DEFORMATIONS OF ELLIPTIC CURVES

MICHAŁ MRUGAŁA

§1. NOTATION AND MOTIVATION

Recall the Heegner setup (cf. notation sheet). Our goal is to compute the local height pairings

$$\langle c, T_m d^\sigma \rangle_v$$

for non-archimedean places v of H. We will henceforth fix a non-archimedean place v.

Suppose $a, b \in \mathrm{Div}^0(X)(H_v)$. Recall from Leonardo's talk that local heights may be computed by solving an intersection problem: If $\mathscr{X}_v$ is a proper, regular model for X_{H_v} over $\mathscr{O}_{H_v}$ and $\widetilde{a}, \widetilde{b}$ are lifts of a, b to $\mathscr{X}_v$ (one of which has zero intersection number with each irreducible component), then

$$\langle a, b \rangle_v = -\left(\widetilde{a} \cdot \widetilde{b}\right) \log q. \tag{1}$$

To carry out this computation we need to do two things:

(1) Find a proper, regular model for X_{H_v} over $\mathscr{O}_v$.
(2) Compute the intersection products $(\widetilde{c} \cdot \widetilde{T_m d^\sigma})$.

For these purposes:

- In Section 2 we describe the integral model of X.
- In Section 3 we discuss lifting Heegner diagrams to $\check{\mathscr{O}}_v$, the maximal unramified extension of $\mathscr{O}_v$.
- In Section 4 we give an informal statement of the Serre–Tate theorem and a formal statement of Grothendieck's existence theorem.
- In Section 5 we introduce p-divisible groups and give a formal statement of the Serre–Tate theorem.
- In Section 6 we introduce formal Lie groups to analyse the connected components of p-divisible groups attached to elliptic curves.
- In Section 7 we describe the deformation theory of ordinary elliptic curves. In particular, we define the Serre–Tate canonical lifts.
- In Section 8 we describe the deformation theory of supersingular elliptic curves. In particular, we define Gross' quasi-canonical lifts.

§2. INTEGRAL MODEL OF X

(2.1) Recall that $Y_0(N)$ is a moduli space parametrizing cyclic isogenies of degree N between elliptic curves. More specifically, for any $\mathbb{Q}$-scheme S

$$Y_0(N)(S) \simeq \left\{ \phi : E \longrightarrow E' \;\middle|\; \begin{array}{c} E, E' \text{ elliptic curves over } S \\ \phi \text{ a cyclic isogeny of degree } N \end{array} \right\} \Big/ \sim .$$

A cyclic isogeny is an isogeny $\phi : E \to E'$ such that

(i) $\ker \phi$ meets every irreducible component of every geometric fiber of E,
(ii) locally on S there is a point P such that

$$\ker \phi = \sum_{j=1}^{n} [jP]$$

as Cartier divisors on E.

(2.2) $X = X_0(N)$ is defined by relaxing the condition on E, E', we instead ask that they are *generalized elliptic curves*. We will not define them here; for our purposes it suffices to have their description over algebraically closed fields. In that case, there are two types of generalized elliptic curves:

(1) Elliptic curves.
(2) Néron polygons C_n: Let $n \in \mathbb{Z}_{\geqslant 1}$. Define the C_n to be the scheme obtained from $\mathbb{P}^1_S \times \mathbb{Z}/n\mathbb{Z}$ by gluing $(\{\infty\}, i)$ with $(\{0\}, i+1)$ for all $i \in \mathbb{Z}/n\mathbb{Z}$.

This moduli problem is not representable, we instead define the integral model of X to be the "best approximation" to a representing object, called the *coarse moduli scheme*. This scheme exists and parametrizes the objects we care about over algebraically closed fields. I will abuse notation and write X for this integral model.

