Lectures on Lubin-Tate spaces
Arizona Winter School
March 2019
(Incomplete draft)

M. J. Hopkins

Department of Mathematics, Harvard University, Cambridge, MA 02138

Email address: mjh@math.harvard.edu

Contents

Introduction

Lubin-Tate formal groups and their moduli play a surprising number of roles in mathematics, especially in number theory and algebraic topology. In number theory, the formal groups were originally used to construct the local class field theory isomorphism. Many years later a program emerged to use the moduli spaces to realize the local Langlands correspondence. In algebraic topology, thanks to Quillen, 1-dimensional commutative formal groups appear in the Adams-Novikov spectral sequence relating complex cobordism groups to stable homotopy groups, and through the work of Morava and many others, the Lubin-Tate groups lead to the "chromatic" picture of homotopy theory.

In both number theory and topology one is interested in the cohomology of Lubin-Tate spaces, but in number theory, one tends to be interested in something like the p-adic etale cohomology while in topology it is the coherent (stack) cohomology. Because of this the two fields have focused on a different set of fundamental questions. One goal of this lecture series is to expose aspects of Lubin-Tate spaces of interest in algebraic topology to a broader audience.

Prerequisites

I will assume the participants are familiar with the notion of a commutative formal group law and Lazard's theorems found in §1,3,5,7 of Part II of Adams [**1**] or the book of Fröhlich [**6**]. The Lubin-Tate formal groups are introduced in [**21**] and the deformation spaces in [**22**]. It will help to have read [**21**] (or Serre's article [**26**]) and to have some understanding of [**22**].

It will also help to know something about the classification of central simple division algebras over the p-adic rationals $\mathbb{Q}_p$. The notes of Serre [**25**] are very good.

Much of the material I will present is covered in the papers [**9, 10**] and [**5**]. Much of my presentation will follow [**5**].

There are many other good expositions of this material. The expository notes notes of Weinstein (`http://math.bu.edu/people/jsweinst/FRGLecture.pdf` are excellent.

Further references: [**18, 17, 19, 16, 15, 14**].

LECTURE 1

Lubin-Tate spaces

1.1. Overview

A *formal group law* (really, a commutative 1-dimensional formal group law) over a ring R is a power series

$$F(x,y) \in R[\![x,y]\!]$$

satisfying

$$\begin{aligned} F(x,y) &\equiv x+y \mod (x,y)^2 \\ F(x,0) &= F(0,x) = x \\ F(x,F(y,z)) &= F(F(x,y),z) \\ F(x,y) &= F(y,x). \end{aligned}$$

It's a lot easier to process these identities if one writes

$$x \underset{F}{+} y = F(x,y)$$

in which case they become the

$$\begin{aligned} x \underset{F}{+} y &\equiv x+y \mod (x,y)^2 \\ x \underset{F}{+} 0 &= 0 \underset{F}{+} x = x \\ (x \underset{F}{+} y) \underset{F}{+} z &= x \underset{F}{+} (y \underset{F}{+} z) \\ x \underset{F}{+} y &= y \underset{F}{+} x. \end{aligned}$$

EXAMPLE 1.1.1. The *additive formal group law* $\mathbf{G}_a$ is given by

$$\mathbf{G}_a(x,y) = x+y.$$

EXAMPLE 1.1.2. The *multiplicative formal group law* $\mathbf{G}_m$ is given by

$$\mathbf{G}_m(x,y) = x+y-xy = (1-(1-x)(1-y)).$$

A *homomorphism* $f : F \to G$ between formal group laws is a power series $f(x)$ satisfying

$$f(x \underset{F}{+} y) = f(x) \underset{G}{+} f(y).$$

There is also a notion of a (commutative 1-dimensional) *formal group* (without the word "law") which you should think of as a formal group law, without a choice of coordinate x. But that's not quite right. A formal group over R is what you get on R by (Zariski) descent datum consisting of formal groups and isomorphisms. The Zariski cotangent space to a formal group law at 0, over a ring R, is the free R-module $(x)/(x)^2$. The Zariski cotangent space at 0 to a formal group will be rank 1 projective R-module which might not be free. Mostly we will be working over local rings so you won't lose anything by thinking of a formal group as a formal group law, only without commitment to a given coordinate.

1.2. Height

Here's a question. Is there a homomorphism from $\mathbf{G}_a$ to $\mathbf{G}_m$? Are they isomorphic? Over $\mathbb{Q}$-algebras the answer is yes (the map $1-\exp(-x)$ gives an isomorphism). It doesn't look so likely in characteristic $p>0$. We will prove that there is no isomorphism. (We will do better in the next lecture).

Suppose that F and G are formal group laws over a field k of characteristic $p>0$, and $f : F \to G$ is a homomorphism.

Lemma 1.2.1. *If $f'(0)=0$ there is a unique g with $f(x)=g(x^p)$.*

Proof: The derivative of f at 0 is zero. Since f is a group homomorphism, this means that the derivative of f is zero everywhere. □

Remark 1.2.2. If you didn't like that proof, here it is in formulas. Take the identity

$$f(x \underset{F}{+} y) = f(x) \underset{G}{+} f(y)$$

and take the partial with respect to y at $y=0$. One gets

$$f'(x)\partial_2 F(x,0) = \partial_2 G(f(x),0) f'(0) = 0,$$

where ∂_2 means "partial with respect to the second variable." Now

$$\partial_2 F(x,0) = 1 + \dots$$

is a unit in $k[\![x]\!]$ so this means that $f'(x)=0$. The expression $\partial_2 F(x,0)\,dx$ is important and we will encounter it again later.

Iterating the above we get the following

Proposition 1.2.3. *If $f : F \to G$ is a non-zero homomorphism of formal group laws over a field k of characteristic $p>0$ there is a unique (g,n) with $g(x)\in k[\![x]\!]$ and $0<n<\infty$ with*

$$\begin{aligned} f(x) &= g(x^{p^n}) \\ g'(0) &\neq 0. \end{aligned}$$

Definition 1.2.4. The *height* of a non-zero homomorphism $f : F \to G$ is the integer n defined above.

One defines the height of the zero homomorphism to be ∞.

Definition 1.2.5. Let Γ be a formal group law over a field k of characteristic $p>0$. The *height* of Γ is the height of the homomorphism $p : \Gamma \to \Gamma$.

Example 1.2.6. The height of $\mathbf{G}_a$ is ∞ while the height of $\mathbf{G}_m$ is 1. It follows that $\mathbf{G}_a$ is not isomorphic to $\mathbf{G}_m$.

Exercise 1.2.1. Show that any homomorphism between $\mathbf{G}_a$ and $\mathbf{G}_m$ must have infinite height. (Hint: In the situation of Lemma 1.2.1 show that the map g must also be a homomorphism.)

1.3. Deformations of formal groups

Let Γ be a formal group over a perfect field k, and B a local ring, with nilpotent maximal ideal $\mathfrak{m}$. It will be convenient to write $r : B \to B/\mathfrak{m}$ for the quotient map.

Definition 1.3.1. A *deformation* of Γ to B is a triple (G, i, f) with G a formal group over B, $i : k \to B/\mathfrak{m}$ a ring homomorphism, and $f : r^*B \to i^*\Gamma$ an isomorphism.

The collection of deformations of Γ to B forms a groupoid $\mathbf{Deform}_\Gamma(B)$ in which an isomorphism t from (G, i, f) to (G', i', f') exists only if $i = i'$, in which case it is isomorphism $t : G \to G'$ making the diagram

$$\begin{tikzcd}
r^*G \arrow[r, "r^*"] \arrow[d, "f"'] & r^*G' \arrow[d, "f'"] \\
i^*\Gamma \arrow[r, "="'] & i^*\Gamma
\end{tikzcd}$$

commute.

While it is sensible to regard $B \mapsto \mathbf{Deform}_\Gamma(B)$ as a sheaf of groupoids (ie a stack) in the B variable, it turns out that $\mathbf{Deform}_\Gamma(B)$ is *codiscrete* in the sense that there is at most one map between any two objects. This is a consequence of the following result, whose proof is left as an exercise.

Proposition 1.3.2. *Suppose that B is a local ring with nilpotent maximal ideal $\mathfrak{m}$, and $B/\mathfrak{m}$ has characteristic $p > 0$. Write $r : B \to B/\mathfrak{m}$ for the quotient map. Suppose that G_1 and G_2 are two formal group laws over B and that r^*G_1 and r^*G_2 have finite height. Show that if $f, g : G_1 \to G_2$ are two homomorphisms having the property that $r^*f = r^*g$ then $f = g$.*

Exercise 1.3.1. Prove Proposition 1.3.2. (I'll add some guidance later.)

This means we might as well replace the groupoid $\mathbf{Deform}_\Gamma(B)$ with the equivalent groupoid $\pi_0 \mathbf{Deform}_\Gamma(B)$ consisting of the set isomorphism classes of objects of $\mathbf{Deform}_\Gamma(B)$, with no non-identity maps.

Write $\mathbb{W}$ for the ring of Witt vectors of k.

Theorem 1.3.3 (Lubin-Tate). *Suppose that Γ is a formal group of height n. The functor $\pi_0 \mathbf{Deform}_\Gamma(-)$ is* representable. *More specifically, there is a deformation $(G_{univ}, i_{univ}, f_{univ})$ over the ring $\mathbb{W}[[u_1, \dots, u_{n-1}]]$ having the property that if $(G, i, f) \in \mathbf{Deform}_\Gamma(B)$ is any deformation, there is a unique ring homomorphism $\phi : \mathbb{W}[[u_1, \dots, u_{n-1}]] \to B$ with the property that $\phi^*(G_{univ}, i_{univ}, f_{univ})$ is isomorphic to (G, i, f).*

Remark 1.3.4. Strictly speaking the local ring $\mathbb{W}[[u_1, \dots, u_{n-1}]]$ is not an allowed B since the maximal ideal $\mathfrak{m} = (p, u_1, \dots, u_{n-1})$ is not nilpotent. One can remedy this by either working with pro-nilpotent local rings, or just agreeing to extend the definition of "representable" to allow for this situation.

The ring $\mathbb{W}[[u_1, \dots, u_{n-1}]]$ is called the *Lubin-Tate* ring, and the associated formal scheme is called Lubin-Tate space. As described above, Lubin-Tate space represents the functor *isomorphisim classes of deformations of* Γ.

We now turn to the functorial dependence of $\mathbf{Deform}_\Gamma(B)$.

Proposition 1.3.5. *Two formal groups Γ and Γ' over an algebraically closed field k of characteristic $p > 0$ are isomorphic if and only if they have the same height.*

Because of this result, we might as well suppose that k is the algebraic closure of $\mathbb{F}_p$ and that we've picked just one Γ. Then the only thing left to understand is the structure of the automorphism group $\operatorname{Aut}(\Gamma)$ and its action on $\mathbb{W}[[u_1, \dots, u_{n-1}]]$. In the algebraic topology the group $\operatorname{Aut}(\Gamma)$ is written

$$\mathbf{S}_n = \operatorname{Aut}(\Gamma)$$

and called the *Morava stabilizer group*. The structure on $\operatorname{Aut}(\Gamma)$ is well understood, and will be explained in the next lecture. Let me give a presentation now, just to make things specific.

Write $\mathbb{Z}_{p^n}$ for the ring of Witt vectors of the field $\mathbb{F}_{p^n}$ with p^n elements. There is a unique ring homomorphism (Frobenius)

$$\phi : \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}$$

having the property that for all x, $\phi(x) \equiv x^p \mod p$. From time to time it will be a bit more convenient to write x^ϕ for $\phi(x)$. Let $F \in \mathrm{Gl}_n(\mathbb{Z}_{p^n})$ be the matrix

$$\Pi = \begin{pmatrix} 0 & 0 & \dots & 0 & p \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

The proof of the following result will be given in the next lecture.

Proposition 1.3.6. *The group $\mathbf{S}_n$ is isomorphic to the subgroup of $\mathrm{Gl}_n(\mathbb{Z}_{p^n})$ consisting of matrices A satisfying*

$$\Pi \cdot A = A^\phi \cdot \Pi.$$

Evidently the group $\mathbf{S}_n$ acts on the Lubin-Tate ring $E_0 = \mathbb{W}[[u_1, \dots, u_{n-1}]]$. The basic questions that will concern us in these lectures are the following.

Question 1.3.7. Can one explicitly describe the action of $\mathbf{S}_n$ on E_0?

Question 1.3.8. What are the cohomology groups $H^*(\mathbf{S}_n; E_0)$?

Question 1.3.9. What is the group of $\mathbf{S}_n$ equivariant line bundle on $\operatorname{Spf} E_0$?

The reasons these are interesting and the approaches one can make on these problems will be spelled out over the course of these lectures and in the projects. For today I want to explain the basic construction of the Lubin-Tate group, and the proof of Theorem 1.3.3.

1.4. Formal complex multiplication in local fields

Lubin and Tate wrote two papers [**21, 22**] introducing what subsequently became known as the Lubin-Tate formal group laws and Lubin-Tate space. In [**21**] they gave a construction of the maximal ramified abelian extension of a local field, providing a new construction of part of the local class field theory isomorphism. Their work generalized the theorem of Kronecker-Weber that the abelian extensions of $\mathbb{Q}$ are contained in cyclotomic fields. I'm assuming you are familiar with the Lubin-Tate paper, but as we will need some details of their construction it's worth reviewing them here.

Let's recall the setup. Suppose that K is a complete local field, with ring of integers $\mathcal{O} \subset K$. Let $\pi \in \mathcal{O}$ be a uniformizer, so that $(\pi) \subset A$ is the maximal ideal. We also assume that the residue field $k = A/(\pi)$ is finite, of order $q = p^n$ for a prime p. For the moment let

$$f(x) = x^q + \pi\, x,$$

and let $f^{(n)}(x)$ be the n-fold composition

$$f(f(\cdots(f(x)))).$$

Lubin and Tate showed that the field obtained from K by adjoining the roots of $f^n(x)$ is an abelian extension with Galois group $A/(\pi^n)^\times$.

Their idea was to show that there is a 1-parameter formal group law F over $\mathcal{O}$, with endomorphism ring A and in which $f^{(n)}$ is the power series representing "multiplication by p^n." Following Lubin and Tate, let $\mathcal{F}_\pi$ be the set of formal power series $f(x) \in \mathcal{O}[\![x]\!]$ satisfying

$$\begin{aligned} f(x) &= \pi x + O(x)^2 \\ f(x) &\equiv x^q \mod \pi. \end{aligned}$$

Given $f \in \mathcal{F}_\pi$ Lubin and Tate constructed a formal group law $F(x,y)$ with a map

$$[\,-\,] : A \to \operatorname{End}(F)$$

having the property that $[\pi](x) = f(x)$.

Lemma 1.4.1. *Suppose that $L(x_1, \dots, x_n) = a_1x_1 + \cdots + a_nx_n$ is any linear form in n-variables $x_1, \dots, x_n$. There is a unique formal power series $F(x_1, \dots, x_n)$ with*

$$F(x_1, \dots, x_n) \equiv L(x_1, \dots, x_n) \mod \deg 2 \tag{1.4.2}$$

and which commutes with f in the sense that

$$F(f(x_1), \dots, f(x_n)) = f(F(x_1, \dots, x_n)). \tag{1.4.3}$$

Proof: Suppose F is any power series satisfying (1.4.2) and satisfying (1.4.3) modulo degree $m > 1$. By assumption

$$f(F(x_1, \dots, x_n)) - F(f(x_1), \dots, f(x_n)) \equiv 0 \mod (\pi)$$

we have

$$f(F(\underline{x})) - F(f(\underline{x})) = \pi g(\underline{x}) + O(\underline{x})^{m+1}.$$

with for some homogeneous polynomial g of degree m. If $h(x_1, \dots, x_n)$ is homogeneous of degree m then

$$\begin{aligned} f(F+h) &\equiv f(F) + hf'(0) \mod \deg(m+1) \\ &\equiv f(F) + h\pi \mod \deg(m+1) \end{aligned}$$

and

$$(F+h)(f) \equiv F(f) + \pi^m h(x_1, \dots, x_n) \mod \deg(m+1). \tag{1.4.4}$$

This means that

$$(F+h)(f) - (f)(F+h) = \pi(\pi^{m-1} - 1)h - \pi g \mod \deg(m+1).$$

Since $m > 1$ there is a unique h for which

$$(F+h)(f) - (f)(F+h) \equiv 0 \mod \deg(m+1).$$

The claim follows easily from this. □

One gets a lot from this result. Taking $L(x,y) = x+y$ one constructs a unique powerseries

$$F(x,y) = x\underset{+}{y}$$

satisfying $F(f(x), f(y)) = f(F(x,y)$, or

$$f(x \underset{F}{+} y) = f(x) \underset{F}{+} f(y).$$

Again, using the lemma one finds that this defines a commutative one dimensional formal group law F. For each $a \in A$ there is a unique power series

$$[a](x) = ax + \dots$$

satisfying

$$f([a](x)) = [a](f(x)).$$

This series automatically satisfies

$$[a](x \underset{F}{+} y) = [a](x) \underset{F}{+} [a](y)$$

so that $a \mapsto [a](x)$ defines a ring homomorphism

$$A \to \operatorname{End}(F).$$

This makes F into a *formal A-module* over A in the sense of the definition below.

Definition 1.4.5. Suppose that $\phi : A \to R$ is a ring homomorphism from a not necessarily commutative ring A to a commutative ring R. A formal A-module is a formal group law F over R, equipped with a ring homomorphism

$$\begin{gathered} A \to \operatorname{End}(F) \\ a \mapsto [a](x) \end{gathered}$$

having the property that

$$[a](x) \equiv \phi(a)\, x \mod \deg 2.$$

This situation is also described by saying that F has *complex multiplication* by A.

