THE STRUCTURE OF THE MODULI STACK OF ELLIPTIC CURVES

CHARMAINE SIA

ABSTRACT. We study the multiplication-by-p map on an elliptic curve, which gives a stratification of the moduli stack of elliptic curves into ordinary and supersingular loci, and discuss how this enables one to study the height one and two strata of the moduli stack of formal groups.

Last week, Saul Glasman introduced the notion of a stack and defined the moduli stack of elliptic curves $\mathscr{M}_{\text{ell}}$. In the present talk, we study the multiplication-by-p map on an elliptic curve E, which gives a stratification of $\mathscr{M}_{\text{ell}}$ into ordinary and supersingular loci, and discuss how this enables us to study the height one and two strata of the moduli stack of formal groups.

1. ORDINARY AND SUPERSINGULAR ELLIPTIC CURVES

Let E be an elliptic curve over a field k and let p be a prime number. The multiplication-by-p map on E is a special case of the multiplication-by-n map on an abelian variety A over a field k:

$$\begin{aligned}[n] : A &\to A \\ x &\mapsto \underbrace{x + \cdots + x}_{n}\end{aligned}$$

Let $A[n]$ denote the scheme-theoretic kernel of $[n]$ and $A(\bar{k})[n]$ its geometric points.

Theorem 1. *The multiplication-by-n map on an abelian variety A of dimension g has degree* $\deg[n] = n^{2g}$*; this is equal to the scheme-theoretic order of the finite group scheme* $A[n]$*. Moreover,*

$$A(\bar{k})[n] \cong \begin{cases} (\mathbb{Z}/n\mathbb{Z})^{2g} & \text{if } \operatorname{char} k \nmid n, \\ (\mathbb{Z}/p^m\mathbb{Z})^i & \text{if } n = p^m, \text{ where } \operatorname{char} k = p, \end{cases}$$

where $0 \leq i \leq g$ *and* i *is independent of* m*.*

Since an elliptic curve is an abelian variety of dimension one, the multiplication-by-p map $[p] : E \to E$ has degree p^2 and $E[p]$ has scheme-theoretic order p^2 (although its number of geometric points can vary). Since $E[p]$ is a group scheme, it has either 1, p or p^2 connected components. From Theorem 1, we see that the last case occurs if and only if $\operatorname{char} k \neq p$, while the first two cases occur in characteristic p.

Definition 2. Let k be a field of characteristic p and let E be an elliptic curve defined over k. The elliptic curve E is called *ordinary* if $E[p]$ has p connected components and *supersingular* if $E[p]$ is connected.

More generally, if E is an elliptic curve defined over an arbitrary base scheme S, there is a natural stratification of S into three strata by the number of connected components of the fibers of the map $E[p] \to S$:

- the stratum over which the fibers of the map $E[p] \to S$ have cardinality p^2 (the Zariski open set $\{p \neq 0\}$),
- the stratum over which the fibers of the map $E[p] \to S$ have cardinality p, called the *ordinary locus*,
- the stratum over which the fibers of the map $E[p] \to S$ consists of a single think point, called the *supersingular locus*.

(See Figure 1.)

Over a field over characteristic p, the derivative of the map $[p] : E \to E$ is identically zero. The prototypical example of a map whose derivative vanishes identically over a field of characteristic p is the Frobenius morphism.

Definition 3. Let X be a scheme of characteristic p. The *absolute Frobenius* morphism $\text{Frob}_X : X \to X$ is given by

Notes prepared for the Juvitop seminar at the Massachusetts Institute of Technology, October 3, 2012. Much of these notes (in particular figures) is borrowed from notes prepared by André Henriques for a talk on the moduli stack of elliptic curves given at the 2007 Talbot Workshop on Topological Modular Forms, available online at `http://math.mit.edu/conferences/talbot/2007/tmfproc/Chapter04/henriques.pdf`.)

