

MODULI STACK OF ELLIPTIC CURVES

LENNART MEIER AND VIKTORIYA OZORNOVA

CONTENTS

1. Introduction	1
2. Elliptic curves	1
3. Moduli stack of elliptic curves	6
4. Weierstraß equations	11
References	17

1. INTRODUCTION

This note does not contain original work by the authors. Its origin is the attempt to understand some details of the construction of the moduli stack of elliptic curves. As the details on several points seem to be hard to find in the literature (but are surely well-known to the experts), we thought it would be good to write them down before we forget them again ourselves. In particular, we tried to be very careful about noetherianity assumptions, as often used in e.g. cohomology and base change statements. The main sources for our note are [KM85], [DR73], [Ols16] and [Vis05].

We do not aim at making self-contained notes, which would be a far more extensive task. Thus, whenever we need a statement e.g. in algebraic geometry which is well-documented, we tend to just cite it (although we are not completely consistent on this).

This note will probably contain errors at every level. Notifications about such as well as more general feedback are welcome.

2. ELLIPTIC CURVES

Before actually discussing the moduli stack of elliptic curves, we want to recall and collect properties of elliptic curves which we will need in the further treatment.

Definition 2.1 ([Har77], Chapter IV). *A **curve** over an algebraically closed field k is an integral regular scheme of dimension 1, proper over k . The **genus** of a curve X over k is defined to be $\dim_k H^1(X, \mathcal{O}_X)$. A curve E of genus 1 together with a chosen distinguished k -valued point $P \in E$ is called **elliptic**.*

Note that this implies in particular that the morphism $X \rightarrow \text{Spec}(k)$ is smooth (cf. e.g. [Har77], Example 10.0.2).

We will need a variant of fpqc descent for elliptic curves over algebraically closed fields, which we discuss in the next lemma.

Lemma 2.2. *Let L be an algebraically closed field and $k \subseteq L$ an algebraically closed field. Moreover, let the square*

$$\begin{array}{ccc} E' & \xrightarrow{p} & \mathrm{Spec}(L) \\ g \downarrow & & \downarrow f \\ E & \xrightarrow{q} & \mathrm{Spec}(k) \end{array}$$

be cartesian. Then E' is a curve of genus g over L if and only if E is a curve of genus g over k .

In particular, (E', P') is an elliptic curve over L if and only if (E, P) is an elliptic curve over k for any choice of L - or k -valued point, respectively.

Proof. Note that f is an faithfully flat and quasi-compact morphism, thus p is proper or smooth if and only if q is proper or smooth, respectively, as shown in [Gro67], Proposition 2.7.1, and Corollaire 17.7.3. By [Sta17, Tag 038H], E being irreducible is equivalent to E' being irreducible. Thus, by Example III.10.0.3 of [Har77], both E and E' are regular integral schemes if one of them is, and by [Har77], Proposition III.10.1, both of dimension 1 if one of them is.

Last we consider their genera. Using that by [Sta17, Tag 02KH], we have

$$H^1(E, \mathcal{O}_E) \otimes_k L \cong H^1(E', \mathcal{O}_{E'}),$$

so the genera of E and E' coincide; thus the claim. \square

Definition 2.3 (cf. e.g. [Ols16]). *An **elliptic curve** over an arbitrary scheme S is a smooth proper morphism $p: E \rightarrow S$ together with a chosen section $e: S \rightarrow E$ so that the pullback of (E, e) to any geometric fiber is an elliptic curve.*

The following easy (and well-known) observation will be helpful.

Lemma 2.4. *Let $p: C \rightarrow S$ be a separated morphism of schemes with a right inverse $e: S \rightarrow C$. Then e is a closed immersion.*

Proof. Indeed, by [Sta17, Tag 01W6], since p is separated and $p \circ e = \mathrm{id}_S$ is proper, we may conclude that e is proper. Since e has a left inverse, it is a monomorphism of schemes. Thus, by [Gro67], Corollaire 18.12.6, it is a closed immersion. \square

Observe that Lemma 2.4 applies immediately to elliptic curves. Note that Lemma 2.4 implies for an elliptic curve E over an algebraically closed field k that specifying a k -valued point is the same as specifying a closed point in E (since E is of finite type over $\mathrm{Spec}(k)$).

Our goal will be to prove a descent property for elliptic curves with respect to fpqc morphisms. We will reduce it to a descent property of polarized schemes, which are roughly speaking schemes with certain additional line bundles which enable the “gluing”.

In our case, we will use as suggested in [Ols16], Section 13.1.4, the line bundle which deserves the name $\mathcal{O}_E(-e)$ on E for (E, p, e) elliptic curve over S . This line bundle will be the inverse of the ideal sheaf of e . We will recall these notions and study the properties of such sheaves in the next lemmas.

Before actually doing so, we will show that every elliptic curve is Zariski locally pulled back from an elliptic curve over a noetherian scheme. This is well-known and is an important tool for reducing problems about elliptic curves over arbitrary basis to elliptic curves over noetherian schemes.

Lemma 2.5.

- (1) Let $p: E \rightarrow \mathrm{Spec}(R)$ be quasi-compact, separated smooth morphism of relative dimension 1. Then it is pulled back from such a morphism over noetherian affine scheme $p_0: X_0 \rightarrow \mathrm{Spec}(R_0)$.
- (2) If p in addition has a section $e: \mathrm{Spec}(R) \rightarrow E$, it can be arranged to be pulled back from a section $\mathrm{Spec}(R_0) \rightarrow X_0$.
- (3) Let $(E, p: E \rightarrow \mathrm{Spec}(R), e)$ be an elliptic curve over an affine scheme. Then it is pulled back from an elliptic curve over noetherian affine scheme.

Proof. (1) We can write the ring R as a filtered colimit over a poset I of subrings R_i which are finite type over \mathbb{Z} , so in particular noetherian, and thus $\mathrm{Spec}(R) \cong \varprojlim \mathrm{Spec}(R_i)$ [GW10, Proposition 10.53].

So we are in the situation of [Sta17, Tag 01ZM]. By possibly restricting to a cofinal subset of I , we may assume I to have an initial object $0 \in I$ and we might assume to have a morphism $p_0: X_0 \rightarrow \mathrm{Spec}(R_0)$ of finite presentation such that p is the pullback of p_0 along the projection $\mathrm{Spec}(R) \rightarrow \mathrm{Spec}(R_0)$, which can in addition be assumed to be of finite presentation. Now we are in the situation of [Sta17, Tag 0C0C], so by possibly restricting to a cofinal subset of I again, we may assume that p_0 is smooth. Next, we use [Gro67, Théorème 8.10.5], so by possibly restricting to a cofinal subset of I again, we may assume that p_0 is separated.

- (2) Using [Sta17, Tag 01ZM] for morphisms, we obtain also a map $e_0: \mathrm{Spec}(R_0) \rightarrow X_0$ of schemes over $\mathrm{Spec}(R_0)$, so a section of p_0 , whose pullback to $\mathrm{Spec}(R)$ is precisely e .
- (3) Now we can apply [Sta17, Tag 0204] to conclude that we also may assume p_0 to be proper. Since its pullback p is of relative dimension 1, so is p_0 .

Our next goal is to show that the geometric fibers of p_0 are connected. We can use [Sta17, Tag 0CC1] to conclude that the image of $\mathrm{Spec}(R)$ is dense in $\mathrm{Spec}(R_0)$ since R_0 is a subring of R . Consider now any geometric point $\mathrm{Spec}(k) \rightarrow \mathrm{Spec}(R_0)$. Since R_0 is a noetherian ring, this implies by [Sta17, Tag 01OZ] and [Sta17, Tag 04MF] that there is a connected open U containing the image of $\mathrm{Spec}(k)$. Since it is open, the image of some point (and thus also of a geometric point) coming from R , so we have a commutative diagram

$$\begin{array}{ccccc} \mathrm{Spec}(k) & \longrightarrow & U & \xrightarrow{\subseteq} & \mathrm{Spec}(R_0) \\ & & \uparrow & & \uparrow \\ & & \mathrm{Spec}(L) & \longrightarrow & \mathrm{Spec}(R), \end{array}$$

where L is some algebraically closed field. The pullback $p_Y: Y := X_0 \times_{\mathrm{Spec}(R_0)} \mathrm{Spec}(L) \rightarrow \mathrm{Spec}(L)$ of p_0 is now again a proper morphism with a section, smooth of relative dimension 1 over a noetherian connected scheme. Over the geometric point $\mathrm{Spec}(L) \rightarrow \mathrm{Spec}(L)$, it is connected since by assumption $(X_0 \times_{\mathrm{Spec}(R_0)} \mathrm{Spec}(L)) \times_{\mathrm{Spec}(L)} \mathrm{Spec}(L) \cong E \times_{\mathrm{Spec}(R)} \mathrm{Spec}(L)$ is an elliptic curve over L .

