ELLIPTIC CURVES AND THEIR MODULI SPACES

ANDREAS MIHATSCH

Abstract. These are lecture notes for a course I taught at Bonn University during Summer 2024. Any comments and corrections are welcome!

Contents

1. Introduction

1.1. **Elliptic curves.** Let k be a field. Elliptic curves over k can be defined in three equivalent ways:

- As marked smooth cubic curves in $\mathbb{P}^2_k$.
- As marked proper smooth connected k-curves of genus 1.
- As 1-dimensional proper smooth connected group schemes over k.

We will get to know all these definitions during the course and will show their mutual equivalence. In this first lecture, we stick to the first one because it is the most concrete.

Definition 1.1. An elliptic curve over a field k is a pair (E, O) that consists of a smooth curve $E/\operatorname{Spec} k$ together with a rational point $O \in E(k)$. We moreover require that E can

Date: September 17, 2024.
E-mail: *mihatsch@math.uni-bonn.de*

be embedded as a cubic curve into $\mathbb{P}^2_k$. That is, we assume that there exist a homogeneous polynomial $F \in k[X,Y,Z]$ of degree 3 and an isomorphism

$$E \xrightarrow{\sim} V_+(F) \subset \mathbb{P}^2_k. \tag{1.1}$$

Remark 1.2. Condition (1.1) also ensures that E is proper and connected. The smoothness of E then further implies that E is irreducible.

We still need to define what it means for $E/\operatorname{Spec} k$ to be smooth. There are several different definitions which are all powerful, and we will learn about them soon in this course. Today, we go with the so-called Jacobi criterion which is especially useful for studying concrete equations such as (1.1).

We use the notion of local dimension: If X is a scheme and $x \in X$, then the local dimension of X in x is defined by

$$\dim_x(X) := \lim_{x \in U \subset X \text{ open affine}} \dim(U) \quad \in [0, \infty].$$

Definition 1.3. (1) The partial derivatives $\partial f / \partial T_j$ of a polynomial $f \in k[T_1, \dots, T_n]$ are defined by the rules from analysis. Note that this is a purely algebraic definition which makes sense over any field. The Jacobi matrix of a tuple $f_1, \dots, f_m \in k[T_1, \dots, T_n]$ is the matrix of all partial derivatives

$$\left(\frac{\partial f_i}{\partial T_j} \right)_{i,j} \in M_{m \times n}\left(k[T_1, \dots, T_n]\right). \tag{1.2}$$

(2) Consider $U = V(f_1, \dots, f_m) \subseteq \mathbb{A}^n_k$ and a point $x \in U$. Let $d = \dim_x U$ denote the local dimension of U in x. We say that the Jacobi criterion holds in x if there exist subsets $I \subseteq \{1, \dots, m\}$, $J \subseteq \{1, \dots, n\}$ with $|I| = |J| = n - d$ and such that the (I,J)-minor $(\partial f_i \,/\, \partial T_j)_{i \in I, j \in J}$ is invertible in x. The latter is the case if and only if the polynomial

$$\det\left((\partial f_i \,/\, \partial T_j)_{i \in I, j \in J} \right) \in k[T_1, \dots, T_n]$$

does not vanish in x.

(3) Let X be a k-scheme of locally finite type. Then X is said to be smooth in $x \in X$ if there exist integers $n, m \geq 0$, polynomials $f_1, \dots, f_m$ as before, an affine open neighborhood $x \in U$, and an isomorphism $U \xrightarrow{\sim} V(f_1, \dots, f_m) \subseteq \mathbb{A}^n_k$ such that the Jacobi criterion holds in x. We call X smooth if it is smooth in every point.

Explanation 1.4. In Definition 1.3 (2) and (3), we do not assume that x is a closed. Let $\mathfrak{p} \subset A = k[T_1, \dots, T_n]$ be the prime ideal defined by x and let $\kappa = \operatorname{Quot}(A/\mathfrak{p})$ be its residue field. A polynomial $p \in A$ not vanishing in x then means $p \notin \mathfrak{p}$, or equivalently $p(x) \neq 0$ where $p(x)$ is the image of p in κ. Similarly, a square matrix $P \in M_n(A)$ is said to be invertible in x if its image in $M_n(\kappa)$ lies in $GL_n(\kappa)$. Equivalently, $\det(A)(x) \neq 0$.

Remark 1.5. The Jacobi criterion is well-known from the implicit function theorem in analysis. (Recall that this theorem states that the vanishing set $V(f_1, \dots, f_m) \subseteq \mathbb{R}^n$ of a tuple of smooth functions with $\det(\partial f_i / \partial T_j)(x) \neq 0$ is isomorphic to $\mathbb{R}^{n-m}$ near x.) Definition 1.3 is an algebraic incarnation of the same idea.

Remark 1.6. Let X be a k-scheme of locally finite type that is smooth in a point $x \in X$. Then, in fact, for *every* choice of affine open neighborhood $x \in U$, integers $n, m \geq 0$, polynomials $f_1, \dots, f_m \in k[T_1, \dots, T_n]$, and isomorphism $U \xrightarrow{\sim} V(f_1, \dots, f_m)$, the Jacobi criterion holds in x. That is, being smooth in x is an intrinsic property.

Our next aim is to construct elliptic curves. Let $h(x) = x^3 + ax + b$ be a monic cubic polynomial (without x^2-term). A polynomial of the form

$$f = y^2 - h(x) \tag{1.3}$$

is called a *simplified Weierstrass equation*. Let

$$F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3 \tag{1.4}$$

be the homogenization of f, and let $E = V_+(F) \subset \mathbb{P}^2_k$ be its vanishing locus.

Lemma 1.7. *Assume that* $\mathrm{char}(k) \neq 2$ *and that* h *is separable. Then* E *is a smooth curve.*

Proof. First observe by direct substitution in (1.4) that $E \cap V_+(Z) = \{[0:1:0]\}$. Thus we can proceed by checking the Jacobi criterion on $E \cap D_+(Z)$ and for the point $[0:1:0]$.

By definition, we have

$$E \cap D_+(Z) \xrightarrow{\sim} V(y^2 - h(x)) \subset \mathbb{A}^2_k.$$

The Jacobi matrix of the Weierstrass polynomial is the gradient

$$(\partial f/\partial x,\ \partial f/\partial y) = (-h'(x),\ 2y). \tag{1.5}$$

Let $e \in E \cap D_+(Z)$ be an arbitrary point and let $(e_1, e_2) \in \kappa(e) \times \kappa(e)$ be the image of (x,y).[1] If $e_2 \neq 0$, then also $2e_2 \neq 0$ by our assumption $\mathrm{char}(k) \neq 2$, meaning $2y$ does not vanish in e. If $e_2 = 0$, however, then $h(e_1) = 0$ since $f(e_1, e_2) = 0$. We have assumed that h is separable, which is equivalent to $h(x)$ and $h'(x)$ being coprime. Thus $h'(e_1) \neq 0$. In summary, we have seen that the gradient (1.5) does not vanish in e.

We now consider the point $[0:1:0]$. An affine chart is given by

$$E \cap D_+(Y) \xrightarrow{\sim} V(z - x^3 - axz^2 - bz^3) \subset \mathbb{A}^2_k.$$

In these coordinates, $[0:1:0]$ maps to $(0,0)$. Moreover, the gradient of that equation is

$$(-3x^2 - az^2,\ 1 - 2axz - bz^2). \tag{1.6}$$

Its second entry does not vanish in $(0,0)$, so the Jacobi criterion holds in $(0,0)$. The proof of the lemma is now complete. □

Definition 1.8. Assume that $\mathrm{char}(k) \neq 2$ and that $h(x) = x^3 + ax + b$ is separable. Let F be as in (1.4). The elliptic curve defined by the Weierstrass equation $y^2 - h(x)$ is the pair

$$(E, O) := \big(V_+(F),\ [0:1:0]\big).$$

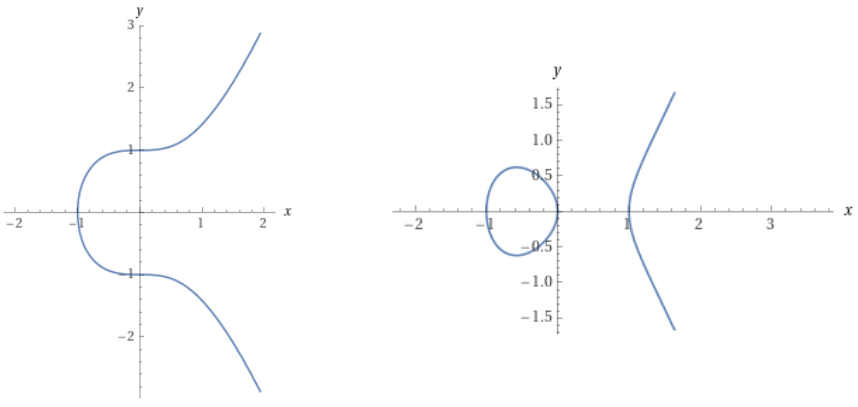


FIGURE 1. The $\mathbb{R}$-points of the two Weierstrass equations $y^2 = x^3 + 1$ and $y^2 = x^3 - x$. Note that $V(y^2 - (x^3 - x)) \subset \mathbb{A}^2_{\mathbb{R}}$ is a connected scheme. Only its $\mathbb{R}$-points endowed with the real topology are disconnected.

[1] Given a scheme X and a point $x \in X$, we use $\kappa(x) = \mathrm{Quot}(\mathcal{O}_{X,x}/\mathfrak{m}_x)$ to denote the residue in x.

1.2. **Group structure.** The following will be one of our first major results.

Theorem 1.9. *Let (E, O) be an elliptic curve over k. Then E has a unique group scheme structure such that O becomes the identity element. This group structure is abelian.*

We will define group schemes later in the course. Here, we will discuss how to endow the set of rational points $E(k)$ with a group structure.

Lemma 1.10. *Let $F \in k[X, Y, Z]$ be homogeneous of degree 3 without linear factor and let $E = V_+(F)$. Let $L \subset \mathbb{P}^2_k$ be any line. Then E intersects L in three points when counted with multiplicities. More precisely, $E \cap L = \operatorname{Spec} A$ for a k-algebra A with $\dim_k(A) = 3$.*

Here, by line we mean a curve of the form $V_+(aX + bY + cZ)$, where $(a, b, c) \neq (0, 0, 0)$.

Proof. After a linear change of coordinates, we may assume that $L = V_+(Z)$. Since F has no linear factor, $Z \nmid F$. Thus $F|_L = F(X, Y, 0)$ is a non-zero homogeneous polynomial of degree 3 and hence has three zeroes (counted with multiplicities) as claimed. □

Construction 1.11. Let $E = V_+(F) \subset \mathbb{P}^2_k$ be a smooth cubic curve with a fixed point $O \in E(k)$. Given $P_1, P_2 \in E(k)$, define a line $L \subset \mathbb{P}^2_k$ as follows:

(1) If $P_1 \neq P_2$, then let L be the unique line that passes through P_1 and P_2.
(2) If $P_1 = P_2$, then let L be the tangent line to E in that point.

The definition of the tangent uses the smoothness of E. (In a local chart, take the line perpendicular to the gradient of the equation defining E.) The smoothness of E also implies that F has no linear factor. Hence Lemma 1.10 applies and shows that E and L intersect in three points (counting multiplicities). But two of these points are known to be P_1 and P_2 which lie in $L(k)$! And if a cubic polynomial has two rational roots, then the third root is rational as well. Thus there exists a unique third rational intersection point $P_3 \in (E \cap L)(k)$. Repeating this construction with O, P_3 instead of P_1, P_2, defines a fourth point $P_4 \in E(k)$.

Remark 1.12. A nice illustration of the above construction can be found here.

Definition 1.13. The sum of $P_1, P_2 \in E(k)$ is defined as $P_1 + P_2 := P_4$.

It is true, but not obvious, that this indeed defines a group structure on $E(k)$. The fun and easy part is to show that O is a neutral element and that every element has an inverse (exercise). It is moreover clear that the operation $(P_1, P_2) \mapsto P_1 + P_2$ is commutative, which is why we have written it additively.

A difficulty is to show associativity. Moreover, it is true, but again not obvious, that the construction of P_3 and P_4 only depends on (E, O) and not on the (auxiliary) choices of F and $E \xrightarrow{\sim} V_+(F)$. During the course, we will take a different approach to the group structure on E which will be in terms of line bundles. All the mentioned properties will then follow immediately.

1.3. **Small panoramic outlook.** Elliptic curves play a central role in many branches of algebraic geometry and number theory. In this last section of today's introduction, I want to mention some important aspects and results.

Example 1.14. First consider the case $k = \mathbb{C}$. A general theorem provides an equivalence of categories

$$\left\{\begin{array}{c}\text{Connected proper smooth}\\ \text{algebraic curves over } \mathbb{C}\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\text{Connected compact}\\ \text{Riemann surfaces}\end{array}\right\}. \tag{1.7}$$

Under this equivalence, elliptic curves are precisely the compact Riemann surfaces of the form $\mathbb{C}/\Lambda$ for a $\mathbb{Z}$-lattice $\Lambda \subset \mathbb{C}$. The group structure here is the additive group structure on $\mathbb{C}/\Lambda$.

Note that while one can always find an isomorphism of real Lie groups

$$\mathbb{C}/\Lambda \xrightarrow{\sim} \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}, \tag{1.8}$$

it is not true that the quotients $\mathbb{C}/\Lambda$ (for varying lattices Λ) are isomorphic as Riemann surfaces. In fact, their isomorphism classes form a 1-dimensional space which is called the modular curve. This space coincides with the $\mathbb{C}$-points of the moduli space we will construct later in the course.

Example 1.15. Now assume that $k = \mathbb{F}_q$ is a finite field, $p = \mathrm{char}(k)$. There are only finitely many elliptic curves over $\mathbb{F}_q$ (up to isomorphism) because there are only finitely many cubic homogeneous polynomials in three variables over $\mathbb{F}_q$.

Note that the n-torsion $(\mathbb{C}/\Lambda)[n]$ of a complex elliptic curve is isomorphic to $(\mathbb{Z}/n)^{\oplus 2}$ which is clear from (1.8). A fascinating result we will show during the course is that for an elliptic curve E over $\mathbb{F}_q$, the n-torsion $E[n]$ is also a group scheme of degree n^2. If $(n,p) = 1$, then it behaves just like $(\mathbb{Z}/n)^{\oplus 2}$. If $p \mid n$, however, then $E[n]$ will be a non-reduced group scheme. We will study its structure in the course and learn about the ordinary/supersingular distinction.

Another feature over $\mathbb{F}_q$ is the existence of the q-Frobenius endomorphism $\mathrm{Frob}_q \in \mathrm{End}(E)$. Its characteristic polynomial determines the number of points $E(\mathbb{F}_{q^r})$ for every r, and enables a classification of elliptic curves over $\mathbb{F}_q$ by the Honda–Tate theorem.

Example 1.16. Finally, assume that k is a number field, i.e. a finite extension of $\mathbb{Q}$. The central structure theorem goes back to Mordell (1922):

Theorem 1.17 (Mordell's Theorem)**.** *For every elliptic curve $(E,O)/k$, the group $E(k)$ is finitely generated.*

By the structure theorem for finitely generated abelian groups, we can thus write

$$E(k) \xrightarrow{\sim} E(k)_{\mathrm{tors}} \oplus \mathbb{Z}^r \tag{1.9}$$

for a unique integer $r \geq 0$ called the algebraic rank of E. This rank is a central object of study in number theory. For example, the Birch and Swinnerton-Dyer conjecture, one of the seven Clay Millennium problems, asserts that it equals the vanishing order of the L-function of E at its center of symmetry.

Fixing the number field k, there is an upper bound on the size $\#E(k)_{\mathrm{tors}}$ of the torsion group. For example, $\#E(\mathbb{Q})_{\mathrm{tors}} \leq 16$ for every elliptic curve $E/\mathbb{Q}$ (Mazur's torsion theorem). It is an open question, however, whether or not the rank r in (1.9) is similarly bounded in terms of k. We refer to the homepage of Dujella for a list of rank records.

Part 1. Elliptic curves as group schemes and algebraic curves

2. Group schemes

In this course, we will always work with the following definition.

Definition 2.1. Let k be a field. An elliptic curve over k is a proper, smooth, connected and 1-dimensional k-group scheme.

We will now first discuss group schemes in some detail because this notion will play an important role throughout the lecture. Our first result about elliptic curves (next section) will then be that they are always commutative. This does not require the one-dimensionality, so the argument will apply to abelian varieties as well:

Definition 2.2. An abelian variety over k is a proper, smooth and connected k-group scheme.

2.1. **Group schemes.**

Definition 2.3. Let S be a scheme. A group scheme over S is a pair (G, m) that consists of an S-scheme G and an S-scheme morphism (called multiplication morphism)

$$m : G \times_S G \longrightarrow G$$

such that for every S-scheme T, the resulting map on T-valued points

$$m(T) : G(T) \times G(T) \longrightarrow G(T)$$

makes $G(T)$ into a group. We call G commutative if $G(T)$ is a commutative group for every T.

Observe that for every morphism $u : T' \to T$ of S-schemes, the diagram

$$\begin{array}{ccc} G(T) \times G(T) & \xrightarrow{m(T)} & G(T) \\ {\scriptstyle u^* \times u^*}\downarrow & & \downarrow{\scriptstyle u^*} \\ G(T') \times G(T') & \xrightarrow{m(T')} & G(T') \end{array} \tag{2.1}$$

commutes which means that $u^* : G(T) \to G(T')$ is a group homomorphism. Before discussing further general properties, we give some examples.

Example 2.4 (The multiplicative group)**.** Assume that $S = \operatorname{Spec} R$ is affine. Define $\mathbb{G}_{m,S} = \operatorname{Spec} R[t, t^{-1}]$ which we would like to make into a group scheme over S. Recall that $\operatorname{Spec}(-)$ is an anti-equivalence from R-algebras to affine S-schemes. We define the multiplication map $m : \mathbb{G}_{m,S} \times_S \mathbb{G}_{m,S} \to \mathbb{G}_{m,S}$ as $\operatorname{Spec}(m^*)$ where m^* is

$$\begin{array}{rcl} m^* : R[t, t^{-1}] & \longrightarrow & R[t, t^{-1}] \otimes_R R[t, t^{-1}] \\ t & \longmapsto & t \otimes t. \end{array} \tag{2.2}$$

We next verify that this makes $\mathbb{G}_{m,S}$ into an S-group scheme. For every S-scheme T, we identify

$$\begin{array}{rcl} \mathbb{G}_{m,S}(T) & \xrightarrow{\sim} & \mathcal{O}_T(T)^\times \\ [g : T \to \mathbb{G}_{m,S}] & \longmapsto & g^*(t). \end{array} \tag{2.3}$$

Note that this map is obviously defined; the fact that it is an isomorphism is the adjunction $\operatorname{Mor}_S(T, \operatorname{Spec}(A)) \xrightarrow{\sim} \operatorname{Hom}_R(A, \mathcal{O}_T(T))$. Given two morphisms $g_1, g_2 : T \to \mathbb{G}_{m,S}$, we have

$$\begin{array}{ccccc} R[t, t^{-1}] & \xrightarrow{m^*} & R[t, t^{-1}] \otimes_R R[t, t^{-1}] & \xrightarrow{g_1^* \otimes g_2^*} & \mathcal{O}_T(T) \\ t & \longmapsto & t \otimes t & \longmapsto & g_1^*(t) g_2^*(t). \end{array}$$

Thus we see that the operation $m(T)$ on $\mathbb{G}_{m,S}(T)$ translates to the usual multiplication under (2.3). In particular, $m(T)$ is a group structure for every T, and hence $(\mathbb{G}_{m,S}, m)$ a group scheme. It represents the functior $T \mapsto (\mathcal{O}_T(T)^\times, *)$.

Example 2.5 (The additive group)**.** In an analogous way, we define a group structure $a = \operatorname{Spec}(a^*)$ on the affine line $\mathbb{G}_{a,S} = \operatorname{Spec} R[t]$ by

$$\begin{array}{rcl} a^* : R[t] & \longrightarrow & R[t] \otimes_R R[t] \\ & & t \longmapsto t \otimes 1 + 1 \otimes t. \end{array}$$

In this case, we obtain (exercise) an isomorphism of sets with binary operation

$$\begin{array}{rcl} (\mathbb{G}_{a,S}(T), a) & \xrightarrow{\sim} & (\mathcal{O}_T(T), +) \\ [g : T \to \mathbb{G}_{m,S}] & \longmapsto & g^*(t). \end{array} \tag{2.4}$$

In particular, $(\mathbb{G}_{a,S}, a)$ is a group scheme that represents $T \mapsto (\mathcal{O}_T(T), +)$.

Recall that the Yoneda Lemma states that taking functor of points defines a fully faithful embedding

$$\begin{aligned}(\mathrm{Sch}/S) &\longrightarrow \mathrm{Fun}\left((\mathrm{Sch}/S)^{\mathrm{op}},\ \mathrm{Sets}\right)\\ X &\longmapsto [T \mapsto \mathrm{Mor}(T, X)].\end{aligned}$$

We may thus reverse the logic of Definition 2.3: Giving a group scheme structure on an S-scheme G is equivalent to giving a group structure on $G(T)$ for every T such that for every S-scheme morphism $u : T' \to T$, the pullback $u^* : G(T) \to G(T')$ is a group homomorphism. Examples 2.4 and 2.5 show that this is often a very intuitive way of thinking about a group scheme.

Example 2.6 (The general linear group)**.** The (underlying scheme of the) general linear group in n variables over S is defined as

$$GL_{n,S} = \operatorname{Spec} R\left[t_{ij},\ 1 \le i, j \le n;\ \det((t_{ij})_{i,j})^{-1}\right].$$

There is a natural isomorphism (exercise) of the functor of points of $GL_{n,S}$ and the functor $T \mapsto GL_n(\mathcal{O}_T(T))$ which is given by

$$\Phi : [g : T \to GL_{n,S}] \longmapsto (g^*(t_{ij}))_{i,j}. \tag{2.5}$$

We endow $GL_n(\mathcal{O}_T(T))$ with the usual matrix multiplication. Clearly, for every $u : T' \to T$, the pullback map

$$u^* : GL_n(\mathcal{O}_T(T)) \longrightarrow GL_n(\mathcal{O}_{T'}(T'))$$

is a group homomorphism. Hence, as explained before, there exists a unique S-morphism $m : GL_{n,S} \times_S GL_{n,S} \to GL_{n,S}$ such that Φ becomes a group isomorphism for every $T \to S$. It is also easy to write m down in terms of coordinates:

$$m^*(t_{ij}) = \sum_{k=1}^{n} t_{ik} \otimes t_{kj}.$$

Note that if (G, m) is a group scheme over S and if $T \to S$ is a morphism, then

$$(G_T, m_T) := (T \times_S G, \mathrm{id}_T \times m) \tag{2.6}$$

is a group scheme over T, called its base change. At this point, we say a word about intuition: If G is a variety[2] over $\operatorname{Spec} k$, where k is an algebraically closed field, then a group scheme structure on G is the same as a group structure on $G(k)$ that comes from a morphism $G \times G \to G$. For a general scheme S, a group scheme over S is best thought of as a family of group schemes over the residue fields of S.

The above three examples make sense for every base S, not necessarily affine: Simply set

$$\mathbb{G}_{m,S} := S \times_{\operatorname{Spec}\mathbb{Z}} \mathbb{G}_{m,\mathbb{Z}}, \qquad \mathbb{G}_{a,S} := S \times_{\operatorname{Spec}\mathbb{Z}} \mathbb{G}_{a,\mathbb{Z}}$$

and analogously for $GL_{n,S}$. In fact, recall that affine S-schemes (in the sense that the structure morphism $X \to S$ is affine) are anti-equivalent to quasi-coherent $\mathcal{O}_S$-algebras by the relative Spec construction,

$$\begin{aligned}[u : X \to S] &\longmapsto u_*\mathcal{O}_X\\ \underline{\operatorname{Spec}}(\mathcal{A}) &\longmapsfrom \mathcal{A}.\end{aligned} \tag{2.7}$$

Thus we could have worked with a general base from the beginning. For example,

$$(\mathbb{G}_{m,S}, m) = \underline{\operatorname{Spec}}(\mathcal{O}_S[t, t^{-1}], m^*(t) = t \otimes t).$$

The following provides examples of group schemes that do not necessarily come by base change from $\mathbb{Z}$.

[2] That is, G is of finite type over k and integral.

Example 2.7. Let S be any scheme and let $\mathcal{E}$ be a vector bundle of rank n on S.[3] Then the functor

$$[u : T \to S] \longmapsto \mathrm{Aut}(u^*\mathcal{E})$$

is representable by an affine S-group scheme $G = \underline{\mathrm{Aut}}(\mathcal{E})$ (exercise). If $U \subseteq S$ is an open subscheme such that $\mathcal{E}|_U \cong \mathcal{O}_U^{\oplus n}$, then $G|_U := U \times_S G$ is isomorphic to $GL_{n,U}$.

2.2. **Further structure on group schemes.** We come back to Definition 2.3 and deduce some general properties. First, $G(S)$ is a group which means that there exists an identity element $e : S \to G$. Because of (2.1), for every $u : T \to S$, we find that $u^*(e) = e \circ u \in G(T)$ is the neutral element. The faithfulness part of the Yoneda lemma thus implies that the following triangle commutes,

$$\begin{array}{ccc} S \times_S G & \xrightarrow{e\times \mathrm{id}} & G \times_S G \\ & \searrow^{=} \quad \swarrow_{m} & \\ & G. & \end{array} \tag{2.8}$$

Moreover, for each $T \to S$, there is an inverse map $i(T) : G(T) \to G(T)$, $g \mapsto g^{-1}$. For each $u : T \to T'$, (2.1) implies that $u^* \circ i(T) = i(T') \circ u^*$, so the fullness part of the Yoneda lemma implies that $\{i(T)\}_T$ is induced from a morphism $i : G \to G$. Applying the Yoneda lemma once more shows that

$$\begin{array}{ccc} G \times_S G & \xrightarrow{\mathrm{id}\times i} & G \times_S G \\ \downarrow & & \downarrow{\scriptstyle m} \\ S & \xrightarrow{e} & G \end{array} \tag{2.9}$$

commutes. Finally, again by the Yoneda lemma, associativity (and possibly commutativity) for all the groups $G(T)$ imply the commutativity of the squares

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{m\times \mathrm{id}} & G \times_S G \\ \downarrow{\scriptstyle \mathrm{id}\times m} & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccc} G \times_S G & \xrightarrow{(g,h) \,\mapsto\, (h,g)} & G \times_S G \\ & \searrow_{m} \quad \swarrow^{m} & \\ & G. & \end{array} \tag{2.10}$$

In fact, one may also reverse the logic of this section and obtains the more classical definition of a group scheme over S: It is the same as an S-scheme G together with a morphism $m : G \times_S G \to G$ such that there exist morphisms $e : S \to G$ and $i : G \to G$ such that the diagrams in (2.8), (2.9) and (2.10) commute.

Example 2.8. Neutral element and inverse of $\mathbb{G}_{m,S} = \underline{\mathrm{Spec}}\mathcal{O}_S[t, t^{-1}]$ are given by $e^*(t) = 1$ and $i^*(t) = t^{-1}$. What are these morphisms for $\mathbb{G}_{a,S}$ and $GL_{n,S}$?

2.3. **Group scheme homomorphisms.**

Definition 2.9. Let (G_1, m_1) and (G_2, m_2) be group schemes over S. A group scheme morphism from G_1 to G_2 is a morphism of S-schemes $f : G_1 \to G_2$ such that $m_2 \circ (f \times f) = f \circ m_1$. Equivalently, for all $T \to S$, the induced map

$$f(T) : G_1(T) \longrightarrow G_2(T)$$

is a group homomorphism.

[3] That is, $\mathcal{E}$ is a quasi-coherent $\mathcal{O}_S$-module that is locally free of rank n.

Example 2.10. Let S be any scheme. There is a group scheme morphism realization of the determinant $\det : GL_{n,S} \to \mathbb{G}_{m,S}$ which may be defined in either of the following equivalent ways. First, we may define it using (2.7) by $\det = \underline{\mathrm{Spec}}(\det^*)$ where

$$\begin{aligned} \det{}^* : \mathcal{O}_S[t,t^{-1}] &\longrightarrow \mathcal{O}_S[t_{ij}, 1 \le i,j \le n;\ \det((t_{ij})_{ij})^{-1}] \\ t &\longmapsto \det((t_{ij})_{ij}). \end{aligned}$$

Second, we may apply the Yoneda lemma and define det as the unique morphism such that for every $T \to S$,

$$\det(T) : GL_n(\mathcal{O}_T(T)) \longrightarrow \mathcal{O}_T(T)^\times$$

is the usual determinant. Here, we have used the identifications from (2.3) and (2.5).

Example 2.11. Assume that $(G,+)$ is a commutative group scheme over S. Then the set of group scheme endomorphisms $\mathrm{End}(G,+)$ is a (not necessarily commutative) ring: Multiplication is defined as composition of group scheme endomorphisms, addition by the rule $(\phi+\psi)(g) = \phi(g)+\psi(g)$ for all $T \to S$ and $g \in G(T)$. In particular, for every $n \in \mathbb{Z}$, there is a multiplication-by-n homomorphism

$$[n] : G \longrightarrow G$$

obtained by adding id_G (or the inverse morphism i, if n is negative) $|n|$ times. For every $T \to S$ and $g \in G(T)$, we have $[n](g) = ng$.

Proposition 2.12. *Let S be a connected scheme. Then* $\mathrm{End}(\mathbb{G}_{m,S}) = \mathbb{Z}$.

Proof. Step 1: The case of fields. Let k be any field. By definition, a group scheme endomorphism f of $\mathbb{G}_{m,k}$ is the same as $f = \mathrm{Spec}(f^*)$ for a unique k-algebra morphism $f^* : k[t,t^{-1}] \longrightarrow k[t,t^{-1}]$ such that

$$(f^* \otimes f^*) \circ m^* = m^* \circ f^* \tag{2.11}$$

where $m^*(t) = t \otimes t$ is as in (2.2). Giving a k-algebra morphism f^* is equivalent to specifying its image $f^*(t) \in k[t,t^{-1}]^\times$. These units are

$$k[t,t^{-1}]^\times = \{\lambda t^n \mid \lambda \in k^\times, n \in \mathbb{Z}\}.$$

If $f^*(t) = \lambda t^n$, then (2.11) evaluated at t becomes

$$\lambda t^n \otimes \lambda t^n \stackrel{?}{=} \lambda (t \otimes t)^n \tag{2.12}$$

which holds if and only if $\lambda^2 = \lambda$, meaning $\lambda = 1$. Note that $f^*(t) = t^n$ precisely defines the multiplication-by-n morphism $[n]$ (meaning taking n-th power in this context) and thus $\mathrm{End}(\mathbb{G}_{m,k}) = \mathbb{Z}$ is proved.
Step 2: The case of reduced S. Assume that S is reduced and let $f : \mathbb{G}_{m,S} \to \mathbb{G}_{m,S}$ be any morphism. Step 1 provides a function $S \to \mathbb{Z}$ which takes s to the unique integer $n(s)$ such that the fiber

$$f(s) : \kappa(s) \otimes_S \mathbb{G}_{m,S} \longrightarrow \kappa(s) \otimes_S \mathbb{G}_{m,S}$$

equals $[n(s)]$. We claim that for every $n \in \mathbb{Z}$, the set

$$\{s \in S \mid n(s) = n\} \tag{2.13}$$

is open and closed. This is a topological property that we can check locally. So assume $S = \mathrm{Spec}\, R$ is affine. Then $f = \mathrm{Spec}(f^*)$ for a (unique) R-algebra endomorphism f^* of $R[t,t^{-1}]$. Any such endomorphism is uniquely determined by the image $f^*(t) \in R[t,t^{-1}]^\times$. By step 1, the n-th coefficient c_n of $f^*(t)$ has the property that for every point $s \in S$, the value in the residue field $c_n(s) \in \kappa(s)$ is either 0 or 1. It is 1 if and only if $n(s) = n$.

Recall now that since R is a reduced ring, it embeds into the product of all its residue fields,

$$R \hookrightarrow \prod_{s \in \operatorname{Spec} R} \kappa(s).$$

Thus an element $e \in R$ is an idempotent if and only if all its specializations $e(s) \in \kappa(s)$ are idempotents. We obtain that each coefficient of $f^*(t)$ is an idempotent, and hence that each of the sets (2.13) is open and closed as claimed.

Note that if S is connected, then this implies $\operatorname{End}(\mathbb{G}_{m,S}) = \mathbb{Z}$.

Step 3: The general case. Extending from the reduced to the general case can again be done locally. So assume $S = \operatorname{Spec}(R)$ as before and $f = \operatorname{Spec}(f^*)$ for some f^* as above. Assume further that $f^*(t) = t^n + h(t)$ where $h(t)$ has nilpotent coefficients. Our aim is to show that $h(t) = 0$.

Let $I \subset R$ be a nilpotent ideal such that $h(t) \equiv 0 \bmod I$. (For example, take I as the ideal generated by the coefficients of $h(t)$.) We show that then $h(t) \equiv 0 \bmod I^2$ which finishes the proof of the proposition by induction. Indeed, since f is a group scheme endomorphism, f^* satisfies (2.11) which we may evaluate at t to obtain

$$(t^n + h(t)) \otimes (t^n + h(t)) = (t \otimes t)^n + h(t \otimes t).$$

Subtracting $t^n \otimes t^n$ on both sides we obtain that

$$t^n \otimes h(t) + h(t) \otimes t^n \equiv h(t \otimes t) \mod I^2[t, t^{-1}].$$

Comparing the coefficients of each monomial $t^a \otimes t^b$ in this expression first shows that necessarily $h(t) = \lambda t^n$ for some $\lambda \in I$, and then

$$2\lambda t^n \otimes t^n \equiv \lambda t^n \otimes t^n \mod I^2[t, t^{-1}].$$

This implies that $\lambda \in I^2$ and hence $h(t) \in I^2[t, t^{-1}]$ which finishes the proof. □

Proposition 2.12 is sometimes called the "rigidity of endomorphisms of $\mathbb{G}_m$". The word "rigidity" refers to the property of an endomorphism (say of a fiber $\kappa(s) \otimes_S \mathbb{G}_m$) spreading out in at most one way to all of the connected scheme S. We will see that this is a property of homomorphisms between abelian varieties as well. For most group schemes, however, there is no such phenomenon:

Example 2.13. Let $S = \operatorname{Spec} R$; consider the additive group $\mathbb{G}_{a,S} = \operatorname{Spec} R[t]$. Then

$$\begin{aligned} R &\longrightarrow \operatorname{End}_{S\text{-grp sch}}(\mathbb{G}_{a,S}) \\ r &\longmapsto [r] := \operatorname{Spec}(r^* : t \mapsto rt). \end{aligned} \tag{2.14}$$

The functor of points description of $[r]$ is as follos: For every $u : T \to S$, the endomorphism $[r](T)$ of $\mathcal{O}_T(T)$ is multiplication by $u^*(r)$.

2.4. **Kernels.** It is easy to define kernels of group scheme homomorphisms because of the existence of fiber products of S-schemes. Defining quotients is much more tricky and will be discussed later in the course.

Definition 2.14. Let $f : G_1 \to G_2$ be a homomorphism of S-group schemes. Let $e_2 : S \to G_2$ be the neutral element section of G_2. The kernel of f is defined as the fiber product

$$\begin{array}{ccc} \ker(f) & \longrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle e_2} \\ G_1 & \xrightarrow{f} & G_2. \end{array} \tag{2.15}$$

It is clear from its definition that $\ker(f)$ represents the functor (on S-schemes)

$$T \longmapsto \ker\left(f(T) : G_1(T) \longrightarrow G_2(T)\right). \tag{2.16}$$

In particular, $\ker(f)(T) \subset G_1(T)$ is a subgroup for every T, and hence (by Yoneda) $\ker(f)$ is again an S-group scheme. It also follows that the natural map (see (2.15)) $\ker(f) \to G_1$ is a group scheme homomorphism. The multiplication morphism on $\ker(f)$ can be characterized as the unique one that makes the following diagram commute:

$$\begin{array}{ccc} \ker(f) \times_S \ker(f) & \dashrightarrow & \ker(f) \\ \downarrow & & \downarrow \\ G \times_S G & \xrightarrow{\quad m \quad} & G. \end{array} \tag{2.17}$$

Remark 2.15. Recall that if $X \to S$ is a separated morphism, then every section $\sigma : S \to X$ is a closed immersion. Thus, if $G \to S$ is a separated group scheme (e.g. affine or proper), then the neutral element e is a closed immersion. It follows that if in (2.15) $G_2 \to S$ is separated, then $\ker(f) \to G_1$ is a closed immersion.

Example 2.16 (Roots of unity)**.** Let S be any and let $n \geq 1$ be an integer. The group scheme $\mu_{n,S} \to S$ of n-th roots of unities is defined by

$$\mu_{n,S} := \ker\left([n] : \mathbb{G}_{m,S} \longrightarrow \mathbb{G}_{m,S}\right).$$

Its functor of points is

$$\mu_{n,S}(T) = \{\zeta \in \mathcal{O}_T(T) \mid \zeta^n = 1\}.$$

Since fiber products of affine morphisms are given by simply applying the (relative) spectrum construction to the tensor product of rings, we obtain from (2.15) that

$$\begin{aligned} \mu_{n,S} &= \underline{\mathrm{Spec}}\left(\mathcal{O}_S \otimes_{1 \leftarrow t,\ \mathcal{O}_S[t,t^{-1}],\ t \mapsto t^n} \mathcal{O}_S[t,t^{-1}]\right) \\ &= \underline{\mathrm{Spec}}\left(\mathcal{O}_S[t]/(t^n - 1)\right). \end{aligned}$$

It follows e.g. from (2.17) that the multiplication morphism on $\mu_{n,S}$ is still described by $m^*(t) = t \otimes t$.

Example 2.17. The n-th roots of unity behave very differently depending on whether or not $n \in \mathcal{O}_S(S)^\times$. Let $S = \operatorname{Spec} k$ for a field k and first assume $n \in k^\times$. Then $t^n - 1 \in k[t]$ is a separable polynomial. Hence $V(t^n - 1) \subset \mathbb{A}^1_k$ satisfies the Jacobi criterion (Definition 1.3) and thus $\mu_{n,k}$ is smooth. If there exists a primitive n-th root of unity $\zeta \in k$, then

$$t^n - 1 = \prod_{i \in \mathbb{Z}/n} (t - \zeta^i)$$

and thus

$$\mu_{n,k} \xrightarrow{\sim} \coprod_{i \in \mathbb{Z}/n} \operatorname{Spec} k. \tag{2.18}$$

If T is a connected k-scheme, then (2.18) shows that $\mu_{n,k}(T) \cong \mathbb{Z}/n$.

Assume now that $\operatorname{char}(k) = p$ and $n = p^r$. Observe that $(t^{p^r} - 1) = (t-1)^{p^r}$ and thus

$$\mu_{p^r,k} \xrightarrow{\sim} \operatorname{Spec} k[t]/(t-1)^{p^r} \xrightarrow{\sim} \operatorname{Spec} k[\varepsilon]/(\varepsilon)^{p^r} \tag{2.19}$$

is a non-reduced k-scheme. For a k-scheme T, whenever $x \in \mathcal{O}_T(T)$ satisfies $x^{p^r} = 0$, then $(1+x)^{p^r} = 1 + x^{p^r} = 1$, and hence

$$1 + x \in \mu_{p^r,k}(T).$$

In particular, $\mu_{p^r,k}(T)$ can be a large group whose structure depends on $\mathcal{O}_T$ (and not just on $\pi_0(T)$ as in the previous situation.)

3. Rigidity and abelian varieties

3.1. The rigidity theorem.

Theorem 3.1. *(Rigidity) Let k be an algebraically closed field and let X, Y and Z be integral and finite type k-schemes. Assume further that X is proper and Z separated. Let*

$$f : X \times_k Y \longrightarrow Z$$

be a morphism of k-schemes. Assume that there exist rational points $y_0 \in Y(k)$ and $z_0 \in Z(k)$ such that $f(X \times_k \{y_0\}) = \{z_0\}$. Then there exists a k-morphism $g : Y \to Z$ such that $f = g \circ \mathrm{pr}_Y$:

$$\begin{array}{ccc} X \times_k Y & & \\ {\scriptstyle \mathrm{pr}_Y}\downarrow & \searrow^{f} & \\ Y & \xrightarrow{g} & Z. \end{array} \tag{3.1}$$

Proof. First we give a candidate for g: Pick any rational point $x_0 \in X(k)$. (Existence is ensured by the assumption that k is algebraically closed.) Then define g as the composition

$$g : Y \xrightarrow{\sim} \{x_0\} \times_k Y \hookrightarrow X \times_k Y \xrightarrow{f} Z$$

which is the only possibility for g if the theorem indeed holds.

Step 1: Reduction to Y and Z affine. We need to see that $f = g \circ \mathrm{pr}_Y$. Since Z is separated, it is enough to check this identity on any schematically dense open $U \subseteq X \times Y$. Here, recall that U is called schematically dense if the natural map $\mathcal{O}_X \to \mathrm{inc}_{U,*}\mathcal{O}_U$ is injective. Now we use the following lemma:[4]

Lemma 3.2 ([8, Tag 05P3])**.** *Let k be an algebraically closed field, and let X and Y be integral finite type k-schemes. Then $X \times_k Y$ is again integral.*

The lemma applies to our $X \times_k Y$ and hence every open $U \subset X \times_k Y$ is schematically dense. It is thus enough to check $f = g \circ \mathrm{pr}_Y$ on any open U, and we next make a suitable choice.

Next, let $z_0 \in W \subseteq Z$ be an open affine neighborhood. Then $f^{-1}(Z \setminus W) \subseteq X \times_k Y$ is a closed subset. By the properness of $\mathrm{pr}_Y : X \times_k Y \to Y$, the image $\mathrm{pr}_Y(f^{-1}(Z \setminus W)) \subseteq Y$ is closed. It does not contain y_0 by definition of W and the assumption $f(X \times_k \{y_0\}) = \{z_0\}$. Choose an affine open neighborhood V of y_0 such that

$$y_0 \in V \subseteq Y \setminus \mathrm{pr}_Y(f^{-1}(Z \setminus W)).$$

We now choose U in the previous argument as

$$U := X \times_k V.$$

Replacing Y by V and Z by W from now on, we have reduced to the case that Y and Z are affine.

Step 2: The case Y and Z affine. Adjunction for morphisms to affine schemes states that

$$\mathrm{Mor}_k(X \times_k Y, Z) \xrightarrow{\sim} \mathrm{Hom}_{k\text{-alg}}\left(\mathcal{O}_Z(Z), \mathcal{O}_{X \times_k Y}(X \times_k Y)\right). \tag{3.2}$$

Thus in order to prove the equality $f = g \circ \mathrm{pr}_Y$, it suffices to show that they induce the same pullback map on global sections. Now we claim that there is a commutative triangle

[4] The cited reference also includes a separatedness assumption which however is not needed for the lemma as stated here.

with all arrows isomorphisms

$$\begin{array}{ccc} \mathcal{O}_{\{x_0\}\times_k Y}(\{x_0\}\times_k Y) & \xleftarrow{\text{inc}^*} & \mathcal{O}_{X\times_k Y}(X\times_k Y) \\ & \searrow & \uparrow{\scriptstyle \text{pr}_Y^*} \\ & & \mathcal{O}_Y(Y). \end{array} \tag{3.3}$$

Assume this claim for a moment. By definition of g, we have

$$f \circ \text{inc} = g \circ \text{pr}_Y \circ \text{inc}.$$

Passing to global sections and using that inc^* is an isomorphism, we obtain $f^* = \text{pr}_Y^* \circ g^*$ and the proof is complete. It is thus only left to prove the claim.

Step 3: Proof of the claim. The triangle clearly commutes and the projection $\{x_0\}\times Y \to Y$ is an isomorphism. It thus suffices to show that pr_Y^* is an isomorphism. First we observe that $k \xrightarrow{\sim} \mathcal{O}_X(X)$. Namely, since X is proper over k and $\mathcal{O}_X$ coherent, $\mathcal{O}_X(X)$ is a finite dimensional k-algebra. As X is reduced, also $\mathcal{O}_X(X)$ is reduced. Thus $\mathcal{O}_X(X)$ is a product of finite field extensions of k. Since k is algebraically closed, it is even a product of copies of k. Finally, since X is integral by assumption, in particular connected, $k \xrightarrow{\sim} \mathcal{O}_X(X)$ is the only possibility.

Next, we show that this implies $\text{pr}_Y^* : \mathcal{O}_Y(Y) \xrightarrow{\sim} \mathcal{O}_{X\times_k Y}(X\times_k Y)$. Let $X = \bigcup_{i=1}^r X_i$ be a finite open affine covering. By separatedness of $X \to \operatorname{Spec} k$, the intersections $X_{ij} = X_i \cap X_j$ are again affine. Write $X_i = \operatorname{Spec} A_i$ and $X_{ij} = \operatorname{Spec} A_{ij}$ in the following. By the sheaf property and the fact $\mathcal{O}_X(X) = k$, there is an exact sequence

$$0 \longrightarrow k \longrightarrow \prod_{i=1}^r A_i \xrightarrow{r_1 - r_2} \prod_{i,j=1}^r A_{ij}. \tag{3.4}$$

Here, r_1 and r_2 denote the two restriction maps. We have assumed Y to be affine, say $Y = \operatorname{Spec} B$. Since every k-algebra is flat (k is a field), we may apply $- \otimes_k B$ to (3.4) and obtain the exact sequence

$$0 \longrightarrow B \longrightarrow \prod_{i=1}^r A_i \otimes_k B \xrightarrow{r_1 - r_2} \prod_{i,j=1}^r A_{ij} \otimes_k B. \tag{3.5}$$

(Here, we have also used that the indexing set here are finite which allows to interchange the tensor product with the products.) Since $\operatorname{Spec}(A_i \otimes_k B) = X_i \times_k Y$ and $\operatorname{Spec}(A_{ij} \otimes_k B) = X_{ij} \times_k Y$, the second exact sequence precisely computes that $B \xrightarrow{\sim} \mathcal{O}_{X\times_k Y}(X\times_k Y)$. This completes the proof of all remaining claims. □

3.2. **Applications.** Recall the definition of abelian varieties (Definition 2.2). We begin with two auxiliary results that pertain to properties of finite type k-schemes.

Lemma 3.3. *Let $(A, m)/k$ be an abelian variety and let K/k be a field extension. Then $(K \otimes_k A, K \otimes_k m)$ is an abelian variety over K.*

Proof. We already know that the base change is a K-group scheme, see (2.6). Moreover, $K \otimes_k A$ is proper over K because this property is stable under base change. Similarly, $K \otimes_k A$ is again smooth over K directly from definitions: If the Jacobi criterion (over k) holds in a point $x \in A$, then it holds (over K) in every preimage of x in $K \otimes_k A$.

It is only left to show that $K \otimes_k A$ is connected. By assumption, A is connected which means that $R := \mathcal{O}_A(A)$ contains no idempotents except 0 and 1. Since R is a 0-dimensional k-algebra by the properness of A, this means R has a unique maximal ideal $\mathfrak{m}$. There also exists the neutral element $e \in A(k)$ which means that there exists a k-algebra map $R/\mathfrak{m} \to k$. This implies $k \xrightarrow{\sim} R/\mathfrak{m}$, which further implies that $K \otimes_k R$ also

has a unique maximal ideal (whose residue field is K). Finally, by the same argument as for (3.5),

$$K \otimes_k R \xrightarrow{\sim} \mathcal{O}_{K\otimes_k A}(K \otimes_k A)$$

which shows that $K \otimes_k A$ is connected. □

Remark 3.4. The second part of the proof is generalized by [8, Tag 056R]: A connected k-scheme that has a k-rational point stays connected after base change to every field extension K/k.

