Deformation Theory of Formal Modules

by Yu Yasufuku

Harvard University
Cambridge, Massachusetts
April 3, 2000

To my parents

Acknowledgement

I would like to express my great appreciation to my thesis adviser Professor Richard Taylor for all the mathematical help, for his generosity, and for his kind support. He always welcomed me into his office with a warm smile. I truly appreciate his great advisorship.

I would also like to express my thanks to Professor Brian Conrad, who kindly helped me with profinite modules and commutative formal group schemes. I would not have been able to complete Section 4.3 without his help.

I thank Max Lieblich, a great roommate and a friend, for many interesting and exciting conversation, including helpful math conversations; Dan Lee for being a great friend of mine and for checking grammar in this thesis (though of course I still take full responsibility for all the mistakes); Nils Barth for all the LaTeX help; and suitemates Henry Fu, Kaiwen Kam, Liam McAllister, and Albert Pan for all the laughs I shared.

Finally, I would like to express my deep and heartfelt thanks to my parents, who have greatly supported me throughout my life. I would like to especially thank my mother, who has given me tremendous mental support and constant encouragement.

Thank you all!

Contents

1 Introduction **3**
1.1 Notation . . . 4

2 Introduction to Formal Groups and Formal Modules **5**
2.1 Basic Properties . . . 5
2.2 Properties of Formal Groups: Lazard's Theorem . . . 8
2.3 Generalized Formal R-Modules . . . 11

3 Formal R-Modules for Various R **17**
3.1 Universal Formal R-Modules . . . 17
3.2 R is a Field . . . 19
3.3 R is the Valuation Ring of Local Field . . . 21
3.3.1 A Special Case: A Is A Field Over $R/(\pi)$ . . . 23

4 Deformation Theory **29**
4.1 Deformations . . . 30
4.1.1 Cohomology . . . 31
4.1.2 Universal Deformation . . . 33
4.2 Deformations With Level Structure . . . 35
4.3 The Deformations of Divisible Modules . . . 41

5 Applications of Deformation Theory **51**
5.1 Applications to Local Class Field Theory . . . 51
5.2 Applications to the Arithmetic of Function Fields . . . 53

A Profinite Modules and Commutative Formal Group Schemes **55**
A.1 Preliminary . . . 55
A.2 Formal Schemes . . . 57
A.3 Duality and Commutative Group Schemes . . . 57
A.4 Formal Étaleness . . . 58
A.5 Formal Smoothness . . . 59

Chapter 1

Introduction

In [5], Drinfel'd proved the analogues of the Fundamental Theorem of Complex Multiplication and the Langlands Conjecture for global function fields (for $d = 1, 2$). As discussed in [10], this paper has inspired much work in the arithmetic of global function fields, including some explicit class field theory. It has also been directly influential in number theory, for example, in the theory of moduli spaces of elliptic curves.

To prove these analogues, Drinfel'd introduced the notion of elliptic modules (now called Drinfel'd modules in the literature), an analogue of elliptic curves. Further, he studied their moduli problems, determining the 'parameter space' of all Drinfel'd modules with some additional structures, namely the level structures. Before studying 'all' Drinfel'd modules simultaneously as required for the determination of moduli spaces, he first analyzed them 'locally,' that is, analyzing Drinfel'd modules which are 'close' to a given one. This 'local' analysis of Drinfel'd modules led to deformations of formal modules. So the deformation theory of formal modules lies at a foundation of [5].

Despite its importance and beauty, however, the state of the literature on this deformation theory of formal modules leaves something to be desired. The original source [5, §1 and 4] certainly has all the results and main ideas of proofs, but it is extremely dense (Section 4.3 is condensed into 20 lines) and lacks some important details that one might want to see to better understand the theory. It also assumes knowledge of earlier results, such as the basic theory of formal groups as covered in [8] and their deformations [19]. The only other literature on deformation of formal modules that the author is aware of are [2] and [30]. These give many of the important details that are missing in [5], but as lecture notes, they are not full accounts of the theory, either.

To remedy the situation, this thesis is intended to give a thorough treatment of this deformation theory of formal modules for the reader at or around the level of beginning graduate students. As such, it covers necessary facts from [8] and [19], and develops the theory with details. In order to convey the big picture as well, however, we will give overviews of chapters, sections, and proofs.

We will now give an overview of this thesis. Chapter 2 discusses definitions and basic properties of formal groups and formal modules, together with examples. Chapter 3 analyzes the possibilities of formal R-modules when R is a field and when R is the valuation ring of a local field. These results about *all* formal modules are obtained by determining and carefully analyzing *one* formal module, namely the universal one. This category-theoretic technique will be used throughout this thesis. In Chapter 4, deformation theory of formal modules (without and with level structures) is presented, using results from Chapters 2 and 3. The last chapter is devoted to applications of the deformation theory developed in Chapter 4. In addition to a brief description of how it is used in the study of global function fields in [5], we will include an application to local class field theory.

Naturally the main reference of this thesis is [5]. The notes [2] and [30] were extremely helpful, especially [2] for Section 4.3 and [30] for Section 3.3.1. Other references will be given for each section.

We will assume that the reader is familiar with basic category theory [15], with commutative algebra [1], and with some valuation theory of local fields [22] [23]. We will also assume some familiarity with the language of modern algebraic geometry [11]. Everything else will be either developed or cited explicitly. In particular, there is an appendix on profinite modules and commutative formal group schemes which

summarizes results that we need from [3].

1.1 Notation

We now set forth standard notations which are used throughout this thesis. As usual, $\mathbb{Z}$ and $\mathbb{Q}$ indicate the integers and the rational numbers. p and ℓ will *always* denote a prime number (while l is sometimes used for index, but only in places where ℓ is not around), q is always a power of p. We will denote the finite field with p^n elements $\mathbb{F}_{p^n}$. All rings are *commutative* with 1 unless otherwise specified. If B is an A-algebra by $f : A \to B$, we will often write $a \in B$ instead of $f(a)$, even if f is not injective. This does clarify the exposition significantly, and whenever there is a possibility of confusion, we will write $\cdot$ after a, just like modules. We will use a bar over a field to denote its algebraic closure, and we will use a bar over a ring to indicate the ring modulo an ideal. If F is a power series (in several variables), we often refer to the sum of all monomials in F with total degree strictly less than n as 'F modulo polynomial degree n' and write this as $\pmod{\text{poly. deg. } n}$. The standard notation for this seems to be $\pmod{\deg n}$, but since we will have another notion of degree (on the universal formal R-module ring) we need to distinguish the two.

Unfortunately, we must use two different definitions of 'formal modules' in this thesis, the one in Section 2.3 more general than the one in Section 2.1. We will use definition of Section 2.3 only in Sections 2.3 and 4.3, and in these sections, we will call those satisfying the definition of Section 2.1 the CFS formal modules (name to be explained later). We could have referred to the formal modules of Section 2.1 as CFS formal modules everywhere, but since this thesis is mostly about CFS formal modules, it only clutters up the writing. We will remind the reader about this change of definition in the corresponding sections.

Chapter 2

Introduction to Formal Groups and Formal Modules

This chapter discusses definitions and elementary properties of formal groups and formal modules. Section 2.1 is mostly definitions and examples. Among the examples, the image (Example 2.1.10) and push-forward will be used throughout this thesis.

The second section describes an elementary formal group theory [8, III §1]. In particular, we show Lazard's Theorem which gives the possibilities of $F(X,Y) - G(X,Y)$ when F and G are formal groups with $F \equiv G \pmod{\text{poly. deg. } n}$. We will also prove an easy way of characterizing formal groups which are isomorphic to the additive group. Although this thesis is about formal modules, knowing the underlying formal group structure sometimes severely limits the possibilities of the module structures, so this section will be useful.

Section 2.3 gives a more general notion of formal R-modules that we will need for Section 4.3. This section assumes knowledge of Appendix A. After giving this general definition, we will show that this definition is indeed more general than the one given in Section 2.1, and we will show an example (the étale formal R-module) which does not satisfy the definition in Section 2.1. The rest of the section is devoted to short exact sequences of formal R-modules, in particular to the connected-étale sequences and to the group structure on the extension classes of formal R-modules. Main reference for this section is [3], but [27], [29], and [31] were all used.

2.1 Basic Properties

In this section, we will introduce the notions of formal groups and modules, with some examples. First, we define formal groups:

Definition 2.1.1. A *one-dimensional commutative formal group* over a ring A is a power series $F(X,Y) \in A[\![X,Y]\!]$ satisfying the following four conditions:
(1) $F(X,F(Y,Z)) = F(F(X,Y),Z)$
(2) $F(X,Y) = F(Y,X)$
(3) $F(X,0) = X \quad$ and $\quad F(0,Y) = Y$
(4) There exists a unique $G(X) \in (X) \subseteq A[\![X]\!]$ such that $F(X,G(X)) = F(G(X),X) = 0$

It is helpful to think of a formal group as a formal group *law*, by viewing the variables X and Y as the hypothetical 'group elements' and the power series F as the law of 'adding' X and Y (in fact, [13] and [25] use the terminology formal group law). Although a formal group does not give us any specific group elements, this view enables us to see condition (1) as associativity, (2) as commutativity, (3) as existence of 0, and (4) as existence and uniqueness of inverses. Taking this one step further, if for example A is $\mathfrak{a}$-adically complete (thus also separated in the $\mathfrak{a}$-adic topology), then for elements $x, y \in \mathfrak{a}$, $F(x,y)$ is a well-defined element of $\mathfrak{a}$, and $F(x,y) = x \underset{F}{+} y$ defines a (usual) abelian group structure on $\mathfrak{a}$. We will use $F(\mathfrak{a})$ to denote this abelian group structure on $\mathfrak{a}$.

Example 2.1.2. As an example of how a formal group naturally arises, we will briefly discuss elliptic curves [28]. They can be thought of as (smooth) curves E of genus 1 over a ring A with a specified base point, or as the locus in $\mathbb{P}^2$ of the equation ($x = X/Z, y = Y/Z$ are the non-homogeneous coordinates)

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

together with the 'point of infinity' $O = [0 : 1 : 0] \in \mathbb{P}^2$. We can define an addition on the points on elliptic curves, with O serving as the identity. The completion of the localization of the coordinate ring at the origin is a complete discrete valuation ring, with $z = -\frac{x}{y}$ as a uniformizer. Letting $w = -\frac{1}{y}$, (z, w) gives a local coordinate around O. Using (2.1) recursively, we can obtain an expression for w as an element $g(z) \in A[\![z]\!]$, so we can define $F(z_1, z_2) \in A[\![z]\!]$ to be the z-coordinate of the sum of two points $(z_1, g(z_1))$ and $(z_2, g(z_2))$. This F is a formal group. Note that F arises by analyzing the addition law in an 'infinitesimal' neighborhood around O.

We can generalize Definition 2.1.1 to higher dimensions: writing $X = \{X_1, \ldots, X_n\}$ and $Y = \{Y_1, \ldots, Y_n\}$, an **n-dimensional formal group** F over A is a set of n power series $F_i(X, Y) \in A[\![X, Y]\!]$ such that $F = (F_1, \ldots, F_n)$ satisfies the conditions of Definition 2.1.1. In this thesis, however, we will only need one-dimensional commutative formal groups, so from now on, a formal group will *always mean a one-dimensional commutative formal group.*

Though we need all four conditions in Definition 2.1.1 to get a parallel of abelian groups, it is actually only necessary to check the first three conditions:

Proposition 2.1.3. *If $F \in A[\![X, Y]\!]$ satisfies* (1) *through* (3) *of Definition* 2.1.1*, then it satisfies* (4)*.*

Proof. To avoid infinite sums of elements of A, we *must* pick $G(X)$ from the ideal $(X) \subseteq A[\![X]\!]$. We will inductively construct $G_n(X) = \sum_{i=1}^{n} \lambda_i X^i$ such that $F(X, G_n(X)) \equiv 0 \pmod{\text{poly. deg. } n+1}$. This kind of 'successive approximation' will be used very frequently. $\lambda_1 = -1$ starts us off, so suppose we have constructed up to $G_{n-1}(X)$. We can write $F(X, G(X)) = X + G(X) + \sum a_{ij} X^i (G(X))^j$, where the sum runs over $i + j \geq 2$. Now, modulo X^{n+1}, there is no contribution of terms involving λ_n from inside the sum, so we can solve for λ_n to continue induction. Commutativity implies $F(G(X), X) = 0$ for the same G, and if G_1 and G_2 both satisfy (4), then we have (just like the usual group theory case)

$$G_1(X) = G_1(X) \underset{F}{+} 0 = G_1(X) \underset{F}{+} \left(X \underset{F}{+} G_2(X) \right) = \left(G_1(X) \underset{F}{+} X \right) \underset{F}{+} G_2(X) = G_2(X).$$

□

There are two simple examples of formal groups. First, $\widehat{\mathbb{G}}_{\mathrm{a}}(X, Y) = X + Y$ defines the **additive** formal group, corresponding to the addition in A. Secondly, $\widehat{\mathbb{G}}_{\mathrm{m}}(X, Y) = X + Y + XY$ defines the **multiplicative** formal group, corresponding to the multiplication on the set $1 + \mathfrak{a}$ for a proper ideal $\mathfrak{a}$ of A.

Next, we introduce the notion of homomorphisms.

Definition 2.1.4. Given formal groups F, G over A, $\alpha(X) \in (X) \subseteq A[\![X]\!]$ is a *formal group homomorphism* from F to G if $G(\alpha(X), \alpha(Y)) = \alpha(F(X, Y))$. An *endomorphism* of the formal group F is a formal group homomorphism from F to F, and the set of all endomorphisms is denoted $\mathrm{End}(F)$. By the *derivative* of α, we mean the coefficient of X in α. As usual, we call α an *isomorphism* if there exists a formal group homomorphism $\beta : G \to F$ such that $\alpha(\beta(X)) = X$ and $\beta(\alpha(X)) = X$. Here, $\alpha(\beta(X)) = \alpha \circ \beta$ denotes the power series

$$a_1 \left(\sum b_i X^i \right) + a_2 \left(\sum b_i X^i \right)^2 + \cdots,$$

where $\alpha(X) = \sum a_j X^j$ and $\beta(X) = \sum b_i X^i$. In this case, we denote $\beta = \alpha^{-1}$.

Note that α does not have a constant term, so α^{-1} cannot possibly refer to the inverse of α as an element of $A[\![X]\!]$, so there should be no confusion. By viewing formal groups as giving laws of addition, the above condition says $\alpha(X \underset{F}{+} Y) = \alpha(X) \underset{G}{+} \alpha(Y)$, which makes sense. As in the case of abelian group homomorphisms, we have the following fact:

Proposition 2.1.5. $\mathrm{End}(F)$ *is a (not necessarily commutative) ring for any formal group* F.

Proof. Given $\alpha_1, \alpha_2 \in \mathrm{End}(F)$, we define the ring structure by

$$(\alpha_1 \underset{F}{+} \alpha_2)(X) = F(\alpha_1(X), \alpha_2(X)) \quad \text{and} \quad (\alpha_1 \cdot \alpha_2)(X) = \alpha_1(\alpha_2(X)).$$

Using (1) through (4) of the definition of formal groups, it is straight-forward to check that these operations produce elements of $\mathrm{End}(F)$ and that this forms a ring. □

In particular, we have a ring homomorphism $\mathbb{Z} \longrightarrow \mathrm{End}(F)$, sending $m \mapsto [m]_F(X) = \underbrace{X \underset{F}{+} \cdots \underset{F}{+} X}_{m}$. We also have an easy way of detecting isomorphisms:

Proposition 2.1.6. *Suppose that* α *is a formal group homomorphism from* F *to* G *over* A. *Then* α *is an isomorphism if and only if the derivative is in* A^*.

Proof. $\Longleftarrow$: Using the successive approximation method as in the proof of Proposition 2.1.3, because of the derivative hypothesis on α, we can construct $\beta(X)$ such that $\alpha(\beta(X)) = X$. By the same argument, since the derivative of β is a unit, there exists $\alpha_2(X)$ such that $\beta(\alpha_2(X)) = X$. But then $\alpha(X) = \alpha(\beta(\alpha_2(X))) = \alpha_2(X)$, so α and β are inverses. Also, β is a formal group homomorphism, since

$$\beta(G(X,Y)) = \beta\Big(G\big(\alpha(\beta(X)), \alpha(\beta(Y))\big)\Big) = F(\beta(X), \beta(Y)).$$

The converse is clear by looking at the derivative of $\alpha(\beta(X)) = X$. □

Given the above proposition, we will define an element $\alpha \in A[\![X]\!]$ to be **∘-invertible** if its derivative is in A^*, and denote its ∘-inverse by α^{-1} (this is not a standard terminology).

Example 2.1.7. Suppose $pA = 0$. If $\sum a_i X^i$ is an endomorphism of $\widehat{\mathbb{G}}_{\mathrm{a}}$, then $a_i X^i + a_i Y^i = a_i (X+Y)^i$. If $i = p^\nu s$ with $(p,s) = 1$ and $s > 1$, then $\left(\binom{i}{p^\nu}, p\right) = 1$, so $a_i = 0$. On the other hand $\sum a_i X^{p^i}$ *is* an endomorphism of $\widehat{\mathbb{G}}_{\mathrm{a}}$. Thus, an element of $\mathrm{End}(\widehat{\mathbb{G}}_{\mathrm{a}})$ is of the form $\sum a_i \tau^i$, where each a_i corresponds to the endomorphism $a_i X$ and τ corresponds to X^p, with the ring structure given by the relation $a^p \tau = \tau a$. We will denote this ring by $A\{\{\tau\}\}$. Automorphisms are elements of $A\{\{\tau\}\}$ whose constant term is in A^*.

We will now define formal R-modules over A, where R is a ring and A is an R-algebra.

Definition 2.1.8. A *formal R-module* over A is a pair $(F, [\ ]_F)$ such that $F \in A[\![X,Y]\!]$ is a formal group, and the map $[\ ]_F : R \to \mathrm{End}(F)$ sending $r \mapsto [r]_F$ is a ring homomorphism satisfying the condition $[r]_F \equiv r \cdot X \pmod{\text{poly. deg. } 2}$.

Again this parallels the definition of usual modules. Note that the additive formal group over A can be made into the **additive formal R-module** $\widehat{\mathcal{G}}_{\mathrm{a}}$, just by defining $[r]_F = r \cdot X$. Similarly as before, if A is $\mathfrak{a}$-adically complete, then we can view the set $\mathfrak{a}$ as an R-module via F; we denote this module by $F(\mathfrak{a})$.

To facilitate successive approximation of formal R-modules, it is useful to define the notion of a germ: a formal R-module **germ** of degree n over A is $(F, [\ ]_F)$ with $F \in A[\![X,Y]\!]/(X,Y)^n$ and $[r]_F \in A[\![X]\!]/(X)^n$ such that all the relations of a formal R-module are satisfied modulo polynomial degree n.

Definition 2.1.9. $\alpha : F \to G$ is a *formal R-module homomorphism* if it is a formal group homomorphism and $\alpha([r]_F(X)) = [r]_G(\alpha(X))$ for all $r \in R$.

Given two formal R-module homomorphisms α_i, both the 'addition' $\alpha_1 \underset{G}{+} \alpha_2 = G(\alpha_1(X), \alpha_2(X))$ and the composition $\alpha_1 \circ \alpha_2$ result in a formal R-module homomorphism. With these operations, the set $\mathrm{End}_R(F)$ of all formal R-module endomorphisms of F becomes a (not necessarily commutative) ring, just as in Proposition 2.1.5. We will continue to use $\mathrm{End}(F)$ to denote the set of formal group homomorphisms of the underlying formal group. By employing the same argument as in the proof of Proposition 2.1.6, we can detect formal R-module isomorphisms using the derivative. We will now discuss a simple but important example of formal R-modules and their homomorphisms.

Example 2.1.10. Let $(F, [\ ])$ be a formal R-module over A and let $\alpha \in (X) \subseteq A[\![X]\!]$ be $\circ$-invertible. Let $G(X,Y) = \alpha(F(\alpha^{-1}(X), \alpha^{-1}(Y)))$ and $[r]_G(X) = \alpha([r]_F(\alpha^{-1}(X)))$. This makes G into a formal R-module over A, with α as a formal R-module isomorphism from F to G. We will call G the **image** of F via the isomorphism α (this is not a standard terminology). In particular, if $\alpha(X) \equiv X + aX^n \pmod{\text{poly. deg. } n+1}$ for some $a \in A$, then $\alpha^{-1}(X) \equiv X - aX^n \pmod{\text{poly. deg. } n+1}$, and so we obtain

$$\begin{aligned} G(X,Y) &\equiv F(X,Y) + a((X+Y)^n - X^n - Y^n) && \pmod{\text{poly. deg. } n+1} \\ [r]_G(X) &\equiv [r]_F(X) + (r^n - r) \cdot aX^n && \pmod{\text{poly. deg. } n+1}. \end{aligned}$$

These formulae will be useful for successive approximation later on.

Another important operation is the following. Given a formal R-module F over A and an R-algebra homomorphism $f : A \to B$, the **push-forward** $f_*(F)$, defined by changing all the coefficients of $F(X,Y)$ and $[r]_F(X)$ via f, is a formal R-module over B. A special case is reduction of a formal R-module over A modulo an ideal $\mathfrak{a} \subseteq A$. With push-forwards, the association sending an R-algebra A to the set of formal R-modules over A becomes a functor. This functor will be studied for various R's and A's in Chapter 3.

More sophisticated examples of the formal modules will be given throughout this thesis. From now on, just as we do with modules, we will slightly abuse the notation by using F to refer to both the entire formal R-module structure and $F(X,Y)$ in particular, depending on context.

2.2 Properties of Formal Groups: Lazard's Theorem

Although our primary focus in this thesis is formal modules, we first need to understand the possibilities and limitations of formal groups. In particular, we will present Lazard's Theorem which is useful for successive approximation. As a consequence of this, we will be able to characterize formal groups which are isomorphic to $\widehat{\mathbb{G}}_{\mathrm{a}}$.

Before stating Lazard's theorem, we need to introduce a notation. Let $\epsilon(n)$ be 1 if n is not a power of a prime, and let it be ℓ when n is a power of a prime ℓ. Then define

$$C_n(X,Y) = \frac{1}{\epsilon(n)} \left((X+Y)^n - X^n - Y^n \right).$$

$C_n(X,Y)$ has coefficients in $\mathbb{Z}$, and moreover it is *primitive*. Indeed, suppose on the contrary that a prime p divided all the coefficients. If n is a power of p, then p^2 divides all the coefficients of $(X+Y)^n - X^n - Y^n$, so by induction, $m^n \equiv m \pmod{p^2}$ for all positive integers m, a contradiction. If $n = p^\nu r$ with $(p,r) = 1$ and $r > 1$, then $p \nmid \binom{n}{p^\nu}$, contradiction.

Theorem 2.2.1 (Lazard)**.** *If F and G are formal groups over A such that $F \equiv G \pmod{\text{poly. deg. } n}$, then $F \equiv G + aC_n(X,Y) \pmod{\text{poly. deg. } n+1}$ for some $a \in A$.*

This is obvious for $n \leq 1$, so let us assume that $n \geq 2$. Let $h(X,Y)$ be the homogeneous polynomial of degree n such that $F - G \equiv h \pmod{\text{poly. deg. } n+1}$. Because F and G are formal groups, $h(X,Y) = h(Y,X)$, and $h(X,0) = h(0,X) = 0$. Letting $G_2(X,Y) = G(X,Y) - X - Y$ (i.e. the higher order terms), modulo polynomial degree $n+1$, we have

$$\begin{aligned} F(F(X,Y),Z)) &\equiv G(F(X,Y),Z) + h(F(X,Y),Z) \equiv F(X,Y) + Z + G_2(F(X,Y),Z) + h(X+Y,Z) \\ &\equiv G(X,Y) + h(X,Y) + Z + G_2(G(X,Y),Z) + h(X+Y,Z) \\ &\equiv G(G(X,Y),Z) + h(X,Y) + h(X+Y,Z). \end{aligned}$$

Similarly, $F(X,F(Y,Z)) = G(X,G(Y,Z)) + h(Y,Z) + h(X,Y+Z)$, so $h(X,Y) + h(X+Y,Z) = h(Y,Z) + h(X,Y+Z)$. Therefore, for the theorem, it suffices to prove

Proposition 2.2.2. *A homogeneous polynomial $h(X,Y)$ of degree n with coefficients in A such that $h(X,Y) = h(Y,X)$, $h(X,0) = h(0,X) = 0$, and $h(X,Y) + h(X+Y,Z) = h(Y,Z) + h(X,Y+Z)$, must be of the form $aC_n(X,Y)$ for some $a \in A$.*

Proof. We will first prove this when A is a field. Let $h(X,Y) = \sum a_i X^i Y^{n-i}$. Then the conditions put on h in this proposition are all linear in terms of a_i. Moreover, by primitivity of C_n, the coefficients for $C_n(X,Y)$ form a *nonzero* solution of these linear conditions, so it suffices to show that the space of (a_i) satisfying these linear conditions is a vector space of dimension at most 1 over A. By the first two equations, we know $a_0 = a_n = 0$ and $a_i = a_{n-i}$. Comparing the coefficients of $X^i Y^j Z^{n-i-j}$ in the third equation with $i > 0$ and $n-i-j > 0$, we obtain $a_{i+j}\binom{i+j}{j} = a_i\binom{n-i}{j}$. We note two special cases: when $i = 1$ and $j = k-1$ for some $1 \le k < n$, we get

$$a_k k = a_1 \binom{n-1}{k-1}, \tag{2.2}$$

and when $j = 1$ and $i = k$ for some $0 \le k < n-1$, we get

$$a_{k+1}(k+1) = a_k(n-k). \tag{2.3}$$

If the characteristic of A is zero, then (2.2) finishes the proof. So let us now assume that the characteristic of R is p. If $n = p$ or $(n,p) = 1$, then for all $1 \le k \le n-1$, we have $ka_k = \binom{n-1}{k-1}a_1$ and $(n-k)a_k = \binom{n-1}{n-k-1}$, so we are done in this case as well. So we are now left with the case $n = mp$ with $m > 1$; we prove this by induction. Note that in this case, if $p|k$, then $n-k = 0$ and $k+1$ is invertible, so (2.3) shows $a_{k+1} = 0$. Similarly, if $a_k = 0$ and $p \nmid (k+1)$, then $a_{k+1} = 0$. Combined with $a_{n-k} = a_k$, we conclude that $a_k = 0$ for all $(k,p) = 1$, so $h(X,Y) = h'(X^p, Y^p)$. Then $h'(X,Y)$ must satisfy the conditions of the proposition. Hence, $h'(X,Y) = aC_m(X,Y)$ by induction, so it now suffices to check the following to finish the case of R being a field.

Claim. *When A is a field of characteristic p, $C_m(X^p, Y^p) = bC_n(X,Y)$ for some $b \in A$.*

Proof. If m is not a power of p, then $C_m = u \cdot ((X+Y)^m - X^m - Y^m)$ with $u \in A$ a unit. Then $uC_n(X,Y) = u((X+Y)^n - X^n - Y^n) = u\Big(\big((X+Y)^p\big)^m - X^n - Y^n\Big) = C_m(X^p, Y^p)$. If m is a power of p, working over $\mathbb{Z}$, we have

$$\begin{aligned} pC_m(X^p,Y^p) &= (X^p+Y^p)^m - X^n - Y^n = ((X+Y)^p - pC_p(X,Y))^m - X^n - Y^n \\ &= pC_n(X,Y) + \sum_{i=1}^{m} \binom{m}{i}(-1)^i p^i (C_p(X,Y))^i (X+Y)^{p(m-i)}, \end{aligned}$$

where each term inside the summation has coefficient divisible by p^2. Thus, dividing the above formula, $C_m(X^p, Y^p) \equiv C_n(X,Y) \pmod{p}$. □

Amazingly, the above case for a field is really all the content of this theorem. The important observation is that the three conditions that are put on $h(X,Y)$ and the final conclusion that we draw about $h(X,Y)$ only use the *additive* structure of A, and not the ring structure. So we can completely forget about the ring structure. Since $h(X,Y)$ has a finite number of coefficients, it suffices to show the proposition for a finitely generated abelian group. If h has coefficients in $A_1 \oplus A_2$ and satisfies these three conditions, these three conditions are satisfied for each component A_i. So by the structure theorem for finitely-generated abelian groups, it suffices to check the proposition for $A = \mathbb{Z}$ and $A = \mathbb{Z}/p^\nu$.

Suppose $A = \mathbb{Z}$. By above, $h(X,Y) = aC_n(X,Y)$ for $a \in \mathbb{Q}$, but by primitivity of C_n, $a \in \mathbb{Z}$.

