THE MODULI STACK OF ELLIPTIC CURVES

ANDRÉ HENRIQUES

1. The geometry of $\mathcal{M}_{ell}$

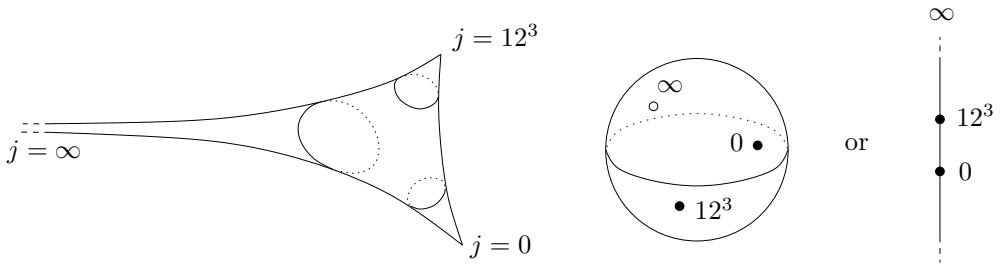
1.1. **$\mathcal{M}_{ell}$ over the complex numbers.** Over the complex numbers, any elliptic curve C is isomorphic to $C_\tau := \mathbb{C}/\mathbb{Z}\{1,\tau\}$ for some complex number τ in the upper half plane $\mathbb{H}$. Two elliptic curves C_τ and $C_{\tau'}$ are then isomorphic if and only if $\tau' = g\cdot\tau$ for some element $g \in SL_2(\mathbb{Z})$, where the (non-faithful) action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ is given by $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)\cdot\tau = \frac{a\tau+b}{c\tau+d}$. More precisely, there is a bijective correspondence between isomorphisms $C_\tau \xrightarrow{\sim} C_{\tau'}$, and group elements $g \in SL_2(\mathbb{Z})$ satisfying $\tau' = g\cdot\tau$. The map corresponding to $g = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ is then given by $C_\tau \to C_{\tau'} : z \mapsto \frac{z}{c\tau+d}$. It follows that $\mathcal{M}_{ell}$ is the quotient stack

$$\mathcal{M}_{ell} = [\mathbb{H}/SL_2(\mathbb{Z})].$$

The automorphism group of the elliptic curve C_τ then corresponds to the stabilizer group of τ by the action of $SL_2(\mathbb{Z})$.

The j-invariant provides an algebraic map $\mathcal{M}_{ell} \to \mathbb{C}$, expressing $\mathbb{C}$ as the coarse moduli space of $\mathcal{M}_{ell}$. By definition, this means that the above map is initial among all maps from $\mathcal{M}_{ell}$ to a variety. By a generalized elliptic curve we mean a curve that is either an elliptic curve or isomorphic to the multiplicative curve $\mathbb{G}_m = \mathbb{C}^\times$. The moduli space $\overline{\mathcal{M}}_{ell}$ of generalized elliptic curves can then be thought as the one point compactification of $\mathcal{M}_{ell}$, and the j-invariant extends to a map $\overline{\mathcal{M}}_{ell} \to \mathbb{CP}^1$.

There are two distinguished j-invariants, corresponding to curves with extra symmetries. These are $j = 0$, which corresponds to the elliptic curve obtained by modding out $\mathbb{C}$ by an equilateral lattice, and $j = 12^3 = 1728$, which corresponds to the elliptic curve $\mathbb{C}_i = \mathbb{C}/\mathbb{Z}\{1,i\}$. Those elliptic curves have automorphism group $\mathbb{Z}/6$ and $\mathbb{Z}/4$, respectively, while all the other generalized elliptic curves have automorphism group $\mathbb{Z}/2$. Depending on one's taste, one might then draw $\mathcal{M}_{ell}$ as

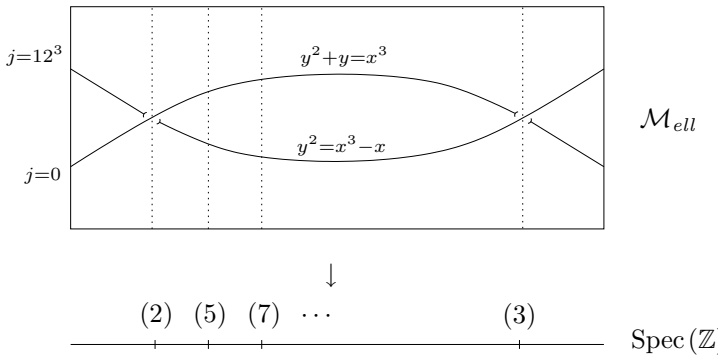


The first one of the above pictures is the most geometric, but it is only the third one that we will be able to generalize to the case when our base is $\mathrm{Spec}\,(\mathbb{Z})$.

