# AWS LECTURE NOTES: MODULAR CURVES AT INFINITE LEVEL

JARED WEINSTEIN

## 1. Introduction

These lectures[1] concern the arithmetic of modular curves, and in particular the geometry of integral models of modular curves in the neighborhood of their singular points. These singularities only appear modulo $p$. If $X$ is a modular curve and $x$ is a singular point, then the nature of the singularity is measured by the completed local ring $\hat{\mathcal{O}}_{X,x}$.

Let us first review the basics of integral models of modular curves. Let $\Gamma$ be one of the congruence subgroups $\Gamma_0(N)$, $\Gamma_1(N)$, or $\Gamma(N)$. Then the modular curve $X(\Gamma)$, a priori defined over $\mathbb{Q}$, admits a smooth model over $\mathbb{Z}[1/N]$. That is, modular curves have good reduction modulo primes which do not divide the level. If $p \nmid N$, and if $x \in X(\Gamma)(\overline{\mathbb{F}}_p)$ is a geometric point of the special fiber, then we have

$$\hat{\mathcal{O}}_{X(\Gamma),x} \cong W[\![t]\!],$$

where $W = W(\overline{\mathbb{F}}_p)$.

When a prime $p$ does divide the level, care must be taken to construct an integral model of $X(\Gamma)$ over $\mathbb{Z}_p$, and singularities begin to appear in the special fiber. The first investigation of the bad reduction of modular curves was carried out by Deligne-Rapoport [DR73], who constructed a model of $X_0(Np)$ over $W$ whose reduction is the union of two copies of $X_0(N)_{\overline{\mathbb{F}}_p}$ which meet transversely at the supersingular points.

This has the consequence that if $x \in X_0(Np)(\overline{\mathbb{F}}_p)$ is a supersingular point, then the completed local ring of $X_0(Np)$ at $x$ is

$$\hat{\mathcal{O}}_{X_0(Np),x} \cong W[\![t,u]\!]/(ut-p)$$

(note that this is a regular local ring).

The book of Katz-Mazur [KM85] constructs integral models of the modular curves $X(\Gamma)$ (for the familiar congruence subgroups $\Gamma$) by carefully defining moduli problems of elliptic curves with level structure. Note that the usual notion of level structure on an elliptic curve

[1]Apr. 30, 2013. Many thanks to Rebecca Bellovin, Kestutis Cesnavicius, and Chao Li for pointing out numerous errors.

$E$ (that is, a subgroup, point, or basis of $E[N]$) is problematic over schemes in characteristic $p$ which divide $N$. Katz and Mazur resolved this issue by using the notion of Drinfeld level structure.

Let $N \geq 5$ be prime to $p$, and let $X_n = X(\Gamma_1(N) \cap \Gamma(p^n))$. Then the Katz-Mazur model of $X_n$ over $W$ has special fiber equal to the union of smooth curves (called Igusa curves) which meet, once again, at the supersingular points.

But for large $n$, the singularities at the supersingular points are far from being ordinary double points. Which is to say that the completed local rings $\hat{\mathcal{O}}_{X_n,x}$ ($x$ supersingular) are more complicated than before, and don't seem to have any obvious presentation.

**Goal**. Give a description of the complete local ring

$$\hat{\mathcal{O}}_{X_\infty,x} := \text{ completion of } \left( \varinjlim_n \mathcal{O}_{X_n,x} \right).$$

Here the completion is taken with respect to the maximal ideal of $\mathcal{O}_{X_0,x}$ (or the maximal ideal of any particular $\mathcal{O}_{X_n,n}$, it doesn't matter).

This is a rather *ad hoc* definition, because we haven't defined the infinite-level modular curve $X_\infty$. But whatever $X_\infty$ is, the above seems like a reasonable definition for its completed local ring at $x$. As it turns out, despite being non-noetherian, $\hat{\mathcal{O}}_{X_\infty,x}$ has a rather simple description which makes it easier to work with than the finite level rings $\hat{\mathcal{O}}_{X_n,x}$.

## 2. Moduli of elliptic curves

2.1. **Basic definitions.** Modular curves are usually introduced as Riemann surfaces of the form $\Gamma\backslash\mathcal{H}$, where $\mathcal{H}$ is the upper half-plane and $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup (meaning it contains a principal congruence subgroup $\Gamma(N)$ for some integer $N$). This definition produces a perfectly good algebraic curve $Y(\Gamma)$ over $\mathbb{C}$ whose points correspond to elliptic curves with some extra structure. Then one adds a finite set of points to $Y(\Gamma)$ to produce a complete algebraic curve $X(\Gamma)$.

Since we are interested in the fine arithmetic of modular curves, the above definition isn't quite good enough. We need a model for $Y(\Gamma)$ over $\mathbb{Z}$, not $\mathbb{C}$ (or even $\mathbb{Q}$). Furthermore, this model ought to solve a *moduli problem* over general base schemes $S$, in the sense that morphisms from $S$ into $Y(\Gamma)$ should correspond to elliptic curves over $S$ with some additional structure. The construction of these models is the primary accomplishment of [KM85]. For many congruence subgroups

$\Gamma$, Katz and Mazur pose a moduli problem for elliptic curves and level structures which turns out to be representable much of the time.

Since elliptic curves are front and center of this story, it is appropriate to begin with the following definition:

**Definition 2.1.1.** *Let $S$ be a scheme, and let $f\colon E \to S$ be a morphism of schemes. Then $E/S$ is an* elliptic curve over $S$ *if $f$ is proper and smooth of relative dimension 1, such that the geometric fibers of $f$ are connected of genus 1. There must also be a special point $0 \in E(S)$, called the* zero section.

As expected, elliptic curves carry an abelian scheme structure. That is, for every scheme $T/S$, $E(T)$ can be given the structure of an (abelian) group in a way which is compatible with $S$-morphisms $T \to T'$. This is because $E(T)$ can be naturally identified with the relative Picard group $\mathrm{Pic}^0(E_T/T)$ (see Thm. 2.1.2 of [KM85]).

If $E/S$ is an elliptic curve, and $N \geq 1$ is an integer, we write $E[N]$ for the kernel (meaning the primage of the zero section) of the multiplication by $N$ map $E \to E$. This is a finite locally free group scheme of rank $N^2$ over $S$, which is étale if $N$ is invertible on $S$ (Thm. 2.3.1).

2.2. **A short aside on group schemes.** If you haven't dealt with finite group schemes before, here is a little informal perspective. A group scheme over a scheme $S$ is a scheme $G/S$ equipped with $S$-morphisms $G \times_S G \to G$, $e\colon S \to G$, and $i\colon G \to G$ which mimic the multiplication, identity, and inverse operations in a group.

This definition is a little dry, but it comes to life when we consider that whenever $T \to S$ is an $S$-scheme, the set $G(T)$ (this is the set of $S$-morphisms $T \to G$) becomes an honest *group*. Furthermore, whenever $T' \to T$ is an $S$-morphisms, we get a homomorphism of groups $G(T) \to G(T')$. Thus a group scheme gives us a contravariant functor $T \mapsto G(T)$ from the category of $S$-schemes to the category of groups. In fact, an equivalent definition of a group scheme is a functor from $S$-schemes to groups which happens to be representable (in which case the representing object $G$ is a group scheme as originally defined). The equivalence of these definitions is an exercise using Yoneda's lemma, which once mastered allows us to simultanously view $G$ as a functor and as a scheme in its own right. This sort of schizophrenia will be enormously useful when we consider other sorts of group-like objects (elliptic curves, $p$-divisible groups, formal groups, and so on).

Standard examples of groups schemes include the additive group $\mathbb{G}_a = \operatorname{Spec} \mathbb{Z}[T]$, and the multiplicative group $\mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[T, T^{-1}]$

(both considered as schemes over $\operatorname{Spec}\mathbb{Z}$). Whenever $R$ is a commutative ring, we have $\mathbb{G}_a(R) = R$ (as an abelian group, forgetting the ring structure) and $\mathbb{G}_m(R) = R^\times$. (Note that we have abbreviated $G(\operatorname{Spec} R)$ as $G(R)$ in these examples.) Also note that any (abstract) group $G$ can be considered as a *constant* group scheme $\underline{G}$ over a scheme $S$, by defining $\underline{G}$ to be the disjoint union of copies of $S$, one for each element of $G$. Finally, if $G$ is a group scheme over $S$, and $T \to S$ is an $S$-scheme, we write $G_T$ for the base change of $G$ to $T$. If $T = \operatorname{Spec} A$ is affine, we will abbreviate $G_{\operatorname{Spec} A}$ as $G_A$.

**Example 2.2.1** (The group scheme $\mu_N$)**.** Another important example of a group scheme is the kernel of the "$N$th power map" on $(\mathbb{G}_m)_A$, which is denoted $\mu_N$ (with the tacit understanding that the base scheme is $\operatorname{Spec} A$). As a scheme, we have $\mu_N = \operatorname{Spec} A[X]/(X^N - 1)$. Thus for an $A$-algebra $R$ we have $\mu_N(R) = \left\{x \in R | x^N = 1\right\}$, with its obvious structure as an abelian group. Since $\mu_N$ is finite over $\operatorname{Spec} A$, this makes $\mu_N$ a *finite group scheme*. Note that if $A$ is a $\mathbb{Z}[1/N]$-algebra which contains a primitive $N$th root of unity $\zeta$, then $G$ is isomorphic to the constant group scheme $\underline{\mathbb{Z}/N\mathbb{Z}}$. (Check that $A[X]/(X^N - 1)$ is isomorphic to the direct product $A^N$!) If $A$ is a $\mathbb{Z}[1/N]$-algebra which doesn't necessarily contain a primitive $N$th root of unity, then $\mu_N$ might not be constant, but after passing to an étale (unramified) extension $B/A$, $\mu_N$ does become constant. Thus over schemes on which $N$ is invertible, $\mu_N$ is *étale*, meaning that it becomes constant after passing to an étale extension of the base. One consequence of this is that $\mu_N$ seems to have the right number of "physical points": if $k$ is an $A$-algebra which is a field, then $\mu_N(k)$ has at most $N$ elements, and if $k$ is enlarged it will have exactly $N$ elements.

The behavior of $\mu_N$ over schemes on which $N$ is not invertible is quite different. As an extreme example, let $p$ be prime and consider $\mu_p$ as a group scheme over $\operatorname{Spec}\mathbb{F}_p$. Then if $K$ is a field containing $\mathbb{F}_p$, then $\mu_p(k) = 0$ no matter how large $k$ is. Thus $\mu_p/\mathbb{F}_p$ seems to suffer from a lack of physical points. (But please don't think that $\mu_p$ is simply the trivial group: over an $\mathbb{F}_p$-algebra with lots of nilpotents, like $R = \mathbb{F}_p[x]/x^p$, the group $\mu_p(R)$ will be nontrivial.) Over $\mathbb{F}_p$, $\mu_p$ is *connected*, meaning that its underlying topological space is connected.

For more on finite group schemes, consult the excellent article by Tate, [Tat97].

2.3. **The group schemes $E[N]$, and the Weil pairing.** Let $S$ be a scheme, and let $E/S$ be an elliptic curve. Then the kernel of multiplication by $N$ is a finite group scheme over $S$ denoted by $E[N]$. The

first thing to note is that, as with $\mu_N$, the nature of $E[N]$ is quite different depending on whether $N$ is invertible on $S$. If $N$ is invertible on $S$, then $E[N]$ is étale. This fact manifests in the property that $E[N]$ has the "right" number of points over an algebraically closed field. If $S = \operatorname{Spec} K$ is the spectrum of an algebraically closed field in which $N \neq 0$, then $E[N](K) \approx (\mathbb{Z}/N\mathbb{Z})^2$.

On the other hand, if $N = p$ is prime, and $S = \operatorname{Spec} K$ is the spectrum of a field of characteristic $p$, then $E[p]$ is *never* étale. Those familiar with the behavior of elliptic curves over such fields know that there are two possibilities:

$$E[p](\overline{K}) \approx \begin{cases} \mathbb{Z}/p\mathbb{Z}, & E \text{ is ordinary} \\ 0, & E \text{ is supersingular} \end{cases}$$

In the supersingular case, $E[p]$ is a connected finite group scheme. In the ordinary case, $E[p]$ is neither étale nor connected, but is rather a hybrid of the two cases.

Returning to the general case of an elliptic curve over an arbitrary base scheme $S$, an important property of the finite group scheme $E[N]$ is that it is *autodual*. This means that there is a $\mathbb{Z}/N\mathbb{Z}$-bilinear and alternating morphism

$$e_N \colon E[N] \times E[N] \to \mu_N,$$

known as the *Weil pairing*, which identifies $E[N]$ with the group scheme of $S$-group homomorphisms $E[N] \to \mathbb{G}_m$ (see §2.8 of [KM85]).

2.4. **The moduli problems $\Gamma(N)$ and $\Gamma_1(N)$.** Informally, a $\Gamma(N)$-structure (or "full level $N$ structure") on an elliptic curve $E/S$ is a pair of $N$-torsion points $P, Q \in E[N](S)$ which constitute a basis for the $(\mathbb{Z}/N\mathbb{Z})$-module $E[N](S)$. This definition suffices as long as $N$ is invertible on $S$, but is woefully inadequate otherwise. For instance if $p$ is prime and $E$ is an elliptic curve over a field $k$ of characteristic $p$, then $E[p](k)$ is an $\mathbf{F}_p$ vector space of dimension at most 1, so any pair $(P, Q)$ as above would have to be linearly dependent.

The correct definition is slightly more subtle, and involves the group of Cartier divisors on a scheme. Recall that a *Cartier divisor* on a scheme $X$ is a collection of rational functions $f_i$ on open affine sets $U_i$ which cover $X$, such that $f_i/f_j$ is regular on $U_i \cap U_j$ for all pairs $(i, j)$. (This is up to the obvious equivalence relation involving refinements of the open cover $\{U_i\}$.) A Cartier divisor is effective if the $f_i$ may all be taken to be regular. In this case the ideal sheaf generated by the $f_i$ cuts out a subscheme $Y$ of $X$ of codimension 1, and we write this divisor as $[Y]$.

**Definition 2.4.1.** *Let $E$ be an elliptic curve over a scheme $S$. A* $\Gamma(N)$-structure *on $E/S$ is a group homomorphism*

$$\phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N](S)$$

*such that we have an equality of effective Cartier divisors in $E$:*

$$E[N] = \sum_{a,b\in\mathbb{Z}/N\mathbb{Z}} [\phi(a,b)].$$

*A* $\Gamma_1(N)$-structure *on $E/S$ is a group homomorphism*

$$\phi\colon \mathbb{Z}/N\mathbb{Z} \to E[N](S)$$

*such that the effective Cartier divisor*

$$\sum_{a\in\mathbb{Z}/N\mathbb{Z}} [\phi(a)]$$

*is a subgroup scheme of $E[N]$.*

In the case that $N$ is invertible on $S$, so that $E[N]$ is an étale group scheme, one can show that a $\Gamma(N)$-structure on $E/S$ is simply a pair of linearly independent elements of $E[N]$, and that a $\Gamma_1(N)$-structure on $E/S$ is a point of $E[N]$ of exact order $N$. But when $N$ is not invertible, this simply cannot be the case. For instance, if $E$ is a supersingular elliptic curve over an algebraically closed field $k$ of characteristic $p$, then the map $\phi\colon (\mathbb{Z}/p\mathbb{Z})^2 \to E[p](k)$ which sends everything to 0 is a perfectly good (and in fact is the only) $\Gamma(p)$-structure on $E/k$. If $E$ is ordinary, then a $\Gamma(p)$-structure $\phi\colon (\mathbb{Z}/p\mathbb{Z})^2 \to E[p](k)$ will have to surject onto $E[p](k)$ (which has order $p$), but then there will necessarily be a kernel of order $p$.