(2.3) X is a proper, flat curve over $\mathbb{Z}$, smooth over $\mathbb{Z}[1/N]$. To say more about the regularity properties of X over $\mathbb{Z}$ we need the notion of automorphisms of geometric points of X. Let x be such a point of X corresponding to an isogeny $\phi : E \to E'$ over an algebraically closed field k. The automorphism group $\mathrm{Aut}_k(x)$ is the subgroup of $(f, f') \in \mathrm{Aut}_k(E) \times \mathrm{Aut}_k(E')$ such that

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ E & \xrightarrow{\phi} & E' \end{array}$$

commutes. Say x has non-trivial automorphisms if $\mathrm{Aut}_k(x) \neq \langle \pm 1 \rangle$. We also need to distinguish three types of field valued points of X:

(i) a point is **ordinary** if it corresponds to $\phi : E \to E'$ with E, E' ordinary,
(ii) a point is **supersingular** if it corresponds to $\phi : E \to E'$ with E, E' supersingular,
(iii) a point is a **cusp** if it corresponds to a diagram of Néron polygons.

X is regular except at supersingular points in characteristics $p \mid N$ that admit non-trivial automorphisms.

(2.4) When $p \mid N$ the mod p reduction $X_{\mathbb{F}_p}$ is singular and reducible over $\mathbb{Z}/p\mathbb{Z}$. Fortunately, we can still describe the irreducible components.

Let $N = p^n M$ with $(p, M) = 1$. All of the irreducible components are isomorphic to $X_0(M)_{\mathbb{F}_p}$. We can parametrize them with $a, b \in \mathbb{Z}_{\geqslant 0}$ such that $a + b = n$. For such a pair, the associated component $X^{a,b}_{\mathbb{F}_p}$ appears with multiplicty $\phi(p^c)$. All of the components intersect at each supersingular point of X. Every other point of $X^{a,b}_{\mathbb{F}_p}$ corresponds to a diagram with $\ker \phi$ locally isomorphic to $\mu_{p^a} \times \mathbb{Z}/p^b M\mathbb{Z}$.

We also have an explicit description of the subscheme C of cusps of X. It is finite over $\mathbb{Z}$ with irreducible components indexed by $d \in \mathbb{Z}_{\geqslant 1}$ dividing N. The component $C(d)$ parametrizes diagrams of Néron polygons with $\ker \phi \simeq \mu_d \times d\mathbb{Z}/N\mathbb{Z}$. It has $\phi((d, N/d))$ geometric points and is isomorphic to $\mathrm{Spec}\, \mathbb{Z}[\mu_f]$. The reduction of $C(d)$ mod p lies in $X^{a,b}_{\mathbb{F}_p}$ where a is $v_p(d)$.

§3. HEEGNER DIAGRAMS

Before we move on to deformation theory, we need to address an important point that will show up in Benjamin's talks. Let $\breve{H}_v$ be the maximal unramified extension of H_v and $\breve{\mathscr{O}}_v$ be its ring of integers. We will need to study points in $X(\breve{\mathscr{O}}_v)$ which arise from Heegner points.

(3.1) Let $x \in X(H)$ be a Heegner point. The action of $\mathrm{Gal}(H/\mathbb{Q})$ on x is free, so $x : \mathrm{Spec}(H) \to X_{\mathbb{Q}}$ is a closed immersion. For any closed point $v \in \mathrm{Spec}\, \mathscr{O}_H$ we can uniquely extend x to a point in $X(\mathscr{O}_{H,v})$ by the valuative criterion of properness. Base changing, we see that x defines a unique point $\breve{x} \in X(\breve{\mathscr{O}}_v)$. We say that $\breve{x}$ **arises from** x. The following proposition is needed to do intersection theory *on*

$$X_v = X \times_{\mathbb{Z}} \mathscr{O}_v.$$

Proposition. — *The point $\widetilde{x}_v : \mathrm{Spec}(\mathscr{O}_v) \to X_v$ arising from a Heegner point $x \in X(H)$ is in the relative smooth locus over $\mathscr{O}_v$.*

Proof. Omitted. □

(3.2) Let $\breve{x} \in X(\breve{H}_v)$ arise from a Heegner point $x \in X(H)$. Since X does not represent the moduli problem, it is not at all obvious that $\breve{x}$ arises from a cyclic isogeny over W. But in fact:

Proposition. — *$\breve{x}$ is induced by a Heegner diagram over $\breve{\mathscr{O}}_v$.*

Proof Sketch. Let $\phi : E \to E'$ be the Heegner diagram over H inducing x. This diagram does not admit good reduction over W in general.