Fact 3.5. *Let X be a connected k-scheme of locally finite type. If X is smooth, then X is integral. In particular, abelian varieties are integral schemes.*

Proposition 3.6. *Let (A_1, m_1) and (A_2, m_2) be abelian varieties over k and let $f : A_1 \to A_2$ be a morphism of k-schemes such that $f(e_1) = e_2$. Then f is a group scheme homomorphism. Here, $e_i \in A_i(k)$ denotes the neutral element.*

Proof. Step 1: The case when k is algebraically closed. Consider the morphism

$$\begin{aligned} \phi : A_1 \times_k A_1 &\longrightarrow A_2 \\ (x, y) &\longmapsto f(x \cdot y)f(y)^{-1}f(x)^{-1}. \end{aligned}$$

Here, the notation is meant in the sense that $x, y \in A_1(T)$ are arbitrary T-valued points, and the group operations on the right hand side refer to the group structure on $A_2(T)$. (Thus we have implicitly used the Yoneda lemma to define ϕ.)

We see by substitution that $\phi|_{A_1\times_k\{e_1\}} = \{e_2\}$. By Fact 3.5 and since we assumed k to be algebraically closed, Theorem 3.1 applies and provides a morphism $\psi : A_1 \to A_2$ such that $\phi(x, y) = \psi(y)$ for all T and all $(x, y) \in A_1(T)$. Then we find

$$\phi(x, y) = \psi(y) = \phi(e_1, y) = e_2$$

for all (x, y), which precisely means that f is a group homomorphism.

Step 2: Reduction to $k = \bar{k}$. The morphism ϕ is defined in the same way for general k. We again need to show that it equals the composition

$$A_1 \times_k A_1 \longrightarrow \operatorname{Spec} k \xrightarrow{e_2} A_2.$$

Such an equality can be shown after base change to $\bar{k}$. (This follows from the fact that a k-algebra homomorphism $B_1 \to B_2$ is uniquely determined by its base change $\bar{k} \otimes_k B_1 \to \bar{k} \otimes_k B_2$. This fact in turn is obvious from the injectivity $B_i \to \bar{k} \otimes_k B_i$.) It is easy to see that the base change $\bar{k} \otimes_k \phi$ of ϕ is nothing but the morphism ϕ defined for $\bar{k} \otimes_k f : \bar{k} \otimes_k A_1 \to \bar{k} \otimes_k A_2$. We are done with Lemma 3.3. □

Corollary 3.7. *The group structure of an abelian variety is commutative.*

Proof. Given A/k, consider the inverse morphism

$$i : A \longrightarrow A, \ x \longmapsto x^{-1}.$$

The notation here is meant in the sense of the Yoneda Lemma: For any $T \to \operatorname{Spec} k$ and any $x \in A(T)$ we have $i(x) = x^{-1}$.

It is clear that $i(e) = e$, so Proposition 3.6 applies and states that i is a group homomorphism. This means

$$xy = i(y^{-1}x^{-1}) = i(y^{-1})i(x^{-1}) = yx$$

for all $T \to \operatorname{Spec} k$ and all $x, y \in A(T)$. □

Corollary 3.8. *Let $h : A_1 \to A_2$ be any k-scheme morphism between abelian varieties over k. Then there exist a rational point $x \in A_2(k)$ and a group homomorphism $f : A_1 \to A_2$ such that $h = f + x$.*

The statement is again meant in the sense of the Yoneda lemma: For every $u : T \to \operatorname{Spec} k$ and every $y \in A_1(T)$ we have $h(y) = f(y) + u^*(x)$.

Proof. Let $x = h(e_1)$. Then $f := h - x$ satisfies $f(e_1) = e_2$. Now apply Proposition 3.6. □

4. Kähler differentials and smoothness

Definition 4.1 (Genus of a curve)**.** Let k be a field and let C be a proper, smooth, geometrically[5] connected curve over k. The genus of C is the integer

$$\dim_k H^0(C, \Omega^1_{C/k}).$$

The sheaf $\Omega^1_{C/k}$ is the so-called sheaf of Kähler differentials which will be introduced below. Because of the smoothness of C, it is a line bundle that is also called the canonical bundle. Our aim is to prove the following result:

Proposition 4.2. *Let E be an elliptic curve over k. Then E has genus 1.*

The genus of a curve controls the arithmetic of its meromorphic functions through the Riemann–Roch theorem. In particular, it is closely related to how the curve can be embedded into projective space. In the case of elliptic curves, we will later use Proposition 4.2 to prove that every elliptic curve can be defined as a plane cubic.

4.1. Kähler differentials.

Definition 4.3. Let R be a ring, let A be an R-algebra, and let M be an A-module. An R-derivation from A to M is an R-linear map $\delta : A \to M$ such that the Leibniz rule holds: For all $a, b \in A$,

$$\delta(ab) = a\delta(b) + b\delta(a). \tag{4.1}$$

Note that $\delta(1) = \delta(1 \cdot 1) = \delta(1) + \delta(1)$, so $\delta(1) = 0$. Then, by the R-linearity of R-derivations, we obtain for all $r \in R$ that

$$\delta(r) = r\delta(1) = 0.$$

Furthermore, if $\delta_1, \delta_2 : A \to M$ are two R-derivations and if $\lambda_1, \lambda_2 \in A$ are scalars, then

$$\begin{aligned} \lambda_1\delta_1 + \lambda_2\delta_2 : A &\longrightarrow M \\ a &\longmapsto \lambda_1\delta_1(a) + \lambda_2\delta_2(a) \end{aligned}$$

is again an R-derivation. Thus R-derivations from A to M form an A-module which we denote by $\operatorname{Der}_R(A, M)$.

Example 4.4. Assume that $A = R[X_1, \ldots, X_n]$ is a polynomial ring over R and let $M = A$. The partial derivatives

$$\frac{\partial}{\partial X_i} : A \longrightarrow A$$

are R-linear and define R-derivations. Given polynomials $f_1, \ldots, f_n \in A$, the linear combination

$$t = \sum_{i=1}^{n} f_i \cdot \frac{\partial}{\partial X_i} \in \operatorname{Der}_R(A, A) \tag{4.2}$$

[5] A k-scheme X is said to be *geometrically* connected, irreducible, integral, regular etc. if the base change $\bar{k} \otimes_k X$ is connected, irreducible, integral, regular etc. A non-trivial statement is that if X is geometrically $\mathbb{P}$, then for every field extension K/k, the base change $K \otimes_k X$ is $\mathbb{P}$.

is another derivation. Assume that $R = k$ is a field. Then t should be thought of as the vector field on $\mathbb{A}^n_k$ whose value in a point $x = (x_1, \dots, x_n) \in k^n$ is the tangent vector

$$\sum_{i=1}^{n} f_i(x_1, \dots, x_n) \cdot \frac{\partial}{\partial X_i}.$$

If R is general, then t can be thought of as a fiber-by-fiber vector field for $\pi : \mathbb{A}^n_R \to \operatorname{Spec} R$. The value of t in a point $x \in \mathbb{A}^n_R$ is a tangent vector of the fiber $\mathbb{A}^n_{\kappa(\pi(x))}$ in x; it is in particular parallel to the fiber.

Lemma 4.5. *Let R be any ring and let $A = R[X_1, \dots, X_n]$. Then the construction of (4.2) defines an isomorphism of A-modules*

$$\begin{aligned} A^n &\xrightarrow{\sim} \operatorname{Der}_R(A, A) \\ (f_1, \dots, f_n) &\longmapsto \sum_{i=1}^{n} f_i \cdot (\partial/\partial X_i). \end{aligned} \tag{4.3}$$

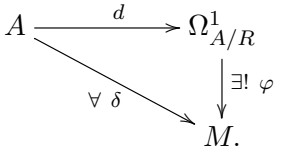
Proof. First observe that $(\partial/\partial X_i)(X_j) = \delta_{ij}$ (Kronecker delta). This shows that

$$\big(\sum_{i=1}^{n} f_i \cdot (\partial/\partial X_i)\big)(X_j) = f_j$$

and hence that (4.3) is injective. Given any derivation $\delta \in \operatorname{Der}_R(A, A)$, set $f_i = \delta(X_i)$. The Leibniz rule then ensures that $\delta = \sum_{i=1}^n f_i \cdot (\partial/\partial X_i)$, proving the surjectivity. □

Motivated by this lemma, we now try to give a general description of $\operatorname{Der}_R(A, M)$.

Definition 4.6. Let A be an R-algebra. A universal R-derivation of A is a pair $(\Omega^1_{A/R}, d)$ that consists of an A-module $\Omega^1_{A/R}$ and an R-derivation $d : A \to \Omega^1_{A/R}$ with the following universal property: Every R-derivation $\delta : A \to M$ factors through a unique A-module homomorphism $\varphi : \Omega^1_{A/R} \to M$. As diagram,



(4.4)

Lemma 4.7. *A universal derivation $\Omega^1_{A/R}$ exists and is unique up to unique isomorphism. It is called the module of Kähler differentials of A over R.*

Proof. The construction is standard: Let $\widetilde{\Omega}$ be the free A-module generated by symbols da, for $a \in A$. Let $U \subseteq \widetilde{\Omega}$ be the A-submodule generated by all elements of the form

$$\begin{array}{ll} d(ra) - rda & r \in R,\ a \in A \\ d(a+b) - da - db & a, b \in A \\ d(ab) - adb - bda & a, b \in A. \end{array}$$

Then the map $d : A \to \widetilde{\Omega}/U$, $a \mapsto da$ is an R-derivation by definition. Moreover, for every R-derivation $\delta : A \to M$, there exists a unique A-linear map $\widetilde{\varphi} : \widetilde{\Omega} \to M$ such that $\widetilde{\varphi}(da) = \delta(a)$. (Use that $\widetilde{\Omega}$ is a free A-module.) As δ is a derivation by assumption, $\widetilde{\varphi}(U) = 0$ and hence $\widetilde{\varphi}$ factors in a unique way through $\widetilde{\Omega}/U$. Thus we may set $(\Omega^1_{A/R}, d) = (\widetilde{\Omega}/U, d)$ and obtain a universal derivation. The uniqueness up to unique isomorphism follows from the universal property. □

Example 4.8. Extending Example 4.4, let $A = R[X_i, i \in I]$ be a polynomial ring over R. Then

$$\begin{aligned} A^{\oplus I} &\xrightarrow{\sim} \Omega^1_{A/R} \\ (f_i)_{i\in I} &\longmapsto \sum_{i\in I} f_i dX_i. \end{aligned} \tag{4.5}$$

In this case, the Leibniz rule ensures that the universal derivation $d : A \to \Omega^1_{A/R}$ is described by

$$df = \sum_{i\in I} \frac{\partial f}{\partial X_i} \cdot dX_i.$$

Example 4.9. A concrete numerical example for $A = \mathbb{Z}[X, Y]$ is

$$d(XY + Y^2) = YdX + (X + 2Y)dY \in AdX \oplus AdY.$$

Assume we are given a commutative square of ring maps

$$\begin{array}{ccc} A_2 & \xleftarrow{\varphi} & A_1 \\ \uparrow & & \uparrow \\ R_2 & \longleftarrow & R_1. \end{array} \tag{4.6}$$

The composition $A_1 \to A_2 \to \Omega^1_{A_2/R_2}$ defines an R_1-derivation of A_1. Also extending scalars from A_1 to A_2, it factors through a unique A_2-linear map

$$\begin{aligned} A_2 \otimes_{A_1} \Omega^1_{A_1/R_1} &\longrightarrow \Omega^1_{A_2/R_2} \\ a \otimes df &\longmapsto a \cdot d\varphi(f). \end{aligned} \tag{4.7}$$

In the following lemma, the maps between Kähler differentials are all special cases of construction (4.7).

Lemma 4.10 (Kähler differential arithmetic)**.** *(1) Let $A \twoheadrightarrow A/I$ be a surjection of R-algebras. Then the natural map $\Omega^1_{A/R} \to \Omega^1_{(A/I)/R}$ fits into an exact sequence*

$$I/I^2 \xrightarrow{f\mapsto 1\otimes df} A/I \otimes_A \Omega^1_{A/R} \longrightarrow \Omega^1_{(A/I)/R} \longrightarrow 0. \tag{4.8}$$

(2) Let $S \subseteq A$ be a subset of an R-algebra A. Then the natural map $\Omega^1_{A/R} \to \Omega^1_{A[S^{-1}]/R}$ induces an isomorphism

$$A[S^{-1}] \otimes_A \Omega^1_{A/R} \xrightarrow{\sim} \Omega^1_{A[S^{-1}]/R}.$$

(3) Let A be an R_1-algebra and let $R_1 \to R_2$ be a ring morphism. Then the natural map induces an isomorphism

$$R_2 \otimes_{R_1} \Omega^1_{A/R_1} = (R_2 \otimes_{R_1} A) \otimes_A \Omega^1_{A/R_1} \xrightarrow{\sim} \Omega^1_{(R_2\otimes_{R_1} A)/R_2}.$$

(4) Assume that $R \to A \to B$ are ring maps. The natural maps form an exact sequence

$$B \otimes_A \Omega^1_{A/R} \longrightarrow \Omega^1_{B/R} \longrightarrow \Omega^1_{B/A} \longrightarrow 0.$$

(5) Assume that A_1 and A_2 are R-algebras and set $B = A_1 \otimes_R A_2$. The natural maps induce an isomorphism

$$B \otimes_{A_1} \Omega^1_{A_1/R} \oplus B \otimes_{A_2} \Omega^1_{A_2/R} \xrightarrow{\sim} \Omega^1_{B/R}.$$

Proof. The proofs are not difficult and we refer to [8, Tag 00RM] and [6, §5–§7] for more details. □

Example 4.11. An important observation is that Example 4.8 and Lemma 4.10 (1) give an expression for the Kähler differentials of any R-algebra A. Namely, choose any presentation $\widetilde{A} = R[X_k, k \in K]$, $A = \widetilde{A}/I$ of A as quotient of a polynomial R-algebra. Then (4.8) implies that

$$\big(\bigoplus_{k\in K} A \cdot dX_k\big)/\big(df,\ f \in I\big) \xrightarrow{\sim} \Omega^1_{A/R}. \tag{4.9}$$

A related statement which also follows immediately from the Leibniz rule is that if a subset $S \subset A$ generates A as R-algebra, then the differentials $\{df \mid f \in S\}$ generate $\Omega^1_{A/R}$ as A-module.

Example 4.12 (Relation with the Jacobi matrix)**.** In the case that A is of finite presentation, say $A = R[X_1, \dots, X_n]/(f_1, \dots, f_m)$, (4.9) specializes to the statement that $\Omega^1_{A/R}$ is isomorphic to the cokernel of the Jacobi matrix $J = (\partial f_i/\partial X_j)_{ij}$,

$$A^m \xrightarrow{J} A^n \longrightarrow \Omega^1_{A/R} \longrightarrow 0. \tag{4.10}$$

Example 4.13. Consider a prime $p \neq 2$ and the ring $A = \mathbb{Z}[\sqrt{p}]$. We know that $\Omega^1_{A/\mathbb{Z}}$ is generated by the differential $d\sqrt{p}$, and hence is of the form $(A/\mathfrak{a}) \cdot d\sqrt{p}$ for some ideal $\mathfrak{a} \subseteq A$. How to determine $\mathfrak{a}$?

Choose the presentation $\mathbb{Z}[T]/(T^2 - p) \xrightarrow{\sim} A$, where $T \mapsto \sqrt{p}$. We obtain from (4.10) that

$$\Omega^1_{A/\mathbb{Z}} \xrightarrow{\sim} A \cdot dT/2TdT \xrightarrow{\sim} A/(2\sqrt{p}) \cdot d\sqrt{p}, \tag{4.11}$$

meaning $\mathfrak{a} = (2\sqrt{p})$.

Definition 4.14. Let $\pi : X \to S$ be a morphism of schemes. The uniqueness up to unique isomorphism of $(\Omega^1_{A/R}, d)$, and the compatibility with localizations (Lemma 4.10 (2)), imply that there is a unique quasi-coherent $\mathcal{O}_X$-module $\Omega^1_{X/S}$ together with a $\pi^{-1}\mathcal{O}_S$-derivation $d : \mathcal{O}_X \to \Omega^1_{X/S}$ such that for all open affines $V \subseteq S$ and $U \subseteq \pi^{-1}(U)$, the map

$$d(U) : \mathcal{O}_X(U) \longrightarrow \Omega^1_{X/S}(U)$$

is a universal $\mathcal{O}_S(V)$-derivation. In more down to earth terms, say $V = \operatorname{Spec} R$ and $U = \operatorname{Spec} A$. Then

$$\Omega^1_{X/S}|_U = (\Omega^1_{A/R})^\sim$$

and the gluing maps are induced from (4.7). The uniqueness up to unique isomorphism ensures the cocycle condition of that gluing. Given a commutative square

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ \downarrow & & \downarrow \\ T & \longrightarrow & S, \end{array}$$

there is a unique pullback map $f^* : f^*\Omega^1_{X/S} \to \Omega^1_{Y/T}$ which is locally induced from (4.7). In the case $Y = T \times_S X$, Lemma 4.10 (3) implies that

$$f^* : f^*\Omega^1_{X/S} \xrightarrow{\sim} \Omega^1_{T\times_S X/T}.$$

4.2. **Regularity.** We recall the definition of regularity and some related results for later use. Recall that if $(A, \mathfrak{m})$ is a noetherian local ring, then we have the inequality

$$\dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \geq \dim(A).$$

Definition 4.15. A local ring $(A, \mathfrak{m})$ is said to be regular if it is noetherian and if

$$\dim_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = \dim(A).$$

A scheme X is said to be regular if all the local rings $\mathcal{O}_{X,x}$ are regular.

Easy examples of regular local rings are the power series rings $k[\![X_1, \dots, X_n]\!]$, where k is a field, or $R[\![X_1, \dots, X_n]\!]$, where R is a DVR. A slightly less obvious example is $R[\![X, Y]\!]/(XY - \pi)$, where R is a DVR and $\pi \in R$ a uniformizer. In these cases, one may check regularity directly from the definition. In Theorem 4.18 below, we will see that the local rings of a smooth variety are also regular local rings.

Lemma 4.16 ([8, Tag 00NP])**.** *Any regular local ring is a domain.*

In fact, a regular local ring is a *factorial* domain, in particular integrally closed.

Lemma 4.17 ([8, Tag 0AFS])**.** *Let A be a regular local ring. Then for every prime ideal $\mathfrak{p} \subset A$, the localization $A_\mathfrak{p}$ is again regular.*

4.3. **Relation with smoothness.** Recall that we defined smoothness of a locally finite type k-scheme in terms of the Jacobi criterion (Definition 1.3).

Theorem 4.18. *Let X be a locally finite type k-scheme and let $x \in X$. The following conditions are equivalent:*

(1) X is smooth in x.

(2) There exists an open neighborhood $x \in U$ such that $\bar{k} \otimes_k U$ is regular.

(3) $\Omega^1_{X/k}$ is free of rank $\dim_x(X)$ on an open neighborhood of x.

Example 4.19. It is true that if $\bar{k} \otimes_k U$ is regular as in (2) above, then U is regular. The converse need not hold, as the following example shows.

Let $k = \mathbb{F}_p(t)$ and $K = k(t^{1/p})$. Then $\operatorname{Spec} K$ is a regular, 0-dimensional scheme. However, $\bar{k} \otimes_k K \cong \bar{k}[\varepsilon]/(\varepsilon^p)$ is not reduced (and also clearly not regular).

We start with some lemmas. If X is a scheme, $\mathcal{F}$ a quasi-coherent $\mathcal{O}_X$-module, and $x \in X$, then we write $\mathcal{F}(x)$ for the *fiber* $\kappa(x) \otimes_{\mathcal{O}_{X,x}} \mathcal{F}_x$. This notation is not to be confused with the *stalk* $\mathcal{F}_x$.

Lemma 4.20. *Let A be a finite type k-algebra and let $x : A \twoheadrightarrow k$ be a rational point of $\operatorname{Spec}(A)$ with maximal ideal $\mathfrak{m}$. Then*

$$\begin{aligned} \mathfrak{m}/\mathfrak{m}^2 &\xrightarrow{\sim} \Omega^1_{A/k}(x) \\ f &\longmapsto df. \end{aligned} \tag{4.12}$$

Proof. We construct a derivation $\delta : A \to \mathfrak{m}/\mathfrak{m}^2$ as follows. Since $\kappa(x) = k$, for every function $f \in A$ we may consider the value $f(x) \in k$ and define $\delta(f) := f - f(x) \bmod \mathfrak{m}^2$. It is a derivation because

$$fg - f(x)g(x) = f(x)(g - g(x)) + g(x)(f - f(x)) + (f - f(x))(g - g(x))$$

and the last summand lies in $\mathfrak{m}^2$. By the universal property of $(\Omega^1_{A/k}, d)$, it factors through an A-linear map

$$\begin{aligned} \Omega^1_{A/k}(x) &\longrightarrow \mathfrak{m}/\mathfrak{m}^2 \\ df &\longmapsto (f - f(x)). \end{aligned} \tag{4.13}$$

This map is surjective because $df \mapsto f \bmod \mathfrak{m}^2$ for all $f \in \mathfrak{m}$. On the other hand, we have $df = d(f - f(x))$ for every element $f \in A$, so $\{df \mid f \in \mathfrak{m}\}$ generate $\Omega^1_{A/k}$ as A-module. Moreover, if $f, g \in \mathfrak{m}$, then $d(fg) \in \mathfrak{m}\Omega^1_{A/k}$ by the Leibniz rule. So

$$\dim_k \Omega^1_{A/k}(x) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$$

and hence (4.13) has to be an isomorphism for dimension reasons. □

Next, we note some semi-continuity properties in a more abstract setting. Let A be a ring, $n, m \geq 0$ integers, $J \in M_{n\times m}(A)$ a matrix, and $\Omega = \operatorname{coker}(J)$. That is, we consider an exact sequence

$$A^m \xrightarrow{J} A^n \longrightarrow \Omega \longrightarrow 0.$$

For each point $x \in \operatorname{Spec} A$, we can specialize J to obtain a matrix $J(x) \in M_{n\times m}(\kappa(x))$. We may also take the fiber $\Omega(x)$, which is a finite dimensional $\kappa(x)$-vector spaces. Since $\kappa(x) \otimes_A -$ is right exact, we always have the exact sequence

$$\kappa(x)^m \xrightarrow{J(x)} \kappa(x)^n \longrightarrow \Omega(x) \longrightarrow 0.$$

In particular, we always have the relation

$$\operatorname{rk} J(x) + \dim_{\kappa(x)} \Omega(x) = n. \tag{4.14}$$

Now observe that $\operatorname{rk} J(x) \leq r$ if and only if the determinants of all $(r+i)\times(r+i)$-minors of $J(x)$ vanish at x, where $i \geq 1$. (In fact, it is enough to consider all $(r+1)\times(r+1)$-minors.) This condition defines a closed subset of $\operatorname{Spec} A$. Thus we have proved the following result.

Lemma 4.21 (Semi-continuity)**.** *In the above situation, for every $r \geq 0$, the two subsets $\{x \in \operatorname{Spec}(A) \mid \operatorname{rk} J(x) \leq r\}$ and $\{x \in \operatorname{Spec}(A) \mid \dim_{\kappa(x)} \Omega(x) \geq r\}$ are closed.*

We now apply this to prove inequalities on the fiber dimensions of $\Omega^1_{X/k}$.

Lemma 4.22. *Let $U = V(f_1, \dots, f_m) \subseteq \mathbb{A}^n_k$ be a closed subscheme of affine space. Let $A = \mathcal{O}_U(U)$ and denote by $J \in M_{n\times m}(A)$ the Jacobi matrix of $f_1, \dots, f_m$. Then, for every point $x \in U$, we have the inequalities*

$$\begin{aligned} \dim_{\kappa(x)} \Omega^1_{X/k}(x) &\geq \dim_x(U). \\ \operatorname{rk} J(x) &\leq n - \dim_x(U). \end{aligned} \tag{4.15}$$

Proof. By (4.10), there is an exact sequence

$$A^m \xrightarrow{J} A^n \longrightarrow \Omega^1_{A/k} \longrightarrow 0.$$

In particular, $\operatorname{rk} J(x) + \dim_{\kappa(x)} \Omega^1_{A/k}(x) = n$ for all $x \in U$ as in (4.14). Hence the two inequalities in (4.15) are equivalent.

Now apply Lemma 4.21: By semi-continuity, there exists an open neighborhood $V \subseteq U$ of x such that

$$\dim_{\kappa(x)} \Omega^1_{A/k}(x) \geq \dim_{\kappa(y)} \Omega^1_{A/k}(y)$$

for all $y \in V$. Moreover, for every $y \in \overline{\{x\}}$, we have $\dim_y(U) \geq \dim_x(U)$ because if $Z \subseteq U$ is an irreducible component that contains x, then it also contains $\overline{\{x\}}$. Since we are working with finite type algebras over a field, there exists a closed point $y \in V \cap \overline{\{x\}}$ for which we now have

$$\dim_{\kappa(x)} \Omega^1_{A/k}(x) \geq \dim_{\kappa(y)} \Omega^1_{A/k}(y) \overset{?}{\geq} \dim_y(U) \geq \dim_x(U).$$

Thus we may henceforth assume that x is a closed point. Next, let $\bar{x} \in \bar{k} \otimes_k U$ be a preimage of x. Then

$$\Omega^1_{\bar{k}\otimes_k A/\bar{k}}(\bar{x}) = \kappa(\bar{x}) \otimes_{\kappa(x)} \Omega^1_{A/k}(x)$$

by Lemma 4.10 (3). Moreover, also $\dim_{\bar{x}}(\bar{k} \otimes_k U) = \dim_x(U)$, so we can also assume that $k = \bar{k}$.

End of proof, assuming x closed and $k = \bar{k}$. Let $\mathfrak{m} \subset A$ be the maximal ideal defined by x. We obtain from Lemma 4.20 that

$$\dim_{\kappa(x)} \Omega^1_{A/k}(x) = \dim_{\kappa(x)}(\mathfrak{m}/\mathfrak{m}^2) \geq \dim(A_{\mathfrak{m}}) = \dim_x(U)$$

and the proof is complete. (The inequality in the middle holds for every local noetherian ring. The last equality holds because x is closed.) □

Proof of (1) ⇔ (2) *in Theorem 4.18.* First assume that (1) holds, i.e. assume that X is smooth in x. By definition, this means there exists an affine open neighborhood $x \in U = \operatorname{Spec} A$ together with a presentation $U \xrightarrow{\sim} V(f_1, \dots, f_m) \subseteq \mathbb{A}^n_k$ such that the Jacobi matrix J of $f_1, \dots, f_m$ satisfies

$$\operatorname{rk} J(x) = n - \dim_x(U).$$

By (4.14), this is equivalent to $\dim_{\kappa(x)} \Omega^1_{A/k}(x) = \dim_x(U)$. By the same argument as during the proof of Lemma 4.22, there exists a closed point $y \in \overline{\{x\}}$ such that

$$\dim_{\kappa(y)} \Omega^1_{A/k}(y) = \dim_{\kappa(x)} \Omega^1_{A/k}(x).$$

By the inequality from Lemma 4.22, necessarily $\dim_y(U) = \dim_x(U)$.

Let $\bar{y} \in \bar{U} := \bar{k} \otimes_k U$ lie above y. Then, letting $\bar{\mathfrak{m}} \subset \mathcal{O}_{\bar{U},\bar{y}}$ denote the maximal ideal, we find

$$\begin{aligned} \dim_{\bar{k}} \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 &= \dim_{\bar{k}} \Omega^1_{\bar{U}/\bar{k}}(\bar{y}) \\ &= \dim_{\kappa(y)} \Omega^1_{U/k}(y) \\ &= \dim_y(U) \\ &= \dim_{\bar{y}}(\bar{U}). \end{aligned} \tag{4.16}$$

Here, the first equality is Lemma 4.20 and the second comes from Lemma 4.10 (3). The third equality is by construction of y. The final dimension equality was already used in the previous proof. The conclusion of (4.16) is that $\bar{U}$ is regular in $\bar{y}$. This was the main argument; the remainder is about spreading out this regularity to an open neighborhood as in (2) of Theorem 4.18.

Spreading out the regularity. By Lemma 4.16, $\mathcal{O}_{\bar{U},\bar{y}}$ is a domain. Consider the pullback map $\mathcal{O}_{U,y} \to \mathcal{O}_{\bar{U},\bar{y}}$. It is flat because $\mathcal{O}_{\bar{U},\bar{y}}$ is a localization of $\bar{k} \otimes_k \mathcal{O}_{U,y}$, which is flat over $\mathcal{O}_{U,y}$. Since y is a specialization of every point of $\operatorname{Spec} \mathcal{O}_{U,y}$, and since $\bar{y} \mapsto y$, the following lemma implies the surjectivity of $\operatorname{Spec} \mathcal{O}_{\bar{U},\bar{y}} \to \operatorname{Spec} \mathcal{O}_{U,y}$.

Lemma 4.23 ([8, Tag 00HS])**.** *Assume that $A \to B$ is a flat ring map, that $\mathfrak{p} \subset \mathfrak{p}'$ are prime ideals in A, and that $\mathfrak{q}' \subset B$ is a prime ideal above $\mathfrak{p}'$. Then there exists a prime ideal $\mathfrak{q} \subset \mathfrak{q}'$ that lies above $\mathfrak{p}$.*

In other words, $\mathcal{O}_{U,y} \to \mathcal{O}_{\bar{U},\bar{y}}$ is faithfully flat, and in particular injective. Thus we deduce that $\mathcal{O}_{U,y}$ is an integral domain as well. Then $\mathcal{O}_{U,x}$ is also an integral domain because it is a localization of $\mathcal{O}_{U,y}$.

There exists an open neighborhood $x \in V \subseteq U$ that is integral: The closed subscheme $V(\mathcal{N})$ defined by the sheaf of nilpotent elements $\mathcal{N} \subset \mathcal{O}_U$ does not meet x by reducedness of $\mathcal{O}_{U,x}$. Hence there is an open neighborhood $x \in V' \subseteq U \setminus V(\mathcal{N})$. Since $\mathcal{O}_{U,x}$ is an integral domain, there exists a unique irreducible component $Z \subseteq V'$ that contains x. Then we set $V = V' \setminus \bigcup_{Z' \neq Z} Z'$, where Z' runs through the irreducible components of V'.

For every $y \in V$, the local dimension $\dim_y(V)$ equals $d = \dim(V)$ by integrality. Our assumption was that U is smooth in x, i.e. $\dim_{\kappa(x)} \Omega^1_{U/k}(x) = d$. Using semi-continuity again, there exists an open neighborhood $x \in W \subseteq V$ such that $\dim_{\kappa(y)} \Omega^1_{W/k}(y) = d$ for all $y \in W$. This means that W is smooth. By the previous arguments, the base change $\bar{k} \otimes_k W$ is regular in all closed points. By the stability of regularity under localization (Lemma 4.17), we obtain that $\bar{k} \otimes_k W$ is regular, and the proof of (2) is complete.

Step (2) ⇒ (1). Assume that $x \in U$ is an open affine neighborhood such that $\bar{U} = \bar{k} \otimes_k U$ is regular. By Lemma 4.20, this means that $\dim_{\kappa(\bar{y})} \Omega^1_{\bar{U}/\bar{k}}(\bar{y}) = \dim_{\bar{y}}(\bar{U})$ for all closed points $\bar{y} \in \bar{U}$. Moreover, since all local rings of $\bar{U}$ are integral domains by the

regularity (Lemma 4.16), the function $\bar{U} \ni \bar{y} \mapsto \dim_{\bar{y}}(\bar{U})$ is locally constant. The semi-continuity of $\dim_{\kappa(\bar{y})} \Omega^1_{\bar{U}/\bar{k}}(\bar{y})$ together with the inequality from Lemma 4.22 then implies that $\dim_{\kappa(\bar{y})} \Omega^1_{\bar{U}/\bar{k}} = \dim_{\bar{y}}(\bar{U})$ for all points $\bar{y} \in \bar{U}$. Since the local dimensions of U and the fiber rank of $\Omega^1_{U/k}$ are unchanged by base change from k to $\bar{k}$, we obtain that $\dim_{\kappa(y)} \Omega^1_{U/k} = \dim_y(U)$ for all $y \in U$. Using (4.14) again, this precisely means that U is smooth. □

It is left to prove the equivalence with (3). The implication (3) ⇒ (1) is quite straightforward: If the stalk $\Omega^1_{X/k,x}$ is free of rank $\dim_x(X)$, then in particular $\dim_{\kappa(x)}(\Omega^1_{X/k}(x)) = \dim_x(X)$. After choosing local coordinates, (4.14) implies that the Jacobi criterion holds in x, i.e. that (1) holds. For the converse direction, we first formulate two commutative algebra statements.

Lemma 4.24. *Let A be a reduced ring and let $J : A^m \to A^n$ be an $(n \times m)$-matrix such that the rank $r = \operatorname{rk} J(y)$ is independent of $y \in \operatorname{Spec} A$. Then $\ker(J)$ and $\operatorname{coker}(J)$ are locally free A-modules of ranks $m - r$ and $n - r$, respectively.*

Proof. Let $x \in \operatorname{Spec} A$ be any point. By assumption, there exists an $(r \times r)$-minor J_0 of J such that $J_0(x) \in GL_r(\kappa(x))$. Let $f = \det(J_0) \in A$. Then $\operatorname{Spec} A[f^{-1}]$ is an open neighborhood of x. We claim that $\ker(J)[f^{-1}]$ and $\operatorname{coker}(J)[f^{-1}]$ are free of the claimed ranks. This will be obvious after a number of change of basis operations on $A[f^{-1}]^m$ and $A[f^{-1}]^n$: First, after a reordering of coordinates, we may assume that J takes the form

$$J = \begin{pmatrix} J_0 & J_{12} \\ J_{21} & J_{22} \end{pmatrix}.$$

Multiplying with $\operatorname{diag}(J_0^{-1}, 1_{n-r}) \in GL_n(A[f^{-1}])$ from the left, we may assume that $J_0 = 1_r$. Then row and column operations allow to assume $J = \operatorname{diag}(1_r, K)$ for some $(n - r, m - r)$-matrix K with values in $A[f^{-1}]$. Our assumption implies that, for all $y \in \operatorname{Spec} A[f^{-1}]$,

$$\operatorname{rk} J(y) = r + \operatorname{rk} K(y) = r,$$

i.e. that $\operatorname{rk} K(y) = 0$ for all such y. Since A and hence also $A[f^{-1}]$ are reduced, this means that all entries of K vanish. □

Corollary 4.25. *Let X be a reduced scheme and let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module that is locally finitely presented. Assume that $d = \dim_{\kappa(x)} \mathcal{F}(x)$ is independent of $x \in X$. Then $\mathcal{F}$ is locally free of rank d.*

Proof. Given $x \in X$, choose an affine open neighborhood $x \in U$, integers $m, n \geq 0$, and a presentation

$$\mathcal{O}_U^{\oplus m} \xrightarrow{J} \mathcal{O}_U^{\oplus n} \longrightarrow \mathcal{F}|_U \longrightarrow 0.$$

Then apply Lemma 4.24. □

Proof of (1), (2) ⇒ (3). Assume that X is smooth in x. Let U be an open neighborhood of x such that $\bar{k} \otimes_k U$ is regular; in particular U is smooth by what was already proved. Since $\bar{k} \otimes_k U$ is regular, it is reduced, and hence U is reduced. (In fact, U is also regular, see [8, Tag 045K].) The two functions $x \mapsto \dim_x(U)$ and $x \mapsto \dim_{\kappa(x)} \Omega^1_{U/k}(x)$ are locally constant and equal by (2). Then Corollary 4.25 applies and shows that $\Omega^1_{U/k}$ is locally free and of rank $\dim_x(U)$ near x. □

Here is an interesting consequence: Closed immersions between smooth schemes are locally defined by codimension many equations. This is completely in line with what we intuitively expect from the implicit function theorem (Remark 1.5)!

Corollary 4.26. *Let $i : Z \hookrightarrow X$ be the closed immersion of smooth k-schemes defined by the sheaf of ideals $\mathcal{I} \subseteq \mathcal{O}_X$. Let $c(z) := \dim_z(X) - \dim_z(Z)$ denote the codimension in a point $z \in Z$.*

Then $\mathcal{I}/\mathcal{I}^2$ is a locally free $\mathcal{O}_Z$-module whose rank in z is $c(z)$. In particular, for every $z \in Z$, there exist an open neighborhood U of z in X and functions $g_1, \ldots, g_{c(z)} \in \mathcal{I}(U)$ such that $Z \cap U = V(g_1, \ldots, g_{c(z)})$.

Proof. Define

$$\mathcal{K} := \ker\left(i^* : i^*\Omega^1_{X/k} \twoheadrightarrow \mathcal{O}_{Z/k}\right)$$

as the kernel of pullback map of differentials. Since $\Omega^1_{X/k}$ and $\Omega^1_{Z/k}$ are locally free of ranks $\dim_z(X)$ and $\dim_z(Z)$ near z by Theorem 4.18 (3), the kernel $\mathcal{K}$ is locally free of rank $c(z)$ near z. Lemma 4.10 (1) moreover provides a surjection

$$\begin{aligned} \mathcal{I}/\mathcal{I}^2 &\twoheadrightarrow \mathcal{K} \\ g &\mapsto 1 \otimes dg. \end{aligned}$$

Thus there exist an open neighborhood U of z in X and functions $g_1, \ldots, g_{c(z)} \in \mathcal{I}(U)$ with

$$(dg_1, \ldots, dg_{c(z)}) : \mathcal{O}_{Z\cap U}^{\oplus c(z)} \xrightarrow{\sim} \mathcal{K}|_{Z\cap U}.$$

Let $Y = V(g_1, \ldots, g_{c(z)}) \subseteq U$ be the closed subscheme defined by these functions and note that $Z \cap U \subseteq Y$. By Lemma 4.10 (1), for every $z \in Z \cap U$, we have that

$$\begin{aligned} \Omega^1_{Y/k}(z) &= \left(\Omega^1_{U/k}/(dg_1, \ldots, dg_{c(z)})\right)(z) \\ &= \Omega^1_{U/k}(z)/\mathcal{K}(z) \\ &= \Omega^1_{Z/k}(z). \end{aligned}$$

Since also $\dim_z(Y) \geq \dim_z(Z)$, this means that Y is smooth and of the same dimension as Z in every point $z \in Z \cap U$. By the integrality of local rings of smooth k-schemes (which follows from Theorem 4.18 (2)), this means that $Z \cap U \to Y$ is the inclusion of a union of connected components, and the proof is complete. □

5. Invariant differential forms

5.1. **Lie groups.** Let G be a real Lie group of dimension n with identity element e. We write $\mathcal{O}_G$ for the sheaf of smooth functions on G, and Ω^1_G for the sheaf of differential 1-forms. Note that Ω^1_G is locally free of rank n as $\mathcal{O}_G$-module. In fact, we will see in this section that $\Omega^1_G \cong \mathcal{O}_G^{\oplus n}$ and that the global generators can be chosen to be translation invariant differential forms:

Definition 5.1. Given an element $g \in G$, we denote by $\ell_g, r_g : G \xrightarrow{\sim} G$ the left and right translation maps

$$\ell_g(h) = gh, \quad r_g(h) = hg.$$

A differential form $\omega \in \Omega^1_G(G)$ is called left translation invariant if $\ell_g^*(\omega) = \omega$ for all $g \in G$. It is called right translation invariant if $r_g^*(\omega) = \omega$ for all $g \in G$.

For every point $g \in G$, we denote by $\Omega^1_G(g) = \mathbb{R} \otimes_{g,\mathcal{O}_G} \Omega^1_G$ the fiber of Ω^1_G in g. For a smooth function $f \in \mathcal{O}_G(U)$ defined on an open neighborhood U of g we denote by $df(g)$ the image of the differential df in $\Omega^1_G(g)$. (This notation should not lead to confusion because it would not make sense to first evaluate f in g and then take differential.) If

$$x_1, \ldots, x_n : U \xrightarrow{\sim} U' \subset \mathbb{R}^n$$

are coordinate functions on U, then $\Omega^1_U = \mathcal{O}_U dx_1 \oplus \ldots \oplus \mathcal{O}_U dx_n$. In particular, $dx_1(g)$, …, $dx_n(g)$ provide a basis of $\Omega^1_G(g)$.

Example 5.2. (1) Let $G = (\mathbb{R}, +)$ with coordinate function x. The invariant differential forms on G are precisely those of the form λdx, $\lambda \in \mathbb{R}$. Namely, a differential form $f(x)dx \in \Omega^1_G(G)$ is translation invariant if and only if for all $t \in \mathbb{R}$,

$$(\ell_t^*)(f(x)dx) = f(x+t)d(x+t) = f(x+t)dx \overset{!}{=} f(x)dx.$$

That is, we need $f(x+t) = f(x)$ for all $x, t \in \mathbb{R}$, meaning f is constant.

(2) Let $G = (\mathbb{R}^\times, *)$ with coordinate x. The invariant differential forms on G are precisely those of the form $\lambda \frac{dx}{x}$, $\lambda \in \mathbb{R}$. Namely, $f(x)dx$ satisfies

$$f(xt)d(tx) = tf(xt)dx \overset{!}{=} f(x)dx$$

for all $t \neq 0$ if and only if f is a scalar multiple of the function $1/x$.

Proposition 5.3. *For every $\omega_e \in \Omega^1_G(e)$, there exists a unique left translation invariant differential form $\omega \in \Omega^1_G(G)$ such that $\omega(e) = \omega_e$.*

Proof. (1) Uniqueness. In the current manifold context, taking all the fibers $\omega(g)$ of a differential form ω defines an injection

$$\Omega^1_G(G) \hookrightarrow \prod_{g \in G} \Omega^1_G(g). \tag{5.1}$$

Moreover, $\ell_g^* : \Omega^1_G(g) \xrightarrow{\sim} \Omega^1_G(e)$. So there is at most one left translation invariant form with $\omega(e) = \omega_e$ and this form has to be pointwise given by $\omega(g) = (\ell_g^*)^{-1}(\omega_e)$. We need to see that the datum $\big((\ell_g^*)^{-1}(\omega_e)\big)$ comes from a smooth form on G under (5.1).

(2) Preparations. Denote by $p_1, p_2 : G \times G \to G$ the two projection maps. Observe that

$$\Omega^1_{G\times G} = p_1^*\Omega^1_G \oplus p_2^*\Omega^1_G. \tag{5.2}$$

Namely, if $x_1, \ldots, x_n : U \xrightarrow{\sim} U' \subset \mathbb{R}^n$ and $y_1, \ldots, y_n : V \xrightarrow{\sim} V' \subset \mathbb{R}^n$ are charts, then $x_1, \ldots, x_n, y_1, \ldots, y_n$ are coordinate functions for $U \times V$ and

$$\Omega^1_{U\times V} = \underbrace{\mathcal{O}_{G\times G}dx_1 \oplus \ldots \oplus \mathcal{O}_{G\times G}dx_n}_{p_1^*\Omega^1_G} \oplus \underbrace{\mathcal{O}_{G\times G}dy_1 \oplus \ldots \oplus \mathcal{O}_{G\times G}dy_n}_{p_2^*\Omega^1_G}.$$

Next, for every $g \in G$, there is a diagonal action

$$\begin{aligned} \delta_g : G \times G &\xrightarrow{\sim} G \times G \\ (h_1, h_2) &\longmapsto (h_1 g^{-1}, g h_2). \end{aligned}$$

This is really just the map $r_g^{-1} \times \ell_g = (r_g^{-1} \times \mathrm{id}) \circ (\mathrm{id} \times \ell_g)$. The pullback map

$$(\mathrm{id} \times \ell_g)^*(\Omega^1_{G\times G}) \xrightarrow{\sim} \Omega^1_{G\times G}$$

preserves the decomposition (5.2) in the sense that it restricts to isomorphisms

$$(\mathrm{id} \times \ell_g)^*(p_i^*\Omega^1_G) \xrightarrow{\sim} p_i^*\Omega^1_G, \qquad i = 1, 2.$$

The same applies to $r_g^{-1} \times \mathrm{id}$ and hence also to δ_g. After these preparations, we can prove the proposition.

(3) Existence. Starting with $\omega_e \in \Omega^1_G(e)$, choose an open neighborhood U of e and a differential form $\eta \in \Omega^1_G(U)$ such that $\eta(e) = \omega_e$.[6] The preimage $m^{-1}(U) \subseteq G \times G$ is stable under δ_g for every $g \in G$ because $h_1 h_2 = h_1 g^{-1} g h_2$ for all (h_1, h_2). Let

$$m^*(\eta) = \eta_1 + \eta_2$$

[6] In fact, since we are dealing with smooth forms on real manifolds, we may directly take $U = G$.

be the decomposition into components obtained from (5.2). Since $m\circ\delta_g = m$ for all $g \in G$, and since δ_g^* preserves (5.2), both η_1 and η_2 are δ_g-invariant. Now consider the twisted diagonal

$$\tau : G \longrightarrow G \times G, \quad \tau(h) = (h^{-1}, h)$$

and define $\omega = \tau^*(\eta_2)$. Observe that for all $g \in G$, the following diagram commutes

$$\begin{array}{ccc} G & \xrightarrow{\ell_g} & G \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ G \times G & \xrightarrow{\delta_g} & G \times G. \end{array} \tag{5.3}$$

Hence $\ell_g^*(\omega) = \omega$ for all $g \in G$, meaning ω is left translation invariant. It is left to show that $\omega(e) = \omega_e$.

Consider for this the map $\varepsilon : \{e\} \times G \hookrightarrow G \times G$. On the one hand, for every $\eta_1 \in p_1^*\Omega^1_G$, the pullback differential form $\varepsilon^*(\eta_1)$ vanishes. Thus, we obtain on an open neighborhood of e that

$$\varepsilon^*(\eta_2) = \varepsilon^*(\eta_1 + \eta_2) = \varepsilon^*(m^*(\eta)) = \eta. \tag{5.4}$$

On the other hand, we can make this pullback very explicit: Let $x_1, \ldots, x_n$ be coordinates on G near e. Composing with the two projections, we have coordinates $x_i \circ p_j$ for $G \times G$ near (e, e). In these, η_2 near (e, e) takes the form

$$\eta_2 = \sum_{i=1}^{n} f_i d(x_i \circ p_2) \tag{5.5}$$

for smooth functions $f_1, \ldots, f_n$ defined near (e, e). Now note that $p_2 \circ \tau = \mathrm{id}_G = p_2 \circ \varepsilon$, meaning that

$$\tau^* d(x_i \circ p_2) = dx_i = \varepsilon^* d(x_i \circ p_2).$$

Since $\tau(e) = \varepsilon(e)$ also $f_i(\tau(e)) = f_i(\varepsilon(e))$ for all $i = 1, \ldots, n$. So (5.5) implies that $(\tau^*(\eta_2))(e) = (\varepsilon^*(\eta_2))(e)$. Combining with (5.4), this means

$$\omega_e = \eta(e) \overset{(5.4)}{=} (\varepsilon^*(\eta_2))(e) = (\tau^*(\eta_2))(e) = \omega(e)$$

and the proof is complete. □

Example 5.4. We explain the previous proof in a non-trivial example. Consider $G = SL_2(\mathbb{R})$ with coordinate functions x_{ij}, $i, j \in \{1, 2\}$. (These are related by $x_{11}x_{22} - x_{12}x_{21} = 1$ because we are dealing with the special linear group.) Let us denote by $y_{ij} = x_{ij} \circ p_1$ and $z_{ij} = x_{ij} \circ p_2$ the coordinate functions on $G \times G$. The multiplication map is described by

$$\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} \cdot \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix} = \begin{pmatrix} y_{11}z_{11} + y_{12}z_{21} & \cdots \\ \cdots & \cdots \end{pmatrix}. \tag{5.6}$$

The twisted diagonal map is given by

$$\tau\left(\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}\right) = \left(\begin{pmatrix} x_{22} & -x_{12} \\ -x_{21} & x_{11} \end{pmatrix}, \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}\right). \tag{5.7}$$

Now consider the form $\omega_e = dx_{11}(e)$. An extension to all of G is given by $\eta = dx_{11}$. The formula in (5.6) shows that

$$\begin{aligned} m^*(\eta) = m^*(dx_{11}) &= d(y_{11}z_{11} + y_{12}z_{21}) \\ &= \underbrace{z_{11}dy_{11} + z_{21}dy_{12}}_{\eta_1} + \underbrace{y_{11}dz_{11} + y_{12}dz_{21}}_{\eta_2}. \end{aligned}$$

We obtain from (5.7) that the following form is left invariant:

$$\omega = \tau^*(\eta_2) = x_{22}dx_{11} - x_{12}dx_{21}.$$

Evaluating the coefficients of ω at the identity element $x_{11} = x_{22} = 1$, $x_{12} = x_{21} = 0$, we recover $\omega_e = dx_{11}$ as expected.