Using an obvious generalization of Lemma 1.4.1 one can also show that the formal group laws F_{f_1} and F_{f_2} are isomorphic (by a unique isomorphism with derivative 1 at 0) for any $f_1, f_2 \in \mathcal{F}_\pi$, and furthermore that the group is independent of the choice of π. The resulting formal group is often called *the* Lubin-Tate group, however the term "Lubin-Tate" group is more commonly used to describe the induced formal group Γ over $k = A/(\pi)$.

Definition 1.4.6. The *Lubin-Tate* formal group is the formal group Γ obtained by reducing any choice of F_f modulo (π).

The formal group Γ is unique up to (non-unique) isomorphism.

1.5. Formal moduli for one-parameter formal Lie groups

In their second paper, Lubin and Tate turned to the question of describing deformations of the formal group Γ, and defined the famous Lubin-Tate spaces.

First note that the set of deformations is non-empty and in fact has a canonical element, namely the Lubin-Tate lift constructed in the previous section. To classify lifts it therefore suffices to find a means of comparing two different lifts. For this on proceeds by working modulo successive powers of $\mathfrak{m}$. Fix $k > 1$ and suppose that we have two formal group laws $F(x, y), G(x, y) \in B/\mathfrak{m}^{k+1}[\![x, y]\!]$ with

$$F(x,y) \equiv G(x,y) \mod \mathfrak{m}^k.$$

We study the difference by writing

$$G(x,y) = x \underset{F}{+} y \underset{F}{+} h(x,y)$$

for $h(x, y) \in \mathfrak{m}^k/\mathfrak{m}^{k+1}[\![x, y]\!]$. The commutativity of G gives the identity

$$h(x,y) = h(y,x).$$

Next we get an identity on h from the associativity law

$$G(x, y \underset{G}{+} z) = G(x \underset{G}{+} y, z).$$

Since

$$G(x, y \underset{G}{+} z) = x \underset{F}{+} (y \underset{G}{+} z) \underset{F}{+} h(x, y \underset{G}{+} z) = x \underset{F}{+} (y \underset{F}{+} z \underset{F}{+} h(y,z)) \underset{F}{+} h(x, y \underset{G}{+} z)$$

and

$$G(x \underset{G}{+} y, z) = (x \underset{G}{+} y) \underset{F}{+} z \underset{F}{+} h(x \underset{G}{+} y, z) = (x \underset{F}{+} y \underset{F}{+} h(x,y)) \underset{F}{+} z \underset{F}{+} h(x, y \underset{G}{+} z).$$

Using the associativity law, and formal "F" subtraction, one gets

$$h(y,z) \underset{F}{+} h(x \underset{G}{+} y, z) = h(x,y) \underset{F}{+} h(x, y \underset{G}{+} z).$$

This can be simplified a little but not a lot. Since the product of any two $h(-,-)$ terms is zero the $\underset{F}{+}$ can be replaced by $+$. Also the terms s and t in $h(s,t)$ depend only on their values modulo $\mathfrak{m}$. This means that $\underset{G}{+}$ may be replaced by $\underset{\Gamma}{+}$, So the condition in $h(x, y)$ may be written

$$h(y,z) - h(x \underset{\Gamma}{+} y, z) + h(x, y \underset{\Gamma}{+} z) - h(x,y) = 0.$$

Put differently, h is a symmetric 2-cocycle on Γ with values in $\mathfrak{m}^n$.

Suppose that F and G are isomorphic, by an isomorphism ϕ reducing to the identity modulo $\mathfrak{m}^m$. This means that $\phi(x)$ satisfies

$$\phi(x \underset{F}{+} y) = \phi(x) \underset{G}{+} \phi(y),$$

and so

$$\begin{aligned} \phi(x \underset{G}{+} y) &= \phi(x \underset{F}{+} y \underset{F}{+} h(x,y)) \\ &= \phi(x) \underset{G}{+} \phi(y) \underset{G}{+} \phi(h(x,y)). \end{aligned}$$

Since $\phi(x) \equiv x + \cdots$, using the above considerations we can rewrite this as

$$h(x,y) = \phi(x \underset{\Gamma}{+} y) - \phi(x) - \phi(y).$$

So if we declare F and G to be "isomorphic" if they are isomorphic by an isomorphism reducing to the identity modulo $\mathfrak{m}^m$ then we have found that the set of isomorphism classes of "lifts" of G from $B/\mathfrak{m}^m$to $B/\mathfrak{m}^{m+1}$ is given by

$$H^2_{\text{sym}}(\Gamma; \mathfrak{m}^m/\mathfrak{m}^{m+1}) \approx H^2(\Gamma; k)_{\text{sym}} \otimes \mathfrak{m}^m/\mathfrak{m}^{m+1}.$$

I will fill in the proof of the next result later.

Proposition 1.5.1. *If Γ has height n, the group $H^2_{sym}(\Gamma; k)$ has rank $n-1$.*

Using Proposition 1.5.1, Lubin and Tate then derive the following easy corollary.

Proposition 1.5.2. *Let G be a formal group law over $\mathbb{W}[\![u_1, \dots, u_{n-1}]\!]$ deforming Γ. The group G is a universal deformation if*

$$x \underset{G}{+} y = x + y + u_1 C_p(x,y) + \cdots + u_{n-1} C_{p^{n-1}}(x,y) + C_{p^n}(x,y) \mod \mathfrak{m}^2.$$

What remains of the proof of Theorem 1.3.3 is the construction of a formal group law G satisfying the criterion of Proposition 1.5.2. There are many approaches to this and in one way or another this construction is a key to understanding Question 1.3.7.

1.6. Deformations a la Kodaira-Spencer

Working with a formula based approach is convenient for making computations and making new progress. However it opens the door to a lot of unintended choices, and it is useful to know how things look from a completely conceptual point of view. Think of it as the analogue of writing down a model in physics. You can get a good idea what a formula has to look like by thinking about what has to happen for the physical units to work out.

There are a lot of ways of getting to the general "deformation theory" picture. Here I'll describe the one I find easiest to remember. Suppose you have a family $p : E \to B$ of something. By family I might mean a locally trivial bundle, and everything needs to be appropriately smooth. In the classic example p is a family of Riemann surfaces over B. The derivative of p is a map of tangent bundles

$$dp : TE \to TB.$$

Now pick a point $b \in B$. For each tangent vector $v \in T_bB$ the object $dp^{-1}(b, v)$ is some kind of object related to $p^{-1}(b)$. The Kodaira-Spencer map is the map

$$T_bB \to \{\text{whatever classifies } dp^{-1}(b, v)\}.$$

That was kind of vague, so let me go through a couple of examples.

Example 1.6.1. Suppose that $E \to B$ is a family of Riemann surfaces (smooth projective algebraic curves.) Then $p^{-1}(b)$ is a specific curve Σ, and $dp^{-1}(b, 0)$ is the tangent $T\Sigma$ to Σ. So what is $dp^{-1}(b, v)$? Well, if you have a linear map $W \to V$, the inverse image of v is a torsor for the inverse image of 0. So $dp^{-1}(b, v)$ is a torsor for $T\Sigma$, and is classfied by an element of $H^1(\Sigma; T\Sigma)$. This gives a map

$$T_bB \to H^1(\Sigma; T\Sigma).$$

This is the Kodaira-Spencer map, and one expects it to be an isomorphism when B is the universal family.

Example 1.6.2. How does this work out in the case of Lubin-Tate space? In this case we imagine a family of formal groups $p : E \to B$ with $p^{-1}(b) = \Gamma$. In case $v = 0$, the group $p^{-1}(b, v)$ is the tangent bundle to Γ which sits in an exact sequence

$$0 \to \operatorname{Lie}\Gamma \to E \to \Gamma \to 0.$$

This sequence splits by the choice of "0" in each tangent space. When v is not zero there is no longer a canonical choice of splitting, and you get a commutative group extension of Γ by $\operatorname{Lie}\Gamma$. Such group extensions are classified by $H^2(\Gamma; \operatorname{Lie}\Gamma)$. This gives a map

$$T_b(B) \to H^2(\Gamma; \operatorname{Lie}\Gamma)$$

which, as Lubin-Tate showed, is an isomorphism in case B is Lubin-Tate space. This is important for getting explicit formulas, as we will see later. To summarize, the Kodaira-Spencer map exhibits an isomorphism

$$(\mathfrak{m}/\mathfrak{m}^2)^* \approx H^2(\Gamma; \operatorname{Lie}\Gamma)$$

where $\mathfrak{m} \subset E_0$ is the maximal ideal, and $(\,-\,)^*$ indicates vector space dual.

LECTURE 2

Toward explicit formulas

2.1. Differentials and the log

The Lubin-Tate construction gives a terrific way of constructing formal group laws. However it isn't always the best way of getting explicit formulas. Often it is easier to work with the "logarithm" of the formal group.

EXERCISE 2.1.1. Suppose that A is a $\mathbb{Q}$-algebra and F is a formal group law over A. There is a unique power series $\log_F(x)$ with the properties

$$\begin{aligned} d\log_F(0) &= 1 \\ \log_F(x \underset{F}{+} y) &= \log_F(x) + \log_F(y). \end{aligned}$$

To do this exercise you work modulo succesive powers of x and use the symmetric 2-cocycle lemma. The function $\log_F(x)$ is the unique isomorphism of F with the additive formal group law having derivative 1 at 0.

Write $\exp_F(y)$ for the inverse function of $\log_F(x)$. Then one has

$$x \underset{F}{+} y = \exp_F(\log_F(x) + \log_F(y)). \tag{2.1.1}$$

Most of the time it is easier to work with the log of a formal group law than it is to work with the coefficients of $F(x, y)$.

The expression "log of a formal group law" is used for lots of things. If F is a formal group law over a torsion free ring A, then F has a log over $A \otimes \mathbb{Q}$

$$x + m_1 x + \cdots + m_n x^{n+1} + \cdots \in A \otimes \mathbb{Q}[\![x]\!]. \tag{2.1.2}$$

This is also called the "log" of F. Given an arbitrary power series

$$\log_F(x) \in A \otimes \mathbb{Q}[\![x]\!]$$

the formal group law defined by (2.1.1) may or may not be defined over A. There are, however, some cool conditions that guarantee that it is. I will hopefully get to some of them in a later version of this lecture. At any rate the question isn't really as hard as it looks at first blush.

For any ring A one can find a torsion free ring $\tilde{A}$ and a surjective map $\tilde{A} \to A$. By Lazard's theorem, the formal group law F over A can be lifted to a formal group law $\tilde{F}$ over $\tilde{A}$. The formal group law $\tilde{F}$ has a log over $\tilde{A} \otimes \mathbb{Q}$ which is often called the log of F (or the "log of a lift.").

Let's return to the situation of a formal group law F over a torsion free ring A, and write

$$\log_F(x) = x + m_1 x^2 + \cdots + m_n x^{n+1} + \dots.$$

Even though $\log_F(x)$ does not necessarily have coefficients in A, the form

$$d\log_F(x) = (1 + 2m_1 x + \cdots + (n+1) m_n x^n + \dots)\, dx \tag{2.1.3}$$

actually does. Why is that? If we think if $\log_F(x)$ has a map

$$F \to \mathbf{G}_a$$

(given by $y = \log_F(x)$) then the 1-form (2.1.3) is the pullback along the log of the 1-form dy. Now dy can be characterized uniquely. It is the unique translation invariant 1-form whose value at 0 is dy. This has to pull back to the unique translation invariant 1-form on F whose value at 0 is dx. Since we've described it without mentioning $A \otimes \mathbb{Q}$ it must be defined over A.

There are two good ways to get a formula for the log of F. One is to start with the equation

$$\log_F(x \underset{F}{+} y) = \log_F(x) + \log_F(y)$$

and take the partial with respect to y at $y = 0$. One gets

$$\log_F'(x)\partial_2(F(x,0)) = 1$$

or

$$d\log_F(x) = \frac{dx}{\partial_2 F(x,0)}$$

where ∂_2 means "take the derivative with respect to the second variable." This is kind of a cool formula. The expression on the right is a formula for the invariant differential on F and is meant to remind you of the formula for the invariant differential on an elliptic curve.

You can also derive the formula for the invariant differential in the usual way. Suppose it is $g(x)\,dx$. The condition that $g(x)\,dx$ be invariant is that for every constant t

$$g(t \underset{F}{+} x)d(t \underset{F}{+} x) = g(t)\,dt$$

or

$$g(t \underset{F}{+} x)F_2(t,x) = g(t).$$

Setting $t = 0$ one gets

$$g(x)F_2(0,x) = g(0) = 1.$$

One can translate the Lubin-Tate criterion of Proposition 1.5.2 into a statement about the log.

Proposition 2.1.4. *Let G be a formal group law over $\mathbb{W}[[u_1,\dots,u_{n-1}]]$ deforming Γ and write*

$$\log_G(x) = \sum b_n x^{n+1},$$

with $b_n \in \mathbb{Q} \otimes \mathbb{W}[[u_1,\dots,u_{n-1}]]$. The group G is a universal deformation if for $i < n$,

$$pb_{p^i} \equiv u_i \mod (u_1,\dots,u_{n-1})^2$$

and

$$pb_n \equiv u \mod (u_1,\dots,u_{n-1})^2 \qquad u \in E_0^\times.$$

2.2. p-typical coordinates

Let's go back to the case of a torsion free ring A and a power series

$$f(x) = \sum a_n x^n \in (A \otimes \mathbb{Q})[\![x]\!]. \tag{2.2.1}$$

It turns out that if (2.2.1) is the log of a formal group law F over a p-local ring A, then so is

$$g(y) = \sum b_n y^{p^n} \tag{2.2.2}$$

where $b_n = a_{p^n}$. This seems somewhat surprising and hard to prove if you take it on directly. The trick is to find a substitution $y = x + \cdots \in A[\![x]\!]$ and show that the log of F, expressed in the coordinate y is given by (2.2.2).

Definition 2.2.3. Suppose that F is a formal group law over a ring A. A *curve on* F is a power series $\gamma(x) \in A[\![x]\!]$, with $\gamma(0) = 0$. The set of curves on F forms a group under the operation

$$\gamma_1(x) \underset{F}{+} \gamma_2(x).$$

Remark 2.2.4. In the language of formal geometry, a curve on F is a map of formal schemes

$$\mathbb{A}^1 \to F.$$

Exercise 2.2.1. Show that if A is a p-local ring, then the group of curves on A is a $\mathbb{Z}_{(p)}$-module.

There are operations that take curves to curves. The n^{th} *Vershiebung operator* is the operator defined by

$$(V_n\gamma)(x) = \gamma(x^n)$$

and the n^{th} *Frobenius operator* is given, formally as

$$F_n(\gamma(x)) = \sum{}^{F} \gamma(\zeta^i x^{1/n})$$

in which ζ is a primitive n^{th} root of unity and i is running from 0 to $(n-1)$.

Example 2.2.5. If F is the additive group and

$$\gamma(x) = \sum a_n x^n$$

then

$$(V_\ell\gamma)(x) = \sum a_n x^{\ell n}$$
$$(F_\ell\gamma)(x) = \sum \ell a_{n\ell} x^n.$$

Note that if A is p-local, and $(\ell, p) = 1$ then one can form the operator

$$\varepsilon_\ell = 1 - \frac{1}{\ell} V_\ell F_\ell.$$

In the case of the additive group one has

$$\varepsilon_\ell\big(\sum a_n x^n\big) = \sum_{(n,\ell)=1} a_n x^n.$$

From this one can check that ε_ℓ is a projection operator. Now let π be the composition of all of the projection operators ε_ℓ for primes $\ell \neq p$. Then in the additive group

$$\pi\bigl(\sum a_n x^n\bigr) = \sum a_{p^n} x^{p^n}.$$

It follows that if we take $\gamma(x) = x$ then $y = \pi\gamma$ is the desired new coordinate.

Definition 2.2.6. A curve γ is *p-typical* if for all $(\ell, p) = 1$, $F_\ell \gamma = 0$.

Remark 2.2.7. When A is p-local a curve γ is p-typical if and only if $\epsilon_\ell \gamma = \gamma$.

Definition 2.2.8. A curve $\gamma(x)$ on F is a *coordinate* if $\gamma'(0)$ is a unit in A.

We have shown that every formal group over a p-local ring has a p-typical coordinate. Unless otherwise stated, we will restrict our attention to p-typical formal group laws.

2.3. Hazewinkel's functional equation lemma

Building on work of Honda and others, on the functional equation satisfied by the logarithm of many formal group laws, Hazewinkel abstracted a general lemma saying that a power series satisfying a suitable functional equation was the log of a formal group. The proof is one of those "Frobenius contraction" arguments.

Before turning to the general result, let me give you an example. Consider the series

$$\ell(x) = x + \frac{x^p}{p} + \cdots \frac{x^{p^n}}{p^n} + \cdots .$$

It turns out that this is the log of a formal group law defined over $\mathbb{Z}_{(p)}$. How can we tell that? One way is to try and work out the height. Suppose that the multiplication by p map is

$$[p](x) = a_1 x + a_2 x^2 + \cdots .$$

Then from the identity

$$\ell([p](x)) = p\ell(x)$$

one works out that

$$\begin{aligned} a_1 &= p \\ a_i &= 0 \qquad 1 < i < p \\ a_p &= (1 - p^{p-1}) \equiv 1 \mod p. \end{aligned}$$

So if it is the log of a formal group its reduction has height 1 and by the Lubin-Tate theorem it isomorphic to the multiplicative formal group law. So to show that it defines a formal group law over $\mathbb{Z}_{(p)}$ is equivalent to showing that

$$\exp(\ell(x))$$

has coefficients in $\mathbb{Z}_p$. Now this is a classic result. This series is called the "Artin-Hasse" exponential. To prove it has integer coefficents one can observe it is the series gotten from the standard coordinate on the multiplicative group using the projection operator of §2.2. Alternatively one can use the following cool lemma of Dwork.

Lemma 2.3.1. *A power series*

$$f(x) \in \mathbb{Q}[\![x]\!]$$

with $f(0) = 1$ *has coefficients in* $\mathbb{Z}_{(p)}[\![x]\!]$ *if and only if*

$$f(x^p)/f(x)^p$$

is in $1 + p\mathbb{Z}_{(p)}[\![x]\!]$.