(1) There exists a twist of E over $\breve{H}_v$ with good reduction. It is given by an element
$$\chi \in H^1(\mathrm{Gal}(\breve{H}_v), \mathscr{O}_K^\times)$$
(with the trivial Galois action). Choose such a χ.
(2) As ϕ is $\mathscr{O}_K$-equivariant, we can twist E' by χ as well. This way we get a Heegner diagram over $\breve{H}_v$ with good reduction. Furthermore, this diagram induces the same $X(\breve{H}_v^s)$ point as x.
(3) We can extend the twisted diagram to W using functoriality of Néron models.

□

§4. TOOLS OF DEFORMATION THEORY

(4.1) Let $(R, \mathfrak{m})$ be a local ring and A, B be abelian schemes over R. Write $(\bullet)_n$ for reduction mod $\mathfrak{m}^{n+1}$ functor.

Proposition. — *The map*

$$\mathrm{Hom}_R(A, B) \longrightarrow \mathrm{Hom}_{R_n}(A_n, B_n)$$

is injective.

Proof. Omitted. □

Writing $k = R/\mathfrak{m}$ for the residue field, we thus have a filtration

$$\ldots \hookrightarrow \mathrm{Hom}_{R_2}(A_2, B_2) \hookrightarrow \mathrm{Hom}_{R_1}(A_1, B_1) \hookrightarrow \mathrm{Hom}_k(A_0, B_0).$$

In our setting we are interested in the case $R = \breve{\mathscr{O}}_v$ and $A = E, B = E'$. We will want to compute

(i) $\mathrm{Hom}_{R_n}(A_n, B_n)$ for each n (or at least their sizes),
(ii) $\mathrm{Hom}_R(A, B)$.

The Serre–Tate theorem and Grothendieck's existence theorem will help us deal with (i) and (ii) respectively.

(4.2) Let S_0 be a scheme such that p vanishes on S_0. Let A_0 be an abelian scheme over S_0. We will define an object $A_0[p^\infty]$ called the **p-divisible group attached to** A. Let $S_0 \hookrightarrow S$ be a closed immersion whose associated ideal sheaf is nilpotent. Informally the Serre–Tate theorem says that

> The deformations of abelian schemes and their homomorphisms from S_0 to S are completely controlled by their p-divisible groups and their homomorphisms.

For example, let A, B be abelian schemes over S with pullbacks A_0, B_0 to S_0 and $f_0 : A_0 \to B_0$ be a homomorphism. One of the consequences of the Serre–Tate theorem is that f_0 lifts to a homomorphism $f : A \to B$ if and only if the induced homomorphism $f_0[p^\infty] : A_0[p^\infty] \to B_0[p^\infty]$ of p-divisible groups lifts to a homomorphism $f[p^\infty] : A[p^\infty] \to B[p^\infty]$ of p-divisible groups.

In our case $S_0 = \operatorname{Spec} \check{\kappa}_v$, $S = \operatorname{Spec} \check{\mathcal{O}}_{v,n}$ for some $n \in \mathbb{Z}_{\geqslant 0}$ this will help us compute the groups $\mathrm{Hom}_{\check{\mathcal{O}}_{v,n}}(E_n, E'_n)$.

(4.3) Going back to the setup of Paragraph 4.1, we know that

$$\mathrm{Hom}_R(A, B) \subset \bigcap_n \mathrm{Hom}_{R_n}(A_n, B_n) \simeq \varprojlim_n \mathrm{Hom}_{R_n}(A_n, B_n).$$

But is this an equality?