Now consider the Stein factorization $Y \rightarrow Y' \xrightarrow{g} \mathrm{Spec}(L)$ of the proper morphism of noetherian schemes $p_Y: Y \rightarrow \mathrm{Spec}(L)$ (cf. [FGI⁺05], Theorem 8.2.12). By [Sta17, Tag 034E], the fibers of the smooth map p_Y are geometrically reduced, so we can apply Proposition 8.5.16 of [FGI⁺05] to conclude that

$Y' \rightarrow U$ is étale. Thus also $Y' \times_U \text{Spec } L \rightarrow \text{Spec } L$ is étale, and so $Y' \times_U \text{Spec}(L)$ is a finite disjoint union of copies of $\text{Spec}(L)$ (cf. [Sta17, Tag 02GL]). Next, we know by Zariski's connectedness theorem ([FGI⁺05], Theorem 8.2.12) that the fibers of $Y \rightarrow Y'$ are non-empty and connected. Since being non-empty is compatible with faithfully flat base change, we conclude that also the fibers of $Y \times_U \text{Spec}(L) \rightarrow Y' \times_U \text{Spec}(L)$ are non-empty. Since $Y \times_U \text{Spec}(L)$ is connected, we conclude $Y' \times_U \text{Spec } L \cong \text{Spec } L$. Moreover, by definition of Stein factorization, the map $g: Y' \rightarrow U$ is finite, thus we can apply [Sta17, Tag 02KB] to conclude that $g_*\mathcal{O}_{Y'}$ is a vector bundle on U . Employing cohomology and base change [Sta17, Tag 02KG] and the fact that the pullback of g to $\text{Spec}(L)$ is an isomorphism, we conclude that $g_*\mathcal{O}_{Y'}$ is a vector bundle of rank 1 on the connected scheme U . Thus, also the pullback of g to $\text{Spec}(k)$ is an isomorphism, and using Zariski's connectedness theorem once again implies that the fibers of $Y \rightarrow U$ are geometrically connected.

So we now that the geometric fibers of p_Y are geometrically connected. Again by [Har77], Example III.10.0.3, the geometric fibers are regular of dimension 1. Thus they are in particular normal [Sta17, Tag 0569], and thus [Sta17, Tag 033M] integral since we have already shown that they are connected.

This implies that the geometric fibers of p_Y (and thus also of p_0) are curves. We still need to determine the genus of these curves. With the notation above, we know that the curve $Y \times_U \text{Spec } L \rightarrow \text{Spec } L$ has genus 1. As explained in [Oss], Theorem 1.3, one can deduce from [Gro63, Théorème 7.9.4] that the Euler characteristic of the geometric fibers is constant on the connected scheme U (we also use compatibility of cohomology with faithfully flat base change [Sta17, Tag 02KH]). By [Liu02], Corollary 3.3.21, we know that $H^0(Y \times_U \text{Spec } k, \mathcal{O}_{Y \times_U \text{Spec } k})$ is 1-dimensional, and by Grothendieck's vanishing theorem [Sta17, Tag 02UZ], cohomology groups in dimensions ≥ 2 vanish, so we conclude that all geometric fibers of p_Y and thus of p_0 are indeed elliptic curves. This completes the proof of the lemma. \square

Recall (e.g. from [Har77], Section II.5) that if $i: Z \rightarrow X$ is a closed immersion, we define the corresponding **ideal sheaf** of Z on X as the kernel of the surjective morphism $i^\#: \mathcal{O}_X \rightarrow i_*\mathcal{O}_Z$.

We will be considering the ideal sheaf of the section of an elliptic curve, which makes sense due to Lemma 2.4. Now we have equipped each elliptic curve (E, p, e) over any scheme S with a particular quasi-coherent sheaf, namely with the ideal sheaf of its section $e: S \rightarrow E$. To obtain a polarized scheme, we need to show that this sheaf is a line bundle and that its inverse is ample. Moreover, we will need this construction to be functorial in the sense made more precise below. Before actually dealing with elliptic curves, we will show some more general statements about ideal sheaves.

We have already seen that the section of an elliptic curve $(E, p: E \rightarrow S, e)$ exhibits the image of S as a closed subscheme of E . Our next goal is to show (as stated in [Ols16], Section 13.1.4) that this subscheme is indeed an effective Cartier divisor, i.e., that its ideal sheaf is an invertible \mathcal{O}_E -module. The proof follows [KM85], Sections 1.1 and 1.2.

Proposition 2.6 ([KM85], Section 1.2). *Let $p: C \rightarrow S$ be a smooth morphism of relative dimension 1 which is separated and quasi-compact. Let $e: S \rightarrow C$ be a section of p . Then it defines an effective Cartier divisor in C .*

Proof. We can apply Lemma 2.4 to e to see that it is a closed immersion. We still need to show that the corresponding ideal sheaf on C is a locally free \mathcal{O}_C -module.

First, the ideal sheaf of e being a locally free \mathcal{O}_C -module of rank 1 is a Zariski-local statement, so we can assume S to be an affine scheme, say, $\text{Spec}(R)$. Furthermore, we apply Lemma 2.5 to see that $C \rightarrow \text{Spec}(R)$ is a pullback of an elliptic curve (E_0, p_0, e_0) over a noetherian affine scheme.

It is enough to prove the lemma over noetherian schemes (using the pullback property [KM85, Section 1.1.4] of effective Cartier divisors; note that the flatness assumption in the relative setting is satisfied since $p_0 \circ e_0 = \text{id}_{S_0}$). This is precisely done in [KM85, Corollary 1.1.5.2]. \square

Next, to formalize functoriality properties for the ideal sheaf of the section $e: S \rightarrow E$ of an elliptic curve (E, p, e) over S , we need to introduce a notion of morphism for elliptic curves.

Definition 2.7. *Let (E, p, e) be an elliptic curve over S and (E', p', e') an elliptic curve over S' . A **morphism** of elliptic curves*

$$(f, g): (E, p, e) \rightarrow (E', p', e')$$

consists of morphisms of schemes $f: S \rightarrow S'$ and $g: E \rightarrow E'$ which satisfy $g \circ e = e' \circ f$ and make the diagram

$$\begin{array}{ccc} E & \xrightarrow{g} & E' \\ \downarrow p & & \downarrow p' \\ S & \xrightarrow{f} & S' \end{array}$$

cartesian.

We define composition and identity morphisms for elliptic curves componentwise.

Proposition 2.8 ([Ols16], Section 13.1.4). *Let (E, p, e) be an elliptic curve over S and (E', p', e') an elliptic curve over S' . Let $\mathcal{J} \subset \mathcal{O}_E$ and $\mathcal{J}' \subset \mathcal{O}_{E'}$ be the ideal sheaves of e and e' , respectively. Moreover, let $(f, g): (E, p, e) \rightarrow (E', p', e')$ be a morphism of elliptic curves as above. Then:*

- (1) $g^* \mathcal{J}'^{\otimes r} \cong \mathcal{J}^{\otimes r}$ for any $r \in \mathbb{Z}$, and these isomorphisms are compatible with composition of morphisms.
- (2) \mathcal{J}^{-1} is an ample line bundle over S .

Proof. First, we observe that e and e' are actually closed immersions by Lemma 2.4 so that it makes sense to talk about corresponding ideal sheaf.