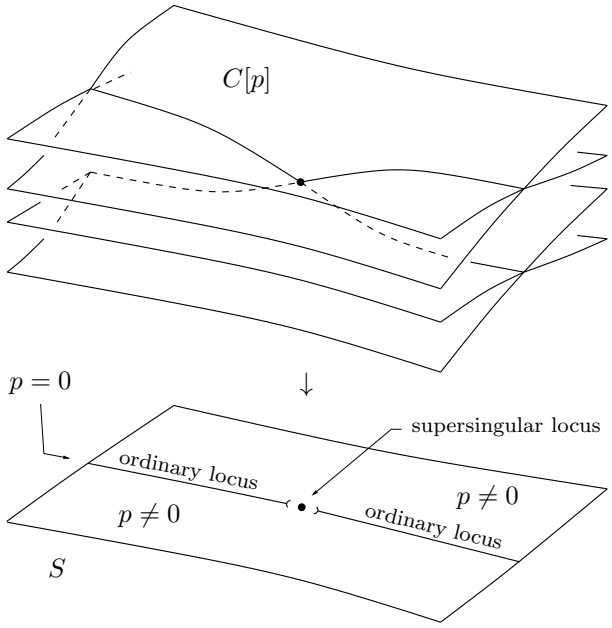
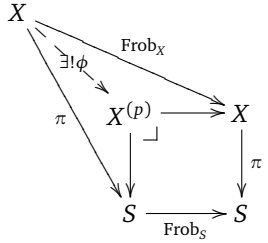


FIGURE 1. Stratification of the base scheme S into the Zariski open set $\{p \neq 0\}$, the ordinary locus and the supersingular locus.

- Frob_X is the identity on the underlying topological space $|X|$,
- $\mathrm{Frob}_X^\sharp : \mathcal{O}_X \to \mathcal{O}_X$ is given on sections by $f \mapsto f^p$.

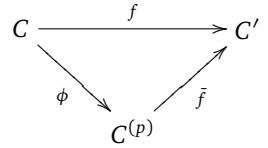
Unfortunately, for an S-scheme $\pi : X \to S$, the absolute Frobenius is in general *not* a morphism of S-schemes (unless, for instance, $S = \mathrm{Spec}\,\mathbb{F}_p$). To remedy this, we define the relative Frobenius, which will be a morphism of S-schemes.

Definition 4. Let $X^{(p)} = X \times_{\mathrm{Frob}_S, S} S$ be the pullback in the following diagram. The *relative Frobenius* morphism $\phi : X \to X^{(p)}$ is the unique morphism given by the universal property of the pullback.



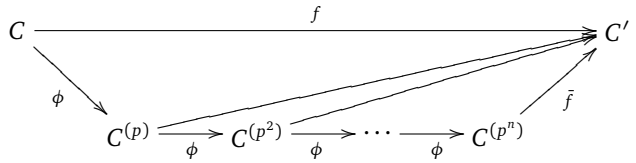
Concretely, $X^{(p)}$ has the same underlying topological space as X but instead has structure sheaf $\mathcal{O}_{X^{(p)}}(U) = \{f^p \mid f \in \mathcal{O}_X(U)\}$. The map $\phi : X \to X^{(p)}$ is given by the identity on the underlying topological space and by the inclusion $\mathcal{O}_{X^{(p)}} \hookrightarrow \mathcal{O}_X$ on the level of structure sheaves.

Proposition 5. *Let C and C' be curves defined over a field of characteristic p, and let $f : C \to C'$ be a map whose derivative vanishes identically. Then the map f can be factored through the relative Frobenius of C:*



Corollary 6. *Let E be an elliptic curve defined over a field of characteristic p. Then the map $[p] : E \to E$ factors through $\phi : E \to E^{(p)}$.*

Define $C^{(p^{m+1})} := (C^{(p^m)})^{(p)}$ inductively. Given a non-constant map $f : C \to C'$, there is a maximal number n of times f can be factored through relative Frobenii:



Since $\deg \phi = p$, we have that $\deg f = p^n \deg \bar{f}$.