Now suppose that $A = \mathbb{Z}/p^\nu$. The $\nu = 1$ case is a field, so we will prove this by induction. Taking lifts to $\mathbb{Z}$, what we need is $h(X,Y) \equiv aC_n(X,Y) \pmod{p^{\nu+1}}$ for some $a \in \mathbb{Z}$, given that h satisfies the three conditions modulo $p^{\nu+1}$. By the inductive hypothesis, we can write $h(X,Y) \equiv aC_n(X,Y) + p^\nu h_1(X,Y) \pmod{p^{\nu+1}}$ for some h_1 with coefficients in $\mathbb{Z}$. Then $h_1(X,Y)$ must satisfy the three conditions modulo p, so $h_1(X,Y) \equiv a_1 C_n(X,Y) \pmod{p}$ for some $a_1 \in \mathbb{Z}$. Hence, $h(X,Y) \equiv (a + p^\nu a_1)C_n(X,Y) \pmod{p^{\nu+1}}$. □

Before proving a theorem characterizing formal groups isomorphic to the additive group, we need a preliminary lemma.

Lemma 2.2.3. *If F, G are formal groups and $F(X,Y) \equiv G(X,Y) + aC_n(X,Y)$ (mod poly. deg. $n+1$), then for any natural number m, we have*

$$[m]_F(X) \equiv [m]_G(X) + \frac{m^n - m}{\epsilon(n)} aX^n \pmod{\text{poly. deg. } n+1}.$$

Proof. By induction, we can show that $[m]_F(X)$ and $[m]_G(X)$ both start out with mX. When $m = 1$, $[m]_F = [m]_G = X$, so assume that we have proven the lemma for m. Working modulo polynomial degree $n+1$,

$$\begin{aligned}
[m+1]_F(X) = F([m]_F(X), X) &\equiv G\left([m]_G(X) + \frac{m^n - m}{\epsilon(n)} aX^n, X\right) + aC_n([m]_F(X), X) \\
&= G([m]_G(X), X) + \frac{m^n - m}{\epsilon(n)} aX^n + aC_n(mX, X) \\
&= [m+1]_G(X) + \frac{m^n - m}{\epsilon(n)} aX^n + \frac{1}{\epsilon(n)} a((m+1)^n - m^n - 1)X^n \\
&= [m+1]_G(X) + \frac{(m+1)^n - (m+1)}{\epsilon(n)} aX^n.
\end{aligned}$$

□

Theorem 2.2.4. *A formal group F over A is isomorphic to the additive group if and only if for all primes p, $[p]_F(X)$ has coefficients in pA.*

Proof. If $\alpha : F \to G$ is an isomorphism of formal groups, then $[m]_F = \alpha^{-1} \circ [m]_G \circ \alpha$ by induction, so in particular, $[p]_{\widehat{\mathbb{G}}_a} = pX$ shows the necessity.

For sufficiency, we use the method of successive approximations. Specifically, we will successively construct $\circ$-invertible power series β_n such that

$$\beta_{n-1} \equiv \beta_n \pmod{\text{poly. deg. } n}, \quad \text{and} \quad \beta_n \circ F \circ \beta_n^{-1} \equiv X + Y \pmod{\text{poly. deg. } n+1}.$$

Start with $\beta_1 = X$. Suppose that we have constructed up to β_{n-1}. By Example 2.1.10, we know that $H = \beta_{n-1} \circ F \circ {\beta_{n-1}}^{-1}$ is a formal group with β_{n-1} a formal group isomorphism from F to H, satisfying $H \equiv X + Y$ (mod poly. deg. n). By composing with β_{n-1}, it suffices to find a power series $\alpha \in A[\![X]\!]$ such that $\alpha \equiv X$ (mod poly. deg. n) and $\alpha \circ H \circ \alpha^{-1} \equiv X + Y$ (mod poly. deg. $n+1$). By Lazard's Theorem, $H \equiv X + Y + aC_n(X,Y)$ (mod poly. deg. $n+1$) for some $a \in A$. Note that when n is a power of a prime p, Lemma 2.2.3 shows $[p]_H(X) \equiv pX + (p^{n-1} - 1)aX^n$ (mod poly. deg. $n+1$). The first paragraph shows $[p]_H(X) \in (pA)[\![X]\!]$, so in particular, $a = pa'$ for some $a' \in A$.

Hence (including the case when n is not a power of a prime), $H \equiv X + Y + a'\left((X+Y)^n - X^n - Y^n\right)$ (mod poly. deg. $n+1$). Then $\alpha = X - a'X^n$ works by Example 2.1.10. □

Corollary 2.2.5. *Suppose F is a formal group over A.*
(1) *If A is a $\mathbb{Q}$-algebra (e.g. a field of characteristic zero), F is isomorphic to $\widehat{\mathbb{G}}_a$.*
(2) *If $pA = 0$ for some prime p, F is isomorphic to $\widehat{\mathbb{G}}_a$ if and only if $[p]_F$ is identically equal to zero.*
(3) *If A is a local ring with residue field characteristic p, F is isomorphic to $\widehat{\mathbb{G}}_a$ if and only if $[p]_F(X)$ has coefficients in pA.*

Proof. (1) follows from the fact that every p is a unit of A. The necessities of (2) and (3) are clear, and for sufficiency, note that a prime $\ell \neq p$ is a unit in A. □

These results are useful even in the analysis of formal R-modules, since knowing that a formal R-module is isomorphic as a formal group to the additive formal group severely limits the potential actions of R (cf the proof of Theorem 3.2.1).

2.3 Generalized Formal R-Modules

It turns out that we can generalize the notion of formal R-modules to something that does not arise from power series. For Section 4.3 *only*, we will need this more general version, so we will cover the basic definitions and results of formal R-modules in this general sense to clarify the proofs later. This section assumes knowledge of profinite modules and commutative formal group schemes, as discussed in Appendix A, and we will also be using the same notations.

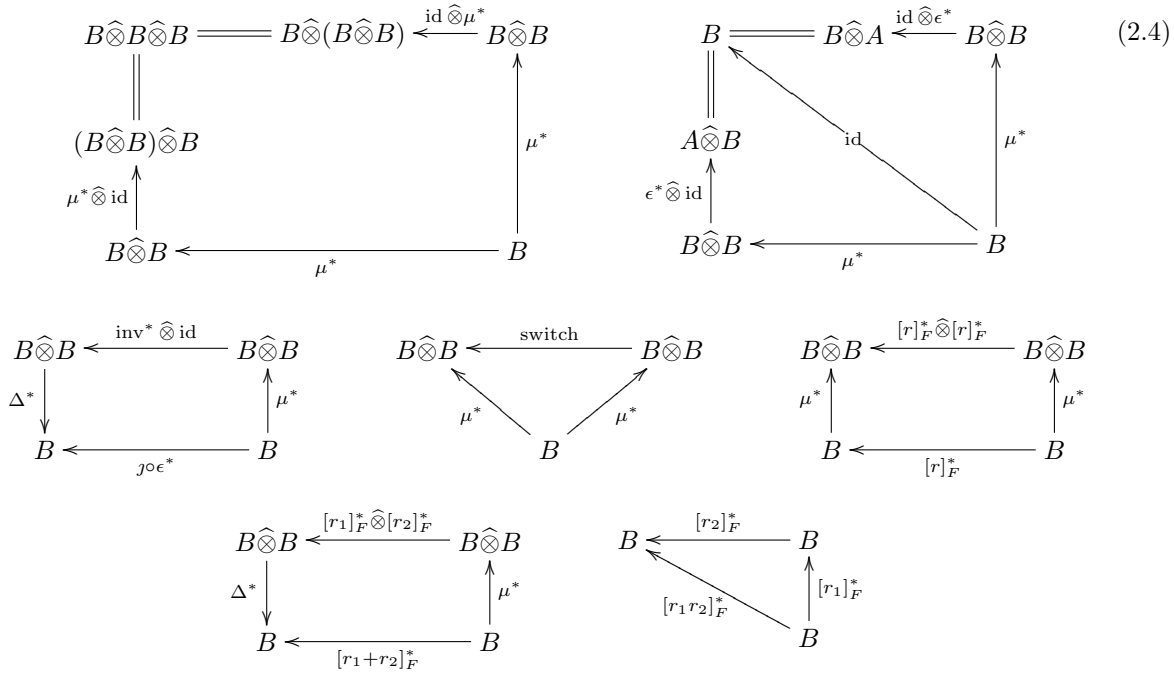
Throughout this section, we let A be a pseudocompact *local* ring with maximal ideal $\mathfrak{m}$. For example, A can be a complete noetherian local ring. We consider the category of formal schemes over A, i.e. those of the form $\mathrm{Spf}_A(B)$ for some $B \in \mathcal{PA}_A$. It is tempting to define a formal R-module over A to be an R-module object in this category. But recalling that commutative formal group schemes over A are defined to be topologically flat over A to obtain a well-behaved concept of short exact sequences (see Section A.3), we will define formal R-modules as follows.

Definition 2.3.1. A formal scheme $F = \mathrm{Spf}_A(B)$ over A is said to be a *formal R-module over A* if it is an R-module object in the category of formal schemes over A and if B is topologically flat over A. We will denote $B = \mathscr{O}(F)$. A map $F_1 \longrightarrow F_2$ between two formal R-modules is said to be an *R-module homomorphism* if it is an R-module object homomorphism.

When a terminology that can be applied to a profinite A-module or a profinite A-algebra is applied to a formal R-module F, we mean that the underlying ring $\mathscr{O}(F)$ satisfies the terminology over A. For example, we will talk about formally étale formal R-modules or topologically faithfully flat formal R-modules.

Although it is often better in algebraic geometry to state everything in terms of geometry and not in terms of its underlying rings, in this thesis we will usually have to be working directly with underlying rings of formal R-modules. There are several reasons for this. First, the easiest way to establish that the formal R-modules defined in Section 2.1 are formal R-modules as defined in this section, is via the underlying rings (Proposition 2.3.2). Second, most of the constructions we do in this section and Section 4.3.4 will be directly from the rings, though sometimes motivated by geometry.

Therefore, as a reference, we will now list various properties of formal R-modules in terms of underlying rings. First, $F = \mathrm{Spf}_A(B)$ with B topologically flat over A is a formal R-module if and only if there exist continuous A-algebra maps $\mu^*, \epsilon^*, \mathrm{inv}^*$ and $[r]_F^*$ for each $r \in R$ such that $[1]_F = \mathrm{id}$ on B and the following diagrams commute:



(2.4)

(where Δ^* is the diagonal map, $\jmath$ is the unique map $A \to B$, and 'switch' switches the two components).

Secondly, a map $\alpha : F_1 = \mathrm{Spf}_A(B_1) \longrightarrow F_2 = \mathrm{Spf}_A(B_2)$ between formal R-modules is an R-module homomorphism if and only if α^* is a continuous A-algebra map which makes

$$\begin{array}{ccc} B_1 \widehat{\otimes} B_1 & \xleftarrow{\alpha^* \widehat{\otimes} \alpha^*} & B_2 \widehat{\otimes} B_2 \\ {\scriptstyle \mu_1^*}\uparrow & & \uparrow{\scriptstyle \mu_2^*} \\ B_1 & \xleftarrow[\alpha^*]{} & B_2 \end{array} \qquad \begin{array}{ccc} B_1 & \xleftarrow{\alpha^*} & B_2 \\ {\scriptstyle [r]^*_{F_1}}\uparrow & & \uparrow{\scriptstyle [r]^*_{F_2}} \\ B_1 & \xleftarrow[\alpha^*]{} & B_2 \end{array} \tag{2.5}$$

commute for all $r \in R$. For example, $F_1 \xrightarrow{\jmath_{F_1}} \mathrm{Spf}_A(A) \xrightarrow{\epsilon_{F_2}} F_2$ is an R-module homomorphism, called the zero map. The set of all R-module homomorphisms is denoted by $\mathrm{Hom}_R(F_1, F_2)$, and the set of all homomorphisms of the underlying commutative formal group schemes (i.e. having the commutativity of the first diagram of (2.5)) will be denoted $\mathrm{Hom}_{\mathbb{Z}}(F_1, F_2)$ (and similarly with End). In contrast, the set of all formal *scheme* maps from F_1 to F_2 (i.e. no commutativity of diagram) will be denoted by $\mathrm{Mor}_A(F_1, F_2)$.

Finally, for a formal R-module F over A and a formal scheme T over A, the evaluation $F(T) = \mathrm{Mor}_A(T, F)$ is an R-module, with the actions given by

$$\varphi_1 \underset{F(T)}{+} \varphi_2 : \mathscr{O}(F) \xrightarrow{\mu^*} \mathscr{O}(F) \widehat{\otimes}_A \mathscr{O}(F) \xrightarrow{\varphi_1 \widehat{\otimes} \varphi_2} \mathscr{O}(T) \widehat{\otimes}_A \mathscr{O}(T) \xrightarrow{\Delta^*} \mathscr{O}(T) \tag{2.6}$$

$$r \cdot \varphi : \mathscr{O}(F) \xrightarrow{[r]^*_F} \mathscr{O}(F) \xrightarrow{\varphi} \mathscr{O}(T). \tag{2.7}$$

Now we are ready to discuss some examples. First, we will show that this new definition of formal R-module does include the formal R-modules that we have been dealing with so far.

Proposition 2.3.2. *Let A be a complete noetherian local ring. If $(F, [\ ])$ is a formal R-module over A in the sense of Definition* 2.1.8*, then it is a formal R-module. Its underlying formal scheme is* $\mathrm{Spf}_A(A[\![T]\!])$*, and the evaluation* $\mathrm{Spf}_A(A[\![T]\!])(A)$ *is isomorphic to $F(\mathfrak{m}_A)$ as R-modules.*

Proof. $A[\![T]\!]$ is clearly topologically free over A. Let us define $\mathcal{PA}_A$-maps $\mu^* : A[\![T]\!] \to A[\![T]\!] \widehat{\otimes}_A A[\![T]\!] \cong A[\![X, Y]\!]$ by $T \mapsto F(X, Y)$, $[r]^* : A[\![T]\!] \to A[\![X]\!]$ by $T \mapsto [r](X)$, $\mathrm{inv}^* : A[\![T]\!] \to A[\![X]\!]$ by $T \mapsto g(X)$ where $g(X)$ is the unique power series with the property $F(X, g(X)) = 0$, and $\epsilon^* : A[\![T]\!] \to A$ by $T \mapsto 0$. The conditions required on $F(X, Y)$, $g(X)$, and $[r](T)$ by the definition of formal R-module are exactly what we need for the commutativity of the seven diagrams in (2.4). For the last statement, note that $\mathrm{Spf}_A(A[\![T]\!])(A)$ is in one-to-one correspondence with elements of $\mathfrak{m}$, so using (2.6), we are done. □

We call a formal R-module F **connected** if $\mathscr{O}(F)$ is local. Thus, the example above is a connected formal R-module. It turns out that a formal R-module over a complete noetherian local ring which is one-dimensional, connected, and formally smooth always has the form discussed in Proposition 2.3.2 ([3, Theorem 2.3.5]). Since we will never discuss anything which is not one-dimensional, we will refer to formal R-modules of the form in Proposition 2.3.2 as **CFS** (connected formally smooth) **formal R-modules** in this section and Section 4.3.

We will now go back to a more general pseudocompact local ring A, and discuss examples of formal R-modules that we have not seen.

Proposition 2.3.3. *For any R-module S, we can define a formal R-module structure on $F = \mathrm{Spf}_A(A^S)$, where A^S is the direct product of S copies of A with the product topology. This formal R-module is formally étale. $F(A)$ is canonically isomorphic to S as R-modules, and for any formal R-module H, there is a one-to-one correspondence via the evaluation at A between the set of all formal R-module homomorphisms $F \to H$ and the set of all R-module homomorphisms $S \to H(A)$.*

Proof. Intuitively speaking, F is the 'disjoint union' of S copies of 'a single point' $\mathrm{Spf}_A(A)$ with the formal R-module structure defined directly from the R-module structure of S, so all the statements in this proposition are certainly reasonable.

More precisely, by viewing an element of $B = A^S$ as a set map $S \to A$ and an element of $B\widehat{\otimes}_A B$ as a set map $S \times S \to A$, we can define $(\mu^*(b))(s,s') = b(s+s')$, $\epsilon^*(b)(s) = b(0)$, $(\mathrm{inv}^*(b))(s) = b(-s)$, and $([r]^*(b))(s) = b(rs)$. Since B is topologically free over A, we conclude that F is a formal R-module by checking (2.4). Theorem A.4.1 immediately tells us that this is étale.

Note that $\mathrm{Spf}_A(A^S)(A) = \coprod \mathrm{Spf}_A(A)(A)$ by the same proof used in obtaining (A.2), so we now know that every element of $\mathrm{Spf}_A(A^S)(A)$ is a projection onto the value of $b \in B$ at s for some $s \in S$. Using (2.6), we can check that $\mathrm{Spf}_A(B)(A) \cong S$ as R-modules.

Now we show the last statement. A map $\alpha : F \longrightarrow H$ of formal schemes over A corresponds to a continuous A-algebra map $\alpha^* : \mathscr{O}(H) \longrightarrow A^S$, which in turn corresponds to a family of continuous A-algebra maps $\alpha_s^* : \mathscr{O}(H) \longrightarrow A$ for all $s \in S$. Thus, α corresponds to a (set-theoretic) map $S \to H(A)$. Because of the way we defined the formal R-module structure on F, we can check using (2.5) and (2.6) that α is a formal R-module homomorphism if and only if the corresponding $S \to H(A)$ is an R-module homomorphism. □

Because $\mathrm{Spf}_A(A^S)$ can be thought of as a 'disjoint union of a single point', it is far from the connected formally smooth case that we have been dealing with previously. In fact, connected and étale formal R-modules can be considered as 'opposite extremes.' More precisely,

Proposition 2.3.4. *If $\mathrm{Spf}_A(B)$ is a connected formal R-module, then $B^{\text{ét}} = A$, identified via the algebra structure map. If $\mathrm{Spf}_A(B)$ is a connected formal R-module and $\mathrm{Spf}_A(B')$ is an étale formal R-module, then there are no non-trivial formal R-module homomorphisms from $\mathrm{Spf}_A(B)$ to $\mathrm{Spf}_A(B')$.*

Proof. By Theorem A.4.1, A is a formally étale closed subalgebra of B, so it is contained in $B^{\text{ét}}$. On the other hand, $B^{\text{ét}}\widehat{\otimes}_A(A/\mathfrak{m}) = (B\widehat{\otimes}_A(A/\mathfrak{m}))^{\text{ét}} \hookrightarrow B\widehat{\otimes}_A(A/\mathfrak{m}) \cong B/\overline{\mathfrak{m}B}$. Since B is local and $B^{\text{ét}}\widehat{\otimes}_A(A/\mathfrak{m})$ is a product of finite separable extensions of $A/\mathfrak{m}$, $B^{\text{ét}}\widehat{\otimes}_A(A/\mathfrak{m})$ is a field extension of $A/\mathfrak{m}$. But $B^{\text{ét}}\widehat{\otimes}_A(A/\mathfrak{m}) \to B/\overline{\mathfrak{m}B} \to A/\mathfrak{m}$ via the identity section, so $B^{\text{ét}}\widehat{\otimes}_A(A/\mathfrak{m}) \cong A/\mathfrak{m}$. By Nakayama's lemma, $B^{\text{ét}} = A$.

For the second statement, note that $B \leftarrow B'$ factors through $B^{\text{ét}} = A$ since B' is étale (see Section A.4). But since $\mathrm{Spf}_A(B) \to \mathrm{Spf}_A(B')$ sends the identity section to the identity section, it must factor through the identity section of B'. □

In Section 4.3, both connected and étale formal R-modules will be important. Indeed, the main objects of study in Section 4.3 are formal R-modules which can be constructed by 'combining' these two extremes of formal R-modules. This combination process is achieved through the use of short exact sequences of formal R-modules, so for the rest of this section, we will discuss some properties of short exact sequences of formal R-modules. We define

Definition 2.3.5. A sequence of formal R-modules and R-module homomorphisms $0 \to F' \to F \to F'' \to 0$ is said to be a *short exact sequence* if the underlying commutative formal group schemes form a short exact sequence.

From Appendix A.3, this means that (as commutative formal group schemes) $F' \to F$ is a closed immersion, $F \to F''$ is topologically faithfully flat, $F' \longrightarrow F''$ vanishes, and we can identify F' as the kernel of $F \to F''$. Thus, applying a continuous (i.e. local) base change to a short exact sequence of formal R-modules results in a short exact sequence.

To justify this definition, we want to be able to complete to a short exact sequence given either a closed immersion $F' \hookrightarrow F$ or topologically faithfully flat map $F \twoheadrightarrow F''$ of formal R-modules. In the first case, note that the construction of the quotient discussed in Section A.3 creates a formal R-module if we start with formal R-modules, because the duality process is functorial. We then get a short exact sequence $0 \to F' \to F \to F'' \to 0$. In the second case, the kernel $F' = F \times_{F''} \mathrm{Spf}_A(A)$ has a natural formal R-module structure coming from F, and we then get a short exact sequence of formal R-modules $0 \to F' \to F \to F'' \to 0$.

As discussed in Section A.3, this definition of short exactness is equivalent to requiring $F' \longrightarrow F''$ to vanish and the sequence to form a short exact sequence over the closed fiber $A/\mathfrak{m}$. In particular, if we construct a map over general A in a manner compatible with base change, monomorphisms and epimorphisms can be checked over the closed fiber. Since commutative formal group schemes over a field form an abelian category by Theorem A.3.2, this definition often allows us to reduce many statements of short exactness to the case over an abelian category. We will use this technique repeatedly in the following discussion.

The notion of short exact sequences of formal R-modules has properties that we expect short exact sequences to have; we will prove these properties in the process of proving the next proposition. Before stating it, we need to introduce the notion of extensions in this setting. Fix two formal R-modules F', F'' over A. Let $\mathscr{E}xt_{R,A}(F'', F')$ denote the set of short exact sequences

$$0 \to F' \to F \to F'' \to 0$$

of formal R-modules over A modulo the equivalence which identifies extensions fitting into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F' & \longrightarrow & F_1 & \longrightarrow & F'' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \alpha} & & \| & & \\ 0 & \longrightarrow & F' & \longrightarrow & F_2 & \longrightarrow & F'' & \longrightarrow & 0 \end{array}$$

where α is a formal R-module homomorphism. As in the case of modules, α must then be a formal R-module *isomorphism*, since over the closed fiber we have an abelian category (so the five lemma holds). In particular, we have defined an equivalence relation. Note that we have a well-defined base change map of sets $\mathscr{E}xt_{R,A}(F'', F') \longrightarrow \mathscr{E}xt_{R,\widetilde{A}}(\widetilde{F}'', \widetilde{F}')$.

We are now ready to prove

Proposition 2.3.6. *$\mathscr{E}xt_{R,A}(F'', F')$ is a group in a manner compatible with base change on A (by the 'same' operations as in the case of R-modules).*

Proof. Recall that we can define the group structure on extensions of objects in abelian categories by a process called Yoneda Ext ([4], [6]). This agrees with the usual homological method in the case of modules ([15, page 353]), and it has the advantage of not requiring projectives and injectives. Unfortunately, we cannot quote this result in the present setting, as formal R-modules over A do not form an abelian category. But we will be able to prove the proposition by the technique of reduction to the closed fiber, where we *do* have an abelian category. Essentially, we will make all the requisite constructions by category-theoretic methods, then check that these constructions create formal R-modules and formal R-module homomorphisms, and finally use base change compatibility of our constructions to reduce to checking the necessary properties over the closed fiber. For notational shorthand, we will write $F' \hookrightarrow F \twoheadrightarrow F''$ for a short exact sequence.

There are three main constructions in the definition of the addition on $\mathscr{E}xt_{R,A}$: taking products, pull-back, and push-out. We will now discuss how each of them adapts the Yoneda Ext construction in an abelian category to the present setting.

(1) Taking the product of two exact sequences $F' \hookrightarrow F_i \twoheadrightarrow F''$: then the product diagram

$$0 \to F' \times F' \to F_1 \times F_2 \to F'' \times F'' \to 0$$

is a diagram of formal R-modules with the composite of the two maps zero, and this construction is compatible with base change. Thus, short exactness may be checked on the closed fiber, where the usual abelian category argument works.

(2) Pull-back: suppose $F' \hookrightarrow F \twoheadrightarrow F''$ is short exact and $G'' \to F''$ is a formal R-module map. Consider $F \times_{F''} G''$. This is topologically flat over A, as $F \to F''$ and $G'' \to \mathrm{Spf}_A(A)$ are topologically flat, so it is a formal R-module. The maps $F' \to F$ and $F' \to \mathrm{Spf}_A(A) \xrightarrow{\epsilon} G''$ induce $F' \to F \times_{F''} G''$, which is a formal R-module homomorphism. So we have a sequence of formal R-modules $F' \to F \times_{F''} G'' \to G''$. Since the composite of the two maps is zero and this construction is compatible with base change, we can again reduce to checking over the closed fiber.

(3) Push-out: suppose $F' \hookrightarrow F \twoheadrightarrow F''$ is short exact and $F' \to G'$ is a formal R-module map. Since $F' \to G' \times F$ is a closed immersion of formal R-modules, let $G' \times^{F'} F$ be the quotient formal R-module. Since $F' \to G' \times F \to F \to F''$ is zero, $G' \times^{F'} F \to F''$ is a well-defined formal R-module homomorphism. Thus, we have a sequence of formal R-modules $G' \to G' \times^{F'} F \to F''$ whose composite is zero, and this construction is compatible with base change. Similarly, as above, we are done by the usual abelian category argument.

Note that all three constructions send equivalent extensions to equivalent extensions. Further, the operations of pull-back and push-out make $\mathscr{E}xt_{R,A}$ a bifunctor: if $\mathscr{F} \in \mathscr{E}xt_{R,A}(F'', F')$ represents $F' \to F \to F''$ and $\alpha' : F' \to G'$ and $\alpha'' : G'' \to F''$ are formal R-module homomorphisms, then $(\alpha')_* \circ (\alpha'')^*(\mathscr{F})$ is represented by

$$G' \hookrightarrow \Big(\big((F \times_{F''} G'') \times G'\big)/(\text{image of } F')\Big) \twoheadrightarrow G''$$

and $(\alpha'')^* \circ (\alpha')_*(\mathscr{F})$ is represented by

$$G' \hookrightarrow \Big(\big(F \times G'/\text{image of } F'\big) \times_{F''} G''\Big) \twoheadrightarrow G'',$$

so we have a map of formal R-module from the first to the second making the diagram commute.

Now given two sequences $F' \hookrightarrow F_i \twoheadrightarrow F''$, we can define their sum to be the element

$$(\Delta_{F''})^* \circ (\nabla_{F'})_*(F' \times F' \to F_1 \times F_2 \to F'' \times F'') = (\nabla_{F'})_* \circ (\Delta_{F''})^*(F' \times F' \to F_1 \times F_2 \to F'' \times F'')$$

in $\mathscr{E}xt_{R,A}$, where $\Delta_{F''} : F'' \to F'' \times F''$ is the diagonal and $\nabla_{F'} : F' \times F' \to F'$ corresponds to the addition of the formal R-module F'. To check that this defines a group structure with the split extension class as the identity, we can just follow [4]: to check for associativity and existence of inverses, we need to define certain formal R-modules and homomorphisms using bifunctoriality and coproducts and products. Once we do this in a manner compatible with base change, checking that these constructions really work reduces to checking it over the closed fiber, where we have an abelian category, so the arguments in [4] go through. □

We will prove one more general property of a short exact sequence:

Proposition 2.3.7. *If $0 \to F' \to F \to F'' \to 0$ is an exact sequence of formal R-modules over A, then for any formal scheme X over A, the evaluation at X results in an exact sequence $0 \to F'(X) \to F(X) \to F''(X)$ as R-modules.*

Proof. By definition of short exact sequence, the injectivity of $F'(X) \to F(X)$ and vanishing of $F'(X) \to F''(X)$ follow. If $\varphi : X \to F$ is such that $X \to F \to F''$ factors through the identity section, then we have a well-defined map of formal schemes $X \to F \times_{F''} \mathrm{Spf}_A(A) \cong F'$. □

For the rest of this section, we will briefly discuss an important class of short exact sequences, called the connected-étale sequences. [3] covers this for finite flat group schemes but does not explicitly cover it for formal group schemes. Since we need a corresponding result for the formal R-*modules*, we will construct and prove fundamental properties about this sequence.

