a particular form, as well as give a good definition of what they are in the first place. For this subsection, we will take the following convention regarding curves:

Definition 3.51. A *nice* curve over a field k is a geometrically connected, smooth, and integral projective curve over k.

Remark 3.52. Recall that the above conditions let us conclude that $p_g = p_a$, so that we may refer to these as simply the genus.

Definition 3.53. Let k be a field. An *elliptic curve* is a pair (E, o) with E a nice curve over k of genus one, and $o \in E(k)$. Notationally, we often omit mention of the priviledged point o.

Before we begin with proving properties of elliptic curves, we need a lemma about $\ell(D)$ for divisors with $D < 0$.

Lemma 3.54. *Let X be an integral projective curve over a field k, and let D be a divisor with $D < 0$ (i.e. $-D \geq 0$ and $D \neq 0$). Then $\ell(D) = 0$.*

Proof. See [Liu10, p. 280, Prop. 3.25]. ■

Theorem 3.55. *Let E/k be an elliptic curve. Then there exists a closed immersion $i \colon E \to \mathbb{P}^2_k$ with image given by an equation of the form*

$$v^2 w = u^3 + auw^2 + bw^3, \text{ where } a, b \in k.$$

Proof. We will get the above theorem by inspecting the divisors given by natural number multiples of o. Let $m \in \mathbb{N}$. Then the above lemma tells us that $\ell(-mo) = 0$. Furthermore, [Liu10, p. 283, Exm. 3.35] gives $\mathcal{O}_X \cong \omega_{E/k}$ so that $\omega_{E/k} \otimes \mathcal{O}_X(-mo) = \mathcal{O}_X(-mo)$. Furthermore, note that $\deg_k(mo) = m$, since $o \in E(k)$, which implies that $k(o) = k$. Hence, Riemann–Roch gives

$$\ell(mo) = \ell(mo) - \ell(-mo) = \deg_k(mo) = m.$$

By the description of $L(D)$ given in Remark 3.48, we see that there is a natural inclusion $L(no) \subseteq L(mo)$ if $n \leq m$. We have that $1 \in L(o)$, so we let $\{1, u\}$ be a basis for $L(2o)$ and $\{1, u, v\}$ be a basis for $L(3o)$. We then consider these, via the natural inclusion, as elements of $L(6o)$, and produce the collection of elements $\{1, u, v, v^2, uv, u^2, u^3\} \subseteq L(6o)$. These are in $L(6o)$ since $\operatorname{div}(fg) = \operatorname{div}(f) + div(g)$. There are seven quantities here, and so we have a non-trivial relation

$$b_0 v^2 + b_1 v + b_2 uv = a_0 u^3 + a_1 u^2 + a_3 u + a_4.$$

We now use that u^2 and uv are independent of $\{1, u, v\}$, so that $b_0 a_0 \neq 0$ (otherwise we would get that $\ell(5o) \neq 5$, which is a contradiction). We can then, by a change of coordinates, assume that $b_0 = a_0 = 1$. Furthermore, we can perform the transformation $v \mapsto v + \frac{1}{2}(b_1 u + b_2)$ to complete the square on the left, giving us that we may assume $b_1 = b_2 = 0$. Finally, we apply the standard change of variables for depressing a cubic $u \mapsto u - a_1/3$ to get that we may assume that $a_1 = 0$. Thus, setting $a = a_2$ and $b = a_3$, we are left with the equation

$$v^2 = u^3 + au + b.$$

We now want to embed E into $\mathbb{P}^2_k$. For D any divisor, and $s \in \mathcal{O}_X(D)(E)$, set $E_s := \{x \in E \mid \mathcal{O}_E(D)_x = [s]_x \mathcal{O}_{E,x}\}$. This is an open set, and one gets an isomorphism $s\mathcal{O}_E|_{E_s} \cong \mathcal{O}_E(D)|_{E_s}$. We can then consider, for any $t \in \mathcal{O}_E(D)(E)$, the quotient t/s as an element of $\mathcal{O}_E(X_s)$. We now apply this to the elements u, v above. The elements $\{1, u, v\}$ are a basis for $L(3o)$, so $\{E_1, E_u, E_v\}$ covers E. For notational purposes, set $(s_0, s_1, s_2) = (1, u, v)$. We now construct, for each i, a map $f_i \colon E_{s_i} \to D_+(t_i) \subseteq \mathbb{P}^2_k = \operatorname{Proj} k[t_0, t_1, t_2]$. This map is induced by

$$\mathcal{O}_{\mathbb{P}^2_k}(D_+(t_i)) \to \mathcal{O}_E(E_{s_i}), \quad t_j/t_i \mapsto s_j/s_i \in \mathcal{O}_E(E_{s_i}),$$

where we use Proposition 2.72 to turn this into a full morphism (recall that $D_+(t_i)$ is affine). The maps f_i agree on overlap, and so we use Lemma 2.118 to glue these together to a map $f \colon E \to \mathbb{P}^2_k$, which clearly has image

$$V_+(t_2^2 t_0 - t_1^3 - a t_1 t_0^2 - b t_0^3).$$

We now just need to know that this map is a closed immersion. However, this results from the notion of a *very ample* divisor, whose definition boils down to saying that a divisor is very ample if the analogue of the above map for that divisor is a closed immersion. We then have a proposition, [Liu10, p. 286, Prop. 1.4], which states that a divisor D is very ample whenever $\deg D \geq 2g + 1$. In our case, $g = 1$, and $\deg(3o) = 3$, so $3o$ is very ample, and hence the above map is a closed immersion. Hence, we get the theorem. Furthermore, since both u, v necessarily have poles at o, it must be that $f(o) = [0 : 0 : 1]$, i.e. o is sent to the point at infinity on the v-axis (i.e. the t_2-axis). ■

Remark 3.56. The above basically states that an elliptic curve is, in "common notation", given by an equation of the form $y^2 = x^3 + ax + b$. The above theorem gives exactly that if one looks at the chart $D_+(t_0)$, where we may divide away the t_0's.

Proposition 3.57. *Any two equations defining a fixed elliptic curve as above are related by a change of coordinates of the form* $u = \alpha_1^2 u' + \alpha_2$*,* $v = \alpha_1^3 v' + \alpha_1^2 \alpha_2 u' + \alpha_3$*.*

Proof. See [Sil09, p. 59–60, Prop. 3.1]. ■

Definition 3.58. Let E/k be an elliptic curve. An equation of the form of the above theorem for E is called a *Weierstrass equation* for E. If $k = K$ is a number field (i.e. a finite extension of $\mathbb{Q}$), then we may multiply away denominators to get an equation with all coefficients in $\mathscr{O}_K$, i.e. the ring of integers of K, and use the above coordinate transformations to set the coefficient on x^3 to be one. We then call this an *integral* Weierstrass equation for E.

Suppose we are given some "Weierstrass-type" equation $v^2 = u^3 + au + b$ (we write it here in inhomogeneous coordinates for convenience). To this we can associate a quantity called the *discriminant*, which will tell us when this defines a "true" elliptic curve.

Definition 3.59. Let C be a projective curve given by an equation of the form $A \colon v^2 = u^3 + au + b$, with $a, b \in R$. The *discriminant* of the equation A is the quantity $\Delta := -16(4a^3 + 27b^2)$.

Proposition 3.60. *Let C be a projective curve given by the equation A above. Then C is smooth if and only if* $\Delta \neq 0$*.*

Proof. See [Sil09, p. 45, Prop. 1.4] and [Liu10, p. 130, Thm. 2.19]. The proof is based on the Jacobian criterion for regularity (which becomes a criterion for smoothness when one recognizes that smoothness over a field is the same as geometric regularity). The statement of the Jacobian criterion in [Liu10] is for affine algebraic varieties, but this is easily extended to projective varieties by standard "affine chart" arguments. ■

Remark 3.61. The above lets us essentially check if a curve given by a "Weierstrass-type" equation defines a well-behaved elliptic curve, in the sense that we require an elliptic curve to be nice (hence smooth).

The aim of this thesis is the weak Mordell–Weil theorem for elliptic curves, which concerns the behavior of the group structure on the rational points on an elliptic curve. Hence, we will now sketch a proof of the existence of such a group structure. First, we need to know what it means for a scheme to be a group scheme.