- (1) This follows from Proposition 2.6 together with the fact [KM85, Section 1.1.2] that relative effective Cartier divisors behave well under pullbacks

and finally the observation that in the commutative diagram

$$(2.1) \quad \begin{array}{ccc} S & \xrightarrow{f} & S' \\ \downarrow e & & \downarrow e' \\ E & \xrightarrow{g} & E' \\ \downarrow p & & \downarrow p' \\ S & \xrightarrow{f} & S' \end{array}$$

the outer and the lower square are cartesian, thus so is the upper square.

(2) By Proposition 2.6, \mathcal{J} is an invertible line bundle.

To check that \mathcal{J}^{-1} is ample, we use the criterion of Corollaire 9.6.5 from [Gro67], saying that it is enough to check that \mathcal{J}^{-1} is ample in every fiber. Moreover, by [Sta17, Tag 0D2P], it is enough to consider the geometric points. By the first part, we can identify $\mathcal{J}_{\mathrm{Spec}(k)}^{-1}$ with $\mathcal{O}_{E_{\mathrm{Spec}(k)}}(e_{\mathrm{Spec}(k)})$. Thus, we can use Example IV.3.3.3 of [Har77] to see that $\mathcal{J}_{\mathrm{Spec}(k)}^{-3} \cong \mathcal{O}_{E_{\mathrm{Spec}(k)}}(3e_{\mathrm{Spec}(k)})$ is very ample. \square

3. MODULI STACK OF ELLIPTIC CURVES

The aim of this section is to define the moduli stack of elliptic curves and to prove that it is actually a stack in the fpqc topology on $\mathrm{Sch}/\mathrm{Spec}\mathbb{Z}$. The material of this section is well-known to the experts. We would like to provide some details for the convenience of the reader. Large part of the following are taken from [Ols16], Chapter 13. More background on fpqc topology and stacks can be found in [Vis05].

Definition 3.1 ([Ols16], Chapter 13). *The moduli stack of elliptic curves \mathcal{M}_{ell} over $\mathrm{Spec}\mathbb{Z}$ is the category over $\mathrm{Sch}/\mathrm{Spec}\mathbb{Z}$ with:*

- *objects $(S, (E, p, e))$, where S is a scheme and (E, p, e) is an elliptic curve over S ,*
- *morphisms are morphisms of elliptic curves.*

The functor $\mathcal{M}_{ell} \rightarrow \mathrm{Sch}/\mathrm{Spec}\mathbb{Z}$ is given by $(S, (E, p, e)) \mapsto S$ on objects and $(f, g) \mapsto f$ on morphisms.

It is easy to see that \mathcal{M}_{ell} is a category fibered in groupoids over $\mathrm{Sch}/\mathrm{Spec}\mathbb{Z}$. Our goal is now to prove that \mathcal{M}_{ell} is a stack in the fpqc (and thus in particular in the étale) topology on $\mathrm{Sch}/\mathrm{Spec}\mathbb{Z}$.

Theorem 3.2 ([Ols16], Chapter 13). *\mathcal{M}_{ell} is a stack in the fpqc topology on $\mathrm{Sch}/\mathrm{Spec}\mathbb{Z}$.*

We will imitate the proof of Theorem 4.38 in [Vis05].

Thus, we will show first that \mathcal{M}_{ell} is an fpqc prestack. Recall that $\mathcal{M}_{ell}(U)$ for a scheme U denotes the fiber of $\mathcal{M}_{ell} \rightarrow \mathrm{Sch}/\mathrm{Spec}\mathbb{Z}$ over U (and identity of U). Recall moreover that given an fpqc covering $\{U_i \xrightarrow{\sigma_i} U\}_{i \in I}$, the category of descent data (cf. [Vis05], Definition 4.2) $\mathcal{M}_{ell}(\{U_i \xrightarrow{\sigma_i} U\})$ is defined as follows:

- An object of $\mathcal{M}_{ell}(\{U_i \xrightarrow{\sigma_i} U\})$ consists of an elliptic curve $(U_i, (E_i, p_i, e_i))$ for every $i \in I$, together with isomorphisms of elliptic curves

$$\varphi_{ij}: (U_i \times_U U_j, (\mathrm{pr}_2^* E_j, \mathrm{pr}_2^*(p_j), \mathrm{pr}_2^*(e_j))) \rightarrow (U_i \times_U U_j, (\mathrm{pr}_1^* E_i, \mathrm{pr}_1^*(p_i), \mathrm{pr}_1^*(e_i)))$$

for all $i, j \in I$, and these isomorphisms are required to satisfy a cocycle condition.

- A morphism

$$(U_i, (E_i, p_i, e_i), \varphi_{ij}) \rightarrow (U_i, (E'_i, p'_i, e'_i), \varphi'_{ij})$$

consists of a morphism of elliptic curves $(\text{id}, g_i): (E_i, p_i, e_i) \rightarrow (E'_i, p'_i, e'_i)$ for each $i \in I$ such that $\varphi'_{ij} \circ \text{pr}_2^*(\text{id}, g_j) = \text{pr}_1^*(\text{id}, g_i) \circ \varphi_{ij}$.

Composition and identities are defined again componentwise.

Lemma 3.3. \mathcal{M}_{ell} is a prestack in the fpqc topology on $\text{Sch}/\text{Spec } \mathbb{Z}$, i.e., the functor

$$\mathcal{M}_{ell}(S) \xrightarrow{(\sigma_i^*)} \mathcal{M}_{ell}(\{U_i \xrightarrow{\sigma_i} S\})$$

induced by pullbacks is fully faithful for any fpqc covering $\{U_i \xrightarrow{\sigma_i} S\}_{i \in I}$.

Proof. We will check faithfulness first. Let (E, p, e) and (E', p', e') be two elliptic curves over S and let $(\text{id}, f), (\text{id}, g): (S, (E, p, e)) \rightarrow (S, (E', p', e'))$ be two morphisms in \mathcal{M}_{ell} which agree on the covering $\{U_i \rightarrow S\}$. More precisely, we recall that we have chosen pullbacks to define functors $\sigma_i^*: \mathcal{M}_{ell}(S) \rightarrow \mathcal{M}_{ell}(U_i)$ and require $\sigma_i^*(f) = \sigma_i^*(g)$ for all $i \in I$. Note that $\{\sigma_i^* E \xrightarrow{\tau_i} E\}$ is an fpqc covering again. Thus, the two maps $f, g: E \rightarrow E'$ are equal since they are equal composed with $\sigma_i^* E \xrightarrow{\tau_i} E$ (here, we are using that the fpqc site is subcanonical, as shown e.g. in [Vis05], Theorem 2.55).

Next, we want to show that our functor is full. Let (E, p, e) and (E', p', e') be two elliptic curves over S again, and assume that with the same choice of σ_i^* , we are given morphisms

$$\begin{aligned} \beta_i: ((\sigma_i^* E, \sigma_i^* p, (\text{id}, e \circ \sigma_i)), \alpha_{\text{pr}_1, \sigma_i}^{-1}(E) \circ \alpha_{\text{pr}_2, \sigma_j}(E)) \rightarrow \\ ((\sigma_i^* E', \sigma_i^* p', (\text{id}, e' \circ \sigma_i)), \alpha_{\text{pr}_1, \sigma_i}^{-1}(E') \circ \alpha_{\text{pr}_2, \sigma_j}(E')), \end{aligned}$$

compatible with the transition maps, where $\alpha_{f,g}(X): f^* g^* X \rightarrow (gf)^* X$ is the canonical isomorphism. It is easy to check that the pullback $\text{pr}_1^* \sigma_i^* E$ is canonically isomorphic to $\sigma_i^* E \times_E \sigma_j^* E$, and thus also that β_i and β_j coincide when pulled back to this fiber product and composed with the corresponding $\alpha_{?,?}$'s. This implies that (using again that $\{\sigma_i^* E \xrightarrow{\tau_i} E\}$ is an fpqc covering and that E' is a sheaf on the fpqc site) there is a unique map $\beta: E \rightarrow E'$ so that $\beta \circ \tau_i$ coincides with the composition $\sigma_i^* E \xrightarrow{\beta_i} \sigma_i^* E' \xrightarrow{\tau'_i} E'$. So we have a commutative diagram

$$\begin{array}{ccccc} \sigma_i^* E & \xrightarrow{\beta_i} & \sigma_i^* E' & \xrightarrow{\sigma_i^*(p')} & U_i \\ \downarrow \tau_i & & \downarrow \tau'_i & & \downarrow \sigma_i \\ E & \xrightarrow{\beta} & E' & \xrightarrow{p'} & S. \end{array}$$