1.2. **$\mathcal{M}_{ell}$ over the integers.** Over $\mathrm{Spec}\,(\mathbb{Z})$, the coarse moduli spaces of $\mathcal{M}_{ell}$ and $\overline{\mathcal{M}}_{ell}$ are still isomorphic $\mathbb{A}^1$ and $\mathbb{P}^1$, respectively. However, $\mathrm{Spec}\,(\mathbb{Z})$ being one-dimensional, it is now preferable to draw $\mathbb{A}^1_{\mathrm{Spec}\,(\mathbb{Z})}$ as a plane, as opposed to a line. The elements $0, 12^3 \in \mathbb{Z}$ then correspond to sections of the projection map $\mathbb{A}^1_{\mathrm{Spec}\,(\mathbb{Z})} \to \mathrm{Spec}\,(\mathbb{Z})$. Note that, since the difference $12^3 - 0$ is divisible by 2 and 3, the values of those two sections agree over the points $(2), (3) \in \mathrm{Spec}\,(\mathbb{Z})$.

Date: 2007.

The elliptic curves $\{y^2 + y = x^3\}$ and $\{y^2 = x^3 - x\}$ have j-invariants 0 and 12^3, respectively. Their discriminants are -27 and -64. Therefore, as elliptic curves, they are actually only defined over $\mathbb{Z}_{(3)}$ and $\mathbb{Z}_{(2)}$, respectively. By definition of $\mathcal{M}_{ell}$, an elliptic curve defined over a ring R gives rise to a map $\mathrm{Spec}\,(R) \to \mathcal{M}_{ell}$. So the above elliptic curves correspond to maps $\mathrm{Spec}\,(\mathbb{Z}_{(3)}) \to \mathcal{M}_{ell}$ and $\mathrm{Spec}\,(\mathbb{Z}_{(2)}) \to \mathcal{M}_{ell}$.



Given a variety X defined over $\mathbb{F}_p$, one typically needs to base change to $\bar{\mathbb{F}}_p$ in order to "see" all the automorphisms of X. But for elliptic curves it turns out that $\mathbb{F}_{p^2}$ is always enough. The automorphism groups of an elliptic curve C defined over a finite field $\mathbb{F}$ containing $\mathbb{F}_{p^2}$ are given by:

$$\mathrm{Aut}(C) = \begin{cases} \mathbb{Z}/2 & \text{if} \quad j \neq 0, 12^3 \\ \mathbb{Z}/6 & \text{if} \quad j = 0\,, \qquad p \neq 2,3 \\ \mathbb{Z}/4 & \text{if} \quad j = 12^3, \qquad p \neq 2,3 \\ \mathbb{Z}/4 \ltimes \mathbb{Z}/3 & \text{if} \quad j = 0 = 12^3, \quad p = 3 \\ \mathbb{Z}/3 \ltimes Q_8 & \text{if} \quad j = 0 = 12^3, \quad p = 2 \end{cases}$$

The last group is the semi-direct product of $\mathbb{Z}/3$ with the quaternion group Q_8, where the action permutes the generators i, j and k.