Proof: The only if direction is obvious from Fermat's little theorem. The if direction is by induction on n. Write $f(x) = 1 + a_1 x + \dots$ and suppose by induction we have shown that $a_i \in \mathbb{Z}_{(p)}$ for $i < n$. Write

$$\tilde{f}(x) = \sum_{i<n} a_i x^i$$

so that $f(x) = \tilde{f}(x) + a_n x^n + \cdots$. Then

$$f(x)^p/f(x^p) = \tilde{f}(x)^p/\tilde{f}(x^p) + pa_n x^n + O[x]^{n+1}.$$

By the only if direction $\tilde{f}(x)^p/\tilde{f}(x^p)$ is in $1+p\mathbb{Z}_{(p)}[\![x]\!]$ and by assumption the entire expression is as well. This means that $pa_n \in p\mathbb{Z}_{(p)}$ and so $a_n \in \mathbb{Z}_p$. □

Using Dwork's Lemma it's easy to show that $\exp(\ell(x))$ has coefficients in $\mathbb{Z}_{(p)}$ and so $\ell(x)$ is the log of a formal group over $\mathbb{Z}_{(p)}$, and it is isomorphic to the multiplicative formal group. The key thing here was that

$$p\ell(x) - \ell(x^p) = px$$

or that $\ell(x)$ satisfied the functional equation

$$\ell(x) = x + \frac{1}{p}\ell(x^p).$$

Hazewinkel's general result implies that under suitable circumstances, a power series $f(x)$ satisfying a functional equation of the form

$$\ell(x) = g(x) + \frac{s_1}{p}\ell^{\phi}(x^p) + \frac{s_2}{p}\ell^{\phi^2}(x^{p^2}) + \cdots$$

will define a formal group law over a reasonable ring.

Here is the setup. We have a pair of rings $A \subset L$. For the moment picture that A is the ring of integers in a p-adic field L. We have an ideal $I \subset A$ which you can think of as the maximal ideal, but the only thing we really ask is that p is in I. We assume we have a "lift of (a power of) Frobenius" which will mean a choice of a fixed power q of p, and ring automorphism

$$\phi : L \to L$$

that restricts to an automorphism $\phi : A \to A$, having the property that

$$\phi(a) \equiv a^q \mod I.$$

Finally we have parameters $s_i \in L$ whose denominators are bounded in the sense that they satisfy

$$\phi^r(s_i)I \subset A$$

for all i and r. In this situation one has

Theorem 2.3.2 (Hazewinkel). *Fix a power series $g(x) \in A[\![x]\!]$ with $g'(0) \in A^\times$, and let $f(x)$ be the power series defined recursively by the functional equation*

$$f(x) = g(x) + s_1 f^\phi(x^p) + \cdots s_i f^{\phi^i}(x^{p^i}) + \cdots$$

where f^ϕ is the power series obtained by applying the map ϕ to the coefficients of f. In this situation the power series

$$f^{-1}(f(x) + f(y))$$

has coefficients in A and so $f(x)$ is the log of a formal group law over A.

There are several other aspects to the functional equation lemma which are useful. The next result asserts that the formal group you get this way depends only on the parameters s_i and not on g.

Theorem 2.3.3. *In the situation of Theorem 2.3.3, suppose f and $\tilde{f}$ are defined from the data (g, s_i) and $(\tilde{g}, s_i)$ respectively. Then the power series $f^{-1}(\tilde{f}(x))$ has coefficients in A and so gives an isomorphism of the formal group $F_{(g,s_i)}$ and $F_{(\tilde{g},s_i)}$.*

2.4. The Hazewinkel parameters

Consider the ring $A = \mathbb{Z}_p[v_1, v_2, \dots]$ with $I = (p)$ and $\phi(v_i) = v_i^p$. Then the series $f(x)$ defined by the functional equation

$$f(x) = x + \sum \frac{v_i}{p} f^{\phi^i}(x^{p^i})$$

is the log of a formal group over A. If one writes

$$f(x) = \sum m_n x^{p^n}$$

then from the functional equation one gets the recursive relation

$$m_n = \frac{v_1}{p} m_{n-1}^\phi + \cdots + \frac{v_{n-1}}{p} m_1^{\phi^{n-1}} + \frac{v_n}{p}.$$

It's not hard to expand this out and get a complete expression for m_n as a polynomial in the v_i with coefficients in $\frac{1}{p}\mathbb{Z}$. The first few terms are

$$\begin{aligned} m_1 &= \frac{v_1}{p} \\ m_2 &= \frac{v_2}{p} + \frac{v_1^{1+p}}{p^2} \\ m_3 &= \frac{v_3}{p} + \frac{v_1 v_2^p}{p^2} + \frac{v_2 v_1^{p^2}}{p^2} + \frac{v_1^{1+p+p^2}}{p^3} \\ m_n &= \sum_{i_1 + \cdots + i_k = n} \frac{v_{i_1} v_{i_2}^{p^{i_1}} \cdots v_{i_k}^{p^{i_1 + i_2 + \cdots + i_{k-1}}}}{p^k} \end{aligned}$$

The above formula formula defines parameters v_n for any formal group law. The v_n are called the *Hazewinkel* parameters (or "generators") and one has the following result

Proposition 2.4.1. *Suppose that A is a $\mathbb{Z}_{(p)}$-algebra. A p-typical series*

$$f(x) = \sum m_n x^{p^n}$$

is the log of a formal group law over A if and only if the Hazewinkel parameters v_n are in A for all n. □

This result can be derived from Lazard's theorem, and the result of §2.2.

Hazewinkel's result gives a formal group law over

$$\mathbb{Z}_{(p)}[v_1, \dots,].$$

One way of constructing the Lubin-Tate universal deformation is to change base along the map

$$\mathbb{Z}_{(p)}[v_1, \dots,] \to \mathbb{W}[\![u_1, \dots, u_{n-1}]\!]$$

defined by

$$v_i \mapsto \begin{cases} u_i & i < n \\ 1 & i = n \\ 0 & i > n. \end{cases}$$

2.5. Dieudonné modules

There is a really great way of understanding formal groups over a perfect field k. Let's start with the mechanics of the Dieudonné theory and get to the "theory" part of the theory later. A word of warning. I'm going to talk about the *covariant* Dieudonné module. There are various reasons why it isn't as good as the *contraviariant* Dieudonné theory, but it's also got some advantages. I'll try and lay out the relative merits a bit later.

Let k be a perfect field of characteristic $p > 0$ and write $\mathbf{FGL}_k$ for the category of commutative formal groups of finite dimension over k and homomorphisms. I could have said formal group *laws* over k and gotten an equivalent category. The Dieudonné theory gives an equivalence of $\mathbf{FGL}_k$ with a category easily described in the language of linear algebra.

Let $\mathbb{W}$ be the ring of Witt vectors of k,

$$\begin{aligned} \phi : \mathbb{W} &\to \mathbb{W} \\ a &\mapsto a^{\phi} \end{aligned}$$

the Frobenius automorphism. Let $\mathbf{Dieud}_k^{\text{big}}$ be the category of left $\mathbb{W}$ modules M equipped with abelian group homomorphisms

$$F, V : M \to M$$

satisfying

$$\begin{aligned} F(am) &= a^{\phi} F(m) \qquad a \in \mathbb{W} \\ V(a^{\phi} m) &= a V(m) \qquad a \in \mathbb{W} \\ FV &= VF = p. \end{aligned}$$

(and $\mathbb{W}$-linear maps compatible with F and V). Let $\mathbf{Dieud}_k \subset \mathbf{Dieud}_k^{\text{big}}$ be the full subcategory of modules M satisfying the following conditions

i) M is free of finite rank over $\mathbb{W}$

ii) The map $M \to \varprojlim M/V^j M$ is an isomorphism.

Remark 2.5.1. The assumptions imply that for each j, the map $V^j : M/VM \to V^jM/V^{j+1}M$ is an isomorphism. The map is obviously surjective. To see that it is injective, suppose that $V^j\gamma = V^{j+1}\eta$. Multiply both sides by F^j to get

$$p^j(\gamma - V\eta) = 0.$$

Since we have assumed that M is p-torsion free this means that $\gamma = V\eta$.

The Dieudonné theory provides an equivalence of categories between $\mathbf{FGL}_k$ and $\mathbf{Dieud}_k$. Let's just assume this for the moment and work out a few things. Suppose that $M \in \mathbf{Dieud}_k$ is a Dieudonné module. The properties of M imply that M/VM naturally has the structure of a k-vector space.

Definition 2.5.2. The *height* of a Dieudonné module is the rank of M over $\mathbb{W}$. The *dimension* of M is the dimension $\dim_k M/VM$.

Under the equivalece of categories, the height and dimension of a Dieudonné module correspond to the height and dimension of the corresponding formal group.

When working with the covariant Dieudonné theory, the elements of M are called *p-typical curves* or just *curves* for short. A *coordinate system* on M is an ordered set $(\gamma_1, \dots, \gamma_m) \subset M$ of curves whose image in M/VM form a k-basis. Coordinate systems on M correspond to (p-typical) coordinate systems on the corresponding formal group law. It follows that what we have been studying, (p-typical) formal group *laws* of dimension 1 over k correspond to Dieudonne modules M equipped with a choice of curve $\gamma \in M$ with the property that the image of γ in M/VM generates M/VM as a k-vector space.

Exercise 2.5.1. Show that if k is algebraically closed, two Dieudonné modules of the same height and dimension are isomorphic. If this seems hard just try it in the case of dimension 1. The case of dimension 1 gives a proof of Proposition 1.3.5.

Example 2.5.3. Let M_n be the Dieudonné module with basis $\{\gamma, V\gamma, \cdots, V^{n-1}\gamma\}$ and $F\gamma = V^{n-1}\gamma$. You can check that this defines a Dieudonné module of dimension 1 and height n. Under the equivalence of categories, this is the Dieudonné module corresponding to the formal group law Γ.

Exercise 2.5.2. Choose integers $a, b > 0$ with $(a, b) = 1$. Show that there is a free Dieudonné module $M_{a,b}$ generated by a curve γ subject to the relation $F^a\gamma = V^b\gamma$. What are the dimension and height of $M_{a,b}$?

Under the Dieudonné correspondence the Lubin-Tate formal group Γ corresonds to M_n. Using the equivalence we can easily determine the endomorphism ring of Γ, as well as the automorphism group of Γ. Let's do that.

We will suppose for convenience that k is algebraically closed. Obviously any endomorphism is determined by where the generator γ goes. So suppose

$$\gamma \mapsto a_1\gamma + \cdots + a_nV^{n-1}\gamma.$$

Using the fact that ϕ is an isomorphism (since k was assumed to be perfect) we can apply the relation $V^n = p$ to both sides and get

$$p\gamma \mapsto pa_1^{\phi^{-n}}\gamma + \cdots pa_n^{\phi^{-n}}V^{n-1}\gamma$$

from which we conclude that

$$a_i^{\phi^n} = a_i.$$

I claim that is the only condition. We're supposed to check that our map is compatible with the relation $F\gamma = V^{n-1}\gamma$, but this is now automatic:

$$\begin{aligned} F\gamma &\mapsto F(a_1\gamma + \cdots + a_n V^{n-1}\gamma) \\ &= a_1^{\phi} V^{n-1}\gamma + \cdots + a_i^{\phi} V^{i-1+(n-1)}\gamma + \cdots \\ V^{n-1}\gamma &\mapsto V^{n-1}(\sum a_i V^{i-1}\gamma) \\ &= \sum a_i^{\phi^{-(n-1)}} V^{i-1+n-1}\gamma \\ &= \sum a_i \phi V^{i-1+n-1}\gamma. \end{aligned}$$

Writing the above out in matrix form gives the computation described in Proposition 1.3.6.

Remark 2.5.4. The automorphism denoted Π in Proposition 1.3.6 is usually called F, but this get's kind of confusing because of the operator F. The operator F acts on the right of M and is ϕ-linear. The automorphism Π is W-linear and you can think of it as acting on the right. The matrix for Π looks a lot like the one for V but the operator V is ϕ^{-1} linear.

There is another useful way to describe this endomorphism ring. Let $T : M \to M$ be the map sending γ to $V\gamma$. (Usually T is called F). One can check that $\text{End}(M)$ is isomorphic to the algebra of not quite commutative power series

$$\mathbb{W}\langle T\rangle/(Ta = a^{\phi}T, T^n = p).$$

This is the maximal order in the division algebra $D = D_n$ with Hasse invariant $\frac{1}{n}$. It's a little more professional to write it as $\mathcal{O}_D$ and state Proposition 1.3.6 as an isomorphism $\mathbf{S}_n = \mathcal{O}_D^{\times}$.

It's easy to check that every non-zero endomorphism of M_n divides a power of p, so that $\mathbb{Q} \otimes \text{End}(M_n)$ is a central simple division algebra over $\mathbb{Q}_p$.

Exercise 2.5.3. Show that the Hasse invariant of this division algebra is $\frac{1}{n}$. More generally show that $\mathbb{Q} \otimes \text{End}(M_{a,b})$ is a central simple division algebra with Hasse invariant $\frac{a}{a+b}$.

2.6. Dieudonné modules and logarithms

Here's a question. How can we get our hands on the formal group law associated to a Dieudonné module M equipped with a coordinate γ? Here is how Choose a $\mathbb{W}$-linear homomorphism $T : M \to \mathbb{W}$ having the property that

$$T(\gamma) = 1.$$

Proposition 2.6.1. *The power series*

$$\ell(x) = \sum T(F^n\gamma)\frac{x^{p^n}}{p^n} \in \mathbb{W}[\![x]\!]$$

is the log of a formal group law over $\mathbb{W}$.

The formal group law associated to M is the reduction of this formal group law to $k = \mathbb{W}/p$.

We will talk about ways to prove Proposition 2.6.1. One is to try and get it from the Lubin-Tate argument and the other is to use Hazewinkel's Functional

Equation Lemma (Theorem 2.3.2). Except in special cases these methods aren't totally straightforward. We will deduce it from another result below.

2.7. Tapis de Cartier

Cartier showed [**4**] that in fact the above construction gives bijection between the set of equivalence class of lifts of Γ and a suitable set of lifts

$$\begin{tikzcd} & \mathbb{W} \arrow[d] \\ M \arrow[ur, dashed, "T"] \arrow[r] & k . \end{tikzcd}$$

in which the bottom map is the reduction M/VM followed by a choice of isomorphism of k-vector spaces $M/VM \approx k$. Let me state this more formally.

Theorem 2.7.1 (Tapis de Cartier). *Suppose that Γ is a formal group law over k of dimension 1 and height $n < \infty$ and let M be the Diedonné module of Γ. Let $\gamma \in M - VM$ be a p-typical coordinate, and write $\epsilon : M \to k$ for the unique map satisfying*

$$\begin{aligned} \epsilon(VM) &= 0 \\ \epsilon(\gamma) &= 1. \end{aligned}$$

The formula of Proposition 2.6.1 gives a bijection between the set of isomorphism classes of lifts of Γ to $\mathbb{W}$ and the set of $\mathbb{W}$-linear homomorphism

$$T : M \to \mathbb{W}$$

with $T(\gamma) = 1$.

We will give a proof of both Proposition 2.6.1 and Theorem 2.7.1 below. But let's just go along a bit and believe in the two statements. The proof will kind of pop out of that.

In principle Theorem 2.7.1 should allow us to get a good description of the Lubin-Tate ring. It tells us that the lifts to $\mathbb{W}$ correspond to suitable ring homomorphisms $\mathrm{Sym}(M) \to \mathbb{W}$, and this suggests that there is some relationship between $\mathrm{Sym}(M)$ and the Lubin-Tate ring E_0. That would be a good thing, as it's easy to understand how $\mathbf{S}_n$ acts on $\mathrm{Sym}(M)$. There are a lot of little things to straighten out, but once we get that done we will see that there is indeed such a relation, and it can be described geometrically in terms of the crystalline period mapping.

Let's try and directly make this work. We will take $M = M_n$ and give it the basis $\{\gamma, V\gamma, \dots, V^{n-1}\gamma\}$. Our map $\epsilon : M \to k$ is the one sending γ to 1 and $V^i\gamma$ to 0 for $i > 0$. Let's define variable w and ww_i on the space of lifts T by

$$\begin{aligned} w(T) &= T(\gamma) \\ w_i(T) &= T(V^i\gamma)/T(\gamma) \qquad i = 1, \dots, n-1. \end{aligned}$$

By Proposition 2.6.1 the log of the lift corresponding to T is

$$\log(x) = w\ell(x) + \frac{ww_1}{p}\ell(x^p) + \cdots + \frac{ww_{n-1}}{p}\ell(x^{p^{n-1}})$$

where

$$\ell(x) = \sum_{k \geq 0} \frac{x^{p^{nk}}}{p^k}.$$

The element w will be invertible, so changing the coordinate on the additive group we could write the log as

$$f(x) = \ell(x) + \frac{w_1}{p}\ell(x^p) + \cdots + \frac{w_{n-1}}{p}\ell(x^{p^{n-1}}). \tag{2.7.2}$$

Now this looks promising. This series certainly satisfies the criterion of Proposition 2.1.4. If it worked out to be the log of a formal group law over $\mathbb{W}[\![w_1, \dots, w_{n-1}]\!]$ we would have succeeded in writing down the universal deformation in a manner well related to the action of $\mathbf{S}_n$. Promising as it looks, it doesn't work. You can check this yourself by trying to work out the Hazewinkel parameters. You get

$$\begin{aligned} w_1 &= pm_1 = v_1 \\ w_2 &= pm_2 = v_2 + m_1 v_1^p = v_2 + \frac{v_1^{1+p}}{p}, \end{aligned}$$

and you see that v_1^{1+p} has to be divisible by p.