Fact 7. The relative Frobenius $\phi : C \to C^{(p)}$ is purely inseparable. The multiplication-by-p morphism $[p] : E \to E$ is purely inseparable if and only if $E(\bar{k})[p] = 0$.

Taking C and C' to be the elliptic curve E and f to be $[p]$ and using the multiplicativity of inseparable degrees, we see that two cases can occur, depending on the cardinality of $E(\bar{k})[p]$:

- E is ordinary. Then $n = 1$ and $\overline{[p]} : E^{(p)} \to E$ is separable of degree p.
- E is supersingular. Then $n = 2$ and $\overline{[p]} : E^{(p^2)} \to E$ is an isomorphism.

The second case yields the following corollary.

Corollary 8. *If E is a supersingular elliptic curve defined over a field k of characteristic p, then its j-invariant is an element of $k \cap \mathbb{F}_{p^2}$. In particular, there are at most p^2 isomorphism classes of supersingular elliptic curves.*

Proof. By writing the equation for an elliptic curve in terms of Weierstrass coefficients and using the fact that a power map $k \to k$ is a homomorphism, one sees that $j(E^{(p^2)}) = j(E)^{p^2}$. But $j(E^{(p^2)}) = j(E)$ if E is supersingular, so $j(E) \in k \cap \mathbb{F}_{p^2}$. □

Thus, at a prime p, the supersingular locus $\mathscr{M}_{\text{ell}}^{\text{ss}}$ is a closed substack of the moduli stack of elliptic curves $\mathscr{M}_{\text{ell}}$, formed as a disjoint union of stacks

$$\coprod_{\substack{[E] \\ \text{supersingular}}} B\operatorname{Aut}(E) = \coprod_{\substack{[E] \\ \text{supersingular}}} */\operatorname{Aut}(E),$$

and the associated coarse moduli space is a disjoint union of points. The ordinary locus $\mathscr{M}_{\text{ell}}^{\text{ord}}$ is the open complement of $\mathscr{M}_{\text{ell}}^{\text{ss}}$ in $\mathscr{M}_{\text{ell}}|_{\operatorname{Spec}\mathbb{F}_p}$. As a coarse moduli space, $\mathscr{M}_{\text{ell}}^{\text{ord}}|_{\operatorname{Spec}\overline{\mathbb{F}_p}}$ is the affine line $\mathbb{A}^1_{\overline{\mathbb{F}_p}}$ with punctures corresponding to the isomorphism classes of supersingular elliptic curves.

In fact, there are approximately $p/12$ isomorphism classes of supersingular elliptic curves in characteristic p, and if one weights the isomorphism classes by the reciprocal of the order of the automorphism group, then one has the celebrated Eichler-Deuring mass formula:

Theorem 9 (Eichler-Deuring)**.**

$$\sum_{\substack{[E]:E/\overline{\mathbb{F}_p} \\ \textit{supersingular}}} \frac{1}{\operatorname{Aut} E} = \frac{p-1}{24}.$$

2. Formal groups

Definition 10. A *(one-dimensional, commutative) formal group* over a scheme S is a formal scheme $\mathbb{G} \to S$ which is isomorphic to the infinitesimal neighborhood of the zero section of a line bundle, and which is equipped with an addition law

$$+ : \mathbb{G} \times_S \mathbb{G} \to \mathbb{G}$$

that makes it an abelian group object, with the identity element given by the zero section $S \to \mathbb{G}$.

Remark 11. For those who prefer to think about formal group *laws* instead of formal groups, a formal group law is essentially a formal group together with a choice of coordinate, that is, a formal group law over a commutative ring R is equivalent to the data of a formal group $\mathbb{G}$ over $\operatorname{Spec} R$ together with a specified isomorphism $\mathbb{G} \cong \operatorname{Spf} R[[x]]$ (but with different addition laws on the formal schemes; the formal group law relates the addition laws on $\mathbb{G}$ and $\operatorname{Spf} R[[x]]$).

Given an elliptic curve E over a field k, let $\hat{E}$ be an infinitesimal neighborhood around the identity. Then $\hat{E}$ has the structure of a formal group.