If C is defined over $\mathbb{F}_p$, then it is better to view $\mathrm{Aut}(C)$ as a finite group scheme, as opposed to a mere finite group. In general, the data of a finite group scheme over some field k is equivalent to that of a finite group and an action of $\mathrm{Gal}(K/k)$ by group automorphisms, where K is some finite extension of k. In our case, $k = \mathbb{F}_p$, $K = \mathbb{F}_{p^2}$, and $\mathrm{Aut}(C)$ is given by $\mathrm{Aut}\left(C \times_{\mathrm{Spec}\,(\mathbb{F}_p)} \mathrm{Spec}\,(\mathbb{F}_{p^2})\right)$, along with its action of $\mathbb{Z}/2 = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. The actions of $\mathbb{Z}/2$ on the above groups is given by:

$\mathbb{Z}/2$	:	the trivial action;
$\mathbb{Z}/6$	:	trivial iff 3 divides $p-1$;
$\mathbb{Z}/4$	:	trivial iff 4 divides $p-1$;
$\mathbb{Z}/4 \ltimes \mathbb{Z}/3$	:	non-trivial on $\mathbb{Z}/4$, trivial on $\mathbb{Z}/3$;
$\mathbb{Z}/3 \ltimes Q_8$	:	non-trivial action on $\mathbb{Z}/3$; the action on Q_8 exchanges $i \leftrightarrow -i$, $j \leftrightarrow -k$, and $k \leftrightarrow -j$.

Note that the group schemes corresponding to the first three rows of the above list are isomorphic to μ_2, μ_6, and μ_4, respectively.

2. Multiplication by p

Let C be an elliptic curve defined over a field $\mathbb{F}$. Like any abelian group, it has a natural endomorphism $[p] : C \to C$ given by $x \mapsto x + \cdots + x$ (p times). Clearly, the derivative of $[p]$ at the identity element is multiplication by p. If p is invertible in $\mathbb{F}$, then the derivative of $[p]$ is non-zero at the identity element, and therefore everywhere non-zero since it is a group homomorphism. On the other hand, if $\mathbb{F}$ has characteristic p, then the derivative of $[p]$ is identically zero.

Let $C[p]$ denote the scheme-theoretical kernel of $[p]$. From the above discussion, we see that $C[p]$ is a reduced scheme if and only if $p \neq 0$. The number of geometric points of $C[p]$ can vary. But if we count points with multiplicities, then that number is always p^2.

Theorem 2.1. *Let C be an elliptic curve defined over a field $\mathbb{F}$. Then $[p]: C \to C$ has degree p^2. Equivalently, the vector space $\Gamma(C[p], \mathcal{O})$ has dimension p^2.*

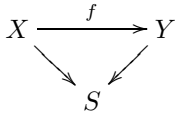
Proof. We begin by the observation that, if C_1 and C_2 are smooth curves over a field $\mathbb{F}$, then any non-constant map $f: C_1 \to C_2$ is flat. Indeed, flatness can be checked on formal neighborhoods of points. So without loss of generality, we may replace C_1 and C_2 by their completions around some given points. The map f can then be written locally as

$$\begin{array}{rcccl} f : \mathrm{Spf}\left(\mathbb{F}[[x]]\right) & \to & \mathrm{Spf}\left(\mathbb{F}[[y]]\right) & & \\ \mathbb{F}[[x]] & \leftarrow & \mathbb{F}[[y]] & : & f^* \\ f^*(y) & \mapsto & y & & \end{array} \tag{1}$$

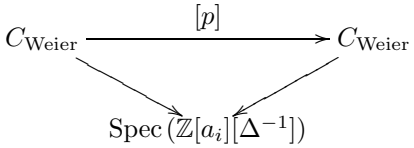
The power series $f^*(y) \in \mathbb{F}[[x]]$ is non-zero by assumption, so can be written as $f^*(y) = ax^d + (\text{higher terms})$ for some $a \neq 0$. One then checks that $\mathbb{F}[[x]]$ is a free $\mathbb{F}[[y]]$ module with basis $\{1, x, \ldots, x^{d-1}\}$. In particular, it is flat.

Now let C be an elliptic curve defined over a field. Since $[p]: C \to C$ is not the constant map [3, Prop. III.4.2], it is flat.