Definition 3.62. Let S be a scheme. A *group scheme* over S is an S-scheme G equipped with three morphisms: a *multiplication map* $\mu\colon G \times_S G \to G$, a *unit selection map* $\eta\colon S \to G$, and an *inversion map* $\nu\colon G \to G$, satisfying the following commutative diagrams:

$$\begin{tikzcd}
G \times_S G \times_S G \arrow[r, "\mu \times_S \mathrm{id}_G"] \arrow[d, "\mathrm{id}_G \times_S \mu"'] & G \times_S G \arrow[d, "\mu"] \\
G \times_S G \arrow[r, "\mu"] & G
\end{tikzcd} \qquad \text{(associativity),}$$

$$\begin{tikzcd}
G \times_S S \arrow[r, "\mathrm{id}_G \times_S \eta"] \arrow[dr, "\mathrm{id}_G"'] & G \times_S G \arrow[d, "\mu"] \\
 & G
\end{tikzcd} \qquad \text{(right-identity),}$$

$$\begin{tikzcd}
G \arrow[r, "\Delta_{G/S}"] \arrow[d] & G \times_S G \arrow[r, "\mathrm{id}_G \times \nu"] & G \times_S G \arrow[d, "\mu"] \\
S \arrow[rr, "\eta"] & & G
\end{tikzcd} \qquad \text{(right-inverse)}$$

Remark 3.63. Let T be an S-scheme and G be a groups scheme over S. Then the morphisms above induce a "real" group structure on $G(T)$, since the commutative diagrams translate directly to the standard group axioms.

Definition 3.64. Let S be a scheme, and let G be a group scheme over S. Then we say G is commutative if for every S-scheme T, the induced group $G(T)$ is Abelian.

Definition 3.65. Let G be a group scheme over S. A *subgroup scheme* of G is a closed subscheme H of G such that $H(T)$ is a subgroup of $G(T)$ for all $T \in \mathbf{Sch}/S$.

Definition 3.66. Let G and G' be group schemes over S. A homomorphism of group schemes $f : G \to G'$ is a morphism of schemes that is compatible with the multiplication maps μ. In particular, f should satisfy $f \circ \mu = \mu \circ (f \times_S f)$. The *kernel* of f is $\ker f := G \times_{G'} S$, where one takes the fiber product with respect to the map $\eta\colon S \to G'$.

Remark 3.67. The above has some nice functorial interpretations. A major theme within modern algebraic geometry is that one replaces a scheme with a functor representing the scheme. This is justified by the Yoneda lemma, which says that an S-scheme X is equivalent to the functor $X(-) : (\mathbf{Sch}/S)^{\mathrm{op}} \to \mathbf{Set}$. One says that a functor $F : (\mathbf{Sch}/S)^{\mathrm{op}} \to \mathbf{Set}$ is *representable* if there is some scheme X such that $F \cong X(-)$. In this framework, a group scheme over S is a representable functor $G : (\mathbf{Sch}/S)^{\mathrm{op}} \to \mathbf{Grp}$, a commutative group scheme over S is a representable functor $(\mathbf{Sch}/S)^{\mathrm{op}} \to \mathbf{Ab}$, and a morphism of group schemes is simply a natural transformation $G \to G'$. See also [Sil94, p. 309, Prop. 3.2] for a proof of the main content of this remark.

Definition 3.68. Let k be a field. An *algebraic group* over k is a group scheme over k of finite type. An *Abelian variety* over k is an algebraic group over k that is geometrically integral and proper over k.

Remark 3.69. An Abelian variety is always commutative and projective. See the reference from [Liu10, p. 298, Defn. 4.37] for a proof of this.

Definition 3.70. Let m be a natural number, and let G be an Abelian variety over a field k. Then the *multiplication-by-m* homomorphism, denoted $[m]$, is constructed by composing the map $\mu \circ \Delta_{G/S}$ with itself $m-1$ times. If T is an S-scheme, then this induces the standard multiplication-by-m map on $G(T)$. We write $G[m] := \ker([m])$, and call this the group (scheme) of *m-torsion points* of G. Clearly, if T is a k-scheme then $G[m](T)$ is the m-torsion part of $G(T)$.

There is an important theorem about the structure of $G[m]$ for an Abelian variety G, which is of interest to us since it is required for a reduction in the proof of the weak Mordell–Weil theorem.

Theorem 3.71. *Let A be an Abelian variety of dimension d over a field k, and let m be some natural number. If m is coprime to the characteristic of k, then $A[m]$ is étale over k and we have $A[m](\bar{k}) \cong (\mathbb{Z}/m\mathbb{Z})^{2d}$; if $\operatorname{char}(k) = p > 0$ and $m = p^n$ then there exists some $0 \leq d' \leq d$ such that $A[m](\bar{k}) = (\mathbb{Z}/m\mathbb{Z})^{d'}$.*

Proof. See the reference in [Liu10, p. 299, Thm. 4.38]. ■

Corollary 3.72. *Let A be an Abelian variety of finite dimension over a field k with $\operatorname{char}(k) = 0$. Then, for any $m > 0$, the Abelian variety $A[m]$ is finite as a set, and for any finite extension k'/k, $A[m](k')$ is finite.*

Proof. The above theorem says $A[m]$ is étale. Hence, by Proposition 2.194, $A[m]$ is finite as a set, since étale implies unramified. The second statement follows from the fact that $A[m](k') \subseteq A[m](\bar{k})$, and the latter is finite. ■

Proposition 3.73. *Let (E, o) be an elliptic curve over a field k. Then*

(a) for any extension k'/k and pair of points $(x, y) \in E(k') \times E(k')$, there exists a unique point $m_{k'}(x, y) \in E(k')$ such that, as divisors, we have

$$m_{k'}(x, y) + o \sim x + y.$$

The map $m_{k'}$ gives $E(k')$ the structure of an Abelian group with identity o. If k''/k' is some further extension, then $m_{k'} = m_{k''}|_{E(k') \times E(k')}$.

(b) if $x \in E(k)$, there exists a k-automorphism $t_x : E \to E$, called the translation by x, such that for any extension k'/k the map $E(k') \to E(k')$ is the map $z \mapsto m_{k'}(z, x)$ (i.e. the traditional translation by x map).

Proof. See [Liu10, p. 490, Lemma 2.8] for a full proof. We will sketch the proof of part (a).

Riemann-Roch gives that $\ell(x + y - 0) = \dim_{k'} \mathrm{H}^0(\mathcal{O}_{E_{k'}}(o - x - y)) + 1 = 1 \neq 0$, so that $x + y - o$ is linearly equivalent to a divisor D which is effective and of degree one, hence equivalent to a rational point $z \in E(k')$. This point is unique, since otherwise (by [Liu10, p. 277, Cor. 3.12]) E would be isomorphic to $\mathbb{P}^1_{k'}$. We then set $m_{k'}(x, y) = z$. The fact that this gives $E(k')$ an Abelian group structure is then immediate, since it is inherited from the group structure on the divisors. ■

Remark 3.74. Geometrically, the above group law is given finding remaining intersection c between the line given by x, y and $E(k')$, then taking the remaining intersection of $E(k')$ with the line given by c, o. Practically speaking, this is the same as reflecting c about the horizontal axis.

Theorem 3.75. *Let (E, o) be an elliptic curve over a field k. Then E has the structure of an Abelian variety with identity given by o, and such that if k'/k is any extension then the induced group structure on $E(k')$ coincides with that given in Proposition 3.73.*

Proof. See [Liu10, p. 291, Prop. 2.9]. The proof essentially consists of constructing $\mu\colon E\times_k E \to E$ from the translation map t_x from Proposition 3.73. In particular, one uses the translation-by-ξ map, where ξ is the generic point of E, to get an automorphism $E \times_k E \to E \times_k E$, which one then composes with the first projection to get a map $E \times_k E \to E$. One constructs the other required maps in a similar way. One then just checks that these maps satisfy the required properties. ■

3.4 Reduction

In number theory, it is incredibly useful to study the solutions of an equation by reducing modulo a prime. Similarly, one can also study certain schemes in this way, through a related technique. The main idea is to define the notion of a *model*. A model is meant to act as a kind of "amalgamation" of all possible reductions of a scheme, whereby one produces a particular one by choosing a particular fiber. A great amount of effort is taken in the general theory of models in choosing a "good" model that still retains enough information about the original scheme (see, for example, [Liu10, Ch. 10]).

We will mainly be interested in models over *Dedekind domains*. These are generalizations of integers in many contexts (e.g. the ring of integers of a number field, or of a similar situation for local fields).

Definition 3.76. Let R be an integral domain with field of fractions K. We say R is a *Dedekind domain* if it is Noetherian, of Krull dimension one (i.e. every prime ideal is maximal), and if whenever $x \in K$ satisfies a polynomial equation $x^n + a_{n-1}x^n + \cdots a_1 x + a_0 = 0$ with $a_i \in R$ then $x \in R$.

For the rest of this subsection, let R denote a Dedekind domain with fraction field K, and let X be a K-scheme.

Definition 3.77. Let $\xi \in \operatorname{Spec} R$ denote the generic point. An *R-model* of X is an R-scheme $\hat{X}$ equipped with an isomorphism $X \cong \hat{X}_\xi$. Let $\mathfrak{p} \subseteq R$ be a prime ideal. The *reduction* of X at $\mathfrak{p}$ with respect to the model $\hat{X}$ is the fiber over $\mathfrak{p}$, i.e. $\hat{X}_\mathfrak{p}$.