We are now ready to define the moduli problems relevant to these lectures.

**Definition 2.4.2.** *Let $[\Gamma(N)]$ (resp, $[\Gamma_1(N)]$) denote the functor*[2] *which assigns to a scheme $S$ the set of elliptic curves $E/S$ together with a $\Gamma(N)$-structure (resp., $\Gamma_1(N)$) structure) on $E/S$.*

We are interested in the representability of these functors. For $[\Gamma]$ to be representable ($\Gamma = \Gamma(N)$ or $\Gamma_1(N)$), it would mean that there is a scheme $Y(\Gamma)$, an elliptic curve $\mathcal{E}/Y(\Gamma)$, and a $\Gamma$-structure $\phi$ on $\mathcal{E}/Y(\Gamma)$, such that for any scheme $S$, the function

$$\begin{aligned} \{\text{Morphisms } S \to Y(\Gamma)\} &\to \{\text{Elliptic curves}/S \text{ with } \Gamma\text{-structure}\} \\ f &\mapsto f^*(\mathcal{E}), \text{with } \Gamma\text{-structure induced by } \phi \end{aligned}$$

[2]This is not quite how $[\Gamma(N)]$ and $[\Gamma_1(N)]$ are defined in [KM85]; there, these symbols are used to represent functors on the moduli stack of elliptic curves.

is bijective.

It is not the case that these moduli problems are always representable. In fact $[\Gamma(1)]$ isn't even representable. The trouble is that elliptic curves always have automorphisms: every elliptic curve has an involution $[-1]$, and some elliptic curves have more automorphisms still. But it turns out that if the level structure is big enough, the situation becomes rigidified, and these moduli problems become representable. For instance, let $S$ be a connected scheme, let $E/S$ be an elliptic curve, and let $\phi$ be a $\Gamma_1(N)$-level structure on $E/S$. As long as $N \geq 5$, any automorphism of $E/S$ which preserves $\phi$ must be the identity ([KM85], Cor. 2.7.3).

In our study of modular curves over $\mathbb{Z}_p$, then, it will be useful to fix an auxiliary integer $N \geq 5$ which is prime to $p$, simply for the reason that it ensures that certain moduli problems are representable. Primarily we will be interested in the moduli problems $[\Gamma(p^n)]$ for $n \geq 0$, but we will run into a representability issue if $p^n \leq 2$. Therefore we define the moduli problem $[\Gamma_1(N) \cap \Gamma(p^n)]$ to be the functor which assigns to a $\mathbb{Z}_p$-scheme $S$ the set of elliptic curves $E/S$ together with a $\Gamma_1(N)$-structure *and* a $\Gamma(p^n)$-structure.

**Theorem 2.4.3.** *The moduli problem $[\Gamma_1(N) \cap \Gamma(p^n)]$ is representable by a regular scheme $Y_n$ of dimension 2 which is flat over $\operatorname{Spec} \mathbb{Z}_p$. The generic fiber $(Y_n)_{\mathbb{Q}_p}$ is a smooth curve.*

*Proof.* Let us briefly indicate where to look in [KM85]. There is a notion of "relatively representable" which we have not defined here, see (4.2). Roughly this means that the functor is representable modulo the problem with automorphisms of elliptic curves. It is shown (Thm. 5.1.1) that the moduli problems $[\Gamma_1(N)]$ and $[\Gamma(N)]$ are relatively representable and finite (hence affine) no matter what the value of $N$. Furthermore, it is shown (4.7) that relatively representable plus rigid plus affine means representable. It is also shown that (4.3.4) if $\mathcal{P}$ and $\mathcal{P}'$ are moduli problems, with $\mathcal{P}$ representable and $\mathcal{P}'$ relatively representable, then the simultaneous problem $\mathcal{P} \times \mathcal{P}'$ is representable. Applying this to $\mathcal{P} = [\Gamma_1(N)]$ and $\mathcal{P}' = [\Gamma(p^n)]$ shows that $[\Gamma_1(N) \cap \Gamma(p^n)]$ is representable. The regularity claim follows the same strategy as in the proof of Thm. 5.1.1. The claim about $(Y_n)_{\mathbb{Q}_p}$ follows from Cor. 4.7.2, which says that modular curves become smooth as soon as you invert every prime dividing the level. □

The scheme $Y_n$ admits automorphisms by the finite group $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$, since it acts on the moduli problem $[\Gamma(p^n)]$: an element $a \in \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$

acts on a pair $(E/S, \phi)$ as $(E/S, \phi \circ a)$. (Please note the difference between automorphisms of elliptic curves, which get in the way of representability, and automorphisms of the moduli problem, which certainly do not.)

2.5. **Geometrically connected components.** Suppose an $S$-point of $Y_n = Y(\Gamma_1(N) \cap \Gamma(p^n))$ represents an elliptic curve $E/S$, a point $P \in E[N](S)$, and a $\Gamma(p^n)$-structure $\phi\colon (\mathbb{Z}/p^n\mathbb{Z})^2 \to E[p^n](S)$. We have the Weil pairing

$$e_{p^n}\colon E[p^n] \times E[p^n] \to \mu_{p^n},$$

and so our $S$-point gives us an element

$$\zeta = e_{p^n}(\phi(1,0), \phi(0,1)) \in \mu_{p^n}(S).$$

We have therefore defined a morphism of schemes $e\colon Y_n \to \mu_{p^n}$ (recall that $\mu_{p^n}$ was the group scheme defined in Example 2.2.1)). This indicates that $Y_n$ is not *geometrically connected*; once we extend scalars to the field $K = \mathbb{Q}_p(\mu_{p^n})$, $Y_n$ will break up into a disjoint union of fibers of $e$ over the $p^n$th roots of unity in $\mu_{p^n}(K)$.

We'd rather work with geometrically connected schemes, so we'll do the following. Let $\zeta = \zeta_{p^n}$ be a primitive $p^n$th root of unity in $\mathcal{O}_K$, and let $Y_n^\zeta$ be the preimage of $\zeta$ under the map $(Y_n)_{\mathcal{O}_K} \to (\mu_{p^n})_{\mathcal{O}_K}$. Thus as a moduli problem, an $S$-point of $Y_n^\zeta$ (where $S$ is a scheme over $\mathcal{O}_L = \mathbb{Z}_p[\mu_{p^n}]$ corresponds to an elliptic curve $E/S$, a $\Gamma_1(N)$-structure on $E/S$, and a $\Gamma_{p^n}$-structure $\phi$ on $E/S$ for which $e_{p^n}(\phi(1,0), \phi(0,1)) = \zeta$.

It might be a good time to mention that if $\Gamma = \Gamma_1(N) \cap \Gamma(p^n)$ (as a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then $\Gamma\backslash\mathcal{H}$ isn't actually $Y_n(\mathbb{C})$, because the former is connected and the latter is disconnected. In fact $\Gamma\backslash\mathcal{H}$ is $Y_n^\zeta(\mathbb{C})$, where $\zeta = e^{2\pi i/p^n}$ (exercise!).

2.6. **The special fiber of $Y_n^\zeta$.** This section summarizes Chapter 13 of [KM85] concern the reductions modulo $p$ of various modular curves, applied to the case of our curve $Y_n^\zeta$.

There is a unique ring homomorphism $\mathbb{Z}_p[\zeta_{p^n}] \to \mathbb{F}_p$, given by $\zeta_{p^n} \mapsto 1$. Let us consider the special fiber of $Y_n^\zeta$, which is the base change of $Y_n^\zeta$ through $\mathbb{Z}_p[\zeta_{p^n}] \to \mathbb{F}_p$. For an $\mathbb{F}_p$-scheme $S$, a point of $(Y_n^\zeta)_{\mathbb{F}_p}$ over $S$ is an elliptic curve $E/S$ together with a point $P \in E[N](S)$ of order $N$ and a level structure

$$\phi\colon (\mathbb{Z}/p^n\mathbb{Z})^2 \to E[p^n](S),$$

such that $e_{p^n}(\phi(1,0), \phi(0,1)) = 1$. But since we are now in characterstic $p$, $\phi$ cannot be injective. It turns out that $\ker\phi$ must contain a line

$\ell \subset (\mathbb{Z}/p^n\mathbb{Z})^2$, by which I mean a free $\mathbb{Z}/p^n\mathbb{Z}$-submodule. This suggests that we can break up $(Y_n^\zeta)_{\mathbb{F}_p}$ according to which line (or lines!) are contained in $\ker\phi$. The set of such lines $\ell$ is denoted $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$.

For each line $\ell \in \mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$ we can define a moduli problem $Y_\ell$ (in characteristic $p$) which associates to $S$ the set of triples $(E/S, P, \phi)$ as above which satisfy $\ell \subset \ker\phi$. It turns out that this moduli problem is representable by a smooth affine curve over $\mathbb{F}_p$ which does not depend on the choice of $\ell$. This curve is called an Igusa curve and will be denoted $\mathrm{Ig}(p^n, N)$. (Actually, what we get here is something called an exotic Igusa curve, but the distinction will not concern us.) In brief, $\mathrm{Ig}(p^n, N)$ classifies elliptic curves $E$ in characteristic $P$ together with a point of order $N$ and a generator (in the sense of Cartier divisors) for the kernel of the Vershiebung map $V\colon E^{p^n} \to E$.

When $E/S$ is ordinary, $\ker\phi$ is exactly a line $\ell$, so that the point represented by $(E/S, P, \phi)$ lies on $Y_\ell$ and no other $Y_{\ell'}$. However, if $E/S$ is supersingular, then $\phi$ is necessarily the zero map. Therefore $(E/S, P, \phi)$ lies on *all* the $Y_\ell$! The following theorem summarizes the situation.

**Theorem 2.6.1** (adaptation of Thm. 13.7.6 of [KM85])**.** *The reduction mod $p$ of $Y_n^\zeta$ is a union of $p^{n-1}(p+1)$ smooth irreducible closed subvarieties $Y_\ell$, one for each line $\ell \in \mathbf{P}^1(\mathbb{Z}/p^n\mathbb{Z})$. Each $Y_\ell$ is isomorphic to the Igusa curve* $\mathrm{Ig}(p^n, N)$*. The $Y_\ell$ all meet simultaneously at the supersingular points of $Y_n^\zeta(\overline{\mathbb{F}}_p)$.*

This theorem tells us quite a bit about the geometry of $Y_n^\zeta$. The Igusa curves are fairly well-understood: their genera, and indeed their zeta functions, are amenable to computation. But then the neighborhoods of $Y_n^\zeta$ surrounding the singular points (which in this case are the supersingular points) are still rather mysterious. To study them, the standard thing to do is to choose a point $x \in Y_n^\zeta(\overline{\mathbb{F}}_p)$ and form the completed local ring $\hat{\mathcal{O}}_{Y_n^\zeta, x}$. Since $Y_n^\zeta$ was regular of dimension 2 to begin with, and regularity is preserved under localization and completion, $\hat{\mathcal{O}}_{Y_n^\zeta, x}$ is a 2-dimensional regular local ring. But it is quite difficult to give a presentation of $\hat{\mathcal{O}}_{Y_n^\zeta, x}$ directly. For this we shall need some understanding of $p$-divisible groups, especially those arising from elliptic curves over $p$-adic rings. That is the topic of the next section.

## 3. $p$-DIVISIBLE GROUPS

> It is possible to write endlessly on elliptic curves. (This is not a threat.)
>
> –Serge Lang

I don't mean to threaten you, dear reader, but **it is possible to write endlessly on $p$-divisible groups as well**. Many of the interesting features of elliptic curves (and abelian varieties) have analogues in the $p$-divisible world. Some examples:

| Elliptic curve phenomenon | $p$-divisible analogue |
|---|---|
| Elliptic curve $E$ | $p$-divisible group $G$, height 2 |
| Tate module $T_p(E)$ | Tate module $T(G)$ |
| CM by $K/\mathbb{Q}$ quadratic | CM by $K/\mathbb{Q}_p$ quadratic |
| $E$ supersingular | $G$ connected |
| Modular curves | Rapoport-Zink spaces |
| Modular forms | admissible reps. of $\mathrm{GL}_2(\mathbb{Q}_p)$ |

Abelian varieties are schemes with the structure of a $\mathbb{Z}$-module (abelian group), whereas $p$-divisible groups are schemes (actually ind-schemes) with the structure of a $\mathbb{Z}_p$-module. As we study the geometry of modular curves in a neighborhood of a point modulo $p$, $p$-divisible groups will start to move to the center of the discussion.

3.1. **Some motivation.** Let $E$ be an elliptic curve over a field $K$, and let $\ell$ be a prime unequal to the characteristic of $K$. Anyone who studies the arithmetic of elliptic curves eventually encounters the Tate module

$$T_\ell(E) = \varprojlim E[\ell^n](\overline{K}).$$

This is a free $\mathbb{Z}_\ell$-module of rank 2, and it comes equipped with an action of Galois:

$$\rho_\ell \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}\, T_\ell(E) \approx \mathrm{GL}_2(\mathbb{Z}_\ell).$$

If $K$ happens to be a local field (such as $\mathbb{Q}_p$) of residue characteristic $p \neq \ell$, then $\rho_\ell$ seems to "know" quite a bit about $E$. For instance, $\rho_\ell$ is unramified if and only if $E$ has good reduction, and the other types of reduction of $E$ are detected by $\rho_\ell$ as well. In the case of good reduction, $\rho_\ell$ factors through a representation of the Galois group of the residue field $k$ of $K$, and it determines the zeta function of the reduction of $E$. Futhermore, $\rho_\ell$ determines the isogeny class of the reduction of $E$ (by the Tate conjecture over finite fields).

But let's say we don't want two primes floating around. That is, we want to attach an object to $E$ which is $p$-adic rather than $\ell$-adic. Over a $p$-adic field, the Tate module $T_p(E)$ is going to be very ramified regardless of the reduction type of $E$ (although it is still quite interesting nonetheless). Over a finite field of characteristic $p$, $T_p(E)$ is going to

be quite inadequate, because it might be 0 if $E$ is supersingular. So instead, we use a stand-in for the $p$-adic Tate module: the sequence of finite group schemes $E[p]$, $E[p^2]$, etc. This sequence is the $p$-divisible group attached to $E$.

3.2. **Definitions.** We start with the definition of a $p$-divisible group over a ring.

**Definition 3.2.1.** *Let $p$ a prime and $h$ an integer, and let $R$ be a ring. A* $p$-divisible group *$G$ over $R$ (also called* Barsotti-Tate group*) of height $h$ is a directed system*

$$G = \varinjlim G_n = (G_1 \to G_2 \to \dots)$$

*of commutative finite flat group schemes $G_n$ over $R$, such that $G_n$ is a $p$-torsion group which is locally free of rank $p^{nh}$ and such that the inclusion $G_n \to G_{n+1}$ induces an isomorphism of $G_n$ onto $G_{n+1}[p^n]$.*

The most basic example of a $p$-divisible group is $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim \frac{1}{p^n}\mathbb{Z}/Z$, which has height 1 over whatever base. If $A$ is an abelian scheme of constant dimension $g$ over $R$, then $A[p^\infty] = \varinjlim A[p^n]$ is a $p$-divisible group of height $2g$.

We say $G$ is étale if each $G_n$ is étale. This means that after passing to some finite étale extension of $R$, $G_n$ becomes constant, but it may well be that no finite étale extension suffices to make all the $G_n$ constant. In contrast, $G$ is connected if each $G_n$ is.

One can also define the dimension of $G$, at least in the case that $R$ is a complete local noetherian ring whose residue field has characteristic $p$. In that case, we let $G_n^\circ$ be the connected component of $G_n$ containing the origin; then $G_n^\circ$ is a locally free group scheme, and $G^\circ = \varinjlim G_n^\circ$ is a $p$-divisible group. It turns out that $G^\circ$ arises from the $p$-power torsion in a *formal group* $\mathscr{G}$, and we set $\dim G = \dim \mathscr{G}$. This will be discussed in detail in §4.3. For now we just mention that $\dim G \le h$, and $\dim G = \dim G^\circ$.