Theorem (Grothendieck's existence theorem). — *Let R be a Noetherian ring, I an ideal of R. Write $(\bullet)_n$ for reduction mod I^{n+1}. Assume that R is complete and separated for the I-adic topology.*

(1) Let X, Y be proper R-schemes. The natural map

$$\mathrm{Hom}_R(X, Y) \longrightarrow \varprojlim \mathrm{Hom}_{R_n}(X_n, Y_n)$$

is an isomorphism.

(2) Let $\{X_n\}$ be a compatible system of proper schemes over R_n. Let $\mathscr{L}_n$ be a compatible system of line bundles on X_n. There exists a pair $(X, \mathscr{L})$, unique up to unique isomorphism, lifting each $(X_n, \mathscr{L}_n)$.

So yes, we do get an equality. Also, since elliptic curves have canonical line bundles, a compatible system of elliptic curves lifts to the projective limit.

Combining with the Serre–Tate theorem, we get:

Corollary. — *Let $(R, \mathfrak{m})$ be a complete, Noetherian, local ring with residue field $k = R/\mathfrak{m}$ of positive characteristic. Let A, B be abelian schemes over R, then*

$$\mathrm{Hom}_R(A, B) = \mathrm{Hom}_k(A_0, B_0) \cap \bigcap_n \mathrm{Hom}_{R_n}(A_n[p^\infty], B_n[p^\infty]).$$

§5. p-DIVISIBLE GROUPS

(5.1) Let S be a scheme and A be an abelian scheme over S. Let p be a prime. The system

$$A[p] \hookrightarrow A[p^2] \hookrightarrow A[p^3] \hookrightarrow \dots$$

is the **p-divisible group attached to** A, denoted $A[p^\infty]$. Notice that:

(i) For each n, the subgroup $A[p^n]$ is a finite, flat, commutative group scheme over S.
(ii) $A[p^n] = A[p^{n+1}][p^n]$.

More generally, a **p-divisible group** is an inductive system $G = (G_n)$ of finite flat commutative group schemes, such that $G_n = G_{n+1}[p^n]$. The **height** of G is the unique $h \in \mathbb{Z}_{\geqslant 0}$ such that G_n is of order p^{nh} for all n. A homomorphism of p-divisible groups is just a compatible system of group scheme homomorphisms.

Example. — Let $g = \dim A$, then $A[p^\infty]$ is a p-divisible group of height $2g$.

(5.2) Let S be a scheme on which p is locally nilpotent. Let $S_0 \hookrightarrow S$ be a closed subscheme defined by a nilpotent sheaf of ideals. Let $\mathsf{A}(S)$ be the category of abelian schemes over S. Let $\mathsf{Def}(S, S_0)$ be the category of triples (A_0, G, ε) where

(i) A_0 is an abelian scheme over S_0,
(ii) G is a p-divisible group over S,
(iii) $\varepsilon : G_0 \to A_0[p^\infty]$ is an isomorphism of p-divisible groups over S_0.

Theorem (Serre–Tate). — *The functor*

$$\begin{aligned} \mathsf{A}(S) &\longrightarrow \mathsf{Def}(S, S_0) \\ A &\longmapsto (A_0, A[p^\infty], \textit{canonical}) \end{aligned}$$

is an equivalence of categories.

(5.3) The Serre–Tate theorem says at least three interesting things. The first one is essential surjectivity, which allows us to reduce the problem of finding deformations of abelian schemes to the problem of finding deformations of p-divisible groups, which is much more tractable. To explain the other two we need a few lemmas. Throughout $S_0 \hookrightarrow S$ is as in the Serre–Tate setup.

Lemma. — *Let A, A' be abelian schemes over S, then*

$$\mathrm{Hom}_S(A, A') \longrightarrow \mathrm{Hom}_{S_0}(A_0, A_0')$$

is injective.

Lemma. — *Let G, G' be p-divisible groups over S, then*

$$\mathrm{Hom}_S(G, G') \longrightarrow \mathrm{Hom}_{S_0}(G_0, G_0')$$

is injective.