Example 3.78. Set $f = t_2^2 t_0 - t_1^3 - 5t_1t_0^2 - t_0^3 \in \mathbb{Q}[t_0, t_1, t_2]$, and let $X = \operatorname{Proj} \mathbb{Q}[t_0, t_1, t_2]/(f)$, i.e. X is the elliptic curve given by the equation $y^2 = x^3 + 5x + 1$. Then we see by an easy calculation that $\hat{X} = \operatorname{Proj} \mathbb{Z}[t_0, t_1, t_2]/(f)$ is a $\mathbb{Z}$-model of X. From this, if we pick a prime $\mathfrak{p} = (p)$ of $\mathbb{Z}$ then

$$\hat{X}_\mathfrak{p} = \hat{X} \times_\mathbb{Z} \operatorname{Spec}(\mathbb{F}_p) = \operatorname{Proj}(\mathbb{Z}[t_0, t_1, t_2]/(f) \otimes_\mathbb{Z} \mathbb{F}_p) = \operatorname{Proj}(\mathbb{F}_p[t_0, t_1, t_2]/(t_2^2 t_0 - t_1^3 - 5t_1t_0^2 - t_0^3).$$

In other words, this does indeed reduce the coefficients of the defining equation as desired. For example, if $p = 3$, then $\hat{X}_\mathfrak{p} = \operatorname{Proj}(\mathbb{F}_3[t_0, t_1, t_2]/(t_2^2 t_0 - t_1^3 - 2t_1t_0^2 - t_0^3))$.

The question is now when these reductions are well-behaved. In particular, we will want to know about how often reducing by a prime produces a scheme which is not smooth.

Definition 3.79. Let $\mathfrak{p}$ be a prime of R. We say X has *good reduction* at $\mathfrak{p}$ if there exists some $R_\mathfrak{p}$-model $\hat{X}$ of X such that $\hat{X} \to \operatorname{Spec} R_\mathfrak{p}$ is proper and smooth. We say X has good reduction if it has good reduction at all primes of R. If X does not have good reduction at $\mathfrak{p}$, then we say it has *bad reduction* at $\mathfrak{p}$.

Remark 3.80. Note that if we have some R-model $\hat{X}'$ of X, then we may perform a base change by $R_\mathfrak{p}$ to get an $R_\mathfrak{p}$-model $\hat{X}'_{R_\mathfrak{p}}$. Hence, we can exhibit good reduction at $\mathfrak{p}$ by choosing an R-model such that the induced $R_\mathfrak{p}$ model is smooth.

Proposition 3.81. *An elliptic curve over K has bad reduction at only a finite number of primes.*

Proof. See [Liu10, p. 462, Prop. 1.21]. This also follows from Proposition 3.60. ■

Remark 3.82. The primes where E has good reduction are essentially those where reducing gives another elliptic curve, now over a finite field. In our definition of an elliptic curve, we disallowed fields of characteristic two, but this is really for simplicity, and the case of characteristic two isn't that different from the others. Additionally, one can simply add the primes with characteristic two residue fields to the set of primes with bad reduction at no cost, since there are also usually only finitely many of them.

Since elliptic curves come with a description via a Weierstrass equation, they automatically have models given by these equations. In particular, one chooses some integral equation $y^2 = x^3 + ax + b$ for the elliptic curve, then produces a model via

$$\operatorname{Proj} R[t_0, t_1, t_2]/(t_2^2 t_0 - t_1^3 - a t_1 t_0^2 - b t_0^3).$$

This is called the *Weierstrass model* associated to the pair (a, b).

Definition 3.83. We denote the Weierstrass model associated to (a, b) as $\mathcal{W}(a, b)$.

We now want to define a reduction map of some sort. In particular, let E be some elliptic curve over K and let $\hat{E} = \mathcal{W}(a, b)$ be a Weierstrass model for E. We want to end up with some kind of map $E(K) \to \hat{E}_{\mathfrak{p}}(k(\mathfrak{p}))$, and we want this map to be a group homomorphism. How do we achieve this? First, we will note that we require $\hat{E}$ to be sufficiently smooth over $\mathfrak{p}$ for this to work (actually, it is possible to work with this even when the model is not entirely smooth by taking the largest smooth subscheme, but this is not necessary for us). Hence, we will consider a model over a ring which removes the troublesome primes. Recall from Proposition 3.60 that a curve defined by a Weierstrass equation is smooth if and only if the discriminant is zero. In the case of reduction, this translates to the model $\hat{E}$ being smooth over those primes $\mathfrak{p}$ with $\Delta \notin \mathfrak{p}$.

Definition 3.84. Let S be a collection of primes of R. The *S-localization* of R is the localization

$$R_S := \{x \in K \mid \forall \mathfrak{p} \notin S,\, x \in R_{\mathfrak{p}}\}.$$

In other words, we remove the primes in S from $\operatorname{Spec} R$.

Now consider the set $S = \{\mathfrak{p} \in \operatorname{Spec} R \mid \Delta \in \mathfrak{p}\}$. We move the model $\hat{E}$ to being over R_S by taking the fiber product $\hat{E}_{R_S}$. Bear in mind that this still has the same defining equation, and we have $\hat{E}_{\mathfrak{p}} \cong \hat{E}_{R_S,\mathfrak{p}}$ when $\mathfrak{p} \notin S$. Furthermore, this is a smooth model of E. We then have the following theorem:

Theorem 3.85. *Let $\hat{E}$ be as above. Then the natural composition $\hat{E}_{R_S}(R_S) \to \hat{E}_{R_S}(K) \to E(K)$ is an isomorphism, and the group structure on E extends to $\hat{E}_{R_S}$, and make the latter into a smooth group scheme.*

Proof. See [Sil94, p. 321, Thm. 5.3 & p. 329, Cor. 6.3]. ■

Now we will define the reduction map. First of all, note that we have a map $\hat{E}_{R_S}(R_S) \to \hat{E}_{R_S}(k(\mathfrak{p}))$ stemming from the map $R_S \to R_S/\mathfrak{p}$. We then note that for any (S-)scheme X and (S-scheme) Y, one has $X(Y) \cong X_Y(Y)$. Hence, we see that $\hat{E}_{R_S}(k(\mathfrak{p})) \cong \hat{E}_{R_S,\mathfrak{p}}(k(\mathfrak{p})) \cong \hat{E}_{\mathfrak{p}}(k(\mathfrak{p}))$. From this, we get reduction.

Definition 3.86. Let $\mathfrak{p}$ be a prime in R with $\Delta \notin \mathfrak{p}$. Then we define the *reduction modulo* $\mathfrak{p}$ map $r_{\mathfrak{p}}$ as the composition

$$E(K) \xrightarrow{\sim} \hat{E}_{R_S}(R_S) \to \hat{E}_{R_S}(k(\mathfrak{p})) \xrightarrow{\sim} \hat{E}_{\mathfrak{p}}(k(\mathfrak{p})).$$

Proposition 3.87. *The reduction modulo $\mathfrak{p}$ map is a group homomorphism.*

Proof. Let T be any R_S-scheme. Then we have a commutative diagram

$$\begin{tikzcd}
\hat{E}_{R_S} \times_S \hat{E}_{R_S} \arrow[r, "\mu"] & \hat{E}_{R_S} \\
\hat{E}_{R_S,T} \times_T \hat{E}_{R_S,T} \arrow[r, "\mu"] \arrow[u] & \hat{E}_{R_S,T} \arrow[u]
\end{tikzcd}$$

where the horizontal arrows arise from the group-scheme structures on $\hat{E}_{R_S}$ and $\hat{E}_{R_S,T}$, and the vertical arrows are induced by the canonical projections. Taking R_S and T points here, and combining this with $\hat{E}_{R_S,T}(T) \cong \hat{E}_{R_S}(T)$, we see that the canonical map $\hat{E}_{R_S}(R_S) \to \hat{E}_{R_S}(T)$ is compatible with the induced group structure on these, hence is a group homomorphism. Taking $T = \operatorname{Spec} K$ and $T = \operatorname{Spec} k(\mathfrak{p})$, we get the desired result since $r_{\mathfrak{p}}$ is then the composition of a number of group homomorphisms. (Note also [Sil94, p. 309, Prop. 3.2].) ■

Remark 3.88. If we instead worked purely over R instead of R_S, we would get an analogous statement about the map $r_{\mathfrak{p}}$ being a group homomorphism when restricted to the smooth points. Since there are essentially no differences in presentation aside from a few details, we will not explicitly deal with this case, and in particular, the following discussion remains practically unchanged. See [Sil94, p. 231, Thm. 5.3], in particular part (c), and the remarks right after, which say almost exactly this.

