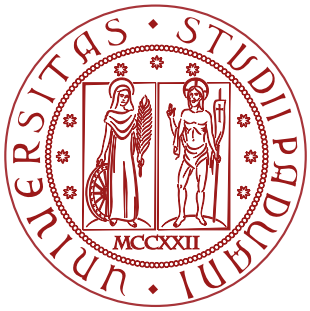


UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DEPARTMENT OF MATHEMATICS "TULLIO LEVI-CIVITA" – UNIVERSITY OF PADOVA

Master Thesis in Mathematics

THE CANONICAL LIFTS OF ELLIPTIC CURVES THROUGH WITT VECTORS

Supervisor
NICOLA MAZZARI
UNIVERSITY OF PADOVA

Master Candidate
BENJAMIN JEFFERS

Student ID
2140406

Academic Year 2024-2025
Graduation Date 19/09/2025

Abstract

In this thesis, we study the canonical liftings of ordinary elliptic curves over fields of characteristic $p > 0$. Building on the theory of Witt vectors and their relation to the moduli space of ordinary elliptic curves, we show that the canonical lift construction extends to families of ordinary elliptic curves over p-adic sheaves. Our approach highlights the formal nature of the construction and its dependence on the universal property of Witt vectors.

Contents

1 Introduction

Solving polynomial equations is one of the oldest and most fundamental problems in mathematics. For example, consider the quadratic polynomial

$$f(x) = x^2 + 1.$$

Over the integers, this equation has no root. However, working modulo 5, we find that $x = 2$ is a solution, since $2^2 + 1 = 5 \equiv 0 \mod 5$.

Although this does not yield a root in the integers, Hensel's lemma provides an improvement: Under certain conditions, a modulo solution p can be *lifted* to a solution in the ring of p-adic integers $\mathbb{Z}_p$. This was one of the first results to demonstrate how problems in characteristic p can inform and lead to solutions in characteristic 0. It has since become a common technique to reduce a problem modulo p, and then lift it to characteristic 0, when possible.

This approach was taken by Serre and Tate in their paper [1]. They demonstrated that an abelian variety over a perfect field k of characteristic p admits a lift to characteristic zero over the ring of Witt vectors $W(k)$, along with a compatible lift of the Frobenius endomorphism. This result laid the groundwork for a theory of canonical lifts.

In this thesis, we investigate this problem in the more general context of elliptic curves over p-adic sheaves. Our goal is to construct and understand canonical lifts in this setting, where the base is no longer a field, but a ring R with p nilpotent, or even a more general

basis called a *p-adic sheaf* which is a colimit $\operatorname{colim}_i S_i$ where each $S_i = \operatorname{Spec} Ri$ is affine with p nilpotent in R. Borger and Gurney work over these more general objects, but we will prove all the results in the setting of an affine scheme with p nilpotent and then show how to pass to the general result by taking colimits. We explain the recent result of Borger and Gurney in [2] which says the following:

Theorem 1.0.1. *There is a unique way of lifting ordinary elliptic curves E over an affine scheme $S = \operatorname{Spec} R$ on which p is nilpotent, to an elliptic curve $\widetilde{E}$ over $W(S)$ such that the construction $E \mapsto \widetilde{E}$ is compatible with base change in S and such that $\widetilde{E}$ admits a Frobenius lift.*

We begin by introducing Witt vectors through δ-structures. While we are primarily interested in Frobenius lifts, a map of rings $\phi : A \to A$ such that $\phi(x) \equiv x^p \mod pA$, δ-structures are stronger and the category of rings with δ-structures is much better behaved than the category of rings with Frobenius lifts. However, given a δ-structure we obtain a Frobenius lift by letting $\phi(x) = x^p + p\delta(x)$, the definition of δ is reverse engineered to make this expression a Frobenius lift. We follow the perspective in [3] as well as [4].

Although we do not need the theory of δ-structures beyond using them to introduce the Witt vectors, in the higher-dimensional continuation of this work in [5] Borger and Gurney extend this work to families of abelian varieties over p-adic sheaves. Because the moduli problem of abelian varieties in higher dimension is more difficult, they use the extra structure provided by δ-structures.

Once we have established the theory of δ-structures and given several examples, we will look at the right adjoint to the forgetful functor $\mathbf{Ring}_\delta \to \mathbf{Ring}$. This will turn out to be the Witt vector functor, which, among other important properties, can lift a characteristic p ring to one in characteristic 0. The primary example being $W(\mathbb{F}_p) = \mathbb{Z}_p$. This is the first and simplest case of what we set out to do in this thesis. We are interested in these types of liftings, and the Witt vectors provide the basis on which we work.

There are many different approaches one can take to defining the Witt vectors. The definition we use here is often called the δ-coordinates, while there is a much more classical way to construct the Witt vectors using the Witt polynomials [6], these are called the Witt coordinates. The third way to view Witt vectors is through the Ghost coordinates [4], this is the best way to do calculations with Witt vectors. The δ-coordinates are useful because of the universal properties that come from them, but they are difficult to use to compute anything. It is more efficient to pass to the ghost coordinates, complete the

calculation, and map back to the δ-coordinates, as explained in [3]. We take up the study of the ghost coordinates and the ghost map in section 2.0.7.

After showing that the Witt vectors exist as a right adjoint to the forgetful functor, we will compute several examples to illustrate the complexity of working with the Witt vectors.

Then we continue with an exposition of the background material needed to understand the main theorem, including Grothendieck topologies, and specifically the étale topology, a refinement of the Zariski topology, as well as formal schemes, moduli problems, and the canonical subgroup.

The canonical subgroup, E^{can}, will play an important role in the proof of the main theorem, because for ordinary elliptic curves, the canonical subgroup is the canonical lift of the kernel of the Frobenius. So when we try to construct the Frobenius lift on the canonical lift of an elliptic curve, it will be necessary to appeal to the quotient of E/E^{can}

In the final chapter, we explain the proof of Theorem 1.0.1. We first prove the theorem in the case of some stronger structure, called a level-N structure. This will reduce the proof to showing the representability of the moduli problem of full level-N structure. We explain this problem in section 6.0.2, and a complete proof can be found in [7]. Then we show that the canonical lift is independent of the choice of the level-N structure. Finally, we prove it in full generality. Starting with an elliptic curve E/S, we can reduce to the case where S is an affine scheme on which p is nilpotent, and then consider an étale cover $S' \to S$ such that $(E \times_S S')/S'$ has a level structure. Using the previous section, we can then lift this, and after constructing a descent datum, we can descend to the canonical lift of our original curve E/S.

2

Witt Vectors

The Witt vectors were first studied by Witt in [8]. We give some motivation for the construction following [9] and [10]. Suppose we have a finite unramified extensions $K/\mathbb{Q}_p$, and assume that we want to write down an element of the ring of integers $\mathcal{O}_K$. Since K is local and unramified, p is a uniformizer, so the typical way to write an element $x \in \mathcal{O}_K$ is as

$$x = \sum_{n=0}^{\infty} x_n p^n$$

where the x_n are some representatives for $\mathcal{O}_K/p\mathcal{O}_K \cong k$. The problem is that these expressions are very difficult to add or multiply because there will be a lot of carrying digits. Instead, consider the homomorphism

$$\begin{aligned} \omega \colon k^\times &\to \mathcal{O}_K^\times \\ x &\mapsto \lim_{n\to\infty} x^{|k|^n} \end{aligned}$$

This map satisfies the property that $\omega(x) \equiv x \pmod{p}$ and $\omega(x)^p = \omega(x)$, and in addition, it is multiplicative. This map is called the *Teichmüller lift* and can be extended to

$$\omega \colon k \to \mathcal{O}_K$$

by letting $\omega(0) = 0$. Now we can write representatives of the image of ω as the representatives in the p-adic expansion. For each $x \in \mathcal{O}_K$, there exists a unique sequence $x_n \in k$ such that

$$x = \sum_{n=0}^{\infty} \omega(x_n) p^n.$$

Now we look at how to add these expressions. Consider

$$\sum_{n=0}^{\infty} a_n p^n + \sum_{n=0}^{\infty} b_n p^n = \sum_{n=0}^{\infty} c_n p^n$$

where the a_n's and b_n's are Teichmüller lifts. We first note that we have

$$c_0 \equiv a_0 + b_0 \pmod{p}$$

and therefore

$$c_0^p \equiv (a_0 + b_0)^p \pmod{p^2}.$$

Now we consider the expansions modulo p^2 which gives

$$c_0^p + c_1 p \equiv a_0^p + a_1 p + b_0^p + b_1 p \pmod{p^2}.$$

Here we use the fact that $x^p = x$ for Teichmüller coefficients. Since $c_0^p \equiv (a_0 + b_0)^p \pmod{p^2}$ and since $a_0^p + b_0^p - (a_0 + b_0)^p$ is divisible by p by the binomial expansion, we have

$$c_1 \equiv a_1 + b_1 - \frac{(a_0 + b_0)^p - a_0 - b_0}{p} \pmod{p^2}$$

We can continue doing this for higher powers of p. For each n we will find polynomials α_n with integer coefficients such that

$$a + b = (\alpha_0(a_0, b_0), \alpha_1(a_0, b_0, a_1, b_1), \ldots).$$

We can do the same thing for multiplication and find polynomials π_n such that

$$ab = (\pi_0(a_0, b_0), \pi_1(a_0, b_0, a_1, b_1), \ldots)$$

This defines a ring structure on $\prod_{n\geq 0}\mathbb{F}_q$ which identifies it with $\mathbb{Z}_p[\zeta_{q-1}]$. Now, defining the *Witt polynomials* to be

$$W_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}$$

we get maps $W_n\colon \prod \mathbb{F}_p \to \mathbb{F}_p$ and the ring structure was determined once we knew the polynomials relations

$$W_n(a+b) = W_n(a) + W_n(b) \text{ and } W_n(ab) = W_n(a)W_n(b) \text{ in } \mathbb{F}_p.$$

Thus, given a commutative ring A, we define the *ring of Witt vectors* $W(A)$ to be $\prod_{n\geq 0} A$ as a set with multiplication and addition given above.

This is the classical way to develop Witt vectors and is done in more detail in [6]. While it is useful to have concrete polynomials on which to do calculations, this definition becomes messy for our goals. There is a simpler categorical situation in which Witt vectors appear as the right adjoint to a forgetful functor. In the following chapter we first introduce this categorical setting and then take a closer look at Witt vectors and conclude with computing several examples.

2.0.1 p-DERIVATIONS AND δ-RINGS

Throughout this section let p be a prime and let R be a commutative ring.

Definition 2.0.1. A ring endomorphism $\phi\colon R \to R$ is a *Frobenius lift* if for all $x \in R$

$$\phi(x) \equiv x^p \pmod{pR}.$$

Equivalently, it is a map making the following diagram commute:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R \\ \downarrow & & \downarrow \\ R/pR & \xrightarrow[r\mapsto r^p]{} & R/pR \end{array}$$

Example 2.0.2.

1. If $R = \mathbb{Z}$ or $R = \mathbb{Z}_{(p)}$ (localization at p), then the identity is a Frobenius lift because Fermat's little theorem tells us that $x^p \equiv x \pmod{p}$.

2. Let $R = \mathbb{Z}[x]$, then let $\phi(x) = x^p + p \cdot r(x)$, with $r(x) \in \mathbb{Z}[x]$. Any choice of $r(x) \in \mathbb{Z}[x]$ will result in ϕ being a Frobenius lift.

3. Let $K/\mathbb{Q}_p$ be an unramified finite extension with residue field k and ring of integers $\mathscr{O}_K$. Since $K/\mathbb{Q}_p$ is unramified,

$$\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathrm{Gal}(k/\mathbb{F}_p)$$

and the group $\mathrm{Gal}(k/\mathbb{F}_p)$ is generated by the pth power Frobenius. Let ϕ denote the preimage of the Frobenius in $\mathrm{Gal}(K/\mathbb{Q}_p)$. This lift of the Frobenius stabilizes $\mathscr{O}_K$ and thus defines a lift of the Frobenius on it.

4. The ring of integers of a number field has a Frobenius lift at all the unramified primes. Consider the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, this is a degree two extension, with ring of integers $\mathbb{Z}[\sqrt{2}]$, and every prime outside of (2) is unramified. So if we look at the residue field of (3), we see that it is $k/\mathbb{F}_3$, a degree two extension. The Galois group consists of the Frobenius and the identity. So the map

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \to \mathrm{Gal}(k/\mathbb{F}_3)$$

sends the identity automorphism to the identity automorphism, and it sends the map that takes $\sqrt{2} \to -\sqrt{2}$ to the Frobenius. Thus this map is a lift of the Frobenius on $\mathbb{Z}[\sqrt{2}]$.

5. Let $A = \mathbb{Z}[\mu_n \colon \gcd(n,p) = 1]$. The automorphism $\phi \colon A \to A$ given by $\phi(\zeta_n) = \zeta_n^p$ is a Frobenius lift.

6. If p is invertible in the ring A, then every endomorphism of A is a Frobenius lift. Indeed, since p is invertible $pA = A$, so $\phi(x) \equiv 0 \mod pA$.

Definition 2.0.3. Given two rings with Frobenius lifts (A, ϕ_a) and (B, ϕ_B), a morphism between them is a map $f \colon A \to B$ that respects the structure of the Frobenius:

$$f \circ \phi_A = \phi_B \circ f.$$

We denote by $\mathbf{Ring}_\phi$ the category of rings with a Frobenius lift and morphisms as given above.

Remark 2.0.4. While the notion of a Frobenius lift is useful and we are interested in studying it further there are a couple problems:

1. There are a couple reasons why the category $\mathbf{Ring}_\phi$ is not sufficient for many purposes, and why it is often termed a "bad category". One object that is often used in a category is the "free object", in our case this would be the free object with a Frobenius lift. The way to show the existence of such a free object is to show that a forgetful functor has a left adjoint. For us this would be asking for the existence of a left adjoint to the forgetful functor $\mathbf{Ring}_\phi \to \mathbf{Ring}$. This would require that the forgetful functor commutes with limits since right adjoints always commute with limits.

2. To see the failure mentioned above we examine an example with equalizers, since equalizers are limits. Let $A = \mathbb{Z}_{(p)}[x,y]$ with a Frobenius lift $\phi : A \to A$ defined by $x \mapsto x^p + py$ and $y \mapsto y^p$. Then $\phi_A((py)) \subseteq (py)$. Letting $B = A/(py)$ we see that the Frobenius lift ϕ_A induces a lift on B: $\phi_B : B \to B$ given by $\phi_B(x+(py)) = x^p + (py)$ and $\phi_B(y) = y^p + (py)$. Now, define

$$\begin{aligned} f : A &\to B \\ x &\mapsto x + (py) \\ y &\mapsto 0 + (py) \end{aligned}$$

Then one can check that $f \circ \phi_A = \phi_B \circ f$, so f is a morphism in $\mathbf{Ring}_\phi$. We let $E = \mathrm{eq}(f,p)$ where p is the canonical projection $A \to B$. We claim that $E = \mathbb{Z}_{(p)}[x] + (py)\mathbb{Z}_{(p)}[x,y]$. Indeed, if $a(x) + \alpha \cdot b(x,y) \in \mathbb{Z}_{(p)}[x] + (py)\mathbb{Z}_{(p)}[x,y]$ where $\alpha \in (py)$, then

$$\begin{aligned} f(a(x) + \alpha \cdot b(x,y)) &= f(a(x)) + pf(y)f(b(x,y)) \\ &= (a(x) + (py)) + 0 + (py) \\ &= (a(x) + (py)) + 0 + (py) = a(x) + (py) \end{aligned}$$

and

$$g(a(x) + \alpha \cdot b(x,y)) = a(x) + \alpha \cdot b(x,y) + (py) = a(x) + (py)$$

since $\alpha \cdot b(x,y) \in (py)$. Conversely, if $a(x,y) \in E$, then

$$\begin{aligned} f(a(x,y)) - g(a(x,y)) &\in (py) \\ a(x,0) - a(x,y) &\in (py) \end{aligned}$$

so $a(x,y) = a(x,0) + py \cdot r(x,y)$ for some $r(x,y) \in (py)$, and this means that $a(x,y) \in \mathbb{Z}_{(p)}[x] + (py)\mathbb{Z}_{(p)}[x,y]$.

Then we note that $y \notin E$. Thus there is no element T such that $\phi(x) = x^p + pT$. If

this were the case then we would have

$$x^p + pT = x^p + py$$

so that $y \in E$ which would be a contradiction. We can still compute the equalizer in $\mathbf{Ring}_\phi$. As noted above, the problem is that $y \notin E$, so the equalizer will be the smallest subring of A containing E and y, which is A itself. So the equalizer does exist in $\mathbf{Ring})\phi$, but it does not equalizer in **Ring**.

We will revisit this example later to demonstrate that it does not present an obstacle to our proposed solution for rings with Frobenius lifts.

3. There is an implicit "there exists" in the definition of a Frobenius lift: "for all x there exists an x' such that $\phi(x) = x^p + px'$". But x' is only unique up to p-torsion and in the presence of p-torsion we have no control.

A solution to point (3) above, which ends up fixing the first one as well is to provide x' as part of the structure rather than the property and its mere existence, this is what we will call a δ-ring.

1. test

Definition 2.0.5. A δ-ring is a pair (A, δ) where A is a ring and $\delta : A \to A$ is a map of sets such that the following properties hold:

1. $\delta(1) = 0$ and $\delta(0) = 0$,
2. $\delta(x+y) = \delta(x) + \delta(y) + \frac{1}{p}(x^p + y^p - (x+y)^p)$
3. $\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$.

Remark 2.0.6. Sometimes the map δ is called a *p-derivation* because if we look at

$$\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$$

modulo p, we get the Leibniz rule twisted by the Frobenius.

Definition 2.0.7. Let (A, δ_A) and (B, δ_B) be two δ-rings. A map $f\colon A \to B$ is a *morphism of δ-rings* if

$$f \circ \delta_A = \delta_B \circ f.$$

We thus have a category of δ-rings which we will denote by $\mathbf{Ring}_\delta$. This gives a forgetful functor

$$\mathbf{Ring}_\delta \to \mathbf{Ring}$$

that forgets the δ-structure. It turns out that the right adjoint to this forgetful functor will be the ring of Witt vectors, which will be a central object to us moving forward.

Note that in (2), the polynomial $\frac{1}{p}(X^p + Y^p - (X+Y)^p) \in \mathbb{Q}[X,Y]$ has integral coefficients by the binomial theorem. It is also common to see (2) written as

$$\delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} x^i y^{p-i}.$$

Remark 2.0.8. Let A be a δ-ring. Then A has a canonical lift of the Frobenius by setting $\phi(x) = x^p + p\delta(x)$. The properties of δ are reverse engineered exactly to make this work. Indeed, we have

$$\begin{aligned}\phi(xy) = x^p y^p + p\delta(xy) &= x^p y^p + p(x^p \delta(y) + y^p \delta(x)) \\ &= (x^p + \delta(x))(y^p + p\delta(y)) = \phi(x)\phi(y)\end{aligned}$$

and for addition we have

$$\begin{aligned}\phi(x+y) = (x+y)^p + p\delta(x+y) &= (x+y)^p + p\left(\delta(x) + \delta(y) + \frac{1}{p}(x^p + y^p - (x+y)^p\right) \\ &= x^p + p\delta(x) + y^p + p\delta(y) \\ &= \phi(x) + \phi(y).\end{aligned}$$

And lastly, $\phi(0) = 0^p + p\delta(0) = 0$ since $\delta(0) = 0$ and $\phi(1) = 1^p + p\delta(1) = 1$ since we require $\delta(1) = 0$. Furthermore, if R is a ring with a lift of the Frobenius ϕ and R is p-torsion-free, then having a lift of the Frobenius is equivalent to having a δ-structure. This can be seen by setting

$$\delta(x) = \frac{\phi(x) - x^p}{p}.$$

Remark 2.0.9. We can use the fact that $\delta(0) = \delta(1) = 0$ to reconstruct the value of δ on

any integer. Consequently, the action of δ on integers is given by

$$\delta(x) = \frac{x - x^p}{p}$$

and so $\delta(p^n) = \frac{p^n - p^{np}}{p} = p^{n-1}(1 - p^{n(p-1)})$, and the second factor is not divisible by p unless p is invertible in A, so δ lowers the p-adic valuation by 1.

Lemma 2.0.10. *Let (A, δ) be a δ-ring such that for some nonnegative integer n, $p^n = 0$ in A. Then $A = 0$.*

Proof. We induct on n. The base case with $n = 0$ is trivially true. Now, for $n > 0$, A is a $\mathbb{Z}_{(p)}$-algebra. Consequently

$$0 = \delta(0) = \delta(p^n) = p^{n-1}(1 - p^{n(p-1)})$$

and the second factor is a unit in A. Hence $p^{n-1} = 0$ in A also, and the induction hypothesis applies. □

Example 2.0.11. It is also possible to have a p-torsion free ring with no δ-structure. Consider the ring $A = \mathbb{Z}_{(p)}[x, x^p/p]$. If $\delta : A \to A$ is a δ-map, then we would have

$$\begin{aligned}
\frac{1}{p}\left(\frac{x^p}{p}\right)^p &= \frac{1}{p}\left(\phi\left(\frac{x^p}{p}\right) - p\delta\left(\frac{x^p}{p}\right)\right) \\
&= \frac{\phi(x)^p}{p^2} - \delta\left(\frac{x^p}{p}\right) \\
&= \frac{(x^p + p\delta(x))^p}{p^2} - \delta\left(\frac{x^p}{p}\right) \\
&= p^{p-2}\left(\frac{x^p}{p} + \delta(x)\right)^p - \delta\left(\frac{x^p}{p}\right) \in A
\end{aligned}$$

which is a contradiction

Example 2.0.12. Now we return to Example 2.0.4 and show that this does not give us any issues in the category of δ-rings. Recall that we let $A = \mathbb{Z}_{(p)}[x, y]$ with the Frobenius lift given by $\phi_A(x) = x^p + py$ and $\phi_A(y) = y^p$. Then we define $B = A/(py)$ and since $\phi_A((py)) \subseteq (py)$, we have an induced Frobenius lift ϕ_B where $\phi_B(x + (py)) = x^p + (py)$

and $\phi_B(y+(py)) = y^p + (py)$. Then we let

$$\begin{aligned} f\colon A &\to B \\ x &\mapsto x+(py) \\ y &\mapsto 0+(py). \end{aligned}$$

The problem was that the equalizer in the category $\mathbf{Ring}_\phi$ was not equal to the equalizer in **Ring**. However, we don't have this problem in $\mathbf{Ring}_\delta$. The map δ_A is induced by the Frobenius lift:

$$\delta_A(x) = \frac{\phi(x) - x^p}{p} = \frac{x^p + py - x^p}{p} = y$$

and

$$\delta_A(y) = \frac{\phi(y) - y^p}{p} = \frac{y^p - y^p}{p} = 0$$

Similarly, we find that $\delta_B(x+(py)) = y+(py)$ and $\delta(y+(py)) = 0$. Now, with the same map f we have

$$\delta_B(f(x)) = \delta_B(x+(py)) = y+(py)$$

while

$$f(\delta_A(x)) = f(y) = 0+(py)$$

so f is not actually a morphism in $\mathbf{Ring}_\delta$, so we avoid the issue we encountered in Example 2.0.4.