Lemma. — *Let A, A' be abelian schemes over S, then*

$$\mathrm{Hom}_S(A, A') \longrightarrow \mathrm{Hom}_S(A[p^\infty], A'[p^\infty])$$

is injective.

If A, A' are abelian schemes over S, by Serre–Tate the square

$$\begin{array}{ccc} \mathrm{Hom}_S(A, A') & \hookrightarrow & \mathrm{Hom}_S(A[p^\infty], A'[p^\infty]) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{S_0}(A_0, A_0') & \hookrightarrow & \mathrm{Hom}_{S_0}(A_0[p^\infty], A_0'[p^\infty]) \end{array}$$

is Cartesian. This tells us:

(1) which homomorphisms $A[p^\infty] \to A'[p^\infty]$ come from homomorphisms $A \to A'$,
(2) which homomorphisms $A_0 \to A_0'$ lift to homomorphisms $A \to A'$.

(5.4) Let k be a field.

Theorem (Connected-étale exact sequence). — *Let* G *be a finite, flat group scheme over* k.

(1) There is a canonical short exact sequence

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{ét} \longrightarrow 0$$

of group schemes. G^0 *is the identity component of* G *and* $G^{ét}$ *is finite, étale.*

(2) If k *is perfect, the induced map* $G^{red} \to G^{ét}$ *is an isomorphism; in particular, the short exact sequence splits canonically.*

If G is a p-divisible group over k, the connected-étale exact sequences of G_n are compatible and we get a short exact sequence

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 0$$

of p-divisible groups. A p-divisible group is **connected/étale/reduced** if each G_n satisfies the same property. (G_n^{red}) define a p-divisible subgroup of G and when k is perfect the short exact sequence splits.

(5.5)

Example. — Let k be algebraically closed, E be an elliptic curve over k and p be a prime. Since k is perfect,

$$E[p^\infty] \simeq E[p^\infty]^0 \times E[p^\infty]^{\text{ét}}.$$

First, we examine the étale part.

(i) If k has characteristic different from p, then
$$E[p^n] \simeq (p^{-n}\mathbb{Z}/\mathbb{Z})^2$$
is a constant, étale group scheme. The p-divisible group $\mathbb{Q}_p/\mathbb{Z}_p := (p^{-n}\mathbb{Z}/\mathbb{Z})$ is called the **constant** p-divisible group. Hence $E[p^\infty] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2$.

(ii) If E is ordinary, then
$$E[p^n]^{\text{ét}} \simeq p^{-n}\mathbb{Z}/\mathbb{Z}$$
and $E[p^\infty]^{\text{ét}} \simeq \mathbb{Q}_p/\mathbb{Z}_p$. This is a height 1 p-divisible group, so $E[p^\infty]^0$ is a connected p-divisible group of height 1.

(iii) If E is supersingular, then
$$E[p^n]^{\text{ét}} = 0,$$
so $E[p^\infty]$ is a connected p-divisible group of height 2.

Our next goal is to understand the connected part.

§6. Formal Lie Groups

(6.1) Let R be a commutative ring. An **(n-dimensional, commutative) formal Lie group** $\mathscr{G}$ is a suitable R-homomorphism

$$\theta_G : R[\![T_1, \ldots, T_n]\!] \longrightarrow R[\![X_1, \ldots, X_n, Y_1, \ldots, Y_n]\!].$$

By suitable, I mean that if $G(X, Y) = (G_i(X, Y))$ where G_i is $\theta_G(T_i)$, then

(i) $G(X, 0) = X$,
(ii) $G(X, Y) = G(Y, X)$,
(iii) $G(X, G(Y, Z)) = G(G(X, Y), Z)$.