For this map to make (id, β) into a morphism of elliptic curves, we need to check $p' \circ \beta = p$ and $\beta \circ e = e'$. It is enough to check this fpqc-locally.

$$\begin{aligned} p' \beta \tau_i &= p' \tau'_i \beta_i && \text{(definition of } \beta) \\ &= \sigma_i \circ \sigma_i^*(p') \circ \beta_i && \text{(pullback diagram defining } \sigma_i^* E') \\ &= \sigma_i \circ \sigma_i^*(p) && \text{(definition of } \beta_i) \\ &= p \circ \tau_i && \text{(pullback diagram defining } \sigma_i^* E). \end{aligned}$$

Similarly, one can check that $\sigma_i^*(\beta) = \beta_i$ using the universal property of pullbacks.

Similarly, we have

$$\begin{aligned}
\beta e \sigma_i &= \beta \circ \tau_i(\text{id}, e \circ \sigma_i) && \text{(definition of } (\text{id}, e \circ \sigma_i)) \\
&= \tau'_i \circ \beta_i \circ (\text{id}, e \circ \sigma_i) && \text{(definition of } \beta) \\
&= \tau'_i \circ (\text{id}, e' \circ \sigma_i) && \text{(definition of } \beta_i) \\
&= e' \circ \sigma_i && \text{(definition of } (\text{id}, e' \circ \sigma_i)).
\end{aligned}$$

Altogether, this proves the fullness and thus we have shown that \mathcal{M}_{ell} is a prestack in the fpqc topology. \square

We will use Lemma 4.25 of [Vis05], stating that to prove Theorem 3.2 it is enough to check the following two points:

- (1) \mathcal{M}_{ell} is a stack in the Zariski topology.
- (2) For any flat surjective morphism of affine schemes $V \rightarrow U$, the functor $\mathcal{M}_{ell}(U) \rightarrow \mathcal{M}_{ell}(V \rightarrow U)$ is an equivalence of categories.

We have already shown that \mathcal{M}_{ell} is an fpqc prestack, so in particular a Zariski prestack. Next, we want to show the “gluing” property for elliptic curves for Zariski coverings.

Lemma 3.4. *\mathcal{M}_{ell} is a stack in the Zariski topology.*

Proof. Let S be any scheme and let $\{U_i \xrightarrow{\sigma_i} S\}_{i \in I}$ be a Zariski covering of S . In order to show that the functor given by chosen pullbacks

$$\mathcal{M}_{ell}(S) \rightarrow \mathcal{M}_{ell}(\{U_i \rightarrow S\})$$

is an equivalence of categories, by Lemma 3.3 we only need to check that it is essentially surjective.

We will use that morphisms of schemes form a stack in Zariski topology, which we will denote by Mor . The stack property is explained in [Vis05], Section 4.3. Note that this category is fibered just in categories and not in groupoids.

Thus, assume that we are given an object with descent data: A family of $(E_i, p_i, e_i) \in \mathcal{M}_{ell}(U_i)$ together with isomorphisms of elliptic curves $\varphi_{ij}: \text{pr}_2^* E_j \rightarrow \text{pr}_1^* E_i$ satisfying the cocycle condition (taking into account the composition isomorphisms $\alpha_{\gamma, \gamma'}$). We need to construct an elliptic curve E over S with $\sigma_i^* E \cong E_i$ (as elliptic curves, compatible with transition maps). Since Mor is a Zariski stack, we know that we obtain a map $p: E \rightarrow S$ so that $\sigma_i^*(E)$ is isomorphic to E_i for all $i \in I$, and these isomorphisms are compatible with φ_{ij} and with p_i and $\sigma_i^*(p)$, respectively. It is proper and smooth since these properties can be checked Zariski locally.

For the section, consider the compositions $U_i \xrightarrow{e_i} E_i \cong \sigma_i^* E \rightarrow E$. These coincide on intersections, so define a map $e: S \rightarrow E$ so that $e \sigma_i = e_i$. We need to check $pe = \text{id}_S$. Again, we can do this Zariski locally, and there it is implied by the commutativity of the following diagram:

$$\begin{array}{ccccccc}
U_i & \xrightarrow{e_i} & E_i & \xrightarrow{\cong} & \sigma_i^* E & \xrightarrow{\tau_i} & E \\
& \searrow & \searrow & \searrow & \downarrow & & \downarrow \\
& & & & U_i & \xrightarrow{\sigma_i} & S \\
& & & & \downarrow & & \\
& & & & \sigma_i^*(p) & & p
\end{array}$$

Next, we need to check that the pullbacks of (E, e) to geometric fibers are elliptic curves again. Note that since $\{U_i \rightarrow S\}$ is a Zariski covering, any map $\text{Spec}(\bar{k}) \rightarrow S$ factors through some U_i , so that the pullback of E to $\text{Spec}(\bar{k})$ is isomorphic to the pullback of E_i to $\text{Spec}(\bar{k})$, and also the induced sections coming from e and e_i coincide. Thus, the geometric fibers of p are elliptic curves since so are the geometric fibers of p_i by assumption.

This completes the proof. \square

The main difficulty now is the fact that “gluing” of schemes given on an fpqc (in fact, even on an étale) covering does not yield a scheme again. In the étale case, we could in general obtain an algebraic space in this way. So we need some care to see that in the case of elliptic curves (which goes back to the case of polarized schemes), the gluing does work out. Note that this would not work for genus 1 curves without section, cf. [Vis05], Example 4.39.

The ideal sheaf \mathcal{J} which we discussed in Proposition 2.8 will make every elliptic curve into a polarized scheme. We will use this fact in combination with the following theorem, which is a slightly stronger statement than Proposition 4.4.12 of [Ols16] and of [Sta17, Tag 0D40], and actually proven in the proof of Theorem 4.38 of [Vis05].

Proposition 3.5 (cf. [Ols16], Proposition 4.4.12 and Theorem 4.38 of [Vis05]). *Let $\mathcal{P}ol$ be the category whose objects are pairs $(f: X \rightarrow Y, \mathcal{L})$, where f is proper flat morphism of finite presentation and \mathcal{L} a relatively ample line bundle on X . A morphism*

$$(a, b, \varepsilon): (f: X \rightarrow Y, \mathcal{L}) \rightarrow (f': X' \rightarrow Y', \mathcal{L}')$$

consists of morphisms of schemes $a: X \rightarrow X'$ and $b: Y \rightarrow Y'$ making the diagram

$$\begin{array}{ccc} X & \xrightarrow{a} & X' \\ \downarrow f & & \downarrow f' \\ Y & \xrightarrow{b} & Y' \end{array}$$

cartesian, and $\varepsilon: a^ \mathcal{L} \rightarrow \mathcal{L}'$ isomorphism of sheaves on X' . Composition is defined componentwise (using composition isomorphisms for pullbacks).*

Then $\mathcal{P}ol$ is fibered over $\text{Sch} / \text{Spec } \mathbb{Z}$ via $(f: X \rightarrow Y, \mathcal{L}) \mapsto Y$, and it is a stack in the fpqc topology.

Proof. This is exactly done on pp. 99-103 of [Vis05]. The main point where the assumptions on objects of $\mathcal{P}ol$ are used is for applying Proposition 4.37 of [Vis05], which is a version of cohomology and base change without noetherianity assumptions. \square

Proof of Theorem 3.2. Using Lemma 4.25 of [Vis05], we are left to show that for a flat surjective morphism of affine schemes $\varphi: V = \text{Spec}(B) \rightarrow U = \text{Spec}(A)$ (so in particular an fpqc covering), the functor $\mathcal{M}_{ell}(U) \rightarrow \mathcal{M}_{ell}(V \rightarrow U)$ is an equivalence of categories. By Lemma 3.3 again, we only need to check that it is essentially surjective. This is very similar to Theorem 4.38 in [Vis05] and to Theorems 4.4.13 and 4.4.10 in [Ols16].