Suppose that $F = \mathrm{Spf}_A(B)$ is a formal R-module over A. Since $B^{\text{ét}} \hookrightarrow B$ is topologically faithfully flat and B is topologically flat over A, $B^{\text{ét}}$ is topologically flat over A. Note that the restriction of μ^* to $B^{\text{ét}}$ factors through $(B\widehat{\otimes}_A B)^{\text{ét}} = B^{\text{ét}}\widehat{\otimes}_A B^{\text{ét}}$ (see Appendix A.4). Similarly, the structure map, the identity section, the inverse, and $[r]_F^*$ for all $r \in R$ all factor through $B^{\text{ét}}$, so we can canonically put a formal R-module structure on $B^{\text{ét}}$ in a way so that $\mathrm{Spf}_A(B) \to \mathrm{Spf}_A(B^{\text{ét}})$ is a topologically faithfully flat formal R-module homomorphism. We can now complete the exact sequence of formal R-modules by taking the kernel F^0.

We will show that F^0 is connected, i.e. $B^0 = \mathscr{O}(F^0)$ is local. It certainly suffices to show locality after base changing to the algebraic closure of $A/\mathfrak{m}$, so we assume that everything is over an algebraically closed field k. We write $B = \prod B_{\mathfrak{n}}$ over all open maximals, and using Theorem A.4.1 and locality of $B_{\mathfrak{n}}$, $B^{\text{ét}} = \prod k$ indexed by open maximals of B. Thus $B^0 \cong B\widehat{\otimes}_{\prod k} k \cong B_{\mathfrak{n}_0}$, where $\mathfrak{n}_0$ is the unique component which is not killed by the identity section $\prod k \to k$. Hence F^0 is connected, and we have constructed an exact sequence of formal R-modules called the **connected-étale sequence** $0 \to \mathrm{Spf}_A(B^0) \to \mathrm{Spf}_A(B) \to \mathrm{Spf}_A(B^{\text{ét}}) \to 0$ of the formal R-module $\mathrm{Spf}_A(B)$. We call $\mathrm{Spf}_A(B^0)$ and $\mathrm{Spf}_A(B^{\text{ét}})$ the **connected component** and the **étale component**, respectively. In view of Proposition 2.3.4, we are 'decomposing' a formal R-module into two opposite extremes.

Since the construction of the maximal étale subalgebra is compatible with local base change and taking products, the connected-étale sequence is compatible with local base change and taking products. The following will be used in Section 4.3

Proposition 2.3.8. *Suppose $A = k$ is an algebraically closed field. Then for a formal R-module G over k, the connected-étale sequence splits. Further, there are no non-trivial homomorphisms from an étale formal R-module to a connected formal R-module. Thus the connected-étale sequence splits uniquely (in a manner compatible with base change and taking products).*

Proof. Let $G = \mathrm{Spf}_k(B)$, and let τ be the set of topological nilpotents of B. As discussed in Appendix A.1, $B/\tau \cong \prod B_{\mathfrak{n}}/\mathfrak{n}B_{\mathfrak{n}}$. $\bar{k} = k$ implies $B_{\mathfrak{n}}/\mathfrak{n}B_{\mathfrak{n}} \cong k$, and so $(B/\tau)\widehat{\otimes}_k(B/\tau) \cong \prod k$ have no topological nilpotents. Thus, $B \to B\widehat{\otimes}_k B \to (B/\tau)\widehat{\otimes}_k(B/\tau)$ factors through B/τ. Similarly, $\mathrm{inv}^*, \epsilon^*, [r]^*_G$ can be defined on B/τ, so $\mathrm{Spf}_k(B/\tau)$ is a formal R-module. Since $B_{\mathfrak{n}}$ is local and $\bar{k} = k$, Theorem A.4.1 shows ${B_{\mathfrak{n}}}^{\text{ét}} \cong k$. Thus, ${B_{\mathfrak{n}}}^{\text{ét}} \hookrightarrow B_{\mathfrak{n}} \to B_{\mathfrak{n}}/\mathfrak{n}B_{\mathfrak{n}}$ is an isomorphism. Taking products, $B^{\text{ét}} \hookrightarrow B \to B/\tau$ is an isomorphism, inducing an isomorphism of formal R-modules. This gives the splitting.

For the second statement, on the level of rings, it suffices to check that there is only one $\mathcal{PA}_k$ map from a local B' to an étale B''. But by Theorem A.4.1 and $\bar{k} = k$, $B'' = \prod k$, so it now suffices to show that there is only one $\mathcal{PA}_k$ map from $B' \to k$. But any such $B' \to k$ factors through $B'/\mathfrak{m}_{B'} \cong k$, so we are done. If we have two splittings, i.e. two formal R-module sections $\mathrm{Spf}_k B^{\text{ét}} \to \mathrm{Spf}_k(B)$, then taking the 'difference' of the sections, we get a formal R-module homomorphism from an étale formal R-module to a connected one. □

Chapter 3

Formal R-Modules for Various R

Our goal in this chapter is to determine the possibilities of formal R-modules when R is the valuation ring of a local field. This lies at the foundation of the deformation theory of Chapter 4.

Our main technique will be the use of universal objects. Because any object can be viewed as the image of the universal object (if such a thing exists), the universal object often contains useful information about 'all' objects simultaneously. Thus, determination of the universal object and its properties is extremely important. As an example from this chapter, knowledge of the universal formal R-module allows us to systematically construct formal R-modules of a given height. The use of universal objects continues into Chapter 4.

In Section 3.1, as a starting point, we will talk in general about universal formal R-modules. We will recall the definition of universal objects, and discuss properties of universal formal R-modules that hold for any R. We will see that the ring Λ_R over which the universal formal R-module is defined turns out to be a quotient of a polynomial ring, having a natural gradation.

In Section 3.2, we prove that for an infinite field R, Λ_R is simply $R[\Omega_1, \Omega_2, \ldots]$ where each Ω_i has degree i in Λ_R.

In Section 3.3, we discuss many specific properties of formal R-modules when R is the valuation ring of a local field. These will be important, as Chapter 4 is entirely on formal modules with this R. We will show that Λ_R is again the polynomial ring $R[\Upsilon_1, \Upsilon_2, \ldots]$ with $\deg \Upsilon_i = i$ in Λ_R, using the result from Section 3.2. Moreover, we will characterize formal R-modules which are isomorphic to the additive module $\widehat{\mathcal{G}}_{\mathrm{a}}$ (an analogue of Theorem 2.2.4). Furthermore, we will show an extremely useful formula, which tells us the degree n part of $F - G$ given $(F, [\ ]_F) \equiv (G, [\ ]_G)$ (mod poly. deg. n). This formula enables us to successively approximate differences of formal R-modules, going up one polynomial degree at a time. Finally, subsection 3.3.1 deals with the case of formal R-modules over a separably closed field of characteristic p. This case turns out to be particularly nice, as the height of a formal R-module determines the isomorphism class. This fact will be essential in Chapter 4.

3.1 Universal Formal R-Modules

In this section, we will discuss properties of universal formal R-modules which hold for any R. This sets up the stage for the rest of this chapter.

Let us first recall the notion of a universal and representing object, since we will need this concept throughout this thesis (cf. [20]). A covariant representable functor is a covariant functor $\mathscr{F} : \mathscr{C} \to \mathbf{Set}$ such that there exist $C^{\mathrm{univ}} \in \mathscr{C}$ and a set map $\phi_C : \hom_{\mathscr{C}}(C^{\mathrm{univ}}, C) \xrightarrow{\cong} \mathscr{F}(C))$ for each $C \in \mathscr{C}$ making the

diagram

$$\begin{array}{ccc} \hom_{\mathscr{C}}(C^{\mathrm{univ}}, C_1) & \xrightarrow{\phi_{C_1}} & \mathscr{F}(C_1) \\ \downarrow & & \downarrow \\ \hom_{\mathscr{C}}(C^{\mathrm{univ}}, C_2) & \xrightarrow[\phi_{C_2}]{} & \mathscr{F}(C_2) \end{array}$$

commutative (i.e. the functor $\mathscr{F}$ is naturally isomorphic to the Hom functor). For such a functor, $(C^{\mathrm{univ}}, \phi)$ is called a **representing object**. The same concept, put in a different language, is the notion of the universal element. We call (C^{univ}, u) an **universal object** of $\mathscr{F}$ if for any $C \in \mathscr{C}$ and $x \in \mathscr{F}(C)$, there exists a unique map $f \in \hom_{\mathscr{C}}(C^{\mathrm{univ}}, C)$ such that $\mathscr{F}(f)(u) = x$. For a fixed C^{univ}, there is a bijection between representing objects $(C^{\mathrm{univ}}, \phi)$ and universal elements (C^{univ}, u), given by $u = \phi_{C^{\mathrm{univ}}}(\mathrm{id}_{C^{\mathrm{univ}}})$ and $\phi_C(f) = \mathscr{F}(f)(u)$. And if $(C^{\mathrm{univ}}, \phi, u)$ and $(C^{\mathrm{univ}'}, \phi', u')$ both represent $\mathscr{F}$, then there is an isomorphism $C^{\mathrm{univ}} \to C^{\mathrm{univ}'}$ with compatible representing and universal objects.

Let $\mathscr{C}$ be the category of all R-algebras, and consider the functor $\mathscr{F}\colon \mathscr{C} \to \mathbf{Set}$ which sends A to the set of all formal R-modules over A and which sends $f : A_1 \to A_2$ to the push-forward f_* from the set of formal R-modules over A_1 to the set of formal R-modules over A_2. Note that a formal R-module over A is just $(F(X,Y), [r]_F(X))$ with coefficients in A such that these coefficients satisfy certain polynomial conditions (by comparing coefficients of each monomial in X and Y). Therefore, $\mathscr{F}$ is represented by $R[\Gamma_{i,j}, \Theta_{k,r}]$ modded out by relations imposed by the definition of formal R-modules, where $\Gamma_{i,j}$ corresponds to the coefficient of X^iY^j in $F(X,Y)$ and $\Theta_{k,r}$ corresponds to the coefficient of X^k in $[r]_F(X)$. In other words, the universal formal R-module is $F^{\mathrm{univ}}(X,Y) = \sum \Gamma_{i,j} X^i Y^j$ and $[r]_{F^{\mathrm{univ}}}(X) = \sum \Theta_{k,r} X^k$, and the representing object Λ_R is the polynomial ring $R[\Gamma_{i,j}, \Theta_{k,r}]$ modded out by relations which make F^{univ} into a formal R-module. We will now analyze Λ_R.

Proposition 3.1.1. *Λ_R can be given a gradation in such a way that $\Gamma_{i,j}$ has degree $i+j-1$ and $\Theta_{k,r}$ has degree $r-1$, and that every degree 0 element can be identified with an element of R.*

Proof. We need to show that the polynomial relations by which we mod out to obtain Λ_R from $R[\Gamma_{i,j}, \Theta_{k,r}]$ are all homogeneous with the degree assignment in the statement of the proposition. Note that this degree assignment is reasonable, as $\Gamma_{1,0} = \Gamma_{0,1} = 1$ and $\Theta_{1,r} = r$ can be homogeneous only if these variables have degree 0. It certainly suffices to show that in these polynomial relations by which we mod out to obtain Λ_R, the degree of the coefficient (i.e. involving Γ's and Θ's) is *always* one less than the polynomial degree of the variables (i.e. involving X's and Y's) in any monomial. We will not check everything here, but as an example, let us pick out $\Gamma_{i,j} X^i Y^j$ from the inside F and $\Gamma_{i',j'}$ from the outside F in the expansion $F(F(X,Y),Z)$. Then we get $\Gamma_{i',j'} \Gamma_{i,j}^{i'} X^{ii'} Y^{ji'} Z^{j'}$. Note that the degree of the coefficient in Λ_R is $(i'+j'-1)+i'(i+j-1) = ii' + ji' + j' - 1$, which is indeed one less than the polynomial degree.

Once we have the gradation, the last statement is clear since the elements of degree 0 among Γ and Θ can be identified with elements of R, as noted above. □

So we have two different notions of degree. We will distinguish them by always saying 'polynomial degree' whenever we mean the total degree of the monomial in X and Y and saying degree to refer to the degree of Λ_R. We will denote the n-th degree component by Λ_R^n. Knowing this gradation is extremely useful. For example, to obtain a formal R-module germ G of degree n over A, we need to specify up to coefficients of monomials of *polynomial* degree $n-1$ in such a way that it forms a formal R-module. Thus, by above, this is same as giving an R-module map $\varphi : \oplus_{i=0}^{n-2} \Lambda_R^i \to A$ such that it is a ring homomorphism wherever it is defined.

Note that Λ_R is in general huge, and in order to construct the formal R-module corresponding to $f : \Lambda_R \to A$, all we need to know are the images of various Γ's and Θ's, and not their products (of course it is important that f is a ring map, but if we somehow know this already then all we need are the images of Γ's and Θ's). This motivates us to define a smaller ring (a quotient of Λ_R) in which various Γ's and Θ's are not identified with each other but in which we can ignore all products of two such variables. Specifically, let I_1 be the ideal of Λ_R generated by homogeneous elements of degree at least 1, and let $\widetilde{\Lambda_R} = \Lambda_R / I_1^2$. This is a

much smaller ring with gradation. Using Lazard's Theorem, we actually have a pretty good grasp of what this ring is:

Proposition 3.1.2. *Let $n \geq 2$. As an R-module, $\widetilde{\Lambda_R^{n-1}}$ is exactly the R-module generated by γ_{n-1} and $\theta_{n-1,r}$ (for each $r \in R$) satisfying the relations*

$$(r^n - r) \cdot \gamma_{n-1} = \epsilon(n)\theta_{n-1,r} \tag{3.1}$$

$$\theta_{n-1,r_1+r_2} - \theta_{n-1,r_1} - \theta_{n-1,r_2} = C_n(r_1, r_2) \cdot \gamma_{n-1} \tag{3.2}$$

$$r_1\theta_{n-1,r_2} + r_2^n\theta_{n-1,r_1} = \theta_{n-1,r_1r_2}, \tag{3.3}$$

where $\epsilon(n)$ and $C_n(X,Y)$ are as defined in Section 2.2, γ_{n-1} here is an element such that $\sum \Gamma_{i,n-i}X^iY^{n-i} = \gamma_{n-1}C_n(X,Y)$ in $\widetilde{\Lambda_R^{n-1}}$, and $\theta_{n-1,r}$ is the image of $\Theta_{n,r}$ in $\widetilde{\Lambda_R^{n-1}}$.

Proof. In Λ_R, if a monomial of total degree $n-1$ in Γ and Θ do not contain a variable of degree $n-1$, then it must be a product of at least two positive-degreed variables. These monomials of degree $n-1$ vanish when we mod out by I_1^2, so as an R-module, $\widetilde{\Lambda_R^{n-1}}$ is generated by images of $\Gamma_{i,n-i}$ and $\Theta_{n,r}$ satisfying the formal R-module identities (with the assumption that any product of two positive-degreed Γ's or Θ's are zero). Let $\theta_{n-1,r}$ be the image of $\Theta_{n,r}$ in $\widetilde{\Lambda_R^{n-1}}$.

In order to obtain γ_{n-1}, let $F_n^{\text{univ}} = \sum \widetilde{\Gamma_{i,n-i}} X^iY^{n-i}$ over $\widetilde{\Lambda_R}$. Clearly, $F_n^{\text{univ}}(X,Y) = F_n^{\text{univ}}(Y,X)$ and $F_n^{\text{univ}}(X,0) = F_n^{\text{univ}}(0,X) = 0$. Now, look at the polynomial degree n part of $F^{\text{univ}}(F^{\text{univ}}(X,Y),Z) = F^{\text{univ}}(X,F^{\text{univ}}(Y,Z))$. On the LHS, in order to get a nonzero expression, if we use a positive-degreed coefficient from the outside F^{univ}, then we cannot use any positive-degreed coefficient from the inside F^{univ}. Thus, the only nonzero monomial contribution comes from either using a degree $(n-1)$ coefficient from the outside F^{univ} or using a degree $(n-1)$ coefficient from the inside F^{univ}. In other words, we get $F_n^{\text{univ}}(X+Y,Z) + F_n^{\text{univ}}(X,Y)$ from the LHS. By a similar computation for the RHS and equating both sides we get

$$F_n^{\text{univ}}(X+Y,Z) + F_n^{\text{univ}}(X,Y) = F_n^{\text{univ}}(X,Y+Z) + F_n^{\text{univ}}(Y,Z).$$

By Proposition 2.2.2, $F_n^{\text{univ}}(X,Y) = \gamma_{n-1}C_n(X,Y)$ for some $\gamma_{n-1} \in \widetilde{\Lambda_R}$. Thus, γ_{n-1} has degree $n-1$ in Λ_R ($\because C_n(X,Y)$ has $\mathbb{Z}$-coefficients) and all $\Gamma_{i,n-i}$'s are generated by γ_{n-1} as an R-module. All the formal group identities (viewed inside $\widetilde{\Lambda_R}$) hold now, so in order to determine all the relations that γ_{n-1} and $\theta_{n-1,r}$ satisfy, we now only need to look at the identities about the R actions.

Denoting $[r]$ for $[r]_{F^{\text{univ}}}$, looking at polynomial degree n terms of $F^{\text{univ}}([r](X),[r](Y)) = [r](F^{\text{univ}}(X,Y))$ in $\widetilde{\Lambda_R}$, we obtain $F_n^{\text{univ}}(rX,rY) + \theta_{n-1,r}X^n + \theta_{n-1,r}Y^n = \theta_{n-1,r}(X+Y)^n + rF_n^{\text{univ}}(X,Y)$. So

$$(r^n - r)\gamma_{n-1}C_n(X,Y) = \theta_{n-1,r}((X+Y)^n - X^n - Y^n) = \theta_{n-1,r}\epsilon(n)C_n(X,Y),$$

resulting in the first identity ($\because C_n(X,Y)$ is a $\mathbb{Z}$-coefficient *primitive* polynomial). Similarly, comparing T^n coefficients of $[r_1+r_2](T) = F^{\text{univ}}([r_1](T),[r_2](T))$ and $[r_1]([r_2](T)) = [r_1r_2](T)$, we get the second and third equations, respectively. □

3.2 R is a Field

We will now analyze the possibilities for the formal R-modules, when R is a field. Actually, as in the following theorem, the possibilities are extremely limited in this case: they are all isomorphic to the additive formal module. This case will serve as a stepping stone for the case of R being the ring of integers of local fields.

Theorem 3.2.1. *Let R be a field, and A be an R-algebra. Then every formal R-module over A is isomorphic to $\widehat{\mathcal{G}}_{\text{a}}$. If further $|R| = \infty$, then there exists a unique isomorphism $\alpha_F(X) \in A[\![X]\!]$ from F to $\widehat{\mathcal{G}}_{\text{a}}$ with derivative 1, and $\Lambda_R \cong R[\Omega_1, \Omega_2, \ldots]$ where Ω_i has degree i and corresponds to the coefficients of X^{i+1} in $\alpha_F(X)$.*

Proof. We first assume that R is characteristic 0. Then by Corollary 2.2.5 (1), there exists an $\circ$-invertible $\alpha \in A[\![X]\!]$ such that $\alpha(F(X,Y)) = \alpha(X) + \alpha(Y)$. Let G be the image of F via α (cf. Example 2.1.10). Then $G(X,Y) = X + Y$, so in particular, $[r]_G(X) + [r]_G(Y) = [r]_G(X+Y)$. By looking at the coefficients of XY^{i-1} on both sides, we conclude that $[r]_G(X) = r \cdot X$. Thus, G must be the additive module. If α_1 and α_2 are both isomorphisms from F to $\widehat{\mathcal{G}}_{\mathrm{a}}$ with derivative 1, then $\alpha_1 \circ \alpha_2^{-1}$ is an isomorphism of $\widehat{\mathcal{G}}_{\mathrm{a}}$ with derivative 1, but by a similar argument as above, this can only be X. Thus, we have a unique isomorphism. For the last statement, given an R-algebra map $f : R[\Omega_1, \ldots] \to A$, let

$$F = (X + f(\Omega_1)X^2 + f(\Omega_2)X^3 + \cdots)^{-1} \circ \widehat{\mathcal{G}}_{\mathrm{a}} \circ (X + f(\Omega_1)X^2 + f(\Omega_2)X^3 + \cdots)$$

be the formal R-module corresponding to f. This association is a natural isomorphism by above, so we have $\Lambda_R \cong R[\Omega_1, \Omega_2, \ldots]$.

Now assume that R is characteristic p. Since $R \longrightarrow \mathrm{End}(F)$ is a ring homomorphism, $[p]_F = 0$. Thus, $pA = 0$ together with Corollary 2.2.5 (2) implies that there exists an isomorphism $\alpha : F \to \widehat{\mathbb{G}}_{\mathrm{a}}$ of formal groups. Let G be the image of F via α; as above, $G(X,Y) = X+Y$. From Example 2.1.7, $\mathrm{End}(G) = A\{\{\tau\}\}$. We will successively construct isomorphisms to eventually obtain the isomorphism with the additive module:

Claim. *Fix $k \geq 1$. Suppose $[r]_G \equiv r + \omega(r)\tau^k \pmod{\tau^{k+1}}$ inside $A\{\{\tau\}\}$ for all $r \in R$ with $\omega(r) \in A$. Then there is an element $a \in A$ such that in the ring $A\{\{\tau\}\}$, $(1+a\tau^k)[r]_G(1+a\tau^k)^{-1} \equiv r \pmod{\tau^{k+1}}$. Moreover, this choice of a is unique if R is infinite.*

Proof. Note that in $\mathrm{End}(G)$, $(1+a\tau^k)(r+\omega(r)\tau^k)(1+a\tau^k)^{-1} \equiv (1+a\tau^k)(r+\omega(r)\tau^k)(1-a\tau^k) \equiv r + ar^{p^k}\tau^k + \omega(r)\tau^k - ra\tau^k \pmod{\tau^{k+1}}$, so what we desire is being able to find $a \in A$ such that $(r^{p^k} - r)a = \omega(r)$. Because $[\ ]_G : R \to A\{\{\tau\}\}$ is a ring homomorphism, we certainly have $\omega(r_1 + r_2) = \omega(r_1) + \omega(r_2)$. Moreover,

$$[r_1]_G[r_2]_G \equiv (r_1 + \omega(r_1)\tau^k)(r_2 + \omega(r_2)\tau^k) \equiv r_1r_2 + r_2^{p^k}\omega(r_1)\tau^k + r_1\omega(r_2)\tau^k \pmod{\tau^{k+1}},$$

and using $r_1r_2 = r_2r_1$ and rearranging terms, we have

$$r_2^{p^k}\omega(r_1) - r_2\omega(r_1) = r_1^{p^k}\omega(r_2) - r_1\omega(r_2).$$

Thus, if $R \not\subseteq \mathbb{F}_{p^k}$, then we have uniqueness and existence of the desired a, as $a = \frac{\omega(r)}{r^{p^k} - r}$ for some $r \in R \backslash \mathbb{F}_{p^k}$.

Now suppose that $R \subseteq \mathbb{F}_{p^k}$. Then the above calculation shows that $\omega(r_1 + r_2) = \omega(r_1) + \omega(r_2)$ and $\omega(r_1r_2) = r_1\omega(r_2) + r_2\omega(r_1)$, i.e. ω is a derivation. By induction, we can show that $\omega(r^m) = mr^{m-1}\omega(r)$ (just like derivatives), so for any $r \in R$, we have $\omega(r) = \omega(r^{p^k}) = p^k r^{p^k - 1}\omega(r) = 0$. Thus we are done. $\square$

We know that $[r]_G \equiv r + \omega_1(r)\tau \pmod{\tau^2}$ for all $r \in R$ in $A\{\{\tau\}\}$, so by the claim there exists $a_1 \in A$ such that $(1 + a_1\tau)[r]_G(1 + a_1\tau)^{-1} \equiv r \mod \tau^2$ for all $r \in R$. Since $1 + a_1\tau \in \mathrm{End}(F)$, the image G_1 of G via this map keeps the additive formal group structure while it now has the property that $[r]_{G_1} \equiv r + \omega_2(r)\tau^2 \equiv \pmod{\tau^3}$ for all $r \in R$. So we can continue by induction, and the product $\cdots(1 + a_3\tau^3)(1 + a_2\tau^2)(1 + a_1\tau)$ is the desired isomorphism of G with the additive R-module with derivative 1 (this infinite product makes sense, since the relation $a^p\tau = \tau a$ keeps the power of τ).

Now suppose that R is infinite, and let $\sum a_i'\tau^i$ be a formal R-module isomorphism from G to $\widehat{\mathcal{G}}_{\mathrm{a}}$ with $a_0' = 1$. Then note that $(1 + a_1'\tau)[r]_G(1 + a_1'\tau)^{-1} \equiv r \pmod{\tau^2}$, so a_1' is uniquely determined by the claim. Similarly, $(1 + a_1'\tau + a_2'\tau^2)[r]_G(1 + a_1'\tau + a_2'\tau^2)^{-1} \equiv r \pmod{\tau^3}$ and $1 + a_1'\tau + a_2'\tau^2 \equiv (1 + a_2'\tau^2)(1 + a_1'\tau) \pmod{\tau^3}$, so again we can use the claim above to conclude the uniqueness of a_2'. We continue by induction, and obtain uniqueness of the isomorphism with the additive module with derivative 1. $\Lambda_R \cong R[\Omega_1, \ldots]$ follows by the same argument as in the characteristic zero case. $\square$

It is *not* true that every formal group over a field of finite characteristic is isomorphic to the additive group. For instance, if R is a field of characteristic 2 and A is an R-algebra, $F(X,Y) = X + Y + XY$ over A is not isomorphic to the additive group, because of $[2]_F(X) = F(X,X) = X^2 \neq 0$ and Corollary 2.2.5 (2). So this is an example of a formal group which cannot be made into a formal R-module.

3.3 R is the Valuation Ring of Local Field

Now we come to what we are most interested in, namely formal R-modules when R is the valuation ring of a local field. Since we will be working with this set-up for the rest of this thesis, we will fix the following notations from now on: K is a local field with the valuation ring R (i.e. R is a discrete valuation ring with finite residue field), π is a uniformizer of R, and k is the residue field $R/(\pi)$ of order q which is a power of a prime p.

It turns out that we can use the results from the field case in analyzing Λ_R. The first step is analyzing the closely-related ring $\widetilde{\Lambda_R}$:

Proposition 3.3.1. *Let $n \geq 2$. Then $\widetilde{\Lambda_R^{n-1}}$ is isomorphic to R as R-modules. More specifically, using the notation from Proposition* 3.1.2*, we can pick a generator η of $\widetilde{\Lambda_R^{n-1}}$ so that*
(1) *if n is not a power of q, $(r^n - r)\eta = \theta_{n-1,r}$ for all $r \in R$ and $\gamma_{n-1} \cdot C_n(X,Y) = \eta \cdot ((X+Y)^n - X^n - Y^n)$.*
(2) *if n is a power of q, $\theta_{n-1,r} = \frac{r^n - r}{\pi} \cdot \eta$ for all $r \in R$ and $\gamma_{n-1} = \frac{p}{\pi} \cdot \eta$.*

Proof. (1a) Suppose n is not a power of p. Let $\eta = \gamma_{n-1}$. From (3.1), $\theta_{n-1,r} \in R\gamma_{n-1} = \eta$ for all r, since any other prime is a unit in R. So by Proposition 3.1.2, $\widetilde{\Lambda_R^{n-1}}$ is generated by η. Plugging $\theta_{n-1,r} = \frac{(r^n - r)}{\epsilon(n)}\eta$ into (3.2) and (3.3), we get $0 = 0$ in both cases, so by the same proposition, $\widetilde{\Lambda_R^{n-1}} \cong R$ by $\eta \mapsto 1$.

(1b) Suppose n is a power of p, but not a power of q. If $r^n - r \in (\pi)$ for all $r \in R$, then $R/(\pi) = \mathbb{F}_q \subseteq \mathbb{F}_n$, which is a contradiction. Thus, let $r \in R$ be such that $r^n - r \notin (\pi)$ (so a unit). Let $\eta = (r^n - r)^{-1}\theta_{n-1,r}$. By (3.1), $\gamma_{n-1} = p\eta \in R\eta$. Using (3.3) and $rr_1 = r_1 r$, we obtain $(r^n - r)\theta_{n-1,r_1} = (r_1^n - r_1)\theta_{n-1,r}$, so $\theta_{n-1,r_1} \in R\eta$ for all $r_1 \in R$. Thus, $\widetilde{\Lambda_R^{n-1}}$ is generated by η. Plugging $\gamma_{n-1} = p\eta$ and $\theta_{n-1,r} = (r^n - r)\eta$ into (3.1), (3.2), and (3.3), we get $0 = 0$, so we conclude that $\widetilde{\Lambda_R^{n-1}} \cong R$ via $\eta \mapsto 1$.