2.0.2 Differential Rings

Now we return to the forgetful functor $\mathbf{Ring}_\delta \to \mathbf{Ring}$. We are interested in understanding its right and left adjoints. The right adjoint allows us to lift a characteristic p ring to one in characteristic 0—a typical example being the lift of $\mathbb{F}_p$ to $\mathbb{Z}_p$. This will play a central role in the remainder of the thesis, as we aim to lift elliptic curves from characteristic p to characteristic 0.

The left adjoint provides a "free" δ-ring construction. This will be useful not only for understanding the right adjoint from a different perspective, but also for proving results about the right adjoint that will assist in explicit computations.

Before analyzing the forgetful functor on δ-rings in detail, we begin with the simpler and more familiar case of differential rings. These examples will help build intuition for

what we might expect from such a functor in the setting of δ-rings.

Definition 2.0.13. Let R be a ring and let $d\colon R \to R$ be such that

$$d(ab) = a \cdot d(b) + b \cdot d(a),$$

then R is a *differential ring*. The category of differential rings will be denoted **DRing**.

There is a forgetful functor **DRing** $\to$ **Ring** which forgets the map d.

Proposition 2.0.14. *The forgetful functor* **DRing** $\to$ **Ring** *has a right adjoint.*

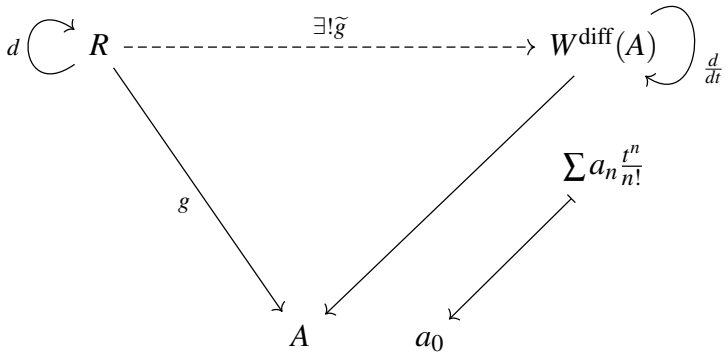
Proof. Given a ring A, define

$$W^{\mathrm{diff}}(A) = \left\{ \sum_{-n \geq 0} a_n \frac{t^n}{n!} \mid a_n \in A \right\},$$

the ring of divided power series of A. The ring structure is given by

$$\frac{t^m}{m!} \cdot \frac{t^n}{n!} = \binom{m+n}{n} \frac{t^{m+n}}{(m+n)!}$$

and the differential map is the usual derivative $\frac{d}{dt}$. Now, suppose R is a differential ring with differential map $d\colon R \to R$, and that there is a map of rings $R \to A$. Then consider



where the map $\widetilde{g}$ is given explicitly by

$$\widetilde{g}(r) = \sum_{n \geq 0} g\left(d^{(n)}(r)\right) \frac{t^n}{n!}.$$

This applies g to the Taylor series of an element $r \in R$. This is indeed a differential ring map:

$$\widetilde{g}(d_R(r)) = \sum_{n\geq 0} g\left(d_R^{(n+1)}(r)\right)\frac{t^n}{n!}$$
$$d_W(\widetilde{g}(r)) = d_W\left(\sum_{n\geq 0} g(d_R^{(n)}(r))\frac{t^n}{n!}\right) = \sum_{n\geq 0} g(d_R^{(n)}(r))\frac{t^{n-1}}{(n-1)!}$$

and after re-indexing we see that these are equal so $\widetilde{g}$ is indeed a morphism of differential rings. Thus, by the universal property of right adjoints, [3], W^{diff} is the right adjoint to the forgetful functor **DRing** $\to$ **Ring**. □

Remark 2.0.15. There is an alternative viewpoint of the above operation that we can take. Consider the map

$$W^{\text{diff}}(A) \xrightarrow{\sim} A \times A \times A \times \cdots$$
$$\sum_{n=0}^{\infty} a_n \frac{t^n}{n!} \mapsto (a_0, a_1, \ldots).$$

Then

$$\frac{d}{dt}((a_0, a_1, \ldots)) = (a_1, a_2, \ldots)$$

is a shift to the left operator and

$$\widetilde{g}(r) = (g(r), g(d(r)), g(d^2(r)), \ldots)$$

where d the the differential map coming from R. Then the ring structure on the infinite product is forced on it, it's a purely syntactic re-expression of the Leibniz rules for $d^{(n)}$:

$$(a_0, a_1, \ldots)\cdot(b_0, b_1, \ldots) = (\ldots, \sum_{i+j=n}\binom{n}{i}a_i b_j, \ldots).$$

Comparing this with the Leibniz rule we find it is identical with a_i playing the role of the ith derivative:

$$d^{(n)}(xy) = \sum_{i+j=n}\binom{n}{i}d^{(i)}(x)d^{(j)}(y).$$

2.0.3 DEFINITION OF $W(A)$

Now we finally return to our original goal of defining the right adjoint of the forgetful functor from $\mathbf{Ring}_\delta$ to **Ring**. We can now mimic the simpler case of differential rings we saw in section 2.0.2.

Definition 2.0.16. Let A be a ring. Then $W(A) = A \times A \times A \times \cdots$ with the ring structure at the nth position given by the Leibniz rules for $\delta^{(n)}$ with respect to addition and multiplication. The additive identity is $0 = (0,0,0,\ldots)$ and the multiplicative identity is $1 = (1,0,0,\ldots)$.

Example 2.0.17. If A is a ring, then the iteration of δ is given by

$$\begin{aligned}\delta^{(2)}(xy) &= \delta\left(x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)\right)\\ &= \text{some polynomial in } x, y, \delta(x), \delta(y), \delta^{(2)}(x), \delta^{(2)}(y).\end{aligned}$$

We also have

$$\begin{aligned}(a_0,a_1,\ldots) + (b_0,b_1,\ldots) &= (a_0+b_0, a_1+b_1 - \sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}a_0^i b_0^{p-i}, \ldots)\\ (a_0,a_1,\ldots)(b_0,b_1,\ldots) &= (a_0b_0, a_0^p b_1 + b_0^p a_1 + pa_1b_1, \ldots).\end{aligned}$$

Proposition 2.0.18. *The forgetful functor* $\mathbf{Ring}_\delta \to \mathbf{Ring}$ *has a right adjoint given by* W.

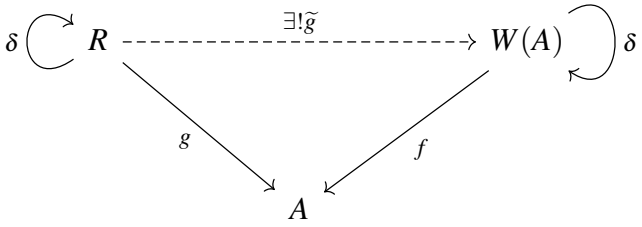
Proof. We proceed as in the case of differential rings. The δ map on W is given by a shift to the left

$$\delta(a_0,a_1,\ldots) = (a_1,a_2,\ldots).$$

Let R be a δ-ring with δ map $\delta_R\colon R \to R$ and suppose there is a map of rings $g\colon R \to A$. There is a natural map

$$\begin{aligned}f\colon W(A) &\to A\\ (a_0,a_1,\ldots) &\mapsto a_0\end{aligned}$$

Consider the diagram

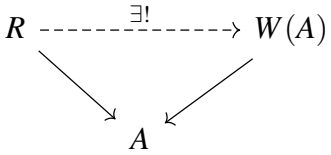


where the map f is given by $f((a_0,a_1,\ldots)) = a_0$. Again, we can explicitly describe $\widetilde{g}$ as

$$\widetilde{g}(r) = (g(r), g(\delta(r)), g(\delta^{(2)}(r)), \ldots)$$

which is a δ-ring map by construction and thus W. We can take the completion of a diagram of this type to be the definition of the right adjoint by [3], and thus W is the right adjoint to the forgetful functor. □

Remark 2.0.19. One important point is the following: let R be a δ-ring and let $X = \mathrm{Spec}(R)$, then if we have a ring map $R \to A$ we get the following diagram by the universal property of W:



Now, note that $X(A) = \mathrm{Hom}_{\mathbf{Ring}}(R,A) = \mathrm{Hom}_{\mathbf{Ring}_\delta}(R, W(A))$ by the above diagram, so we have

$$\begin{array}{ccc} X(A) & \xrightarrow{=} & \mathrm{Hom}_{\mathbf{Ring}}(R,A) \\ \downarrow & & \downarrow = \\ X(W(A)) & \longleftarrow & \mathrm{Hom}_{\mathbf{Ring}_\delta}(R, W(A)) \end{array}$$

This can be thought of as a canonical way of thickening A points to $W(A)$ points.

2.0.4 Truncated Witt Vectors

Here we look at another way to define Witt vectors using truncated Witt vectors. This will be used later on when we want to prove that the forgetful functor $\mathbf{Ring}_\delta \to \mathbf{Ring}$ has both a left and a right adjoint. The 2-truncated Witt vectors in particular are important because

it turns out that having a section from the ring to the 2-truncated Witt vectors is equivalent to a δ-structure. Furthermore, it is also possible to build up the full Witt vectors by taking a limit of the truncated Witt vectors.

Definition 2.0.20. Let R be a ring, the *ring of 2-truncated Witt vectors* is the ring $W_2(R)$, which as a set is R^2. Addition and Multiplication are given by

$$(a_1,b_1)+_W(a_2,b_2)=\left(a_1+b_1,a_2+b_2+\frac{a_1^p+b_1^p-(a_1+b_1)^p}{p}\right)$$

and

$$(a_1,b_1)\cdot_W(a_2,b_2)=(a_1b_1,a_1^pb_2+b_1^pa_2+pa_2b_2)$$

Lemma 2.0.21. *Let A be a ring. Then $W_2(A)$ is also a ring.*

Proof. In $W_2(A)$ the additive unit is $(0,0)$ and the multiplicative unit is $(1,0)$. We now verify the axioms of a commutative ring with 1. Consider the following map of sets:

$$\begin{aligned}\underline{W}\colon W_2(A)&\to A\times A\\(x_0,x_1)&\mapsto(x_0,x_0^p+px_1)\end{aligned}$$

We give the set on the right the product ring structure. Note that this map of sets is compatible with the binary operations $(+,\cdot)$ on both sides. Indeed,

$$\begin{aligned}\underline{W}((x,y)+_W(z,w))&=\underline{W}\left(x+z,y+w+\frac{x^p+z^p-(x+z)^p}{p}\right)\\&=(x+z,x^p+z^p+py+pw)\end{aligned}$$

and

$$\begin{aligned}\underline{W}(x,y)+\underline{W}(z,w)&=(x,x^p+py)+(z,z^p+pw)\\&=(x+z,x^p+z^p+py+pw),\end{aligned}$$

thus $\underline{W}((x,y)+_W(z,w))=\underline{W}(x,y)+\underline{W}(z,w)$. Similarly,

$$\begin{aligned}\underline{W}((x,y)\cdot_W(z,w))&=\underline{W}(xz,x^pw+z^py+pyw)=(xz,x^pz^p+px^pw+pz^py+p^2yw)\\\underline{W}(x,y)\cdot\underline{W}(z,w)&=(x,x^p+py)\cdot(z,z^p+pw)=(xz,x^pz^p+px^pw+pz^py+p^2yw)\end{aligned}$$

so we also have $\underline{W}((x,y)\cdot_W(z,w)) = \underline{W}(x,y)\cdot\underline{W}(z,w)$.

If the map $\underline{W}$ were injective, then we could deduce the identities that we have to verify from the known identities on the right. Indeed, suppose we want to show that $w +_W w' = w' +_W w$. Then we have

$$\underline{W}(w +_W w') = \underline{W}(w) + \underline{W}(w') = \underline{W}(w') + \underline{W}(w) = \underline{W}(w' +_W w),$$

then since $\underline{W}$ is injective this implies that $w +_W w' = w' +_W w$. This map is injective if A is p-torsion free.

Thus we can choose a ring that is p-torsion free to get the result. For our ring A we can choose a polynomial ring that surjects onto A, one choice is $\mathbb{Z}_{(p)}[x_a : a \in A]$. Then we have a map

$$\begin{aligned} f : \mathbb{Z}_{(p)}[x_a : a \in A] &\twoheadrightarrow A \\ x_a &\mapsto a \end{aligned}$$

and on the underlying ring $\mathbb{Z}_{(p)}$ we have the natural map given by the fact that it is the initial object in $\mathbf{Ring}_\delta$. Now consider the map

$$\begin{aligned} \widetilde{f} : W_2\left(\mathbb{Z}_{(p)}[x_a : a \in A]\right) &\twoheadrightarrow W_2(A) \\ (x,y) &\mapsto (f(x), f(y)) \end{aligned}$$

This map respects the operations in the two rings, i.e., $\widetilde{f}((x,y) +_{W_{\mathbb{Z}}} (z,w)) = \widetilde{f}((x,y)) +_{W_A} \widetilde{f}(z,w))$ and $\widetilde{f}((x,y)\cdot_{W_{\mathbb{Z}}}(z,w)) = \widetilde{f}((x,y))\cdot_{W_A}\widetilde{f}(z,w))$. Letting $\mathbb{Z}_{(p)}[S] = \mathbb{Z}_{(p)}[x_a : a \in A]$, gives us a diagram

$$\begin{array}{ccc} W_2(\mathbb{Z}_{(p)}[S]) & \xrightarrow{\widetilde{f}} & W_2(A) \\ \downarrow{\scriptstyle \underline{W}_{\mathbb{Z}_{(p)}}} & & \downarrow{\scriptstyle \underline{W}_A} \\ \mathbb{Z}_{(p)}[S]\times\mathbb{Z}_{(p)}[S] & \twoheadrightarrow & A\times A \end{array}$$

So if we want to prove that $w +_{W_A} w' = w' +_{W_A} w$, then we choose $\widetilde{a} \in f^{-1}(a)$ and $\widetilde{a'} \in f^{-1}(a')$. Then letting $\underline{W} = \underline{W}_{\mathbb{Z}_{(p)}}$

$$\underline{W}(\widetilde{a} +_{W_{\mathbb{Z}}} \widetilde{a'}) = \underline{W}(\widetilde{a}) + \underline{W}(\widetilde{a'}) = \underline{W}(\widetilde{a'}) + \underline{W}(\widetilde{a}) = \underline{W}(\widetilde{a'} +_{W_{\mathbb{Z}}} \widetilde{a}).$$

Thus since $\underline{W}$ is injective since $\mathbb{Z}_{(p)}[x_a : a \in A]$ is torsion free, and so $\widetilde{a} +_{W_{\mathbb{Z}}} \widetilde{a'} = \widetilde{a'} +_{W_{\mathbb{Z}}} \widetilde{a}$ and thus

$$f(\widetilde{a} +_{W_{\mathbb{Z}}} \widetilde{a'}) = f(\widetilde{a'} +_{W_{\mathbb{Z}}} \widetilde{a}) \implies f(\widetilde{a}) +_{W_A} f(\widetilde{a'}) = f(\widetilde{a'}) +_{W_A} f(\widetilde{a})$$

and since we chose $\widetilde{a}$ and $\widetilde{a'}$ to be pre-images of a and a' we get that $a +_{W_A} a' = a' +_{W_A} a$. Thus proof can be repeated to get the other ring axioms such as associativity and distributivity. □

Now that we know $W_2(R)$ is a ring, we see that the map

$$\begin{aligned} w_0 : W_2(R) &\to R \\ (x,y) &\mapsto x \end{aligned}$$

is a ring homomorphism. We also note that there is a very strong similarity between the definition of addition and multiplication on $W_2(R)$ and the definition of a δ-structure. We see that if we replace (a_1,b_1) and (a_2,b_2) with $(x,\delta(x))$ and $(y,\delta(y))$ we have that

$$(x,\delta(x)) +_W (y,\delta(y)) = (x+y, \delta(x+y)).$$

Similarly, for multiplication we have

$$(x,\delta(x)) \cdot_W (y,\delta(y)) = (xy, \delta(xy)).$$

This observation leads us to the following lemma.

Lemma 2.0.22. *The datum of a δ-structure on a ring R is equivalent to the datum of a ring homomorphism $R \to W_2(R)$ which composes with w_0 to the identity.*

Proof. Given a δ-structure on R, we have a ring homomorphism

$$\begin{aligned} R &\to W_2(R) \\ x &\mapsto (x,\delta(x)) \end{aligned}$$

and this map composes with w_0 to the identity. Conversely, suppose we have a section $g : R \to W_2(R)$, with $g(x) = (g_1(x), g_2(x))$ which composes with w_0 to the identity, i.e., $g_1(x) = x$. Then we can just define $\delta(x) = g_2(x)$. □

Now we want to define higher truncated Witt vectors. There are a couple ways to do this. We can just truncate the ring $W(A)$ so that if $(a,b,c),(a',b',c') \in W_3(A)$, then

$$(a,b,c) \cdot_W (a',b',c') = (aa', a^p b' + a'^p b + pbb', f(a,a',b,b',c,c'))$$

where $f(a,a',b,b',c,c')$ is the polynomial obtained by applying δ to $a^p b' + a'^p b + pbb'$ and replacing $\delta(a)$ with b, $\delta(a')$ with b', $\delta(b)$ with c, and $\delta(b')$ with c'.

We can do this for any n, by applying δ to the next coordinate to obtain the rings $W_n(A)$. This is used in the following way: suppose we want to compute $W(A)$. Then, if we can compute $W_n(A)$ for all $n \geq 2$, then we can write

$$W(A) = \lim_{\leftarrow} W_n(A).$$

A simple example is that if we know that $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$, then we quickly find that

$$W(\mathbb{F}_p) = \lim_{\leftarrow} W_n(\mathbb{F}_p) = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

2.0.5 Adjoint Functors

Here we quickly prove why the forgetful functor $\mathbf{Ring}_\delta \to \mathbf{Ring}$ has both a right and a left adjoint.

Lemma 2.0.23. *The category* $\mathbf{Ring}_\delta$ *has all limits and colimits and they commute with the forgetful functor to* **Ring**.

Proof. We start with the existence of limits. Let $F : J \to \mathbf{Ring}_\delta$ be a functor from a small category J. We can compose F with the forgetful functor $\mathbf{Ring}_\delta \to \mathbf{Ring}$ to get a functor $F : J \to \mathbf{Ring}$. Since limits exist in **Ring** we know that there exists a limit (L,π) as rings. We need to show that there is a δ-structure on (L,π). We do this using the projections. The element $\delta_L(x)$ for some $x \in L$ is uniquely defined by $\pi_X(\delta_L(x)) = \delta_X(\pi_X(x))$ for all X in J, because it holds that

$$F(f) \circ \delta_X \circ \pi_X = \delta_Y \circ F(f) \circ \pi_X = \delta_Y \circ \pi_Y.$$

This is the only δ-structure such that the π_X are δ-maps and thus the only possible δ-structure the limit can have to exist in the category of δ-rings. The properties of the δ-structure directly follow from the fact that the properties are all fulfilled in all the $F(X)$.

Now we look at the universal property. Let (A, δ_A) be a δ-ring with δ-maps $\varphi_X : A \to F(X)$. Then there is a unique map of rings $\varphi : A \to L$ and it is left to check that this map is also a δ-map. For this we can see that for every X in J it holds

$$\pi_X \circ \varphi \circ \delta_A = \varphi_X \circ \delta_A = \delta_X \circ \varphi_X = \delta_X \circ \pi_X \circ \varphi = \pi_X \circ \delta_L \circ \varphi$$

and thus $\varphi \circ \delta_A = \delta_L \circ \varphi$ is valid, i.e., the diagram

$$\begin{array}{ccc} A & \xrightarrow{\delta_A} & A \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ L & \xrightarrow[\delta_L]{} & L \end{array}$$

commutes.

Now, for the colimit we use the description of a δ-structure by constructing a section from the ring of truncated Witt vectors. Let $F : J \to \mathbf{Ring}_\delta$ be a functor from a small category to the category of δ-rings. Thus, for every X in J there is a δ-structure on $F(X)$. Composed with the forgetful functor from $\mathbf{Ring}_\delta \to \mathbf{Ring}$ we get a functor from J to the category of commutative rings, where the colimit of the given diagram exists. Thus we get the colimit (C, ψ) for rings. Since every $F(X)$ for some object X in J is a δ-ring, there is a homomorphism $F(X) \to W_2(F(X))$, which is the identity in the first component. Using the functorality of colimits there is a homomorphism $g : C \to D$, where (D, ψ') denotes the colimit of the diagram $W_2 \circ F : J \to \mathbf{Ring}$. Thus, it holds that the diagram

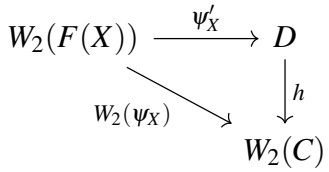
$$\begin{array}{ccc} F(X) & \xrightarrow{\psi_X} & C \\ {\scriptstyle w_X}\downarrow & & \downarrow{\scriptstyle g} \\ W_2(F(X)) & \xrightarrow[\psi'_X]{} & D \end{array}$$

commutes, where w_X denotes the section $F(X) \to W_2(F(X))$, which we get out of the δ-structure on $F(X)$.

Additionally, for every X in J there is a natural morphism $\psi_X : F(X) \to C$. Using the functorality of $W_2(-)$ we obtain a morphism

$$W_2(\phi_X) : W_2(F(X)) \to W_2(C).$$

Now, since D is a colimit, there is a morphism $h\colon D \to W_2(C)$, which satisfies $h \circ \psi'_X := W_2(\psi_X)$ for all X, i.e., the diagram



commutes. Altogether, we obtain the map $w = h \circ g\colon C \to W_2(C)$. Composed with the projection on the first component $p_1\colon W_2(C) \to C$ this is the identity on C, because for every X in J we have

$$p_1 \circ w \circ \psi_X = p_1 \circ h \circ g \circ \psi_X = p_1 \circ h \circ \psi'_X \circ w_X = p_1 \circ W_2(\psi_X) \circ w_X = \psi_X$$

where the second and third equalities hold from the previous two diagrams and the last equality comes from the fact that w_X is the identity on the first component. Thus since we have $p_1 \circ w = \mathrm{id}_C$, we have a δ-structure on the colimit C.

