UNIVERSITÀ
DEGLI STUDI
DI MILANO

ALGANT Master's Thesis

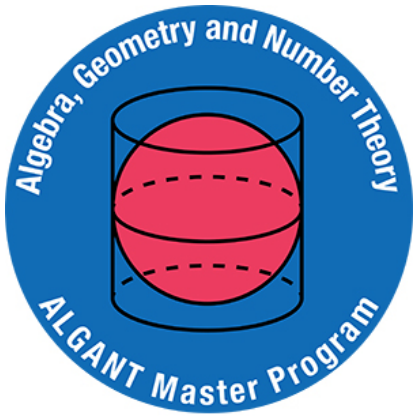
---

p-adic Modular Forms

Ananyo Kazi

Supervisor: Prof. Fabrizio Andreatta

Co-supervisor: Prof. Adrian Iovita



Academic Year 2018/19

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: Ananyo Kazi

Entitled: p-adic Modular Forms

and submitted in partial fulfillment of the requirements for the degree of

Master of Science in Mathematics

complies with the regulations of the University and meets the accepted standard with respect to originality and quality.

Signed by the final examining committee:

Chair	Prof. Carlo Mazza
Examiner	Prof. Peter Stevenhagen
Thesis supervisor	Prof. Fabrizio Andreatta
Thesis co-supervisor	Prof. Adrian Iovita

Approved by

Graduate Program Director	Dr. Galia Dafni
Dean of Graduate Studies	Dr. Paula Wood-Adams

Date: 15/07/2019

Introduction

In his 1973 paper, *Formes modulaires et fonctions zêta p-adiques* [Ser73], J.P. Serre showed that if a sequence of modular forms (thought of as power series expansions with coefficients in $\mathbb{Z}_{(p)}$) converge (in the p-adic uniform topology) then so do their weights in the group of continuous characters of $\mathbb{Z}_p^\times$. Such a p-adic limit of modular forms was his definition for a p-adic modular form. The proof relied on certain congruence relations for the coefficients of Eisenstein series due to Kummer and Clausen-von Staudt. More precisely, for any prime $p \geq 5$, $E_{p-1} \equiv 1 \bmod p$. Hence for any $m \geq 1$, $(E_{p-1})^{p^{m-1}} \equiv 1 \bmod p^m$. Thus modulo p^m a modular form f of weight k is equal to the modular form $f(E_{p-1})^{p^{m-1}}$ whose weight is congruent to $k \bmod (p-1)p^{m-1}$. Serre proved the converse, i.e. if two non-zero modular forms are equal mod p^m, then their weights are equal mod $(p-1)p^{m-1}$. The proof used the structure theorem of mod p modular forms due to Swinnerton-Dyer [Swi73], and in particular the fact that the graded algebra of mod p modular forms is integrally closed.

These results become more transparent upon studying the geometry of modular curves classifying isomorphism classes of elliptic curves, with some level N structure prime to p to avoid representability issues. In this optic meromorphic modular forms become sections of a line bundle $\underline{\omega}$ on the affine modular curve $Y(N)$, and are said to be holomorphic if they can be extended to the cusps. The line bundle in question is the direct image of the sheaf of differential on the universal elliptic curve, which locally on $Y(N)$ is nothing but the sheaf of invariant differentials on the universal elliptic curve. A global section of the k-th power of this sheaf is a modular form of weight k. This is the approach taken by N.M. Katz in his paper *p-adic properties of modular schemes and modular forms* [Kat73]. Chapter 1 of this thesis studies this approach with a brief section on elliptic curve. We follow Katz-Mazur [KM85] for the section

on elliptic curves, and Katz [Kat73] for the section on modular forms.

Since over $\mathbb{F}_p$ we have the Hasse invariant, which is a modular form of weight $p-1$ whose q-expansions at the cusps are all equal to 1, in a p-adic theory of modular forms one expects a lift of the Hasse invariant to be invertible. This is made precise by Katz by focusing on "rigid analytic" open subsets of the modular curve obtained by removing p-adic discs of various radii around the supersingular points. In particular one can focus on the locus where the Hasse invariant is invertible, called the ordinary locus. One can consider the formal scheme associated to the compatible family of $\mathbb{Z}/p^m\mathbb{Z}$-schemes corresponding to the open subscheme where any lift of the Hasse invariant is invertible, and get the formal ordinary locus $\mathfrak{X}^{\text{ord}}$. A p-adic ordinary modular form according to Katz's definition is a section of $\underline{\omega}^k$ over the formal ordinary locus. We study this in detail in Chapter 2, closely following Katz [Kat73].

Over $\mathbb{Z}/p^m\mathbb{Z}$ the sheaf $\underline{\omega}$ becomes trivial once the connected part of the p^m-torsion (or dually the étale quotient) of the universal elliptic curve is trivialized. That is if we consider a cover of the ordinary locus, that classifies isomorphism classes of elliptic curves with good ordinary reduction and a trivialization of the connected part of the p^m-torsion, then this cover is representable and the projection is étale of degree $\varphi(p^m) = (p-1)p^{m-1}$. It is also a $(\mathbb{Z}/p^m\mathbb{Z})^\times$-torsor, with the group acting naturally on the generators of $E[p^m]^\circ$ (dually $E[p^m]^{\text{ét}}$). Thus a section of $\underline{\omega}^k$ over this cover descends to a section over the ordinary locus iff it is invariant under the action of the Galois group $(\mathbb{Z}/p^m\mathbb{Z})^\times$. This construction of the cover for varying m gives rise to the Katz tower, at the infinite level of which, the formal group of the universal elliptic curve has been trivialized. Ordinary p-adic modular forms are just the ring of functions on this space, transforming via a continuous character of $\mathbb{Z}_p^\times$.

In a similar fashion one can construct the tower which simultaneously trivializes both the connected part and the étale quotient of $E[p^\infty]$ or equivalently extensions of $E[p^\infty]$ as $\mu_{p^\infty} \to E[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p$. This is called the Igusa tower and it is an étale Galois extension over the Katz tower. There is a natural section of the projection $M_{\text{Igusa}} \to M_{\text{Katz}}$, given by the duality of $\hat{E}[p^\infty]$ and $E[p^\infty]^{\text{ét}}$. Over M_{Igusa} one can consider covers classifying splittings of $E[p^\infty]$. One can show that these covers are representable too, but unfortunately no longer étale. In fact they are totally ramified, and the tower at the infinite level, called the big Igusa tower is the perfection of the Igusa tower over $\mathbb{F}_p$.This is the object of study of Chapter 3. We primarily follow the article by Sean

Howe [How18].

Nevertheless the $M_{\text{big Igusa}}$ tower has nice geometric properties. Since it classifies splittings of $E[p^\infty]$, it also gives an isomorphism of the universal cover [SW12, Section 3.1] of $E[p^\infty]$ with $\widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p$. In fact while it does not classify "isomorphism" classes of ordinary elliptic curves E with an isomorphism of $\widetilde{E[p^\infty]} \xrightarrow{\sim} \widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p$, one can show that it does classify "quasi-p-isogeny" classes of such objects.

The big Igusa tower has a group action coming from the automorphisms of $\mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$. The previous paragraph shows that this action can be extended to include automorphisms of the universal cover. The natural projection $M_{\text{big Igusa}} \to M_{\text{Igusa}}$ realizes $M_{\text{big Igusa}}$ as a fpqc $T_p\mu_{p^\infty}$-torsor over M_{Igusa}. One can consider the unipotent subgroup $\widetilde{\mu_{p^\infty}}$ of the extended group. The $\mathfrak{X}^{\text{ord}}$-automorphisms of M_{Igusa} (say M_p°) act via conjugation on this unipotent group and the semi-direct product extends the semi-direct product $T_p\mu_{p^\infty} \rtimes M_p^\circ$. The quotient of these two groups is exactly $\widehat{\mathbb{G}_m}$, which extends the usual action of M_p° on M_{Igusa}. This action no longer induces a morphism over $\mathfrak{X}^{\text{ord}}$. But one can show with some computation that the image of M_{Katz} under the canonical section is left invariant by this action. Hence the extended action descends to an action over M_{Katz} too.

In his paper Serre [Ser73] showed using p-adic Hecke operators that the Eisenstein series E_2, which is not a modular form in the classical sense, is in fact a p-adic modular form. If one recalls the classical result that $(\theta - k/12E_2)f$ is a modular form of weight $k+2$ for any f of weight k, then one sees immediately that θ is an operator of weight 2 on the space of p-adic modular forms. Katz showed that θ is the dual derivation of the square of the canonical differential coming from the trivialization of $\underline{\omega}$ over M_{Katz}. In the work of Sean Howe [How18], he shows that the θ operator arises as the derivation of the $\widehat{\mathbb{G}_m}$-action on M_{Katz}, by studying its effect on q-expansion. Chapter 4 is an extended study of this action. We build the necessary theory of p-divisible groups following Messing [Mes72]. For the rest we follow Sean Howe's article [How18].

Acknowledgement

I would like to take this opportunity to express my deep gratitude towards my supervisor Prof. Fabrizio Andreatta, for introducing me to this wonderful topic, besides helping me in ways unimaginable. It was a great pleasure to learn under his guidance, to sit through his fantastic lectures, and I am immensely grateful for the time and care he invested in reading and correcting early drafts of this work.

I am extremely grateful to Prof. Adrian Iovita, for being the caring person he has been, for teaching me rudiments of p-adic Hodge theory by hand, for guiding me to this course of study and always motivating me to work harder. I have been extremely fortunate to come across these two people and have them as my mentors.

I am thankful to Prof. Jan Kohlhasse for teaching me p-divisible groups and providing me the opportunity to spend the summer in Essen.

I am thankful to my parents for everything.

Lastly, I extend my gratitude to my friends Kunjakanan, Subham and Arnab in Montreal, who housed me when I didn't have a home, Sushant for sharing elephant videos, my friend Luca, without whom this thesis and probably many other things would not have been completed, and everyone else who kept me in their heart when I strayed further and further away. Thank you P. for introducing me to the obscure yet unbelievably rich craft of pencil sharpening. We all have had our days of ill-sharpened void, but there is hope.

Contents

Chapter 1

Moduli Scheme and q-Expansion Principle

1.1 Elliptic Curves

Definition 1.1.1. An elliptic curve E over a scheme S is a proper, smooth morphism $p : E \to S$, whose geometric fibres are connected curves of genus 1, together with a distinguished section $e : S \to E$

$$\begin{array}{c} E \\ {\scriptstyle p}\big\downarrow\big\uparrow{\scriptstyle e} \\ S \end{array}$$

Theorem 1.1.1. (Abel) *There exists a unique structure of commutative group scheme on E/S such that for any S-scheme T, and any three points P, Q, R in $E(T) = E_T(T)$, we have*

$$P + Q = R$$

iff there exists an invertible sheaf $\mathfrak{L}_0$ on T and an isomorphism of invertible sheaves on E_T

$$I^{-1}(P) \otimes I^{-1}(Q) \otimes I(0) \simeq I^{-1}(R) \otimes p_T^*(\mathfrak{L}_0).$$

Proof. We recall that over an algebraically closed field k the group structure is given by constructing an isomorphism between the set of closed points of the curve and

$\mathrm{Pic}^0(E_k/k)$, given by

$$P \mapsto P - [e]$$

where $[e]$ is the zero section. The general case follows by reducing it to the case of algebraically closed fields. For a complete proof, [cf. KM85, Theorem 2.1.2]. □

Let us prove a general fact about the sheaf of relative differentials of a separated group scheme $p : G \to S$.

Lemma 1.1.1. *Suppose $p : G \to S$ is a separated group scheme. Let $e : S \to G$ be the zero section. Suppose $\mathcal{I}$ is the sheaf of ideal of the zero section (thought of as a closed subscheme of G). Then there is a canonical isomorphism*

$$p^*(\mathcal{I}/\mathcal{I}^2) \simeq \Omega^1_{G/S}$$

Proof. Consider the two group scheme homomorphisms

$$G \xrightarrow{\Delta} G \times_S G$$

$$G \xrightarrow{(ep,\mathrm{id})} G \times_S G$$

Both are closed immersions since G is separated over S. If $\mathcal{J}$ is the ideal sheaf of $\Delta(G)$ then $\Omega^1_{G/S} = \Delta^*(\mathcal{J}/\mathcal{J}^2)$. Since Δ is a closed immersion we will henceforth drop the pull back and simply write $\Omega^1_{G/S} = \mathcal{J}/\mathcal{J}^2$. We have a commutative fibre diagram

$$\begin{array}{ccccccc} G & \xrightarrow{(p,\mathrm{id})} & S \times_S G & \xrightarrow{(e,\mathrm{id})} & G \times_S G & \longrightarrow & G \\ & & \downarrow p & & \downarrow p' & & \downarrow p \\ & & S & \xrightarrow{e} & G & \xrightarrow{p} & S \end{array}$$

Hence the ideal sheaf of $(ep, \mathrm{id})(G)$ is $(p')^*(\mathcal{I})$. Let $\varphi : G \times G \to G \times G$ be the map which is described on points as

$$\begin{aligned} G \times G &\xrightarrow{\varphi} G \times G \\ (g, h) &\mapsto (gh, h) \end{aligned}$$

Then φ is an isomorphism of group schemes and we have $\Delta = \varphi \circ (ep, \mathrm{id})$. In particular

we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{J} & \longrightarrow & \mathcal{O}_{G\times G} & \xrightarrow{\Delta^{\#}} & \mathcal{O}_G & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \varphi^{\#}} & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & (p')^*\mathcal{I} & \longrightarrow & \mathcal{O}_{G\times G} & \xrightarrow{(ep,\mathrm{id})^{\#}} & \mathcal{O}_G & \longrightarrow & 0 \end{array}$$

Since both the vertical arrows are isomorphisms, we get an isomorphism $\mathcal{J} \xrightarrow{\sim} (p')^*\mathcal{I}$. This induces an isomorphism $\mathcal{J}/\mathcal{J}^2 \simeq (p')^*\mathcal{I}/(p')^*\mathcal{I}^2 \simeq (p')^*(\mathcal{I}/\mathcal{I}^2)$. Since $\mathcal{I}/\mathcal{I}^2$ is supported on the zero section, $(p')^*(\mathcal{I}/\mathcal{I}^2) \simeq p^*(\mathcal{I}/\mathcal{I}^2)$ which proves the lemma. □

Fact: Serre-Grothendieck duality defines a canonical trace isomorphism $R^1 f_* \Omega^1_{E/S} \xrightarrow{\sim} \mathcal{O}_S$ of formation compatible with arbitrary base change.

Definition 1.1.2. Given an elliptic curve $p : E \to S$, define

$$\underline{\omega}_{E/S} := p_* \Omega^1_{E/S}$$

Lemma 1.1.2. *$\underline{\omega}_{E/S}$ is an invertible sheaf on S, whose formation commutes with arbitrary change of base.*

Proof. Note that $\Omega^1_{E/S}$ is S-flat as it is an invertible $\mathcal{O}_E$-module and E is S-flat. So we can apply the cohomology and base change formalism developed in the appendix. Consider the base change maps induced on higher direct image sheaves by the inclusion maps of points $s \in S$, $\mathrm{Spec}\, k(s) \to S$

$$\varphi^i_s : R^i p_* \Omega^1_{E/S} \otimes_{\mathcal{O}_{S,s}} k(s) \to H^i(E_s, \Omega^1_{E/S_s})$$

By Remark A.0.1, we know that $\varphi^1_s : R^1 p_* \Omega^1_{E/S} \otimes_{\mathcal{O}_{S,s}} k(s) \to H^1(E_s, \Omega^1_{E/S_s})$ is surjective for all $s \in S$. In fact the canonical trace isomorphism coming from Serre-Grothendieck duality as stated above, shows that $R^1 p_* \Omega^1_{E/S}$ is free of rank 1. Thus φ^0_s is surjective for all $s \in S$ by Theorem A.0.1. Since φ^{-1}_s is trivially surjective, this implies that $\underline{\omega}_{E/S}$ is locally free, necessarily of rank 1 as the geometric fibres of p are connected genus 1 curves. Also, Proposition A.0.1 implies that the formation of $\underline{\omega}_{E/S}$ commutes with arbitrary change of base. □

The natural adjunction map $\Omega^1_{E/S} \to e_* e^* \Omega^1_{E/S}$ induces a map of invertible $\mathcal{O}_S$-modules

$$\underline{\omega}_{E/S} = p_* \Omega^1_{E/S} \to p_* e_* e^* \Omega^1_{E/S} = e^* \Omega^1_{E/S}$$

Lemma 1.1.3. *Over any geometric fibre this map is precisely the map that assigns to a non-vanishing 1-form its corresponding invariant differential.*

Proof. Indeed, over an algebraically closed field $\bar{k}$, an elliptic curve $E/\bar{k}$ has the property that the sheaf $\mathcal{I}/\mathcal{I}^2$ of Lemma 1.1.1 is a one-dimensional $\bar{k}$-space, by virtue of being regular. Then $\Omega^1_{E/\bar{k}} \simeq \mathcal{O}_E$. In particular, the global sections are just the constant multiples of any chosen basis of the invariant differentials. □

Thus $\underline{\omega}_{E/S}$ can be naturally identified Zariski locally with the invariant differentials of E. Also, the invertible sheaf $\Omega^1_{E/S}$ is fibrewise of degree 0.

1.1.1 The Structure of the Multiplication by N Map

We follow [KM85, (2.2)] to sketch the fact that if E/S is an elliptic curve, then Zariski locally on S, E is given by a Weierstrass cubic in $\mathbb{P}^2_S$.

We have seen that Zariski locally on S, $\underline{\omega}_{E/S}$ is free. So supposing $S = \operatorname{Spec} A$, over which $\underline{\omega}_{E/S}$ admits a basis ω, we see that the formal completion $\hat{E}$ of E along its 0 section is of the form

$$\hat{E} \simeq \operatorname{Spf}(A[[T]])$$

where T is a formal parameter at 0 which is adapted to ω, i.e.

$$\omega = (1 + \text{higher terms})\, \mathrm{d}T$$

Let $\mathcal{L}(e) = \mathcal{I}^{-1}$ where $\mathcal{I}$ is the ideal sheaf of the zero section. We see that $f_*(\mathcal{L}(ne))$ is locally free of rank n on S, since by Riemann-Roch and Serre duality on the fibral cohomology, $H^1(E_s, \mathcal{L}(ne))$ vanishes for all $n > 0$. In fact since by our assumption we have a formal parameter T at 0, these sheaves are free with (non-unique) basis as follows

$$f_*(\mathcal{L}(2e)) \text{ is free on } 1,\ x$$

where $x \sim 1/T^2(1 + \text{higher terms})$, and

$$f_*(\mathcal{L}(3e)) \text{ is free on } 1,\ x, y$$

where $y \sim 1/T^3(1 + \text{higher terms})$. The powers of x and y give basis for $f_*(\mathcal{L}(ne))$ for $n \geq 4$. We see that $1, x, y, x^2, xy$ is a basis for $n = 5$ and $y^2 - x^3 \in f_*(\mathcal{L}(5e))$ since the poles of order 6 cancel each other. Thus we get a relation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Such an equation is called a generalized Weierstrass equation.

The affine ring of the complement of the zero section is given by Deligne's formula

$$H^0(E \setminus 0, \mathcal{O}_E) \simeq \varinjlim_n H^0(E, \mathcal{L}(ne))$$

and the right side is just $A[x, y]/(\text{the Weierstrass equation})$.

We quote a result about regularity in ring extensions:

Theorem 1.1.2. *Suppose A and B are Noetherian local rings and $A \to B$ is a local homomorphism via which B is a finite A-module. Assume A is regular. Then B is Cohen-Macaulay iff B is free as an A-module.*

Proof. [See Ser12, Theorem 13, pg. 83]. □

Lemma 1.1.4. *Suppose E/k is an elliptic curve over an algebraically closed field k. If N is invertible in k, the map "multiplication by N"*

$$[N] : E \to E$$

is finite étale, and the kernel is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Proof. $[N]$ induces a map by pull-back on the cotangent space at 0 given by

$$\begin{aligned} [N]^* : \mathfrak{m}/\mathfrak{m}^2 &\to \mathfrak{m}/\mathfrak{m}^2 \\ x &\mapsto Nx \end{aligned}$$

Since N is invertible in k this map is an isomorphism. Hence, in fact the map on the stalks is an isomorphism as the local rings are DVR.

$$\begin{array}{ccc} E[N] & \longrightarrow & \operatorname{Spec} k \\ \downarrow & & \downarrow \\ E & \xrightarrow{[N]} & E \end{array}$$

Since any map between complete, non-singular curves over an algebraically closed field is either constant or finite, this shows that $[N]$ is a non-constant finite morphism. Thus $E[N]$ is a finite group scheme over $\operatorname{Spec} k$. We need to show that it is étale. If $A = \Gamma(E[N], \mathcal{O}_{E[N]})$, and $\mathfrak{m}_A$ the augmentation ideal of A (i.e. the ideal sheaf of 0), then $A_{\mathfrak{m}_A} = \mathcal{O}_{E,0}/[N](\mathfrak{m}) = k$. Thus $\mathfrak{m}_A/\mathfrak{m}_A^2 = 0$. This implies $\Omega_{A/k} = A \otimes_k (\mathfrak{m}_A/\mathfrak{m}_A^2) = 0$. Thus A is separable and $E[N]$ is étale.

The result about the kernel follows from basic group theory as $E[N]$ is a finite etale group scheme over an algebraically closed field, and hence constant. □

Theorem 1.1.3. *Let S be an arbitrary scheme, E/S an elliptic curve, $N \geq 1$ an integer. Then the S-homomorphism "multiplication by N"*

$$[N] : E \to E$$

is finite locally free of rank N^2. If N is invertible on S, its kernel $E[N]$ is finite étale over S, locally for the étale topology on S isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Proof. We have seen in the beginning of the subsection that Zariski locally on S, E is given by a Weierstrass cubic in $\mathbb{P}^2_S$ with origin at $(0:1:0)$. Conversely any smooth Weierstrass cubic is an elliptic curve with origin $(0:1:0)$. Hence by reduction to the universal case, we may assume that S is the open set in $\operatorname{Spec}(\mathbb{Z}[a_1, a_2, a_3, a_4, a_6])$ over which the cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a6$$

is smooth. Note that S is regular in this case. Hence E is also regular, being smooth over S.

We first show that $[N] : E \to E$ is finite. This would imply by Theorem 1.1.2 that it

is also flat. Being proper over S, it suffices to show that the geometric fibres are finite. If $\mathrm{Spec}\, k$ is a geometric point such that $\mathrm{char}(k)$ does not divide N, $[N]$ is finite étale over k by the above lemma. So $[N]$ is finite étale over $S[1/N]$, and over an étale cover of $S[1/N]$, $E[N]$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$.

For the general case, in order to show that $[N]$ is finite flat, we need to show that it is not the zero map over geometric fibres. Take an integer M, prime to N and $\mathrm{char}(k)$ where $\mathrm{Spec}\, k$ is a geometric point. Then $E(k)$ has M^2 points of order M. Because $(N, M) = 1$, $[N]$ induces an automorphism of these points. Hence $[N]$ is not constant. Therefore $[N]$ is always finite flat. To prove that $E[N]$ is locally free of rank N^2 it suffices to pass to a geometric fibre (in fact any geometric fibre as S is connected and the rank is locally constant). There it follows from the classical theory [cf. Sil09, III, Theorem 6.2]. □

We saw in the above thoerem that $E[N]$ is étale whenever N is invertible on S. Thus it makes sense to ask if $E[N]$ is in fact the constant group scheme $(\mathbb{Z}/N\mathbb{Z})^2_S$.

Definition 1.1.3. Given an elliptic curve E/S such that N is invertible on S, a level N structure is an isomorphism

$$\alpha_N : (\mathbb{Z}/N\mathbb{Z})^2_S \to E[N]$$

Definition 1.1.4. Given two elliptic curves E, E' over S, a S-homomorphism $f : E \to E'$ is called an isogeny if it is finite locally free. In this case the kernel of the homomorphism is finite, locally free of locally constant rank. If the rank is a constant d, we say f is of degree d.

Definition 1.1.5. Given two elliptic curves E and E' over a ring R, we say $f : E \to E'$ is a p-isogeny if it is an isogeny of elliptic curves of degree p^n for some n. A global section f of $\underline{\mathrm{Hom}}_R(E, E') \otimes_{\mathbb{Z}} \mathbb{Q}$ is called a quasi-p-isogeny if $p^m f$ is a p-isogeny for some m.

Theorem 1.1.4. (Rigidity) *Let S be an arbitrary scheme, E_1 and E_2 two elliptic curves over S, and $f : E_1 \to E_2$ an S-homomorphism. Then Zariski locally on S, either $f = 0$ or f is an isogeny, i.e., f is finite locally free.*

Proof. [See KM85, Theorem 2.4.2]. □

Theorem 1.1.5. *Let E/S be an elliptic curve. The structure of an S-group scheme on E/S as given by Theorem 1.1.1 is the unique structure of S-group scheme on E/S for which $[e] = 0$ is the origin. If E and E' are two elliptic curves over S, any S-morphism $f : E \to E'$ with $f(0) = 0$ is a homomorphism.*

Proof. [See KM85, Theorem 2.5.1]. □

Theorem 1.1.6. *Let $f : E \to E'$ be an isogeny of elliptic curves over a connected base S. Then there exist a unique dual isogeny $f^t : E' \to E$ such that $f^t f = \deg(f)$.*

Proof. We recall the construction of the dual isogeny for elliptic curves E, E' over a field k. For the general case, [cf. KM85, Theorem 2.5.1, Theorem 2.6.1]. Under the identification

$$\begin{array}{ccc} E & \xrightarrow{\sim} & \mathrm{Pic}^0(E/k) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_*} \\ E' & \xrightarrow{\sim} & \mathrm{Pic}^0(E'/k) \end{array}$$

the dual map is given by the pull-back

$$f^* : \mathrm{Pic}^0(E'/k) \to \mathrm{Pic}^0(E/k)$$

If $\deg(f) = d$, then for any point $Q \in E'$, $f^*([Q]) = (\deg_i f)([P_1] + \ldots [P_s])$ where $f^{-1}(Q) = \{P_1, \ldots, P_s\}$ and $\deg_i f$ is the inseparable degree of f, which is the same as the ramification index for all the P_i. Here s is the separable degree $\deg_s f$ of f. Similarly, $f^*([0]) = (\deg_i f)([T_1] + \cdots + [T_s])$ where $f^{-1}(0) = \{T_1, \ldots, T_s\}$. Hence

$$f^*([Q] - [0]) = (\deg_i f) \sum_{i=1}^{s} ([P_i] - [T_i])$$

By choosing one particular $P \in f^{-1}(Q)$, we see that all the P_i are the translates of P by the T_i's. That is, $[P_i] = [P] + [T_{\sigma(i)}] - [0]$ for some permutation σ of $\{1, \ldots, s\}$. Hence the equality becomes

$$f^*([Q] - [0]) = (\deg_i f)(\deg_s f)([P] - [0]) = (\deg f)([P] - [0])$$

Applying this to $Q = f(P)$ we get the desired map. The uniqueness of f^t follows from

the surjectivity of f in the fppf topology. □

Theorem 1.1.7. *For a pair of dual isogenies $f : E \to E'$ and $f^t : E' \to E$ of degree N between elliptic curves over a base S, there is a canonical bilinear pairing of finite locally free commutative S-group schemes called the Weil pairing.*

$$e_f : \ker f \times \ker f^t \to \mu_N$$

Proof. [See KM85, (2.8)]. □

1.1.2 Lattices and Elliptic Curves

Given a lattice $L \subset \mathbb{C}$, we can form the quotient $\mathbb{C}/L$, which is a one-dimensional complex torus with an abelian group structure inherited from that of $\mathbb{C}$. The Weierstrass $\wp$ function gives an embedding of $\mathbb{C}/L$ into $\mathbb{P}^2$ by the inhomogeneous equation

$$y^2 = 4x^3 - g_2 x - g_3$$

such that the translation invariant 1-form $\omega = \mathrm{d}z$ is the differential $\mathrm{d}x/y$. The embedding is given as

$$0 \neq z \in \mathbb{C}/L \mapsto (\wp(z; L), \wp'(z; L))$$

where

$$\wp(z; L) = \frac{1}{z^2} + \sum_{l \in L - \{0\}} \Big(\frac{1}{(z-l)^2} - \frac{1}{l^2} \Big)$$

$$g_2 = 60 \sum_{l \in L - \{0\}} 1/l^4, \;\; g_3 = 140 \sum_{l \in L - \{0\}} 1/l^6$$

The inhomogeneous equation defines a non-singular, cubic curve which thus is an elliptic curve. Conversely, given an elliptic curve $E/\mathbb{C}$, together with a non-vanishing everywhere holomorphic differential ω, it arises in the above way from the lattice of periods of ω,

$$L(E, \omega) = \Big\{ \int_\gamma \omega \mid \gamma \in H_1(E; \mathbb{Z}) \Big\} \subset \mathbb{C}.$$

Under this correspondence the effect of replacing (E, ω) by $(E, \lambda\omega)$, $\lambda \in \mathbb{C}^\times$, is to

replace L by λL.

1.2 Modular Forms

1.2.1 Classical Complex Modular Forms

Definition 1.2.1. A complex modular form of weight k and level 1 is a holomorphic function $f(\tau)$ defined on the upper half plane which satifies the following transformation equation

$$f(\frac{a\tau+b}{c\tau+d}) = f(\tau)\cdot(c\tau+d)^k \qquad \forall \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$$

Associated to such a f one can define a function of lattices. Given a lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\mathrm{Im}(\omega_1/\omega_2) > 0$ one can define $F(L) = \omega_2^{-k} f(\omega_1/\omega_2)$. Then F is the unique function such that $f(\tau) = F(\mathbb{Z}\tau + \mathbb{Z})$, and which is homogeneous of degree $-k$ in L, i.e. $F(\lambda L) = \lambda^{-k} F(L)$ for a homothety $\lambda \in \mathbb{C}^\times$.