(2) For this part, it is helpful to think of each $\theta_{n-1,r}$ as evaluation of the function $\theta : R \to \widetilde{\Lambda_R^{n-1}}$ at r. We will first show $\widetilde{\Lambda_R^{n-1}}$ is generated by $\theta(\pi)$ as an R-module by showing $M = \widetilde{\Lambda_R^{n-1}}/(\theta(\pi)) = 0$. For any $r \in R$, by (3.3), $r\theta(\pi) + \pi^n\theta(r) = \theta(r\pi) = \theta(\pi r) = \pi\theta(r) + r^n\theta(\pi)$, so in M we must have $\overline{\theta(\pi r)} = \pi^n\overline{\theta(r)} = \pi\overline{\theta(r)}$. Hence $(\pi^n - \pi)\overline{\theta(r)} = 0$, so

$$\pi\overline{\theta(r)} = \overline{\theta(r\pi)} = 0 \qquad \text{for all } r \in R. \tag{3.4}$$

Now (3.3) shows $\theta(1) = 0$. Further, using (3.2),

$$\begin{aligned}\theta(p) &= C_n(p-1,1)\gamma_{n-1} + \theta(p-1) + \theta(1) = C_n(p-1,1)\gamma_{n-1} + C_n(p-2,1)\gamma_{n-1} + \theta(p-2) + \theta(1) \\ &= \cdots = (C_n(p-1,1) + C_n(p-2,1) + \cdots + C_n(1,1))\,\gamma_{n-1} = (p^{n-1} - 1)\gamma_{n-1}.\end{aligned}$$

Thus by (3.4), we have $0 = \overline{\theta(p)} = (p^{n-1} - 1)\overline{\gamma_{n-1}}$, so $\overline{\gamma_{n-1}} = 0$. Using this together with (3.2) and (3.4), we see that $\overline{\theta} : R \xrightarrow{\theta} \widetilde{\Lambda_R^{n-1}} \to M$ is an additive map factoring through $R \to R/(\pi)$. By assumption, $r^n - r \in (\pi)$ for all $r \in R$, so by (3.3) and (3.4), $\overline{\theta} : R/(\pi) \to M$ is a derivation. As before, this means $\overline{\theta} = 0$. On the other hand, by definition of the map and by $\overline{\gamma_{n-1}} = 0$, $\overline{\theta}$ is surjective, so $M = 0$.

We can check by the three equations in Proposition 3.1.2 that there is a well-defined R-module homomorphism $\widetilde{\Lambda_R^{n-1}} \to R$ by $\gamma_{n-1} \mapsto \frac{p}{\pi}$ and $\theta(r) \mapsto \frac{r^n - r}{\pi}$. Since $\theta(\pi)$ is sent to $\pi^{n-1} - 1$ (a unit), this homomorphism is surjective. Since $\widetilde{\Lambda_R^{n-1}}$ is generated by $\theta(\pi)$ as above and $\pi^{n-1} - 1$ is a unit, we have the injectivity of this homomorphism, so we get the desired isomorphism. Thus $\eta = \frac{1}{\pi^{n-1} - 1}\theta(\pi)$ is sent to 1 via this R-module isomorphism, and we have now proved everything. □

The fact that we know explicitly what each of $\widetilde{\Lambda_R^{n-1}}$ is in the above proposition will be useful later when we need successive approximation techniques for formal R-modules. Moreover, we can use the above and Theorem 3.2.1 to obtain Λ_R:

Theorem 3.3.2. $\Lambda_R \cong R[\Upsilon_1, \Upsilon_2, \ldots]$ *as graded* R*-algebras, with* $\deg \Upsilon_i = i$.

Proof. For each $n \geq 2$, letting Υ_{n-1} map to a lift of the generator of $\widetilde{\Lambda_R^{n-1}}$ given in Proposition 3.3.1 to an element of Λ_R^{n-1}, we obtain a graded R-algebra homomorphism $f : R[\Upsilon_1, \Upsilon_2, \ldots] \to \Lambda_R$. The degree-0 part of this map is surjective, so assume by induction that everything up to the degree-$(n-1)$ part of this map is surjective. Then since all elements of degree n can be written as a sum of $r \cdot f(\Upsilon_n)$ and an element in $I_1^2 \cap \Lambda_R^n$ for some $r \in R$ by construction, we get the surjectivity for the degree-n-part by induction. Therefore f is surjective, and in particular, $R[\Upsilon_1, \ldots] \otimes_R K \twoheadrightarrow \Lambda_R \otimes_R K$.

Now let F be the image of $\widehat{\mathcal{G}}_{\mathrm{a}}$ via the isomorphism $X + \Omega_1 X^2 + \cdots$ defined over $R[\Omega_1, \ldots]$. This corresponds to a graded R-algebra homomorphism $g : \Lambda_R \to R[\Omega_1, \ldots]$. Thus, $g \otimes 1 : \Lambda_R \otimes_R K \to R[\Omega_1, \ldots] \otimes_R K$ is a graded K-algebra homomorphism sending $\Gamma_{i,j}^{(R)} \otimes 1$ to the coefficient of $X^i Y^j$ in F and $\Theta_{l,r}^{(R)} \otimes 1$ to the coefficient of X^l in $[r]_F$. By Proposition 3.2.1, composing $g \otimes 1$ with the isomorphism $K[\Omega_1, \ldots] \cong \Lambda_K$, we send $\Gamma_{i,j}^{(R)} \otimes 1$ to $\Gamma_{i,j}^{(K)}$ and $\Theta_{l,r}^{(R)} \otimes 1$ to $\Theta_{l,r}^{(K)}$. By the proof of Proposition 2.1.6, $\Theta_{l,r^{-1}}^{(K)}$ can be expressed as a finite sum of products of elements of K and $\Theta_{l',r}^{(K)}$ for $l' \leq l$, so we conclude that $g \otimes 1$ is surjective.

Hence we have graded R-algebra homomorphisms $R[\Upsilon_1, \ldots] \xrightarrow{f} \Lambda_R \xrightarrow{g} R[\Omega_1, \ldots]$ such that both $f \otimes 1$ and $g \otimes 1$ are surjective. But the corresponding graded components of $K[\Upsilon_1, \ldots]$ and $K[\Omega_1, \ldots]$ have the same dimension, so surjectivity of K-vector space map between them implies injectivity. Hence $(g \otimes 1) \circ (f \otimes 1)$ is injective. By freeness of $R[\Upsilon_1, \ldots]$ as an R-module, we can recover $g \circ f$ as

$$R[\Upsilon_1, \ldots] \otimes_R R \hookrightarrow R[\Upsilon_1, \ldots] \otimes_R K \xrightarrow{(g \circ f) \otimes 1} R[\Omega_1, \ldots] \otimes_R K \ ,$$

thus obtaining injectivity of $g \circ f$. Hence, f is indeed an isomorphism as graded R-algebras. □

Because Λ_R is simple, we will be able to get a lot of information about formal R-modules. For example, we have the following:

Corollary 3.3.3. (1) *Any formal* R*-module germ over an* R*-algebra* A *actually arises from a formal* R*-module over* A.

(2) *If* $A \to B$ *is a surjective* R*-algebra homomorphism, then any formal* R*-module over* B *is the image of a formal* R*-module over* A.

Proof. (1) As remarked earlier, a germ of degree n corresponds to an R-module homomorphism $f : \oplus_{i=0}^{n-2} \Lambda_R^i \to A$ such that $f(1) = 1$ and f is a ring homomorphism wherever it is defined. There is an R-algebra homomorphism $\widetilde{f} : \Lambda_R \cong R[\Upsilon_1, \ldots] \to A$ defined by $\widetilde{f}(\Upsilon_i) = f(\Upsilon_i)$ for $1 \leq i \leq n-2$ and $\widetilde{f}(\Upsilon_i) = 0$ for $i \geq n-1$, and by the assumption $\widetilde{f}$ agrees with f on $\oplus_{i=0}^{n-2} \Lambda_R^i$.

(2) Given $R[\Upsilon_1, \ldots] \to B$, we can lift each of the image of Υ_i to A and then extend this unqiuely to an R-algebra homomorphism $R[\Upsilon_1, \ldots] \to A$. By functoriality, this is what we need. □

One more consequence of Proposition 3.3.1 is that we can prove an analogue of Lazard's Theorem in the setting of formal R-modules. It turns out that equality of two formal R-modules modulo polynomial degree n puts a severe restriction on the difference of two formal R-modules. This is extremely useful when we employ the successive approximation techniques.

Proposition 3.3.4. *Suppose that* F *and* G *are two formal* R*-modules over* A *such that* $(F, [\ ]_F) \equiv (G, [\ ]_G)$ (mod poly. deg. n). *If* n *is not a power of* q, *then there exists* $a \in A$ *such that*

$$F(X,Y) \equiv G(X,Y) + a\left((X+Y)^n - X^n - Y^n\right) \pmod{\text{poly. deg. } n+1}$$
$$[r]_F(X) \equiv [r]_G(X) + (r^n - r) \cdot aX^n \pmod{\text{poly. deg. } n+1} \qquad \forall r \in R.$$

If n is a power of q, then there exists $a \in A$ such that

$$F(X,Y) \equiv G(X,Y) + \frac{p}{\pi} \cdot aC_n(X,Y) \pmod{\text{poly. deg. } n+1}$$
$$[r]_F(X) \equiv [r]_G(X) + \frac{r^n - r}{\pi} \cdot aX^n \pmod{\text{poly. deg. } n+1} \qquad \forall r \in R.$$

Proof. Suppose F, G correspond to R-algebra homomorphisms $f, g : \Lambda_R \to A$. By restriction, we obtain R-module homomorphisms $\oplus_{i=0}^{n-1} \Lambda_R^i \to A$ which are ring homomorphisms wherever it is defined. Since the coefficients of monomials in F and G and $[\ ]_F$ and $[\ ]_G$ agree up to polynomial degree $n-1$, by the ring homomorphism property of f and g, f and g agree on all of $\oplus_{i=0}^{n-2} \Lambda_R^i$. Using the ring homomorphism property of f and g again, f and g must agree on $I_1^2 \cap \Lambda_R^{n-1}$. Thus, if we let $h : \oplus_{i=0}^{n-1} \Lambda_R^i \to A$ be the R-module homomorphism created by taking the difference of f and g, h must be zero on $I_1^2 \cap \Lambda_R^{n-1}$. Hence, we have an R-module homomorphism $\overline{h} : \widetilde{\Lambda_R^{n-1}} = \Lambda_R^{n-1}/(I_1^2 \cap \Lambda_R^{n-1}) \to A$. Using the notation in Proposition 3.3.1, let $a = \overline{h}(\eta)$. What we are interested in are $f(\Gamma_{i,n-i}) - g(\Gamma_{i,n-i}) = h(\Gamma_{i,n-i}) = \overline{h}(\widetilde{\Gamma_{i,n-i}})$ and $f(\Theta_{n,r}) - g(\Theta_{n,r}) = h(\Theta_{n,r}) = \overline{h}(\widetilde{\Theta_{n,r}})$. Therefore, using the fact that $\overline{h}$ is an R-module homomorphism, we are done by Propositions 3.1.2 (for description of γ_{n-1}) and 3.3.1. □

Just as Lazard's Theorem led to Theorem 2.2.4 in the formal group case, the above result gives an easy criterion for when formal R-modules are isomorphic to the additive module:

Corollary 3.3.5. *If a formal R-module F over A satisfies $(F,[\ ]_F) \equiv \widehat{\mathcal{G}}_{\mathrm{a}}$ (mod poly. deg. n) and the coefficient of X^n in $[\pi]_F(X)$ is in $\pi \cdot A$, then there exists a power series $\alpha \equiv X$ (mod poly. deg. n) such that the image of F via the isomorphism α is congruent to the additive module $\widehat{\mathcal{G}}_{\mathrm{a}}$ (mod poly. deg. $n+1$). If a formal R-module F over A is such that the coefficients of $X, \ldots, X^n$ in $[\pi]_F(X)$ are in $\pi \cdot A$, then $(F,[\ ]_F)$ is isomorphic to a formal R-module which is congruent to $\widehat{\mathcal{G}}_{\mathrm{a}}$ modulo polynomial degree $n+1$ (from now on, we will write this as 'F is isomorphic to $\widehat{\mathcal{G}}_{\mathrm{a}}$ modulo polynomial degree $n+1$'). In particular, F is isomorphic to the additive module $\widehat{\mathcal{G}}_{\mathrm{a}}$ if and only if all the coefficients of $[\pi]_F(X)$ are in $\pi \cdot A$.*

Proof. Suppose $(F,[\ ]_F) \equiv \widehat{\mathcal{G}}_{\mathrm{a}}$ (mod poly. deg. n). We will use Proposition 3.3.4. If n is not a power of q, then $F \equiv X + Y + a((X+Y)^n - X^n - Y^n)$ (mod poly. deg. $n+1$) and $[r]_F(X) = rX + (r^n - r) \cdot aX^n$ (mod poly. deg. $n+1$) for some $a \in A$, so if we let $\alpha = X - aX^n$ in Example 2.1.10, we conclude that $\alpha \circ F \circ \alpha^{-1} \equiv X + Y$ (mod poly. deg. $n+1$). If n is a power of q, then $F \equiv X + Y + \frac{p}{\pi} \cdot aC_n(X,Y)$ (mod poly. deg. $n+1$) and $[r]_F(X) \equiv rX + \frac{r^n - r}{\pi} \cdot aX^n$ (mod poly. deg. $n+1$). Since $\frac{\pi^n - \pi}{\pi}$ is a unit, the assumption implies that $a = \pi \cdot a'$ for some $a' \in A$. Using $\alpha = X - a'X^n$ in Example 2.1.10, we obtain $\alpha \circ F \circ \alpha^{-1} \equiv F(X,Y) - a'((X+Y)^n - X^n - Y^n) \equiv X + Y + \frac{p}{\pi} \cdot \pi \cdot a' C_n(X,Y) - a'((X+Y)^n - X^n - Y^n) \equiv X + Y$ (mod poly. deg. $n+1$), and similarly $\alpha \circ [r]_F \circ \alpha^{-1}(X) \equiv rX$ (mod poly. deg. $n+1$).

We always have $(F,[\ ]_F) \equiv \widehat{\mathcal{G}}_{\mathrm{a}}$ (mod poly. deg. 2), so by above, we obtain $\alpha_2 = X - a_2X^2$ such that the image F_2 of F via α_2 is congruent to $\widehat{\mathcal{G}}_{\mathrm{a}}$ modulo polynomial degree 3. $[\pi]_{F_2} = (X - a_2X^2) \circ [\pi]_F \circ (X - a_2X^2)^{-1}$ has coefficients of $X, \ldots, X^n$ in $\pi \cdot A$, so we now apply the first part to F_2. We can thus continue by induction, ending with $\alpha_n = X - a_nX^n$ such that the image of F_n via α_n is congruent to $X + Y$ modulo polynomial degree $n+1$. $\alpha_n \circ \alpha_{n-1} \circ \cdots \circ \alpha_2$ is the desired isomorphism. The 'if' part of the last statement holds by the same process, since the infinite composition $\cdots \circ (X - a_nX^n) \circ (X - a_{n-1}X^{n-1}) \circ \cdots \circ (X - a_2X^2)$ converges in $A[\![X]\!]$. The 'only if' part is clear, since if $\widehat{\mathcal{G}}_{\mathrm{a}} \xrightarrow{\alpha} F$ is an isomorphism, then $[\pi]_F = \alpha \circ (\pi \cdot X) \circ \alpha^{-1}$. □

In particular, we get a parallel of Corollary 2.2.5 (2): if image of π in A is zero, then a formal R-module F is isomorphic to the additive module if and only if $[\pi]_F(X) = 0$.

3.3.1 A Special Case: A Is A Field Over $R/(\pi)$

We continue the discussion of formal R-modules for R the valuation ring of local fields, but now we will specialize our R-algebra A and give more specific results. Some results such as Theorem 3.3.11 below will be crucial in the deformation theory of Chapter 4.

The 'specialized' R-algebras that we ultimately want to study are separably closed fields $A = E$ over $R/(\pi)$, where the R-algebra map is defined by $R \to R/(\pi) \hookrightarrow E$. In this case, a number called the height of a formal module determines its isomorphism class (Proposition 3.3.9, Theorem 3.3.11). Formal R-modules of height ∞ are isomorphic to the additive formal module, and the endomorphism rings of formal R-modules of finite height have a very nice property. But in proving these theorems for separably closed fields, we will need to restrict our attention to some subfield which is not separably closed, so we will first develop some theory for the case when E is just a field over $R/(\pi)$. Thus for now, let us assume that E is a field over $R/(\pi) = k$, with the R-algebra map $R \to R/(\pi) \hookrightarrow E$. In this setting, we have the following:

Proposition 3.3.6. *If F and G are formal R-modules over E and $\alpha : F \to G$ is a nonzero formal R-module homomorphism, then we can rewrite $\alpha(X)$ as $\beta(X^{q^h})$ with $\beta'(0) \neq 0$ for some $h \geq 0$.*

Proof. First, let us focus on the fact that α is a formal *group* homomorphism. If $\alpha'(0) \neq 0$, then we are done, so let us assume that $\alpha'(0) = 0$. By applying the 'chain rule' (which can be proven directly in this algebraic setting) to $G(\alpha(X), \alpha(Y)) = \alpha(F(X,Y))$, we obtain $\frac{\partial G}{\partial X}(\alpha(X), \alpha(Y)) \cdot \alpha'(X) = \alpha'(F(X,Y)) \cdot \frac{\partial F}{\partial X}(X,Y)$. Setting $X = 0$, we get

$$0 = \alpha'(Y) \cdot \frac{\partial F}{\partial X}(0, Y) = \alpha'(Y) \cdot (1 + \text{higher terms})$$

as elements in $E[\![Y]\!]$, so $\alpha'(Y) = 0$. Because any integer which is not divisible by p is a unit in E, it now follows that $\alpha(X) = \alpha_1(X^p)$. Because the Frobenius map $E \to E$ taking every element to its p-th power is a ring homomorphism (*not* an R-algebra homomorphism), $F^{(p)}$ defined by raising every coefficient to its pth power is a formal group (not in general a formal R-module). Moreover, we have

$$\alpha_1(F^{(p)}(X^p, Y^p)) = \alpha_1((F(X,Y))^p) = \alpha(F(X,Y)) = G(\alpha(X), \alpha(Y)) = G(\alpha_1(X^p), \alpha_1(Y^p)),$$

so α_1 is a formal group homomorphism from $F^{(p)}$ to G, thus we can continue the process by induction. Since $\alpha \neq 0$, we end at some point, that is, $\alpha = \beta(X^{p^l})$ with $\beta'(0) \neq 0$ for some l.

Now we use the fact that α is a formal R-module homomorphism. Note that $\alpha([r]_F(X)) = [r]_G(\alpha(X))$ implies $\beta(([r]_F(X))^{p^l}) = [r]_G(\beta(X^{p^l}))$. Comparing X^{p^l} coefficients, we obtain $r^{p^l} \cdot \beta'(0) = r \cdot \beta'(0)$ in E. Because E is a field and $\beta'(0) \neq 0$, we have $r^{p^l} = r$ in E for all $r \in R$. This happens if and only if $\mathbb{F}_q \subseteq \mathbb{F}_{p^l}$, i.e. if and only if p^l is a power of q. □

Using this proposition, we define

Definition 3.3.7. The *height* $\operatorname{ht}\alpha$ of a nonzero formal R-module homomorphism α between formal R-modules over E is the integer h such that $\alpha(X) = \beta(X^{q^h})$ with $\beta'(0) \neq 0$. The height of the zero homomorphism is defined to be ∞.

Next, we put together easy computational results about height of formal R-module homomorphisms.

Proposition 3.3.8. (1) $\operatorname{ht}(\alpha_1 \circ \alpha_2) = \operatorname{ht}(\alpha_1) + \operatorname{ht}(\alpha_2)$.
(2) $\operatorname{ht}(\alpha) = 0$ *if and only if α is a formal R-module isomorphism.*
(3) $\operatorname{ht}(\alpha_1 \underset{G}{+} \alpha_2) \geq \min(\operatorname{ht}(\alpha_1), \operatorname{ht}(\alpha_2))$, *for $\alpha_1, \alpha_2 : F \to G$.*

Proof. All the statements become trivial with the zero map, so we will only check these for nonzero maps. By definition, the height is $\log_q$ of the first exponent which has a nonzero coefficient.
(1) $(a_1 X^{q^{h_1}} + \cdots) \circ (a_2 X^{q^{h_2}} + \cdots) = a_1 a_2^{q^{h_1}} X^{q^{h_1+h_2}} + \cdots$.
(2) $\operatorname{ht}(\alpha) = 0$ iff the coefficient of X is nonzero (i.e. $\circ$-invertible), so we are done by Proposition 2.1.6.
(3) $G(\alpha_1(X), \alpha_2(X)) = \alpha_1(X) + \alpha_2(X) +$ higher order terms. □

Given a formal R-module F over E, every $[r]_F$ is a formal R-module endomorphism. For a unit $u \in R$, Proposition 3.3.8 (2) shows that $\operatorname{ht}([u]_F(X)) = 0$, so by (1), we know $\operatorname{ht}([\pi u]_F(X)) = \operatorname{ht}([\pi]_F(X))$. Thus, we can now define the **height** $\operatorname{ht}(F)$ of a formal R-module to be $\operatorname{ht}([\pi]_F(X))$.

As an example of a formal R-module with finite height, consider $\widehat{\mathbb{G}}_{\mathrm{m}}$ as a $\mathbb{Z}_p$-module over $\mathbb{F}_p$. Then we can prove by induction that $[p](X) = X^p$, so it has height 1.

One property of the height of a formal R-module is immediate: $\alpha([\pi]_F(X)) = [\pi]_G(\alpha(X))$ together with Proposition 3.3.8 (1) shows $\mathrm{ht}(\alpha) + \mathrm{ht}(F) = \mathrm{ht}(G) + \mathrm{ht}(\alpha)$, so if $\alpha \neq 0$, then $\mathrm{ht}(F) = \mathrm{ht}(G)$. In other words, there exists a nonzero formal R-module homomorphism only if the two formal R-modules are of the same height, and in particular, isomorphic formal R-modules have the same height. Using knowledge of universal formal R-modules we can prove the following:

Proposition 3.3.9. (1) *Given $h \geq 0$, we can construct a formal R-module over E of height h.*

(2) *A formal R-module over E of height h is isomorphic to the additive module modulo polynomial degree q^h.*

(3) *A formal R-module over E is isomorphic to the additive module if and only if the height is ∞.*

Proof. (1) Because $\Lambda_R \cong R[\Upsilon_1, \ldots]$ by Proposition 3.3.2, let F be the formal R-module over E corresponding to the R-algebra homomorphism $R[\Upsilon_1, \ldots] \to E$ defined by sending Υ_{q^h-1} to 1 and everything else to zero. Since $\Gamma_{i,j}$ and $\Theta_{l,r}$ with $1 \leq i + j - 1$, $l - 1 \leq q^h - 2$ are R-linear combinations of products of Υ's of degree between 1 and $q^h - 2$, it follows that the coefficients in $(F, [\ ]_F)$ of polynomial degree between 2 and $q^h - 1$ are all zero. In other words, $F \equiv \widehat{\mathcal{G}}_{\mathrm{a}}$ (mod poly. deg. q^h), so by Proposition 3.3.4, there exists $a \in E$ such that $F(X,Y) \equiv X + Y + \frac{p}{\pi} \cdot aC_{q^h}(X,Y)$ (mod poly. deg. $q^h + 1$) and $[r]_F(X) \equiv r \cdot X + \frac{r^{q^h} - r}{\pi} \cdot aX^{q^h}$ (mod poly. deg. $q^h + 1$). If $a = 0$, then these formula imply that every $\Gamma_{i,j}$ and $\Theta_{l,r}$ up to and including degree $q^h - 1$ are sent to 0 via f, so as a sum of products of these elements, Υ_{q^h-1} must have been sent to 0 by f, contradiction. So $a \neq 0$, and $[\pi]_F(X) \equiv (\pi^{q^h-1} - 1) \cdot aX^{q^h}$ (mod poly. deg. $q^h + 1$) shows that F has height exactly h.

(2) We know that the coefficients of $X, \ldots, X^{q^h-1}$ in the expression $[\pi]_F(X)$ are $0 \in (0) = \pi \cdot E$, so we are done by the second statement in Corollary 3.3.5.

(3) $\pi = 0$ in E shows $\mathrm{ht}(\widehat{\mathcal{G}}_{\mathrm{a}}) = \infty$, so every formal R-module isomorphic to $\widehat{\mathcal{G}}_{\mathrm{a}}$ also has height ∞. Conversely, if $\mathrm{ht}(F) = \infty$, then $[\pi]_F(X) = 0 \in \pi \cdot E$, so by Corollary 3.3.5, F is isomorphic to $\widehat{\mathcal{G}}_{\mathrm{a}}$. □

So we understand the formal R-modules over E of height ∞ very well. To get a similar nice result for the possibilities for the finite height case, we will need to put more conditions on E, namely separable closure. This special case is all we need in our usage in the deformation theory. Thus, for the rest of the section, we will further assume that E is **separably closed**. Let us now fix a non-negative integer h, and we will now analyze formal R-modules of height h over a separably closed field E, with the R-algebra map $R \to R/(\pi) \hookrightarrow E$.

Since E is separably closed, $\mathbb{F}_{q^h} \subseteq E$ as *the* subset of elements satisfying $x^{q^h} - x = 0$. We now define the central player of the formal R-modules over E of height h:

Definition 3.3.10. A formal R-module F over E satisfying

(1) $[\pi]_F(X) = X^{q^h}$

(2) $F(X,Y) \in \mathbb{F}_{q^h}[\![X,Y]\!]$ and $[r]_F(X) \in \mathbb{F}_{q^h}[\![X]\!]$.

(3) $(F, [\ ]_F) \equiv \widehat{\mathcal{G}}_{\mathrm{a}}$ (mod poly. deg. q^h)

is said to be *π-normal of height h*.

Here is the analogue of Proposition 3.3.9 (3) in the finite height case:

Theorem 3.3.11. *Every formal R-module over E of height h is isomorphic to a π-normal one, and given any two π-normal formal R-modules over E of height h, there is an isomorphism between them which is $\equiv X$ (mod poly. deg. $q^h + 1$). In particular, all formal R-modules over E of height h are isomorphic to each other.*

Proof. Let $n = q^h$. By height consideration, $[\pi]_F \equiv aX^n$ (mod poly. deg. $2n$) for some $a \in E$. Because of separable closure, there exists $a_1 \in E$ such that $a_1^{n-1} = a$. Then the image F_2 of F via the isomorphism $\alpha_1 = a_1 X$ satisfies $[\pi]_{F_2}(X) \equiv X^n$ (mod poly. deg. $2n$). Now assume by induction that for a formal R-module F_i, $[\pi]_{F_i}(X) \equiv X^n$ (mod poly. deg. in) for some $i \geq 2$. Let $[\pi]_{F_i}(X) \equiv X^n + b_i X^{in}$ (mod poly. deg. $in + 1$) for some $b_i \in E$. There exist $a_i \in E$ such that $a_i^n - a_i + b_i = 0$, and the image F_{i+1} of F_i via the isomorphism $(X + a_i X^i)^{-1}$ has the property that $[\pi]_{F_{i+1}}(X) \equiv X^n$ (mod poly. deg. $in + 1$). By height

consideration, $[\pi]_{F_{i+1}}(X) \equiv X^n \pmod{\text{poly. deg. } (i+1)n}$. Thus, the image F_∞ of F via the isomorphism made from the infinite composition $\cdots \circ (X + a_4X^4)^{-1} \circ (X + a_3X^3)^{-1} \circ (X + a_2X^2)^{-1} \circ a_1X$ has the property that $[\pi]_{F_\infty}(X) = X^n$. So we may now assume that our original F has the property that $[\pi]_F(X) = X^n$. But now, $F([\pi]_F(X), [\pi]_F(Y)) = [\pi]_F(F(X,Y))$ and $[r]_F \circ [\pi]_F(X) = [\pi]_F \circ [r]_F(X)$ with coefficients in characteristic p, imply that all the coefficients of F and $[r]_F(X)$ are in $\mathbb{F}_n$. Therefore, F is actually a formal R-module over $\mathbb{F}_n$. By Proposition 3.3.9 (2), there exists an $\circ$-invertible $\alpha \in \mathbb{F}_n[\![X]\!]$ such that the image G of F via the isomorphism α is congruent to the additive module modulo polynomial degree q^h. If we let $\alpha^{-1}(X) = \sum c_i X^i$, $[\pi]_G(X) = \alpha \circ [\pi]_F \circ (\sum c_i X^i) = \alpha\left(\sum c_i^n X^{in}\right) = \alpha \circ \alpha^{-1}(X^n) = X^n$. Therefore, we get the desired isomorphism with a π-normal formal R-module over E of height h.

