Toward a Moduli Stack of Elliptic Curves

April 26, 2024

The following is a very early draft on work in progress by Felix Cherubini and Hugo Moeneclaey.

Contents

1 Weierstrass Curves

1.1 Definition

We assume the characteristic different from 2 and 3.

Definition 1.1.1 Given $a, b : R$, we define the standard cubic curve $E_{a,b}$ as the type of zeros of:

$$Y^2Z - X^3 - aXZ^2 - bZ^3$$

in $\mathbb{P}^2$, pointed by $\infty = [0 : 1 : 0]$.

Definition 1.1.2 Given $a, b : R$ we define the discriminant Δ of $E_{a,b}$ as:

$$\Delta = 4a^3 + 27b^2$$

Definition 1.1.3 A Weierstrass curve is a pointed type $(X, *)$ such that there merely exists $a, b : R$ with $\Delta \neq 0$ and:

$$(X, *) = (E_{a,b}, \infty)$$

Lemma 1.1.4 The standard cubic $E_{a,b}$ curve has an open cover by two affine pieces of the form:

$$\mathrm{Spec}(R[X, Y]/Y^2 - X^3 - aX - b)$$

and:

$$\mathrm{Spec}(R[X, Z])/Z - X^3 - aXZ^2 - bZ^3)$$

Proof As a closed subscheme of $\mathbb{P}^2$, we know that any standard cubic curve is covered by affines given by $x \neq 0$, $y \neq 0$ and $z \neq 0$. But since for any $[x : y : z] : E_{a,b}$ we have that:

$$y^2z - x^3 - axz^2 - bz^3 = 0$$

we have that:

$$x \neq 0 \to (y \neq 0 \vee z \neq 0)$$

so we can conclude. □

1.2 Connectedness and smoothness for standard cubic curves

Lemma 1.2.1 Standard cubic curves are connected.

Proof By lemma 1.4.2 we know that $(E_{a,b} \to R) = R$. Then a map from $E_{a,b}$ to $\mathbf{2}$ gives an idempotent in R, which is 0 or 1 by locality of R, and we conclude from this. □

Lemma 1.2.2 A standard cubic curve $E_{a,b}$ is smooth if and only if $\Delta \neq 0$. Then it is of dimension 1.

Proof Assume $\Delta \neq 0$. Then by lemma 1.1.4 it is enough to show that:

$$\mathrm{Spec}(R[X,Y]/Y^2 - X^3 - aX - b)$$

and:

$$\mathrm{Spec}(R[X,Z])/Z - X^3 - aXZ^2 - bZ^3)$$

are smooth. To do this it is enough to prove that the differential of the defining polynomial is surjective in both cases:

- When $z \neq 0$, we need to prove that for all $x, y : R$ such that:

  $$y^2 = x^3 + ax + b$$

  we have that:

  $$(2y \neq 0) \vee (3x^2 + a \neq 0)$$

  To do this we can assume:

  $$(2y = 0) \wedge (3x^2 + a = 0)$$

  and reach a contradiction by proving $\Delta = 0$.
- When $y \neq 0$, we need to prove that for all $x, z : R$ such that:

  $$z - x^3 - axz^2 - bz^3$$

  we have that:

  $$(3x^2 + az^2 \neq 0) \vee (1 - 2axz - 3bz^2 \neq 0)$$

  To do this we can assume:

  $$(3x^2 + az^2 = 0) \wedge (1 - 2axz - 3bz^2 = 0)$$

  and reach a contradiction directly (done in Macaulay, not sure it is correct...).

Now let us assume given a smooth Weierstrass curve. Since it is connected we know it has constant dimension 1 or 2.

- Dimension 2 is not possible, by fixing $z \neq 0$ and $x = 0$ we would get that $y^2 = b$ implies $y = 0$ for all $y : R$ which is contradictory.
- If it is of dimension 1, then by fixing $z \neq 0$ and $y = 0$, by surjectivity of the differentials we have that $x^3 + ax + b$ is a separable polynomial. Now we assume $\Delta = 0$ and reach a contradiction. We use case distinction on a and b being 0.

  If $a = b = 0$, then we would have x^3 separable, a contradiction.