5.2. **Invariant differentials of group schemes.** Let $\pi : G \to S$ be a group scheme over S with unit section $e : S \to G$. We have defined the sheaf of Kähler differentials $\Omega^1_{G/S}$ in the previous section. It is a quasi-coherent $\mathcal{O}_G$-module. We first explain what it means for a differential form to be translation invariant.

Definition 5.5. (1) Let T be an S-scheme and let $g \in G(T)$ be a T-valued point of G. Denote by $G_T = T \times_S G$ the base change group scheme over T. We call the morphism

$$\ell_g : G_T \xrightarrow{\sim} G_T, \quad h \longmapsto gh$$

left translation by g. The notation here is meant in the sense of the Yoneda Lemma. That is, ℓ_g is the unique morphism such that for every T-scheme $T' \to T$ and every T'-valued point $h \in G_T(T') = G(T')$, we have $\ell_G(h) = gh$.

(2) Let $\omega \in \Omega^1_{G/S}(G)$ be a differential form. For every S-scheme T, let ω_T denote the pullback $p_G^*(\omega) \in \Omega^1_{G_T/T}(G_T)$, where $p_G : G_T \to G$ is the projection. We call ω left translation invariant if, for every $T \to S$ and every $g \in G(T)$,

$$\ell_g^*(\omega_T) = \omega_T. \tag{5.8}$$

Of course, there are also the right translation $r_g : G_T \xrightarrow{\sim} G_T$ and the notation of ω being right translation invariant. These behave in the exact same way, so we will formulate all our results only for left translation.

Lemma 5.6. *A differential form $\omega \in \Omega^1_{G/S}(G)$ is left translation invariant in the sense of Definition 5.5 if and only if*

$$m^*(\omega) = p_2^*(\omega),$$

where $m, p_2 : G \times_S G \longrightarrow G$ denote the multiplication and second projection, respectively.

Proof. First assume ω is translation invariant. Apply Definition 5.5 to the datum $(T, g) := (G, \mathrm{id})$. By definition, ℓ_{id} is the morphism

$$\begin{array}{ccc} G \times_S G & \xrightarrow{\ell_{\mathrm{id}} = (\mathrm{id}, m)} & G \times_S G \\ & {\scriptstyle p_1} \searrow \quad \swarrow {\scriptstyle p_1} & \\ & G & \end{array} \tag{5.9}$$

and (5.8) states that

$$m^*(\omega) = (\mathrm{id}, m)^*(p_2^*(\omega)) = \ell_g^*(\omega_T) \overset{!}{=} \omega_T = p_2^*(\omega)$$

which we needed to prove.

We now make a general observation. Consider $T \to S$, $\omega \in \Omega^1_{G/S}(G)$, and $g \in G(T)$. Let $u : T' \to T$ be a further morphism and use u to also denote the base change $u : G_{T'} \to G_T$. If (5.8) holds for (T, g), then by base change also

$$\ell_{u^*g}(\omega_{T'}) = u^*(\ell_g^*(\omega_T)) = u^*(\omega_T) = \omega_{T'}$$

which means that (5.8) also holds for $(T', g \circ u)$. But this observation applies to *every* (T, g)! Namely, any such g can be factored as

$$T \xrightarrow{g} G \xrightarrow{\mathrm{id}} G.$$

Thus if (5.8) holds for (G, id), i.e. if $m^*(\omega) = p_2^*(\omega)$, then (5.8) holds for every (T, g) which means that ω is translation invariant. The proof is complete. □

The argument just given is typical in algebraic geometry and called reduction to the universal case. The morphism $\ell_{\mathrm{id}} = (\mathrm{id}, m)$ in (5.9) is called the universal translation. It is universal in the following sense: Given (T, g), the following diagram is cartesian.

$$\begin{array}{ccc} T \times_S G & \xrightarrow{g\times \mathrm{id}} & G \times_S G \\ {\scriptstyle \ell_g}\downarrow & & \downarrow{\scriptstyle (\mathrm{id},m)} \\ T \times_S G & \xrightarrow{g\times \mathrm{id}} & G \times_S G. \end{array}$$

That is, every left translation morphism is a pullback of the universal left translation.

Proposition 5.7. *There exists an isomorphism*

$$\gamma : \pi^* e^* \Omega^1_{G/S} \xrightarrow{\sim} \Omega^1_{G/S} \tag{5.10}$$

which is characterized as follows. Assume that $\omega \in (e^*\Omega^1_{G/S})(U)$ is a section on an open $U \subseteq X$. Then $\gamma(\pi^*\omega) \in \Omega^1_{G/S}(\pi^{-1}U)$ is the unique left translation invariant differential form with $e^*(\gamma(\pi^*\omega)) = \omega$.

Proof. This can be proved with exatly the same construction as for Proposition 5.3. We refer to [1, §4.2] for details. The argument we give here is slightly different and implicitly takes the perspective of descent theory. Also, we will only explain why there is an isomorphism $\pi^* e^* \Omega^1_{G/S} \xrightarrow{\sim} \Omega^1_{G/S}$ and not give the relation with the characterization in terms of invariant differential forms.

Consider again the universal translation

$$\begin{array}{ccc} G \times_S G & \xrightarrow{\ell=(\mathrm{id},\, m)} & G \times_S G \\ & {\scriptstyle p_1}\searrow \quad \swarrow{\scriptstyle p_1} & \\ & G. & \end{array} \tag{5.11}$$

It is an automorphism of the G-scheme $G \times_S G$, where the structure morphism is p_1. In particular, pullback defines an isomorphism of sheaves

$$\varphi = \ell^* : \ell^* \Omega^1_{G\times_S G/G} \xrightarrow{\sim} \Omega^1_{G\times_S G/G}.$$

By Lemma 4.10 (3), we have $\Omega^1_{G\times_S G/G} = p_2^* \Omega^1_{G/S}$. Thus φ is an isomorphism of $\mathcal{O}_{G\times_S G}$-modules

$$\varphi : \ell^* p_2^* \Omega^1_{G/S} \xrightarrow{\sim} p_2^* \Omega^1_{G/S}.$$

Now consider $\varepsilon = (\mathrm{id}, e \circ \pi) : G \to G \times_S G$. Then $p_2 \circ \varepsilon = e \circ \pi$ while $p_2 \circ \ell \circ \varepsilon = \mathrm{id}$. It follows that $\varepsilon^*(\varphi)$ is an isomorphism

$$\varepsilon^*(\varphi) : \Omega^1_{G/S} \xrightarrow{\sim} \pi^* e^* \Omega^1_{G/S}$$

of the kind we wanted to construct. □

Remark 5.8. Let $k = \bar{k}$ be an algebraically closed field and G a reduced k-group scheme of finite type. Then $\omega \in \Omega^1_{G/k}(G)$ is translation invariant if and only if it is invariant under translation by all rational points $G(k)$. If G is an algebraic group such as $GL_{n,k}$, $SO(V)_k$, $Sp_{2g,k}$ etc., then the same formulas as in the Lie group setting apply.

Remark 5.9. Let k be any field and let G be an arbitrary k-group scheme. Write $\Gamma(G, \Omega^1_{G/k})^G$ for the G-invariant forms. Then one can show

$$\begin{aligned} \Gamma(\bar{k} \otimes_k G, \Omega^1_{\bar{k}\otimes_k G/\bar{k}})^{\bar{k}\otimes_k G} &= \bar{k} \otimes_k \Gamma(G, \Omega^1_{G/k})^G \\ \Gamma(G, \Omega^1_{G/k})^G &= \Gamma(G, \Omega^1_{G/k}) \cap \Gamma(\bar{k} \otimes_k G, \Omega^1_{\bar{k}\otimes_k G/\bar{k}})^{\bar{k}\otimes_k G}. \end{aligned} \tag{5.12}$$

In many cases, this allows to reduce the computation of invariant differential forms to algebraically closed fields.

Remark 5.10. Differential forms of degree i are defined by $\Omega^i_{G/S} := \bigwedge^i_{\mathcal{O}_G} \Omega^1_{X/S}$. Everything we have said and proved above also applies to forms of degree i.

5.3. **Applications.**

Corollary 5.11. *Let A be an abelian variety over k of dimension g. Then $\Omega^i_{A/k}$ is free of rank $\binom{g}{i}$.*

Proof. Abelian varieties are smooth schemes by definition. By Theorem 4.18, this implies (equivalent, in fact) that $\Omega^1_{A/k}$ is a vector bundle of degree $g = \dim(A)$. Hence $\Omega^i_{A/k}$ is a vector bundle $\binom{g}{i}$. The pullback $e^*\Omega^i_{A/k}$ is then a vector bundle of that rank over $\operatorname{Spec} k$, and in particular free. Thus $\pi^* e^* \Omega^i_{A/k}$ is free of rank $\binom{g}{i}$. By Proposition 5.7, it is isomorphic to $\Omega^i_{A/k}$ and the proof is complete. □

Corollary 5.12. *Let A be an abelian variety over k and let $\omega \in H^0(A, \Omega^i_{A/k})$ be a differential form on A. Then ω is translation invariant.*

Proof. Let us first note a lemma which we have essentially already proved in §3.2.

Lemma 5.13. *Let X be a proper, smooth, geometrically connected scheme over a field k. Then $k \xrightarrow{\sim} \mathcal{O}_X(X)$.*

Proof. The base change $\bar{k} \otimes_k X$ is proper, smooth, and connected. Thus $\mathcal{O}_{\bar{k}\otimes_k X}(\bar{k} \otimes_k X)$ is a 0-dimensional, reduced $\bar{k}$-algebra with a unique maximal ideal. The only possibility is $\bar{k} \xrightarrow{\sim} \mathcal{O}_{\bar{k}\otimes_k X}(\bar{k} \otimes_k X)$. Since taking global sections commutes with flat base change (see the argument around (3.5)), also $\bar{k} \otimes_k \mathcal{O}_X(X) \xrightarrow{\sim} \mathcal{O}_{\bar{k}\otimes_k X}(\bar{k} \otimes_k X)$. Thus $k \xrightarrow{\sim} \mathcal{O}_X(X)$. □

By Corollary 5.11, $\Omega^i_{A/k}$ is free of rank $\binom{g}{i}$, where $g = \dim(A)$. By Lemma 5.13, this means $\dim H^0(A, \Omega^i_{A/k}) = \binom{g}{i}$. By Proposition 5.7, the subspace of translation invariant differential forms has dimension $\dim_k(e^*\Omega^i_{A/k}) = \binom{g}{i}$, and hence has to be equal to $H^0(A, \Omega^i_{A/k})$. □

6. Elliptic curves are cubics

Let k be a field. In this section, by curve over k, we mean a proper, smooth, geometrically connected k-scheme C of dimension 1. Note that any such C is integral. By Lemma 5.13, $k \xrightarrow{\sim} H^0(C, \mathcal{O}_C)$. By Theorem 4.18, C is a normal scheme.

6.1. **Meromorphic functions and divisors.** Let C be a curve over k and let $\eta \in C$ be the generic point. The local ring $\mathcal{O}_{C,\eta}$ is a field by integrality, and called the field of meromorphic functions on C. (It is equal to $\kappa(\eta)$.) It is of transcendence degree 1 over k. We denote by $\mathcal{M}_C$ the constant sheaf

$$C \supseteq U \longmapsto \mathcal{O}_{C,\eta}.$$

It is a quasi-coherent $\mathcal{O}_C$-module. Let $U \subseteq C$ be an open subset and $x \in U$ be a closed point. By normality, the local ring $\mathcal{O}_{C,x}$ is a DVR. Let

$$\operatorname{ord}_x : \mathcal{M}_C(U) \longrightarrow \mathbb{Z} \cup \{\infty\}$$

be the corresponding valuation on $\mathcal{O}_{C,\eta}$. Concretely, if $t_x \in \mathcal{O}_{C,x}$ is a generator of the maximal ideal, and if $f \in t_x^n \mathcal{O}^\times_{C,x}$, then $\operatorname{ord}_x(f) = n$. We also put $\operatorname{ord}_x(0) = \infty$.

Definition 6.1. (1) The group of divisors on U is the free abelian group generated by the closed points of U, i.e.

$$\mathrm{Div}(U) = \bigoplus_{x \in U \text{ closed}} \mathbb{Z} \cdot [x].$$

(2) The divisor of a meromorphic function $f \in \mathcal{M}_C(U)$ is defined as

$$\mathrm{div}(f) = \sum_{x \in U \text{ closed}} \mathrm{ord}_x(f) \cdot [x].$$

A divisor $D \in \mathrm{Div}(U)$ is called principal if there exists a meromorphic function f with $D = \mathrm{div}(f)$.

It is clear that this defines a group homomorphism

$$\mathrm{div} : \mathcal{M}_C(U)^\times \longrightarrow \mathrm{Div}(U). \tag{6.1}$$

Note that $\mathrm{ord}_x(f) \geq 0$ for all $x \in U$ is equivalent to $f \in \mathcal{O}_C(U)$. Thus the kernel of (6.1) is precisely $\mathcal{O}_C(U)^\times$, because a function $f \in \mathcal{O}_X(U)$ on an open U of a scheme X is invertible if and only if all its stalks are invertible. We next consider functoriality properties of divisors.

Lemma 6.2. *Let $\varphi : C_1 \to C_2$ be a non-constant morphism of curves over k. Then φ is a finite morphism. The pushforward $\varphi_*(\mathcal{O}_{C_1})$ is a locally free $\mathcal{O}_{C_2}$-module.*

Proof. Morphisms between proper schemes are proper, so φ is proper. Hence $\varphi(C_1)$ is closed. It is also connected since C_1 is connected. Since C_2 is irreducible and 1-dimensional, the only closed connected subsets of C_2 are $C_2 = \overline{\{\eta\}}$ and individual closed points. We have excluded the second possibility, so $\varphi(C_1) = C_2$.

Next, for every closed point $y \in C_2$, the fiber $\varphi_1^{-1}(y) \subseteq C_1$ is closed. The closed subsets of C_1 are either finite or all of C_1. The second case is excluded by the previous argument, so the fibers of φ are finite. In this situation, the following, extremely useful statement applies and yields that φ is finite.

Proposition 6.3 ([8, Tag 02LS])**.** *Let $f : X \to S$ be a morphism of schemes. Then f is finite if and only if it is proper and has finite fibers.*

Thus $\varphi_*(\mathcal{O}_{C_1})$ is a coherent $\mathcal{O}_{C_2}$-module. It is torsion free because both C_1 and C_2 are integral and because the map $\mathcal{O}_{C_2,\eta_2} \to \mathcal{O}_{C_1,\eta_1}$ is injective. (This map is the field extension $\kappa(\eta_2) \to \kappa(\eta_1)$ that corresponds to the morphism $\varphi : C_1 \to C_2$ under the equivalence from [5, §24].) By the structure theorem for finitely generated modules over DVRs or Dedekind rings, $\varphi_*(\mathcal{O}_{C_1})$ is locally free as $\mathcal{O}_{C_2}$-module. □

Since C_2 is connected, the rank of $\varphi_*(\mathcal{O}_{C_1})$ as vector bundle is constant. It is called the degree $\deg(\varphi)$ of φ and equals the degree $[\kappa(\eta_1) : \kappa(\eta_2)]$ of the function field extension corresponding to $C_1 \to C_2$.

Let $x \in C_1$ and consider the map of local rings

$$\varphi^* : \mathcal{O}_{C_2,\varphi(x)} \longrightarrow \mathcal{O}_{C_1,x}.$$

It is a finite extension of DVRs. As such, there are a residue field extension degree $f_x := [\kappa(x) : \kappa(\varphi(x))]$ and a ramification index e_x defined by

$$\mathfrak{m}_{\varphi(x)} \mathcal{O}_{C_1,x} = (\mathfrak{m}_x)^{e_x}.$$

Corollary 6.4 (to Proposition 6.3)**.** *Let $\varphi : C_1 \to C_2$ be a non-constant morphism of curves over k. Then for every $y \in C_2$, the fiber $\varphi^{-1}(y)$ has cardinality $\deg(\varphi)$ in the sense that*

$$\sum_{x \in \varphi^{-1}(y)} e_x f_x = \deg(\varphi).$$

Next, a non-constant morphism $\varphi : C_1 \to C_2$ provides pushforward and pullback maps for divisors,

$$\varphi_* : \mathrm{Div}(C_1) \longrightarrow \mathrm{Div}(C_2), \quad \varphi^* : \mathrm{Div}(C_2) \longrightarrow \mathrm{Div}(C_1). \tag{6.2}$$

Pushforward is defined by $\varphi_*([x]) = f_x \cdot [\varphi(x)]$. Pullback is given by

$$\varphi^*([y]) = \sum_{x \in f^{-1}(y)} e_x \cdot [x].$$

Definition 6.5. The degree of a divisor $D = \sum n_x[x] \in \mathrm{Div}(C)$ is the integer

$$\deg(D) = \sum_{x \in C \text{ closed}} n_x \cdot [\kappa(x) : k].$$

Proposition 6.6 (Properties of the divisors)**.** *(1) Let $\varphi : C_1 \to C_2$ be a non-constant morphism of curves over k and let $D_i \in \mathrm{Div}(C_i)$. Then*

$$\deg(\varphi_*(D_1)) = \deg(D_1), \quad \deg(\varphi^*(D_2)) = \deg(\varphi) \cdot \deg(D_2), \quad \varphi_*(\varphi^*(D_2)) = \deg(\varphi) \cdot D_2.$$

(2) Let $f \in \mathcal{M}_C(C)$ be a meromorphic function on C. Then $\deg(\mathrm{div}(f)) = 0$.

We leave the proof as an exercise but give the following hints: Part (1) can be proved from definitions and Corollarly 6.4. Part (2) can be deduced from part (1) as follows. Consider $\mathbb{P}^1_k = \mathbb{A}^1_k \cup \{\infty\}$ with variable t. It is clear that $\mathrm{div}(t) = [0] - [\infty]$ has degree 0. Now apply the next lemma.

Lemma 6.7. *(1) For every non-constant meromorphic function f on C, there exists a unique non-constant morphism $\varphi : C \to \mathbb{P}^1_k$ such that $\varphi^*(t) = f$. This defines a bijection*

$$\kappa(\eta) \setminus k \xrightarrow{\sim} \mathrm{Mor}_k(C, \mathbb{P}^1_k) \setminus k.$$

(2) Let $\varphi : C_1 \to C_2$ be a non-constant morphism of curves over k and let $f_2 \in \kappa(\eta_2)$ be a meromorphic function on C_2. Then

$$\mathrm{div}(\varphi^*(f_2)) = \varphi^*(\mathrm{div}(f_2)).$$

6.2. **Divisors and line bundles.** The theory of algebraic curves relies on the study of their meromorphic functions. We already know that the only meromorphic functios f on C with $\mathrm{ord}_x(f) \geq 0$ for all closed points $x \in C$ are the constant functions $k = H^0(C, \mathcal{O}_C)$. (This also follows from Lemma 6.7; a non-constant meromorphic function defines a surjective morphism $C \to \mathbb{P}^1_k$ and hence has a pole.) Thus, in order to obtain non-trivial meromorphic functions, we need to allow some flexibility with poles which is encapsulated in the next definition.

Definition 6.8. Let $D \in \mathrm{Div}(C)$ be a divisor, say $D = \sum_{x \in C} n_x[x]$. Let $\mathcal{O}_C(D) \subset \mathcal{M}_C$ be the subsheaf

$$\mathcal{O}_C(D)(U) = \{f \in \mathcal{M}_C(U) \mid \mathrm{ord}_x(f) \geq -n_x \text{ for all } x \in U\}. \tag{6.3}$$

Note that $\mathcal{O}_C(D)$ is a line bundle on C. Concretely, let $U = \mathrm{Spec}\, A \subseteq C$ be an affine open subset. Then

$$\mathfrak{a} = \prod_{x \in U \text{ closed}} \mathfrak{m}_x^{-n_x} \subset \kappa(\eta) = \mathrm{Frac}(A) \tag{6.4}$$

is a fractional ideal of the Dedekind ring A, and $\mathcal{O}_C(D)|_U = \mathcal{O}_U \cdot \mathfrak{a}$. We call a divisor $D = \sum_{x \in C} n_x[x]$ effective and write $D \geq 0$ if $n_x \geq 0$. By definition,

$$D \text{ effective} \quad \Longleftrightarrow \quad \mathcal{O}_C(-D) \subseteq \mathcal{O}_C.$$

In this case, $\mathcal{O}_C(-D)$ is an ideal sheaf and defines a closed subscheme $V(\mathcal{O}_C(-D))$. It is the unique finite closed subscheme $Z \subset C$ such that for all closed points $x \in C$,

$$\mathrm{len}_{\mathcal{O}_{C,x}}(\mathcal{O}_{Z,x}) = n_x.$$

In this way, there are bijections

$$\{\text{Effective } D\} \xleftrightarrow{\sim} \{\text{Non-zero ideal sheaves } \mathcal{I} \subset \mathcal{O}_C\} \xleftrightarrow{\sim} \{\text{Finite } Z \subset C\}.$$

Extending (6.4), we also obtain

$$\begin{aligned} \mathrm{Div}(C) &\xrightarrow{\sim} \{\mathcal{O}_C\text{-line bundles } \mathcal{L} \subset \mathcal{M}_C\} \\ D &\longmapsto \mathcal{O}_C(D). \end{aligned} \tag{6.5}$$

Lemma 6.9. *The map $D \mapsto \mathcal{O}_C(D)$ is compatible with multiplication and inversion of fractional ideals in the sense that*

$$\mathcal{O}_C(D_1 + D_2) = \mathcal{O}_C(D_1) \cdot \mathcal{O}_C(D_2), \quad \mathcal{O}_C(-D) = \mathcal{O}_C(D)^{-1}. \tag{6.6}$$

Here, for a line bundle $\mathcal{L} \subseteq \mathcal{M}_C$, we defined

$$\mathcal{L}^{-1} = \{f \in \mathcal{M}_C \mid f\mathcal{L} \subseteq \mathcal{O}_C\}.$$

Moreover, the multiplication map defines an isomorphism

$$\mathcal{O}_C(D_1) \otimes_{\mathcal{O}_C} \mathcal{O}_C(D_2) \xrightarrow{\sim} \mathcal{O}_C(D_1 + D_2). \tag{6.7}$$

Proof. This follows from (6.4) and the properties of fractional ideals over Dedekind rings. □

Definition 6.10 (Picard group)**.** Let $\mathrm{Pic}(C)$ denote the group of isomorphism classes of line bundles on C. The group structure is given by the tensor product.

Theorem 6.11. *Taking the isomorphism class of $\mathcal{O}_C(D)$ defines a surjective group homomorphism*

$$\begin{aligned} \mathcal{O}_C(-) : \mathrm{Div}(C) &\longrightarrow \mathrm{Pic}(C) \\ D &\longmapsto [\mathcal{O}_C(D)]. \end{aligned} \tag{6.8}$$

Its kernel is precisely the subgroup $\{\mathrm{div}(f) \mid f \in \mathcal{M}_C(C)\}$ of principal divisors.

Proof sketch. The group homomorphism property is (6.7). Let $\mathcal{L}$ be any line bundle on C. Let $U \subseteq C$ be an open such that $\mathcal{L}|_U \cong \mathcal{O}_U$. Then we can define an embedding

$$\mathcal{L}|_U \xrightarrow{\sim} \mathcal{O}_U \hookrightarrow \mathcal{M}_U.$$

Because of the integrality of C, there exists a unique extension to an embedding $\mathcal{L} \hookrightarrow \mathcal{M}$. Thus $\mathcal{L} \cong \mathcal{O}_C(D)$ for some divisor D, see (6.5). This proves the surjectivity of (6.8).

Assume that $\mathcal{O}_C(D) \cong \mathcal{O}_C$. This means there exists a meromorphic function $f \in \Gamma(C, \mathcal{O}_C(D)) \subset \mathcal{M}_C(C)$ that generates $\mathcal{O}_C(D)$ in the sense $\mathcal{O}_C(D) = \mathcal{O}_C \cdot f$. Then $D = \mathrm{div}(f)$. □

Corollary 6.12. *There exists a unique definition of the degree of a line bundle that fits into the diagram*

$$\begin{array}{ccc} \mathrm{Div}(C) & \twoheadrightarrow & \mathrm{Pic}(C) \\ & \searrow^{\deg} & \downarrow{\scriptstyle \deg} \\ & & \mathbb{Z}. \end{array}$$

Proof. Theorem 6.11 states that $\mathrm{Div}(C) \to \mathrm{Pic}(C)$ is surjective and has kernel precisely the principal divisors. By Proposition 6.6 (2), principal divisors have degree 0. □

Example 6.13. Consider $C = \mathbb{P}^1_k$ with coordinate function t and let $x \neq \infty$ be a closed point. It corresponds to a prime ideal $(p) \subset k[t]$. Observe that

$$\sum_{i=0}^{n} a_i t^i = (t^{-1})^{-n} \sum_{i=0}^{n} a_i t^{n-i}$$

which implies that $\deg_\infty(p) = \deg(p)$. Thus

$$\mathrm{div}(p) = [x] - \deg(p) \cdot [\infty]$$

and hence $\mathcal{O}_{\mathbb{P}^1}(x) \cong \mathcal{O}_{\mathbb{P}^1}([\kappa(x) : k] \cdot [\infty])$. We hence obtain that $\mathcal{L} \cong \mathcal{O}_{\mathbb{P}^1}(\deg(\mathcal{L}) \cdot [\infty])$ for every line bundle on $\mathbb{P}^1$ which means that

$$\deg : \mathrm{Pic}(\mathbb{P}^1_k) \xrightarrow{\sim} \mathbb{Z}.$$

6.3. **Cech Cohomology.**

Motivation 6.14. Let $\mathcal{L}$ be a line bundle on a curve C. The main problem is to determine the space of global sections $\Gamma(C, \mathcal{L})$. If we choose a divisor D with $\mathcal{L} \cong \mathcal{O}_C(D)$, this problem is equivalent to finding all meromorphic functions on C whose pole orders are bounded by D. The main idea now is as follows. Consider the simplest possible case, namely $D = [x]$ for a rational point $x \in C(k)$. There is an exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_C \longrightarrow \mathcal{O}_C([x]) \longrightarrow i_{x,*}k \longrightarrow 0.$$

(The first map here is the inclusion $\mathcal{O}_C \subset \mathcal{O}_C([x])$ which comes by definition (6.3). For the second map, we have chosen a basis for the skyscraper sheaf $\mathcal{O}_C([x])/\mathcal{O}_C$ concentrated at x.) Taking global sections is left exact, so we obtain an exact sequence

$$0 \longrightarrow k \longrightarrow \Gamma(C, \mathcal{O}_C([x])) \xrightarrow{\alpha} k \tag{6.9}$$

and in particular find $\dim_k \Gamma(C, \mathcal{O}_C([x])) \leq 2$. Equality holds if and only if α is surjective. So how can we decide whether or not α has this property? The systematic answer is given by continuing (6.9) to a long exact sequence of cohomology groups. The purpose of this section is to introduce this concept.

Let X be a quasi-compact and separated scheme. Let $X = U_1 \cup \ldots \cup U_m$ be an open affine covering of X. We set $\mathcal{U} = (U_i)_{1 \leq i \leq m}$. For every subset $I \subseteq \{1, \ldots, m\}$, the intersection $U_I := \bigcap_{i \in I} U_i$ is again affine by the separatedness.

Definition 6.15. Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. Set $C^i(\mathcal{U}, \mathcal{F}) = \prod_{|I|=i+1} \Gamma(U_I, \mathcal{F})$. The Cech complex of $\mathcal{F}$ (for the given open covering $\mathcal{U}$) is the complex

$$C^\bullet(\mathcal{U}, \mathcal{F}) : \quad 0 \longrightarrow C^0(\mathcal{U}, \mathcal{F}) \xrightarrow{d^0} C^1(\mathcal{U}, \mathcal{F}) \xrightarrow{d^1} C^1(\mathcal{U}, \mathcal{F}) \longrightarrow \ldots \tag{6.10}$$

with differential defined as follows. Given $(f_I)_{|I|=i+1} \in C^i(\mathcal{U}, \mathcal{F})$, the $J = \{j_0, \ldots, j_{i+1}\}$-component of $d^i(f_I)$ is given by

$$\big(d^i(f_I)\big)_J = \sum_{r=0}^{i+1} (-1)^r f_{J \setminus \{j_r\}}|_{U_J}.$$

The i-th Cech cohomology group of $\mathcal{F}$ is defined as the i-th cohomology group of the Cech complex of $\mathcal{F}$. It can be shown to be independent of $\mathcal{U}$. We denote it by

$$H^i(X, \mathcal{F}) = \ker(d^i)/\mathrm{Im}(d^{i-1}).$$

Remark 6.16. Cohomology of quasi-coherent sheaves can more generally be defined in terms of derived functors, see e.g. [6]. The two definitions agree for separated and quasi-compact schemes, [8, Tag 01XD].

We now give some examples.

Example 6.17. The 0-th cohomology group is

$$H^0(X, \mathcal{F}) = \ker \left[\prod_{1 \leq i \leq m} \mathcal{F}(U_i) \longrightarrow \prod_{1 \leq i < j \leq m} \mathcal{F}(U_i \cap U_j) \right]$$

which equals $\mathcal{F}(X)$ by the sheaf axiom.

Example 6.18. Consider the open covering $\mathbb{P}^1_k = \operatorname{Spec} k[t] \cup \operatorname{Spec} k[t^{-1}]$. The Cech complex for $\mathcal{O}_{\mathbb{P}^1}(n \cdot [\infty])$ becomes

$$\begin{aligned} 0 \longrightarrow k[t] \oplus t^n k[t^{-1}] &\longrightarrow k[t, t^{-1}] \longrightarrow 0 \\ (f, g) &\longmapsto g - f. \end{aligned} \tag{6.11}$$

The global sections of $\mathcal{O}_{\mathbb{P}^1}(n \cdot [\infty])$ are given by the kernel and equal

$$H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(n \cdot [\infty])) = \begin{cases} \bigoplus_{i=0}^{n} k \cdot t^i & \text{if } n \geq 0 \\ 0 & \text{otherwise.} \end{cases}$$

The first cohmology group of $\mathcal{O}_{\mathbb{P}^1}(n \cdot [\infty])$ is given by the cokernel

$$H^1(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(n \cdot [\infty])) = \begin{cases} 0 & \text{if } n \geq -1 \\ \bigoplus_{i=n+1}^{-1} k \cdot t^i & \text{otherwise.} \end{cases}$$

Lemma 6.19. *Assume that X has a covering by n affines. Then, for every quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$,*

$$H^i(X, \mathcal{F}) = 0, \qquad i \geq n.$$

Proof. Clear because if $\mathcal{U} = \{U_1, \ldots, U_n\}$ is an affine open covering of X, then $C^i(\mathcal{U}, \mathcal{F}) = 0$ for all $i \geq n$. □

Example 6.20. Assume that X is affine and $\mathcal{F}$ any. Then $H^i(X, \mathcal{F}) = 0$ for $i \geq 1$.

Example 6.21. Assume that X is a closed subscheme of the n-dimensional projective space $\mathbb{P}^n_R$ over an affine scheme $\operatorname{Spec} R$. Then X is covered by the affines $D_+(T_i) \cap X$, where $T_0, \ldots, T_n$ are the coordinates on $\mathbb{P}^n$. Hence $H^i(X, \mathcal{F}) = 0$ for $i \geq n + 1$.

The following provides a much stronger statement. Recall that the support of a sheaf $\mathcal{F}$ on X is defined by

$$\operatorname{Supp}(\mathcal{F}) = \{x \in X \mid \mathcal{F}|_U \neq 0 \text{ for every open neighborhood } U \text{ of } x\}.$$

It is a closed subset of X.

Theorem 6.22 (Grothendieck, [8, Tag 02UZ])**.** *Assume that X is noetherian and that $\dim(\operatorname{Supp}(\mathcal{F})) \leq d$. Then $H^i(X, \mathcal{F}) = 0$ for all $i \geq d + 1$.*

For the proof, one first has to compare our definition of cohomology with the derived functor definition for abelian sheaves. Then one can apply the noetherian induction argument as in [8, Tag 02UZ]. We will only use this result for the next corollary:

Corollary 6.23. *Let C be a curve over some field k. Then, for every quasi-coherent $\mathcal{O}_C$-module $\mathcal{F}$,*

$$H^i(C, \mathcal{F}) = 0, \qquad i \neq 0, 1.$$

6.4. **The long exact sequence.** Given a complex of abelian groups (or in any abelian category)

$$K^\bullet: \quad \ldots \longrightarrow K^{i-1} \xrightarrow{d^{i-1}} K^i \xrightarrow{d^i} K^{i+1} \longrightarrow \ldots,$$

we denote by $H^i(K^\bullet) := \ker(d^i)/\operatorname{Im}(d^{i-1})$ its i-th cohomology group. Recall the following important and simple principle from homological algebra. Assume we are given a short exact sequences of complexes

$$0 \longrightarrow A^\bullet \xrightarrow{\alpha^\bullet} B^\bullet \xrightarrow{\beta^\bullet} C^\bullet \longrightarrow 0.$$

That is, assume we are given homomorphisms $\alpha^i : A^i \to B^i$ and $\beta^i : B^i \to C^i$ such that the below diagram commutes and has exact columns.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & A^{i-1} & \longrightarrow & A^i & \longrightarrow & A^{i+1} & \longrightarrow & \dots \\
 & & \downarrow{\scriptstyle \alpha^{i-1}} & & \downarrow{\scriptstyle \alpha^i} & & \downarrow{\scriptstyle \alpha^{i+1}} & & \\
\dots & \longrightarrow & B^{i-1} & \longrightarrow & B^i & \longrightarrow & B^{i+1} & \longrightarrow & \dots \\
 & & \downarrow{\scriptstyle \beta^{i-1}} & & \downarrow{\scriptstyle \beta^i} & & \downarrow{\scriptstyle \beta^{i+1}} & & \\
\dots & \longrightarrow & C^{i-1} & \longrightarrow & C^i & \longrightarrow & C^{i+1} & \longrightarrow & \dots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{6.12}$$

Then there is a straightforward diagram chase that defines a connection morphism $\delta^i : H^i(C^\bullet) \to H^{i+1}(A^\bullet)$. These connect to a long exact sequence

$$\dots \xrightarrow{\delta^{i-1}} H^i(A^\bullet) \xrightarrow{\alpha^i} H^i(B^\bullet) \xrightarrow{\beta^i} H^i(C^\bullet) \xrightarrow{\delta^i} H^{i+1}(A^\bullet) \xrightarrow{\alpha^{i+1}} H^{i+1}(B^\bullet) \xrightarrow{\beta^{i+1}} \dots \tag{6.13}$$

Exercise 6.24. If you have not done so before, then carry out the construction of $\delta^\bullet$ and prove the exactness of (6.13).

Proposition 6.25. *Let $0 \to \mathcal{A} \xrightarrow{\alpha} \mathcal{B} \xrightarrow{\beta} \mathcal{C} \to 0$ be an exact sequence of quasi-coherent $\mathcal{O}_X$-modules. Then there are natural connection homomorphisms $\delta^i : H^i(X, \mathcal{C}) \to H^{i+1}(X, \mathcal{A})$ that define a long exact sequence*

$$\begin{aligned}\dots \xrightarrow{\delta^{i-1}} H^i(X, \mathcal{A}) \xrightarrow{\alpha^i} H^i(X, \mathcal{B}) \xrightarrow{\beta^i} H^i(X, \mathcal{C}) \\ \xrightarrow{\delta^i} H^{i+1}(X, \mathcal{A}) \xrightarrow{\alpha^{i+1}} H^{i+1}(X, \mathcal{B}) \xrightarrow{\beta^{i+1}} \dots .\end{aligned} \tag{6.14}$$

Proof. Let $\mathcal{U}$ be an open affine covering of X as in Definition 6.15. Recall that for an affine scheme Y, the global sections functor $\mathcal{F} \mapsto \Gamma(Y, \mathcal{F})$ is exact. Applying this to each of the affine schemes U_I in Definition 6.15 and taking products, we obtain exact sequences

$$0 \longrightarrow C^i(\mathcal{U}, \mathcal{A}) \xrightarrow{\alpha} C^i(\mathcal{U}, \mathcal{B}) \xrightarrow{\beta} C^i(\mathcal{U}, \mathcal{C}) \longrightarrow 0.$$

(The indicated morphisms could more precisely be written as $C^i(\mathcal{U}, \alpha)$ and $C^i(\mathcal{U}, \beta)$, viewing $C^i(\mathcal{U}, -)$ as a functor from sheaves to abelian groups.) These define an exact sequence of complexes

$$0 \longrightarrow C^\bullet(\mathcal{U}, \mathcal{A}) \xrightarrow{\alpha} C^\bullet(\mathcal{U}, \mathcal{B}) \xrightarrow{\beta} C^\bullet(\mathcal{U}, \mathcal{C}) \longrightarrow 0.$$

Now we apply the construction from (6.12) and (6.13). □

Let $X, \mathcal{U}$ and $\mathcal{F}$ be as in Definition 6.15. If X is a scheme over $\operatorname{Spec} R$ for some ring R, then $C^\bullet(\mathcal{U}, \mathcal{F})$ is a complex of R-modules. Hence $H^i(X, \mathcal{F})$ is an R-module for every $i \geq 0$.

Theorem 6.26. *Let $X \to \operatorname{Spec} R$ be a proper scheme over a noetherian ring R. Let $\mathcal{F}$ be a coherent[7] $\mathcal{O}_X$-module. Then $H^i(X, \mathcal{F})$ is a finitely generated R-module for every $i \geq 0$.*

[7] Since R is noetherian and X finite type over R, also X is noetherian. Then coherent $\mathcal{O}_X$-modules are the same as locally finitely generated quasi-coherent $\mathcal{O}_X$-modules.

Proof for curves $C \to \operatorname{Spec} k$. We leave the general case to the AG 2 lecture, see [6, Theorem 14.2]. Here, we give an argument for curves over fields. It is not completely self-contained but illustrates some properties of coherent sheaves on curves.

Let $\mathcal{F}$ be a coherent $\mathcal{O}_C$-module. We need to show that $H^1(C, \mathcal{F})$ is a finite-dimensional k-vector space.[8] There is a coherent subsheaf $\mathcal{F}_{\mathrm{tor}} \subseteq \mathcal{F}$ whose sections $\mathcal{F}_{\mathrm{tors}}(U)$ on an open U are the torsion elements of $\mathcal{F}(U)$. Since $\operatorname{Supp}(\mathcal{F}_{\mathrm{tors}})$ is finite, we know by direct computation or from Theorem 6.26 that $H^1(C, \mathcal{F}_{\mathrm{tors}}) = 0$. Passing to the cohomology exact sequence for

$$0 \longrightarrow \mathcal{F}_{\mathrm{tors}} \longrightarrow \mathcal{F} \longrightarrow \mathcal{F}/\mathcal{F}_{\mathrm{tors}} \longrightarrow 0,$$

we have reduced to showing that $H^1(C, \mathcal{F}/\mathcal{F}_{\mathrm{tors}}) = 0$. Note that $\mathcal{E} = \mathcal{F}/\mathcal{F}_{\mathrm{tors}}$ is torsion-free. Let $\varphi : C \to \mathbb{P}^1_k$ be any non-constant morphism. We have seen (Lemma 6.2) that φ is necessarily finite. Thus $\varphi_*(\mathcal{E})$ is a torsion-free coherent $\mathcal{O}_{\mathbb{P}^1_k}$-module. By normality of $\mathbb{P}^1_k$, it is locally free. By the classification of vector bundles on $\mathbb{P}^1_k$ (this is where the proof is not self-contained), there exist integers $a_1, \dots, a_r \in \mathbb{Z}$, unique up to ordering, such that

$$\varphi_*(\mathcal{E}) \xrightarrow{\sim} \bigoplus_{i=1}^{r} \mathcal{O}_{\mathbb{P}^1_k}(a_i).$$

By Example 6.18, we obtain that

$$H^1(\mathbb{P}^1, \varphi_*(\mathcal{E})) = \bigoplus_{i=1}^{r} H^1(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1_k}(a_i))$$

is a finite-dimensional k-vector space. It is only left to apply the next lemma. □

Lemma 6.27. *Let $\varphi : X \to Y$ be an affine morphism of quasi-compact, separated schemes. Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. Then $H^i(X, \mathcal{F}) = H^i(Y, \varphi_*(\mathcal{F}))$ for every $i \geq 0$.*

Proof. Let $\mathcal{V} = \{V_1, \dots, V_m\}$ be an open affine covering of Y. Since φ is affine by assumption, $\varphi^{-1}(\mathcal{V}) = \{\varphi^{-1}(V_1), \dots, \varphi^{-1}(V_m)\}$ is an open affine covering of X. By definition of pushforward and since $\varphi^{-1}(\bigcap_{i\in I} V_I) = \bigcap_{i\in I} \varphi^{-1}(V_i)$ for all sets of indices I, we have $C^i(\mathcal{V}, \varphi_*(\mathcal{F})) = C^i(\varphi^{-1}(\mathcal{V}), \mathcal{F})$. The lemma now follows from Definition 6.15. □

So far, our discussion has been mostly formal. Using the vanishing result Theorem 6.22, we have learnt that we can extend (6.9) into an exact sequcen

$$0 \longrightarrow k \longrightarrow \Gamma(C, \mathcal{O}_C([x])) \xrightarrow{\alpha} k \longrightarrow H^1(C, \mathcal{O}_C) \longrightarrow H^1(C, \mathcal{O}_C([x])) \longrightarrow 0.$$

We next have to understand how to control the occurring H^1-terms. This will be the topic of the next section.

6.5. **Riemann–Roch and Serre duality.**

Definition 6.28. Let X be a proper k-scheme and let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module. The Euler–Poincaré characteristic of $\mathcal{F}$ is the integer

$$\chi(\mathcal{F}) := \sum_{i=0}^{\dim X} (-1)^i \, h^i(\mathcal{F}), \qquad h^i(\mathcal{F}) = \dim_k H^i(X, \mathcal{F}).$$

Lemma 6.29. *Let $0 \to \mathcal{E} \to \mathcal{F} \to \mathcal{G} \to 0$ be a short exact sequence of coherent $\mathcal{O}_X$-modules. Then*

$$\chi(\mathcal{F}) = \chi(\mathcal{E}) + \chi(\mathcal{G}).$$

[8] Theorem 6.26 also makes the non-trivial statement that $H^0(X, \mathcal{F})$ is a finitely generated R-module. We have already used this statement for $R = k$ when looking at the global section $\mathcal{O}_A(A)$ of abelian varieties during the proof of Lemma 3.3. The argument we give for $H^1(C, \mathcal{F})$ here also applies to $H^0(C, \mathcal{F})$.

Proof. By Proposition 6.25, there is a long exact cohomology sequence

$$0 \longrightarrow H^0(X,\mathcal{E}) \longrightarrow H^0(X,\mathcal{F}) \longrightarrow H^0(X,\mathcal{G}) \longrightarrow \dots$$
$$\dots \longrightarrow H^{\dim X}(X,\mathcal{E}) \longrightarrow H^{\dim X}(X,\mathcal{F}) \longrightarrow H^{\dim X}(X,\mathcal{G}) \longrightarrow 0. \quad (6.15)$$

Now apply the next lemma. □

Lemma 6.30. *Let $\dots \to V^i \xrightarrow{d^i} V^{i+1} \to \dots$ be an exact sequence of finite-dimensional k-vector spaces with only finitely many non-zero terms. Then*

$$\sum_{i\in\mathbb{Z}} (-1)^i \dim(V^i) = 0.$$

Proof. For every $i \in \mathbb{Z}$, we have $\dim(V^i) = \dim(\mathrm{Im}(d^i)) + \dim(\ker(d^i))$. By exactness of the sequence, we also have $\dim(\mathrm{Im}(d^i)) = \dim(\ker(d^{i+1}))$. Taking the alternating sum, we obtain a term-by-term cancellation. □

Theorem 6.31 (Riemann–Roch)**.** *Let C be a curve over k and let $\mathcal{L}$ be a line bundle on C. Then*

$$\chi(\mathcal{L}) = \chi(\mathcal{O}_C) + \deg(\mathcal{L}).$$

Proof. Assume that D is an effective divisor and let $Z = V(\mathcal{O}_C(-D))$ be the corresponding finite closed subscheme of C. In particular, there is an exact sequence of coherent $\mathcal{O}_X$-modules

$$0 \longrightarrow \mathcal{O}_C(-D) \longrightarrow \mathcal{O}_C \longrightarrow \mathcal{O}_Z \longrightarrow 0$$

and thus $\chi(\mathcal{O}_C(-D)) = \chi(\mathcal{O}_C) - \chi(\mathcal{O}_Z)$. Since Z is finite, $H^1(X,\mathcal{O}_Z) = 0$ and then

$$\chi(\mathcal{O}_Z) = h^0(\mathcal{O}_Z) = \deg(D).$$

We find $\chi(\mathcal{O}_C(-D)) = \chi(\mathcal{O}_C) - \deg(D)$ as claimed. For a general divisor D, we can write $D = D_+ - D_-$ with effective divisors D_+ and D_-. We have already seen $\chi(\mathcal{O}_C(-D_-)) = \chi(\mathcal{O}_C) - \deg(D_-)$. Set $Z_+ = V(\mathcal{O}_C(-D_+))$. Tensoring the exact sequence

$$0 \longrightarrow \mathcal{O}_C(-D_+) \longrightarrow \mathcal{O}_C \longrightarrow \mathcal{O}_{Z_+} \longrightarrow 0$$

with $\mathcal{O}_C(D)$, we obtain an exact sequence

$$0 \longrightarrow \mathcal{O}_C(-D_-) \longrightarrow \mathcal{O}_C(D) \longrightarrow \mathcal{O}_C(D) \otimes_{\mathcal{O}_X} \mathcal{O}_{Z_+} \longrightarrow 0.$$

The rightmost term is a locally free $\mathcal{O}_{Z_+}$-module of rank 1. Since Z_+ is finite, it is free (i.e. isomorphic to $\mathcal{O}_{Z_+}$). We get

$$\chi(\mathcal{O}_C(D)) = \chi(\mathcal{O}_C(-D_-)) + \deg(D_+) = \chi(\mathcal{O}_C) + \deg(D).$$

□

The significance of the Riemann–Roch theorem is that it ensures the existence of global sections of line bundles of sufficiently high degree (depending on the curve). Namely,

$$h^0(\mathcal{L}) \geq h^0(\mathcal{L}) - h^1(\mathcal{L}) \overset{\text{Thm. } 6.31}{=} 1 - h^1(\mathcal{O}_C) + \deg(\mathcal{L})$$

where the right hand side is positive as soon as $\deg(\mathcal{L}) \geq h^1(\mathcal{O}_C)$. This reasoning gets extra powerful once we also take control of $h^1(\mathcal{O}_C)$ and $h^1(\mathcal{L})$ with Serre duality:

Theorem 6.32 (Serre duality, [6, Theorem 17.11])**.** *Let X be a proper smooth d-dimensional scheme over a field k. Let $\omega_{X/k} := \Omega^d_{X/k}$ denote its line bundle of degree d forms. Then for every vector bundle $\mathcal{E}$ on X and every $i \geq 0$, there is a perfect pairing*

$$H^i(X,\mathcal{E}) \times H^{d-i}(X,\mathcal{E}^\vee \otimes \omega_{X/k}) \longrightarrow k.$$

Definition 6.33. Let C be a curve. By Serre duality, $H^1(C, \mathcal{O}_C) \xrightarrow{\sim} H^0(C, \Omega^1_{C/K})^\vee$. The integer

$$g(C) := h^1(\mathcal{O}_C) = h^0(\Omega^1_{C/k})$$

is called the genus of C. Observe that $\chi(\mathcal{O}_C) = 1 - g(C)$, so Riemann–Roch can be rewritten as

$$\chi(\mathcal{L}) = 1 - g(C) + \deg(\mathcal{L}). \tag{6.16}$$

Corollary 6.34. *Let C be a curve of genus g. Then $\deg(\Omega^1_{C/k}) = 2g - 2$.*

Proof. By Serre duality, $h^1(\Omega^1_{C/K}) = h^0(\mathcal{O}_C) = 1$. Then by the weak Riemann–Roch Theorem, we find

$$\begin{aligned}\deg(\Omega^1_{C/k}) &= h^0(\Omega^1_{C/k}) - h^1(\Omega^1_{C/k}) - \chi(\mathcal{O}_C)\\ &= g - 1 - (1 - g)\\ &= 2g - 2.\end{aligned}$$

□

Example 6.35. (1) The genus of $\mathbb{P}^1_k$ is 0. This follows from Example 6.18 where we have computed $g(\mathbb{P}^1_k) = h^1(\mathcal{O}_{\mathbb{P}^1}) = 0$. One may also compute directly (exercise) that $\Omega^1_{\mathbb{P}^1} \cong \mathcal{O}_{\mathbb{P}^1}(-2)$. Then the degree formula from Corollary 6.34 implies $g(\mathbb{P}^1_k) = 0$.