Now suppose that F and G are two π-normal formal R-modules over E of height h. Since $F \equiv G \pmod{\text{poly. deg. } q^h}$ and $[\pi]_F = [\pi]_G$, Proposition 3.3.4 shows that $F \equiv G \pmod{\text{poly. deg. } q^{h+1}}$. From here, we can use the successive approximation, as in the proof of Corollary 3.3.5. That is, if we know $F \equiv G \pmod{\text{poly. deg. } m}$ with m not a power of q, it is the same proof. If m is a power of q, $[\pi]_F = [\pi]_G = X^{q^h}$ shows that $F \equiv G \pmod{\text{poly. deg. } m+1}$. The important point is that by thinking of F and G as formal R-modules over $\mathbb{F}_{q^h}$, the isomorphism that we obtain by this process have coefficients in $\mathbb{F}_{q^h}$, so as before, the $[\pi]_F(X) = X^{q^h}$ property (thus normality) is preserved via isomorphisms. □

The above theorem often enables us to reduce studying formal R-modules of height h to studying π-normal formal R-modules of height h, if we are over a separably closed field. We will frequently use this method in Chapter 4. Moreover, we can prove the following about $\mathrm{End}(F)$ when F has height h, which is an analogue of [8, page 72]. Although we will not need this in our discussion of deformation theory, it is a beautiful and important result so we include here. For this proof only, we will assume some knowledge of central division algebra and Brauer groups in connection with local fields [23].

Theorem 3.3.12. *If F is a π-normal formal R-module of height h, then $\mathrm{End}_R(F)$ is isomorphic to the integral closure of R in a central division algebra D of dimension h^2 over K whose invariant is $\frac{1}{h}$.*

Proof. Let $\mathscr{E}$ be $\mathrm{End}_R(F)$. *In this proof only*, given $\alpha_i \in \mathscr{E}$, $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2$ indicate the addition and multiplication in this (not necessarily commutative) ring, unless otherwise specified (so we are not using the usual addition and multiplication of power series rings). We have a ring homomorphism $R \to \mathscr{E}$ defined by $r \mapsto [r]_F(X)$, and we will often write the image of r in $\mathscr{E}$ as simply r. By definition, $r\alpha = \alpha r$ for all $\alpha \in \mathscr{E}$ and $r \in R$, and in particular, $(\alpha(X))^{q^h} = \pi\alpha = \alpha\pi = \alpha(X^{q^h})$ over a field of characteristic p shows that all coefficients of α lie in $\mathbb{F}_{q^h}$. The same equation also shows that $\pi\alpha = 0$ if and only if $\alpha = 0$.

If $\mathrm{ht}\,\alpha \geq nh$, then Proposition 3.3.6 enables us to write $\alpha(X) = \beta(X^{q^{nh}}) = \beta\pi^n = \pi^n\beta$, and this β is an element of $\mathscr{E}$. So we conclude $\pi^n\mathscr{E} = \{\alpha \in \mathscr{E} : \mathrm{ht}\,\alpha \geq nh\}$. Thus, $\bigcap \pi^n\mathscr{E} = (0)$. Using this and Proposition 3.3.8, the infinite sum $\sum \pi^n\alpha_n$ is a well-defined power series with coefficients in $\mathbb{F}_{q^h}$, and checking that this is an element of $\mathscr{E}$ reduces to checking for various finite sums. Hence, $\mathscr{E}$ is a π-adically complete R-module.

Lemma 3.3.13. *The map $\varphi : \mathscr{E} \to (\mathbb{F}_{q^h})^{\oplus h}$ sending α to the coefficients of $X, X^q, X^{q^2}, \ldots, X^{q^{h-1}}$ is an R-module homomorphism (R-module action is given via $R \to R/(\pi) \hookrightarrow \mathbb{F}_{q^h}$), inducing an isomorphism $\mathscr{E}/\pi\mathscr{E} \to (\mathbb{F}_{q^h})^{\oplus h}$. From this, we obtain an R-module isomorphism $\mathscr{E} \to R^{\oplus h^2}$.*

Proof. $F \equiv \widehat{\mathcal{G}}_{\mathrm{a}} \pmod{\text{poly. deg. } q^h}$ shows that φ is an R-module homomorphism. Proposition 3.3.6 shows that any $\alpha \in \mathscr{E}$ must start from a monomial with exponent a power of q, so $\varphi(\alpha) = 0 \iff \mathrm{ht}\,\alpha \geq h \iff \alpha \in \pi\mathscr{E}$. For surjectivity of φ, by the additivity it suffices to check the existence of α such that $\varphi(\alpha) = (\lambda_0, \ldots, \lambda_{h-1}) \in (\mathbb{F}_{q^h})^{\oplus h}$ for $\lambda_0 \neq 0$. Now, $\beta = \lambda_0 X + \lambda_1 X^q + \cdots + \lambda_{h-1}X^{q^{h-1}}$ is $\circ$-invertible, so as in Example 2.1.10, β is an R-module isomorphism from F to G, where G is the image of F under β. As before, $[\pi]_G(X) = X^{q^h}$, and $G \equiv \widehat{\mathcal{G}}_{\mathrm{a}} \pmod{\text{poly. deg. } q^h}$ because of $(X+Y)^q = X^q + Y^q$. In other words, G is π-normal of height h, and Theorem 3.3.11 (2) gives us a formal R-module isomorphism $\beta_2 : G \to F$ with $\beta_2 \equiv X \pmod{\text{poly. deg. } q^h + 1}$. Composition $\beta_2 \circ \beta$ gives the desired element.

For the last statement, note that as R-modules, $(\mathbb{F}_{q^h})^{\oplus h} \cong (\mathbb{F}_q)^{\oplus h^2}$. For $i = 1, \ldots, h^2$, let $\alpha_i \in \mathscr{E}$ be a pull-back via φ of a generator of the i-th component of $(\mathbb{F}_q)^{\oplus h^2}$. Given $\alpha \in \mathscr{E}$, there exist $r_{0,i} \in R$ such that $\alpha - \sum r_{0,i}\alpha_i = \pi\beta_1$ for some $\beta_1 \in \mathscr{E}$. We can then start from β_1 and find $r_{1,i}$ and β_2 with the similar property, and continue by induction. Note that

$$\alpha - \sum_i \left(\sum_n \pi^n r_{n,i} \right) \alpha_i \in \bigcap_{i=0}^{\infty} \pi^n \mathscr{E} = (0),$$

because $\pi^n \alpha'_n + \pi^{n+1}\alpha'_{n+1} + \cdots \in \pi^n\mathscr{E}$ by the completeness of $\mathscr{E}$ for $\alpha'_i \in \mathscr{E}$. By the completeness of R, each $\sum_n \pi^n r_{n,i}$ converges, so we now know that α_i's generate $\mathscr{E}$. Suppose $\sum r_i\alpha_i = 0$. Modding out by $\pi\mathscr{E}$, we see that each $r_i = \pi r_{1,i}$. Thus $\pi(\sum r_{1,i}\alpha_i) = 0$, implying that $\sum r_{1,i}\alpha_i = 0$. Continuing this process, we conclude that each $r_i = 0$. □

Let $D = K \otimes_R \mathscr{E}$, a K-algebra of dimension h^2. By transferring all high powers of π to the side of $\mathscr{E}$, we see that every element of D is of the form $\pi^n \otimes \alpha$ for some $n \in \mathbb{Z}$ and $\alpha \in \mathscr{E}$. Because $\mathscr{E} \cong R^{\oplus h^2}$, $\pi^n \otimes \alpha = 0$ implies $\alpha = 0$ for any n. Thus, the fact that $\mathscr{E}$ has no zero-divisor (checked by height consideration) implies that D has no zero-divisors. Hence, by finite-dimensionality, D is a division algebra over K. Note also that by definition, K is contained in the center of D.

By freeness of $\mathscr{E}$ over R, $\mathscr{E} \hookrightarrow K \otimes_R \mathscr{E}$. Moreover, since $R \hookrightarrow K \hookrightarrow K \otimes_R \mathscr{E}$ agrees with $R \to \mathscr{E} \to K \otimes_R \mathscr{E}$, $R \to \mathscr{E}$ is injective. Identifying $\mathscr{E}$ and R with their images in D, we will now prove that $\mathscr{E}$ is the integral closure of R in D. By defining $\mathrm{ht}(\pi^n \otimes \alpha) = hn + \mathrm{ht}(\alpha)$, we get a well-defined function on D, and by transferring the powers of π across $\otimes$ and using Proposition 3.3.8, we can show that this is a valuation on D. If $\mathrm{ht}(\pi^{-n} \otimes \alpha) \geq 0$, then as before, $\alpha = \beta(X^{q^{nh}}) = \pi^n\beta$ for some $\beta \in \mathscr{E}$, and $\pi^{-n} \otimes \alpha = 1 \otimes \beta \in \mathscr{E}$. Thus, $\mathscr{E}$ is exactly the subset of D where ht is non-negative. Now, for $d \in D$, $K(d)/K$ must be a (commutative) finite extension of local fields. Since $\mathrm{ht}(r) = h \cdot v(r)$ for all $r \in R$ where v is the normalized π-adic valuation on K, and by valuation theory [23, Theorem 8.17], $\mathrm{ht}(d) \geq 0$ if and only if d is integral over R. Thus, $\mathscr{E}$ is the integral closure of R inside D.

To prove that the center L of D is K, we will first need the following computational lemma:

Lemma 3.3.14. *For $\alpha, \beta \in \mathscr{E}$, if $\mathrm{ht}(\alpha) = n$ then $\mathrm{ht}(\alpha\beta - \beta^{q^n}\alpha) \geq n + 1$.*

Proof. If $\mathrm{ht}(\beta) > 0$, then this follows by Proposition 3.3.8. Otherwise, since both $\alpha\beta$ and $\beta^{q^n}\alpha$ start with the same X^{q^n} monomial, $\alpha\beta - \beta^{q^n}\alpha \equiv 0 \pmod{\text{poly. deg. } q^n + 1}$. By Proposition 3.3.6, we are done. □

Let M be the maximal unramified extension of K inside L. Let $\beta \in \mathscr{O}_M$, the valuation ring of M. Since β is integral over R, $\beta \in \mathscr{E}$. Let α be a height 1 element of $\mathscr{E}$, which exists by Lemma 3.3.13. By Lemma 3.3.14 and centrality, $\mathrm{ht}(\beta\alpha - \beta^q\alpha) \geq 2$, so multiplying on the right by α^{-1} in D, we conclude that $\mathrm{ht}(\beta - \beta^q) \geq 1$. Thus $\beta \equiv \beta^q \pmod{\mathfrak{m}_{\mathscr{O}_M}}$ for *all* $\beta \in \mathscr{O}_M$. So by unramifiedness, M must be K. Thus, L/K is totally ramified, so let us write $\mathscr{O}_L = \mathscr{O}_K(\Pi)$ for some uniformizer Π in L. Suppose on the contrary that $L \neq K$ so that $\mathrm{ht}(\Pi) < \mathrm{ht}(\pi) = h$ by Proposition 3.3.8.

In order to get a contradiction from this, we need to first show that D contains a copy of K_h, an unramified extension of K of degree h (this is unique if we work inside an algebraic closure, but inside D we cannot do this). Letting $\mathfrak{m}_{\mathscr{E}}$ be the (two-sided) ideal of $\mathscr{E}$ consisting of elements of height at least 1, we have an R-algebra isomorphism $\mathscr{E}/\mathfrak{m}_{\mathscr{E}} \to \mathbb{F}_{q^h}$ defined by sending α to its derivative (use Lemma 3.3.13 for surjectivity). Lifting a primitive element of $\mathbb{F}_{q^h}/\mathbb{F}_q$ via this isomorphism to $d \in \mathscr{E}$, we know that $K(d)/K$ is a finite extension of local fields. Since $\mathfrak{m}_{\mathscr{O}_{K(d)}} = \mathscr{O}_{K(d)} \cap \mathfrak{m}_{\mathscr{E}}$, the residue field of $K(d)$ is $\mathbb{F}_{q^h}$. By [23, Theorem 8.26], $K(d)/K$ contains an unramified extension K_h of degree h over K, so in particular, D does contain a copy of K_h.

So now let $\beta \in \mathscr{O}_{K_h}$. Then similarly as before, we have $\mathrm{ht}(\beta\Pi - \beta^{q^{\mathrm{ht}\,\Pi}}\Pi) \geq \mathrm{ht}(\Pi) + 1$ by Lemma 3.3.14 and centrality of Π, so by multiplying on the left by Π^{-1} in D, we obtain $\mathrm{ht}(\beta - \beta^{q^{\mathrm{ht}\,\Pi}}) \geq 1$. This implies

that the residue field of $\mathscr{O}_{K_h}$ has at most $q^{\operatorname{ht}\Pi}$ elements, contradiction. Thus, the center L of D must be K, and so we have finally proved that $\mathscr{E}$ is the integral closure of R inside the central division algebra D over K of dimension h^2.

Before proving the last statement, note that we have a group homomorphism $\varphi : D^* \longrightarrow \operatorname{Gal}\big((\mathscr{E}/\mathfrak{m}_{\mathscr{E}})/k\big)$ by letting $\varphi(d)$ be the map $x \mapsto dxd^{-1}$. Since $\mathscr{E}/\mathfrak{m}_{\mathscr{E}} \cong \mathbb{F}_{q^h}$ is commutative, any element of $\mathscr{E}^*$ (i.e. height 0 elements) is sent to the identity map by φ. Moreover, π is in K which is the center of D, so $\mathscr{E}^* \times \langle\pi\rangle$ is in the kernel of φ. On the other hand, given any element of $\operatorname{Gal}(\mathbb{F}_{q^h}/\mathbb{F}_q)$ there exists a (unique) lift to $\sigma \in \operatorname{Gal}(K_h/K)$. By Noether-Skolem Theorem, $\sigma : K_h \longrightarrow K_h \hookrightarrow D$ is given by a conjugation by some $d \in D^*$. By construction, $\varphi(d)$ is the element of $\operatorname{Gal}(\mathbb{F}_{q^h}/\mathbb{F}_q)$ that we started out with, so we now have proved that φ is surjective. Since $D^*/\big(\mathscr{E}^* \times \langle\pi\rangle\big)$ is just $\mathbb{Z}/(\operatorname{ht}(\pi)\mathbb{Z})$, counting shows that the kernel of φ is exactly $\mathscr{E}^* \times \langle\pi\rangle$. Therefore, $d_1, d_2 \in D^*$ induce the same conjugation map on $\operatorname{Gal}\big((\mathscr{E}/\mathfrak{m}_{\mathscr{E}})/k\big)$ if and only if $\operatorname{ht}(d_1) - \operatorname{ht}(d_2)$ is a multiple of $h = \operatorname{ht}(\pi)$. In other words, there exists a unique coset mod $\mathbb{Z}$ formed by $\frac{v(d)}{v(\pi)}$, where v is a valuation on D and $d \in D^*$ is an element satisfying

$$dd_1d^{-1} \equiv (d_1)^q \pmod{\mathfrak{m}_D} \qquad \text{for all } d_1 \in \mathscr{O}_D. \tag{3.5}$$

By the same argument as above, there exists some d such that $x \mapsto dxd^{-1}$ defines the unique element of $\operatorname{Gal}(K_h/K)$ which reduces to the Frobenius map $\sigma \in \operatorname{Gal}(\mathbb{F}_{q^h}/\mathbb{F}_q)$. Such a d satisfies (3.5). In this case, d^h commutes with every element of K_h, so $d^h \in K_h$. Moreover, $\sigma(d^h) = dd^hd^{-1} = d^h$ shows that $d^h \in K$. Thus D is isomorphic to the cyclic algebra $[K_h/K, \sigma, d^h]$, by dimension comparison and simplicity of cyclic algebras. Now the invariant of such a cyclic algebra over a local field is defined by $v(d^h)/h$ where v is the normalized valuation of K ([23]). Therefore, the previous paragraph shows that the invariant of D is the unique coset mod $\mathbb{Z}$ formed by $\frac{v(d)}{v(\pi)}$ with d satisfying (3.5).

By Lemma 3.3.14, any height 1 element $d \in D$ satisfies (3.5), so the invariant must be $\frac{1}{h}$. We are finally done with the proof. □

Chapter 4

Deformation Theory

We are finally ready to begin discussing deformation theory. Before giving an overview of the chapter, we will set forth the notations that are used throughout. As before, K is a local field, R the valuation ring, π a uniformizer, $k = R/(\pi)$ the residue field of order q, a power of p. After fixing an algebraic closure of K, we can speak of *the* maximal unramified extension K^{nr}. The completion of K^{nr} with π-adic topology is denoted $\widehat{K}^{\mathrm{nr}}$ with valuation ring $\widehat{R}^{\mathrm{nr}}$. Here, π still generates the maximal ideal, and $\widehat{R}^{\mathrm{nr}}/(\pi) \cong \bar{k}$, the algebraic closure of k. Let $\mathscr{C}$ be the category whose objects are complete noetherian local $\widehat{R}^{\mathrm{nr}}$-algebra A with maximal ideal $\mathfrak{m}_A$ such that $\widehat{R}^{\mathrm{nr}}/(\pi) \cong A/\mathfrak{m}_A$ via the algebra map $\jmath : \widehat{R}^{\mathrm{nr}} \to A$ and whose morphisms are local $\widehat{R}^{\mathrm{nr}}$-algebra homomorphisms. We will often implicitly identify $\widehat{R}^{\mathrm{nr}}/(\pi)$ with $A/\mathfrak{m}_A$ via $\jmath$: for instance, a formal R-module over one of them is automatically considered a formal R-module over the other via push-forward by $\jmath$ (or its inverse).

A deformation over $A \in \mathscr{C}$ of a formal R-module G over $\bar{k}$ refers to a formal R-module F over A which reduces modulo $\mathfrak{m}_A$ to G. We identify two deformations F_1 and F_2 of G over A whenever there is an isomorphism of formal R-modules which reduces modulo $\mathfrak{m}_A$ to the identity. The first section of the chapter studies such deformation classes. More specifically, we are interested in knowing the universal deformation, i.e. the universal object of the functor which associates $A \in \mathscr{C}$ with the set of deformation classes over A. It turns out that the universal deformation ring is a power series ring over $\widehat{R}^{\mathrm{nr}}$ with the number of variables one less than the height of G, with a specific description of the universal deformation F^{univ} (at least we know what $[\pi]_{F^{\mathrm{univ}}}(X)$ looks like). To prove this theorem, we will need to study a connection between cohomology and formal R-modules.

The second section introduces the notion of level structures to formal R-modules. This definition of level structures was a great insight of Drinfel'd's. For a formal R-module F over A, the structure of level n (for $n \geq 1$) is a homomorphism $\varphi : (\pi^{-n}R/R)^h \to F(\mathfrak{m}_A)$ such that

$$P_\varphi(X) = \prod_{s \in (\pi^{-1}R/R)^h} (X - \varphi(s)) \quad \Big| \quad [\pi]_F(X),$$

where h is the height of $\overline{F}$. The main theorem of the section determines the universal deformation with structure of level n. The universal deformation ring $D_{h,n}$ is very nice; it is a regular local ring of dimension h with a system of local parameters given by the images of the standard basis of $(\pi^{-n}R/R)^h$ under the universal level structure, and the natural map $D_{h,n} \to D_{h,n+1}$ is finite and flat. The proof uses the fact that we know the universal deformation ring from Section 4.1. At the end, we will use some of these nice properties of $D_{h,n}$ to construct a level structure on a 'quotient' formal R-module.

In the final section, we will be using the more general notion of formal R-modules as discussed in Section 2.3. We define a divisible formal R-module of type (h, j) to be a formal R-module F whose connected component F^0 is a CFS formal R-module (i.e. those satisfying Definition 2.1.8) with $\mathrm{ht}(\overline{F^0}) = h$ and whose étale component is $\mathrm{Spf}_A(A^{(K/R)^j})$. We will then define the notion of level structures for each n in this setting. Unlike the deformations of the previous section, there is more than one choice of level structure on G, so we

will discuss deformations of (G, ϕ), where ϕ is a fixed level structure on G. The universal deformation ring $E_{h,n,j}$ of (G, ϕ) with structure of level n turns out to be a regular local ring again (in fact, it is simply the power series ring over $D_{h,n}$ with j variables). So $E_{h,n,j} \to E_{h,n+1,j}$ is finite and flat.

The deformation theory of Section 4.3 is what Drinfel'd was really after in [5], as the 'local' analysis of Drinfel'd modules results in deformations of divisible formal R-modules. On the other hand, both divisible formal R-modules and level structures on them are defined using the corresponding notions for the CFS formal R-modules, so the deformation theory of divisible formal R-modules is heavily based on the deformation theory discussed in the first two sections of this chapter.

The descriptions of the universal formal R-module that we obtained in the last chapter will be used throughout this chapter. Moreover, we will frequently use the fact that every formal R-module of a given finite height is isomorphic to a π-normal one over a separably closed field.

4.1 Deformations

Let us fix $A \in \mathscr{C}$ and let $\mathfrak{m} = \mathfrak{m}_A$. Geometrically speaking, a deformation of a geometric object X_0 is a 'continuous family' of geometric objects including X_0. In the language of modern algebraic geometry, 'continuous family' corresponds to a flat morphism $X \to T$ for some scheme T and the notion of X_0 being a part of this family corresponds to the statement that X_0 is isomorphic to a fiber of this morphism at some point $t \in T$. Recall that we can always view a formal R-module F (in the sense of Definition 2.1.8) as $\mathrm{Spf}_A(A[\![X]\!])$ by Proposition 2.3.2. Since the structure map $\mathrm{Spf}_A(A[\![X]\!]) \to \mathrm{Spf}_A(A)$ is topologically flat, it makes sense to say that the formal R-module F is a deformation of a formal R-module G over $A/\mathfrak{m}$ if G is isomorphic to the unique closed fiber, i.e. G is isomorphic to $\overline{F}$ (F reduced modulo $\mathfrak{m}$). This motivates us to define deformation of a formal R-module G over $\widehat{R}^{\mathrm{nr}}/(\pi)$ as follows:

Definition 4.1.1. The pair (F, ι) is said to be a *deformation* of G over A if F is a formal R-module F over A and ι is an isomorphism over $\widehat{R}^{\mathrm{nr}}/(\pi)$ from F modulo $\mathfrak{m}$ (identified via $\jmath$) to G. We define two deformations (F_i, ι_i) to be *isomorphic* if there exists a formal R-module isomorphism $\alpha : F_1 \to F_2$ over A such that

$$\begin{array}{ccc} F_1 \bmod \mathfrak{m} & \xrightarrow{\overline{\alpha}} & F_2 \bmod \mathfrak{m} \\ & {\scriptstyle \iota_1} \searrow \quad \swarrow {\scriptstyle \iota_2} & \\ & G & \end{array}$$

commutes.

We will also use the following:

Definition 4.1.2. F is said to be a *deformation* of G over A if F is a formal R-module over A such that reducing modulo $\mathfrak{m}$ (and identifying via $\jmath$) results in G. We say two deformations F_1 and F_2 over A are *isomorphic* if there exists an isomorphism $\alpha : F_1 \to F_2$ of formal R-modules which reduces to the identity map modulo $\mathfrak{m}$.

We will classify deformations up to isomorphisms, and this concept is the same no matter which definition we use. Given a deformation F in the sense of 4.1.2, (F, id) is a deformation in the sense of 4.1.1. Given a deformation (F, ι) in the sense of 4.1.1, we can lift $\iota \in \big(\widehat{R}^{\mathrm{nr}}/(\pi)\big)[\![X]\!]$ to a $\circ$-invertible element $\widetilde{\iota}$ of $A[\![X]\!]$, and then letting $\widetilde{F}$ be the image of F via $\widetilde{\iota}$, $(\widetilde{F}, \mathrm{id})$ is isomorphic to (F, ι) as deformations. These processes send isomorphic deformations to isomorphic deformations, and we now see that the two definitions of deformations up to isomorphism indeed agree.

Both definitions have advantages. Definition 4.1.2 treats fewer things as deformations, and this is an advantage in proving a general fact about deformations but it is a disadvantage whenever we want to show something is a deformation. So we will use both of these definitions in this chapter, using more convenient one for each occasion. We *always* deal with deformations up to isomorphism, so this should not cause any confusion.

We already have high hopes for classifying deformations in the present setting, because formal R-modules over $\widehat{R}^{\mathrm{nr}}/(\pi)$ are well-understood by Proposition 3.3.9 and Theorem 3.3.11, and deformations are supposed to be in some sense 'close' to these well-understood ones. Furthermore, the following makes this situation even better:

Proposition 4.1.3. *Suppose that a formal R-module F over A reduces to $\overline{F}$ over $A/\mathfrak{m}$ which has a finite height, and that F' is a formal R-module over A. Then the reduction modulo $\mathfrak{m}$ map $\mathrm{Hom}_R(F,F') \longrightarrow \mathrm{Hom}_R(\overline{F},\overline{F'})$ is injective.*

Proof. Because $\mathrm{Hom}_R(F,F') \longrightarrow \mathrm{Hom}_R(\overline{F},\overline{F'})$ is an abelian group homomorphism, we need to prove $\alpha \in \mathrm{Hom}_R(F,F')$ with $\overline{\alpha}=0$ implies $\alpha = 0$. If $\mathfrak{m}=0$, then we are done. Otherwise, suppose on the contrary that $\alpha \neq 0$, so there exists $i \geq 1$ such that $\alpha \equiv 0 \pmod{\mathfrak{m}^i}$ and $\alpha \not\equiv 0 \pmod{\mathfrak{m}^{i+1}}$. We then obtain a nonzero formal R-module homomorphism $\widetilde{\alpha}: \widetilde{F} \to \widetilde{F'}$ over $\widetilde{A} = A/\mathfrak{m}^{i+1}$ whose coefficients all lie inside $\mathfrak{m}^i$. As $(\mathfrak{m}^i)^2 = 0$, $\widetilde{\alpha}(\widetilde{F}(X,Y)) = \widetilde{F'}(\widetilde{\alpha}(X),\widetilde{\alpha}(Y)) = \widetilde{\alpha}(X)+\widetilde{\alpha}(Y)$ and $\widetilde{\alpha}([r]_{\widetilde{F}}(X)) = [r]_{\widetilde{F'}}(\widetilde{\alpha}(X)) = r\cdot\widetilde{\alpha}(X)$. Let $\widetilde{a} \in \widetilde{A}$ be a coefficient of $\widetilde{\alpha}$ which is nonzero. Since $\mathfrak{m}^i \subseteq \widetilde{A}$ is an $(A/\mathfrak{m})$-vector space, there exists an $(A/\mathfrak{m})$-linear map $f: \mathfrak{m}^i \to A/\mathfrak{m}$ which is nonzero at $\widetilde{a}$. Letting $\beta(X)$ denote $f_*(\widetilde{\alpha})(X)$, we see that $\beta \in (A/\mathfrak{m})[\![X]\!]$ is a nonzero formal R-module homomorphism from F modulo $\mathfrak{m}$ to the additive module $\widehat{\mathcal{G}}_{\mathrm{a}}$ over the field $A/\mathfrak{m}$, contradicting Proposition 3.3.8. □

In particular, if F_1 and F_2 are isomorphic deformations of a finite height G, then there exists a unique isomorphism of deformations between F_1 and F_2.

Our goal is the determination of the universal object, i.e. the universal deformation up to isomorphism. Before moving on, however, we will first develop some cohomology theory for formal R-modules to clarify proofs later.

4.1.1 Cohomology

In this subsection, we will prove a relationship between 'cohomology' and formal R-modules which differ from a fixed one by a power of the maximal ideal. Here, to simplify notation, we will assume that $A \in \mathscr{C}$ has the property that $\mathfrak{m}^{i+1}=0$ for some $i \geq 0$. We fix a formal R-module G over $\widehat{R}^{\mathrm{nr}}/(\pi)$ of finite height h.

Definition 4.1.4. A pair (Ξ,ξ) is said to be a 2-*cocycle* of G with coefficients in $\mathfrak{m}^i$ if $\Xi(X,Y) \in (X,Y) \subseteq \mathfrak{m}^i[\![X,Y]\!]$ and $\xi_r(X) \in (X) \subseteq \mathfrak{m}^i[\![X]\!]$ for each $r \in R$ satisfying the following five equations:

$$\begin{aligned}
\Xi(Y,Z)+\Xi(X,G(Y,Z)) &= \Xi(X,Y)+\Xi(G(X,Y),Z)\\
\Xi(X,Y) &= \Xi(Y,X)\\
\xi_r(X)+\xi_r(Y)+\Xi([r]_G(X),[r]_G(Y)) &= r\cdot\Xi(X,Y)+\xi_r(G(X,Y))\\
\xi_{r_1}(X)+\xi_{r_2}(X)+\Xi([r_1]_G(X),[r_2]_G(X)) &= \xi_{r_1+r_2}(X)\\
r_1\cdot\xi_{r_2}(X)+\xi_{r_1}([r_2]_G(X)) &= \xi_{r_1r_2}(X).
\end{aligned}$$

These equations make sense, since the different lifts of coefficients of G to A differ by $\mathfrak{m}$, which becomes negligible because the coefficients of Ξ and ξ are in $\mathfrak{m}^i$. We denote the set of all 2-cocycles by $Z^2(G,\mathfrak{m}^i)$. We say a pair (Ξ,ξ) is a 2-*coboundary* of G with coefficients in $\mathfrak{m}^i$ if there exists $\varphi \in \mathfrak{m}^i[\![X]\!]$ such that

$$\Xi(X,Y) = \varphi(G(X,Y))-\varphi(X)-\varphi(Y) \quad \text{and} \quad \xi_r(X) = \varphi([r]_G(X))-r\cdot\varphi(X).$$

These make sense for the same reasoning, and we denote the set of all 2-coboundaries $d(\varphi)$ by $B^2(G,\mathfrak{m}^i)$.