All is not lost though. The expression looks a lot like it would work if we could use Hazewinkel's functional equation lemma. In fact if we set $\phi(w_i) = 0$ for all i then $f(x)$ satisfies the functional equation

$$f(x) = x + \frac{w_1}{p} f^{\phi}(x^p) + \cdots + \frac{w_{n-1}}{p} f^{\phi^{p^{n-1}}}(x^{p^{n-1}}) + \frac{1}{p} f^{\phi^{p^n}}(x^{p^n}).$$

Now why aren't we allowed to do this? We have to specify and ideal $I \subset R$ containing p with the properties that

$$\phi(x) \equiv x^p \mod I$$

and among other things having the property that

$$\begin{aligned} \phi^j(w_i/p) I &\subset R \\ \phi^j(1/p) I &\subset R. \end{aligned}$$

This last condition means that I is contained in pR, so we must have $I = (p)$. So the only way this can work is if for all i, $w_i^p \in pR$. But this isn't quite enough. If $x = \phi(w_i^p)/p$ is in R then x^p must also be divisible by p. If you think this through a bit you'll come to the conclusion that this will work if the ideal $(w_1, \dots, w_{n-1})$ has divided powers. So let

$$\mathbb{W}\langle\!\langle w_1, \dots, w_{n-1} \rangle\!\rangle$$

be the "divided power completion" of the complete local ring $\mathbb{W}[\![w_1, \cdots, w_n]\!]$. Over this ring the functional equation lemma implies that (2.7.2) is the log of a formal group law. This defines a deformation of Γ to $\mathbb{W}\langle\!\langle w_1, \dots, w_{n-1} \rangle\!\rangle$. It is classified by a map

$$E_0 \to \mathbb{W}\langle\!\langle w_1, \dots, w_{n-1} \rangle\!\rangle$$

and one can easily write down the Hazewinkel parameters u_i in terms of the w_i. We will do this in detail a little later. For now let's just note that, by construction, the leading terms are

$$\begin{aligned} u_i &= w_i + \cdots \qquad 1 < i < n \\ u_n &= 1. \end{aligned}$$

This means that the group we have constructed is the universal deformation of Γ to local rings $(B, \mathfrak{m})$ equipped with a divided power structure on $\mathfrak{m}$. We also have excellent control on the action of $\mathbf{S}_n$.

Here is one immediate consequence of this. Since the ideal $(p) \subset \mathbb{W}$ has a (unique) divided power structure, the deformations of Γ to $\mathbb{W}$ are classified by (continuous) ring homomorphisms

$$\mathbb{W}\langle\!\langle w_1, \dots, w_{n-1} \rangle\!\rangle \to \mathbb{W},$$

and so have a logarithm given by (2.7.2). This proves both Proposition 2.6.1 and Theorem 2.7.1.

There's another remarkable thing that comes out of this formula. It's pretty clear that the formula of Proposition 2.6.1 is gotten by applying T to something that depends only on the Dieudonné module M. Let's try and work it out. We want to make sense of the formula

$$f(x) = \sum F^n \gamma \frac{x^{p^n}}{p^n}$$

but a small amount of typechecking shows this doesn't quite make sense. It would if we chose a basis for M and wrote F as a matrix A, and if the symbol x stood for an h-tuple

$$x = (x_1, \dots, x_h)$$

with $h = \dim_{\mathbb{W}} M$ the height of the Dieudonné module. In this case case $f(x)$ would be an h-tuple of power series in the variables x_i. One might hope that $f(x)$ is the log of a formal group law of dimension h over $\mathbb{W}$. This is indeed the case, and follows easily from the higher dimensional version of Hazewinkel's functional equation lemma. Indeed, this f satisfies the functional equation

$$f(x) = x + \frac{A}{p} f^{\phi}(x^p)$$

and works out to be

$$f(x) = x + \sum A A^{\phi} \cdots A^{\phi^n} \frac{x^{p^n}}{p^n}.$$

This construction is also called the "tapis de Cartier." Magically, it associates to a formal group law Γ of finite height h over a perfect field of characteristic p, with Dieudonné module M, an h-dimensional formal group law $\mathcal{G}$ over the ring of Witt vectors of k. The assertions of Proposition 2.6.1 and 2.7.1 imply that every lift G of Γ to $\mathbb{W}$ is a quotient of $\mathcal{G}$:

$$1 \to V \to \mathcal{G} \to G \to 1. \tag{2.7.3}$$

By construction one has $\operatorname{Lie} \mathcal{G} = M$, and the map on Lie algebras associated to (2.7.3) becomes, after choosing an isomorphism $\operatorname{Lie} G \approx \mathbb{W}$, the sequence

$$0 \to \operatorname{Lie} V \to M \xrightarrow{T} \operatorname{Lie} G \approx \mathbb{W} \to 0.$$

One can check that V is isomorphic to the additive group and so determined by its Lie algebra. The sequence (2.7.3) turns out to be the *universal extension of G by an additive group* in the sense that the map

$$\hom(V, \mathbf{G}_a) \to \operatorname{Ext}(G, \mathbf{G}_a)$$

gotten by cobase change of (2.7.3) along $V \to \mathbf{G}_a$, is an isomorphism. It is possible to construct $\mathcal{G}$ directly as the universal additive extension, and show that it is independent of the choice of lift G. This gives a definition of the Dieudonné module as the "Lie algebra of the universal additive extension of a lift." At least this would be a definition if one make it a functor of Γ alone. This can be done. See [**23**]. Getting this straight was one of the motivations for the introduction of the crystalline topos. We will return to this a bit later.

2.8. Cleaning things up

Before turning to a more invariant version of the theory we clean a few things up. If M is a Diedonné module of a formal group Γ then M/VM is naturally isomorphic to the Lie algebra $\operatorname{Lie}\Gamma$. The choice of curve $\gamma \in M$ is used only through the isomorphism $M/VM \approx k$ or in other words only through the induced isomorphism $\operatorname{Lie}\Gamma \approx k$. The lift G_T associate to $T : M \to W$ comes equipped with an isomorphism $\operatorname{Lie} G_T \approx \mathbb{W}$. This makes it clear that we are really working with formal groups G which are *rigidified* in the sense that they come equipped with a basis $\operatorname{Lie} G$ of the Lie algebra. Let's step back a bit and systematically incorporate this choice.

Suppose that G is a 1-dimensional formal group law over a ring R. The Lie algebra $\operatorname{Lie} G$ is then a locally free R-module of rank 1, with dual the cotangent space $\omega = \omega_G$ to G at the identity section. Geometrically, $\operatorname{Lie} G$ is a line bundle over $\operatorname{Spec} R$ (or $\operatorname{Spf} R$). For a map $R \to S$, an isomorphism

$$S \underset{R}{\otimes} \operatorname{Lie} G$$

corresponds to a lift

$$\begin{tikzcd}
 & P \arrow[d] \\
\operatorname{Spec} S \arrow[r] \arrow[ur, dashed] & \operatorname{Spec} R
\end{tikzcd}$$

to the principal Gl_1-bundle underlying $\operatorname{Lie} G$. This means we should probably be working over P to begin with. Now the ring of functions on P is graded by the eigenspaces of the Gl_1-action. So given Γ over k we should work with the graded ring k_* whose homogeneous components correspond to sections of $\operatorname{Lie}\Gamma^{\otimes j}$ or $\omega_\Gamma^{\otimes j}$. The convention in the algebraic topology literature is to make the ring k_* be *evenly graded* with

$$k_{2n} \approx H^0(\operatorname{Spec} k; \omega_\Gamma^n).$$

An isomorphism $k \to \operatorname{Lie}\Gamma$ corresponds to an invertible element $u \in k_{-2}$, and once one is chosen one gets an isomorphism

$$k_* \approx k[u, u^{-1}] \qquad |u| = -2.$$

To connect the Dieudonné theory to deformations, we should also work on the principal $\operatorname{Lie} G$-bundle of a deformation G. This motivates looking at the graded ring E_* associated to the ring of formal functions on the universal deformation of Γ. Again, following the conventions in topology the homogeneous component E_{2n} is the space of sections of $\omega_{G_{\text{univ}}}$. A choice of isomorphism $u : E_0 \approx \operatorname{Lie} G_{\text{univ}}$ specifies an element $u \in E_{-2}$ and enables us to write

$$E_* \approx \mathbb{W}[\![u_1, \dots, u_{n-1}]\!][u, u^{-1}].$$

But it's important to remember that the parameters u_i and u are not canonically chosen. In fact a *good* choice would be one in which one could understand the action of $\operatorname{Aut}\Gamma$.

OK. How does the Tapis de Cartier match the Dieudonné theory with this graded ring? Let

$$\mathcal{G}_{\text{univ}} \to G_{\text{univ}}$$

be the universal additive extension of G_{univ} by an additive group. There is then a map

$$\operatorname{Lie}\mathcal{G}_{\text{univ}} \to \operatorname{Lie}G_{\text{univ}}.$$

If we imagine that the Dieudonné module M is somehow related to $\operatorname{Lie}\mathcal{G}_{\text{univ}}$ then we would have a map, or relationship between M and the module of sections of $\operatorname{Lie}G_{\text{univ}}$. In terms of our graded ring, this sets up the expectation that there is a map, or at least a relationship between M and E_{-2}. This will be the subject of the next two lectures.

Exercise 2.8.1. Can you work out how this squares with the Kodaira-Spencer picture of deformations from §1.6?

LECTURE 3

Crystals

3.1. A further formula

In the last section we introduced deformation parameters w and w_i which can be used to study deformations of formal group to local rings whose maximal ideal has a divided power structure. There are also Hazewinkel's deformation parameters u and u_i. Can we get a formula relating these?

With Hazewinkel's parameters, the log of the universal deformation satisfies the functional equation

$$f(x) = x + \frac{u_1}{p} f^{\phi}(x^p) + \cdots + \frac{u_{n-1}}{p} f^{\phi^{n-1}}(x^{p^{n-1}}) + \frac{1}{p} f^{\phi^n}(x^{p^n}).$$

Writing

$$f(x) = \sum m_n x^{p^n}$$

these expand into the recursive formuals

$$\begin{aligned} m_i &= 0 \qquad i < 0 \\ m_0 &= 1 \\ pm_\ell &= u_1 m_{\ell-1}^{\phi} + \cdots + u_{n-1} m_{\ell-(n-1)}^{\phi^{n-1}} + u_{n-\ell}. \end{aligned}$$

These are easily solved and one can write down a closed (albeit a bit complicated) formual for m_ℓ. Here is what you get if $n = 2$.

$$\begin{aligned}
m_0 &= 1 \\
m_1 &= \frac{u_1}{p} \\
m_2 &= \frac{1}{p} + \frac{u_1^{p+1}}{p^2} \\
m_3 &= \frac{u_1}{p^2} + \frac{u_1^{p^2}}{p^2} + \frac{u_1^{p^2+p+1}}{p^3} \\
m_4 &= \frac{1}{p^2} + \frac{u_1^{p+1}}{p^3} + \frac{u_1^{p^3+1}}{p^3} + \frac{u_1^{p^3+p^2}}{p^3} + \frac{u_1^{p^3+p^2+p+1}}{p^4} \\
m_5 &= \frac{u_1}{p^3} + \frac{u_1^{p^4}}{p^3} + \frac{u_1^{p^2}}{p^3} + \frac{u_1^{p^2+p+1}}{p^4} + \frac{u_1^{p^4+p+1}}{p^4} + \frac{u_1^{p^4+p^3+1}}{p^4} + \frac{u_1^{p^4+p^3+p^2}}{p^4} + \frac{u_1^{p^4+p^3+p^2+p+1}}{p^5} \\
m_6 &= \frac{1}{p^3} + \frac{u_1^{p+1}}{p^4} + \frac{u_1^{p^5+1}}{p^4} + \frac{u_1^{p^5+p^4}}{p^4} + \frac{u_1^{p^5+p^4+p+1}}{p^5} + \frac{u_1^{p^5+p^2+p+1}}{p^5} + \frac{u_1^{p^3+1}}{p^4} + \frac{u_1^{p^5+p^4+p^3+1}}{p^5} \\
&\quad + \frac{u_1^{p^5+p^2}}{p^4} + \frac{u_1^{p^3+p^2+p+1}}{p^5} + \frac{u_1^{p^3+p^2}}{p^4} + \frac{u_1^{p^5+p^4+p^3+p^2}}{p^5} + \frac{u_1^{p^5+p^4+p^3+p^2+p+1}}{p^6}
\end{aligned}$$

There is a visible pattern here. The terms $p^n m_{2n}$ seem to be converging on something, as do the terms $p^n m_{2n-1}$.

Now the log $g(x)$ for the w_i deformation is given by

$$g(x) = x + \frac{w_1}{p}\ell(x^p) + \cdots + \frac{w_{n-1}}{p}\ell(x^{p^{n-1}}) + \frac{1}{p}\ell(x^{p^n}). \tag{3.1.1}$$

Writing

$$g(x) = \sum \eta_k x^{p^k}$$

one sees that

$$\eta_\ell = \frac{w_r}{p^t}$$

in which we have written

$$\begin{aligned} \ell &= tn - r \qquad 0 \le r < n \\ w_n &= 1. \end{aligned}$$

It might be easier to process this when $n = 2$:

$$g(x) = x + \frac{w_1}{p}x^p + \frac{1}{p}x^{p^2} + \frac{w_1}{p^2}x^{p^3} + \frac{1}{p^2}x^{p^4} + \cdots$$

so

$$\begin{aligned} \eta_{2m} &= \frac{1}{p^m} \\ \eta_{2m-1} &= \frac{w_1}{p^m}. \end{aligned}$$

This suggests the formula

$$ww_r = \lim_{t\to\infty} p^n m_{tn-r} \qquad (w_0 = 1)$$

This is in fact correct and is proved in [**5**, Theorem 4.4] from this point of view. There is a nice way of writing this formula. Let's do this when $n = 2$. The recursion formula (3.1.1) defining m_n is

$$\begin{aligned} m_{-1} &= 0 \\ m_0 &= 1 \\ m_n &= \frac{u_1}{p}m_{n-1}^{\phi} + \frac{1}{p}m_{n-1}^{\phi^2} \end{aligned}$$

can be written as the matrix equation

$$\begin{bmatrix} m_n & \frac{1}{p}m_{n-1}^{\phi} \\ m_{n-1} & \frac{1}{p}m_{n-2}^{\phi} \end{bmatrix} = \begin{bmatrix} m_{n-1} & \frac{1}{p}m_{n-2}^{\phi} \\ m_{n-2} & \frac{1}{p}m_{n-3}^{\phi} \end{bmatrix}^{\phi} \begin{pmatrix} \frac{u_1}{p} & \frac{1}{p} \\ 1 & 0 \end{pmatrix}$$

from which one gets the formula

$$\begin{bmatrix} p^n m_{2n} \\ p^n m_{2n-1} \end{bmatrix} = p^n \begin{pmatrix} \frac{u_1^{p^{2n-1}}}{p} & \frac{1}{p} \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} \frac{u_1}{p} & \frac{1}{p} \\ 1 & 0 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Writing

$$A = \begin{pmatrix} \frac{u_1}{p} & \frac{1}{p} \\ 1 & 0 \end{pmatrix} \qquad A(0) = \begin{pmatrix} 0 & \frac{1}{p} \\ 1 & 0 \end{pmatrix},$$

one can also write the term on the right as

$$A^{\phi^{2n-1}} \cdots A \cdot A(0)^{-2n}$$

and one gets the formula

$$\begin{pmatrix} w & (ww_1)^{\phi} \\ ww_1 & w^{\phi} \end{pmatrix} = \lim_{m\to\infty} A^{\phi^m} A^{\phi^{m-1}} \cdots A \cdot A(0)^{-(m+1)}.$$

This expression turns out to have a nice geometric interpretation.

In the height n case one writes

$$\begin{aligned} w &= \varinjlim p^k m_{nk} = 1 + \cdots \\ ww_i &= \varinjlim p^{k+1} m_{nk+i} = u_i + \cdots . \end{aligned}$$

Let ϕ be the ring homomorphism with $\phi(u_i) = u_i^p$. Then Hazewinkel's recursion relation

$$m_\ell = \frac{u_1}{p} m_{\ell-1}^{\phi} + \cdots + \frac{u_{n-1}}{p} m_{\ell-(n-1)}^{\phi^{n-1}} + \frac{1}{p} m_{\ell-n}^{\phi^n}$$

becomes

$$\begin{aligned} ww_1 &= u_1 w^{\phi} + u_2 (ww_{n-1})^{\phi^2} + \cdots + u_{n-1}(ww_2)^{\phi^{n-1}} + (ww_1)^{\phi^n} \\ ww_2 &= \frac{1}{p} u_1 (ww_1)^{\phi} + u_2 w^{\phi^2} + \cdots + u_{n-1}(ww_3)^{\phi^{n-1}} + (ww_2)^{\phi^n} \\ &\vdots \\ ww_{n-1} &= \frac{1}{p} u_1 (ww_{n-2})^{\phi} + \cdots + \frac{1}{p} u_{n-1}(ww_1)^{\phi^{n-1}} + w^{\phi^{n-1}} + (ww_{n-1})^{\phi^n} \\ w &= \frac{u_1}{p}(ww_1)^{\phi} + \cdots + \frac{u_{n-1}}{p}(ww_{n-1})^{\phi^{n-1}} + w^{\phi^n} \end{aligned} \tag{3.1.2}$$

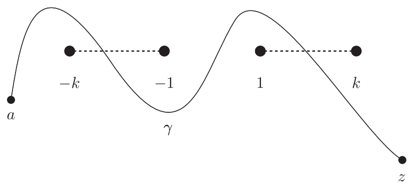
We will express this as a matrix equation in §3.4.