Let an elliptic curve $p: E \rightarrow V$ with section $e: V \rightarrow E$ be given, together with descent data, i.e. an isomorphism $\beta: \text{pr}_2^* E \rightarrow \text{pr}_1^* E$ of elliptic curves over $V \times_U V$ satisfying the appropriate cocycle condition. Observe that Proposition 2.8

implies that we have a morphism of fibered categories over $\text{Sch}/\text{Spec } \mathbb{Z}$ from \mathcal{M}_{ell} to $\mathcal{P}ol$ given by $(S', (E', p', e')) \mapsto (p': E' \rightarrow S', \mathcal{J}'^{-1})$ where \mathcal{J}' is the ideal sheaf corresponding to e' (see Proposition 2.8 for details). This implies in particular that we have a 2-commutative diagram of categories

$$\begin{array}{ccc} \mathcal{M}_{ell}(U) & \longrightarrow & \mathcal{P}ol(U) \\ \downarrow & & \downarrow \\ \mathcal{M}_{ell}(V \rightarrow U) & \longrightarrow & \mathcal{P}ol(V \rightarrow U). \end{array}$$

Since in Proposition 3.5, we discussed $\mathcal{P}ol$ to be an fpqc stack, we conclude there is a scheme X and a flat proper morphism of finite presentation $q: X \rightarrow U$ and an isomorphism $\sigma: \varphi^* X \rightarrow E$ of schemes over V , satisfying certain compatibilities. (Actually, we also get a relatively ample invertible sheaf \mathcal{L} on X and an isomorphism $\sigma^* \pi^* \mathcal{L} \cong \mathcal{J}^{-1}$ of \mathcal{O}_E -modules, where π denotes the projection $\varphi^* X \rightarrow X$, but we will not use this.) In particular, this means that σ is an isomorphism of descent data, and more explicitly, we have a commutative diagram

$$(3.1) \quad \begin{array}{ccc} \text{pr}_2^* \varphi^* X & \xrightarrow{\text{pr}_2^* \sigma} & \text{pr}_2^* E \\ \alpha_{?,?} \downarrow & & \downarrow \beta \\ (\varphi \circ \text{pr}_2)^* X & & \\ \alpha_{?,?}^{-1} \downarrow & & \downarrow \text{pr}_1^* \sigma \\ \text{pr}_1^* \varphi^* X & \xrightarrow{\text{pr}_1^* \sigma} & \text{pr}_1^* E. \end{array}$$

The last piece of data we need to construct is a section for q . To do so, we will use that X is a sheaf in the fpqc topology (as shown in [Vis05], Theorem 2.55). Observe that we have a map $V \rightarrow X$, defined as

$$V \xrightarrow{e} E \xrightarrow{\sigma^{-1}} \varphi^* X \xrightarrow{\pi} X.$$

We have to show that precomposing this map with either projection $\text{pr}_i: V \times_U V \rightarrow V$ yields the same result. Since β is an isomorphism of elliptic curves, it satisfies $\beta \circ \text{pr}_2^*(e) = \text{pr}_1^*(e)$. Thus we have

$$\begin{aligned} \pi \circ \sigma^{-1} \circ e \circ \text{pr}_1 &= \pi \circ \sigma^{-1} \circ \text{pr}_1 \circ \text{pr}_1^*(e) && \text{(as in (2.1))} \\ &= \pi \circ \sigma^{-1} \circ \text{pr}_1 \circ \beta \circ \text{pr}_2^*(e) && \text{(definition of } \beta) \\ &= \pi \circ \text{pr}_1 \circ \text{pr}_1^*(\sigma)^{-1} \circ \beta \circ \text{pr}_2^*(e) && \text{(definition of } \text{pr}_1^*(\sigma)) \\ &= \pi \circ \text{pr}_1 \circ \alpha_{?,?}^{-1} \circ \alpha_{?,?} \circ \text{pr}_2^*(\sigma)^{-1} \circ \text{pr}_2^*(e) && \text{(commutativity of (3.1))} \\ &= \pi \circ \text{pr}_2 \circ \text{pr}_2^*(\sigma)^{-1} \circ \text{pr}_2^*(e) && \text{(definition of } \alpha_{?,?}(e)) \\ &= \pi \circ \sigma^{-1} \circ \text{pr}_2 \circ \text{pr}_2^*(e) && \text{(definition of } \text{pr}_2^*(\sigma)) \\ &= \pi \circ \sigma^{-1} \circ e \circ \text{pr}_2 && \text{(as in (2.1)).} \end{aligned}$$

Thus, we obtain a map $j: U \rightarrow X$ so that $j \circ \varphi = \pi \circ \sigma^{-1} \circ e$. We still need to show that $qj = \text{id}_U$. Since U is a sheaf in fpqc topology, we only need to check $qj\varphi = \varphi$, which is straightforward.

Next, we conclude by [Gro67], Corollaire 17.7.3, that $q: X \rightarrow U$ is actually smooth since its pullback along the faithfully flat and quasi-compact map φ is smooth.

We are left to show that for any algebraically closed field k and any morphism $\text{Spec}(k) \rightarrow U$, the pullback (X_k, j_k) of (X, j) is an elliptic curve over k . Recall that $U = \text{Spec}(A), V = \text{Spec}(B)$ were assumed to be affine. Then we know that $\text{Spec}(k) \times_U V \cong \text{Spec}(B \otimes_A k)$. Note that $B \otimes_A k$ is not the 0-ring since the map $A \rightarrow B$ was assumed to be faithfully flat, thus it has some maximal ideal \mathfrak{m} . Let L be the algebraic closure of the quotient field $B \otimes_A k/\mathfrak{m}$; then we have the commutative diagram

$$\begin{array}{ccc} \text{Spec}(L) & \longrightarrow & V \\ \downarrow & & \downarrow \\ \text{Spec}(k) & \longrightarrow & U. \end{array}$$

Let E_L be the pullback of E along $\text{Spec}(L) \rightarrow V$. Note that then the diagram

$$\begin{array}{ccc} E_L & \xrightarrow{p_L} & \text{Spec}(L) \\ \downarrow g & & \downarrow \tilde{g} \\ X_k & \xrightarrow{q_k} & \text{Spec}(k) \end{array}$$

is cartesian, which can be (roughly) seen as follows:

$$\begin{aligned} E_L &= E \times_V \text{Spec}(L) \cong (X \times_U V) \times_V \text{Spec}(L) \\ &\cong X \times_U \text{Spec}(L) \cong (X \times_U \text{Spec}(k)) \times_{\text{Spec}(k)} \text{Spec}(L) \\ &= X_k \times_{\text{Spec}(k)} \text{Spec}(L). \end{aligned}$$

It is easy to check that also the pullback of the section $j_k: \text{Spec}(k) \rightarrow X_k$ is the section e_L , and recall we assumed that (E_L, e_L) is an elliptic curve over L . Thus, by Lemma 2.2, we conclude that (X_k, j_k) is an elliptic curve over k .

All in all, this finishes the proof that the tuple (X, q, j) constructed above is an elliptic curve over U whose pullback is up to isomorphism given by the descent data we started with. This shows that \mathcal{M}_{ell} is indeed a stack in fpqc topology. \square

4. WEIERSTRASS EQUATIONS

We have established in the previous section the stack property of the moduli stack of elliptic curves. Our next objective is to show that it is an algebraic stack. (In fact, it is even a Deligne-Mumford stack, but proving this requires more effort and will be done at a later point.) Recall that we need to show that the diagonal of \mathcal{M}_{ell} is representable and that it possesses a smooth atlas. The key ingredient will be the fact that any elliptic curve is Zariski locally given by a Weierstraß equation. These statements are well-known and can be found in e.g. [KM85] and [Ols16].