Given a formal group $\mathbb{G}$, one can consider the multiplication-by-p map $[p] : \mathbb{G} \to \mathbb{G}$.

Lemma 12. *Let $\mathbb{G}$ be a formal group over a field k of characteristic p, and suppose that the map $[p] : \mathbb{G} \to \mathbb{G}$ is nonzero. After choosing an identification of $\mathbb{G}$ with $\mathrm{Spf}(k[[x]])$, the map $[p]$ is given by a power series expansion of the form*

$$[p](x) = \sum_{i \geq 1} a_i x^{ip^n}$$

for some integer $n \geq 1$ and elements $a_i \in k$, $a_1 \neq 0$, called the p-series of $\mathbb{G}$.

Proof. The derivative of $[p] : \mathbb{G} \to \mathbb{G}$ vanishes identically, so we can factor $[p]$ as in Proposition 5. Let n be the maximal number for which $[p]$ factors as $[p] = \bar{f} \circ \phi^n$, then the power series expansion of $[p]$ is

$$[p](x) = \bar{f}'(x^n) = \sum_{i \geq 1} a_i x^{ip^n}$$

for some $a_i \in k$. One has to show that $a_1 \neq 0$.

Since ϕ is a surjective group homomorphism, $\bar{f}$ is also a group homomorphism, hence its derivative $\bar{f}'$ is either identically zero or everywhere nonzero. If $\bar{f}' = 0$, then by Proposition 5, we can factor $\bar{f}$ further, contradicting the maximality of n. Hence $a_1 = \bar{f}'(0) \neq 0$. □

Definition 13. Let $\mathbb{G}$ be a formal group over a field of k of characteristic p. The *height* of $\mathbb{G}$ is the smallest number n such that the coefficient of x^{p^n} in the p-series of $\mathbb{G}$ is nonzero. If the p-series of $\mathbb{G}$ is identically zero, then we say that $\mathbb{G}$ has height ∞.

As mentioned by Mark Behrens in the first talk, this is equivalent to $\mathbb{G}[p]$ being a finite flat group scheme of order p^n.

From Lemma 12, we see that a formal group has height n if and only if

$$a_p = a_{p^2} = \cdots = a_{p^{n-1}} = 0, \quad a_{p^n} \neq 0$$

in its p-series. One customarily writes v_n for a_{p^n}.

From our factorizations of $[p] : E \to E$ through the relative Frobenius, we see that for an elliptic curve E over a field of characteristic p, $\hat{E}$ can only be of height one or two: $\hat{E}$ is of height one if E is ordinary and of height two if E is supersingular. To obtain formal groups of height greater than two, it is necessary to consider more general abelian varieties.

Just as there is a moduli stack of elliptic curves, there is also a moduli stack of formal groups $\mathscr{M}_{\mathrm{FG}}$ with $\mathscr{M}_{\mathrm{FG}}(R)$ the category whose objects are formal groups over R and whose morphisms are isomorphisms between them. The assignment $E \mapsto \hat{E}$ defines a map $\mathscr{M}_{\mathrm{ell}} \to \mathscr{M}_{\mathrm{FG}}$ which maps the ordinary locus to formal groups of height one and the supersingular locus to formal groups of height two. We close this talk with a brief description of $\mathscr{M}_{\mathrm{FG}}$.

Lazard's theorem tells us that the structure of $\mathscr{M}_{\mathrm{FG}}|_{\mathrm{Spec}\,\overline{\mathbb{F}_p}}$ is extremely simple:

Theorem 14 (Lazard)**.** *Let k be an algebraically closed field of characteristic p. Then there is exactly one isomorphism class of formal groups of each height $1, 2, 3, \ldots, \infty$ over k.*