3.2. Periods

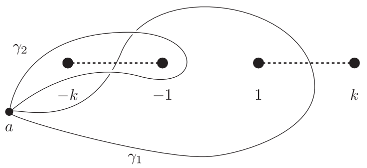
The classical story of Abelian integrals and their periods arises when one considers the complex analytic function

$$\int_a^z \frac{dx}{\sqrt{(x^2-1)(x^2-k^2)}}. \tag{3.2.1}$$

In order to even talk about the integral one needs to choose branch cuts between the branch points so one can be careful about which branch of the square root one is using. The branch points are at $x = \pm 1$ and $x = \pm k$. In the picture below I've chosen some branch cuts, and drawn a typical curve



Now the value of the integral is almost independent of the choice of curve. The only ambiguity comes from adding the values of the integrals around γ_1 and γ_2 below



Let's write

$$\eta_1 = \oint_{\gamma_1} \frac{dx}{\sqrt{(x^2-1)(x^2-k^2)}}$$
$$\eta_2 = \oint_{\gamma_2} \frac{dx}{\sqrt{(x^2-1)(x^2-k^2)}}.$$

It turns out that η_1 and η_2 are linearly independent over $\mathbb{R}$ and generate a lattice $\Lambda = \Lambda_k \subset \mathbb{C}$. The function (3.2.1) thus determines two pieces of data: the lattice $\Lambda_k \subset \mathbb{C}$ and what turns out to be an analytic isomorphism

$$X \to \mathbb{C}/\Lambda$$

from (the desingularizatin of) the plane curve X defined by the equation

$$y^2 = (x^2-1)(x^2-k^2) \tag{3.2.2}$$

to a complex torus.

The generalization of this to higher genus curves is as follow. For a smooth compact analytic curve X of genus g on finds a basis

$$\{\omega_1, \dots, \omega_g\}$$

for the space of holomorphic differentials and a basis

$$\gamma_1, \dots, \gamma_{2g} \subset H_1(X;\mathbb{Z})$$

for the first homology group with integer coefficients. The vectors

$$\int_{\gamma_i} \omega_j \in \mathbb{C}^g$$

generate a lattice $\Lambda \subset \mathbb{C}^g$ and the set of integrals

$$\int_a^z \omega_j \qquad j = 1, \cdots, g$$

an embedding $X \to \mathbb{C}^g/\Lambda$. This is the *Abel-Jacobi map*, the complex torus $\mathbb{C}^g/\Lambda$ is the *Jacobian variety* of X, and the integrals used to define it are called *Abelian integrals*. Suitably formulated the association $X \mapsto \Lambda$ gives an emedding of the moduli space of curves into and appropriate moduli space of lattices. This is the famous *Torelli Theorem*. The *Shottky problem* is the problem of characterizing the image.

The remarkable thing about this is that much of the story can be made to work for formal groups! We have to set things up a bit differently to make it work. Once we do, the display of identities at the end of §3.1 will have an interpretation in terms of periods.

The key is to look at the Hodge sequence

$$0 \to H^0(X;\Omega^1) \to H^1_{\mathrm{DR}}(X;\mathbb{C}) \to H^1(X;\Omega^0) \to 0.$$

The vector space $H^0(X/;\Omega^1)$ is the space of holomorphic differentials, while, by de Rham's Theorem (and the universal coefficient theorem) the de Rham cohomology group in the middle is isomorphic to

$$\hom(H_1(X/\mathbb{Z}),\mathbb{C}).$$

The left map is the map sending a differential ω to the complex "period"

$$\gamma \mapsto \int_\gamma \omega.$$

With point of view the Jacobian variety is

$$H^0(\Omega^1 X)^*/H_1(X;\mathbb{Z}).$$

At this point this just looks like a structureless embedding of a complex vector space of dimension g into on of dimension $2g$. But the two groups have very different characters. To see this look at the integral (3.2.1), and think k as a parameter specifying the "modulus" of the curve X. The form $\omega = \frac{dx}{\sqrt{(x^2-1)(x^2-k^2)}}$ varies with k, however the integer cohomology (and hence the de Rham cohomology) depends only on the topological space underlying X and not on its complex structure. So it is, in some sense, rigid.

Now it's kind of surprising but one can account for the rigidity of de Rham cohomology in purely "algebraic" terms. Let's go back to our motivating example of the curve defined by (3.2.2), but now think of k as a parameter. To emphasize that I'll write X_k for the specific curve. Then what we really have is a map

$$p : X \to K$$

where X is the totality of all the curves X_k and K is the parameter space of values of k (in our example $K = \mathbb{C} \setminus \{\pm 1\}$). The fiber of p over a point $k \in K$ is our curve X_k. Now X is something 2-dimensional and so it's de Rham complex in degree 1 will have things that look like

$$f(x,y,k)\,dx + g(x,y,k)\,dy + h(x,y,k)\,dk,$$

and from (3.2.2) one has

$$2y\,dy = 2x\big((x^2-k^2)+(x^2-1)\big)\,dx - 2k\,dk.$$

When we think about the de Rham cohomology of an *individual* X_k we are ignoring the terms $h(x,y,k)\,dk$. More specifically, we are modding them out. This situation was analyzed in a beautiful paper of Katz and Oda [**13**]. Here is how it goes.

Let's write $\Omega^* X$ for the de Rham complex of X and $\Omega^*(K)$ for the de Rham complex of K. Then the pullback of forms gives a map of differential graded algebras

$$\Omega^*(K) \to \Omega^*(X).$$

Let

$$I = \bigoplus_{n\ge 1} \Omega^n K \subset \Omega^*(K)$$

be the (differential graded) ideal of forms of positive degree. Then we have

$$\Omega^*(K)/I = \Omega^0(K)$$

in which the latter is regarded as a differential graded algebra with $d = 0$ and concentrated entirely in degree 0. The relative de Rham complex $\Omega^*(X/K)$is the (derived) quotient

$$\Omega^*(X/K) = \Omega^*(X)/I = \Omega^*(X) \underset{\Omega^*(K)}{\otimes} \Omega^0 K.$$

It is the cohomology of $\Omega^*(X/K)$ that is the aggregate of the individual de Rham cohomology groups of the X_k.

Now this setup is part of a spectral sequence. It is the Leray spectral sequence of the map p for de Rham cohomology, and you can think of it as constructed by filtering $\Omega^* K$ by powers of the ideal I. The E_1-term of the spectral sequence is

$$H^s_{\mathrm{DR}}((X/K)) \otimes \Omega^t(K)$$

and the above term contributes to $H^{s+t}_{\mathrm{DR}}(X)$. The first differential is rather interesting. It gives a map

$$H^s_{\mathrm{DR}}(X/K) \to H^s_{\mathrm{DR}}(X/K) \otimes \Omega^1(K).$$

This piece of structure is a connection on $H^*_{\mathrm{DR}}(X/K)$, and the fact that $d^2 = 0$ shows that the connection is flat. This is the *Gauss-Manin* connection and was analyzed in this form by Katz and Oda.

REMARK 3.2.3. In fact Katz goes further ([**12**, p. 186]) and analyzes the next differential, showing that it is given by “cup product with the Kodaira-Spencer class.” This is the piece of structure mentioned in§1.6. Let’s at least check that everything lives in the right place. First of all where do the differentials go? Like the Serre spectral sequence for a fibration, the differential d_r goes from sub quotient of $H^s_{\mathrm{DR}}(X/K) \otimes \Omega^t(K)$ to a sub quotient of $H^{s-r+1}_{\mathrm{DR}}(X/K) \otimes \Omega^{t+r}(K)$, so d_2 maps a subgroup of $H^s_{\mathrm{DR}}(X/K) \otimes \Omega^t(K)$ to a quotient of $H^{s-1}_{\mathrm{DR}}(X) \otimes \Omega^{t+2}(K)$. As described in §1.6, the Kodaira-Spencer map is a map from $T_k K$ to $H^1(X_k; TX_k)$. Put differently it is an element of

$$\Omega^1(K; H^1(X/K; TX/K)). \tag{3.2.4}$$

Now an element of $H^s_{\mathrm{DR}}(K; H^t_{\mathrm{DR}}(X/K))$ is represented by a element of

$$\Omega^s(K) \otimes \Omega^t(X/K).$$

Multiplying these by (3.2.4) and contracting the tangent vectors against the forms give an element of $\Omega^{s+1}(K) \otimes \Omega^{t-1}(X/K)$ which is what we wanted.

3.3. Crystals

3.3.1. Formal Lie Varieties. The takeaway from the previous section is that we probably ought to be looking at de Rham cohomology. We now turn to doing so. Much of this section follows the presentation of Katz [**11**].

3.3.1.1. *De Rham cohomology.* Let S be a ring. Following Katz [**11**] we define the category $\mathbf{FormalLie}_S$ of *pointed formal Lie varieties over* S to be the category with objects $\{\mathbb{A}^n = \mathbb{A}^n_S \mid n = 0, 1, \dots\}$ in which a map $\mathbb{A}^n_S \to \mathbb{A}^1_S$ is a formal power series

$$f(x_1, \dots, x_n) \in S[\![x_1, \dots, x_n]\!]$$

satisfying $f(0, \dots, 0) = 0$. The maps x_i have the property that

$$\mathbb{A}^n_S \xrightarrow{(x_1,\dots,x_n)} \left(\mathbb{A}^1_S\right)^n$$

is an isomorphism, and the composition of maps is given by composition of power series. Thus a map of formal Lie varieties $\mathbb{A}^n_S \to \mathbb{A}^m_S$ is a column vector

$$\big[f_1, \dots, f_m\big]^T$$

of functions $f_i(x_1, \dots, x_n)$.

The category of formal Lie varieties over S is functorial in S. Given a map $S \to T$ there is a functor from $\textbf{FormalLie}_S \to \textbf{FormalLie}_T$. To ease the burden on the typist I will often write $\mathbb{A}^n$ instead of $\mathbb{A}^n_S$ when the ground ring S is understood.

Remark 3.3.1. In this language a formal group law of dimension n is a group structure on $\mathbb{A}^n$.

Remark 3.3.2. The category $\textbf{FormalLie}_S$ is the opposite of the category with objects the augmented formal power series rings

$$\epsilon : S[\![x_1, \dots, x_n]\!] \to S$$
$$\epsilon(x_i) = 0$$

and ring homomorphisms of augmented rings.

3.3.1.2. *Differential forms and the De Rham complex.* Just as in differential topology one can talk about k-forms on $\mathbb{A}^n_S$. The space $\Omega^k(\mathbb{A}_S/S)$ of (relative) of k-forms on $\mathbb{A}^n_S$ is a free module over the ring of formal functions on $\mathbb{A}^n_S$ with basis the set of

$$dx_I = dx_{i_1} \wedge \cdots \wedge dx_{i_k}$$

in which $I = (i_1 < \cdots < i_k)$ is running through the k-element subsets of $\{1, \dots, n\}$. The usual formulas for exterior differentiation make sense and one can construct the de Rham complex

$$\Omega^*(\mathbb{A}^n_S/S) = \Omega^0(\mathbb{A}^n_S/S) \xrightarrow{d} \Omega^1(\mathbb{A}^n_S/S) \to \cdots \xrightarrow{d} \Omega^n(\mathbb{A}^n_S/S).$$

The i^{th} cohomology of the de Rham complex will be denoted $H^i_{\text{DR}}(\mathbb{A}^n_S/S)$.

Exercise 3.3.1. Show that $H^0_{\text{DR}}(\mathbb{A}^1_S/S) = S$. Show that if S is the ring $\mathbb{Z}_p$ of p-adic numbers, then

$$H^1_{\text{DR}}(\mathbb{A}^1_S/S) = \prod_{(n,p)=1} \prod_{k \geq 1} \mathbb{Z}/p^k \tag{3.3.3}$$

in which the factor $\mathbb{Z}/p^k$ with index n is the form

$$d\big(x^{np^k}/p^k\big) = x^{np^k-1}\, dx.$$

When S is a $\mathbb{Q}$-algebra the proof of the usual Poincaré Lemma applies and one has

Proposition 3.3.4. *When S is a $\mathbb{Q}$-algebra then for all $i > 0$,*

$$H^i_{DR}(\mathbb{A}^n_S/S) = 0.$$

3.3.1.3. *Functorial properties of De Rham cohomology.* The de Rham cohomology has surprising functorial properties.

Definition 3.3.5. Suppose that S is a torsion free ring, which we will regard as a subring of $S \otimes \mathbb{Q}$. A *divided power ideal* is ideal $I \subset S$ with the property that if $x \in I$ then for all n, the element $x^n/n!$ is in I.

Example 3.3.6. The ideal (p) in $\mathbb{Z}_p$ has divided powers.

Remark 3.3.7. When $I \subset S$ is an ideal which is not torsion free (over $\mathbb{Z}$), one has to talk about a *divided power structure* on I. This means a sequence of functions $\gamma^n : I \to I$, often just written as $x \mapsto x^{(n)}$ satisfying the formal algebraic properties of $x^n/n!$. The advantage of sticking with the torsion free case is that the existence of divided powers is a condition and not data.

Exercise 3.3.2. Suppose that S is a torsion free ring and $I \subset S$ is an ideal with divided powers. Show that if $f, g : \mathbb{A}^n_S \to \mathbb{A}^m_S$ are two maps satisfying $f \equiv g \mod I$ then for all $i \geq 0$

$$f^* = g^* : H^i_{\mathrm{DR}}(\mathbb{A}^m_S) \to H^i_{\mathrm{DR}}(\mathbb{A}^m_S).$$

Here $f$and g are column vectors of formal power series over S in n variables and $f \equiv g \mod I$ means that all of the the coefficients of these power series are the same modulo I.

3.3.1.4. *De Rham cohomology with coefficients.* The results of the previous section apply to what one might think of as de Rham cohomology with coefficients. We're not going to use them in that form, but it's a convenient way to introduce modules with connection, which will play an important role.

Let's suppose that V is a formal Lie variety of dimension n over S. In our main example, V will not be a formal group, but will be Lubin-Tate space itself. Suppose we have a vector bundle M over V of rank k. Since the ring

$$\mathbf{FormalLie}_S(V, \mathbb{A}^1) = S[\![x_1, \dots, x_n]\!]$$

of functions on V is a local ring the $\mathbf{FormalLie}_S(V, \mathbb{A}^1)$-module of sections of M is free of rank k. We want to add structure to M that allows us to form the de Rham complex

$$\Omega^0(V) \otimes M \xrightarrow{d} \Omega^1(V) \otimes M \xrightarrow{d} \cdots \xrightarrow{d} \Omega^n(V) \otimes M \tag{3.3.8}$$

and be able to talk about $H^*_{\mathrm{DR}}(V; M)$. The first thing we need is a map

$$M \xrightarrow{d} \Omega^1(V) \otimes M$$

which, written terms of a section m of M is

$$m \mapsto \sum D_i(m)\, dx_i.$$

The operator D_i has the property that

$$D_i(fm) = \frac{\partial f}{\partial x_i} + f D_i(m) \qquad f : V \to \mathbb{A}^1.$$

The operators D_i endow M with a *connection*, and you can think of $D_i(m)$ as $\partial(m)/\partial x_i$.

What corresponds to the condition that $d^2 = 0$? In terms of the operators D_i, the 2-form $d^2 m$ is given by

$$\sum_{i,j} D_i D_j(m)\, dx_i\, dx_j = \sum_{i<j} (D_i D_j(m) - D_j D_i(m))\, dx_i\, dx_j.$$

The condition that $d^2 = 0$ is thus equivalent to the condition that the operators D_i and D_j commute. A connection with these properties is called *integrable.* A section m of M is called *horizontal* if $D_i m = 0$ for all i and so $H^0_{\mathrm{DR}}(M)$ is the space of *horizontal sections* of M. The results of 3.3.1.3 apply to the cohomology groups

$$H^*_{\mathrm{DR}}(V; M)$$

of a formal Lie variety with coefficients in a vector bundle with an integrable connections.

Suppose that (M, D^M_i) and (N, D^N_i) are modules equipped with with integrable connections. A module map $T : M \to N$ is *horizontal* if it is compatible with the connection:

$$T^*(D^M_i(m)) = D^N_i(T(m)).$$

A horizontal map gives a map of de Rham cohomology with coefficients

$$H^*_{\mathrm{DR}}(V; M) \to H^*_{\mathrm{DR}}(V; N).$$

3.3.1.5. *De Rham cohmology of groups.* Let G be a formal group law of dimension n over S, thought of as a group structure on $\mathbb{A}^n_S$. Now here's an annoying thing about the notation. In the usual theory of groups, when a group is a set endowed with a composition law, a group is denoted G, the underlying set is also denoted G, and no special notation is used for the composition law. I'd like to follow this notation when we are working with formal groups. Thus a formal group G of dimension n will consist of a formal Lie variety (which abstractly isomorphic to $\mathbb{A}^n$) equipped with a group structure. I'd like to use the symbol G for this variety and just write the composition law as a map

$$\mu : G \times G \to G$$

and try not to mention μ all that much. A coordinate system on G is a choice of isomorphism $G \to \mathbb{A}^n$ and in terms of the coordinate system the map μ is given by an n-tuple of power series in variables $\underline{x} = (x_1, \dots, x_n)$ and $\underline{y} = (y_1, \dots, y_n)$. The symbol G is also used to denote this power series:

$$G(\underline{x}, \underline{y}) = \begin{bmatrix} G_1(\underline{x}, \underline{y}) \\ \vdots \\ G_n(\underline{x}, \underline{y}) \end{bmatrix}.$$

Hopefully overloading the symbol G like this won't cause confusion.

Let's go back to the situation in which S is a torsion free ring and G is a formal group over S. In that case the composition law gives the de Rham cohomology of G an additional piece of structure, namely a map

$$\mu^* : H^i_{\mathrm{DR}}(G) \to H^i_{\mathrm{DR}}(G \times G).$$

Definition 3.3.9. An element $\omega \in H^i_{\mathrm{DR}}(G)$ is *primitive* if

$$\mu^*(\omega) = \mathrm{pr}_1^* \omega + \mathrm{pr}_2^* \omega.$$

The group of primitive elements of $H^i_{\mathrm{DR}}(G)$ will be denoted $\mathbf{D}^i(G)$.