  If $b \neq 0$ or $a \neq 0$ then both holds because $\Delta = 0$. Then $-\frac{3b}{2a}$ is a double root of $x^3 + ax + b$, which contradicts it being separable. □

Corollary 1.2.3 Weierstrass curves are smooth projective schemes of dimension 1.

1.3 A remark on affine Weierstrass curves

One might be tempted to try to reduce the study of Weierstrass curves to the study of affine schemes of the form:

$$\sum_{x,y:R} y^2 = x^3 + ax + b$$

We indeed have that for any Weierstrass curve $(X, *)$, the scheme $X - \{*\}$ merely is of this form, indeed for any $[x : y : z] : E_{a,b}$ we have that $[x : y : z] \neq [0 : 1 : 0]$ if and only if $z \neq 0$.

However we do not expect this to be part of an equivalence as the affine versions have infinitesimal deformations of the identity that are automorphisms, e.g. for any ϵ such that $\epsilon^2 = 0$ we have an automorphism of $E_{a,b}$ given by:

$$\phi : (x, y) \mapsto (x + y\epsilon, y + \frac{3x^2 + a}{2}\epsilon)$$

$$\phi^{-1} : (x', y') \mapsto (x' - y'\epsilon, y' - \frac{3{x'}^2 + a}{2}\epsilon)$$

1.4 Standard cubic curves have cohomological genus 1

Lemma 1.4.1 Let X be a standard cubic curve and M be a wqc module on X. Then $H^i(X, M) = 0$ when $i > 1$.

Proof By lemma 1.1.4 and Mayer-Vietoris, with the fact that affine schemes have trivial cohomology with coefficent in wqc modules. □

Lemma 1.4.2 Let X be a standard cubic curve. Then we have:

$$H^0(X, R) = R$$

$$H^1(X, R) = R$$

Proof We can assume $X = E_{a,b}$ for some $a, b : R$. By lemma 1.1.4 and Mayer-Vietoris, we have an exact sequence:

$$0 \to H^0(E_{a,b}, R) \to \left(\frac{R[X, Y]}{Y^2 - X^3 - aX - b} \oplus \frac{R[X, Z]}{Z - X^3 - aXZ^2 - bZ^3}\right) \to \left(\frac{R[X, Y]_Y}{Y^2 - X^3 - aX - b}\right) \to H^1(E_{a,b}, R) \to 0$$

where the middle map sends:

$$(P, Q) : \frac{R[X, Y]}{Y^2 - X^3 - aX - b} \oplus \frac{R[X, Z]}{Z - X^3 - aXZ^2 - bZ^3}$$

to:

$$P(X, Y) - Q(X/Y, 1/Y)$$

We have countable basis for the modules involved, so the middle map is the map in:

$$R\langle X^k Y^m \rangle_{0 \le k \le 2, 0 \le m} \oplus R\langle X^k Z^m \rangle_{0 \le k \le 2, 0 \le m} \to R\langle X^k Y^m \rangle_{0 \le k \le 2}$$

defined by sending:

$$X^k Y^m \mapsto X^k Y^m$$

$$X^k Z^m \mapsto -X^k Y^{-k-m}$$

So we are in the situation where we have countably free modules M, N, P with $M, N \subset P$ and we want to find the kernel and cokernel of the map:

$$M \oplus N \to P$$

- The image of this map is precisely the vector space spanned by $X^k Y^m$ when $k \neq 2$ or $m \neq -1$, so its cokernel is isomorphic to the space spanned by $\frac{X^2}{Y}$. This means that:

$$H^1(E_{a,b}, R) = R$$

- Its kernel is the intersection of both subspaces, which is spanned by 1. This means that:

$$H^0(E_{a,b}, R) = R$$

□

From $H^1(X, R) = R$, we should get that Weierstrass curves have genus 1 more or less by definition. We might need the next lemma as well, as we do not know whether smoothness implies flatness.

Lemma 1.4.3 Standard cubic curves are flat. In particular Weierstrass curves are flat.

Proof It is enough to prove that the pieces from lemma 1.1.4 are flat. But both corresponding are free with a countable basis when seen as modules, so they are flat. □

1.5 The j-invariant

Beware, the j-invariant as defined below should not determine the iso class of the elliptic curve.