It will be useful to allow more general base schemes. Recall [1, section 11.3.11] that given a diagram

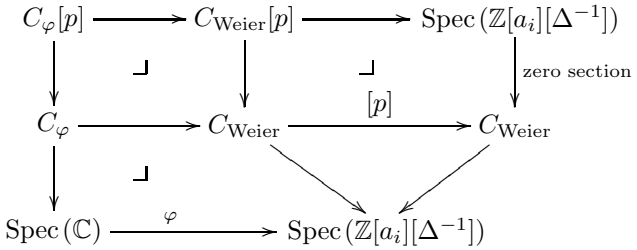


where X and Y are flat and of finite type over S, the map f is flat iff for every field $\mathbb{F}$ and every map $\mathrm{Spec}(\mathbb{F}) \to S$, the pullback map $f: X \times_S \mathrm{Spec}(\mathbb{F}) \to Y \times_S \mathrm{Spec}(\mathbb{F})$ is flat. Let C_{Weier} denote the universal Weierstrass elliptic curve, defined over the ring $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\Delta^{-1}]$. By the above criterion, and using our knowledge about elliptic curves over fields, we see that



is flat.

Fix a map $\varphi: \mathrm{Spec}(\mathbb{C}) \to \mathrm{Spec}(\mathbb{Z}[a_i][\Delta^{-1}])$, and let C_φ be the elliptic curve it classifies. Since C_φ is topologically isomorphic to $S^1 \times S^1$, one sees immediately that $C_\varphi[p] \simeq (\mathbb{Z}/p)^2$. Now consider the following commutative diagram:



Being an elliptic curve, C_{Weier} is proper over $\mathrm{Spec}(\mathbb{Z}[a_i][\Delta^{-1}])$. Any map between proper schemes is proper, and so $[p]$ is proper. The projection $C_{\mathrm{Weier}}[p] \to \mathrm{Spec}(\mathbb{Z}[a_i][\Delta^{-1}])$ is pulled back from $[p]$. It is therefore flat and proper, and in particular, it has constant relative dimension. To compute the latter, we note that the relative dimension of a map is left unchanged by pullbacks, and that $C_\varphi[p] \to \mathrm{Spec}(\mathbb{C})$ is of relative dimension zero.

We have shown that $C_{\text{Weier}}[p] \to \operatorname{Spec}(\mathbb{Z}[a_i][\Delta^{-1}])$ is proper, flat, and of relative dimension zero. It is therefore a finite map. Being flat and finitely generated, the $\mathbb{Z}[a_i][\Delta^{-1}]$ module $\Gamma(C_{\text{Weier}}[p]; \mathcal{O})$ is therefore projective of finite rank. The rank of a projective module is stable under pullbacks. It is therefore equal to the complex dimension of $\Gamma(C_\varphi[p]; \mathcal{O})$, namely p^2.

Now let C be an arbitrary elliptic curve, defined over a field $\mathbb{F}$. By the following pullback square

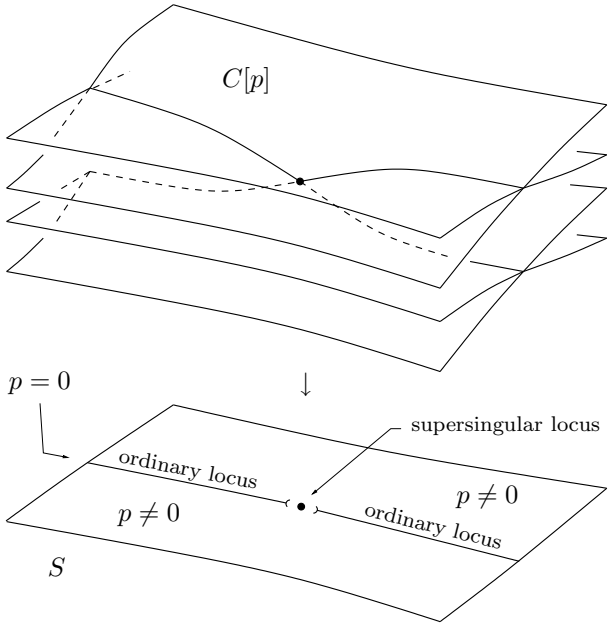
$$\begin{array}{ccc} C[p] & \longrightarrow & C_{\text{Weier}}[p] \\ \downarrow & \lrcorner & \downarrow \\ \operatorname{Spec}(\mathbb{F}) & \longrightarrow & \operatorname{Spec}(\mathbb{Z}[a_i][\Delta^{-1}]) \end{array}$$

we see that the dimension of $\Gamma(C[p]; \mathcal{O})$ is equal to the rank of $\Gamma(C_{\text{Weier}}[p]; \mathcal{O})$, which is p^2. □

The scheme theoretic cardinality of $C[p]$ is always p^2. Since $C[p]$ is a group, the number of connected components of $C[p]$ is therefore either p^2, p, or 1. All those cases can occur. The first one happens iff $C[p]$ is reduced, namely iff the base field is of characteristic different from p. The two other cases happen in characteristic p.