The ψ_X maps are also δ-maps because they fulfill $h \circ g \circ \psi_X = W_2(\psi_X) \circ w_X$ and thus also commute with the δ-structures.

Now, the pair (C, ψ) also fulfills the universal property of a colimit in $\mathbf{Ring}_\delta$. Indeed, let (A, δ) be a δ-ring and $\varphi_X\colon F(X) \to A$ δ-maps such that for every $f\colon X \to Y$ in J it holds that $\varphi_Y \circ F(f) = \varphi_X$. Since (C, ψ) is a colimit in **Ring** there is a unique homomorphism of rings $\varphi\colon C \to A$ such that $\varphi \circ \psi_X = \varphi_X$ for all X in J. In fact, this is a δ-map because for every X in J it holds that

$$\begin{aligned} w_A \circ \varphi \circ \psi_X &= w_A \circ \varphi_X \circ w_A \\ &= W_2(\varphi_X) \circ w_X \\ &= W_2(\varphi \circ \psi_X) \circ w_X \\ &= W_2(\varphi) \circ W_2(\psi_X) \circ w_X \\ &= W_2(\varphi) \circ w \circ \psi_X \end{aligned}$$

and so $w_A \circ \varphi = W_2(\varphi) \circ w$. Thus φ commutes with the sections w and w_A and also has to commute with the δp-structures. □

Now knowing that $\mathbf{Ring}_\delta$ has all limits and colimits and that they commute with the

forgetful functor to **Ring** we can just apply the general adjoint functor theorem to see that the forgetful functor has both a left and a right adjoint.

The following discussion comes from [11], [12, §4.6], and [4, Exercises 2.5.12, 2.5.14]. We first need a few definitions before stating the theorem.

Definition 2.0.24. A category $\mathbf{C}$ is *complete* if it has all small limits, i.e., if every small diagram

$$F : D \to C$$

where D is a small category has a limit in $\mathbf{C}$. Similarly, we say a category is cocomplete if it contains all colimits.

Example 2.0.25. Most of the most familiar categories are complete, **Set**, **Grp**, **Top**, etc. And as shown in Lemma 2.0.23, the category $\mathbf{Ring}_\delta$ has all limits and colimits.

There are two versions of the general adjoint functor that we need, one for the left adjoint and one for the right.

Theorem 2.0.26 (General Adjoint Functor Theorem - Right)**.** *Let $F : \mathbf{C} \to \mathbf{D}$ be a functor. If $\mathbf{C}$ is complete, locally small, and satisfies the solution set condition: for every $y \in \mathbf{D}$ there is a set of elements $x_i \in \mathbf{C}$ such that for any $x \in \mathbf{C}$, any morphism $f : F(x) \to y$ factors as $f_i \circ F($g for some i, some $g : x \to x_i$ and some $f_i : F(x_i) \to F(y)$.*

Theorem 2.0.27 (General Adjoint Functor Theorem - Left)**.** *Let $F : \mathbf{C} \to \mathbf{D}$ be a functor. If $\mathbf{C}$ is cocomplete, locally small, and satisfies the solution set condition: for every $y \in \mathbf{D}$, there is a set of element $x_i \in \mathbf{C}$ such that for any $x \in C$, any morphism $f : y \to F(x)$ factors as $F(g) \circ f_i$ for some i, some $f_i : y \to F(x_i)$ and some $g : x_i \to x$.*

Example 2.0.28. Now we consider our situation with the forgetful functor $\mathbf{Ring}_\delta \to$ **Ring**. We first show that it satisfies the solution set condition for the left adjoint. Let $A \in \mathbf{Ring}, B \in \mathbf{Ring}_\delta$ and consider $f : A \to B$ as a map in **Ring**. Now, let

$$\Omega = \{A_i \in \mathbf{Ring} \mid |A_i| \leq \max\{|A|, \aleph_0\}\}.$$

Then the δ-subring of B generated by $f(A)$ has cardinality at most $\max\{|A|, \aleph_0\}$, so if we let the δ-subring generated by $f(A)$ be called A', then $A' \in \Omega$. Then we have

$$A \to A' \to B$$

and we can factor our map.

Example 2.0.29. Now for the right adjoint, let $A \to B$ with $A \in \mathbf{Ring}_\delta$ and $B \in \mathbf{Ring}$. Let

$$\Omega = \left\{ A_i \in \mathbf{Ring}_\delta \mid |A_i| \leq 2^{\max\{|B|, \aleph_0\}} \right\}.$$

Let I be the set of $x \in A$ for which $\delta^m(x) \in \ker f$ for all $m \geq 0$. Then I is a δ-stable ideal of A and the map

$$\begin{aligned} A/I &\to B \times B \times \cdots \\ x &\mapsto (f(x), f(\delta(x), f(\delta^2(x), \ldots) \end{aligned}$$

is injective. Thus $|A/I| \leq 2^{\max\{|B|, \aleph_0\}}$ and so $A/I \in \Omega$ and we have

$$A \to A/I \to B$$

where the last map is induced by f.

2.0.6 Left Adjoint

Now that we have investigated the right adjoint to the forgetful functor

$$\mathbf{Ring}_\delta \to \mathbf{Ring}$$

we will now take a look at the left adjoint. Typically, left adjoints to the forgetful functor are used to obtain a "free" object in the category. Having such a free object can be very useful. One way we will use it is as an object that represents the Witt vectors functor W.

Similar to the case of the right adjoint we first consider the analogous case with differential rings which was explained in [13].

Proposition 2.0.30. *The forgetful functor* $\mathbf{DRing} \to \mathbf{Ring}$ *has a left adjoint, denoted* $D \odot -$*:*

$$\begin{array}{c} \mathbf{DRing} \\ {\scriptstyle D\odot -}\uparrow \downarrow \uparrow {\scriptstyle W^{\mathrm{diff}}} \\ \mathbf{Ring} \end{array}$$

Proof. We first define D as the free differential ring on one generator:

$$D = \mathbb{Z}[e, d, d^{(2)}, d^{(3)}, \ldots]$$

where d is the derivative of e. Now, let $\xi \in D$ and let R be a differential ring, so

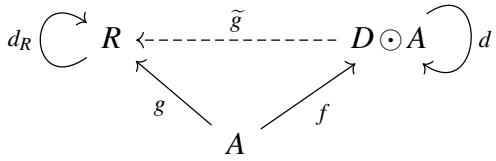
$$\xi : R \to R$$

induces a map and we get $D \xrightarrow{\sim} \{\text{natural 1-ary operations on differential rings}\}$. Then

$$D \odot A = \mathbb{Z}[d^{(n)}(a) \mid a \in A, n \geq 0] / \left(d^{(n)}(ab) = \sum_{i+j=n} \binom{n}{i} d^{(i)}(a), d^{(j)}(b), \ldots \right).$$

There is a canonical map

$$\begin{aligned} f : A &\to D \odot A \\ a &\mapsto a. \end{aligned}$$



the map $\widetilde{g}$ is given by

$$g\left(\sum b_{n,a} d^{(n)}(a)\right) = \sum b_{n,a} g(d^{(n)}(a)).$$

Thus $D \odot -$ is a left adjoint. □

Now we turn our attention back to Witt vectors.

Definition 2.0.31. Let $\Delta = \mathbb{Z}[e, \delta, \delta^{(2)}, \delta^{(3)}, \ldots]$ be the free δ-ring on one generator e. The δ-structure on this ring is given by

$$\delta(\delta^{(n)}) = \delta^{(n+1)}.$$

With this δ-structure we also inherit a Frobenius lift which is given by

$$\phi(\delta^{(n)}) = \left(\delta^{(n)}\right)^p + p\delta^{(n+1)}$$

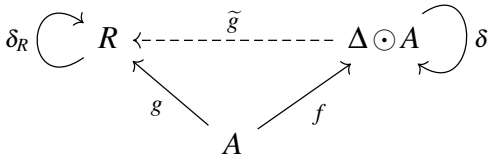
Now, analogously to the case with differential rings, we make the following definition.

Definition 2.0.32. Let A be a ring. Define $\widehat{A} = \mathbb{Z}[\delta^{(n)}(a) \mid a \in A, n \geq 0]/$ and then let

$$\Delta \odot A = \widehat{A} / \left(\delta^{(n)}(ab) = \text{Leibniz rule in } \delta^{(i)}(a), \delta^{(j)}(b), \delta^n(a+b) = \cdots, \delta^{(n)}(0) = 0, \delta^{(n)}(a) = 0\right)$$

Proposition 2.0.33. *The forgetful functor* $\mathbf{Ring})_\delta \to \mathbf{Ring}$ *has a left adjoint given by* $\Delta \odot -$.

Proof. Suppose A is a ring, R a δ-ring and suppose there is a map of rings $A \to R$. Consider the following diagram



where the map $\widetilde{g}$ is given by

$$\widetilde{g}\left(\sum b_{n,a}\delta^{(n)}(a)\right) = \sum b_{n,a} g(\delta^{(n)}(a)).$$

And thus $\Delta \odot -$ is a left adjoint to the forgetful functor. □

Remark 2.0.34. One of the other important uses of Δ is that it represents W, i.e.,

$$\begin{aligned} \mathrm{Hom}(\Delta, A) \xrightarrow{\sim} W(A) &= \prod_{\mathbb{N}} A \\ \alpha &\mapsto (\alpha(e), \alpha(\delta), \alpha(\delta^{(2)}), \ldots). \end{aligned}$$

Remark 2.0.35. It is also common to denote the this free δ-ring as

$$\mathbb{Z}\{y\} = \mathbb{Z}[y_0, y_1, \ldots]$$

This notation will be used in the following section.

2.0.7 GHOST COORDINATES

The ghost coordinates are used to do computations in $W(A)$. While the δ-definitions are very useful to prove some of the statements we are interested in, it is difficult to do exact computations. This is where the ghost coordinates are useful.

We now take a look at the ring map $W(A) \to \prod_{n\in\mathbb{N}} A$, where we consider $\prod_{n\in\mathbb{N}} A$ with componentwise addition and multiplication. As sets, these are equal, but the ring structures differ. We need a few lemmas before we are ready to tackle this.

Remark 2.0.36. [4, Remark 3.1.2] One identity we will use throughout this section is the following:

$$(x+py)^p \cong x^p \pmod{p^2 y}$$

Lemma 2.0.37. *[4, Lemma 3.1.3] In the ring $\mathbb{Z}\{y\}$ there exist elements*

$$x_n \in y_n + (y_1,\dots,y_{n-1})\mathbb{Z}[y_0,\dots,y_{n-1}]$$

such that $x_0 = y_0, x_1 = y_1$ and

$$\phi^n(x_0) = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n.$$

Proof. Suppose we have already defined $x_0,\dots,x_{n-1} \in \mathbb{Z}\{y\}$ satisfying the required relation. Now we use Remark 2.0.36 to write

$$\begin{aligned}
\phi^n(x_0) &= \phi(\phi^{n-1}(x_0)) \\
&= \phi(x_0)^{p^{n-1}} + \cdots + p^{n-1}\phi(x_{n-1}) \\
&= (x_0^p + p*)^{p^{n-1}} + \cdots + p^{n-2}(x_{n-2}^p + p*)^p + p^{n-1}\phi(x_{n-1}) \\
&= x_0^{p^n} + \cdots p^{n-2}x_{n-2}^{p^2} + p^{n-1}(x_{n-1}^p + p\delta(x_{n-1})) + p^n * \\
&= x_0^{p^n} + \cdots + p^{n-2}x_{n-2}^{p^2} + p^{n-1}x_{n-1}^p + p^n(\delta(x_{n-1}) + *)
\end{aligned}$$

where each $*$ denotes a quantity in $(y_1,\dots,y_{n-1})\mathbb{Z}[y_0,\dots,y_{n-1}]$. We thus can take

$$x_n = \delta(x_{n-1}) + *.$$

Now, since $x_{n-1} - y_{n-1} \in \mathbb{Z}[y_0, \ldots, y_{n-2}]$ we have

$$\begin{aligned}\delta(x_{n-1}) &= \delta(y_{n-1} + x_{n-1} - y_{n-1}) \\ &= \delta(y_{n-1}) + \delta(x_{n-1} - y_{n-1}) + \frac{1}{p}(y_{n-1}^p + (x_{n-1} + y_{n-1})^p - x_{n-1}^p) \\ &= y_n + *\end{aligned}$$

and so $x_n - y_n = * \in (y_1, \ldots, y_{n-1})\mathbb{Z}[y_0, \ldots, y_{n-1}]$. □

Corollary 2.0.38. *Let $(x_n)_{n\in\mathbb{N}}$ be those defined in Lemma 2.0.37. For $w_n = \sum_{m=0}^{n} p^m x_m^{n-m} \in \mathbb{Z}\{y\}$, we have*

$$\phi^n(w_n) = w_{n+m}.$$

Proof. By Lemma 2.0.37 we have $w_m = \phi^m(x_0)$ and so

$$\phi^n(w_m) = \phi^n(\phi^m(x_0)) = \phi^{n+m}(x_0) = w_{n+m}.$$

□

Now we're ready to define the ghost map.

Definition 2.0.39 (Ghost Map)**.** Define the elements w_n as in Corollary 2.0.38. These define a set-theoretic map

$$\begin{aligned} w\colon W(A) &\to \prod_{\mathbb{N}} A \\ (x_n)_{n=0}^{\infty} &\mapsto \left(\sum_{m=0}^{n} p^m x_m^{p^{n-m}} \right)_{n=0}^{\infty} \end{aligned}$$

which we call the *ghost map*.

Remark 2.0.40. The ghost map is neither injective nor surjective in general. Injectivity requires there to be no p-torsion, and the map can be surjective if A is p-divisible. Despite this, we will still refer to the terms of $w(x) = (w_0, w_1, \ldots)$ as the *ghost coordinates* of x. By Corollary 2.0.38, the ghost coordinates of $\phi^n(x)$ are $(w_n, w_{n+1}, \ldots)$.

Definition 2.0.41 (Verschiebung)**.** For any ring A, the *Verschiebung* map $V\colon W(A) \to W(A)$ is defined by

$$V(x_0, x_1, \ldots) = (0, x_0, x_1, \ldots)$$

In ghost coordinates this corresponds to the map

$$(x_0, x_0^p + px_1, x_0^{p^2} + px_1^p + p^2x_2, \ldots) \mapsto (0, px_1, px_0^p + p^2x_1, px_0^{p^2} + p^2x_1^p + p^3x_2, \ldots),$$

i.e., $(w_0, w_1, w_2, \ldots) \mapsto (0, pw_0, pw_1, pw_2, \ldots)$.

We also note that the Verschiebung map is additive and that $\phi \circ V$ is multiplication by p.

One important use of the Verscheibung map is the following identity:

$$W(A)/V^n(W(A)) \cong W_n(A).$$

By taking the quotient with the nth iteration of the Verscheibung map, we end up only with the first n coordinates being nonzero, which is isomorphic to the nth truncated Witt vectors.

2.0.8 Computing Examples

In this section we compute examples, taking bits and pieces from different sources like Kedlaya, Borger, Serre.

Example 2.0.42. We want to find $W_n(\mathbb{F}_p)$. This will help us compute $W(\mathbb{F}_p)$. A direct way to see this, is to consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_1(\mathbb{F}_p) & \xrightarrow{a_1 \mapsto (0,a_1)} & W_2(\mathbb{F}_p) & \xrightarrow{(a_0,a_1)\mapsto a_0} & W_1(\mathbb{F}_p) & \longrightarrow & 0 \\ & & \cong\downarrow & & & & \downarrow\cong & & \\ 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{a \mapsto pa} & \mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where the rows are exact. Then we have a map

$$\begin{aligned} f\colon W_2(\mathbb{F}_p) &\to \mathbb{Z}/p^2\mathbb{Z} \\ (a_0, a_1) &\mapsto a_0^p + pa_1 \end{aligned}$$

Note that this is a ring homomorphism. Indeed,

$$f(a_0, a_1) + f(b_0, b_1) = a_0^p + pa_1 + b_0^p + pb_1$$

while

$$\begin{aligned} f((a_1,a_1)+(b_0,b_1)) &= f\left(a_0+b_0, a_1+b_1 - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} a_0^i b_0^{p-i}\right) \\ &= (a_0+b_0)^p + p(a_1+b_1) - \sum_{i=1}^{p-1} \frac{p!}{i!(p-i)!} a_0^i b_0^{p-i} \\ &= a_0^p + b_0^p + pa_1 + pb_1. \end{aligned}$$

Since we are working modulo p^2. So $f(a_0,a_1)+f(b_0,b_1) = f((a_0,a_1)+(b_0,b_1))$. Similarly,

$$f(a_0,a_1)f(b_0,b_1) = (a_0^p + pa_1)(b_0^p + pb_1) = a_0^p b_0^p + pa_1 b_0^p + pa_0^p b_1.$$

and

$$f((a_0,a_1)(b_0,b_1)) = f(a_0b_0, a_0^p b_1 + b_0^p a + pa_1b_1) = a_0^p b_0^p + pa_1 b_0^p + pa_0^p b_1.$$

So f is indeed a homomorphism. Lastly, we can see that it is an isomorphism from the five lemma.

To compute for higher n, start by choosing a lift $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, that takes $\overline{a} \mapsto a$. Then we have a map,

$$\begin{aligned} \phi_n &\colon W_n(\mathbb{F}_p) \to \mathbb{Z}/p^n\mathbb{Z} \\ (\overline{a}_0, \ldots, \overline{a}_{n-1}) &\mapsto (a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-1}a_{n-1}) + p^n\mathbb{Z} \end{aligned}$$

which is bijective and hence we get the isomorphism.

Example 2.0.43. Now, knowing that $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$, we see that

$$W(\mathbb{F}_p) = \varprojlim W_n(\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

Example 2.0.44. There is another way to compute $W(\mathbb{F}_p)$. We can represent a p-adic integer using the Teichmüler character $\omega \colon \mathbb{F}_p \to \mathbb{Z}_p^\times \cup \{0\}$ which sends $a \in \mathbb{F}_p^\times$ to the unique $(p-1)st$ root of unity in $\mathbb{Z}_p$ which reduces to a modulo p. This map has the

property that $\omega(a)^p = \omega(a)$ for any $a \in \mathbb{F}_p^\times$. Thus, instead of writing

$$x = \sum_{i=0}^{\infty} a_i p^i$$

with $a_i \in \{0, 1, \ldots, p-1\}$ for $x \in \mathbb{Z}_p$, we can write

$$x = \sum_{i=0}^{\infty} \omega(a_i) p^i.$$

Adding up the coefficients yields polynomials α_n with coefficients such that

$$a + b = (\alpha_0(a_0, b_0), \alpha_1(a_0, b_0, a_1, b_1), \ldots).$$

We can repeat the same thing for multiplication to find that there are polynomials π_n such that

$$ab = (\pi_0(a_0, b_0), \pi_1(a_0, b_0, a_1, b_1), \ldots).$$

This defines a ring structure on $\prod_{n \geq 0} \mathbb{F}_p \cong \mathbb{Z}_p$ and $\prod_{n \geq 0} \mathbb{F}_p$ with this ring structure is $W(\mathbb{F}_p)$.

Example 2.0.45. We would like to compute $W(\mathbb{F}_p[T])$. We will use the following Theorem:

Theorem 2.0.46. *Let A be a p-adically complete and separated ring such that A/pA is perfect. Then*

$$A \cong W(A/pA)$$

Proof. See [14, Corollaire 1.3.23] □

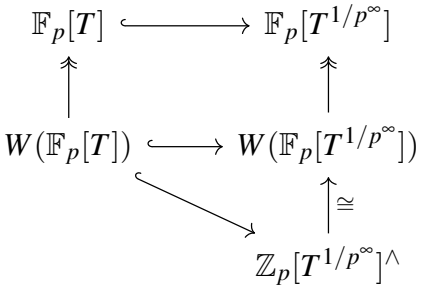
Now, take $A = \mathbb{Z}_p[T^{1/p^\infty}]^\wedge$, the p-adic completion of $\mathbb{Z}_p[T^{1/p^n}; n \geq 0]$. Then

$$A/pA = \mathbb{F}_p[t^{1/p^\infty}],$$

which is a perfect ring in characteristic p. Thus we have an isomorphism

$$\begin{gathered} A = \mathbb{Z}_p[T^{1/p^\infty}] \xrightarrow{\cong} W(A/pA) = W(\mathbb{F}_p[T^{1/p^\infty}] \\ T^{1/p} \mapsto (T^{1/p}, 0, 0, \ldots) \end{gathered}$$

Now we come back to the original goal of calculating $W(F_p[T])$. We have the following diagram



Thus we see that $W(\mathbb{F}_p[T])$ is topologically generated by the elements V(Teichmüller elements) and $V(T) = pT^{1/p}$.

Example 2.0.47. We want to compute $W(\mathbb{F}_p[x])$. Note that

$$W_n(\mathbb{F}_p[x]) \cong W(\mathbb{F}_p[x])/V^n(\mathbb{F}_p[x])$$

where V is the *Verscheibung* map

$$V(a_0, a_1, \ldots) = (0, a_1, \ldots).$$

So the image of V^n is the set of elements divisible by p^n. This gives

$$W_2(\mathbb{F}_p[x]) = (\mathbb{Z}/p^2\mathbb{Z})[x, px^{1/p}].$$

Indeed, we get the elements $px^{1/p}$ since $\phi \circ V$ is multiplication by p, so

$$V(x) = p\phi^{-1}(x) = px^{1/p}.$$

We can extend this to get $W_n(\mathbb{F}_p[x]) = (\mathbb{Z}/p^n\mathbb{Z})[x, px^{1/p}, p^2x^{1/p^2}, \ldots, p^{n-1}x^{1/p^{n-1}}]$. Then

$$W(\mathbb{F}_p[x]) = \lim_n W_n(\mathbb{F}_p[x]) = \lim_n (\mathbb{Z}/p^n\mathbb{Z})[x, px^{1/p}, p^2x^{1/p^2}, \ldots, p^{n-1}x^{1/p^{n-1}}] = \widehat{\mathbb{Z}_p[x^{1/p^\infty}]}$$

where the completion is with respect to the p-adic topology.