Note that $Z^2(G,\mathfrak{m}^i)$ and $B^2(G,\mathfrak{m}^i)$ form $A/\mathfrak{m}$-vector spaces. Also, by direct computation using formal R-module conditions on G, one can check that every 2-coboundary is a 2-cocycle. Thus, we can define the 2-cohomology $H^2(G,\mathfrak{m}^i)$ to be the $A/\mathfrak{m}$-vector space $Z^2(G,\mathfrak{m}^i)/B^2(G,\mathfrak{m}^i)$.

Recall that in the definition of the usual cohomology of a group G with coefficients in a G-module M, $\Xi: G\times G \to M$ is a 2-cocycle if it satisfies $g_0\cdot\Xi(g_1,g_2)+\Xi(g_0,g_1g_2) = \Xi(g_0g_1,g_2)+\Xi(g_0,g_1)$ and Ξ is a 2-coboundary if there exists $\varphi: G\to M$ such that $\Xi(g_0,g_1) = \varphi(g_0g_1)-g_0\cdot\varphi(g_1)-\varphi(g_0)$. Thus, the first

equations for the definition of both cocycle and coboundary really are cohomological conditions, when we view the formal module G as giving the 'group structure' and take the trivial action of the variables X, Y, Z.

We get the equations of Definition 4.1.4 by 'linear approximation' of differences between formal R-modules. We will see this more specifically in the proof of the following proposition, which links cohomology with coefficients in $\mathfrak{m}^i$ with isomorphic deformations up to $\mathfrak{m}^i$. By $(\partial_1 F)(X,Y)$, we mean the formal partial derivative of $F(X,Y)$ with respect to X, i.e. given $F(X,Y) = \sum a_{ij}X^iY^j$, $(\partial_1 F)(X,Y) = \sum i a_{ij}X^{i-1}Y^j$. Note that $(\partial_1 F)(0,Y)$ starts from the constant term 1, so it is invertible with the usual multiplication in $A[\![Y]\!]$ (not $\circ$-invertibility here). We have an analogue of [19, Proposition 2.4]:

Proposition 4.1.5. *Let $i \geq 1$. Suppose F_1 and F_2 are two deformations of G over A, and suppose $\alpha \in A[\![X]\!]$ is such that $\overline{\alpha} \in (A/\mathfrak{m})[\![X]\!]$ is X, $\alpha(F_1(X,Y)) \equiv F_2(\alpha(X),\alpha(Y)) \pmod{\mathfrak{m}^i}$, and $\alpha([r]_{F_1}(X)) \equiv [r]_{F_2}(\alpha(X)) \pmod{\mathfrak{m}^i}$ for all $r \in R$. Using usual multiplication in power series rings,*

$$\Xi(X,Y) = \frac{\alpha(F_1(X,Y)) - F_2(\alpha(X),\alpha(Y))}{(\partial_1 G)(0,G(X,Y))}$$
$$\xi_r(X) = \frac{\alpha([r]_{F_1}(X)) - [r]_{F_2}(\alpha(X))}{(\partial_1 G)(0,G(X,Y))}$$

defines $\Xi \in \mathfrak{m}^i[\![X,Y]\!]$ and $\xi_r \in \mathfrak{m}^i[\![X]\!]$, and further (Ξ,ξ) is a 2-cocycle. Moreover, $(\Xi,\xi) \in B^2(G,\mathfrak{m}^i)$ if and only if there exists $\beta \in A[\![X]\!]$ such that $\beta \equiv \alpha \pmod{\mathfrak{m}^i}$ and $\beta(F_1(X,Y)) = F_2(\beta(X),\beta(Y))$ in $A[\![X,Y]\!]$.

Proof. Since the numerators of the expressions for Ξ and ξ are in $\mathfrak{m}^i$, the other coefficients only matter modulo $\mathfrak{m}$, so the expressions for Ξ and ξ make sense and create elements in $\mathfrak{m}^i[\![X,Y]\!]$ and $\mathfrak{m}^i[\![X]\!]$, respectively. For any formal R-module F, by differentiating $F(X,F(Y,Z)) = F(F(X,Y),Z)$ with respect to X and then evaluating at $X=0$, we obtain $(\partial_1 F)(0,F(Y,Z)) = (\partial_1 F)(Y,Z)\cdot(\partial_1 F)(0,Z)$ by the 'chain rule.' Also, $F(X+Y,Z) \equiv F(X,Z) + (\partial_1 F)(X,Z)\cdot Y \pmod{Y^2}$. Using these identities and noting that product of elements in $\mathfrak{m}^i$ are 0 (so we are 'linear approximating') and that coefficients matter only modulo $\mathfrak{m}$ whenever an $\mathfrak{m}^i$-valued coefficient is present, we have

$$\begin{aligned}
\alpha(F_1(F_1(X,Y),Z)) &= F_2\big(\alpha(F_1(X,Y)),\alpha(Z)\big) \;+\; \Xi(F_1(X,Y),Z)\cdot(\partial_1 G)\big(0,\; G(F_1(X,Y),Z)\big)\\
&= F_2\Big(F_2(\alpha(X),\alpha(Y)) + \Xi(X,Y)\cdot(\partial_1 G)(0,G(X,Y)),\;\; \alpha(Z)\Big)\\
&\qquad + \Xi(G(X,Y),Z)\cdot(\partial_1 G)\big(0,G(G(X,Y),Z)\big)\\
&= F_2\Big(F_2\big(\alpha(X),\alpha(Y)\big),\alpha(Z)\Big) \;+ (\partial_1 G)\big(G(X,Y),Z\big)\cdot\Xi(X,Y)\cdot(\partial_1 G)(0,G(X,Y))\\
&\qquad + \Xi(G(X,Y),Z)\cdot(\partial_1 G)\big(0,G(G(X,Y),Z)\big)\\
&= G\big(G(\alpha(X),\alpha(Y)),\alpha(Z)\big) + (\partial_1 G)\big(0,G(G(X,Y),Z)\big)\cdot\Big(\Xi(X,Y)+\Xi(G(X,Y),Z)\Big).
\end{aligned}$$

By symmetry, we get the first identity for a cocycle. Other relations can be similarly proved.

If $(\Xi,\xi) = d(\varphi)$ for some $\varphi \in \mathfrak{m}^i[\![X]\!]$, we can define $\beta(X) = \alpha(X) + (\partial_1 G)(0,X)\cdot\varphi(X)$; conversely given β with $\beta \equiv \alpha \pmod{\mathfrak{m}^i}$, we can solve for $\varphi \in \mathfrak{m}^i[\![X]\!]$ satisfying the same equation. For these β and φ, one can show by a similar technique that

$$(\partial_1 G)\big(0,G(X,Y)\big)\cdot\Xi(X,Y) = \psi(F_1(X,Y)) - F_2(\psi(X),\psi(Y)) + (\partial_1 G)(0,X)\cdot(\varphi(X)+\varphi(Y)-\varphi(G(X,Y)))$$
$$(\partial_1 G)\big(0,[r]_G(X)\big)\cdot\xi_r(X) = \psi([r]_{F_1}(X)) - [r]_{F_2}(\psi(X)) + \varphi([r]_G(X)) - r\cdot\varphi(X).$$

Thus, the last statement is now proved. □

Since cohomology can be viewed as the 'first approximation' of the difference between formal R-modules, we can use the 'successive approximation' results from Section 3.3:

Proposition 4.1.6. *Let $i \geq 0$. Suppose $(\Xi,\xi) \in Z^2(G,\mathfrak{m}^i)$ such that $(\Xi,\xi) \equiv 0 \pmod{\text{poly. deg. } n}$. Then there exists $a \in A$ such that*

$$(\Xi,\xi) \equiv \begin{cases} \Big(a\big((X+Y)^n - X^n - Y^n\big),\, (r^n - r)\cdot aX^n\Big) & n \text{ is not a power of } q\\ \Big(\frac{p}{\pi}\cdot aC_n(X,Y),\, \frac{r^n-r}{\pi}\cdot aX^n\Big) & n \text{ is a power of } q \end{cases} \pmod{\text{poly. deg. } n+1}.$$

Proof. Fix a deformation F over A of G, and define $H(X,Y) = F(\Xi(X,Y),F(X,Y))$ and $[r]_H(X) = F(\xi_r(X),[r]_F(X))$. We can check that the cocycle conditions are exactly those necessary for $(H,[\ ]_H)$ to be a formal R-module germ of degree $n+1$ (by the similar arguments as the beginning of the proof of Theorem 2.2.1). But Corollary 3.3.3 tells us that H arises from a formal R-module $\widetilde{H}$ over A, so Proposition 3.3.4 and $(\widetilde{H},[r]_{\widetilde{H}}) \equiv (H,[r]_H) \equiv (F,[r]_F) + (\Xi,\xi_r)$ (mod poly. deg. $n+1$) give us the desired result. □

4.1.2 Universal Deformation

Theorem 4.1.7. *Suppose G is a formal R-module over $\widehat{R}^{\mathrm{nr}}/(\pi)$ of height h. The functor from $\mathscr{C}$ to* **Set** *defined by $A \rightsquigarrow$ the set of deformations of G over A up to isomorphism is represented by $\widehat{R}^{\mathrm{nr}}[\![\beth_1,\dots,\beth_{h-1}]\!]$, the power series ring in $h-1$ variables. If G is π-normal, the universal deformation F^{univ} can be chosen to have the property that the coefficient of X^{q^j} in $[\pi]_{F^{\mathrm{univ}}}(X)$ is equal to $(\pi^{q^j-1}-1)\cdot\beth_j$ for all $1 \le j \le h-1$.*

Proof. By Theorem 3.3.11, there exists a formal R-module isomorphism $\beta : G \to G^{\mathrm{nor}}$ over $\widehat{R}^{\mathrm{nr}}/(\pi)$ where G^{nor} is π-normal of height h, so given a deformation (F,ι) of G, $(F,\beta\circ\iota)$ is a deformation of G^{nor}, preserveing isomorphism classes. Therefore, once we prove that $(F^{\mathrm{univ}},\iota^{\mathrm{univ}})$ defined over $\widehat{R}^{\mathrm{nr}}[\![\beth_1,\dots,\beth_{h-1}]\!]$ is a universal object for the above functor for G^{nor}, $(F^{\mathrm{univ}},\beta^{-1}\circ\iota^{\mathrm{univ}})$ is a universal object for the functor for G. Thus, we can assume that G is normal, so the corresponding R-algebra homomorphism $g : \Lambda_R = R[\Upsilon_1,\dots] \to \widehat{R}^{\mathrm{nr}}/(\pi)$ (obtained from Theorem 3.3.2) sends $\Upsilon_i \mapsto 0$ for all $i < q^h-1$. For the rest of the proof, we will be dealing with deformations in the sense of Definition 4.1.2.

Let us define the R-algebra homomorphism $f^{\mathrm{univ}} : R[\Upsilon_1,\dots,] \to \widehat{R}^{\mathrm{nr}}[\![\beth_1,\dots,\beth_{h-1}]\!]$ by

$$\begin{aligned} f^{\mathrm{univ}}(\Upsilon_{q^i-1}) &= \beth_i && 1 \le i \le h-1 \\ f^{\mathrm{univ}}(\Upsilon_j) &= 0 && 1 \le j < q^h-1 \text{ and } j+1 \text{ not a power of } q \\ f^{\mathrm{univ}}(\Upsilon_j) &= \text{a lift of } g(\Upsilon_j) \text{ to } \widehat{R}^{\mathrm{nr}} && \text{otherwise.} \end{aligned}$$

Let F^{univ} be the corresponding formal R-module over $\widehat{R}^{\mathrm{nr}}[\![\beth_1,\dots,\beth_{h-1}]\!]$. Since Λ_R is the universal formal R-module, F^{univ} is a deformation of G by construction. Also, note that by chasing constructions in Propositions 3.1.2, 3.3.1, and 3.3.2, we can choose the universal formal R-module so that Υ_{q^j-1} is sent to $(\pi^{q^j-1}-1)^{-1}\Theta_{q^j,\pi}$ in Λ_R. In other words, in this case, we know that the coefficient of X^{q^j} in $[\pi]_{F^{\mathrm{univ}}}(X)$ is $(\pi^{q^j-1}-1)\beth_j$.

We will now show that F^{univ} is a universal object. In other words, given a deformation F of G over A, we will show the existence and uniqueness of a local $\widehat{R}^{\mathrm{nr}}$-algebra map $f : \widehat{R}^{\mathrm{nr}}[\![\beth_1,\dots,\beth_{h-1}]\!] \to A$ such that F is isomorphic to $f_*(F^{\mathrm{univ}})$ as deformations.

Suppose that for each $i \ge 1$, we have proven

$$\begin{aligned} &\text{There exists a unique local } \widehat{R}^{\mathrm{nr}}\text{-algebra map } f^{(i)} : \widehat{R}^{\mathrm{nr}}[\![\beth_1,\dots,\beth_{h-1}]\!] \to A/\mathfrak{m}^i \text{ such that} \\ &\qquad f^{(i)}_*(F^{\mathrm{univ}}) \cong \overline{F} \text{ as deformations of } G \text{ over } A/\mathfrak{m}^i. \end{aligned} \tag{4.1}$$

By Proposition 4.1.3, there exists a unique isomorphism $\alpha^{(i)} : \overline{F} \to f^{(i)}_*(F^{\mathrm{univ}})$ of deformations over $A/\mathfrak{m}^i$ for each i. Reducing $\alpha^{(i)}(F(X,Y)) = f^{(i)}_*(F^{\mathrm{univ}})(\alpha^{(i)}(X),\alpha^{(i)}(Y))$ mod $\mathfrak{m}^{i-1}$ and using uniqueness of $f^{(i-1)}$ and $\alpha^{(i-1)}$, we see that $f^{(i)}$ and $\alpha^{(i)}$ are compatible with the inverse system $\{A/\mathfrak{m}^i\}$. Thus, by completeness of A, we obtain a unique local $\widehat{R}^{\mathrm{nr}}$-algebra map $f : \widehat{R}^{\mathrm{nr}}[\![\beth_1,\dots,\beth_{h-1}]\!] \to A$ and $\alpha \in A[\![X]\!]$ such that $f_*(F^{\mathrm{univ}})$ is isomorphic to F via α, finishing the proof.

We will prove (4.1) by induction on i. When $i=1$, the only way to get $f^{(i)}$ to be a homomorphism is by sending all $\beth_j$ to 0. Since this is same as reducing modulo the maximal ideal, this $f^{(i)}$ works with the identity isomorphism.

So suppose that we have proved (4.1) until i. For the rest of the proof, it is helpful think of $F^{\mathrm{univ}}(X,Y)$ and $[r]_{F^{\mathrm{univ}}}(X)$ as $F^{\mathrm{univ}}(\beth_1,\dots,\beth_{h-1})(X,Y)$ and $[r]_{F^{\mathrm{univ}}}(\beth_1,\dots,\beth_{h-1})(X)$. For the $i+1$ step of (4.1), we may assume $\mathfrak{m}^{i+1}=0$ and prove existence and uniqueness of $m^{(i+1)} = (m_1^{(i+1)},\dots,m_{h-1}^{(i+1)}) \in \mathfrak{m}^{\oplus(h-1)}$ such that the formal R-module $\left(F^{\mathrm{univ}}(m^{(i+1)})(X,Y),\ [r]_{F^{\mathrm{univ}}}(m^{(i+1)})(X)\right)$ is isomorphic to F, assuming by induction that there exists $m^{(i)} = (m_1^{(i)},\dots,m_{h-1}^{(i)}) \in \mathfrak{m}^{\oplus(h-1)}$ (defined by an arbitrary lift of the solution

from step i) such that the above isomorphism holds modulo $\mathfrak{m}^i$ with $m^{(i)}$ unique modulo $\mathfrak{m}^i$. By uniqueness at step i, what we need to show is the existence and the uniqueness of $\delta = (\delta_1, \dots, \delta_{h-1}) \in (\mathfrak{m}^i)^{\oplus(h-1)}$ such that the formal R-module $\left(F^{\mathrm{univ}}(m^{(i)}+\delta)(X,Y),\ [r]_{F^{\mathrm{univ}}}(m^{(i)}+\delta)(X)\right)$ is isomorphic to F.

Suppose $\alpha^{(i)} \in A[\![X]\!]$ is a lift of the isomorphism obtained in the i-th step, so that we have $\alpha^{(i)}(F(X,Y)) \equiv F^{\mathrm{univ}}(m^{(i)})(\alpha^{(i)}(X), \alpha^{(i)}(Y))\ (\mathrm{mod}\ \mathfrak{m}^i)$ and similar statements concerning each $[r](X)$. These equations still hold when we use $F^{\mathrm{univ}}(m^{(i)}+\delta)(\alpha^{(i)}(X),\ \alpha^{(i)}(Y))$ on the RHS, so by Proposition 4.1.5, we obtain a cocycle $(\Xi^{(\delta)}, \xi^{(\delta)})$ by

$$\Xi^{(\delta)}(X,Y) = \frac{\alpha^{(i)}(F(X,Y)) - F^{\mathrm{univ}}(m^{(i)}+\delta)(\alpha^{(i)}(X), \alpha^{(i)}(Y))}{(\partial_1 G)(0, G(X,Y))}$$
$$\xi^{(\delta)}(X) = \frac{\alpha^{(i)}([r]_F(X)) - [r]_{F^{\mathrm{univ}}}(m^{(i)}+\delta)(\alpha^{(i)}(X))}{(\partial_1 G)(0, [r]_G(X))}.$$

Since $(\mathfrak{m}^i)^2 = 0$, linear approximation is exact, so

$$F^{\mathrm{univ}}(m^{(i)}+\delta)(\alpha^{(i)}(X), \alpha^{(i)}(Y)) = F^{\mathrm{univ}}(m^{(i)})(\alpha^{(i)}(X), \alpha^{(i)}(Y)) + \sum_j \frac{\partial F^{\mathrm{univ}}}{\partial \beth_j}(m^{(i)})(\alpha^{(i)}(X), \alpha^{(i)}(Y))\delta_j$$
$$[r]_{F^{\mathrm{univ}}}(m^{(i)}+\delta)(\alpha^{(i)}(X)) = [r]_{F^{\mathrm{univ}}}(m^{(i)})(\alpha^{(i)}(X)) + \sum_j \frac{\partial [r]_{F^{\mathrm{univ}}}}{\partial \beth_j}(m^{(i)})(\alpha^{(i)}(X))\delta_j.$$

$\delta_j \in \mathfrak{m}^i$ implies that in the above equation, we need to look at other coefficients inside the sum modulo $\mathfrak{m}$, so combining with $\overline{\alpha^{(i)}} = X$ and $m = \overrightarrow{0}$ modulo $\mathfrak{m}$ (we know this from induction), we conclude

$$\Xi^{(0)}(X,Y) - \Xi^{(\delta)}(X,Y) = \sum_j \frac{\overline{\frac{\partial F^{\mathrm{univ}}}{\partial \beth_j}}(0)(X,Y)}{(\partial_1 G)(0, G(X,Y))}\delta_j \tag{4.2}$$
$$\xi^{(0)}(X) - \xi^{(\delta)}(X) = \sum_j \frac{\overline{\frac{\partial [r]_{F^{\mathrm{univ}}}}{\partial \beth_j}}(0)(X)}{(\partial_1 G)(0, [r]_G(X))}\delta_j.$$

Claim.

$$(\Xi_j, \xi_j) = \left(\frac{\overline{\frac{\partial F^{\mathrm{univ}}}{\partial \beth_j}}(0)(X,Y)}{(\partial_1 G)(0, G(X,Y))},\ \frac{\overline{\frac{\partial [r]_{F^{\mathrm{univ}}}}{\partial \beth_j}}(0)(X)}{(\partial_1 G)(0, [r]_G(X))} \right)$$

is a cocycle with coefficients in $\widehat{R}^{\mathrm{nr}}/(\pi)$ (so $i = 0$ case of Section 4.1.1) for each $j = 1, \dots, h-1$, and they form a basis of the cohomology.

Proof. Let us apply Proposition 4.1.5 with $\overline{k}[\epsilon]/\epsilon^2$ as the ring, $i = 1$, identity as the isomorphism mod the maximal, and $\overline{F^{\mathrm{univ}}(0)}(X,Y)$ and $F_j = \overline{F^{\mathrm{univ}}(0, \dots, 0, \epsilon, 0, \dots, 0)}(X,Y)$ with ϵ in the j-th spot as formal R-modules (without the bar, these formal modules are defined over $\widehat{R}^{\mathrm{nr}}$ by definition, so no $\beth$ terms exist even before modding out). Since $\epsilon^2 = 0$, the linear approximation is precise, so

$$F_j = \overline{F^{\mathrm{univ}}(0)}(X,Y) + \overline{\frac{\partial F^{\mathrm{univ}}}{\partial \beth_j}}(0)(X,Y)\epsilon$$

and similarly for $[r]$, so by Proposition 4.1.5, $\epsilon(\Xi_j, \xi_j)$ is a cocycle with coefficients in $\overline{k}[\epsilon]/\epsilon^2$. Therefore, we see that (Ξ_j, ξ_j) is a cocycle over $\bar{k}$. As noted above, Υ_{q^j-1} is sent to $(\pi^{q^j-1}-1)^{-1}$ times the coefficient of X^{q^j} in $[\pi]_{F^{\mathrm{univ}}}(X)$. So in this case,

$$\overline{\frac{\partial [\pi]_{F^{\mathrm{univ}}}}{\partial \beth_j}}(0)(X) \equiv (\pi^{q^j-1}-1)^{-1} X^{q^j} \not\equiv 0 \quad (\mathrm{mod\ poly.\ deg.}\ q^j+1).$$

In particular, by Proposition 4.1.6, $(\Xi_j,\, \xi_j) \equiv (\frac{p}{\pi}\cdot a'_j C_n(X,Y), \frac{r^n-r}{\pi}\cdot a'_j X^n)$ with a'_j invertible in $\widehat{R}^{\mathrm{nr}}/(\pi)$.

Now we are ready to prove that these form a basis of the cohomology. If $\sum \lambda_j(\Xi_j,\xi_j) = 0$, then using $\overline{\frac{\partial[\pi]_{F^{\mathrm{univ}}}}{\partial \beth_j}}(0)(X) \equiv 0 \pmod{\text{poly. deg. } q^j}$ and $\not\equiv 0 \pmod{\text{poly. deg. } q^j+1}$ for each j, we get $\lambda_j = 0$ by induction. For span, let us prove by induction that a cocycle $(\Xi,\xi) \equiv \sum \lambda_j(\Xi_j,\xi_j) + d(\varphi_{n-1}) \pmod{\text{poly. deg. } n}$. The $n=1$ case is automatic, so suppose we have done up to n. If n is not a power of q, then by Proposition 4.1.6,

$$\begin{aligned}(\Xi,\, \xi) &\equiv \sum \lambda_j(\Xi_j,\, \xi^{(j)}) + d(\varphi_{n-1}) + \Big(a\cdot((X+Y)^n - X^n - Y^n),\ a\cdot(r^n-r)X^n\Big)\\ &= \sum \lambda_j(\Xi_j,\, \xi_j) + d(\varphi_{n-1} + X^n) \pmod{\text{poly. deg. } n+1}.\end{aligned}$$

If $n = q^1,\dots,q^{h-1}$, then Proposition 4.1.6 and invertibility of a'_j show what we need. Suppose now $n = q^i$ for $i \geq h$. We can write $G(X,Y) \equiv X+Y+\frac{p}{\pi}\cdot a'' C_{q^h}(X,Y) \pmod{\text{poly. deg. } q^h+1}$ and $[r]_G(X) \equiv rX + \frac{r^{q^h}-r}{\pi}\cdot a'' X^{q^h} \pmod{\text{poly. deg. } q^h+1}$ by Proposition 3.3.4. Working modulo polynomial degree q^i+1,

$$\begin{aligned}d(X^{q^{i-h}}) &\equiv \Big(\frac{p}{\pi}\cdot (a'')^{q^i} C_{q^h}(X^{q^{i-h}}, Y^{q^{i-h}}),\ \ \frac{r^{q^i}-r}{\pi}\cdot (a'')^{q^i} X^{q^i}\Big)\\ &= \Big(\frac{p}{\pi}\cdot (a'')^{q^i} C_{q^i}(X,Y),\ \ \frac{r^{q^i}-r}{\pi}\cdot (a'')^{q^i} X^{q^i}\Big),\end{aligned}$$

because elements in $R/(\pi)$ are fixed under taking q-th powers and $C_{q^h}(X^{q^{i-h}}, Y^{q^{i-h}}) = C_{q^i}(X,Y)$ (see the proof of the claim in Proposition 2.2.2). Thus, we are done by Proposition 4.1.6. □

Now, because $\mathfrak{m}^i$ is an $A/\mathfrak{m}$-vector space, (4.2) and the above claim show the existence and uniqueness of δ such that $(\Xi^{(\delta)}(X,Y), \xi^{(\delta)}(X))$ is zero as an element in the cohomology. Therefore, by Proposition 4.1.5, we obtain (4.1). □

By this theorem, we now know that there is only one deformation class of height 1 over any $A \in \mathscr{C}$. This fact will be important in our application to local class field theory (Section 5.1). Also, if G is a π-normal formal R-module of height h over $\widehat{R}^{\mathrm{nr}}/(\pi)$, two deformations F_1 and F_2 of G over A are isomorphic if and only if $[\pi]_{F_1}(X)$ and $[\pi]_{F_2}(X)$ agree on the coefficients of $X, X^q, \dots, X^{q^{h-1}}$. This is an extremely convenient way of checking for isomorphic deformations.

4.2 Deformations With Level Structure

In this section, we consider deformations with level structure. As mentioned in the introduction, Drinfel'd's used analogues of elliptic curves and modular curves to prove analogues of the Fundamental Theorem of Complex Multiplication and the Langlands Conjecture for global function fields ($d = 1, 2$). Just as we have modular curves $X_1(n)$ for each level n in the case of elliptic curves, Drinfel'd creates modular varieties for each level structure (which he defines) on Drinfel'd modules. The level structure on formal modules discussed in this section is the one coming from the level structure on Drinfel'd modules via the process of going from the 'global' moduli problem to the 'local' deformation theory, so the result in this section is the 'local' version of the moduli problem of Drinfel'd modules with level structure.

Coming up with the appropriate level structure on formal modules was one of the many great insights of Drinfel'd's in [5]. A naive notion of level structure on a formal R-module F over $A \in \mathscr{C}$ with $\mathrm{ht}(\overline{F}) = h$ can be given by an R-module homomorphism

$$\varphi : \big(\pi^{-n}R/R\big)^h \longrightarrow F(\mathfrak{m}_A)$$

which is an isomorphism with the π^n-torsion in $F(\mathfrak{m}_A)$. But this does not work very well. For example, if we take F to be the $\mathbb{Z}_p$-module $\widehat{\mathbb{G}}_{\mathrm{m}}$ over a field of characteristic p, then we can check by induction that $[p](X) = X^p$, i.e. it is height 1. It is clear that there is no level structure (according to the above definition) on this $\mathbb{Z}_p$-module $\widehat{\mathbb{G}}_{\mathrm{m}}$. Drinfel'd's great idea was to define a level structure to be just a homomorphism but with the additional condition that $[\pi](X)$ to be a unit multiple of $\prod(X - \varphi(s))$, where s runs through $\left(\pi^{-1}R/R\right)^h$. This makes the zero homomorphism a level n structure of the $\mathbb{Z}_p$-module $\widehat{\mathbb{G}}_{\mathrm{m}}$ over a field of characteristic p for any n.

Our goal of the section is determination of the universal deformation ring with level n structure. After we determine the universal deformation with level structure, we will be able to explicitly see what Drinfel'd's definition of level-n structure captures (Example 4.2.6).

As before, assume that G is a formal R-module over $\widehat{R}^{\mathrm{nr}}/(\pi)$ of finite height h, and that $A \in \mathscr{C}$ with maximal ideal $\mathfrak{m}$.