Let $\mathscr{F}, \mathscr{G}$ be formal Lie groups of dimensions n, m respecfively, and let F, G be their corresponding families of power series. A **homomorphism** $f : \mathscr{F} \to \mathscr{G}$ is a family $f = (f_1, \dots, f_m)$ of n-power series in $X_1, \dots, X_n$ with no constant terms, such that

$$f(F(X, Y)) = G(f(X), f(Y)).$$

If $f, g \in \mathrm{Hom}_R(\mathscr{F}, \mathscr{G})$ then we define

$$(f + g)(T) = G(f(T), g(T)).$$

Defining multiplication to be composition in $\mathrm{End}_R(\mathscr{G})$ we get a non-commutative ring structure, and the canonical homomorphism $\mathbb{Z} \to \mathrm{End}_R(\mathscr{G})$ defines endomorphisms $[n]$ for all $n \in \mathbb{Z}$. We can reinterpret these as homomorphisms

$$[n] : R[\![T_1, \dots, T_n]\!] \longrightarrow R[\![T_1, \dots, T_n]\!].$$

Note that the linear term of $[n](T)$ is nT.

(6.2) If $[p] : \mathscr{G} \to \mathscr{G}$ is finite, we say $\mathscr{G}$ is p**-divisible**. In that case,

$$F[p^n] = \mathrm{Spec}(R[\![T_1, \dots, T_n]\!]/[p^n]((T_1, \dots, T_n)))$$

is a finite, flat, connected commutative group scheme over R and the system $F[p^\infty] = (F[p^n])$ defines a connected p-divisible group.

Theorem (Tate). — *Let R be a complete, Noetherian, local ring with residue field of characteristic $p > 0$. The functor $F \mapsto F[p^\infty]$ is an equivalence of categories between p-divisible formal Lie groups and connected p-divisible groups over R.*

Remark. — Using the formalism of sheaves for the fppf site we can actually identify p-divisible formal Lie groups with connected p-divisible groups. This will be important later, because we will need to study the deformations of p-divisible groups and we'd like to do that by studying deformations of formal Lie groups.

The **dimension** of a p-divisible group G over R as in the theorem is the dimension of the formal Lie group corresponding to G^0.

Example (Continued). — For the rest of this section take k to be algebraically closed of characteristic $p > 0$. The formal Lie group corresponding to $E[p^\infty]^0$ is a 1-dimensional formal Lie group.

(6.3)

Lemma. — *Let $\mathscr{F}, \mathscr{G}$ be 1-dimensional formal Lie groups over k and $f \in \mathrm{Hom}_k(\mathscr{F}, \mathscr{G})$. Then*

$$f(T) = a_1 T^{p^h} + a_2 T^{2p^h} + \dots, \qquad a_1 \neq 0$$

*for some $h \in \mathbb{Z}_{\geqslant 1}$ or $f = 0$. Such h, if it exists, is the **height** of f. The height of $f = 0$ is defined to be ∞.*

Now let $\mathscr{G}$ be a formal Lie group over k, then the **height** of $\mathscr{G}$ is the height of $[p]$.

Theorem (Lazard). — *The height is a complete invariant of formal Lie groups over k.*

Theorem (Dieudonné–Lubin). — *Let $\mathscr{G}$ be a formal Lie group of height $h < \infty$. Then $\mathrm{End}_k(\mathscr{G})$ is isomorphic to the maximal order in the central division algebra of invariant $1/h$ and rank h^2 over $\mathbb{Q}_p$.*

§7. Ordinary Elliptic Curves

(7.1) Let k be an algebraically closed field of characteristic $p > 0$. Let E_0 be an ordinary elliptic curve over k. We know that $E_0[p^\infty]^{\text{ét}} \simeq \mathbb{Q}_p/\mathbb{Z}_p$. We also know that $E_0[p^\infty]^0$ is a 1-dimensional formal Lie group of height 1. This formal Lie group is actually isomorphic to μ_{p^∞}:

$$\mu_p \hookrightarrow \mu_{p^2} \hookrightarrow \mu_{p^3} \hookrightarrow \dots$$

(7.2) Let $\operatorname{Spec} k \hookrightarrow S$ be a closed immersion defined by a nilpotent ideal sheaf. Let E be a lift of E_0 to S and consider the connected-étale sequence

$$0 \longrightarrow E[p^\infty]^0 \longrightarrow E[p^\infty] \longrightarrow E[p^\infty]^{\text{ét}} \longrightarrow 0.$$