If $G$ is a $p$-divisible group over a ring $A$ and $R$ is an $A$-algebra, we let $G(R) = \varinjlim G_n(R)$. In this way $G$ is a functor from the category of $A$-algebras to the category of torsion $\mathbb{Z}_p$-modules. (It is not the case that $G(R)$ has to be $p$-divisible as an abstract abelian group.)

**Example 3.2.2.** Let $\mu_{p^\infty} = \varinjlim \mu_{p^n}$ over a ring $A$. This is a $p$-divisible group of height 1. For any ring $R$, $\mu_{p^\infty}(R)$ is the group of roots of unity of $p$-power order in $R$. If $p$ is invertible in $R$, then $\mu_{p^\infty}$ is étale. But if $R = \mathbb{F}_p$, then $\mu_{p^\infty}$ is connected.

3.3. **$p$-divisible groups over a perfect field of characteristic $p$.** Over a perfect field $k$ of characteristic $p$, the category of $p$-divisible groups is very well understood in terms of semilinear algebra objects known as Dieudonné modules. Somewhat surprisingly, these objects live in characteristic 0. Let $W(k)$ be the ring of Witt vectors of $k$. If you aren't terribly familiar with these, it's best to keep these examples in mind: $W(\mathbb{F}_p) = \mathbb{Z}_p$, while $W(\overline{\mathbb{F}}_p)$ is the ring of integers in the completion of the maximal unramified extension of $\mathbb{Q}_p$. In any case, $W(k)$ is always a complete discrete valuation ring with $W(k)/pW(k) = k$. The association $k \mapsto W(k)$ is functorial in $k$. In particular, the $p$th power Frobenius automorphism $k \to k$ induces an automorphism $\sigma\colon W(k) \to W(k)$.

**Definition 3.3.1.** *The category of* finite free Dieudonné modules *over $W(k)$ has objects which are free $W(k)$-modules $M$ of finite rank equipped with a $\sigma$-linear endomorphism $F$ and a $\sigma^{-1}$-linear endomorphism $V$ satisfying $FV = p$ in* $\operatorname{End} M$*. (Here $\sigma$-linear means that $F(ax) = \sigma(a)F(x)$ for $a \in W(k)$, $x \in M$.) Morphisms between objects are $W(k)$-linear maps preserving $F$ and $V$. If $M$ is such a Dieudonné module, its* dual *is $M^\vee = \operatorname{Hom}_{W(k)}(M, W(k))$; the action of $F$ is by $(F\ell)(v) = \sigma(\ell(Vv))$, where $v \in M$, $\ell \in M^\vee$.*

**Theorem 3.3.2** (Dieudonné)**.** *Let $k$ be a perfect field of characteristic $p$.*

1. *$G \mapsto M(G)$ is an exact anti-equivalence between the category of $p$-divisible groups over $k$ and the category of finite free Dieudonné modules.*
2. *If $G$ has height $h$, then $M(G)$ is free of rank $h$.*
3. *The dimension of $G$ equals the dimension of $M(G)/FM(G)$ as a $k$-vector space.*
4. *$G$ is connected if and only if $F$ is topologically nilpotent on $M(G)$ (equivalently, that $F^n M(G) \subset pM(G)$ for $n$ large enough). $G$ is étale if and only if $F$ is bijective.*
5. *$G \mapsto M(G)$ commutes with base change in $k$.*

The following examples are important to keep in mind: For the constant $p$-divisible group $\mathbb{Q}_p/\mathbb{Z}_p$ over $\mathbb{F}_p$, we have $M(\mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Z}_p$ with $F = 1$ and $V = p$. For the multiplicative $p$-divisible group $\mu_{p^\infty}$, we have $M(\mu_{p^\infty}) = \mathbb{Z}_p$ with $F = p$ and $V = 1$. These two modules are dual to one another; this manifests the fact that $\mathbb{Q}_p/\mathbb{Z}_p$ and $\mu_{p^\infty}$ are Cartier dual to one another.

**Exercise 3.3.3.** *Let $k$ be an algebraically closed field of characteristic $p$. For each $h \geq 1$, show there is a unique connected 1-dimensional $p$-divisible group $\mathscr{G}$ over $k$ of height $h$.*

**Example 3.3.4.** Let $E/k$ be an elliptic curve over a perfect field $k$ of characteristic $p$, and let $E[p^\infty]$ be the associated $p$-divisible group. Then $E[p^\infty]$ has height 2 and dimension 1. $E[p^\infty]$ is connected if and only if $E$ is supersingular. Let us further assume that $k$ is algerbaically clsoed. If $E$ is supersingular, then $E[p^\infty]$ is the unique connected 1-dimensional $p$-divisible group of height 2. Its Diedonné module is $W(k)e_1 \oplus W(k)e_2$, where $Fe_1 = e_2$ and $Fe_2 = pe_1$. On the other hand if $E$ is ordinary, then one can use Dieudonné modules to show that

$$E[p^\infty] = \mathbb{Q}_p/\mathbb{Z}_p \oplus \mu_{p^\infty}.$$

3.4. **The Serre-Tate theorem.** Let $N \geq 5$, so that the moduli problem $[\Gamma_1(N)]$ is representable by a scheme $Y_1(N)$ which is smooth over $\operatorname{Spec} \mathbb{Z}[1/N]$. Let the point $x \in Y_1(N)(\overline{\mathbb{F}}_p)$ correspond to the pair $(E_0/\overline{\mathbb{F}}_p, P_0)$. We will be considering the moduli problem of deformations of $(E_0, P_0)$ to $W$-algebras, where $W = W(\overline{\mathbb{F}}_p)$. The Serre-Tate theorem says that deforming $E_0$ is tantamount to deforming the $p$-divisible group $E[p^\infty]$.

**Theorem 3.4.1** (see Thm. 2.9.1 in [KM85])**.** *Let $R$ be a ring, $I$ an ideal of $R$, $p$ a prime number. Assume that the ideal $(I, p)$ is nilpotent. Let $R_0 = R/I$. Let $\mathrm{Ell}_R$ denote the category of elliptic curves over $R$. Let $\mathcal{A}_R$ denote the category of triples $(E_0/R_0, G, \iota)$, where $E_0/R_0$ is an elliptic curve, $G/R$ is a $p$-divisible group, and*

$$\iota\colon E_0[p^\infty] \xrightarrow{\sim} G \otimes_R R_0$$

*is an isomorphism of $p$-divisible groups over $R_0$. A morphism between objects $(E_0/R_0, G, \iota)$ and $(E_0'/R_0, G', \iota')$ in $\mathcal{A}_R$ are pairs $(f_0, f)$, where $f_0\colon E_0 \to E_0'$ is a morphism of elliptic curves over $R_0$, and $f\colon G \to G'$ is a morphism of $p$-divisible groups over $R$ such that the obvious diagrams commute.*

*The functor $\mathrm{Ell}_R \to \mathcal{A}_R$ which sends $E/R$ to $(E \otimes_R R_0, E[p^\infty], \mathit{identity})$ is an equivalence of categories.*

The Serre-Tate theorem allows us to give a moduli interpretation for the completed local ring $\hat{\mathcal{O}}_{Y_1(N),x}$: it is the *deformation ring* of the $p$-divisible group $E_0[p^\infty]$.

**Proposition 3.4.2.** *Let $x$ correspond to the pair $(E_0, P)$ over $\overline{\mathbb{F}}_p$. Let $\mathcal{C}$ be the category of complete local noetherian $W$-algebras whose residue field is $\overline{\mathbb{F}}_p$. Let $\mathcal{F}\colon \mathcal{C} \to \mathrm{Sets}$ be the functor which assigns to $R$ the set of*

*isomorphism classes of pairs $(G, \iota)$, where $G$ is a $p$-divisible group over $R$ and $\iota\colon E_0[p^\infty] \to G \otimes_R \overline{\mathbb{F}}_p$ is an isomorphism of $p$-divisible groups over $\overline{\mathbb{F}}_p$. Then $\mathcal{F}$ is representable by the completed local ring $\hat{\mathcal{O}}_{Y_1(N),x}$.*

**Remark 3.4.3.** This interpretation of $\hat{\mathcal{O}}_{Y_1(N),x}$ shows that it does not depend on the $N$-torsion point $P$, nor does it even depend on the value of $N$! Really, then, the function of the auxiliary integer $N \geq 5$ is to ensure that the moduli problem $[\Gamma_1(N)]$ is representable. With a careful study of stacks, it would be possible to remove $N$ from the discussion.

**Remark 3.4.4.** Since $Y_1(N)$ is smooth over $W$, its completed local rings at points modulo $p$ are not very complicated:

$$\hat{\mathcal{O}}_{Y_1(N),x} \approx W[\![t]\!].$$

Thus by Prop. 3.4.2, the deformation ring of $p$-divisible group $E_0[p^\infty]$ is a formal power series ring in one variable over $W$. We will recover this result independently; see Thm. 4.6.1

*Proof.* Let $R$ be an object of $\mathcal{C}$, with maximal ideal $M$. Let us first assume that $M$ is nilpotent. For every pair $(G, \iota)$ in $\mathcal{F}(R)$, we have that the triple $(E_0, G, \iota)$ is an object in the category $\mathcal{A}_R$ of Thm. 3.4.1. By that theorem, there exists an elliptic curve $E/R$ such that $\iota\colon E_0[p^\infty] \to G \otimes_R \overline{\mathbb{F}}_p$ extends to an isomorphism $E[p^\infty] \to G$.

*Because $E[N]$ is étale over $R$*, the point $P_0 \in E[N](\overline{\mathbb{F}}_p)$ lifts uniquely to a point $P \in E[N](R)$ (this is essentially Hensel's lemma). We get a pair $(E, P)$ over $R$, where $E$ is a lift of $E_0$ to $R$. This data corresponds to a morphism $\operatorname{Spec} R \to Y_1(N)$ for which the diagram

$$\begin{array}{ccc} \operatorname{Spec} R & \longrightarrow & Y_1(N) \\ \uparrow & & \uparrow \\ \operatorname{Spec} \overline{\mathbb{F}}_p & \longrightarrow & \{x\} \end{array}$$

commutes. The morphism $\operatorname{Spec} R \to Y_1(N)$ localizes to a homomorphism of local $W$-algebras $\mathcal{O}_{Y_1(N),x} \to R$ (note that $\mathcal{O}_{\operatorname{Spec} R, M} = R$ because $R$ is already local). Thus as long as $M$ is nilpotent, pairs $(G, \iota)$ over $R$ give rise to homomorphisms $\mathcal{O}_{Y_1(N),x} \to R$. It is not hard to go in the other direction: If a homomorphism $\mathcal{O}_{Y_1(N),x} \to R$ is given, let $E/R$ be the push-forward of the universal elliptic curve, and use it to form the pair $(E[p^\infty], \text{identity})$.

For general objects $R$ of $\mathcal{C}$, we have $R = \varprojlim R/M^n$. A pair $(G, \iota)$ over $R$ corresponds to compatible family of such pairs over the $R/M^n$, which by the previous paragraph corresponds to a compatible family

of homomorphism of local $W$-algebras $\mathcal{O}_{Y_1(N),x} \to R/M^n$, which corresponds to a homomorphism $\hat{\mathcal{O}}_{Y_1(N),x} \to R$ in $\mathcal{C}$. □

What if we introduce $p$-power level structures into the picture? Let $Y_n$ be the scheme which represents the moduli problem $[\Gamma_1(N) \cap \Gamma(p^n)]$, and let $x \in Y_n(\overline{\mathbb{F}}_p)$ be a supersingular point. Consider the completed local ring $\hat{\mathcal{O}}_{Y_n,x}$. If $x$ is an ordinary point, then $Y_n$ is nonsingular at $x$, and once again we have $\hat{\mathcal{O}}_{Y_n,x} = W[\![t]\!]$. But if $x$ is supersingular, then $Y_n$ is singular at $x$ (possibly very badly so). Nonetheless we can give a moduli interpretation for the completed local ring $\hat{\mathcal{O}}_{Y_n,x}$ as the deformation of the connected $p$-divisible group $E[p^\infty]$ together with some sort of level structure. To make precise what such a level structure could mean, and to form the correct generalization of Prop. 3.4.2, we need to take a rather serious detour into the world of formal groups.

## 4. Formal groups and their deformation spaces

4.1. **Definitions.** A *one-dimensional commutative formal group law*[3] $\mathscr{G}$ over a commutative ring $A$ is a power series $\mathscr{G}(X,Y) \in A[\![X,Y]\!]$ satisfying the properties

- $\mathscr{G}(X,Y) = X + Y +$ higher order terms
- $\mathscr{G}(X,Y) = \mathscr{G}(Y,X)$
- $\mathscr{G}(\mathscr{G}(X,Y),Z) = \mathscr{G}(X,\mathscr{G}(Y,Z))$
- There exists $i(X) \in A[\![X]\!]$ with $\mathscr{G}(X,\iota(X)) = 0$

That is, $\mathscr{G}$ behaves like the addition law on an abelian group. (The existence of the inverse actually follows from the other axioms. Also, there is a notion of formal group laws of dimension $n$; for these, the $\mathscr{G}$ is $n$ power series in two sets of $n$ variables.) To stress the analogy we write $X +_{\mathscr{G}} Y$ for $\mathscr{G}(X,Y)$. The additive formal group law $\hat{\mathbb{G}}_{\mathrm{a}}$ is simply $X+Y$, while the multiplicative formal group law $\hat{\mathbb{G}}_{\mathrm{m}}$ is $X + Y + XY$. (This expression is $(1+X)(1+Y)-1$, and therefore represents multiplication for a parameter centered around 0 rather than 1.) Other formal group laws are much harder to make explicit. There is an evident notion of homomorphism $f\colon \mathscr{G} \to \mathscr{G}'$ between formal groups; this is a power series without constant term satisfying $f(X +_{\mathscr{G}} Y) = f(X) +_{\mathscr{G}'} f(Y)$. Then $\operatorname{End}\mathscr{G}$ is a (not necessarily commutative) ring. For $n \in \mathbb{Z}$ we write $[n]_{\mathscr{G}}(X)$ for the $n$-fold addition of $X$ with itself.

We can generalize slightly from formal groups to formal modules. Let $\mathcal{O}$ be a commutative ring, and let $A$ be an $\mathcal{O}$-algebra with structure map $\iota\colon \mathcal{O} \to A$, not presumed injective. A *formal $\mathcal{O}$-module law* over $A$ is a

[3]Also called: one-parameter formal Lie group. All the formal groups we consider will be commutative, so we will be dropping the "commutative" from now on.

formal group law $\mathscr{G}$ over $A$ together with a family of endomorphisms $[a]_{\mathscr{G}} \in \operatorname{End}\mathscr{G}$ for $a \in \mathcal{O}$ which together represent a homomorphism $\mathcal{O} \to \operatorname{End}\mathscr{G}$. It is required that $[a]_{\mathscr{G}}(X) = \iota(a)X + O(X^2)$; that is, the *derivative* of the action of $\mathcal{O}$ on $\mathscr{G}$ is just $\iota$.