Definition 2.2. Let $\mathbb{F}$ be a field of characteristic p, and C an elliptic curve defined over $\mathbb{F}$. Then C is called *ordinary* if $C[p]$ has p connected components, and *supersingular* if $C[p]$ is connected.

If C is an elliptic curve defined over an arbitrary base scheme S, then there is a natural stratification of S: the stratum over which the fibers of the map $C[p] \to S$ have cardinality p^2, the one over which they have cardinality p, and the one over which they consist of a single thick point. The first of the above three strata is the Zariski open set $\{p \neq 0\}$. The other two strata are called the *ordinary locus* and the *supersingular locus*.



3. The relative Frobenius

In characteristic zero, the derivative of a non-constant map $f : C_1 \to C_2$ can only vanish at a finite number of points. But in characteristic p, the derivative of f can vanish identically without f being constant. For example, this is the case for the map $[p] : C \to C$, where C is an elliptic curve. The prototypical example of a map whose derivative vanishes identically is the relative Frobenius.

Definition 3.1. Let C be a curve defined over a perfect field $\mathbb{F}$ of characteristic p. Define $C^{(p)}$ to be the scheme with same underlying space as C, but with structure sheaf

$$\mathcal{O}_{C^{(p)}}(U) := \{x^p \,|\, x \in \mathcal{O}_C(U)\}.$$

The relative Frobenius of C is the map

$$\phi : C \longrightarrow\!\!\!\!\!\rightarrow C^{(p)}$$

given by the identity on the underlying spaces, and by the inclusion $\mathcal{O}_{C^{(p)}} \hookrightarrow \mathcal{O}_C$ at the level of structure sheaves.

In local coordinates, the relative Frobenius is given by

$$\begin{array}{ccccc} \phi & : & \mathrm{Spf}(\mathbb{F}[[x]]) & \to & \mathrm{Spf}(\mathbb{F}[[x]])^{(p)} = \mathrm{Spf}(\mathbb{F}[[y]]) \qquad (\text{where } y = x^p) \\ & & x^p & \mapsfrom & y \end{array}$$

We see in particular that its derivative ϕ' vanishes identically.

Remark 3.2. If C is defined by equations in $\mathbb{P}^n$, then $C^{(p)}$ can be identified with the curve defined by those same equations, but where all the coefficients have been replaced by their pth powers. In those coordinates, the relative Frobenius is given by $\phi([x_0, \ldots, x_n]) = [x_0^p, \ldots, x_n^p]$. Using that as our working definition, we could have removed the condition that $\mathbb{F}$ be perfect in Definition 3.1.

In the rest of this chapter, we assume for convenience that the base field $\mathbb{F}$ is perfect. All the statements remain true without that assumption.

Proposition 3.3. *Let C_1, C_2 be curves defined over a perfect field of characteristic p, and let $f : C_1 \to C_2$ be a map whose derivative vanishes identically. Then the map f can then be factored through the relative Frobenius of C_1:*

(2)
$$\begin{array}{ccc} C_1 & \xrightarrow{\quad f \quad} & C_2\,. \\ & {\scriptstyle\phi}\searrow \quad \nearrow{\scriptstyle\bar{f}} & \\ & C_1^{(p)} & \end{array}$$

Proof. In local coordinates, the map f is given by some power series expansion, as in (1). Since $f^*(y) = \sum a_i x^i \in \mathbb{F}[[x]]$ has zero derivative, it follows that $a_i = 0$ for all i not divisible by p.