(2) Let E/k be an elliptic curve. We have shown in §5.3 that $\Omega^1_{E/k} \cong \mathcal{O}_E$. Hence

$$g(E) = h^0(\Omega^1_{E/k}) = h^0(\mathcal{O}_E) = 1.$$

Proposition 6.36. *Let $F \in k[X, Y, Z]$ be a homogeneous polynomial of degree d and let $X = V_+(F) \subseteq \mathbb{P}^2_k$ be the closed subscheme defined by F. Then $\chi(\mathcal{O}_X) = 1-(d-1)(d-2)/2$. In particular, if X is a smooth curve, then $g(X) = (d-1)(d-2)/2$.*

Proof. The ideal sheaf defining X is a line bundle on $\mathbb{P}^2$ isomorphic to $\mathcal{O}_{\mathbb{P}^2}(-d)$. (Recall that, in general, $\mathbb{Z} \xrightarrow{\sim} \mathrm{Pic}(\mathbb{P}^n_k)$ via $r \mapsto \mathcal{O}_{\mathbb{P}^n}(r)$.) So there is an exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^2}(-d) \longrightarrow \mathcal{O}_{\mathbb{P}^2} \longrightarrow \mathcal{O}_X \longrightarrow 0$$

and hence $\chi(\mathcal{O}_X) = \chi(\mathcal{O}_{\mathbb{P}^2}) - \chi(\mathcal{O}_{\mathbb{P}^2}(-d))$. Now we may simply substitute the general result for the cohomology of the line bundles $\mathcal{O}_{\mathbb{P}^n_k}(d)$ to finish the proof, see e.g. [6, Propositions 13.3 and 13.4]. Another argument would be as follows. Consider the exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^2}(-1) \longrightarrow \mathcal{O}_{\mathbb{P}^2} \longrightarrow \mathcal{O}_{\mathbb{P}^1} \longrightarrow 0.$$

For every $d \in \mathbb{Z}$, we may tensor it by $\mathcal{O}_{\mathbb{P}^2}(d)$ while also using that $\mathcal{O}_{\mathbb{P}^2}(d)|_{\mathbb{P}^1} \cong \mathcal{O}_{\mathbb{P}^1}(d)$ to obtain an exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^2}(d-1) \longrightarrow \mathcal{O}_{\mathbb{P}^2}(d) \longrightarrow \mathcal{O}_{\mathbb{P}^1}(d) \longrightarrow 0.$$

It follows that

$$\begin{aligned}\chi(\mathcal{O}_{\mathbb{P}^2}(d)) - \chi(\mathcal{O}_{\mathbb{P}^2}(d-1)) &= \chi(\mathcal{O}_{\mathbb{P}^1}(d))\\ &= 1 + d.\end{aligned}$$

The second equality is from Riemann–Roch for $\mathbb{P}^1_k$ or from Example 6.18. Now assume that we know by a small computation that $h^1(\mathcal{O}_{\mathbb{P}^2}) = h^2(\mathcal{O}_{\mathbb{P}^2}) = 0$ and hence that $\chi(\mathcal{O}_{\mathbb{P}^2}) = 1$. Then we get by induction that

$$\chi(\mathcal{O}_{\mathbb{P}^2}(d)) = \frac{(d+1)(d+2)}{2}.$$

Setting $d = -\deg(F)$ proves the proposition. □

Proposition 6.36 also gives an obstruction for embedding curves into $\mathbb{P}^2_k$. For example no smooth curve of genus 2 can be embedded into $\mathbb{P}^2_k$.

6.6. **Projective embeddings of curves.** Recall from [5, Theorem 10.7] that the functor of points description of $\mathbb{P}^n$ is

$$\mathbb{P}^n(S) = \left\{ (\mathcal{L}, \alpha) \,\middle|\, \begin{array}{c} \mathcal{L} \text{ a line bundle on } S \\ \alpha : \mathcal{O}_S^{n+1} \twoheadrightarrow \mathcal{L} \text{ a surjection} \end{array} \right\} / \cong .$$

Here, $(\mathcal{L}, \alpha)$ and $(\mathcal{L}', \alpha')$ are isomorphic if there exists an isomorphism $\gamma : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ with $\alpha' = \gamma \circ \alpha$.

Theorem 6.37. *Let C be a curve of genus g, and let $\mathcal{L}$ be a line bundle on C.*
(1) If $\deg(\mathcal{L}) \geq 2g-1$, then $h^1(\mathcal{L}) = 0$ and, in particular,

$$h^0(\mathcal{L}) = 1 - g + \deg(\mathcal{L}).$$

(2) If $\deg(\mathcal{L}) \geq 2g$, then $\mathcal{L}$ is globally generated. Any choice of k-basis $s_0, \ldots, s_n \in H^0(C, \mathcal{L})$ hence defines a morphism

$$[s_0 : \ldots : s_n] : C \longrightarrow \mathbb{P}^n_k. \tag{6.17}$$

(3) If $\deg(\mathcal{L}) \geq 2g+1$, then the map (6.17) is a closed immersion.

Proof. (1) A general statement is that if $\mathcal{M}$ is a line bundle on C with $\deg(\mathcal{M}) < 0$, then $h^0(\mathcal{M}) = 0$. Namely, if $f \in \Gamma(C, \mathcal{O}_C(D))$ is a non-zero meromorphic function, then $\operatorname{div}(f) \geq -D$ which implies that $0 \leq \deg(D)$. Another argument is as follows: A non-zero global section $s \in \Gamma(C, \mathcal{L})$ defines an injective map $s : \mathcal{O}_C \to \mathcal{L}$. We obtain an exact sequence

$$0 \longrightarrow \mathcal{O}_C \xrightarrow{s} \mathcal{L} \longrightarrow \mathcal{L}/\mathcal{O}_C \longrightarrow 0$$

where the rightmost term is finite. Then

$$\deg(\mathcal{L}) = \chi(\mathcal{L}) - \chi(\mathcal{O}_C) = h^0(\mathcal{L}/\mathcal{O}_C) \geq 0.$$

After these generalities, let us consider a line bundle $\mathcal{L}$ with $\deg(\mathcal{L}) \geq 2g-1$. By Serre duality, $h^1(\mathcal{L}) = h^0(\Omega^1_{C/k} \otimes \mathcal{L}^{-1})$. By assumption,

$$\deg(\Omega^1_{C/k} \otimes \mathcal{L}^{-1}) = 2g - 2 - \deg(\mathcal{L}) < 0$$

and hence $h^1(\mathcal{L}) = h^0(\Omega^1_{C/k} \otimes \mathcal{L}^{-1}) = 0$ as was to be shown.

(2) Being globally generated means that the natural map

$$\mathcal{O}_C \otimes_k \Gamma(C, \mathcal{L}) \longrightarrow \mathcal{L} \tag{6.18}$$

is surjective. Equivalently, for every closed point $x \in C$, there exists a global section $s \in \Gamma(C, \mathcal{L})$ whose image $s(x) \in \mathcal{L}(x)$ is non-zero. This may be rephrased in terms of exact sequences. Given $x \in C$, consider the natural sequence

$$0 \longrightarrow \mathcal{O}_C(-[x]) \longrightarrow \mathcal{O}_C \longrightarrow i_{x,*}\kappa(x) \longrightarrow 0.$$

Tensoring with $\mathcal{L}$, we obtain an exact sequence

$$0 \longrightarrow \mathcal{L}(-[x]) \longrightarrow \mathcal{L} \longrightarrow i_{x,*}\mathcal{L}(x) \longrightarrow 0.$$

Here, by definition, $\mathcal{L}(D) := \mathcal{O}_C(D) \otimes_{\mathcal{O}_C} \mathcal{L}$. From the long exact cohomology sequence, we obtain that $\Gamma(C, \mathcal{L}) \to \mathcal{L}(x)$ is surjective if and only if

$$H^1(C, \mathcal{L}(-[x])) \longrightarrow H^1(C, \mathcal{L}) \tag{6.19}$$

is injective. After these generalities, we give the proof of (2). First observe that (6.18) can be checked after the faithfully flat extension $\bar{k} \otimes_k -$. That is, we may assume k algebraically closed. Then, using the assumption $\deg(\mathcal{L}) \geq 2g$, for every closed point $x \in C$,

$$\deg(\mathcal{L}(-[x])) = \deg(\mathcal{L}) - 1 \geq 2g - 1.$$

It follows from (1) that $h^1(\mathcal{L}(-[x])) = 0$, so (6.19) is injective, which is what we needed to show.

(3) Let $\mathcal{L}$ be a globally generated line bundle on C, let $s_0, \ldots, s_n \in \Gamma(C, \mathcal{L})$ be a basis, and let $\varphi = [s_0 : \ldots : s_n] : C \to \mathbb{P}^n_k$ be the so-defined morphism. Being a closed immersion can be checked after faithfully flat base change, so we may assume $k = \bar{k}$. Also observe that if φ is an injective map of sets, then it is a closed immersion of topological spaces by properness. Our first aim is to show prove this injectivity.

The points of $\mathbb{P}^n(k)$ are in bijection with the n-dimensional subspaces of $\Gamma(C, \mathcal{L})$. Namely, to $[x_0 : \ldots : x_n]$ associate all those $\sum_{i=0}^n a_i s_i$ such that $\sum_{i=0}^n x_i a_i = 0$. In this description, a closed point $x \in C$ (recall $\kappa(x) = k$ since we assumed $k = \bar{k}$) gets mapped to the subspace

$$\varphi(x) = \{s \in \Gamma(C, \mathcal{L}) \mid \mathcal{L}(x) \ni s(x) = 0\}.$$

Let $x \neq y$ be two closed points on C. We see that $\varphi(x) \neq \varphi(y)$ if and only if there exists a section $s \in \Gamma(C, \mathcal{L})$ such that $s(x) = 0$ but $s(y) \neq 0$.

Now we use the assumption $\deg(\mathcal{L}) \geq 2g + 1$. By (1) applied to $\mathcal{L}$, $\mathcal{L}(-[x])$ and $\mathcal{L}(-[x] - [y])$, we see that

$$h^0(\mathcal{L}(-[x])) = h^0(\mathcal{L}) - 1, \qquad h^0(\mathcal{L}(-[x] - [y])) = h^0(\mathcal{L}) - 2.$$

In other words, there exists a section $s \in \Gamma(C, \mathcal{L})$ with $s(x) = 0$ but $s(y) \neq 0$, which is what we wanted to show.

In order to see that φ is a closed immersion of schemes, we additionally need to show that for every closed point $x \in C$, the map of local rings $\mathcal{O}_{\mathbb{P}^n_k, \varphi(x)} \to \mathcal{O}_{C,x}$ is surjective. Since the residue fields of x and $\varphi(x)$ are both k by our assumption $k = \bar{k}$, this is equivalent to $\mathfrak{m}_{\varphi(x)} \to \mathfrak{m}_x$ being surjective. Since φ is finite (Proposition 6.3) and the involved rings noetherian, $\mathfrak{m}_x$ is a finite $\mathcal{O}_{\mathbb{P}^n_k, \varphi(x)}$-module. By Nakayama's Lemma, surjectivity follows once we prove that $\mathfrak{m}_{\varphi(x)} \to \mathfrak{m}_x / \mathfrak{m}_{\varphi(x)} \mathfrak{m}_x$ is surjective. The target is a cyclic module because $\mathcal{O}_{C,x}$ is a DVR, so it suffices to prove that $\mathfrak{m}_{\varphi(x)} \to \mathfrak{m}_x / \mathfrak{m}_x^2$ is surjective.

After a change of basis, we may assume that $s_0(x) \neq 0$ while $s_1(x) = \ldots = s_n(x) = 0$. Then locally near x, the morphism φ is described as Spec of the k-algebra map

$$\varphi^* : k[\sigma_1, \ldots, \sigma_n] \longrightarrow \mathcal{O}_{C,x}, \quad \sigma_i \longmapsto s_i / s_0 \in \mathfrak{m}_x.$$

Thus $\mathfrak{m}_{\varphi(x)} \to \mathfrak{m}_x / \mathfrak{m}_x^2$ is surjective if and only if there exists $i \in \{1, \ldots, n\}$ with $\varphi^*(\sigma_i) \notin \mathfrak{m}_x^2$, which means that $s_i \notin \Gamma(C, \mathcal{L}(-2[x]))$.

Now we use again that $\deg(\mathcal{L}) \geq 2g + 1$. Just as before, we obtain from (1) that

$$h^0(\mathcal{L}(-2[x])) = h^0(\mathcal{L}(-[x])) - 1,$$

meaning there exists $i \in \{1, \ldots, n\}$ with $s_i \notin \Gamma(C, \mathcal{L}(-2[x]))$ as was to be shown. □

Corollary 6.38. *Let E be an elliptic curve. Then there exists a cubic homogeneous polynomial $F \in k[X, Y, Z]$ and an isomorphism*

$$E \xrightarrow{\sim} V_+(F) \subseteq \mathbb{P}^2_k.$$

Proof. Let $e \in E(k)$ denote the neutral element. Recall from Example 6.35 that $g(E) = 1$. Apply Theorem 6.37 to the line bundle $\mathcal{L} = \mathcal{O}_E(3[e])$, which has degree $3 = 2g(E) + 1$. Part (1) states that $h^0(\mathcal{L}) = 3$. Part (3) states that any choice of basis $s_0, s_1, s_2 \in \Gamma(E, \mathcal{L})$ provides a closed immersion

$$\varphi = [s_0 : s_1 : s_2] : E \hookrightarrow \mathbb{P}^2_k.$$

By Proposition 6.36, the homogeneous polynomial F such that $\varphi(E) = V_+(F)$ has degree 3. □

Here is a more constructive variant: Let $\mathcal{L} = \mathcal{O}_E([e])$ which has degree 1. Theorem 6.37 (1) states that $h^0(\mathcal{L}) = 1$, meaning $\Gamma(C, \mathcal{L}) = k$. The theorem furthermore states that $h^0(\mathcal{L}^{\otimes 2}) = 2$. Hence there exists a non-constant meromorphic function $x \in \Gamma(E, \mathcal{L}^{\otimes 2}) \setminus k$.

We have $\mathrm{ord}_e(x) = 2$ since $x \notin \Gamma(C, \mathcal{L})$. By the same reasoning, there exists a meromorphic function $y \in \Gamma(E, \mathcal{L}^{\otimes 3}) \backslash \Gamma(E, \mathcal{L}^{\otimes 2})$. In particular, $\mathrm{ord}_e(y) = 3$. In this way, we have chosen a basis

$$1, x, y \in \Gamma(E, \mathcal{L}^{\otimes 3}). \tag{6.20}$$

Now consider the products

$$1, x, y, x^2, xy, x^3, y^2 \in \Gamma(E, \mathcal{L}^{\otimes 6}).$$

These define 7 elements of a 6-dimensional vector space. Hence there exists a non-trivial linear combination

$$u_0 y^2 + a_1 xy + a_3 y = a_0 x^3 + a_2 x^2 + a_4 x + a_6. \tag{6.21}$$

The monomials y^2 and x^3 are the only ones with pole order 6 at e, the others all have smaller pole order at e. So necessarily $u_0, a_0 \in k^\times$. Scaling x and y by u_0/a_0, we obtain choices for x, y for which $u_0 = a_0 = 1$. We obtain that E is isomorphic to the projective curve defined by an equation of the form[9]

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{6.22}$$

If $\mathrm{char}(k) \neq 2$, then we may replace y by $y - (a_1 x + a_3)/2$ to arrange $a_1 = a_3 = 0$. If $\mathrm{char}(k) \neq 3$, then we may also replace x by $x - a_2/3$ to assume $a_2 = 2$. In this way, we may bring (6.22) into the simplified form

$$y^2 = x^3 + ax + b. \tag{6.23}$$

We have now proved that every elliptic curve can be described as the (closure in $\mathbb{P}^2_k$ of the) vanishing locus of a general Weierstrass equation (6.22). If $\mathrm{char}(k) \neq 2, 3$, then it suffices to consider simplified Weierstrass equations (6.23). Note that for the chosen coordinates $1, x, y$ in (6.20), $e = [0 : 1 : 0]$ because $\mathrm{ord}_e(y) > \mathrm{ord}_e(x), \mathrm{ord}_e(1)$.

7. Marked cubics are elliptic curves

We have now shown that any elliptic curve is a curve of genus 1 (Proposition 4.2), and that any curve of genus 1 that has a rational point is a cubic plane curve (Corollary 6.38). We also know that every smooth plane cubic is of genus 1 (Proposition 6.36). The following result will complete the cycle.

Theorem 7.1. *Let E/k be a curve of genus 1 and let $e \in E(k)$ be a rational point. Then there is a unique way to make E into a group scheme with identity element e.*

We already proved uniqueness in §3.2. Namely, let (A, m_1) be an abelian variety over k with identity $e \in A(k)$, and let $m_2 : A \times_k A \to A$ be another group scheme structure that also has identity e. The identity map $\mathrm{id}_A : A \to A$ preserves e. By Corollary 3.8, it is a group scheme homomorphism $(A, m_1) \to (A, m_2)$. This means $m_1 = m_2$.

7.1. **The group structure on $E(k)$.** Let (E, e) be as in Theorem 7.1. We first explain how to define a group structure on $E(k)$. The construction of the group structure on $E(S)$ will use the exact same ideas, but requires the setup of additional machinery.

Corollary 7.2. *(1) Let E/k be a curve of genus 1 and let $\mathcal{L}$ be a line bundle on E with $\deg(\mathcal{L}) \geq 1$. Then $h^1(\mathcal{L}) = 0$ and $h^0(\mathcal{L}) = \deg(\mathcal{L})$.*

(2) Let E/k be a curve of genus 1 and let $e \in E(k)$ be a rational point. Given a line bundle $\mathcal{L}$ of degree d on E, there exists a unique rational point $z \in E(k)$ such that $\mathcal{L} \cong \mathcal{O}_E([z] + (d-1)[e])$.

[9] The a_i in (6.21) and (6.22) are not the same.

Proof. Part (1) is a special case of Theorem 6.37 (1). For part (2), consider a line bundle $\mathcal{L}$ of degree 1. By (1), there exists a non-zero global section $s \in \Gamma(E, \mathcal{L})$, unique up to scaling by $k^\times$. Since $\deg(\mathcal{L}) = 1$ and since the Euler characteristic is additive in exact sequences (Lemma 6.29), the cokernel

$$\operatorname{coker}[s : \mathcal{O}_E \longrightarrow \mathcal{L}]$$

is a skyscraper sheaf of length 1. This means it is of the form $i_{z,*}k$ for a (unique) rational point $z \in E(k)$. Twisting the exact sequence

$$0 \longrightarrow \mathcal{O}_E \xrightarrow{s} \mathcal{L} \longrightarrow i_{z,*}k \longrightarrow 0$$

by $\mathcal{L}^{-1}$, we see that $\mathcal{L}^{-1} \cong \mathcal{O}_E(-[z])$. Equivalently, $\mathcal{L} \cong \mathcal{O}_E([z])$. Uniqueness of z is the observation that this procedure recovers z when applied to the line bundle $\mathcal{O}_E([z])$. In this way, we have shown (2) for line bundles of degree 1. For a general line bundle $\mathcal{L}$, we apply the previous reasoning to $\mathcal{L} \otimes \mathcal{O}_E([e])^{\otimes(1-\deg(\mathcal{L}))}$. □

Construction 7.3. Let $x, y \in E(k)$ be two rational points. The line bundle $\mathcal{L} = \mathcal{O}_E([x]+[y]-[e])$ has degree 1. By Corollary 7.2, there exists a point $z \in E(k)$ with $\mathcal{L} \cong \mathcal{O}_E([z])$. We define $x + y := z$.

Let $\operatorname{Pic}^0(E) \subseteq \operatorname{Pic}(E)$ denote the subgroup of isomorphism classes of line bundles of degree 0.

Proposition 7.4. *The map $x \mapsto \mathcal{O}_E([x]-[e])$ defines a bijection*

$$E(k) \xrightarrow{\sim} \operatorname{Pic}^0(E).$$

By definition, the group structure on $E(k)$ is the one compatible with this bijection.

Proof. As explained in Construction 7.3, every line bundle $\mathcal{L}$ of degree 1 is of the form $\mathcal{O}_E([x])$ for a unique rational point $x \in E(k)$. Shifting by the fixed point $e \in E(k)$, we find that every line bundle of degree 0 is of the form $\mathcal{O}_E([x]-[e])$ for a unique $x \in E(k)$. This proves the claimed bijection. Tensoring $\mathcal{O}_E([x]+[y]-[e]) \cong \mathcal{O}_E([x+y])$ by $\mathcal{O}_E([e])^{-1}$, we find

$$\mathcal{O}_E([x]-[e]) \otimes \mathcal{O}_E([y]-[e]) \;\cong\; \mathcal{O}_E([x+y]-[e]) \tag{7.1}$$

which shows the compatibility with group structures. □

In other words, the group structure on $E(k)$ is defined by identifying it with $\operatorname{Pic}^0(E)$. Our aim in this section is to upgrade the definition of $\operatorname{Pic}^0(E)$ to a group scheme Pic^0_E, and to construct an isomorphism $E \xrightarrow{\sim} \operatorname{Pic}^0_E$. The group structure on E is then defined by pullback from that of Pic^0_E.

7.2. **Cohomology and base change.** We formulate the general problem. Let $X \to \operatorname{Spec} A$ be a separated morphism with X quasi-compact, and let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. Let further $\mathcal{U}$ be a finite affine covering of X. Recall that we defined the cohomology groups of $\mathcal{F}$ as the cohomology groups of the Cech complex:

$$H^i(X, \mathcal{F}) := H^i(C^\bullet(\mathcal{U}, \mathcal{F})).$$

Now consider an A-algebra B and the Cartesian square

$$\begin{array}{ccc} X_B & \longrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} B & \longrightarrow & \operatorname{Spec} A. \end{array}$$

The fiber product of affines is affine, so $\mathcal{U}_B = \{B \otimes_A U \mid U \in \mathcal{U}\}$ is an affine open covering of X_B. Moreover, denoting by $\mathcal{F}_B = B \otimes_A \mathcal{F}$ the pullback of $\mathcal{F}$ to X_B, we find

$$C^\bullet(\mathcal{U}_B, \mathcal{F}_B) = B \otimes_A C^\bullet(\mathcal{U}, \mathcal{F}). \tag{7.2}$$

In general, if $K^\bullet$ is a complex of A-modules, then there is a natural map of complexes of A-modules $K^\bullet \to B \otimes_A K^\bullet$. It induces a map in cohomology $H^i(K^\bullet) \to H^i(B \otimes_A K^\bullet)$. Extending scalars to B, we obtain a natural map

$$B \otimes_A H^i(K^\bullet) \longrightarrow H^i(B \otimes_A K^\bullet).$$

We are interested in this construction for (7.2) in which case we obtain a natural morphism

$$B \otimes_A H^i(X, \mathcal{F}) \longrightarrow H^i(X_B, \mathcal{F}_B). \tag{7.3}$$

Problem 7.5. The map (7.3) is called the base change morphism of cohomology. The general task is to understand the properties of this map in dependence on X, $\mathcal{F}$ and $A \to B$. In particular, the problem is to decide under which conditions (7.3) is an isomorphism.

Example 7.6 (Flat base change)**.** Assume that $A \to B$ is flat. It is well-known that then $B \otimes_A H^i(K^\bullet) \xrightarrow{\sim} H^i(B \otimes_A K^\bullet)$ for every complex of A-modules $K^\bullet$. In particular, for all X and $\mathcal{F}$

$$B \otimes_A H^i(X, \mathcal{F}) \xrightarrow{\sim} H^i(X_B, \mathcal{F}_B).$$

This argument was already used for H^0 around (3.5). In particular, we see that taking cohomology is local on the base in the sense that for every $u \in A$,

$$A[u^{-1}] \otimes_A H^i(X, \mathcal{F}) \xrightarrow{\sim} H^i(A[u^{-1}] \otimes_A X, A[u^{-1}] \otimes_A \mathcal{F}). \tag{7.4}$$

Definition 7.7. Identity (7.4) allows to glue cohomology. Let $f : X \to S$ be a quasi-compact separated morphism, and let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. The i-th higher direct image $(R^i f_*)(\mathcal{F})$ of $\mathcal{F}$ is the quasi-coherent $\mathcal{O}_S$-module such that for every open affine $\operatorname{Spec} A \subseteq S$,

$$R^i f_* \mathcal{F}|_{\operatorname{Spec} A} = H^i(X|_{\operatorname{Spec} A}, \mathcal{F}|_{\operatorname{Spec} A})^\sim,$$

and where the gluing maps are given by (7.3).

Example 7.8 (The universal degree 0 line bundle on an elliptic curve)**.** Let E be an elliptic curve over a field k with identity element e. Set $S = E$ and $E_S = S \times_k E$. Let $\delta : S \to E_S$ be the diagonal, and let

$$\gamma : S \xrightarrow{(\mathrm{id}, e)} E_S$$

be the constant map e. Then δ and γ are sections of the separated morphism $E_S \to S$, and hence closed immersions. Let $\Delta, \Gamma \subseteq E_S$ denote their image closed subschemes. Both are of codimension 1 in the smooth k-scheme E_S. By Corollary 4.26, they are locally defined by a single non-zero equation. In other words, the defining ideal sheaves $\mathcal{I}_\Delta$ and $\mathcal{I}_\Gamma$ are line bundles on E_S. Set $\mathcal{L} = \mathcal{I}_\Delta^{-1} \otimes \mathcal{I}_\Gamma$ and let $\pi : E_S \to S$ denote the projection map. Our aim is to study the base change properties of the pushforward $\pi_*(\mathcal{L})$. Concretely, let $s : \operatorname{Spec} \kappa \to S$ be a κ-valued point where κ/k is a field extension. We want to understand the natural map

$$(\pi_* \mathcal{L})(s) \longrightarrow H^0(E_\kappa, \mathcal{L}(s)) \tag{7.5}$$

in dependence on the point s.

Analysis of the situation. The fiber $\mathcal{L}(s) := \kappa \otimes_{\mathcal{O}_S} \mathcal{L}$ is a line bundle on the base change elliptic curve $E_\kappa = \kappa \otimes_k E$. How to describe it? First, $\otimes$-products and pullbacks always commute, so we have $\mathcal{L}(s) = \mathcal{I}_\Delta(s)^{-1} \otimes \mathcal{I}_\Gamma(s)$. Next, it is clear that $\mathcal{I}_\Gamma(s) = \mathcal{O}_{E_\kappa}(-[e])$ because $\mathcal{I}_\Gamma$ is by definition the pullback $\mathcal{O}_S \otimes_k \mathcal{O}_E(-[e])$. Finally, consider the exact sequence

$$0 \longrightarrow \mathcal{I}_\Delta \longrightarrow \mathcal{O}_{E_S} \longrightarrow \mathcal{O}_\Delta \longrightarrow 0.$$

The projection $\pi|_\Delta : \Delta \to S$ is an isomorphism, in particular flat. A local computation then shows that the following natural surjection is, in fact, an isomorphism:

$$\mathcal{I}_\Delta(s) = \mathcal{O}_{E_\kappa} \otimes_{q^{-1}\mathcal{O}_{E_S}} q^{-1}\mathcal{I}_\Delta \xrightarrow{\sim} \mathcal{I}_{\Delta(s)}.$$

Here, $q : E_\kappa \longrightarrow E$ denotes the projection. So we obtain that $\mathcal{I}_\Delta(s) = \mathcal{O}_{E_\kappa}(-[s])$ and finally

$$\mathcal{L}(s) \cong \mathcal{O}_{E_\kappa}([s] - [e]).$$

Note/Recall that a degree 0 line bundle $\mathcal{O}_C(D)$ on a curve C has a non-zero global section f (a meromorphic function on C) if and only if $D = \operatorname{div}(f)$ is a principal divisor. We have seen in Proposition 7.4 that $\mathcal{O}_{E_\kappa}([s]-[e]) \cong \mathcal{O}_{E_\kappa}$ if and only if $s = e$. So $H^0(E_\kappa, \mathcal{O}_{E_\kappa}([s]-[e])) \neq 0$ if and only if $s = e$.

Conclusion. On the one hand, apply the above to the generic point $s = \operatorname{Spec}\kappa(\eta) \to S$, which is unequal e. Using Example 7.6, we see that

$$\begin{aligned}(\pi_*\mathcal{L})_\eta &\overset{\text{Ex. } 7.6}{=} \pi_*(\mathcal{L}_\eta) \\ &= H^0(E_{\kappa(\eta)}, \mathcal{O}_{E_{\kappa(\eta)}}([s] - [e])) \\ &= 0.\end{aligned} \tag{7.6}$$

Since $\mathcal{O}_{E_S}$ is stalk-by-stalk a torsion-free $\mathcal{O}_S$-module, we also know that the pushforward $\pi_*\mathcal{L}$ is a torsion-free $\mathcal{O}_S$-module. We have just seen $(\pi_*\mathcal{L})_\eta = 0$, so we conclude $\pi_*\mathcal{L} = 0$.

On the other hand, consider the point $s = e : \operatorname{Spec} k \to S$. Then $\mathcal{L}(s) = \mathcal{O}_E([e]-[e]) = \mathcal{O}_E$. In particular, the natural map

$$0 = (\pi_*\mathcal{L})(e) \longrightarrow H^0(E, \mathcal{L}(e)) \cong k$$

is not an isomorphism.

We will come back to Example 7.8 repeatedly below. Let us now state the technical result that is at the heart of most cohomology and base change considerations for proper morphisms. Recall that a complex $K^\bullet$ of A-modules is called perfect

(1) if $K^i \neq 0$ only for finitely many $i \in \mathbb{Z}$ and
(2) if each K^i is a finitely generated projective A-module.

Theorem 7.9. *Let A be a noetherian ring and let X be a proper A-scheme. Let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module that is flat over A. Then there exists a perfect complex $K^\bullet$ that represents the cohomology of $\mathcal{F}$ in the sense that for every A-algebra B,*

$$H^i(B \otimes_A K^\bullet) \xrightarrow{\sim} H^i(X_B, \mathcal{F}_B). \tag{7.7}$$

Moreover, let $d = \max_{s \in \operatorname{Spec} A} \dim(\operatorname{Supp} \mathcal{F}(s))$. Then $K^\bullet$ can be chosen such that $K^i \neq 0$ only for $i \in [0, d]$.

The two assumptions X proper and $\mathcal{F}$ flat over A are crucial for the statement. Example/Exercise: Consider $X = \operatorname{Spec}\mathbb{F}_p \to \operatorname{Spec}\mathbb{Z}$ with $\mathcal{F} = \mathcal{O}_X$ and show that there is no perfect complex of $\mathbb{Z}$-modules that represents cohomology in the sense of (7.7).

Proof sketch. Choose a finite affine open covering $\mathcal{U}$ of X. The Cech complex $C^\bullet(\mathcal{U}, \mathcal{F})$ is a complex of A-modules that represents cohomology in the sense that for all $A \to B$,

$$H^i(X_B, \mathcal{F}_B) = H^i(B \otimes_A C^\bullet(\mathcal{U}, \mathcal{F})).$$

This was noted in (7.2). Moreover, $C^\bullet(\mathcal{U}, \mathcal{F})$ is concentrated in the finitely many degrees $[0, |U| - 1]$. Theorem 6.26 also states that it has finitely generated cohomology groups. Using only these properties, there is an inductive construction (starting from the highest degree) of a perfect complex $K^\bullet$ together with a quasi-isomorphism

$$K^\bullet \xrightarrow{\sim} C^\bullet(\mathcal{U}, \mathcal{F}).$$

(Recall that a map of complexes $K^\bullet \to C^\bullet$ is a quasi-isomorphism if it induces isomorphisms of all cohomology groups.) By the flatness of $\mathcal{F}$ over A, all terms $C^i(\mathcal{U}, \mathcal{F})$ are flat A-modules (i.e. acyclic for every $B \otimes_A -$). This implies that for every A-algebra B,

$$B \otimes_A K^\bullet \xrightarrow{\sim} B \otimes_A C^\bullet(\mathcal{U}, \mathcal{F})$$

is a quasi-isomorphism as well and in particular that

$$H^i(B \otimes_A K^\bullet) \xrightarrow{\sim} H^i(X_B, \mathcal{F}_B)$$

as desired. Now one may use Theorem 6.22 to cut down $K^\bullet$ to be concentrated in degrees $[0, \max_{s \in \operatorname{Spec} A} \dim(\operatorname{Supp} \mathcal{F}(s))]$. □

Example 7.10. Consider again Example 7.8. Let $e \in \operatorname{Spec} A \subseteq S$ be an affine open neighborhood of e. Theorem 7.9 states that there exists a two term complex $K^0 \to K^1$ of finite projective A-modules such that for every point $s : \operatorname{Spec} \kappa \to \operatorname{Spec} A$,

$$H^0(E_\kappa, \mathcal{L}(s)) = \quad \ker[\kappa \otimes_A K^0 \longrightarrow \kappa \otimes_A K^1]$$

$$H^1(E_\kappa, \mathcal{L}(s)) = \operatorname{coker}[\kappa \otimes_A K^0 \longrightarrow \kappa \otimes_A K^1].$$

We know that $h^0(\mathcal{L}(s))$ and $h^1(\mathcal{L}(s))$ are non-zero only for $s = e$ in which case both equal 1 by Serre duality. Using that A is a Dedekind domain, this implies that d is injective with cokernel a cyclic module $A/\mathfrak{m}_e^r$ for some $r \geq 1$. With an additional argument, one can show that $r = 1$. Gluing this result for H^1 over all of S, we find that the first cohomology of $\mathcal{L}$ is a skyscraper sheaf,

$$(R^1\pi_*)(\mathcal{L}) \xrightarrow{\sim} i_{e,*}(k).$$

7.3. **General applications.**

Corollary 7.11 (The Euler characteristic is locally constant)**.** *Let $X \to S$ be a proper morphism to a locally noetherian scheme, and let $\mathcal{F}$ be an $\mathcal{O}_S$-flat coherent $\mathcal{O}_X$-module. Then the fiber-wise Euler characteristic*

$$S \longrightarrow \mathbb{Z}, \quad s \longmapsto \chi(\mathcal{F}(s))$$

is locally constant.

Proof. Local constancy can be proven locally. So we may assume $S = \operatorname{Spec} A$ for a noetherian ring A. Let $K^\bullet$ be a perfect complex of A-modules that represents cohomology of $\mathcal{F}$ in the sense of Theorem 7.9. Then, for all $s \in S$,

$$\begin{aligned}\chi(s) &= \sum_{i \in \mathbb{Z}} (-1)^i \dim_{\kappa(s)} H^i(X(s), \mathcal{F}(s)) \\ &= \sum_{i \in \mathbb{Z}} (-1)^i \dim_{\kappa(s)} H^i(\kappa(s) \otimes_A K^\bullet) \\ &= \sum_{i \in \mathbb{Z}} (-1)^i \operatorname{rk}_{\mathcal{O}_{S,s}}(K^i_s).\end{aligned}$$

The rank of a finite projective module is locally constant, so the argument is complete. □

Definition 7.12. A morphism $\pi : X \to S$ is said to be smooth if it is flat, locally of finite presentation and if for every $s \in S$, the fiber $\pi(s) : X(s) \to \operatorname{Spec} \kappa(s)$ is smooth.

If π is smooth, then $\Omega^1_{X/S}$ is a locally free $\mathcal{O}_X$-module. Its rank in a point $x \in X$ equals the local dimension $\dim_x(X(\pi(x)))$ of the fiber of x.

Let $\mathbb{P}$ by some type of algebraic variety object. A general philosophy in algebraic geometry is that a family of objects of type $\mathbb{P}$ parametrized by a scheme S is a flat morphism to S that is fiber-by-fiber of type $\mathbb{P}$. We give some examples.

Definition 7.13. Let S be a scheme.

(1) A curve over S is a proper smooth morphism $\pi : X \to S$ with 1-dimensional geometrically connected fibers.

(2) An elliptic curve over S is a proper smooth S-group scheme (E, m) with 1-dimensional connected fibers.

(3) An abelian scheme over S is a proper smooth S-group scheme (A, m) with connected fibers.

Example 7.14. A typical case is when the base S provides the parameters for a system of equations. Here is the example of the universal plane curve of degree d. Consider the polynomial ring $R = \mathbb{Z}[a_{ijk},\ i+j+k=d]$ and set $S = \operatorname{Spec} R$. Define

$$X := V_+\big(\textstyle\sum_{i,j,k}\ a_{ijk}\, x^i y^j z^k\big) \subset \mathbb{P}^2_S, \qquad \pi : X \longrightarrow S. \tag{7.8}$$

There exist maximal open subschemes $S_{\mathrm{sm}} \subseteq S_{\mathrm{flat}} \subseteq S$ such that the restrictions

$$\pi|_{S_{\mathrm{flat}}} : X|_{S_{\mathrm{flat}}} \longrightarrow S_{\mathrm{flat}}, \qquad \pi|_{X_{\mathrm{sm}}} : X|_{S_{\mathrm{sm}}} \longrightarrow S_{\mathrm{sm}}$$

are flat resp. smooth. These can be defined as follows. In general, the locus on X where a morphism $\pi : X \to S$ of locally finite presentation is $\mathcal{O}_S$-flat (resp. smooth) is open. If π is additionally proper, then S_{flat} and S_{sm} can be set as

$$S_{\mathrm{flat}} = S \setminus \pi(X_{\mathrm{non-flat}}), \qquad S_{\mathrm{sm}} = S \setminus \pi(X_{\mathrm{non-smooth}}).$$

In the case of (7.8), S_{flat} is simply the open subscheme $\bigcup_{i,j,k} D(a_{ijk})$ where at least one of the parameters is invertible. This follows e.g. from [8, Tag 00MF]. The locus $S_{\mathrm{sm}} \subseteq S_{\mathrm{flat}}$ is the open subscheme over which the Jacobi criterion holds. In conclusion, we obtain a family of curves

$$\pi|_{S_{\mathrm{sm}}} : X|_{S_{\mathrm{sm}}} \longrightarrow S_{\mathrm{sm}} \tag{7.9}$$

in the sense of Definition 7.13 (1).

By Proposition 6.36, every fiber of (7.9) is a curve of genus $(d-1)(d-2)/2$. This constancy of the fiber-wise genus is a completely general phenomenon:

Corollary 7.15. *Let S be locally noetherian*[10] *and let $\pi : X \to S$ be a family of curves in the sense of Definition 7.13.*

(1) The fiber-wise genus $g(X(s))$, $s \in S$, is locally constant.

(2) Let $\mathcal{L}$ be a line bundle on X. The fiber-wise degree $\deg(\mathcal{L}(s))$, $s \in S$, is locally constant.

Proof. By definition, π is proper and flat. So Corollary 7.11 applies with $\mathcal{F} = \mathcal{O}_X$ and shows that $\chi(\mathcal{O}_{X(s)})$, $s \in S$, is locally constant. By Riemann–Roch, $g(X(s)) = 1 - \chi(\mathcal{O}_{X(s)})$ and the proof of (1) is complete. Similary, the fiber-wise Euler characteristic $\chi(\mathcal{L}(s))$ is locally constant and hence $\deg(\mathcal{L}(s)) = \chi(\mathcal{L}(s)) - 1 + g(X(s))$ is locally constant as well. □

Proposition 7.16 (Extending Theorem 6.37)**.** *Let S be locally noetherian and let $\pi : X \to S$ be a family of curves of fiber-wise genus g. Let $\mathcal{L}$ be a line bundle on X of fiber-wise degree d.*

(1) If $d \geq 2g-1$, then $R^1\pi_*(\mathcal{L}) = 0$ and the push forward $\pi_*\mathcal{L}$ is a vector bundle of rank $1-g+d$. Moreover, its formation commutes with base change in the sense that $(\pi_*\mathcal{L})_T \xrightarrow{\sim} \pi_*(\mathcal{L}_T)$ for all $T \to S$.

(2) If $d \geq 2g$, then $\mathcal{L}$ is locally on S globally generated in the sense that the adjoint morphism $\pi^*\pi_*\mathcal{L} \to \mathcal{L}$ is surjective. In particular, it defines a morphism[11]

$$X \longrightarrow \mathbb{P}(\pi_*\mathcal{L}).$$

(3) If $d \geq 2g+1$, then this morphism is a closed immersion.

[10] Corollary 7.15, Proposition 7.16, Lemma 7.18 and Theorem 7.20 hold true without noetherian assumption.

[11] For a scheme S with vector bundle $\mathcal{E}$, the projective bundle $\mathbb{P}(\mathcal{E}) \to S$ is defined to represent the functor of line bundle quotients of $\mathcal{E}$. That is, $\mathbb{P}(\mathcal{E})(u : T \to S) = \{u^*\mathcal{E} \twoheadrightarrow \mathcal{M} \mid \mathcal{M} \text{ line bundle on } T\}/\cong$.

Proof. All claims are local on S. So assume $S = \operatorname{Spec} A$. Let $d : K^0 \to K^1$ be a two term complex of finite projective A-modules that represents cohomology of $\mathcal{L}$ in the sense of Theorem 7.9. Assume $d \geq 2g-1$. By Riemann–Roch (see Theorem 6.37 (1)), $h^1(\mathcal{L}(s)) = 0$ for all $s \in S$. This means that

$$\kappa(s) \otimes_A K^0 \longrightarrow \kappa(s) \otimes_A K^1$$

is surjective for all $s \in S$. By Nakayama's Lemma, this is equivalent to $K^0 \to K^1$ being surjective which means $(R^1\pi_*)(\mathcal{L}) = \operatorname{coker}(d) = 0$. Since K^1 is projective, there exists a splitting $K^0 \leftarrow K^1$ which means that $K^\bullet$ is isomorphic to

$$\ker(d) \oplus K^1 \xrightarrow{\text{pr}} K^1.$$

Hence $\pi_*(\mathcal{L}) = \ker(d)$ is projective as claimed. Moreover, for every A-algebra B,

$$B \otimes_A [\ker(d) \oplus K^1 \longrightarrow K^1] = \ker(\mathrm{id}_B \otimes d) \oplus (B \otimes_A K^1) \xrightarrow{\text{pr}} (B \otimes_A K^1)$$

which means that push forward of $\mathcal{L}$ commutes with base change. This proves (1).

Now assume $d \geq 2g$ and consider the adjoint morphism $\pi^*\pi_*\mathcal{L} \to \mathcal{L}$. By Nakayama, it is surjective if for every point $s \in S$, the map

$$(\pi^*\pi_*\mathcal{L})(s) \longrightarrow \mathcal{L}(s) \tag{7.10}$$

of vector bundles on the fiber $X(s)$ is surjective. We interchange the order of operations:

$$(\pi^*\pi_*\mathcal{L})(s) \xrightarrow{\sim} \pi(s)^*\big((\pi_*\mathcal{L})(s)\big) \xrightarrow{\sim} \pi(s)^*\big(\pi(s)_*(\mathcal{L}(s))\big).$$

The first equality here just rewrote the pullback using the commutativity of the diagram

$$\begin{array}{ccc} X(s) & \longrightarrow & X \\ {\scriptstyle \pi(s)}\downarrow & & \downarrow{\scriptstyle \pi} \\ \operatorname{Spec}\kappa(s) & \longrightarrow & S. \end{array}$$

The second equality used part (1). In this way, (7.10) identifies with the natural map

$$\mathcal{O}_{X(s)} \otimes_{\kappa(s)} H^0(X(s), \mathcal{L}(s)) \longrightarrow \mathcal{L}(s)$$

which is surjective by Theorem 6.37 (2). This proves (2).

Part (3) follows from Theorem 6.37 (3). Namely, a morphism of proper S-schemes is a closed immersion if and only if it is a closed immersion fiber-by-fiber. □

7.4. **Application to elliptic curves.**

Definition 7.17. Let $\pi : E \to S$ be a family of curves of genus 1 and let $e \in E(S)$ be a section. Define

$$\begin{aligned} \mathrm{Pic}_E : (\mathrm{Sch}/S)^{\mathrm{op}} &\longrightarrow (\mathrm{Ab}) \\ T &\longmapsto \left\{ (\mathcal{L}, \gamma) \,\middle|\, \begin{array}{c} \mathcal{L} \text{ line bundle on } E_T \\ \gamma : \mathcal{O}_T \xrightarrow{\sim} e^*\mathcal{L} \end{array} \right\} / \cong . \end{aligned}$$

Here, $E_T := T \times_S E$. An isomorphism of two pairs $(\mathcal{L}, \gamma)$, $(\mathcal{L}', \gamma')$ is an isomorphism of line bundles $\alpha : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ such that $\alpha \circ \gamma = \gamma'$. The group structure is given by the tensor product. Denote by

$$\mathrm{Pic}^d_E \subseteq \mathrm{Pic}_E$$

the subfunctor of line bundles that are fiber-wise of degree d. Note that Pic^0_E is again valued in abelian groups.

We consider Pic_E and the Pic_E^d as contravariant functors and currently do not need any further properties. But we will often use a more convenient description: Let $\mathcal{M}$ be any line bundle on E_T. Then one can define the pair

$$[\mathcal{M}] := \left(\mathcal{L} = \mathcal{M} \otimes (\pi^* e^* \mathcal{M})^{-1},\ \mathrm{can} : \mathcal{O}_T \xrightarrow{\sim} e^*\mathcal{L}\right) \in \mathrm{Pic}_E(T).$$

In this way, there is an isomorphism (check this)

$$\mathrm{Pic}(E_T)/\pi^*(\mathrm{Pic}(T)) \xrightarrow{\sim} \mathrm{Pic}_E(T). \tag{7.11}$$

We have discussed in §6 how to pass between finite closed subschemes of curves, divisors, and line bundles. Next, we explain these concepts in more generality. An *effective Cartier divisor* on a scheme X is a closed subscheme $Z \subset X$ that is locally defined by the vanishing of a single non-zero divisor equation. Equivalently, Z has the property that its defining ideal sheaf $\mathcal{I}_Z$ is a line bundle. In this situation, we define

$$\mathcal{O}_X([Z]) = \mathcal{I}_Z^{-1}.$$

If $D = \sum_{i=1}^r n_i[Z_i]$ is a finite formal linear combination of effective Cartier divisors, then we extend this definition by

$$\mathcal{O}_X(D) = \bigotimes_{i=1}^r \mathcal{O}_X([Z_i])^{n_i}.$$

We are mainly interested in the effective Cartier divisors that come from sections of families of curves.