By Weierstrass, we can thus associate to f a "holomorphic" function $\mathbb{F}$ of pairs (E, ω) consisting of an elliptic curve over $\mathbb{C}$ together with a nowhere vanishing differential which is homogeneous of degree $-k$ in the second variable. $\mathbb{F}(E,\omega) := F(L(E,\omega))$.

This leads us to the modern, algebraic definition of modular forms. But before we get to it, we will recall the definition of the Tate curve.

1.2.2 Holomorphy at ∞ and the Tate Curve

Recall that a complex modular form $f(\tau)$ is said to be meromorphic (resp. holomorphic) at ∞, if the periodic function $f(\tau) = f(\tau+1)$, when viewed as a function of $q = \exp(2\pi i\tau)$, holomorphic for $0 < |q| < 1$, in fact extends to a meromorphic (resp. holomorphic) function of q in $|q| < 1$.

In terms of $\mathbb{F}$ we are asking about the behaviour of

$$\mathbb{F}(\mathbb{C}/2\pi i\mathbb{Z} + 2\pi i\tau\mathbb{Z}, 2\pi i \mathrm{d}z) = \mathbb{F}(\mathbb{C}^\times/q^{\mathbb{Z}}, \mathrm{d}t/t)$$

(where $t = \exp(2\pi i z)$ is the parameter on $\mathbb{C}^\times$, and $q^{\mathbb{Z}}$ denotes the subgroup of $\mathbb{C}^\times$ generated by q), as q tends to 0. By standard calculations, the curve $\mathbb{C}/L$, $L = 2\pi i\mathbb{Z} + 2\pi i\tau\mathbb{Z}$ with differential $2\pi i \mathrm{d}z$ is given as the plane cubic

$$Y^2 = 4X^3 - \frac{E_4}{12}X + \frac{E_6}{216} \quad \text{with differential } \mathrm{d}X/Y \tag{1.1}$$

The coefficients are the Eisenstein series

$$12 \cdot (2\pi i)^4 g_2(\tau) = E_4 = 1 + 240 \sum \sigma_3(n) q^n$$
$$216 \cdot (2\pi i)^6 g_3(\tau) = E_6 = 1 - 504 \sum \sigma_5(n) q^n$$

Thus to ask that the modular form f be meromorphic (resp. holomorphic) at ∞ is to ask that $\mathbb{F}\big(Y^2 = 4X^3 - E_4/12X + E_6/216, \mathrm{d}X/Y\big)$ lie in the ring $\mathbb{C}((q))$ of finite tailed Laurent series (resp. that it lie in $\mathbb{C}[[q]]$, the ring of formal power series in q).

Equation (1.1) in fact defines an elliptic curve over the ring $\mathbb{Z}[1/6]((q))$. In fact, if we let

$$X = x + 1/12, \quad Y = x + 2y$$

then we can rewrite the equation in the form

$$y^2 + xy = x^3 + B(q)x + C(q) \tag{1.2}$$

with coefficients

$$B(q) = -5\Big(\frac{E_4 - 1}{240}\Big) = -5\sum_{n\geq 1} \sigma_3(n) q^n$$
$$C(q) = \frac{-5\big(\frac{E_4-1}{240}\big) - 7\big(\frac{E_6-1}{-504}\big)}{12} = \sum_{n\geq 1} \Big(\frac{-5\sigma_3(n) - 7\sigma_5(n)}{12}\Big) q^n$$

Equation (1.2) defines an elliptic curve over $\mathbb{Z}((q))$ whose restriction to $\mathbb{Z}[1/6]((q))$ is the above curve, and the nowhere vanishing differential $\mathrm{d}x/2y + x$ restricts to give $\mathrm{d}X/Y$ over $\mathbb{Z}[1/6]((q))$.

By definition the Tate curve $\mathrm{Tate}(q)$ with its canonical differential ω_{can} is the elliptic curve over $\mathbb{Z}((q))$ defined by equation (1.2), with differential $\omega_{\mathrm{can}} = \mathrm{d}x/2y + x$. For each

integer $n \geq 1$, the Tate curve $\mathrm{Tate}(q^n)$ with its canonical differential ω_{can} is deduced from $(\mathrm{Tate}(q), \omega_{\mathrm{can}})$ by the extension of scalars $\mathbb{Z}((q)) \to \mathbb{Z}((q))$ sending $q \mapsto q^n$.

Let ζ_n be a primitive nth root of unity. The points of order n on $\mathbb{C}^\times/q^{n\mathbb{Z}}$ are the images of the n^2 points

$$(\zeta_n^i)q^j, \qquad 0 \leq i, j \leq n-1$$

Using the explicit expressions for x and y as functions of $t = \exp(2\pi i z)$

$$x(t) = \sum_{k\in\mathbb{Z}} \frac{q^{nk}t}{(1-q^{nk}t)^2} - 2\sum_{k\geq 1}\frac{q^{nk}}{1-q^{nk}}$$
$$y(t) = \sum_{k\in\mathbb{Z}} \frac{(q^{nk})^2}{(1-q^{nk}t)^3} + \sum_{k\geq 1}\frac{q^{nk}}{1-q^{nk}},$$

one sees that each of the non-zero points of order n has x and y coordinates in $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_n, 1/n]$. Hence all level n structures on $\mathrm{Tate}(q^n)$ over $\mathbb{Z}((q))$ are defined over $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_n, 1/n]$ (rather than just over $\mathbb{Z}[\zeta_n, 1/n]((q))$).

1.2.3 Modular Forms of Level 1

Definition 1.2.2. A modular form of weight $k \in \mathbb{Z}$ and level 1 is a rule f which assigns to any elliptic curve E/S a section $f(E/S)$ of $(\underline{\omega}_{E/S})^{\otimes k}$ over S such that the following two conditions are satisfied:

1. $f(E/S)$ depends only on the S-isomorphism class of the elliptic curve E/S.
2. The formation of $f(E/S)$ commutes with arbitrary change of base $g : S' \to S$; i.e. $f(E_{S'}/S') = g^* f(E/S)$.

We denote by $M(\mathbb{Z}; 1, k)$ the $\mathbb{Z}$-module of such forms.

Equivalently, a modular form of weight k and level 1 is a rule f which assigns to every pair $(E/R, \omega)$ for a ring R together with a basis ω of $\underline{\omega}_{E/R}$, an element $f(E/R, \omega) \in R$, such that the following three conditions are satisfied:

1. $f(E/R, \omega)$ depends only on the R-isomorphism class of the pair $(E/R, \omega)$.

2. f is homogeneous of degree $-k$ in the"second variable"; i.e. for any $\lambda \in R^\times$,

$$f(E, \lambda\omega) = \lambda^{-k} f(E, \omega)$$

.

3. The formation of $f(E/R, \omega)$ commutes with arbitrary extension of scalars $g : R \to R'$; i.e. $f(E_{R'}/R', \omega_{R'}) = g(f(E/R, \omega))$.

The correspondence between the two notions is given by the formula

$$f(E/\operatorname{Spec} R) = f(E/R, \omega) \cdot \omega^{\otimes k}$$

(valid whenever $\underline{\omega}_{E/R}$ is a free R-module, with basis ω).

If in the preceding definitions we restricted ourselves to the category of elliptic curves over a fixed base scheme $\operatorname{Spec} R_0$, we obtain the notion of a modular form of weight k and level one defined over R_0, the R_0 module of which is denoted by $M(R_0; 1, k)$.

A modular form of weight k and level 1 defined over R_0 can be evaluated on the pair $(\mathrm{Tate}(q), \omega_{\mathrm{can}})_{R_0}$ consisting of the Tate curve and its canonical differential, viewed as an elliptic curve with differential over $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$.

Definition 1.2.3. The q-expansion of a modular form f is defined to be the finite tailed Laurent series

$$f((\mathrm{Tate}(q), \omega_{\mathrm{can}})_{R_0}) \in \mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$$

Definition 1.2.4. A modular form f is called holomorphic at ∞ if its q-expansion lies in the subring $\mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0$. The module of all such is denoted by $S(R_0; 1, k)$.

Remark 1.2.1. The q-expansion of a modular form f lies in $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$, i.e., it is a finite R_0-linear combination of elements of $\mathbb{Z}((q))$. This implies for instance that if R_0 is the field of fractions of a discrete valuation ring, then the q-expansion coefficients of any modular form of weight k and level 1 over R_0 have bounded denominators.

1.2.4 Modular Forms of Level N

Definition 1.2.5. Assume S is a scheme where N is invertible. A modular form of weight k and level N is a rule which assigns to each pair $(E/S, \alpha_N)$ consisting of an elliptic curve together with a level N structure, a section $f(E/S, \alpha_N)$ of $(\underline{\omega}_{E/S})^{\otimes k}$ over S, in a way which only depends on the S-isomorphism class of $(E/S, \alpha_N)$, and which commutes with arbitrary change of base $g : S' \to S$.

Exactly as in the case of modular forms of level 1, one can define the notion of a modular form of weight k and level N defined over a ring R_0, by restricting to the category of elliptic curves over R_0. The R_0-module of all such is denoted by $M(R_0; N, k)$.

A modular form of weight k and level N defined over R_0 which contains $1/N$ and a N-th root of unity ζ_N can be evaluated on the triples $((\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \alpha_N)_{R_0})$ consisting of the Tate curve $\mathrm{Tate}(q^N)$ with its canonical differential, viewed as defined over $\mathbb{Z}((q))\otimes_{\mathbb{Z}} R_0$, together with any of its level N structures.

Definition 1.2.6. The q-expansions of the modular form f are the finitely many finite-tailed Laurent series

$$f((\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \alpha_N)_{R_0}) \in \mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$$

obtained by varying over all the level N structures.

Definition 1.2.7. A modular form defined over any ring R_0 is said to be holomorphic at ∞ if its inverse image on $R_0[1/N, \zeta_N]$ has all its q-expansions in $\mathbb{Z}[[q]]\otimes_{\mathbb{Z}} R_0[1/N, \zeta_N]$. The module of all such is denoted by $S(R_0; N, k)$.

A modular form (resp. holomorphic at ∞) of weight k and level N which does not depend on the "last variable" α_N is a modular form (resp. holomorphic at ∞) of weight k and level 1 defined over $R_0[1/N]$.

1.2.5 The Modular Schemes $Y(N)$ and $X(N)$

In this section we are going to assume the existence of the modular scheme $Y(N)$ which represents the moduli problem that classifies for each integer $N \geq 3$ the isomorphism

classes of elliptic curves with level N structure over $\mathbb{Z}[1/N]$. We are going to state some facts and properties of this scheme following Katz, [Kat73, Section 1.4] whose proofs are beyond the scope of this work.

The modular scheme $Y(N)$ is an affine smooth curve over $\mathbb{Z}[1/N]$, finite and flat of degree $= \#(\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1)$ over the affine j-line $\mathrm{Spec}\,(\mathbb{Z}[1/N, j])$, and étale over the open set of the affine j-line where j and $j-1728$ are invertible. We will denote the universal elliptic curve over $Y(N)$ as $\mathcal{E}/Y(N)$. The normalization of the projective j-line $\mathbb{P}^1_{\mathbb{Z}[1/N]}$ in $Y(N)$ is a proper and smooth curve $X(N)$ over $\mathbb{Z}[1/N]$, whose global sections are $\mathbb{Z}[1/N, \zeta_N]$. The curve $Y(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N]$ (resp $X(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N]$) is a disjoint union of $\varphi(N)$ affine (resp. proper) smooth geometrically connected curves over $\mathbb{Z}[1/N, \zeta_N]$, the partitioning into components given by the $\varphi(N)$ primitive roots of 1 occurring as values of the Weil pairing on the basis of $E[N]$ specified by the level N structure. The scheme $X(N) - Y(N)$ with its reduced induced structure is finite and étale over $\mathbb{Z}[1/N]$, and over $\mathbb{Z}[1/N, \zeta_N]$, it is a disjoint union of sections, called the cusps of $X(N)$. The completion of $X(N)$ along any of the cusps is isomorphic to $\mathbb{Z}[1/N, \zeta_N][[q]]$. The cusps correspond naturally to the set of isomorphism classes of level N structures on the Tate curve $\mathrm{Tate}(q^N)$ viewed over $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} \mathbb{Z}[1/N, \zeta_N]$. The completion of the projective j-line $\mathbb{P}^1_{\mathbb{Z}[1/N,\zeta_N]}$ along ∞ itself is isomorphic to $\mathbb{Z}[1/N, \zeta_N][[q]]$, via the formula $j(\mathrm{Tate}(q)) = 1/q + 744 + \ldots$, and the endomorphism of $\mathbb{Z}[1/N, \zeta_N][[q]]$ arising from the projection $X(N) \to \mathbb{P}^1$ is given by $q \mapsto q^N$.

1.2.6 The Invertible Sheaf $\underline{\omega}$ on $X(N)$, and Holomorphic Modular Forms

There is a Kodaira-Spencer isomorphism

$$\left(\underline{\omega}_{\mathcal{E}/Y(N)}\right)^{\otimes 2} \xrightarrow{\sim} \Omega^1_{Y(N)/\mathbb{Z}[1/N]}$$

There is a unique invertible sheaf $\underline{\omega}$ on $X(N)$ whose restriction to $Y(N)$ is $\underline{\omega}_{\mathcal{E}/Y(N)}$ and whose sections over the completion $\mathbb{Z}[1/N, \zeta_N][[q]]$ at each cusp are precisely the $\mathbb{Z}[1/N, \zeta_N][[q]]$ multiples of the canonical differential of the Tate curve. The Kodaira-

Spencer isomorphism extends to an isomorphism

$$(\underline{\omega})^{\otimes 2} \xrightarrow{\sim} \Omega^1_{X(N)/\mathbb{Z}[1/N]}(\log(\text{cusps}))$$

Over $\mathbb{Z}[1/N, \zeta_N][[q]]$, the square of the canonical differential ω_{can} on $\text{Tate}(q^N)$ corresponds to $N \cdot \mathrm{d}q/q$.

Putting together our definition of a modular form (resp. holomorphic) from before and the existence of a universal elliptic curve over the modular scheme $Y(N)$, we get

Definition 1.2.8. A modular form of level N and weight k defined over any ring R_0 is a global section of the line bundle $(\underline{\omega}_{\mathcal{E}/Y(N)})^{\otimes k}$ on $Y(N) \otimes_{\mathbb{Z}[1/N]} R_0$.

A modular form is called holomorphic at ∞ if such a section can be extended to a section of $(\underline{\omega})^{\otimes k}$ on $X(N) \otimes_{\mathbb{Z}[1/N]} R_0$.

1.2.7 The q-Expansion Principle

For any $\mathbb{Z}[1/N]$-module K, we define a modular form of level N and weight k, holomorphic at ∞, with coefficients in K, to be an element of $H^0(X(N), (\underline{\omega})^{\otimes k} \otimes_{\mathbb{Z}[1/N]} K)$. As each cusp, such a modular form has a q-expansion in $K \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N] \otimes_{\mathbb{Z}} \mathbb{Z}[[q]]$.

The q-expansion principle tells us that a holomorphic modular form can be determined by its q-expansions at the cusps.

Theorem 1.2.1. *Let $N \geq 3$, K a $\mathbb{Z}[1/N]$-module, and f a modular form of level N and weight k, with coefficients in K. Suppose that on each of the $\varphi(N)$ connected components of $X(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N]$ there exist at least one cusp at which the q-expansion vanishes identically. Then $f = 0$.*

Proof. By considering the ring of dual numbers on K, $D(K) = \mathbb{Z}[1/N] \oplus K$, (where multiplication is given by $(a, k)(a', k') = (aa', ak' + a'k)$) we are reduced to the case where K is a ring over $\mathbb{Z}[1/N]$. Since the formation of cohomology of quasi-coherent sheaves commutes with filtered colimits, we are reduced to the case where K is a finitely generated ring over $\mathbb{Z}[1/N]$. Then by localising we assume K is a Noetherian, local ring. By faithful flatness of completion of a Noetherian local ring, we pass to the

completion. Using the theorem on formal functions we are reduced to the case of an Artin local ring K. Suppose $x \in X(N) \otimes_{\mathbb{Z}[1/N]} K[\zeta_N]$ be a cusp such that f vanishes in the completion along x. (Note that it makes sense to talk of a cusp as a point as $\operatorname{Spec} K[\zeta_N]$ is singleton). Consider an affine neighbourhood of x, say $\operatorname{Spec} A$. Assume x is cut out by an ideal I. Then denoting the I-adic completion of A by $\hat{A}$, we see that f lies in the kernel of the natural map $A \to \hat{A}$. By Krull's intersection theorem, this implies that there exists some $g \in 1 + I$ such that $gf = 0$. Thus f vanishes identically on $D(g)$. Hence around each cusp there is an open neighbourhood where f vanishes identically, which in turn implies that f vanishes on an open dense subset of $X(N) \otimes K$. Thus $\operatorname{Supp}(f)$ is a closed subset Z of $X(N) \otimes K$ which does not contain any of the generic points of the irreducible components. Suppose z is a generic point of Z. Then f is supported in the maximal ideal $\mathfrak{m}_z$ of $\mathcal{O}_{z,X(N)\otimes K}$. Since $\underline{\omega}$ is invertible, we can identify f (non-canonically) with an element of $\mathcal{O}_{z,X(N)\otimes K}$ such that for any $h \in \mathfrak{m}_z$, $h^n f = 0$ for some $n > 0$. Thus every element of $\mathfrak{m}_z$ is a zero divisor and hence z has depth 0. Since $X(N) \otimes K$ is smooth over K which is Artin local, it is Cohen-Macaulay. Hence the only points of depth 0 are the generic points. This is a contradiction. □

Corollary 1.2.1. (The q-expansion principle) Let $N \geq 3$, K a $\mathbb{Z}[1/N]$-module, $L \subset K$ a $\mathbb{Z}[1/N]$ submodule. Let f be a modular form of weight k, level N, holomorphic at ∞, with coefficients in K. Suppose that on each of the $\varphi(N)$ connected components of $X(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N]$ there is at least one cusp at which all the q-coefficients of f lie in $L \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N]$. Then f is a modular form with coefficients in L.

Proof. The exact sequence of $\mathbb{Z}[1/N]$-modules

$$0 \to L \to K \to K/L \to 0$$

induces on cohomology an exact sequence

$$0 \to H^0(X(N), L \otimes \underline{\omega}^{\otimes k}) \to H^0(X(N), K \otimes \underline{\omega}^{\otimes k}) \to H^0(X(N), (K/L) \otimes \underline{\omega}^{\otimes k})$$

The theorem then applied to the image of f in $H^0(X(N), (K/L) \otimes \underline{\omega}^{\otimes k})$ proves the corollary. □

1.2.8 Base-change of Modular Forms of Level $N \geq 3$

Theorem 1.2.2. *Let $N \geq 3$, and suppose either that $k \geq 2$ or that $k = 1$ and $N \leq 11$. Then for any $\mathbb{Z}[1/N]$-module K, the canonical base-change map*

$$K \otimes H^0(X(N), \underline{\omega}^{\otimes k}) \to H^0(X(N), K \otimes \underline{\omega}^{\otimes k})$$

is an isomorphism.

Proof. As stated in Corollary A.0.1, it is enough to show that $H^1(X(N), \underline{\omega}^k) = 0$. The isomorphism $(\underline{\omega})^{\otimes 2} \simeq \Omega^1_{X(N)/\mathbb{Z}[1/N]}(\log(\text{cusps}))$ and the fact that each connected component of $X(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N]$ contains at least one cusp shows that the degree of $\underline{\omega}^{\otimes k}$ is strictly greater than $2g - 2$ where g is the (common) genus of any of these connected components. Then Riemann-Roch shows that $H^1(X(N), \underline{\omega}^{\otimes k}) = 0$. The other cases follow by explicit calculation. □

1.2.9 Base-change of Modular Forms of Level 1 and 2

Theorem 1.2.3. *Let R_0 be any ring in which 2 is invertible. For every integer $k \geq 1$, the canonical map $S(\mathbb{Z}; 2, k) \otimes_{\mathbb{Z}} R_0 \to S(R_0; 2, k)$ is an isomorphism.*

Proof. Modular forms of level 2 and weight k, holomorphic at ∞ over any ring $R_0 \ni 1/2$ are precisely those modular forms of level 4 and weight k which are invariant under the action of the subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ consisting of those matrices which are $\equiv I \bmod 2$. As this group has order 16, a power of 2, we apply the projector $\frac{1}{16} \sum_{g \equiv I \ (2)} g$ to the base-change isomorphism of Theorem 1.2.2 to get the result. □

Remark 1.2.2. There are no non-zero modular forms of level 2 and odd weight k. The automorphism $-I$ transforms (E, ω, α_2) to $(E, -\omega, -\alpha_2)$. But $\alpha_2 = -\alpha_2$. Hence $f(E, \omega, \alpha_2) = f(E, -\omega, -\alpha_2) = (-1)^k f(E, \omega, \alpha_2)$.

Theorem 1.2.4. *Let R_0 be any ring in which 6 is invertible. For every integer $k \geq 1$, the canonical map*

$$S(\mathbb{Z}; 1; k) \otimes_{\mathbb{Z}} R_0 \to S(R_0; 1, k)$$

is an isomorphism.

Proof. A modular form of level 1 can be viewed as a modular form of level 4 (resp. level 3) invariant under $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ (resp. $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, defined over R_0. $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ has order 96 and $\mathrm{GL}_(\mathbb{Z}/3\mathbb{Z})$ has order 48. Their only prime factors are 2 and 3. Hence using the projection technique as above, we see that

$$S(\mathbb{Z}[1/6]; 1, k) \otimes_{\mathbb{Z}[1/6]} R_0 \to S(R_0; 1, k)$$

is an isomorphism. Now we only need to pass from $\mathbb{Z}[1/6]$ to $\mathbb{Z}$. But for any ring R, we have the fibre diagram

$$\begin{array}{ccc} S(R; 1, k) & \longrightarrow & H^0(X(3) \otimes R, \underline{\omega}^{\otimes k}) \\ \downarrow & & \downarrow \\ H^0(X(4) \otimes R, \underline{\omega}^{\otimes k}) & \longrightarrow & H^0(X(12) \otimes R, \underline{\omega}^{\otimes k}) \end{array}$$

As the formation of the diagram above commutes with flat extension of scalars, the extension $\mathbb{Z} \to \mathbb{Z}[1/6]$ gives the desired result. □

1.2.10 Modular Schemes of Level 1 and 2

We state some facts about moduli schemes of level 1 and 2. Interested readers can look up [Kat73, Section 1.9] for more details. The moduli problems for level 1 and 2 are not representable. But, for each $N \geq 3$, one can form the quotients

$$\begin{aligned} Y(N)/\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) &= \text{the affine } j-\text{line } \mathbb{A}^1_{\mathbb{Z}[1/N]} \\ X(N)/\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) &= \text{the projective } j-\text{line } \mathbb{P}^1_{\mathbb{Z}[1/N]} \end{aligned}$$

which fit together for variable N to give the affine and projective j-lines over $\mathbb{Z}$. We define $Y(1) = \mathbb{A}^1_{\mathbb{Z}}$ and $X(1) = \mathbb{P}^1_{\mathbb{Z}}$.

Similarly for $N = 2$ we define

$$\begin{aligned} Y(2) &= Y(4)/\text{the subgroup of } \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \text{ consisting of matrices } \equiv I \bmod 2 \\ X(2) &= X(4)/\text{the subgroup of } \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \text{ consisting of matrices } \equiv I \bmod 2 \end{aligned}$$

The scheme $Y(2)$ is $\mathrm{Spec}\,\mathbb{Z}[\lambda][1/2\lambda(1-\lambda)]$, and $X(N)$ is the projective λ-line $\mathbb{P}^1_{\mathbb{Z}[1/2]}$.

1.2.11 Modular Forms of Level 1 and 2: q-Expansion Principle

Definition 1.2.9. For $N = 1, 2$, and any $\mathbb{Z}[1/N]$-module K, define a modular form of level N and weight k, holomorphic at ∞, with coefficients in K to be (i) for $N = 1$, an element of the fibre product of the diagram

$$\begin{array}{ccc} S(K;1,k) & \longrightarrow & H^0(X(3), \underline{\omega}^{\otimes k} \otimes_{\mathbb{Z}[1/3]} (K \otimes_{\mathbb{Z}} \mathbb{Z}[1/3])) \\ \downarrow & & \downarrow \\ H^0(X(4), \underline{\omega}^{\otimes k} \otimes_{\mathbb{Z}[1/4]} (K \otimes_{\mathbb{Z}} \mathbb{Z}[1/4])) & \longrightarrow & H^0(X(12), \underline{\omega}^{\otimes k} \otimes_{\mathbb{Z}[1/12]} (K \otimes_{\mathbb{Z}} \mathbb{Z}[1/12])) \end{array}$$

(ii) for $N = 2$, an element of $H^0(X(4), \underline{\omega}^{\otimes k} \otimes_{\mathbb{Z}[1/4]} K)$ invariant under the action of the subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ consisting of matrices $\equiv I \bmod 2$.

The module of all such is denoted $S(K; N, k)$.

Corollary 1.2.2. (q-expansion principle) Let $N = 1$ or 2, K a $\mathbb{Z}[1/N]$-module, and $L \subset K$ a $\mathbb{Z}[1/N]$-module. Let f be a modular form of weight k, level N, holomorphic at ∞, with coefficients in K. Suppose that at one of the cusps (for $N = 1$ there is exactly one, $j = \infty$, while for $N = 2$ there are 3, $\lambda = 0, 1, \infty$), the q-coefficients of f all lie in L. Then f is a modular form with coefficients in L.

Proof. Follows from Theorem 1.2.1. □

Chapter 2

p-adic Modular Forms

2.1 The Hasse Invariant

Let S be an $\mathbb{F}_p$-scheme and consider an elliptic curve E/S. Let us recall the Frobenius isogeny and its dual Vershchiebung.

2.1.1 Frobenius and Verschiebung

Definition 2.1.1. For any $\mathbb{F}_p$-scheme S, the absolute Frobenius is defined to be the map $\mathrm{Frob} : S \to S$ which is identity on the underlying topological space, and induces the $\mathbb{F}_p$-endomorphism $x \mapsto x^p$ on the sheaf $\mathcal{O}_S$.

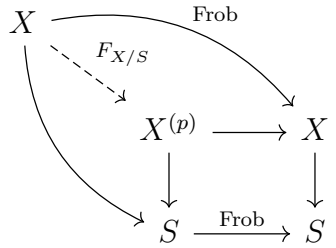
For a scheme $X/S/\mathbb{F}_p$, the absolute Frobenius defines a scheme $X^{(p)}$ as the base change of X through $\mathrm{Frob} : S \to S$. That is, we have the following commutative diagram

$$\begin{array}{ccc} X^{(p)} & \longrightarrow & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{\mathrm{Frob}} & S \end{array}$$

The absolute Frobenius for both X and S gives a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\text{Frob}} & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{\text{Frob}} & S \end{array}$$

This then induces a natural map by the universal property of the fibre product



Definition 2.1.2. For any scheme $X/S/\mathbb{F}_p$ the S-linear map $F_{X/S}$ defined by the above construction is called the relative Frobenius. When there is no confusion about the schemes, we will write $F = F_{X/S}$.

If we assume both $S = \operatorname{Spec} A$ and $X = \operatorname{Spec} B$ are affine, and

$$B = A[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$$

then $X^{(p)} = \operatorname{Spec} B^{(p)}$ with

$$B^{(p)} = A[x_1, \ldots, x_n]/(f_1^{(p)}, \ldots, f_m^{(p)})$$

where the polynomials $f_i^{(p)}$ are obtained from f_i just by raising their coefficients to the p-th power. On R-valued points the relative Frobenius F is given by

$$(a_1, a_2, \ldots) \mapsto (a_1^p, a_2^p, \ldots)$$

Let us now suppose E/S is an elliptic curve and $F = F_{E/S}$ the relative Frobenius of E over S.

Lemma 2.1.1. *If $S = \operatorname{Spec} k$ where k is an algebraically closed field of characteristic p, then $F_{E/S}$ is an isogeny of degree p.*

Proof. The description of F on affine coordinates as

$$(x, y) \mapsto (x^p, y^p)$$

shows that it is a non-constant surjective map. Also $F(0) = 0$ and thus F is an isogeny. If K is the function field of E then the function field of $E^{(p)}$ is K^p. This follows from the local description of the affine coordinate ring of E and the fact that k is perfect. The statement about degree then follows from the fact that K is a finite extension of $k(t)$ for some parameter t and the multiplicativity of degrees for field extensions. □

Corollary 2.1.1. If S is an $\mathbb{F}_p$-scheme, and E/S an elliptic curve, then the relative Frobenius $F_{E/S} : E \to E^{(p)}$ is an isogeny of degree p.

Proof. It's enough to check over geometric fibres. □

Definition 2.1.3. Given E/S an elliptic curve, the dual isogeny of $F_{E/S}$ is called the Verschiebung, denoted as $V_{E/S}$ (or V when there is no confusion). It is of degree p and satisfies the property $VF = [p]$ and $FV = [p]$.