Lemma 4.1. *Let R be an arbitrary ring, and let f_1, \dots, f_n be homogeneous polynomials in $R[T_1, \dots, T_k]$ with $n \leq k - 1$. Then*

$$X = \text{Proj}(R[T_1, \dots, T_k]/(f_1, \dots, f_n))$$

is smooth over $\mathrm{Spec}(R)$ of relative dimension $k - 1 - n$ if and only if for any ring homomorphism into a field $\alpha: R \rightarrow K$, the scheme

$$X_K = \mathrm{Proj}(K[T_1, \dots, T_k]/(\alpha(f_1), \dots, \alpha(f_n)))$$

is smooth over K of relative dimension $k - 1 - n$.

Proof. If $X \rightarrow \mathrm{Spec}(R)$ is smooth of relative dimension $k - 1 - n$, so is any pullback $X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(K) \rightarrow \mathrm{Spec}(K)$. (Here, we are using [Sta17, Tag 01N2].)

For the converse, it is enough to show that $X \rightarrow \mathrm{Spec}(R)$ is smooth of relative dimension $k - 1 - n$ when restricted to each of the $D_+(T_i)$. Thus, we need to check whether the map

$$R \rightarrow R[T_1, \dots, \widehat{T}_i, \dots, T_k]/(f_1(T_i = 1), \dots, f_n(T_i = 1))$$

is smooth of relative dimension $k - 1 - n$. We already know that the restriction to $D_+(T_i) \subset X_K$ is smooth of the same relative dimension for any $\alpha: R \rightarrow K$, so that

$$K \rightarrow K[T_1, \dots, \widehat{T}_i, \dots, T_k]/(\alpha(f_1(T_i = 1)), \dots, \alpha(f_n(T_i = 1)))$$

is smooth of same relative dimension and thus also standard smooth [Sta17, Tag 00TA]. This means that the matrix

$$\left(\frac{\partial \alpha(f_r(T_i = 1))}{\partial T_s} \right)_{1 \leq r \leq n, 1 \leq s \leq k, s \neq i}$$

has rank n . By Definition 6.18 of [GW10], this is enough to see smoothness. \square

Remark 4.2. Note that a priori, Definition 6.18 of [GW10] and [Sta17, Tag 01V5] do not coincide. They can be shown to be equivalent.

Lemma 4.3. Let R be any ring. Then the closed subscheme of \mathbb{P}_R^2 cut out by the Weierstraß equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

is an elliptic curve over R if $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ is invertible in R , where

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Moreover, if this equation cuts out a smooth scheme over $\mathrm{Spec}(R)$, then Δ is invertible in R .

Proof. First, recall that we mean

$$E = \mathrm{Proj}(R[x, y, z]/(y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3))$$

by “cut out by this equation”. This comes with a natural map $E \rightarrow \mathrm{Spec}(R)$ as in [Sta17, Tag 01ME]. A section to $D_+(y)$ is given by

$$(4.1) \quad \begin{aligned} R[x, z]/(z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3) &\rightarrow R \\ x &\mapsto 0, \\ z &\mapsto 0. \end{aligned}$$

By [Sta17, Tag 01NH], the map $\mathbb{P}_R^2 \rightarrow \mathrm{Spec}(R)$ is proper (being of finite type is obvious here), and so is the closed immersion $E \rightarrow \mathbb{P}_R^2$ ([Sta17, Tag 01N0] and [Sta17, Tag 01W5]), thus the map $E \rightarrow \mathrm{Spec}(R)$ is proper.

For equivalence of smoothness and invertibility of Δ , we use the Lemma 4.1. Note that using faithfully flat descent, it is enough to consider algebraically closed fields. This is then shown in Proposition III.1.4(a) of [Sil92]. Moreover, Proposition III.3.1 of [Sil92] shows that the geometric fibers are elliptic curves. This implies the claim. \square

To be able to produce certain embedding into projective spaces later on, we will prove the following lemma.

Lemma 4.4. *Let $f: X \rightarrow Y$ be a morphism of proper S -schemes such that for every geometric point $\mathrm{Spec}(k) \rightarrow S$, the pullback $f_k: X_k \rightarrow Y_k$ is a closed immersion. Then f is a closed immersion.*

Proof. First, by [Sta17, Tag 01W6] we conclude that f itself is proper. Now we want to apply [Gro67], Corollaire 18.12.6, so we only need to show that for every $y \in Y$ with residue field $\kappa(y)$, the pullback map

$$X_{\kappa(y)} := X \times_Y \mathrm{Spec} \kappa(y) \rightarrow \mathrm{Spec} \kappa(y)$$

is radicial (or equivalently, universally injective [Sta17, Tag 01S4]) and geometrically reduced. Let $s = f(y)$. The map $Y \rightarrow S$ induces a map of residue fields $\kappa(s) \rightarrow \kappa(y)$ and a commutative diagram

$$\begin{array}{ccc} \mathrm{Spec} \kappa(y) & \longrightarrow & Y \\ \downarrow & & \downarrow \\ \mathrm{Spec} \kappa(s) & \longrightarrow & S, \end{array}$$

so that we also obtain a map $\mathrm{Spec} \kappa(y) \rightarrow Y_{\kappa(s)} := Y \times_S \mathrm{Spec} \kappa(s)$ compatible with the above morphisms. In particular, the map $\mathrm{Spec} \kappa(y) \rightarrow Y$ factors through $Y_{\kappa(s)} \rightarrow Y$, and a standard pullback manipulation yields shows that all the squares below are pullback squares:

$$\begin{array}{ccccc} X_{\kappa(y)} & \longrightarrow & X_{\kappa(s)} & \longrightarrow & X \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec} \kappa(y) & \longrightarrow & Y_{\kappa(s)} & \longrightarrow & Y. \end{array}$$

Moreover, observe that $\kappa(y)$ is indeed the residue field $\kappa(y')$ of its image point y' in $Y_{\kappa(s)}$ since the morphism $Y_{\kappa(s)} \rightarrow Y$ by construction has the property $\kappa(y) \subset \kappa(y')$. So using [Gro67], Corollaire 18.12.6 once again, we conclude that it is enough to show that $X_{\kappa(s)} \rightarrow Y_{\kappa(s)}$ is a closed immersion. We already know by assumption that $X_{\overline{\kappa(s)}} \rightarrow Y_{\overline{\kappa(s)}}$ is a closed immersion, with $\overline{\kappa(s)}$ the algebraic closure of $\kappa(s)$. Since $\mathrm{Spec} \overline{\kappa(s)} \rightarrow \mathrm{Spec} \kappa(s)$ is fpqc, so is $Y_{\overline{\kappa(s)}} \rightarrow Y_{\kappa(s)}$, and thus by fpqc descent (e.g. [Vis05], Proposition 1.15(xii)), the map $X_{\kappa(s)} \rightarrow Y_{\kappa(s)}$ is a closed immersion. This completes the proof. \square

Our next objective is to provide local Weierstraß equations for all elliptic curves. We will follow [Ols16], Section 13.1.6, but the statement can be found in many other sources.