Example 2.0.48. Similarly, we can compute $W(\mathbb{F}_p[T, T^{-1}])$ using the same method as when we computed $W(\mathbb{F}_p[T])$. Let $A = \mathbb{Z}_p[T^{1/p^\infty}, T^{-1/p^\infty}]^\wedge$, the p-adic completion of

$\mathbb{Z}_p[T^{1/p^n}, T^{-1/p^n}; n \geq 0]$. Then

$$A/pA = \mathbb{F}_p[T^{1/p^\infty}, T^{-1/p^\infty}]$$

is perfect, so again we have an isomorphism

$$\begin{gathered}\mathbb{Z}_p[T^{1/p^\infty}, T^{-1/p^\infty}]^\wedge \cong A \xrightarrow{\cong} W(A/pA) = W(\mathbb{F}_p[T^{1/p^\infty}, T^{-1/p^\infty}]) \\ T^{1/p} \mapsto (T^{1/p}, 0, 0, \ldots) \\ T^{-1/p} \mapsto (T^{1/p}, 0, 0, \ldots).\end{gathered}$$

And thus we get a diagram

$$\begin{array}{ccc} \mathbb{F}_p[T, T^1] & \hookrightarrow & \mathbb{F}_p[T^{1/p^\infty}, T^{-1/p^\infty}] \\ \uparrow\!\!\uparrow & & \uparrow\!\!\uparrow \\ W(\mathbb{F}_p[T, T^{-1}]) & \hookrightarrow & W(\mathbb{F}_p[T^{1/p^\infty}, T^{-1/p^\infty}]) \\ & \searrow & \downarrow \cong \\ & & \mathbb{Z}_p[T^{1/p^\infty}, T^{-1/p^\infty}]^\wedge \end{array}$$

and like before we find that $W(\mathbb{F}_p[T, T^{-1}])$ is topologically generated by the Verscheibung applied to the Teichmüller elements, as well as $V(T) = pT^{1/p}$ and $V(T^{-1}) = pT^{-1}$.

Example 2.0.49. Now we want to compute $W(\overline{\mathbb{F}}_p)$.

We make use the following theorem [6, §2.5 Theorem 3].

Theorem 2.0.50. *For every perfect field k of characteristic p, there exists a complete discrete valuation ring and only one (up to unique isomorphism) which is absolutely unramified and has k as its residue field.*

The ring in the statement is defined to be exactly $W(k)$. However, we also know that $\mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{unr}}}}$, the ring of integers of the p-adic completion of the maximal unramified extension of Q_p is also a complete DVR, which is unramified and has $\overline{\mathbb{F}}_p$ as its residue field. Thus

$$W(\overline{\mathbb{F}}_p) \cong \mathcal{O}_{\widehat{\mathbb{Q}_p^{\mathrm{unr}}}}.$$

Since $W(K)$ is the degree n unramified extension of $\mathbb{Q}_p$ when K is the degree n extension

of $\mathbb{F}_p$, we see that taking the Witt vectors of the closure of $\overline{F}_p$ we should get end up with a composite of all the unramified extensions of $\mathbb{Q}_p$. Indeed, we have

$$W(\overline{\mathbb{F}}_p) = \mathscr{O}_{\widehat{\mathbb{Q}_p^{\text{unr}}}}$$

where $\widehat{\mathbb{Q}_p^{\text{unr}}}$ is the p-adic completion of the maximal unramified extension of $\mathbb{Q}_p$. We have to take the p-adic completion because taking the Witt vectors always results in a compete ring.

For the next example we will first need an example:

Definition 2.0.51 (Strict p-ring)**.** A ring R is called a *strict p-ring* if it is p-adically complete, p-torsion free, and such that R/pR is a perfect $\mathbb{F}_p$-algebra.

Theorem 2.0.52 ([6] Theorem 5 p.39)**.** *For every perfect ring k of characteristic p, there exists a unique strict p-ring $W(k)$ with residue ring k.*

Example 2.0.53 ([6] Theorem 5, p. 39)**.** t We have that

$$W\left(\mathbb{F}_p[x^{1/p^\infty}]\right) \cong \mathbb{Z}_p[x^{1/p^\infty}]^\wedge.$$

Indeed, since $\widehat{\mathbb{Z}}[x^{1/p^\infty}]$ is a strict p-ring with $\mathbb{F}_p[x^{1/p^\infty}]$ as its residue field we see that the above must be true.

3

Étale Topology

3.1 Étale Topology

In this section, we provide a brief overview of the étale topology, which will serve as the foundational setting for the remainder of this thesis.

The classical Zariski topology on a scheme is very coarse—most open sets are dense—which can be limiting in many contexts. To obtain a finer topology, we move beyond the traditional notion of open subsets and instead consider étale morphisms $U \to X$ as generalized "open sets" of a scheme X. We still want to mimic the category of open sets on a topological space, and to do this we still want a notion of intersection. The natural way to do this is to replace intersections of open sets with fiber products since in the poset category of open sets on a topological space, intersections are fiber products.

Étale morphisms behave well under base change and composition, which ensures that our construction has the desired stability properties. Once we have defined the étale topology and introduced notions of covers and finite intersections, we will be in a position to define sheaves in this new setting.

This chapter is organized as follows. Section 5.1 develops the necessary definitions and foundational results on étale morphisms, along with several illustrative examples. We then introduce the concept of Grothendieck topologies and compare the Zariski and étale sites. Finally, we explore representable functors in the context of sheaves and provide a

definition of elliptic curves over sheaves.

3.1.1 Étale Maps

Definition 3.1.1. Let A be an R-algebra. Let C be an R-algebra with an ideal $I \subseteq C$ such that $I^2 = 0$ and suppose that the diagram

$$\begin{array}{ccc} C/I & \longleftarrow & A \\ \uparrow & & \uparrow \\ C & \longleftarrow & R \end{array}$$

commutes. Then A is *formally étale over* R (resp. formally unramified, resp. formally smooth) if there exists exactly one (resp. at most one, resp. at least one) lift $A \to C$ making the diagram

$$\begin{array}{ccc} C/I & \longleftarrow & A \\ \uparrow & \swarrow & \uparrow \\ C & \longleftarrow & R \end{array}$$

commute. It is étale (resp. unramified, resp. smooth) if it is formally étale and locally of finite presentation (resp. locally of finite type resp. locally of finite presentation).

A morphism of affine schemes $\operatorname{Spec} A \to \operatorname{Spec} R$ is étale if the corresponding map of rings $R \to A$ is étale.

Example 3.1.2. We show that if R is a perfect (i.e., $x \mapsto x^p$ is a bijection) $\mathbb{F}_p$-algebra, then it is formally étale. Suppose we have a diagram of the form

$$\begin{array}{ccc} C/I & \overset{f}{\longleftarrow} & R \\ \uparrow & \swarrow & \uparrow \\ C & \longleftarrow & \mathbb{F}_p \end{array}$$

We want to show that exactly one dotted arrow exists. Let $r \in R$, and choose a lift $c \in C$ of $f(r)$. Then we set $\widetilde{f}(r) = c^p$. This does not depend on the choice of lift since if we had two different choices c, c', then $c - c' = b \in I$, and $(c - c')^p = c^p - (c')^p = b^p = 0$ in I since $I^2 = 0$. Thus this is the unique lift.

Example 3.1.3. Consider the map $\operatorname{Spec} \mathbb{Z}/2\mathbb{Z} \to \operatorname{Spec} \mathbb{Z}$. This is a closed immersion, but

it is not étale. Indeed, consider the diagram

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \longleftarrow & \mathbb{Z}/2\mathbb{Z} \\ \downarrow & \swarrow & \uparrow \\ \mathbb{Z}/4\mathbb{Z} & \longleftarrow & \mathbb{Z} \end{array}$$

where $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the identity and the rest of the solid arrows are the canonical projections. Then there is no lift $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, because there are no homomorphisms between these two rings, so the map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is not étale.

We also want to quickly recall the use of differentials in determining if a map is unramified.

Theorem 3.1.4. *A morphism of schemes $f\colon X \to S$ is formally unramified if and only if $\Omega^1_{X/S} = 0$.*

Proof. See [15, Proposition 18.6] □

Example 3.1.5. Let $A = R[x]/(f)$, then $\Omega^1_{A/R} \cong R[x]/(f, f')$, and if $X = \operatorname{Spec} A$ and $S = \operatorname{Spec} R$, then $X \to S$ is unramified if and only if $f + f' = R[T]$, since otherwise $\Omega^1_{X/S} = \widetilde{\Omega^1_{A/R}} \neq 0$.

Example 3.1.6. Any open immersion is étale. Indeed, suppose $f\colon X \to S$ is an open immersion, and consider the diagram

$$\begin{array}{ccc} T' & \longrightarrow & X \\ \downarrow & \nearrow & \downarrow f \\ T & \longrightarrow & S \end{array}$$

where $T = \operatorname{Spec} A$ and $T' = \operatorname{Spec} A/I$ for some $I^2 = 0$. Then we know that $T \to S$ factors over X if and only if $f(|T|) \subseteq |X|$. Since the underlying topological spaces of T and T' are identical, we obtain the result.

With the following proposition we can give a large class of étale maps.

Proposition 3.1.7. *Let R be a ring, $f \in R[T]$ a polynomial and set $A = R[T]/(f)$. Let $g \in R[T]$ such that the image of the formal derivative f' of f in A_g is invertible. Then A_g is an étale R-algebra.*

Proof. (see [15, Proposition 18.38])

Set $A = R[T]/(f)$. Clearly A_g is an R-algebra of finite presentation. Hence it remains to prove that A_g is formally étale. Let C be an R-algebra, $I \subseteq C$ an ideal with $I^2 = 0$, and let $p\colon C \to C/I$ be the canonical projection. Let $u_0\colon A_g \to C/I$ be an R-algebra homomorphism. We have the following diagram

$$\begin{array}{ccc} C/I & \xleftarrow{u_0} & A_g \\ {\scriptstyle p}\uparrow & \swarrow_{l} & \uparrow \\ C & \longleftarrow & R \end{array}$$

and we want to show that exactly one such l exists. Let $x \in A_g$ be the image of T. Let B be an R-algebra Then sending an R-algebra homomorphism $v\colon A_g \to B$ to $b = v(x)$ defines a bijection

$$\mathrm{Hom}_{\mathbf{R-alg}}(A_g, B) \xrightarrow{\sim} \left\{ b \in B \mid f(b) = 0, g(b) \in B^\times \right\}.$$

By the hypothesis we have $f'(b) \in B^\times$ for any such b.

Let $c_0 \in C/I$ be the element corresponding to u_0 and $\widetilde{c} \in C$ be any element with $p(\widetilde{c}) = c_0$. Then $g(\widetilde{c}) \in C^\times$. It remains to show that there exists a unique $i \in I$ such that $f(\widetilde{c}+i) = 0$. Then $\widetilde{c}+i$ defines the unique lift $u\colon A_g \to C$ of u_0.

We have $f(\widetilde{c}) \in I$ and for $i \in I$ we obtain as Taylor expansion

$$f(\widetilde{c}+i) = f(\widetilde{c}) + if'(\widetilde{c})$$

because $I^2 = 0$. As $f'(c_0) \in (C/I)^\times$, we have $f'(\widetilde{c}) \in C^\times$ and hence there exists a unique $i \in I$ such that $f(\widetilde{c}+i) = 0$. □

Example 3.1.8. Consider $B = A[x]/(x^n - a)$ where n and a are units in A. Then $f' = nx^{n-1}$ and we have $x^n - a = 0$, so $a^{-1}x^n = 1$, so we find that

$$f'a^{-1}n^{-1} = (nx^{n-1})(x^n)^{-1}n^{-1} = 1$$

and thus f' is invertible and so B is an étale A-algebra.

In the next example we want to return to example 3.1.5 and show that if $f \in R[T]$ is a monic polynomial of degree $n \geq 1$ and $A = R[T]/(f)$, then A is étale over R if and only if $(f) + (f') = R[T]$. However, to do this we need an alternate, but equivalent, definition of an étale map. We will not provide the proof here but it can be found in [15].

Proposition 3.1.9. *[15, Theorem 18.44] Let $f: X \to S$ be locally of finite presentation. Then the following conditions are equivalent*

1. *f is étale.*
2. *f is flat and unramified.*
3. *f is smooth of relative dimension 0.*

Example 3.1.10. Let R be a ring, $f \in R[T]$ a monic polynomial of degree $n \geq 1$. Set $A = R[T]/(f)$. Then A is a free R-module of rank n, and in particular, is flat over R. Hence A is étale over R if and only if $\Omega^1_{A/R} = R[T]/(f, f') = 0$, i.e., if $(f) + (f') = R[T]$.

Example 3.1.11. We want to show that any separable field extension K/k is étale. This can be done in two steps. We first quickly see that by the above proposition if K/k is finite, then we can write $K = k[x]/(f(x))$, and thus by the above, this is formally étale, since f is separable. Then to generalize to an arbitrary separable extension we use the following lemma:

Lemma 3.1.12. *[16, § 17.3 Lemma 3.1] Let R be a ring, I a directed partially ordered set, and (S_i, ϕ_{ij}) a system of R-algebras. If each $R \to S_i$ is formally étale over R, then $S = \operatorname{colim}_i S_i$ is formally étale over R.*

Proof. Consider the diagram

$$\begin{array}{ccc} C/I & \longleftarrow & \operatorname{colim}_i S_i \\ \uparrow & \nearrow & \uparrow \\ C & \longleftarrow & R \end{array}$$

with $I^2 = 0$. We want to find a lift $\operatorname{colim}_i S_i \to C$. By assumption each S_i has a lift which makes the following diagram commute

$$\begin{array}{ccc} C/I & \longleftarrow & S_i \\ \uparrow & \swarrow & \uparrow \\ C & \longleftarrow & R \end{array}$$

and these lifts are compatible with the ϕ_{ij}, thus we get a lift $S \to C$. This lift is unique since if there was a second, then we could restrict them both to S_i and find that they must be the same since S_i is formally étale over R. □

Now we can use this lemma to finish the proof by noting that any separable field extension K/k can be written as a limit of finite separable extensions, which we already know are formally étale.

Remark 3.1.13. It can actually be shown that locally on the source every étale morphism of schemes has this form with f monic, so we have the following definition:

Definition 3.1.14. An R-algebra of the form $(R[T]/(f))_g$, where $f, g \in R[T]$ such that f is monic and such that f' is invertible in $(R[T]/(f))_g$ is called a *standard étale algebra over R*.

The following proposition states some properties of étale morphisms that will help us later on when we define the étale site.

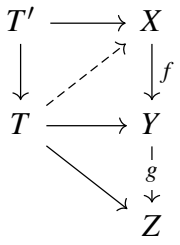
Proposition 3.1.15.

1. *If $f\colon X \to Y$ and $g\colon Y \to Z$ are étale, so is the composite $g \circ f$.*
2. *If $f\colon X \to X'$ and $g\colon Y \to Y'$ are étale S-morphisms, so is*

$$f \times_S g\colon X \times_S Y \to X' \times_S Y'.$$

Proof.

1. Since a composition of morphisms locally of finite presentation, is locally of finite presentation, we just have to show that a composition of formally étale morphisms is formally étale. Let $T = \operatorname{Spec} A$ be an affine scheme and let $T' = \operatorname{Spec} A/I$ be a closed subscheme with $I^2 = 0$. We see this from the following diagram

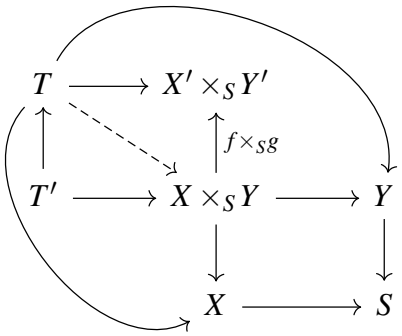


where the diagram commutes, so the lift $T \to X$ lifts the map $g \circ f\colon X \to Z$.

2. Again, we know that the property holds for morphisms that are locally of finite presentation so we just have to prove it in the formally étale case. Suppose $T = \operatorname{Spec} A$ and $T' = \operatorname{Spec} A/I$ with $I^2 = 0$. Then since f and g are étale, we have unique lifts $T \to X$ and $T \to Y$ making the diagrams

$$\begin{array}{ccc} T' & \longrightarrow & X \\ \downarrow & \nearrow & \downarrow f \\ T & \longrightarrow & X' \end{array} \qquad \begin{array}{ccc} T' & \longrightarrow & Y \\ \downarrow & \nearrow & \downarrow g \\ T & \longrightarrow & Y' \end{array}$$

commute. Then, using the universal property of fiber products we obtain a unique lift $T \to X \times_S Y$:



□

Definition 3.1.16. An S-scheme $X \xrightarrow{\pi} S$ is étale whenever π is. We denote by $\mathbf{Ét}/S$ the category of étale S-schemes along with arrows given by étale morphisms of S-schemes.

Remark 3.1.17. By the Proposition 3.1.15, the category $\mathbf{Ét}/S$ has fibre products.

3.1.2 Grothendieck Topologies and the Étale Site

Definition 3.1.18. [17, p. 86] A family $\left\{ X_i \xrightarrow{\phi_i} X \right\}_i$ of morphisms in $\mathbf{Ét}/\mathbf{X}$ is called *surjective* if $X = \bigcup_i \phi_i(X_i)$.

Example 3.1.19. If we look at $S = \operatorname{Spec} k$, then an étale map $X \to S$ is a disjoint union of spectra of finite separable extensions of k. Any map of this type will also be an étale cover.

Example 3.1.20. Let R be a ring. Let $f \in R[T]$ be a monic polynomial such that f and f' generate $R[T]$ as an ideal. Then $\operatorname{Spec} R[T]/(f) \to \operatorname{Spec} R$ is an étale cover.

Definition 3.1.21. Let $\mathbf{C}$ be a category. A *Grothendieck topology* J consists of the following data: for each object U in $\mathbf{C}$, a collection $J(U)$ of sets of maps $\{\phi_i \colon U_i \to U\}$ in $\mathbf{C}$ where each set is called a *covering of* U, satisfying the following conditions:

1. for any morphism $V \to U$ in $\mathbf{C}$, the fiber product $U_i \times_U V$ exists, and induces a covering $\{U_i \times_U V \to V\}_i$ of V.
2. If for each i, $\{V_{ij} \to U_i\}_j$ is a covering of U_i, then $\{V_{ij} \to U\}_{ij}$ is also a covering of U.
3. The class consisting only of the identity map $U \to U$ is a covering of U.

A pair $(\mathbf{C}, J)$ is called a *site*.

Example 3.1.22. [18, Tag 020T] Let X be a scheme. A *Zariski covering* of X is a family of morphisms $\left\{X_i \xrightarrow{\phi_i} X\right\}_i$ of schemes such that each ϕ_i is an open immersion and such that $X = \bigcup_i f_i(X_i)$. The *small Zariski site* of a scheme X, denoted X_{zar} is the site whose objects are schemes U/X such that $U \to X$ is an open immersion. The three properties of sites are easily seen to be verified:

1. If $X' \to X$ is a morphism and $\{X_i \to X\}_i$ is a covering, then $\{X' \times_X X_i \to X\}_i$ is still a covering.
2. If $\{X_i \to X\}_i$ is a Zariski covering and for each i, we have a Zariski covering $\{X_{ij} \to X_i\}_j$ is a covering, then since all the morphisms are open immersions, $\{X_{ij} \to X\}_{ij}$ is also an open cover.
3. Finally, if $X' \to X$ is an isomorphism, then $\{X' \to X\}$ is a Zariski covering.

Example 3.1.23. Let T be a scheme, an *fppf covering of* T is a family of morphisms $\{f_i \colon T_i \to T\}_i$ of schemes such that each f_i is flat, locally of finite presentation and such that $T = \bigcup_i f_i(T_i)$. By [18, Tag 021O], fppf coverings are stable under composition and base change, and thus we can form the fppf topology over a scheme S which has the underlying category $\mathbf{Sch}_S$ and the coverings are fppf coverings. This topology will again be used during our main proof.

Also, note that since étale morphisms are flat, unramified, and locally of finite presentation, any étale morphism is also fppf, so the fppf topology is finer than the étale and Zariski topologies.

We see in the next proposition that the definition extends the definition of covering on a topological space.

Proposition 3.1.24. *Any classical open cover $\{U_i\}$ on a topological space X is a covering as defined above.*

Proof. Let $\mathbf{U}(X)$ be the poset category which has objects given by open sets of X, and arrows given by inclusions. For any open $V \subseteq X$ the fiber products $U_i \times_X V$ are given by $U_i \cap V$. Since $U_i \cap V$ are also subsets of X, they are objects in $\mathbf{U}(X)$ and form an open cover of V. To prove (2), let $\{V_{ij}\}$ be a covering of U_i for each i. Then V_{ij} is an open cover of U. Finally U is an open cover of itself. □

Definition 3.1.25. Let $(\mathbf{C}, J), (\mathbf{C}', J')$ be sites. A *morphism of sites* $f\colon (\mathbf{C}, J) \to (\mathbf{C}', J')$ is a functor $\mathbf{C} \to \mathbf{C}'$ with the following properties

1. $\{U_i \to U\}_i \in J(U)$ implies that $\{f(U_i) \to f(U)\}_i \in J'(f(U))$.
2. For $\{U_i \to U\}_i \in J(U)$ and a morphism $V \to U$ in $\mathbf{C}$, the canonical morphism

$$f(U_i \times_U V) \to f(U_i) \times_{f(U)} f(V)$$

is an isomorphism,

i.e., morphisms of sites preserve coverings and fiber products.

Definition 3.1.26. A *sheaf* on a site $(\mathbf{C}, J)$ is a contravariant functor $\mathscr{F}\colon \mathbf{C}^{\mathrm{op}} \to \mathbf{Sets}$ such that the sequence

$$\mathscr{F}(U) \to \prod_i \mathscr{F}(U_i) \rightrightarrows \prod_{i,j} \mathscr{F}(U_i \times_U U_j)$$

is exact. Thus, $\mathscr{F}(U)$ can be defined with the collection $(s_i) \in \prod_i \mathscr{F}(U_i)$ satisfying

$$s_i|_{U_i \times_U U_j} = s_j|_{U_i \times_U U_j}.$$

Definition 3.1.27. A *topos* is a category equivalent to the category of sheaves on a site.