Lemma 7.18. *Let S be a locally noetherian scheme, let $\pi : X \to S$ be a family of curves, and let $x \in X(S)$ be a section. Then the graph $\Gamma_x = x(S)$ is an effective Cartier divisor.*

Proof. Sections of separated morphisms are closed immersions so $\Gamma := \Gamma_x \subseteq X$ is indeed a closed subscheme. Let $\mathcal{I}$ be the defining sheaf of ideals. For every $s \in S$, the fiber $\Gamma(s) \subset X(s)$ is a finite closed subscheme of a normal curve and hence locally defined by a single equation that is not a zero-divisor. By Nakayama's Lemma, $\mathcal{I}$ is locally defined by a single equation. The non-zero divisor property follows from the next lemma. □

Lemma 7.19 ([8, Tag 00MF])**.** *Let $A \to B$ be a flat and local ring homomorphism of noetherian local rings. Denote by $\mathfrak{m}$ the maximal ideal of A. Suppose that $f \in B$ is not a zero-divisor in $B/\mathfrak{m}B$. Then B/fB is flat over A, and f is not a zero-divisor in B.*

Coming back to a pair $(E, e)/S$ as in Definition 7.17, Lemma 7.18 in particular defines the line bundle $\mathcal{O}_E([\Gamma_e])$ which is fiber-wise of degree 1. For example, we see that for every $d \in \mathbb{Z}$,

$$\mathrm{Pic}_E^0 \xrightarrow{\sim} \mathrm{Pic}_E^d, \quad [\mathcal{M}] \longmapsto [\mathcal{M} \otimes \mathcal{O}_E([\Gamma_e])^{\otimes d}].$$

Theorem 7.20. *Let $E \to S$ be a family of curves of genus 1 and let $e \in E(S)$ be a section. After restriction to locally noetherian schemes, there is an isomorphism of functors*

$$\begin{aligned} E &\xrightarrow{\sim} \mathrm{Pic}_E^0 \\ E(T) \ni x &\longmapsto [\mathcal{O}_{E_T}([\Gamma_x] - [\Gamma_e])]. \end{aligned} \tag{7.12}$$

In particular, if S is locally noetherian, then there exists a unique structure of S-group scheme on E such that (7.12) becomes an isomorphism of group-valued functors. Its identity section is e.

Remark 7.21. The group scheme structure on E with identity e is, in fact, unique. This can be proved with a strengthened version of the rigidity theorem from §3.1.

Proof. Let $T \to S$ be a locally noetherian scheme. Twisting by $\mathcal{O}_{E_T}([\Gamma_e])$ like during the proof of Proposition 7.4, we need to see that for every line bundle $\mathcal{L}$ on E_T that is fiber-wise of degree 1, there exists a unique T-valued point $x : T \to E$ such that $[\mathcal{L}] = [\mathcal{O}_{E_T}([\Gamma_x])]$. Here, $\Gamma_x \subset E_T$ denotes the graph of x. Working with $E_T \to T$ instead of $E \to S$, we may and will assume during the proof that $S = T$. (In particular, we assume S locally noetherian.)

By Proposition 7.16 (1), $\pi_*(\mathcal{L})$ is a line bundle on S. Consider the adjunction map $\gamma : \pi^*\pi_*\mathcal{L} \to \mathcal{L}$. It is a map of line bundles on E and we claim that it is injective. (Equivalently, γ is locally after trivialization given by multiplication with a non-zero divisor.)

By Proposition 7.16 (1) again, the formation of γ commutes with base change. So for every $s \in S$, the fiber $(\pi^*\pi_*\mathcal{L})(s) \to \mathcal{L}(s)$ can be identified with the map

$$\mathcal{O}_{E(s)} \otimes_{\kappa(s)} H^0(E(s), \mathcal{L}(s)) \longrightarrow \mathcal{L}(s).$$

We know this map to be injective. By Lemma 7.19, this implies the claimed properties of γ.

Let $Z = V(\gamma) \subset E$ be the vanishing locus of γ. The defining ideal sheaf $\mathcal{I}$ is isomorphic to $\pi^*\pi_*\mathcal{L} \otimes \mathcal{L}^{-1}$. In particular,

$$[\mathcal{O}_E([Z])] = [\mathcal{I}]^{-1} = [\mathcal{L}]$$

and it is left to show that $Z = \Gamma_x$ for a (necessarily unique) section $x \in E(S)$.

Lemma 7.19 implies that Z is flat over S. Moreover, the map $\pi : Z \to S$ is set-theoretically a bijection which can be checked fiber-wise and follows from the assumption that $\mathcal{L}$ is of degree 1. In particular, π is both quasi-finite and proper, and hence finite (Proposition 6.3). By flatness of π, the formation of $\mathcal{I}$ commutes with base change (Homework sheet 7, Problem 2) in the sense that for every $s \in s$, there is an exact sequence

$$0 \longrightarrow \mathcal{I}(s) \longrightarrow \mathcal{O}_{E(s)} \longrightarrow (\pi_*\mathcal{O}_Z)(s) \longrightarrow 0.$$

Since $\mathcal{I}(s)$ has degree -1, additivity of the Euler characteristic implies that $Z(s) \cong \operatorname{Spec} \kappa(s)$.

Recall that being flat coherent on a locally noetherian scheme is the same as being locally free. We have just seen that $\pi_*\mathcal{O}_Z$ has these properties and moreover that it has fibers of dimension 1. Since it is also a coherent $\mathcal{O}_S$-algebra (not just a coherent $\mathcal{O}_S$-module), we have $\mathcal{O}_S \xrightarrow{\sim} \pi_*\mathcal{O}_Z$. This means that $\pi : Z \xrightarrow{\sim} S$ is an isomorphism. The inverse $x = \pi^{-1} : S \to E$ defines the desired section. This shows that (7.12) is an isomorphism.

Now assume that S itself is locally noetherian. Then E and $E \times_S E$ are locally noetherian as well, and $E \times_S E$ is a fiber product in the category of locally noetherian S-schemes. Applying the Yoneda lemma in the category of noetherian S-schemes constructs a group scheme structure on E such that (7.12) becomes an isomorphism of group-valued functors. □

7.5. **Complements.** In the previous sections, we have changed perspective and started to consider families of elliptic curves $E \to S$ or abelian varieties $A \to S$. In this section, we extend (without proofs) our main results from the case of fields to general bases.

Theorem 7.22. *(Rigidity v2.0) Let $f : X \to Y$ be a morphism of S-schemes. Assume*

- *S is connected and there exists a point $s \in S$ such that $f(s)$ factors through a morphism $\operatorname{Spec} \kappa(s) \to Y$,*
- *$p : X \to S$ is proper, flat, of finite presentation, and surjective with $\mathcal{O}_S \xrightarrow{\sim} p_*\mathcal{O}_X$,*
- *$q : Y \to S$ is separated and locally of finite presentation.*

Then there exists a morphism $g : S \to Y$ such that $f = g \circ p$.

The proof follows the same ideas as that of Theorem 3.1. We require the following technical input for its application.

Lemma 7.23 ([8, Tag 0E0L])**.** *Let $f : X \to S$ be a morphism of schemes.*

- *Assume that f is proper, flat, of finite presentation, and surjective.*
- *Assume that the fibers of f are geometrically reduced and geometrically connected.*

Then $\mathcal{O}_S \xrightarrow{\sim} f_*\mathcal{O}_X$, and this also holds after every base change.

This can be deduced from Theorem 7.9; we refer to the reference. Note that Lemma 7.23 in particular applies to families of abelian varieties or products thereof. The following corollaries can then be obtained with the ideas from §3.2.

Corollary 7.24 (Commutativity)**.** *Let $A \to S$ be an abelian variety in the sense of Definition 7.13. Then A is a commutative S-group scheme.*

So we will usually write $+$ for the group operation on a family of abelian varieties, and 0 for its neutral element.

Corollary 7.25. *Let A_1 and A_2 be abelian varieties over S and let $f : A_1 \to A_2$ be a morphism of S-schemes with $f(0) = 0$. Then f is a group scheme homomorphism.*

In particular, the group structure we defined on a family (E, e) of genus 1 curves with section (see Theorem 7.20) is uniquely determined.

Corollary 7.26 (Rigidity for homomorphisms)**.** *Let A_1 and A_2 be two abelian varieties over S. Let $f, g : A_1 \to A_2$ be two homomorphisms of S-group schemes. Then the set $S_0 = \{s \in S \mid f(s) = g(s)\}$ is open and closed in S. Moreover, the two maps*

$$f|_{S_0}, g|_{S_0} : S_0 \times_S A_1 \longrightarrow S_0 \times_S A_2$$

agree.

In particular, if S is connected and if there exists a point $s \in S$ such that $f(s) = g(s)$, then already $f = g$.

Part 2. Arithmetic of elliptic curves

The aim of this part is to prove various fundamental results about elliptic curves, such as:

- We will show that the n-torsion $E[n]$ of an elliptic curve is a finite group scheme of degree n^2.
- We will see that $\mathrm{End}(E)$ is an order in a finite-dimensional skew-field of characteristic 0.
- We will classify the possibilities for this skew-field: They are $\mathbb{Q}$, an imaginary-quadratic extension of $\mathbb{Q}$, or a quaternion division algebra over $\mathbb{Q}$.

Along the way, we will introduce important concepts such as the Tate module and the Rosati involution.

8. Elliptic curves over $\mathbb{C}$

8.1. **Description by lattices.** There is an analytification functor

$$\begin{aligned} \{\text{Smooth } \mathbb{C}\text{-schemes}\} &\longrightarrow \{\text{Smooth complex manifolds}\} \\ X &\longmapsto X(\mathbb{C}). \end{aligned} \tag{8.1}$$

Its construction is as follows. If $X \subseteq \mathbb{A}^n_{\mathbb{C}}$ is a smooth affine scheme embedded into affine space, then $X(\mathbb{C}) \subseteq \mathbb{C}^n$ has a unique structure as a smooth complex submanifold. (The Jacobi criterion holds in the algebraic sense for X, so it holds in the analytic sense for $X(\mathbb{C})$.) This construction is functorial. Namely, if $f : X \to Y$ is a morphism of affine smooth $\mathbb{C}$-schemes and if $X \subseteq \mathbb{A}^n_{\mathbb{C}}$ and $Y \subseteq \mathbb{A}^m_{\mathbb{C}}$ are embeddings, then there exists an extension of f to a morphism $\varphi : \mathbb{A}^n_{\mathbb{C}} \to \mathbb{A}^m_{\mathbb{C}}$. Passing to $\mathbb{C}$-points, we obtain a diagram

$$\begin{array}{ccc} X(\mathbb{C}) & \xrightarrow{f(\mathbb{C})} & Y(\mathbb{C}) \\ \downarrow & & \downarrow \\ \mathbb{C}^n & \xrightarrow{\varphi(\mathbb{C})} & \mathbb{C}^m \end{array}$$

where $\varphi(\mathbb{C})$ is holomorphic because it is given by polynomials. It follows that $f(\mathbb{C})$ is holomorphic. In particular, if f is an isomorphism, then $f(\mathbb{C})$ is biholomorphic which shows that the complex manifold sturcture on $X(\mathbb{C})$ does not depend on the chosen embedding $X \subseteq \mathbb{A}^n_{\mathbb{C}}$. Moreover, the functoriality allows to glue the construction from the affine to the general case. Analytification has various nice properties of which we mention a few:

- If $X \subseteq \mathbb{P}^n_{\mathbb{C}}$ is a projective variety defined by the vanishing of homogeneous polynomials $F_1, \dots, F_r \in \mathbb{C}[T_0, \dots, T_n]$, then $X(\mathbb{C}) \subseteq \mathbb{P}^n(\mathbb{C})$ is the submanifold defined by the vanishing of the same polynomials. For example, the analytification of a complex algebraic curve (in the sense of this course) is a compact Riemann surface.
- X is connected if and only if $X(\mathbb{C})$ is connected.
- X is proper if and only if $X(\mathbb{C})$ is compact.
- Analytification restricts to an equivalence

$$\{\text{Curves over } \mathbb{C}\} \longrightarrow \{\text{Compact connected Riemann surfaces}\}. \tag{8.2}$$

This is a non-trivial theorem whose proof requires some functional analysis, see [3, §14]. For curves of genus 1, there is a much simpler proof using the Weierstrass $\wp$-function.

- Analytification is a faithful functor. It is fully faithful when restricted to proper $\mathbb{C}$-schemes.

In particular, if $A/\mathbb{C}$ is an abelian variety, then $A(\mathbb{C})$ is a compact connected complex Lie group and, for abelian varieties A_1, A_2 over $\mathbb{C}$,

$$\mathrm{Hom}_{\mathbb{C}\text{-group scheme}}(A_1, A_2) = \mathrm{Hom}_{\text{complex Lie group}}(A_1(\mathbb{C}), A_2(\mathbb{C})).$$

Theorem 8.1. *Let X be a compact connected complex Lie group of dimension g. Then there exists a lattice $\Lambda \subset \mathbb{C}^g$ such that $\mathbb{C}^g/\Lambda \xrightarrow{\sim} X$.*

Proof sketch following [4, p. 1–2]. First, conjugation preserves the identity $e \in X$ and hence defines a holomorphic homomorphism $\mathrm{ad} : X \to GL_{\mathbb{C}}(V)$ to the general linear group of the tangent space $V = T_eX$ at e. Since $GL_{\mathbb{C}}(V)$ is affine and X compact connected, this map is constant so X is commutative.

Next, consider the exponential map $\exp : T_eX \to X$ which is defined for every complex Lie group. Since X is commutative, it is a group homomorphism. Its image contains a neighborhood of e and any such neighborhood generates X as group, so exp is surjective. Since exp is even biholomorphic near the identity, we find $X = V/\Lambda$ for a discrete subgroup $\Lambda \subset V$. Any discrete subgroup of a finite-dimensional real vector space with compact quotient is a lattice, completing the proof. □

Complex Lie groups of the form $X = V/\Lambda$ are called complex tori. (Here, V is a finite-dimensional $\mathbb{C}$-vector space and $\Lambda \subset V$ a lattice.) They always satisfy $X \cong (\mathbb{R}/\mathbb{Z})^{2g}$ as real Lie group, where $g = \dim_{\mathbb{C}}(V)$, but the complex structure is an additional piece of information.

Consider the case $g = 1$. Any complex torus of the form $\mathbb{C}/\Lambda$ is a compact connected Riemann surfaces of genus 1, and hence of the form $E(\mathbb{C})$ for an elliptic curve $E/\mathbb{C}$ by (8.2). This is exceptional: In higher dimensions, there exist complex tori that are not the $\mathbb{C}$-points of an abelian variety. More precisely, a complex torus X is the analytification of an abelian variety if and only if it is a projective complex manifold.

8.2. **Arithmetic of complex tori.**

Corollary 8.2. *Let X be a complex torus of dimension g. Then $X[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.*

Proof. Clear, since $X \cong (\mathbb{R}/\mathbb{Z})^{2g}$ as group. □

Consider two complex tori $X_i = V_i/\Lambda_i$, $i = 1, 2$. The quotient maps $V_i \twoheadrightarrow V_i/\Lambda_i$ are universal coverings in the sense of topology. Taking the neutral elements $0 \in V_i$ as base point, it follows that for every homomorphism of complex Lie groups $f : X_1 \to X_2$, there exists a unique lifting to a $\mathbb{C}$-linear map $\widetilde{f} : V_1 \to V_2$. It satisfies $\widetilde{f}(\Lambda_1) \subseteq \Lambda_2$. Conversely, any $\mathbb{C}$-linear map $\widetilde{f}$ such that $\widetilde{f}(\Lambda_1) \subseteq \Lambda_2$ descends to a map $f : X_1 \to X_2$. In this way,

$$\begin{aligned} \mathrm{Hom}_{\text{complex Lie group}}(X_1, X_2) &= \{f \in \mathrm{Hom}_{\mathbb{C}}(V_1, V_2) \mid f(\Lambda_1) = \Lambda_2\} \\ &= \{f \in \mathrm{Hom}_{\mathbb{Z}}(\Lambda_1, \Lambda_2) \mid \mathrm{id}_{\mathbb{R}} \otimes f \text{ is } \mathbb{C}\text{-linear}\} \\ &= \mathrm{Hom}_{\mathbb{Z}}(\Lambda_1, \Lambda_2) \cap \mathrm{Hom}_{\mathbb{C}}(V_1, V_2). \end{aligned} \tag{8.3}$$

The intersection in the last line is taken in $\mathrm{Hom}_{\mathbb{R}}(V_1, V_2)$.

Proposition 8.3. *(1) Let $g_i = \dim_{\mathbb{C}}(X_i)$. Then $\mathrm{Hom}(X_1, X_2)$ is a torsion-free $\mathbb{Z}$-module of rank $\leq 2g_1g_2$.*

(2) Assume that $X = \mathbb{C}/\Lambda$ is a 1-dimensional complex torus. Then $\mathrm{End}(X)$ either equals $\mathbb{Z}$ or is isomorphic to an order in an imaginary quadratic field.

Proof. (1) $\mathrm{Hom}_{\mathbb{C}}(V_1, V_2)$ is a vector space of real dimension $2g_1g_2$. Thus

$$\mathrm{Hom}(X_1, X_2) = \mathrm{Hom}(\Lambda_1, \Lambda_2) \cap \mathrm{Hom}_{\mathbb{C}}(V_1, V_2)$$

is a torsion-free $\mathbb{Z}$-module of rank $\leq 2g_1g_2$.

(2) In the 1-dimensional case, we are looking at

$$\mathrm{End}(X) = \mathrm{End}_{\mathbb{Z}}(\Lambda) \cap \mathbb{C} \subset \mathrm{End}_{\mathbb{R}}(\Lambda).$$

If this intersection is larger than $\mathbb{Z}$, then it is a subring of $\mathbb{C}$ that is of rank 2 as $\mathbb{Z}$-module. This means it is an order in a quadratic field extension of $\mathbb{Q}$ that embeds into $\mathbb{C}$, as claimed. □

Example 8.4. Theorem 8.1 together with (8.2) allows to describe the isomorphism classes of complex elliptic curves. Namely, $\mathbb{C}/\Lambda_1 \xrightarrow{\sim} \mathbb{C}/\Lambda_2$ if and only if there exist $\alpha \in \mathbb{C}^\times$ with $\alpha\Lambda_1 = \Lambda_2$. In other words,

$$\{\text{Ellipt. curves}/\mathbb{C}\}/\text{iso.} \xrightarrow{\sim} \{\text{Lattices } \Lambda \subset \mathbb{C}\}/\mathbb{C}^\times. \tag{8.4}$$

How can we describe the right hand side? The idea is to first overparametrize the set of lattices by considering the set of triples $(\Lambda, \tau_1, \tau_2)$ where (τ_1, τ_2) is a $\mathbb{Z}$-basis for Λ. The product $\mathbb{C}^\times \times GL_2(\mathbb{Z})$ acts on such triples by

$$\alpha \cdot (\Lambda, \tau_1, \tau_2) = (\alpha\Lambda, \alpha\tau_1, \alpha\tau_2), \qquad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot (\Lambda, \tau_1, \tau_2) = (\Lambda, a\tau_1 + b\tau_2, c\tau_1 + d\tau_2).$$

The set of possible choices of a basis for a fixed lattice form a simply transitive $GL_2(\mathbb{Z})$-orbit, so taking the quotient for the $GL_2(\mathbb{Z})$-action recovers (8.4). However, we may also first take the quotient by $\mathbb{C}^\times$. Let $\mathbb{H}^\pm = \mathbb{C} \setminus \mathbb{R}$ be the union of upper and lower complex half-plane. Consider the map

$$\{(\Lambda, \tau_1, \tau_2)\} \longrightarrow \mathbb{H}^\pm, \quad (\Lambda, \tau_1, \tau_2) \longmapsto \tau_1/\tau_2.$$

This map *is* the quotient by $\mathbb{C}^\times$ (check this). In this way, we have constructed a diagram

$$\begin{array}{ccc} GL_2(\mathbb{Z})\backslash\{\text{Triples } (\Lambda, \tau_1, \tau_2)\}/\mathbb{C}^\times & \xrightarrow[(\tau_1,\tau_2)\mapsto\tau_1/\tau_2]{\cong} & GL_2(\mathbb{Z})\backslash\mathbb{H}^\pm \\ \cong \big\downarrow & & \\ \{\text{Lattices } \Lambda \subset \mathbb{C}\}/\mathbb{C}^\times. & & \end{array}$$

Tracing through the upper arrow, the remaining $GL_2(\mathbb{Z})$-action on $\mathbb{H}^\pm$ is by Moebius transformations,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}. \tag{8.5}$$

In conclusion, we have constructed a bijection

$$\{\text{Ellipt. curves}/\mathbb{C}\}/\text{iso.} \xrightarrow{\sim} GL_2(\mathbb{Z})\backslash\mathbb{H}^\pm. \tag{8.6}$$

In particular, this computation explains in a precise sense how to parametrize all complex

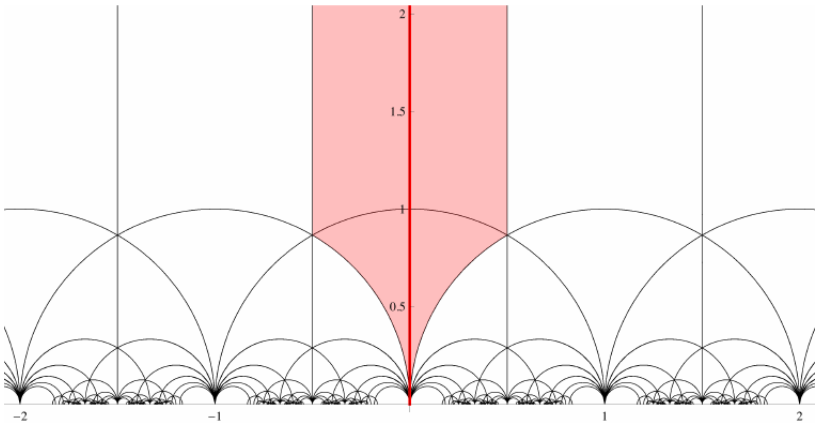


FIGURE 2. The image shows the upper half plane $\{\mathrm{Im}(\tau) > 0\}$. The subset $\mathcal{F} = \{-1/2 \leq \mathrm{Re}(\tau) \leq 1/2\} \cap \{|\tau| \geq 1\}$ is a fundamental domain for the $GL_2(\mathbb{Z})$-action on $\mathbb{H}^\pm$. (This is the upper part of the red area.) The remaining areas show $GL_2(\mathbb{Z})$-translates of $\mathcal{F}$.

structures on $\mathbb{R}^2/\mathbb{Z}^2$ up to isomorphism. It also allows to get some intuition for the distribution of the endomorphism rings $\mathrm{End}(E)$ when varying E. Namely, let $\tau \in \mathbb{H}^{\pm}$, let $\Lambda = \mathbb{Z} + \mathbb{Z} \cdot \tau$ be the generated lattice, and let $E = \mathbb{C}/\Lambda$ be the so-defined elliptic curve. Assume there exists an element $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ such that $\alpha\Lambda \subseteq \Lambda$. Then $\alpha = \alpha(1) = a\tau + b$ for two integers $a, b \in \mathbb{Z}$. Since $\alpha \notin \mathbb{Z}$ by assumption, $a \neq 0$. Since also $\alpha(\tau) = a\tau^2 + b\tau$ has to lie in Λ, the element τ has to satisfy a quadratic polynomial over $\mathbb{Q}$ and we find

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E) = \mathbb{Q}(\alpha) = \mathbb{Q}(\tau). \tag{8.7}$$

Conversely, if $\mathbb{Q}(\tau)$ is a quadratic extension of $\mathbb{Q}$, then E acquires additional endomorphisms and (8.7) holds (check this). In this way, we see that there exist only countably many isomorphism classes of elliptic curves over $\mathbb{C}$ that have endomorphism ring larger than $\mathbb{Z}$. The uncountable complement has $\mathrm{End}(E) = \mathbb{Z}$.

9. Torsion of elliptic curves

9.1. **Isogenies.** Let E, E_1 and E_2 be elliptic curves over a scheme S. We write $\mathrm{End}(E)$ and $\mathrm{Hom}(E_1, E_2)$ for endomorphisms and homomorphisms as S-group schemes. Note that these are abelian groups by

$$(\phi + \psi)(x) = \phi(x) + \psi(x), \qquad T \to S,\ x \in E(T),\ \text{resp. } x \in E_1(T).$$

Moreover, $\mathrm{End}(E)$ becomes a (non-commutative) ring with multiplication

$$(\phi\psi)(x) = \phi(\psi(x)), \qquad T \to S,\ x \in E(T).$$

A homomorphism $\phi : E_1 \to E_2$ is called an *isogeny* if it is finite and flat.

Lemma 9.1. *Assume that $\phi : E_1 \to E_2$ is an isogeny. Then ϕ is finite locally free in the sense that $\phi_*(\mathcal{O}_{E_1})$ is a finite and locally free quasi-coherent $\mathcal{O}_{E_2}$-module.*

Proof. Both E_1, E_2 are of finite presentation over S by definition. This implies that ϕ is of finite presentation. By assumption, ϕ is an isogeny, so we obtain that $\phi_*(\mathcal{O}_{E_1})$ is a locally finitely generated, flat, quasi-coherent $\mathcal{O}_{E_2}$-algebra that is locally of finite presentation *as algebra*. As shown in [8, Tag 02K9], this is equivalent to $\phi_*(\mathcal{O}_{E_1})$ being locally of finite presentation as $\mathcal{O}_{E_2}$-module. □

Lemma 9.2. *Let $\phi : E_1 \to E_2$ be any homomorphism. Then ϕ is an isogeny if and only if for every $s \in S$, the fiber $\phi(s)$ is non-zero. (This is meant in the sense that $\phi(s) : E_1(s) \to E_2(s)$ is not the 0-map.)*

Proof. If ϕ is an isogeny, then it is finite by definition, so $\phi(s)$ is non-constant for every $s \in S$. Conversely, assume $\phi(s) = 0$ for every $s \in S$. The fibers $E_1(s)$ and $E_2(s)$ are proper smooth connected curves, so this implies that $\phi(s)$ is finite and flat for every s (Lemma 6.2). The statement now follows from the so-called fiber criterion for flatness (see below). □

Proposition 9.3 (Fiber criterion for flatness [8, Tag 039E])**.** *Let $f : X \to Y$ be a morphism of S-schemes. Assume*

(1) X and Y are locally of finite presentation over S,
(2) X is flat over S,
(3) for every $s \in S$, the morphism $f(s) : X(s) \to Y(s)$ is flat.

Then f is flat.

Remark 9.4. If S is connected, then Lemma 9.2 and Corollary 7.26 together imply that ϕ is an isogeny already if there exists a single point $s \in S$ such that $\phi(s) \neq 0$.

Assume that $\phi : E_1 \to E_2$ is an isogeny. The *degree of* ϕ is defined as the rank of $\phi_*(\mathcal{O}_{E_1})$ as vector bundle on E_2. It is a locally constant function on E_2. The fibers of $E_2 \to S$ are all connected, so we may (and will) view it as a locally constant function on S. Note that the degree is multiplicative. That is, if $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_3$ are isogenies, then

$$\deg(\phi\psi) = \deg(\phi)\deg(\psi). \tag{9.1}$$

Recall that the kernel of ϕ is defined by the Cartesian diagram

$$\begin{array}{ccc} \ker(\phi) & \longrightarrow & E_1 \\ \downarrow & & \downarrow{\scriptstyle \phi} \\ S & \xrightarrow{0} & E_2. \end{array}$$

Being finite and locally free with degree function $\deg(\phi)$ is stable under pullback, so $\ker(\phi) \to S$ is a finite locally free S-group scheme of degree $\deg(\phi)$.

Also recall that $[n] : E \to E$ denotes the multiplication-by-n endomorphism and that $E[n] = \ker([n])$. Our next major result is the following theorem.

Theorem 9.5. *Let E/S be an elliptic curve. Then $[n] : E \to E$ is an isogeny of degree n^2. In particular* $\ker[n]$ *is a finite locally free S-group scheme of degree n^2.*

By Lemma 9.2, Theorem 9.5 reduces to the case $S = \operatorname{Spec} k$ for a field k. There are then at least two proofs: The first is purely algebraic and relies on the so-called Theorem of the cube; we refer to [4]. The second, which we present here, uses the analytic results from §8 when $\operatorname{char}(k) = 0$ and a spreading out argument to extend to $\operatorname{char}(k) > 0$.

9.2. **Proof of Theorem 9.5 in characteristic 0.** *Step 1: Reduction to finitely generated fields.* Let E be an elliptic curve over a field k with $\operatorname{char}(k) = 0$. We have seen (Theorem 6.37 or Corollary 6.38) that elliptic curves are projective. Hence there exists a subfield $k' \subseteq k$ that is finitely generated over $\mathbb{Q}$ together with a curve E'/k' of genus 1 such that there exists an isomorphism $\gamma : k \otimes_{k'} E' \xrightarrow{\sim} E$. After fixing such an identification, $E'(k') \subseteq E'(k) = E(k)$. Enlarging k', we may assume that also $0 \in E'(k')$. (Concretely, fix a cubic equation F such that $E = V_+(F)$. Also pick $x, y, z \in k$ such that $0 = [x : y : z] \in \mathbb{P}^2(k)$. Then take $k' \subseteq k$ as the subfield generated over $\mathbb{Q}$ by the coefficients of F and x, y, z.) By Theorem 7.20, there exists a unique elliptic curve structure with neutral element 0 on E'. Then γ is an isomorphism of elliptic curves and we have

$$\gamma : k' \otimes_k E'[n] \xrightarrow{\sim} E[n].$$

In this way, we have reduced Theorem 9.5 for E/k to Theorem 9.5 for E'/k'.

Step 2: The finitely generated case. If k is finitely generated over $\mathbb{Q}$, then there exists an embedding $k \to \mathbb{C}$. Since

$$\mathbb{C} \otimes_k E[n] \xrightarrow{\sim} (\mathbb{C} \otimes_k E)[n],$$

it suffices to prove the claim for $k = \mathbb{C}$. By Corollary 8.2, we know $E[n](\mathbb{C}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^{\oplus 2}$. We claim that $E[n]$ is an étale group scheme.

End of Step 2 assuming this claim. $E[n]$ being étale means that $E[n] = \operatorname{Spec} A$ for a finite-dimensional k-algebra that is a product of fields. Then

$$\deg(E[n]) = \dim_k(A) \overset{A \text{ étale}}{=} \#\operatorname{Hom}_{k\text{-alg}}(A, \mathbb{C}) = (E[n])(\mathbb{C}) = n^2.$$

9.3. **Proof that $E[n]$ is étale in characteristic 0.** We prove a more general statement:

Proposition 9.6. *Let $G \to S$ be a finite locally free group scheme. Assume that G is n-torsion in the sense that $g^n = e$ for every $g \in G(T)$. Also assume that $n \in \mathcal{O}_S^\times$. Then G is finite étale.*

Proof. By assumption, G is flat over S. It is left to see that the fibers of G are étale which reduces us to the case $S = \operatorname{Spec} k$. By Theorem 4.18, we need to see that $\Omega^1_{G/k} = 0$. This can be shown after base change to $\bar{k}$ so we may assume all closed points of G to be rational. By a translation argument using the group structure, we really only need to see that the stalk $\Omega^1_{G/k,e}$ vanishes (e denotes the neutral element). This follows from the classical statement (which we will prove in the following) that the pullback map $[n]^* : \Omega^1_{G/k}(e) \to \Omega^1_{G/k}(e)$ is multiplication by n.[12]

Lemma 9.7. *Let X/k be a finite type k-scheme and let $x \in X(k)$ be a rational point. Then there are bijections*

$$\operatorname{Mor}_x(\operatorname{Spec} k[\varepsilon]/(\varepsilon)^2, X) \xrightarrow{\sim} (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee \xrightarrow{\sim} \operatorname{Der}_k(\mathcal{O}_{X,x}, k) \xrightarrow{\sim} (\Omega^1_{X/k})(x)^\vee.$$

Proof. We have seen this in §4 and only briefly recall how the maps were defined. Given a k-scheme morphism

$$\phi : \operatorname{Spec} k[\varepsilon]/(\varepsilon)^2 \longrightarrow X$$

with image x, we map it to

$$\varphi := \phi^*|_{\mathfrak{m}_x/\mathfrak{m}_x^2} : \mathfrak{m}_x/\mathfrak{m}_x^2 \longrightarrow k\varepsilon \xrightarrow[\varepsilon \mapsto 1]{\sim} k.$$

We send φ to the derivation

$$\delta : [f \longmapsto \varphi(f - f(0))] \in \operatorname{Der}_k(\mathcal{O}_{X,x}, k).$$

A derivation δ gets mapped to

$$[dh \longmapsto \delta(h)] \in \operatorname{Hom}_{\mathcal{O}_{X,x}}(\Omega^1_{X/k,x}, k).$$

□

Definition 9.8. The tangent space $T_x X$ of X in x is defined as the vector space(s) from Lemma 9.7. If G/k is a finite type group scheme, then we set $\operatorname{Lie}(G) := T_e G$. Taking the tangent space is a covariant functor: If $f : X \to Y$ is a morphism of finite type k-schemes and $x \in X(k)$ a rational point, then we denote by

$$df : T_x X \longrightarrow T_{f(x)} Y$$

the map that is dual to pullback $f^* : \Omega^1_{Y/k}(y) \to \Omega^1_{X/k}(x)$.

Lemma 9.9. *Let G/k be a finite type group scheme. Let $[n] : G \to G$ denote the morphism $g \mapsto g^n$ (in the Yoneda Lemma sense). Then $d[n] : \operatorname{Lie}(G) \to \operatorname{Lie}(G)$ is multiplication by n.*

Proof. Clearly, for any (X, x) and (Y, y) over k,

$$T_x X \oplus T_y Y \xrightarrow{\sim} T_{(x,y)}(X \times_k Y).$$

Consider the diagonal $\Delta : G \to G \times_k \cdots \times_k G = G^n$. On the one hand, for every $v \in \operatorname{Lie}(G)$,

$$d\Delta(v) = (v, \ldots, v) \in T_{(e,\ldots,e)}(G^n) = T_e(G)^{\oplus n}.$$

On the other hand,

$$\begin{aligned} dm : T_{(e,e)}(G \times_k G) &\longrightarrow T_e(G) \\ (v, w) &\longmapsto v + w \end{aligned} \tag{9.2}$$

[12] Here, $[n] : G \to G$ denotes the n-th power map $g \mapsto g^n$, $g \in G(T)$. If G is commutative, then it is a group scheme homomorphism. In general, it is just a morphism of S-schemes.

because $m|_{e\times_k G} = m|_{G\times_k e} = \mathrm{id}_G$. Combining these two statements concludes the proof. □

We come back to our setting of a finite locally free group scheme G/k of degree n with $\mathrm{char}(k) \nmid n$. On the one hand, Deligne's result (if G is commutative) or [7, Corollary 2.2] (for general G) state that G is n-torsion. So $d[n] = 0$. On the other hand, Lemma 9.9 states that $d[n] = n \in k^\times$. The only possibility is $\mathrm{Lie}(G) = 0$, which means that G is étale as explained before. □

Example 9.10. Let $G = GL_{n,k}$ be the general linear group scheme over k. Then

$$\begin{aligned}\mathrm{Lie}(G) &= \mathrm{Mor}_e(\mathrm{Spec}\, k[\varepsilon]/(\varepsilon^2), G)\\ &= \{1 + \varepsilon X \mid X \in M_n(k)\} \subseteq GL_n(k[\varepsilon]/(\varepsilon^2)).\end{aligned}$$

Lemma 9.9 generalizes the identity

$$(1+\varepsilon X)^n = 1 + n\varepsilon X.$$

The example also illustrates another description of the Lie algebra, namely

$$\mathrm{Lie}(G) = \ker\big(G(k[\varepsilon]/(\varepsilon^2)) \longrightarrow G(k)\big).$$

9.4. **Proof of Theorem 9.5 in positive characteristic.** Assume now that $p = \mathrm{char}(k) > 0$ and that E/k is an elliptic curve.

Lemma 9.11. *There exists a local ring $(R, \mathfrak{m})$ together with a ring map $R/\mathfrak{m} \to k$ and an elliptic curve $\widetilde{E}/\mathrm{Spec}\, R$ with the following two properties.*

(1) For the special fiber, we have $k \otimes_R \widetilde{E} \cong E$.

(2) $\mathbb{Q} \otimes_{\mathbb{Z}} R \neq 0$, meaning $\mathrm{Spec}\, R$ has a point in characteristic 0.

Proof. Choose a Weierstrass equation (6.22) that defines E/k; let $a_i \in k$ denote its coefficients. Consider the polynomial ring $R_0 = \mathbb{Z}[t_1, t_2, t_3, t_4, t_6]$ and the specialization map

$$R_0 \longrightarrow k, \quad t_i \longmapsto a_i.$$

Let $\mathfrak{p} \subset R_0$ be its kernel (a prime ideal) and set $R = R_{0,\mathfrak{p}}$. Then R is a local ring together with a map $R/\mathfrak{m} \to k$ as desired. Define the R-scheme

$$\widetilde{E} = V_+(Y^2Z + t_1XY + t_3YZ^2 - X^3 - t_2X^2Z - t_4XZ^2 - t_6Z^3) \subset \mathbb{P}^2_R.$$

Then $\widetilde{E} \to \mathrm{Spec}\, R$ is flat with 1-dimensional fibers (Lemma 7.19). Moreover, $k \otimes_R \widetilde{E}$ is smooth, meaning the special fiber of $\widetilde{E}$ is smooth. Being smooth is an open condition, so $\widetilde{E} \to \mathrm{Spec}\, R$ is smooth (R is local). Moreover, $[0:1:0] \in \mathbb{P}^2_R(R)$ lies on $\widetilde{E}$ and extends 0_E because this is a property of Weierstrass equations. By Theorem 7.20, $\widetilde{E}$ is an elliptic curve over $\mathrm{Spec}\, R$. As a localization of a polynomial ring over $\mathbb{Z}$, the ring R is torsion-free and, in particular, $\mathrm{Spec}\, R$ has points in characteristic 0. □

Let $\widetilde{E} \to \mathrm{Spec}\, R$ be as in Lemma 9.11. Observe that $\mathrm{Spec}\, R$ is connected because R is a local ring. We deduce from Lemmas 9.2 and 9.1, together with Theorem 9.5 for fields of characteristic 0, that $[n] : \widetilde{E} \to \widetilde{E}$ is an isogeny of degree n^2. Specializing this along $R \to k$, we have proved the same statement for E/k, and our proof of Theorem 9.5 is complete. □

9.5. **Finite Étale group schemes.** Proposition 9.6 together with Theorem 9.5 states that for every elliptic curve E/S and every integer $n \in \mathcal{O}_S^\times$, $E[n]$ is a finite étale S-group scheme of degree n^2. What else can we say about $E[n]$? If $S = \mathrm{Spec}\, \mathbb{C}$, then Corollary 8.2 states that $E[n](\mathbb{C}) \cong (\mathbb{Z}/n\mathbb{Z})^{\oplus 2}$. Our aim in this section is to formulate a generalization for arbitrary base S. The precise statement will be that every finite étale group scheme is locally in the étale topology a constant group scheme.

Let $G \to S$ be a finite étale group scheme. Then G is, in particular, finite, flat, and of finite presentation over S. As during the proof of Lemma 9.1, [8, Tag 02K9] implies that $G \to S$ is finite locally free.

Example 9.12 (Constant group schemes)**.** Let Γ be a finite group and S a scheme. Consider the disjoint union $\underline{\Gamma}_S := \coprod_{\gamma\in\Gamma} S$ and write $S_\gamma \subseteq \underline{\Gamma}_S$ for the copy indexed by γ. The S-scheme structure is given by the identity mapping on each copy of S. Then $\underline{\Gamma}_S$ becomes an S-group scheme with multiplication m that is copy by copy given as

$$m|_{S_{\gamma_1}\times_S S_{\gamma_2}} = [S_{\gamma_1} \times_S S_{\gamma_2} = S \xrightarrow{\mathrm{id}} S_{\gamma_1\gamma_2}].$$

$\underline{\Gamma}_S$ is called the *constant S-group scheme with fiber Γ*. If T is a connected S-scheme, e.g. $T = \operatorname{Spec} k$ for a field k, then directly from the definition

$$\Gamma \xrightarrow{\sim} \underline{\Gamma}_S(T). \tag{9.3}$$

In general, $\underline{\Gamma}_S$ represents the functor (on S-schemes)

$$T \longmapsto \mathrm{Cont}(|T|, \Gamma) \tag{9.4}$$

where Γ has the discrete topology.

Example 9.13 (Kernels of étale isogenies)**.** Let E_1 and E_2 be elliptic curves over a scheme S. Let $\phi : E_1 \to E_2$ be an isogeny such that $\deg(\phi) \in \mathcal{O}_S^\times$ is invertible on S. Then ϕ and $\ker(\phi) \to S$ are étale.

Proof. The kernel $\ker(\phi) \to S$ is the base change of ϕ along $0 : S \to E_2$. Being étale is stable under base change, so it suffices to prove that ϕ is étale.

We already have that ϕ is finite by definition of isogeny, so the lemma only adds that ϕ is smooth. This means that ϕ is flat with smooth fibers. Flatness is also part of the definition of isogeny, so we really only need to see that ϕ has smooth fibers. This can be shown fiber-wise over S.

So let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves over a field k with $\mathrm{char}(k) \nmid \deg(\phi)$. The last conditions says that $\mathrm{char}(k) \nmid [\mathcal{O}_{E_1,\eta_1} : \mathcal{O}_{E_2,\eta_2}]$ and hence this field extension is étale. In other words, ϕ is generically étale. The locus where a morphism is smooth is open, so there exists an open subset $U \subseteq E_1$ such that $\phi|_U$ is smooth. Since ϕ is a group homomorphism, for every $x \in E(k)$ also $\phi|_{x+U}$ is smooth. Finally, smoothness can be shown after base change to $\bar{k}$ where the translates $x + \bar{k} \otimes_k U$, $x \in E_1(\bar{k})$ cover all of $\bar{k} \otimes_k E_1$, and we win. □

Example 9.14 (Roots of unity)**.** Let S be a scheme and let $n \geq 1$ be such that $n \in \mathcal{O}_S^\times$. Then $\mu_{n,S} = \underline{\mathrm{Spec}}\mathcal{O}_S[x]/(x^n - 1)$ is a finite étale S-group scheme. Set $U = \mu_{n,S}$ and define

$$\zeta := (x \bmod (x^n - 1)) \in \mathcal{O}_U(U).$$

The base change $\mu_{n,U} = U \times_S \mu_{n,S}$ is a U-group scheme and ζ defines a U-group scheme homomorphism

$$\underline{\mathbb{Z}/n\mathbb{Z}}_U \longrightarrow \mu_{n,U}. \tag{9.5}$$

Concretely, (9.5) is given on T-valued points of U with T connected by

$$\underline{\mathbb{Z}/n\mathbb{Z}}_U(T) \overset{(9.3)}{=} \mathbb{Z}/n\mathbb{Z} \ni i \longmapsto \zeta^i \in \mu_n(U).$$

For general T and in terms of (9.4), the morphism (9.5) is given by

$$[f : |T| \to \mathbb{Z}/n\mathbb{Z}] \longmapsto \zeta^f \in \mu_n(T).$$

Exercise 9.15 (Generalizing construction (9.5))**.** Let G be an S-group scheme, Γ a finite group, and $\phi : \Gamma \to G(S)$ a group homomorphism. Show that there exists a unique group scheme homomorphism $\underline{\Gamma}_S \to G$ that restricts to ϕ on $\Gamma \subseteq \mathrm{Cont}(|S|, \Gamma)$.

The point of these definitions is that Example 9.14 is a completely general phenomenon: Every finite étale group scheme is étale locally a constant group scheme.

Theorem 9.16. *Let $G \to S$ be a finite étale group scheme. Then there exist a decomposition $S = \coprod_{i\in I} S_i$ into open and closed subschemes, finite groups Γ_i, finite étale surjections $T_i \to S_i$, and group scheme isomorphisms*

$$\underline{\Gamma_i}_{T_i} \xrightarrow{\sim} T_i \times_S G.$$

Conversely, if G is a group scheme such that a set of such data exists, then G is a finite étale group scheme.

Proof. The converse direction follows immediately from étale descent for the property "finite étale" and the étale covering $\coprod_{i\in I} T_i \to S$; we mentioned it here only for completeness and will not go into details. In order to prove the other direction, we start with some intermediate statements.

Lemma 9.17. *Let $f : X \to Y$ be a morphism of finite étale S-schemes. Then f is finite étale.*

Proof. It is clear that f is finite. Following Definition 7.12, we need to see that f is flat and fiber-wise étale. Both X and Y are flat over S. For every $s \in S$, the fibers $X(s)$ and $Y(s)$ are spectra of finite étale $\kappa(s)$-algebras. It is clear that any map between such is flat, even étale. We conclude with the fiber criterion for flatness Proposition 9.3. □

Proposition 9.18. *Let $X \to S$ be finite étale of degree n. There exist a finite étale surjection $T \to S$ and an isomorphism of T-schemes $\coprod_{i=1}^n T \xrightarrow{\sim} T \times_S X$.*

Proof. The statement is clear if $n = 1$; in this case, $X \xrightarrow{\sim} S$ and we may take $T = S$. If $n \geq 2$, then consider $U = X$ and the base change to U,

$$X_U = U \times_S X \longrightarrow U.$$

It is finite étale of degree n because this property is stable under base change. The diagonal $\Delta : U \to X_U$ defines a section as U-scheme. Both U and X_U are finite étale U-schemes, so Lemma 9.17 implies that Δ is finite étale. We now need an important statement about flat morphisms.

Proposition 9.19 ([8, Tag 01UA])**.** *A flat morphism of locally finite presentation is open.*

Applying this proposition, we obtain that Δ is open. As finite (hence proper) morphism it is also closed. So $\Delta(U) \subset X_U$ is an open and closed subset which means there is an isomorphism $U \sqcup Y \xrightarrow{\sim} X_U$ where $Y \to U$ is finite étale of degree $n-1$. By induction, there exists a finite étale surjective $T \to U$ such that $\coprod_{i=1}^{n-1} T \xrightarrow{\sim} T \times_U Y$. The composition $T \to U \to S$ then satisfies $X_T \cong \coprod_{i=1}^n T$, and the proof is complete. □

Proof of Theorem 9.16. Let $f : G \to S$ be a finite étale group scheme. The rank of $f_*\mathcal{O}_G$ as $\mathcal{O}_S$-module is locally constant. Writing S as a disjoint union, we may assume it to be constant, say equal to n. By Proposition 9.18, there exists a finite étale surjective morphism $T \to S$ with $G_T \cong \coprod_{i=1}^n T$. Fixing such an isomorphism, the group structure is given by maps

$$m_{ij} : T = T_i \times_T T_j \longrightarrow \coprod_{i=1}^n T.$$

For each $1 \leq i, j, k \leq n$, the preimage $m_{ij}^{-1}(T_k) \subset T$ is open and closed. In this way, we find for each group structure Γ on $\{1, \dots, n\}$ an open and closed subset

$$T_\Gamma = \bigcap_{1\leq i,j\leq n} m_{ij}^{-1}(T_{i \bullet_\Gamma j})$$

over which the group structure is that of $\underline{\Gamma}_{T_\Gamma}$, and $T = \coprod_\Gamma T_\Gamma$. It is only left to construct from this a decomposition of S.