One can also consider the iterates F^n of F and V^n of V and the duality of F and V gives duality for the iterates. This gives the exact sequence for all $n > 0$

$$0 \to \ker F^n \to E[p^n] \to \ker V^n \to 0$$

Recall that the Weil pairing introduced in Theorem 1.1.7 gives the Cartier duality

$$\ker V^n \simeq (\ker F^n)^D$$

Over an algebraically closed field k, F is purely inseparable of degree p and hence $\ker F$ consists of only 1 point, i.e. $[0]$ is a generator for $\ker F$. This means $\ker F$ is a connected finite flat group scheme over k of order p. Hence by the classification of connected group schemes of order p over algebraically closed fields, it can either be μ_p or α_p, depending on whether $\ker V$ is étale or connected respectively.

Before proceeding to the definition of the Hasse invariant, we need to define the formal group of an elliptic curve.

Let S be a scheme, and X, Y with $Y \hookrightarrow X$ two sheaves on S for the fppf topology.

Definition 2.1.4. $\mathrm{Inf}_Y^k(X)$ is the subsheaf of X whose sections over an S-scheme T are given as follows: $\Gamma(T, \mathrm{Inf}_Y^k(X)) := \{t \in \Gamma(T, X) \mid$ there is a covering $\{T_i \to T\}$ and for each T_i a closed subscheme $\overline{T}_i$ defined by an ideal whose $k{+}1^{\text{st}}$ power is 0 with the property that $t|\overline{T}_i \in \Gamma(\overline{T}_i, Y)\}$

Lemma 2.1.2. *If X and Y are schemes and $Y \hookrightarrow X$ is a closed immersion then this definition coincides with the usual one of [Gro67, §16].*

Proof. [See Mes72, II, Lemma 1.02]. □

Lemma 2.1.3. *Let E/S be an elliptic curve. Let $\hat{E}$ be its formal completion along the zero section. Then $\hat{E}$ is a group object in the category of formal schemes.*

Proof. It is enough to show that $\hat{E}$ is closed under addition. So if $f, g \in \Gamma(T, \mathrm{Inf}^k(E))$, where $\mathrm{Inf}^k(E)$ is the k-th infinitesimal neighborhood of the zero section, we need to show that there is $k' \geq k$ such that $f + g \in \Gamma(T, \mathrm{Inf}^{k'}(E))$. Choose a covering family $T_i \to T$ and nilpotent immersions of order k $\overline{T}_i \hookrightarrow T_i$ such that $f|_{\overline{T}_i} = 0$. Choose covering $T_j \to T$ and nilpotent immersions of order k $\overline{T}_j \hookrightarrow T_j$ similarly for g. Then $T_i \times T_j \to T$ is a covering such that $\overline{T}_i \times \overline{T}_j \hookrightarrow T_i \times T_j$ are nilpotent immersions of order 2k. $f + g|_{\overline{T}_i \times \overline{T}_j} = 0$ and hence $f + g \in \Gamma(T, \mathrm{Inf}^{2k}(E))$. □

Let X be a sheaf on S and $e_X : S \to X$ be a section. Let $\mathrm{Inf}^k(X)$ be $\mathrm{Inf}_Y^k(X)$ where Y is the subsheaf defined by e_X.

Definition 2.1.5. A pointed sheaf (X, e_X) is ind-infinitesimal if $X = \varinjlim \mathrm{Inf}^k(X)$.

Definition 2.1.6. A pointed sheaf (X, e_X) on S is said to be a formal Lie variety if the following conditions are satisfied:

1. X is ind-infinitesimal and $\mathrm{Inf}^k(X)$ is representable for all $k \geq 0$.
2. $\underline{\omega}_X = e_X^*(\Omega^1_{\mathrm{Inf}^k(X)/S})$ is locally free of finite type. (Note that for any $k > 0$ the sheaf on the right side is the same).

3. Let $\mathrm{gr}^{\inf}(X)$ be the unique graded $\mathcal{O}_S$-algebra, such that $\mathrm{gr}_i^{\inf}(X) = \mathrm{gr}_i(\mathrm{Inf}^i(X))$ holds for all $i \geq 0$. Then we have an isomorphism $\mathrm{Sym}\,(\underline{\omega}_X) \xrightarrow{\sim} \mathrm{gr}^{\inf}(X)$ induced by the canonical mapping $\underline{\omega}_X \xrightarrow{\sim} \mathrm{gr}_1^{\inf}(X)$.

Definition 2.1.7. A formal Lie group over S, (G, e_G) is a group object in the category of formal Lie varieties.

Proposition 2.1.1. *With the definitions as above, the formal completion of an elliptic curve E/S along its zero section, denoted by $\hat{E}$, is a formal Lie group.*

Proof. $\hat{E}$ is by definition ind-infinitesimal, and $\mathrm{Inf}^k(E)$ is clearly representable. We have seen that the sheaf of invariant differentials $\underline{\omega}_{E/S}$ is locally free of rank 1 and $\underline{\omega}_{E/S} \simeq \mathcal{I}/\mathcal{I}^2$ where $\mathcal{I}$ is the ideal sheaf of the zero section. These two facts imply that $\hat{E}$ satisfies the last two conditions of Definition 2.1.6. □

Remark 2.1.1. Locally on S, a formal Lie group (G, e_G) is represented by the formal spectrum of a power series ring. Indeed, one only needs to have a trivialization of $\underline{\omega}_G$ to get such a representation.

2.1.2 The Hasse Invariant

Definition 2.1.8. The Hasse invariant A is a modular form of weight $p-1$ and level 1 defined as the tangent of the Verschiebung map $V : E^{(p)} \to E$

$$\begin{aligned} \mathrm{tg}(V) &\in \mathrm{Hom}_S(\mathrm{Lie}(E^{(p)}/S), \mathrm{Lie}(E/S)) \\ &= \mathrm{Hom}_S((\mathrm{Lie}(E/S)^{\otimes p}, \mathrm{Lie}(E/S)) \\ &= H^0(S, (\underline{\omega})_{E/S}^{\otimes(p-1)}) \end{aligned}$$

The fact that $\mathrm{Lie}(E^{(p)}/S) = (\mathrm{Lie}(E/S))^{\otimes p}$ follows from the base-change theorem applied to the base-change map $\mathrm{Frob} : S \to S$.

There are a bunch of ways to compute the Hasse invariant, listed in [KM85, (12.4)]. Here we mention one of them.

First we assume by localising that $S = \operatorname{Spec} R$ is affine and $\underline{\omega}_{E/R}$ is free of rank 1. Choose an R-basis of $\underline{\omega}_{E/R}$, say $\omega \in H^0(E, \Omega^1_{E/R})$. Choose a local coordinate X for the formal group $\hat{E}/R$ which is adapted to the invariant differential ω, i.e.

$$\omega = (1 + \text{higher terms})\mathrm{d}X$$

In terms of the basis ω we have $A = \mathrm{A}(E, \omega)\omega^{\otimes p-1}$ where $A(E, \omega) \in R$.

Calculating A: In the formal group expression of "multiplication by p" on $\hat{E}$ as a power series in X,

$$[p](X) = V(F(X)) = V(X^p)$$

Hence we see that $\mathrm{A}(E, \omega) = \mathrm{tg}(V) =$ coefficient of X^p in $[p](X)$.

Theorem 2.1.1. *Over any $\mathbb{F}_p$-algebra R, the value of the Hasse invariant on the Tate curve $Tate(q)/R((q))$ is given by*

$$\mathrm{A}(\mathit{Tate}(q), \omega_{\mathit{can}}) = 1$$

Proof. Let $\phi_{\mathrm{can}} : \widehat{\mathrm{Tate}(q)} \xrightarrow{\sim} \widehat{\mathbb{G}_m}$ be the unique isomorphism of formal Lie groups under which $\omega_{\mathrm{can}} = \phi^*_{\mathrm{can}}(\mathrm{d}X/X)$. Computing the coefficient of X^p in the power series expression of "multiplication by p" on $\widehat{\mathbb{G}_m}$ we see that

$$[p](X) = (1 + X)^p - 1 = X^p$$

Thus $\mathrm{A}(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = 1$. □

This theorem proves that the zeroes of the Hasse invariant lie away from the cusps. The next theorem, due to Igusa shows that the zeroes are actually simple.

Theorem 2.1.2. (Igusa) *If k is a perfect field of characteristic p, and $(R, \mathfrak{m})$ an Artin local k-algebra with residue field k, then for any elliptic curve E/R, the following conditions are equivalent:*

1. *The Verschiebung $V : E^{(p)} \to E$ has $tg(V) = 0$*
2. *There exists a supersingular elliptic curve E_0/k and an R-isomorphism $E_0 \otimes_k R \simeq E$.*

Proof. (2) $\implies$ (1) is clear. Let us prove the converse. If $\mathrm{tg}(V) = 0$, $\ker(V)$ which is finite flat of rank p, and a subgroup of $E^{(p)}[p]$ must coincide with the connected part of $E^{(p)}[p]$, having non-zero sheaf of differentials. Thus it is a subgroup of the formal group of $E^{(p)}$.

Being formal groups over characteristic p, $\hat{E}$ and $\hat{E}^{(p)}$ has an action of $\mathbb{Z}_p$, given by taking limit of the endomorphisms induced by truncated p-adic expansions. (The limit exists as $[p](X) \subset (X^p)$). Choose a coordinate X for $\hat{E}$ which linearizes the action of $\mu_{p-1} \subset \mathbb{Z}_p^\times$, and use the pullback of X on $\hat{E}^{(p)}$. For any R-homomorphism $f : \hat{E}^{(p)} \to \hat{E}$, given by

$$f(X) = \sum_{n \geq 1} a(n) X^n,$$

the formulas

$$f([\zeta](X)) = [\zeta](f(X))$$
$$f(\zeta X) = \zeta f(X)$$

for a primitive $(p-1)$th root of unity ζ, implies that

$$\zeta a(n) = \zeta^n a(n)$$

for all n. This implies that $a(n) = 0$ unless $n \equiv 1 \bmod (p-1)$ and $a(1) = \mathrm{tg}(f)$.

Therefore if $\mathrm{tg}(V) = 0$,

$$V(X) = a(p) X^p + \text{ higher order terms.}$$

$a(p) \in R^\times$ because modulo $\mathfrak{m}$, E is a supersingular elliptic curve over a field where we know the result by classical theory. Also $\ker(V) = \ker(F)$ with both coinciding with the connected part of $E^{(p)}[p]$, and is more explicitly given by $X^p = 0$.

Thus we have an isomorphism

$$\begin{array}{ccc} E^{(p)}/\ker(V) & \xrightarrow{=} & E^{(p)}/\ker(F) \\ \downarrow{\scriptstyle V} & & \downarrow{\scriptstyle F} \\ E & \xrightarrow{\sim} & E^{(p^2)} \end{array}$$

Iterating this isomorphism, we get

$$E \simeq E^{(p^2)} \simeq E^{(p^4)} \simeq \cdots \simeq E^{(p^{2n})} \simeq \ldots$$

Since R is Artin local, $\mathrm{Frob}^{2n} : R \to R$ factors through k for sufficiently large n. Thus

$$E \simeq E^{(p^{2n})} \simeq ((E \otimes_R k)^{(p^{2n})}) \otimes_k R$$

□

Corollary 2.1.2. Let k be an algebraically closed field of characteristic p, $(p, N) = 1$, $Y(N)_k$ the affine modular curve over k (which is regular). The Hasse invariant A has only simple zeroes on $Y(N)_k$.

Proof. We have seen the Hasse invariant is non-zero at the cusps. Hence it vanishes only at closed points of $Y(N)_k$. Suppose $y \in Y(N)_k$ is such a point. Denote the local ring at y by $(\mathcal{O}_{Y,y}, \mathfrak{m}_y)$. This is a DVR by regularity and we need to show that $(\mathrm{A}) = \mathfrak{m}_y$. Suppose not. Then $(\mathrm{A}) = \mathfrak{m}_y^n$ for some $n > 1$. Let $R = \mathcal{O}_{Y,y}/\mathfrak{m}_y^n$. Then the natural map $\psi : \mathrm{Spec}\, R \to Y(N)_k$ determines an elliptic curve E/R with a level N structure. For any basis ω_E of the invariant differentials of E, $\mathrm{A}(E, \omega_E) = 0$. But then by Igusa's theorem E comes from some E_0/k. Since N is coprime to p, the level N structure descends to a level N structure on E_0 by étaleness, and hence defines a point $\varphi : \mathrm{Spec}\, k \to Y(N)_k$ such that ψ factors through φ. Also the thickening map $R = \mathcal{O}_{Y,y}/\mathfrak{m}_y^n \to \mathcal{O}_{Y,y}/\mathfrak{m}_y = k$ defines a k-valued point which must be the same as φ. Hence $\mathrm{A}(E_0, \omega_{E_0}) = 0$ which contradicts the assumption that $\mathrm{ord}_y(A) > 1$. □

2.2 Deligne's Congruence $\mathrm{A} \equiv E_{p-1}$ mod p

Recall from the classical theory that for all even integer $k \geq 4$, the Eisenstein series E_k is a modular form of weight k and level 1 over $\mathbb{C}$ whose q-expansion is

$$E_k = 1 - 2k/B_k \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

where B_k is the k-th Bernoulli number and

$$\sigma_{k-1}(n) = \sum_{\substack{d|n \\ d\geq 1}} d^{k-1}$$

As its q-expansion coefficients lie in $\mathbb{Q}$, E_k is defined over $\mathbb{Q}$ by the q-expansion principle.

Lemma 2.2.1. *Let $k \in \mathbb{N}$.*

1. *(Kummer's congruence) $p-1 \nmid k$ iff $B_k/2k \in \mathbb{Z}_p$. Moreover,*

$$B_k/2k \equiv B_{k'}/2k' \ mod\ p \quad if\ k \equiv k' \not\equiv 0 \ mod\ p-1$$

2. *(Clausen-von Staudt congruence) If $p-1|k$, then $pB_k \in \mathbb{Z}_p$ and $pB_k \equiv -1$ mod p. In particular, $v_p(B_k) = -1$.*

Proof. [See BS86, Section 5.8, Theorem 4, Theorem 5]. □

The lemma shows that for $k = p-1$, $p \geq 5$, the coefficients of E_{p-1} lie in $\mathbb{Z}_{(p)}$ (the localization of $\mathbb{Z}$ at the prime (p)) and moreover, $E_{p-1} \equiv 1 \bmod p$. We have already seen a modular form of level 1 and weight $p-1$ over $\mathbb{F}_p$ whose q-expansion is 1 – the Hasse invariant. Thus we conclude by the q-expansion principle that $E_{p-1} \equiv \mathrm{A} \bmod p$.

For $p = 2, 3$ it is not possible to lift A to a modular form of level 1, holomorphic at ∞, over $\mathbb{Z}_{(p)}$. However, for $p = 2$ and $3 \leq N \leq 11$, $2 \nmid N$ we can lift A to a modular form of level N and weight 1, holomorphic at ∞, over $\mathbb{Z}[1/N]$ using the base-change theorem (Theorem 1.2.2). For $p = 3$ and any $N \geq 3$, $3 \nmid N$, we can lift A to a holomorphic modular form of level N and weight 2, over $\mathbb{Z}[1/N]$ again by the same theorem. Anyway, for each of these cases we choose a lift of A of level N (as described above) and call it E_{p-1}.

2.3 p-adic Modular Forms with Growth Conditions

In this section we will give a definition of a p-adic modular form as functions of elliptic curves over $\mathbb{Z}_p$ whose Hasse invariant (or rather its lift) has p-adic absolute value greater than some chosen constant. So we will be removing p-adic discs of various radii around the supersingular points and consider the sections of $\underline{\omega}^{\otimes k}$ restricted to the remaining "rigid analytic" open subsets.

Definition 2.3.1. Let R_0 be a p-adically complete ring. Choose $r \in R_0$. For any integer $N \geq 1$, prime to p (resp. $3 \leq N \leq 11$ for $p = 2$, and $N \geq 2$ for $p = 3$) we define a p-adic modular form over R_0 of growth r, level N and weight k as a rule which assigns to any triple $(E/S, \alpha_N, Y)$ consisting of:

1. an elliptic curve E/S, where S is a R_0-scheme where p is nilpotent
2. a level N structure α_N
3. a section Y of $\underline{\omega}_{E/S}^{\otimes(1-p)}$ satisfying $Y \cdot E_{p-1} = r$

a section $f(E/S, \alpha_N, Y)$ of $\underline{\omega}_{E/S}^{\otimes k}$ over S, which depends only on the isomorphism class of the triple, and whose formation commutes with abitrary base change of R_0-schemes.

The module of all such is denoted by $M(R_0; r, N, k)$.

Equivalently, choosing a basis ω of $\underline{\omega}_{E/R}$, one can define f to be the rule that attaches to each quadruple $(E/R, \omega, \alpha_N, Y)$ an element of R whose formation depends only on the isomorphism class of the quadruple, commutes with base extensions, and satisfies

$$f(E/R, \lambda\omega, \alpha_N, \lambda^{p-1}Y) = \lambda^{-k} f(E/R, \omega, \alpha_N, Y)$$

for $\lambda \in R^\times$. By passing to the limit, we can allow R to be a p-adically complete ring in the above definition.

f is said to be homlomorphic at ∞ if for any integer $n \geq 1$, its value on $(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \alpha_N, r(E_{p-1}(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}))^{-1})$, lies in $\mathbb{Z}[[q]] \otimes (R_0/p^n R_0)[\zeta_N]$, for each level N structure α_N. We denote by $S(R_0; r, N, k)$ the submodule of $M(R_0; r, N, k)$ consisting of forms holomorphic at ∞.

Clearly,

$$M(R_0; r, N, k) = \varprojlim M(R_0/p^n R_0; r, N, k)$$
$$S(R_0; r, N, k) = \varprojlim S(R_0/p^n R_0; r, N, k).$$

2.3.1 The Ordinary Locus $Y(N)^{\mathbf{ord}}$

We assume that p is nilpotent in R_0. In this section we will show that the moduli problem classifying isomorphism classes of triples $(E/S, \alpha_N, Y)$ over R_0-schemes S is representable for any $N \geq 3$.

Define the moduli problem

$$\begin{aligned} &\mathbf{Sch}/R_0 \xrightarrow{\mathcal{P}_{R_0,r}} \mathbf{Sets} \\ &\qquad S \mapsto S\text{-isomorphism classes of triples } (E/S, \alpha_N, Y) \end{aligned}$$

where everything is defined as above. The data of a triple $(E/S, \alpha_N, Y)$ is the same as the data of

1. A R_0-morphism $g : S \to Y(N) \otimes R_0$
2. A section Y of $g^*(\underline{\omega}^{\otimes(1-p)})$ satisfying $Y \cdot g^*(E_{p-1}) = r$.

Theorem 2.3.1. *$\mathcal{P}_{R_0,r}$ is representable.*

Proof. Denote $\underline{\omega}^{\otimes 1-p}$ by $\mathfrak{L}$ for notational convenience. Clearly $\mathcal{P}_{R_0,r}$ is a subfunctor of the functor

$$\begin{aligned} &\mathbf{Sch}/R_0 \xrightarrow{\mathcal{P}'} \mathbf{Sets} \\ &\qquad S \mapsto \{R_0\text{-morphisms } g : S \to Y(N), \text{ plus a section } Y \text{ of } g^*(\mathfrak{L})\} \end{aligned}$$

$\mathcal{P}'$ is clearly representable by the geometric vector bundle $\mathbf{V}(\mathfrak{L}^\vee)$ on $Y(N) \otimes R_0$ associated to $\mathfrak{L}^\vee$ which is the relative affine spectrum of the symmetric algebra on the line bundle $\mathfrak{L}^\vee$ [see Har13, II, exercise 5.18]. Then the subfunctor $\mathcal{P}_{R_0,r}$ is represented by the closed subscheme of $\mathbf{V}(\mathfrak{L}^\vee)$ defined by the vanishing of $E_{p-1} - r$. The universal elliptic curve with level N structure is just the pullback of the universal elliptic curve

$\mathcal{E}/(Y(N) \otimes R_0)$ under the natural projection

$$\begin{array}{c} \mathbf{V}(\mathfrak{L}^{\check{}}) \\ \big\downarrow \\ Y(N) \otimes R_0 \end{array}$$

□

Remark 2.3.1. The scheme representing $\mathcal{P}_{R_0,r}$ is in fact affine.

Having seen that $\mathcal{P}_{R_0,r}$ is representable it's now obvious that the module $M(R_0; r, N, k)$ is the global sections of the pullback of $\underline{\omega}$ on this scheme. But before we get to a good description of this module, let us say a few more things about the representing scheme.

Although we defined p-adic modular forms of growth r for any $r \in R_0$, the case of most importance to us will be when $r = 1$. Now further assume that $R_0 = \mathbb{F}_p$. Let us also denote by $\mathcal{P}_{R_0,r}$, the scheme representing the functor.

Note firstly, that $E_{p-1} = \mathrm{A}$ as we are over $\mathbb{F}_p$. Following the construction of the scheme $\mathcal{P}_{\mathbb{F}_p,1}$, we see that it is exactly the open subscheme of $Y(N)_{\mathbb{F}_p}$ where the Hasse invariant is invertible. This open subscheme is obtained by removing the finitely many closed points on $Y(N)_{\mathbb{F}_p}$ corresponding to the supersingular elliptic curves.

We see that $\mathcal{P}_{\mathbb{F}_p,1}$ is a closed subscheme of $\mathcal{P}_{\mathbb{Z}/p^m\mathbb{Z},1}$ defined by the vanishing of p which is nilpotent. Hence the underlying topological spaces of both these schemes are the same. Thus we are in a situation where we have

1. a directed system of affine schemes $\{\mathcal{P}_{\mathbb{Z}/p^m\mathbb{Z},1}\}_{m\in\mathbb{N}}$,
2. thickenings $\mathcal{P}_{\mathbb{Z}/p^m\mathbb{Z},1} \hookrightarrow \mathcal{P}_{\mathbb{Z}/p^n\mathbb{Z},1}$ for every $m < n$.

Then we can take the colimit of this system and get an affine formal scheme which we denote by $\mathfrak{X}^{\mathrm{ord}}$.

Definition 2.3.2. The formal ordinary locus is defined to be $\mathfrak{X}^{\mathrm{ord}}$. It is an affine formal scheme over $\operatorname{Spf}\mathbb{Z}_p$.

This definition also solves the problem of choice involved in a lift of A for $p = 2, 3$. Since the underlying topological space depends only on A, we can define the ordinary

locus in that case to be the formal completion of the structure sheaf of $Y(N)$ restricted to the non-vanishing locus of A, along $p = 0$.

For $r \neq 1$, one can still consider the compatible system of $\mathbb{Z}/p^m\mathbb{Z}$ family of schemes $\mathcal{P}_{\mathbb{Z}/p^m\mathbb{Z},r}$, only this time it is not guaranteed that the underlying topological space can be viewed as an open subspace of $Y(N)$. Nevertheless one can consider the formal scheme associated to this compatible family, and call it $Y(N)(R_0, r)$.

2.3.2 $M(R_0; r, N, k)$ and $S(R_0; r, N, k)$ when p is Nilpotent in R_0

Proposition 2.3.1. *When p is nilpotent in R_0, and $N \geq 3$ is prime to p, there is a canonical isomorphism*

$$\begin{aligned} M(R_0; r, N, k) &= H^0(\mathcal{P}_{R_0,r}, \underline{\omega}^{\otimes k}) \\ &= H^0\Big(Y(N) \otimes R_0, \oplus_{j\geq 0}(\underline{\omega})^{\otimes(k+j(p-1))}/(E_{p-1} - r)\Big) \\ (\textit{because } Y(N) \textit{ is affine}) &= H^0\Big(Y(N) \otimes R_0, \oplus_{j\geq 0}(\underline{\omega})^{\otimes(k+j(p-1))}\Big)/(E_{p-1} - r) \\ &= \oplus_{j\geq 0} M(R_0; N, k + j(p-1))/(E_{p-1} - r). \end{aligned}$$

Proposition 2.3.2. *Let $N \geq 3$, $p \nmid N$. Under the isomorphism of Proposition 2.3.1 the submodule $S(R_0; r, N, k) \subset M(R_0; r, N, k)$ is*

$$S(R_0; r, N, k) = H^0\Big(X(N) \otimes R_0, \oplus_{j\geq 0}\ \underline{\omega}^{\otimes k+j(p-1)}/(E_{p-1} - r)\Big)$$

.

Proof. It suffices to treat the case $R_0 \ni \zeta_N$. The completion of $X(N)$ along any of its cusps is isomorphic to $R_0[[q]]$. Just as in the proof of Theorem 2.3.1, we can consider the geometric vector bundle over $X(N) \otimes R_0$ associated to $\mathfrak{L}^\vee$. Call it $\overline{\mathbf{V}}(\mathfrak{L}^\vee)$. Denote by $\overline{\mathcal{P}}_{R_0,r}$ the closed subscheme of $\overline{\mathbf{V}}(\mathfrak{L}^\vee)$ defined by $E_{p-1} - r$. Then the ring of completion of $\overline{\mathcal{P}}_{R_0.r}$ along the inverse image of any cusp is isomorphic to

$$R_0[[q]][Y]/(Y \cdot E_{p-1}(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \alpha_N) - r) \simeq R_0[[q]]$$

as E_{p-1} is invertible at the cusps. Thus a p-adic modular form f seen as a section of $\underline{\omega}^{\otimes k}$ over $\mathcal{P}_{R_0,r}$ is holomorphic at ∞ iff it extends to $\overline{\mathcal{P}}_{R_0,r}$. The description of the module is then obvious. □

2.3.3 Determination of $S(R_0; r, N, K)$ in the Limit

Theorem 2.3.2. *Let $N \geq 3$ and suppose either that $k \geq 2$ or that $k = 1$ and $n \leq 11$, or that $k = 0$ and $p \neq 2$, or that $k = 0$, $p = 2$ and $n \leq 11$. Let R_0 be a p-adically complete ring and suppose $r \in R_0$ is not a zero-divisor in R_0. Then the homomorphism*

$$\begin{array}{c} \varprojlim H^0(X(N), \oplus_{j\geq 0}\, \underline{\omega}^{\otimes k+j(p-1)}) \otimes_{\mathbb{Z}[1/N]} (R_0/p^nR_0)/(E_{p-1} - r) \\ \downarrow \\ S(R_0; r, N, k) = \varprojlim S(R_0/p^nR_0; r, N, k) \end{array}$$

is an isomorphism.

Proof. Denote by $\mathfrak{F}$ the quasi-coherent sheaf $\oplus_{j\geq 0}\, \underline{\omega}^{k+j(p-1)}$ on $X(N)$ and put $\mathfrak{F}_n = \mathfrak{F} \otimes R_0/p^nR_0$. The inverse system of short exact sequences

$$0 \to \mathfrak{F}_n \xrightarrow{E_{p-1}-r} \mathfrak{F}_n \to \mathfrak{F}_n/(E_{p-1} - r) \to 0$$

induces an inverse system of long exact sequence in cohomology

$$\begin{array}{l} 0 \longrightarrow H^0(X(N), \mathfrak{F}_n) \longrightarrow H^0(X(N), \mathfrak{F}_n) \longrightarrow H^0(X(N), \mathfrak{F}_n/(E_{p-1} - r)) \\ \quad \hookrightarrow H^1(X(N), \mathfrak{F}_n) \longrightarrow H^1(X(N), \mathfrak{F}_n) \longrightarrow H^1(X(N), \mathfrak{F}_n/(E_{p-1} - r)) \longrightarrow 0 \end{array}$$

Suppose first that $k > 0$. Then under our hypothesis the base-change theorem (1.2.2) applies and we see that $H^0(X(N), \mathfrak{F}_n) = H^0(X(N), \mathfrak{F}) \otimes R_0/p^nR_0$, and $H^1(X(N), \mathfrak{F}_n) = 0$. Thus the H^0 terms form a short exact sequence of inverse systems, the first of which has surjective transition morphisms. Hence the inverse limit forms the desired short exact sequence.

For $k = 0$ and $p \neq 2$ or $k = 0$, $p = 2$ and $n \leq 11$, we have $H^1(X(N), \underline{\omega}^{\otimes k}) = 0$ for

all $k \geq 2$. Hence $H^1(X(N), \mathfrak{F}) = H^1(X(N), \mathcal{O})$ and then again by cohomology and base change we get $H^0(X(N), \mathfrak{F}_n) = H^0(X(N), \mathfrak{F}) \otimes R_0/p^n R_0$. The sequence on H^1 becomes

$$H^1(X(N), \mathcal{O}) \otimes R_0/p^n R_0 \xrightarrow{-r} H^1(X(N), \mathcal{O}) \otimes R_0/p^n R_0 \to H^1(X(N), \mathcal{O}) \otimes R_0/(p^n, r)$$

For variable n they form a six-term exact sequence of inverse systems. If their inverse limit was exact the theorem would follow because multiplication by r on $H^0(X(N), \mathcal{O}) \otimes R_0$ is injective.

The proof for the exactness follows using spectral sequences of hypercohomology for the functor $\varprojlim$ which the author is not familiar with. Interested readers can look up [Kat73, Lemma 2.5.2]. □

Remark 2.3.2. In terms of the formal scheme (Section 2.3.1) one can interpret p-adic modular forms over a p-adically complete ring R_0 as $H^0\Big(Y(N)(R_0, r), \underline{\omega}^{\otimes k}\Big)$. One can also consider the formal completion along $p = 0$ of the vector bundle above $X(N)$. Denoting it by $X(N)(R_0, r)$ we see that p-adic modular forms which are holomorphic at the cusps are exactly $H^0\Big(X(N)(R_0, r), \underline{\omega}^{\otimes k}\Big)$. That is

$$M(R_0; r, N, k) = H^0\Big(Y(N)(R_0, r), \underline{\omega}^{\otimes k}\Big)$$
$$S(R_0; r, N, k) = H^0\Big(X(N)(R_0, r), \underline{\omega}^{\otimes k}\Big)$$

When $r = 1$ this means that p-adic modular forms of weight k are global section of $\underline{\omega}^{\otimes k}$ over the ordinary locus $\mathfrak{X}^{\text{ord}}$. This will be our definition of p-adic modular forms in the next chapter.