$E[p^\infty]^0$ and $E[p^\infty]^{\text{ét}}$ are lifts of μ_{k,p^∞} and $\underline{\mathbb{Q}_p/\mathbb{Z}_p}_k$ respectively. Both of these have unique lifts to S, namely μ_{S,p^∞} and $\underline{\mathbb{Q}_p/\mathbb{Z}_p}_S$. Hence the deformations of E_0 to S are in bijection with

$$\operatorname{Ext}^1(\underline{\mathbb{Q}_p/\mathbb{Z}_p}_S, \mu_{S,p^\infty}).$$

In particular, they form a group, and the identity element, the **Serre–Tate canonical lift**, corresponds to the deformation for which the exact sequence splits.

§8. Supersingular Elliptic Curves

(8.1) We will need an additional piece of structure in the supersingular case. Let A be a ring and B be an A-algebra, then a **formal A-module** of dimension 1 over B is a pair $(\mathscr{G}, g)$ of

(i) a 1-dimensional formal Lie group $\mathscr{G}$ over B,
(ii) a homomorphism $g : A \to \operatorname{End}_B(\mathscr{G})$ such that $g(a)'(0) = a$.

If A is the ring of integers of a local field, and π is a uniformizer, then the **height** of $(\mathscr{G}, g)$ is the height of $g(\pi)$.

(8.2) For the purposes of Gross-Zagier we will be in the following situation:

- $\check{x} \in X(\check{\mathscr{O}}_v)$ comes from a Heegner point $x \in X(H)$,
- p is a rational prime which is either split or ramified in K,
- so v comes from the unique prime w in $\mathscr{O}_K$ dividing p,
- E is an elliptic curve for a Heegner diagram of $\check{x}$,
- E_0 is the supersingular reduction of E.

Note that we have inclusions

$$\mathscr{O}_K \hookrightarrow \operatorname{End}_{\check{\mathscr{O}}_v}(E) \hookrightarrow \operatorname{End}_{\check{\mathscr{O}}_v}(E_0) \hookrightarrow \operatorname{End}_k(E_0) \hookrightarrow \operatorname{End}_k(E_0[p^\infty]).$$

Also, the endomorphism ring of any p-divisible group has a $\mathbb{Z}_p$-module structure, so we have a map

$$\phi : \mathscr{O}_w \simeq \mathscr{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \operatorname{End}_k(E_0[p^\infty])$$

which makes $(E_0[p^\infty], \phi)$ into an $\mathscr{O}_w$-module over k of height 1. Also note that $E_0[p^\infty]$ is a $\mathbb{Z}_p$-module of height 2.

(8.3) Write $\mathscr{G} = E_0[p^\infty]$ and $R = \operatorname{End}_k(\mathscr{G})$. R is the maximal order in the quaternion division algebra Q over $\mathbb{Q}_p$. If we treat $\mathscr{G}$ as a formal $\mathscr{O}_w$-module:

Proposition (Lubin–Tate). — *There is a formal $\mathcal{O}_w$-module $\check{\mathcal{G}}$ over $\check{\mathcal{O}}_v$ lifting $\mathcal{G}$. This lift is unique up to isomorphism.*

Furthermore, we have that

$$\mathrm{End}_{\check{\mathcal{O}}_v}(\check{\mathcal{G}}) = \mathcal{O}_w.$$

(8.4) Now we will treat $\mathcal{G}$ as a formal $\mathbb{Z}_p$-module. We call $\check{\mathcal{G}}$ the **canonical lifting** of $\mathcal{G}$. For $n \in \mathbb{Z}_{\geqslant 0}$ define

$$R_n = \mathrm{End}_{\check{\mathcal{O}}_v/\pi^{n+1}}(\check{\mathcal{G}});$$

in particular, $R_0 = R$. By Paragraph 4.1, we have injections

$$\ldots \hookrightarrow R_2 \hookrightarrow R_1 \hookrightarrow R.$$

By Grothendieck's existence theorem

$$\mathcal{O}_w = \mathrm{End}_{\check{\mathcal{O}}_v}(\check{\mathcal{G}}) = \bigcap_{n \in \mathbb{Z}_{\geqslant 0}} R_n$$