More generally, if $\mathbb{G}$ is a formal group defined over a scheme of characteristic p, one can consider the heights of the fibers $\mathbb{G}|_x$ at the various closed points $x \in S$. This partitions S into strata $S_n := \{x \in S \mid \mathrm{ht}(\mathbb{G}|_x) = n\}$. The closed subsets $S_{>n} := \bigcup_{m>n} S_m$ form a decreasing subsequence

$$S = S_{>0} \supset S_{>1} \supset S_{>2} \supset \cdots$$

where each $S_{>n}$ is of codimension at most one more than $S_{>n-1}$. Thus the moduli substack $\mathscr{M}_{\mathrm{FG}}^{\geq 1} = \mathscr{M}_{\mathrm{FG}}|_{\mathrm{Spec}\,\mathbb{F}_p}$ of formal groups of height at least one looks as in Figure 2. Namely, it consists of a countable sequence of stacky points, with the closure of each point containing all the points of greater height. On the other hand, the moduli stack of formal groups of height 0 is given by $\mathscr{M}_{\mathrm{FG}}^0 = \mathscr{M}_{\mathrm{FG}}|_{\mathrm{Spec}\,\mathbb{Q}} \cong B\mathbb{G}_m = */\mathbb{G}_m$.

If $\mathbb{G}$ is a formal group defined over a scheme not necessarily of characteristic p, then $\mathbb{G}$ has many heights, one for each prime p. By convention, we define the p-height to be zero whenever $p \neq 0$. Over $\mathrm{Spec}\,\mathbb{Z}$, $\mathscr{M}_{\mathrm{FG}}$ looks as in Figure 3.

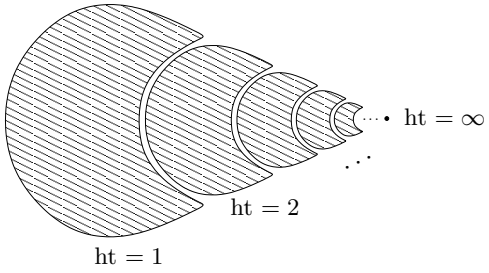


FIGURE 2. Cartoon of $\mathscr{M}_{\mathrm{FG}}$ over $\operatorname{Spec}\mathbb{F}_p$

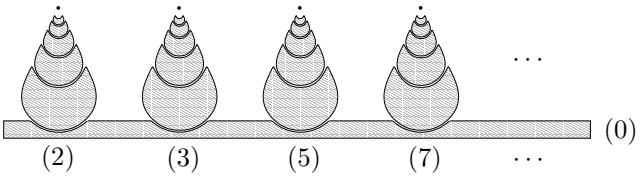


FIGURE 3. Cartoon of $\mathscr{M}_{\mathrm{FG}}$ over $\operatorname{Spec}\mathbb{Z}$

3. SUMMARY

We have given several properties of ordinary and supersingular elliptic curves. With a little more work, one can show the following equivalent criteria for ordinary and supersingular elliptic curves.

Theorem 15. *Let k be a field of characteristic p and let E be an elliptic curve defined over k. For each integer $r \geq 1$, let*

$$\phi_r : E \to E^{(p^r)} \quad \text{and} \quad \hat{\phi}_r : E^{(p^r)} \to E$$

be the p^r-th power Frobenius map and its dual isogeny, that is, $\hat{\phi}_r \circ \phi_r = [p^r]$.

(a) The following conditions on E are equivalent, and in this situation E is supersingular:
- *(i) $E(\bar{k})[p^r] = 0$ for one (all) $r \geq 1$.*
- *(ii) $\hat{\phi}_r$ is (purely) inseparable for one (all) $r \geq 1$.*
- *(iii) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.*
- *(iv) The formal group $\hat{E}/k$ associated to E has height two.*
- *(v) $\operatorname{End}_{\bar{k}}(E)$ is an order in a quaternion algebra.*

(b) Otherwise, if the equivalent conditions in (a) do not hold, then E is ordinary,

$$E(\bar{k})[p^r] = \mathbb{Z}/p^r\mathbb{Z} \quad \text{for all } r \geq 1$$

and the formal group $\hat{E}/k$ has height one. Moreover, if $j(E) \in \overline{\mathbb{F}_p}$, then $\operatorname{End}_{\bar{k}}(E)$ is an order in an imaginary quadratic field.