2.4 A "Basis" of $S(R_0; r, N, k)$ in the Limit

Lemma 2.4.1. *Under the numerical hypotheses of Theorem 2.3.2, for each $j \geq 0$ the injective homomorphism*

$$H^0(X(N) \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+j(p-1)}) \xrightarrow{E_{p-1}} H^0(X(N) \otimes \mathbb{Z}_p, \underline{\omega}^{\otimes k+(j+1)(p-1)}) \tag{2.1}$$

admits a section.

Proof. It is necessary and sufficient to show that the cokernel of (2.1) is a finite, free $\mathbb{Z}_p$ module. First consider the exact sequence of sheaves on $X(N) \otimes \mathbb{Z}_p$

$$0 \to \mathcal{O}_{X(N)} \xrightarrow{E_{p-1}} \underline{\omega}^{\otimes p-1} \to \underline{\omega}^{\otimes p-1}/E_{p-1} \to 0 \tag{2.2}$$

We claim that $\underline{\omega}^{\otimes p-1}/E_{p-1}$ is a flat $\mathbb{Z}_p$ sheaf. Denote this sheaf by $\mathfrak{F}$. Choose a point $x \in \mathrm{Supp}(\mathfrak{F})$ and assume without loss of generality that x lies over the closed point of $\mathrm{Spec}\,\mathbb{Z}_p$. Choosing a trivialization of $\underline{\omega}$, suppose $\mathfrak{F}_x \simeq \mathcal{O}_{X,x}/(f)$ for some $f \in \mathfrak{m}_x$. We need to show that $\mathcal{O}_{X,x}$ is a flat $\mathbb{Z}_p$-algebra, or in other words p is not a zero-divisor in this ring. From the Tor exact sequence it is sufficient to show that $\mathrm{Tor}^1_{\mathbb{Z}_p}(\mathcal{O}_{X,x}/(f), \mathbb{F}_p) = 0$. Since $\mathcal{O}_{X,x}$ is a domain we have an exact sequence

$$0 \to \mathcal{O}_{X,x} \xrightarrow{f} \mathcal{O}_{X,x} \to \mathcal{O}_{X,x}/(f) \to 0$$

Over $\mathbb{F}_p$ this sequence is exact as the Hasse invariant has simple zeros by Igusa's theorem (Corollary 2.1.2). Thus $\mathrm{Tor}^1_{\mathbb{Z}_p}$ vanishes. This proves our claim.

Thus we can apply the cohomology and base-change formalism to (2.2) twisted by $\underline{\omega}^{\otimes k+j(p-1)}$ and get an exact sequence of finite free $\mathbb{Z}_p$-modules whose formation commutes with arbitrary change of base.

$$\begin{aligned} 0 \longrightarrow H^0\Big(X(N)\otimes\mathbb{Z}_p, \underline{\omega}^{\otimes k+j(p-1)}\Big) &\xrightarrow{E_{p-1}} H^0\Big(X(N)\otimes\mathbb{Z}_p, \underline{\omega}^{\otimes k+(j+1)(p-1)}\Big) \longrightarrow \\ H^0\Big(X(N)\otimes\mathbb{Z}_p, \underline{\omega}^{\otimes k+j(p-1)}\otimes\mathfrak{F}\Big) &\longrightarrow H^1\Big(X(N)\otimes\mathbb{Z}_p, \underline{\omega}^{\otimes k+j(p-1)}\Big) \longrightarrow 0 \end{aligned}$$

Note that $H^1\Big(X(N)\otimes\mathbb{Z}_p, \mathfrak{F}\otimes\underline{\omega}^{\otimes k+j(p-1)}\Big)$ vanishes because $\mathfrak{F}$ is a skycraper sheaf over $\mathbb{F}_p$, again by Igusa's theorem.

From this exact sequence we see that the cokernel of (2.1) is the kernel of a surjective map of finite free $\mathbb{Z}_p$-modules, and hence is itself finite free. □

For each N, k satisfying the conditions of Theorem 2.3.2, and each $j \geq 0$ choose once

and for all a section of the "multiplication by E_{p-1}" map in (2.1), and denote its kernel by $B(N,k,j+1)$. Thus for $j \geq 0$, we have a direct sum decomposition

$$H^0\Big(X(N), \underline{\omega}^{\otimes k+(j+1)(p-1)}\Big) \simeq E_{p-1} \cdot H^0(X(N), \underline{\omega}^{\otimes k+j(p-1)}) \oplus B(N,k,j+1)$$

Definition 2.4.1. $H^0(X(N), \underline{\omega}^{\otimes k}) = B(N,k,0)$.

Definition 2.4.2. $B(R_0,N,k,j) = B(N,k,j) \otimes R_0$ for any p-adically complete ring R_0.

The R_0 analogue of the direct sum decomposition above gives

$$\begin{aligned} \bigoplus_{a=0}^{j} B(R_0,N,k,a) &\xrightarrow{\sim} S(R_0;N,k+j(p-1)) \\ \sum b_a &\mapsto \sum E_{p-1}^{j-a} b_a \end{aligned} \tag{2.3}$$

Definition 2.4.3. Define $B^{\mathrm{rigid}}(R_0;r,N,k)$ to be the R_0-module consisting of all formal sums

$$\sum_{a=0}^{\infty} b_a, \quad b_a \in B(R_0,N,k,a)$$

whose terms tend to 0 in the p-adic topology, i.e. for any $n \in \mathbb{N}$, $b_a \in p^n B(R_0,N,k,a)$ for all $a \gg 0$.

Proposition 2.4.1. *Hypotheses as in Theorem 2.3.2, the inclusion of $B^{rigid}(R_0;r,N,k)$ in the p-adic completion of $H^0\Big(X(N), \oplus_{j\geq 0}\, \underline{\omega}^{\otimes k+j(p-1)}\Big)$ induces via (2.3) an isomorphism*

$$\begin{aligned} B^{rigid}(R_0;r,N,k) &\xrightarrow{\sim} S(R_0;r,N,k) \\ \sum b_a &\mapsto \sum_{a\geq 0} r^a \cdot b_a/(E_{p-1})^a \end{aligned} \tag{2.4}$$

where $\sum_{a\geq 0} r^a \cdot b_a/(E_{p-1})^a = \sum_{a\geq 0} b_a(E/S,\alpha_N) \cdot Y^a$ on $(E/S,\alpha_N,Y)$.

Proof. For injectivity, we need to show that if $\sum_{a\geq 0} b_a \in B^{\mathrm{rigid}}(R_0;r,N,k)$ can be written as $(E_{p-1}-r)\sum_{a\geq 0} s_a$ with $s_a \in S(R_0;N,k+a(p-1))$, and s_a tending to 0

as $a \to \infty$, then all $b_a = 0$. It suffices to prove that for any $n > 0$, $b_a \equiv 0 \bmod p^n$. But modulo p^n both b_a and s_a are finite sums. Suppose $b_a \equiv s_a \equiv 0 \bmod p^n$ for all $a > M$. Let us show the congruence for $a = M$ and use descending induction. As $0 \equiv b_{M+1} \equiv E_{p-1}s_M \bmod p^n$, $s_M \equiv 0 \bmod p^n$. Hence $b_M \equiv E_{p-1}s_{M-1} \bmod p^n$, hence $b_M \equiv 0 \bmod p^n$ by (2.3).

For surjectivity, we use (2.3) again. Given $\sum s_a$ with $s_a \in S(R_0; N, k + a(p-1))$ tending to 0, we can decompose $s_a = \sum_{i+j=a} (E_{p-1})^i b_j(a)$, with $b_j(a) \in B(R_0, N, k, j)$ and $b_j(a)$ tends to 0 as $a \to \infty$, uniformly on j. Then

$$\begin{aligned}\sum_a s_a &= \sum_a \sum_{i+j=a} (E_{p-1})^i b_j(a) \\ &= \sum_a \sum_{i+j=a} r^i b_j(a) + (E_{p-1} - r) \sum_a \sum_{i+j=a} b_j(a) \sum_{u+v=i-1} (E_{p-1})^u \cdot r^v\end{aligned}$$

Hence $\sum s_a$ and $\sum_a \sum_{i+j=a} r^i b_j(a)$ have the same image in $S(R_0; r, N, k)$. But for each j, $\sum_i r^i b_j(i+j)$ converges to an element $b'_j \in B(R_0, N, k, j)$, and b'_j tends to 0 as $j \to \infty$. Thus $\sum_{j \geq 0} b'_j$ have the same image in $S(R_0; r, N, k)$ as $\sum_{a \geq 0} s_a$. □

Corollary 2.4.1. With hypotheses as above, there is a natural transformation of functors

$$\begin{aligned}\mathcal{P}_{R_0,1} &\to \mathcal{P}_{R_0,r} \\ (E/S, \alpha_N, Y) &\mapsto (E/S, \alpha_N, rY)\end{aligned}$$

for any R_0 where p is nilpotent. For any p-adically complete R_0 we see that the transformations for $R_0/p^n R_0$ for varying n are compatible. This then induces a map between the associated formal schemes $Y(N)(R_0, 1) \to Y(N)(R_0, r)$ under which p-adic modular forms of growth r pull back to p-adic modular forms of growth 1. This map restricts to a map $S(R_0; r, N, k) \to S(R_0; 1, N, k)$ between p-adic modular forms holomorphic at ∞. The corresponding map in terms of the bases is given by

$$\begin{aligned}B^{\mathrm{rigid}}(R_0; r, N, k) &\to B^{\mathrm{rigid}}(R_0; 1, N, k) \\ \sum b_a &\mapsto \sum r^a b_a.\end{aligned}$$

2.4.1 Banach Norm and q-Expansion for $r = 1$

Proposition 2.4.2. *Hypothesis as in Theorem 2.3.2, let $x \in R_0$ be any element which divides a power of p. Then the following conditions on an element $f \in S(R_0; 1, N, k)$ are equivalent for $k \geq 0$:*

1. *$f \in x \cdot S(R_0; 1, N, k)$*
2. *the q-expansion of f all lie in $x \cdot R_0[\zeta_N][[q]]$*
3. *on each of the $\varphi(n)$ connected components of $X(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N]$, there is at least one cusp where the q-expansion of f lies in $x \cdot R_0[\zeta_N][[q]]$.*

Proof. (1) $\implies$ (2) $\implies$ (3) is clear. We will prove (3) $\implies$ (1). Firstly, we have

$$S(R_0/xR_0; 1, N, k) \simeq B^{\text{rigid}}(R_0/xR_0; 1, N, k) \simeq B^{\text{rigid}}(R_0; 1, N, k)/x \cdot B^{\text{rigid}}(R_0; 1, N, k)$$

Replacing R_0 by R_0/xR_0 we are reduced to the case where p is nilpotent. Hence $f \in B^{\text{rigid}}(R_0; 1, N, k)$ is a finite sum $\sum_{a=1}^{n} b_a$, with $b_a \in B(R_0, N, k, a)$. It's q-expansion at $\big(\text{Tate}(q^N), \omega_{\text{can}}, \alpha_N, (E_{p-1})^{-1}\big)$ is

$$\sum_{a=0}^{n} b_a \cdot (E_{p-1})^{-a} = \frac{\sum_{a=0}^{n} b_a \cdot (E_{p-1})^{n-a}}{(E_{p-1})^n}$$

By hypothesis, $\sum_{a=0}^{n} b_a (E_{p-1})^{n-a}$ has q-expansion 0 at one or more cusps on each geometric component of $X(N)$. Hence by the q-expansion principle (Corollary 1.2.1) $\sum_{a=0}^{n} b_a (E_{p-1})^{n-a} = 0$. By (2.3) each $b_a = 0$. □

Proposition 2.4.3. *Let N, k, R_0 satisfy the hypothesis of Theorem 2.3.2. Suppose given for each cusp α of $X(N)$ a power series $f_\alpha(q) \in R_0[\zeta_N][[q]]$. The following are equivalent:*

1. *The f_α are the q-expansion of an (necessarily unique) element $f \in S(R_0; 1, N, k)$.*
2. *For every power p^n of p, there exists a positive integer $M \equiv 0 \bmod p^{n-1}$ and a true modular form $g_n \in S(R_0; n, k + M(p-1))$ whose q-expansions are congruent mod p^n to the given f_α.*

Proof. (1) $\implies$ (2). Replace R_0 by R_0/p^nR_0. As we saw in the proof of Proposition 2.4.2, f has the same q-expansion as $g/(E_{p-1})^M$ where g is a true modular form of weight $k+M(p-1)$. Multiplying numerator and denominator by a suitable power of p, assume $M \equiv 0 \bmod p^{n-1}$. Now $E_{p-1} \equiv 1 \bmod p$ implies that $(E_{p-1})^{p^{n-1}} \equiv 1 \bmod p^n$. Thus $f \bmod p^n$ has the same q-expansion as g.

(2) $\implies$ (1). Multiplying g_n by a power of $(E_{p-1})^{p^{n-1}}$, we can assume that the weights $k + M_n(p-1)$ of g_n are strictly increasing with n. Let $\Delta_n = M_{n+1} - M_n$. Then the q-expansions of $g_{n+1} - g_n(E_{p-1})^{\Delta_n}$ are divisible by p^n. Hence the difference lies in $p^nS(R_0; N, k + M_{n+1}(p-1))$ by the q-expansion principle (Corollary 1.2.1). Hence $\sum_n (g_{n+1} - g_n(E_{p-1})^{\Delta_n}$ converges to an element of $S(R_0; 1, N, k)$ whose q-expansion coefficients are congruent to those of g_n modulo p^n. $\square$

Chapter 3

The Katz, Igusa and Big Igusa Moduli Problems

3.1 The Moduli Problem $M_{\mathbf{Katz},N,n}$

We briefly make a summary of the important results that we saw in the last two chapters and will need in this one. Henceforth always assume that p and N are coprime. For $N \geq 3$, the moduli problem classifying isomorphism classes of elliptic curves with tame level N structure is represented by an affine smooth curve over $\mathbb{Z}[1/N]$ denoted by $Y(N)$ which is finite and flat over the affine j-line $\mathbb{Z}[1/N, j]$. There is a universal elliptic curve $p : \mathcal{E} \to Y(N)$. Denote the invariant differentials $p_*\Omega^1_{\mathcal{E}/Y(N)}$ by $\underline{\omega}_{\mathcal{E}/Y(N)}$. The normalization of the projective j-line in $Y(N)$ is a proper and smooth curve $X(N)$. There is a unique invertible sheaf $\underline{\omega}$ on $X(N)$ whose restriction to $Y(N)$ is ω and whose sections over the completion $\mathbb{Z}[1/N, \zeta_N][[q]]$ at each cusp are precisely the $\mathbb{Z}[1/N, \zeta_N][[q]]$ multiples of the canonical differential of the Tate curve. The Kodaira-Spencer style isomorphism

$$\underline{\omega}^2_{\mathcal{E}/Y(N)} \simeq \Omega^1_{Y(N)/\mathbb{Z}[1/N]}$$

extends to an isomorphism

$$\underline{\omega}^2 \simeq \Omega^1_{X(N)/\mathbb{Z}[1/N]}(\log(\text{cusps}))$$

Modular forms of weight k and level N are global sections of ${\underline{\omega}_{\mathcal{E}/Y(N)}}^k$. Modular forms which are holomorphic at ∞ are sections of $\underline{\omega}^k$.

Over $\mathbb{F}_p$, the Verchiebung $V : \mathcal{E}^{(p)} \to \mathcal{E}$ induces a map on the Lie algebra

$$\begin{aligned} \mathrm{tg}(V) &\in \mathrm{Hom}_{Y(N)}\left((\mathrm{Lie}(\mathcal{E}))^{\otimes p} \to \mathrm{Lie}(\mathcal{E})\right) \\ &= H^0(Y(N), \underline{\omega}^{p-1}) \end{aligned}$$

which we call the Hasse invariant A. The locus in $Y(N)$ where A generates the stalk of $\underline{\omega}^{p-1}$ is called the ordinary locus $Y(N)^{\mathrm{ord}}_{\mathbb{F}_p}$. This is an open subscheme of $Y(N)_{\mathbb{F}_p}$. Over $\mathbb{Z}/p^m\mathbb{Z}$ for some $m \geq 1$, the underlying topological space of $Y(N)_{\mathbb{Z}/p^m\mathbb{Z}}$ is the same as $Y(N)_{\mathbb{F}_p}$. Denote by $Y(N)^{\mathrm{ord}}_{\mathbb{Z}/p^m\mathbb{Z}}$ the open subscheme of $Y(N)_{\mathbb{Z}/p^m\mathbb{Z}}$ whose underlying topological space is the same as $Y(N)^{\mathrm{ord}}_{\mathbb{F}_p}$. When there is no confusion about the base scheme we will simply write $Y(N)^{\mathrm{ord}}$. The formal scheme associated to these compatible system of affine schemes is denoted by $\mathfrak{X}^{\mathrm{ord}}$.

Recall from Section 2.1.1 we had a short exact sequence of finite locally free group schemes over any $\mathbb{F}_p$-scheme S and for all $n > 0$

$$0 \to \ker F^n \to E[p^n] \to \ker V^n \to 0$$

$\ker F^n$ and $\ker V^n$ are locally free of rank p^n. Over the ordinary locus $Y(N)^{\mathrm{ord}}$, V induces an isomorphism of invariant differentials of E and $E^{(p)}$. Hence V is an étale morphism and $\ker V^n$ is étale for all $n > 0$. Over an algebraically closed field k, $\ker F^n$ consists of a single point and hence is represented by the affine spectrum of an Artin local ring over k. Since V^n is étale, and hence isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ over k, $\ker F^n$ is isomorphic to μ_{p^n} by Cartier duality coming from the Weil pairing.

A sequence as above is an instance of connected-étale sequence for finite group schemes. One can prove that such a sequence always exists for any finite group scheme over a perfect field [cf. Wat12, pg. 52]. But over arbitrary basis, we need to make precise the notion of the connected part of a finite group scheme. The correct notion is that of a scheme which is radiciel over the base. The next proposition and the corollary following it shows that any finite locally free group scheme can be written as an extension of a finite locally free étale group scheme by a finite locally free radiciel group scheme if the separable rank of its fibres is locally constant.

Proposition 3.1.1. *Let $f : X \to S$ be finite and locally free. Then the separable rank of the fibres of f is locally constant iff there are morphisms $i : X \to X'$ and $f' : X' \to S$ which are finite locally free with i radiciel and surjective, f' etale and $f = f' \circ i$. The factorisation is unique upto unique isomorphism and functorial in X/S.*

Proof. We sketch a proof of this proposition omitting some details. For a complete proof, [cf. Mes72, II, Lemma 4.8].

Because of the uniqueness assertion, it suffices to prove the proposition locally on S. So assume $S = \operatorname{Spec} R$ and the (separable rank (X_s)) is constant. The if part is trivial. Since X is finite locally free, and in particular finitely presented and flat over S, we can assume that S is Noetherian. The proof is accomplished in several steps:

1. existence and uniqueness when S is a field.
2. existence and uniqueness when S is a complete (Noetherian) local ring.
3. uniqueness for arbitrary $S = \operatorname{Spec} A$, A Noetherian.
4. existence of $f' : X' \to S$ when S is a local ring.
5. existence of $i : X \to X'$ when S is a local ring.
6. existence for arbitrary $S = \operatorname{Spec} A$, A Noetherian.
7. functoriality.

1) If $S = \operatorname{Spec} k$ and $X = \operatorname{Spec} B$, X' is the affine spectrum of the unique maximal separable subalgebra of B. Write B as a product of Artin local rings $B = B_1 \times ... \times B_r$. If k_i' is the maximal separable extension of k in the residue field of B_i, there is a unique lift of the natural inclusion $k \to B_i$ to $k_i' \to B_i$ since B_i is Artin.

2) Since complete Noetherian local rings are Henselian, and any finite local algebra over a Henselian local ring is also Henselian, we see that there is a unique solution to the problem by Hensel's lemma.

3) Let $X \xrightarrow{i} X' \xrightarrow{f'} S$ and $X \xrightarrow{i'} X'' \xrightarrow{f''} S$ be two solutions. To construct a unique isomorphism between them it suffices to do so for localisation at any point $s \in S$, because our rings are Noetherian and thus any such isomorphism extends to a neighborhood of s, and on intersections two such extensions agree by uniqueness. Hence

we assume $S = \operatorname{Spec} A$ where A is a Noetherian local ring. Let $S' = \operatorname{Spec} \hat{A}$ and $S'' = \operatorname{Spec}(\hat{A} \otimes_A \hat{A})$. The morphism $S' \to S$ is faithfully flat and quasi-compact and hence we apply fpqc descent. By 2) we have a commutative diagram

$$\begin{array}{ccc} X'_{S'} & \xrightarrow{\quad\eta\quad} & X''_{S'} \\ & {\scriptstyle i_{S'}} \nwarrow \quad \nearrow {\scriptstyle i'_{S'}} & \\ & X_{S'} & \end{array}$$

η is an isomorphism by 2). We need to show that η is a morphism of objects with descent data. To see this, let τ_X (resp. $\tau_{X'}, \tau_{X''}$) denote the canonical isomorphism $p_1^*(X_{S'}) \xrightarrow{\sim} p_2^*(X_{S'})$ (resp. ...). we need to show

$$\tau_{X''} \circ p_1^*(\eta) = p_2^*(\eta) \circ \tau_{X'}$$

We know

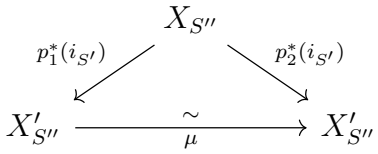
$$\begin{aligned} p_2^*(\eta) \circ \tau_{X'} \circ p_1^*(i_{S'}) &= p_2^*(\eta) \circ p_2^* i_{S'} \circ \tau_X \\ &= p_2^*(i'_{S'}) \circ \tau_X \\ &= \tau_{X''} \circ p_1^*(i'_{S'}) \\ &= \tau_{X''} \circ p_1^*(\eta) \circ p_1^*(i_{S'}) \end{aligned}$$

But $i : X \to X'$ is faithfully flat and hence so is $p_1^*(i_{S'})$. Hence it is an epimorphism of schemes and this completes the proof.

4) To show $f' : X \to S$ exists, we will show that, using the notation of 3) above, the X' which we know from 2) to exists over S' descends to S. Thus we have the standard situation $S'' \rightrightarrows S' \longrightarrow S$ and we have a solution of our problem for $X_{S'}$. Call this solution Y. We want to descend Y to S. By the uniqueness proved in 3) we see there is an isomorphism $p_1^*(Y) \xrightarrow{\sim} p_2^*(Y)$. But using the uniqueness of isomorphisms between solutions we see the isomorphism $p_1^*(Y) \xrightarrow{\sim} p_2^*(Y)$ must satisfy the cocycle condition and hence Y can be descended to an X' étale and finite over S.

5) From 2) and 4) we know that over S' we have a morphism $i_{S'} : X_{S'} \to X'_{S'}$. We want to show that this morphism descends to a similar morphism $i : X \to X'$ over S.

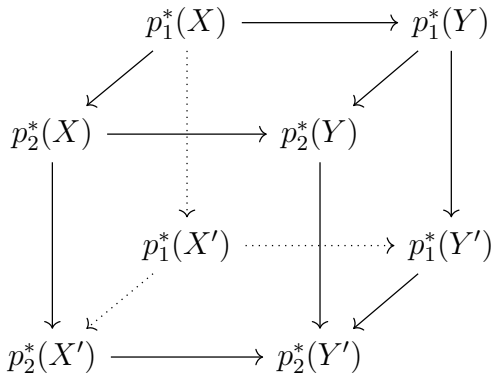
Pulling back to S'', we get a commutative diagram



While μ might not be identity, it is an isomorphism by the uniqueness assertion of part 3). Also by the same reason, it satisfies the cocycle condition $p_{1,3}^*(\mu) = p_{2,3}^*(\mu) \circ p_{1,2}^*(\mu)$. Hence there exist a scheme T, finite and étale over S, and an isomorphism $\varphi : X'_{S'} \xrightarrow{\sim} T_{S'}$, such that X' with descent datum μ is isomorphic to $T_{S'}$ with its canonical descent datum via φ. A computation reveals that $\varphi \circ i : X_{S'} \to T_{S'}$ is a morphism between objects with descent data and hence can be descended. We omit showing the computation. Readers can look up [Mes72, II, Lemma 4.8].

6) The solution from 4) and 5) can be extended to a neighborhood of s for all $s \in S$ [cf. Mes72, II, Lemma 4.8]. By the uniqueness proved in part 3) they can be patched together to give a solution over all of S.

7) Functoriality is obvious for the case of a base field. Also the fact that there is an equivalence of categories between finite étale algebras over a Henselian ring $(R, \mathfrak{m}, k)$ and the category of finite étale algebras over k gives functoriality for the case when $S = \operatorname{Spec} A$ for a complete Noetherian local ring A. To know we can descend the morphism from S' to S, we consider the following diagram



All the faces except possibly the bottom one are commutative. Moreover $p_1^*(i)$ is an epimorphism. This gives functoriality when S is the spectrum of a local ring. Now

extend this first to a neighborhood of any point and finally to all of S. $\square$

Corollary 3.1.1. If $f : G \to S$ is a finite locally free group scheme whose fibres have locally constant separable rank, there is a canonical factorization

$$0 \to G^\circ \to G \to G^{\text{ét}} \to 0$$

where $G^{\text{ét}}$ is a finite locally free étale group scheme and G° is a finite locally free radiciel group scheme.

Proof. Proposition 3.1.1 gives an epimorphism $i : G \to G^{\text{ét}}$ where $G^{\text{ét}}$ is a finite locally free étale scheme. The functoriality assertion and the fact that the construction commutes with fibre products imply that $G^{\text{ét}}$ is a group and i is a homomorphism. G^0 is then defined to be $\ker i$. It is radiciel because i is radiciel. $\square$

Let's now return to the case of elliptic curves. Assume that E/S is an ordinary elliptic curve, such that p is locally nilpotent on S. Localizing, we may assume that p is nilpotent and S is a $\mathbb{Z}/p^m\mathbb{Z}$-algebra. From Corollary 3.1.1 we get an exact sequence,

$$0 \to E[p^n]^\circ \to E[p^n] \to E[p^n]^{\text{ét}} \to 0$$

owing to the fact E is ordinary, and hence the separable rank of $E[p^n]$ over fibres is constant and equal to p^n. Over the special fibre of $\mathbb{Z}/p^m\mathbb{Z}$ we have seen the exact sequence

$$0 \to \ker F^n \to E[p^n] \to \ker V^n \to 0$$

The first sequence restricts to the second over $\mathbb{F}_p$ by the uniqueness of the factorization. The morphisms $E \xrightarrow{f} E' = E/E[p]^\circ$ and $E' \xrightarrow{v} E = E'/E[p]^{\text{ét}}$ are dual isogenies of degree p which lift the relative Frobenius F and the Verschiebung V respectively.

Let's recall that in Section 2.1 we constructed the formal group $\hat{E}$ of an elliptic curve E/S. Let us now assume that $E/S/\mathbb{F}_p$ is an elliptic curve. We want to relate $\hat{E}$ with the connected part of the p^n-torsion for all n.

Lemma 3.1.1. *Let $E/S/\mathbb{F}_p$ be an elliptic curve. Then $\hat{E} \simeq \varinjlim_n \ker F^n$.*

Proof. Since the question is local on S, we may assume $S = \operatorname{Spec} R$ such that $\underline{\omega}_{E/S}$ has a basis. In that case $\hat{E} \simeq \operatorname{Spf} R[[T]]$ for a formal parameter T adapted to $\underline{\omega}_{E/S}$. Now the isomorphism is obvious. □

Remark 3.1.1. The proof didn't use any particular property of the elliptic curve other than the fact that $\hat{E}$ is a formal Lie group. Hence the statement holds for any formal Lie group. Moreover we have the following stronger result concerning formal Lie groups over characteristic p.

Proposition 3.1.2. *Let S be a $\mathbb{F}_p$-scheme. A sheaf of groups G on S is a formal Lie group iff the following three conditions hold:*

1. *G is F-torsion, i.e. $G = \varinjlim G(n)$ where $G(n) = \ker F^n$.*
2. *G is F-divisible, i.e. $F : G \to G^{(p)}$ is an epimorphism.*
3. *$G(n)$ are finite and locally free group schemes.*

Proof. The necessity of the conditions is immediate from the fact that locally on S, G is represented by the formal spectrum of a power series ring. For the sufficiency [cf. Mes72, II, Theorem 2.1.7] or [Tat67, Proposition 1]. □

Lemma 3.1.2. *Let $E/S/\mathbb{F}_p$ be an ordinary elliptic curve. Then*

$$\hat{E}[p^n] \simeq \ker F^n = E[p^n]^\circ$$

Proof. Follows from the fact that $V : \hat{E}^{(p)} \to \hat{E}$ is an isomorphism and $[p^n] = V^n F^n$. □

This shows that for ordinary elliptic curves over $\mathbb{F}_p$-schemes the connected part of the p^n-torsion is the same as the p^n-torsion of its formal group. We would like to have a similar result even for base schemes where p is locally nilpotent. First a few words about the p-divisible group of an elliptic curve.