To describe what the reduction map looks like, note that the equation for $\hat{E}_{\mathfrak{p}}$ is exactly the equation for E but reduced modulo $\mathfrak{p}$, and in particular then has that the rational points are described as solutions to this equation. For $q \in R$, denote by $\bar{q}$ the reduction of q modulo $\mathfrak{p}$. Then we have that

$$\hat{E}_{\mathfrak{p}}(k(\mathfrak{p})) = \{[q_0 : q_1 : q_2] \in \mathbb{P}(k(\mathfrak{p})^{2+1}) \mid q_2^2 q_0 = q_1^3 + \bar{a} q_1 q_0^2 + \bar{b} q_0^3\}.$$

For any $[x_0 : x_1 : x_2] \in \mathbb{P}(K^{2+1})$, we can choose all $x_i \in R$ by clearing denominators. The map $r_{\mathfrak{p}}$ is given by

$$r_{\mathfrak{p}} \colon [x_0 : x_1 : x_2] \mapsto [\bar{x_0} : \bar{x_1} : \bar{x_2}].$$

We are now interested in the behavior of this reduction map. Consider the point $[0 : 0 : 1]$. This clearly reduces to "itself" in the sense that $r_{\mathfrak{p}}([0 : 0 : 1]) = [0 : 0 : 1]$. Now consider a point $q = [1 : q_1 : q_2]$. If $q_i \in R$, then we just have $r_{\mathfrak{p}}(q) = [1 : \bar{q_1} : \bar{q_2}]$. What happens when $q_i \notin R$?

Definition 3.89. Let $\mathfrak{p}$ be a prime ideal of R. Define the function $v_{\mathfrak{p}} \colon R_{\mathfrak{p}} \to \mathbb{N}_{\geq 0}$ via

$$v_{\mathfrak{p}}(x) = \begin{cases} \infty & \text{if } x = 0, \\ \max\{n \in \mathbb{N}_{\geq 0} \mid x \in \mathfrak{p}^n R_{\mathfrak{p}}\} & \text{otherwise.} \end{cases}$$

Extend this to a function $v_{\mathfrak{p}} \colon K \to \mathbb{Z}$ by setting $v_{\mathfrak{p}}(x/y) = v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(y)$.

This function tells us about the "divisibility" of an element of K. First of all, note that $v_{\mathfrak{p}}(x) < 0$ means that there is some $n > 0$ such that $1/x \in \mathfrak{p}^n$. If $R = \mathbb{Z}$, then this is analogous to saying that the denominator of x is divisible by p^n. Furthermore, one observes that $v_{\mathfrak{p}}$ satisfies certain obvious properties:

Lemma 3.90. *Let $x, y \in K$, and set $v = v_{\mathfrak{p}}$. Then*

(a) $v(xy) = v(x) + v(y)$*,*

(b) $v(x) \geq 0$ *if and only if* $x \in R_{\mathfrak{p}}$*,*

(c) $v(x+y) \geq \min\{v(x), v(y)\}$.

Proof. These properties follow trivially from the definition. Particularly, (a) & (b) are immediate. To get (c), note that $\mathfrak{p}R_\mathfrak{p}$ is principally generated; this follows from considering that $R_\mathfrak{p}$ is a local Dedekind domain in the following way: first note that being Dedekind means, by Theorem 4.5, that every ideal in $R_\mathfrak{p}$ has a unique factorization into prime ideals. However, since $R_\mathfrak{p}$ is local, there is only one such ideal, namely $\mathfrak{p}R_\mathfrak{p}$! Therefore, all ideals are powers of $\mathfrak{p}R_\mathfrak{p}$. If $z \in R_\mathfrak{p}$ is such that $v(z) = e$, then it is clear that $zR_\mathfrak{p} = \mathfrak{p}^e R_\mathfrak{p}$, so that all powers of $\mathfrak{p}R_\mathfrak{p}$ are principal. Hence, $R_\mathfrak{p}$ is a principal ideal domain. From this, it is obvious how to prove (c): if z generates $\mathfrak{p}R_\mathfrak{p}$, and you suppose that $v(x) \leq v(y)$, then you just factor out $z^{v(x)}$ from $x+y$ to get that $x + y \in \mathfrak{p}^{v(x)}R_\mathfrak{p}$. Extending this to K from $R_\mathfrak{p}$ is also immediate, since one in essence just performs the same operation as when one factors out a prime p from a fraction x/y in $\mathbb{Q}$. ■

Using Lemma 3.90, we can prove some things about the behavior of a point $[1 : x : y]$. In particular,

Lemma 3.91. *Let* $[1 : x : y] \in E(K)$*, let* $\mathfrak{p}$ *be a prime in* R*, and set* $v = v_\mathfrak{p}$*. Then*

(a) $v(x) \geq 0$ *if and only if* $v(y) \geq 0$*,*
(b) if $\min\{v(x), v(y)\} < 0$ *then there exists some* $n > 0$ *such that* $v(x) = -2n$ *and* $v(y) = -3n$*.*

Proof. We begin with (a): suppose $v(x) \geq 0$. Then, since $y^2 = x^3 + ax + b$, we have that

$$2v(y) = v(x^3 + ax + b) \geq \min\{3v(x), v(a) + v(x), v(b)\} \geq 0,$$

so that $v(y) \geq 0$. Now suppose $v(y) \geq 0$. Then

$$3v(x) = v(y^2 - ax - b) \geq \min\{2v(y), v(a) + v(x), v(b)\} \geq \min\{2v(y), v(x), v(b)\}.$$

From this follows two possibilities: either $3v(x) \geq \min\{2v(y), v(b)\}$, in which case the non-negativity of the latter implies that $v(x) \geq 0$, or $3v(x) \geq v(x)$, which can only happen if $v(x) \geq 0$ (since if $v(x) < 0$ then $3v(x) < v(x)$). Hence $v(x) \geq 0$. This proves part (a).

Now for part (b). Suppose $v(x), v(y) < 0$. Then we can first see that

$$\begin{aligned} 2v(y) = v(x^3 + ax + b) &\geq \min\{3v(x), v(x) + v(a), v(b)\} \\ &\geq \min\{3v(x), v(x)\} = 3v(x). \end{aligned}$$

Hence, $2v(y) \geq 3v(x)$. We now aim to show the reverse inequality. Note that $3v(x) < v(x)$ and compute

$$\begin{aligned} 3v(x) = v(y^2 - ax - b) &\geq \min\{2v(y), v(x) + v(a), v(b)\} \\ &\geq \min\{2v(y), v(x)\}. \end{aligned}$$

Hence, to avoid contradiction, it must be that $3v(x) \geq 2v(y)$. We therefore conclude that $3v(x) = 2v(y)$, which further gives that $2|v(x)$ and $3|v(y)$. Using this, write $v(x) = 2m$ and $v(y) = 3m'$. This gives

$$6m = 3v(x) = 2v(y) = 6m' \implies 6m = 6m' \implies m = m'.$$

Setting $n = -m$, we find the desired positive integer such that $v(x) = -2n$ and $v(y) = -3n$. ■

The above lets us prove a result which will be extremely important for our proof of weak Mordell–Weil. We will first, however, need to restrict ourselves to the part of the reduction map $r_\mathfrak{p}$ which behaves well.

Definition 3.92. Define $E^0(K) := \{q \in E(K) \mid r_{\mathfrak{p}}(q) \text{ is a smooth point}\}$, and define $\hat{E}_{\mathfrak{p}}^{\mathrm{ns}}$ to be the smooth points of $\hat{E}_{\mathfrak{p}}$. Denote by $r_{\mathfrak{p}}^0 : E^0(K) \to \hat{E}_{\mathfrak{p}}^{\mathrm{ns}}$ the *restricted* reduction map. Set $E^1(K) = \ker r_{\mathfrak{p}}^0$.

Lemma 3.93. *Let $\mathfrak{p}$ be a prime of R such that $a, b \in \mathfrak{p}$. Then the curve $\hat{E}_{\mathfrak{p}}$ has $\hat{E}_{\mathfrak{p}}^{ns} \cong (k(\mathfrak{p}), +)$.*

Proof. See [Sil09, p. 196, Prop. 5.1]. ■

Theorem 3.94. *Let $\mathfrak{p}$ be a prime of R, set $v = v_{\mathfrak{p}}$, and suppose $m \in \mathbb{Z}^+$ is such that m is coprime to the characteristic of $k(\mathfrak{p})$. Then $E^1(K)[m] = 0$, i.e. $r_{\mathfrak{p}}^0$ is injective on m-torsion.*