Theorem 4.5 ([Ols16], Section 13.1.6). *Zariski locally, any elliptic curve is given by a Weierstraß form as in Lemma 4.3.*

Proof. By Lemma 2.5, it is enough to show that any elliptic curve $(E, p: E \rightarrow \text{Spec}(R), e)$ for a noetherian ring R is Zariski locally cut out by Weierstraß equations. Recall that we have shown in Proposition 2.6 and Proposition 2.8 that the ideal sheaf \mathcal{I} of the closed immersion $e: \text{Spec}(R) \rightarrow E$ is an invertible line bundle, and also that the formation of $\mathcal{L} := \mathcal{I}^{-1}$ is compatible with base change. By definition, we had an exact sequence

$$0 \rightarrow \mathcal{I} \rightarrow \mathcal{O}_E \rightarrow e_* \mathcal{O}_{\text{Spec}(R)} \rightarrow 0,$$

which yields for any $n \geq 0$ the short exact sequence

$$0 \rightarrow \mathcal{L}^{\otimes n} \rightarrow \mathcal{L}^{\otimes(n+1)} \rightarrow e_* \mathcal{O}_{\text{Spec}(R)} \otimes \mathcal{L}^{\otimes(n+1)} \rightarrow 0.$$

Next, we want to show that $p_*(\mathcal{L}^{\otimes n})$ is a locally free module of rank n for $n \geq 1$. We will use again the variant of cohomology and base change of [Vis05], Proposition 4.37. To apply it, we need to compute $H^1(E_k, \mathcal{L}_k^{\otimes n})$, and it is enough to do so for algebraically closed k . Using Serre duality (cf. [Har77], Section III.7) and the fact that the dualizing sheaf of an elliptic curve over an algebraically closed field is trivial (e.g. [Har77], Example IV.1.3.6), we conclude

$$H^1(E_k, \mathcal{L}_k^{\otimes n}) \cong H^0(E_k, \mathcal{L}_k^{\otimes(-n)}).$$

As in the proof of Proposition 2.8, we can identify $\mathcal{L}_k \cong \mathcal{O}_{E_k}(e_{\text{Spec}(k)})$. Using [Har77], Lemma IV.1.2, we conclude that negative powers of \mathcal{L}_k do not have non-trivial global sections. So we may indeed apply [Vis05], Proposition 4.37 to conclude that $p_*(\mathcal{L}^{\otimes n})$ is a locally free module and its formation commutes with base change. To determine the rank, we use again the pullback to an algebraically closed field k . Riemann-Roch theorem ([Har77], Theorem IV.1.3) immediately implies that there the rank is n , thus so is the rank of $p_*(\mathcal{L}^{\otimes n})$.

Next, we want to show that the quotient of the pushforward map $p_*(\mathcal{L}^{\otimes n}) \rightarrow p_*(\mathcal{L}^{\otimes(n+1)})$ is a locally free module of rank 1. We can choose an affine covering of $\text{Spec}(R)$ trivializing both of these locally free sheaves. For any $\text{Spec}(A)$ in this covering, the quotient corresponds (via global sections) to an A -module M in the exact sequence of the form

$$0 \rightarrow A^n \rightarrow A^{n+1} \rightarrow M \rightarrow 0.$$

Given any A -algebra A' , we pull back to $\text{Spec}(A')$ and obtain an elliptic curve (E', p', e') . We know by Proposition 2.8 that the inverse \mathcal{L}' of the ideal sheaf of e' is precisely the pullback of \mathcal{L} (and same for all its powers). Since the formation of $p_*(\mathcal{L}^{\otimes n})$ commutes with base change, we conclude that the resulting map $A^n \otimes_A A' \rightarrow A^{n+1} \otimes_A A'$ is injective, so that $\text{Tor}_A^1(M, A') = 0$. This is in particular true for all square 0 extensions $A' = A \oplus N$ for any module N , so $\text{Tor}_A^1(M, N) = 0$ for any A -module N . Thus, M is A -flat and finitely generated over A . Since R and thus A are noetherian, we can conclude [Sta17, Tag 00NX] that M is locally free, and then it is necessarily of rank 1.

By possibly restricting further, we may assume $p_*(\mathcal{L}^{\otimes n})$ for $n \in \{1, 2, 3, 6\}$ and also the quotients $p_*(\mathcal{L}^{\otimes 2})/p_*(\mathcal{L}^{\otimes 1})$, $p_*(\mathcal{L}^{\otimes 3})/p_*(\mathcal{L}^{\otimes 2})$ to be trivial over $\text{Spec}(A)$. Moreover, we will use the product structure on $\bigoplus_{n \geq 0} \mathcal{L}^{\otimes n}$ and the fact

that the maps $\mathcal{L}^{\otimes n} \rightarrow \mathcal{L}^{\otimes(n+1)}$ exhibited above are compatible with multiplication. Fixing identifications, we may choose the basis 1 for

$$A \cong \Gamma(\mathrm{Spec}(A), p_*\mathcal{L}) \cong \Gamma(E \times_{\mathrm{Spec}(R)} \mathrm{Spec}(A), \mathcal{L})$$

(coming from $\mathcal{O}_E \rightarrow \mathcal{L}$). Using freeness of the quotients, we can also choose bases 1, x and 1, x, y for the cases $n = 2$ and $n = 3$, respectively. This defines the elements

$$1, x, x^2, x^3, y, xy, y^2 \in \Gamma(\mathrm{Spec}(A), p_*(\mathcal{L}^{\otimes 6})) \cong A^6.$$

Note also that the situation is stable under base change. We will first argue that base change to any algebraically closed field k (and thus to any field, using faithful flatness) of the resulting map $A^7 \xrightarrow{f} A^6$ is surjective. By [Har77], proof of Proposition IV.4.6 (note that the characteristic assumption is not used at this point) and [Sil92], proof of the Proposition III.3.1, we conclude that over k , any relation between the elements above has to be of the form

$$(4.2) \quad \alpha_1 + \alpha_2 x + \alpha_3 y + \alpha_4 x^2 + \alpha_5 xy + \alpha_6 y^2 + \alpha_7 x^3 = 0$$

with $\alpha_6 \alpha_7 \neq 0$, since otherwise every term would have a pole of different order at the point at ∞ . (Note we are using the identification $\mathcal{L}_k \cong \mathcal{O}_{E_k}(e_{\mathrm{Spec}(k)})$ once again.) Over k , we know that the dimension of the kernel is at least one, but the above argument shows also it is precisely 1, since having two such relations would also imply one with $\alpha_6 \alpha_7 = 0$, and this relation is necessarily 0 then. Thus, over k this map is surjective. Using the fact that it is enough to check surjectivity for all localizations at prime ideals and Nakayama's lemma, we conclude that the map $A^7 \rightarrow A^6$ is surjective.

Next, we want to conclude that a Weierstraß relation holds over A . We have a short exact sequence

$$0 \rightarrow \mathrm{Ker}(f) \rightarrow A^7 \xrightarrow{f} A^6 \rightarrow 0,$$

which remains exact after tensoring with any A -algebra since the last term is free. Since we now that the kernel is non-trivial over algebraically closed fields, we conclude that it is non-trivial and we have a relation of the form (4.2). Moreover, since α_6 and α_7 are units after base change to every field, they are units in A . We may immediately divide by α_7 and so assume that $\alpha_7 = 1$.

We want to embed $E_A := E \times_{\mathrm{Spec}(R)} \mathrm{Spec}(A) \rightarrow \mathbb{P}_A^2$ using the map given by the sections $x, y, 1$. This map is a closed immersion if we base-change from A to any algebraically closed field [Har77], Example IV.3.3.3, or [Sil92], Proposition III.3.1. We use Lemma 4.4 to conclude that thus the corresponding map $E \times_{\mathrm{Spec}(R)} \mathrm{Spec}(A) \rightarrow \mathbb{P}_A^2$ is also a closed immersion.

Consider the homogeneous variant of (4.2), namely the polynomial

$$F = \alpha_1 Z^3 + \alpha_2 X Z^2 + \alpha_3 Y Z^2 + \alpha_4 X^2 Z + \alpha_5 X Y Z + \alpha_6 Y^2 Z + X^3 \in A[X, Y, Z].$$

Using the automorphism $Z \mapsto \alpha_6^{-1} Z$ of \mathbb{P}_A^2 , we may assume $\alpha_6 = 1$. Unpacking the construction of the proof of Theorem II.7.1 in [Har77] on the affine parts and keeping track of trivializations of $\mathcal{L}^{\otimes k}$, one can check that the map defined in the sense of the aforementioned theorem by the sections $x, y, 1$ in $\Gamma(E_A, \mathcal{L}^{\otimes 3}) = \Gamma(\mathrm{Spec} A, p_*\mathcal{L}^{\otimes 3})$ factors through the closed subscheme

$$V_+(F) := \mathrm{Proj}(A[X, Y, Z]/(F))$$

of \mathbb{P}_A^2 (cf. [Sta17, Tag 01QP]), and the map to this subscheme is a closed immersion j again. Our goal is to show that the resulting map $E_A \rightarrow V_+(F)$ is an isomorphism of schemes over $\text{Spec } A$.