Definition 3.1.1. Let S be a scheme where p is locally nilpotent. Let E/S be an elliptic curve. Consider its p-divisible group $E[p^\infty]$. Define the formal group of $E[p^\infty]$

to be

$$\widehat{E[p^\infty]} := \varinjlim_k \mathrm{Inf}^k(E[p^\infty])$$

Lemma 3.1.3. *Let S be a scheme where p is locally nilpotent. Let E/S be an elliptic curve. Then the natural inclusion $\widehat{E[p^\infty]} \to \hat{E}$ is an isomorphism.*

Proof. We need to prove that for any k, there is $N \gg 0$ such that $\mathrm{Inf}^k(E) \hookrightarrow E[p^N]$. Since the question is local on S, assume $\hat{E} = \mathrm{Spf}\, R[[T]]$, where $S = \mathrm{Spec}\, R$, p nilpotent on R and T is a formal parameter adapted to $\underline{\omega}_{E/S}$. Then $[p]^\#(I) \subset (pI, I^2)$. Since $\mathrm{Inf}^k(E) = \mathrm{Spec}\, R[T]/(T^k)$ and p is nilpotent, we get the result. □

Next we state a result that links the formal group of a p-divisible group with its connected part, over a scheme where p is locally nilpotent. The proof of the statement is technical and we postpone it to the next Chapter, where we devote a section to p-divisible groups.

Theorem 3.1.1. *Let p be locally nilpotent on S and G be a p-divisible group on S. Suppose $G[p^n]$ has locally constant separable rank over fibres and (separable rank $G[p^n]_s$) = (separable rank $G[p]_s)^n$. For each $n > 0$ denote the connected part of $G[p^n]$ by $G[p^n]^\circ$ and the étale part by $G[p^n]^{ét}$. Then $\{G[p^n]^\circ\}_n$ and $\{G[p^n]^{ét}\}_n$ are p-divisible groups and $\hat{G} = \varinjlim_n G[p^n]^\circ$.*

Proof. See Chapter 4, Theorem 4.1.3. □

Corollary 3.1.2. Let p be locally nilpotent on S. Let E/S be an ordinary elliptic curve. Then $\hat{E}[p^n] \simeq E[p^n]^\circ$

Proof. The separable rank of $E[p^n]$ is constant and is equal to p^n. Since the formal group of the p-divisible group is the same as the formal group of E by Lemma 3.1.3, we get the result by Theorem 3.1.1. □

3.1.1 Representability of $M_{\mathbf{Katz},N,n}$

Definition 3.1.2. Over $\mathbb{Z}/p^m\mathbb{Z}$, the moduli problem $M_{\mathrm{Katz},N,n}$ classifies for any scheme S, the isomorphism classes of tuples $(E, \hat{\varphi}, \alpha_N)$ where E is an elliptic curve over S,

$\hat{\varphi} : \hat{E}[p^n] \xrightarrow{\sim} \mu_{p^n}$ and $\alpha_N : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$.

In this section we will show that this problem is represented by a curve which has a natural map to the ordinary locus $Y(N)^{\mathrm{ord}}$ simply by forgetting $\hat{\varphi}$. We can also define a problem which classifies for schemes S, the isomorphism classes of tuples $(E, \varphi^{\text{ét}}, \alpha_N)$ where $\varphi^{\text{ét}} : \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} E[p^n]/\hat{E}[p^n]$. Since $\hat{E}[p^n]$ and $E[p^n]/\hat{E}[p^n]$ are dual to each other and so are μ_{p^n} and $\mathbb{Z}/p^n\mathbb{Z}$, we see that this problem is naturally isomorphic to $M_{\mathrm{Katz},N,n}$. We will show that the natural map from $M_{\mathrm{Katz},N,n}$ to $Y(N)^{\mathrm{ord}}$ is finite, étale and Galois for the action of the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

We first point to a proof that is found in the book of Katz-Mazur [KM85]. It uses the notion of full sets of sections and while we are not going to provide the details of the proof, we mention it because it might be a useful strategy for proving more general results.

Full sets of sections :
We define full sets of sections following Katz-Mazur [KM85, Section (1.8)]. Let S be a scheme, and Z/S a finite, locally free S-scheme of rank $N \geq 1$. For every affine S-scheme $\operatorname{Spec} R \to S$, the R-scheme Z_R/R obtained by base change is of the form $\operatorname{Spec} B$ where B is a finite, locally free R-algebra of rank N. Since B is locally free of rank N over R, we can speak of the characteristic polynomial of the R-linear endomorphism $f : B \to B$ for any $f \in B$. Indeed, we can choose an open set in $\operatorname{Spec} R$ over which B is free and note that the characteristic polynomial is independent of the choice of a basis.

Definition 3.1.3. We say that a set of N not-necessarily distinct points $P_1, \ldots, P_N$ in $Z(S)$ is a "full set of sections" if for every affine S-scheme $\operatorname{Spec} R$ and for every $f \in B$ as above, we have

$$\det(T - f) = \prod_{i=1}^{N} (T - f(P_i))$$

For any scheme S, the constant group scheme $\mathbb{Z}/N\mathbb{Z}$ for any $N \in \mathbb{N}$ is given by the relative affine spectrum of the algebra

$$\mathcal{O}_S e_0 \times \mathcal{O}_S e_1 \times \cdots \times \mathcal{O}_S e_{N-1}$$

where the $\mathcal{O}_S$-algebra structure is given by the diagonal embedding. It is a finite free

group scheme of rank N. For any T/S, $\mathbb{Z}/N\mathbb{Z}_T \simeq T_0 \sqcup \cdots \sqcup T_N$ where each $T_i = T$.

Definition 3.1.4. Suppose E/S is a finite flat group scheme. Define the functor

$$\underline{\mathrm{Hom}}(\mathbb{Z}/N\mathbb{Z}, E) := \underline{\mathrm{Hom}}(\mathbb{Z}/N\mathbb{Z}, E)(T) = \mathrm{Hom}_{T\text{-gp}}(\mathbb{Z}/N\mathbb{Z}_T, E_T)$$

for any S-scheme T.

Suppose we have a T-group scheme homomorphism $\phi : \mathbb{Z}/N\mathbb{Z}_T \to E_T$. Let $\phi_1 = \phi|_{T_1}$ the restriction. This is a T point of $E_T[N]$. Conversely given any T point of $E_T[N]$ (say P), we will show that there is a T-gp homomorphism $\mathbb{Z}/N\mathbb{Z}_T \xrightarrow{\phi_P} E_T$ such that $\phi_1 = P$.

Lemma 3.1.4. $\underline{\mathrm{Hom}}(\mathbb{Z}/N\mathbb{Z}, E)(T) = \mathrm{Hom}_{gp}(\mathbb{Z}/N\mathbb{Z}, E(T)) = E[N](T)$

Proof. Given $P \in E_T[N](T)$ define $\phi_i : T_i \to E_T$ as $\phi_i = [i] \circ P$. Since $[N]$ kills P, the ϕ_i's together give a T-gp homomorphism $\mathbb{Z}/N\mathbb{Z}_T \xrightarrow{\phi_P} E_T$. The assignments

$$\phi \mapsto \phi_1 \qquad P \mapsto \phi_P$$

are both natural transformations and are inverse to each other by construction. Thus $\underline{\mathrm{Hom}}(\mathbb{Z}/N\mathbb{Z}, E) \simeq E[N]$.

This says that the T point ϕ_1 uniquely determines the map ϕ. Intuitively, the image of "1" determines ϕ. Conversely, given any T point $P \in E[N](T)$, we get a well defined map by declaring the image of "1" to be P. Thus we see that for any S-scheme T,

$$\underline{\mathrm{Hom}}(\mathbb{Z}/N\mathbb{Z}, E)(T) = \mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}/N\mathbb{Z}, E(T)) = E[N](T)$$

□

Let's fix a base scheme $\mathrm{Spec}\,(\mathbb{Z}/p^m\mathbb{Z})$. Denote by $Y(N)^{\mathrm{ord}}$ the ordinary locus of the modular scheme over $\mathbb{Z}/p^m\mathbb{Z}$. Suppose $\mathcal{E}/Y(N)^{\mathrm{ord}}$ is the universal elliptic curve. Let $\mathcal{E}[p^n]^{\text{ét}}$ be the étale quotient of the p^n-torsion of $\mathcal{E}$. $\mathcal{E}[p^n]^{\text{ét}}$ is a finite flat, étale group scheme of order p^n over $Y(N)^{\mathrm{ord}}$.

Proposition 3.1.3. *$M_{Katz,N,n}$ is representable.*

Proof. As we saw above, the scheme $\mathcal{E}[p^n]^{\text{ét}}$ represents the functor $\underline{\text{Hom}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{E}[p^n]^{\text{ét}})$. Let us denote the subfunctor of $\underline{\text{Hom}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{E}[p^n]^{\text{ét}})$ classifying those ϕ which are in fact isomorphisms, by $\underline{\text{Isom}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{E}[p^n]^{\text{ét}})$. Then it is clear that $\underline{\text{Isom}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{E}[p^n]^{\text{ét}})$ is precisely $M_{\text{Katz},N,n}$.

Consider the universal homomorphism ϕ_{univ}. Under the identification

$$\underline{\text{Hom}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{E}[p^n]^{\text{ét}})(T) = \text{Hom}_{\text{gp}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{E}[p^n]^{\text{ét}}(T))$$

consider the sections $\phi_{\text{univ}}(0), \ldots, \phi_{\text{univ}}(p^n-1)$. Define the functor $(\mathbb{Z}/p^n\mathbb{Z})$-Gen$(\mathcal{E}[p^n]^{\text{ét}})$ as

$$T \mapsto \Big\{ \phi : \mathbb{Z}/p^n\mathbb{Z} \to \mathcal{E}[p^n]^{\text{ét}}(T) \text{ group homomorphisms, such that } \phi(0), \ldots, \phi(p^n-1) \text{ are a full set of sections} \Big\}$$

Katz-Mazur [KM85] show in Proposition 1.10.12 (pg 47) that since $\mathcal{E}[p^n]^{\text{ét}}$ is finite étale,

$$(\mathbb{Z}/p^n\mathbb{Z})\text{-Gen}(\mathcal{E}[p^n]^{\text{ét}}) \simeq \underline{\text{Isom}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{E}[p^n]^{\text{ét}})$$

In [KM85, Proposition 1.10.13] they show that $(\mathbb{Z}/p^n\mathbb{Z})$-Gen$(\mathcal{E}[p^n]^{\text{ét}})$ is given by the closed subscheme Z of $\underline{\text{Hom}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{E}[p^n]^{\text{ét}})$ which is universal for the relation

$$\text{“}\phi_{\text{univ}}(0), \ldots, \phi_{\text{univ}}(p^n-1) \text{ are a full set of sections”}.$$

□

Having provided a reference to the proof in the literature, we describe another way to prove representability of $M_{\text{Katz},N,n}$.

Alternate proof:

Proposition 3.1.4. *For $n = 1$ this subscheme is the complement of the zero section of $\mathcal{E}[p]^{ét}$. The complement is open and closed and thus it is finite, locally free and étale over $Y(N)^{ord}$ of degree $\varphi(p) = p-1$. Over a scheme $S \to Y(N)^{ord}$ where $\mathcal{E}[p]^{ét}$ admits*

a generator P, this subscheme is given by the Cartier divisor

$$\sum_{1\leq n\leq p-1}[nP]$$

Proof. To prove this, note that $Y(N)^{\mathrm{ord}}$ (resp. $\mathcal{E}[p]^{\text{ét}}$) are affine, represented by say R (resp. A). A is a Hopf algebra and denoting the augmentation ideal by I we have a decomposition of R-modules $A = R \oplus I$. Since $I/I^2 = 0$, by Nakayama's lemma there exists an element $f \equiv 1 \bmod I$ such that $fI = 0$. Then $f(1-f) = 0$ and hence f is an idempotent such that $Af = R$ and $A(1-f) = I$. Thus $A = Af \times A(1-f) \simeq A/(1-f) \times A/(f)$. Suppose $P : A \to B$ is an R-algebra homomorphism. This determines a $\operatorname{Spec} B$ point of $\mathcal{E}[p]^{\text{ét}}$ and hence a B-Hopf algebra homomorphism

$$A \otimes_R B \xrightarrow{\phi_P} Be_0 \times \cdots \times Be_{p-1}$$

where $A \otimes_R B \xrightarrow{P\circ[i]} Be_i$ and $e_0, e_1, ..., e_{p-1}$ are the obvious idempotents corresponding to the points "0", "1", ..., "$p-1$" of $(\mathbb{Z}/p\mathbb{Z})_B$ resprectively. We will show that ϕ_P is an isomorphism iff P factors through $A/(f) \simeq A(1-f) = I$.

Suppose first that ϕ_P is an isomorphism. Localising, assume B is local. Then since B is connected, either $Pf = 0$ or $P(1-f) = 0$. If $P(1-f) = 0$, $P \circ [i](1-f) = 0$ for all i and hence P factors through $\varepsilon : A \otimes_R B \to B$ and is trivial. Thus P cannot be an isomorphism in this case.

To prove the converse, it is enough to show that the map induced by the projection $A \to A/(f)$, is an isomorphism

$$A \otimes_R A/(f) \xrightarrow{\sim} A/(f) \times \cdots \times A/(f)$$

It is enough to show this is an isomorphism over any geometric point of $A/(f)$ because both the modules are finite locally free. To show isomorphism over a geometric point $\operatorname{Spec}\bar{k}$ of $A/(f)$ it is enough to show that the projection $A \to A/(f) \to \bar{k}$ is a non-zero point of $\mathcal{E}[p]^{\text{ét}}(\bar{k})$, because then it generates the group of order p. But this is obvious because it cannot factor through the zero section $A/(1-f)$.

The other assertions follow by construction. □

Proposition 3.1.5. *For $n > 1$ $M_{Katz,N,n}$ is given by the inverse image of $M_{Katz,N,1}$ under the projection*

$$\mathcal{E}[p^n]^{ét} \xrightarrow{[p]^{n-1}} \mathcal{E}[p]^{ét}$$

Proof. Indeed, $P \in E[p^n]^{\text{ét}}(S)$ generates the group iff $[p]^{n-1}(P)$ generates $E[p]^{\text{ét}}(S)$. Thus $M_{\text{Katz},N,n}$ is finite, flat and étale over $Y(N)^{\text{ord}}$. If $\mathcal{E}[p^n]^{\text{ét}}$ admits a generator P over some S, M_{Katz,N,n_S} is given by

$$\sum_{\substack{(a,p)=1 \\ 0<a<p^n}} [aP]$$

This also shows that $M_{\text{Katz},N,n}$ is of degree $\varphi(p^n)$ over $Y(N)^{\text{ord}}$. □

3.2 p-adic Modular Forms

Varying n over $\mathbb{N}$, we get an inverse system of affine schemes $M_{\text{Katz},N,n}$ over $Y(N)^{\text{ord}}$ where our base scheme is still fixed as $\text{Spec}\,(\mathbb{Z}/p^m\mathbb{Z})$. The universal elliptic curve $\mathcal{E}$ over $M_{\text{Katz},N,n}$ comes with an universal isomorphism upto an action of $\text{Aut}(\mu_{p^n}) = (\mathbb{Z}/p^n\mathbb{Z})^\times$

$$\hat{\varphi}_n : \mathcal{E}[p^n]^\circ \simeq \hat{\mathcal{E}}[p^n] \xrightarrow{\sim} \mu_{p^n}$$

such that the diagram commutes

$$\begin{array}{ccc} \hat{\mathcal{E}}[p^{n+1}] & \xrightarrow{\hat{\varphi}_{n+1}} & \mu_{p^{n+1}} \\ \downarrow{\scriptstyle [p]} & & \downarrow{\scriptstyle [p]} \\ \hat{\mathcal{E}}[p^n] & \xrightarrow{\hat{\varphi}_n} & \mu_{p^n} \end{array}$$

We will now vary the base scheme and to keep track of it introduce new notation. Let $M_{\text{Katz},N,n} = T_{m,n} = \text{Spec}\,\mathbb{V}_{m,n}$, where the index m denotes that we are working over $\text{Spec}\,(\mathbb{Z}/p^m\mathbb{Z})$. Take the limit of these schemes

$$\text{Spec}\,\mathbb{V}_{m,\infty} = T_{m,\infty} = \varprojlim_n T_{m,n} = \text{Spec}\,(\varinjlim_n \mathbb{V}_{m,n})$$

$T_{m,0} = Y(N)^{\mathrm{ord}}$ over $\mathbb{Z}/p^m\mathbb{Z}$. We have natural projections $T_{m,n'} \xrightarrow{\pi^m_{n',n}} T_{m,n}$ for all $n' \geq n$ and closed immersions $T_{m,n} \hookrightarrow T_{m+1,n}$. We have $\mathbb{V}_{m+1,\infty}/p^m\mathbb{V}_{m+1,\infty} \simeq \mathbb{V}_{m,\infty}$. Denote by $\mathbb{V}_{\infty,\infty} = \varprojlim_m \mathbb{V}_{m,\infty}$.

Let us simply write π^m_n for $\pi^m_{n,0}$. Let ω be the invariant differentials for $\mathcal{E}/T_{m,0}$. The invariant differentials of $\mathcal{E}$ over $T_{m,n}$ is $(\pi^m_n)^*\omega$. These are the same as the invariant differentials of its formal group $\hat{\mathcal{E}}$. For any $n \in \mathbb{N}$ we have the exact sequence

$$0 \to \hat{\mathcal{E}}[p^n] \to \hat{\mathcal{E}} \xrightarrow{[p]^n} \hat{\mathcal{E}}$$

Lemma 3.2.1. *The invariant differentials of $\hat{\mathcal{E}}$ is isomorphic to the invariant differentials on $\hat{\mathcal{E}}[p^n] \simeq \mathcal{E}[p^n]^\circ$ for all $n \geq m$.*

Proof. Let $\mathcal{I}$ be the ideal sheaf of the zero section of $\mathcal{E}$. Since $[p]^\#(I) \subset (pI, I^2)$ and $p^n = 0$ for all $n \geq m$, we see that $[p^n]^\#(I) \subset I^p$ for all $n \geq m$. Hence the statement follows. □

Lemma 3.2.2. *The invariant differentials for μ_{p^n} over a $\mathbb{Z}/p^m\mathbb{Z}$-algebra R has a canonical basis given by $\mathrm{d}T/T$, where $\mu_{p^n} = \mathrm{Spec}\, R[T]/(T^{p^n} - 1)$ for all $n \geq m$.*

Proof. Let $A = R[T]/(T^{p^n} - 1)$. Let $f = T^{p^n} - 1$. Then $\mathrm{d}f = 0$ and hence $\Omega^1_{A/R}$ is free of rank 1 over A. Let $\Delta : A \to A \otimes_R A$ be the comultiplication map. Then

$$\mathrm{d}(\Delta T)/(\Delta T) = \mathrm{d}(T \otimes T)/(T \otimes T) = \mathrm{d}(1 \otimes T)/(1 \otimes T) + \mathrm{d}(T \otimes 1)/(T \otimes 1)$$

shows that $\mathrm{d}T/T$ is an invariant differential. It is a basis of the invariant differentials because it is a basis of $\Omega^1_{A/R}$. □

The invariant differentials for $\hat{\mathcal{E}}[p^n]$ has a canonical basis given by $\hat{\varphi}^*_n(\mathrm{d}T/T)$ where

$$\mu_{p^n} = \mathrm{Spec}\,(\mathbb{V}_{m,n}[T]/(T^{p^n} - 1))$$

Thus it is free. Hence,

$$(\pi^m_n)^*\omega^k = \mathcal{O}_{T_{m,n}}(\hat{\varphi}^*_n(\mathrm{d}T/T))^k$$

for all $k \in \mathbb{Z}$, $n \geq m$. In particular, ω is free over $T_{m,\infty}$ for all m.

Let $\mathfrak{X}^{\mathrm{ord}}$ be the formal scheme over $\operatorname{Spf}\mathbb{Z}_p$ given by the compatible family of $\mathbb{Z}/p^m\mathbb{Z}$ schemes $Y(N)^{\mathrm{ord}}$. Let M_{Katz} be the formal scheme over $\mathfrak{X}^{\mathrm{ord}}$ given by the family of $T_{m,\infty}$. M_{Katz} classifies isomorphism classes of tuples $(E/R, \hat{\varphi}, \alpha_N)$ where R is a p-adically complete $\mathbb{Z}_p$ algebra, α_N a level N structure and $\hat{\varphi} : E[p^\infty]^\circ = \hat{E}[p^\infty] \xrightarrow{\sim} \mu_{p^\infty}$ is an isomorphism. Let $\pi : M_{\mathrm{Katz}} \to \mathfrak{X}^{\mathrm{ord}}$ be the projection. For each n, π factors through the formal completion of $T_{m,n}$.

The trivializations of ω over $T_{m,\infty}$ for all $m > 0$ show that $\pi^*\omega$ is trivial over M_{Katz}.

$$\operatorname{Aut}(T_{m,\infty}/T_{m,0}) = \varprojlim_n \operatorname{Aut}(T_{m,n}/T_{m,0}) = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$$

Again any automorphism over $\mathbb{Z}/p^m\mathbb{Z}$ extends uniquely to an automorphism over $\mathbb{Z}/p^{m+1}\mathbb{Z}$, and thus M_{Katz} is Galois over $\mathfrak{X}^{\mathrm{ord}}$ with Galois group $G = \mathbb{Z}_p^\times$.

Action of G:
The action of $g \in G$ on $\mathcal{O}_{M_{\mathrm{Katz}}}$ is given by the map induced by pullback via the action of g^{-1} on M_{Katz}.

Remark 3.2.1. $g \in G$ acts on M_{Katz} by sending $(E/R, \hat{\varphi}, \alpha_N) \mapsto (E/R, g\hat{\varphi}, \alpha_N)$. So one might also define the action of $g \in G$ on $\mathcal{O}_{M_{\mathrm{Katz}}}$ as induced by pullback via the action of g on M_{Katz}. But we chose the other convention because it gives a natural left action on the structure sheaf. Note, this is also the definition in [Kat75, A.1.5, pg. 356].

Lemma 3.2.3. *For any $k \in \mathbb{Z}$,*

$$\omega^k \simeq (\pi_*(\pi^*\omega^k))^G$$

Proof. It's enough to prove over $\mathbb{Z}/p^m\mathbb{Z}$ for all m and for $k = 1$. As ω is invertible, locally on $T_{m,0}$

$$(\pi_*(\pi^*\omega))^G = \omega \otimes (\pi_*\mathcal{O}_{T_{m,\infty}})^G$$

As $T_{m,\infty}$ is Galois over $T_{m,0}$ with group G, $(\pi_*\mathcal{O}_{T_{m,\infty}})^G = \mathcal{O}_{Y(N)^{\mathrm{ord}}}$. Hence the right hand side is precisely ω. □

Let $\hat{\varphi}_{\text{univ}} : \hat{\mathcal{E}} \to \mu_{p^\infty}$ be the universal trivialization of $\hat{\mathcal{E}}$ over M_{Katz}. Then

$$\pi^*\omega = \mathcal{O}_{M_{\text{Katz}}} \cdot \hat{\varphi}^*_{\text{univ}}(\mathrm{d}T/T)$$

Since the action of $g \in G$ on $\pi^*\omega$ is given by pullback via the action of g^{-1} on M_{Katz},

$$\pi^*\omega^k \simeq \mathcal{O}_{M_{\text{Katz}}} \otimes z^{-k}$$

for all $k \in \mathbb{Z}$, where z is the identity character of G. By the lemma above we thus get that p-adic modular forms of integral weight k is the subspace of $H^0(\mathfrak{X}^{\text{ord}}, \mathcal{O}_{M_{\text{Katz}}}) = \mathbb{V}_{\infty,\infty}$ where G acts via the character z^k.

Generalizing this, we get to Katz' definition of p-adic modular forms:

Definition 3.2.1. Suppose R is a p-adically complete, separated algebra, and $k : \mathbb{Z}_p^\times \to R^\times$ is a continuous character. Then we define p-adic modular forms of naive level $\Gamma(N)$ of weight k over R as the R module

$$M(\Gamma(N), R, k) = \left\{ f \in H^0\Big(\mathfrak{X}^{\text{ord}}_R, \mathcal{O}_{M_{\text{Katz}R}}\Big) \mid \forall\ g \in \mathbb{Z}_p^\times,\ g \cdot f = k(g)f \right\}$$

Henceforth we will slightly abuse notation to write $\pi^*\omega = \mathcal{O}_{M_{\text{Katz}}}\, \mathrm{d}T/T$.

3.2.1 θ Operator

Consider the universal derivation

$$\begin{aligned} M(\Gamma(N), R, k) \subset H^0\Big(M_{\text{Katz}R}, \mathcal{O}_{M_{\text{Katz}R}}\Big) &\xrightarrow{\mathrm{d}} H^0\Big(M_{\text{Katz}R}, \Omega^1_{M_{\text{Katz}}/R}\Big) \\ f &\mapsto \mathrm{d}f \end{aligned}$$

Since g induces a R automorphism of $M_{\text{Katz}R}$, the action commutes with the universal

derivation. Thus we have the following diagram

$$\begin{array}{ccc} M(\Gamma(N),R,k) & \xrightarrow{\mathrm{d}} & H^0\Big(M_{\mathrm{Katz}R},\Omega^1_{M_{\mathrm{Katz}}/R}\Big) \\ \Big\downarrow g & & \Big\downarrow g \\ M(\Gamma(N),R,k) & \xrightarrow{\mathrm{d}} & H^0\Big(M_{\mathrm{Katz}R},\Omega^1_{M_{\mathrm{Katz}}/R}\Big) \end{array}$$

Now by the Kodaira-Spencer isomorphism $\pi^*\omega^2 \simeq \Omega^1_{M_{\mathrm{Katz}}/R}$. Thus

$$H^0\Big(M_{\mathrm{Katz}R},\Omega^1_{M_{\mathrm{Katz}}/R}\Big) \simeq H^0\Big(M_{\mathrm{Katz}R},\mathcal{O}_{M_{\mathrm{Katz}R}}\Big)(\mathrm{d}T/T)^2$$

Definition 3.2.2. Suppose f is a p-adic modular form of weight k. Define the θ operator to be $\theta(f) = h$ such that $\mathrm{d}f = h(\mathrm{d}T/T)^2$.

Proposition 3.2.1. *The θ operator is an operator of weight 2.*

Proof. If f is a p-adic modular form of weight $k \in \mathrm{Cont}(\mathbb{Z}_p^\times, R^\times)$, then by definition $g \cdot f = k(g)f$. Then by the above diagram,

$$\mathrm{d}(g \cdot f) = g \cdot (h(\mathrm{d}T/T)^2)$$

This gives $k(g)\,\mathrm{d}f = (g \cdot h)g^{-2}(\mathrm{d}T/T)^2$ which shows $g \cdot h = k(g)g^2h$. Thus θ is a map between $M(\Gamma(N),R,k) \xrightarrow{\theta} M(\Gamma(N),R,k+2)$. □

In order to understand the effect of θ on q-expansions of p-adic modular forms at a cusp, note that $\mathrm{d}T/T$ is the canonical differential ω_{can}. We then recall from Section 1.2.6 that over $\mathbb{Z}[1/N,\zeta_N][[q]]$, $\omega^2_{\mathrm{can}} \leftrightarrow N \cdot \mathrm{d}q/q$. Since θ is dual to $(\mathrm{d}T/T)^2$, this implies that

$$\theta = \frac{1}{N} q \frac{\mathrm{d}}{\mathrm{d}q}$$

3.3 The Moduli Problems $M_{\textbf{Igusa}}$ and $M_{\textbf{big Igusa}}$

3.3.1 $M_{\textbf{Ig},N,n}$

Fix base scheme $\mathbb{Z}/p^m\mathbb{Z}$. The moduli problem $M_{\mathrm{Ig},N,n}$ is defined as the functor classifying isomorphism classes of tuples $(E, \hat{\varphi}, \varphi^{\text{ét}}, \alpha_N)$ where α_N is a level N structure and

$$\hat{\varphi} : \hat{E}[p^n] \xrightarrow{\sim} \mu_{p^n} \qquad \varphi^{\text{ét}} : \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} E[p^n]^{\text{ét}}$$

$M_{\mathrm{Ig},N,n}$ is represented by $M_{\mathrm{Katz},N,n} \times_{Y(N)^{\mathrm{ord}}} M_{\mathrm{Katz},N,n}$ where the first projection forgets $\varphi^{\text{ét}}$ and the second projection forgets $\hat{\varphi}$. Thus $M_{\mathrm{Ig},N,n}$ is finite, etale and Galois over $M_{\mathrm{Katz},N,n}$ of order $\varphi(p^n)$.

3.3.2 $M_{\textbf{split},N,n}$

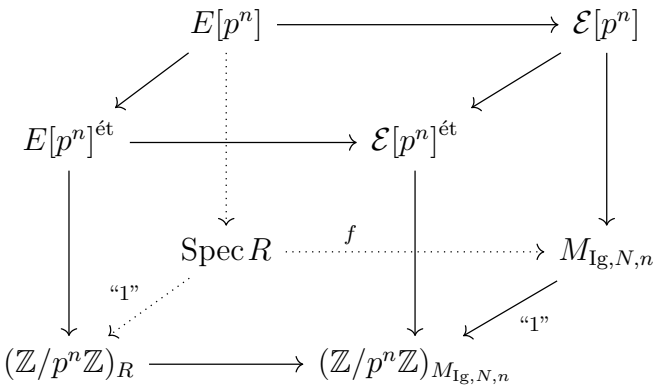
The moduli problem $M_{\mathrm{split},N,n}$ classifies isomorphism classes of tuples (E, φ, α_N) where $\varphi : E[p^n] \xrightarrow{\sim} \mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z}$ is a splitting of the p^n-torsion. This functor has an obvious projection to $M_{\mathrm{Ig},N,n}$.