Let's do a few examples to get the swing of this. We will focus on $\mathbf{D}^1(G)$. We will also restrict our attention to the case in which S is $\mathbb{Z}$-torsion free and so may be regarded as a subring of $S \otimes \mathbb{Q}$. In that case, since every closed one form $\omega \in \Omega^1(G_S)$ is exact over $S \otimes \mathbb{Q}$, we may identify $H^1_{\mathrm{DR}}(G)$ with the quotient

$$\{f \in \Omega^0(G_{S\otimes\mathbb{Q}}) \mid df \in \Omega^1(G_S)\}/\Omega^0(G_S).$$

From this point of view the elements of $\mathbf{D}^1(G)$ are the elements f above satisfying the additional condition that

$$f(\underline{x} \underset{G}{+} \underline{y}) - f(x) - f(y) \in \Omega^0((G \underset{S}{\times} G)). \tag{3.3.10}$$

Now for some examples. We will begin with the case in which G is the one dimensional additive formal group over $\mathbb{Z}_p$. As we saw above $H^1_{\mathrm{DR}}(G)$ is the product of cyclic groups generated by

$$d(\frac{x^{np^k}}{p^k}).$$

When is such an element primitive? First note that

$$(x+y)^{np^k} - x^{np^k} - y^{np^k}$$

is not even divisible by p unless $n = 1$. In that case it is divisible by p but not by p^2. These observations easily imply that

$$\mathbf{D}^1(G) = \prod_{k\geq 0} \mathbb{Z}/p$$

in which the factor with index k is represented by the function x^{p^k}/p.

Before turning to other formal groups let's make a general observation. Suppose that

$$f(x) = \sum a_n x^n \in \mathbb{Q}[\![x]\!]$$

represents an element of $\mathbf{D}^1(G)$. If it happens that some coefficients $\{a_i \mid i \in I\}$ are in S then $f(x) - \sum_{i\in I} a_i x^i$ will also be quasi-primitive and will represent the same element of $\mathbf{D}^1(G)$ as f. We may therefore suppose that the first non-zero term of f is of the form

$$a_k x^k$$

with $0 \neq a_k \in S \otimes \mathbb{Q}/\mathbb{Z}$. Next note that the fact that

$$x \underset{G}{+} y = x + y + \cdots$$

implies that

$$a_k((x+y)^k - x^k - y^k) \in S.$$

As we saw above, this means that k must be a power of p and $pa_k \in S$.

Now let's turn to the case of the Lubin-Tate formal group of height n with logarithm

$$\ell(x) = \sum \frac{x^{p^{nk}}}{p^k} = x + \frac{x^{p^n}}{p} + \cdots .$$

Because

$$\ell(x \underset{G}{+} y) = \ell(x) + \ell(y)$$

this element is actually primitive. This can be used to cancel a term $\frac{x^{p^n}}{p}$. We can get a few more this way. We have

$$p^{m-1}\ell(x) = p^{m-1}x + p^{m-2}x^p + \cdots + x^{p^{(m-1)k}} + \frac{1}{p}x^{p^{(m)k}} + \cdots$$

so we can also cancel leading terms like $x^{p^{mk}}/p$ as well.

How about x^p/p? Well here there is something interesting. I claim that

$$\frac{1}{p}\ell(x^p)$$

is also primitive. Why? This is a little easier to explain in a more general setting.

Let's start with a torsion free p-local ring S and a formal group law Γ over S/pS given y If

$$x \underset{\Gamma}{+} y = \sum a_{ij}x^i y^j$$

We can construct a new formal group law $\phi^*\Gamma$ with

$$x \underset{\phi^*\Gamma}{+} y = \sum \phi(a_{ij})x^i y^j.$$

The fact that

$$(\sum a_{ij}x^i y^j)^p = \sum a_{ij}(x^p)^i(y^p)^j$$

means that the we have a map

$$\begin{aligned} \Gamma &\to \phi^*\Gamma \\ x &\mapsto x^p. \end{aligned}$$

This map is the *Frobenius isogeny.*

Now suppose that S has a map $\phi : S \to S$ which is a lift of Frobenius, in the sense that

$$\phi(x) \equiv x^p \mod pS.$$

Given a power series

$$f(x) = \sum b_i x^i \in (S \otimes \mathbb{Q})[\![x]\!]$$

let

$$f^\phi(x) = \sum \phi(b_i)x^i$$

I claim that if $f(x)$ is the log of a formal group G over S then for any k, the series

$$\frac{1}{p}f^{\phi^k}(x^{p^k})$$

satisfies (3.3.10).

Before turning to the proof I need another general fact about the log of a formal group I haven't had a chance to mention. Suppose $L(x)$ is the log of a formal group G over S. Then by Taylor's theorem

$$L(x+py) = L(x) + \sum_{n>0} L^{(n)}(x)\frac{(py)^n}{n!}.$$

However every term on the right is in pS. We already saw that the derivative of the log has coefficients in S, and you checked above that (p) has divided powers, so $\frac{p^n}{n!}$ is divisible by p.

Returning to G, note that by by naturality, f^{ϕ^k} is a log of G^{ϕ^k}. The fact that

$$(x \underset{G}{+} y)^{p^k} \equiv x^{p^k} \underset{G^{\phi^k}}{+} y^{p^k} \mod pS$$

means that

$$\begin{aligned} f^{\phi^k}(x^{p^k}) + f^{\phi^k}(y^{p^k}) &= f^{\phi^k}(x^{p^i} \underset{G^{\phi^k}}{+} y^{p^k}) \\ &= f^{\phi^k}(x^{p^k} + y^{p^k} + p\epsilon) \\ &= f^{\phi^k}(x^{p^k}) + f^{\phi^k}(y^{p^k}) \mod pS[\![x]\!]. \end{aligned}$$

This implies that $\frac{1}{p}f^{\phi^k}(x^{p^k})$ also satisfies (3.3.10).

Putting this all together, this shows that when G is the Lubin-Tate group with logarithm

$$\ell(x) = \sum x^{p^{nk}}/p^k$$

then $\mathbf{D}^1(G)$ is the free $\mathbb{Z}_p$-module of rank n with basis

$$\{\ell(x), \frac{1}{p}\ell^{\phi}(x^p), \ldots, \frac{1}{p}\ell^{\phi^{n-1}}(x^{p^{n-1}})\}. \tag{3.3.11}$$

3.3.1.6. *Change of base.* Note that the de Rham cohomology $H^*_{\mathrm{DR}}(\mathbb{A}^n_S/S)$ is functorial in S. Given a ring homomorphism $S \to T$ there is a map

$$T \underset{S}{\otimes} H^*_{\mathrm{DR}}(\mathbb{A}^n_S/S) \to H^*_{\mathrm{DR}}(\mathbb{A}^n_T/T).$$

This map is not an isomorphism, but it fails to be for a particular reason. Let's look at the case $n = 1$ Then describe above. we have

$$H^1_{\mathrm{DR}}(\mathbb{A}^1_S/S) = \prod_{(n,p)=1} \prod_{k \geq 1} S/(p^k S).$$

The trouble then is that the tensor product does not, in general, commute with finite products. It does however either T is a finitely presented S module, or if we can avail ourselves of some mechanism of picking out a natural fintely generated sub module of H^{ast}_{DR}. Now when G has finite height, the module $\mathbf{D}(G)$ is exactly such a submodule. This implies the following

Proposition 3.3.12. *Suppose that $f : S \to T$ is a ring homomorphism. If G is a formal group of finite height (and finite dimension) over S then the map*

$$T \underset{S}{\otimes} \mathbf{D}(G/S) \to \mathbf{D}(f^*G/T)$$

is an isomorphism. □

3.3.1.7. *Computing Frobenius.* Suppose that S is a torsion free ring and G_0 is a formal group law over S/p, and that G and G' are lifts of G_0 to S. write Γ for the reduction of G to S/pS. Since

$$x \underset{G}{+} y \equiv x \underset{G'}{+} y \mod (p)$$

and since (p) has divided powers the two group laws

$$(\mathbb{A}^1 \times \mathbb{A}^1)_S \to A^1_S$$

induce the *same* homomorphism on $H^1_{\mathrm{DR}}(\mathbb{A}^1)$. This means that $\mathbf{D}^1(G)$ is *equal* to $\mathbf{D}^1(G')$ when regarded as subsets of $H^1_{\mathrm{DR}}(\mathbb{A}^1_S)$.

In fact it's even better than that. The induced map in de Rham cohomolgy

$$H^1_{\mathrm{DR}}(G) \to H^1_{\mathrm{DR}}(G \times G)$$

can be computed using *any* power series

$$\sum \tilde{a}_{ij} x^i y^j$$

whose reduction mod p is $x \underset{\Gamma}{+} y$. It doesn't actually have to define a group structure on $\mathbb{A}^1$.

All of this means that the object $\mathbf{D}^1(G_S)$ is actually a functor of G_0 and in particular, maps of formal groups over $S/(p)$ give maps of the modules $\mathbf{D}^1(\,-\,)$.

Here is an important example. Consider the Frobenius isogeny

$$\begin{aligned} F : G_0 &\to \phi^* G_0 \\ x &\mapsto x^p. \end{aligned}$$

What is its effect on $\mathbf{D}^1(\,-\,)$? Let G be a lift of G_0 and consider the map $x \mapsto x^p$. This does not quite define a homomorphism $G \to \phi^* G$ but since it lifts a map which is a homomomorphism mod p, it can be used to compute the map

$$\phi^* \mathbf{D}^1(G) = \mathbf{D}^1(\phi^{*G}) \to \mathbf{D}^1(\Gamma).$$

This means that F induces the map

$$\ell^{\phi^k}(x) \mapsto \ell^{\phi^{k+1}}(x^p).$$

Consider the case in which G is the Lubin-Tate group with log

$$\ell(x) = \sum \frac{x^{p^{nk}}}{p^k}.$$

In terms of the basis (3.3.11), the map F has the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ p & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

Now let's work out the matrix of F in case of the universal deformation. We take $S = \mathbb{W}[[u_1, \dots u_{n-1}]]$, $\phi : S \to S$ given by Frobenius on $\mathbb{W}$ and $\phi(u_i) = u_i^p$, and G the formal group law whose log $f(x)$ is defined by the functional equation

$$f(x) = x + \frac{u_1}{p} f^{\phi}(x^p) + \cdots + \frac{u_{n-1}}{p} f^{\phi^{n-1}}(x^{p^{n-1}}) + \frac{1}{p} f^{\phi^n}(x^{p^n}).$$

Then, as above, a basis of $\mathbf{D}^1(\Gamma)$ is

$$\{f(x), \frac{1}{p} f^{\phi}(x^p), \cdots \frac{1}{p} f^{\phi^{n-1}}(x^{p^{n-1}})\},$$

and from the functional equation for f, the map F is given by

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ p & 0 & \cdots & 0 & -u_1 \\ 0 & 1 & \cdots & 0 & -u_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -u_{n-1} \end{pmatrix} \tag{3.3.13}$$

3.3.2. Crystals. To go further it is useful to describe in more abstract terms the nature of the object $\mathbf{D}^1(G)$ that we constructed.

Suppose that S is a ring. Let $\mathbf{Crys}(S)$ be the category of triples $T = (\pi, i, \delta)$ consisting of a diagram of ring homomorphisms

$$\begin{tikzcd} & T \arrow[d, "\pi"] \\ S \arrow[r, "i"'] & U \end{tikzcd} \tag{3.3.14}$$

in which $S \to U$ is a Zariski localization, $T \to U$ is surjective and δ is a divided power structure on the kernel I of π. When I is $\mathbb{Z}$-torsion free the structure δ, if it exists, is unique.

A map in $\mathbf{Crys}(S)$ is map of the above data

$$\begin{tikzcd} & T \arrow[r] \arrow[d, "\pi"] & T' \arrow[d, "\pi'"] \\ S \arrow[r] & U \arrow[r] & U' \end{tikzcd} \tag{3.3.15}$$

in which the map $T \to T'$ is compatible with the divided power structures.

A *crystal* on R consists of a T-module M_T for each diagram (3.3.14) and for each map (3.3.15) in $\mathbf{Crys}(S)$ an isomorphism

$$T' \underset{T}{\otimes} M_T \to M_{T'}$$

satsfying the cocycle condition that if

$$\begin{tikzcd} & T \arrow[r] \arrow[d, "\pi"] & T' \arrow[r] \arrow[d, "\pi'"] & T'' \arrow[d, "\pi''"] \\ S \arrow[r] & U \arrow[r] & U' \arrow[r] & U'' \end{tikzcd} \tag{3.3.16}$$

is a composition in $\mathbf{Crys}(S)$ then the diagram

$$\begin{tikzcd} T'' \underset{T'}{\otimes} T' \underset{T'}{\otimes} M_T \arrow[r] \arrow[d] & T'' \underset{T'}{\otimes} M_{T'} \arrow[d] \\ T'' \underset{T}{\otimes} M_T \arrow[r] & M_{T''} \end{tikzcd} \tag{3.3.17}$$

commutes.

Example 3.3.18. Suppose that S_0 is complete local $\mathbb{F}_p$-algebra and G_0 is deformation to S_0 of a formal group law of finite height. Given a diagram (3.3.14) choose any lift G of i^*G_0 to T and define $M_T = M_T^\Gamma = \mathbf{D}^1(G/T)$. The conditions on G_0 guarantee that $\mathbf{D}^1(G)$ is a finite free T-module and so by all of above discussion this defines a crystal. This is the (contravariant) *Dieudonné crystal* and will be denoted $\mathcal{M}(G_0)$. Thus

$$\mathcal{M}(G_0)_T = \mathbf{D}^1(G)$$

where G is any lift of i^*G to T.

For the crystalline period mapping we will only require the information summarized by Example 3.3.18. But to connect it with the classical period mapping requires another point of view on crystals. Since the language used in describing this situation is derived from the classical period mapping I'll describe it. You can safely skip this section if you wish.

In the situation we are interested in, S is the mod p reduction $k[\![u_1, \dots, u_{n-1}]\!]$ of the Lubin-Tate ring. Since the ideal

$$(p) \subset \mathbb{W}[\![u_1, \dots, u_{n-1}]\!] = E_0$$

has divided powers, a crystal M on S provides an E_0-module M. Given any solid arrow diagram

$$\begin{tikzcd}
\mathbb{W}[\![u_1, \dots, u_{n-1}]\!] \arrow[r, dotted, "f"] \arrow[d] & T \arrow[d] \\
S \arrow[r] & U
\end{tikzcd}$$

a dotted arrow f exists which is compatible with the divided power structure on the kernel of $T \to U$. This means that M_T is determine by M as

$$M_T = T \underset{E_0}{\otimes} M.$$

So a crystal on S is just a module over E_0 equipped with some extra structure.

What is this extra structure? Look at the ring

$$T = E_0\langle\!\langle h_1, \dots, h_{n-1}\rangle\!\rangle \tag{3.3.19}$$

of formal divided power series in variables h_i. There are two maps

$$g_1, g_2 : E_0 \to E_0\langle\!\langle h_1, \dots, h_{n-1}\rangle\!\rangle$$

given by

$$\begin{aligned} g_1(u_i) &= u_i \\ g_2(u_i) &= u_i + h_i. \end{aligned}$$

By definition, if M is to be a crystal, then it must come equipped with an isomorphism

$$\tau : g_1^* M \to g_2^* M.$$

The map τ can be thought of as a map

$$\tau : M \underset{\mathbb{W}[\![\vec{u}]\!]}{\otimes} \mathbb{W}[\![\vec{u}]\!]\langle\!\langle \vec{h}\rangle\!\rangle$$

(in which $\vec{u} = (u_1, \dots, u_{n-1})$, etc) with the property that

$$\tau(f(\vec{u})m) = f(\vec{u} + \vec{h})m. \tag{3.3.20}$$

Write

$$\tau(m) = m + \sum D_i(m)h_i + \cdots .$$

Then (3.3.20) gives

$$D_i(fm) = fD_i(m) + (\partial f/\partial u_i)\, m$$

so that M becomes equipped with a connection.

The operation $\tau = \tau_{\vec{u}}^{\vec{h}}$ satisfies a cocycle condition over

$$\mathbb{W}[\![u_1, \dots, u_{n-1}]\!]\langle\!\langle h_1, \cdots, h_{n-1}, h_1', \cdots, h_{n-1}'\rangle\!\rangle$$

which, in what is hopefully evident notation, is the condition that the diagram

$$\begin{tikzcd}
M_{\vec{u}} \arrow[r, "\tau^{\vec{u}}_{\vec{h}}"] \arrow[dr, "\tau^{\vec{u}}_{\vec{h}+\vec{h}'}"'] & M_{\vec{u}+\vec{h}} \arrow[d, "\tau^{\vec{u}+\vec{h}}_{\vec{h}'}"] \\
 & M_{\vec{u}+\vec{h}+\vec{h}'}
\end{tikzcd}$$

commutes. In terms of the expansion (3.3.20) this implies that the operators D_i commute and so define an integrable connection. In fact the operators D_i determine the operator τ (this is called *integrating the connection form*). In this way one gets an equivalence of categories between crystals on $k[\![u_1, \dots, u_{n-1}]\!]$ and the category of modules over $\mathbb{W}[\![u_1, \dots, u_{n-1}]\!]$ equipped with an integrable connection.