Let $p : T \to S$ denote the map to S. For each Γ, the map $T_\Gamma \to S$ is finite étale. So by Proposition 9.19, $p(T_\Gamma) \subset S$ is open and closed. Let $\Gamma_1, \dots, \Gamma_r$ be an enumeration of the possible group structures on $\{1, \dots, n\}$. For $1 \le i \le r$, define

$$S_i = p(T_{\Gamma_i}) \setminus \bigcup_{1 \le j < i} p(T_{\Gamma_j}).$$

Then the theorem is proved with $S = \coprod_{i=1}^r S_i$, the given Γ_i, and $T_i = p^{-1}(S_i)$. □

Corollary 9.20. *Let E be an elliptic curve over S and let $n \ge 1$ lie in $\mathcal{O}_S^\times$. Then there exist a finite étale surjection $T \to S$ and an isomorphism $\underline{\mathbb{Z}/n\mathbb{Z}}_T^{\oplus 2} \xrightarrow{\sim} E[n]_T$.*

Proof. By Proposition 9.6, the kernel $E[n]$ is étale. Theorem 9.16 states that there exist a finite étale surjective $T \to S$, a decomposition $T = \coprod_{i=1}^r T_i$, finite (in this case abelian) groups Γ_i, and isomorphisms $\underline{\Gamma_i}_{T_i} \xrightarrow{\sim} E[n]_{T_i}$. We know that for all divisors $d \mid n$, the d-torsion $E[n][d] = E[d]$ is of degree d^2. So the only possibility is $\Gamma_i \cong (\mathbb{Z}/n\mathbb{Z})^{\oplus 2}$, and the proof is complete. □

9.6. **Deligne's Theorem.** Let Γ be a finite group of order n and let $g \in \Gamma$ be an element. Then $g^n = e$, i.e. Γ is n-torsion. We end this section with a short discussion of the folklore conjecture that an analogous statement holds for finite locally free group schemes:

Conjecture 9.21 (Grothendieck)**.** Let $G \to S$ be a finite locally free group scheme. Then G is n-torsion.

Using our previous results, we can confirm the conjecture for finite étale group schemes:

Corollary 9.22. *Let G be a finite étale S-group scheme of degree n. Then G is n-torsion.*

Proof. The claim is that the map $[n] : G \to G$, $g \mapsto g^n$, is identical to the composition $G \to S \xrightarrow{e} G$. This can be shown after a faithfully flat base change. By Theorem 9.16, G is locally after a surjective étale base change a constant group scheme. The claim is clear for constant group schemes, and we win. □

Conjecture 9.21 is also known when G is commutative (see below) or when $S = \operatorname{Spec} k$ for a field, see [7].

Theorem 9.23 (Deligne)**.** *A commutative finite locally free group scheme of degree n is n-torsion.*

Corollary 9.24. *Let $G \to S$ be a commutative finite locally free group scheme of degree n. Suppose that $n \in \mathcal{O}_S^\times$. Then G is étale.*

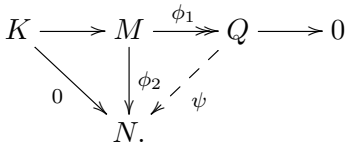
Proof. By Deligne's Theorem, G is n-torsion. The statement now follows from Proposition 9.18. □

Corollary 9.25. *Let $\phi : E_1 \to E_2$ be an isogeny of degree n. Then $\ker(\phi) \subseteq E_1[n]$.*

Proof. Apply Deligne's Theorem to the kernel $\ker(\phi)$, which is finite locally free of degree n. □

10. Endomorphism rings

10.1. **Factorization of isogenies.** Consider a diagram of abelian groups with exact upper row



If ϕ_1 is a cokernel of $K \to M$ and if $\phi_2|_K = 0$, then there exists a unique map $\psi : Q \to N$ with $\phi_2 = \psi\phi_1$. We now prove that the same applies to elliptic curves.[13]

Proposition 10.1. *Let E, E_1 and E_2 be elliptic curves over S. Let $\phi_1 : E \to E_2$ and $\phi_2 : E \to E_2$ be isogenies that fit into the diagram*

$$\begin{array}{ccccc} \ker(\phi_1) & \longrightarrow & E & \xrightarrow{\phi_1} & E_1 \\ & \searrow^{0} & \downarrow{\scriptstyle \phi_2} & \swarrow_{\psi} & \\ & & E_2. & & \end{array}$$

In other words, assume $\ker(\phi_1) \subseteq \ker(\phi_2)$. *Then there exists a unique isogeny $\psi : E_1 \to E_2$ such that $\phi_2 = \psi\phi_1$.*

Proof. For simplicity, we only give the proof when $S = \operatorname{Spec} k$ for a field. Consider the diagram

$$\begin{array}{ccccc} E \times_{E_1} E & \xrightarrow{p,q} & E & \xrightarrow{\phi_1} & E_1 \\ & & \downarrow{\scriptstyle \phi_2} & & \\ & & E_2 & & \end{array} \tag{10.1}$$

where p and q denote the two projections. All its arrows are finite and locally free. Let $x \in E$ be any point. Recall that for any finite subset $Z \subset X$ of a curve over a field, the complement $X \setminus Z$ is affine. (This can be deduced from Theorem 6.37.) Let $U_2 \subseteq E_2$ be any affine open subset containing $\phi_2(\phi_1^{-1}(\phi_1(x)))$. The set

$$U_1 = E_1 \setminus \phi_1(\phi_2^{-1}(E_2 \setminus U_2))$$

is also open affine. Note that $\phi_2(x) \in U_2$ and $\phi_1(x) \in U_1$, so if we vary x, then these open sets cover E_1 and E_2. Moreover, $\phi_1^{-1}(U_1) \subseteq \phi_2^{-1}(U_2)$ by construction. Let $U_2 = \operatorname{Spec} R$, $U_1 = \operatorname{Spec} A$, and $\phi_1^{-1}(U_1) = \operatorname{Spec} B$. Restricting (10.1) to U_1, U_2, and passing to pullback maps on rings of functions, we obtain the diagram

$$\begin{array}{ccccc} B \otimes_A B & \xleftarrow{p^*,q^*} & B & \xleftarrow{\phi_1^*} & A \\ & & \uparrow{\scriptstyle \phi_2^*} & & \\ & & R. & & \end{array} \tag{10.2}$$

The pullback ϕ_1^* is injective because ϕ_1 is flat and surjective. Our task is to show that $\phi_2^*(R) \subseteq A$. We know that the sequence

$$0 \longrightarrow A \longrightarrow B \xrightarrow{p^* - q^*} B \otimes_A B$$

is exact (use the fully faithfulness, [6, Proposition 3.2]). Thus we would like to see that $p^* \circ \phi_2^* = q^* \circ \phi_1^*$. This will finally use our assumption $\ker(\phi_1) \subseteq \ker(\phi_2)$.

Using the Yoneda lemma, we check on T-valued points that there is an isomorphism

$$\begin{aligned} \gamma : \ker(\phi_1) \times_S E &\xrightarrow{\sim} E \times_{E_1} E \\ (t, y) &\longmapsto (t + y, y) \\ (x - y, y) &\longmapsfrom (x, y). \end{aligned}$$

Then we obtain (again for T-valued points)

$$\phi_2(p(\gamma(t, y))) = \phi_2(t + y) \overset{(\star)}{=} \phi_2(y) = \phi_2(q(t, y))$$

[13] The deeper reason for this phenomenon is that an isogeny is a cokernel in the category of fppf-sheaves on S-schemes.

where $(\star)$ holds by $\ker(\phi_1) \subseteq \ker(\phi_2)$. Hence $\phi_2 \circ p = \phi_2 \circ q$, and we obtain that ψ exists. Since $\psi(0) = 0$ by construction, ψ is a group homomorphism and the proof is complete. □

Lemma 10.2. *Let S be connected, and let $E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} E_2$ be two homomorphisms with $\phi_2 \circ \phi_1 = 0$. Then $\phi_1 = 0$ or $\phi_2 = 0$. In particular, $\mathrm{End}(E)$ has no zero divisors.*

Variant: Let $\phi_1 : E \to E_1$ be an isogeny and let $\phi_2, \phi_2' : E_1 \to E_2$ be two homomorphisms such that $\phi_2 \circ \phi_1 = \phi_2' \circ \phi_1$. Then $\phi_2 = \phi_2'$.

Proof. Assume ϕ_1 and ϕ_2 are both non-zero. By rigidity using that S is connected (Corollary 7.26), this means they are both isogenies. This is equivalent to being surjective. A composition of surjective maps is surjective, so $\phi_2 \circ \phi_1$ is then also an isogeny, in particular non-zero. This proves the first part.

The variant follows by applying the first part to $\phi_2 - \phi_2'$. □

Corollary 10.3. *Let $\phi : E_1 \to E_2$ be an isogeny of degree n. Then there exists a unique isogeny $\phi^* : E_2 \to E_1$, called its dual, such that*

$$\phi^* \circ \phi = [n]_{E_1}, \quad \phi \circ \phi^* = [n]_{E_2}.$$

Proof. By Deligne's Theorem (Theorem 9.23), $\ker(\phi)$ is n-torsion. This means $\ker(\phi) \subseteq E[n]$. Proposition 10.1 implies that there exists an isogeny ϕ^* with $\phi^* \circ \phi = [n]_{E_1}$. Then

$$\phi \circ \phi^* \circ \phi = \phi \circ [n]_{E_1} \overset{(\star)}{=} [n]_{E_2} \circ \phi$$

where $(\star)$ is due to the fact that $[n]$ commutes with every group homomorphism. The cancellation law from Lemma 10.2 implies that also $\phi \circ \phi^* = [n]_{E_2}$. □

Definition 10.4. Let S be a quasi-compact scheme, and let E, E_1, E_2 be elliptic curves over S. We define

$$\mathrm{Hom}^0(E_1, E_2) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(E_1, E_2), \quad \mathrm{End}^0(E) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E).$$

Its elements are called quasi-homomorphisms resp. quasi-endomorphisms. An element that is fiber-wise non-zero is called a quasi-isogeny.

Corollary 10.5. *Let E be an elliptic curve over a field. Then $\mathrm{End}^0(E)$ is a skew-field of characteristic 0.*

Proof. This means $n\phi \neq 0$ for all $\phi \neq 0$ and $\phi\psi \neq 0$ whenever $\phi, \psi \neq 0$. These statements follow from Lemma 10.2 and Theorem 9.5. □

10.2. **The Rosati involution.** Corollary 10.3 constructed a bijection (set $0^* = 0$)

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(E_2, E_1), \quad \phi \longmapsto \phi^*.$$

It is clear from its construction that $\deg(\phi) = \deg(\phi^*)$, that $(\phi^*)^* = \phi$ and that $(\phi\psi)^* = \psi^*\phi^*$. We would like to show more properties, especially that ϕ is a group homomorphism. To this end, we next introduce the Rosat involution $\phi \mapsto \phi^\dagger$ and show $\phi^* = \phi^\dagger$.

Construction 10.6. Recall that $\mathrm{Pic}^0_E \to S$ is our notation for the Picard functor of E. Also recall that we proved in Theorem 7.20 that Pic^0_E is representable and that there is a group scheme isomorphism[14]

$$\begin{aligned} \lambda_E : E &\xrightarrow{\sim} \mathrm{Pic}^0_E \\ E(T) \ni x &\longmapsto [\mathcal{O}_{E_T}([\Gamma_x] - [\Gamma_e])]. \end{aligned} \tag{10.3}$$

[14] see again Footnote 10

Assume that $\phi : E_1 \to E_2$ is a homomorphism and that $[\mathcal{L}] \in \mathrm{Pic}^0_{E_2}(T)$. Then pullback defines a point $[\phi_T^*(\mathcal{L})] \in \mathrm{Pic}^0_{E_1}(T)$ which defines an S-group scheme homomorphism (use Yoneda)

$$\phi^\vee : \mathrm{Pic}^0_{E_2} \longrightarrow \mathrm{Pic}^0_{E_1}.$$

Taking compositions, we obtain a group scheme homomorphism

$$\phi^\dagger := \lambda_{E_1}^{-1} \circ \phi^\vee \circ \lambda_{E_2} \in \mathrm{Hom}(E_2, E_1). \tag{10.4}$$

Definition 10.7. The isomorphism λ_E in (10.3) is called the polarization of E. The map $\phi^\dagger$ in (10.4) is called the Rosati adjoint of ϕ.

Theorem 10.8. *(1) The Rosati adjoint $\phi^\dagger$ and the dual homomorphism ϕ^* are equal. In particular, $(\phi^\dagger)^\dagger = \phi$.*
(2) The Rosati adjoint is a group homomorphism, meaning

$$(\phi + \psi)^* = \phi^* + \psi^*.$$

Proof. (1) We need to see $\phi^\dagger \circ \phi = [\deg(\phi)]$. By the rigidity theorem in the form of Corollary 7.26, we can check this fiber-wise. Thus assume E_1 and E_2 are elliptic curves over an algebraically closed field k and let $\phi : E_1 \to E_2$ be an isogeny. It is enough to check that $\phi^\dagger \circ \phi = [\deg(\phi)]$ on the k-valued points $E_1(k)$.[15] So let $x \in E_1(k)$ be a k-rational point. Then

$$\begin{aligned}
\phi^\dagger(\phi(x)) &= \lambda_{E_1}^{-1}(\phi^\vee(\lambda_{E_2}(\phi(x)))) \\
&= \lambda_{E_1}^{-1}(\phi^* \mathcal{O}_{E_2}([\phi(x)] - [e])) \\
&= \lambda_{E_1}^{-1}(\mathcal{O}_{E_1}([\ker(\phi) + x] - [\ker(\phi)])).
\end{aligned}$$

Here, $\ker(\phi) + x$ denotes the x-translate of the finite subscheme $\ker(\phi) \subset E_1$. By definition of λ_{E_1}, we are now looking for the unique point $y \in E_1(k)$ such that

$$\mathcal{O}_{E_1}([\ker(\phi) + x] - [\ker(\phi)]) \xrightarrow{\sim} \mathcal{O}_{E_1}([y] - [e]). \tag{10.5}$$

Recall the fundamental relation of addition from (7.1). By induction, it extends to the following relation. Given divisors $D_+ = \sum_{P \in E(k)} n_P [P]$ and $D_- = \sum_{P \in E(k)} m_P [P]$ with $\deg(D_+) = \deg(D_-)$,

$$\mathcal{O}_E([D_+] - [D_-]) \xrightarrow{\sim} \mathcal{O}_E([Q] - [e])$$

where Q is the E-sum $E\text{-}\sum_P (n_P - m_P)P$ meaning the sum with respect to the elliptic curve addition law. We apply this with $D_+ = [\ker(\phi) + x]$ and $D_- = [\ker(\phi)]$ as in (10.5). As divisor,

$$[\ker(\phi)] = \dim_k \mathcal{O}_{\ker(\phi),e} \cdot \sum_{y \in \ker(\phi)(k)} [y].$$

Thus we obtain the E-sum

$$\begin{aligned}
Q &= \dim_k \mathcal{O}_{\ker(\phi),e} \cdot_E E\text{-}\sum_{y \in \ker(\phi)(k)} (y +_E x -_E y) \\
&= \dim_k \mathcal{O}_{\ker(\phi),e} \cdot |\ker(\phi)(k)| \cdot_E x \\
&= [\deg(\phi)](x).
\end{aligned}$$

In other words, $\phi^\dagger(\phi(x)) = [\deg(\phi)](x)$ as was to be shown.

(2) We now prove that $(\phi + \psi)^\dagger = \phi^\dagger + \psi^\dagger$. It is clear that $\lambda_{E_1}^{-1} \circ -$ and $- \circ \lambda_{E_2}$ are linear, so we really need to show that $(\phi + \psi)^\vee = \phi^\vee + \psi^\vee$. Again by rigidity, we may prove this identity fiber-wise over S and hence assume we are working over an algebraically

[15] A morphism of reduced finite type schemes over an algebraically closed field k is uniquely determined by its restriction to k-points.

closed field k. It again suffices to show $(\phi+\psi)^*(\mathcal{L}) = \phi^*(\mathcal{L}) \otimes \psi^*(\mathcal{L})$ for k-rational points $\mathcal{L} \in \mathrm{Pic}^0_{E_2}(k) = \mathrm{Pic}^0(E_2)$, see Footnote 15.

Consider the map

$$\alpha : \phi \circ p_1 + \psi \circ p_2 : E_1 \times_k E_1 \longrightarrow E_2.$$

Given a degree 0 line bundle $\mathcal{L} \in \mathrm{Pic}^0(E_2)$, define

$$\mathcal{M} = \alpha^*\mathcal{L} \otimes p_1^*\phi^*\mathcal{L}^{-1} \otimes p_2^*\psi^*\mathcal{L}^{-1}.$$

We need to see that the restriction $\mathcal{M}|_\Delta \xrightarrow{\sim} \mathcal{O}_{E_1}$. In fact, it even holds that $\mathcal{M} \xrightarrow{\sim} \mathcal{O}_{E_1 \times_k E_1}$. Namely, view $E_1 \times_k E_1$ as an E_1-scheme via the first projection and view $\mathcal{M}$ as an E_1-valued point $[\mathcal{M}] \in \mathrm{Pic}^0_{E_1}(E_1)$. Its fiber over some $y \in E_1(k)$ is

$$\mathcal{M}(y) = \psi^* t^*_{\phi(y)}\mathcal{L} \otimes \psi^*\mathcal{L}^{-1} = \psi^*(t^*_{\phi(y)}\mathcal{L} \otimes \mathcal{L}^{-1})$$

where $t_{\phi(y)} : E_2 \to E_2$ is the translation map $z \mapsto z + \phi(y)$. But since $\mathcal{L}$ is of degree 0, there exists a point $Q \in E_2(k)$ with $\mathcal{L} \cong \lambda_{E_2}(Q) = \mathcal{O}_{E_2}([Q] - [e])$. Then we may again use the fundamental relation (7.1) and see

$$\mathcal{M}(y) = \psi^*(\mathcal{O}_{E_2}([Q - \phi(y)] - [-\phi(y)] - [Q] + [e])) \overset{(7.1)}{\cong} \psi^*(\mathcal{O}_{E_2}) = \mathcal{O}_{E_1}.$$

So we see that $\mathcal{M}(y)$ is trivial for every closed point $y \in E_1$. As E_1 is reduced, this means that the morphism $[\mathcal{M}] : E_1 \to \mathrm{Pic}^0_{E_1}$ is constant equal to the neutral element $[\mathcal{O}_{E_1}]$. By definition of $\mathrm{Pic}^0_{E_1}$, see (7.11), this means that there exists a line bundle $\mathcal{N}$ on E_1 with $\mathcal{M} \cong p_1^*\mathcal{N}$. Looking at the restriction to $E_1 \times_k \{e\}$, we find

$$\mathcal{N} = e^*\mathcal{M} = e^*(\phi^*\mathcal{L} \otimes \phi^*\mathcal{L}^{-1}) = \mathcal{O}_{E_1}.$$

In conclusion, $\mathcal{M}$ is trivial. This implies that the restriction

$$\Delta^*(\mathcal{M}) = (\phi+\psi)^*(\mathcal{L}) \otimes \phi^*(\mathcal{L})^{-1} \otimes \psi^*(\mathcal{L})^{-1}$$

is trivial, and the proof of the theorem is complete. □

Next, we discuss some applications. These will be purely arithmetic, no algebraic geometry involved. Let E be an elliptic curve over a field k. Recall that $\mathrm{End}(E)$ has no zero-divisors and is $\mathbb{Z}$-torsion free (Corollary 10.5). By Theorem 10.8, the Rosati involution on $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is an involution in the sense that

$$*^2 = \mathrm{id}, \quad (x+y)^* = x^* + y^*, \quad (xy)^* = y^*x^*.$$

These three properties give the usual definition of an involution on a (not necessarily commutative) ring.

Proposition 10.9. *The Rosati involution on* $\mathrm{End}(E)$ *has the following properties.*
(1) For every $x \in \mathrm{End}(E)$*, the endomorphism* $\mathrm{tr}(x) = x + x^*$ *lies in* $\mathbb{Z}$*. It is called the trace of* x*. In particular, the subring* $\mathbb{Z}[x] \subset \mathrm{End}(E)$ *generated by* x *is stable under* $*$*.*
(2) If $x \notin \mathbb{Z}$*, then* $\mathbb{Z}[x]$ *is an order in an imaginary-quadratic extension of* $\mathbb{Q}$*. In particular,* $\mathrm{End}(E)^{*=\mathrm{id}} = \mathbb{Z}$*.*
(3) More precisely, x *is a zero of the following quadratic equation with coefficients in* $\mathbb{Z}$

$$(T - x)(T - x^*) = T^2 - \mathrm{tr}(x)T + \deg(x). \tag{10.6}$$

If $x \notin \mathbb{Z}$*, then* $\mathrm{tr}(x)^2 - 4\deg(x) < 0$*, so* $\mathbb{Q}(x)$ *is an imaginary-quadratic extension.*

Proof. Let $x, y \in \mathrm{End}(E)$ be two endomorphisms. By Theorem 10.8,

$$\begin{aligned}\deg(x+y) &= (x+y)^*(x+y)\\ &= x^*x + (x^*y + xy^*) + y^*y\\ &= \deg(x) + \mathrm{tr}(xy^*) + \deg(y).\end{aligned}$$

Since $\deg(x+y)$, $\deg(x)$ and $\deg(y)$ all lie in $\mathbb{Z}$, we obtain that $\mathrm{tr}(xy^*) \in \mathbb{Z}$. Apply this with $y = 1$ (meaning $y = \mathrm{id}_E$) to obtain that $\mathrm{tr}(x) \in \mathbb{Z}$. Then $x^* = \mathrm{tr}(x) - x \in \mathbb{Z}[x]$. This implies that $\mathbb{Z}[x]$ is $*$-stable and we have proved (1).

Next, it is clear that x is a zero of (10.6). Namely,

$$x^2 - (x + x^*)x + x^*x = x^2 - x^2 - x^*x + x^*x = 0.$$

For every $p/q \in \mathbb{Q}$, $q \neq 0$, we have

$$\left(\frac{p}{q}\right)^2 - \mathrm{tr}(x)\left(\frac{p}{q}\right) + \deg(x) = \frac{\deg(p - qx)}{q^2} \geq 0.$$

So $\lambda^2 - \mathrm{tr}(x)\lambda + \deg(x) \geq 0$ for every $\lambda \in \mathbb{R}$, which means that either $T^2 - \mathrm{tr}(x)T + \deg(x)$ has a double zero in $\mathbb{R}$ or defines an imaginary-quadratic extension of $\mathbb{Q}$. The first case happens if and only if $x = x^*$. Then $2x = \mathrm{tr}(x) \in \mathbb{Z}$ and hence $x \in \mathbb{Q}$. But x is also integral over $\mathbb{Z}$ because it is a zero of $T^2 - \mathrm{tr}(x)T + \deg(x)$, and so even $x \in \mathbb{Z}$. This proves (2) and (3). □

Corollary 10.10. *Assume that* $\mathrm{End}(E)$ *is commutative. Then* $K := \mathrm{End}^0(E)$ *equals* $\mathbb{Q}$ *or an imaginary-quadratic extension of* $\mathbb{Q}$.

Proof. If $\mathrm{End}(E)$ is commutative, then K is a field by Corollary 10.5. Then $* \in \mathrm{Aut}(K)$ is a field automorphism. Moreover, Proposition 10.9 established that $K^{*=\mathrm{id}} = \mathbb{Q}$. So K is either $\mathbb{Q}$ or a quadratic extension. By Proposition 10.9 again, such a quadratic extension has to be imaginary. □

Corollary 10.11. *Assume that* $\mathrm{End}(E)$ *is non-commutative. Then* $B := \mathrm{End}^0(E)$ *is a quaternion algebra over* $\mathbb{Q}$ *and the Rosati involution equals the main involution of* B. *By definition this means that there exist* $a, b \in \mathbb{Q}^\times$ *as well as* $i, j, k \in B$ *such that*

$$B = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$$

with

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k$$

and

$$i^* = -i, \quad j^* = -j, \quad k^* = -k.$$

Moreover, B *is definite in the sense that*

$$\mathbb{R} \otimes_{\mathbb{Q}} B \cong \mathbb{H} \qquad \textit{(Hamilton quaternions)}.$$

Finally, $\mathrm{End}(E) \subset B$ *is a lattice.*

Proof. Since B is non-commutative, $B \neq \mathbb{Q}$. Let $x \in B \setminus \mathbb{Q}$ and set $K = \mathbb{Q}(x)$. This is a quadratic extension of $\mathbb{Q}$. The Rosati involution preserves K by Proposition 10.9 and hence agrees with the Galois conjugation of $K/\mathbb{Q}$. Choose $i \in K^\times$ with $i^* = -i$ and set $a = i^2 \in \mathbb{Q}^\times$.

Next, B can be viewed as K-vector space via left-multiplication or via right-multiplication. In this way, B becomes a $K \otimes_{\mathbb{Q}} K$-module,

$$(x \otimes y) \cdot \alpha := x\alpha y.$$

As ring, $K \otimes_{\mathbb{Q}} K \cong K \times K$, so we obtain a decomposition $B = B_0 \times B_1$ with

$$B_0 = \{\alpha \in B \mid x\alpha = \alpha x \ \forall x \in K\}, \quad B_1 = \{\alpha \in B \mid x\alpha = \alpha x^* \ \forall x \in K\}. \tag{10.7}$$

For every $\alpha \in B_0$, the ring $K(\alpha)$ is a finite commutative $\mathbb{Q}$-algebra without zero-divisors, meaning a finite field extension. Since $*$ preserves $K(\alpha)$ (Proposition 10.9) and satisfies $K(\alpha)^{*=\mathrm{id}} = \mathbb{Q}$, it has to be a quadratic extension of $\mathbb{Q}$. So we see that $K(\alpha) = K$, and hence that $B_0 = K$.

Our assumption is that B is non-commutative. So $K \subsetneq B$, meaning $B_1 \neq 0$. For any two non-zero $j_1, j_2 \in B_1$, the definition of B_1 by (10.7) implies that $j_1 j_2 \in K$. This means

that B_1 is a 1-dimensional K-vector space via left-multiplication. Let $j \in B_1$ be any generator and set $k = ij$. Then

$$ji \overset{\text{Def. of } B_1}{=} (i^*)j = -ij$$

as required.

Consider next the Rosati involution. For $x \in K$, we have

$$(j^*)x = ((x^*)j)^* = (jx)^* = (x^*)(j^*)$$

which means that $j^* \in B_1$. Write $j^* = cj$ with $c \in K$. Then

$$j = (j^*)^* = (cj)^* = j^*c^* = cjc^* \overset{j \in B_1}{=} c^2 j$$

implies that $c^2 = 1$. Since $B^{*=\mathrm{id}} = \mathbb{Q}$, the case $c = 1$ is excluded. This means $c = -1$. As j was fixed arbitrarily, also $k^* = -k$. Alternatively, we directly see that

$$(ij)^* = j^*i^* = -ji^* = -ij.$$

Moreover, $j^* = -j$ implies that

$$b := j^2 = -j^*j \in \mathbb{Q}^\times.$$

At this point, we have shown that B is a quaternion division algebra and that $*$ is its main involution. The fact that $\mathrm{End}(E) \subset B$ is a lattice will be shown in Lemma 10.15. It is then only left to prove that $\mathbb{R} \otimes_{\mathbb{Q}} B \cong \mathbb{H}$. Observe for this that $a, b < 0$ because $\mathbb{Q}(i)$ and $\mathbb{Q}(j)$ have to be imaginary quadratic extensions of $\mathbb{Q}$ (Proposition 10.9). Then

$$i' = \sqrt{-a} \otimes i, \quad j' = \sqrt{-b} \otimes j, \quad k' = i'j'$$

give a standard Hamilton quaternion basis for $\mathbb{R} \otimes_{\mathbb{Q}} B$. □

10.3. **The Tate module.** In §8, we studied elliptic curves over $\mathbb{C}$ in terms of $\mathbb{Z}$-lattices. This technique (obviously) does not extend to fields of characteristic p. However, there is a substitute called the ℓ-adic Tate module which we will introduce next. As an application, we will obtain a remarkable refinement of Corollary 10.11.

Definition 10.12. Given E/k and an integer $\ell \neq \mathrm{char}(k)$, we define the ℓ-adic Tate module of E as

$$T_\ell(E) := \varprojlim_{n \geq 1} E[\ell^n](\bar{k}).$$

The transition maps here are given by multiplication by ℓ,

$$[\ell] : E[\ell^{n+1}] \longrightarrow E[\ell].$$

By Theorem 9.5, it is free of rank 2 as $\mathbb{Z}_\ell$-module. We also set $V_\ell(E) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E)$ which is a 2-dimensional $\mathbb{Q}_\ell$-vector space. It is called the rational Tate module of E.

Any homomorphism $\phi : E_1 \to E_2$ restricts to a compatible family of homomorphisms $\phi[\ell^n] : E_1[\ell^n] \to E_2[\ell^n]$ between ℓ^n-torsion group schemes, and so defines a $\mathbb{Z}_\ell$-linear map $T_\ell(\phi) : T_\ell(E_1) \to T_\ell(E_2)$. In other words, $T_\ell(-)$ is a covariant functor from elliptic curves over k to $\mathbb{Z}_\ell$-modules.

Theorem 10.13. *Let E_1 and E_2 be elliptic curves over k. Then the natural map*

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$

is injective.

Remark 10.14. Note that this is stronger than just saying that the map from $\mathrm{Hom}(E_1, E_2)$ to $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ is injective. For example, $V = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ is a 2-dimensional $\mathbb{Q}$-subvector space, but $\mathbb{R} \otimes_{\mathbb{Q}} V \to \mathbb{R}$ is not injective.

Lemma 10.15. *The $\mathbb{Z}$-module $\mathrm{Hom}(E_1, E_2)$ is finitely generated.*

Proof. We have seen in Corollaries 10.10 and 10.11 that $\mathrm{End}^0(E_2)$ is a finite-dimensional $\mathbb{Q}$-vector space. By Proposition 10.1 and Lemma 10.2, $\mathrm{Hom}^0(E_1, E_2)$ is either 0 or a one-dimensional $\mathrm{End}^0(E_2)$-vector space. In particular, $V = \mathrm{Hom}^0(E_1, E_2)$ is a finite-dimensional $\mathbb{Q}$-vector space and we win once we can show that $L = \mathrm{Hom}(E_1, E_2) \subset V_{\mathbb{R}} = \mathbb{R} \otimes_{\mathbb{Q}} V$ is discrete.

Consider the degree map $\deg : L \to \mathbb{Z}_{\geq 0}$ and note that it only takes positive values (except $\deg(0) = 0$). By Theorem 10.8 (2), there exists a symmetric bilinear form $\beta : L \times L \to \mathbb{Z}$ such that $\deg(x) = \beta(x, x)$, namely

$$\beta(x, y) = x^* \circ y. \tag{10.8}$$

We may uniquely extend β to an $\mathbb{R}$-bilinear form $V_{\mathbb{R}} \times V_{\mathbb{R}} \to \mathbb{R}$ by $\beta(\lambda \otimes x, \mu \otimes y) = \lambda\mu\beta(x, y)$. This form is positive definite because $\deg|_L$ is positive definite. We find that

$$L \cap \{x \in V_{\mathbb{R}} \mid \beta(x, x) < 1\} = \{0\},$$

and hence that L is discrete in $V_{\mathbb{R}}$. □

Remark 10.16. The statement that (10.8) is bilinear, and the overall argument of Lemma 10.15, really require Theorem 10.8 (2). Just knowing that $\deg(n\phi) = n^2 \deg(\phi)$ (which follows directly from definitions) is not enough and does not allow to define deg in a meaningful way to $V_{\mathbb{R}}$.

Proof of Theorem 10.13. First observe that there is an isomorphism (natural in E)

$$\begin{aligned} T_\ell(E)/\ell^n T_\ell(E) &\xrightarrow{\sim} E[\ell^n](\bar{k}) \\ (\ldots, x_3, x_2, x_1) &\longmapsto x_n. \end{aligned}$$

Also note that because $L = \mathrm{Hom}(E_1, E_2)$ is finitely generated by Lemma 10.15, i.e. abstractly isomorphic to $\mathbb{Z}^r$ for some $r \geq 1$, the tensor product $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}(E_1, E_2)$ coincides with its ℓ-adic completion L_ℓ. Now consider some $\widetilde{\phi}$ that lies in the kernel of $L_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$. We can assume that ϕ is not divisible by ℓ in L_ℓ. Let $\phi \in L$ be an approximation in the sense that $\phi - \widetilde{\phi} \in \ell L_\ell$. But then both $\widetilde{\phi}$ and $\phi - \widetilde{\phi}$ restrict to zero on $E_1[\ell]$. Proposition 10.1 then implies that ϕ is divisible by ℓ in L. Then $\widetilde{\phi}$ is divisible by ℓ in L_ℓ — contradiction! □

We can now complete our classification of $\mathrm{End}^0(E)$. Recall that by Proposition 8.3 (2), the case $\mathrm{End}^0(E)$ non-commutative can only occur when $\mathrm{char}(k) = p > 0$.

Corollary 10.17. *Assume that* $\mathrm{char}(k) = p > 0$ *and that* $\mathrm{End}(E)$ *is non-commutative like in Corollary 10.11; set* $B = \mathrm{End}^0(E)$. *Then for every* $\ell \neq p$,

$$\mathbb{Q}_\ell \otimes_{\mathbb{Q}} B \cong M_2(\mathbb{Q}_\ell).$$

That is, B is the (up to isomorphism) unique quaternion division algebra over $\mathbb{Q}$ that is non-split at p and ∞.

Proof. For every $\ell \neq p$, consider the the action of B_ℓ on the rational Tate module $V_\ell(E)$. By Theorem 10.13, it is faithful, meaning induced from an injective map of $\mathbb{Q}_\ell$-algebras

$$B_\ell \longmapsto \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(E)) \cong M_2(\mathbb{Q}_\ell).$$

Both sides here are 4-dimensional $\mathbb{Q}_\ell$-vector spaces, so the map is an isomorphism. The uniqueness statement follows from the classification of central simple algebras over number fields, which is part of class field theory. □

Here are two interesting results to conclude this section.

(1) Let E be an elliptic curve over a field k of $\mathrm{char}(k) = p$ such that $\mathrm{End}^0(\bar{k} \otimes_k E)$ is non-commutative. Such elliptic curves are called supersingular. Then there exists an elliptic

curve E_0 over $\mathbb{F}_{p^2}$ such that $\bar{k} \otimes_k E \cong \bar{k} \otimes_{\mathbb{F}_{p^2}} E_0$. In this sense all supersingular elliptic curves are defined over $\mathbb{F}_{p^2}$.

(2) The mass formula of Deuring–Eichler states that the number of supersingular elliptic curves is given by

$$\sum_{\{E \text{ supersing}\}/\sim} \frac{1}{|\mathrm{Aut}(E)|} = \frac{p-1}{24}. \tag{10.9}$$

Here, the sum runs over all isomorphism classes of supersingular elliptic curves over $\bar{\mathbb{F}}_p$.

Part 3. Moduli Spaces

11. The classification problem

11.1. The j-invariant.

Problem 11.1. Classify elliptic curves up to isomorphism over an algebraically closed field.

This problem follows a familiar pattern: Given an interesting type of structure, classify all its objects up to isomorphism.

Definition 11.2. Let E be an elliptic curve over a field k of characteristic $\neq 2, 3$. Let $y^2 = x^3 + ax + b$ be a simplified affine Weierstrass equation for E. Then its j-invariant $j(E) \in k$ is defined as

$$j(E) := -1728\frac{4a^3}{\Delta}, \quad \Delta = -(4a^3 + 27b^2).$$

The j-invariant can also be defined for elliptic curves in characteristics 2 and 3. Then the formula will be in terms of the coefficients of a general Weierstrass equation (6.22). The factor $1728 = 27 \cdot 64$ is added for consistency with this more general formula.

Lemma 11.3. *The j-invariant $j(E)$ is well-defined, meaning only depends on the isomorphism class of E and not on the choice of simplified Weierstrass equation.*

Before giving the proof, let us fix a convention for Weierstrass equations. For any choice of two non-zero elements

$$x \in \Gamma(E, \mathcal{O}_E(2[e])) \setminus k, \qquad y \in \Gamma(E, \mathcal{O}_E(3[e])) \setminus \Gamma(E, \mathcal{O}_E(2[e])), \tag{11.1}$$

we have seen in (6.21) that there exists a non-trivial linear relation amongst $1, x, y, x^2, xy, x^3$ and y^2. This relation is unique up to scaling by $k^\times$. By convention, we normalize it to be monic in y^2. That is, there is we consider the unique relation of the form

$$y^2 + a_1xy + a_3y = a_0x^3 + a_2x^2 + a_4x + a_6. \tag{11.2}$$

satisfied by x, y, and we call it *the* Weierstrass equation defined by x and y.

Proof of Lemma 11.3. The choice of x and y in (11.1) is unique up to linear transformations of the form

$$\begin{aligned} x &= ux' + p \\ y &= vy' + qx' + r \end{aligned} \tag{11.3}$$

where x', y' are as in (11.1), where $u, v \in k^\times$ and where $p, q, r \in k$. Now assume that x and y are such that their Weierstrass equation is simplified. Substituting (11.3) in $y^2 = x^3 + ax + b$ leads to terms of the form $2vqx'y'$ and $2vry'$. If we insist that the Weierstrass equation for x' and y' is again simplified, then this implies $q = r = 0$. Then we also obtain that $p = 0$ for otherwise there would be the non-zero term $3u^2p(x')^2$. Finally, we find $u^3 = v^2$. In summary, this argument proves that the choice of x and y in (11.1) with simplified Weierstrass equation is unique up to the scaling operation

$$x' = ux, \quad y' = vy, \quad u, v \in k^\times, \quad u^3 = v^2. \tag{11.4}$$

Rescaling

$$(vy)^2 = (ux)^3 + a(ux) + b$$

by $v^{-2} = u^{-3}$ (in order to be monic in y^2) shows that x' and y' give the Weierstrass equation

$$(y')^2 = (x')^3 + u^{-2}ax' + u^{-3}b. \tag{11.5}$$

The identity

$$\frac{(u^{-2}a)^3}{4(u^{-2}a)^3+27(u^{-3}b)^2}=\frac{a^3}{4a^3+27b^2}$$

now shows that the definition of $j(E)$ is independent of the chosen simplified Weierstrass equation. □

Theorem 11.4. *Let k be a field. The j-invariant defines a surjective map*

$$j:\{\textit{Ellipt. curves}/k\}/\sim \twoheadrightarrow k. \tag{11.6}$$

If k is algebraically closed, then this map is also injective. That is, two elliptic curves E, E' over k are isomorphic if and only if $j(E)=j(E')$.

Proof. We stick to $\mathrm{char}(k)\neq 2,3$ and use Definition 11.2.

Surjectivity. Taking $(a,b)=(0,1)$ and $(a,b)=(1,0)$ constructs elliptic curves with $j(E)=0$ and $j(E)=1$. It is left to prove that for any $j\neq 0,1$, we can solve the equation

$$-1728\frac{4a^3}{-(4a^3+27b^2)}=j \tag{11.7}$$

with $a,b\in k$. (Note that the denominator $-(4a^3+27b^2)$ is the discriminant Δ of x^3+ax+b. Thus for any choices a,b with $\Delta\neq 0$, the equation $y^2=x^3+ax+b$ defines an elliptic curve.) Rewriting (11.7) gives

$$1728\cdot\frac{4a^3}{27b^2}=\frac{j}{1-j}. \tag{11.8}$$

Take any $a,b\neq 0$. Scaling both by $\lambda\in k^\times$ scales a^3/b^2 by λ. This shows that (11.8) has a solution.

Injectivity. Short preparation. Now assume that k is algebraically closed. Let a,b be the coefficients of a simplified Weierstrass equation. They cannot both be zero. Assume $a\neq 0$. Since k is algebraically closed and $\mathrm{char}(k)\neq 2$, there exists a square root u of a. Scaling as in (11.4) and (11.5), we may assume $a=1$. Assume otherwise that $b\neq 0$. Since k is algebraically closed and $\mathrm{char}(k)\neq 3$, there exists a cubic root of b. Scaling as before, we may assume that $b=1$.

Injectivity. Final argument. Now consider E,E' over k with $j(E)=j(E')$. Let a,b resp. a',b' be the coefficients of simplified Weierestrass equations for E and E'. If $a=0$, then $j(E)=0$ and hence $a'=0$. If $b=0$, then $j(E)=1$ and hence $b'=0$. Thus in all cases, at least a,a' or b,b' are both non-zero. By the above preparation, we may assume $a=a'=1$ or $b=b'=1$. Then our assumption

$$\frac{4a^3}{4a^3+27b^2}=\frac{4(a')^3}{4(a')^3+27(b')^2}$$

implies that

$$\begin{cases} b^2=(b')^2 & \text{if } a=a'=1\\ a^3=(a')^3 & \text{if } b=b'=1.\end{cases}$$

In the first case, we may scale by $u\in\{\pm 1\}$ in (11.5) as needed to arrange $b=b'$. In the second case, we may scale with u a third root of unity to arrange $a=a'$. In both cases, we find that E and E' can be defined by the same Weierstrass equation, meaning that $E\cong E'$. □

Corollary 11.5 (Field of definition)**.** *Let E be an elliptic curve over a field k. Then $k_0=\mathbb{Q}(j(E))$ resp. $k_0=\mathbb{F}_p(j(E))$, depending on* $\mathrm{char}(k)$*, is the smallest subfield over which E can be defined in the following sense. There exists an elliptic curve E_0 over k_0 such that $k\otimes_{k_0}E_0\cong E$.*

Proof. If $k_0 \subseteq k$ is a subfield and E_0/k_0 and elliptic curve with $k \otimes_{k_0} E_0 \cong E$, then $j(E) = j(E_0) \in k_0$. This explains the "smallest" assertion. The existence is by Theorem 11.4. □

Example 11.6. Let $k_0 \subseteq k$ be a field extension and let E_0, E_0' be elliptic curves over k_0 such that $k \otimes_{k_0} E_0 \cong k \otimes_{k_0} E_0'$. Then it is not necessarily the case that $E_0 \cong E_0'$. The j-invariant on the other hand can be computed after base change, so $j(E_0) = j(E_0')$. This phenomenon spells out the (possible) failure of the injectivity of (11.6) for fields that are not algebraically closed.

Consider for example a square-free integer $D \geq 2$ and the two Weierstrass equations (over $\mathbb{Q}$)

$$y^2 = x^3 + ax + b, \qquad Dy^2 = x^3 + ax + b.$$

Over $\mathbb{Q}(\sqrt{D})$, there is the substitution $y' = \sqrt{D}y$ that transforms one into the other. Thus the elliptic curves defined by by the two equations are isomorphic over $\mathbb{Q}(\sqrt{D})$ and in particular have the same j-invariant. On the other hand, one may check that there are no substitutions of the form (11.3) over $\mathbb{Q}$ that transform one Weierstrass equation into (a $\mathbb{Q}^\times$-multiple of) the other.

11.2. **Moduli spaces.** We would like to go beyond a simple classification of isomorphism classes over algebraically closed fields. Let us first briefly recall the Yoneda formalism. Consider a functor

$$F : (\mathrm{Sch})^{\mathrm{op}} \longrightarrow (\mathrm{Set}) \tag{11.9}$$

and a scheme $\mathcal{M}$. Denote by $h_{\mathcal{M}}$ the functor of points of $\mathcal{M}$.

Lemma 11.7 (Yoneda)**.** *There is a bijection between natural transformations $h_{\mathcal{M}} \to F$ and $F(\mathcal{M})$ given by*

$$\begin{aligned} \mathrm{Mor}(h_{\mathcal{M}}, F) &\xrightarrow{\sim} F(\mathcal{M}) \\ \gamma &\longmapsto \gamma(\mathrm{id}_{\mathcal{M}}) \\ [(S \xrightarrow{u} \mathcal{M}) \longmapsto u^*\alpha] &\longleftarrow\!\shortmid \alpha. \end{aligned} \tag{11.10}$$

Definition 11.8 (Fine moduli space)**.** The functor F is called representable if there exists a scheme $\mathcal{M}$ and a natural isomorphism $\gamma : h_{\mathcal{M}} \to F$. In this case $\mathcal{M}$ is said to represent F and is called a fine moduli space for F. The element $\alpha = \gamma(\mathrm{id}_{\mathcal{M}}) \in F(\mathcal{M})$ is called the universal object.

Consider now the functor of isomorphism classes of elliptic curves

$$\begin{aligned} \mathcal{E}\ell\ell : (\mathrm{Sch})^{\mathrm{op}} &\longrightarrow (\mathrm{Set}) \\ S &\longmapsto \{\text{Ellipt. curves } E \text{ over } S\}/\sim . \end{aligned} \tag{11.11}$$

In an ideal world, this functor would be representable by a scheme $\mathcal{M}$, which would be the moduli space we are interested in. The universal object would be an elliptic curve $\mathcal{E}$ over $\mathcal{M}$ (up to isomorphism) that would be universal in the sense that for ever scheme S and every elliptic curve E/S, there exists a unique morphism $u : S \to \mathcal{M}$ such that

$$E \cong u^*\mathcal{E}.$$

However, reality is more interesting than this rosy picture. For starters, an easy argument shows that $\mathcal{E}\ell\ell$ cannot be representable. Namely, for every scheme $\mathcal{M}$ and every field extension $k_0 \subseteq k$, the pullback map $\mathcal{M}(k_0) \to \mathcal{M}(k)$ is injective. (More generally, $\mathcal{M}(A) \to \mathcal{M}(B)$ is injective for every faithfully flat ring map $A \to B$.) But Example 11.6 explained that the map

$$\mathcal{E}\ell\ell(k_0) \longrightarrow \mathcal{E}\ell\ell(k)$$

need not be injective. So $\mathcal{E}\ell\ell$ cannot be representable. There are now different ways to proceed:

(1) One may insist on working with a representable functor, which requires one to modify $\mathcal{E}\ell\ell$. The standard approach for this is to add level structure to its definition.

(2) If one instead desires to work with $\mathcal{E}\ell\ell$ directly, then one may relax the notion of fine moduli space. There is a definition of coarse moduli space that can be understood as the best approximation of $\mathcal{E}\ell\ell$ by a scheme.

(3) Finally, one can extend the formalism from schemes to stacks. Then one can make sense of the statement that $\mathcal{E}\ell\ell$ is representable by a Deligne–Mumford stack.

Our aim for the remainder of the course is to explain (1) and (2) which are also prerequisites for (3).

12. Weierstrass Moduli

Let $p : E \to S$ be an elliptic curve oven S. Define $\omega_E := e^*\Omega^1_{E/S}$ which is a line bundle on S. It is called the Hodge bundle of E. Recall that we constructed a natural isomorphism (Proposition 5.7)

$$p^*\omega_E \xrightarrow{\sim} \Omega^1_{E/S}.$$

Applying the pushforward p_*, we find

$$\omega_E \xrightarrow{\sim} p_*p^*\omega_E \xrightarrow{\sim} p_*\Omega^1_{E/S}.$$

The first isomorphism here is because $\mathcal{O}_S \xrightarrow{\sim} p_*\mathcal{O}_E$ (Lemma 7.23). In this way, there is a bijection

$$\begin{aligned} \{\text{Generators } \pi \in \Omega^1_{E/S}(E)\} &\longleftrightarrow \{\text{Generators } \bar{\pi} \in \omega_E(S)\} \\ \pi &\longmapsto e^*(\pi). \end{aligned} \tag{12.1}$$

Definition 12.1. The Weierstrass moduli problem is the functor

$$\begin{aligned} \mathcal{W} : (\mathrm{Sch}/\mathbb{Z}[1/6])^{\mathrm{op}} &\longrightarrow (\mathrm{Set}) \\ S &\longmapsto \left\{ (E,\pi) \,\middle|\, \begin{array}{c} E \text{ ellipt. curve over } S \\ \pi \in \Gamma(E,\Omega^1_{E/S}) \text{ generator} \end{array} \right\} / \sim . \end{aligned}$$

Here, $(E,\pi) \cong (E',\pi')$ if there exists an isomorphism $\gamma : E \to E'$ of elliptic curves over S such that $\gamma^*(\pi') = \pi$.

Remark 12.2. A global section $\pi \in \Gamma(E,\Omega^1_{E/S})$ is a generator if and only if for every $s \in S$, the fiber $\pi(s)$ is a generator of $\Omega^1_{E(s)/\kappa(s)}$.