**Example 4.1.1.** For example, $\hat{\mathbb{G}}_{\mathrm{a}}$ is a formal $A$-module over any $A$. Less trivially, the multiplicative formal group $\hat{\mathbb{G}}_{\mathrm{m}}$ becomes a formal $\mathbb{Z}_p$-module over $\mathbb{Z}_p$, because for $a \in \mathbb{Z}_p$ we have the endomorphism

$$[a]_{\hat{\mathbb{G}}_{\mathrm{m}}}(X) = (1+X)^a - 1 = \sum_{n=1}^{\infty} \binom{a}{n} X^n \in \mathbb{Z}_p[\![X]\!].$$

(Here $\binom{a}{n}$ is defined as $a(a-1)\cdots(a-(n-1))/n!$; this always lies in $\mathbb{Z}_p$.) Multiplication by $p$ is the polynomial $[p]_{\hat{\mathbb{G}}_{\mathrm{m}}}(X) = (1+X)^p - 1$, which has the property that $[p]_{\hat{\mathbb{G}}_{\mathrm{m}}}(X) \equiv X^p \pmod{p}$.

**Example 4.1.2.** Let $E$ be an elliptic curve over $A$. The formal completion $\hat{E}$ of $E$ at its origin carries the structure of a formal group over $A$. In fact, given a Weierstrass equation for $E$, one can give an algorithm for determining the addition law in $\hat{E}$. This process is described in Chapter IV of Silverman's book on elliptic curves, [Sil09].

4.2. **Lubin-Tate formal modules and local class field theory.** In [LT65], Lubin and Tate give the first spectacular application of formal groups and formal modules – they use them to give a proof of (the hard part of) local class field theory. Along the way, they give an algorithmic means of constructing nontrivial formal groups. We won't really need Lubin-Tate theory to get across the main point of these lectures, but they do provide the simplest nontrivial examples of formal groups and formal $\mathcal{O}$-modules.

Let $K$ be a nonarchimedean local field, so that $K$ is either a finite extension of $\mathbb{Q}_p$ or else it is isomorphic to $\mathbb{F}_q(\!(\pi)\!)$. Let $q = p^f$ be the cardinality of the residue field of $\mathcal{O}_K$. Lubin and Tate [LT65] construct formal $\mathcal{O}_K$-modules over $\mathcal{O}_K$ by starting with a choice of $[\pi]_{\mathscr{G}}$ and constructing $\mathscr{G}$ in the only consistent way possible. Let $f(X) \in \mathcal{O}_K[\![X]\!]$ be any power series satisfying the properties

- $f(X) = \pi X + O(X^2)$
- $f(X) \equiv X^q \pmod{\pi}$.

The following theorem isn't terribly hard, and is in fact a straightforward application of induction:

**Theorem 4.2.1.** *There exists a unique formal $\mathcal{O}_K$-module law $\mathscr{G}_f$ over $\mathcal{O}_K$ for which $[\pi]_{\mathscr{G}_f}(X) = f(X)$. Furthermore, if $g$ is another power series satisfying the two criteria above, then $\mathscr{G}_f$ and $\mathscr{G}_g$ are isomorphic.*

In particular, up to isomorphism is there is exactly one formal $\mathcal{O}_K$-module law for which multiplication by $\pi$ reduces to $X^q$ over the residue field.

**Example 4.2.2.** The easiest example is when $K = \mathbb{Q}_p$, and $f(X) = (1+X)^p - 1$. Then $\mathscr{G}_f$ is nothing but the formal multiplicative group $\hat{\mathbb{G}}_m$. An example in positive characteristic is given in Project A.

The formal $\mathcal{O}_K$-module $\mathscr{G}_f$ provided by the theorem is the *Lubin-Tate formal module*. It doesn't depend on $f$, so let us call it $\mathscr{G}$ (however note that it does depend on the choice of uniformizer $\pi$). For each $n \geq 1$, let $K_n$ denote the field obtained by adjoining the roots of the power series $[\pi]^n_{\mathscr{G}}(T)$. (By Weierstrass preparation for $\mathcal{O}_K[\![T]\!]$, $[\pi]^n_{\mathscr{G}}(T)$ equals a unit power series times a monic polynomial of degree $q^n$. So $K_n$ is the splitting field of this polynomial.) Lubin and Tate prove that $K_n/K$ is totally ramified and Galois with group $(\mathcal{O}_K/\pi^n)^\times$, which operates on $K_n$ by means of the $\mathcal{O}_K/\pi^n$-module structure of $\mathscr{G}[\pi^n]$. Furthermore, there is a connection to local class field theory. Let $K_\infty = \bigcup_n K_n$, and let $K^{\mathrm{nr}}$ be the maximal unramified extension of $K$. Then $K^{\mathrm{nr}}$ and $K_\infty$ are linearly disjoint, and $K^{\mathrm{ab}} = K^{\mathrm{nr}}K_\infty$ is the maximal abelian extension of $K$.

To summarize, *torsion in a Lubin-Tate formal module gives an explicit construction of abelian extensions of $K$.* This is the local analogue of an elliptic curve with complex multiplication by a quadratic imaginary field $K$, in which the torsion also produces abelian extensions of $K$.

4.3. **$p$-divisible formal groups.** Let $\mathscr{F}$ be a formal group (of whatever dimension) over a ring $A$. Let $\mathcal{A} = A[\![X_1, \ldots, X_d]\!]$ be the coordinate ring of $\mathscr{F}$. Multiplication by $p$ in $\mathscr{F}$ corresponds to a homomorphism $\psi\colon \mathcal{A} \to \mathcal{A}$. Similarly, there are homomorphisms $\psi_n\colon \mathcal{A} \to \mathcal{A}$ corresponding to multiplication by $p^n$ for $n = 1, 2, \ldots$.

**Definition 4.3.1.** *The formal group $\mathscr{F}$ is* $p$-divisible *if $\psi$ makes $\mathcal{A}$ into a locally free module over itself.*

**Example 4.3.2.** The formal multiplicative group $\hat{\mathbb{G}}_m$ is $p$-divisible (exercise!). On the other hand, if $p$ is not a unit in $A$, then the formal additive group $\hat{\mathbb{G}}_a$ is not $p$-divisible.

If $\mathscr{F}$ is $p$-divisible, then let $\mathscr{F}[p^n]$ denote the kernel of multiplication by $p^n$ in $\mathscr{F}$. That is,

$$\mathscr{F}[p^n] = \operatorname{Spec} \frac{A[\![X_1, \dots, X_d]\!]}{(\psi_n(X_1), \dots, \psi_n(X_d))}$$

together with the group operations induced from $\mathscr{F}$. It can be shown that $\mathscr{F}[p^n]$ is a locally free groups scheme over $A$. Passing to the injective limit, we get a $p$-divisible group $\mathscr{F}[p^\infty] = \varinjlim \mathscr{F}[p^m]$.

**Example 4.3.3.** The $p$-divisible group associated to $\hat{\mathbb{G}}_m$ is $\mu_{p^\infty}$.

**Theorem 4.3.4** (Thm. 1 of [Tat67])**.** *Let $A$ be a complete noetherian local ring of residue characteristic $p$. Then $\mathscr{F} \mapsto \mathscr{F}[p^\infty]$ is an equivalence between the category of $p$-divisible formal groups over $A$ and the category of connected $p$-divisible groups over $A$.*

Over a ring $A$ satisfying the hypotheses of Thm. 4.3.4, we may now define the dimension of a $p$-divisible group $G$ as follows: let $G^\circ$ be its connected component, and let $\mathscr{F}$ be the formal group with $\mathscr{F}[p^\infty] = G^\circ$. Then $\dim G = \dim \mathscr{F}$.

The hard part of Thm. 4.3.4 is the essential surjectivity of $\mathscr{F} \mapsto \mathscr{F}[p^\infty]$. If $G$ is a connected $p$-divisible group, let $\mathcal{A}_n$ be the coordinate ring of $G[p^n]$. The gist of the proof is that $\mathcal{A}_n$ is a Hopf algebra of the form

$$A[X_1, \dots, X_d]/I_n$$

for some ideal $I_n$. Taking the inverse limit as $n \geq \infty$ produces an "unobstructed" power series ring $A[\![X_1, \dots, X_d]\!]$, which then inherits the structure of a topological Hopf algebra, which amounts to saying that we have a formal group (of dimension $d$).

We remark that the dimension of a $p$-divisible group $G$ is a rather mysterious invariant–it certainly isn't as transparent as the height. One convenient fact is that if $A$ is an abelian variety, then $A[p^\infty]$ is a $p$-divisible group of the same dimension as $A$. Also, if $G$ is a $p$-divisible group over a perfect field, with Dieudonné module $M(G)$, then we have the formula

$$\dim G = M(G)/FM(G).$$

In particular

$$\begin{aligned} \dim \mathbb{Q}_p/\mathbb{Z}_p &= 0 \\ \dim \mu_{p^\infty} &= 1 \end{aligned}$$

4.4. **Invariant differential forms, logarithms, and $p$-typical formal groups.** Let $\mathscr{G}$ be a 1-dimensional formal group law over a commutative ring $A$. The space of *differential forms* on $\mathscr{G}$ is the $A$-module $\Omega^1_{\mathscr{G}/A}$ of formal differentials $P(T)dT$, where $P(T) \in A[\![T]\!]$.

Let $\Sigma\colon A[\![T]\!] \to A[\![X,Y]\!]$ be the unique homomorphism of topological $A$-algebras which sends $T$ to $X +_{\mathscr{G}} Y$. Also let $\mathrm{pr}_1, \mathrm{pr}_2\colon A[\![T]\!] \to A[\![X,Y]\!]$ be the maps which send $T$ to $X$ and $Y$, respectively. The maps $\Sigma$, $\mathrm{pr}_1$, and $\mathrm{pr}_2$ all induce $A$-linear maps $\Omega^1_{\mathscr{G}} \to \Omega^1_{\mathscr{G}\times\mathscr{G}}$.

**Definition 4.4.1.** *A differential form $\omega \in \Omega^1_{\mathscr{G}/A}$ is* translation invariant *if $\Sigma(\omega) = \mathrm{pr}_1(\omega) + \mathrm{pr}_2(\omega)$. Invariant differentials form an $A$-submodule of $\Omega^1_{\mathscr{G}/A}$.*

**Lemma 4.4.2.** *The module of invariant differentials is a free $A$-module of rank 1, spanned by*

$$\omega = \left[\frac{\partial}{\partial X}\mathscr{G}(X,Y)|_{(X,Y)=(0,T)}\right]^{-1} dT$$

*Proof.* See [Sil09], Prop. 4.2. We remark that there is a version of this lemma for higher-dimensional formal groups as well. □

**Examples 4.4.3.** *For the additive formal group this works out to $\omega = dT$. For the multiplicative formal group, this is $\omega = dT/(1+T)$.*

If $A$ is flat over $\mathbb{Z}$, so that $A$ injects into $A \otimes \mathbb{Q}$, we can construct the *formal logarithm* of $\mathscr{G}$ by

$$\log_{\mathscr{G}}(T) = \int \omega \in (A \otimes \mathbb{Q})[\![T]\!],$$

where we choose the antiderivative in such a way that $\log_{\mathscr{G}}(0) = 0$. For instance, $\log_{\hat{\mathbb{G}}_{\mathrm{m}}}(T) = \int (1+T)^{-1} dT \in \mathbb{Q}[\![T]\!]$ is the series that represents $\log(1+T)$.

The logarithm $\log_{\mathscr{G}}$ is an isomorphism between $\mathscr{G}_{A\otimes\mathbb{Q}}$ and $\hat{\mathbb{G}}_{\mathrm{a}}$. Thus whenever $A$ is a $\mathbb{Q}$-algebra, all one-dimensional commutative formal groups over $A$ are isomorphic to the additive formal group.

Let $\exp_{\mathscr{G}}(T) \in (A\otimes\mathbb{Q})[\![T]\!]$ be the power series which inverts $\log_{\mathscr{G}}(T)$, so that $\log_{\mathscr{G}} \exp_{\mathscr{G}}(T) = T$. We have

$$X +_{\mathscr{G}} Y = \exp_{\mathscr{G}}(\log_{\mathscr{G}}(X) + \log_{\mathscr{G}}(Y)) \tag{4.4.1}$$

as an identity of power series in $(A\otimes\mathbb{Q})[\![X,Y]\!]$. This shows that $\log_{\mathscr{G}}(T)$ actually determines $\mathscr{G}$.

This suggests constructing (and classifying) formal groups by the form of their logarithms. Of course, not every power series in $(A \otimes \mathbb{Q})[\![T]\!]$ is the logarithm of a formal group. But there is a special class

of formal groups (in fact they are formal $\mathbb{Z}_p$-modules) whose logarithms can be made explicit (or at least can be defined through a simple recursion). These are known as the $p$-typical formal groups; the theory is due to Hazewinkel, [Haz78].

Let $A = \mathbb{Z}_p[\mathbf{v}]$ be the polynomial ring in an infinite number of variables $v_1, v_2, \dots$ over $\mathbb{Z}_p$. Let $f(T)$ be the unique power series in $(A \otimes \mathbb{Q}_p)[\![T]\!]$ which satisfies

$$f(T) = T + \sum_{k=1}^{\infty} \frac{v_i}{p} f^{p^i}(T^{p^i})$$

where $f^{p^j}$ is the power series obtained from $f(T)$ by replacing each $v_i$ with $v_i^{p^j}$. The expansion of $f(T)$ is

$$f(T) = \sum_{i=0}^{\infty} b_i T^{p^i} = T + \frac{v_1}{p} T^p + \left( \frac{v_2}{p} + \frac{v_1^{p+1}}{p^2} \right) T^{p^2} + \dots .$$

The coefficients $b_i$ are determined recursively by the rules

$$\begin{aligned} b_0 &= 1 \\ pb_i &= b_0 v_i + b_1 v_{i-1}^p + b_2 v_{i-2}^{p^2} + \dots + b_{i-1} v_1^{p^{i-1}}. \end{aligned}$$

**Theorem 4.4.4** ([Haz78], 21.5)**.** (1) *There exists a unique formal $\mathbb{Z}_p$-module $\mathscr{G}^{p\text{-}univ}$ over $\mathbb{Z}_p[\mathbf{v}]$ for which $\log_{\mathscr{G}^{p\text{-}univ}}(T) = f(T)$.*

(2) *Let $\mathscr{G}$ be a formal $\mathbb{Z}_p$-module over some $\mathbb{Z}_p$-algebra $R$. Then there exists a homomorphism $\mathbb{Z}_p[\mathbf{v}] \to R$ such that $\mathscr{G}$ is isomorphic to $\mathscr{G}^{p\text{-}univ} \otimes_{\mathbb{Z}_p[\mathbf{v}]} R$.*

Any formal $\mathbb{Z}_p$-module over a ring $R$ which arises from $\mathscr{G}^{p\text{-univ}}$ via base change is called *$p$-typical*. For its part, $\mathscr{G}^{p\text{-univ}}$ is the *universal $p$-typical formal $\mathbb{Z}_p$-module*. If $R$ is $\mathbb{Z}_p$-flat, then $\mathscr{G}$ being $p$-typical means exactly that its logarithm takes the form

$$\log_{\mathscr{G}}(T) = T + \sum_{i=1}^{\infty} a_i T^{p^i}, \ a_i \in R \otimes \mathbb{Q}_p.$$

The second part of the theorem states that every formal $\mathbb{Z}_p$-module is isomorphic to a $p$-typical one.

**Example 4.4.5.** Let $h \geq 1$, and let $\mathscr{G} = \mathscr{F} \otimes_{\mathbb{Z}_p[\mathbf{v}]} \mathbb{Z}_p$, where $\mathbb{Z}_p[\mathbf{v}] \to \mathbb{Z}_p$ is the homomorphism

$$v_i \mapsto \begin{cases} 1, & i = h \\ 0, & i \neq h \end{cases}.$$

Then $\mathscr{G}$ is the unique formal $\mathbb{Z}_p$-module over $\mathbb{Z}_p$ with logarithm

$$\log_{\mathscr{G}}(T) = T + \frac{T^{p^h}}{p} + \frac{T^{p^{2h}}}{p^2} + \dots.$$

Note that if $K/\mathbb{Q}_p$ is the unramified extension of degree $h$, so that $K$ is the splitting field for $X^{p^h} - X$, then $\mathscr{G} \otimes \mathcal{O}_K$ becomes a formal $\mathcal{O}_K$-module in such a way that $[\alpha]_{\mathscr{G}}(T) = \alpha T$ whenever $\alpha$ is a root of $X^{p^h} - X$. In fact, $\mathscr{G}$ is a Lubin-Tate formal $\mathcal{O}_K$-module (exercise!).