To do so, we need to show that the corresponding ideal sheaf \mathcal{J} vanishes; recall that it is defined as the kernel

$$0 \rightarrow \mathcal{J} \rightarrow \mathcal{O}_{V_+(F)} \rightarrow j_* \mathcal{O}_{E_A} \rightarrow 0.$$

Once again we exploit that, if we base-change the whole situation to an algebraically closed field k , the pullback \mathcal{J}_k of \mathcal{J} to $V_+(F_k)$ vanishes. Indeed, if we pull back the exact sequence along a morphism $\mathbb{P}_k^2 \rightarrow \mathbb{P}_A^2$ induced by a morphism $\text{Spec } k \rightarrow \text{Spec } A$, the sequence remains exact since $j_* \mathcal{O}_{E_A}$ is flat over $\text{Spec } A$. (We then check the exactness in an affine cover.) Moreover, we can use cohomology and base change for affine maps ([Sta17, Tag 02KG]) to conclude that the pulled back exact sequence is of the form

$$0 \rightarrow \mathcal{J}_k \rightarrow \mathcal{O}_{V_+(F_k)} \rightarrow (j_k)_* \mathcal{O}_{E_k} \rightarrow 0.$$

Since j_k is by construction the closed immersion defined by the sections $x, y, 1$ of $\mathcal{L}_k^{\otimes 3}$ now over k , it is an isomorphism as shown in [Sil92], Proposition 3.1(a). So if we restrict the original exact sequence to standard opens on \mathbb{P}_A^2 , we in each case get a corresponding sequence of A -modules

$$0 \rightarrow J \rightarrow S \rightarrow N \rightarrow 0,$$

where we in addition know that S is a finitely generated A -algebra, thus in particular a noetherian ring. Moreover, after tensoring with k for any ring homomorphism $A \rightarrow k$ to an algebraically closed field k , we have deduced $J \otimes_A k = 0$. Then also $J \otimes_A k = 0$ holds for any ring homomorphism $A \rightarrow k$ into any field k . Now given a ring homomorphism $S \rightarrow K$ to some field K , we obtain by composition with the structure morphism $A \rightarrow S$ a map $A \rightarrow K$, and in particular, the tensor product $J \otimes_S K$ is a quotient of $J \otimes_A K$ and thus 0 itself. This applies in particular to $K = S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ for all prime ideals $\mathfrak{p} \subset S$. Since S is noetherian, we know that J is finitely generated as S -module so we can apply Nakayama's Lemma to conclude $J = 0$.

So we have shown that we obtain an isomorphism over $\text{Spec } A$ from E_A to $V_+(F)$. In particular, by the second statement of Lemma 4.3, we know that the discriminant Δ of the Weierstraß equation (4.2) (or its homogeneous version) is invertible in A . To make the isomorphism into an isomorphism of elliptic curves, we need it to respect the sections. Recall that the section of $V_+(F)$ is given by “[0 : 1 : 0]”, meaning a map from $\text{Spec}(A)$ to $D_+(Y) \subset V_+(F)$ given via

$$\begin{aligned} A[X, Z]/(F(Y=1)) &\rightarrow A \\ X &\mapsto 0, \\ Z &\mapsto 0. \end{aligned}$$

We want to show that for any point $\mathfrak{p} \in \text{Spec } A$, the stalks of the sections x and 1 lie in $\mathfrak{m}_{e(\mathfrak{p})} \mathcal{L}_{e(\mathfrak{p})}^{\otimes 3}$. Since $x, y, 1$ are a basis of global sections of $\mathcal{L}^{\otimes 3}$, we then may conclude that

$$\text{im}(e) \subseteq (E_A)_y := \{P \in E_A \mid y_P \notin \mathfrak{m}_P \mathcal{L}_P^{\otimes 3}\},$$

Then we will show that on this affine subscheme, the isomorphism $E_A \rightarrow V_+(F)$ sends the section e precisely to “[0 : 1 : 0]” (cf. Theorem II.7.1 and Proposition II.7.2 of [Har77]).

For the behaviour the sections x and 1 , consider once again the exact sequence

$$0 \rightarrow \mathcal{I}_A \rightarrow \mathcal{O}_{E_A} \rightarrow e_*\mathcal{O}_{\mathrm{Spec}(A)} \rightarrow 0.$$

Recall that both $1, x$ are images of global sections of $\mathcal{L}^{\otimes 2}$ under the map

$$\mathcal{L}^{\otimes 2} \cong \mathcal{I} \otimes \mathcal{L}^{\otimes 3} \rightarrow \mathcal{O}_{E_A} \otimes \mathcal{L}^{\otimes 3}.$$

For a point $\mathfrak{p} \in \mathrm{Spec} A$, we have $(e_*\mathcal{O}_{\mathrm{Spec}(A)})_{e(\mathfrak{p})} \cong A_{\mathfrak{p}} \neq 0$, so that $\mathcal{I}_{e(\mathfrak{p})} \subseteq \mathfrak{m}_{e(\mathfrak{p})}$ and thus the section e goes into $(E_A)_y$.

According to Proposition II.7.2, [Har77], the open subscheme $(E_A)_y$ is affine, say $\mathrm{Spec} B$. Then the restriction $\mathcal{I}_A|_{\mathrm{Spec} B}$ corresponds to an ideal $I_B \subset B$ such that $B/I_B \cong A$, and the projection is inducing e . Since the restrictions of $x, 1$ are in $\mathcal{I} \otimes \mathcal{L}^{\otimes 3}$, this implies that sections $\frac{x}{y}, \frac{1}{y}$ correspond to elements of $I_B \subset B$ and thus are mapped to 0 in A , making the diagram of sections commute. This completes the proof. \square

Remark 4.6. *The actual proof that local Weierstrass equations imply that \mathcal{M}_{ell} is algebraic will be added later.*

REFERENCES

- [DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. MR 0337993
- [FGI⁺05] Barbara Fantechi, Lothar Göttsche, Luc Illusie, Steven L. Kleiman, Nitin Nitsure, and Angelo Vistoli, *Fundamental algebraic geometry*, Mathematical Surveys and Monographs, vol. 123, American Mathematical Society, Providence, RI, 2005, Grothendieck’s FGA explained. MR 2222646
- [Gro63] Alexander Grothendieck, *Éléments de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné): III. Étude cohomologique des faisceaux cohérents, seconde partie*, Publications Mathématiques de l’IHÉS **17** (1963), 5–91.
- [Gro67] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas*, Inst. Hautes Études Sci. Publ. Math. (1967), no. 32, 361. MR 0238860
- [GW10] Ulrich Görtz and Torsten Wedhorn, *Algebraic geometry I*, Advanced Lectures in Mathematics, Vieweg + Teubner, Wiesbaden, 2010, Schemes with examples and exercises. MR 2675155
- [Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116)
- [KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR 772569
- [Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications. MR 1917232
- [Ols16] Martin Olsson, *Algebraic spaces and stacks*, American Mathematical Society Colloquium Publications, vol. 62, American Mathematical Society, Providence, RI, 2016. MR 3495343
- [Oss] Brian Osserman, *Notes on cohomology and base change*, <https://www.math.ucdavis.edu/~osserman/math/cohom-base-change.pdf>.
- [Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original. MR 1329092
- [Sta17] The Stacks Project Authors, *Stacks Project*, <http://stacks.math.columbia.edu>, 2017.

- [Vis05] Angelo Vistoli, *Grothendieck topologies, fibered categories and descent theory*, Fundamental algebraic geometry, Math. Surveys Monogr., vol. 123, Amer. Math. Soc., Providence, RI, 2005, pp. 1–104. MR 2223406

MATHEMATICAL INSTITUTE, UNIVERSITY OF BONN, 53115 BONN, GERMANY
E-mail address: `lmeier@math.uni-bonn.de`

MATHEMATICAL INSTITUTE, UNIVERSITY OF BONN, 53115 BONN, GERMANY
E-mail address: `ozornova@math.uni-bonn.de`