Definition 3.1.28. The *étale site* on X, $X_{ét}$, has the underlying category $Ét/X$, which consists of X-schemes $T \to X$ which are étale. A covering of X is a surjective family of étale morphisms in $Ét/X$, i.e., a collection of X-schemes $\{\phi_i \colon U_i \to X\}$ maps such that $\bigcup_i \phi_i(U_i) = X$.

Remark 3.1.29. Using Proposition 3.1.15, it can easily be seen that the étale site does indeed satisfy the properties (1)-(3) required to be a site.

Now, one of the goals of introducing the étale topology was that it refines the Zariski topology. This can be seen in the definition of both sites. For the Zariski site on a scheme X we took coverings $\left\{X_i \xrightarrow{f_i} X\right\}_i$ where each f_i is an open immersion. Since open immersions are étale by Example 3.1.6, we see that any covering $\{X_i \to X\}_i$ in X_{zar} is also a covering in $X_{ét}$, but there are coverings in $X_{ét}$ that do not exist in the Zariski case. For example, consider

$$f \colon \operatorname{Spec} \mathbb{Q}[T]/(x^n - 1) \to \operatorname{Spec} \mathbb{Q}.$$

Since n and 1 are invertible in $\mathbb{Q}$, f is étale, and it is an étale cover since $|\operatorname{Spec} \mathbb{Q}| = \{(0)\}$, but this is not an open immersion since there is more than one prime ideal in $\mathbb{Q}[T]/(x^n - 1)$.

Thus the étale site is much finer than the Zariski site, and has many more open sets.

3.1.3 Objects Representable over Sheaves

Now, we let **Aff** be the category of affine schemes and let $\mathbf{Aff}^\sim$ be the category of sheaves of sets on **Aff** with respect to the étale topology. Now, instead of focusing on one scheme with the étale topology like in the site $X_{ét}$, we look at sheaves

$$F \colon \mathbf{Aff} \to \mathbf{Sets}$$

and it is a sheaf if for every étale cover $\{X_i \to X\}_i$ it satisfies that sheaf condition.

Note that any scheme S can be viewed as an object of $\mathbf{Aff}^\sim$ via the functor it represents

$$\operatorname{Spec} R \to \operatorname{Hom}(\operatorname{Spec} R, S).$$

This is a fully faithful embedding and we can regard the category of schemes as a full subcategory of $\mathbf{Aff}^\sim$ in this way.

Recall that if **C** and **D** are categories and $F \colon \mathbf{C} \to \mathbf{D}$ is a functor then the functor F

induces a map

$$F_{X,Y}\colon \operatorname{Hom}_{\mathbf{C}}(X,Y) \to \operatorname{Hom}_{\mathbf{D}}(F(X),F(Y))$$

for every pair of objects X, Y in $\mathbf{C}$. The functor F is said to be

1. *faithful* if $F_{X,Y}$ is injective.
2. *full* if $F_{X,Y}$ is surjective.
3. *fully faithful* if $F_{X,Y}$ is bijective.

In our case the functor is

$$\begin{aligned} \operatorname{Hom}(-,-)\colon \mathbf{Sch} &\to \mathbf{Aff}^{\sim} \\ S &\mapsto \operatorname{Hom}(-,S). \end{aligned}$$

For any $S \in \mathbf{Aff}^{\sim}$, let $\mathbf{Aff}^{\sim}_S$ denote the category of sheaves X equipped with a map $X \to S$, where the morphisms are morphisms over S. If $T \to S$ is a morphism of sheaves, and $X \in \mathbf{Aff}^{\sim}_S$, let X_T denote the sheaf $T \times_S X$ together with the morphism

$$\operatorname{pr}_T\colon T \times_S X \to T.$$

Then, by composing we have a map $T \times_S X \to T \to S$, and thus $T \times_S X \in \mathbf{Aff}^{\sim}_S$.

This construction allows us to define familiar structures on an object X over S by using affine test schemes.

Definition 3.1.30. An *elliptic curve* X over a sheaf S is a sheaf $X \to S$ such that

1. for every affine scheme T with a morphism $T \to S$, the pullback $X_T = T \times_S X$ is a classical elliptic curve over T.
2. Moreover, these elliptic curve structures are compatible with pullbacks along maps of affine schemes $T' \to T$, that is, for any such map the natural base change

   $$(X_T)_{T'} \to X_{T'}$$

   must be an isomorphism of elliptic curves over T', meaning that it also respects the group structure.

The definition of an elliptic curve above defines an elliptic curve over S not just by giving a single curve, but by giving a system of elliptic curves over all affine schemes mapping to S that all fit together in a nice functorial way. This definition also allows us to define families of elliptic curve over an arbitrary base and will lead us to the definition of a moduli space.

Remark 3.1.31. This construction will not actually be that important for the purpose of this thesis. Instead of considering an elliptic curve over a p-adic sheaf S, we can consider a curve over an affine scheme $T = \operatorname{Spec} R$ where p is nilpotent on R. Then since everything we will do will be compatible with base change, to get an elliptic curve over a p-adic sheaf $S = \operatorname{colim}_i S_i$ with S_i affine with p nilpotent, we can consider $E = \operatorname{colim}_i ES_i$.

4

Formal Schemes

We begin by considering the spectrum of a field, $\mathrm{Spec}(k)$. This is just a single point equipped with the structure sheaf $\mathscr{O}_{Spec(k)} = k$. From the perspective of sheaves as functions on a space, these functions are simply constant functions because each map $\mathrm{Spec}(k) \to \mathrm{Spec}\, A$ gives a maximal ideal. So

$$\mathrm{Hom}_{\mathbf{Sch}}(\mathrm{Spec}\, k, \mathrm{Spec}\, A) \cong \{\mathfrak{m} \lhd A \mid \mathfrak{m} \text{ is maximal}\}$$

.

To study functions with higher-order behavior, we might consider the ring of dual numbers $k[x]/(x^2)$. This ring has a single ideal (x), so as a topological space, $|\mathrm{Spec}(k)| = |\mathrm{Spec}(k[x]/(x^2))|$. However, the structure sheaves differ: the sheaf on $\mathrm{Spec}(k[x]/(x^2))$ allows us to speak of functions with a notion of first-order derivatives—directions in which we can "infinitesimally" move away from our point. This is because a map $f\colon \mathrm{Spec}\, k[x]/(x^2) \to \mathrm{Spec}\, A$ gives both a maximal ideal of A and a derivation, i.e., a map that respects the typical Leibniz rule.

To capture even higher-order infinitesimal behavior, we consider the system $(k[x]/(x^n))_{n\geq 1}$, and form the inverse limit:

$$\varprojlim_n k[x]/(x^n) \cong k[[x]].$$

This formal power series ring reflects all higher-order infinitesimal data.

However, a complication arises: the spectrum of $k[[x]]$ contains , (0) and (x), since $k[[x]]$ is an integral domain. Thus, it does not have the same topological structure as the previous examples, and so this approach is not a direct generalization.

This issue can be resolved by transitioning to the language of formal schemes.

Definition 4.0.1. An *adic Noetherian ring* is a noetherian topological ring A that is separated and complete for the I-adic topology, where I is an ideal of A, that is,

$$A = \lim_{n\geq 0} A/I^{n+1}.$$

Example 4.0.2.

1. If $A = \mathbb{Z}_p$ and $I = (p)$, then A is an adic Noetherian ring and it is complete with respect to I.
2. Similarly, if $A = k[\![t]\!]$ and $I = tk[\![t]\!]$, then A is again complete with respect to I.
3. [19, Definition 2.0.6] Let A be a Noetherian I-adic ring, then the *ring of restricted power series* is defined as

$$A\{T_1,\ldots,T_r\} = \lim_{\leftarrow n} A[T_1,\ldots,T_r]/I^{n+1}[T_1,\ldots,T_r] = \lim_{\leftarrow n}(A/I^{n+1})[T_1,\ldots,T_r].$$

4. Another way to create rings of this type is to cut out a variety from some affine space, and take the completion with respect to the variety. Consider $k[x,y]/(f)$ where $I = (f)$ is some polynomial in x and y. We can then take the completion with respect to I: $\lim_{\leftarrow n} k[x,y]/(f)^{n+1}$.

Definition 4.0.3. Let A be an adic Noetherian ring. We associate a topologically ringed space

$$\mathrm{Spf}(A) = \mathrm{colim}_{n\geq 0}\,\mathrm{Spec}(A/I^{n+1})$$

called the *formal spectrum* of A. The underlying topological space is just $\mathrm{Spec}(A/I)$ and the structure sheaf is given by

$$\mathscr{O}_{\mathrm{Spf}(A)} = \lim_{n\geq 0} \mathscr{O}_{\mathrm{Spec}(A/I^{n+1})}.$$

So for an open subset $U \subseteq \mathrm{Spec}A$, $\mathscr{O}_{\mathrm{Spf}(A)}(U) = \varprojlim \mathscr{O}_{\mathrm{Spec}(A/I^{n+1})}(U)$. An *affine formal scheme* is a topologically ringed space isomorphic to $\mathrm{Spf}(A)$ for some A as above.

Remark 4.0.4. [18, Tag 0AHY] Another way to define the topological space of formal schemes is by writing

$$\mathrm{Spf}(A) = \{\text{open prime ideals } \mathfrak{p} \subset A\}.$$

Note that this is homeomorphic to $\mathrm{Spf}(A) = \mathrm{Spec}(A/I)$, the definition given above. Indeed, we can show that a prime ideal is open if and only if it contains I, and hence is in $\mathrm{Spec}(A/I)$. Recall that the I-adic topology is defined by having $\{I^n\}$ be a fundamental basis of open neighborhoods of the identity. If $\mathfrak{p} \in \mathrm{Spec}\, A$ is open, then since $0 \in \mathfrak{p}$ has an open neighborhood $0 \in U \subseteq \mathfrak{p}$. Then by definition of the I-adic topology this means that for some $n \in \mathbb{N}$, $0 \in I^n \subseteq U \subseteq \mathfrak{p}$. Conversely, if $I \subseteq \mathfrak{p}$, then let $x \in \mathfrak{p}$. Consider the open set $x+I$, this is still contained in $\mathfrak{p}$ since both x and I are in $\mathfrak{p}$, so $\mathfrak{p}$ is open.

Example 4.0.5.

1. If A is any ring (with the discrete topology) and $I = (0)$, then $\mathrm{Spf}(A) = \mathrm{Spec}(A)$ is just the affine scheme corresponding to A.
2. If $A = \mathbb{Z}_p$, and $I = p\mathbb{Z}_p$, then

   $$|\mathrm{Spf}(\mathbb{Z}_p)| = |\mathrm{Spec}(\mathbb{F}_p)|$$

   is just a single point, but the structure sheaf is $\mathbb{Z}_p$.
3. Similarly, for $A = k[\![t]\!]$ and $I = t[\![t]\!]$, we have $|\mathrm{Spf}(k[\![t]\!])| = |\mathrm{Spec}\, k|$, which is just a single point, but the structure sheaf is $k[\![t]\!]$.
4. Consider the ring $k[x,y]$, and consider the variety $V(y^2-x^3)$, and let $I = (y^2-x^3)$. Then $k[x,y]$ is not I-adically complete, let

   $$A = \lim_{\leftarrow n} k[x,y]/(y^2-x^3)^n$$

   be its I-adic completion. Then $\mathrm{Spf}(A) = V(I) = \mathrm{Spec}(k[x,y]/(y^2-x^3))$, but it's structure sheaf is the completed ring A.

4.0.1 p-ADIC SHEAVES

Now, the ultimate goal of this thesis is to look at canonical lifts of elliptic curves over schemes S, to a curve over $W(S)$, the Witt vectors of S. We have yet to define what the Witt

vectors of schemes are, however, there is actually a more general statement of the main theorem we will prove. We can generalize the objects from schemes to *p-adic sheaves*. Here we discuss these objects.

Definition 4.0.6. We say that a sheaf $S \in \mathbf{Aff}^{\sim}$ is p-adic if it is isomorphic to a colimit $\operatorname{colim}_i S_i$ of affine schemes S_i on which p is nilpotent.

Example 4.0.7.

1. Let $S = \operatorname{Spec} \mathbb{F}_p[x]$, then S is a p-adic sheaf. Generally, if A is an $\mathbb{F}_p$-algebra, then $S = \operatorname{Spec} A$ is a p-adic sheaf since p is nilpotent on $\operatorname{Spec} A$.

2. Consider
$$\operatorname{Spf}(\mathbb{Z}_p) = \operatorname{colim}_i \operatorname{Spec} \mathbb{Z}/p^{i+1}\mathbb{Z},$$
the formal spectrum of $\mathbb{Z}_p$ which is a p-adic sheaf as each $\mathbb{Z}/p^{i+1}\mathbb{Z}$ is a ring in which p is nilpotent. More generally, if A is a p-adic noetherian ring, then the formal spectrum $\operatorname{Spf}(A)$ will be a p-adic sheaf.

3. [20, p. 6] Let $R_i = \mathbb{F}_p[t]$, and let $R_i \to R_{i+1}$ be given by the Frobenius. Then we could consider $S = \operatorname{colim}_\phi \operatorname{Spec} \mathbb{F}_p[t]$.

Definition 4.0.8. Let T be a scheme. Let

$$T_n = \operatorname{Spec} \mathbb{Z}/p^{n+1}\mathbb{Z} \times_{\operatorname{Spec} \mathbb{Z}} T.$$

Then we call
$$\widehat{T} = \operatorname{colim}_n T_n$$
the *p-adic completion* of T. It is a p-adic sheaf because each T_n is a scheme over $\mathbb{Z}/p^{n+1}\mathbb{Z}$ and hence is a colimit of affine schemes over $\mathbb{Z}/p^{n+1}\mathbb{Z}$.

Remark 4.0.9. The above construction works for any p-adic formal scheme T and this defines a fully faithful embedding of the category of p-adic formal schemes into the category of p-adic sheaves.

5

Witt Vectors for Schemes

In this section we generalize our definition fo Witt vectors to include Witt vectors of schemes. We would hope to simply be able to write $W(\operatorname{Spec} A) = \operatorname{Spec} W(A)$, but unfortunately this is not the case as oftentimes $W(\operatorname{Spec} A)$ will turn out not to even be a scheme, but a formal scheme.

We start by writing $W_n \colon \mathbf{Aff} \to \mathbf{Aff}$ for the functor defined by $W_n(\operatorname{Spec} R) = \operatorname{Spec} W_n(R)$.

Theorem 5.0.1. *The functor $W_n \colon \mathbf{Aff} \to \mathbf{Aff}$ preserves étale maps, étale covering families, and étale base change. In particular, W_n is continuous in the étale topology.*

Proof. See [21, Appendix A] or [22, Theorem 9.2] □

Example 5.0.2. Let $S = \operatorname{Spec} A$ be an affine scheme and let $f \in A$, so that $D(f) = \operatorname{Spec} A_f \subseteq S$ is a principal open subset. Thus $D(f) \to S$ is an open immersion, and is therefore étale. We will see in Lemma 5.0.4 that

$$W_n(D(f)) = W_n(\operatorname{Spec} A_f) = \operatorname{Spec} W_n(A_f) = \operatorname{Spec} W_n(A)[1/[f]] = \operatorname{Spec} W_n(R)_{[f]} = D([f])$$

where $[f] = (f, 0, 0, \ldots)$ is the Teichmüller lift of f. Thus $W_n(D(f)) = D([f]) \subseteq W_n(S) = \operatorname{Spec} W_n(A)$, is a principal open subset, and so it is still étale over S.

This allows us to extend W_n to $\mathbf{Aff}^{\sim}$. Indeed, because W_n is continuous, for any sheaf S, the presheaf $U \mapsto S(W_n(U))$, for any $U \in \mathbf{Aff}$ is a sheaf. This defines a functor

$W_{n*}\colon \mathbf{Aff}^{\sim} \to \mathbf{Aff}^{\sim}$, and it has a left adjoint by [23, III 1.2] W_n^*. Finally, W_n^* extends W_n from **Aff** to $\mathbf{Aff}^{\sim}$ in the sense that we have canonical isomorphisms $W_n^*(\operatorname{Spec} R) \xrightarrow{\sim} \operatorname{Spec} W_n(R)$. So from now on, we often abusively write $W_n = W_n^*$.

Remark 5.0.3. If S is a p-adic sheaf, then so is $W_n(S)$. Indeed, it is sufficient and necessary to observe that if p is nilpotent in a ring R, then it is nilpotent in $W_n(R)$. One way to show this is to observe that the map $W_{m+n}(\mathbb{F}_p) \to W_n(W_m(\mathbb{F}_p))$ maps $W_n(\mathbb{Z}/p^{m+1}\mathbb{Z})$ into a $\mathbb{Z}/p^{m+n+1}\mathbb{Z}$-algebra. This map is obtained by using the universal property of Witt vectors:

$$\begin{array}{ccccc} W_{m+n}(\mathbb{F}_p) & \dashrightarrow & W(W_m(\mathbb{F}_p)) & \longrightarrow & W_n(W_m(\mathbb{F}_p)) \\ & \searrow & \uparrow & & \\ & & W_m(\mathbb{F}_p) & & \end{array}$$

From the truncation map $W_{m+n}(\mathbb{F}_p) \to W_m(\mathbb{F}_p)$, we get a map $W_{m+n}(\mathbb{F}_p) \to W(W_m(\mathbb{F}_p))$, and then using the truncation map again $W(W_m(\mathbb{F}_p)) \to W_n(W_m(\mathbb{F}_p))$ gives the desired map.

Moreover, if S is a scheme on which p is locally nilpotent, then so is $W_n(S)$. As a topological space $W_n(S)$ agrees with S and its structure sheaf $\mathscr{O}_{W_n(S)}$ is given by the presheaf $U \mapsto W_n(\mathscr{O}_S(U))$. One way to show this is to show that for any ring$R$ and any $f \in R$, $W_n(R[1/f]) = W_n(R)[1/[f]]$ where $[f]$ denotes the Teichmüller lift.

Lemma 5.0.4. *For any ring R and any $f \in R$, $W_n(R[1/f]) = W_n(R)[1/[f]]$.*

Proof. Note that

$$W_n(R[1/f]) = \{(a_0, \ldots, a_{n-1}) \mid a_i \in R[1/f]\},$$

while

$$W_n(R)[1/[f]] = \left\{ \frac{w}{[f]^n} \mid w = (r_0, \ldots, r_{n-1}) \in W_n(R) \right\}.$$

First, we claim that

$$(a_0, \ldots, a_{n-1})[f]^{-m} = (a_0, \ldots, a_{n-1})(f^{-m}, 0, \ldots, 0) = (a_0 f^{-m}, a_1 f^{-mp}, \ldots, a_{n-1} f^{-mp^{n-1}}).$$

We proceed by induction. We see that this holds for $n = 0$ and for $n = 1$ we have

$$(a_0, a_1)(f^{-m}, 0) = (a_0 f^{-m}, a_1 f^{-mp} + a_0^p \cdot 0 + p \cdot a_1 \cdot 0) = (a_0 f^{-m}, a_1 f^{-mp}).$$

Now suppose it holds for n, and consider

$$(a_0, \ldots, a_n)(f^{-m}, 0, \ldots, 0) = (a_0 f^{-m}, \ldots, a_{n-1} f^{-mp^{n-1}}, \delta(a_{n-1} f^{-mp^{n-1}})).$$

□

Then we define

$$W(S) = \operatorname{colim}_n W_n(S)$$

where the limit is taken in $\mathbf{Aff}^{\sim}$. Note that even if S is a scheme, $W(S)$ is usually not a scheme as shown by the following proposition.

Proposition 5.0.5. *Let A be a ring. Then $W(\operatorname{Spec}(A)) = \operatorname{Spf}(W(A))$*

Proof. We have

$$W(\operatorname{Spec}(A) = \operatorname{colim}_n W_n(\operatorname{Spec}(A)) = \operatorname{colim}_n \operatorname{Spec}(W_n(A)) = \operatorname{colim} \operatorname{Spf}(W_n(A)) = \operatorname{Spf}(\lim_n W_n(A)) = \operatorname{Spf}(W($$

□

Universal Property of Witt Vectors for p-adic Sheaves

Now we turn to an extremely important universal property that will be crucial in proving our main theorem.

Let A be a p-torsion-free ring with a Frobenius lift ψ. Let $Y_m = \operatorname{Spec} A/p^{m+1}A$ and $\widehat{Y} = \operatorname{colim}_m Y_m$ and let $\widehat{\psi}\colon \widehat{Y} \to \widehat{Y}$ be the induced Frobenius lift.

Example 5.0.6. For the simplest example we can take $A = \mathbb{Z}_p$ with Frobenius lift $\psi(x) = x$. This is indeed a Frobenius lift since $\psi(x) = x \equiv x^p \mod p\mathbb{Z}_p$. Then $Y_m = \operatorname{Spec} \mathbb{Z}_p/p^{m+1}\mathbb{Z}_p = \operatorname{Spec} \mathbb{Z}/p^{m+1}\mathbb{Z}$ and so

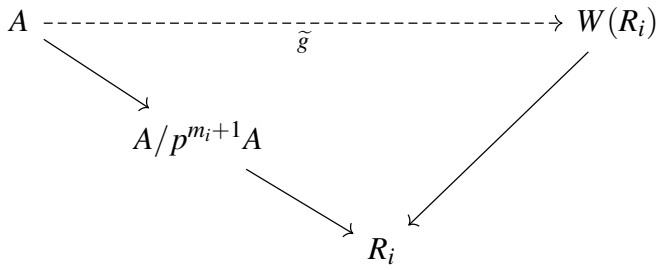
$$\widehat{Y} = \operatorname{colim}_m Y_m = \operatorname{colim}_m \operatorname{Spec} \mathbb{Z}/p^{m+1}\mathbb{Z} = \operatorname{Spf}(\mathbb{Z}_p).$$

Then the induced Frobenius lift $\widehat{\psi}\colon \operatorname{Spf}(\mathbb{Z}_p) \to \operatorname{Spf}(\mathbb{Z}_p)$ is also just the identity.