Now, let $g \in \Gamma(U, \mathcal{O}_{C_1})$ be a function in the image of $f : f^*\mathcal{O}_{C_2} \to \mathcal{O}_{C_1}$. Its derivative g' is identically zero, so g admits a pth root (a priori, this is only true locally, but the local pth roots are unique, so they assemble to a pth root defined on the whole U). It follows that $g \in \mathcal{O}_{C_1}^{(p)}$. We have shown that $f^*\mathcal{O}_{C_2} \to \mathcal{O}_{C_1}$ factors through $\mathcal{O}_{C_1}^{(p)}$, which is equivalent to the statement that f factors through $C_1^{(p)}$. □

Corollary 3.4. *Let C be an elliptic curve defined over a perfect field of characteristic p, Then the map $[p] : C \to C$ factors through ϕ.*

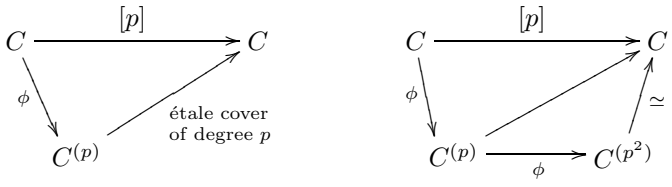
Define inductively $C^{(p^{n+1})} := (C^{(p^n)})^{(p)}$. Given a non-constant map $f : C_1 \to C_2$, there is a maximal number n such that we get factorizations

$$\begin{array}{ccccccc} C_1 & & \xrightarrow{\qquad\qquad f \qquad\qquad} & & & & C_2 \\ {\scriptstyle\phi}\searrow & & & & & & \uparrow{\scriptstyle\bar{f}} \\ & C_1^{(p)} & & & \cdots & & \\ & {\scriptstyle\phi}\searrow & & & & & \\ & & C_1^{(p^2)} & \cdots \xrightarrow[\phi]{} & & C_1^{(p^n)} & \end{array}$$

Note that since $\deg(\phi) = p$, it follows that $\deg(f) = p^n \deg(\bar{f})$.

If C is an elliptic curve and f is the map $[p]\colon C \to C$, then by Theorem 2.1 two cases can occur. Either C is ordinary, in which case $n = 1$ and the map $\bar{f}\colon C^{(p)} \to C$ is an étale cover of order p, or C is supersingular, in which case $n = 2$ and $\bar{f}\colon C^{(p^2)} \to C$ is an isomorphism.

(3)



Lemma 3.5. *If C is a supersingular elliptic curve defined over a perfect field $\mathbb{F}$ of characteristic p, then its j-invariant is an element of $\mathbb{F} \cap \mathbb{F}_{p^2}$. In particular, there are at most p^2 isomorphism classes of supersingular elliptic curves.*

Proof. By (3), we see that $C^{(p^2)}$ is isomorphic to C. It follows that $j(C^{(p^2)}) = j(C)^{p^2} = j(C)$. □

In fact, there are roughly $p/12$ isomorphism classes of supersingular elliptic curves [3, Theorem V.4.1]. More precisely, if we count each isomorphism class with a multiplicity of $1/|\operatorname{Aut}(C)|$, then one has the following formula:

$$\sum_{\substack{[C]\colon C \text{ is} \\ \text{supersingular}}} \frac{1}{|\operatorname{Aut}(C)|} = \frac{p-1}{24}.$$

For small primes, the number of supersingular curves is recorded in the following table:

$p =$	2	3	5	7	11	13	17	19	23	29	$\cdots$
# of ss curves	1	1	1	1	2	1	2	2	3	3	$\cdots$
$\sum \frac{1}{\lvert\operatorname{Aut}(C)\rvert}$	$\frac{1}{24}$	$\frac{1}{12}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{4}+\frac{1}{6}$	$\frac{1}{2}$	$\frac{1}{2}+\frac{1}{6}$	$\frac{1}{2}+\frac{1}{4}$	$\frac{1}{2}+\frac{1}{4}+\frac{1}{6}$	$\frac{1}{2}+\frac{1}{2}+\frac{1}{6}$	$\cdots$

4. Formal groups

Given an elliptic curve C, let $\widehat{C}$ denote its formal completion at the identity. Then $\widehat{C}$ has the structure of a formal group.