Proposition 3.3.1. *$M_{split,N,n}$ is representable.*

Proof. We claim that $M_{\mathrm{split},N,n}$ is represented by the following fibre product

$$\begin{array}{ccc} X & \longrightarrow & M_{\mathrm{Ig},N,n} \\ \downarrow & & \downarrow{\scriptstyle \text{“1”}} \\ \mathcal{E}[p^n] & \longrightarrow & (\mathbb{Z}/p^n\mathbb{Z})_{M_{\mathrm{Ig},N,n}} \end{array}$$

where the lower arrow is the projection followed by the universal isomorphism of the etale quotient with $\mathbb{Z}/p^n\mathbb{Z}$. Indeed, given any (E, φ, α_N) a tuple over a ring R, there is a unique map $f : \operatorname{Spec} R \to M_{\mathrm{Ig},N,n}$ corresponding to the tuple $(E, \hat{\varphi}, \varphi^{\text{ét}}, \alpha_N)$ where $\hat{\varphi}$ and $\varphi^{\text{ét}}$ are defined from φ in the obvious way. We will show that X satisfies the universal property of $M_{\mathrm{split},N,n}$. We have the following diagram.



All the squares except the right square is commutative. We also have a section $\varphi^{-1}(1) : \operatorname{Spec} R \to E[p^n]$ of the projection $E[p^n] \to \operatorname{Spec} R$ which commutes with all the arrows of the left square. We need to show that the following two compositions are the same.

$$\operatorname{Spec} R \xrightarrow{f} M_{\mathrm{Ig},N,n} \xrightarrow{\text{“1”}} (\mathbb{Z}/p^n\mathbb{Z})_{M_{\mathrm{Ig},N,n}}$$

$$\operatorname{Spec} R \xrightarrow{\varphi^{-1}(1)} E[p^n] \to \mathcal{E}[p^n] \to E^{\text{ét}}[p^n] \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})_{M_{\mathrm{Ig},N,n}}$$

But this follows from the commutativity of the other squares. Thus there is a unique map from $\operatorname{Spec} R$ to X.

Conversely, the fibre product has the property that the following diagram commutes

$$\begin{array}{ccc} X & \longrightarrow & \mathcal{E}[p^n] \\ \downarrow{\scriptstyle \text{“1”}} & & \downarrow \\ (\mathbb{Z}/p^n\mathbb{Z})_X & \longrightarrow & (\mathbb{Z}/p^n\mathbb{Z})_{M_{\mathrm{Ig},N,n}} \end{array}$$

Hence this gives a splitting of the p^n-torsion of the universal elliptic curve over X. Hence X represents $M_{\mathrm{split},N,n}$. □

Let's try to understand the projection $M_{\mathrm{split},N,n} \to M_{\mathrm{Ig},N,n}$.

Proposition 3.3.2. *$M_{split,N,n} \to M_{Ig,N,n}$ is finite flat of rank p^n. Moreover it is a μ_{p^n}-torsor.*

Proof. $\mathcal{E}[p^n] \to \mathcal{E}[p^n]^{\text{ét}} \simeq (\mathbb{Z}/p^n\mathbb{Z})_{M_{\text{Ig},N,n}}$ is an epimorphism of finite locally free group schemes. Hence it is finite locally free. Hence $M_{\text{split},N,n} \to M_{\text{Ig},N,n}$ is finite locally free. To show it is a μ_{p^n}-torsor, we will show that $\mathcal{E}[p^n] \to (\mathbb{Z}/p^n\mathbb{Z})_{M_{\text{Ig},N,n}}$ is a μ_{p^n}-torsor. That is, we need to show the following map is an isomorphism

$$\Big((\mu_{p^n})_{\mathbb{Z}/p^n\mathbb{Z}} \times_{\mathbb{Z}/p^n\mathbb{Z}} \mathcal{E}[p^n] \simeq \mu_{p^n} \times_{M_{\text{Ig},N,n}} \mathcal{E}[p^n]\Big) \to \mathcal{E}[p^n] \times_{\mathbb{Z}/p^n\mathbb{Z}} \mathcal{E}[p^n]$$
$$(a, x) \mapsto (a \cdot x, x)$$

where $a \cdot x$ is the multiplication in $\mathcal{E}[p^n]$. But the isomorphism is clear on points as $\mathcal{E}[p^n]^{\text{ét}} \simeq \mathcal{E}[p^n]/\mu_{p^n}$. Hence by Yoneda's lemma, the map of schemes is an isomorphism. Thus $M_{\text{split},N,n} \to M_{\text{Ig},N,n}$ is a μ_{p^n}-torsor, since it is the base change of a μ_{p^n}-torsor. □

Over any ring R, such that $M_{\text{split},N,n}(R)$ is non-empty, suppose two points project to the same point of $M_{\text{Ig},N,n}(R)$. Suppose the two points are (E, φ, α_N) and (E, φ', α_N). Then φ and φ' are related by an R-group automorphism of $(\mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z})_R$. Consider the ring functor

$$\begin{pmatrix} \underline{\text{Hom}}(\mu_{p^n}, \mu_{p^n}) & \underline{\text{Hom}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) \\ \underline{\text{Hom}}(\mu_{p^n}, \mathbb{Z}/p^n\mathbb{Z}) & \underline{\text{Hom}}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{Z}/p^n\mathbb{Z}) \end{pmatrix}$$

Lemma 3.3.1. *Assume p is locally nilpotent on S. Then $\underline{\text{Hom}}(\mu_{p^n}, \mathbb{Z}/p^n\mathbb{Z}) = 0$ on Sch/S.*

Proof. Fix any base scheme, which we can assume to be affine, say $\operatorname{Spec} R$, and such that p is nilpotent in R. Then any homomorphism of R-group schemes $\mu_{p^n} \to \mathbb{Z}/p^n\mathbb{Z}$ is given by a R-Hopf-algebra homomorphism $R[\mathbb{Z}/p^n\mathbb{Z}] \to R[T]/(T^{p^n} - 1)$. Denote the obvious idempotents of $R[\mathbb{Z}/p^n\mathbb{Z}]$ by $e_0, e_1, \ldots, e_{p^n-1}$. Suppose f is a R Hopf-algebra homomorphism. Let $f_i = f(e_i)$ for all i.

Since both the algebras are finite, free modules over R we can assume that R is local. Since p is nilpotent in R, specialising at p doesn't collapse connected components. If $p = 0$ in R, then $R[T]/(T^{p^n} - 1)$ is a local ring and hence connected. Thus μ_{p^n} is connected over any local ring R. Hence $f_i = 0$ for all $i \neq 0$ and $f_0 = 1$, which shows that the only homomorphism is the trivial one. Thus we have proved the lemma. □

The lemma shows that the lower left entry of the matrix above is 0. $\underline{\text{Aut}}(\mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z})$

is a subfunctor (as multiplicative monoids) of the matrix above, and is given by

$$\begin{pmatrix} \underline{\mathrm{Aut}}(\mu_{p^n}) & \underline{\mathrm{Hom}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) \\ 0 & \underline{\mathrm{Aut}}(\mathbb{Z}/p^n\mathbb{Z}) \end{pmatrix} = \begin{pmatrix} (\mathbb{Z}/p^n\mathbb{Z})^\times & \mu_{p^n} \\ 0 & (\mathbb{Z}/p^n\mathbb{Z})^\times \end{pmatrix}$$

Going back to our discussion about the fibre of the projection $M_{\mathrm{split},N,n} \to M_{\mathrm{Ig},N,n}$, we see that (E, φ, α_N) and (E, φ', α_N) project to the same point iff φ and φ' are related by an unipotent matrix. Thus the subgroup functor of $\underline{\mathrm{Aut}}(\mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z})$, consisting of the unipotent matrices, which is exactly μ_{p^n} acts simply transitively on $M_{\mathrm{split},N,n}$. This also shows that $M_{\mathrm{split},N,n}$ is a μ_{p^n}-torsor over $M_{\mathrm{Ig},N,n}$.

3.3.3 The Frobenius

Proposition 3.3.3. *There exists a natural isomorphism $M_{split,N,n} \xrightarrow{\sim} M_{Ig,N,n}$ over $\mathbb{F}_p$ such that the following diagram commutes*

$$\begin{array}{ccc} M_{split,N,n} & \longrightarrow & M_{Ig,N,n} \\ \downarrow\wr & \nearrow_{Frob^n} & \\ M_{Ig,N,n} & & \end{array}$$

Proof. For any elliptic curve E/R where R is an $\mathbb{F}_p$-algebra, denote as usual by $E^{(p^n)}$ the base change of E by the Frobenius morphism of R.

$$\begin{array}{ccc} E^{(p^n)} & \longrightarrow & E \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \xrightarrow{\mathrm{Frob}^n} & \operatorname{Spec} R \end{array}$$

The relative Frobenius $F^n_{E/R} : E \to E^{(p^n)}$ is the product of the structure morphism $E \to \operatorname{Spec} R$ and the absolute Frobenius $F^n_{\mathrm{abs}} : E \to E$ induced by the map on structure sheaf $x \mapsto x^{p^n}$. The relative Frobenius is an isogeny of degree p^n whose kernel is a connected subgroup of $E[p^n]$. Whenever there is an inclusion

$$\mu_{p^n} \hookrightarrow E[p^n]$$

$F^n_{E/R}$ vanishes on the image of μ_{p^n} and hence it is exactly the kernel.

The natural transformation $M_{\mathrm{Ig},N,n} \xrightarrow{\mathrm{Frob}^n} M_{\mathrm{Ig},N,n}$ sends a R-valued point $(E, \hat{\varphi}, \varphi^{\text{ét}}, \alpha_N)$ to the R-valued point $(E^{(p^n)}, \hat{\varphi}^{(p^n)}, \varphi^{\text{ét}(p^n)}, {\alpha_N}^{(p^n)})$, where the isomorphisms are obtained by change of base $R \xrightarrow{\mathrm{Frob}^n} R$.

The isomorphism $\varphi^{\text{ét}} : \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} E[p^n]^{\text{ét}} \simeq E[p^n]/\mu_{p^n} \hookrightarrow E/(\mu_{p^n})[p^n] = E^{(p^n)}[p^n]$ gives a splitting of $E^{(p^n)}[p^n]$

$$\varphi : E^{(p^n)}[p^n] \xrightarrow{\sim} \mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z}$$

where

$$\varphi^{-1}|_{\mu_{p^n}} = (\hat{\varphi}^{(p^n)})^{-1} \quad \text{and} \quad \varphi^{-1}|_{\mathbb{Z}/p^n\mathbb{Z}} = \varphi^{\text{ét}}$$

Define a natural transformation $M_{\mathrm{Ig},N,n} \xrightarrow{f} M_{\mathrm{split},N,n}$ by sending

$$\begin{aligned} M_{\mathrm{Ig},N,n}(R) &\xrightarrow{f} M_{\mathrm{split},N,n}(R) \\ (E, \hat{\varphi}, \varphi^{\text{ét}}, \alpha_N) &\mapsto (E^{(p^n)}, \varphi, {\alpha_N}^{(p^n)}) \end{aligned}$$

Upon composing f with the projection on $M_{\mathrm{Ig},N,n}$ we get the point $(E^{(p^n)}, \hat{\varphi}^{(p^n)}, \varphi_0^{\text{ét}}, {\alpha_N}^{(p^n)})$ where $\varphi_0^{\text{ét}}$ is the composition $\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\varphi^{\text{ét}}} E^{(p^n)}[p^n] \xrightarrow{F_{E^{(p^n)}/R}} E^{(p^n)}[p^n]^{\text{ét}}$.

The commutativity of the following diagram shows that $\varphi^{\text{ét}(p^n)} \circ F_{(\mathbb{Z}/p^n\mathbb{Z})/R} = \varphi_0^{\text{ét}}$

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{\varphi^{\text{ét}}} & E^{(p^n)}[p^n] \\ {\scriptstyle F_{(\mathbb{Z}/p^n\mathbb{Z})/R}}\downarrow & & \downarrow{\scriptstyle F_{E^{(p^n)}/R}} \\ \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow[\varphi^{\text{ét}(p^n)}]{\sim} & E^{(p^n)}[p^n]^{\text{ét}} \end{array} \tag{3.1}$$

But relative Frobenius on the constant group scheme $\mathbb{Z}/p^n\mathbb{Z}$ is just identity. Thus $\varphi_0^{\text{ét}} = \varphi^{\text{ét}(p^n)}$.

Thus we have proved that

$$M_{\mathrm{Ig},N,n} \xrightarrow{f} M_{\mathrm{split},N,n} \longrightarrow M_{\mathrm{Ig},N,n}$$
$$\overset{\mathrm{Frob}^n}{\frown}$$

We need to construct the inverse map of f. Given a point $(E, \varphi, \alpha_N) \in M_{\text{split},N,n}(R)$, let $E' = E/(\mathbb{Z}/p^n\mathbb{Z})$ and denote the projection by $\pi : E \to E'$. Define $(\hat{\varphi}')^{-1}$ to be the inclusion $\mu_{p^n} \xhookrightarrow{\hat{\varphi}^{-1}} E[p^n] \xrightarrow{\pi} E'[p^n]$. Then

$$E'^{(p^n)} \simeq E'/\mu_{p^n} \simeq E/E[p^n] \simeq E$$

Now, $E'[p^n]^{\text{ét}} \hookrightarrow E'^{(p^n)}[p^n] = E[p^n]$. Define $\varphi_0^{\text{ét}} : \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} E'[p^n]^{\text{ét}}$ to be the restriction $\varphi^{-1}|_{\mathbb{Z}/p^n\mathbb{Z}}$. Since

$$\begin{array}{ccccc} E & \xrightarrow{\quad\pi\quad} & E' & \xrightarrow{\quad F_{E'/R}\quad} & E \\ & \searrow^{[p^n]} & & \nearrow & \end{array}$$

$F_{E'/R} : E' \to E$ induces an isomorphism of the N-torsion. Define α'_N to be the unique level N structure such that the following diagram commutes

$$\begin{array}{ccc} E'[N] & \xrightarrow{\quad F_{E'/R}\quad} & E[N] \\ & {\scriptstyle \alpha'_N} \nwarrow \quad \nearrow {\scriptstyle \alpha_N} & \\ & (\mathbb{Z}/N\mathbb{Z})^2 & \end{array}$$

Under the base change $R \xrightarrow{\text{Frob}^n} R$, the map π becomes $V^n_{E/R} : E^{(p^n)} \to E$, which is the dual of $F^n_{E/R}$. The dual of diagram (3.1) shows that $\hat{\varphi} \circ V^n_{E/R} = \hat{\varphi}^{(p^n)}$. It's obvious from the definition that $\varphi_0^{\text{ét}(p^n)} = \varphi^{\text{ét}}$. Also by construction ${\alpha'_N}^{(p^n)} = \alpha_N$. Therefore we can define the map g to be

$$\begin{aligned} M_{\text{split},N,n} &\xrightarrow{g} M_{\text{Ig},N,n} \\ (E, \varphi, \alpha_N) &\mapsto (E', \hat{\varphi}', \varphi_0^{\text{ét}}, \alpha'_N) \end{aligned}$$

Then by construction g followed by the projection is Frob^n. It's easy to check that f and g are inverses of each other. This gives the required natural isomorphism. □

Remark 3.3.1. We showed that over $\mathbb{Z}/p^m\mathbb{Z}$ both $M_{\text{Ig},N,n}$ and $M_{\text{split},N,n}$ are representable. One can consider the tower of $\{M_{\text{Ig},N,n}\}_{n\in\mathbb{N}}$ or $\{M_{\text{split},N,n}\}_{n\in\mathbb{N}}$ just as we did for M_{Katz}. One can then take the limit. In the first case we define $M_{\text{Igusa}} = \varprojlim_n M_{\text{Ig},N,n}$ and in the second case, $M_{\text{big Igusa}} = \varprojlim_n M_{\text{split},N,n}$. We note that in both cases the inverse system consists of affine schemes with the transition maps affine. Hence the

limits are representable and represented by the direct limit of the respective direct system of rings.

One can also vary the base scheme and doing so get a system of thickenings of M_{Igusa} and $M_{\text{big Igusa}}$ which define affine formal schemes over $\mathfrak{X}^{\text{ord}}$.

We will study $M_{\text{big Igusa}}$ in more detail in the next chapter. This functor classifies isomorphism classes of tuples $(E/R, \varphi, \alpha_N)$ where E/R is an elliptic curve over $R \in \text{Nilp}_{\mathbb{Z}_p}$, $\varphi : E[p^\infty] \xrightarrow{\sim} \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$ and $\alpha_N : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$.

Chapter 4

The $\widehat{\mathbb{G}_m}$ Action

4.1 p-divisible Groups

Definition 4.1.1. Let R be a ring. A p-divisible group over R is a sequence $\{G_n\}_{n\in\mathbb{N}}$ of finite, locally free group schemes over R, equipped with closed immersions $i_n : G_n \hookrightarrow G_{n+1}$ such that

1. G_n is p^n-torsion
2. i_n identifies G_n with $G_{n+1}[p^n]$
3. Multiplication by p is a fppf surjection $G_{n+1} \to G_n$

Each G_n defines a fppf sheaf of abelian groups on $\mathrm{Alg}_R^{\mathrm{op}}$. The transition maps are all injective. Since every object of $\mathrm{Alg}_R^{\mathrm{op}}$ is quasi-compact in the fppf topology, this implies that the direct limit presheaf $G := \varinjlim_n G_n$ is already a sheaf, i.e. for any $\operatorname{Spec} A \in \mathrm{Alg}_R^{\mathrm{op}}$, $(\varinjlim G_n)(A) = \varinjlim G_n(A)$.

To say that each G_n is finite, locally free over R it is enough to demand that G_1 is so, because each G_n is a multiple extension of group schemes isomorphic to G_1. The data that G_1 is p-torsion then implies from the theory of finite group schemes over fields, that the fibres of G_1 are of rank p^h for a locally constant function h on $\operatorname{Spec} R$. This leads us to the equivalent definition of a p-divisible group due to Tate [Tat67, section 2.1].

Definition 4.1.2. A p-divisible group on R is a direct system of finite, locally free group schemes $(G_n, i_n)_{n\in\mathbb{N}}$ such that

1. The rank of a fibre of G_n is p^{nh} where h is a locally constant function on $\operatorname{Spec} R$
2. i_n identifies G_n with $G_{n+1}[p^n]$

Example 4.1.1.
1. $\mu_{p^\infty} = \varinjlim \mu_{p^n}$.
2. $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim \mathbb{Z}/p^n\mathbb{Z}$.
3. For any elliptic curve E/R the p^∞ torsion $E[p^\infty]$ is a p-divisible group of height 2.

Definition 4.1.3. For G a p-divisible group on R, we define the formal neighborhood of the identity $\hat{G}$ by

$$\hat{G} := \varinjlim_k \operatorname{Inf}^k(G)$$

Definition 4.1.4. For a p-divisible group G on $\operatorname{Nilp}_R^{\mathrm{op}}$, we define the universal cover following [SW12, section 3.1] as the sheaf on $\operatorname{Nilp}_R^{\mathrm{op}}$

$$\tilde{G} := \varprojlim\ G \xleftarrow{p} G \xleftarrow{p} G \xleftarrow{p} \dots$$

Definition 4.1.5. We define the Tate module of G as a subsheaf of $\tilde{G}$

$$T_pG := \varprojlim\ 0 \xleftarrow{p} G[p] \xleftarrow{p} G[p^2] \dots$$

For $A \in \operatorname{Nilp}_R^{\mathrm{op}}$, write an element of $\tilde{G}(A)$ as a sequence $(x_0, x_1, ...)$ such that $px_{i+1} = x_i$ for all $i \geq 0$. Then we have an exact sequence

$$0 \to T_pG \to \tilde{G} \to G$$

by projecting onto the first coordinate.

Lemma 4.1.1. *T_pG is representable by an affine scheme.*

Proof. This is because each G_n is affine and the transition maps are all affine. □

Lemma 4.1.2. *If G is a p-divisible group*

$$0 \to T_p G \to \tilde{G} \to G \to 0$$

is an exact sequence in the fpqc topology.

Proof. If $G_n = \operatorname{Spec} R_n$ then $\tilde{G} \times_G G[p^n]$ is represented by $\operatorname{Spec}(\varinjlim_{i \geq n} R_i)$. The inclusion $R_n \hookrightarrow \varinjlim_{i \geq n} R_i$ is an fpqc cover. This proves the lemma because any A-point of G, $\operatorname{Spec} A \to G$ factors through some $G[p^n]$. □

A homomorphism of p-divisible groups in Tate's terminology [Tat67] is a morphism of direct system of group schemes.

Definition 4.1.6. Let G and G' be two p-divisible groups over R. A homomorphism $f : G \to G'$ is called an isogeny if it is an fppf epimorphism of sheaves with finite, locally free kernel. A quasi-isogeny is a global section f of $\underline{\operatorname{Hom}}_R(G, G') \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $p^n f$ is an isogeny for some $n \geq 0$.

Example 4.1.2. A p-isogeny of two elliptic curves $f : E \to E'$ over R induces an isogeny of their p-divisible groups. An isogeny of E and E' of degree coprime to p induces an isomorphism of their p-divisible groups. Similarly quasi-isogenies of elliptic curves induce quasi-isogenies of their p-divisible groups.

One can extend our definition of p-divisible groups over arbitrary base scheme S. We have the following proposition.

Proposition 4.1.1. *Suppose S is connected or quasi-compact (eg. affine). A morphism $f : G \to G'$ of p-divisible groups over S is an isogeny iff there exist a morphism $g : G' \to G$ and an integer $N \geq 0$ such that $g \circ f = p^N id_G$ and $f \circ g = p^N id_{G'}$.*

Proof. Suppose f is an isogeny. Since f is an epimorphism there is an isomorphism

$$G/\ker f \xrightarrow{\sim} G'$$

Suppose N be such that $\ker f \subset G[p^N]$. Then the map $p^N : G/\ker f \to G/\ker f$ lifts

through G

$$\begin{array}{ccc} G/\ker f & \xrightarrow{p^N} & G/\ker f \\ \downarrow{\scriptstyle p^N} & \nearrow & \\ G & & \end{array}$$

Then $g : G' \simeq G/\ker f \xrightarrow{p^N} G$ is the morphism we are looking for. Clearly, $g \circ f = p^N \mathrm{id}_G$. Also, $f \circ g \circ f = p^N \mathrm{id}_{G'} \circ f$. Since f is an epimorphism, $f \circ g = p^N \mathrm{id}_{G'}$.

Conversely, suppose $f \circ g = p^N$ and $g \circ f = p^N$. Then

$$G[p^N] \underset{g}{\overset{f}{\rightleftarrows}} G'[p^N]$$

show that $\ker f|_{G[p^N]} = \mathrm{im}\, g|_{G'[p^N]}$. The inclusion $\mathrm{im}\, g|_{G'[p^N]} \subset \ker f|_{G[p^N]}$ is clear. If $x \in \ker f \cap G[p^N]$ then fppf locally $x = p^N y = g(f(y))$ for some y. Then $f(g(f(y))) = f(x) = 0$ implies $f(y) \in G'[p^N]$.

Now $\ker f = \ker f|_{G[p^N]}$ is finite over S of finite presentation. Also since $g|_{G'[p^N]}$ is an epimorphism, it is flat over S. □

Lemma 4.1.3. *A quasi-isogeny of p-divisible groups induce an isomorphism of universal covers.*

Proof. This is trivial as p is invertible in the universal cover. □

Theorem 4.1.1. *If $S \in Nilp_R^{op}$ and G is a p-divisible group over S, then G is formally smooth.*

Proof. [See Mes72, II, Theorem 3.3.13]. □

Lemma 4.1.4. *Let G be a p-torsion group on S, (i.e. $G = \varinjlim_n G[p^n]$), with all $G[p^n]$ representable. Assume X' is an S-scheme and $X \hookrightarrow X'$ is a subscheme defined by an ideal I such that $I^{k+1} = 0$ and $p^N I/I^2 = 0$. Then if $f' : X' \to G$ is such that $f = f'|_{X'} : X' \to G[p^n]$, we have $f' : X' \to G[p^{n+kN}]$.*

Proof. The problem is local on X' and S and hence we can assume both $X' = \mathrm{Spec}\, B$ and $S = \mathrm{Spec}\, R$ are affine and so quasi-compact. But then $f' \in \Gamma(X', G[p^{n'}])$ for some

n'. Therefore we assume that G is representable, say by $\operatorname{Spec} A$. We use induction on k. If we could show that $f'|_{V(I^k)} : V(I^k) \to G[p^{n+(k-1)N}]$, then by the case $k = 1$ we would know $f' : X' \to G[p^{n+kN}]$. Thus it suffices to show for $k = 1$, i.e. $I^2 = 0$. Since $f : X \to G[p^n]$ we have $[p^n]f = 0$. So $[p^n]f' : X \to G$ is a map whose restriction to X is zero. Since $I^2 = 0$ and G is representable, the X' valued points of G whose restriction to X is zero are in bijection with the R derivations $A \to I$. In particular, if $g : A \to R \to B$ is the zero of the group $G(X')$ then $[p^n]f' - g \in \operatorname{Der}_R(A, I)$ and conversely, for any $\delta \in \operatorname{Der}_R(A, I)$, $g + \delta$ is a map whose restriction to X is zero. Since p^N kills I, we have $[p^N][p^n]f' = 0$ which proves the lemma. □

Corollary 4.1.1. Let $p^N = 0$ on S and let G be as in Lemma 4.1.4. Then the k-th infinitesimal neighborhood of $G[p^n]$ in G is the same as that of $G[p^n]$ in $G[p^{n+kN}]$. In particular $\operatorname{Inf}^k(G) = \operatorname{Inf}^k(G[p^{kN}])$ and is therefore representable.

Proof. If $f : T' \to G$ belongs to the k-th infinitesimal neighborhood of $G[p^n]$ in G, then there is a covering family $\{T'_i \to T'\}$ and schemes T_i such that $T_i \hookrightarrow T'_i$ is a nilpotent immersion of order k and $f|_{T_i} : T_i \to G[p^n]$. But then by Lemma 4.1.4 $f|_{T'_i} : T'_i \to G[p^{n+kN}]$ and hence $f \in \Gamma(T', G[p^{n+kN}])$. □

Corollary 4.1.2. If $p^N = 0$ on S and if $k < p^n$ we have $\operatorname{Inf}^k(G) \subset G[p^{n+N-1}]$ and hence $\operatorname{Inf}^k(G) = \operatorname{Inf}^k(G[p^{n+N-1}])$.

Proof. Let X' be an S-scheme and $X \hookrightarrow X'$ be a nilpotent immersion of order k. Denote with the subscript "$\circ$" the object obtained by reducing a given object modulo p. Given $f' : X' \to G$ whose restriction to X is zero, then we have $f'_\circ : X'_\circ \to G_\circ$ belongs to $\operatorname{Inf}^k(G_\circ)$. Since $k < p^n$, $\operatorname{Inf}^k(G_\circ) \subset G_\circ[p^n]$. But this means that the restriction of $f' \in G(X')$ to $G(X'_\circ) = G_\circ(X'_\circ)$ lies in $G[p^n](X'_\circ)$. □

Theorem 4.1.2. *Let $S \in Nilp_R^{op}$ and G a p-divisible group on S. Then $\hat{G}$ (Definition 4.1.3) is a formal Lie group.*

Proof. By Lemma 2.1.3 we know $\hat{G}$ is a subgroup of G. We need to show that it is a formal Lie group. By Corollary 4.1.1 $\operatorname{Inf}^k(G)$ is, locally on S, representable and therefore is globally representable by the sheaf property and gluing lemma.

By Theorem 4.1.1 we know G is formally smooth and this implies that $\hat{G}$ is formally smooth. This tells us that $\mathrm{Inf}^k(G)$ satisfies the lifting condition on points. Since locally on S, $\mathrm{Inf}^k(G) = \mathrm{Inf}^k(G[p^m])$ for appropriate m, and $G[p^m]$ is finite locally free, (and hence of finite presentation) over S it follows from general facts about smooth algebras [cf. Mes72, II, Theorem 3.1.1] imply that locally on S, $\mathrm{Inf}^k(G)$ is isomorphic to a pointed scheme (i.e. a scheme over S with a section to the structure morphism) of the form

$$\mathrm{Spec}\,\mathcal{O}_S[T_1, \ldots, T_n]/(T_1, \ldots, T_n)^{k+1}$$

This shows that $\hat{G}$ satisfies condition 2 and 3 of Definition 2.1.6 and hence it is a formal Lie group. □

Lemma 4.1.5. *If $S \in Nilp_R^{op}$ and $\hat{G}$ is a formal Lie group, then $\hat{G}$ is of p-torsion.*

Proof. We must show $\hat{G} = \varinjlim_n \hat{G}[p^n]$. We can assume that $S = \mathrm{Spec}\,A$ with p nilpotent on A and $\hat{G}$ is given by a power series ring $A[[X_1, \ldots, X_N]]$. If T is any affine S-scheme, say $T = \mathrm{Spec}\,B$, then an element of $\hat{G}(T)$ will be an N-tuple $(b_1, \ldots, d_N)$ with each b_i nilpotent. Let I be the ideal generated by $\{b_1, \ldots, b_N\}$. Then each component of $[p]^{\#}(b_1, \ldots, b_N)$ belongs to $pI + I^2$. Since p and I are both nilpotent, we see that $\hat{G}$ is p-torsion. □

Proposition 4.1.2. *Let $S \in Nilp_R^{op}$ and G a p-divisible group on S. Then $\hat{G} = 0$ iff G is ind-étale.*

Proof. If G is ind-étale, then locally a point of $\mathrm{Inf}^k(G)$ with values in an S-scheme T which we can assume to be affine, must be a point of $G[p^n]$ for some n, and hence is 0 since $G[p^n]$ is étale. Conversely, if $\hat{G} = 0$, then for any $s \in S$, $\hat{G}_s = 0$, which implies $G[p^n]_s$ has no connected part for all n and all s and hence is étale. But $G[p^n]$ is flat over S and has étale fibres. Hence it is étale. □

Lemma 4.1.6. *Let $0 \to G \to H \to K \to 0$ be a complex of finite locally free groups on S. The sequence is exact iff for all $s \in S$, the sequence $0 \to G_s \to H_s \to K_s \to 0$ is exact.*

Proof. ($\Longrightarrow$) is clear.