Proof. Lemma 3.91 tells us that $E^1(K)$ consists of O, along with any points $[1 : x : y]$ such that $v(x), v(y) < 0$, since then (setting, as in the lemma, z to be some generator of $\mathfrak{p}R_{\mathfrak{p}}$) we can write $x = cz^{-2n}$, $y = c'z^{-3n}$, giving

$$[1 : x : y] = [z^{5n} : cz^{3n} : c'z^{2n}] = [z^{3n} : cz : c']$$

which after reduction is clearly $O = [0 : 0 : 1]$. We will now define a sequence of groups, the properties of which will yield the result. Since $E^1(K)\backslash\{O\}$ consists of those points with $v(y) \leq -3 = -3 \cdot 1$, we will define

$$E^n(K) = \{[1 : x : y] \in E^1(K) \mid v(y) \leq -3n\} \cup \{O\}.$$

It is immediately clear that $E^{n+1}(K) \subset E^n(K)$, and that $\bigcap_n E^n(K) = \{O\}$. Now fix some $n > 0$, and consider the change of variables $u' = z^{2n}u$, $v' = z^{3n}v$, so that we get the (inhomogeneous) equation

$$\mathcal{W}' : v'^2 = u'^3 + az^{4n}u' + bz^{6n}.$$

That is, we get the model $\mathcal{W}(az^{4n}, bz^{6n})$. When this is reduced modulo $\mathfrak{p}$, it produces the singular curve $v'^2 = u'^3$. Furthermore, the smooth points of this curve have $(k(\mathfrak{p}), +)$ as their group structure by the preceeding lemma. Let $\ell(q) := \max\{m \in \mathbb{Z}^+ \mid q \in E^m(K)\backslash E^{m+1}(K)\}$. If $\ell(q) < n$, then we see that $q = [1 : x : y]$ gets mapped to a point $q' = [1 : z^{2n}x : z^{3n}y]$, where the divisibility of y is not able to cancel out the z^{3n}, since $v(y) = -3m$ and $m < n$. Hence $r_{\mathfrak{p}}(q)$ is the singular point $[1 : 0 : 0]$. If $\ell(q) = n$, then it cancels out exactly and we get the reduction to some smooth point. If $\ell(q) > n$ then the point q reduces to $O = [0 : 0 : 1]$ by factoring out the remaining powers of z. This shows that the isomorphism $\hat{E}_{\xi} \cong \mathcal{W}(az^{4n}, bz^{6n})_{\xi}$ sends $E^n(K)$ to $(E')^0(K)$, and sends $E^{n+1}(K)$ to $(E')^1(K)$, where we denote by E' the fiber $\mathcal{W}(az^{4n}, bz^{6n})_{\xi}$.

This shows that the E^i's are always groups, and that they are therefore subgroups of each other. Since they are abelian, it follows that we can take the quotient. Then $E^n/E^{n+1} \cong (E')^0/(E')^1 \cong \mathcal{W}(az^{4n}, bz^{6n})_{\mathfrak{p}}^{\mathrm{ns}} \cong (k(\mathfrak{p}), +)$. Since m is coprime to the characteristic of $k(\mathfrak{p})$, it follows that the torsion part of $k(\mathfrak{p})$ is trivial. Now, suppose $q \in E^1(K)$ is such that $mq = 0$. Then, since q has m-torsion, it must map to zero in $E^1(K)/E^2(K) \cong k(\mathfrak{p})$, so that $q \in E^2(K)$. Now suppose $q \in E^n(K)$ with $mq = 0$. Then q maps to zero in $E^n(K)/E^{n+1}(K)$ since the m-torsion of this is also trivial, so that $q \in E^{n+1}$. Induction then gives that if $q \in E^1(K)$ with $mq = 0$, then $q \in E^n(K)$ for all n, i.e. $q \in \bigcap_n E^n(K) = \{O\}$, i.e. $q = O$.

Hence, we see that $E^1(K)[m] = 0$. ■

4 Weak Mordell–Weil

Here we prove the main goal of this thesis: the weak Mordell–Weil theorem. We first state the motivation for the weak Mordell–Weil conjecture, namely that it constitutes roughly "half" of a proof of the full Mordell–Weil theorem. We then quicly introduce some of the necessary concepts from algebraic number theory, afterwhich we proceed to prove the theorem. The information here is based on [Sil09], [Neu99], and [Cla12], with the latter serving mostly as inspiration.

4.1 The Descent Theorem

The theorem presented in this subsection is the basis for the standard proof of Mordell–Weil, and is the motivation for the statement of the weak Mordell–Weil theorem. The basic idea of the descent theorem is that if we have a sufficiently nice function that can measure the "complexity" of a point, and we have the finiteness condition on the quotient group, then we can show that any element can be decomposed into a finite amount of sufficiently simple generators.

Theorem 4.1 (Descent)**.** *Let A be an Abelian group such that there exists an integer $m \geq 2$ with A/mA finite, and let $h\colon A \to \mathbb{R}$ be a function satisfying:*

(a) For every $Q \in A$ there is a constant C_1 (depending on Q) such that

$$h(P+Q) \leq 2h(P) + C_1 \quad \text{for all } P \in A.$$

(b) There is a constant C_2 (depending only on A and m) such that

$$h(mP) \geq m^2 h(P) - C_2 \quad \text{for all } P \in A.$$

(c) For every constant C, the set $\{P \in A \mid h(P) \leq C\}$ is finite.

Then A is finitely generated.

Proof. Let $P \in A$. We will construct P as a linear combination of elements in A, and using (c) above conclude that the number of possible generators is finite by having enough generators satisfy a height condition.

Let $Q_1, \ldots, Q_r \in A$ be a set of elements of A representing each equivalence class in A/mA. We then have that for some $1 \leq i_1 \leq r$, $P \in [Q_{i_1}]$, so that $P = mP_1 + Q_{i_1}$ for some $P_1 \in A$. Similarly, we have that for some $1 \leq i_2 \leq r$, $P_1 \in [Q_{i_2}]$, so that $P_1 = mP_2 + Q_{i_2}$ for some $P_2 \in A$. Continuing this, we produce a list of elements of A:

$$\begin{aligned} P &= mP_1 + Q_{i_1} \\ P_1 &= mP_2 + Q_{i_2} \\ &\vdots \\ P_{n-1} &= mP_n + Q_{i_n}. \end{aligned} \tag{1}$$

This shows that we can write P as a linear combination of the Q_i and some other element $P_n \in A$. We will now show that for some (large) n, $h(P_n)$ is bounded by a constant that is *independent* of P, so that we can later apply (c) from above to show that there are only finitely many possible choices of P_n. To do this, we first examine $h(P_j)$ for any j:

$$\begin{aligned} h(P_j) &\leq \frac{1}{m^2}(h(mP_j) + C_2) && \text{from (b)}, \\ &= \frac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C_2) && \text{from (1)}, \\ &\leq \frac{1}{m^2}(2h(P_{j-1}) + C_1' + C_2) && \text{from (a)}. \end{aligned}$$

Here, C_1' is the maximum of the C_1 constants derived from (a) using $Q \in \{-Q_1, \ldots, -Q_r\}$. Also notice that the constants C_1' and C_2 are independent of P, since both (a) and (b) are independent of P. Now, applying this inequality a second time, we obtain

$$h(P_j) \leq \frac{1}{m^2}\left(\frac{2}{m^2}\left(2h(P_{j-2}) + C_1' + C_2\right) + C_1' + C_2\right) = \left(\frac{2}{m^2}\right)^2 h(P_{j-2}) + \left(\frac{1}{m^2} + \frac{2}{m^4}\right)(C_1' + C_2).$$

Continuing this recursively for $j = n$ all the way down to P, we get that

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2) \\ &\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\frac{1}{1 - \frac{2}{m^2}}(C_1' + C_2) \\ &= \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{m^2 - 2} \\ &\leq \frac{1}{2^n} h(P) + \frac{1}{2}(C_1' + C_2) \qquad \text{since } m \geq 2. \end{aligned}$$

There exists some n such that $2^n \geq h(P)$, so we can conclude that for this sufficiently large n, we have

$$h(P_n) \leq 1 + \frac{1}{2}(C_1' + C_2)$$

which is independent of P (i.e. only dependent on the choices of representatives Q_i). It follows that every element $P \in A$ can be written as a linear combination of the form

$$P = m^r Q + \sum_{j=1}^{r} m^{j-1} Q_{i_j}$$

where Q satisfies the same inequality as P_n above. Using (c), we then see that the set

$$\left\{Q \in A \mid h(Q) \leq 1 + \frac{1}{2}(C_1' + C_2)\right\}$$

is finite, and hence A is finitely generated since it is generated by the union of two finite sets. ■

This theorem then allows one to split a full proof of Mordell–Weil into two parts: showing that the quotient $E(K)/mE(K)$ is finite for some $m \geq 2$, which is the goal of this thesis, and constructing a suitable height function on E that satisfies the inequalities given above. Constructing the height function, in [Sil09], is done by first constructing height functions on $\mathbb{P}^n$, afterwhich one restricts to an elliptic curve embedded in this space.

4.2 Number Fields & Algebraic Number Theory

This subsection is dedicated to providing some of the basic language from algebraic number theory, and stating a result that we will need in the proof of weak Mordell–Weil, namely the Hermite–Minkowski theorem. Number fields (and their rings of integers) are one of the main objects of study in number theory. In this subsection (and the next), when we say "$\mathfrak{p}$ is a prime" we will mean that $\mathfrak{p}$ is a prime ideal.

Definition 4.2. A *number field* K is a finite extension of $\mathbb{Q}$. The *ring of integers* of K, denoted $\mathscr{O}_K$, is

$$\mathscr{O}_K := \{x \in K \mid \exists a_i \in \mathbb{Z} \text{ s.t. } x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 = 0\}.$$

Example 4.3. A trivial example of a number field is $\mathbb{Q}$ itself, which has $\mathscr{O}_{\mathbb{Q}} = \mathbb{Z}$. Another example is provided by $\mathbb{Q}(i)$, which has $\mathscr{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. In general, if $d \not\equiv 1 \pmod 4$ and d is square-free then $K = \mathbb{Q}(\sqrt{d})$ is a number field with $\mathscr{O}_K = \mathbb{Z}[\sqrt{d}]$. A similar statement can be made when $d \equiv 1 \pmod 4$: then $\mathscr{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

There are a number of properties about number fields that we are interested in. First of all, we want to know that we can work with number fields the way we need. For example, we will need to know that we can reduce a curve over a number field.