Definition 1.5.1 Given $E_{a,b}$ a standard Weierstrass curve, we define the the j-invariant by:

$$j = \frac{(4a)^3}{\Delta}$$

Lemma 1.5.2 Consider $E_{a,b}$ and $E_{a',b'}$ two standard Weiestrass curves. If there exists $u : R$ such that $u \neq 0$ and:

$$au^4 = a'$$

$$bu^6 = b'$$

then we have that:

$$\|E_{a,b} = E_{a',b'}\|$$

Proof We just define the map:

$$E_{a,b} \to E_{a',b'}$$

$$[x : y : z] \mapsto [u^2 x : u^3 y : z]$$

and check that it is an isomorphism. □

Remark 1.5.3 We know that $E_{a,b}$ and $E_{a',b'}$ having the same j-invariant does not imply that such u exists, indeed:

- Having the same j-invariant is equivalent to $a^3(b')^2 = (a')^3 b^2$.
- Taking $a = a' = 1$ and $b' = 0$ we would get that for all b such that $b^2 = 0$, we have an invertible u with $bu^6 = 0$, i.e. $b = 0$.

2 Divisors

(This section is preliminary, it is not clear if the notions of divisors presented here are the best we can do synthetically...)

Weil divisors are an important classical tool. They can be used to describe zero and pole orders at closed points or other closed subspaces. In the case of curves over a field in classical algebraic geometry the set of Weil divisors may be defined as the free abelian group over the closed points of the curve.

This is unlikely to be a good way to go synthetically, since it is unclear how to produce actual integers from, say, a rational function which describe its zero or pole orders. As noted by David Jaz Myers [Mye19], it is already not possible to define a degree function with values in the natural numbers and one should therefore pass to upper naturals. We will start by extending Myers' proposed course of action to generalized integers which can serve as "coefficients" for Weil divisors and see how we can assign a Weil divisor to a rational function on a curve.

Following a definition of Weil divisors, we will define Cartier divisors as well and compare the two notions.

2.1 Generalized Integers

The upper naturals are "increasing" sequences of propositions. They can be thought of as upward closed subsets of the naturals and a upper natural is called bounded, if it is inhabited as a subset.

Definition 2.1.1 The *upper naturals* are the following type:

$$\mathbb{N}^{\downarrow} :\equiv (s : \mathbb{N} \to \mathrm{Prop}) \times ((n : \mathbb{N}) \to s(n) \to s(n+1))\,.$$

An upper natural $s : \mathbb{N}^{\downarrow}$ is called *bounded* if there exists an n such that $s(n)$ [1]. We denote the type of bounded upper naturals with $\mathbb{N}^{\downarrow}_b$.

[1] We will suppress the second component of some sigma types here.

As suggested by Myers' we can define addition and multiplication via enriched Day convolution. The latter means, that we view $\mathbb{N}$ as a category given by the order and with monoidal structure given by $+$ or $\cdot$ and monoidally embedd $\mathbb{N}$ into the Prop-valued functors $\mathbb{N} \to \mathrm{Prop}$. This leads to the following definitions:

Definition 2.1.2 Let $s, s' : \mathbb{N}^{\downarrow}$. Then for all $n : \mathbb{N}$ we define:

$$(s + s')(n) :\equiv \exists_{(l,k):\mathbb{N}^2} s(l) \wedge s(k) \wedge (l + k \leq n)$$
$$(s \cdot s')(n) :\equiv \exists_{(l,k):\mathbb{N}^2} s(l) \wedge s(k) \wedge (l \cdot k \leq n)$$

One might expect that this inherits the full structure of a semiring from $\mathbb{N}$, but this is only true if one passes to bounded upper naturals.

Proposition 2.1.3 (a) $+$ and $\cdot$ preserve boundedness of upper naturals.

(b) $\mathbb{N}^{\downarrow}_{b}$ is a commutative semiring with respect to $+$ and $\cdots$.