Proposition. — *For $n \geqslant 1$*

$$R_n = \mathcal{O} + \pi^n R.$$

Proof Idea. One can prove this by mapping R_{n-1}/R_n into the second formal module cohomology groups. □

(8.5) We can give an explicit quaternionic description of R_n, which we will need for computations later. By the Skolem–Noether theorem, there is some $j \in Q^*/K_w^*$ such that conjugation by j induces the non-trivial $\sigma \in \mathrm{Gal}(K_w/\mathbb{Q}_p)$. We get a decomposition

$$Q = K_w \oplus jK_w = Q_+ \oplus Q_-.$$

Given $b \in Q$ write $b = b_+ + b_-$ for the decomposition of b into $Q_+ \oplus Q_-$.

Proposition. — *For $n \geqslant 0$*

$$\begin{aligned} R_n &= \left\{ b \in B \,\middle|\, \mathrm{Tr}(b) \in \mathbb{Z}_p, N(b) \in \mathbb{Z}_p, N(b_-) \equiv 0 \bmod p^{1-e+nf} \right\} \\ &= \{ b \in R | D \cdot N(b_-) \equiv 0 \bmod p \cdot N(\pi)^n \}. \end{aligned}$$

(8.6) Finally, we introduce the notion of quasi-canonical liftings, which we will need in Gross-Zagier. Let

$$T = T\check{\mathcal{G}} = \varprojlim_n \check{\mathcal{G}}[p^n](\overline{\check{H}_v})$$

be the **Tate-module** of $\check{\mathcal{G}}$. Let

$$V = V\check{\mathcal{G}} = T \otimes_{\mathcal{O}_w} K_w.$$

The $\mathbb{Z}_p$-submodules T' of V such that T'/T is finite give rise to

(i) a formal $\mathbb{Z}_p$-module $\check{\mathcal{G}}'$ over $\check{\mathcal{O}}'_v$, the ring of integers of the field $\check{H}'_v$ fixed by

$$\mathrm{Stab}(T') \subset \mathrm{Gal}(\check{H}_v).$$

(ii) an isogeny

$$\check{\mathcal{G}} \longrightarrow \check{\mathcal{G}}'$$

defined over $\check{\mathcal{O}}'_v$.

Now there are two options:

$$\mathrm{End}_{\check{\mathcal{O}}'_v}(\check{\mathcal{G}}') = \begin{cases} \mathcal{O}_w \\ \mathcal{O}_s := \mathbb{Z}_p + p^s\mathcal{O}_w \quad \text{for some } s \geqslant 1. \end{cases}$$

In the first case $\check{\mathcal{G}}' \simeq \check{\mathcal{G}}$, so we get the canonical lift. In the second case we say $\check{\mathcal{G}}'$ is a **quasi-canonical lift of level** s.

(8.7) We finish with a few facts about quasi-canonical liftings.

Proposition. — *(1) There is a quasi-canonical lift of every level* $s \geqslant 1$.
(2) Let $\check{\mathcal{G}}'$ *be a quasi-canonical lift of level* s. *Then* $\check{H}'_v$ *is the abelian extension of* K_w *with norm group* $\mathcal{O}_s^* \subset K_w^*$.
(3) Quasi-canonical lifts of level s *are a* $\mathrm{Gal}(\check{H}'_v/\check{H}_v)$*-torsor.*
(4) If $\check{\mathcal{G}}'$ *is a quasi-canonical lifting, then* $\check{\mathcal{G}}$ *and* $\check{\mathcal{G}}'$ *are not isomorphic mod* $(\pi')^2$ *(where* π' *is a uniformizer of* $\check{\mathcal{G}}'$*).*