4.5. **Formal groups: functorial definition.** Recall our "schizophrenic" approach to group schemes: If $G/S$ is a group scheme, then $G$ can be viewed in two ways at once:

(1) $G$ is a group object in the category of $S$-schemes.
(2) $G$ is a representable functor from the category of $S$-schemes to the category of groups.

We will need to take a similar approach to formal groups. This will require viewing formal groups as geometric objects. Unsurprisingly, formal groups are group objects in the category of formal schemes. Let us give a brief review of formal schemes.

**Definition 4.5.1.** *A topological ring $R$ is* adic *if there exists an ideal $I \subset R$ such that $R$ is separated and complete for the $I$-adic topology. This means that $\{I^n\}_{n\geq 1}$ is a system of open neighborhoods of 0 in $R$, and that we have an isomorphism of rings $R \cong \varprojlim R/I^n$. Such an $I$ is an* ideal of definition *for $R$. If $R$ is an adic ring, an* adic $R$-algebra *$S$ is an adic ring together with a continuous homomorphism $R \to S$. Let* $\mathrm{Adic}_R$ *denote the category of adic $R$-algebras (with continuous $R$-homomorphisms as morphisms).*

Examples include:

- Any ring $A$, when given the discrete topology, becomes an adic ring with ideal of definition 0 (or any nilpotent ideal).
- $\mathbb{Z}_p$ is an adic ring with ideal of definition $p\mathbb{Z}_p$, but $p^n\mathbb{Z}_p$ is also an ideal of definition for any $n \geq 1$.
- For any adic ring $A$ with ideal of definition $I$, the power series ring $A[\![X_1, \dots, X_n]\!]$ is an adic $A$-algebra. An ideal of definition is given by $(I, X_1, \dots, X_n)$. Please note that there are many other possible ideals of definition (for instance $(I^{a_0}, X_1^{a_1}, \dots, X_n^{a_n})$ for any positive integers $a_0, a_1, \dots, a_n$). The set of ideals of definition is not necessarily the set of powers of a particular ideal. (Nor does an adic ring have to be a local ring.)

If $A$ is an adic ring, the *formal spectrum* of $A$ is the set $\mathrm{Spf}\, A$ of open prime ideals of $A$. If $I$ is an ideal of definition, then $\mathrm{Spf}\, A$ may be identified with $\mathrm{Spec}\, A/I$ (exercise!). $\mathrm{Spf}\, A$ is endowed with the structure of a topologically ringed space in a straightforward way. Topologically ringed spaces isomorphic to some $\mathrm{Spf}\, A$ are *affine formal schemes*, and *formal schemes* are topologically ringed spaces which are locally isomorphic to affine formal schemes. This is perhaps a hasty introduction to formal schemes, but all we really need for the moment is that *the category of affine formal schemes is opposite to the category of adic rings.* Similarly, if $A$ is an adic ring, the category of affine formal schemes over $\mathrm{Spf}\, A$ is opposite to the category of adic $A$-algebras.

For an adic $A$-algebra $R$, let $\mathrm{Nil}(R)$ be the set of elements of $R$ which are topologically nilpotent. If $J$ is an ideal of definition of $R$, then the set of topologically nilpotent elements is the radical $\sqrt{J}$ of $J$. The map $R \mapsto \mathrm{Nil}(R)$ is a functor $\mathrm{Adic}_A \to \mathrm{Sets}$, which is representable (exercise!) by $A[\![T]\!]$.

Now let $A$ be an adic ring, and let $\mathscr{G}$ be a formal group over $A$, which we take to be 1-dimensional (keeping in mind that everything that follows generalizes to arbitrary dimension). Let $\mathcal{A} = A[\![T]\!]$. The addition law on $\mathscr{G}$ turns $\mathcal{A}$ into a topological Hopf $A$-algebra: there is a continuous homomorphism of topological $A$-algebras $\mathcal{A} \to \mathcal{A}\hat{\otimes}\mathcal{A} \cong A[\![X, Y]\!]$ which sends $T$ to $X +_{\mathscr{G}} Y$. Let $\mathscr{G}$ *also* denote the formal scheme $\mathrm{Spf}\, \mathcal{A}$. Then $\mathscr{G}$ is a group object in the category of affine formal schemes: we have an addition law $\mathscr{G} \times \mathscr{G} \to \mathscr{G}$ which satisfies the appropriate axioms.

It is also important to be able to view $\mathscr{G}$ as a functor. If $R$ is an adic $A$-algebra, then let $\mathscr{G}(R)$ be (as one would expect) the set of morphisms $\mathrm{Spf}\, R \to \mathrm{Spf}\, \mathscr{G}$ over $\mathrm{Spf}\, A$. This is the same as the set of continuous $A$-linear homomorphisms $\mathcal{A} \to R$, and therefore it gets identified with $\mathrm{Nil}(R)$. The group operation on $\mathscr{G}$ turns $\mathrm{Nil}(R)$ into an abelian group. Indeed, if $f, g \in \mathrm{Nil}(R)$ then the sum $f +_{\mathscr{G}} g$ converges in $R$ (since $R$ is complete), and this is precisely the group operation we mean.

Thus $\mathscr{G}$ is a functor from $\mathrm{Adic}_A$ to the category Ab of abelian groups. It just so happens that the composition $\mathrm{Adic}_A \to \mathrm{Ab} \to \mathrm{Sets}$ (where the second arrow is the forgetful functor) is isomorphic to Nil

In summary, there are (at least) three ways of looking at a 1-dimensional formal group $\mathscr{G}$ over an adic ring $A$:

- $\mathscr{G}$ is a power series in two variables over $A$ which mimics the behavior of an abelian group.
- $\mathscr{G}$ is a group object in the category of affine formal schemes over $\mathrm{Spf}\, A$, which is isomorphic to $\mathrm{Spf}\, A[\![T]\!]$,

- $\mathscr{G}$ is a functor $\mathrm{Adic}_A \to \mathrm{Ab}$, such that the composition $\mathrm{Adic}_A \to \mathrm{Ab} \to \mathrm{Sets}$ is isomorphic to Nil.

I feel obliged to mention that the latter two definitions can be made slightly more general by adding the phrase "locally on Spf $A$".

If $\mathscr{G}$ is $p$-divisible, then the functor $\mathscr{G}\colon \mathrm{Adic}_A \to \mathrm{Ab}$ can be recovered from the $p$-divisible group $G = \mathscr{G}[p^\infty]$ as follows. Whenever $R$ is an adic $A$-algebra with ideal of definition $J$ containing $p$, we have

$$\mathscr{G}(R) = \varprojlim_n \varinjlim_m G_m(R/J^n).$$

To get your head around this, it might be good to work through the example of $\mathscr{G} = \hat{\mathbb{G}}_m$ and $G = \mu_{p^\infty}$.

4.6. **Deformation rings for formal groups.** Let $x$ be a supersingular point of the modular curve $Y_1(N)(\overline{\mathbb{F}}_p)$ corresponding to the pair $(E_0, P)$. By Prop. 3.4.2, the completed local ring $\hat{\mathcal{O}}_{Y_1(N),x}$ may be interpreted as a deformation ring for the $p$-divisible group $G = E_0[p^\infty]$. This fact motivates the study of deformation problems for $p$-divisible groups in general, which turns out to be a very exciting and active subject.

In the case at hand, the $p$-divisible group is connected (because $E_0$ is supersingular); recall from 4.3.4 that the category of connected $p$-divisible groups is isomorphic to the category of $p$-divisible formal groups. Thus to deform $G$ is to deform the formal group $\hat{E}_0$. Lubin and Tate [LT66] showed that if $\mathscr{G}_0$ is a one-dimensional formal group over $\overline{\mathbb{F}}_p$ (such as $\hat{E}_0$), then the deformation ring of $\mathscr{G}_0$ is a formal power series ring over $W = W(\overline{\mathbb{F}}_p)$ in $h-1$ variables, where $h$ is the height of $\mathscr{G}_0$. This theorem is reviewed below. Geometrically speaking, the deformation space of $G$ is an open ball $\mathscr{M}$ of dimension $h-1$.

Fix an integer $h \geq 1$. Let $\mathscr{G}_0/\overline{\mathbb{F}}_p$ be a 1-dimensional $p$-divisible formal group of height $h$. (In fact $\mathscr{G}_0$ is unique up to isomorphism, by Exercise 3.3.3.) Let $W = W(\overline{\mathbb{F}}_p)$. Let $\mathcal{C}$ be the category of complete local noetherian $W$-algebras with residue field $\overline{\mathbb{F}}_p$. Let $M_0$ be the functor $\mathcal{C} \to \mathrm{Sets}$ which assigns to $A$ the set of isomorphism classes of pairs $(\mathscr{G}, \iota)$, where $\mathscr{G}$ is a one-dimensional formal group over $A$ and $\iota\colon \mathscr{G}_0 \to \mathscr{G} \otimes_A \overline{\mathbb{F}}_p$ is an isomorphism.

The role of $\iota$ in this deformation problem is quite important. If instead we had defined $M_0$ to parametrize isomorphism classes of 1-dimensional formal groups $\mathscr{G}$ whose reduction has height $h$, then $M_0$ would act very stacky, because such $\mathscr{G}$ have many automorphisms (by $\mathbb{Z}_p^\times$ at least). The isomorphism $\iota$ rigidifies the situation, because any

automorphism of $\mathscr{G}$ which reduces to the identity on $\mathscr{G} \otimes \overline{\mathbb{F}}_p$ must be the identity.

**Theorem 4.6.1** ([LT66])**.** *$M_0$ is representable by an $W$-algebra $A_0$ which is (non-canonically) isomorphic to a power series ring in $h-1$ variables:*

$$A \approx W[\![u_1, \dots, u_{h-1}]\!].$$

**Remark 4.6.2.** The theorem can be generalized to the case of formal $\mathcal{O}_K$-modules, where $K$ is any nonarchimdean local field.

**Remark 4.6.3.** When $h = 1$ the theorem is interpreted to mean that $\mathcal{M}_0$ is a single point in characteristic 0. That is, there is a unique lift of $\mathscr{G}_0$ (none other than the Lubin-Tate formal module).

The theorem implies that there is a *universal formal group* $\mathscr{G}^{\mathrm{univ}}$ over $W[\![u_1, \dots, u_{h-1}]\!]$, together with an isomorphism $\iota^{\mathrm{univ}}$ from $\mathscr{G}_0$ onto $\mathscr{G}^{\mathrm{univ}} \otimes k$. Since $A_0$ is a $\mathbb{Z}_p$-algebra, $\mathscr{G}^{\mathrm{univ}}$ naturally becomes a formal $\mathbb{Z}_p$-module. We have seen that every formal group is isomorphic to a $p$-typical formal group, and so (up to a change of variable) $\mathscr{G}^{\mathrm{univ}}$ must arise via base change from the universal $p$-typical formal group $\mathscr{G}^{p\text{-univ}}$ from §4.4.4 through a ring homomorphism $\mathbb{Z}_p[\mathbf{v}] \to W[\![u_1, \dots, u_{h-1}]\!]$. This homomorphism is defined by

$$\begin{aligned} v_1 &\mapsto u_1 \\ v_2 &\mapsto u_2 \\ &\vdots \\ v_{h-1} &\mapsto u_{h-1} \\ v_h &\mapsto 1 \\ v_{h+1} &\mapsto 0 \\ v_{h+2} &\mapsto 0 \\ &\vdots \end{aligned}$$

(see [GH94], (12.3).)

By the formulas given in §4.4, we can compute (at least recursively) the formal logarithm of $\mathscr{G}^{\mathrm{univ}}$, which then allows us to compute the addition law in $\mathscr{G}^{\mathrm{univ}}$ via Eq. (4.4.1). But the result would be quite complicated, even in the case $h = 2$, and I don't recommend carrying it out!

4.7. **Drinfeld level structures on formal groups, and Drinfeld's deformation rings.** Suppose $A$ is an adic $\mathbb{Z}_p$-algebra, and let $\mathscr{G}$ be a $p$-divisible formal group of height $h$ over $A$. Drinfeld introduced the

following notion in [Dri74], which was then adapted by Katz-Mazur in the context of elliptic curves.

**Definition 4.7.1.** *Let $R$ be an adic $A$-algebra. A* Drinfeld level $p^n$ structure *on $\mathscr{G}(R)$ is a homomorphism*

$$\phi\colon (\mathbb{Z}/p^n\mathbb{Z})^{\oplus h} \to \mathscr{G}(R)$$

*for which the relation*

$$[p]_{\mathscr{G}}(T) \;\Big|\; \prod_{x\in(p^{n-1}\mathbb{Z}/p^n\mathbb{Z})^{\oplus h}} (T-\phi(x))$$

*holds in $R[\![T]\!]$. If $\phi$ is a Drinfeld level $p^n$ structure, the images under $\phi$ of the standard basis vectors in $(\mathbb{Z}/p^n\mathbb{Z})^{\oplus h}$ form a* Drinfeld basis *of $\mathscr{G}[p^n](R)$.*

Let $M_n$ be the functor $\mathcal{C} \to$ Sets which assigns to $R$ the set of triples $(\mathscr{G}, \iota, \phi)$, where $(\mathscr{G}, \iota) \in M_0(R)$ and $\phi$ is a Drinfeld level $p^n$ structure on $\mathscr{G}/R$. Drinfeld shows that $M_n$ is representable by a local ring $A_n$. $\mathscr{G}^{\mathrm{univ}}[p^n](A_n)$ has a universal Drinfeld basis $X_1^{(n)}, \dots, X_h^{(n)}$. Drinfeld shows that $A_n$ is a regular local ring with parameters $X_1^{(n)}, \dots, X_h^{(n)}$.

The case of height 1 is particularly important.

**Lemma 4.7.2.** *Suppose that $\mathscr{G}_0$ has height 1 (so that it is isomorphic to $\hat{\mathbb{G}}_m$). Then $M_n$ is representable by $W[\mu_{p^n}]$.*

*Proof.* By Lubin-Tate theory, $\mathscr{G}_0$ admits a unique lift to any object in $\mathcal{C}$ (namely the multiplicative group). Let $R \in \mathcal{C}$. The set $M_n(R)$ is the set of Drinfeld bases for $\hat{\mathbb{G}}_m[p^n](R) = \mu_{p^n}(R)$. The condition for $x \in \mu_{p^n}(R)$ to be a Drinfeld basis is the condition that $\prod_{a=0}^{p-1}(T - x^{p^{n-1}a})$ be divisible by $T^p - 1$ in $R[\![T]\!]$. This condition is equivalent (exercise!) to the condition that $x$ be a *primitive* $p^n$th root of unity; that is, $x$ needs to be a root of the $p^n$th cyclotomic polynomial. The set of such $x$ may be identified with the set of $W$-homomoprhisms $W[\mu_{p^n}] \to R$. □

**Remark 4.7.3.** The example of height 1 shows the core idea of a Drinfeld level structure: it is in a sense the right way to generalize the notion of a primitive root of unity. Over a base ring $R$ over which $p$ is not invertible, it's not a good idea to define a "primitive $p^n$th root of unity" as an element $\zeta$ of exact order $p^n$ in $R^\times$, since this property isn't stable under homomorphisms $R \to S$. Rather, $\zeta$ should be considered a primitive $p^n$th root of unity when it is a root of the $p^n$th cyclotomic polynomial $\Phi_{p^n}(T)$; it is this condition that is generalized by the notion of a Drinfeld level structure.