Proof [Com23] in Cubical/Algebra/CommSemiring/Instances/UpperNat. □

The order $\leq$ on $\mathbb{N}$ is decidable and therefore open. Since $+$ and $\cdot$ only use existence over finite sets and $\wedge$, being pointwise open is preserved by these operations. From this we group complete to get generalized integers, which we do not really know how to denote yet.

Definition 2.1.4 Let $\mathbb{N}^{\downarrow}_{\mathcal{O},b} \subseteq \mathbb{N}^{\downarrow}_{b}$ be the sub-semiring of pointwise *open bounded upper naturals*. The *generalized integers* are the group completion of $\mathbb{N}^{\downarrow}_{\mathcal{O},b}$, which is again a commutative semiring and essentially small. We will denote the generalized integers with $\mathbb{Z}_{\mathcal{O}}$.

2.2 Weil divisors and rational functions

We will now aim at definining Weil divisors and start with rational function on a curve. The definition of curve we will use here is not tested much and therefore preliminary.

Definition 2.2.1 A *curve* is an irreducible, inhabited, projective scheme C which is smooth of dimension 1.

Definition 2.2.2 The type of *rational functions* on a type X is the quotient of

$$\mathcal{K}(X) :\equiv \{(f, U) \mid U \subseteq X \text{ dense open, } f : U \to R\}$$

by the relation $(f, U) \sim (g, V) :\equiv (f_{|U \cap V} = g_{|U \cap V})$.

Lemma 2.2.3 Let X be an irreducible scheme.

(a) For any $(f, U) : \mathcal{K}(X)$, any point $x : X$ and affine open V containing x, there is a $g : V \to R$ such that (f, U) is equivalent to $(f_{D(g)}, D(g))$ (and $D(g) \subseteq U$). In other words: Zariski-locally, (f, U) is of the form $(f_{D(g)}, D(g))$

(b) Any non-zero $f : \mathcal{K}(X)$ has a multiplicative inverse.

Proof Let $(f, U) : \mathcal{K}(X)$ be a rational function.

If we assume a point $x : X$ contained in a chart V, and note $V \cap U = D(g_1, \ldots, g_l)$, we have a dense open $D(g_i)$ containing x.

So (f, U) is equivalent to $(f_{D(g)}, D(g))$ for $g :\equiv g_i$.

Now let f be non-zero. Without loss of generality we can assume that f is non-zero on all of U, since by irreducibility of X, the non-empty subset where $f \neq 0$ is dense open and the intersection of dense opens is dense open. But then f is pointwise invertible on U and therefore invertible. □

Lemma 2.2.4 Let X be an irreducible scheme smooth of dimension 1. If $U \subseteq X$ is dense open and $f : U \to R$ non-zero, then for every point $P : X$, there is a natural k such that $f_{|\mathbb{D}(P,k)} \neq 0$.

Proof (MISSING, Hope this can be done by knowing it for $\mathbb{A}^1$ and moving it around using that a smooth scheme is a manifold... Alternative: Throw out the boundedness everywhere, the Weil divisors will still form an abelian group) □

Definition 2.2.5 Let X be an inrreducible scheme smooth of dimension 1. Then for a non-zero function $f : X \to R$ and $P : X$ we define the zero-order of f at P to be the bounded (by Lemma 2.2.4) open upper natural number

$$n_p(f) :\equiv (k : \mathbb{N}) \mapsto f_{|\mathbb{D}(P,k+1)} \neq 0.$$

Lemma 2.2.6 Let X be an inrreducible scheme smooth of dimension 1 and $f, g : X \to R$. Then

$$n_P(f \cdot g) = n_P(f) + n_P(g)$$

for all $P : X$.

Definition 2.2.7 The type of *Weil divisors* $\mathrm{Div}(C)$ on a curve C is the type of functions $C \to \mathbb{Z}_{\mathcal{O}}$ vanishing on a open dense subset.

Theorem 2.2.8
Let X be an irreducible scheme smooth of dimension 1. Then there is a function $\mathrm{div} : \mathcal{K}(C)^\times \to \mathrm{Div}(C)$ given locally by:

$$\mathrm{div}(\frac{f}{g})(P) = n_P(f) - n_P(g)$$

And we have:

(i) There is a dense open $U \subseteq X$ such that $\mathrm{div}(f) = 0$.