($\Longleftarrow$) By the fibrewise criterion of flatness, we know that $H \to K$ is an epimorphism if all maps $H_s \to K_s$ are epimorphisms. Thus it remains to prove the map $G \to \ker u$ is an isomorphism. This can be checked locally on S. Hence we assume $S = \operatorname{Spec} A$, $G = \operatorname{Spec} C$, $\ker u = \operatorname{Spec} B$ where B and C are finite projective A-modules. To show $B \to C$ is an isomorphism, it suffices to prove this at each point. Hence we can assume A is a local ring with maximal ideal $\mathfrak{m}$. By hypothesis $B/\mathfrak{m}B \to C/\mathfrak{m}C$ is an isomorphism. By Nakayama $B \to C$ is surjective, and it is injective since C is flat. □

Lemma 4.1.7. *Let $S \in Nilp_R^{op}$ and let $0 \to G_1 \to G_2 \to G_3 \to 0$ be an exact sequence of p-divisible groups on S. Then $0 \to \hat{G}_1 \to \hat{G}_2 \to \hat{G}_3 \to 0$ is also exact.*

Proof. The sequence for the formal Lie groups is left exact as they are subgroups of the corresponding p-divisible groups. We need to prove $\hat{G}_2 \to \hat{G}_3$ is an epimorphism. Let T be an S-scheme and $y \in \hat{G}_3(T)$. Since $G_2 \to G_3$ is surjective, there is a covering $\{T_i \to T\}$ such that for each i, there is an $x_i \in G_2(T_i)$ whose image is $y|_{T_i}$. By passing to a covering of each T_i we can assume $y|_{T_i}$ has the property that $y|_{\overline{T}_i} = 0$ where $\overline{T}_i \hookrightarrow T_i$ is a nilpotent immersion and T_i is affine. But then $x_i|_{\overline{T}_i} \in G_1(\overline{T}_i)$. Since G_1 is formally smooth, we know there is an $x_i' \in G_1(T_i)$ which lifts $x_i|_{\overline{T}_i}$. Then $x_i - x_i' \mapsto y|_{T_i}$ and has its restriction to $\overline{T}_i$ equal to 0. Hence $x_i - x_i' \in \hat{G}_2(T_i)$ and hence the map $\hat{G}_2 \to \hat{G}_3$ is an epimorphism. □

With all the above preparations, we come to the proof of the Theorem promised in Section 3.1 (Theorem 3.1.1). We state the result in more generality than in Theorem 3.1.1.

Theorem 4.1.3. *Let p be locally nilpotent on S and G a p-divisible group on S. The following conditions are equivalent:*

1. *$\hat{G}$ is a p-divisible group.*
2. *G is an extension of an ind-étale p-divisible group G'' by an ind-infinitesimal p-divisible group G'.*
3. *G is an extension of an ind-étale p-divisible group by a p-divisible formal Lie group.*

4. *For all n, $G[p^n]$ is an extension of a finite étale group scheme by a finite locally free radiciel group scheme.*

5. *$G[p]$ is an extension of a finite étale group by a finite locally free radiciel group.*

6. *Separable rank of the fibres of $G[p]$ over S is a locally constant function.*

Proof. (6) $\implies$ (5) follows from Corollary 3.1.1.

(5) $\implies$ (6) is clear.

(4) $\implies$ (5) is clear.

(5) $\implies$ (4) follows from the fact that

$$\text{separable rank of } G[p^n]_s = (\text{separable rank of } G[p]_s)^n$$

This follows from the exact sequences

$$0 \to G[p^{n-1}] \to G[p^n] \to G[p] \to 0$$

(4) $\implies$ (2) For each n we have an exact sequence

$$0 \to G'[p^n] \to G[p^n] \to G''[p^n] \to 0$$

with $G'[p^n]$ finite locally free and radiciel, and $G''[p^n]$ finite and étale. We will show that the systems $\{G'[p^n]\}_n$ and $\{G''[p^n]\}_n$ give us p-divisible groups. To do this it suffices to see that if $0 \to G \to H \to K \to 0$ is an exact sequence of finite locally free groups satisfying the condition of the lemma, then the corresponding sequences of étale quotients or radiciel kernels are exact. By Lemma 4.1.6 it suffices to prove this statement over geometric fibres. But in that case it is obvious because any finite group H has a splitting $H = H^\circ \times H^{\text{ét}}$.

Therefore by applying the above discussion to the sequences $0 \to G[p^i] \to G[p^n] \xrightarrow{p^i} G[p^{n-i}] \to 0$ we see that $G' = \varinjlim G'[p^n]$ and $G'' = \varinjlim G''[p^n]$ are p-divisible groups. Furthermore, G' is ind-infinitesimal and G'' is ind-étale.

(2) $\implies$ (4) follows from the observation that an exact sequence $0 \to G' \to G \to G'' \to 0$ induces by snake lemma an exact sequence $0 \to G'[p^n] \to G[p^n] \to G''[p^n] \to 0$.

Note that till now we didn't use the assumption that p is nilpotent on S. We will use it now.

(2) $\implies$ (3) G' being ind-infinitesimal, we have $G' = \hat{G'}$ and it is therefore a formal Lie group, by Theorem 4.1.2.

(3) $\implies$ (2) Let $0 \to G' \to G \to G'' \to 0$ be an exact sequence with G' a p-divisible formal Lie group and G'' an ind-étale p-divisible group. We need to show G' is a p-divisible group, i.e. it is p-torsion and $G'[p]$ is finite locally free. Lemma 4.1.5 implies G' is p-torsion. To show $G'[p]$ is finite locally free we apply snake lemma again to the exact sequence, with vertical arrows being multiplication by p, and this gives an exact sequence $0 \to G'[p] \to G[p] \to G''[p] \to 0$. This proves the implication.

(2) $\implies$ (1) Lemma 4.1.7 and Proposition 4.1.2 imply that $G' = \hat{G}$ and hence $\hat{G}$ is a p-divisible group.

(1) $\implies$ (2) If $\hat{G}$ is a p-divisible group then we can form the sequence $0 \to \hat{G} \to G \to G/\hat{G} \to 0$. It is a fact that quotient of two p-divisible groups is a p-divisible group [cf. Mes72, pp. I, 2.4.3]. But Lemma 4.1.7 implies $\widehat{G/\hat{G}} = 0$. Hence by Proposition 4.1.2 it is ind-étale. This completes the proof. □

Theorem 4.1.4. *Let R be a ring where p is nilpotent. Assume G is a p-divisible group that is isogenous to an extension of an ind-étale p-divisible group by a connected p-divisible group. Then the functor G is representable by a formal scheme, which locally admits a finitely generated ideal of definition.*

Proof. First assume G is ind-étale. Since $G[p^{n+1}]$ is étale, the zero section is an open (and closed) immersion. Hence every inclusion $i_{n,n+1} : G[p^n] \hookrightarrow G[p^{n+1}]$ is an open immersion, being the base change of the zero section by the map $p^n : G[p^{n+1}] \to G[p^n]$. Then the representability follows from the gluing lemma for schemes.

For the general case, since the question is local on $\operatorname{Spec} R$, assume R is such that $\hat{G}$ is the formal spectrum of a power series ring. We want to show that $G \times_{G^{\text{ét}}} G^{\text{ét}}[p^n]$ is representable by a formal scheme for all n. This will imply that $G = \varinjlim_n G \times_{G^{\text{ét}}} G[p^n]^{\text{ét}}$ is representable because the transition maps are open immersions.

Over an étale cover $S' = \operatorname{Spec} R' \to \operatorname{Spec} R = S$ where $G^{\text{ét}}[p^n]$ splits into sections, $G \times_{G^{\text{ét}}} G^{\text{ét}}[p^n]$ is the disjoint union of copies of $\hat{G}$. Suppose $(G \times_{G^{\text{ét}}} G^{\text{ét}}[p^n])_{S'} = \operatorname{Spf} A$

where A is a ring complete w.r.t. a finitely generated ideal I. We get a descent datum $\varphi : \operatorname{Spf} A \times_S S' \xrightarrow{\sim} S' \times_S \operatorname{Spf} A$ by the sheaf property. Set $\mathfrak{X}$ equal to the coequalizer in the following diagram

$$\operatorname{Spf} A \times_S S' \underset{\mathrm{pr}_2 \circ \varphi}{\overset{\mathrm{pr}_1}{\rightrightarrows}} \operatorname{Spf} A \longrightarrow \mathfrak{X}$$

Since $\operatorname{Spf} A = \varinjlim_k \operatorname{Spec} A/I^k$, the coequalizer exists and is equal to $\varinjlim_k X_k$ where X_k is the descent of $\operatorname{Spec} A/I^k$ to S [Stacks, Lemma 0245]. The X_k are affine and the transition maps $X_k \to X_{k+1}$ satisfy the property that they are nilpotent thickenings over the étale cover S' of S. Hence they are nilpotent thickenings themselves. Thus $\mathfrak{X}$ is an affine formal scheme with finitely generated ideal of definition because the property of a morphism being of finite presentation is local on the target for the étale topology. Finally $\mathfrak{X}$ represents $G \times_{G^{\text{ét}}} G[p^n]^{\text{ét}}$ by the sheaf property [Stacks, Tag 02W4]. □

Theorem 4.1.5. *Let R be as above. Assume that G is isogenous to an extension of an ind-étale by a connected p-divisible group. Then $\tilde{G}$ is representable by a formal scheme which locally admits a finitely generated ideal of definition.*

Proof. Since the question is local on R, assume by Theorem 4.1.4, G is represented by the formal spectrum of a R-algebra A which is complete w.r.t. a finitely generated ideal I. Since the maps $G \xrightarrow{p} G$ are finite locally free, and in particular affine, $\tilde{G}$ is represented by $\operatorname{Spf} \hat{B}$ where $B = \varinjlim_p A$, the ideal of definition being the ideal generated by the image of I under the inclusion of the first component and the completion being w.r.t the ideal of definition. □

Theorem 4.1.6. *If R is perfect of characteristic p, G is connected and Lie(G) is free of dimension d, then*

$$\tilde{G} \simeq Spf\, R[[x_1^{1/p^\infty}, \ldots, x_d^{1/p^\infty}]]$$

Proof. Let $G^{(p^n)} = G \times_R^{\text{Frob}} R$. Consider the relative Frobenius isogeny $F : G^{(p^n)} \to G^{(p^{n+1})}$ and its dual, Verschiebung $V : G^{(p^{n+1})} \to G^{(p^n)}$. $VF = p \cdot \mathrm{id}_{G^{(p^n)}}$ and $FV = p \cdot \mathrm{id}_{G^{p^{n+1}}}$. There is a natural transformation of functors $\mathcal{V} : \varprojlim_p G \to \varprojlim_F G^{(p^{-n})}$,

given by

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

We claim that $\mathcal{V}$ is an isomorphism. Since G is connected, there exists $m \geq 1$ such that $G[p] \subset \ker F^m$. Then $F^m = pu$ for some isogeny $u : G^{(p^{-m})} \to G$. Use the symbol u to denote the base change to $G^{(p^{-mn})} \to G^{(p^{-m(n-1)})}$, for any $n \in \mathbb{Z}$ so that u^n is an isogeny $G^{(p^{-mn})} \to G$. Denote by $\mathcal{U}$ the natural transformation $\varprojlim_{F^m} G^{(p^{-mn})} \to \varprojlim_p G$ induced by the u^n. We will show that $\mathcal{U}$ and $\mathcal{V}$ are inverses of each other upto the isomorphism $\varprojlim_F G^{(p^{-n})} \simeq \varprojlim_{F^m} G^{(p^{-mn})}$. This last isomorphism comes from the fact that the later inverse system is cofinal in the former. Explicitly, the isomorphism (denoted by φ) is given on points by

$$(a_0, a_1, \dots) \xrightarrow{\varphi} (a_0, a_m, \dots)$$

Let us check that $\mathcal{U} \circ \varphi \circ \mathcal{V} = \mathrm{id}$ on points.

$$(a_0, a_1, ...) \xrightarrow{\mathcal{V}} (a_0, Va_1, ...) \xrightarrow{\varphi} (a_0, V^m a_m, ...) \xrightarrow{\mathcal{U}} (a_0, uV^m a_m, ...)$$

Now, $uV^m p = puV^m = F^m V^m = p^m$. This implies that $uV^m = p^{m-1}$ since p is an epimorphism. Thus $uV^m a_m = p^{m-1} a_m = a_1$. Similarly one can check for the higher indices.

Conversely, let us check that $\mathcal{V} \circ \mathcal{U} \circ \varphi = \mathrm{id}$.

$$(a_0, a_1, ...) \xrightarrow{\varphi} (a_0, a_m, ...) \xrightarrow{\mathcal{U}} (a_0, ua_m, ...) \xrightarrow{\mathcal{V}} (a_0, Vua_m, ...)$$

Now, $Vup = VF^m = pF^{m-1} = F^{m-1}p$. Hence $Vu = F^{m-1}$, again using the fact that p is surjective. Thus $Vua_m = F^{m-1}a_m = a_1$. The check for higher indices is similar.

Finally, it is clear that $\tilde{G}$ is represented by the formal spectrum of the completion of $\varinjlim_F R[[x_1, \dots, x_d]]$. □

Theorem 4.1.7. *Let $S \to R$ be a surjection with nilpotent kernel J and p nilpotent in S. Assume G is a p-divisible group over R which has a lift G_S to S. Then $\tilde{G}_S(S) =$*

$\tilde{G}(R)$.

Proof.

$$\tilde{G}(R) = T_pG(R)[1/p] = \mathrm{Hom}_R(\mathbb{Q}_p/\mathbb{Z}_p, G)[1/p]$$

The natural map $\tilde{G}_S(S) \to \tilde{G}(R)$ is surjective by formal smoothness of G (Theorem 4.1.1). We need to show that the map is injective. Suppose $f \mapsto 0$. Since p is invertible on $\tilde{G}_S$ it is enough to show that $p^n f = 0 \in \tilde{G}_S(S)$ for some $n > 0$. We can even assume that G_S is connected, i.e. a formal group. Suppose I is the augmentation ideal of the formal group.

Denoting by $f^{\#} : \mathcal{O}_G \to \mathcal{O}_{\mathbb{Q}_p/\mathbb{Z}_p}$ the induced map on sheaves we see that $f^{\#}(I) \subset J\mathcal{O}_{\mathbb{Q}_p/\mathbb{Z}_p}$. Since modulo p, the isogeny $[p]$ factors through F, we have $[p]I \subset (pI, I^p)$. Thus $f^{\#}[p](I) \subset (pJ, J^p)\mathcal{O}_{\mathbb{Q}_p/\mathbb{Z}_p}$. Since both p and J are nilpotent, $f^{\#}([p^N]J) = 0$ for $N \gg 0$. □

4.1.1 An Equivalent Definition of $M_{\text{big Igusa}}$

Recall that we defined $M_{\text{big Igusa}}$ over $\mathbb{Z}/p^m\mathbb{Z}$ as classifying splittings of the p-divisible group of ordinary elliptic curves with level N structure. More generally we can assume the base ring to be a ring R where p is nilpotent.

In this section, we will define another functor F to **Sets** on $\mathrm{Alg}_R^{\mathrm{op}}$ and show that $M_{\text{big Igusa}}$ is naturally isomorphic to F.

Definition 4.1.7. Let F be the functor on $\mathrm{Alg}_R^{\mathrm{op}}$ defined as follows:

$$S \mapsto \Big\{(E/S, \tilde{\varphi}, \alpha_N)\Big\}/\sim$$

where $\tilde{\varphi} : \widetilde{E[p^\infty]} \xrightarrow{\sim} \widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p$ and two such tuples are equivalent if they are related by a quasi-p-isogeny of elliptic curves.

Remark 4.1.1. Given any two tuples representing the same point they are related by a necessarily unique quasi-p-isogeny, as any p-isogeny of an elliptic curve inducing identity on the universal cover of its p-divisible group must be the identity itself.

We see that there is a natural map $M_{\text{big Igusa}} \to F$ sending the isomorphism class of (E, φ, α_N) to the quasi-p-isogeny class of $(E, \tilde{\varphi}, \alpha_N)$ where $\tilde{\varphi}$ is induced by φ in the obvious way. We will show that this map is a natural isomorphism.

Theorem 4.1.8. *With definitions as above, $M_{big\ Igusa}$ is naturally isomorphic to F.*

Proof. We need to produce an inverse to this natural map. Thus we need to show that given any $(E/S, \tilde{\varphi}, \alpha_N)$ there is an E'/S, a splitting $\varphi' : E'[p^\infty] \xrightarrow{\sim} \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$ and a quasi-p-isogeny $f : E \to E'$ such that

$$\begin{array}{ccc} \widetilde{E[p^\infty]} & \xrightarrow{\quad\tilde{f}\quad} & \widetilde{E'[p^\infty]} \\ & {\scriptstyle\tilde{\varphi}}\searrow \quad \swarrow{\scriptstyle\tilde{\varphi}'} & \\ & \widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p & \end{array}$$

where $\tilde{\varphi'}$ is induced by φ'.

Let's denote $\mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$ by G to simplify notation. Consider $\widetilde{E[p^\infty]} \xrightarrow{\tilde{\varphi}} \tilde{G} \xrightarrow{\pi_0} G$ where π_0 is the projection onto the first coordinate as in Lemma 4.1.2. Restricting this map to $T_pE := T_pE[p^\infty]$ we get a T_pE valued point of G. Note that by Lemma 4.1.1, T_pE is represented by an affine scheme. Since $G(T_pE) = \varinjlim G_n(T_pE)$ this implies that $\pi_0 \circ \tilde{\varphi}|_{T_pE}$ factors through some G_n for n big enough. This implies that $\pi_0 \circ \tilde{\varphi}|_{p^n T_pE} = 0$. Thus $\pi_0 \circ \tilde{\varphi}$ factors as follows

$$\begin{array}{ccc} \widetilde{E[p^\infty]} & \xrightarrow{\tilde{\varphi}} & \tilde{G} \\ \downarrow{\scriptstyle\pi_n} & & \downarrow{\scriptstyle\pi_0} \\ E[p^\infty] & \xrightarrow{\gamma} & G \end{array}$$

where π_n is the projection onto the $(n+1)$st coordinate. Reasoning similarly for $\tilde{\varphi}^{-1}$ we get an m such that $\pi_0 \circ \tilde{\varphi}^{-1}$ factors through π_m. Choosing $N \geq \max(n, m)$ we get the following commutative diagram

$$\begin{array}{ccccc} \widetilde{E[p^\infty]} & \xrightarrow{\tilde{\varphi}} & \widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p & \xrightarrow{\tilde{\varphi}^{-1}} & \widetilde{E[p^\infty]} \\ \downarrow{\scriptstyle\pi_{2N}} & & \downarrow{\scriptstyle\pi_N} & & \downarrow{\scriptstyle\pi_0} \\ E[p^\infty] & \xrightarrow{g} & \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{h} & E[p^\infty] \end{array}$$

Note also that $\pi_N = \pi_0 \circ p^N$ implies the commutativity of

$$\begin{array}{ccc} \widetilde{E[p^\infty]} & \xrightarrow{\tilde{\varphi}} & \widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p \\ \downarrow{\scriptstyle \pi_N} & & \downarrow{\scriptstyle \pi_0} \\ E[p^\infty] & \xrightarrow{g} & \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

Thus $h \circ g = p^{2N}\mathrm{id}_{E[p^\infty]}$ and $g \circ h = p^{2N}\mathrm{id}_G$. In particular g and h are isogenies. Let H be the kernel of g. Then H is a finite, locally free group scheme over S which is a subgroup of $E[p^{2N}]$. Let $E' = E/H$. The natural projection induces an isomorphism $E'[p^\infty] \xrightarrow{\varphi'} \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$. Denoting the projection $E \to E'$ by q it's easy to see that $f = p^{-N}q$ is the quasi-p-isogeny we are looking for. This proves the theorem. □

Definition 4.1.8. Given $x \in F(S)$ we will call $(E, \varphi, \alpha_N) \in M_{\text{big Igusa}}(S)$ a distinguished representative for x if it represents x under the natural isomorphism described above. Any two distinguished representatives are related by a unique isomorphism.

4.2 Group Actions

Let's revisit some of the Galois groups and their actions we have seen so far. Let us assume our base ring is R where p is nilpotent. We have seen that M_{Katz} is Galois over $\mathfrak{X}^{\text{ord}}$ with Galois group $\mathbb{Z}_p^\times$. For a R-algebra S, $g \in \mathbb{Z}_p^\times(S)$ acts as follows

$$\begin{aligned} M_{\text{Katz}}(S) &\to M_{\text{Katz}}(S) \\ (E, \hat{\varphi}, \alpha_N) &\mapsto (E, g\hat{\varphi}, \alpha_N) \end{aligned}$$

M_{Igusa} is Galois over $\mathfrak{X}^{\text{ord}}$ with Galois group $M_p^\circ := \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$. For a R-algebra S, $g = (\hat{g}, g^{\text{ét}}) \in \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times(S)$ the action is given as follows

$$\begin{aligned} M_{\text{Igusa}}(S) &\to M_{\text{Igusa}}(S) \\ (E, \hat{\varphi}, \varphi^{\text{ét}}, \alpha_N) &\mapsto (E, \hat{g}\hat{\varphi}, \varphi^{\text{ét}} {g^{\text{ét}}}^{-1}, \alpha_N) \end{aligned}$$

4.2.1 Projection From $M_{\mathbf{Igusa}}$ to $M_{\mathbf{Katz}}$

The natural projection M_{Igusa} to M_{Katz} by forgetting $\varphi^{\text{ét}}$ is equivariant w.r.t. the action of $\mathbb{Z}_p^\times$. We remarked in Section 3.1.1 that the problem of classifying tuples $(E, \hat{\varphi}, \alpha_N)$ is equivalent to the problem of classifying tuples $(E, \varphi^{\text{ét}}, \alpha_N)$ by duality and used this later to prove the representability of M_{Igusa}. Let's try to understand this duality more carefully.

Weil Pairing : Given a pair of dual isogenies $E \xrightarrow{\pi} E'$ and $E' \xrightarrow{\check{\pi}} E$ of degree n there is a canonical perfect alternating bilinear pairing called the Weil pairing.

$$e_\pi : \ker \pi \times \ker \check{\pi} \to \mu_n \subset \mathbb{G}_m$$

Thus we have a Weil pairing $\hat{E}[p^n] \times E[p^n]^{\text{ét}} \to \mu_{p^n}$ which identifies one as a Cartier dual of the other. Under this duality, given an isomorphism $\hat{\varphi} : \hat{E}[p^n] \to \mu_{p^n}$ we obtain a dual isomorphism $\varphi^{\text{ét}} : \mathbb{Z}/p^n\mathbb{Z} \to E[p^n]^{\text{ét}}$ which sends "1" to the unique element x such that

$$\langle \hat{\varphi}^{-1}(.), x \rangle : \mu_{p^n} \to \mu_{p^n}$$

is the identity. Thus we have a natural isomorphism

$$\begin{aligned} M_{\text{Katz}}(S) &\xrightarrow{T_S} \check{M}_{\text{Katz}}(S) \\ (E, \hat{\varphi}, \alpha_N) &\mapsto (E, \varphi^{\text{ét}}, \alpha_N) \end{aligned}$$

where $\varphi^{\text{ét}}$ is defined as above, for any R-algebra S. We will sometimes loosely write $T(\hat{\varphi}) = \varphi^{\text{ét}}$. This natural isomorphism has the property that for any $g \in \mathbb{Z}_p^\times(S)$

$$T_S(E, g\hat{\varphi}, \alpha_N) = (E, \varphi^{\text{ét}} g, \alpha_N)$$

In Section 3.3.1, we said that $M_{\text{Ig},N,n} = M_{\text{Katz},N,n} \times_{Y(N)^{\text{ord}}} M_{\text{Katz},N,n}$ where we identified the second component with $\check{M}_{\text{Katz},N,n}$ using this natural isomorphism.

There is a natural section of the projection $M_{\text{Igusa}} \to M_{\text{Katz}}$ which is given by the diagonal embedding $M_{\text{Katz}} \xrightarrow{\Delta} M_{\text{Igusa}}$. On points this is given as

$$(E, \hat{\varphi}, \alpha_N) \xrightarrow{\Delta} (E, \hat{\varphi}, T(\hat{\varphi}), \alpha_N)$$

Let us understand how this section commutes with $\mathbb{Z}_p^\times$ action.

$$(E, g\hat{\varphi}, \alpha_N) \xrightarrow{\Delta} (E, g\hat{\varphi}, T(g\hat{\varphi}), \alpha_N) = (E, g\hat{\varphi}, T(\hat{\varphi})g, \alpha_N)$$

This suggests that if we consider the embedding of $\mathbb{Z}_p^\times$ in M_p° as $a \mapsto (a, a^{-1})$, the canonical section commutes with the $\mathbb{Z}_p^\times$ action.

4.2.2 Projection from $M_{\text{big Igusa}}$ to M_{Igusa}

We have discussed this in detail in Section 3.3.2. Let's just recall the results from that section.

Let $B_p^\circ := \underline{\mathrm{Aut}}(\mu_{p^\infty} \times \mathbb{Q}_p)$. As matrices

$$B_p^\circ = \begin{pmatrix} \underline{\mathrm{Aut}}(\mu_{p^\infty}) & \underline{\mathrm{Hom}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) \\ 0 & \underline{\mathrm{Aut}}(\mathbb{Q}_p/\mathbb{Z}_p) \end{pmatrix} = \begin{pmatrix} {\mathbb{Z}_p}^\times & T_p\mu_{p^\infty} \\ 0 & {\mathbb{Z}_p}^\times \end{pmatrix}$$

Let $N_p^\circ := \underline{\mathrm{Hom}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) = T_p\mu_{p^\infty}$ There are natural inclusions of $M_p^\circ \hookrightarrow B_p^\circ$ and $N_p^\circ \hookrightarrow B_p^\circ$ which realizes B_p° as a semi-direct product $B_p^\circ = N_p^\circ \rtimes M_p^\circ$.

The projection $M_{\text{big Igusa}} \to M_{\text{Igusa}}$ is equivariant for the M_p° action and realizes $M_{\text{big Igusa}}$ as an fpqc N_p° torsor over M_{Igusa}.

Note that so far the actions described for all the groups above give $\mathfrak{X}^{\text{ord}}$-morphisms. We will now describe a group and its action on $M_{\text{big Igusa}}$ in the light of Section 4.1.1 that will not be a $\mathfrak{X}^{\text{ord}}$-morphism.

Let

$$\begin{aligned} B_p &:= \underline{\mathrm{Aut}}(\widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p) \\ M_p &:= \underline{\mathrm{Aut}}(\widetilde{\mu_{p^\infty}}) \times \underline{\mathrm{Aut}}(\mathbb{Q}_p) = \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \\ N_p &:= \underline{\mathrm{Hom}}(\mathbb{Q}_p, \widetilde{\mu_{p^\infty}}) = \widetilde{\mu_{p^\infty}} \end{aligned}$$

We saw in Section 4.1.1 that $M_{\text{big Igusa}}$ can be interpreted as classifying quasi-p-isogeny

classes of tuples $(E, \tilde{\varphi}, \alpha_N)$. This gives a B_p action on $M_{\text{big Igusa}}$ described on points as

$$M_{\text{big Igusa}}(S) \to M_{\text{big Igusa}}(S)$$
$$(E, \tilde{\varphi}, \alpha_N) \mapsto (E, g\tilde{\varphi}, \alpha_N)$$

for $g \in B_p(S)$ for any R-algebra S.

4.3 The $\widehat{\mathbb{G}_m}$ Action

4.3.1 Extending the Action on M_{Igusa}

We have seen M_{Igusa} admits a natural action of M_p° and $M_{\text{Igusa}} = N_p^\circ \backslash M_{\text{big Igusa}}$.

Let $B_p' = N_p \rtimes M_p^\circ \subset B_p$. As matrices

$$B_p' = \begin{pmatrix} \mathbb{Z}_p^\times & \widetilde{\mu_{p^\infty}} \\ 0 & \mathbb{Z}_p^\times \end{pmatrix}$$

Then N_p° is a normal subgroup in B_p'. The conjugation action is given as

$$\begin{pmatrix} a_1 & y \\ 0 & a_2 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_1 & y \\ 0 & a_2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & x^{a_1 a_2^{-1}} \\ 0 & 1 \end{pmatrix}$$

Using Lemma 4.1.2, we see that there is a fpqc quotient

$$B_p'/N_p^\circ = \overline{B_p} := \widehat{\mathbb{G}_m} \rtimes M_p^\circ$$

coming from

$$1 \to T_p\mu_{p^\circ} \to \widetilde{\mu_{p^\infty}} \to \widehat{\mathbb{G}_m} \to 1$$

Using the action of B_p on $M_{\text{big Igusa}}$, we see that the action of B_p' descends to an action of $\overline{B_p}$ on M_{Igusa} and the equivariance of the projection w.r.t. the M_p° action shows that the $\overline{B_p}$ action extends the M_p° action on M_{Igusa}. The new part of the action is that of $\widehat{\mathbb{G}_m} = N_p/N_p^\circ$.