Theorem 4.4. *Let K be a number field. Then $\mathscr{O}_K$ is a Dedekind domain with fraction field K.*

Proof. See [Neu99, p. 17, Thm. 3.1] and [Neu99, p. 45, Prop. 8.1]. ■

The proof strategy for weak Mordell–Weil will involve some properties of the *ramification* of an extension of a number field. The definition of an unramified field extension is dependent on a theorem about factorization in Dedekind domains. In the case of the integers, we have unique factorization for elements: any integer $n \in \mathbb{Z}$ can be written as a unique product of a finite number of primes, up to multiplication by a unit (i.e. -1 or 1). This is not true for all $\mathscr{O}_K$. Instead, one can only guarantee that *ideals* decompose into a unique product of *prime ideals.*

Theorem 4.5. *Let R be a Dedekind domain, and let I be any ideal of R that is not* (0) *or* (1)*. Then we can decompose I into a finite product*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

which is unique up to the order of the factors, and the $\mathfrak{p}_i$ are non-zero prime ideals of R.

Proof. See [Neu99, p. 18, Thm. 3.3]. The proof is rather lengthy. ■

Definition 4.6. Let K be a number field, and let L/K be a finite extension. We say a prime $\mathfrak{P}$ of $\mathscr{O}_L$ *lies over* a prime $\mathfrak{p}$ in $\mathscr{O}_K$ if $\mathfrak{P} \cap \mathscr{O}_K = \mathfrak{p}$, and we write $\mathfrak{P}|\mathfrak{p}$.

Remark 4.7. If L/K is a finite extension of a number field, and $\mathfrak{p}$ is a prime in $\mathscr{O}_K$, we usually make the following simplifications in language: instead of saying $\mathfrak{p}$ is a prime of $\mathscr{O}_K$, we simply say it is a prime of K, and instead of writing $\mathfrak{p}\mathscr{O}_L$ for the ideal generated by $\mathfrak{p}$, we suppress the $\mathscr{O}_L$ and only write $\mathfrak{p}$.

Remark 4.8. Note that a prime of K may not remain prime in L. For example, 2 is prime in $\mathbb{Z}$, but in $\mathbb{Z}[i]$ we have $2 = (1+i)(1-i)$.

Definition 4.9. Let K be a number field, and let $\mathfrak{p} \in \mathscr{O}_K$ be a prime. We write $k(\mathfrak{p})$ for the field $\mathscr{O}_K/\mathfrak{p}$. Note that this agrees with the field $k(\mathfrak{p})$, with $\mathfrak{p}$ considered as a point in $\operatorname{Spec} \mathscr{O}_K$.

Definition 4.10. Let $\mathfrak{p}$ be a prime of K and let L/K be a finite extension. Suppose

$$\mathfrak{p} = \prod_i \mathfrak{P}_i^{e_i},$$

with all $\mathfrak{P}_i$ distinct prime ideals. The integer e_i is called the *ramification degree* of $\mathfrak{P}_i$ over $\mathfrak{p}$ in L. If $e_i = 1$ and the extension $k(\mathfrak{P})/k(\mathfrak{p})$ is separable, then we say $\mathfrak{P}_i$ is *unramified* over $\mathfrak{p}$, and we say L/K is unramified over $\mathfrak{p}$ if all $\mathfrak{P}_i|\mathfrak{p}$ are unramified (one also says that $\mathfrak{p}$ is unramified in this case).

Why do we care about the above? We care because being unramified is a strong condition, and therefore puts strong bounds on what extensions can satisfy it. In particular, we have the *Hermite–Minkowski* theorem, which is going to be an integral part of our proof of weak Mordell–Weil.

Theorem 4.11 (Hermite–Minkowski)**.** *Let K be a number field, let n be some positive integer, and let S be some finite set of primes of K. Then there exists only finitely many extensions of K with degree $\leq n$ which are unramified outside S.*

Proof. See [Neu99, p. 203, Thm. 2.13]. ■

Remark 4.12. It should be noted that there are several statements of Hermite–Minkowski, and they are largely equivalent (though the equivalence may sometimes, or often, be non-trivial). For example, another statement of the theorem replaces "are unramified outside S" with "have bounded discriminant." In [Neu99, p. 206, Thm. 2.16] this is how the theorem is stated when named, and the above formulation is left unnamed. (Furthermore, Neukirch actually refers to this as simply "Hermite's theorem.")

Remark 4.13. Funnily enough, it is also very difficult for a prime to be ramified. In particular, there is a theorem stating that if L/K above is separable, then there can only be finitely many primes that are ramified in L.

The question is now how one may check (un)ramification. The way we will be doing this is using the *inertia group.* In particular, suppose we have a finite Galois extension L/K with K a number field. If $\mathfrak{p}$ is prime in K and $\mathfrak{P}|\mathfrak{p}$, we write

$$G_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

afterwhich we see that an element $\sigma \in G_{\mathfrak{P}}$ induces an automorphism $\bar{\sigma}$ on $k(\mathfrak{P})$, given by $x \pmod{\mathfrak{P}} \mapsto \sigma(x) \pmod{\mathfrak{P}}$. Furthermore, have the following proposition:

Proposition 4.14. *Let L/K be as in the paragraph above. Then $k(\mathfrak{P})/k(\mathfrak{p})$ is a normal extension, and the above map $\sigma \mapsto \bar{\sigma}$ is a surjective homomorphism*

$$G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})).$$

Proof. See [Neu99, p. 56, Prop. 9.4]. ■

Definition 4.15. The kernel of the morphism $G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ is called the *inertia group* of $\mathfrak{P}$, and is denoted $I_{\mathfrak{P}}$. The fixed field of $I_{\mathfrak{P}}$ in L is called the *inertia field* of $\mathfrak{P}$ over K, and is denoted $T_{\mathfrak{P}}$.

We now have the following useful characterization of $I_{\mathfrak{P}}$ and $T_{\mathfrak{P}}$:

Proposition 4.16. *Let $Z_{\mathfrak{P}}$ be the fixed field of $G_{\mathfrak{P}}$ in L, and let $\mathfrak{P}$ be a prime lying over $\mathfrak{p}$ with ramification index e. Then $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ is a normal extension, and*

$$\mathrm{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}}) \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})), \quad \mathrm{Gal}(L/T_{\mathfrak{P}}) \ = I_{\mathfrak{P}}.$$

If, furthermore, the extension $k(\mathfrak{P})/k(\mathfrak{p})$ is separable, then

$$|I_{\mathfrak{P}}| = [L : T_{\mathfrak{P}}] = e, \quad |G_{\mathfrak{P}}/I_{\mathfrak{P}}| = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = [k(\mathfrak{P}) : k(\mathfrak{p})].$$

In this case, one has $G_{\mathfrak{P}} \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, so that the latter can be considered a subset of $\mathrm{Gal}(L/K)$, and

$$\mathfrak{p} \textit{ is unramified} \iff I_{\mathfrak{P}} = 1 \iff T_{\mathfrak{P}} = L.$$

Proof. See [Neu99, p. 57, Prop. 9.6]. ■

4.3 The Weak Mordell–Weil Theorem

Recall from Section 4.1 that one can prove Mordell–Weil by producing a certain kind of function on $E(K)$ and by showing that $E(K)/mE(K)$ is finite for $m \geq 2$. The weak Mordell–Weil theorem concerns the latter statement. The proof of weak Mordell–Weil will be based on relating the finiteness of $E(K)/mE(K)$ to the finiteness of $\mathrm{Gal}(L/K)$ for a particular field extension L/K, which will follow from Hermite–Minkowski.