Theorem 12.3. *The functor $\mathcal{W}$ is representable by the affine scheme* $\operatorname{Spec} R$ *where*

$$R = \mathbb{Z}[1/6][a,b][\Delta^{-1}], \quad \Delta = 4a^3 + 27b^2,$$

with universal elliptic curve given by

$$\mathcal{E} = V_+(Y^2Z - X^3 - aXZ^2 - bZ^3) \subset \mathbb{P}^2_R \tag{12.2}$$

and universal generator the unique $\pi \in \Gamma(\mathcal{E},\Omega^1_{\mathcal{E}/R})$ such that

$$\pi|_{\mathcal{E}\cap D_+(Z)} = -\frac{dx}{2y} \quad \textit{glued with} \quad -\frac{dy}{3x^2+a}. \tag{12.3}$$

Here, the two charts $D(3x^2+a)$ and $D(y)$ cover $\mathcal{E} \cap D_+(Z)$ because $\mathcal{E}$ is smooth (Jacobi criterion). Moreover, the two differential forms glue because

$$0 = d(y^2 - x^3 - ax - b) = 2ydy - (3x^2+a)dx.$$

Remark 12.4. (1) Theorem 12.3 cannot be extended to characteristics 2 and 3. Namely, it states implicitly that pairs (E,π) have no automorphisms which does not hold over the primes $2,3$. For example, $[-1]^*(\pi) = -\pi = \pi$ in characteristic 2.

(2) By definition, if $(E,\pi) \in \mathcal{W}(S)$, then $\omega_E \cong \mathcal{O}_S$ and $\Omega^1_{E/S} \cong \mathcal{O}_E$. This can provide an obstruction for a family of elliptic curves to occur in $\mathcal{W}$.

Proof. Let S be a scheme with $6 \in \mathcal{O}_S(S)^\times$. We need to show that given a pair (E,π) over S, there are unique $a,b \in \mathcal{O}_S(S)$ with $\Delta \in \mathcal{O}_S(S)^\times$ such that (E,π) is given by the formulas (12.2) and (12.3).

The condition $\Delta \in \mathcal{O}_S(S)^\times$ is automatic in the following sense. Assume we have found $a,b \in \mathcal{O}_S(S)^\times$ such that (12.2) defines an elliptic curve over S that is isomorphic to E. Then $\Delta \in \mathcal{O}_S(S)^\times$ by the Jacobi criterion.

Step 1: Trivializing $\mathcal{L}^n/\mathcal{L}^{n-1}$. In order to find a,b, we proceed in the same way as we did over fields (see the discussion around (6.23)). Let $\Gamma = e(S)$ be the graph of the identity section and consider the line bundle $\mathcal{L} = \mathcal{O}_E([\Gamma])$. Recall that it is defined as the dual $\mathcal{I}^{-1} = \mathcal{H}om(\mathcal{I},\mathcal{O}_E)$, where $\Gamma = V(\mathcal{I})$. Clearly there is a chain of inclusions

$$\mathcal{O}_E \supset \mathcal{I} \supset \mathcal{I}^2 \supset \dots.$$

Passing to the dual gives a chain of inclusions

$$\mathcal{O}_E \subset \mathcal{L} \subset \mathcal{L}^2 \subset \dots.$$

This is a more abstract variant of a statement that is obvious for curves over fields: If D and D' are divisors on a curve C and if D' is effective, then $\mathcal{O}_C(D) \subseteq \mathcal{O}_C(D+D')$ by the definition in terms of meromorphic functions (Definition 6.8). Observe that for all $n \in \mathbb{Z}$,

$$\mathcal{L}^n/\mathcal{L}^{n-1} = \mathcal{L}^n/(\mathcal{L}^n \otimes \mathcal{I}) = \mathcal{L}^n \otimes (\mathcal{O}_E/\mathcal{I}) = \mathcal{L}^n|_\Gamma. \tag{12.4}$$

Namely, vector bundles are flat. So tensoring with a line bundle is an exact operation that commutes with inclusions and quotients. Next, note that there is a canonical isomorphism

$$\mathcal{I}/\mathcal{I}^2 \xrightarrow{\sim} \omega_E, \quad f \longmapsto df. \tag{12.5}$$

Namely, for all $u \in \mathcal{O}_E$,

$$d(uf) = udf + fdu \equiv udf \mod \mathcal{I}\cdot\Omega^1_{E/S}$$

which shows that (12.5) really is a map of $\mathcal{O}_E$-modules. Let $\bar\pi = e^*(\pi) \in \omega_E$ be the generator defined by π, compare (12.1). Using (12.4), we obtain trivializations $\mathcal{L}^n/\mathcal{L}^{n-1} = \mathcal{O}_S \cdot \bar\pi^{\otimes(-n)}$.

Step 2: Pushforwards. Consider now the structure map $p : E \to S$ and the pushforwards $p_*(\mathcal{L}^n)$. For $n \geq 1$, this is a vector bundle of rank n on S (Theorem 6.37). Each short exact sequence

$$0 \longrightarrow \mathcal{L}^{n-1} \longrightarrow \mathcal{L}^n \longrightarrow \mathcal{L}^n/\mathcal{L}^{n-1} \longrightarrow 0$$

gives rise to a long exact sequence

$$0 \longrightarrow p_*(\mathcal{L}^{n-1}) \longrightarrow p_*(\mathcal{L}^n) \longrightarrow \mathcal{L}^n/\mathcal{L}^{n-1} \longrightarrow R^1p_*\mathcal{L}^{n-1} \longrightarrow \dots.$$

If $n \geq 2$, then $R^1p_*(\mathcal{L}^{n-1}) = 0$ by Theorem 6.37. So we obtain short exact sequences

$$0 \longrightarrow p_*(\mathcal{L}^{n-1}) \longrightarrow p_*(\mathcal{L}^n) \longrightarrow \omega_E^{\otimes(-n)} \longrightarrow 0.$$

For $n = 1$, we have a natural map

$$\mathcal{O}_S = p_*\mathcal{O}_E \longrightarrow p_*\mathcal{L}.$$

Both source and target are line bundles, and the map is surjective fiber-wise over every $s \in S$. It is hence an isomorphism. In summary, we find inclusions

$$0 \subset \mathcal{O}_S = p_*\mathcal{L} \subset p_*(\mathcal{L}^2) \subset p_*(\mathcal{L}^3) \subset \dots \tag{12.6}$$

with successive quotients $\mathcal{O}_S, \omega_E^{-2}, \omega_E^{-3}, \dots$.

Step 3: Choosing x and y locally. Despite all the successive quotients in (12.6) being trivial (powers of $\bar\pi$ trivialize the ω_E^n), it is not clear that the vector bundles $p_*(\mathcal{L}^n)$ are trivial. For this reason, we now work locally and restrict to S affine. Then the maps

$$\Gamma(S, p_*(\mathcal{L}^n)) \longrightarrow \Gamma(S, \omega_E^{-n})$$

are surjective. So we may pick $x_0 \in \Gamma(S, p_*(\mathcal{L}^2))$ and $y_0 \in \Gamma(S, p_*(\mathcal{L}^3))$ such that

$$x_0 \equiv \bar\pi^{-2} \bmod \mathcal{O}_S(S), \quad y_0 \equiv \bar\pi^{-3} \bmod \Gamma(S, p_*(\mathcal{L}^2)). \tag{12.7}$$

Then $1, x_0$ and y_0 give a trivialization of $p_*(\mathcal{L}^3)$ and, by Theorem 6.37, define a closed immersion

$$E \hookrightarrow \mathbb{P}(p_*(\mathcal{L}^3)^\vee) \underset{1,x_0,y_0}{\xrightarrow{\sim}} \mathbb{P}^2_S.$$

The sections $1, x_0, y_0, x_0^2, x_0y_0, x_0^3$ define a trivialization $\mathcal{O}_S^{\oplus 6} \xrightarrow{\sim} p_*(\mathcal{L}^6)$. (This can be checked fiber-wise for all $s \in S$.) Since also $y_0^2 \in \Gamma(E, \mathcal{L}^6)$, we obtain unique coefficients $a_0, a_2, \dots, a_6 \in \mathcal{O}_S(S)$ such that

$$y_0^2 + a_1x_0y_0 + a_3y_0 = a_0x_0^3 + a_2x_0^2 + a_4x_0 + a_6.$$

But the more precise relation (12.7) shows that $y_0^2 - x_0^3 \in \Gamma(E, \mathcal{L}^5)$. So $a_0 = 1$. We have $6 \in \mathcal{O}_S(S)^\times$ by assumption, so there exists a unique (!) linear transformation[16] of the form

$$\begin{cases} x = x_0 + p \\ y = y_0 + qx_0 + r, \end{cases}$$

where $p, q, r \in \mathcal{O}_S(S)$, such that x and y satisfy a simplified Weierstrass equation

$$y^2 = x^3 + ax + b. \tag{12.8}$$

Note that still $x \equiv \bar\pi^{-2} \bmod \mathcal{O}_S(S)$ and $y \equiv \bar\pi^{-3} \bmod \mathcal{L}^2(E)$. So our intermediate result is:

Lemma 12.5. *Assume that S is affine. Then there are unique $x \in \mathcal{L}^2(E)$ and $y \in \mathcal{L}^3(E)$ with $x \equiv \bar\pi^{-2}$ mod $\mathcal{O}_S(S)$ and $y \equiv \bar\pi^{-3}$ mod $\mathcal{L}^2(E)$ such that their Weierstrass equation (normalized as per being monic in y^2) is of the simple form (12.8). In particular, this determines the coefficients $a, b \in \mathcal{O}_S(S)$.*

Step 4: Gluing to general S. Now assume S is any. Lemma 12.5 constructs unique data (x_i, y_i, a_i, b_i) for an open covering $S = \bigcup_{i\in I} S_i$. By the uniqueness, they glue to a trivialization

$$1, x, y : \mathcal{O}_S^3 \xrightarrow{\sim} p_*(\mathcal{L}^3)$$

and sections $a, b \in \mathcal{O}_S(S)$ such that E is identified with the Weierstrass curve

$$V_+(Y^2Z - X^3 - aXZ^2 - bZ^3) \subset \mathbb{P}^2_S.$$

That is, Lemma 12.5 holds for any S, not just affine ones. It is left to show that this proves Theorem 12.3, meaning that π, x and y also satisfy (12.3) and are uniquely determined by this condition. This is precisely the next lemma.

Lemma 12.6. *Let $p : E \to S$ and $\mathcal{L}$ be as above. Let $x \in \mathcal{L}^2(E)$ and $y \in \mathcal{L}^3(E)$ be global sections that map to generators of $\mathcal{L}^2/\mathcal{L}$ and $\mathcal{L}^3/\mathcal{L}^2$, both viewed as line bundles on S. Assume that the Weierstrass equation of x and y is simple. In particular, there exists a generator $\pi \in \Omega^1_{E/S}(E)$ such that $\pi|_{D_+(YZ)} = -dx/2y$. Then $\bar\pi := e^*(\pi)$ agrees with*

$$(x \bmod \mathcal{L})/(y \bmod \mathcal{L}^2) \in \mathcal{L}^{-1}/\mathcal{L}^{-2} \xrightarrow{\sim} \omega_E.$$

[16] Exercise: Check this.

Proof. This can be checked locally near every point of $\Gamma = e(S)$. So assume $\mathcal{L}^{-1} = \mathcal{I} = (t)$ for some function t, and that

$$x = f/t^2, \quad y = g/t^3.$$

Here, f and g are invertible.

$$\begin{aligned}\bar{\pi} &= (x/y \bmod \mathcal{I}^2)\\ &= (f/g \cdot t \bmod \mathcal{I}^2)\\ &= (f/g)(e) \cdot (t \bmod \mathcal{I}^2)\\ &\overset{(\star)}{=} (f/g)(e) \cdot dt \in \omega_E.\end{aligned}$$

The equality $(\star)$ is along the identification (12.5). Now we compute

$$\begin{aligned}-\frac{dx}{2y} &= -\frac{t^2 df - 2tf dt}{t^4} \cdot \frac{t^3}{2g}\\ &= \frac{f}{g}dt - \frac{t}{2g}df\\ &\overset{e^*}{\longmapsto} (f/g)(e)dt \in \omega_E.\end{aligned}$$

(This computation is justified because t is not a zero-divisor.) □

Step 5: Proof that the x, y from Lemma 12.5 are the unique ones such that (12.3) holds. Let $x \in \mathcal{L}^2(E)$ and $y \in \mathcal{L}^3(E)$ be such that

(1) Their images $\bar{x}$ and $\bar{y}$ in $\mathcal{L}^2/\mathcal{L}$ and $\mathcal{L}^3/\mathcal{L}^2$ are generators.
(2) Their Weierstrass equation is simple.
(3) The identity $\pi|_{D_+(YZ)} = -dx/2y$ holds.

By Lemma 12.6, $\bar{\pi} = \bar{x}/\bar{y}$ where again $\bar{\pi} = e^*(\pi)$. Because the Weierstrass equation of x and y is simple, in particular monic in both y^2 and x^3, we have $\bar{x}^3 = \bar{y}^2$ in $\mathcal{L}^6/\mathcal{L}^5$. Taking their quotient, we find

$$1 = \bar{x}^3/\bar{y}^2 = \bar{x} \cdot \bar{\pi}^2 \in \mathcal{O}_E/\mathcal{I}.$$

This means $\bar{x} = \bar{\pi}^{-2}$. Then also

$$\bar{y} = (\bar{y}/\bar{x}) \cdot \bar{x} = \bar{\pi}^{-3}.$$

We conclude that the x, y constructed by Lemma 12.5 are the unique sections that satisfy (1)–(3). Conversely, the coordinates of every simplified Weierstrass equation give rise to such x, y. This finishes the proof of the theorem. □

13. Coarse moduli space

In the previous section, we have passed from $\mathcal{E}\ell\ell$ to $\mathcal{W}$ in order to obtain a representable functor. Given a pair $(E, \pi) \in \mathcal{W}(T)$ and a unit $\lambda \in \mathcal{O}_T(T)^\times$, there is a new pair $(E, \lambda\pi)$. That is, there is a $\mathbb{G}_m$-action $\mathbb{G}_m \times \mathcal{W} \to \mathcal{W}$. If $\pi' \in \Omega^1_{E/T}(E)$ is another generator, then there is a unique $\lambda \in \mathcal{O}_T(T)^\times$ such that $\pi' = \lambda\pi$. Thus, on an intuitive level, the quotient $\mathbb{G}_m \backslash \mathcal{W}$ (in whatever sense) should be very close to the original functor $\mathcal{E}\ell\ell$. Our aim is to make this precise.

13.1. **Group scheme actions.**

Definition 13.1. Let S be a scheme, let G/S be a group scheme, and let X/S be any scheme. An action of G on X is a morphism

$$\mu : G \times_S X \longrightarrow X$$

such that for every $T \to S$, the induced map $\mu(T) : G(T) \times X(T) \to X(T)$ is a group action.

By the Yoneda lemma, giving an action μ of G on S is the same as giving actions of $G(T)$ on $X(T)$ for every $T \to S$ that are compatible with pullbacks. Yet another equivalent definition can be made in terms of diagrams similar to (2.8), (2.9) and (2.10); they are of the form (13.3) and (13.4).

Example 13.2. Work over $S = \operatorname{Spec} \mathbb{Z}$. There is an action

$$\begin{aligned} \mu : \mathbb{G}_m \times \mathcal{W} &\longrightarrow \mathcal{W} \\ \mathcal{O}_T(T)^\times \times \mathcal{W}(T) \ni (\lambda, (E, \pi)) &\longmapsto (E, \lambda\pi). \end{aligned} \tag{13.1}$$

We have shown that $\mathcal{W}$ is representable by an affine scheme. So the above example is a special case of a $\mathbb{G}_m$-action on an affine scheme.

Construction 13.3 (Gradings from $\mathbb{G}_m$-actions)**.** Work over $S = \operatorname{Spec} R$. Let A be an R-algebra. Let t denote the coordinate on $\mathbb{G}_{m,R}$. That is, write $\mathbb{G}_{m,R} = \operatorname{Spec} R[t, t^{-1}]$ with group law $m^*(t) = t \otimes t$. Let

$$\mu : \mathbb{G}_{m,R} \times_{\operatorname{Spec} R} \operatorname{Spec} A \longrightarrow \operatorname{Spec} A$$

be an action. It is the dual of an R-algebra morphism

$$\mu^* : A \longrightarrow R[t, t^{-1}] \otimes_R A.$$

For each integer $i \in \mathbb{Z}$, we define

$$A_i = \{a \in A \mid \mu^*(a) = t^i \otimes a\}. \tag{13.2}$$

Proposition 13.4. *(1) The definition in (13.2) gives a $\mathbb{Z}$-grading of A. That is, $A = \bigoplus_{i\in\mathbb{Z}} A_i$ as R-module and $A_iA_j \subseteq A_{i+j}$ for all $i, j \in \mathbb{Z}$.*
(2) Passing from μ to its grading defines a bijection between actions of $\mathbb{G}_{m,R}$ on $\operatorname{Spec} A$ and R-module gradings $A = \bigoplus_{i\in\mathbb{Z}} A_i$ with $A_iA_j \subseteq A_{i+j}$.

Proof. The sum of the A_i is direct, meaning $\bigoplus_{i\in\mathbb{Z}} A_i \subseteq A$. Namely, consider an element $a = \sum_{i\in\mathbb{Z}} a_i$. Then

$$\mu^*(a) = \sum_{i\in\mathbb{Z}} t^i \otimes a_i.$$

The elements $\{t_i \otimes 1\}_{i\in\mathbb{Z}} \subset A[t, t^{-1}]$ are A-linearly independent. So $a = 0$ implies $a_i = 0$ for all $i \in \mathbb{Z}$.

Next, let $a \in A$ be any and write $\mu^*(a) = \sum_{i\in\mathbb{Z}} t^i \otimes a_i$. We claim that $a_i \in A_i$ and that $a = \sum_{i\in\mathbb{Z}} a_i$. To prove this, we use the associativity of a group action which states that

$$\begin{array}{ccc} \mathbb{G}_{m,R} \times_R \mathbb{G}_{m,R} \times_R \operatorname{Spec} A & \xrightarrow{m\times\mathrm{id}} & \mathbb{G}_{m,R} \times_R \operatorname{Spec} A \\ \Big\downarrow{\scriptstyle \mathrm{id}\times\mu} & & \Big\downarrow{\scriptstyle \mu} \\ \mathbb{G}_{m,R} \times_R \operatorname{Spec} A & \xrightarrow{\mu} & \operatorname{Spec} A \end{array} \tag{13.3}$$

commutes. Passing to rings of functions and applying the maps to a, this states

$$\sum_{i\in\mathbb{Z}} t^i \otimes \mu^*(a_i) = \sum_{i\in\mathbb{Z}} t^i \otimes t^i \otimes a_i.$$

Comparing both sides, we find $\mu^*(a_i) = t^i \otimes a_i$ and hence $a_i \in A_i$. Now we use another axiom of group actions, namely that the identity element acts trivially. This is expressed by the commutativity of

$$\begin{array}{ccc} \operatorname{Spec} A & \xrightarrow{(e,\mathrm{id})} & \mathbb{G}_{m,R} \times_R \operatorname{Spec} A \\ & \searrow & \Big\downarrow{\scriptstyle \mu} \\ & & \operatorname{Spec} A. \end{array} \tag{13.4}$$

Passing to rings of functions applying the maps to a, this states that

$$a \longmapsto \mu^*(a) = \sum_{i\in\mathbb{Z}} t^i \otimes a_i \overset{t\mapsto 1}{\longmapsto} \sum_{i\in\mathbb{Z}} a_i \overset{!}{=} a.$$

We have now shown that $A = \bigoplus_{i\in\mathbb{Z}} A_i$. Moreover, this grading is by R-modules because μ^* is R-linear. It is left to prove $A_iA_j \subseteq A_{i+j}$. But this is immediate since μ^* is a ring homomorphism,

$$\mu^*(a_ia_j) = \mu^*(a_i)\mu^*(a_j) = (t^i \otimes a_i)(t^j \otimes a_j) = t^{i+j} \otimes (a_ia_j).$$

We leave it as an exercise to verify that this sets up a bijection between actions and gradings as claimed. □

13.2. **Quotients by $\mathbb{G}_m$-actions.**

Definition 13.5. Let $\mu : G \times_S X \to X$ be an action. An S-morphism $f : X \to Y$ is called G-invariant if the two compositions

$$G \times_S X \overset{p_X,\mu}{\longrightarrow} X \overset{f}{\longrightarrow} Y$$

coincide. Equivalently, for every $T \to S$, the map $f(T) : X(T) \to Y(T)$ is $G(T)$-invariant.

A categorical quotient (in the category of S-schemes) is a universal G-invariant morphism. That is, it is a pair (Q, q) consisting of an S-scheme Q and a G-invariant morphism $q : X \to Q$ such that for every G-invariant $f : X \to Y$, there is a unique factorization through q,

$$\begin{array}{ccc} X & \xrightarrow{q} & Q \\ & \searrow^{f} & \downarrow \exists! \\ & & Y. \end{array} \tag{13.5}$$

Categorical quotients need not exist. Even if they do, they might be hard to construct and may have unexpected geometric properties.

Example 13.6. Consider the smooth manifolds $\mathbb{R}^\times$ and $\mathbb{R}$, and the smooth action $\mathbb{R}^\times \circlearrowright \mathbb{R}$ given by scaling. This action has a categorical quotient in smooth manifolds which is given by $\mathbb{R} \to \{\mathrm{pt}\}$ (check this!). But note that there are two orbits, namely $\{0\}$ and $\mathbb{R} \setminus \{0\}$. Thus the underlying set of the categorical quotient differs from the set-theoretic quotient.

The basic technique for constructing quotients by actions of *affine* group schemes is to take rings of invariant functions:

Definition 13.7. Let R be a ring, set $S = \operatorname{Spec} R$, let $G = \operatorname{Spec} H$ be an affine R-group scheme, let $X = \operatorname{Spec} A$ be an affine R-scheme, and let $\mu : G \times_S X \longrightarrow X$ be an action with dual

$$\mu^* : A \longrightarrow H \otimes_R A.$$

The μ-invariants of A are defined as the sub R-algebra

$$A^G := \{a \in A \mid \mu^*(a) = 1 \otimes a\}.$$

In other words, we require $\mu^*(a) = p^*(a)$ where $p : G \times_S X \to X$ denotes the projection.

Lemma 13.8. *Let the notation be as in Definition 13.7. Then the natural map*

$$q : \operatorname{Spec}(A) \longrightarrow Q := \operatorname{Spec}(A^G)$$

is a categorical quotient of X by G in the category of affine S-schemes. That is, (13.5) holds for all G-invariant maps f to affine S-schemes Y.

Proof. This is immediate from definitions: Let $Y = \operatorname{Spec} B$. The map $f : X \to Y$ being G-invariant by definition means that

$$f \circ \mu = f \circ p_X : G \times_S X \longrightarrow Y.$$

This is equivalent to $f^* : B \to A$ having image in A^G. In other words, we have the unique existence in

$$\begin{array}{ccc} A & \hookleftarrow & A^G \\ & \nwarrow^{f^*} & \uparrow \exists! \\ & & B \end{array}.$$

□

Example 13.9. Let R be a ring and A an R-algebra. Assume that $G = \mathbb{G}_{m,R}$ acts on $X = \operatorname{Spec} A$. Let $A = \bigoplus_{i\in\mathbb{Z}} A_i$ be the corresponding grading (Proposition 13.4). Then $A^G = A_0$.

Theorem 13.10. *With notations as in Example 13.9, set $Q = \operatorname{Spec} A_0$ and let $q : X \to Q$ be the map coming from the inclusion $A_0 \subseteq A$. Assume that A is noetherian. Then (Q, q) is a categorical quotient in all R-schemes.*

Proof. Step 1: Sheafy invariants. Let $V \subseteq Q$ be any open. Then $U = q^{-1}(V) \subseteq X$ is open and G-stable because q is G-invariant. Here, G-stable means that the action μ restricts to a morphism

$$\mu|_{G\times U} : G \times_S U \longrightarrow U.$$

Clearly, $\mu|_{G\times_S U}$ is a G-action on U. Set

$$(q_*\mathcal{O}_X)^G(V) := \{f \in (q_*\mathcal{O}_X)(V) \mid \mu^*(f) = p^*(f)\}.$$

The condition $\mu^*(f) = p^*(f)$ can be checked on open covers, so this defines a sub*sheaf* of $q_*\mathcal{O}_X$.

Step 2: In fact, $\mathcal{O}_Q \xrightarrow{\sim} (q_*\mathcal{O}_X)^G$. Namely, since q is G-invariant, the pullback map $q^* : \mathcal{O}_Q \to q_*\mathcal{O}_X$ factors through $(q_*\mathcal{O}_X)^G$. We now have a map of sheaves

$$q^* : \mathcal{O}_Q \longrightarrow (q_*\mathcal{O}_X)^G,$$

and we can check that it is an isomorphism locally on Q. Let $V = D(f) \subset Q$ be any principal open and let $A_0 \to C_0 = A_0[f^{-1}]$ be the corresponding localization. Then $U = q^{-1}(V)$ with its $\mathbb{G}_{m,R}$-action is given by

$$U = \operatorname{Spec}(C_0 \otimes_{A_0} A), \quad (C_0 \otimes_{A_0} A)_i = C_0 \otimes_{A_0} A_i. \tag{13.6}$$

In particular,

$$(C_0 \otimes_{A_0} A)_0 = C_0 \otimes_{A_0} A_0 = C_0$$

which means $\mathcal{O}_Q(D(f)) \xrightarrow{\sim} (q_*\mathcal{O}_X)^G(D(f))$ as was to be shown. We remark that we did not use the property of C_0 being a localization. The description (13.6) holds for any affine base change $A_0 \to C_0$.

We now come to the main part of the proof which is about the topology of $q : X \to Q$.

Definition 13.11. (1) Consider an action $\mu : G \times_S X \to X$. A closed subscheme $Z \subseteq X$ is called G-invariant if μ restricts to a G-action on Z. That is, the upper horizontal arrow exists:

$$\begin{array}{ccc} G \times_S Z & \overset{\exists!}{\dashrightarrow} & Z \\ \downarrow & & \downarrow \\ G \times_S X & \xrightarrow{\mu} & X. \end{array} \tag{13.7}$$

(2) Let $I \subseteq A$ be an ideal in a graded ring $A = \bigoplus_{i\in\mathbb{Z}} A_i$. Then I is called homogeneous if $I = \bigoplus_{i\in\mathbb{Z}}(I \cap A_i)$. This is equivalent to I being generated by homogeneous elements.

Lemma 13.12. *Consider an action of $G = \mathbb{G}_{m,R}$ on an affine R-scheme $X = \operatorname{Spec} A$. Let $Z \subseteq X$ be the closed subscheme defined by the ideal $I \subseteq A$. Then Z is G-stable if and only if I is homogeneous.*

Proof. Passing to the dual of (13.7), we are trying to characterize ideals I such that the upper horizontal arrow exists in

$$\begin{array}{ccc} (A/I)[t,t^{-1}] & \overset{\exists ?}{\dashleftarrow} & A/I \\ \uparrow & & \uparrow \\ A[t,t^{-1}] & \xleftarrow{\mu^*} & A. \end{array} \tag{13.8}$$

In other words, we are trying to characterize ideals I such that $\mu^*(I) \subseteq I[t,t^{-1}]$. Let $a = \sum_{i\in\mathbb{Z}} a_i \in I$. Then $\mu^*(a) = \sum_{i\in\mathbb{Z}} t^i \otimes a_i$. From here it is clear that

$$\mu^*(I) \subseteq I[t,t^{-1}] \quad \Longleftrightarrow \quad \forall\, a \in I \text{ we have } a_i \in I \;\forall\, i \in \mathbb{Z}.$$

□

Step 3: We claim that the map $q : X \to Q$ is surjective. Let $\mathfrak{a}_0 \subseteq A_0$ be any ideal. Then it is checked from the definition of graded R-algebra that

$$\mathfrak{a}_0 = A_0 \cap (\mathfrak{a}_0 A).$$

Apply this to a prime ideal $\mathfrak{p}_0 \in \operatorname{Spec}(A_0)$. By assumption, A is noetherian, so the ring $A/(\mathfrak{p}_0 A)$ has only finitely many minimal prime ideals, say $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. Moreover, there exists an integer $n \geq 1$ with

$$\left(\cap_{i=1}^r \mathfrak{q}_i\right)^n \subseteq \mathfrak{p}_0 A \subseteq (\cap_{i=1}^r \mathfrak{q}_i).$$

Taking the intersection with A_0 we obtain

$$A_0 \cap (\cap_{i=1}^r \mathfrak{q}_i)^n \subseteq \mathfrak{p}_0 \subseteq A_0 \cap (\cap_{i=1}^r \mathfrak{q}_i). \tag{13.9}$$

Let $Z_i = V(\mathfrak{q}_i)$ be the closed subscheme defined by $\mathfrak{q}_i$. At the level of underlying topological spaces, both $V(\cap_{i=1}^r \mathfrak{q}_i)$ and $V((\cap_{i=1}^r \mathfrak{q}_i)^n)$ are just $Z = \cup_{i=1}^r Z_i$. So (13.9) states that

$$V(\mathfrak{p}_0) = \overline{q(\cup_{i=1}^r (Z_i))}.$$

The union on the right hand side is finite and hence agrees with $\cup_{i=1}^r \overline{q(Z_i)}$. Moreover, $\overline{q(Z_i)}$ is nothing but the irreducbible closed subspace with generic point $q(\mathfrak{q}_i)$. Since $V(\mathfrak{p}_0)$ is irreducible with generic point $\mathfrak{p}_0$, there hence has to exist some i with $\mathfrak{p}_0 = q(\mathfrak{q}_i)$, proving the claim.

Step 4: A brief observation. Let $\{I_j\}_{j\in J}$ be a family of homogeneous ideals of A. Then

$$(\sum_{j\in J} I_j) \cap A_0 = \sum_{j\in J} (I_j \cap A_0).$$

Geometrically on the level of topological spaces, this states that for G-invariant closed subschemes $Z_j \subseteq X$,

$$\overline{q(\cap_{j\in J} Z_j))} = \cap_{j\in J} \overline{q(Z_j)}. \tag{13.10}$$

Step 5: We claim that if $Z \subseteq X$ is G-invariant, then $q(Z)$ is closed. Let $y \in \overline{q(Z)} \setminus Z$ be any point. Let $Y = \overline{\{y\}}$ be its closure endowed with its reduced subscheme structure. Then $q^{-1}(Y) \subset X$ is closed and G-invariant. Then we have

$$\begin{aligned} Y &= \overline{q(Z)} \cap Y \\ &\overset{(3)}{=} \overline{q(Z)} \cap q(q^{-1}(Y)) \\ &\overset{(4)}{=} \overline{q(Z \cap q^{-1}(Y))}. \end{aligned} \tag{13.11}$$

Now we argue as during Step 3: Since X is noetherian, $Z \cap q^{-1}(Y)$ has finitely many generic points $z_1, \dots, z_r$ and the last line in (13.11) equals $\cup_{i=1}^r \overline{q(z_i)}$. Since Y is irreducible with generic point y, there exists some i with $y = q(z_i)$. This is in contradiction to our assumption $y \notin q(Z)$, so $\overline{q(Z)} \setminus Z = \emptyset$.

Final step: (Q, q) has the categorical quotient property. Let $v : X \to T$ be any G-invariant morphism of R-schemes. Then for every $W \subseteq T$ affine open, $v^{-1}(W) \subseteq X$ is open and G-stable. Thus $Z = X \setminus v^{-1}(W)$ (with reduced scheme structure) is closed and G-stable. By Step 5, this implies that $q(Z)$ is closed. So $V_W = Q \setminus q(Z)$ is open with $q^{-1}(V_W) \subseteq v^{-1}(W)$. Covering V_W by affine opens and using Step 2, we find a unique morphism $V_W \to W$ that fits into the diagram

$$\begin{array}{ccc} v^{-1}(W) \supseteq & q^{-1}(V_W) & \xrightarrow{q} V_W \\ & & \downarrow \exists! \\ & & W. \end{array} \qquad (v : q^{-1}(V_W) \to W)$$

Step 4 and 5 imply that if we vary W to cover all of T, then the V_W cover all of Q. Indeed,

$$\begin{aligned} \cap_W (Q \setminus V_W) &= \cap_W q(X \setminus v^{-1}(W)) \\ &\overset{(4)+(5)}{=} q(\cap_W X \setminus v^{-1}(W)) \\ &= q(\emptyset). \end{aligned}$$

Moreover, Step 2 ensures that the various maps $V_W \to T$ glue to a morphism $Q \to T$. This finishes the proof of Theorem 13.10. □

Example 13.13. (1) Let k be a field and $A = k[X_1, \dots, X_n]$. Consider the action μ of $\mathbb{G}_{m,k}$ on $\mathbb{A}^n_k$ with coaction map

$$\mu^* : A \longrightarrow k[t, t^{-1}] \otimes_k A, \quad \mu^*(X_i) = t \otimes X_i.$$

On S-valued points, this is nothing but the the scaling action

$$\lambda \cdot (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n).$$

The corresponding grading is the usual grading by degree, meaning $\deg(X_i) = 1$ for $i = 1, \dots, n$. In particular $A_0 = k$. By Theorem 13.10, the map $\mathbb{A}^n_k \to \operatorname{Spec} k$ is a categorical quotient $\mathbb{G}_m \backslash \mathbb{A}^n_k$. This is in line with Example 13.6.

(2) Consider next the localization $A[X_1^{-1}]$. The grading is as before, i.e.

$$\deg(X_1^{r_1} \cdots X_n^{r_n}) = r_1 + \ldots + r_n.$$

The difference is that we now allow $r_1 \in \mathbb{Z}$ and then obtain

$$A[X_1^{-1}]_0 = k[X_2/X_1, \dots, X_n/X_1].$$

This situation is familiar from the construction of $\mathbb{P}^{n-1}_k$.

(3) Consider $A = k[X, Y]$ with the non-standard $\mathbb{G}_{m,k}$-action given by

$$\mu^* : k[X, Y] \longrightarrow k[t, t^{-1}] \otimes_k k[X, Y], \quad \mu^*(X) = t \otimes X, \quad \mu^*(Y) = t^{-1} \otimes Y.$$

On S-valued points, this is the scaling action

$$\lambda \cdot (x, y) = (\lambda x, \lambda^{-1} y).$$

The grading on A is given by $\deg(X) = 1$ and $\deg(Y) = -1$. In particular $A_0 = k[XY]$. So the categorical quotient of μ is isomorphic to $\mathbb{A}^1_k$.

13.3. **Application to $\mathcal{W}$ and $\mathcal{E}\ell\ell$.** Recall that the Weierstrass moduli problem is represented by $\operatorname{Spec} R$ with

$$R = \operatorname{Spec} \mathbb{Z}[1/6][a, b, \Delta^{-1}], \quad \Delta = 4a^3 + 27b^2$$

and universal pair $(\mathcal{E}, \pi)$ given by

$$\mathcal{E} = V_+(\operatorname{homog}(y^2 - x^3 - ax - b)) \subset \mathbb{P}^2_R$$

$$\pi = -dx/2y.$$

Recall that there is a $\mathbb{G}_m$-action on $\mathcal{W}$ give by $\lambda \cdot (E, \pi) = (E, \lambda\pi)$.

Proposition 13.14. *The corresponding grading on $R = \mathbb{Z}[\frac{1}{6}][a, b, \Delta^{-1}]$ is given by*

$$\deg(a) = -4, \quad \deg(b) = -6.$$

The $\mathbb{G}_m$-invariants $R_0 \subset R$ are given by

$$\mathbb{Z}[1/6, j], \quad j = -1728\frac{4a^3}{\Delta}.$$

Sketch of proof. Let (E, π) be a Weierstrass pair over a scheme S with $6 \in \mathcal{O}_S(S)^\times$. We have seen in Lemma 11.3 and during the proof of Theorem 12.3 that the choice of coordinates x, y on E that have a simple Weierstrass equation is unique up to scaling operations of the form (11.4)

$$x' = ux, \quad y' = vy, \quad \text{where} \quad u, v \in \mathcal{O}_S(S)^\times, \quad u^3 = v^2. \tag{13.12}$$

Now assume that $\lambda \in \mathcal{O}_S(S)^\times$, that (x, y) are such that $\pi = -dx/2y$, and that $\pi' = \lambda\pi$. Then the unique (x', y') with $\pi' = -dx'/2y'$ are determined by

$$x' = ux, \quad y' = vy, \quad u^3 = v^2, \quad u/v = \lambda.$$

The unique solution (u, v) is

$$u = \frac{u^2}{v^2} = \lambda^{-2}, \quad v = u/\lambda = \lambda^{-3}.$$

Substituting $x = x'/u$ and $y = y'/v$ in the Weierstrass equation $y^2 = x^3 + ax + b$ gives

$$\lambda^6(y')^2 = \lambda^6(x')^3 + a\lambda^2(x') + b.$$

Renormalizing as to make this monic gives

$$(y')^2 = (x')^3 + \lambda^{-4}ax' + \lambda^{-6}b.$$

This shows that $\deg(a) = -4$ and $\deg(b) = -6$. Now assume that $p(a, b) \in \mathbb{Z}[1/6, a, b]$ and $n \in \mathbb{Z}$ are such that $p(a, b) \cdot \Delta^n$ is homogeneous of degree 0. Then, clearly, $p(a, b)$ has to be homogeneous of degree $12n$. Since

$$4a^3/\Delta = 1 - 27b^2/\Delta,$$

a small argument shows that the ring of $\mathbb{G}_m$-invariants is $\mathbb{Z}[1/6, j]$ as claimed. □

Let $\mathcal{E}\ell\ell[1/6]$ be the restriction of $\mathcal{E}\ell\ell$ to $\mathbb{Z}[1/6]$-schemes. One can show (exercise) that there is a unique natural transformation $\mathcal{J} : \mathcal{E}\ell\ell[1/6] \to \mathbb{G}_m\backslash\mathcal{W}$ that makes the following diagram commute:

$$\begin{array}{ccc} \mathcal{W} & \longrightarrow & \mathcal{E}\ell\ell[1/6] \\ \downarrow & \swarrow_{\mathcal{J}} & \\ \mathbb{G}_m\backslash\mathcal{W}. & & \end{array} \tag{13.13}$$

This can be proved abstractly from the categorical quotient property of $\mathbb{G}_m\backslash\mathcal{W}$, and the resulting $\mathcal{J}$ has the following concrete description. Let E/S be an elliptic curve. Then, after identifying $\mathbb{G}_m\backslash\mathcal{W}$ with the affine scheme $\operatorname{Spec} \mathbb{Z}[1/6, j]$ as in Proposition 13.14, the

map $\mathcal{J}(E)^* : \mathbb{Z}[1/6, j] \to \mathcal{O}_S(S)$ takes j to the j-invariant $j(E)$. It is defined by choosing an open covering $S = \cup_{i\in I} S_i$ such that each restriction $E|_{S_i}$ admits a Weierstrass equation $y^2 = x^3 + a_i x + b_i$. Then $j(E)|_{S_i} = -1728 \cdot 4a_i^3/(4a_i^3 + 27b_i^2)$. As the j-invariant does not depend on the choice of Weierstrass equation, $(j(E)|_{S_i})_{i\in I}$ glues to a global section $j(E) \in \mathcal{O}_S(S)$.

One may further show (exercise) that the morphism $\mathcal{E}\ell\ell[1/6] \to \mathbb{G}_m\backslash\mathcal{W}$ has the following universal property. For every natural transformation $\mathcal{F} : \mathcal{E}\ell\ell[1/6] \to Y$ to a scheme Y, there is a unique morphism $f : \mathbb{G}_m\backslash\mathcal{W} \to Y$ making the following diagram commute:

$$\begin{array}{ccc} & & \mathcal{E}\ell\ell[1/6] \\ & \overset{\mathcal{J}}{\swarrow} & \big\downarrow{\scriptstyle \mathcal{F}} \\ \mathbb{G}_m\backslash\mathcal{W} & \underset{f}{- - \succ} & Y. \end{array} \tag{13.14}$$

That is, $\mathcal{J}$ is a so-called coarse moduli space for $\mathcal{E}\ell\ell[1/6]$. It has to be understood as the best possible approximation to $\mathcal{E}\ell\ell[1/6]$ by a scheme.

Definition 13.15 (Coarse moduli space)**.** Let $\mathcal{M}$ be a contravariant functor on (Sch/S) and let $\mathcal{J} : \mathcal{M} \to M$ be a natural transformation to an S-scheme M. Then $(M, \mathcal{J})$ is called a coarse moduli space for $\mathcal{M}$ if it has the following two properties:

(1) For every algebraically closed S-field k, the map $\mathcal{J}(k) : \mathcal{M}(k) \to M(k)$ is bijective.

(2) Every natural transformation $\mathcal{F} : \mathcal{M} \to Y$ to an S-scheme Y factors uniquely through a morphism $f : M \to Y$.

For the j-invariant, property (1) is precisely Theorem 11.4.

14. Fine moduli spaces

14.1. **Level structure.** Let E/S be an elliptic curve. Recall that $E[n]$ is a finite locally free S-group scheme of degree n^2 (Theorem 9.5). If moreover $n \in \mathcal{O}_S(S)^\times$, then $E[n] \to S$ is finite étale (Corollary 9.20) and there exists a finite étale surjective $T \to S$ together with an isomorphism

$$\underline{\mathbb{Z}/n\mathbb{Z}}_T^{\oplus 2} \xrightarrow{\sim} T \times_S E[n].$$

Definition 14.1. Let $n \geq 1$, let $n \in \mathcal{O}_S(S)^\times$, and let E/S be an elliptic curve. (1) A level-n-structure on an elliptic curve E/S is an isomorphism

$$\alpha : \underline{\mathbb{Z}/n\mathbb{Z}}_S^{\oplus 2} \xrightarrow{\sim} E[n].$$

(2) The functor of level-n-structures on E is defined as

$$\begin{aligned} L_{E,n} : (\mathrm{Sch}/S)^{\mathrm{op}} &\longrightarrow (\mathrm{Set}) \\ [u : T \to S] &\longmapsto \left\{ \alpha : \underline{\mathbb{Z}/n\mathbb{Z}}_T^{\oplus 2} \xrightarrow{\sim} T \times_S E[n] \ \text{ level str.} \right\}. \end{aligned} \tag{14.1}$$

There is an action of $GL_2(\mathbb{Z}/n\mathbb{Z})$ (even of the constant group scheme $\underline{GL_2(\mathbb{Z}/n\mathbb{Z})}_S$) on $L_{E,n}$ that is given by composition: $g \bullet \alpha := \alpha \circ g$.

Definition 14.2 (Torsor)**.** Let G be an S-group scheme acting on an S-scheme X. Then X is called a G-torsor (for the Zariski/étale/fppf/fpqc topology, respectively) if there exists a covering $T \to S$ for said topology and a G-equivariant isomorphism

$$\gamma : T \times_S G \xrightarrow{\sim} T \times_S X.$$

Here, G-equivariant means that $\gamma(gh) = g \cdot \gamma(h)$ for all $U \to T$ and $g, h \in G(U)$.

Remark 14.3 (Terminology in special cases)**.** (1) Let $G = GL_{n,S}$, for example $G = \mathbb{G}_{m,S}$. Then any G-torsor for the fpqc topology is already a G-torsor for the Zariski topology. For this reason, the topology is usually not explicitly mentioned in this case.

(2) Let Γ be a finite group. By Γ-torsor over S, one means a $\underline{\Gamma}_S$-torsor for the étale topology. Moreover, any $\underline{\Gamma}_S$-torsor for the fpqc topology is already a $\underline{\Gamma}_S$-torsor for the étale topology.

Proposition 14.4. *The functor $L_{E,n}$ is representable by a finite étale S-scheme. It is a $GL_2(\mathbb{Z}/n\mathbb{Z})$-torsor.*[17] *More precisely, there exists a finite étale surjective $T \to S$ together with an $GL_2(\mathbb{Z}/n\mathbb{Z})$-equivariant isomorphism*

$$\underline{GL_2(\mathbb{Z}/n\mathbb{Z})}_T \xrightarrow{\sim} T \times_S L_{E,n}.$$

In particular, $L_{E,n} \to S$ is finite locally free of degree $|GL_2(\mathbb{Z}/n\mathbb{Z})|$.

Proof. Giving a group homomorphism

$$\alpha : \underline{\mathbb{Z}/n\mathbb{Z}}_T^{\oplus 2} \longrightarrow T \times_S E[n]$$

is equivalent to giving the images $\alpha(1,0), \alpha(0,1) \in E(T)$. Hence we consider $X := E[n] \times_S E[n]$. Then $L_{E,n} \subseteq X$ is the subfunctor of T-valued points such that the two sections define a level structure (i.e. s.th. α is a homomorphism). For each pair $(a,b) \in (\mathbb{Z}/n\mathbb{Z})^{\oplus 2} \setminus (0,0)$, consider the map that takes linear combination

$$m_{a,b} : X \longrightarrow E[n], \quad m_{a,b}(x,y) = ax + by.$$

Note that X and $E[n]$ are finite étale S-schemes, so $m_{a,b}$ is automatically finite étale (Lemma 9.17). Similarly, $0 : S \to E[n]$ is finite étale. Consider the fiber product

$$B_{a,b} = X \times_{m_{a,b},\ E[n],\ 0} S \longrightarrow X. \tag{14.2}$$

It is the "bad locus" where the two sections $(x,y) \in X$ are linearly dependent via (a,b). Being finite étale is stable under products, so $B_{a,b} \to S$ is finite étale. By Lemma 9.17 again, or by stability under pullbacks, (14.2) is finite étale. By Proposition 9.19, (14.2) is open and closed. (Since (14.2) is also a monomorphism, this means that $B_{a,b}$ is an open subscheme of X that is also closed.) Similarly, any T-morphism $\alpha : \underline{\mathbb{Z}/n\mathbb{Z}}_T^{\oplus 2} \to T \times_S E[n]$ is open and closed. So it can be checked fiber by fiber whether α is an isomorphism, and we obtain

$$L_{E,n} \xrightarrow{\sim} X \setminus \cup_{(a,b)\neq(0,0)} B_{a,b}.$$

This proves the representability of $L_{E,n}$ by an open and closed subscheme of X.

For the second claim, consider a finite étale surjectiven $T \to S$ and an isomorphism $\underline{\mathbb{Z}/n\mathbb{Z}}_T^{\oplus 2} \xrightarrow{\sim} T \times_S E[n]$. Then clearly

$$T \times_S L_{E,n} \xrightarrow{\sim} \underline{GL_2(\mathbb{Z}/n\mathbb{Z})}_T.$$

Being finite locally free of degree d can be checked after fpqc base change, so $L_{E,n} \to S$ is finite locally free of degree $|GL_2(\mathbb{Z}/n\mathbb{Z})|$. □

Definition 14.5. (1) Let $\mathcal{E}\ell\ell_n/\mathbb{Z}[1/6n]$ be the functor of isomorphism classes of pairs (E,α), where α is a level-n-structure for E. Here,

$$(E,\alpha) \cong (E',\alpha') \iff \exists \gamma : E \xrightarrow{\sim} E' \text{ s.th. } \gamma \circ \alpha = \alpha'.$$

(2) Let $\mathcal{W}_n/\mathbb{Z}[1/6n]$ be the functor of isomorphism classes of pairs (E,α,π), where α is a level structure and where $\pi \in \Omega^1_{E/S}(E)$ is a generator. There are forgetful maps to $\mathcal{E}\ell\ell_n$

[17] See Remark 14.3.

and $\mathcal{W}$ that fit into a commutative (not Cartesian!) diagram

$$\begin{array}{ccc} \mathcal{W}_n & \longrightarrow & \mathcal{E}\ell\ell_n \\ \downarrow & & \downarrow \\ \mathcal{W} & \longrightarrow & \mathcal{E}\ell\ell. \end{array} \tag{14.3}$$

(3) Endow $\mathcal{W}_n$ with the $\mathbb{G}_m$-action $\lambda \cdot (E, \alpha, \pi) = (E, \alpha, \lambda\pi)$. Denote by

$$q : \mathcal{W}_n \longrightarrow \mathcal{M}_n := \mathbb{G}_m \backslash \mathcal{W}_n \tag{14.4}$$

the categorical quotient. ("$\mathcal{M}$" is for moduli space.)