Now we turn to the case of formal groups of height 2. Recall that $Y_n$ is the scheme which represents the moduli problem $[\Gamma_1(N) \cap \Gamma(p^n)]$; let us consider $Y_n$ as a scheme over $\operatorname{Spec} W$.

**Proposition 4.7.4.** *Let $n \geq 0$, and let $x$ be a supersingular point in $Y_n(\overline{\mathbb{F}}_p)$. Let $A_n$ be the deformation ring of a formal group of dimension 1 and height 2 over $\overline{\mathbb{F}}_p$. Then the completed local ring $\hat{\mathcal{O}}_{Y_n,x}$ is isomorphic to $A_n$.*

*Proof.* Let $x$ represent the pair $(E_0, P)$. Let $\mathscr{G}$ be the formal group attached to $E_0$. The completed local ring $\hat{\mathcal{O}}_{Y_n,x}$ classifies deformations of $E_0$ together with level $p^n$ structure. By Prop. 3.4.1, deforming $E_0$ is equivalent to deforming $\mathscr{G}_0$. It just remains to show that level structures on $E[p^n]$ are the same as Drinfeld level structures on $\mathscr{G}[p^n]$, and this turns out to be formal. □

Remaining in the height 2 case, let $M_n$ be the formal scheme $\operatorname{Spf} A_n = \operatorname{Spf} \hat{\mathcal{O}}_{Y_n,x}$. For an adic $W$-algebra $R$, $M_n(R)$ is the set of deformations of $E$ to $R$ together with a Drinfeld basis $P, Q$ of $E[p^n]$. Then the Weil pairing $e_{p^n}(P, Q)$ is a primitive $p^n$th root of unity in $R$ (exercise!). Thus to every $R$-point of $M_n$, we get an $R$-point of $\operatorname{Spf} W[\mu_{p^n}]$. In other words, the Weil pairing induces a morphism

$$e_{p^n} \colon M_n \to \operatorname{Spf} W[\mu_{p^n}],$$

or equivalently, a $W$-linear homomorphism $W[\mu_{p^n}] \to A_n$.

## 5. The universal cover, and formal vector spaces

In this discussion, we fix a prime $p$. For any abelian group $G$ whatsoever, one can form another group $\tilde{G}$ by

$$\tilde{G} = \varprojlim_{p} G,$$

where the inverse limit is taken with respect to multiplication by $p$. Then $\tilde{G}$ is a module over $\mathbb{Z}[1/p]$; indeed, multiplication by $1/p$ sends $(x_0, x_1, \dots)$ to $(x_1, x_2, \dots)$. In particular if $G$ is a $\mathbb{Z}_p$-module, then $\tilde{G}$ is a $\mathbb{Q}_p$-vector space. Note also that

$$\widetilde{\mathbb{Q}_p/\mathbb{Z}_p} = \mathbb{Q}_p.$$

Let $A$ be an adic $\mathbb{Z}_p$-algebra, and let $\mathscr{G}$ be a $p$-divisible formal group over $A$. We define the *universal cover* $\tilde{\mathscr{G}}$ as the functor from $\operatorname{Adic}_A$ to $\mathbb{Q}_p$-vector spaces, defined by

$$\tilde{\mathscr{G}}(R) = \varprojlim \mathscr{G}(R),$$

where the inverse limit is taken with respect to multiplication by $p$.

**Example 5.0.5** (The multiplicative group)**.** Consider the case of $\hat{\mathbb{G}}_m$, considered as a formal group over some base ring $A$ in $\mathrm{Adic}_{\mathbb{Z}_p}$. Then for objects $R$ in $\mathrm{Adic}_A$, $\hat{\mathbb{G}}_m(R)$ equals $\mathrm{Nil}(R)$ under the group law $(x, y) \mapsto x + y + xy$. Let $(x_0, x_1, \dots) \in \varprojlim_p \hat{\mathbb{G}}_m(R)$, so that $x_i \in \mathrm{Nil}(R)$ and $(1 + x_{n+1})^p = 1 + x_n$. Observe that the limit

$$y_0 = \lim_{n\to\infty} x_n^{p^n}$$

converges in $\mathrm{Nil}(R)$. Indeed, the relation $(1+x_{n+1})^p = 1+x_n$ shows that $x_{n+1}^p \equiv x_n \pmod{pR}$, from which it follows from the binomial theorem (check this!) that $x_{n+1}^{p^{n+1}} \equiv x_n^{p^n} \pmod{p^n R}$. Since $p$ is topologically nilpotent in $R$, the sequence $x_n^{p^n}$ converges.

We can also form the limit

$$y_i = \lim_{n\to\infty} x_n^{p^{n-i}},$$

and a little thought shows that $y_i^p = y_{i-1}$ for all $i \geq 1$. We thus have a function

$$\begin{array}{rcl} \varprojlim_p \hat{\mathbb{G}}_m(R) & \to & \varprojlim_{y\mapsto y^p} \mathrm{Nil}(R) \\ (x_0, x_1, \dots) & \mapsto & (y_0, y_1, \dots). \end{array}$$

This is even a bijection, with inverse given by

$$x_i = \lim_{n\to\infty} (1 + y_n)^{p^{n-i}} - 1.$$

What's more, this function is functorial in $R$. In summary, if we let $\mathrm{Nil}_A^\flat$ be the functor

$$\begin{array}{rccl} \mathrm{Nil}_A^\flat \colon & \mathrm{Adic}_A & \to & \mathrm{Sets} \\ & R & \mapsto & \varprojlim_{y\mapsto y^p} \mathrm{Nil}(R), \end{array}$$

then we have an isomorphism of functors between $\tilde{\hat{\mathbb{G}}}_m$ and $\mathrm{Nil}_A^\flat$. This isn't precisely accurate, because the target category of $\tilde{\hat{\mathbb{G}}}_m$ is $\mathbb{Q}_p$-vector spaces and the target category of $\mathrm{Nil}_A^\flat$ is Sets. What we really mean is that the composition of $\tilde{\hat{\mathbb{G}}}_m$ with the forgetful functor from $\mathbb{Q}_p$-vector spaces to sets is isomorphic to $\mathrm{Nil}_A^\flat$.

**Remark 5.0.6.** The universal cover appears in a paper of Faltings, [Fal10], where it is linked with $p$-adic Hodge theory. The idea is further developed in the preprint of Fontaine-Fargues, *Courbes et fibrés vectoriels en théorie de Hodge p-adique* (avaiable on Fargues' website), which establishes many of the main properties of the universal cover.

The $\mathrm{Nil}^\flat$ functor may already look familiar to readers familiar with Fontaine's period ring $\mathbf{B}_{dR}$. A stepping stone in that construction is a curious ring $\mathcal{R}$, defined as a set by

$$\mathcal{R} = \varprojlim_{x \mapsto x^p} \mathcal{O}_{\mathbb{C}_p},$$

so that elements are sequences $x_\bullet = \{x_n\}_{n \geq 0}$. Multiplication is defined componentwise, and addition is defined via

$$(x_\bullet + y_\bullet)_n = \lim_{m \to \infty} (x_{m+n} + y_{m+n})^{p^m}.$$

The reader must be warned that the following definition is somewhat provisional.

**Definition 5.0.7.** *Let $A \in \mathrm{Adic}_{\mathbb{Z}_p}$. A* formal $\mathbb{Q}_p$-vector space *of dimension $d$ over $A$ is a functor $\mathcal{V}$ from $\mathrm{Adic}_A$ to the category of $\mathbb{Q}_p$-vector spaces. It is required that when $\mathcal{V}$ is composed with the forgetful functor from $\mathbb{Q}_p$-vector spaces to* Sets*, the result is isomorphic to $(\mathrm{Nil}^\flat_A)^d$.*

**Remark 5.0.8.** The functor $(\mathrm{Nil}^\flat_A)^d$ is representable by the ring

$$A[\![X_1^{1/p^\infty}, \ldots, X_d^{1/p^\infty}]\!].$$

This ring is defined as the completion of $A[X_1^{1/p^\infty}, \ldots, X_d^{1/p^\infty}]$ under the $(I, X_1, \ldots, X_d)$-adic topology, where $I$ is an ideal of definition for $A$. A little care must be taken with this sort of ring. For instance, an element of the ring $\mathbb{Z}_p[\![T^{1/p^\infty}]\!]$ is a certain kind of fractional power series of the form

$$\sum_{\alpha \in \mathbb{Z}[1/p]_{\geq 0}} c_\alpha T^\alpha,$$

with $c_\alpha \in \mathbb{Z}_p$ It is required that for all positive integers $N$, only finitely many terms in the above series are allowed to lie outside of the ideal $(p^N, T^N)$. Thus

$$T + pT^{1/p} + p^2 T^{1/p^2} + \ldots$$

and

$$T + T^2 + T^3 + \ldots$$

are valid expressions for elements of $\mathbb{Z}_p[\![T^{1/p^\infty}]\!]$, whereas

$$T + T^{1+\frac{1}{p}} + T^{1+\frac{1}{p}+\frac{1}{p^2}} + \ldots$$

is not. Finally, one really has to check (though it is not difficult) that $A[\![X_1^{1/p^\infty}, \ldots, X_n^{1/p^\infty}]\!]$ is an object of $\mathrm{Adic}_A$; that is, one must check that it is complete with respect to the $(I, X_1, \ldots, X_d)$-adic topology. (While it is true that the completion of a noetherian ring at one of its

ideals is complete, this is not true without the noetherian assumption, and $A[X_1^{1/p^\infty}, \dots, X_n^{1/p^\infty}]$ is not noetherian!)

The universal cover of $\hat{\mathbb{G}}_m$ is a 1-dimensional formal vector space. In fact this is true in rather broad generality. First let us study the case of $p$-divisible formal groups over perfect fields in characteristic $p$:

**Lemma 5.0.9** (cf. [SW12], Prop. 3.1.3)**.** *Assume that $k$ is a perfect field in characteristic $p$, and that $\mathscr{G}$ is a $p$-divisible formal group of dimension $d$ over $k$. Then $\tilde{\mathscr{G}}$ is a $d$-dimensional formal $\mathbb{Q}_p$-vector space over $k$.*

*Proof.* We'll assume $\mathscr{G}$ has dimension 1, the general case being similar. Let $\Phi\colon k \to k$ be the $p$th power map, which is an automorphism because $k$ is perfect. For $n \in \mathbb{Z}$, let $\mathscr{G}^{(p^n)} = \mathscr{G} \otimes_{k,\Phi^n} k$. In other words, $\mathscr{G}^{(p^n)}$ is the formal group over $A$ obtained by applying $\Phi^n$ to all coefficients of the power series $\mathscr{G}(X,Y)$. The substitution $T \mapsto T^p$ defines a morphism $F\colon \mathscr{G} \to \mathscr{G}^{(p)}$, called the Frobenius isogeny. We use the same letter $F$ to denote the Frobenius isogeny $\mathscr{G}^{(p^{-n})} \to \mathscr{G}^{(p^{-n+1})}$. We have a factorization $[p]_{\mathscr{G}} = FV$, where $V\colon \mathscr{G}^{(p)} \to \mathscr{G}$ is the Verschiebung morphism.

Let us observe that the functor $\varprojlim_F \mathscr{G}^{(p^{-n})}$ (once its $\mathbb{Z}_p$-module structure is forgotten) is isomorphic to $\mathrm{Nil}_k^\flat$. Indeed, for an adic $k$-algebra $R$, $\mathscr{G}^{(p^{-n})}(R) \cong \mathrm{Nil}(R)$, and the Frobenius isogeny $F\colon \mathscr{G}^{(p^{-n})} \to \mathscr{G}^{(p^{-n+1})}$ corresponds to $x \mapsto x^p$, so that $\varprojlim_F \mathscr{G}^{(p^{-n})}(R) \cong \varprojlim_{x\mapsto x^p} \mathrm{Nil}(R)$ as required.

Thus it suffices to find an isomorphism

$$\mathcal{V}\colon \varprojlim_p \mathscr{G} \to \varprojlim_F \mathscr{G}^{(p^{-n})}.$$

We define $\mathcal{V}$ by the diagram

$$\begin{array}{ccccccc}
\mathscr{G} & \xleftarrow{p} & \mathscr{G} & \xleftarrow{p} & \mathscr{G} & \longleftarrow & \cdots \\
{\scriptstyle =}\downarrow & & \downarrow{\scriptstyle V} & & \downarrow{\scriptstyle V^2} & & \\
\mathscr{G} & \xleftarrow[F]{} & \mathscr{G}^{(p^{-1})} & \xleftarrow[F]{} & \mathscr{G}^{(p^{-2})} & \longleftarrow & \cdots
\end{array}$$

We claim that $\mathcal{V}$ is an isomorphism. Since $\mathscr{G}$ is formal, its $p$-divisible group $G = \mathscr{G}[p^\infty]$ is connected. This shows that the Frobenius map $F\colon M(G) \to M(G)$ is topologically nilpotent. We can therefore let $h$ be large enough so that $F^h = pu$ for a morphism $u\colon G^{(p^{-h})} \to G$. We get a natural transformation $\mathcal{U} = \varprojlim_{F^h} G^{(p^{-hn})} \to \varprojlim_p G$ induced by $(1, u, u^2, \dots)$. Then $\mathcal{U}$ is the double-sided inverse to $\mathcal{V}$. $\square$

The following proposition, though easy to prove, is somewhat miraculous.

**Proposition 5.0.10** (The crystalline nature of $\tilde{\mathscr{G}}$.)**.** *Let $A \in \mathrm{Adic}_{\mathbb{Z}_p}$. Let $I$ be an ideal of definition of $A$. For a $p$-divisible formal group $\mathscr{G}$ over $A$, the reduction-mod-$I$ map*

$$\tilde{\mathscr{G}}(A) \to \tilde{\mathscr{G}}(A/I)$$

*is an isomorphism.*

**Remark 5.0.11.** The proposition shows that $\tilde{\mathscr{G}}$ doesn't depend on $\mathscr{G}$ so much as it depends on $\mathscr{G} \otimes A/I$. Switching perspective a bit, we can start with the ring $A_0 = A/I$, and consider the formal vector space $\tilde{\mathscr{G}}_0$ over $A_0$. The proposition says that $\tilde{\mathscr{G}}_0$ lifts to $A$ in a unique way, namely by lifting $\mathscr{G}_0$ to a formal group $\mathscr{G}/A$ arbitrarily, and then forming $\tilde{\mathscr{G}}$, which will not depend on the choice of lift.

This is what we mean when we say talk about the "crystalline nature" of $\tilde{\mathscr{G}}$: it is an object that always lifts uniquely from $A$ to $A_0$ whenever we have a surjection $A \to A_0$. From Grothendieck's letter to Tate: "A crystal posssess two characteristic properties: rigidity, and the ability to grow in an appropriate neighborhood. There are crystals of all kinds of substances: sodium, sulfur, modules, rings, relative schemes, etc." Our $\tilde{\mathscr{G}}$ is a crystal of sheaves of $\mathbb{Q}_p$-vector spaces on the infinitesimal site of $A_0$.

*Proof.* The following proof assumes that $\mathscr{G}$ is 1-dimensional, but this is only for ease of notation.

Without loss of generality we may enlarge $I$ so that it contains $p$. If $(x_1, x_2, \dots) \in \tilde{\mathscr{G}}(A)$ lies in the kernel of $\tilde{\mathscr{G}}(A) \to \tilde{\mathscr{G}}(A/I)$, then each $x_i$ lies in $I$. By the power series giving multiplication by $p$ in $\mathscr{G}$ has $p$ as its linear term, so it carries $I$ onto $I^2$. It follows that each $x_i$ lies in $\bigcap_{n\geq 1} I^n = 0$. Thus the reduction map is injective.