Now we let S be a p-adic sheaf (take $S = \operatorname{colim}_\phi \mathbb{F}_p[t]$ for example). We write $S = \operatorname{colim}_n \operatorname{Spec} R_n$, with p nilpotent in each ring R_i. Then for each i, there exists an m_i such that the map $\operatorname{Spec} R_i \to \widehat{Y}$ factors through the inclusion $Y_{m_i} \to \widehat{Y}$, thus inducing a map $A/p^{m_i+1}A \to R_i$ (in our example this would be a map $\mathbb{F}_p[t] \to \mathbb{Z}/p^{n+1}\mathbb{Z}$). Let g denote the composition

$$A \to A/p^{m_i+1}A \to R_i,$$

and let $\widetilde{g}$ denote the canonical lift:



Then for each n, since we have this factoring, we see that the composition $A \to W(R_i) \to W_n(R_i)$ factors through $A \to A/p^{N_{i,n}+1}A$ for some $A_{i,n}$. Taking the maps induced on Spec, we get a compatible family of maps

$$\operatorname{Spec} W_n(R_i) \to \operatorname{Spec} A/p^{N_{i,n}+1} = Y_{N_{i,n}} \to \widehat{Y}.$$

Then, using the universal property of colimits, we get a map

$$\widehat{f}\colon W(S) = \operatorname{colim}_{n,i} W_n(\operatorname{Spec} R_i) \to \widehat{Y}.$$

This map is called the *canonical lift* of the map $f\colon S \to \widehat{Y}$ since it lifts to the Witt vectors of the p-adic sheaf. Note that we also have $\widehat{f} \circ \widehat{\psi} = F \circ \widehat{f}$, where $F\colon W(S) \to W(S)$ is the usual Witt vector Frobenius map.

Our goal in this thesis is to lift elliptic curves over p-adic sheaves to elliptic curves over the Witt vectors of p-adic sheaves and this universal property will be crucial so we will state it again below:

Example 5.0.7. For a simple example we let $A = \mathbb{Z}$ with $\phi = \mathrm{id}_Z$. Then

$$\widehat{Y} = \operatorname{colim}_m \mathbb{Z}/p^{n+1}\mathbb{Z} \cong \operatorname{Spf}(\mathbb{Z}_p).$$

Recall that $|\operatorname{Spf}(\mathbb{Z}_p)| = \{(0)\}$ as a topological space. For our S we choose $S = \operatorname{Spec}\mathbb{Z}/p^n\mathbb{Z}$ for some $n \geq 1$. Then $|\operatorname{Spec}\mathbb{Z}/p^n\mathbb{Z}| = \{(p)\}$. We define the map from S to $\widehat{Y}$ in the only possible way:

$$\begin{aligned} f\colon S &\to \widehat{Y} \\ (p) &\mapsto (0). \end{aligned}$$

The corresponding map on sheaves is the canonical projection $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$. Now, we need a map $\widehat{f}\colon W(S) \to \widehat{Y}$. To do this we note that the map $\operatorname{Spec}\mathbb{Z}/p^n\mathbb{Z} \to \widehat{Y}$ factors through $Y_n = \operatorname{Spec}\mathbb{Z}/p^n\mathbb{Z}$, and we have the induced identity map $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. Then we use the universal property for Witt vectors to get a map

$$\mathbb{Z} \xrightarrow{\widehat{g}} W(\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}_p[\zeta_{p^n-1}].$$

This gives a map $A \xrightarrow{\widehat{g}} W(\mathbb{Z}/p^n\mathbb{Z}) \to W_n(\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p^{n^2}\mathbb{Z}$, which factors through $A_{n^2} = \mathbb{Z}/p^{n^2}\mathbb{Z}$. This defines a compatible family of maps

$$\operatorname{Spec} W_n(\operatorname{Spec}\mathbb{Z}/p^n\mathbb{Z}) \cong \mathbb{Z}/p^{n^2}\mathbb{Z} \to Y_{n^2} = \operatorname{Spec}\mathbb{Z}/p^{n^2}\mathbb{Z} \to \widehat{Y}.$$

Then the universal property of colimits gives us a map $\widehat{f}\colon W(S) = \operatorname{colim}_n W_n(\operatorname{Spec}\mathbb{Z}/p^n\mathbb{Z}) \to \widehat{Y}$

6

Witt Vectors

In this section, we develop the theory of moduli spaces over the category **Ell** of elliptic curves. Our aim is to formalize the notion of a moduli problem in this context and to investigate criteria under which such problems are representable. We begin by introducing moduli functors valued in sets, defined on the category **Ell**, and explore their basic properties with respect to representability and relative representability. We follow the notation and approach of [7] and [24].

The goal in this section is to understand when a moduli problem corresponds to an actual geometric object—namely, a scheme that represents the functor. We focus in particular on the concept of relative representability, which allows us to understand how moduli problems behave in families, and rigidity, which ensures the absence of automorphisms in the objects we classify.

The main result of this section is a representability criterion: we show that moduli problems that are both relatively representable and rigid are in fact representable. This result provides a powerful tool for constructing and understanding moduli spaces in concrete terms. It will be crucial in the main argument of this thesis, where we need to know that certain moduli problems of elliptic curves equipped with additional structure are representable by affine schemes.

We begin with some motivation. By the classical theory of elliptic curves over $\mathbb{C}$ we

know that

$$\{\text{isomorphism classes of elliptic curves } E/\mathbb{C}\} \cong \mathscr{H}/\operatorname{SL}_2(\mathbb{Z}) \cong \mathbb{C},$$

where $\mathscr{H}/\operatorname{SL}_2(\mathbb{Z})$ is the complex upper half-plane under the identification of the action by $\operatorname{SL}_2(\mathbb{Z})$. Thus, we would hope that for an arbitrary scheme S,

$$\{\text{isomorphism classes of elliptic curves } E/S\} \cong \mathbb{A}^1(S).$$

Suppose that this is true so that there is a scheme $\mathscr{M}$ such that

$$\mathscr{M}(S) = \operatorname{Hom}_{\mathbf{Sch}}(S, \mathscr{M}) \cong \{\text{isomorphism classes of elliptic curves } E/S\}.$$

There are a couple reasons why $\mathscr{M}$ cannot exist.

We first illustrate this problem with a concrete example. Suppose again that the moduli problem of sending a scheme S to the isomorphism classes of elliptic curves over S is represented $\mathscr{M}$, and let $\mathscr{E}\mathscr{M}$ be the universal elliptic curve. Let $E/\mathbb{C}$ be an elliptic curve and let

$$T = \operatorname{Spec}\left(\frac{\mathbb{C}[s^{\pm 1}, t]}{t^2 - s}\right) \xrightarrow{\pi} S = T/\langle\sigma\rangle$$

which is a $G = \mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\} \cong \langle\sigma\rangle$ cover, i.e., $S = T/\langle\sigma\rangle$ with $\sigma(s,t) = (s,-t)$. Then the trivial family corresponds to the map

$$\begin{array}{ccccc} E \times S & \longrightarrow & E & \longrightarrow & \mathscr{E} \\ \downarrow & & \downarrow & & \downarrow \\ S & \xrightarrow[\text{can}]{} & \operatorname{Spec}\mathbb{C} & \xrightarrow[e]{} & \mathscr{M} \end{array}$$

where E is equivalent to $e \in \mathscr{M}(\mathbb{C})$. We can construct an isotrivial family X/S as the quotient of $E \times T$ by the diagonal action $\sigma(P,Q) = (\sigma P, \sigma Q)$ where $P \in E$ and $Q \in T$ and $\sigma P = -P$. There is a canonical projection

$$E \times T \to X = (E \times T)/\langle\sigma\rangle.$$

We make two claims, first that X/S is not isomorphic to $(E \times S)/S$. Secondly, we claim that $\mathscr{M}$ cannot exist.

For the first claim, suppose

$$\begin{array}{ccc} E \times S & \xrightarrow{\phi} & X \\ & \searrow \quad \swarrow & \\ & S & \end{array}$$

exists. Then by pullback along π, there is a G-equivalence isomorphism

$$\begin{array}{ccc} (E \times S) \times T = E \times T & \xrightarrow{\phi} & X \times T = E \times T \\ & \searrow \quad \swarrow & \\ & T & \end{array}$$

and we necessarily have $\phi(P,Q) = (\alpha(P,Q),Q)$ and G-equivalence gives $\sigma\alpha(P,Q) = \alpha(P,\sigma Q)$. Now, fix $Q_0 \in T(\mathbb{C})$, then there is a continuous map given by

$$\begin{aligned} T(\mathbb{C}) &\xrightarrow{\widetilde{\alpha}} \mathrm{Aut}(E(\mathbb{C})) \\ Q &\mapsto \alpha(-,Q) \circ \alpha(-,Q_0)^{-1} \\ Q_0 &\mapsto \mathrm{id}_E \\ \sigma Q_0 &\mapsto -\mathrm{id}_E \end{aligned}$$

Then the image of $\widetilde{\alpha}$ contains $\mathbb{Z}/2\mathbb{Z} \cong \langle\sigma\rangle$, but $T(\mathbb{C})$ is connected, hence this is not possible.

Now, we can conclude the second claim about the impossibility of $\mathscr{M}$ as well. We know that X/S corresponds to a map $g\colon S \to \mathscr{M}$, and we know that $\pi^*X = E \times T$. Hence we have a commutative diagram

$$\begin{array}{ccccc} T & \xrightarrow{\pi} & S & \xrightarrow{f} & M \\ {\scriptstyle\pi}\downarrow & & & & \downarrow{\scriptstyle\mathrm{id}} \\ S & & \xrightarrow[g]{} & & M \end{array}$$

Since the image of f is $e \in \mathscr{M}(\mathbb{C})$, the same is true of g, hence $g = d$, but this contradicts our first claim.

There is a second way in which we can see that $\mathscr{M}$ cannot exist. If $\mathscr{M}$ existed, then

it would mean that $\mathrm{Hom}_{\mathbf{Sch}}(-,\mathscr{M})$ is a sheaf of sets on **Aff** with respect to the étale topology. Now, consider the two curves

$$E_1 : y^2 = x^3 + x + 1, \;\; E_2 : 3y^2 = x^3 + x + 1.$$

These are not isomorphic over $\mathbb{Q}$, but they are isomorphic over $\mathbb{Q}(\sqrt{3})$ which implies that

$$\mathrm{Hom}_{\mathbf{Sch}}(\mathrm{Spec}\,\mathbb{Q}), \mathscr{M}) \to \mathrm{Hom}_{\mathbf{Sch}}(\mathrm{Spec}\,\mathbb{Q}(\sqrt{3}), \mathscr{M})$$

is not injective, so it cannot be a sheaf, and therefore $\mathscr{M}$ does not exist.

We can fix these issues by considering

$$\{\text{isomorphism classes } (E/S, \alpha) \mid \alpha \text{ is a level structure } \}$$

where α is some data attached to E/S so that $\mathrm{Aut}(E/S, \alpha)$ is trivial. This choice of α is motivated by the classical theory of modular forms.

6.0.1 Representability

We will work in the category **Ell** whose objects are elliptic curves

$$\begin{array}{c} E \\ \downarrow \pi \\ S \end{array}$$

over variable base-schemes. The morphisms in this category are cartesian squares of elliptic curves

$$\begin{array}{ccc} E_1 & \xrightarrow{a} & E \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi} \\ S_1 & \xrightarrow[f]{} & S \end{array}$$

This means that there is an isomorphism of elliptic curves over S_1

$$E_1 \xrightarrow{a \times_S \pi_1} E \times_S S_1$$

We will be interested in moduli problems in this category.

Definition 6.0.1. A contravariant functor $\mathscr{P}\colon \mathbf{Ell} \to \mathbf{Sets}$ is called a *moduli problem for elliptic curves*. Given an elliptic curve E/S, an element of $\mathscr{P}(E/S)$ is called a *level $\mathscr{P}$ structure* on E/S. The category of *elliptic curves with $\mathscr{P}$ structure* is denoted $\mathbf{Ell}_{\mathscr{P}}$. The objects are pairs $(E/S,\alpha)$ with $\alpha \in \mathscr{P}(E/S)$. A morphism in the category from $(E'/S',\alpha')$ to $(E/S,\alpha)$ is an element $\phi \in \mathrm{Hom}_{\mathbf{Ell}}(E'/S',E/S)$ such that the map of sets $\mathscr{P}(\phi)\colon \mathscr{P}(E'/S') \to \mathscr{P}(E/S)$ maps α' to α. There is a forgetful functor

$$F_{\mathscr{P}}\colon \mathbf{Ell}_{\mathscr{P}} \to \mathbf{Ell}.$$

Definition 6.0.2. We say that a moduli problem $\mathscr{P}$ is *representable* if it is representable as a functor on **Ell**, meaning that there exists an elliptic curve over a scheme

$$\begin{array}{c} \mathscr{E} \\ \downarrow \\ \mathscr{M}(\mathscr{P}) \end{array}$$

together with a functorial isomorphism

$$\mathscr{P}(E/S) \cong \mathrm{Hom}_{\mathbf{Ell}}(E/S, \mathscr{E}/\mathscr{M}(\mathscr{P}))$$

If a moduli problem $\mathscr{P}$ is representable by $\mathscr{E}/\mathscr{M}(\mathscr{P})$, then the scheme $\mathscr{M}(\mathscr{P})$ represents the functor on **Sch** sending a scheme S to the set of isomorphism classes of pairs $(E/S,\alpha)$ with E an elliptic curve over S and $\alpha \in \mathscr{P}(E/S)$ a level $\mathscr{P}$ structure on E/S.

Every elliptic curve E/S defines a representable moduli problem

$$H^{E/S} = \mathrm{Hom}_{\mathbf{Ell}}(-, E/S)$$

given by sending an elliptic curve E'/S' to the set of pairs of morphisms $(f'\colon S' \to S, g'\colon E' \to E)$ such that the square

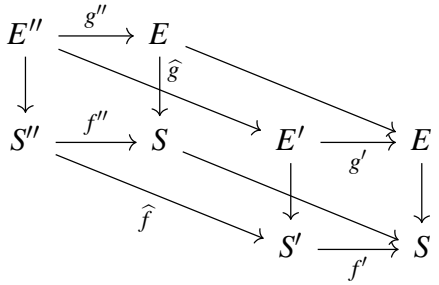
$$\begin{array}{ccc} E' & \xrightarrow{g'} & E \\ \downarrow & \square & \downarrow \\ S' & \xrightarrow{f'} & S \end{array}$$

is cartesian. Similar to a $\mathscr{P}$ structure, we say that an element of $h^{E/S}(E'/S')$ is an E/S-

structure on E'/S'. Then the category of elliptic curves with E/S-structure has cartesian squares

$$\begin{array}{ccc} E' & \xrightarrow{g'} & E \\ \downarrow & \square & \downarrow \\ S' & \xrightarrow{f'} & S \end{array}$$

as objects and a morphism taking $(E''/S'', f'', g'')$ to $(E'/S', f', g')$ the morphism $(\widehat{f}, \widehat{g}) \in \mathrm{Hom}_{\mathbf{Ell}}(E''/S'', E'/S')$ such that $f'\widehat{f} = f''$ and $g'\widehat{g} = g''$, i.e., so that the prism



commutes. This category is isomorphic to $\mathbf{Ell}_{h^{E/S}}$ and there is a forgetful functor

$$F_{E/S} \colon \mathbf{Ell}_{E/S} \to \mathbf{Ell}.$$

Definition 6.0.3. A moduli problem $\mathscr{P}'$ is *relatively representable* if for every elliptic curve E/S, the functor

$$\mathscr{P}' \circ F_{E/S} \colon \mathbf{Ell}_{E/S} \to \mathbf{Sets}$$

is representable.

Remark 6.0.4. For a moduli problem $\mathscr{P}'$, the above definition is equivalent to the following: for every elliptic curve E/S the functor

$$\begin{aligned} \overline{\mathscr{P}'} \colon \mathbf{Sch}_S &\to \mathbf{Sets} \\ T &\mapsto \mathscr{P}'(E \times_S T/T) \end{aligned}$$

is representable.

Proposition 6.0.5. *Let $\mathscr{P}'$ be a moduli problem. The following are equivalent:*

1. *$\mathscr{P}'$ is relatively representable.*

2. *For every representable moduli problem $\mathscr{P}$, the functor*

$$\mathscr{P}' \circ F_{\mathscr{P}} \colon \mathbf{Ell}_{\mathscr{P}} \to \mathbf{Sets}$$

is representable.

3. *For every representable moduli problem $\mathscr{P}$, the product moduli problem*

$$\begin{aligned} \mathscr{P} \times \mathscr{P}' \colon \mathbf{Ell} &\to \mathbf{Sets} \\ E/S &\mapsto \mathscr{P}(E/S) \times \mathscr{P}'(E/S). \end{aligned}$$

Proof. We see that $(1) \implies (2)$ from the definition. Conversely, since $\mathscr{P}$ is representable, $\mathscr{P} \cong h^{E/S}$ for some elliptic curve E/S, so (1) and (2) are equivalent.

For $(2) \implies (3)$, let $\mathscr{P}$ be a moduli problem represented by an elliptic curve E/S. If $\mathscr{P}' \circ F_{E/S} \colon \mathbf{Ell}_{E/S} \to \mathbf{Sets}$ is representable by an object

$$\begin{array}{ccc} E' & \longrightarrow & E \\ \downarrow & \square & \downarrow \\ S' & \longrightarrow & S \end{array}$$

then the object E'/S' represents $\mathscr{P} \times \mathscr{P}'$. Indeed, suppose we have another elliptic curve F/T, and are given a map $F/T \to E'/S'$ in **Ell**. Well, then this induces a map $F/T \to E/S$ in **Ell**, since we have

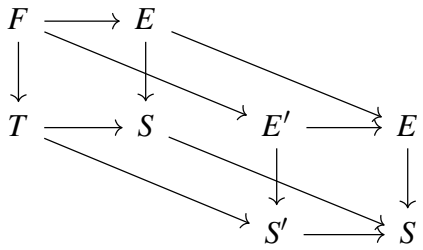
$$\begin{array}{ccccc} F & \longrightarrow & E' & \longrightarrow & E \\ \downarrow & \square & \downarrow & \square & \downarrow \\ T & \longrightarrow & S' & \longrightarrow & S \end{array}$$

and thus

$$F \cong E' \times_{S'} T \cong (E \times_S S') \times_{S'} T \cong E \times_S T$$

so we have a morphism $F/T \to E/S$ in **Ell**. Then, we also have a morphism in $\mathbf{Ell}_{E/S}$

which is clear from the diagram



Therefore, given a map $F/T \to E'/S'$ in **Ell**, we get a map $F/T \to E/S$ in **Ell** and a map $F/T \to E'/S'$ in $\mathbf{Ell}_{E/S}$, so E'/S' does indeed represent $\mathscr{P} \times \mathscr{P}'$.

Conversely, if $\mathscr{P} \times \mathscr{P}'$ is represented by an elliptic curve E'/S', then Yoneda's lemma gives a morphism $E'/S' \to E/S$ corresponding to the projection $\mathscr{P} \times \mathscr{P}' \to \mathscr{P}$. Viewing this as an object of $\mathbf{Ell}_{E/S}$, we get an object representing $\mathscr{P}' \circ F_{E/S}$. □

The following proposition finally shows that representability is a stronger condition than relative representability.

Proposition 6.0.6. *Every representable moduli problem is relatively representable.*

Proof. Let $\mathscr{P}$ be a representable moduli problem. The result relies on the existence of products in **Ell**, that is, given two elliptic curves E/S and E'/S', there exists an elliptic curve E''/S'' with morphisms to E/S and E'/S' such that the map of sets

$$\mathrm{Hom}_{\mathbf{Ell}}(F/T, E''/S'') \to \mathrm{Hom}_{\mathbf{Ell}}(F/T, E/S) \times \mathrm{Hom}_{\mathbf{Ell}}(F/T, E'/S')$$

is an isomorphism for all elliptic curves F/T. The proof of this fact goes beyond the scope of this thesis but can be found in [25, III, Theorem 2.5].

Then $\mathscr{P} \times \mathscr{P}'$ is representable for every representable moduli problem $\mathscr{P}'$, so by Proposition 6.0.5, $\mathscr{P}$ is relatively representable. □

Definition 6.0.7. Let $\mathscr{P}$ be a moduli problem. For any elliptic curve E/S, with $f\colon E \to S$, the group

$$\mathrm{Aut}_S(E) = \left\{ g\colon E \xrightarrow{\sim} E \mid fg = f \right\}$$

acts on the set $\mathscr{P}(E/S)$ by the functorality of $\mathscr{P}$. The moduli problem $\mathscr{P}$ is *rigid* if $\mathrm{Aut}_S(E)$ acts freely on $\mathscr{P}(E/S)$, meaning that for every elliptic curve E/S and every $\alpha \in \mathscr{P}(E/S)$, the only element of $\mathrm{Aut}_S(E)$ fixing α is the identity.

Definition 6.0.8. If $\mathscr{P}$ is relatively representable, we say that $\mathscr{P}$ is *affine* (resp. *étale, finite, etc.*) if for every elliptic curve E/S, the object representing $\mathscr{P} \circ F_{E/S}$, $\mathscr{M}_{\mathscr{P},E/S}$, is affine (resp. étale, finite, etc.) over S.

The following theorem will be used to show that the moduli problem we will be interested in is representable. A proof can be found in [7].

Theorem 6.0.9. *[7, Theorem 4.7.0] Let $\mathscr{P}$ be relatively representable and affine over* **Ell**. *Then $\mathscr{P}$ is representable if and only if $\mathscr{P}$ is rigid.*

We will also use the following corollary.

Corollary 6.0.10. *[7, Corollary 4.7.1] Any relatively representable moduli problem $\mathscr{P}$ which is affine and étale over* **Ell***, and rigid, is representable by a smooth affine curve over $\mathbb{Z}$.*

6.0.2 Level-N Structures

We now turn our attention to the specific moduli problem on elliptic curves that will be of interest for the rest of this thesis: full level-N structures on elliptic curves.

If S is a scheme, E/S is an elliptic curve, and $N \geq 1$ is an integer, then we denote by $E[N]$ the kernel of the multiplication by N map $E \to E$, which is really the preimage of the zero section. This turns out to be a finite locally free group scheme of rank N^2 over S, and it is étale if N is invertible on S [7, Theorem 2.3.1].

Definition 6.0.11. A *full level-N structure*, or a $\Gamma(N)$-structure, on an elliptic curve E/S where S is a scheme, is a group homomorphism

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

which is a generator of $E[N]$, i.e., we have an equality of effective Cartier divisors in E

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

Note that if N is invertible on S, then $E[N]$ is an étale group scheme, then we can show that a full level-N structure is just a pair of linearly independent elements of $E[N]$, [26, p. 6].

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

Theorem 6.0.12. *The moduli problem* $[\Gamma(n)]$ *is representable for* $n \geq 3$ *and its moduli scheme is a smooth affine curve over* $\operatorname{Spec}\mathbb{Z}[1/n]$.