3.4. The crystalline period map

Now let's put this all together. Γ be a 1-dimensional formal group of height n over the algebraic closure k of $\mathbb{F}_p$, G the universal deformation of Γ over $E_0 = \mathbb{W}[\![u_1, \dots, u_{n-1}]\!]$ and G_0 the pullback of G to $k[\![u_1, \dots, u_{n-1}]\!]$. Write $\mathcal{M}_\Gamma$ and $\mathcal{M}_{G_0}$ for the Dieudonné crystals. We have seen that the de Rham cohomology $\mathcal{M}_{G_0}(E_0) = \mathbf{D}^1(G)$ depends only on G_0. The lift G gives us some extra structure. Namely, a particular 1-dimensional subspace generated by

$$d \log_G(x).$$

This is subspace of primitive elements in $H^0(G; \Omega^1)$, and gives a line $H^{0,1} \subset \mathbf{D}^1(G)$. This is called the *Hodge line* in $\mathbf{D}^1(G)$. In this language, the crystalline Dieudonne theory tells us that $\mathbf{D}^1(G)$ determines G_0 while the Tapis de Cartier tells us that the lift G is determined by $\mathbf{D}^1(G)$, equipped with its Hodge structure, which in this case is the Hodge line

$$H^{0,1}(G) \subset \mathbf{D}^1(G).$$

Now lets pull everything back to $\mathbb{W}\langle\!\langle u_1, \dots, u_{n-1}\rangle\!\rangle$. Over this ring the two maps

$$\begin{aligned} u_i &\mapsto u_i \\ u_i &\mapsto 0 \end{aligned}$$

agree modulo the maximal ideal of $\mathbb{W}\langle\!\langle u_1, \dots, u_{n-1}\rangle\!\rangle$, which has divided powers. This means that we have a $\mathbb{W}$-linear map

$$B : M \to \mathbf{D}^1(G)$$

which extends to an isomorphism of E_0-modules

$$M \otimes E_0 \to \mathbf{D}^1(G).$$

So here is the picture, over $\mathbb{W}\langle\!\langle u_1, \dots, u_{n-1}\rangle\!\rangle$

$$\begin{tikzcd}
 & M \arrow[d, "B"] \\
H^{0,1}(G) \arrow[r] & \mathbf{D}^1(G),
\end{tikzcd}$$

analogous to the diagram

$$\begin{tikzcd} & H^1(X;\mathbb{Z}) \arrow[d] \\ H^0(X;\Omega^1) \arrow[r] & H^1_{\mathrm{DR}}(X). \end{tikzcd}$$

Using this we have an abstract period map from the subspace of Lubin-Tate space defined by $\mathbb{W}\langle\langle u_1, \ldots, u_{n-1}\rangle\rangle$ to the projective space $P(M)$. Everything is functorial in Γ so this map is $\mathrm{Aut}(\Gamma)$ equivariant.

How to compute this map? Here there is an amazing thing: the map B is determined by the fact that it is compatible with Frobenius. Let's see how. Let A be the matrix of Frobenius

$$F : \phi^*\mathbf{D}^1(G) \to \mathbf{D}^1(G)$$

computed in §3.3.1.7 and A_0 the one for M. Then specifically

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ p & 0 & \cdots & 0 & -u_1 \\ 0 & 1 & \cdots & 0 & -u_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -u_{n-1} \end{pmatrix}$$

and

$$A_0 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ p & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

Then the compatibilty of B with Frobenius is a commutative diagram

$$\begin{tikzcd} \phi^* M \arrow[r, "A_0"] \arrow[d, "\phi^* B"'] & M \arrow[d, "B"] \\ \phi^*\mathbf{D}^1(G) \arrow[r, "A"'] & \mathbf{D}^1(G). \end{tikzcd}$$

In terms of matrices this is the identity

$$BA(0) = AB^{\phi}$$

or,

$$B = AB^{\phi}A(0)^{-1}.$$

Now just keep substituting this into itself

$$B = AA^{\phi}\cdots A^{\phi^n}B^{\phi^{n+1}}A(0)^{-(n+1)}$$

and take the limit as $n \to \infty$, noting that

$$\lim_{n\to\infty} B^{\phi^{n+1}}$$

is the identity matrix. This gives

$$B = \lim_{n\to\infty} AA^{\phi}\cdots A^{\phi^n}A(0)^{-(n+1)}.$$

In our setup it's actually the first column of B^{-1} that we want. It's not too hard to expand this all out. But for our purposes we don't really need to. All we need to know is that B is uniquely determined by A from the properties

$$B(0) = I_n$$
$$BA(0) = AB^{\phi}.$$

Since it's really B^{-1} we want I'll write these as

$$B^{-1}(0) = I_n$$
$$\left(B^{-1}\right)^{\phi} A(0) = AB^{-1}.$$

Now the matrix A is given by (3.3.13) and if you check it you'll see that the identites (3.1.2) are equivalent to the assertion that the matrix

$$\begin{pmatrix} w & \frac{1}{p}(ww_{n-1})^{\phi} & \frac{1}{p}(ww_{n-2})^{\phi^2} & \cdots & \frac{1}{p}(ww_1)^{\phi^{n-1}} \\ ww_1 & w^{\phi} & (ww_{n-1})^{\phi^2} & \cdots & (ww_2)^{\phi^{n-1}} \\ ww_2 & \frac{1}{p}(ww_1)^{\phi} & w^{\phi^2} & \cdots & (ww_3)^{\phi^{n-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ ww_{n-1} & \frac{1}{p}(ww_{n-1})^{\phi} & \frac{1}{p}(ww_{n-3})^{\phi^2} & \cdots & w^{\phi^{n-1}} \end{pmatrix}$$

Satisfies the identites for B^{-1} described above. (in this matrix the $\frac{1}{p}$ factors disappear in a row as soon as you get to the w term). This means that the period mapping is given in homogeneous coordinates by

$$[w, ww_1, \ldots, ww_{n-1}].$$

LECTURE 4

The crystalline approximation

LECTURE 5

Projects

5.1. Project: finite subgroups

Let $D = D_n$ be the division algebra over $\mathbb{Q}_p$ and $\mathcal{O}_D$ the maximal compact sub algebra, so that the group of units $\mathcal{O}_d^\times$ is the automorphism group of the Lubin-Tate group. The purpose of this project is to work out as many of the finite subgroups of $D^\times$. This is something that appears in print (see [**7**]), but in a given instance there is often something more straightforward one can do. There are three facts that you will use.

Fact 5.1.1. The maximal commutative subalgebras of D are the field extension of $\mathbb{Q}_p$ of degree n. If $L/\mathbb{Q}_p$ is a field extension of degree n then there is an algebra embedding $L \hookrightarrow D$ and any two embeddings of L in D are conjugate.

Fact 5.1.2. Let $L \subset D$ be a maximal commutative subalgebra, and $N \subset D^\times$ the normalizer of L. The natural map $N/L^\times \to \mathrm{Gal}(L/\mathbb{Q}_p)$ is an isomorphism.

Fact 5.1.3. Write $G = \mathrm{Gal}(L/\mathbb{Q}_p)$. The group $H^2(G; L^\times)$ is cyclic of order n with generator the element corresponding to the extension

$$1 \to L^\times \to N \to G \to 1 \tag{5.1.4}$$

ocurring in the central simple division alebra with Hasse invariant $1/n$

Remark 5.1.5. One goes from an extension (5.1.4) to an algebra D by

$$D = \mathbb{Z}[N] \underset{\mathbb{Z}[L^\times]}{\otimes} L.$$

When the extension (5.1.4) is a generator of the group this is a division algebra (see [**25**]).

Exercise 5.1.1. Show that any element of finite order in $D^\times$ is actually in $\mathcal{O}_D^\times$.

Exercise 5.1.2. Show that any finite abelian subgroup of $D^\times$ is cyclic. Suppose that $D^\times$ contains an element of order k. Show that if $(k, p) = 1$ then k divides $p^n - 1$. Show that if $k = p^m$ then $(p-1)p^{m-1}$ divides n. Suppose if $D^\times$ contains an element of order ap^b with $(a, p) = 1$. Show that the maximal finite cyclic subgroups of $D^\times$ have order $(p^f - 1)p^m$ where $f(p-1)p^{m-1}$ divides n.

Now let's work out an example. Suppose that $p = 3$ and $n = 2$. We wish to find all of the finite subgroups of $D^\times$. By Exercise 5.1.2, the elements of finite order must have order dividing 8 ($f = 2$ in the previous exercise), or 6 ($f = 1$, $m = 1$ in the previous exercise). Suppose that $\omega \in D^\times$ has order 3. Then the field extension L of $\mathbb{Q}_3$ generated by ω is a degree 2 extension, and so the Galois group has order 2. It follows that there is a group extension

$$1 \to L^\times \to N \to \mathbb{Z}/2 \to 1.$$

The first order of business is to work out if restricts to an extension

$$1 \to \mathcal{O}_L^\times \to \tilde{N} \to \mathbb{Z}/2 \to 1.$$

This is a question about the long exact cohomology sequence

$$\begin{aligned} H^1(\mathbb{Z}/2; \mathcal{O}_L^\times) \to H^1(\mathbb{Z}/2; L^\times) \to H^1(\mathbb{Z}/2; \mathbb{Z}) \\ \to H^2(\mathbb{Z}/2; \mathcal{O}_L^\times) \to H^2(\mathbb{Z}/2; L^\times) \to H^2(\mathbb{Z}/2; \mathbb{Z}) \end{aligned}$$

Since L is ramified over $\mathbb{Q}_3$ there is no invariant uniformizer. This means that the map $H^2(\mathbb{Z}/2; L^\times) \to H^2(\mathbb{Z}/2; \mathbb{Z})$ is the zero map so the extension does lift.

Next note that the group of units of $\mathcal{O}_L$ has the structure

$$\mathcal{O}_L^\times \approx \mu_6 \times (1 + p\mathcal{O}_L)^\times.$$

Since $H^2(\mathbb{Z}/2; M)$ is trivial if 2 is invertible in M this means that this extension

$$1 \to \mu_6 \to G \to \mathbb{Z}/2 \to 1.$$

splits over $\mu_3 \times (1 + p\mathcal{O}_L)^\times$, and does not over μ_2 (since the cohomology class must generate H^2). This shows that at $p = 3$ the group $\mathbf{S}_2$ contains a finite subgroup isomorphic to the semidirect product

$$Z/3 \rtimes \mathbb{Z}/4.$$

You can check that this is a maximal finite subgroup, and that any two are conjugate.

Exercise 5.1.3. Show that the only p-groups in ℓ-adic division algebras are cyclic if $p > 2$, and either $\mathbb{Q}_8$ if $p = 2$ or cyclic. For which n do the $\mathbb{Q}_8$'s occur?

Exercise 5.1.4. Show that if $\mathcal{O}_D^\times$ contains an element of order p^k then n is divisible by $p^{k-1}(p-1)$.

Exercise 5.1.5. Show that for $p > 2$ the group $\mathbf{S}_{p-1}$ contains a maximal finite subgroup and that it has order $p(p-1)^2$. Show that any two subgroups of this order are conjugate. What happens with $\mathbf{S}_{p(p-1)}$?

5.2. Project: Action of finite subgroups

As described in an earlier lecture, it is proved in [**8**] that if $G \subset \operatorname{Aut} \Gamma$ is finite subgroup whose p-Sylow subgroup is cyclic, then there are deformation parameters for which the crystalline approximation is an isomorphism. This can be checked by hand at heights $(p-1)$ and at height 2 for $p = 2$ (where there is a twist). In this project you will explore some explicit ways of checking this result in these cases.

5.2.1. Height $(p-1)$.

Exercise 5.2.1. Prove this result directly for $p = 2$.

Now assume $p > 2$ and write $n = (p-1)$. In this case there is a maximal finite subgroup which can be written as $\mathbb{Z}/p \rtimes \mathbb{Z}/n^2$ (this is worked out in another one of the projects for this course.) The goal is to find a G-equivariant map

$$M \to E_{-2}$$

inducing the Cartier isomorphism

$$M/pM \approx E_{-2}/(p, \mathfrak{m}^2).$$

Since one can always average over groups of order prime to p you can reduce this to the problem of finding a $\mathbb{Z}/p$-equivariant map. Let $g \in G$ be an element of order p.

EXERCISE 5.2.2. Show that it suffices to find an invertible element $u \in E_{-2}$ with

$$u + gu + \cdots + g^{(p-1)}u = 0.$$

and $u \notin \mathfrak{m}E_{-2}$.

You will do this by finding an element $v \in E_{2(p-1)}$ with the analogous properties, and setting

$$u = v \cdot N(\tilde{u})$$

where $\tilde{u} \in E_{-2}$ is any invertible element, and

$$N(\tilde{u}) = \prod_{i=0}^{p-1} g^i(\tilde{u}).$$

Consider the power series $[p](x)$ representing multiplication by p on the universal deformation. By Lemma 1.2.1 one has

$$[p](x) = v_1 x^p + \cdots .$$

EXERCISE 5.2.3. Show that this formula defines an element $v_1 \in E_{2(p-1)} \otimes \mathbb{Z}/p$ and that this element is in fact invariant under $\operatorname{Aut}\Gamma$.

Now lift v_1 to an element $\tilde{v}_1 \in E_{2(p-1)}$ and define $v \in E_{2(p-1)}$ be defined by

$$pv = g(v_1) - v_1.$$

EXERCISE 5.2.4. Why is the right side divisible by p? Show that the element v satisfies

$$v + gv + \cdots + g^{(p-1)}v = 0.$$

It remains to show that v is not zero modulo the maximal ideal. Let $\mathcal{O} = \mathbb{Z}_p[\zeta_p]$ and $A = \mathbb{W} \underset{\mathbb{Z}_p}{\otimes} \mathcal{O}$, where ζ_p is a primitive p^{th} root of unity. Let $\Gamma_{\mathcal{O}}$ be the $\mathcal{O}$-module over A gotten by change of base of the Lubin-Tate formal $\mathcal{O}$-module along the map $\mathcal{O} \to A$. By construction, the group $G_{\mathcal{O}}$ is a deformation of Γ, and so classified by a map

$$E_0 \to A.$$

The group $G_{\mathcal{O}}$ has complex multiplicaton by ζ_p so the map $E_0 \to A$ is equivariant for the action of G (which acts trivially on A). You can prove that v is not in $\mathfrak{m}E_{2(p-1)}$ by mapping over to $A_{2(p-1)}$ and doing the computation there.

5.3. Project: Line bundles in height 2

This project also concerns material that is well represented in the literature. But it is a very informative exercise to explore. Also the results on cohomology from this point of view are derived in Kohlhaase [**17**]. Behrens [**3**] describes the computation of the Picard group. More details can be found in Beaudry et. al. [**2**] and in the thesis of Lader [**20**]. In this project you will work out the computation of the Picard group of the Lubin-Tate stack at $p \geq 5$ and height $n = 2$. More concretely you will prove the following theorem

THEOREM 5.3.1. *For $p \geq 5$, the restriction map*

$$H^1(\mathbf{S}_2; E_0^\times)^{\mathrm{Gal}} \to \hom(\mathbb{W}^\times, \mathbb{W}^\times)^{\mathrm{Gal}}$$

is a monomorphism, with image the subgroup topologically generated by the identity map and the norm.

Here Gal is the Galois group of k over $\mathbb{F}_p$. I'll leave it to you to pass to Galois invariants at the end.

We will use the crystalline approximation to the action of the $\mathbf{S}_2$ on the ring

$$E_* = \mathbb{W}[u^{\pm 1}][\![u_1]\!]$$

via the map

$$\begin{aligned} M &\to E_{-2}/(p, u_1^p) \\ \gamma &\mapsto u \\ V\gamma &\mapsto uu_1. \end{aligned}$$

Not quite following the conventions in [**5**]) write we will write an automorphism $g \in \mathbf{S}_2$ as

$$\begin{aligned} g(\gamma) &\mapsto a\gamma + bV\gamma \\ g(V\gamma) &\mapsto pb^{\phi^{-1}}\gamma + a^{\phi^{-1}}V\gamma \end{aligned}$$

and so corresponding to a matrix

$$g = \begin{pmatrix} a & pb^{\phi^{-1}} \\ b & a^{\phi^{-1}}. \end{pmatrix}$$

Note that since $n = 2$ one has $\phi^2 = 1$ and so you won't go wrong if you write ϕ^{-1}

The determinant is a map

$$\det : \mathbf{S}_2 \to \mathbb{Z}_p^\times \subset \mathbb{W}^\times.$$

There is an inclusion

$$\begin{aligned} \mathbb{Z}_p^\times \times &\to \mathbf{S}_2 \\ a &\mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}. \end{aligned}$$

The composite is the squaring map and so, since p is odd, is an isomorphism on the 1-units

$$(1 + p\mathbb{Z}_p)^\times.$$

It follows that $\mathbf{S}_2$ can be written as a product

$$\mathbb{Z}_p \times \left(\mathbf{S}_2^s \rtimes \mu_{p^2-1} \right)$$

in which $\zeta \in \mu_{p^2-1}$ corresponds to the matrix

$$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^p \end{pmatrix} \tag{5.3.2}$$

and

$$\mathbf{S}_2^s \subset \mathbf{S}_2$$

is the subgroup of matrices of determinant 1. The factor of $\mathbb{Z}_p$ is acting trivially on everything we will consider and can just be put in at the end. We can make our computation with $\mathbf{S}_2^s$ as long as we project to the invariant part of the action of μ_{p^2-1}.