To show surjectivity, suppose $(x_0, x_1, \dots) \in \tilde{\mathscr{G}}(A/I)$. Since $I$ is topologically nilpotent, we may lift each $x_i$ to a topologically nilpotent element $y_i$ of $A$. The sequence $y_i, [p]_{\mathscr{G}}(y_{i+1}), \dots$ converges in $\mathrm{Nil}(A)$ (exercise!). Let

$$z_i = \lim_{n\to\infty} [p^n]_{\mathscr{G}}(y_{n+i}).$$

Then $(z_0, z_1, \dots)$ is a lift of $(x_0, x_1, \dots)$ to $\tilde{\mathscr{G}}(A)$. □

With this result, we can now extend Lemma 5.0.9 to base rings in characteristic 0.

**Corollary 5.0.12.** *Let $A \in \mathrm{Adic}_{\mathbb{Z}_p}$. Assume that $A$ admits an ideal of definition $I$ for which $A/I$ is a perfect ring in characteristic $p$. Let*

*$\mathscr{G}$ be a $p$-divisible formal group over $A$. Then $\tilde{\mathscr{G}}$ is a formal $\mathbb{Q}_p$-vector space over $A$.*

*Proof.* For an object $R$ of $\mathrm{Adic}_A$, we have a functorial isomorphism $\tilde{\mathscr{G}}(R) \to \tilde{\mathscr{G}}(R/I)$, by Prop. 5.0.10. By Prop. 5.0.9, the base change $\tilde{\mathscr{G}}_{A/I}$ is a formal $\mathbb{Q}_p$-vector space, so there is an isomorphism of functors between $\tilde{\mathscr{G}}_{A/I}$ and $(\mathrm{Nil}^\flat_{A/I})^d$. But then also $\mathrm{Nil}^\flat(R) \to \mathrm{Nil}^\flat(R/I)$ is a bijection (same argument as the proof of Prop.5.0.10). Thus $\tilde{\mathscr{G}}$ is isomorphic to $(\mathrm{Nil}^\flat_R)^d$. □

5.1. **The Weil pairing at infinite level.** In this section we use the Weil pairing on a supersingular elliptic curve $E_0$ in characteristic $p$ to cook up a Weil pairing on the universal cover of the formal group $\hat{E}_0$. Since universal covers are crystals, this also gives us a Weil pairing on the universal cover of any lift of $\hat{E}_0$ to characteristic 0.

First we need a lemma concerning the Tate module of a $p$-divisible formal group over a discrete ring.

**Lemma 5.1.1.** *Let $A \in \mathrm{Adic}_{\mathbb{Z}_p}$ be discrete, so that any ideal of definition is nilpotent. Let $\mathscr{G}$ be a 1-dimensional $p$-divisible formal group over $A$. Then for all $R \in \mathrm{Adic}_A$, the inclusion $\varprojlim_p \mathscr{G}[p^n](R) \to \varprojlim_p \mathscr{G}(R) = \tilde{\mathscr{G}}(R)$ induces an isomorphism*

$$\left(\varprojlim \mathscr{G}[p^n](R)\right) \otimes \mathbb{Q}_p \xrightarrow{\sim} \tilde{\mathscr{G}}(R)$$

**Remark 5.1.2.** The inverse limit $\varprojlim \mathscr{G}[p^n](R)$ is the Tate module of $\mathscr{G}$ (over $R$). Note that $\varprojlim_p \mathscr{G}[p^n](R)$ is the set of sequences $(x_0, x_1, \dots) \in \tilde{\mathscr{G}}(R)$ such that $x_0 = 0$. For base rings (such as $\mathbb{Z}_p$) which are not discrete, the Tate module is much, much smaller than $\tilde{\mathscr{G}}(R)$ (finite rank vs. uncountable rank). But for discrete rings (such as $\mathbb{F}_p$), the Tate module is essentially a lattice inside of $\tilde{\mathscr{G}}(R)$.

*Proof.* Since $\varprojlim_p \mathscr{G}[p^n](R) \to \tilde{\mathscr{G}}(R)$ is an injection, and $\tilde{\mathscr{G}}(R)$ is a $\mathbb{Q}_p$-vector space, so injectivity is automatic. For surjectivity, we must show that every element of $\mathscr{G}(R)$ is $p$-power torsion. This follows from the facts that $p \in A$ is nilpotent, and that $[p]_{\mathscr{G}}(T) = pT + \dots$. □

Let $E$ be a supersingular elliptic curve over a perfect field $k$ of characteristic $p$. Recall that we have the Weil pairing on the torsion subgroup scheme $E[p^n]$:

$$e_{p^n} : E[p^n] \times E[p^n] \to \mu_{p^n}.$$

The pairings $e_{p^n}$ coalesce into an alternating form on Tate modules:

$$e_{p^\infty} : \varprojlim E[p^n] \times \varprojlim E[p^n] \to \varprojlim \mu_{p^n}.$$

Let $\mathscr{G}_0$ be the formal group attached to $E$, so that $\mathscr{G}_0$ is a $p$-divisible formal group of dimension 1 and height 2. Tensoring the pairing above with $\mathbb{Q}_p$ and applying Lemma 5.1.1 yields

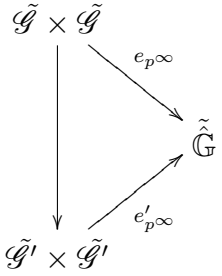
$$e_{p^\infty} : \tilde{\mathscr{G}}_0 \times \tilde{\mathscr{G}}_0 \to \hat{\tilde{\mathbb{G}}}_m,$$

which can be seen as a Weil pairing on the formal vector space $\tilde{\mathscr{G}}_0$ in characteristic $p$.

Now let $A$ be an adic $\mathbb{Z}_p$-algebra admitting an ideal of definition $I$ such that $A/I = k$. Let $\mathscr{G}$ be any lift of $\mathscr{G}_0$ to $A$. By Prop. 5.0.10, the universal cover $\tilde{\mathscr{G}}$ only depends on $\mathscr{G}_0$ and not on the choice of lift $\mathscr{G}$. The pairing $e_{\mathscr{G}_0}$ lifts uniquely to a pairing on $\mathscr{G}$:

$$e_{p^\infty} : \tilde{\mathscr{G}} \times \tilde{\mathscr{G}} \to \hat{\tilde{\mathbb{G}}}_m.$$

The crystalline nature of formal vector spaces can be used to show that $e_{p^\infty}$ *does not depend on the choice of lift of* $\mathscr{G}_0$ *to* $A$. That is, suppose $\mathscr{G}'$ is another lift of $\mathscr{G}_0$, and let $e'_{p^\infty}$ be the corresponding Weil pairing on $\mathscr{G}'$. By Prop. 5.0.10 we have an isomorphism $\tilde{\mathscr{G}} \to \tilde{\mathscr{G}}'$. Then the diagram




commutes.

## 6. Drinfeld's ring at infinite level

Let us review some important notation.

- $W$, the ring of Witt vectors of $\overline{\mathbb{F}}_q$
- $K$, the fraction field of $W$
- $N$, an auxiliary integer $\geq 5$ which will momentarily be forgotten forever
- $X_n$, the Katz-Mazur model of $X(\Gamma_1(N) \cap \Gamma(p^n))$ over $\mathbb{Z}_p$ ($n = 0, 1, \dots$)
- $x$, a supersingular point of $X_0(\overline{\mathbb{F}}_p)$
- $E_0$, a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ corresponding to $x$
- $\mathscr{G}_0$, the formal completion of $E_0$ at its origin
- $A_n$, the deformation ring of $\mathscr{G}_0$ with Drinfeld $p^n$ level structure
- $M_n = \operatorname{Spf} A_n$, an affine formal scheme over $\operatorname{Spf} W$.

- $\mathscr{G}^{\mathrm{univ}}$, the universal deformation of $\mathscr{G}_0$ to $A_0$

Since $\mathscr{G}_0$ is a formal group over $\overline{\mathbb{F}}_q$ of height 2, there is a (non-canonical) isomorphism $A_0 \cong W[\![u]\!]$. We have also seen (Prop. 4.7.4) that $A_n \cong \hat{\mathcal{O}}_{X_n,x}$. Define

$$A_\infty = \text{completion of} \varinjlim A_n,$$

Here completion is taken with respect to the topology on $\varinjlim A_n$ induced by the maximal ideal $I$ of $A_0$ (or any of the $A_n$, it doesn't matter). It is unclear at this moment whether $A_\infty$ represents any interesting functors. (For one thing $A_\infty$ isn't noetherian, and so cannot represent any functor $\mathcal{C} \to \mathrm{Sets}$.) But we will find a surprising description of the affine formal scheme $\operatorname{Spf} A_\infty$ in terms of the Weil pairing on a formal vector space.

It will be helpful to work with the category of affine formal schemes over $\operatorname{Spf} W$, rather than the category of adic $W$-algebras (recall that these are opposite to one another). Recall from Eq. (4.7.1) that the Weil pairing induces a morphism $e_{p^n} \colon M_n \to \operatorname{Spf} W[\mu_{p^n}]$. Let $M_\infty = \operatorname{Spf} A_\infty$. These morphisms induce a morphism

$$e_{p^\infty} \colon M_\infty \to \operatorname{Spf} \widehat{W[\mu_{p^\infty}]}. \tag{6.0.1}$$

Over the ring $A_n$, we obtain a Drinfeld basis $X_n^{\mathrm{univ}}, Y_n^{\mathrm{univ}}$ for $\mathscr{G}^{\mathrm{univ}}(A_n)$. Assembling these together, we get sequences $X^{\mathrm{univ}} = (X_1^{\mathrm{univ}}, X_2^{\mathrm{univ}}, \dots)$ and $Y^{\mathrm{univ}} = (Y_1^{\mathrm{univ}}, Y_2^{\mathrm{univ}}, \dots)$ which lie in $\tilde{\mathscr{G}}^{\mathrm{univ}}(A_\infty)$.

It is at this point that we do the following strange thing: let $\mathscr{G}$ be a *completely arbitrary* lift of $\mathscr{G}_0$ to $W$. We now make use of the crystalline nature of formal vector spaces (Prop. 5.0.10): Since $\mathscr{G}^{\mathrm{univ}}$ and $\mathscr{G} \otimes_W A_0$ are both lifts of $\mathscr{G}_0$ from $\overline{\mathbb{F}}_p$ to $A_0$, their universal covers are isomorphic (by the crystalline nature of universal covers). Let

$$\psi \colon \tilde{\mathscr{G}}^{\mathrm{univ}} \to \tilde{\mathscr{G}} \otimes_W A_0$$

be the unique isomorphism which lifts the identity map on $\mathscr{G}_0$. Let $X = \psi(X^{\mathrm{univ}})$ and $Y = \psi(Y^{\mathrm{univ}})$, so that $X, Y \in \tilde{\mathscr{G}}(A_\infty)$. The data of $X$ and $Y$ give us a morphism $M_\infty = \operatorname{Spf} A_\infty \to \tilde{\mathscr{G}} \times \tilde{\mathscr{G}}$.

Putting this together with the morphism of Eq. (6.0.1), we have a commutative diagram of formal schemes over $\operatorname{Spf} W$:

$$\begin{array}{ccc} M_\infty & \xrightarrow{e_{p^\infty}} & \operatorname{Spf} \widehat{W[\mu_{p^\infty}]} \\ \downarrow & & \downarrow \\ \tilde{\mathscr{G}} \times \tilde{\mathscr{G}} & \xrightarrow[e_{p^\infty}]{} & \hat{\tilde{\mathbf{G}}}_m \end{array} \tag{6.0.2}$$

**Theorem 6.0.3** ([Wei12], Thm. 2.8.1)**.** *The above diagram is Cartesian. That is, $M_\infty$ is isomorphic to the fiber product of $\tilde{\mathscr{G}} \times \tilde{\mathscr{G}}$ and $\widehat{\mathrm{Spf}\, W[\mu_{p^\infty}]}$ over $\hat{\tilde{\mathbf{G}}}_m$.*

The theorem is a little suprising for this reason: $M_\infty$ was built out of formal schemes $M_n$ which parametrize deformations of the formal group $\mathscr{G}_0$. But Thm. 6.0.3 gives an alternative description of $M_\infty$ which has nothing to do with deformations of anything. Or rather, there was a *particular* choice of deformation $\mathscr{G}$ over $W$ involved in this description of $M_n$, but the choice of $\mathscr{G}$ makes no difference (nor should it, since $\tilde{\mathscr{G}}$ doesn't depend on $\mathscr{G}$).

Informally speaking, Thm. 6.0.3 says that $M_\infty$ owes all its complexity to the Weil pairing $e_{p^\infty} : \tilde{\mathscr{G}} \times \tilde{\mathscr{G}} \to \hat{\tilde{\mathbf{G}}}_m$. This pairing corresponds to a continuous $W$-linear homomorphism $W[\![T^{1/p^\infty}]\!] \to W[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$. Thm. 6.0.3 can then be interpreted as a formula for $A_\infty$, namely

$$A_\infty \cong W[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!] \hat{\otimes}_{W[\![T^{1/p^\infty}]\!]} \widehat{W[\mu_{p^\infty}]},$$

where $W[\![T^{1/p^\infty}]\!] \to \widehat{W[\mu_{p^\infty}]}$ carries $T$ onto $\lim_{n\to\infty}(1-\zeta_{p^n})^{p^n}$.

This gives a rather satisfying description of $M_\infty$, modulo the caveat that the morphism $e_{p^\infty}$ is rather mysterious. We can also give a description of the "geometrically connected components" of $M_\infty$. Let us recall some notation from §2.5. The Weil pairing induces a morphism $e_{p^n} : Y_n \to \mu_{p^n}$ of schemes over $\mathrm{Spec}\, W$. After extending scalars to $\mathrm{Spec}\, W[\mu_{p^n}]$, $Y_n$ breaks up into a disjoint union of fibers $Y_n^{\zeta_{p^n}}$, one for each primitive $p^n$th root of unity.

Let $\zeta = (\zeta_p, \zeta_{p^2}, \dots)$ be a compatible family of $p$th power roots of unity. We are now concerned with the rings

$$A_n^{\zeta_{p^n}} = \hat{\mathcal{O}}_{Y_n^{\zeta_{p^n}}, x}$$

and

$$A_\infty^\zeta = \hat{\mathcal{O}}_{Y_\infty^\zeta, x} = \text{ completion of } \varinjlim A_n^{\zeta_{p^n}}.$$

Finally, let $M_\infty^\zeta = \mathrm{Spf}\, A_\infty^\zeta$. Adapting Thm. 6.0.3 to this situation, we get a cartesian diagram of formal schemes over $\widehat{\mathrm{Spf}\, W[\mu_{p^\infty}]}$:

$$\begin{array}{ccc} M_\infty^\zeta & \xrightarrow{e_{p^\infty}} & \widehat{\mathrm{Spf}\, W[\mu_{p^\infty}]} \\ \downarrow & & \downarrow \\ \tilde{\mathscr{G}} \times \tilde{\mathscr{G}} & \xrightarrow[e_{p^\infty}]{} & \hat{\tilde{\mathbb{G}}}_m \end{array}$$

Once again we can use the diagram to give a formula for the ring $A_\infty^\zeta$. For the remainder of this discussion, the base ring is $\widehat{W[\mu_{p^\infty}]}$. The formal scheme $\tilde{\mathscr{G}} \times \tilde{\mathscr{G}}$ is isomorphic to $\operatorname{Spf} W[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$. Therefore the morphism $e_{p^\infty} \colon \tilde{\mathscr{G}} \times \tilde{\mathscr{G}} \to \hat{\tilde{\mathbb{G}}}_m$ corresponds to an element of $\hat{\tilde{\mathbb{G}}}_m(W[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!])$, which is to say, a sequence $\Delta(X,Y), \Delta(X,Y)^{1/p}, \ldots$ of elements of $W[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$ with $\Delta(0,0) = 1$.