Proof. By [7, Theorem 3.7.1], $[\Gamma(n)]$ is relatively representable and finite étale. Then, $\Gamma(n)$ is rigid by [7, Corollary 2.7.2], so by [7, Theorem 4.7.0], since $[\Gamma(n)]$ for $n \geq 3$ is relatively representable and rigid, it is representable. □

Example 6.0.13. By [25, p. 148], we can write the scheme representing $[\Gamma(3)]$ explicitly as

$$\mathscr{M}_3 = \operatorname{Spec}\left(\mathbb{Z}\left[\zeta_3, \frac{1}{3}, \mu, (\mu^3-1)^{-1}\right]\right)$$

where ζ_3 is a third root of unity. We can then also write the universal elliptic curve sitting over $\mathscr{M}_3$ as

$$\mathscr{E} : X^3 + Y^3 + Z^3 = 3\mu XYZ.$$

A more in depth explanation of this calculation can be found in [24]. In [27, §3.5], there are tables for calculating these schemes, but they become quite unwieldily quite quickly.

Later on we will also consider the moduli problem which assigns to an elliptic curve E/S, two level-N structures. This can be viewed as a product of the moduli problem $\Gamma[N] \times \Gamma[N] \colon \mathbf{Ell} \to \mathbf{Sets}$, and thus by Proposition 6.0.5, it is representable since $[\Gamma(N)]$ is.

7

The Canonical Subgroup

The canonical subgroup of an elliptic curve was first studied by Lubin [28], and was extended by Katz [29]. If an elliptic curve has ordinary reduction, then the canonical subgroup is a canonical lift of the kernel of the Frobenius morphism on E modulo p. We follow the exposition given in [30] and [31].

Let $K/\mathbb{Q}_p$ be a finite extension, and let $R = \mathcal{O}_K$, and let E/R be an elliptic curve. Let k be the residue field of K. Then $E(\overline{K})[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$ contains $p+1$ subgroups of order p. These $p+1$ subgroups will vary as the elliptic curve varies, however there is one "canonical subgroup" that varies smoothly as the curve varies smoothly.

If E has ordinary reduction, then $E(\overline{k})[p] \cong \mathbb{Z}/p\mathbb{Z}$, so the kernel of

$$E(\overline{K})[p] \to E(\overline{k})[p]$$

is a cyclic subgroup of $E(\overline{K})$ of order p; this is the *canonical subgroup* of E, we denote it by E^{can}.

Remark 7.0.1. If E is not too supersingular, then it also has a canonical subgroup, but that will not be necessary for our work. Indeed, there is a number called the *Hasse invariant* that can be attached to an elliptic curve. As long as the Hasse invariant is less than $\frac{p}{p+1}$, we can designate a canonical subgroup of the elliptic curve [30].

Example 7.0.2. We provide an example from [30] of an elliptic curve that is not too

supersingular to illustrate this idea. Let $a \in \overline{\mathbb{Q}}_2$ (an algebraic closure of $\mathbb{Q}_2$), with $|a|_2 \leq 1$ and define the elliptic curve

$$E_a \colon y^2 + y + axy = x^3 + x^2.$$

We can reduce this curve modulo 2 and there are two cases. First, if $|a|_2 = 1$, then the curve reduces to

$$y^2 + y + \bar{a}xy = x^3 + x^2$$

which is an ordinary elliptic curve over $\overline{\mathbb{F}}_2$. However, in the second case, if $|a|_2 < 1$, then the curve E_a reduces to

$$y^2 + y = x^3 + x^2$$

which is supersingular. To help figure out what happens in the second case we put the curve into canonical form, define $Y = y + \frac{1}{2}(1 + ax)$ and the equation for E_a becomes $Y^2 = f(x)$ where

$$f(x) = x^3 + \left(\frac{a^2}{4} + 1\right)x^2 + \frac{a}{2}x + \frac{1}{4}.$$

The points of order 2 on E_a correspond to the roots of $f(x)$. We now look at the valuation of these roots to help us establish what the canonical subgroup should be. We do this using Newton polygons and we break it up into three cases:

1. If $|a|_2 = 1$, then the valuations of the coefficients of $f(x)$ are $0, -2, -1, -2$. Hence f has one root with valuation -2 and two roots with valuation 0. The root with valuation -2 is the one which reduces to the point at infinity in the reduction map.

2. If $|a|_2 = 1 - \varepsilon$ with ε small, then a similar argument shows that one of the roots of f has valuation $-2 + 2\varepsilon$ and the other two have valuation $-\varepsilon$. One of these is quite different from the other, and it does not reduce to the point at infinity in the reduction map, so this point will generate the canonical subgroup of E_a.

3. If $|a|_2$ is very small, then all three of the roots will have valuation $-2/3$ and we cannot distinguish them in a canonical manner.

Remark 7.0.3. By [29, Theorem 3.1], if E is an elliptic curve over an $\mathbb{F}_p$-algebra R, then the canonical subgroup is exactly the kernel of the Frobenius map on E.

Remark 7.0.4. In the case when E is an ordinary elliptic curve, let $[p]_E$ be the multiplication by p map. Since E is ordinary, exactly p points in $\ker[p]_E$ go to the identity under reduction modulo p. Thus we have

$$\ker(\text{reduction modulo } p) \cap \ker[p]_E$$

is the subgroup of E of order p whose associated subgroup scheme is the lifting of the kernel of Frobenius map [28].

The most important point of the canonical subgroup is that for ordinary elliptic curves over a characteristic p ring, the canonical subgroup is the kernel of the Frobenius [29], while over a mixed characteristic ring, it is a lifting of the Frobenius morphism [28].

8

Canonical Lifts

8.0.1 Statement of the Theorem

Let R be a ring in which p is nilpotent. There is a lift of the Frobenius map on the Witt vectors of R given by

$$\begin{aligned} F &: W_{n+1}(R) \to W_n(R) \\ &(x_0,\ldots,x_n) \mapsto r_n(x_0,\ldots,x_n)^p + p\delta(x_0,\ldots,x_n) \end{aligned}$$

where $r_n : W_{n+1}(R) \to W_n(R)$ is the truncation map, $r(x_0,\ldots,x_n) = (x_0,\ldots,x_{n-1})$, and the δ-map is given by $\delta(x_0,\ldots,x_n) = (x_1,\ldots,x_n)$. By taking the limit along the truncation maps r_n, we obtain a map

$$F : W(R) \to W(R)$$

such that for any $n \geq 1$, $F(x_0,x_1,\ldots) = r(x_0,x_1,\ldots)^p + pW_n(R)$, where $r : W(R) \to W_n(R)$ is the natural projection. This map is a lift of the Frobenius on $W(R)$. From the map $F : W_{n+1}(R) \to W_n(R)$ we get a map

$$\operatorname{Spec}(F) : \operatorname{Spec} W_n(R) \to \operatorname{Spec} W_{n+1}(R)$$

and by the properties of W_n this is a map $\operatorname{Spec}(F) : W_n(T) \to W_{n+1}(T)$ where $T = \operatorname{Spec} R$. Taking the colimit of this map gives a map $\operatorname{Spec}(F) : W(S) \to W(S)$. By taking colimits

again, we get a lift of the Frobenius $\mathrm{Spec}(F)\colon W(S) \to W(S)$ for an arbitrary $S \in \mathbf{Aff}^{\sim}$. By abuse of notation, we will denote this Frobenius lift on $W(S)$ by F as well. This Frobenius lift agrees with the usual pth power Frobenius on the special fiber over p, $\mathrm{Spec}\,\mathbb{F}_p \times_{\mathrm{Spec}\,\mathbb{Z}} W(S)$. This leads us to the following definition.

Definition 8.0.1. A *Frobenius lift* on an elliptic curve E over $W(S)$ is a morphism $E \to F^*(E)$ of elliptic curves over $W(S)$ restricting to the usual Frobenius map over the locus $\mathrm{Spec}\,\mathbb{F}_p \times_{\mathrm{Spec}\,\mathbb{Z}} W(S)$.

Now we're able to state the final version of the theorem we seek to prove.

Theorem 8.0.2. *There is a unique way of lifting ordinary elliptic curves E over p-adic sheaves S to elliptic curves $\widetilde{E}$ over $W(S)$ such that the construction $E \mapsto \widetilde{E}$ is compatible with base change in S and such that each $\widetilde{E}$ admits a Frobenius lift.*

The uniqueness statement in the theorem needs to be clarified. if $E \to \check{E}$ is any other such construction, then there is a unique family of morphisms $\widetilde{E} \to \check{E}$ where E runs over all ordinary elliptic curves E over all p-adic base sheaves S. This uniqueness statement does not apply to lifts of a single elliptic curve or even all elliptic curves over a given base S, but only to all families of elliptic curves over all bases.

While in [2], this theorem is proved directly for S a p-adic sheaf, we will work with an affine scheme $S = \mathrm{Spec}\,R$ where p is nilpotent on R. Then taking colimits, we will be able to obtain the same result with a simpler exposition. Indeed, the construction will be compatible with base change along morphisms of affine schemes, so if S is an arbitrary p-adic sheaf and E is an ordinary elliptic curve over S, we can write $S = \mathrm{colim}_i S_i$ where each S_i is an affine scheme on which p is nilpotent, and define $\widetilde{E}$ over $W(S)$ to be $\mathrm{colim}_i (E_{S_i})^{\sim}$ over $W(S) = \mathrm{colim}_i W(S_i)$. So we may proceed with S as an affine scheme with p nilpotent without issue.

8.0.2 Existence With Level Structure

The first step in proving Theorem 8.0.2 is to prove it in the presence of more structure.

Proposition 8.0.3. *There is a unique way of lifting ordinary elliptic curves $(E/S, \xi)$ with a full level-N structure over an affine scheme S with p nilpotent, to an elliptic curve $(E/W(S), \xi)^{\sim}$ such that the construction $(E/S, \xi) \mapsto (E/W(S), \xi)^{\sim}$ is compatible with base change in S and such that $(E/S, \xi)^{\sim}$ admits a Frobenius lift.*

Proof. Let $Y(N)$ denote the moduli space of elliptic curves E/S with full level-N structure, i.e. with morphisms $\xi\colon (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N](S)$. We assume that $p \nmid N$ and that $N \geq 3$ to make the moduli problem representable by Theorem 6.0.12. In this case $Y(N)$ is a smooth affine scheme of relative dimension 1 over $\operatorname{Spec}(\mathbb{Z}[1/N])$.

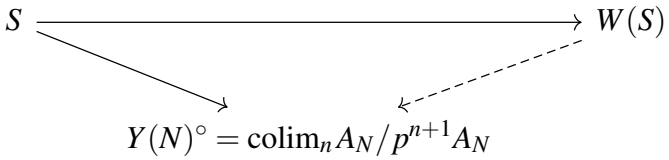
Let T denote the open subscheme of $Y(N)$ which is the complement of the supersingular locus on the fiber over p, and let $Y(N)^\circ$ denote it's p-adic completion. $Y(N)_p = Y(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{F}_p$, and the supersingular locus of $Y(N)_p$ is the set of points corresponding to supersingular elliptic curves. These points are finite and isolated, removing them gives the ordinary locus T. Then the p-adic completion of T is given by

$$\widehat{T} = Y(N)^\circ = \operatorname{colim}_n \operatorname{Spec} \mathbb{Z}/p^{n+1}\mathbb{Z} \times_{\operatorname{Spec}\mathbb{Z}} T.$$

Now, since $Y(N)$ is affine, write $Y(N) = \operatorname{Spec} R$, and let $Q \subseteq R$ be such that $\operatorname{Spec} R[Q^{-1}]/(p)$ is the ordinary locus of the fiber of $Y(N)$ over p, $Y(N)_p$. So Q is a subset of elements that defines an open subscheme and avoids the supersingular locus in characteristic p. Then if A_N is the p-adic completion of $R[Q^{-1}]$, we have

$$Y(N)^\circ \cong \operatorname{colim}_n \operatorname{Spec} A_N/p^{n+1}A_N$$

and A_N is p-adically complete and p-torsion free, so we actually see that $Y(N)^\circ \cong \operatorname{Spf}(A_N)$. The reason for writing $Y(N)^\circ \cong \operatorname{colim}_n \operatorname{Spec} A_N/p^{n+1}A_N$ in this form is that now it is in the form needed to apply the universal property of Witt vectors for p-adic sheaves from Section 5:



if we can obtain a map $S \to Y(N)^\circ$.

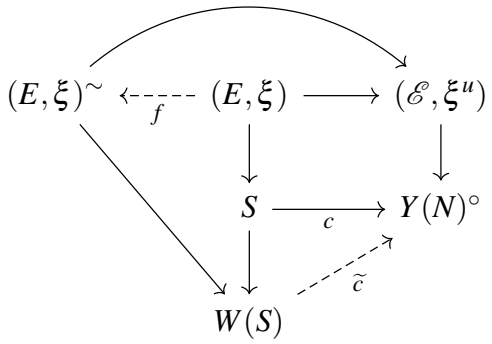
Now, let (E, ξ) be an ordinary elliptic curve with level-N structure over an affine scheme S with p nilpotent. Since the moduli problem of elliptic curves with full level-N structure is representable, the pair (E, ξ) is the pull-back of the universal object $(\mathscr{E}, \xi^u)$ through a unique map $c\colon S \to Y(N)^\circ$:

$$\begin{array}{ccc} (E,\xi) & \longrightarrow & (\mathscr{E},\xi^u) \\ \downarrow & & \downarrow \\ S & \xrightarrow[c]{} & Y(N)^\circ \end{array}$$

This gives us the map we needed to apply the universal property of Witt vectors for p-adic sheaves, write

$$\widetilde{c}\colon W(S) \to Y(N)^\circ$$

for the morphism induced by c. We then let $(E,\xi)^\sim$ denote the canonical lift of (E,ξ) which is the pull-back $\widetilde{c}^*((\mathscr{E},\xi^u))$ of the universal elliptic curve with level-N structure. The following diagram depicts the situation:



□

The map $f\colon (E,\xi) \to (E,\xi)^\sim$ will denote the canonical lift. We do not yet write $(E,\xi)^\sim = (\widetilde{E},\widetilde{\xi})$ since we have not yet shown that the canonical lift is independent of the choice of level-N structure.

8.0.3 Standard Frobenius Lift on $Y(N)^\circ$

We quickly review the standard Frobenius lift on $Y(N)^\circ$ because a similar strategy will be used to show that the canonical lift functor for curves with level-N structure is independent of the choice of the level-N structure.

Let E be an ordinary elliptic curve over an affine scheme S on which p is nilpotent, and let E^{can} denote its canonical subgroup. Let E/E^{can} denote the usual quotient, by this we mean the quotient in the fppf topology and not the quotient object in $\mathbf{Aff}^\sim$. Thus E/E^{can} is also a family of elliptic curves over S and the quotient map $E \to E/E^{\text{can}}$ is faithfully flat.

If, ξ is a level-N structure on E, then its image $\overline{\xi}$ in E/E^{can} is also a level-N structure. We then let ψ denote the map $Y(N)^\circ \to Y(N)^\circ$ that, for any S, sends an S-valued point (E,ξ) to $(E/E^{\mathrm{can}},\overline{\xi})$. It is a Frobenius lift because for ordinary elliptic curves over $\mathbb{F}_p$-algebras, the connected component of the p-torsion subgroup scheme agrees with the kernel of the Frobenius by [28].

8.0.4 Independence of Level Structure

Proposition 8.0.4. *The construction sending $(E/S,\xi) \to (E/S,\xi)^\sim$ is independent of the choice ξ on E/S.*

Proof. Let $Y(N,N)$ denote the moduli space of elliptic curves with a pair of full level-N structures (ξ_1,ξ_2) . Forgetting one or the other defines projections $Y(N,N) \rightrightarrows Y(N)$, both of which are finite étale.

Now we proceed as before; let $Y(N,N)^\circ$ denote the p-adic completion of the complement of the supersingular locus on the fiber over p. Then again $Y(N,N)^\circ$ is of the form $\mathrm{colim}_n A_{N,N}/p^{n+1}A_{N,N}$ where $A_{N,N}$ is a p-adically complete and p-torsion-free ring and it has a Frobenius lift, ψ, given by sending an elliptic curve to its quotient by the canonical subgroup with the image of the level structures.

This defines a theory of canonical lifts for elliptic curves with pairs of full level-N structures. It is compatible with the projections $Y(N,N) \rightrightarrows Y(N)$ in the sense that taking the canonical lift commutes with forgetting each of the level structures. This is because the Frobenius lift commutes with the projections. □

8.0.5 Canonical Lifts in Generality

Now we proceed to full generality.

Proceeding as above, let E be an ordinary curve over an affine scheme S in which p is nilpotent. In contrast to what we have done previously, we are not assuming that there is a level-N structure on E/S. It is possible that no such structure exists on E/S. Since N is co-prime to p, and by the Serre-Tate Theorem on good reduction ensures that there exists an S' and that the curve $E \times_S S'$ has a level-N structure over S', and that the map $f\colon S' \to S$ is finite étale and a cover [1]. The S' that we obtain is universal because any other S'' will be an S'-scheme.

Let ξ be the level-N structure on $(E \times_S S')/S'$, then this corresponds to a unique map $c_1 : S' \to Y(N)^\circ$. We obtain the following diagram

$$\begin{array}{ccc} S' \times_S S' & \xrightarrow[c_2]{} & Y(N,N)^\circ \\ \downarrow\downarrow & & \downarrow\downarrow \\ S' & \xrightarrow[c_1]{} & Y(N)^\circ \end{array}$$

Both columns of this diagram have the structure of a groupoid. We quickly recall this construction:

Definition 8.0.5. A *groupoid* is a category in which every morphism is invertible.

A groupoid can be denoted $G_1 \rightrightarrows G_0$ where G_1 is the set of morphisms and the two arrows represent the source and the target. So if the two morphisms are f and g, then for some $\alpha \in G_1$, the morphism is $\alpha\colon f(\alpha) \to g(\alpha)$.

In our diagram above, $Y(N,N)^\circ \to Y(N)^\circ$ is a groupoid, where the morphisms are of the form (E, ξ_1, ξ_2) which maps (E, ξ_1) to (E, ξ_2), since the two maps forget one fo the level structures. Composition of these maps is given by

$$(E, \xi_1, \xi_2) \circ (E', \xi_1', \xi_2') = (E, \xi_1, \beta^*(\xi_2'))$$

whenever there exists $\beta\colon (E, \xi_2) \xrightarrow{\sim} (E', \xi_1')$, which is unique if it exists.

The fiber product $S' \times_S S'$ also defines a groupoid. Indeed, we have the two projection maps $S' \times_S S' \rightrightarrows S'$ which give us the source and target maps. The objects of the groupoid are the points in S', and composition is given in the following way: by [18, Tag 01JT] a point of $S' \times_S S'$ can be represented by a quadruple $(x, y, s, \mathfrak{p})$ where $x, y \in S'$ and $s \in S$ such that if $f(x) = f(y) = s$ where f is the map from $S' \to S$, and $\mathfrak{p}$ is a prime ideal of the ring $\kappa(x) \times_{\kappa(s)} \kappa(y)$ which corresponds to the residue field of the point $(x, y, s, \mathfrak{p})$. Given two points $(x, y, s, \mathfrak{p})$ and $(x', y', s', \mathfrak{p}')$ we can compose them if $y = x'$. In this case we would get

$$(x, y, s, \mathfrak{p}) \circ (y, z, s, \mathfrak{p}') = (x, z, s, \mathfrak{p}'').$$

Now that we have these structures, we see that the diagram is actually a morphism of groupoid structures. We can again use the universal property of Witt vectors for schemes since the column $Y(N,N)^\circ \rightrightarrows Y(N)^\circ$ has a Frobenius lift which is compatible with the projections, we get maps $W(S' \times_S S') \xrightarrow{\widetilde{c_2}} Y(N,N)^\circ$ and $S' \xrightarrow{\widetilde{c_1}} Y(N)^\circ$ which fit into the

following diagram:

$$\begin{array}{ccc} W(S' \times_S S') & \xrightarrow{\widetilde{c}_2} & Y(N,N)^\circ \\ \downarrow\downarrow & & \downarrow\downarrow \\ W(S') & \xrightarrow[\widetilde{c}_1]{} & Y(N)^\circ \end{array}$$

Since truncated Witt vectors for schemes preserve étale base change by 5.0.1 we have

$$W(S' \times_S S') = \operatorname{colim}_n W_n(S' \times_S S') = \operatorname{colim}_n W_n(S') \times_{W_n(S)} W_n(S') = W(S') \times_{W(S)} W(S')$$

and the diagram above becomes

$$\begin{array}{ccc} W(S') \times_{W(S)} W(S') & \xrightarrow{\widetilde{c}_2} & Y(N,N)^\circ \\ \downarrow\downarrow & & \downarrow\downarrow \\ W(S') & \xrightarrow[\widetilde{c}_1]{} & Y(N)^\circ \end{array}$$

which is again a morphism of groupoid objects, and this actually gives us a descent datum of a family over $W(S')$ to $W(S)$. Indeed, a descent datum can be given by a groupoid by [18, Tag 0APC], the category of groupoid schemes which are cartesian over $(X, X \times_Y X, \mathrm{pr}_0, \mathrm{pr}_1, c)$ is equivalent to the category of descent data relative to X/Y where $f\colon X \to Y$ is a morphism of X schemes. This translates to our situation in the following way: we have

$$\begin{array}{ccccc} (\widetilde{E}, \widetilde{\xi}_1, \widetilde{\xi}_2) & \longrightarrow & W(S') \times_{W(S)} W(S') & \longrightarrow & Y(N,N)^\circ \\ \downarrow\downarrow & & \downarrow\downarrow & & \downarrow\downarrow \\ (\widetilde{E}, \widetilde{\xi}) & \longrightarrow & W(S') & \longrightarrow & Y(N)^\circ \end{array}$$

where the curve $(\widetilde{E}, \widetilde{\xi}_1, \widetilde{\xi}_2)$ corresponds to the map $\widetilde{c}_2\colon W(S') \times_{W(S)} W(S') \to Y(N,N)^\circ$ and $(\widetilde{E}, \widetilde{\xi})$ corresponds to the map $\widetilde{c}_1\colon W(S') \to Y(N)^\circ$. We then have two projections $(\widetilde{E}, \widetilde{\xi}_1, \widetilde{\xi}_2) \to (\widetilde{E}, \widetilde{\xi})$, each forgetting one of the level-N structures, and thus it is a groupoid.