Theorem (Weak Mordell–Weil)**.** *Let K be a number field, and let E/K be an elliptic curve. Then for every integer $m \geq 2$, $E(K)/mE(K)$ is finite.*

We first have a lemma that allows the first of a number of reductions:

Lemma 4.17. *Let K be a number field, let $m \geq 2$, and let L/K be a finite Galois extension. Then $E(L)/mE(L)$ finite $\implies$ $E(K)/mE(K)$ finite.*

Proof. We have a canonical inclusion $E(K) \hookrightarrow E(L)$ from Proposition 2.130, which induces a map $\alpha\colon E(K)/mE(K) \to E(L)/mE(L)$. Let $\Phi = \ker\alpha$. Then

$$\Phi = \frac{E(K) \cap mE(L)}{mE(K)}.$$

Now, for any $[P] \in \Phi$, we may choose some (not necessarily unique) $Q_P \in E(L)$ with $mQ_p = P$. This defines a *set*-map $\lambda_P\colon \mathrm{Gal}(L/K) \to E[m](L)$, given by $\lambda_P(\sigma) = \sigma(Q_P) - Q_P$. This is since we have

$$m\lambda_P(\sigma) = m\sigma(Q_P) - mQ_P = \sigma(P) - P = P - P = 0,$$

since $E(K)$ is fixed by the action of $\mathrm{Gal}(L/K)$. Now let $P, P' \in E(K) \cap mE(L)$, and suppose $\lambda_P = \lambda_{P'}$. Then, by definition, we have

$$\sigma(Q_P) - Q_P = \sigma(Q_{P'}) - Q_{P'} \implies \sigma(Q_P - Q_{P'}) = Q_P - Q_{P'}$$

for any $\sigma \in \mathrm{Gal}(L/K)$. Hence, $Q_P - Q_{P'} \in E(K)$, since this is also the only subset of $E(L)$ that is fixed by $\mathrm{Gal}(L/K)$. Therefore,

$$P - P' = mQ_P - mQ_{P'} = m(Q_P - Q_{P'}) \in mE(K) \implies P - P' \in mE(K)$$

so that $[P] = [P']$ in $E(K)/mE(K)$. This gives us that the map $\Phi \to \mathrm{Hom}_{\mathbf{Set}}(\mathrm{Gal}(L/K), E[m](L))$, $P \mapsto \lambda_P$ is injective. Now, from Corollary 3.72, $E[m](L)$ is finite, and by assumption we have that $\mathrm{Gal}(L/K)$ is finite, hence Φ injects into a finite set, so it is finite itself. Finally, we conclude that $E(K)/mE(K)$ is finite since taking quotient by Φ yields $E(L)/mE(L)$, which is finite by assumption. ■

For the remainder, let K be a number field, and let E be an elliptic curve over K. The above lemma lets us reduce to the case where $E[m](\overline{K}) = E[m](K)$, i.e. the m-torsion points of E are all K-rational. This is because if it were not the case, we simply extend K to some Galois finite K' that ensures $E_{K'}[m](\overline{K}) = E_{K'}[m](K')$ (which is possible due to the finiteness of $E[m](\overline{K})$), and then prove the weak Mordell–Weil theorem for $E_{K'}$ instead. Using the above, this then implies that E also satisfies the weak Mordell–Weil theorem. Hence, we now assume that $E[m](\overline{K}) = E[m](K)$.

We now want to relate the finiteness of $E(K)/mE(K)$ to the finiteness of a particular extension of K. To do this, we will make use of the *Kummer pairing.* Roughly speaking, one applies the above construction with $L = \overline{K}$.

Definition 4.18. Let $P = [p_0 : \dots : p_n] \in \mathbb{P}^n_K(\overline{K})$. The *field of definition* of P is

$$K(P) := K(p_0/p_i, \dots, p_n/p_i),$$

where we choose any $0 \leq i \leq n$ such that $p_i \neq 0$. This is independent of the choice of i.

Definition 4.19. The Kummer pairing $\kappa \colon E(K) \times G_K \to E[m](K)$ is defined as follows: let $P \in E(K)$ and pick some $Q_P \in E(\overline{K})$ with $mQ_P = P$. Then define $\kappa(P, \sigma) = \sigma(Q_P) - Q_P$.

Proposition 4.20. *The Kummer pairing is well-defined, and bilinear. Furthermore,*

$$\bigcap_{\sigma \in G_K} \ker \kappa(-, \sigma) = mE(K), \qquad \bigcap_{P \in E(K)} \ker \kappa(P, -) = G_{\overline{K}/L},$$

where $L = K([m]^{-1}E(K))$ is the compositum of the fields of definition $K(Q)$ as Q ranges over the points in $E(\overline{K})$ with $mQ \in E(K)$, and so the Kummer pairing induces a perfect bilinear pairing

$$E(K)/mE(K) \times G_{L/K} \to E[m](K).$$

Proof. First of all, κ is indeed a map of the form described, as shown in the proof of the previous lemma. Now we just need to show that the choice of the point Q_P does not change the value of κ. Note that if we have some Q'_P also satisfying $mQ'_P = P$, then we can find some $T \in E[m](K)$ ($= E[m](\overline{K})$) such that $Q'_P = Q_P + T$, since $m(Q_P - Q'_P) = P - P = 0$. We then calculate:

$$\sigma(Q_P + T) - Q_P - T = \sigma(Q_P) + \sigma(T) - Q_P - T = \sigma(Q_P) - Q_P + T - T = \sigma(Q_P) - Q_P,$$

where $\sigma(T) = T$ since $T \in E[m](K)$, and so is fixed by the action of G_K. Hence, κ does not depend on the choice of Q_P, and so we get a well-defined map.

To show bilinearity, note that linearity in the first variable is obvious. To show linearity in the second variable, we will add zero. Let $\sigma, \tau \in G_K$. Then

$$\kappa(P, \sigma \circ \tau) = \sigma(\tau(Q_P)) - Q_P = \sigma(\tau(Q_P) - Q_P) + \sigma(Q_P) - Q_P = \sigma(\kappa(P, \tau)) + \kappa(P, \sigma).$$

Since $E[m](K)$ is fixed by G_K, we get $\kappa(P, \sigma \circ \tau) = \kappa(P, \sigma) + \kappa(P, \tau)$.

We now want to show the "kernel" part of the proposition. Suppose $P \in mE(K)$, and write $P = mQ$ with $Q \in E(K)$. Then all $\sigma \in G_K$ fix Q, so $\kappa(P, \sigma) = \sigma(Q) - Q = 0$. Now suppose we have some $P \in E(K)$ such that $\kappa(P, \sigma) = 0$ for all $\sigma \in G_K$. Then we pick some $Q \in E(\overline{K})$ with $mQ = P$, and note that $\kappa(P, \sigma) = 0 \implies \sigma(Q) = Q$ for all $\sigma \in G_K$, i.e. all $\sigma \in G_K$ fix Q, so that $Q \in E(K)$. Hence $P = mQ \in mE(K)$.

Now, if $\sigma \in G_{\overline{K}/L}$, then $\kappa(P, \sigma) = \sigma(Q) - Q = 0$, since per definition $Q \in E(L)$. Conversely, if $\sigma \in G_K$ satisfies $\kappa(P, \sigma) = 0$ for all $P \in E(K)$, then for all $Q \in E(\overline{K})$ with $mQ \in E(K)$ we have $\sigma(Q) - Q = \kappa(mQ, \sigma) = 0$ so that σ fixes Q. But this shows that σ fixes $E(L)$, so that $\sigma \in G_{\overline{K}/L}$.

The above shows that $G_{\overline{K}/L}$ is normal in G_K (being the kernel of $G_K \to \mathrm{Hom}(E(K), E[m](K))$), with quotient $G_K/G_{\overline{K}/L} \cong G_{L/K}$, so that furthermore L/K is Galois. From this, we get that the map

$$E(K)/mE(K) \to \mathrm{Hom}(G_{L/K}, E[m](K))$$

is an isomorphism. ■

Corollary 4.21. *$E(K)/mE(K)$ is finite if and only if the Galois extension L/K from the above proof is finite.*

Due to the importance of the extension L from the proof above, we will fix it as notation for the remainder of this section. We now just need to show that this extension is finite to have proven the weak Mordell–Weil theorem. For this, we will make use of the Hermite–Minkowski theorem. First, we need to show that L is sufficiently unramified.

Proposition 4.22. *Let $m \geq 2$, and let*

$$S = \{\mathfrak{p} \in \operatorname{Spec} \mathscr{O}_K \mid E \textit{ has bad reduction at } \mathfrak{p} \textit{ or } \operatorname{char} k(\mathfrak{p}) \textit{ divides } m\} \cup \{\textit{primes lying over } 2 \textit{ and } 3\}.$$

Then L/K is unramified outside S, i.e. if $\mathfrak{p}$ is a prime in K not in S then $\mathfrak{p}$ is unramified.