4.3.2 Extending the Action on $M_{\mathbf{Katz}}$

We have a canonical embedding of M_{Katz} inside M_{Igusa} as described in Section 4.2.1. We want to show that the closed subscheme of M_{Igusa} defined by the diagonal embedding is invariant under the extended action of $\widehat{\mathbb{G}_m}$. Then this will give us an extension of the $\mathbb{Z}_p^\times$ action on M_{Katz}. But before proving that we need some more preparation.

For an elliptic curve E/R recall that since $p^n : E \to E$ is self dual the p^n-Weil pairing is a perfect, bilinear, antisymmetric pairing

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

Lemma 4.3.1. *Given $E \xrightarrow{\pi_1} E' \xrightarrow{\pi_2} E$. Then for any $P \in \ker \pi_1(S)$ for an R-algebra S and $Q \in \ker(\pi_2 \circ \pi_1)(S)$*

$$e_{\pi_2 \circ \pi_1}\langle P, Q\rangle = e_{\pi_1}\langle P, \check{\pi}_2(Q)\rangle$$

Proof. [See KM85, (2.8.4.1)]. □

Suppose we have a splitting $\varphi : E[p^n] \xrightarrow{\sim} \mu_{p^n} \times 1/p^n\mathbb{Z}/\mathbb{Z}$. Let $\pi : E \to E/\hat{E}[p^n]$. Then $\check{\pi} \circ \pi = p^n$. Applying the above lemma to this situation, we see that

$$\varphi^{\text{ét}} = \pi \circ \varphi^{-1} : 1/p^n\mathbb{Z}/\mathbb{Z} \xrightarrow{\sim} E[p^n]^{\text{ét}}$$

is $T(\hat{\varphi})$ iff

$$e_{p^n}\langle \varphi^{-1}(.), \varphi^{-1}(1/p^n)\rangle : \mu_{p^n} \to \mu_{p^n} \tag{4.1}$$

is the identity.

Remark 4.3.1.

$$e_{p^n}\langle \varphi^{-1}(.), \varphi^{-1}(.)\rangle : \mu_{p^n} \times \mu_{p^n} \to \mu_{p^n}$$

is trivial by Lemma 4.3.1.

The p^n-Weil pairings for varying n induce an antisymmetric $\mathbb{Q}_p$-bilinear pairing

$$\begin{aligned} \tilde{e} : \widetilde{E[p^\infty]} \times \widetilde{E[p^\infty]} &\to \widetilde{\mu_{p^\infty}} \\ ((a_i), (b_j)) &\mapsto (c_k) \end{aligned}$$

where

$$c_k = \langle a_i, b_j \rangle_{p^t}^{p^s}$$

for $i + j = k + t + s$ and t large enough for the right-hand side to make sense. It can be checked easily that $\tilde{e}$ is well-defined.

A point $x \in M_{\text{Igusa}}(S)$ lies in $\Delta(M_{\text{Katz}})(S)$ iff equation (4.1) holds.

Lemma 4.3.2. *Equation (4.1) holds iff*

$$\tilde{e}\langle \tilde{\varphi}^{-1}(a), \tilde{\varphi}^{-1}(b) \rangle = a^b$$

for any $a \in \widetilde{\mu_{p^\infty}}(S)$ and $b \in \mathbb{Q}_p(S)$ for any R-algebra S.

Proof. Obvious. □

Now we can prove that the extended group action stabilizes the canonical section. Indeed, suppose $(E, \varphi, \alpha_N) \in M_{\text{big Igusa}}(S)$ be a distinguished representative for a point x. Let $g \in B_p(S)$. Suppose $(E', \varphi', \alpha'_N)$ be a distinguished representative for the point gx.

Proposition 4.3.1. *Suppose $(\det g)p^{-v_p(\det g)} = 1$. Then equation (4.1) holds for φ iff it holds for φ'.*

Proof. Write $\det_p g = (\det g)p^{-v_p(\det g)}$.

By definition of a distinguished representative, there exists a unique quasi-p-isogeny $f : E \to E'$ such that

$$\begin{array}{ccc} \widetilde{E[p^\infty]} & \xrightarrow{\tilde{\varphi}} & \widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p \\ \downarrow{\scriptstyle \tilde{f}} & & \downarrow{\scriptstyle g} \\ \widetilde{E'[p^\infty]} & \xrightarrow{\tilde{\varphi'}} & \widetilde{\mu_{p^\infty}} \times \mathbb{Q}_p \end{array}$$

From this diagram we see that $\deg f = p^{v_p(\det g)}$. It is enough to show that equation (4.1) holds for φ implies that it holds for φ'. So assume (2) for φ. Suppose

$$g = \begin{pmatrix} a & z \\ 0 & a' \end{pmatrix} \in \begin{pmatrix} \mathbb{Q}_p^\times & \widetilde{\mu_{p^\infty}} \\ 0 & \mathbb{Q}_p^\times \end{pmatrix}$$

Then

$$g^{-1} = \begin{pmatrix} a^{-1} & z^{-(aa')^{-1}} \\ 0 & a'^{-1} \end{pmatrix}$$

For $x \in \widetilde{\mu_{p^\infty}}(S)$ and $y \in \mathbb{Q}_p(S)$,

$$\begin{aligned} \tilde{e}\langle \tilde{\varphi}'^{-1}(x), \tilde{\varphi}'^{-1}(y)\rangle &= \langle f\tilde{\varphi}^{-1}(g^{-1}x), f\tilde{\varphi}^{-1}(g^{-1}y)\rangle \\ &= \langle \tilde{\varphi}^{-1}(x^{a^{-1}}), \tilde{\varphi}^{-1}(z^{-(aa')^{-1}y}, a'^{-1}y)\rangle^{\deg f} \\ &= \langle \tilde{\varphi}^{-1}(x), \tilde{\varphi}^{-1}(y)\rangle^{\det_p g^{-1}} \end{aligned}$$

where we use bilinearity and Remark 4.3.1 in the last step. This proves the proposition. □

Corollary 4.3.1. Let $\mathbb{Z}_p^\times \hookrightarrow M_p^\circ$ by $a \mapsto \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$. Then the action of $\widehat{\mathbb{G}_m} \rtimes \mathbb{Z}_p^\times \subset \widehat{\mathbb{G}_m} \rtimes M_p^\circ$ stabilizes the canonical section.

Proof. Given $(E, \hat{\varphi}, \varphi^{\text{ét}}, \alpha_N) \in \Delta(M_{\text{Katz}})(S)$ choose a fpqc cover of S where the extension

$$\mu_{p^\infty} \xrightarrow{\hat{\varphi}^{-1}} E[p^\infty] \xrightarrow{\varphi^{\text{ét}}} \mathbb{Q}_p/\mathbb{Z}_p$$

splits and the given element of $\widehat{\mathbb{G}_m}$ lifts to an element of $\widetilde{\mu_{p^\infty}}$. Then apply Proposition 4.3.1. □

Thus we have extended the action of $\mathbb{Z}_p^\times$ to an action of $\widehat{\mathbb{G}_m} \rtimes \mathbb{Z}_p^\times$ on M_{Katz}.

4.4 Kummer p-divisible Groups

For any ring R and $q \in R^\times$ we will construct an extension of p-divisible groups over $\operatorname{Spec} R$,

$$\mathbb{E}_q : \mu_{p^\infty} \to G_q \to \mathbb{Q}_p/\mathbb{Z}_p$$

We will call the G_q arising from such extensions Kummer p-divisible groups. Our construction will be modeled on the p-divisible group of the Tate curve.

Consider the fppf sheaf in groups

$$\mathrm{Roots}_q \subset \mathbb{G}_m \times \mathbb{Z}[1/p]$$

consisting of pairs (x, m) such that for k sufficiently large, $x^{p^k} = q^{p^k m}$.

Projection to the second component gives a natural map $\mathrm{Roots}_q \to \mathbb{Z}[1/p]$ whose kernel is μ_{p^∞}. The projection admits a canonical section over $\mathbb{Z}$ given by $1 \mapsto (q, 1)$. Let

$$G_q := \mathrm{Roots}_q/\mathbb{Z}$$

be the quotient by the image of this section.

Lemma 4.4.1. *G_q is a p-divisible group, and the maps*

$$\mu_{p^\infty} \to \mathit{Roots}_q \text{ and } \mathit{Roots}_q \to \mathbb{Z}[1/p]$$

induce the structure of an extension

$$\mathbb{E}_q : \mu_{p^\infty} \to G_q \to \mathbb{Q}_p/\mathbb{Z}_p$$

Proof. Let Roots'_q be the subsheaf of sets of Roots_q of elements (x, m) with $m \in \mathbb{Z}[1/p]$ for $0 \leq m < 1$. The group law induces an isomorphism

$$\mathrm{Roots}'_q \times \mathbb{Z} \to \mathrm{Roots}_q$$

Thus Roots'_q as a sheaf of sets is isomorphic to $\mathrm{Roots}_q/\mathbb{Z}$. For any R-algebra A with $\operatorname{Spec} A$ connected

$$G_q(A) = \mathrm{Roots}_q/(q, 1)^{\mathbb{Z}}$$

Any element of $G_q(A)$ has a unique representative of the form $(x, m) \in \mathrm{Roots}_q(A)$ with $0 \leq m < 1$. Such an element is p^k-torsion iff $m \in 1/p^k\mathbb{Z}$ and $x^{p^k} = q^{p^k m}$. In particular $G_q = \varinjlim_k G_q[p^k]$. Moreover multiplication by p is an epimorphism in the fppf topology. Thus to see that G_q is a p-divisible group we nee to show $G_q[p^k]$ is

finite, locally free over R. But this is obvious as $G_q[p^k]$ is represented by

$$\prod_{a=0}^{p^k-1} R[x]/(x^{p^k} - q^a)$$

with multiplication given by carrying, i.e. for x_1 a root of q^{a_1} and x_2 a root of q^{a_2}, in the group structure

$$x_1 \cdot x_2 = \begin{cases} x_1 x_2 & \text{as a root of } q^{a_1+a_2} \text{ if } a_1 + a_2 < p^k \\ x_1 x_2 / q & \text{as a root of } q^{a_1+a_2-p^k} \text{ if } a_1 + a_2 \geq p^k \end{cases}$$

This is clearly a finite, flat group scheme. □

Example 4.4.1. As noted in the beginning, for the Tate curve over $\mathbb{Z}((q))$, $\mathrm{Tate}(q)[p^\infty] = G_q$.

4.5 Serre-Tate Lifting

For R a ring in which p is nilpotent, and $R_0 = R/I$ for I a nilpotent ideal, let

$$\mathrm{Def}(R, R_0)$$

be the category of triples

$$(E_0, G, \epsilon)$$

where E_0/R_0 is an elliptic curve, G is a p-divisible group, and $\epsilon : G|_{R_0} \xrightarrow{\sim} E_0[p^\infty]$ is an isomorphism.

For the category $\mathbf{Ell}/R$ of elliptic curves over R, there is a natural functor

$$\begin{aligned} \mathbf{Ell}/R &\to \mathrm{Def}(R, R_0) \\ E &\mapsto (E_{R_0}, E[p^\infty], \epsilon_E) \end{aligned} \tag{4.2}$$

where $\epsilon_E : E[p^\infty]_{R_0} \xrightarrow{\sim} E_{R_0}[p^\infty]$ is the canonical isomorphism.

Theorem 4.5.1. (Serre-Tate) *The functor (3) is an equivalence of categories.*

Proof. [See Kat81, Theorem 1.2.1]. □

Here we list two immediate corollaries of Theorem 4.5.1 whose proofs are obvious.

Corollary 4.5.1. For $R \in \mathrm{Nilp}_{\mathbb{Z}_p}$, and π nilpotent in R, the natural reduction map

$$M_{\text{big Igusa}}(R) \to M_{\text{big Igusa}}(R/\pi)$$

is a bijection.

Let A be a p-adically complete ring and let $\pi \in A$ be a topologically nilpotent element for its p-adic topology. Consider the moduli problem $M_{\text{Igusa-}\pi}$ which classifies for $\operatorname{Spec} R \in \mathrm{Nilp}_A^{\mathrm{op}}$, the isomorphism classes of quadruples

$$(E_0, \mathbb{E}, \psi, \alpha_N)$$

where E_0 is an elliptic curve over R/π, α_N is a level N structure on E_0, $\mathbb{E}$ is an extension of p-divisible groups over R

$$\mathbb{E} : \mu_{p^\infty} \to G_{\mathbb{E}} \to \mathbb{Q}_p/\mathbb{Z}_p$$

and $\psi : E_0[p^\infty] \xrightarrow{\sim} G_{\mathbb{E}}|_{R/\pi}$.

There is a natural map $M_{\text{Igusa},A} \to M_{\text{Igusa-}\pi}$ given by sending

$$(E/R, \hat{\varphi}, \varphi^{\text{ét}}, \alpha_N) \mapsto (E_{(R/\pi)}, \mathbb{E}_{E[p^\infty],\hat{\varphi},\varphi^{\text{ét}}}, \psi_{\text{can}}, \alpha|_{R/\pi})$$

where $\mathbb{E}_{E[p^\infty],\hat{\varphi},\varphi^{\text{ét}}}$ is the extension defined by $\hat{\varphi}$ and $\varphi^{\text{ét}}$ and $\psi_{\text{can}} : E_{R/\pi}[p^\infty] \simeq E[p^\infty]_{R/\pi}$ is the canonical isomorphism.

Corollary 4.5.2. The map $M_{\text{Igusa},A} \to M_{\text{Igusa-}\pi}$ described above is an isomorphism.

4.6 Computing the $\widehat{\mathbb{G}_m}$ Action

4.6.1 Action of the Unipotent Subgroup on the Distinguished Representatives

In order to describe the $\widehat{\mathbb{G}_m}$ action on M_{Katz} it will be useful to understand the action of the unipotent subgroup $N_p = \widehat{\mu_{p^\infty}}$ (Section 4.2.2) on the distinguished representatives of $M_{\text{big Igusa}}$.

Suppose $R \in \text{Nilp}_{\mathbb{Z}_p}$, $n = (\zeta_k) \in N_p(R)$ and let I be a nilpotent ideal of R containing $\zeta_0 - 1$. Then

$$n \bmod I = (1, \zeta_1 \bmod I, \dots)$$

is an element of $N_p^\circ(R/I) = T_p\mu_{p^\infty}(R/I)$. Now if $x = (E, \tilde{\varphi}, \alpha_N) \in M_{\text{big Igusa}}(R)$ is a distinguished representative for x such that $\tilde{\varphi}$ comes from an isomorphism

$$\varphi : E[p^\infty] \xrightarrow{\sim} \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$$

then

$$n \cdot x = (E', \tilde{\varphi'}, \alpha'_N)$$

where E' is the Serre-Tate lift from R/I to R of $E_{R/I}$ determined by the isomorphism

$$(n \bmod I) \circ \varphi_{R/I} : E_{R/I}[p^\infty] \xrightarrow{\sim} (\mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p)_{R/I},$$

φ' is the natural isomorphism $E'[p^\infty] \xrightarrow{\sim} (\mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p)$ and α'_N is the unique lift of $\alpha_N|_{R/I}$.

Theorem 4.6.1. *Let R be a p-adically complete ring. Suppose $\zeta \in \widehat{\mathbb{G}_m}(R)$ and $\pi \in R$ is such that $\zeta \equiv 1$ mod π, and $(E_0, \mathbb{E}_q, \psi, \alpha_N) \in M_{Igusa\text{-}\pi}(R)$ where $\mathbb{E}_q$ is the Kummer extension of Section 4.4 and $q \in \mathbb{G}_m(R)$. Then*

$$\zeta \cdot (E_0, \mathbb{E}_q, \psi, \alpha_N) = (E_0, \mathbb{E}_{\zeta^{-1}q}, \psi', \alpha_N)$$

where ψ' is the composition of ψ with the canonical identification

$$\mathbb{E}_q|_{R/\pi} = \mathbb{E}_{\zeta^{-1}q}|_{R/\pi}$$

coming from $q \equiv \zeta^{-1}q \ mod\ \pi$.

Proof. If we write x_1 for the point $(E_0, \mathbb{E}_q, \psi, \alpha_N)$ and x_2 for the point $\zeta \cdot x_1$, it suffices to show that over the cover $R[q^{1/p^\infty}, \zeta^{1/p^\infty}]$, these points lift to points $\tilde{x}_1$ and $\tilde{x}_2$ in $M_{\text{big Igusa}}$, and there is a lift $\tilde{\zeta}$ of ζ in $N_p = \widetilde{\mu_{p^\infty}}$ such that $\tilde{\zeta}\tilde{x}_1 = \tilde{x}_2$. The desired lifts are given by the splittings

$$1/p^n \mapsto (q^{1/p^n}, 1/p^n) \text{ and } 1/p^n \mapsto (\zeta^{-1/p^n} q^{1/p^n}, 1/p^n)$$

of $\mathbb{E}_q$ and $\mathbb{E}_{\zeta^{-1}q}$ respectively, and $\tilde{\zeta} = (\zeta^{1/p^n})_n$. That $\tilde{\zeta} \cdot \tilde{x}_1 = \tilde{x}_2$ follows from the commutativity of the following diagram mod π

$$\begin{array}{ccc} G_q & \xrightarrow{=} & G_{\zeta^{-1}q} \\ {\scriptstyle 1/p^n \mapsto (q^{1/p^n}, 1/p^n)}\uparrow & & \uparrow{\scriptstyle 1/p^n \mapsto (\zeta^{-1/p^n} q^{1/p^n}, 1/p^n)} \\ \widehat{\mathbb{G}_m} \times \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow[\left(\begin{smallmatrix} 1 & \tilde{\zeta} \\ 0 & 1 \end{smallmatrix}\right)]{} & \widehat{\mathbb{G}_m} \times \mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

□

4.6.2 Action on the Tate Curve and q-Expansions

Definition 4.6.1. A cusp for $M_{\text{Katz},R}$ for a p-adically complete ring R is a $R((q))$ valued point of $M_{\text{Katz},R}$ which corresponds to the Tate curve $\text{Tate}(q^N)$ with the canonical trivialization of its formal group and any level N structure.

Let $R = \mathbb{Z}_p[\zeta_N]((q))$ and consider the Tate curve $\text{Tate}(q^N)$ over R. We have the canonical trivialization

$$\varphi_{\text{can}} : \widehat{\text{Tate}(q^N)} \xrightarrow{\sim} \widehat{\mathbb{G}_m}$$

We have a basis (ζ_N, q) for the N-torsion. The Tate curve $(\text{Tate}(q^N), \varphi_{\text{can}}, \alpha_N)$ corresponds to one of the cusps c (say).

Corollary 4.6.1. Suppose $g \in M(\Gamma_1(N), A, k)$, with A p-adically complete. For the cusp c of M_{Katz}, suppose the q-expansion of g is given by

$$\sum_{\substack{k \geq M \\ M \in \mathbb{Z}}} a_k q^k \in A \hat{\otimes} R$$

Then for any $\zeta \in \widehat{\mathbb{G}_m}(R)$

$$\zeta \cdot g := (\zeta^{-1})^* \cdot g$$

has q-expansion at c

$$\sum_{k \geq M} a_k (\zeta^{1/N} q)^k = \sum_{k \geq M} \zeta^{k/N} a_k q^k$$

Proof. It follows from Theorem 4.6.1 that

$$\zeta^{-1} \cdot \Big(\mathrm{Tate}(q^N), \hat{\varphi}_{\mathrm{can}}, (\zeta_N, q) \Big) = \Big(\mathrm{Tate}(\zeta q^N), \hat{\varphi}_{\mathrm{can}}, (\zeta_N, \zeta^{1/N} q) \Big)$$

This is the base change of $\mathrm{Tate}(q^N)$ through $q \mapsto \zeta^{1/N} q$. Hence the corollary follows. □

To differentiate the action of $\widehat{\mathbb{G}_m}$ is to compose the action with the canonical tangent vector to $\widehat{\mathbb{G}_m}$ at the identity. This corresponds to the $R[\epsilon]$ valued point given by

$$R[[x]] \to R[\epsilon]$$
$$x \mapsto \epsilon$$

where $\epsilon^2 = 0$ and $1 + x$ is the multiplicative coordinate on $\widehat{\mathbb{G}_m}$. Applying this to Corollary 4.6.1, we get

Corollary 4.6.2. For $\zeta = 1 + \epsilon \in \widehat{\mathbb{G}_m}(R[\epsilon])$, the effect on q-expansions induced by pullback through the action on $M_{\mathrm{Katz}\, R[\epsilon]}$, $(\zeta)^* \cdot g = \zeta^{-1} \cdot g$ is

$$\sum a_k q^k \mapsto \sum (1 - \epsilon)^{k/N} a_k q^k = \Big(\mathrm{id} - \epsilon \frac{1}{N} q \frac{\mathrm{d}}{\mathrm{d}q} \Big) \sum a_k q^k$$

Thus, differentiating the $\widehat{\mathbb{G}_m}$ action on M_{Katz} we get back $-\theta$.

Appendix A

Cohomology and Base Change

In this appendix we recall some results about cohomology and base change for proper, smooth morphisms. We follow a handout by [Con].

Theorem A.0.1. (Grothendieck) *Let $f : X \to S$ be a proper morphism of schemes with S locally Noetherian, and let $\mathfrak{F}$ be a S-flat coherent sheaf on X. Let s be a point in S. Assume for all $i \geq 0$, the natural base change morphism $\varphi_s^i : R^i f_*(\mathfrak{F}) \otimes_{\mathcal{O}_{S,s}} k(s) \to H^i(X_s, \mathfrak{F}_s)$ is surjective. Then $\varphi_{s'}^i$ is an isomorphism for all s' in a suitable neighbourhood of s. Moreover, the following are equivalent:*

1. *φ_s^{i-1} is surjective*
2. *$R^i f_*(\mathfrak{F})_s$ is finite free.*

Proof. The theorem is proved in [Har13, III, Theorem 12.11] for the case when X/S is projective. The more general result for proper morphisms is proved in [Gro61, Proposition 4.6.1]. □

Corollary A.0.1. If $H^i(X_s, \mathfrak{F}_s) = 0$ for some $s \in S$, then

1. $\varphi_{s'}^i$ is an isomorphism for all s' near s
2. $R^i f_*(\mathfrak{F})$ vanishes near s
3. $\varphi_{s'}^{i-1}$ is an isomorphism for all s' near s.

In the case $i = 1$, $f_*\mathfrak{F}$ is locally free near s and $\varphi^0_{s'} : f_*\mathfrak{F}_{s'} \otimes_{\mathcal{O}_{S,s'}} k(s') \to H^0(X_{s'}, \mathfrak{F}_{s'})$ is an isomorphism for all s' near s.

Proof. (1) follows from Theorem A.0.1. (2) follows from (1) using Nakayama's lemma. (3) follows from (2) using Theorem A.0.1. □

Corollary A.0.2. Let $f : X \to S$ be a proper, surjective, flat map whose geometric fibres are reduced and connected. Then the natural map $\mathcal{O}_S \to f_*\mathcal{O}_X$ is an isomorphism.

Proof. For any $s \in S$ the $k(s)$-algebra of global sections of X_s is non-zero and finite-dimensional since X_s is proper and non-empty. Its formation commutes with any extension on $k(s)$. After passing to the geometric fibre, we get a reduced, proper, connected scheme over an algebraically closed field whose global sections thus will be equal to $\overline{k(s)}$. Thus $H^0(X_s, \mathcal{O}_{X_s})$ is one-dimensional and hence the natural map $k(s) \to H^0(X_s, \mathcal{O}_{X_s})$ is an isomorphism.

Since X is flat over S, we can apply Theorem A.0.1 to $\mathcal{O}_X$. The natural map

$$\varphi^0_s : f_*(\mathcal{O}_X) \otimes_{\mathcal{O}_{S,s}} k(s) \to H^0(X_s, \mathcal{O}_{X_s}) \simeq k(s)$$

is surjective as $1 \mapsto 1$. Thus it is an isomorphism. Since φ_s^{-1} is trivially surjective, $f_*\mathcal{O}_X$ is free near s, necessarily of rank 1 as it is so over the fibre. Thus $f_*\mathcal{O}_X$ is a line bundle. The structure morphism $\mathcal{O}_S \to f_*\mathcal{O}_X$ is an isomorphism as it is so modulo the maximal ideal of $\mathcal{O}_{S,s}$. □

Remark A.0.1. A special case of Corollary A.0.1 is $i = d + 1$ when f is a morphism whose fibres have dimension $\leq d$. In that case $H^{d+1}(X_s, \mathfrak{F}_s)$ vanishes for all $s \in S$ by Grothendieck vanishing. This implies that φ^d_s is a surjection (hence an isomorphism) for all $s \in S$ by the corollary.

Now consider the general setup of Theorem A.0.1. We will use the fibral base change morphisms φ^i_s to study more general base change morphisms.

Proposition A.0.1. *Assume φ^i_s is an isomorphism for all $s \in S$, and that φ^{i-1}_s is also an isomorphism for all $s \in S$ (or equivalently, that $R^i f_*(\mathfrak{F})$ is locally free on S).*

Consider a locally Noetherian S-scheme S', the resulting Cartesian diagram

$$\begin{array}{ccc} X' & \xrightarrow{q} & X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ S' & \xrightarrow{p} & S \end{array}$$

and the S'-flat coherent coherent sheaf $\mathfrak{F}' = q^*\mathfrak{F}$ on X'. The natural base change morphism $p^*(R^i f_*\mathfrak{F}) \to R^i f'_*(\mathfrak{F}')$ is an isomorphism.

Proof. We recall that the formation of coherent cohomology commutes with flat base change (because flat base change of a Čech complex is a Čech complex). Hence in particular for any $s' \in S'$ lying over $s \in S$, the natural base change map

$$k(s') \otimes_{k(s)} H^i(X_s, \mathfrak{F}_s) \to H^i(X'_{s'}, \mathfrak{F}'_{s'}) \tag{A.1}$$

is an isomorphism.

The natural pullback map $R^i f_*(\mathfrak{F}_s) \otimes_{\mathcal{O}_{S,s}} \mathcal{O}_{S',s'} \to R^i f'_*(\mathfrak{F}')_{s'}$ induces the commutative diagram

$$\begin{array}{ccc} R^i f_*(\mathfrak{F}_s) \otimes_{\mathcal{O}_{S,s}} k(s') & \longrightarrow & R^i f'_*(\mathfrak{F}')_{s'} \otimes_{\mathcal{O}_{S',s'}} k(s') \\ {\scriptstyle \varphi^i_s}\downarrow & & \downarrow{\scriptstyle \varphi^i_{s'}} \\ H^i(X_s, \mathfrak{F}_s) \otimes_{k(s)} k(s') & \simeq & H^i(X_{s'}, \mathfrak{F}'_{s'}) \end{array}$$

Hence the surjectivity of φ^i_s implies the surjectivity of $\varphi^i_{s'}$. Thus the hypothesis implies that both $\varphi^i_{s'}$ and $\varphi^{i-1}_{s'}$ are surjective for all $s' \in S'$. Thus $R^i f'_*(\mathfrak{F}')$ is finite locally free on S'. Thus to prove that the natural base change map is an isomorphism (at the stalk at $s' \in S'$) it is enough to prove it modulo the maximal ideal $\mathfrak{m}_{s'}$ of $\mathcal{O}_{S',s'}$ which is exactly the isomorphism of (A.1). □

Bibliography

[BS86] Zenon Ivanovich Borevich and Igor Rostislavovich Shafarevich. *Number theory*. Vol. 20. Academic press, 1986.

[Con] Brian Conrad. *Applications of base change for coherent cohomology*. URL: http://virtualmath1.stanford.edu/~conrad/248BPage/handouts/cohom.pdf.

[Gro61] Alexander Grothendieck. "Éléments de géométrie algébrique: III. Étude cohomologique des faisceaux cohérents, première partie". In: *Publications Mathématiques de l'IHÉS* 11 (1961), pp. 5–167.

[Gro67] Alexander Grothendieck. "Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie". fr. In: *Publications Mathématiques de l'IHÉS* 32 (1967), pp. 5–361. URL: http://www.numdam.org/item/PMIHES_1967__32__5_0.

[Har13] Robin Hartshorne. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[How18] Sean Howe. *A unipotent circle action on p-adic modular forms*. 2018. URL: http://web.stanford.edu/~seanpkh/papers/unipotent-circle-action.pdf.

[Kat73] Nicholas M Katz. "p-adic properties of modular schemes and modular forms". In: *Modular functions of one variable III*. Springer, 1973, pp. 69–190.

[Kat75] Nicholas M Katz. "Higher congruences between modular forms". In: *Annals of Mathematics* (1975), pp. 332–367.

[Kat81] Nicholas M Katz. "Serre-Tate local moduli". In: *Surfaces algébriques*. Springer, 1981, pp. 138–202.

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

[Mes72] William Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Vol. 264. Lecture Notes in Mathematics. Springer, 1972.

[Ser12] Jean-Pierre Serre. *Local algebra*. Springer Science & Business Media, 2012.

[Ser73] Jean-Pierre Serre. "Formes modulaires et fonctions zêta p-adiques". In: *Modular functions of one variable III*. Springer, 1973, pp. 191–268.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer Science & Business Media, 2009.

[Stacks] The Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`. 2018.

[SW12] Peter Scholze and Jared Weinstein. "Moduli of p-divisible groups". In: *arXiv preprint arXiv:1211.6357* (2012).

[Swi73] Henry Peter Francis Swinnerton-Dyer. "On l-adic representations and congruences for coefficients of modular forms". In: *Modular functions of one variable III*. Springer, 1973, pp. 1–55.

[Tat67] John T Tate. "p-divisible groups". In: *Proceedings of a conference on Local Fields*. Springer. 1967, pp. 158–183.

[Wat12] William C Waterhouse. *Introduction to affine group schemes*. Vol. 66. Springer Science & Business Media, 2012.