Definition 4.2.1. Let $n \geq 1$. For a formal R-module F over A, a structure of level n on F is an R-module homomorphism $\varphi : \left(\pi^{-n}R/R\right)^h \to F(\mathfrak{m})$ such that the monic polynomial of degree q^h

$$P_\varphi(X) = \prod_{s \in (\pi^{-1}R/R)^h} (X - \varphi(s))$$

divides $[\pi]_F(X)$.

In this case, reducing $[\pi]_F(X) = g(X) \cdot P_\varphi(X)$ modulo $\mathfrak{m}$, we obtain $X^{q^h} \cdot \mathrm{unit} = \overline{g}(X) \cdot X^{q^h}$ in $(A/\mathfrak{m})[\![X]\!]$. Therefore, $[\pi]_F(X)$ and P_φ are unit multiples of each other.

If α is an isomorphism and φ is structure of level n for a formal R-module F ($n \geq 1$), then $\alpha \circ \varphi$ does define a level structure for the image of F via α. Indeed,

$$\prod_{(\pi^{-1}R/R)^h} (X - \alpha(\varphi(s)))\Bigg| \alpha \circ [\pi]_F \circ \alpha^{-1} \iff \prod_{(\pi^{-1}R/R)^h} \Big(\alpha(X) - \alpha(\varphi(s))\Big)\Bigg| \alpha \circ [\pi]_F,$$

and noting that $\alpha(X) - \alpha(\varphi(s)) = (X - \varphi(s)) \cdot \mathrm{unit}$ (because α is an isomorphism and $\varphi(s) \in \mathfrak{m}$), we are done.

Definition 4.2.2. A *deformation of G of level 0 over A* simply refers to a deformation F of G over A. For $n \geq 1$, a *deformation of G of level n over A* is a pair (F, φ), where F is a deformation of G over A (in the sense of Definition 4.1.2) and φ is a structure of level n on F.

Two deformations (F_1, φ_1) and (F_2, φ_2) of G of level n over A to are said to be *isomorphic* if there exists an isomorphism $\alpha : F_1 \to F_2$ as deformations such that $\left(\pi^{-n}R/R\right)^h \xrightarrow{\varphi_1} F_1(\mathfrak{m}) \xrightarrow{\alpha} F_2(\mathfrak{m})$ is φ_2.

As in Section 4.1, we can also define a deformation of level n as a triple (F, ι, φ), where ι is the isomorphism identifying F modulo $\mathfrak{m}$ with G, and define the isomorphic deformations by a commutative diagram as in Definition 4.1.1. By lifting the isomorphism over $\widehat{R}^{\mathrm{nr}}/(\pi)$ to that over A, we again see that these two definitions agree when we discuss deformations up to isomorphism.

When $A = \widehat{R}^{\mathrm{nr}}/(\pi)$, there is only one homomorphism $\left(\pi^{-n}R/R\right)^h \to F(\mathfrak{m})$, namely the zero map. This is indeed a level structure, since we are assuming that the height of G is h. Because of unicity of level structure in this case, we do not need to specify in Definition 4.2.2 what the level structure φ over A becomes over the residue field (cf. Definition 4.3.3).

The goal is the determination of the universal object of the functor which associates $A \in \mathscr{C}$ to the set of deformations of G of level n over A up to isomorphisms. Before launching into this discussion, we will digress a little and discuss properties of power series over $A \in \mathscr{C}$.

Proposition 4.2.3. (1) *$\alpha \in A[\![X]\!]$ such that $\alpha \equiv X^\nu \pmod{\mathfrak{m}}$ for some ν. Then we can write $\alpha(X) = \beta(X)\gamma(X)$, where $\beta(X)$ is a monic polynomial of degree ν, $\gamma(X)$ is a unit in $A[\![X]\!]$, and $\beta \equiv X^\nu$ and $\gamma \equiv 1$ modulo $\mathfrak{m}$.*

(2) *If $\beta(X)$ is a monic polynomial of degree ν such that $\beta \equiv X^\nu \pmod{\mathfrak{m}}$, then $A' = A[\![X]\!]/(\beta(X))$ is a finite free A-module with basis $1, X, \ldots, X^{\nu-1}$.*
(3) *If $\alpha \in A[\![X]\!]$ such that $\alpha(m) = 0$ for some $m \in \mathfrak{m}$, then $\alpha(X)$ is a product of $(X-m)$ and another power series.*

Proof. (1) Starting from $\beta_1(X) = X^\nu$ and $\gamma_1(X) = 1$, we create monic polynomials $\{\beta_i(X)\}$ of degree ν and power series $\{\gamma_i(X)\}$, such that $\beta_{i+1} - \beta_i \in \mathfrak{m}^i[\![X]\!]$, $\gamma_{i+1} - \gamma_i \in \mathfrak{m}^i[\![X]\!]$, and $\alpha \equiv \beta_i \cdot \gamma_i \pmod{\mathfrak{m}^i}$. If we have constructed until the i-th step, then define

$$\beta_{i+1} = \beta_i + \widetilde{\beta}, \quad \text{and} \quad \gamma_{i+1} = \gamma_i + \frac{\alpha - \beta_i\gamma_i - \widetilde{\beta}\gamma_i}{X^\nu},$$

where $\widetilde{\beta}$ is the polynomial obtained by taking up to degree $\nu - 1$ of the power series $\frac{\alpha - \beta_i\gamma_i}{\gamma_i}$.
(2) Suppose $\beta(X) = X^\nu + \widetilde{\beta}(X)$, so that $\widetilde{\beta}$ has coefficients in $\mathfrak{m}$. Then $X^\nu = -\widetilde{\beta}(X)$ in A'. Thus, for $i \geq \nu$, if we can write X^i in terms of $1, \ldots, X^{\nu-1}$ with coefficients in $\mathfrak{m}^j$, then we can write X^{i+1} in terms of $1, \ldots, X^{\nu-1}$ with coefficients in $\mathfrak{m}^j$. Moreover, $X^{j\nu}$ can be written with coefficients in $\mathfrak{m}^j$, so it now follows that any power series in $A[\![X]\!]$ can be spanned by these ν elements, using completeness of A. For linear independence, if a polynomial of degree strictly less than ν can be written as $\beta(X)\gamma(X)$, then modding out by $\mathfrak{m}$, we see that $\gamma \equiv 0 \pmod{\mathfrak{m}}$. Plugging this back in and writing $\beta(X) = \widetilde{\beta}(X) + X^\nu$, we then obtain $\gamma \equiv 0 \pmod{\mathfrak{m}^2}$. We can continue by induction.
(3) Writing $\alpha = \sum a_i X^i$, $\alpha(X) = \alpha(X) - \alpha(a) = a_1(X-a) + a_2(X-a)(X+a) + a_3(X-a)(X^2+aX+a^2) + \cdots$, where the coefficient of X^i on the RHS converges for each i. □

Now we are ready to determine the universal deformation of level n. For convenience, let $e_1, \ldots, e_h$ denote the standard $R/(\pi^n)$-module basis of $(\pi^{-n}R/R)^h$, and let $D_0 = \widehat{R}^{\mathrm{nr}}[\![\beth_1, \ldots, \beth_{h-1}]\!]$ be the universal deformation ring. As a piece of notation, let $\beth_0 = \pi \in \widehat{R}^{\mathrm{nr}}$.

Theorem 4.2.4. *A universal element of the functor which sends $A \in \mathscr{C}$ to the set of deformations of G of level n over A up to isomorphism is given by $(F_n^{\mathrm{univ}}, \varphi_n^{\mathrm{univ}})$ defined over a regular local ring $D_{h,n} \in \mathscr{C}$. For $n \geq 1$, $\varphi_n^{\mathrm{univ}}$ is injective, and the images of e_i's under $\varphi_n^{\mathrm{univ}}$ form a system of local parameters of $D_{h,n}$. Further, the natural homomorphism $D_{h,n} \to D_{h,n+1}$ (obtained from Yoneda's lemma) is finite and flat.*

Proof. By the same argument as in the proof of Theorem 4.1.7, we may assume that G is a π-normal formal R-module of height h. The case when $n = 0$ was completely done in Theorem 4.1.7. Because the condition of $P_\varphi(X) \mid [\pi]_F$ only involves looking at $s \in \left(\pi^{-1}R/R\right)^h$, $n = 1$ turns out to be the main case of this theorem. Note that a D_0-algebra $A \in \mathscr{C}$ corresponds to (an isomorphism class representative of) a deformation F_A of G over A.

Lemma 4.2.5. *Let $j = 0, \ldots, h$. The universal object of the functor which sends a D_0-algebra $A \in \mathscr{C}$ to the set of R-module homomorphisms $\varphi : \left(\pi^{-1}R/R\right)^j \to F_A(\mathfrak{m}_A)$ satisfying*

$$P_{j,\varphi}(X) = \prod_{s \in (\pi^{-1}R/R)^j} (X - \varphi(s)) \,\Bigg|\, [\pi]_{F_A}(X) \tag{4.3}$$

is $(L_j, \varphi_{j,1}^{\mathrm{univ}})$, where $\varphi_{j,1}^{\mathrm{univ}}$ is injective and L_j is a regular local ring with a system of parameters given by $\varphi_{j,1}^{\mathrm{univ}}(e_1), \ldots, \varphi_{j,1}^{\mathrm{univ}}(e_j)$ in L_j together with images of $\beth_j, \ldots, \beth_{h-1}$. The natural map $L_{j-1} \to L_j$ is finite and flat for all $j = 1, \ldots, h$.

Proof. Observe first that this functor is well-defined, since the condition (4.3) does not depend on the representative of the deformation class. When $j = 0$, only the zero homomorphism works as φ, so $L_0 = D_0$ and $\varphi_{1,0}^{\mathrm{univ}} = 0$. Suppose that the lemma has been proved up to j, $0 \leq j < h$. Let $\alpha(X) \in L_j[\![X]\!]$ such that $\alpha(X) \cdot P_{j,\varphi_{j,1}^{\mathrm{univ}}}(X) = [\pi]_{F_{L_j}}(X)$, and let $L_{j+1} = L_j[\![x]\!]/(\alpha(x))$. Before constructing $\varphi_{j+1,1}^{\mathrm{univ}}$ and showing (4.3), we will establish that L_{j+1} is a regular local ring.

Since G is normal, $\alpha(X) \equiv X^{q^h-q^j} \pmod{\mathfrak{m}_{L_j}}$. Writing $\alpha = \beta\gamma$ as in Proposition 4.2.3, we see that $L_{j+1} = L_j[\![x]\!]/(\beta(x))$. So by the same proposition, L_{j+1} is finite and free over L_j, so in particular, the dimension of these two rings are the same. Therefore, by the inductive hypothesis, we get the regularity of L_{j+1} if we show that $I = (\varphi_{j,1}^{\mathrm{univ}}(e_1), \dots, \varphi_{j,1}^{\mathrm{univ}}(e_j), x, \beth_{j+1}, \dots, \beth_{h-1})$ is equal to the maximal ideal $\mathfrak{m}_{L_{j+1}} = I + (\beth_j)$.

By Theorem 4.1.7, the coefficient of X^{q^j} in $[\pi]_{F_{D_0}}(X)$ is $(\pi^{q^j-1}-1)\beth_j$, so by definition, the coefficient of X^{q^j} in $[\pi]_{L_j}(X)$ is the image of this under $D_0 \to L_j$. Using $P_{j,\varphi_{j,1}^{\mathrm{univ}}} \equiv X^{q^j}$, $\beta(X) \equiv X^{q^h-q^j}$, and $\gamma(X) \equiv 1$ modulo $\mathfrak{m}_{L_j}$, we can check that the coefficient of X^{q^j} in $P_{j,\varphi}(X)\alpha(X)$ is $\beta(0)$ modulo $\mathfrak{m}_{L_j}^2$. Hence,

$$(\pi^{q^j-1}-1)\beth_j \equiv \beta(0) \pmod{\mathfrak{m}_{L_j}^2}. \tag{4.4}$$

Since

$$\alpha(X) = \alpha(0) + X^{q^h-q^j} + X \cdot \left((\mathfrak{m}_{L_j})\text{-coefficient power series}\right),$$

upon multiplying (4.4) by $\gamma(0)$, we have $\beth_j \equiv (\pi^{q^j-1}-1)\gamma(0)^{-1}x^{q^h-q^j} \pmod{\mathfrak{m}_{L_j}\mathfrak{m}_{L_{j+1}}}$. Thus,

$$\mathfrak{m}_{L_{j+1}} = I + \mathfrak{m}_{L_j}\mathfrak{m}_{L_{j+1}} = I + \mathfrak{m}_{L_j}^2\mathfrak{m}_{L_{j+1}} = \cdots = I$$

by the Krull intersection theorem (applied to the module $\mathfrak{m}_{L_{j+1}}/I$ with $\mathfrak{m}_{L_j}$-adic topology), so we now know that L_{j+1} is a regular local ring.

Define

$$\varphi_{j+1,1}^{\mathrm{univ}}(\sum \lambda_i e_i) = F_{L_{j+1}}(\varphi_{j,1}^{\mathrm{univ}}(\lambda_1 e_1 + \cdots + \lambda_j e_j), [\lambda_{j+1}]_{F_{L_{j+1}}}(x)),$$

for $\lambda_i \in R/(\pi)$. Since $[\pi]_{L_j}(x) = \alpha(x)P_{j,\varphi_{j,1}^{\mathrm{univ}}}(x) = 0$ in L_{j+1} and $F_{L_{j+1}}$ is the push-forward of F_{L_j} by $L_j \to L_{j+1}$, $\varphi_{j+1,1}^{\mathrm{univ}}$ is a well-defined R-module homomorphism $\left(\pi^{-1}R/R\right)^{j+1} \to F_{L_{j+1}}(\mathfrak{m}_{L_{j+1}})$. Also, if $\sum \lambda_i e_i$ is in kernel of $\varphi_{j+1,1}^{\mathrm{univ}}$,

$$\begin{aligned} 0 = \varphi_{j+1,1}^{\mathrm{univ}}(\sum \lambda_i e_i) &= [\lambda_1](\varphi_{j,1}^{\mathrm{univ}}(e_1)) \underset{F_{L_{j+1}}}{+} \cdots \underset{F_{L_{j+1}}}{+} [\lambda_j](\varphi_{j,1}^{\mathrm{univ}}(e_j)) \underset{F_{L_{j+1}}}{+} [\lambda_{j+1}](x) \\ &\equiv \lambda_{j+1}x + \sum_{i=1}^{j} \lambda_i \varphi_{j,1}^{\mathrm{univ}}(e_j) \pmod{\mathfrak{m}_{L_{j+1}}^2}, \end{aligned}$$

but a system of parameters of a regular local ring form a basis of $\mathfrak{m}_{L_{j+1}}/\mathfrak{m}_{L_{j+1}}^2$, so this implies $\lambda_i \in (\pi)$. Thus, $\varphi_{j+1,1}^{\mathrm{univ}}$ is injective. Now, $[\pi]_{F_{L_{j+1}}}(\varphi_{j+1,1}^{\mathrm{univ}}(\sum \lambda_i e_i)) = 0$ and Proposition 4.2.3 shows that $[\pi]_{F_{L_{j+1}}}(X)$ is divisible by each $X - \varphi_{j+1,1}^{\mathrm{univ}}(\sum \lambda_i e_i)$, so by injectivity of $\varphi_{j+1,1}^{\mathrm{univ}}$ and domainness of L_{j+1}, we obtain (4.3) for $\varphi_{j+1,1}^{\mathrm{univ}}$.

Finally, let us show that $\varphi_{j+1,1}^{\mathrm{univ}}$ is the universal element of this functor. Suppose $\varphi : \left(\pi^{-1}R/R\right)^{j+1} \to F_A(\mathfrak{m}_A)$ is an R-module homomorphism satisfying (4.3). Then $\varphi|_{(\pi^{-1}R/R)^j}$ gives rise to a unique map $L_j \to A$ sending $\varphi_{j,1}^{\mathrm{univ}}$ to $\varphi|_{(\pi^{-1}R/R)^j}$. Thus, the only candidate of the requisite $L_{j+1} \to A$ is obtained by using this $L_j \to A$ and sending x to $\varphi(e_{j+1})$. In order for this to work, $\alpha(\varphi(e_{j+1})) = 0$. But by functoriality, via $L_j \to A$, $\alpha(X)$ is sent to

$$\frac{[\pi]_{F_A}(X)}{\prod_{s \in (\pi^{-1}R/R)^j}(X - \varphi(s))},$$

so $\alpha(\varphi(e_{j+1})) = 0$. □

We now continue the proof of Theorem 4.2.4. Let $D_{h,1} = L_h$ and $\varphi_1^{\mathrm{univ}} = \varphi_{1,h}^{\mathrm{univ}}$. If (F, φ) is a deformation of G of level 1 over A, then there exists a unique map $D_0 \to A$ which pushes-forward F^{univ} to the deformation class of F, and given this, the above lemma shows that there exists a unique D_0-algebra homomorphism $D_{h,1} \to A$ pushing-forward $\varphi_1^{\mathrm{univ}}$ to φ, so we have now proven the theorem for $n = 1$.

So suppose that we have proven the theorem up to n, $n \geq 1$. Let e_i be the standard basis of $\left(\pi^{-n+1}R/R\right)^h$ and $b_i = \varphi_n^{\text{univ}}(\pi e_i) \in \mathfrak{m}_{D_{h,n}}$. We claim that

$$D_{h,n+1} = D_{h,n}[\![\urcorner_1, \ldots, \urcorner_h]\!] / \Big([\pi]_{F_{D_{h,n}}}(\urcorner_1) - b_1, \ \ldots, \ [\pi]_{F_{D_{h,n}}}(\urcorner_h) - b_h \Big)$$

and $\varphi_{n+1}^{\text{univ}}$ sending e_i to $\urcorner_i$ form the desired universal element. Because $\varphi_{n+1}^{\text{univ}}$ agrees with φ_n^{univ} on $(\pi^{-n}R/R)^h$ (in particular on $\left(\pi^{-1}R/R\right)^h$), $\varphi_{n+1}^{\text{univ}}$ is a well-defined R-module homomorphism and a structure of level $n+1$. By adding one $\urcorner_i$ at a time, Proposition 4.2.3 tells us that $D_{h,n+1}$ is a noetherian local ring which is finite and free as a $D_{h,n}$-module. Since the maximal ideal is $(b_1, \ldots, b_h, \urcorner_1, \ldots, \urcorner_h) = (\urcorner_1, \ldots, \urcorner_h)$, $D_{h,n+1}$ is a regular local ring. By the same argument as in proof of the lemma, $\varphi_{n+1}^{\text{univ}}(\sum \lambda_i e_i) = 0$ shows each $\lambda_i \in (\pi)$, and then by the injectivity of φ_n^{univ}, we obtain injectivity of $\varphi_{n+1}^{\text{univ}}$. Checking universality is similar as before: given (F, φ) over A, restrict φ to $(\pi^{-n}R/R)^h$ and get $D_{h,n} \to A$, and then note that there is only one way of making the requisite map $D_{h,n+1} \to A$, namely by sending $\urcorner_i$ to $\varphi(e_i)$, and this is well-defined by construction. □

Example 4.2.6. We will now trace the proof to obtain an explicit description of the universal deformation of level n for small h. First, let $h = 1$. For $n = 1$, by the proof of Lemma 4.2.5, $L_1 = D_{1,0}[\![x]\!] / \left(\frac{[\pi]_{F^{\text{univ}}}(x)}{x} \right)$. Note also that φ_1^{univ} sends $\frac{1}{\pi}$ to x by construction. For $n = 2$, tracing the construction yields (by functoriality, $[\pi]$ for different formal modules are all images of the universal one over $D_{1,0}$, so they are compatible)

$$D_{1,2} \cong \frac{D_{1,1}[\![\urcorner_1]\!]}{\Big([\pi](\urcorner_1) - \varphi_1^{\text{univ}}(\frac{1}{\pi}) \Big)} \cong \frac{D_{1,0}[\![x, \urcorner_1]\!]}{\Big(\frac{[\pi](x)}{x}, \ [\pi](\urcorner_1) - \varphi_1^{\text{univ}}(\frac{1}{\pi}) \Big)} \cong \frac{D_{1,0}[\![\urcorner_1]\!]}{\frac{[\pi^2](\urcorner_1)}{[\pi](\urcorner_1)}}.$$

Similarly, we can continue by induction to show that $D_{1,n} \cong D_{1,0}[\![\urcorner_1]\!] / \frac{[\pi^n](\urcorner_1)}{[\pi^{n-1}](\urcorner_1)}$. Thus, for $\mathbb{Z}_p$-module $\widehat{\mathbb{G}}_{\text{m}}$ over $\overline{\mathbb{F}_p}$, deformation classes of level n over A correspond to maps $\widehat{R}^{\text{nr}}[\![\urcorner]\!] / (\urcorner^{p^n - p^{n-1}}) \to A$ in $\mathscr{C}$.

Now let $h = 2$. For $n = 1$, tracing through Lemma 4.2.5 yields

$$L_2 = \frac{\Big(D_{2,0}[\![x]\!] \ / \ \big(\frac{[\pi](x)}{x} \big) \Big)[\![y]\!]}{\left(\frac{[\pi](y)}{\prod_{\lambda \in (\pi^{-1}R/R)^1} (y - [\lambda](x))} \right)} \cong \frac{D_{2,0}[\![x, y]\!]}{\left(\frac{[\pi](x)}{x}, \ \frac{[\pi](y)}{\prod_{\lambda \in (\pi^{-1}R/R)^1} (y - [\lambda](x))} \right)}.$$

Similarly to the $h = 1$ case, we can show by induction that $D_{2,n}$ is $D_{2,0}[\![\urcorner_1, \urcorner_2]\!]$ modded out by the same relations as in the last ring above except we replace x by $[\pi^{n-1}](\urcorner_1)$ and y by $[\pi^{n-1}](\urcorner_2)$.

We can now explicitly see the connection between Drinfel'd's level structures and π^n-torsions.

We will next use the nice properties of the universal deformation of level n to create a deformation of level $n' < n$ which is a 'quotient' deformation of what we started out with. To deal with quotients in general, we need to expand the notion of formal R-modules; we will do so in Section 4.3. But this particular example of a quotient can be concretely constructed while staying in the realm of the formal R-modules discussed so far. This construction will only work over regular local rings, but every deformation of level n over A is a push-forward of the universal one defined over a regular local ring by Theorem 4.2.2, so we can simply take the push-forward of the quotient constructed over regular local ring to be the quotient in general. This is an example of why nice properties of universal deformation rings are important. This construction does play an important role in Drinfel'd's paper (see Section 5.2).

Let $S \subseteq (\pi^{-n}R/R)^h$ be an R-submodule. We will construct the quotient $F/\varphi_n^{\text{univ}}(S)$, i.e. the formal R-module in which the S part of the deformation is forced to be 0. Let $\alpha(X) = \prod_{s \in S} F_n^{\text{univ}}(X, \varphi_n^{\text{univ}}(s))$. Since $\alpha(X) \equiv X^{|S|} \pmod{\mathfrak{m}_{D_{h,n}}}$ and $D_{h,n}[\![\alpha]\!]$ is a complete noetherian local ring, Proposition 4.2.3 tells us that $D_{h,n}[\![\alpha]\!] \longrightarrow D_{h,n}[\![X]\!] \cong D_{h,n}[\![\alpha]\!][\![X]\!]$ is injective and free of rank $|S|$. In other words, two power series in one variable which agree upon evaluation at $\alpha(X)$ must actually be the same. By induction (using the fact that $D_{h,n}[\![X]\!]$ is also regular local), two power series in a finite number of variables which agree upon evaluation at $\alpha(X)$'s must agree. This will be important.

For each $s \in S$, let $\sigma_s : D_{h,n}[\![X]\!] \to D_{h,n}[\![X]\!]$ be a ring homomorphism defined by $X \mapsto F_n^{\mathrm{univ}}(X, \varphi_n^{\mathrm{univ}}(s))$, which is well-defined since $\varphi_n^{\mathrm{univ}}(s) \in \mathfrak{m}_{D_{h,n}})$. Note that $\sigma_{s_1} \circ \sigma_{s_2}$ sends X to

$$F_n^{\mathrm{univ}}(F_n^{\mathrm{univ}}(X, \varphi_n^{\mathrm{univ}}(s_2)), \varphi_n^{\mathrm{univ}}(s_1)) = F_n^{\mathrm{univ}}(X, F_n^{\mathrm{univ}}(\varphi_n^{\mathrm{univ}}(s_2), \varphi_n^{\mathrm{univ}}(s_1))) = F_n^{\mathrm{univ}}(X, \varphi_n^{\mathrm{univ}}(s_1 + s_2)),$$

so $\sigma_{s_1} \circ \sigma_{s_2} = \sigma_{s_1+s_2}$. Also, $\sigma_0 = \mathrm{id}$. Therefore, the additive group S acts on $D_{h,n}[\![X]\!]$. The same calculation also shows that $\sigma_s(\alpha(X)) = \alpha(X)$ for all $s \in S$, so $D_{h,n}[\![\alpha]\!]$ is fixed by this action of S.

We will now prove that $D_{h,n}[\![\alpha]\!] = (D_{h,n}[\![X]\!])^S$. Since $D_{h,n}$ is a domain, we can extend this action of S on $D_{h,n}[\![X]\!]$ to $\mathrm{Frac}(D_{h,n}[\![X]\!])$, where Frac denotes the field of fractions. We have already proved

$$\mathrm{Frac}(D_{h,n}[\![X]\!]) \supseteq (\mathrm{Frac}(D_{h,n}[\![X]\!]))^S \supseteq \mathrm{Frac}(D_{h,n}[\![X]\!]^S) \supseteq \mathrm{Frac}(D_{h,n}[\![\alpha]\!]).$$

By Artin's Theorem in Galois theory, the extension degree of the first two fields is $|S|$. Since $D_{h,n}$ is a regular local ring, it is a UFD [21, Theorem 20.3], so it is integrally closed. This implies that any basis of $D_{h,n}[\![X]\!]$ over $D_{h,n}[\![\alpha]\!]$ is actually a basis for the field extension, so the extension degree of the extreme two fields is also $|S|$. Therefore, $\mathrm{Frac}(D_{h,n}[\![X]\!]^S) = \mathrm{Frac}(D_{h,n}[\![\alpha]\!])$. Now, $\dim D_{h,n}[\![\alpha]\!] = \dim D_{h,n}[\![X]\!]$ and the number of generators of the maximal ideals is the same, so $D_{h,n}[\![\alpha]\!]$ is also a regular local ring, thus integrally closed. Therefore, we now conclude that $D_{h,n}[\![X]\!]^S = D_{h,n}[\![\alpha]\!]$. By the same argument, we can show that $D_{h,n}[\![X, Y]\!]^{S\times S} = D_{h,n}[\![\alpha(X), \alpha(Y)]\!]$.

Note that

$$\begin{aligned}
\sigma_{s_1}\Big(\alpha\big([r]_{F_n^{\mathrm{univ}}}(X)\big)\Big) &= \alpha\Big([r]_{F_n^{\mathrm{univ}}}\big(F_n^{\mathrm{univ}}(X,\ \varphi_n^{\mathrm{univ}}(s_1))\big)\Big) = \alpha\Big(F_n^{\mathrm{univ}}\big([r]_{F_n^{\mathrm{univ}}}(X),\ [r]_{F_n^{\mathrm{univ}}}(\varphi_n^{\mathrm{univ}}(s_1))\big)\Big) \\
&= \prod_s F_n^{\mathrm{univ}}\Big(F_n^{\mathrm{univ}}\big([r]_{F_n^{\mathrm{univ}}}(X),\ [r]_{F_n^{\mathrm{univ}}}(\varphi_n^{\mathrm{univ}}(s_1))\big),\quad \varphi_n^{\mathrm{univ}}(s)\Big) \\
&= \prod_s F_n^{\mathrm{univ}}\big([r]_{F_n^{\mathrm{univ}}}(X),\ \varphi_n^{\mathrm{univ}}(rs_1 + s)\big) = \alpha([r]_{F_n^{\mathrm{univ}}}(X)),
\end{aligned}$$

for all $s_1 \in S$, so $\alpha([r]_{F_n^{\mathrm{univ}}}(X)) = [r]_H(\alpha(X))$ for a unique $[r]_H \in D_{h,n}[\![X]\!]$. Similarly, we can check that $\alpha(F_n^{\mathrm{univ}}(X, Y))$ is $H \times H$-invariant, so we must have $\alpha(F_n^{\mathrm{univ}}(X, Y)) = H(\alpha(X), \alpha(Y))$ for a unique $H \in D_{h,n}[\![X, Y]\!]$. Furthermore, we can show the following:

Proposition 4.2.7. *$(H, [\ ]_H)$ defines a formal R-module over $D_{h,n}$, and α is a formal R-module homomorphism $F_n^{\mathrm{univ}} \to H$. The map $(\pi^{-n}R/R)^h \xrightarrow{\varphi_n^{\mathrm{univ}}} F_n^{\mathrm{univ}}(\mathfrak{m}_{D_{h,n}}) \xrightarrow{\alpha} H(\mathfrak{m}_{D_{h,n}})$ factors through $(\pi^{-n}R/R)^h/S$, and if $\left(\pi^{-n'}R/R\right)^h \hookrightarrow (\pi^{-n}R/R)^h/S$ for some $n' \geq 1$, then*

$$\psi : \left(\pi^{-n'}R/R\right)^h \hookrightarrow \Big(\left(\pi^{-n}R/R\right)^h/S\Big) \to H(\mathfrak{m}_{D_{h,n}})$$

is a structure of level n' on H.