Write $q = p^2$. Note that reducing the matrices modulo p gives a map

$$\begin{aligned} \alpha\langle p-1\rangle : \mathbf{S}_2^s &\to \mathbb{F}_q = \mu_{q-1} \\ \begin{pmatrix} a & pb^{\phi^{-1}} \\ b & a^{\phi^{-1}}. \end{pmatrix} &\mapsto b. \end{aligned}$$

For ζ as in (5.3.2), we have

$$\alpha\langle p-1\rangle(\zeta g \zeta^{-1}) = \zeta^{p-1}\alpha\langle p-1\rangle(g),$$

so that $\alpha\langle p-1\rangle$ is an element of $H^1(\mathbf{S}_2^s; \mathbb{F}_q)$ transforming in the ζ^{p-1} eigenspace. The element

$$\alpha\langle 1-p\rangle \in H^1(\mathbf{S}_2^s; \mathbb{F}_q)$$

given by

$$\alpha\langle 1-p\rangle(g) = b^{\phi}$$

is in the $\zeta^{(1-p)}$ eigenspace. One easily checks that these form a basis for $H^1(\mathbf{S}_2^s; \mathbb{F}_q)$. Taking the Bockstein of these gives two more elements

$$\begin{aligned} \beta\langle p-1\rangle &= \beta(\alpha\langle p-1\rangle) \in H^2(\mathbf{S}_2^s; \mathbb{F}_q) \\ \beta\langle p-1\rangle &= \beta(\alpha\langle p-1\rangle) \in H^2(\mathbf{S}_2^s; \mathbb{F}_q). \end{aligned}$$

Notation 5.3.3. I've adopted some non-standard notation here in order to make the eigenspace decomposition more transparent. In the topology literature one finds

$$\begin{aligned} &\alpha\langle p-1\rangle \leftrightarrow h_0 u^{p-1} \\ &\alpha\langle 1-p\rangle \leftrightarrow h_1 u^{p(p^2-1)} \\ &\beta\langle p-1\rangle \leftrightarrow g_0 u^{p^2+p-2} \leftrightarrow b_1 u^{p^2(p-1)} \\ &\beta\langle 1-p\rangle \leftrightarrow g_1 u^{(p)(p^2+p-2)} \leftrightarrow b_0 u^{p(p-1)} \end{aligned}$$

Exercise 5.3.1. Show that for $p > 3$, the cohomolgy ring $H^*(\mathbf{S}_2^s; \mathbb{F}_q)$ is the graded commutative ring generated by the classes $\alpha\langle 1-p\rangle$, $\alpha\langle p-1\rangle$, $\beta\langle 1-p\rangle$, $\beta\langle p-1\rangle$ subject to the relations

$$\begin{aligned} \alpha\langle 1-p\rangle\beta\langle p-1\rangle &= \alpha\langle p-1\rangle\beta\langle 1-p\rangle \\ \beta\langle p-1\rangle^2 = \beta\langle 1-p\rangle^2 &= 0. \end{aligned}$$

(This is not straightforward, but it is doable and it is informative. I'll add some guidance an a later revision of these notes.)

The computation will be gased on the following striking theorem of Shimomura and Tamura [**27**].

Theorem 5.3.4. *The map*

$$H^*(\mathbf{S}_2^s; k) \to H^*(\mathbf{S}_2^s; E_0/p)$$

is an isomorphism on μ_{p^2-1} invariants.

Corollary 5.3.5. *The map $H^*(\mathbf{S}_2; \mathbb{W}) \to H^*(\mathbf{S}_2; E_0)$ is an isomorphism.*

EXERCISE 5.3.2. Deduce the Corollary from the Theorem. (The main point of this is to come to grips with what kind of cohomology one is talking about here).

The proof of Theorem 5.3.4 requires some details of the proof of 5.3.5 to which we not turn. It is done by filtering the ring

$$k[\![u_1]\!]$$

by powers of the maximal ideal and running the spectral sequence. The E_1-term is the sum of the cohomology groups

$$H^*(\mathbf{S}_2^s; (u_1)^s/(u_1)^{s+1}).$$

From the crystalline approximation, for $g \in \mathbf{S}_2^s$ (and working modulo p) we have

$$\begin{aligned} g \cdot u &= au + buu_1 + O[u_1]^p \\ &= u + buu_1 + O[u_1]^p \\ g \cdot uu_1 &= pb^{\phi^{-1}}u + a^{\phi^{-1}}uu_1 + O[u_1]^p \\ &= uu_1 + O[u_1]^p \\ g \cdot u_1 &= \frac{a^{\phi^{-1}}u_1 + pb^{\phi^{-1}}}{bu_1 + a} + O[u_1]^p \\ &= \frac{u_1}{1 + bu_1}. \end{aligned}$$

From the above formulas one sees that modulo $(u_1)^2$ the element u_1 transforms in the representation $\zeta^{(p-1)}$, so that the classes

$$\alpha\langle 1-p\rangle u_1 \text{ and } \alpha\langle p-1\rangle u_1^p$$

are invariant. This leads to the following basis for the μ_{p^2-1}-invariant part of the cohomology of the associated graded ring, in which $m = 0, 1, 2, \ldots$

$$\begin{aligned} H^0 : &\quad \{u_1^{m(p+1)}\} \\ H^1 : &\quad \{\alpha\langle 1-p\rangle u_1^{m(p+1)+1}\} \cup \{\alpha\langle p-1\rangle u_1^{m(p+1)+p}\} \\ H^2 : &\quad \{\beta\langle 1-p\rangle u_1^{m(p+1)+1}\} \cup \{\beta\langle p-1\rangle u_1^{m(p+1)+p}\} \\ H^3 : &\quad \{\alpha\langle 1-p\rangle\beta\langle p-1\rangle u_1^{m(p+1)}\}. \end{aligned}$$

Now for the differentials. The first ones are in Miller-Ravenel-Wilson [**24**]. From the transformation formula

$$g \cdot u_1 = \frac{u_1}{1 + b^{\phi}u_1} + O[u_1]^p \quad \text{mod } p$$

we get, for $g \in \mathbf{S}_2^s$

$$u_1 \mapsto u_1 - b^{\phi^{-1}}u_1^2 + O[u_1]^3$$

leading to the differential

$$u_1^{s(p+1)} \mapsto -su_1^{(s-1)(p+1)+1}\alpha\langle 1-p\rangle.$$

From the formula

$$u_1^p \mapsto \frac{u_1^p}{1 + bu_1^p} + O[u_1]^{p^2}$$

we get for $g \in \mathbf{S}_2^s$

$$u_1^p \mapsto u_1^p - bu_1^{2p} + O[u_1]^{3p}$$

and so the differential

$$du_1^{sp(p+1)} = -su_1^{sp(p+1)+p}\alpha\langle p-1\rangle.$$

This looks pretty good, but at the next step there is a bit of trouble. For $g \in \mathbf{S}_2^s$ we have

$$\begin{aligned} u_1^{p^2} &\mapsto \frac{u_1^{p^2}}{1+b^\phi u_1^{p^2}} + O[u_1]^{p^3} \\ &\equiv u_1^{p^2} - b^\phi u_2^{2p^2} + \cdots + O[u_1]^{p^3}. \end{aligned}$$

However since

$$u_1^{2p^2-1} \mapsto u_1^{2p^2-1} + b^\phi u_1^{2p^2} + \cdots$$

we can add this term to the above and get a longer differential. If you do this you find that

$$u_1^{(2)} := u_1^{p^2} + u_1^{2p^2-1} = u_1^{p^2}(1+u_1^{p^2-1})$$

satisfies

$$g(u_1^{(2)}) = u_1^{(2)} + O[u_1^{2p^2+p-1}]$$

and so to go further one requires a more accurate expression for the action. It's not so easy to get the final answer from this point of view. If you want to know how to do it, you should consult the references [**18, 20, 2**].

I'll now just report on all of the differentials

5.3.1. Differentials from H^0 to H^1.

$$\begin{aligned} u_1^{s(p+1)} &\mapsto -su_1^{s(p+1)}u_1\alpha\langle 1-p\rangle \\ u_1^{sp(p+1)} &\mapsto -s\big(u_1^{sp(p+1)}\big)u_1^p\alpha\langle p-1\rangle \\ u_1^{sp^n(p+1)} &\mapsto -2s\big(u_1^{sp^n(p+1)}\big)u_1^{p^n+p^{n-1}-1}\alpha\langle p-1\rangle \qquad n>1 \end{aligned}$$

5.3.2. Differentials from H^1 to H^2. We start with the differentials on the classes $u_1^{s(p+1)}u_1\alpha\langle 1-p\rangle$. The classes with $s \not\equiv 0 \mod p$ are in the image of the differentials from H^0 so are in the kernel of the differential from H^1 to H^2. I won't remark on this kind of thing further, and will leave it to you to check that all of the necessary differentials have been reported.

$$u_1^{sp(1+p)}u_1\alpha\langle 1-p\rangle \mapsto u_1^{sp(1+p)}u_1u_1^{p-1}\beta\langle p-1\rangle. \tag{5.3.6}$$

Exercise 5.3.3. These differentials are within the range of the cryatalline approximation. Can you account for them? (I haven't tried this).

The differentials on the classes

$$u_1^{s(p+1)}u_1^p\alpha\langle p-1\rangle$$

break into cases. For $s \not\equiv 1 \mod p^2$ one has

$$d(u_1^{(s-1)(1+p)}\,u_1^p\alpha\langle p-1\rangle) \mapsto -\binom{s}{2}u_1^{s(1+p)}\,u_1\beta\langle 1-p\rangle \tag{5.3.7}$$

(5.3.8)

$$d(u_1^{(sp^n-1)(1+p)}\,u_1^p\alpha\langle p-1\rangle) \mapsto -\frac{(-1)^n}{2}\binom{s}{2}u_1^{sp^n(1+p)}\,u_1^{(p+1)\frac{p^n-1}{p-1}}\,u_1\beta\langle 1-p\rangle$$

For $s \equiv 1 \mod p^2$ one has

(5.3.9)

$$d(u_1^{(s-1)(1+p)}\, u_1^p \alpha\langle p-1\rangle) \mapsto -u_1^{sp^n(1+p)}\, u_1^{(1+p)(p-1)}\, u_1\beta\langle 1-p\rangle$$

(5.3.10)

$$d(u_1^{(sp^n-1)(1+p)}\, u_1^p \alpha\langle p-1\rangle) \mapsto -\frac{(-1)^n}{4} u_1^{sp^n(1+p)}\, u_1^{(1+p)(\frac{p^n-1}{p-1}+p^n(p-1))}\, u_1\beta\langle 1-p\rangle$$

(5.3.11)

5.3.3. Differentials from H^2 to H^3. The differentials from H^2 to H^3 are actually determined by Poincaré duality. I'll record them here and if there is interest set up a project/guided exercise for deducing them.

First the differentials on the elements

$$u_1^{(p+1)m} u_1\beta\langle 1-p\rangle.$$

Every integer m can be written uniquely in the form

$$m = 1 + p + \cdots + tp^{n-1}$$

with $t \not\equiv 1 \mod p$. The differential on the classes $u_1^{(p+1)\ell} u_1^p \alpha\langle p-1\rangle$ hit the classes with

$$t \not\equiv 0 \mod p.$$

This leaves the elements of the form

$$m = 1 + \cdots + p^{n-2} + sp^n.$$

In this way we associate n and s to each eligible m. The differential is

$$u_1^{(p+1)m} u_1\beta\langle 1-p\rangle \mapsto -2(s-1)u_1^{(p+1)m}\, u_1^{(p+1)p^{n-1}} \alpha\langle p-1\rangle\beta\langle 1-p\rangle.$$

The differentials on the classes

$$u_1^{(p+1)m} u_1^p \beta\langle p-1\rangle$$

follows from the differentials on $u_1^{(p+1)s}$ with $s \not\equiv 0 \mod p$. The formula is

$$u_1^{(p+1)s} u_1^p \beta\langle p-1\rangle \mapsto -su_1^{(p+1)s} u_1^{(p+1)} \alpha\langle 1-p\rangle\beta\langle p-1\rangle.$$

Exercise 5.3.4. How accurately would one need the formula for $g(u_1)$ to account for all of these differentials?

Exercise 5.3.5. Assuming these differentials deduce Theorem 5.3.4. (This is just a matter of bookkeeping, but it's worthwhile straightening it out.)

We can now turn to the proof of Theorem 5.3.1.

Exercise 5.3.6. Show that there is a short exact sequence of $\mathbf{S}_2^s$-modules

$$0 \to E_0 \xrightarrow{\exp(px)} E_0^\times \to (E_0/p)^\times \to 1.$$

This short exact sequence gives a long exact sequence in cohomology. You can work out one third of the terms from Theorem 5.3.5, so the computation reduces to knowing

$$H^1(\mathbf{S}_2^s; (E_0/p)^\times) = H^1(\mathbf{S}_2^s; k[\![u_1]\!]^\times).$$

You do this by filtering by kernels of the map

$$k[\![u_1]\!]^\times \to k[\![u_1]\!]/(u_1^j)^\times$$

and studying the spectral sequence

$$\bigoplus H^*(\mathbf{S}_2^s; (1+u_1^\ell k[\![u_1]\!])^\times/(1+u_1^{\ell+1}k[\![u_1]\!])^\times) \Rightarrow H^*(\mathbf{S}_2^s; (k[\![u_1]\!]^\times). \tag{5.3.12}$$

You can finish the project by doing this. There are two observations you will need.

Observation 5.3.13. For each n, the module E_{-n} is invertible. It maps the element of $H^1(\mathbf{S}_2^s; k[\![u_1]\!]^\times)$ given by the crossed homomorphism

$$g \mapsto g(u^n)/u^n.$$

You can work out what you need of this from the chromatic approximation. This gives a bunch of elements that you know survive this spectral sequence.

Observation 5.3.14. The group

$$(1+u_1^\ell k[\![u_1]\!])^\times/(1+u_1^{2\ell}k[\![u_1]\!])^\times$$

is isomorphic to $(u_1^\ell)/(u_1^{2\ell})$ so in a certain range the "multiplicative" spectral sequence (5.3.12) is isomorphic to the "additive" spectral sequence analyzed by Shimomura, and you can use those differentials.

Armed with these two observations it is possible to prove Theorem 5.3.1.

Bibliography

1. J. F. Adams, *Stable homotopy and generalised homology*, University of Chicago Press, Chicago, 1974.
2. Agnes Beaudry, Naiche Downey, Connor McCranie, Luke Meszar, Andy Riddle, and Peter Rock, *Computations of orbits for the lubin-tate ring*, J. Homotopy Relat. Struct. (2018) (2018), 1–28.
3. Mark Behrens, *The homotopy groups of $S_{E(2)}$ at $p \geq 5$ revisited*, Adv. Math. **230** (2012), no. 2, 458–492. MR 2914955
4. Pierre Cartier, *Relèvements des groupes formels commutatifs*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. Exp. No. 359, 217–230. MR 3077128
5. Ethan S. Devinatz and Michael J. Hopkins, *The action of the Morava stabilizer group on the Lubin-Tate moduli space of lifts*, Amer. J. Math. **117** (1995), no. 3, 669–710. MR 97a:55007
6. A. Fröhlich, *Formal groups*, Lecture Notes in Mathematics, vol. 74, Springer–Verlag, New York, 1968.
7. Thomas Hewett, *Finite subgroups of division algebras over local fields*, J. Algebra **173** (1995), no. 3, 518–548. MR 1327867
8. Michael A. Hill, Michael J. Hopkins, and Douglas Ravenel, *Crystalline deformation parameters adapted to finte quotients of Lubin-Tate space*, in preparation.
9. M. J. Hopkins and B. H. Gross, *Equivariant vector bundles on the Lubin-Tate moduli space*, Topology and representation theory (Evanston, IL, 1992), Contemp. Math., vol. 158, Amer. Math. Soc., Providence, RI, 1994, pp. 23–88. MR 1263712
10. ______, *The rigid analytic period mapping, Lubin-Tate space, and stable homotopy theory*, Bull. Amer. Math. Soc. (N.S.) **30** (1994), no. 1, 76–86. MR 1217353
11. N. Katz, *Crystelline cohomology, Dieudonné modules and Jacobi sums*, Automorphic forms, Representation theory and Arithmetic (Bombay), Tata Institute of Fundamental Research, 1979, pp. 165–246.
12. Nicholas M. Katz, *Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin*, Inst. Hautes Études Sci. Publ. Math. (1970), no. 39, 175–232. MR 0291177
13. Nicholas M. Katz and Tadao Oda, *On the differentiation of de Rham cohomology classes with respect to parameters*, J. Math. Kyoto Univ. **8** (1968), 199–213. MR 0237510
14. Jan Kohlhaase, *Invariant distributions on p-adic analytic groups*, Duke Math. J. **137** (2007), no. 1, 19–62. MR 2309143
15. ______, *The cohomology of locally analytic representations*, J. Reine Angew. Math. **651** (2011), 187–240. MR 2774315
16. ______, *Lubin-Tate and Drinfeld bundles*, Tohoku Math. J. (2) **63** (2011), no. 2, 217–254. MR 2812452
17. ______, *On the Iwasawa theory of the Lubin-Tate moduli space*, Compos. Math. **149** (2013), no. 5, 793–839. MR 3069363
18. ______, *Iwasawa modules arising from deformation spaces of p-divisible formal group laws*, Iwasawa theory 2012, Contrib. Math. Comput. Sci., vol. 7, Springer, Heidelberg, 2014, pp. 291–316. MR 3586818
19. Jan Kohlhaase and Benjamin Schraen, *Homological vanishing theorems for locally analytic representations*, Math. Ann. **353** (2012), no. 1, 219–258. MR 2910788
20. O. Lader, *Une résolution projective pour le second groupe de morava pour $p \geq 5$ et applications*, Ph.D. thesis, Université de Strasbourg, 2013.
21. J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Annals of Mathematics **81** (1965), 380–387.

22. ———, *Formal moduli for one parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–60.
23. B. Mazur and W. Messing, *Universal extensions and one dimensional crystalline cohomology*, Lecture Notes in Mathematics, vol. 370, Springer–Verlag, Berlin and New York, 1974.
24. H. R. Miller, D. C. Ravenel, and W. S. Wilson, *Periodic phenomena in the Adams–Novikov spectral sequence*, Annals of Mathematics **106** (1977), 469–516.
25. J.-P. Serre, *Applications algébriques de la cohomologie des groupes I,II*, Séminaire H. Cartan de l'Ecole Normal Supérieure, 1951–1952, publisher unknown, 1952.
26. ———, *Local class field theory*, Algebraic Number Theory (University of Sussex, Brighton) (J. W. S. Cassels and A. Fröhlich, eds.), London Mathematical Society, Academic Press, 1967.
27. K. Shimomura and H. Tamura, *Non–triviality of some compositions of β–elements in the stable homotopy of the Moore spaces*, Hiroshima Mathematical Journal **16** (1986), 121–133.