The punchline of the course is this:

**Corollary 6.0.4.** *We have an isomorphism*

$$A_\infty^\zeta \cong \frac{\widehat{W[\mu_{p^\infty}]}[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]}{(\Delta(X,Y)^{1/p^m} - \zeta_{p^m})_{m \geq 0}}.$$

Project B is dedicated to deriving a convenient expression for the fractional power series $\Delta(X,Y)$.

## 7. Project A: Exercises in positive characteristic

Let $K = \mathbb{F}_q(\!(\pi)\!)$ be the field of Laurent series in one variable over the finite field $\mathbb{F}_q$. Let $f(T) = \pi T + T^q \in \mathcal{O}_K[T]$. It is quite easy to find the Lubin-Tate formal $\mathcal{O}_K$-module $\mathscr{F} = \mathscr{F}_f$. Namely, $\mathscr{F}$ is characterized by

- $X +_{\mathscr{F}} Y = X + Y$
- $[a]_{\mathscr{F}}(T) = aT,\ a \in \mathbb{F}_q$
- $[\pi]_{\mathscr{F}}(T) = f(T)$

Let $t_1$ be a nonzero root of $f(T)$, and for $n \geq 2$ define $t_n$ inductively as a root of $f(T) - t_{n-1}$. Let $K_n = K(t_n)$, and let $K_\infty = \bigcup_{n \geq 1} K_n$. Let $H_n = \mathrm{Gal}(K_n/K)$ and $H = \mathrm{Gal}(K_\infty/K) = \varprojlim H_n$. The formalism of Lubin-Tate theory shows that there are isomorphisms $\rho_n \colon (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \to H_n$ and $\rho \colon \mathcal{O}_K^\times \to H$. These satisfy $\rho(\alpha)(t_n) = [\alpha]_{\mathscr{F}}(t_n)$ for all $\alpha \in \mathcal{O}_K^\times$.

Let $L$ be the completion of $K_\infty$.

**Exercise A1**. Show that the sequence $t_1^q, t_2^{q^2}, \ldots$ converges to an element $t \in \mathcal{O}_L$. Also show that $t^{1/q^i} \in \mathcal{O}_L$ for all $i \geq 0$.

**Exercise A2**. The action of $H$ on $K_\infty$ extends to $L$. Show that if $\alpha = \sum_{m \geq 0} a_m \pi^m \in \mathcal{O}_K^\times$, then

$$\rho(\alpha)(t) = \sum_{m=0}^{\infty} a_m t^{q^m}. \tag{7.0.3}$$

**Exercise A3**. Show that $\mathcal{O}_L = \mathbb{F}_q[\![t^{1/q^\infty}]\!]$, this being the $t$-adic completion of $\mathbb{F}_q[t^{1/q^\infty}]$. (Hint: first show that $\mathcal{O}_L/t = \mathbb{F}_q[t^{1/q^\infty}]/t$.) That is, every element of $\mathcal{O}_L$ can be expressed uniquely as a "fractional power series" of the form $\sum_\alpha c_\alpha t^\alpha$, where $\alpha$ runs through $\mathbb{Z}[1/q]_{\geq 0}$, and for every $N \geq 0$, there are only finitely many $\alpha \geq N$ with $c_\alpha \neq 0$. In particular, $L$ is a perfect field.

**Exercise A4**. It follows from Exercise A3 that the element $\pi$ is expressible as a fractional power series in $t$, which has to be invariant under all of the substitutions of the type described by Eq. (7.0.3). In fact, show that

$$\pi = \lim_{n \to \infty} \prod_{(a_0, \ldots, a_{n-1})} \left( a_0 t + a_1 t^q + \cdots + a_{n-1} t^{q^{n-1}} \right)^{q^{-n}}.$$

Here $(a_0, \ldots, a_{n-1})$ runs over tuples of elements of $\mathbb{F}_q$, with $a_0 \neq 0$. (Warning: I haven't done this exercise. But the expression on the right seems like a very natural way of coming up with a Galois-invariant

element, and it has the right valuation, so what else could it be but $\pi$?)

**Exercise A5**. Show that $L^H$ (the field of $H$-invariant elements of $L$) is a perfect field containing $K$which is closed inside of $L$. In fact, show that it is the smallest such field. That is, $L^H$ is the completion of the perfect closure of $K$ in $L$.

**Exercise A6**. Find similar formulas for $t_1, t_2, \ldots$ in terms of $t$.

**Exercise A7**. Show that there is a canonical isomorphism between the absolute Galois groups $G_L$ and $G_{K_\infty}$. Also show that $G_L$ is isomorphic to the absolute Galois group of $\mathbb{F}_q(\!(t)\!)$. Since this field is (non-canonically) isomorphic to $K = \mathbb{F}_q(\!(\pi)\!)$, we therefore have an isomorphism between $G_K$ and its subgroup $G_{K_\infty}$.

## 8. Project B: Determinants of formal groups

The Artin-Hasse exponential is the formal power series

$$AH(T) = \exp\left(T + \frac{T^p}{p} + \frac{T^{p^2}}{p^2} + \ldots\right).$$

A priori it lies in $\mathbb{Q}_p[\![T]\!]$.

**Exercise B1**. (Dwork's lemma) Show that if $f(T) = 1 + T + \cdots \in \mathbb{Q}_p[\![T]\!]$ is a power series satisfying $f(T^p)/f(T)^p \equiv 1 \pmod{p\mathbb{Z}_p[\![T]\!]}$, then in fact $f(T) \in \mathbb{Z}_p[\![T]\!]$. Use this to show that $AH(T) \in \mathbb{Z}_p[\![T]\!]$.

**Exercise B2**. Give another proof that $AH(T) \in \mathbb{Z}_p[\![T]\!]$ by showing formally that

$$AH(T) = \prod_{p \nmid n} (1 - x^n)^{-\mu(n)/n}.$$

**Exercise B3**. By Hazewinkel's theory of $p$-typical formal groups, there exists a formal group law $\mathscr{F}$ over $\mathbb{Z}_p$ of height 1 whose logarithm is

$$\log_{\mathscr{F}}(T) = T + \frac{T^p}{p} + \frac{T^{p^2}}{p^2} + \ldots$$

Show that $[p]_{\mathscr{F}}(T) \equiv T^p \pmod{p\mathbb{Z}_p[\![T]\!]}$. By Lubin-Tate theory, if $\mathscr{G}$ and $\mathscr{G}'$ are two one-dimensional formal groups of height 1 over $\mathbb{Z}_p$ for which $[p]_{\mathscr{G}}$ and $[p]_{\mathscr{G}'}$ are congruent mod $p$, then $\mathscr{G} \cong \mathscr{G}'$. Conclude that $\mathscr{F}$ is isomorphic to the formal multiplicative group $\hat{\mathbb{G}}_m$, and that the isomorphism between them is $AH(T) - 1$ (which gives a third proof of integrality).

**Exercise B4**. Let $\lambda$ be a nonzero root of $[p]_{\mathscr{F}}(T)$, so that $\log_{\mathscr{F}}(\lambda) = \sum_{i=0}^{\infty} \lambda^{p^i}/p^i = 0$. Since $AH(T)$ is an isomorphism onto the formal multiplicative group, $AH(\lambda)$ must be a primitive $p$th root of 1. On the other hand $AH(\lambda) = \exp(\sum_{i=0}^{\infty} \lambda^{p^i}/p^i) = \exp(0) = 1$. Resolve this apparent contradiction.

**Exercise B5**. Show that the limit

$$G(T) = \lim_{n\to\infty} AH(T^{1/p^n})^{p^n}$$

exists in $\mathbb{Z}_p[\![T^{1/p^\infty}]\!]$. Show that this power series satisfies the identities $G(0) = 1$ and $G(T^p) = G(T)^p$. Then give the following interpretation for $G(T)$. The isomorphism of formal groups $AH\colon \mathscr{F} \to \hat{\mathbb{G}}_m$ induces an isomorphism of formal vector spaces $\tilde{AH}\colon \tilde{\mathscr{F}} \to \tilde{\hat{\mathbb{G}}}_m$. On the other hand, once we forget the $\mathbb{Q}_p$-vector space structures, we have an isomorphism $\tilde{\mathscr{F}} \to \mathrm{Nil}^\flat$ (see Cor. 5.0.12). Show that the composite map

$$\mathrm{Nil}^\flat \longrightarrow \tilde{\mathscr{F}} \xrightarrow{\tilde{AH}} \tilde{\hat{\mathbb{G}}}_m$$

is given by $(x_0, x_1, \dots) \mapsto (G(x_0), G(x_1), \dots)$.

**Exercise B6**. Show that

$$G(T) = \exp\left(\sum_{i=-\infty}^{\infty} \frac{T^{p^i}}{p^i}\right) \tag{8.0.4}$$

Actually, this statement, while formally easy, needs to be made more precise. To what ring does that power series even belong? We need to make a slight detour into the world of affinoid algebras.

For each $m \geq 1$, consider

$$\begin{aligned} A_m^+ &= \mathbb{Z}_p\langle T, T^m/p\rangle = p\text{-adic completion of } \mathbb{Z}_p[T, T^m/p] \\ A_m &= \mathbb{Q}_p\langle T, T^m/p\rangle = A_m^+[1/p] \end{aligned}$$

Then $A_m$ is the affinoid algebra of functions on the closed disk $\left\{|T| \leq |p|^{1/m}\right\}$, and $A_m^+$ becomes the subalgebra of functions which are integral on that disk. We have that $A_m$ contains $A_{m+1}$. Set $\mathbb{Q}_p\{\{T\}\} = \bigcap_{m\geq 1} A_m$; you can think of this as the algebra of functions on the open disk. On the other hand, $\bigcap_{m\geq 1} A_m^+$ is the algebra of integral functions on the open disk; this is just $\mathbb{Z}_p[\![T]\!]$. The series $\sum_{i=0}^{\infty} T^{p^i}/p^i$ lies in $\mathbb{Q}_p\{\{T\}\}$, and its exponential is $AH(T)$.

To make sense of Eq. (8.0.4), we need to pass to the larger world of *perfectoid affinoid algebras*. Let

$$\begin{aligned} B_m^+ &= \mathbb{Z}_p\left\langle T^{1/p^\infty}, T^m/p\right\rangle = p\text{-adic completion of } \mathbb{Z}_p[T^{1/p^\infty}, T^m/p] \\ B_m &= \mathbb{Q}_p\left\langle T^{1/p^\infty}, T^m/p\right\rangle = B_m^+[1/p]. \end{aligned}$$

Then $B_m$ is the algebra of functions on what might be called the "perfectoid closed disk" of radius $|p|^{1/m}$. Set $\mathbb{Q}_p\left\{\left\{T^{1/p^\infty}\right\}\right\} = \bigcap_{m\geq 1} B_m$. Then the series $\sum_{i=-\infty}^{\infty} T^{p^i}/p^i$ lies in $\mathbb{Q}_p\left\{\left\{T^{1/p^\infty}\right\}\right\}$, and it is in this ring that Eq.(8.0.4) takes place.

**Exercise B7 (the main problem of the project)**. Now let $\mathscr{G}$ be the formal group law of height 2 whose logarithm is

$$\log_{\mathscr{G}}(T) = \sum_{i=0}^{\infty} \frac{T^{p^{2i}}}{p^i}.$$

Let $L(T)$ be the fractional power series

$$L(T) = \sum_{i=-\infty}^{\infty} \frac{T^{p^{2i}}}{p^i},$$

so that $L(T)$ lies in $\mathbb{Q}_p\left\{\left\{T^{1/p^\infty}\right\}\right\}$.

The problem at hand is to show that the fractional power series

$$\Delta(X,Y) = \exp\det\begin{pmatrix} L(X) & L(Y) \\ L(X^p) & L(Y^p) \end{pmatrix}$$

lies in $\mathbb{Z}_p[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$. (Is there a ring containing $\mathbb{Z}_p[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$ in which $\Delta(X,Y)$ lives a priori? If $B = \mathbb{Z}_p\left\langle X^{1/p^\infty}, Y^{1/p^\infty}, X/p, Y/p\right\rangle$, then the entries of the matrix lie in $pB$, so the determinant lies in $p^2B$. Since $B$ is $p$-adically complete, exp is well-defined on $p^2B$, so that indeed, $\Delta(X,Y)$ belongs to $B$. The problem is to show that $\Delta$ lies in the subring $\mathbb{Z}_p[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$.)

*Post-AWS note: Members of our research group noticed that the above formula for $\Delta(X,Y)$ isn't integral after all. The fix we found was this: let $\mathbb{Z}_{p^2}$ be the ring of integers in the unramified quadratic extension of $\mathbb{Q}_p$. Let $\alpha \in \mathbb{Z}_{p^2}^\times$ be an element with $\alpha^p = -\alpha$. The right formula for $\Delta(X,Y)$ is*

$$\Delta(X,Y) = \exp\alpha\det\begin{pmatrix} L(X) & L(Y) \\ L(X^p) & L(Y^p) \end{pmatrix};$$

*it turns out this lies in $\mathbb{Z}_{p^2}[\![X^{1/p^\infty}, Y^{1/p^\infty}]\!]$.*

**Exercise B8**. Show that $\Delta$ satisfies the properties

(1) $\Delta(X^{p^2}, Y) = \Delta(X,Y)^p$

(2) $\Delta(X, Y^{p^2}) = \Delta(X,Y)^p$
(3) $\Delta(X^p, Y^p) = \Delta(X,Y)^{-p}$
(4) $\Delta(Y,X) = \Delta(X,Y)^{-1}$.

More generally, show that

$$((x_0, x_1, \dots), (y_0, y_1, \dots)) \mapsto (\Delta(x_0, y_0), \Delta(x_1, y_1)^{-1}, \dots)$$

(the signs alternate) defines an alternating map of formal $\mathbb{Q}_p$-vector spaces

$$\tilde{\mathscr{G}} \times \tilde{\mathscr{G}} \to \hat{\tilde{\mathbb{G}}}_m.$$

**Exercise B9**. If $V$ is a 2-dimensional vector space, and $\lambda\colon V \times V \to W$ is an alternating map, then of course $\lambda$ must factor through the exterior square $\wedge^2 V$. Does something like this hold when we replace $V$ with the formal vector space $\tilde{\mathscr{G}}$, and $\wedge^2 V$ with $\hat{\tilde{\mathbb{G}}}_m$? If so, it will be easy to use Exercise B8 to argue that (perhaps up to an element of $\mathbb{Q}_p^\times$) that the expression for $\Delta(X,Y)$ in these exercises actually agrees with the one used in Cor. 6.0.4 (which was derived from the Weil pairing on an elliptic curve).

## 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.

[Dri74] V. G. Drinfel′d, *Elliptic modules*, Mat. Sb. (N.S.) **94(136)** (1974), 594–627, 656. MR 0384707 (52 #5580)

[Fal10] Gerd Faltings, *Coverings of p-adic period domains*, J. Reine Angew. Math. **643** (2010), 111–139.

[GH94] B. H. Gross and M. J. Hopkins, *Equivariant vector bundles on the Lubin-Tate moduli space*, Topology and representation theory (Evanston, IL, 1992), Contemp. Math., vol. 158, Amer. Math. Soc., Providence, RI, 1994, pp. 23–88.

[Haz78] Michiel Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, vol. 78, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[LT65] Jonathan Lubin and John Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), 380–387.

[LT66] ———, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–59.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[SW12] Peter Scholze and Jared Weinstein, *Moduli of p-divisible groups*, Available on the arxiv., 2012.

[Tat67] J. T. Tate, *p-divisible groups*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 158–183.

[Tat97] John Tate, *Finite flat group schemes*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 121–154.

[Wei12] Jared Weinstein, *Semistable models for modular curves of arbitrary level*, Available on the arxiv., 2012.