Definition 4.1. A (one dimensional, commutative) formal group over S is a formal scheme $G \to S$ which is isomorphic to the formal completion of a line bundle along its zero section, and which comes equipped with an addition law

$$+ : G \times_S G \to G,$$

making it into an abelian group object, with neutral element given by the zero section $S \to G$.

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

Lemma 4.2. *Let G be formal group over a perfect field $\mathbb{F}$ of characteristic p, and let us assume that the map $[p]\colon G \to G$ is not constant. Then, after picking an identification of G with $\operatorname{Spf}(\mathbb{F}[[x]])$, the power series expansion of $[p]$ is of the form*

$$[p](x) = a_1 x^{p^n} + a_2 x^{2p^n} + a_3 x^{3p^n} + \dots \tag{4}$$

for some integer $n \geq 1$, and elements $a_i \in \mathbb{F}$, $a_1 \neq 0$.

Proof. The first derivative of $[p]$ vanishes identically, so we can factor $[p]$ as in (2). Letting n be the biggest number for which we get a factorization $[p] = \bar{f} \circ \phi^n$, the power series expansion for $[p]$ then looks as in (4). We need to show that $a_1 \neq 0$.

Since ϕ is a surjective group homomorphism, $\bar{f}$ is also a homomorphism. The first derivative of $\bar{f}$ is therefore either everywhere non-zero or identically zero. If $\bar{f}' = 0$, then by Proposition 3.3, we get a further factorization by ϕ, contradicting the maximality of n. So $\bar{f}'(0) = a_1 \neq 0$. □

The power series (4) is called the *p-series* of G. By the above lemma, we see that the first non-zero coefficient of the p-series is always that of some x^{p^n}.

Definition 4.3. Let G be formal group over a field of characteristic p. The *height* of G is the smallest number n such that the coefficient of x^{p^n} in the p-series of G is non-zero. If the p-series is identically zero, then we declare G to have height ∞.

Writing the p-series as $[p](x) = \sum a_i x^i$, we see by Lemma 4.2 that the condition of being of height greater than n is given by exactly n equations:

$$a_p = 0, \qquad a_{p^2} = 0, \qquad a_{p^3} = 0, \qquad \cdots, \qquad a_{p^n} = 0.$$

It is customary to write v_n for the coefficient a_{p^n}.

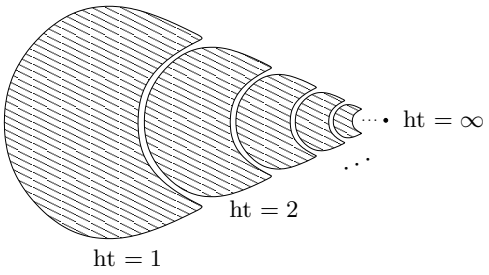
If C is an elliptic curve over a field of characteristic p, then by (3), the only possible heights for $\widehat{C}$ are 1 and 2. The height is 1 if C is ordinary, and 2 if is C is supersingular.

Theorem 4.4 (Lazard [2])**.** *Let $\mathbb{F}$ be an algebraically closed field of characteristic p. Then the height provides a bijection between the isomorphism classes of formal groups over $\mathbb{F}$, and the set $\{1, 2, 3, \ldots\} \cup \{\infty\}$.* □

Given a formal group G defined over a scheme S of characteristic p, one can consider the heights of the fibers $G|_x$ at the various closed points $x \in S$. This yields a partition of S into strata $S_n := \{x \in S : \mathrm{ht}(G|_x) = n\}$. The closed subsets $S_{>n} := \bigcup_{m>n} S_m$ then form a decreasing sequence

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

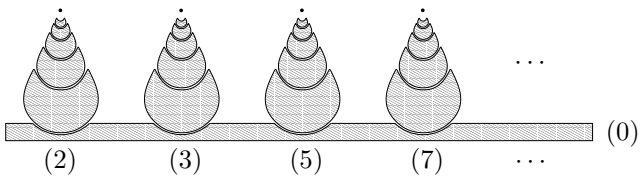
where each one is of codimension at most one in the previous one. Let $\mathcal{M}_{FG}$ denote the the moduli space of formal groups. From the above discussion, we see that $\mathcal{M}_{FG}|_{\mathrm{Spec}\,(\mathbb{F}_p)}$ looks roughly as follows:



Namely, it consists of a countable sequence of stacky points, each point containing all the next ones in its closure, and each point being of codimension one in the previous one.