Note that the curve we get from the pullback of $\widetilde{c}_1$ and the curve from the pullback of $\widetilde{c}_2$ are the same curve because we also get two maps $p_i \circ c_2\colon W(S') \times_{W(S)} W(S') \to Y(N)^\circ$ for $i = 1,2$ where $p_i\colon Y(N,N)^\circ \to Y(N)^\circ$ are the maps which forget one of the level-N

structures. Then we have the diagram

$$\begin{array}{ccc}
(\widetilde{E},\widetilde{\xi}_1,\widetilde{\xi}_1) & \longrightarrow & (\mathscr{E},\xi_1^u,\xi_2^u) \\
\downarrow & & \downarrow \\
W(S')\times_{W(S)} W(S') & \xrightarrow[\widetilde{c}_2]{} & Y(N,N)^\circ \\
 & \searrow & \downarrow{\scriptstyle p_1} \quad \downarrow{\scriptstyle p_2} \\
 & \searrow & Y(N)^\circ
\end{array}$$

and we get two elliptic curves with level-N structure, $(p_1\circ\widetilde{c}_2)^*(\mathscr{E})$ and $(p_2\circ\widetilde{c}_2)^*(\mathscr{E})$, and these curves will agree with the one coming from $\widetilde{c}_2$.

To see that the left square in the above diagram is cartesian in the category of schemes over the groupoid $(W(S'),W(S')\times_{W(S)}W(S'))$, and hence gives a descent data, note that if $(\mathscr{E},\xi^u)$ is the universal object, we have

$$\begin{aligned}
\widetilde{E}\times_{W(S')}\left(W(S')\times_{W(S)}W(S')\right) &= (\mathscr{E}\times_{Y(N)^\circ}W(S'))\times_{W(S')}\left(W(S')\times_{W(S)}W(S')\right) \\
&= \mathscr{E}\times_{Y(N)^\circ}\left(W(S')\times_{W(S)}W(S')\right) \\
&= \widetilde{E}
\end{aligned}$$

by the above remarks. And thus it is indeed a cartesian square and we do get a descent datum.

Further, since W preserves epimorphisms because it is a left adjoint, the map $W(S')\to W(S)$ is an effective descent [18, Tag 0BTJ]. So we can define $\widetilde{E}$ to be the object descended over $W(S)$. This is our canonical lift in the general setting, it is unique up to isomorphism, and we can extended this construction to general p-adic sheaves by taking colimits.

8.0.6 Frobenius Lifts

Proposition 8.0.6. *Let E/S be an elliptic curve and let $\widetilde{E}/W(S)$ be the canonical lift. Then there exists a Frobenius lift*

$$\widetilde{E}\to F^*(\widetilde{E})$$

where F denotes the Frobenius on Witt Vectors $F\colon W(S)\to W(S)$.

Proof. We begin by defining a map

$$\eta_E \colon \widetilde{E}/\widetilde{E}^{\mathrm{can}} \xrightarrow{\sim} F^*(\widetilde{E})$$

We want to show that if such an η_E exists, then the composition

$$\widetilde{E} \to \widetilde{E}/\widetilde{E}^{\mathrm{can}} \xrightarrow{\sim} F^*(\widetilde{E})$$

with $\widetilde{E} \to \widetilde{E}/\widetilde{E}^{\mathrm{can}}$ being the usual quotient map, is a Frobenius lift. We first need the following lemma.

Lemma 8.0.7. *If such an η_E exists, then it is unique.*

Proof. Suppose there are two isomorphisms

$$\eta_1, \eta_2 \colon \widetilde{E}/\widetilde{E}^{\mathrm{can}} \to F^*(\widetilde{E})$$

such that the composition with the quotient map $\widetilde{E} \to \widetilde{E}/\widetilde{E}^{\mathrm{can}}$ is a Frobenius lift. It is enough to check that the agree after any base change to a $W_n(S_i)$ where S_i is an arbitrary affine scheme which maps to S with p nilpotent.

However, the difference of two such maps is zero over $\operatorname{Spec}\mathbb{F}_p \times_{\operatorname{Spec}\mathbb{Z}} W_n(S_i)$ since by the definition of a Frobenius lift in this setting 8.0.1, both η_1 and η_2 will reduce to the usual Frobenius map in characteristic p, and thus their difference is zero. Finally, by the Rigidity Theorem [7, Theorem 2.4.2], $\eta_1 - \eta_2$ will be zero on $W_n(S_i)$ since it is zero on the special fiber. □

Now, to show that η_E exists globally, we can simply show that it exists locally. Thus, we may assume that E admits a level-N structure and then, by base change, that $S = Y(N)^\circ$ and that E is the universal elliptic curve $\mathscr{E}/Y(N)^\circ$.

There is a classifying morphism $c = \widetilde{\mathrm{id}} \colon W(Y(N)^\circ) \to Y(N)^\circ$:

$$\begin{array}{ccc} \widetilde{\mathscr{E}} & \longrightarrow & \mathscr{E} \\ \downarrow & & \downarrow \\ W(Y(N)^\circ) & \xrightarrow[c]{} & Y(N)^\circ \end{array}$$

and this map c is Frobenius equivariant meaning that

$$c^*\psi^*(\mathscr{E}) = F^*c^*(\mathscr{E})$$

where ψ is the lift of the Frobenius on $Y(N)^\circ$ which takes $\psi^(\mathscr{E}) = \mathscr{E}/\mathscr{E}^{\text{can}}$ and F is the lift of the Frobenius on $W(Y(N)^\circ)$. In addition, these maps are compatible with the level structure. We have

$$\widetilde{\mathscr{E}}/\widetilde{\mathscr{E}}^{\text{can}} = c^*(\mathscr{E}/\mathscr{E}^{\text{can}}) = c^*\psi^* = F^*c^*(\mathscr{E}) = F^*(\widetilde{\mathscr{E}})$$

and these identifications are compatible with the level structure, and hence unique.

Finally, the composition $\widetilde{\mathscr{E}} \to \widetilde{\mathscr{E}}/\widetilde{\mathscr{E}}^{\text{can}} = F^*(\widetilde{\mathscr{E}})$ reduces to the pth power Frobenius map modulo p because, writing

$$\widetilde{\mathscr{E}_0} = \operatorname{Spec}\mathbb{F}_p \times_{\operatorname{Spec}\mathbb{Z}} \widetilde{\mathscr{E}}$$

the actual Frobenius map $\widetilde{\mathscr{E}_0} \to \text{Fr}^*(\widetilde{\mathscr{E}_0})$ has kernel $\widetilde{\mathscr{E}_0}^{\text{can}}$ and is compatible with the level structure.

Thus, we have our desired Frobenius lift.

□

8.0.7 Uniqueness

Now that we have constructed the functor $E \to \widetilde{E}$, we would like to show it is unique. The following theorem is proved in full generality in [2, Theorem 6.1], but we will only need it in the case where E is the universal elliptic curve corresponding to the identity morphism $\text{id} \in \text{Hom}_{\mathbf{Sch}}(Y(N)^\circ, Y(N)^\circ)$.

Theorem 8.0.8. *Let R be a p-adically complete ring such that $W(R)$ is p-torsion free. Let $S = \operatorname{colim}_n \operatorname{Spec} R/p^{n+1}R$, and let E be an ordinary elliptic curve over S. Suppose X_1 and X_2 are lifts of E to $W(S)$ with Frobenius lifts ψ_1 and ψ_2. Then there is a unique Frobenius equivariant isomorphism $\beta : X_1 \to X_2$ restricting to the identity on E.*

Proposition 8.0.9. *Suppose $E \mapsto \check{E}$ is another functor that satisfies the conditions of Theorem 8.0.2. Then there is a unique family of isomorphisms $\widetilde{E} \to \check{E}$, where E runs over all ordinary elliptic curves over all base schemes $S = \operatorname{Spec} R$ where p is nilpotent on R.*

Proof. Suppose we have another functor which sends $E \to \check{E}$, which sends elliptic curves E/S to elliptic curves $\check{E}/W(S)$ with a Frobenius lift which is compatible with change of base S. Our goal is to give an isomorphism $\check{E} \to \widetilde{E}$, but it is actually enough to give isomorphisms locally on S which are compatible with a base change of S. Thus, we can assume that E admits a level-N structure over S. Let $d\colon S \to Y(N)^\circ$ denote the classifying morphisms, i.e., the morphism that makes the following diagram a pullback:

$$\begin{array}{ccc} E & \longrightarrow & \mathscr{E} \\ \downarrow & & \downarrow \\ S & \xrightarrow[d]{} & Y(N)^\circ \end{array}$$

Now, since $Y(N)^\circ \cong \operatorname{colim}_n \operatorname{Spec} A_N/p^{n+1}A_N$, where A_N is p-adically complete and p-torsion free, we can apply Theorem 8.0.8 to the universal elliptic curve $\mathscr{E}/Y(N)^\circ$. The theorem gives a unique Frobenius equivariant isomorphisms

$$\check{\mathscr{E}} \xrightarrow{\sim} \widetilde{\mathscr{E}}$$

which restricts to the identity on $\mathscr{E}$. Since the constructions $E \mapsto \check{E}$ and $E \mapsto \widetilde{E}$ are both compatible with base change of S, the first by assumption and the second by construction in the previous section, the family of morphisms

$$\check{E} = W(d)^*(\check{\mathscr{E}}) \xrightarrow{\sim} W(d)^*(\widetilde{\mathscr{E}}) = \widetilde{E}$$

is the unique family of Frobenius equivariant isomorphisms $\check{E} \to \widetilde{E}$ that is compatible with base change of S. In particular, the functor $E \mapsto \widetilde{E}$ constructed before is independent of the choice of the level N, up to unique isomorphism. □

Remark 8.0.10. As before, we can extend Proposition 8.0.9 to a base which is a p-adic sheaf S since everything is compatible by base change so if we have a family of affine schemes S_i on which p is nilpotent then we can write $\widetilde{E} = \operatorname{colim}_i \widetilde{E}_{S_i}$, and we will also get an induced Frobenius lift on the colimit.

8.0.8 j-INVARIANTS

Now that we can canonically lift families of elliptic curves, we might want to distinguish that these lifts are different from each other. One way to do this is by computing the

j-invariants. After reviewing the j-invariant in characteristic p, following [32], we will show how to do this over $Y(N)^\circ$, and then do it in generality.

Definition 8.0.11. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a field k. Then the *j-invariant* is

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

Theorem 8.0.12. *Let E and E' be elliptic curves over k. Then $E_{\overline{k}} \cong E'_{\overline{k}}$ if and only if $J(E) = j(E')$. If $j(E) = j(E')$ and $\mathrm{Char}(k) \neq 2,3$, then there is a field extension K/k of degree at most 6, 4, or 2, for $j(E) = 0, j(E) = 1728$, or $j(E) \neq 0, 1728$ such that $E_K \cong E_{K'}$.*

So the j-invariant helps us determine if curves are isomorphic. It can also tell us if an elliptic curve might have good reduction.

Proposition 8.0.13. *Let E/K be an elliptic curve. Then E has potential good reduction if and only if its j-invariant is integral.*

Proof. See [32, §7 Proposition 5.5] □

Recall that potential good reduction for an elliptic curve E/K means that there exists a finite extension K'/K such that E has good reduction over K'.

We quickly consider the case of the j-invariant of the canonical lifting of an ordinary ellitpic curve E/k over a perfect field of characteristic $p > 0$. There have been some examples computed in [33].

Example 8.0.14. Let E be an elliptic curve with j-invariant j_0. Then for the j-invariant of the canonical lift we write

$$\widetilde{j} = (j_0, j_1, j_2, \ldots) \in W(k).$$

It can be shown that

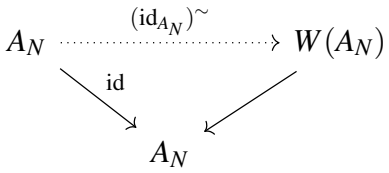
$$j_1 = \begin{cases} 3j_0^3 + j_0^4, & \text{if } p = 5 \\ 3j_0^5 + 5j_0^6, & \text{if } p = 7 \end{cases}$$

Where p refers to the characteristic of the base field. While one would hope that $j_n \in \mathbb{F}_p[j_0]$ for all n, this turns out not to be the case. For example, $j_2 \notin \mathbb{F}_7[j_0]$ for $p = 7$. However, it is in $\mathbb{F}_7(j_0)$, because it has a poll of order 7 at -1. It turns out that for $p \geq 5$, $j_n \in \mathbb{F}_p(j_0)$ for an elliptic curve E with j-invariant j_0 [33, Proposition 2.1].

With some basic properties of the j-invariant recalled, we jump into the case of j-invariants for canonical lifts. Let $Y(N)^\circ = \mathrm{Spf}(A_N)$ and $Y(N,N)^\circ = \mathrm{Spf}(A_{N,N})$, where A_N and $A_{N,N}$ are both p-adically complete and p-torsion-free rings. Forgetting the level structures, gives a pair of Frobenius equivariant maps $A_N \rightrightarrows A_{N,N}$. Let A_1 be the equalizer of these maps

$$A_1 \to A_N \rightrightarrows A_{N,N}.$$

Now, we get a map $(\mathrm{id}_{A_N})^\sim : A_N \to W(A_N)$ from the universal property of Witt vectors **??**:



The map $(\mathrm{id}_{A_N})^\sim$ is a Frobenius lift, and so it reduces to a Frobenius lift $s : A_1 \to W(A_1)$.

Now, we can write $A_1 = \mathbb{Z}_p\left[j, \frac{1}{f(j)}\right]^\wedge$, where j is an indeterminate identified with the j-function, $f(j)$ is a monic polynomial whose roots lift the supersingular j-invariants, and then we take the p-adic completion of the ring. The image of j under the map $s : A_1 \to W(A_1)$ has ghost components

$$\langle j, \psi(j), \psi^{\circ 2}(j), \ldots \rangle \in \prod_{n=1}^{\infty}$$

where ψ is the induced map from the usual Frobenius lift on $Y(N)^\circ$. Thus, if E is a family of ordinary elliptic curves over $Y(N)^\circ$, then the ghost components of $j(\widetilde{E})$ are obtained by evaluating the universal expressions $\psi^{\circ n}(j) \in \mathbb{Z}_p\left[j, \frac{1}{f(j)}\right]^\wedge$ at $j = j(E)$, the usual j-invariant.

We could also consider the usual Witt components $(j_0, j_1, \ldots)$ of $s(j)$. Then the Witt components of $j(\widetilde{E})$ are obtained by evaluating the universal expressions $j_n \in \mathbb{Z}_p\left[j, \frac{1}{f(j)}\right]^\wedge$ at $j = j(E)$.

An example of the calculations is given in [2], and a result over perfect fields of characteristic p can be found in [34].

Now that we have a special case of computing the j-invariant, we want to be able to compute the j-invariant of a family of elliptic curves over an arbitrary base. We start with the case of a p-torsion-free base. Let E be a family of curves over $\mathrm{Spf}(R)$ where R is a p-adically complete and p-torsion-free ring. Then $j(\widetilde{E})$ is an element of $W(R)$ with ghost

components

$$\langle j(E_0), j(E_1), j(E_2), \ldots \rangle = \langle j(E), \psi(j(E)), \psi^{\circ 2}(j(E)), \ldots \rangle \in \prod_{n=1}^{\infty} R.$$

where $E_0 = E$ and $E_{n+1} = E_n / E_n^{\mathrm{can}}$. And since R is p-torsion-free, the map $W(R) \to \prod_{n=1}^{\infty} R$ is injective, $j(\widetilde{E})$ is determined by the ghost coordinates.

In general, given a family of elliptic curves E, we can lift it to a family E' over a p-torsion-free extension R' of R. Then $j(\widetilde{E})$ is determined by the ghost coordinates as above, and $j(\widetilde{E})$ is the image of $j((E')^{\sim})$ under $W(R') \to W(R)$.

To end, we describe a particularly nice situation from [2] where R is a perfect $\mathbb{F}_p$-algebra and R' is $W(R)$. Then the projection

$$W(\mathrm{pr}_0(: W(W(R)) \to W(R)$$

sends a Witt vector with ghost components $\langle a_0, a_1, \ldots \rangle \in \prod_{n=1}^{\infty} W(R)$ to $\lim_{n\to\infty} F^{-n}(a_n) \in W(R)$, and so we have

$$j(\widetilde{E}) = \lim_{n\to\infty} F^{-n}(j(E'_n)) = \lim_{n\to\infty} F^{-n}(\phi^{\circ n}(j(E'))),$$

where E' is an arbitrary lift to $W(k)$ of E and $E'_{n+1} = E'_n / (E'_n)^{\mathrm{can}}$. If R is a field with p^r elements, then $F^r = \mathrm{id}_{W(R)}$, and we have

$$j(\widetilde{E}) = \lim_{n\to\infty} j(E'_{rn}).$$

References

[1] J.-P. Serre and J. Tate, "Good reduction of abelian varieties," *Annals of Mathematics*, vol. 88, no. 3, pp. 492–517, 1968. [Online]. Available: http://www.jstor.org/stable/1970722

[2] J. Borger and L. Gurney, "Canonical lifts of families of elliptic curves," *Nagoya Mathematical Journal*, vol. 233, pp. 193–213, 2019.

[3] J. Borger, "Introduction to witt vectors, delta-rings, and prisms (lecture 1)," https://www.youtube.com/watch?v=_y2Tcu-iJV4&t=237s, accessed: 2024-10-31.

[4] K. Kedlaya, "Notes on prismatic cohomology," https://kskedlaya.org/prismatic/sec_overview.html, accessed: 2025-05-18.

[5] J. Borger and L. Gurney, "Canonical lifts and δ-structures," *Selecta Mathematica*, vol. 26, no. 5, p. 67, 2020.

[6] J.-P. Serre, *Local fields*. Springer Science & Business Media, 2013, vol. 67.

[7] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*. Princeton University Press, 1985, no. 108.

[8] E. Witt, "Zyklische körper und algebren der charakteristik p vom grad p^n. struktur diskret bewerteter perfekter körper mit vollkommenem restklassenkörper der charakteristik p," *Journal für die reine und angewandte Mathematik*, vol. 176, pp. 126–140, 1937.

[9] C. Kothari, "Motivating witt vectors and delta rings," https://math.uchicago.edu/~ckothari/WittAndDelta.pdf, accessed: 2025-05-22.

[10] D. Kim, "Witt vectors," https://web.stanford.edu/~dkim04/blog/witt-vectors/, accessed: 2025-05-22.

[11] nLab authors, "adjoint functor theorem," https://ncatlab.org/nlab/show/adjoint+functor+theorem, Feb. 2025, Revision 80.

[12] E. Riehl, *Category theory in context*. Courier Dover Publications, 2017.

[13] J. Borger, "Introduction to witt vectors, delta-rings, and prisms (lecture 2)," https://www.youtube.com/watch?v=BP5I-dB9TYk, accessed: 2024-10-31.

[14] L. Illusie, "Complexe de de rham-witt et cohomologie cristalline," *Annales scientifiques de l'École Normale Supérieure. Quatrième série*, vol. 12, no. 4, pp. 501–661, 1979. [Online]. Available: https://www.numdam.org/articles/10.24033/asens.1374/

[15] U. Görtz and T. Wedhorn, "Algebraic geometry ii: cohomology of schemes," *Spring Spektrum*, 2023.

[16] A. Mathew, "The cring project," https://math.uchicago.edu/~amathew/cr.html, 2011, open-source textbook on commutative algebra.

[17] G. Tamme, *Introduction to étale cohomology*. Springer Science & Business Media, 2012.

[18] T. Stacks Project Authors, "*Stacks Project*," https://stacks.math.columbia.edu, 2018.

[19] A. Nobile *et al.*, "On formal schemes and smoothings," 2022.

[20] B. Bhatt, "Lecture notes for a class on perfectoid spaces," *Lecture notes*, vol. 14, 2017.

[21] A. Langer and T. Zink, "De rham–witt cohomology for a proper and smooth morphism," *Journal of the Institute of Mathematics of Jussieu*, vol. 3, no. 2, pp. 231–314, 2004.

[22] J. Borger, "The basic geometry of witt vectors, i: The affine case," *Algebra & Number Theory*, vol. 5, no. 2, pp. 231–285, 2011.

[23] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des topos et cohomologie etale des schémas. Tome 1: Théorie des topos'*. Springer-Verlag, 1973.

[24] P. Bruin, "Moduli of elliptic curves," in *Notes for seminar on moduli spaces and modular forms*, vol. 12, 2007.

[25] P. Deligne and M. Rapoport, "Les schémas de modules de courbes elliptiques," in *Modular Functions of One Variable II: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972*. Springer, 1973, pp. 143–316.

[26] J. Weinstein, "Aws lecture notes: Modular curves at infinite level," 2013.

[27] S. Gal, "Arithmetic hyperbolic lattices in dimension 3," PhD thesis, University of Auckland, Auckland, New Zealand, 2020, available at https://www.math.auckland.ac.nz/~sgal018/thesis.pdf.

[28] J. Lubin, "Canonical subgroups of formal groups," *Transactions of the American Mathematical Society*, vol. 251, pp. 103–127, 1979.

[29] N. M. Katz, "P-adic properties of modular schemes and modular forms," in *Modular Functions of One Variable III: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972*. Springer, 1973, pp. 69–190.

[30] K. Buzzard, "p-adic modular forms - lecture 3," https://swc-math.github.io/notes/files/01BuzzardL3.pdf, accessed: 2025-01-8.

[31] F. Calegari, "Congruences between modular forms," https://swc-math.github.io/aws/2013/2013CalegariLectureNotes.pdf, accessed: 2025-4-21.

[32] J. H. Silverman, *The arithmetic of elliptic curves*. Springer, 2009, vol. 106.

[33] L. R. Finotti, "Lifting the j-invariant: Questions of mazur and tate," *Journal of Number Theory*, vol. 130, no. 3, pp. 620–638, 2010.

[34] A. Erdoğan, "A universal formula for the j-invariant of the canonical lifting," *Journal of Number Theory*, vol. 150, pp. 26–40, 2015.

Acknowledgments

First, I would like to thank my advisor Professor Nicola Mazzzari. I am extremely grateful for all his patience during our many meetings, and for all the help he provided throughout this project. I would also like to thank Professors Cabral Balreira, Ryan Daileda, and Luke Tunstall at Trinity University for helping me reach this point, this thesis never would have happened without their endless support and encouragement.

Moreover, I am thankful to all the friends I met through the ALGANT program, Trinity, and Budapest Semesters in Math. Jay, thank you for the long conversations at Massolit and Vaslap, Emma for always being there to talk, Daksh for always answering my algebraic geometry questions, Gavi for always picking up when I was at my lowest, but especially to Eva, for all the card games, travels, and for supporting me along the way. I never would have finished this without you, je t'aime.

Finally, I would like to thank my parents, who have supported me throughout this whole process. Your support has gone a long way, and I wouldn't be here without all your help.