(ii) $\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g)$.

Proof Let $f : \mathcal{K}(X)^\times$. The local requirement defines a unique value $\mathrm{div}(f)$ by multiplicativity of n_P.

(i) This is locally the case since f is of the form $\frac{h}{g}$ and both $D(h)$ and $D(g)$ are dense.

(ii) By multiplicativity of n_P. □

2.3 Cartier divisors

Definition 2.3.1 Let X be a type.

(a) A *Cartier divisor* on X is given by an open cover $U_1, \dots, U_n$ of X together with rational functions $f_i : \mathcal{K}(U_i)^\times$ such that there are (uniquely determined) $\lambda_{ij} : U_i \cap U_j \to R^\times$ with $\lambda_{ij} f_i = f_j$.

(b) Two Cartier divisors $(U_i, f_i)_i$ and $(V_j, g_j)_j$ are equal if there are $\lambda_{ij} : U_i \cap V_j \to R^\times$ such that $\lambda_{ij} f_i = g_j$. This notion of equality defines a set-quotient $\mathrm{Ca}(X)$, the *type of Cartier divisors*.

Lemma 2.3.2 Let X be a type. Let $(U_i, f_i)_i : \mathrm{Ca}(X)$ and $(V_j)_j$ be a an open cover of X. Then $(U_i \cap V_j, f_{i|U_i \cap V_j})_{(i,j)}$ is a Cartier divisor and equal to $(U_i, f_i)_i$.

Proof $(U_i \cap V_j)_{(i,j)}$ is an open cover of X and on $(U_i \cap V_j) \cap U_l$, the $\lambda_{il} : U_i \cap U_l \to R^\times$ shows that the restrictions of f_i and f_l only differ by a unit. □

This means, given a finite list of Cartier divisors, we can assume they are all defined on the same open covering.

Definition 2.3.3 Let X be a type.

(a) For Cartier divisors $(U_i, f_i)_i$ and $(U_i, g_i)_i$ we define the following multiplication:

$$(U_i, f_i)_i \cdot (U_i, g_i)_i :\equiv (U_i, f_i \cdot g_i).$$

$\mathrm{Ca}(X)$ is an abelian group with this multiplication.

(b) A Cartier divisor is called *principal* if it is of the form (X, f) with $f : \mathcal{K}(X)^\times$.

(c) The quotient of the group $\mathrm{Ca}(X)$ by the subgroup of principal divisors is denoted with $\mathrm{CaCl}(X)$ and called the (Cartier) *divisor class group*.

Proposition 2.3.4 Let X be a type and $D :\equiv (U_i, f_i)_i : \mathrm{CaCl}(X)$. We can define a line bundle $\mathcal{L}_D : X \to \mathrm{Lines}$, given by the trivial line bundle on each U_i identified using the λ_{ij}.

Proof We can use a Krauss-lemma as stated in [CCH23][Lemma 1.2.3], since the λ_{ij} satisfy the neccessary cocycle condition. □

(Mapping D to $\mathcal{L}_D$ should be a group homomorphism with respect to the tensor product of line bundles. So the map should also descent to divisor classes.)

(Taking div should give a map from Ca(X) to Weil divisors on X)

(Is it possible, for a point P on a curve, to construct a Cartier divisor D such that the line bundle $\mathcal{L}_D$ is $\mathcal{O}(P)$? Equivalent question: if for a standard smooth of dimenstion 1 affine scheme X and a point P in X, we can construct a function on X which is zero at P and non-zero at all points different from P.)

Index

References

[CCH23] Felix Cherubini, Thierry Coquand, and Matthias Hutzler. *A Foundation for Synthetic Algebraic Geometry*. 2023. arXiv: 2307.00073 [math.AG]. URL: https://www.felix-cherubini.de/iag.pdf (cit. on p. 7).

[Com23] The Agda Community. *Cubical Agda Library*. Version 0.6. 2023. URL: https://github.com/agda/cubical (cit. on p. 5).

[Mye19] David Jaz Myers. *Degrees, Dimensions, and Crispness*. 2019. URL: https://www.felix-cherubini.de/abstracts.html#myers (cit. on p. 4).