Proof. Let $\mathfrak{p} \in \operatorname{Spec} \mathscr{O}_K \backslash S$, and let $Q \in E(\overline{K})$ be such that $mQ \in E(K)$. We may reduce to checking that $K(Q)$ is unramified over $\mathfrak{p}$, since L is the compositum of all these fields, and being unramified is preserved by this. Let $\mathfrak{P}$ be a prime in $K(Q)$ lying over $\mathfrak{p}$. E has good reduction at $\mathfrak{p}$, and so also has good reduction at $\mathfrak{P}$, since the fiber product preserves smoothness. Let $\sigma \in I_{\mathfrak{P}}$ be an element in the inertia group. Per definition, σ acts trivially after reduction, so

$$r_{\mathfrak{P}}(\sigma(Q) - Q) = \bar{\sigma}(r_{\mathfrak{P}}(Q)) - r_{\mathfrak{P}}(Q) = O.$$

We now use $mQ \in E(K)$ to see that

$$m(\sigma(Q) - Q) = m\sigma(Q) - mQ = \sigma(mQ) - mQ = O,$$

since σ fixes K. We therefore see that $\sigma(Q) - Q \in E^1(K)[m]$, so that $\sigma(Q) - Q = O$ by Theorem 3.94. Hence $\sigma(Q) = Q$ so that σ fixes Q, and so fixes any point in $E(K(Q))$. We now note that one can identify fixed fields by identifying fixed points, and we see that $I_{\mathfrak{P}}$ fixes all points in $E(K(Q))$, i.e. $T_{\mathfrak{P}} = K(Q)$, so that $K(Q)$ is unramified at $\mathfrak{p}$ by Proposition 4.16. ■

Theorem 4.23 (Weak Mordell–Weil)**.** *Let $m \geq 2$. Then $E(K)/mE(K)$ is finite.*

Proof. We have seen that $E(K)/mE(K)$ is finite if and only if L/K is a finite extension. Furthermore, this field L is the compositum of a number of fields $K(Q)$, where $mQ \in E(K)$. Our aim is to apply Hermite–Minkowski to show that there are only finitely many distinct such fields. This will follow from bounding the degree of the $K(Q)$'s.

For each $P \in E(K)$, there are only m^2 points $Q \in E(\overline{K})$ such that $mQ = P$, and these are all Galois conjugate. This follows from considering the difference: if Q' is another such point, then $m(Q - Q') = mQ - Q' = P - P = 0$, so $Q - Q' \in E[m](K)$, and this set has cardinality m^2 by Theorem 3.71 and Theorem 3.75. This also shows that $Q' = Q + T$ for some $T \in E[m](K)$. Furthermore, if $\sigma \in \operatorname{Gal}(L/K)$, then similar reasoning shows that $\sigma(Q) - Q \in E[m](K)$, so that $\sigma(Q)$ is one of the other points Q' with $mQ' = P$. Now, the degree of the the extension $K(Q)/K$ is the number of embeddings $K(Q) \to K(Q)^{\text{nor}}$ into the normal closure of $K(Q)$, since this is also the smallest Galois field containing $K(Q)$. Such an embedding has to send Galois conjugates to Galois conjugates and must be injective, hence there are at most m^2 embeddings. Hence, the degree of $K(Q)$ is at most m^2 for each Q.

We now apply Hermite–Minkowski (which we can, since the $K(Q)$'s are all unramified outside a finite set of primes) to conclude that L is the compositum of a finite number of finite degree fields $K(Q)$, and hence L/K is a finite degree extension. ■

Symbol	Meaning
$\mathbb{A}^n_R$	Affine n-space over the ring R, i.e. $\operatorname{Spec} R[t_1, \dots, t_n]$.
$\mathbb{A}^n_S$	Affine n-space over the scheme S, i.e. $A^n_{\mathbb{Z}} \times_{\mathbb{Z}} S$.
$\operatorname{Aut}(X)$	The automorphism group of the object X, i.e. the collection of isomorphisms $X \xrightarrow{\sim} X$.
$B_{(f)}$	The elements of B_f that are of degree zero, with B a graded ring and $f \in B$ homogeneous.
$\mathcal{C}/A$	The slice category over A, i.e. the category of morphisms to A.
$\mathcal{C}^{\mathrm{op}}$	The opposite category of $\mathcal{C}$.
$\coprod$	Coproduct/disjoint union.
$\Delta_{X/Y}$	The diagonal morphism $X \to X \times_Y X$ associated to a morphism $X \to Y$.
$\mathcal{F}_x$	The stalk of the (pre)sheaf $\mathcal{F}$ at x.
$\mathcal{F}^\dagger$	The sheafification (a.k.a. *sheaf associated to*) the presheaf $\mathcal{F}$.
$\mathcal{F}^\vee$	The dual of the $\mathcal{O}_X$-module $\mathcal{F}$, i.e. $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{O}_X)$.
$f_*\mathcal{F}$, $f^{-1}\mathcal{F}$	The direct image and inverse image sheaves associated to the function f and sheaf $\mathcal{F}$.
$\mathbb{F}_q$	The finite field of order $q = p^n$.
$\operatorname{Frac}(R)$	The (total) field of fractions of the commutative ring R.
$G[m]$	The m-torsion part of a group(-scheme) G.
G_K	The absolute galois group of K, i.e. $\operatorname{Gal}(\overline{K}/K)$.
$\operatorname{Gal}(L/K)$, $G_{L/K}$	The Galois group of the extension L/K.
$\Gamma(X, \mathcal{F})$	The global sections of $\mathcal{F}$ over X, i.e. $\mathcal{F}(X)$.
$\mathrm{H}^n(X, \mathcal{F})$	The nth (sheaf) cohomology group of X with coefficients in $\mathcal{F}$.
$\operatorname{Hom}_{\mathcal{C}}(A, B)$	The collection of morphisms $A \to B$ in the category $\mathcal{C}$.
$\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$	“Sheaf-Hom,” given by $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})(U) := \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{F}\vert_U, \mathcal{G}\vert_U)$.
$\operatorname{im} f$	The image of the morphism f.
$\sqrt{I}$	The radical of the ideal $I \subseteq R$, i.e. $\{f \in R \mid \exists n > 0 \text{ s.t. } f^n \in I\}$.
$X \xrightarrow{\sim} Y$	An isomorphism $X \to Y$.
$X \hookrightarrow Y$	An injection/monomorphism $X \to Y$.
$X \twoheadrightarrow Y$	A surjection/epimorphism $X \to Y$.
$k(x)$	The residue field at $x \in X$ where X is a locally ringed space, i.e. $k(x) := \mathcal{O}_{X,x}/\mathfrak{m}_x$.
$\overline{K}$	The algebraic closure of the field K.
K^{nor}	A normal closure of the field K.
$K(X)$	The function field of the irreducible scheme X.
$\varprojlim$, $\varinjlim$	The categorical limit and colimit.
$\mathfrak{m}_x$	The unique maximal ideal of the stalk $\mathcal{O}_{X,x}$ at $x \in X$, where X is a locally ringed space.
$\operatorname{Open}(X)$	The category of open sets of X.
$\mathcal{O}_X$	The structure sheaf of the ringed space X.
$\mathcal{O}_X(D)$	The $\mathcal{O}_X$-module associated to the divisor D.
$p_a(X)$	The arithmetic genus of the curve X.
$p_g(x)$	The geometric genus of the curve X.
$\operatorname{Proj} B$	The projective scheme associated to the graded ring B.
$\mathbb{P}(V)$	The projective space given by the vector space V.
$\mathbb{P}^n_R$	Projective n-space over the ring R, i.e. $\operatorname{Proj} R[t_0, t_1, \dots, t_n]$.
$\mathbb{P}^n_S$	Projective n-space over the scheme S, i.e. $\mathbb{P}^n_{\mathbb{Z}} \times_{\mathbb{Z}} S$.

Symbol	Meaning
R_f	The localization of R with respect to an element $f \in R$, i.e. $R_f := \{1, f, f^2, \dots\}^{-1}R$.
$R_\mathfrak{p}$	The localization of R with respect to the prime ideal $\mathfrak{p}$, i.e. $R_\mathfrak{p} := (R \backslash \mathfrak{p})^{-1}R$.
$\operatorname{Spec} R$	The (prime) spectrum of the commutative ring R.
$\operatorname{Spec} \phi$	The morphism $\operatorname{Spec} R' \to \operatorname{Spec} R$ associated to the morphism $\phi \colon R \to R'$ of commutative rings.
$[s]_x$	The germ of s at x, i.e. image of the section $s \in \mathcal{O}_X(U)$ in the stalk $\mathcal{O}_{X,x}$, where $x \in U \subseteq X$.
s.t.	"such that."
X^G	The fixed points of the action $G \to \operatorname{Aut}(X)$.
$\chi_k(\mathcal{F})$	The Euler–Poincaré characteristic of $\mathcal{F}$.

References

[Cla12] Pete L. Clark. *Supplementary Lecture Notes on Elliptic Curves*. 2012. URL: `http://alpha.math.uga.edu/~pete/8430Elliptic_Curves.pdf`.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1977. ISBN: 978-0-387-90244-9.

[Liu10] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics. Oxford University Press, 2010. ISBN: 978-0-19-920249-2.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer, 1999. ISBN: 978-3-540-65399-8.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd edition. Graduate Texts in Mathematics. Springer, 2009. ISBN: 978-0-387-09493-9.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. 2nd printing. Graduate Texts in Mathematics. Springer, 1994. ISBN: 978-0-387-94328-2.

[Stacks] The Stacks Project authors. *The Stacks Project*. 2021. URL: `https://stacks.math.columbia.edu`.

[Vak17] Ravi Vakil. *Foundations of Algebraic Geometry*. 2017. URL: `http://math.stanford.edu/~vakil/216blog/FOAGnov1817public`.

[Wei95] Charles A. Weibel. *An Introduction to Homological Algebra*. Cambridge studies in advanced mathematics. Cambridge University Press, 1995. ISBN: 978-0-521-55987-4.