Corollary 14.6. *The functor $\mathcal{W}_n$ is representable by an affine $\mathbb{Z}[1/6n]$-scheme. The forgetful map $\mathcal{W}_n \to \mathcal{W}$ is a $GL_2(\mathbb{Z}/n\mathbb{Z})$-torsor.*

Proof. Theorem 12.3 states that $\mathcal{W}[1/n]$ is representable. Apply Proposition 14.4 to the universal elliptic curve $\mathcal{E} \to \mathcal{W}$. We obtain that $\mathcal{W}_n$ is representable by a finite étale $GL_2(\mathbb{Z}/n\mathbb{Z})$-torsor over $\mathcal{W}[1/n]$. Being finite over an affine scheme, $\mathcal{W}_n$ is in particular affine. □

The $\mathbb{G}_m$-action on $\mathcal{W}_n$ commutes with the $GL_2(\mathbb{Z}/n\mathbb{Z})$-action. This implies that the $GL_2(\mathbb{Z}/n\mathbb{Z})$-action preserves the ring of invariants $\Gamma(\mathcal{W}_n, \mathcal{O}_{\mathcal{W}_n})_0$ and hence that $GL_2(\mathbb{Z}/n\mathbb{Z})$ acts on the quotient $\mathbb{G}_m\backslash\mathcal{W}_n$. In this way, we obtain the $GL_2(\mathbb{Z}/n\mathbb{Z})$-equivariant diagram

$$\begin{array}{ccc} & \mathcal{W}_n & \\ \swarrow & & \searrow \\ \mathcal{E}\ell\ell_n & \overset{\Phi}{\dashrightarrow} & \mathbb{G}_m\backslash\mathcal{W}_n \end{array} \tag{14.5}$$

where the dotted arrow exists for the same abstract reasons as in (13.13). One may also show with the same arguments that Φ is a coarse moduli space for $\mathcal{E}\ell\ell_n$. The next theorem is the main result of our course.

Theorem 14.7. *Assume that $n \geq 3$. Then Φ is an isomorphism. In particular, $\mathcal{E}\ell\ell_n$ is representable by an affine scheme.*

14.2. **The $\mathbb{G}_m$-action on $\mathcal{W}_n$ when $n \geq 3$.** We begin with a statement that explains why Theorem 14.7 is plausible. Relatedly, it also provides the motivation for considering level structures in the first place.

Proposition 14.8. *Let $n \geq 3$, and let $(E, \alpha)/S$ be an elliptic curve together with a level-n-structure. Then*

$$\mathrm{Aut}(E, \alpha) = \{\mathrm{id}\}.$$

Proof. Let $\phi : E \xrightarrow{\sim} E$ be an automorphism such that $\phi|_{E[n]} = \mathrm{id}$. Then $E[n] \subseteq \ker(\phi - 1)$. By Proposition 10.1, there exists a homomorphism $\psi : E \to E$ such that $\phi - 1 = n\psi$. We obtain that

$$\begin{aligned} n^2 \deg(\psi) &= \psi^* \circ \psi \\ &= (\phi - 1)(\phi^* - 1) \\ &= \deg(\phi) - (\phi + \phi^*) + 1 \\ &= 2 - (\phi + \phi^*). \end{aligned}$$

By Proposition 10.9 (2), ϕ is a 6-th root of unity. In particular, $\phi + \phi^* \in [-2, 2]$.[18] Thus we obtain $n^2 \deg(\psi) \leq 4$. Since $n^2 \geq 9$ by assumption, the only possibility is $\psi = 0$. □

[18] More precisely, by Corollary 7.26, $\phi + \phi^*$ is locally constant on S with values in $\{-2, -1, 0, 1, 2\}$.

Definition 14.9. Let G be an S-group scheme and let X be an S-scheme. An action $\mu : G \times_S X \to X$ of G on X is called free if the morphism

$$G \times_S X \xrightarrow{\mu \times \mathrm{pr}_X} X \times_S X \tag{14.6}$$

is a closed immersion.

Let T be an S-scheme and consider the map

$$(\mu \times \mathrm{pr}_X)(T) : G(T) \times X(T) \longrightarrow X(T) \times X(T). \tag{14.7}$$

Assume the images of two points (g, x) and (g', x') are equal; that is,

$$(gx, x) = (g'x', x').$$

Then $x = x'$, and hence $gx = g'x$. This means that $g^{-1}g'$ lies in the stabilizer $G(T)_x$. In this way, we see that (14.6) is a monomorphism if and only if all stabilizers $G(T)_x$ are trivial (here T/S and $x \in X(T)$ any). In set theory, this is precisely the definition of a free action. The slightly stronger requirement for (14.6) to be a closed immersion is added to exclude certain topological pathologies.

Proposition 14.10. *Assume that $n \geq 3$. Then the $\mathbb{G}_m$-action on $\mathcal{W}_n$ is free.*

Proof. We use the following criterion to check that $f : \mathbb{G}_m \times \mathcal{W}_n \to \mathcal{W}_n \times \mathcal{W}_n$ is a closed immersion.

Lemma 14.11 ([8, Tag 04XV])**.** *Let $f : X \to Y$ be a morphism of schemes. Then f is a closed immersion if and only if it is a proper monomorphism.*

f is a monomorphism. As explained after (14.7), this is equivalent to the stabilizers of all T-valued points $(E, \alpha, \pi) \in \mathcal{W}_n$ being trivial. By Proposition 14.8, the only automorphism

$$(E, \alpha) \xrightarrow{\sim} (E, \alpha)$$

is the identity. So $(E, \alpha, \pi) \cong (E, \alpha, \lambda\pi)$ if and only if $\pi = \lambda\pi$ if and only if $\lambda = 1$.

f is proper. $\mathcal{W}_n$ is a finite type $\mathbb{Z}[1/n]$-scheme, so f is of finite type. We need to check the valuative criterion of properness.

Proposition 14.12 (Weil's extension theorem)**.** *Let S be a connected Dedekind scheme[19] with generic point η. Let E_1 and E_2 be elliptic curves over S. Then*

$$\mathrm{Hom}(E_1, E_2) \xrightarrow{\sim} \mathrm{Hom}(E_1(\eta), E_2(\eta)). \tag{14.8}$$

The proof is beautiful and not difficult, but we skip it for now. We remark that the analog of (14.8) also holds for abelian varieties (Néron model property of abelian schemes, see [1, §1]).

We check the valuative criterion for f. Let R be a DVR with quotient field K and such that $n \in R^\times$. We need to see the unique existence of the dotted arrow for any diagram of the form

$$\begin{array}{ccc} \mathrm{Spec}\, K & \longrightarrow & \mathrm{Spec}\, R \\ \downarrow & \nearrow & \downarrow \\ \mathbb{G}_m \times \mathcal{W}_n & \longrightarrow & \mathcal{W}_n \times \mathcal{W}_n. \end{array}$$

The uniqueness is clear because all involved schemes are separated. For the existence, translating to the moduli definition of $\mathcal{W}_n$ yields the following. Let (E_1, α_1, π_1) and (E_2, α_2, π_2) lie in $\mathcal{W}_n(R)$. Assume that there exists a datum $(\lambda, (E, \alpha, \pi)) \in K^\times \times \mathcal{W}_n(K)$ together with isomorphisms

$$(E, \alpha, \lambda\pi) \xrightarrow{\sim} K \otimes_R (E_1, \alpha_1, \pi_1), \quad (E, \alpha, \pi) \xrightarrow{\sim} K \otimes_R (E_2, \alpha_2, \pi_2). \tag{14.9}$$

[19] That is, S is noetherian, integral, normal and 1-dimensional.

We need to see that $(\lambda, (E, \alpha, \pi)) \in R^\times \times \mathcal{W}_n(R)$.[20] Composing the isomorphisms from (14.8), we obtain an isomorphism

$$\gamma_K : K \otimes_R (E_1, \alpha_1) \xrightarrow{\sim} K \otimes_R (E_1, \alpha_2)$$

such that $\gamma_K^*(\pi_2) = \lambda\pi_1$. By Weil's extension theorem, there exists a unique isomorphism $\gamma : E_1 \to E_2$ such that $K \otimes_R \gamma = \gamma_K$. Then also

$$\alpha_2 = \gamma \circ \alpha_1 : \underline{\mathbb{Z}/n\mathbb{Z}}_R^{\oplus 2} \xrightarrow{\sim} E_2[n] \tag{14.10}$$

because this identity holds after $K \otimes_R -$, and because both source and target in (14.10) are flat affine R-schemes. Now both π_1 and $\gamma^*(\pi_2)$ are generators of the free rank one R-module $\Omega^1_{E_1/R}(E_1)$ and hence differ by an element $\lambda_0 \in R^\times$. Necessarily $\lambda_0 = \lambda$ because this holds after $K \otimes_R -$, so $\lambda \in R^\times$ and the proof is complete. □

14.3. **Quotients by free $\mathbb{G}_m$-actions.**

Proposition 14.13. *Let $S = \operatorname{Spec} R$ be an affine scheme, let $X = \operatorname{Spec} A$ be an affine S-scheme, and let $\mu : \mathbb{G}_{m,S} \times_S X \to X$ be a $\mathbb{G}_m$-action. Assume that μ is free. Then the quotient*

$$X \longrightarrow Q := \operatorname{Spec} A_0$$

is a $\mathbb{G}_m$-torsor for the Zariski topology. More precisely, A_1 is a line bundle over A_0 and $A = \bigoplus_{i\in\mathbb{Z}} A_1^{\otimes i}$.

Proof. The action μ being free means that the dual to (14.6), which in our case is

$$\mu^* : A \otimes_R A \longrightarrow R[t, t^{-1}] \otimes_R A$$
$$A_i \otimes_R A \ni a_i \otimes b \longmapsto t^i \otimes a_i b,$$

is surjective. In particular, $t \otimes 1$ lies in its image. This means there exist $e_1, \ldots, e_r \in A_1$ and $b_1, \ldots, b_r \in A$ such that $1 = e_1 b_1 + \ldots + e_r b_r$. Arranging this identity degree by degree, we see that we may assume that $e_1, \ldots, e_r$ are homogeneous of degree 1 and that $b_1, \ldots, b_r$ are homogeneous of degree -1. Set $u_i = e_i b_i$. Then

$$\operatorname{Spec} A_0 = \cup_{i=1}^r D(u_i).$$

Claim: There is a $\mathbb{G}_m$-equivariant isomorphism $\mathbb{G}_{m,D(u_i)} \xrightarrow{\sim} D(u_i) \times_Q X$. To prove this, note that $u_i \in A[u_i^{-1}]$ is invertible. So e_i and b_i are invertible in $A[u_i^{-1}]$. Given any $a \in A_1[u_i^{-1}]$, we may write $a = (ae_i^{-1})e_i$. In other words, multiplication by e_i defines an isomorphism of $A_0[u_i^{-1}]$-modules

$$e_i : A_0[u_i^{-1}] \xrightarrow{\sim} A_1[u_i^{-1}].$$

This shows that A_1 is a line bundle over A_0 that is trivialized by e_i above $D(u_i)$. Given $a \in A_d[u_i^{-1}]$, we similarly have $a = (a \cdot e_i^{-d}) \cdot e_i^d$. So the natural map

$$\bigoplus_{i\in\mathbb{Z}} A_1^{\otimes i} \xrightarrow{\sim} A$$

is an isomorphism. Over $D(u_i)$, this states that $A[u_i^{-1}] = (A_0[u_i^{-1}])[e_i, e_i^{-1}]$ as graded ring (e_i sits in degree 1), meaning that there is a $\mathbb{G}_m$-equivariant isomorphism

$$\mathbb{G}_{m,D(u_i)} \xrightarrow{\sim} D(u_i) \times_Q X \tag{14.11}$$

as claimed. In particular, $X \to Q$ is a $\mathbb{G}_m$-torsor for the Zariski topology in the sense of Definition 14.2 that is trivialized by the covering $\sqcup_{i=1}^r D(u_i) \to Q$. The proof is complete. □

[20] This notation is justified because $\mathcal{W}_n(R) \subseteq \mathcal{W}_n(K)$ which follows from the fact that $\mathcal{W}_n$ is representable by an affine scheme/resp. is separated. The more precise meaning is that $\lambda \in R^\times$ and that there exists a datum $(\widetilde{E}, \widetilde{\alpha}, \widetilde{\pi}) \in \mathcal{W}_n(R)$ with $K \otimes_R (\widetilde{E}, \widetilde{\alpha}, \widetilde{\pi}) \cong (E, \alpha, \pi)$.

14.4. **Proof of Theorem 14.7.** Recall that $n \geq 3$. Our aim is to construct two mutually quasi-inverse functors Φ and Ψ that make the following diagram commute,

$$\begin{array}{ccc} & \mathcal{W}_n & \\ {\scriptstyle q}\swarrow & & \searrow{\scriptstyle q} \\ \mathcal{E}\ell\ell_n & \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} & \mathcal{M}_n. \end{array} \tag{14.12}$$

Construction of Φ. This is the same as the construction of $\mathcal{J}$ in (13.13). Given an isomorphism class $(E,\alpha) \in \mathcal{E}\ell\ell_n(S)$, pick an open covering $S = \cup_{i\in I} S_i$ such that $\omega_E|_{S_i}$ is trivial. Choose generators $\pi_i \in \Omega^1_{E/S}(E_i)$. These define points $(E|_{S_i}, \alpha, \pi_i) \in \mathcal{W}_n(S_i)$ which map to points $x_i = q(E|_{S_i}, \alpha, \pi_i) \in \mathcal{M}_n(S_i)$ of the quotient. On overlaps $S_i \cap S_j$, the choices $\pi_i|_{S_i\cap S_j}$ and $\pi_j|_{S_i\cap S_j}$ differ by a (unique) unit from $\mathcal{O}_S(S_i \cap S_j)^\times$. In other words, they are $\mathbb{G}_m(S_i \cap S_j)$-translates of each other. Since q is $\mathbb{G}_m$-invariant, this implies

$$x_i|_{S_i\cap S_j} = x_j|_{S_i\cap S_j} \in \mathcal{M}_n(S_i \cap S_j).$$

Hence the datum $(x_i)_{i\in I}$ glues to an S-valued point $\Phi(E,\alpha) \in \mathcal{M}_n(S)$. Note that this is the unique way to define a natural transformation Φ that makes (14.12) commute.

Construction of Ψ. We now use that $n \geq 3$ and apply our previous preparations. Note that constructing Ψ is equivalent to constructing an isomorphism class $(E,\alpha) \in \mathcal{E}\ell\ell_n(\mathcal{M}_n)$. Combining Proposition 14.10 with Proposition 14.13, we have shown that $\mathcal{W}_n \to \mathcal{M}_n$ is a $\mathbb{G}_m$-torsor for the Zariski topology. In particular, there exists an open covering $\mathcal{M}_n = \cup_{i\in I} U_i$ together with sections σ_i

$$\begin{array}{ccc} & & \mathcal{W}_n \\ & {\scriptstyle \sigma_i}\nearrow & \big\downarrow{\scriptstyle q} \\ U_i & \hookrightarrow & \mathcal{M}_n. \end{array}$$

(Concretely, choose the U_i as the $D(u_i)$ in (14.11), and note that $\mathbb{G}_{m,U_i}$ has the constant section 1.) By the moduli definition of $\mathcal{W}_n$, the sections σ_i correspond to triples (E_i, α_i, π_i) over U_i.

Part of the torsor property is that for each pair i, j, there exists a unique unit $\lambda_{ij} \in \mathcal{O}_{\mathcal{M}_n}(U_i \cap U_j)^\times$ with

$$(E_i, \alpha_i, \pi_i)|_{U_i\cap U_j} \;\cong\; \lambda_{ij} \cdot (E_j, \alpha_j, \pi_j)|_{U_i\cap U_j}.$$

Namely, up to isomorphism, we are comparing two sections

$$\sigma_i|_{U_i\cap U_j},\ \sigma_j|_{U_i\cap U_j} : U_i \cap U_j \longrightarrow \mathbb{G}_{m,U_i\cap U_j},$$

and such sections always differ by left multiplication with an element of $\mathbb{G}_m(U_i \cap U_j)$.

The conclusion is that, in particular, there exist isomorphisms

$$\gamma_{ij} : (E_i, \alpha_i)|_{U_i\cap U_j} \xrightarrow{\sim} (E_j, \alpha_j)|_{U_i\cap U_j}.$$

By Proposition 14.8, the cocycle condition is automatically satisfied for $\{\gamma_{ij}\}$, and hence the datum $(E_i, \alpha_i)_{i\in I}$ glues to a (unique up to isomorphism) pair $(E,\alpha) \in \mathcal{E}\ell\ell_n(\mathcal{M}_n)$.

Tracing through the definitions of Φ and Ψ, a small check shows that they are mutually quasi-inverse. □

15. The Deuring–Eichler Mass Formula

In this last section, we present an application of the construction of the moduli space for $\mathcal{M}_n$, $n \geq 3$. Namely, we will explain a proof of the mass formula of Deuring–Eichler

(10.9):

$$\sum_{\{E \text{ supersing. over } \bar{\mathbb{F}}_p\}/\sim} \frac{1}{|\mathrm{Aut}(E)|} = \frac{p-1}{24}. \tag{15.1}$$

We will take several statements on faith in this section, but the proof logic will still demonstrate the significance of having a universal family of elliptic curves.

15.1. **Ordinary and supersingular elliptic curves.** Let E/k be an elliptic curve over a field of characteristic p. We have seen that $E[p]$ is a k-group scheme of degree p^2. What else can we say? We know:

(1) The $\bar{k}$-points $E[p](\bar{k})$ form a p-torsion group of order $\leq p^2$. Up to isomorphism, the only possibilities are 0, $\mathbb{Z}/p\mathbb{Z}$, or $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$.

(2) The identity connected component of $E[p]$, call it $E[p]^\circ$, is a closed subscheme of $\operatorname{Spec}\mathcal{O}_{E,e}$. The local ring $\mathcal{O}_{E,e}$ is a DVR because E is a smooth curve, and its residue field is k. Let $t \in \mathcal{O}_{E,e}$ be a uniformizer. There is hence an integer $m \geq 1$ such that $E[p]^\circ \cong \operatorname{Spec} k[t]/(t^m)$. By a translation argument, $|E[p](\bar{k})| \cdot m = p^2$, so $m \in \{1, p, p^2\}$.

(3) The group scheme $E[p]$ cannot be étale because we have shown that

$$e^*\Omega^1_{E[p]/k} = \ker\left(p : e^*\Omega^1_{E/k} \longrightarrow e^*\Omega^1_{E/k}\right). \tag{15.2}$$

This shows that the only possibilities are $m = p$ or p^2.

Definition 15.1. We call E ordinary if $m = p$, or equivalently if $|E[p](\bar{k})| = p$. We call E supersingular in the complementary case: $m = p^2$ and $|E[p](\bar{k})| = \{0\}$.

We note without proof that this is equivalent to the definition we gave at the end of §10:

Proposition 15.2. *Let E/k be an elliptic curve over a field of characteristic p. The following are equivalent:*

(1) E is supersingular, meaning $E[p](\bar{k}) = \{0\}$.

(2) $\mathrm{End}(\bar{k} \otimes_k E)$ is non-commutative, meaning an order in a quaternion algebra.

15.2. **Frobenius and Verschiebung.** Let X be a scheme over $\mathbb{F}_p$. Then there is the absolute Frobenius morphism $F_X : X \to X$: It is (by definition) the identity on the topological space of X and given by

$$F_X^*(f) = f^p, \quad f \in \mathcal{O}_X(U),\ U \subseteq X \text{ open}$$

on functions. Now assume that X is an S-scheme. Clearly, F_X need not be a morphism of S-schemes because it also acts by $f \mapsto f^p$ on functions coming from $\mathcal{O}_S$. More precisely, the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{F_X} & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{F_S} & S. \end{array} \tag{15.3}$$

Set $X^{(p)} = S \times_{F_S,\, S} X$. By the universal property, (15.3) gives rise to an S-morphism $F_{X/S}$ called the relative Frobenius,

$$\begin{array}{ccccc} & & & \overset{F_X}{\frown} & \\ X & \xrightarrow{F_{X/S}} & X^{(p)} & \longrightarrow & X \\ & \searrow & \downarrow & & \downarrow \\ & & S & \xrightarrow{F_S} & S. \end{array} \tag{15.4}$$

Apply this to an elliptic curve E/S. The pullback $E^{(p)}$ is again an elliptic curve over S, called the Frobenius twist of E. The relative Frobenius $F_{E/S} : E \to E^{(p)}$ preserves the unit section. By Corollary 7.25, it defines a homomorphism.

Example 15.3. Locally on S, the relative Frobenius has the following description. Suppose E is given by the Weierstrass equation $y^2 = x^3 + ax + b$ where $a, b \in \mathcal{O}_S(S)$. Then $E^{(p)}$ is defined by

$$E^{(p)} : \ y^2 = x^3 + a^p x + b^p.$$

In particular, the Hasse invariants of E and $E^{(p)}$ are related by $j(E^{(p)}) = j(E)^p$. On the affine opens $E \setminus \{e(S)\}$ and $E^{(p)} \setminus \{e(S)\}$, the relative Frobenius is given by

$$F_{E/S} : V(y^2 - x^3 - ax - b) \longrightarrow V(y^2 - x^3 - a^p x - b^p), \quad F^*_{E/S}(x) = x^p, \ F^*_{E/S}(y) = y^p.$$

This makes sense because

$$F^*_{E/S}(y^2 - x^3 - a^p x - b^p) = (y^2 - x^3 - ax - b)^p \in (y^2 - x^3 - ax - b).$$

The relative Frobenius $F_{E/S}$ is bijective on topological spaces. It is, in particular, fiber-wise non-zero and hence an isogeny. We know (Lemma 9.1) that this implies that $\ker(F_{E/S})$ is a finite locally free group scheme over S. Let $\mathcal{I} \subset \mathcal{O}_E$ be the ideal sheaf defining the unit section $e(S)$. When computing the kernel via the Cartesian diagram

$$\begin{array}{ccc} \ker(F_{E/S}) & \longrightarrow & S \\ \downarrow & & \downarrow e \\ E & \xrightarrow[F_{X/S}]{} & E^{(p)}, \end{array}$$

it is not hard to show that $\ker(F_{E/S}) = V(\mathcal{I}^p)$: For example, the definition of $F_{E/S}$ immediately gives $V(\mathcal{I}^p) \subseteq \ker(F_{E/S})$. Then we can check in fibers (i.e. for smooth curves over a field) that $\deg(F_{E/S}) = p$, so equality has to hold.

Definition 15.4. By the above, the degree of $F_{E/S}$ is p. Define the Verschiebung

$$V : E^{(p)} \longrightarrow E$$

as the unique homomorphism such that $VF_{E/S} = [p]_E$ (use Proposition 10.1). Equivalently, define V as the Rosati adjoint $F^*_{E/S}$.

Proposition 15.5. *Let E/k be an elliptic curve over a field in characteristic p. Then E is ordinary if and only if $V : E^{(p)} \to E$ is an étale isogeny.*

Proof. We have essentially seen during §9 that an isogeny $f : E_1 \to E_2$ is étale if and only if $\ker(f)$ is an étale group scheme. Assume the base is a field, say $S = \operatorname{Spec} k$. By Theorem 9.16, we know

$$\begin{aligned} \ker(f) \text{ is étale} &\iff \bar{k} \otimes_k \ker(f) \text{ is constant} \\ &\iff |\ker(f)(\bar{k})| = \deg(\ker(f)). \end{aligned} \tag{15.5}$$

Specializing to the situation of the proposition, we need to show that E is ordinary if and only if $|\ker(V)(\bar{k})| = p$. (Note that $\deg(V) = p$.) Since $VF_{E/k} = [p]$, we have $F^{-1}_{E/k}(\ker(V)) = E[p]$. If E is supersingular, then $E[p] \cong \operatorname{Spec} k[t]/(t^{p^2})$ and this implies $\ker(V)(\bar{k}) = \{0\}$. If V is ordinary, then we know that $E[p](\bar{k}) \cong \mathbb{Z}/p\mathbb{Z}$. We also know that $\ker(F_{E/k}) \cong \operatorname{Spec} k[t]/(t^p)$, so necessarily $\ker(V)(\bar{k}) \cong \mathbb{Z}/p\mathbb{Z}$. □

Example 15.6. Consider a prime $p \nmid 6n$ and the special fiber $\mathcal{M}_{n,\mathbb{F}_p}$. Denote by $\mathcal{E}/\mathcal{M}_{n,\mathbb{F}_p}$ the universal elliptic curve. (We do not require the universal level-n-structure on $\mathcal{E}$.) Then all that has been said before applies to $\mathcal{E}$: There is the Verschiebung morphism

$V : \mathcal{E}^{(p)} \to \mathcal{E}$. The kernel $\ker(V)$ is a finite locally free $\mathcal{M}_{n,\mathbb{F}_p}$-group scheme of degree p. Its fibers are étale (resp. connected) precisely over those points of $\mathcal{M}_{n,\mathbb{F}_p}$ over which $\mathcal{E}$ is ordinary (resp. supersingular). Only finitely many points are supersingular, and our aim is to count them.

15.3. **The Hasse invariant.** Recall that we defined the Hodge bundle of E/S by $\omega_E = e^*\Omega^1_{E/S}$. If $f : E_1 \to E_2$ is a homomorphism, then pullback of differential forms defines a map of line bundles $f^* : \omega_{E_2} \to \omega_{E_1}$.

Lemma 15.7. *Let $f : E_1 \to E_2$ be a homomorphism of elliptic curves over S. Then f is an étale isogeny if and only if the induced pullback $f^* : \omega_{E_2} \to \omega_{E_1}$ is an isomorphism.*

Proof. The map f is étale if $\Omega^1_{E_1/E_2} = 0$. By a translation argument that one can carry out in geometric fibers, for example, this is equivalent to $e^*\Omega^1_{E_1/E_2} = 0$. Consider the exact sequence

$$f^*\Omega^1_{E_2/S} \longrightarrow \Omega^1_{E_1/S} \longrightarrow \Omega^1_{E_1/E_2} \longrightarrow 0.$$

Pullback along the unit section of E_1 gives an exact sequence

$$\omega_{E_2} \xrightarrow{f^*} \omega_{E_1} \longrightarrow e^*\Omega^1_{E_1/E_2} \longrightarrow 0.$$

Both ω_{E_2} and ω_{E_1} are line bundles on S, so f^* is not invertible precisely if $e^*\Omega^1_{E_1/E_2}$ is non-zero, as was to be shown. □

Lemma 15.8. *Let E/S be an elliptic curve over an $\mathbb{F}_p$-scheme S. There is a natural isomorphism $\omega_{E^{(p)}} \xrightarrow{\sim} \omega_E^{\otimes p}$.*

Proof. Consider the diagram that defines $E^{(p)}$:

$$\begin{array}{ccc} E^{(p)} & \xrightarrow{h} & E \\ {\scriptstyle e^{(p)}}\uparrow\downarrow & & \uparrow\downarrow{\scriptstyle e} \\ S & \xrightarrow[F_S]{} & S. \end{array} \tag{15.6}$$

We have denoted the unit section of $E^{(p)}$ by $e^{(p)}$ because it comes via base change of e along F_S. Now recall that the formation of Ω^1 commutes with base change. That is,

$$h^* : h^*\Omega^1_{E/S} \xrightarrow{\sim} \Omega^1_{E^{(p)}/S}.$$

If we now apply the definition of $\omega_{E^{(p)}}$, then we find

$$\omega_{E^{(p)}} = e^{(p),*}\big(h^*\Omega^1_{E/S}\big) = F_S^*\big(e^*\Omega^1_{E/S}\big) = F_S^*\omega_E. \tag{15.7}$$

Given any line bundle $\mathcal{L}$ on an $\mathbb{F}_p$-scheme S, we have $F_S^*(\mathcal{L}) = \mathcal{L}^{\otimes p}$. Namely, if $(\phi_{ij})_{i,j} \in H^1(S, \mathcal{O}_S^\times)$ is a cocycle defining $\mathcal{L}$, then $(\phi_{ij}^p)_{i,j}$ is a cocycle defining $F_S^*(\mathcal{L})$. Applying this to (15.7) finishes the proof. □

Definition 15.9 (Hasse invariant)**.** Let E/S be an elliptic curve over an $\mathbb{F}_p$-scheme S. Consider the pullback map on Hodge bundles induced by the Verschiebung,

$$V^* : \omega_E \longrightarrow \omega_{E^{(p)}/S} = \omega_E^{\otimes p}. \tag{15.8}$$

Let $\mathrm{Ha}_E \in H^0(S, \omega_E^{p-1})$ be the corresponding section of ω_E^{p-1}. It is called the Hasse invariant of E.

Corollary 15.10. *For every point $s \in S$,*

$$\mathrm{Ha}_E(s) = 0 \quad \Longleftrightarrow \quad E(s) \text{ is supersingular.} \tag{15.9}$$

Proof. By Lemma 15.7, $\mathrm{Ha}_E(s) = 0$ if and only if $V(s) : E(s)^{(p)} \to E(s)$ is not étale. By Proposition 15.5, this happens if and only if $E(s)$ is supersingular. □

15.4. **Application to our counting problem.**

Example 15.11. Suppose that $n \geq 3$ and $p \nmid 6n$. Consider the geometric special fiber $\mathcal{M}_{n,\bar{\mathbb{F}}_p} = \bar{\mathbb{F}}_p \otimes_{\mathbb{Z}[1/6n]} \mathcal{M}_n$ with its universal elliptic curve $\mathcal{E}$. Corollary 15.10 implies that

$$\#\left\{(E,\alpha)/\bar{\mathbb{F}}_p \;\middle|\; \begin{matrix} E \text{ supersing.} \\ \alpha \text{ level-}n\text{-str.}\end{matrix}\right\}/\text{iso.} \;=\; \#\{x \in \mathcal{M}_{n,\bar{\mathbb{F}}_p} \mid \mathrm{Ha}_{\mathcal{E}}(x) = 0\}. \tag{15.10}$$

Proposition 15.12. *Suppose $n \geq 3$. The morphism $\mathcal{M}_n \to \operatorname{Spec}\mathbb{Z}[1/6n]$ is smooth of relative dimension 1.*

Proof. The Weierstrass moduli problem $\mathcal{W}$ is representable by an open subscheme of $\mathbb{A}^2_{\mathbb{Z}}$ (Theorem 12.3). In particular, it is smooth of relative dimension 2 over $\mathbb{Z}$. The morphism $\mathcal{W}_n \to \mathcal{W}$ is finite étale by Corollary 14.6. So $\mathcal{W}_n$ is also smooth of relative dimension 2 over $\mathbb{Z}$.

Next note the following fact. Let $X \to Y \to Z$ be two morphisms of locally finite presentation. Suppose that $X \to Y$ is surjective and smooth of dimension d, and that $X \to Z$ is smooth of dimension e. Then $Y \to Z$ is smooth of dimension $e - d$.

We know that $\mathcal{W}_n \to \mathcal{M}_n$ is a $\mathbb{G}_m$-torsor, in particular surjective and smooth of relative dimension 1. We deduce that $\mathcal{M}_n \to \mathbb{Z}$ is smooth of relative dimension 1. □

In particular, $\mathcal{M}_{n,\bar{\mathbb{F}}_p}$ is a smooth, affine, 1-dimensional $\bar{\mathbb{F}}_p$-scheme. It need not be connected, but each connected component is integral and normal. Let $\mathrm{Ha} \in \omega^{p-1}(\mathcal{M}_{n,\bar{\mathbb{F}}_p})$ be the Hasse invariant of the universal elliptic curves. We can view the vanishing locus $V(\mathrm{Ha})$ as a divisor on $\mathcal{M}_{n,\bar{\mathbb{F}}_p}$. In this context, we have the following important result of Igusa:

Proposition 15.13 (Igusa)**.** *The multiplicities of* $\operatorname{div}(\mathrm{Ha})$ *are all equal to* 1*. In particular,*

$$\deg(\operatorname{div}(\mathrm{Ha})) = \#\left\{(E,\alpha)/\bar{\mathbb{F}}_p \;\middle|\; \begin{matrix} E \textit{ supersing.} \\ \alpha \textit{ level-}n\textit{-str.}\end{matrix}\right\}/\textit{iso.} \tag{15.11}$$

The right hand side in (15.11) is closely related to our original counting problem. Namely fix an elliptic curve E over an algebraically closed field k. Let $n \geq 1$ be an integer such that $\mathrm{char}(k) \nmid n$. Then $E[n] \cong \underline{\mathbb{Z}/n\mathbb{Z}}_k^{\oplus 2}$ and there are precisely

$$|GL_2(\mathbb{Z}/n\mathbb{Z})| = |\mathrm{Isom}\left((\mathbb{Z}/n\mathbb{Z})^{\oplus 2}, E[n](k)\right)|$$

many level structures on E. Let α_0 and α_1 be two such level structures. Then (E,α_0) and (E,α_1) are isomorphic in the sense of $\mathcal{E}\ell\ell_n(k)$ if and only if there exists an automorphism $\gamma \in \mathrm{Aut}(E)$ such that $\alpha_1 = \gamma \circ \alpha_0$.

Suppose in addition that $n \geq 3$. Then $\mathrm{Aut}(E) \to \mathrm{Aut}(E[n](k))$ is injective by Proposition 14.8 and we see that there are $|GL_2(\mathbb{Z}/n\mathbb{Z})|/|\mathrm{Aut}(E)|$ many pairs (E,α) up to isomorphism. So dividing both sides of (15.11) by $|GL_2(\mathbb{Z}/n\mathbb{Z})|$, we obtain

$$\frac{\deg(\operatorname{div}(\mathrm{Ha}))}{|GL_2(\mathbb{Z}/n\mathbb{Z})|} \;=\; \sum_{\{E/\bar{\mathbb{F}}_p \text{ supersing.}\}/\text{iso.}} \frac{1}{|\mathrm{Aut}(E)|}. \tag{15.12}$$

15.5. **Compactification of $\mathcal{M}_n$.** It is clear from (15.12) that our aim is to determine $\deg(\operatorname{div}(\mathrm{Ha}))$, where $\mathrm{Ha} \in \omega^{p-1}(\mathcal{M}_{n,\bar{\mathbb{F}}_p})$ is the Hasse invariant of the universal elliptic curve. Recall that if D is a divisor on a proper curve X in the sense of §6, then $\deg(D)$ only depends on the line bundle $\mathcal{O}_X(D)$. In order to apply this logic to Ha, we need to compactify $\mathcal{M}_{n,\bar{\mathbb{F}}_p}$. This is easy to do abstractly: Every connected affine smooth curve has a natural smooth projective compactification ([5, Theorem 24.1]). Applying this to each connected component of $\mathcal{M}_{n,\bar{\mathbb{F}}_p}$, we can define

$$\overline{\mathcal{M}_{n,\bar{\mathbb{F}}_p}} \;:=\; \begin{matrix}\text{disjoint union of the smooth compactifications} \\ \text{of all connected components of } \mathcal{M}_{n,\bar{\mathbb{F}}_p}.\end{matrix} \tag{15.13}$$

The subtle question is how to extend the pair $(\omega^{p-1}, \mathrm{Ha})$ to this compactification. Moreover, we would like to have a description of the boundary points $\overline{\mathcal{M}_{n,\bar{\mathbb{F}}_p}} \setminus \mathcal{M}_{n,\bar{\mathbb{F}}_p}$. These questions were answered in a classical article by Deligne–Rapoport [2] who constructed a compactification of $\mathcal{M}_n$ in terms of generalized elliptic curves. The first page of their article already shows that this involves certain singular genus 1 curves:

II Courbes elliptiques généralisées.

Dans ce chapitre, nous définissons les courbes elliptiques généralisées sur un schéma de base quelconque, et prouvons les théorèmes qui rendent viable la définition adoptée.

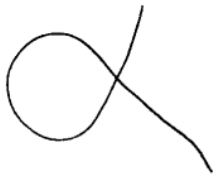
1. Polygones de Néron.

1.1 Soit $\tilde{C} = \mathbb{P}^1 \times \mathbb{Z}/n$ la somme disjointe de n copies de $\mathbb{P}^1$, indexées par $\mathbb{Z}/n$ ($n \geq 1$). En recollant la i-ième copie de $\mathbb{P}^1$ avec la (i+1)-ième, par identification de la section 0 de la i-ième copie avec la section ∞ de la (i+1)-ième, on obtient une courbe de genre un C sur Spec($\mathbb{Z}$), de normalisée $\tilde{C}$.

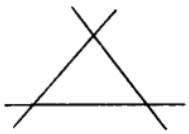
Pour tout schéma S, on appelle polygone de Néron à n côtés standard sur S, ou simplement n-gone standard sur S, le schéma sur S qui s'en déduit par extension des scalaires. Un polygone de Néron (resp. un n-gone) sur un corps algébriquement clos k est un schéma sur k isomorphe à l'un des polygones standards (resp. au n-gone standard).

Exemples.

n = 1



n = 3



We will mostly be interested in the case $n \geq 3$. Then a Néron n-gon over an algebraically closed field k is a proper reduced connected k-scheme X of dimension 1 with the following properties:

(1) X has n irreducible components all of which are isomorphic to $\mathbb{P}^1_k$.

(2) Each irreducible component intersects precisely two other irreducible components, each in a single point. (Note that since X is connected, the irreducible components then necessarily form a circle.

(3) All intersections are transversal. This notion can be defined in general, but here it means that each intersection point has an affine neighborhood that is isomorphic to $\operatorname{Spec} k[x,y]/(xy)$.

Definition 15.14 ([2, Definition II.1.4])**.** Let S be a scheme. A stable curve of genus 1 over S is a morphism $X \to S$ that is proper, flat, of finite presentation, with 1-dimensional fibers and the following property: For each $s \in S$, the geometric fiber $\operatorname{Spec}\overline{\kappa(s)} \times_S X$ is either a smooth curve of genus 1 like in §6, or a Néron n-gon over $\overline{\kappa(s)}$ (where n is allowed to depend on s).

Let $p : X \to S$ is a stable curve of genus 1. We denote by $X^{\mathrm{sm}} \subseteq X$ the locus where p is smooth. This is an open subset which agrees with the complement of all the n-gon intersection points of the non-smooth fibers.

Definition 15.15. (1) A generalized elliptic curve over S is a stable curve $E \to S$ of genus 1 together with a multiplication morphism

$$m : E^{\mathrm{sm}} \times_S E \longrightarrow E$$

that restricts to a group scheme structure on E^{sm}.

(2) Assume $n \in \mathcal{O}_S(S)^\times$. A generalized elliptic curve with level-n-structure (E, α) over S is a generalized elliptic curve $E \to S$ whose fibers are either smooth or n-gons together with a trivialization

$$\alpha : \underline{\mathbb{Z}/n\mathbb{Z}}_S^{\oplus 2} \xrightarrow{\sim} E^{\mathrm{sm}}[n].$$

Let k be an algebraically closed field and E/k an n-gon. Up to isomorphism, there is precisely one possibility[21] to define a generalized elliptic curve structure on E and then

$$(E^{\mathrm{sm}},\ m|_{E^{\mathrm{sm}} \times_k E^{\mathrm{sm}}}) \ \cong\ \mathbb{Z}/n\mathbb{Z} \times \mathbb{G}_{m,k}.$$

In particular, $E^{\mathrm{sm}}[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mu_{n,k}$. Torsion subgroups also behave well in families: If $E \to S$ is a generalized elliptic curve with fibers smooth or n-gons, then $E[n]$ is a finite locally free S-group scheme of degree n^2.

Theorem 15.16 (Deligne–Rapoport)**.** *Assume that $n \geq 3$. Consider the functor of isomorphism classes of generalized elliptic curves with level-n-structure (E, α) on $\mathbb{Z}[1/6n]$-schemes. It is representable by a proper smooth morphism $\overline{\mathcal{M}_n} \to \operatorname{Spec}\mathbb{Z}[1/6n]$.*

We assume $n \geq 3$ from now on. For $p \nmid 6n$, the special fiber $\bar{\mathbb{F}}_p \otimes_{\mathbb{Z}} \overline{\mathcal{M}_n}$ is a proper smooth curve over $\bar{\mathbb{F}}_p$ that contains $\mathcal{M}_{n,\bar{\mathbb{F}}_p}$ as dense open subscheme. It is hence isomorphic to the abstract compactification from (15.13).

Moreover, let $\bar{\mathcal{E}}$ be the universal generalized elliptic curve on $\overline{\mathcal{M}_n}$. Then $\bar{\omega} := e^*\Omega^1_{\bar{\mathcal{E}}/\overline{\mathcal{M}_n}}$ provides a natural extension of the Hodge bundle from $\mathcal{M}_n$ to $\overline{\mathcal{M}_n}$.

Proposition 15.17. *The Hasse invariant $\mathrm{Ha} \in \omega^{p-1}(\mathcal{M}_{n,\bar{\mathbb{F}}_p})$ extends to a section $\overline{\mathrm{Ha}} \in \bar{\omega}^{p-1}(\overline{\mathcal{M}_{n,\bar{\mathbb{F}}_p}})$ that does not vanish in any of the boundary points $\overline{\mathcal{M}_{n,\bar{\mathbb{F}}_p}} \setminus \mathcal{M}_{n,\bar{\mathbb{F}}_p}$.*

Intuitively, the lemma holds because the n-torsion in a Néron n-gon is $\mathbb{Z}/n\mathbb{Z} \times \mu_n$, which is just like for an ordinary elliptic curve. We obtain that

$$\deg(\operatorname{div}(\mathrm{Ha})) = (p-1) \cdot \deg(\bar{\omega}) \tag{15.14}$$

where the right hand side denotes the degree as line bundle on a proper smooth curve.[22]

[21] Main idea and exercise for this: Determine all automorphisms of $\mathbb{P}^1_k$ that fix 0 and ∞.

[22] More precisely, take the sum of the degrees on all connected components.

15.6. **The degree of $\bar{\omega}$.**

Proposition 15.18. *The degree of $\bar{\omega}$ on $\overline{\mathcal{M}}_{n,\bar{\mathbb{F}}_p}$ is given by*

$$\deg(\bar{\omega}) = \frac{|GL_2(\mathbb{Z}/n\mathbb{Z})|}{24}. \tag{15.15}$$

Proof. Step 1: The discriminant. Let $y^2 = x^3 + ax + b$ be the simple Weierstrass equation for a pair $(E, \pi) \in \mathcal{W}(S)$. We have seen during the Proof of Proposition 13.14 that if we scale π to $\lambda\pi$, then (a, b) scale to $(\lambda^{-4}a, \lambda^{-6}b)$. Now recall that $\pi \in \omega(S)$ is nothing but a trivialization of the Hodge bundle. It follows that for any family of elliptic curves E/S with $6 \in \mathcal{O}_S(S)^\times$, we have defined natural sections

$$a \in \omega^{-4}(S), \quad b \in \omega^{-6}(S).$$

(Concretely, let $S = \cup_{i\in I} S_i$ be an open covering such that there exist trivializations $\omega|_{S_i} = \mathcal{O}_S \cdot \pi_i$. Let $a_i, b_i \in \mathcal{O}_S(S_i)$ be the corresponding Weierstrass equation coefficients. On each intersection $U_{ij} = U_i \cap U_j$, there exists λ_{ij} such that $\pi_i = \lambda_{ij}\pi_j$. Then $a_i = \lambda_{ij}^{-4} a_j$ and $b_i = \lambda_{ij}^{-6} b_j$ which shows that they glue to sections of ω^{-4} resp. ω^{-6}.) In particular, the discriminant defines a nowhere vanishing section

$$\Delta = 4a^3 + 27b^2 \in \omega^{-12}(S).$$

Step 2: Application to the universal family. We apply all this with $S = \mathcal{M}_{n,\bar{\mathbb{F}}_p}$ and obtain a nowhere vanishing section $\Delta \in \omega^{-12}(S)$.

Proposition 15.19. *The inverse $\Delta^{-1} \in \omega^{12}(S)$ extends to a section of $\bar{\omega}^{12}$ that has simple zeroes at all points of the boundary $\overline{\mathcal{M}}_{n,\bar{\mathbb{F}}_p} \setminus \mathcal{M}_{n,\bar{\mathbb{F}}_p}$.*

The proof of Proposition 15.19 requires one to understand the complete local rings at boundary points. This is done in terms of the so-called Tate curve. We take the statement on faith and obtain that

$$\deg(\bar{\omega}) = \frac{|\overline{\mathcal{M}}_{n,\bar{\mathbb{F}}_p} \setminus \mathcal{M}_{n,\bar{\mathbb{F}}_p}|}{12}. \tag{15.16}$$

Step 3: The number of boundary points. Let k be an algebraically closed field with $\mathrm{char}(k) \nmid n$ and let E_∞/k be an n-gon generalized elliptic curve. How many pairs $(E_\infty, \alpha) \in \overline{\mathcal{M}}_n(k)$ are there? The argument is the same as before (15.12). It is not too hard to see that $\mathrm{Aut}(E_\infty) = \{\pm 1\}$ and $\{\pm 1\} \hookrightarrow \mathrm{Aut}(E_\infty^{\mathrm{sm}}[n])$. So the number of isomorphism classes (E_∞, α) is

$$|\overline{\mathcal{M}}_{n,\mathbb{F}_p} \setminus \mathcal{M}_{n,\bar{\mathbb{F}}_p}| = \frac{|GL_2(\mathbb{Z}/n\mathbb{Z})|}{2}. \tag{15.17}$$

Combining (15.16) and (15.17), we find

$$\deg(\bar{\omega}) = \frac{|GL_2(\mathbb{Z}/n\mathbb{Z})|}{24}$$

as was to be shown. □

15.7. **Proof of the Deuring–Eichler mass formula.** Our proof is for all $p \geq 5$. Pick an auxiliary integer $n \geq 3$ with $p \nmid n$. We now combine all the results we obtained about $\mathcal{M}_{n,\bar{\mathbb{F}}_p}$:

$$\begin{aligned} \sum_{\{E/\bar{\mathbb{F}}_p \text{ supersing.}\}/\text{iso.}} \frac{1}{|\mathrm{Aut}(E)|} &\overset{(15.12)}{=} \frac{\deg(\mathrm{div}(\mathrm{Ha}))}{|GL_2(\mathbb{Z}/n\mathbb{Z})|} \\ &\overset{(15.14)}{=} (p-1)\cdot \deg(\bar{\omega}) \\ &\overset{(15.15)}{=} \frac{p-1}{24}, \end{aligned} \tag{15.18}$$

and the proof is complete!

References

[1] Bosch, S.; Lütkebohmert, W.; Raynaud, M., *Néron models*, Ergeb. Math. Grenzgeb. (3) **21**, Springer-Verlag, Berlin, 1990.

[2] Deligne, P.; Rapoport, M., *Les schémas de modules de courbes elliptiques*, Lecture Notes in Math. **349**, Springer-Verlag, Berlin-New York, 1973, pp. 143–316.

[3] Forster, O., *Lectures on Riemann surfaces*, Graduate Texts in Mathematics **81**, Springer-Verlag, New York, 1981.

[4] Mumford, D., *Abelian varieties*, Tata Institute of Fundamental Research, Mumbai, Corrected Reprint, 2012.

[5] Scholze, P., *Lecture notes on algebraic geometry, I*, written by J. Davies (2017), https://www.math.uni-bonn.de/people/mihatsch/24%20SS/ec/notes1.pdf.

[6] Scholze, P., *Lecture notes on algebraic geometry, II*, written by J. Davies (2017), https://www.math.uni-bonn.de/people/mihatsch/24%20SS/ec/notes2.pdf.

[7] Schoof, R., *Is a finite locally free group scheme killed by its order?*, Weblink.

[8] The Stacks Project Authors, *Stacks Project* (2018), https://stacks.math.columbia.edu.