When considering formal groups over schemes S that are not necessarily of characteristic p, then one has many heights: one for each prime p. By convention, we let the p-height be 0 whenever $p \neq 0$. Here's a picture of $\mathcal{M}_{FG}$ over $\mathrm{Spec}\,(\mathbb{Z})$:

(5)



The assignment $C \mapsto \widehat{C}$ defines a map $\mathcal{M}_{ell} \to \mathcal{M}_{FG}$. As we have seen, that map only hits the first three layers of (5), namely the ones where the p-heights are 0, 1, and 2.

To complete the picture, we give some examples of formal groups of height n. The following result of Lazard will be useful to us.

Proposition 4.5 (Lazard [2])**.** *Let R be a ring, and let*

$$\widetilde{+}_F : \mathrm{Spf}(R[[x]])^2 = \mathrm{Spf}(R[[x,y]]) \to \mathrm{Spf}(R[[x]])$$

be a binary operation satisfying the axioms for abelian groups, modulo error terms of total degree $\geq d$. Then there exists another operation $+_F$, which does satisfy the abelian group axioms, and which agrees with $\widetilde{+}_F$ modulo terms of degree $\geq d$. □

Let R be any ring, and consider the example:

$$x \mathbin{\widetilde{+}_F} y \;:=\; x + y + \frac{(x+y)^q - x^q - y^q}{p}\,,$$

where $q = p^n$, and p is a prime. It satisfies commutativity, unitarity, and associativity modulo terms of degree $\geq 2q-1$:

$$\begin{aligned}
\big(x \mathbin{\widetilde{+}_F} y\big) \mathbin{\widetilde{+}_F} z &= x + y + \frac{(x+y)^q - x^q - y^q}{p} + z \\
&\qquad + \frac{\big(x + y + \frac{(x+y)^q - x^q - y^q}{p} + z\big)^q - \big(x + y + \frac{(x+y)^q - x^q - y^q}{p}\big)^q - z^q}{p} \\
&= x + y + \frac{(x+y)^q - x^q - y^q}{p} + z + \frac{\big(x+y+z\big)^q - \big(x+y\big)^q - z^q}{p} \quad (\text{mod deg} \geq 2q-1) \qquad (6)\\
&= x + y + z + \frac{(x+y+z)^q - x^q - y^q - z^q}{p} \\
&= x \mathbin{\widetilde{+}_F} \big(y \mathbin{\widetilde{+}_F} z\big) \qquad (\text{mod degree} \geq 2q-1)
\end{aligned}$$

So, by the above proposition, there exists an abelian group law on $\mathrm{Spf}(R[[x]])$ of the form:

$$x \;+_F\; y \;:=\; x + y + \frac{(x+y)^q - x^q - y^q}{p} \;+\; (\text{terms of degree} \geq 2q-1). \qquad (7)$$

Generalizing the computation (6), it is easy to get the following formula:

$$x_1 \;+_F\; x_2 \;+_F \cdots +_F\; x_r \;=\; \sum x_i + \frac{\big(\sum x_i\big)^q - \sum x_i^q}{p} \qquad (\text{mod degree} \geq 2q-1).$$

In particular, if $R = \mathbb{F}$ is a field of characteristic p, then the p-series of (7) looks as follows:

$$[p](x) \;=\; px + \frac{(px)^q - px^q}{p} \;=\; -\,x^q \qquad (\text{mod degree} \geq 2q-1).$$

The first non-zero coefficient is that of $x^q = x^{p^n}$, therefore (7) defines an abelian group law of height n on $\mathrm{Spf}(\mathbb{F}[[x]])$.

References

[1] Alexandre Grothendieck. *Eléments de géométrie algébrique. IV*. Inst. Hautes Études Sci. Publ. Math. Étude locale des schémas et des morphismes de schémas.

[2] Michel Lazard. Sur les groupes de lie formels à un paramètre. (French). *Bull. Soc. Math. France*, 83:251–274, 1955.

[3] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.