Proof. Using $H \circ \alpha = \alpha \circ F_n^{\mathrm{univ}}$ and $[r]_H \circ \alpha = \alpha \circ [r]_{F_n^{\mathrm{univ}}}$, we get identities such as $H(H(\alpha(X), \alpha(Y)), \alpha(Z)) = H(\alpha(X), H(\alpha(Y), \alpha(Z)))$, so H must be a formal R-module. For $s \in S$,

$$\alpha(\varphi_n^{\mathrm{univ}}(s)) = \prod_{s'} F_n^{\mathrm{univ}}(\varphi_n^{\mathrm{univ}}(s), \varphi_n^{\mathrm{univ}}(s')) = \prod_{s'} \varphi_n^{\mathrm{univ}}(s + s') = 0,$$

so $\alpha \circ \varphi_n^{\mathrm{univ}}$ factors through $(\pi^{-n}R/R)^h/S$. We now prove the last statement. Since $\alpha(\varphi_n^{\mathrm{univ}}(t)) = \prod_s(\varphi_n^{\mathrm{univ}}(t) - \varphi_n^{\mathrm{univ}}(s))$ for $t \in \left(\pi^{-n'}R/R\right)^h \hookrightarrow (\pi^{-n}R/R)^h$ and $D_{h,n}$ is an integral domain, injectivity of $\varphi_n^{\mathrm{univ}}$ (Theorem 4.2.4) shows injectivity of ψ. Moreover, for $t \in (\pi^{-n}R/R)^h$, $[\pi]_H(\psi(t)) = [\pi]_H(\alpha(\varphi_n^{\mathrm{univ}}(t))) = \alpha([\pi]_{F_n^{\mathrm{univ}}}(\varphi_n^{\mathrm{univ}}(t))) = 0$, so similarly as before, ψ is a structure of level n' on H. □

Remark. As mentioned earlier, we could construct this H as a quotient of more generalized notion of formal R-modules, discussed in Section 2.3. Just as a reference, we will briefly describe the above results in this language. We need to prove that

$$0 \longrightarrow \Big(F' = \mathrm{Spf}_{D_{h,n}}\big(D_{h,n}[\![X]\!]/\prod_{s\in S}(X-\varphi_n^{\mathrm{univ}}(s))\big)\Big) \longrightarrow \Big(F = \mathrm{Spf}_{D_{h,n}}(D_{h,n}[\![X]\!])\Big) \longrightarrow \Big(H = \mathrm{Spf}_{D_{h,n}}(D_{h,n}[\![\alpha]\!])\Big) \longrightarrow 0.$$

is a short exact sequence of formal R-modules. Indeed, all of these rings are topologically flat over $D_{h,n}$ (use Proposition 4.2.3), $D_{h,n}[\![X]\!] \hookleftarrow D_{h,n}[\![\alpha]\!]$ is topologically faithfully flat (it is free), and

$$D_{h,n}[\![X]\!]/\prod_{s\in S}(X-\varphi_n^{\mathrm{univ}}(s)) \;\leftarrow\; D_{h,n}[\![X]\!]$$

is a surjection. Further, injectivity of $\varphi_n^{\mathrm{univ}}$ and $\alpha(\varphi_n^{\mathrm{univ}}(s))=0$ as derived above show that α is a multiple of $\prod_{s\in S}(X-\varphi_n^{\mathrm{univ}}(s))$. So these must differ by a unit in $D_{h,n}[\![X]\!]$, because $\alpha \equiv \prod(X-\varphi_n^{\mathrm{univ}}(s)) \equiv X^{|S|} \pmod{\mathfrak{m}_{D_{h,n}}}$. This shows

$$D_{h,n}[\![X]\!]/\prod_{s\in S}(X-\varphi_n^{\mathrm{univ}}(s)) \overset{\cong}{\leftarrow} D_{h,n}[\![X]\!]\widehat{\otimes}_{D_{h,n}[\![\alpha]\!]}D_{h,n},$$

showing exactness, as desired. By chasing maps, we also get identities such as $H(\alpha(X),\alpha(Y))=\alpha(F(X,Y))$. So H can be viewed as the quotient F/F' with this broader definition of formal R-modules.

4.3 The Deformations of Divisible Modules

We are finally ready to discuss deformation theory of formal R-modules that Drinfel'd was after, namely deformations of divisible formal R-modules. Although this is a more general notion of formal R-modules, they are restricted enough so that we can 'extend' the notion of the level structures and the results of deformation theory that we have developed in the previous two sections. Again, our goal is determining the universal deformation ring with level structures and deriving their properties.

In this section, formal R-modules refer to those satisfying Definition 2.3.1, and the formal R-modules of the form discussed previously (the power series form) will be called CFS formal R-modules. We will freely use the results and notations from both Section 2.3 and Appendix A.

Let $A \in \mathscr{C}$, j be a fixed non-negative integer, and let S be the R-module $(K/R)^j$ (j will never be changed in this section, so this notation should not cause confusion). Here is the central object of study in this section:

Definition 4.3.1. A *divisible formal R-module over A of type (h,j)* is a formal R-module over A such that (1) the connected component F^0 of F is a CFS formal R-module over A such that $\overline{F^0}$ over $\widehat{R}^{\mathrm{nr}}/(\pi)$ is of height h, and (2) there is a short exact sequence of formal R-modules

$$0 \longrightarrow F^0 \longrightarrow F \longrightarrow \mathrm{Spf}_A(A^S) \longrightarrow 0.$$

By Proposition 2.3.3, $\mathrm{Spf}_A(A^S)$ is étale and it can be viewed as the 'discrete' formal R-module over A made from the R-module S. So by putting condition (2) on the connected-étale sequence of a divisible formal R-module F, we are in some sense forcing F to be S disjoint copies of the CFS formal R-modules with 'twists'. This statement can be made precise (see the construction of the divisible formal R-module F in the proof of Proposition 4.3.5 below), and explains why it is not surprising to get a nice deformation theory of divisible formal modules by generalizing the results proven already for the CFS formal R-modules.

Note that divisiblity of F does not come with a specified short exact sequence in (2) above. We only know that F can be fit into such a sequence. From Section 2.3, we do know that quotients are well-defined in this setting, so we get every possibility of $F \to \mathrm{Spf}_A(A^S)$ by starting from one $F \to \mathrm{Spf}_A(A^S)$ and compose with

all formal R-module isomorphisms $\mathrm{Spf}_A(A^S) \to \mathrm{Spf}_A(A^S)$. Whenever we use this sequence of F, we must always remember to make sure that we are not making a choice for the quotient map.

We will now give the definition of level structure on a divisible formal R-module F. Recall by Propositions 2.3.3, 2.3.2, and 2.3.7, $\mathrm{Spf}_A(A^S)(A) \cong S$ canonically, $F^0(A)$ is $F^0(\mathfrak{m})$, and evaluating a connected-étale sequence at A gives a left-exact sequence of R-modules.

Definition 4.3.2. For $n \geq 0$, a *structure of level* n on a divisible formal R-module F of type (h, j) is an R-module homomorphism $\Phi : (\pi^{-n}R/R)^{h+j} \to F(A)$ such that (1) The image of $\Phi|_{(\pi^{-n}R/R)^h}$ lies in $F^0(\mathfrak{m}) = F^0(A) \hookrightarrow F(A)$, giving a structure of level n for the CFS formal R-module F^0, and (2) The image of the composition $(\pi^{-n}R/R)^{h+j} \xrightarrow{\Phi} F(A) \longrightarrow \mathrm{Spf}_A(A^S)(A) \cong S$ is exactly equal to $(\pi^{-n}R/R)^j$.

Note that although we are using the quotient map $F \to \mathrm{Spf}_A(A^S)$ in condition (2) for the level structure, another choice would result in composing with an isomorphism $S \to S$. Since this isomorphism does not change the π^n-torsions, we see that (2) is a well-defined condition for divisible modules. From now on, we will not always go through this kind of reasoning every time we use the quotient map part of the connected-étale sequence for F.

If $j = 0$, F is a CFS formal R-module, and this definition of level structure does agree with that of Section 4.2. Moreover, this definition is relatively restrictive. For example, the two conditions above and the exactness of $F^0(A) \to F(A) \to \mathrm{Spf}_A(A^S)(A)$ together with finiteness of $(\pi^{-n}R/R)^j$ imply that the composition

$$\left(\pi^{-n}R/R\right)^j \hookrightarrow \left(\pi^{-n}R/R\right)^{h+j} \xrightarrow{\Phi} F(A) \longrightarrow \left(\pi^{-n}R/R\right)^j$$

is an isomorphism. This fact will be used later for constructing level structures. In this section, a level structure will *always* be denoted by one of ϕ, Φ, ψ.

When $A = \bar{k}$, the connected-étale sequence splits (Proposition 2.3.8), so a divisible formal R-module G of type (h, j) has the form $G^0 \times \mathrm{Spf}_{\bar{k}}(\bar{k}^S)$. As the maximal ideal is 0, $G(\bar{k}) \longrightarrow \mathrm{Spf}_{\bar{k}}(\bar{k}^S)(\bar{k}) = S$ is an isomorphism. This shows that level structures on G correspond to R-module automorphisms of $(\pi^{-n}R/R)^j$, since the level structure must be defined 0 on $(\pi^{-n}R/R)^h$.

We next define a deformation of level n, essentially by following what we did for the CFS case. There is one significant difference, however. As noted above, there is more than one level structure on a divisible formal R-module G over $\bar{k}$ of type (h, j) when $j > 0$, in contrast to the case $j = 0$. Therefore it is cleaner to develop the deformation theory of divisible formal R-modules by *fixing* a level structure ϕ on G over the residue field. So we will discuss deformations of (G, ϕ), where G is a divisible formal R-module over $\bar{k}$ of type (h, j) and ϕ is a structure of level n on G. The deformations should have the property that the formal module and the level structure 'reduce mod $\mathfrak{m}_A$' to (G, ϕ). More precisely,

Definition 4.3.3. A triple (F, ι, Φ) is said to be a *deformation of* (G, ϕ) *over* A if (1) F is a divisible formal R-module over A of type (h, j) and ι is an isomorphism from $\overline{F}$ (i.e. base change by $(A/\mathfrak{m}_A)$ and identify $\widehat{R}^{\mathrm{nr}}/(\pi) \cong A/\mathfrak{m}_A$) to G over $\bar{k}$, and (2) Φ is a structure of level n on F such that the composition

$$\left(\pi^{-n}R/R\right)^{h+j} \xrightarrow{\Phi} F(A) \longrightarrow \overline{F}(\overline{A}) \xrightarrow{\iota} G(\bar{k})$$

is ϕ.

We call two deformations (F_i, ι_i, Φ_i) of (G, ϕ) of level n over A *isomorphic* if there exists an isomorphism $\alpha : F_1 \longrightarrow F_2$ of formal R-modules such that $(\pi^{-n}R/R)^{h+j} \xrightarrow{\Phi_1} F_1(A) \xrightarrow{\alpha} F_2(A)$ is Φ_2 and

$$\begin{array}{ccc} F_1 \bmod \mathfrak{m}_A & \xrightarrow{\quad\alpha\quad} & F_2 \bmod \mathfrak{m}_A \\ & {\scriptstyle \iota_1} \searrow \quad \swarrow {\scriptstyle \iota_2} & \\ & G & \end{array}$$

commutes.

In this section, we will not use the definition of deformation which takes ι to be id. Also, note that this definition agrees with the definition given in the last section when $j = 0$.

As usual, our goal is the determination of the universal deformation (up to isomorphism) of (G, ϕ) of level n:

Theorem 4.3.4. *Suppose (G, ϕ) is a divisible formal R-module G of type (h, j) over $\bar{k}$ with a structure ϕ of level n. The functor which associates $A \in \mathscr{C}$ to the set of all deformations of (G, ϕ) over A up to isomorphism is represented by $E_{h,n,j} = D_{h,n}[\![\mho_1, \ldots, \mho_j]\!]$, where $D_{h,n}$ is as in Theorem 4.2.4. $E_{h,n,j}$ is a regular local ring of dimension $h + j$, and the natural map $E_{h,n,j} \longrightarrow E_{h,n+1,j}$ is finite and flat.*

We will spend the rest of this section proving this theorem. The proof takes advantage of the relatively strong conditions put on divisible modules and their level structures so that we can use deformation theory of the CFS formal R-modules developed in Section 4.2. More specifically, given a deformation (F, ι, Φ) of (G, ϕ), it follows by definition that $(F^0, \iota|_{F^0}, \Phi|_{(\pi^{-n}R/R)^h})$ is a deformation of level n of the CFS formal R-module G^0 ($\because \iota$ induces an isomorphism η from $\overline{F^0} = \overline{F}^0$ to G^0). Therefore to prove the theorem (which requires knowing what the possibilities are for deformations), we will first classify all the deformations of (G, ϕ) that restrict to a certain fixed deformation of level n of G^0, and then use the deformation theory of the CFS case to 'naturally' change the deformation on the connected component.

We use the notion of 'extensions' to classify all the deformations (F, ι, Φ) of (G, ϕ) which restrict to a given deformation (H, η, ψ) of G^0. This may be a bit concerning, because the deformation F does not come with the information of identifying F/F^0 with $\mathrm{Spf}_A(A^S)$. However we will get around this problem by fixing a quotient map $G/G^0 \to \mathrm{Spf}_{\bar{k}}(\bar{k}^S)$ over the residue field. A complete justification on why we can use the notion of extensions to prove Theorem 4.3.4 will be given at the very end of the proof.

Studying 'extensions' will be divided into two big parts. First we will deal with extensions of formal R-modules (Proposition 4.3.5). That is, we will ignore the level structure and just analyze formal R-modules F with connected component H. This sets up the stage for the second part, which add consideration of the level structures (Proposition 4.3.7). Before stating this proposition we will precisely define the notion of an 'extension' of a deformation of G^0 to a deformation of G.

Proving these two propositions in detail actually require a lot of work. To clarify the main ideas of the proofs, we will have a brief overview section at the beginning of each proof.

We will now begin the proof of Theorem 4.3.4. Our first task as noted above is analyzing the possibilities of divisible formal R-modules when we fix the connected component, using the notion of extensions of formal R-modules (cf. Proposition 2.3.6).

Proposition 4.3.5. *There is a natural bijection between $\mathscr{E}xt_{R,A}(\mathrm{Spf}_A(A^S), H)$ and $\mathrm{Ext}_R(S, H(\mathfrak{m}_A))$ given by evaluation at A.*

Proof. We will first give an overview of the proof. First, we will show that evaluation at A produces a well-defined element of $\mathrm{Ext}_R(S, H(\mathfrak{m}_A))$ if we start from an element in $\mathscr{E}xt_{R,A}(\mathrm{Spf}_A(A^S), H)$. We will then construct an element of $\mathscr{E}xt_{R,A}$ from an element of Ext_R, after we describe each element of Ext_R in a form suitable for motivating this construction. Next comes the tedious verification that this construction 'works'. Then we show that $\mathrm{Ext}_R \to \mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$ is the identity. Finally, after showing that $\mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$ is a group homomorphism ($\mathscr{E}xt_{R,A}$ is a group by Proposition 2.3.6), we will show that the kernel of $\mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$ is 0.

Given an extension of the form

$$0 \to H \to F \to \mathrm{Spf}_A(A^S) \to 0,$$

we now show that the evaluation on the base

$$0 \to H(A) \to F(A) \to \mathrm{Spf}_A(A^S)(A) \to 0$$

is an exact sequence of R-modules. By definition, these are R-modules and R-module homomorphisms. The left-exactness follows from Proposition 2.3.7. The right-exactness comes from the fact that F is formally smooth, but we will include a more explicit proof here since this will be useful later. Let $F = \mathrm{Spf}_A(B)$, and let $B = \prod B_{\mathfrak{n}}$ where $\mathfrak{n}$ runs through open maximals of B. Base changing by $A/\mathfrak{m}$ and using Proposition

2.3.8, we must have $\prod(B_{\mathfrak{n}}\widehat{\otimes}_A\bar{k}) \cong \bar{k}[\![T]\!]^S$. Because rings inside the product sign are all local for both sides, this isomorphism induces an isomorphism on each local factor (by the same argument as given in Section A.5). In other words, $\bar{k}[\![T]\!] \cong B_{\mathfrak{n}}\widehat{\otimes}_A\bar{k}$ for each $\mathfrak{n}$, and $\mathfrak{n}$'s are in a bijective correspondence with elements of S. Lifting the image of T under this isomorphism to $B_{\mathfrak{n}}$, we get a map $A[\![T]\!] \to B_{\mathfrak{n}}$ of $\mathcal{PA}_A$ which reduces to an isomorphism modulo $\mathfrak{m}_A$. Because $B_{\mathfrak{n}}$ is topologically flat ($\because$ B is topological flat and $B = \prod B_{\mathfrak{n}}$), the Nakayama/projectivity argument discussed in Appendix A gives us $A[\![T]\!] \cong B_{\mathfrak{n}}$ as elements of $\mathcal{PA}_A$, so $A[\![T]\!]^S \cong B$. Moreover, since products and $(-)^{\text{ét}}$ commute, we obtain $(A[\![T]\!]^S)^{\text{ét}} = A^S$ by Proposition 2.3.4. Now, by definition of connected-étale sequences, $F \to \mathrm{Spf}_A(A^S)$ corresponds to $B \cong A[\![T]\!]^S \hookleftarrow A^S$, so it is now clear that $F \to \mathrm{Spf}_A(A^S)$ has a formal A-scheme section. Hence, $F(A) \to \mathrm{Spf}_A(A^S)(A)$ is surjective, as desired.

Since every map of formal R-modules functorially induces a map of R-modules upon evaluation, this process sends equivalent extensions of formal R-modules to equivalent extensions of R-modules. Therefore, we have now created $\mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$.

So we are now in the second stage of our proof, where we will reinterpret an R-module extension

$$0 \to H(\mathfrak{m}_A) \xrightarrow{f} E \xrightarrow{g} S \to 0 \tag{4.5}$$

in a way suitable for motivating our construction of the corresponding element of $\mathscr{E}xt_{R,A}$. We choose a set-theoretic section g' of the map $E \to S$ with the property that $g'(-s) = -g'(s)$ for every $s \in S$. Then we denote how off this g' is from being an R-module homomorphism by letting

$$\Xi(s,s') = g'(s) + g'(s') - g'(s+s'), \qquad \text{and} \qquad \xi_r(s) = rg'(s) - g'(rs) \qquad \forall s,s' \in S,\, r \in R.$$

Note that $\Xi(s_1,s_2)$ and $\xi_r(s)$ take values in $H(\mathfrak{m}_A) \hookrightarrow E$. Also, by the assumption on g', $\Xi(s,0) = \Xi(s,-s) = \xi_r(0) = 0$ for all $r \in R$ and $s \in S$. Using these, we can check directly that the diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H(\mathfrak{m}_A) & \longrightarrow & S \times H(\mathfrak{m}_A) & \longrightarrow & S & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & H(\mathfrak{m}_A) & \xrightarrow[f]{} & E & \xrightarrow[g]{} & S & \longrightarrow & 0 \end{array} \tag{4.6}$$

commutes, where we give $S \times H(\mathfrak{m}_A)$ the structure of an R-module by

$$(s_1,m_1) + (s_2,m_2) = (s_1+s_2, m_1+m_2+\Xi(s_1,s_2)) \qquad \text{and} \qquad r(s,m) = (rs, rm + \xi_r(s)), \tag{4.7}$$

$H(\mathfrak{m}_A) \to S \times H(\mathfrak{m}_A)$ by $m \mapsto (0,m)$, $S \times H(\mathfrak{m}_A) \to S$ by $(s,m) \mapsto s$, and $S \times H(\mathfrak{m}_A) \to E$ by $(s,m) \mapsto g'(s) + f(m)$.

So there is a representative of the R-module extension class of (4.5) such that it is $S \times H(\mathfrak{m}_A)$ (as a set) with the R-module structure 'twisted' by the section g'. This serves as a good motivation for our construction of the corresponding element of $\mathscr{E}xt_{R,A}$, with middle term F. In other words, we should take F to be 'S copies of H' with the formal R-module structure 'twisted' by the section g' as in (4.7). So let us define $F = \mathrm{Spf}_A(A[\![T]\!]^S)$ and

$$(\mu^*(b))\,(s,s') = b(s+s')(X \underset{H}{+} Y \underset{H}{+} \Xi(s,s')) \qquad \text{and} \qquad ([r]_F^*(b))\,(s) = b(rs)([r]_H(T) \underset{H}{+} \xi_r(s)),$$

where we have viewed an element $b \in B = A[\![T]\!]^S$ as a (set) map from $S \to A[\![T]\!]$ and an element of $B\widehat{\otimes}_A B \cong (A[\![X,Y]\!])^{S\times S}$ as a (set) map from $S \times S \to A[\![X,Y]\!]$. We also need maps $\alpha : H \longrightarrow F$ and $\beta : F \longrightarrow \mathrm{Spf}_A(A^S)$. Again, looking at the re-interpretation of module extensions above, α should be a 'closed immersion' into the $s = 0$ part (so on rings, take $A[\![T]\!] \leftarrow A[\![T]\!]^S$ defined by evaluation at 0), and β should be the projection onto the S-component (so on rings, take $A[\![T]\!]^S \leftarrow A^S$ defined by the natural inclusion on each component).

Now, we have come to the stage of tedious verification. Here is what we need to check:

(1) F *is* a formal R-module.

(2) α and β are formal R-module homomorphisms.
(3) $0 \to H \to F \to \mathrm{Spf}_A(A^S) \to 0$ is an exact sequence of formal R-modules.
(4) Different choices of section g' result in equivalent extensions of formal R-modules.
(5) Equivalent extensions in Ext_R are sent to equivalent extensions in $\mathscr{E}xt_{R,A}$.

In this detail-checking process, we will often have to check commutativity of diagrams. We will use arrows such as $\overset{\leftarrow}{\uparrow}$ to indicate which way we are tracing a diagram, and given these arrows, we will note the image of an element b via the first map by $b^\dagger$ and its image via the second map by $b^{\dagger\dagger}$ etc. This allows us to trace through diagrams without having to label all the maps.

(1) Note that B is topologically flat. Let

$$\epsilon^*(b) = b(0)(0), \qquad \text{and} \qquad (\mathrm{inv}^*(b))(s) = b(-s)(\mathrm{inv}_H(T)),$$

where $\mathrm{inv}_H(T)$ is the power series satisfying $H(T, \mathrm{inv}_H(T)) = 0$. Since $\mu^*, [r]_F^*, \epsilon^*, \mathrm{inv}^*$ are all maps of $\mathcal{PA}_A$ and $([1]_F(b))(s) = b(s)(T)$, it suffices to check the commutativity of the seven diagrams (2.4). Here we will only check the first diagram (associativity); other diagrams are checked by the same methods.

We will first trace by $\overset{\leftarrow}{\uparrow}$. By definition, $b^\dagger(s, s') = b(s+s')(X \underset{H}{+} Y \underset{H}{+} \Xi(s, s'))$. In other words, this map μ sends every occurrence of T in $(s+s')$-th component to $X \underset{H}{+} Y \underset{H}{+} \Xi(s, s')$ in (s, s')-th component (thinking this way helps computing $\mathrm{id}\,\widehat{\otimes}_\mu$ etc). Denoting $B\widehat{\otimes}B\widehat{\otimes}B \cong A[\![U, V, W]\!]^{S\times S\times S}$, we have

$$\begin{aligned} b^{\dagger\dagger}(t, t', t'') &= b^\dagger(t, t'+t'')\Big(U,\ \ (V \underset{H}{+} W \underset{H}{+} \Xi(t', t''))\Big) \\ &= b(t+t'+t'')\Big(U \underset{H}{+} V \underset{H}{+} W \underset{H}{+} (\Xi(t', t'') \underset{H}{+} \Xi(t, t'+t''))\Big). \end{aligned}$$

By assumption, $H(\mathfrak{m}) \hookrightarrow E$ as R-modules, so identifying $H(\mathfrak{m})$ as a submodule of E,

$$\begin{aligned} \Xi(t', t'') \underset{H}{+} \Xi(t, t'+t'') &= (g'(t') + g'(t'') - g'(t'+t'')) + (g'(t) + g'(t'+t'') - g'(t+t'+t'')) \\ &= g'(t) + g'(t') + g'(t'') - g'(t+t'+t'') \end{aligned}$$

This expression of $b^{\dagger\dagger}$ does not show that we traced the diagram $\overset{\leftarrow}{\uparrow}$ rather than $\uparrow_{\leftarrow}$, so we get the commutativity of the first diagram.

Thus, $F = \mathrm{Spf}_A(B)$ is indeed a formal R-module.

(2) Since α and β are maps of $\mathcal{PA}_A$, we need commutativity of two diagrams (2.5). Here we will explicitly show this for α; we can use the same methods for β. Going $\overset{\leftarrow}{\uparrow}$ in the first diagram, we obtain $b^{\dagger\dagger} = b^\dagger(0,0) = b(0)(H(X,Y))$. Going $\uparrow_{\leftarrow}$, we obtain $b^{\dagger\dagger} = b(0)(H(X,Y))$, so the first diagram commutes. For the second diagram, going $\overset{\leftarrow}{\uparrow}$ results in $b^{\dagger\dagger} = b^\dagger(0) = b(0)([r]_H(T))$. Going $\uparrow_{\leftarrow}$ results in $b^{\dagger\dagger} = b(0)([r]_H(T))$, so the second diagram commutes.

(3) Since $A[\![T]\!] \leftarrow A[\![T]\!]^S \leftarrow A^S$ is given by evaluation at 0, $\beta \circ \alpha$ is indeed the zero map. α is clearly a closed immersion. As shown in the first stage of the proof, A^S is the maximal étale subalgebra of $A[\![T]\!]^S$, so as discussed in Appendix A, β is topologically faithfully flat. Finally, $A[\![T]\!] \overset{\cong}{\leftarrow} A[\![T]\!]^S\widehat{\otimes}_{A^S}A$ follows, since $(0, (1, 1, \ldots))\widehat{\otimes}1$ is 0 in $(A \times A^{S-\{0\}})\widehat{\otimes}_{A^S}A$. Because A^S is the maximal étale subalgebra of $A[\![T]\!]^S$, we can conclude by the exactness of this sequence that H is the connected component of F.

(4) Suppose g_1 and g_2 are two sections of g (both satisfying $g_i(-s) = -g_i(s)$), resulting in formal R-modules F_1 and F_2. Since $g_1(s) - g_2(s) \in H(\mathfrak{m})$ for all $s \in S$, we can define $\gamma^* : B = \mathscr{O}(F_2) \to \mathscr{O}(F_1) = B$ by $(\gamma^*(b))(s) = b(s)\big(T \underset{H}{+} (g_1(s) - g_2(s))\big)$. By a direct computation, we can check that

$$\begin{array}{ccccc} A[\![T]\!] & \xleftarrow{\alpha_1} & \mathscr{O}(F_1) & \xleftarrow{\beta_1} & A^S \\ & {\scriptstyle\alpha_2}\nwarrow & \uparrow{\scriptstyle\gamma^*} & \nearrow{\scriptstyle\beta_2} & \\ & & \mathscr{O}(F_2) & & \end{array}$$

is commutative. Now, we show that $\gamma : F_1 \to F_2$ is a formal R-module homomorphism by checking commutativity of the two diagrams (2.5). We will only check the second diagram here. Going $\uparrow_{\leftarrow}$, we have

$$b^{\dagger\dagger}(s) = b^{\dagger}(rs)([r]_H(T) \underset{H}{+} \xi_1(r)(s)) = b(rs)\left([r]_H(T) \underset{H}{+} \xi_1(r)(s) \underset{H}{+} (g_1(rs) - g_2(rs))\right).$$

Going $\overset{\leftarrow}{\uparrow}$, we have

$$b^{\dagger\dagger}(s) = b^{\dagger}(s)\left(T \underset{H}{+} (g_1(s) - g_2(s))\right) = b(rs)\left([r]_H\big(T \underset{H}{+} (g_1(s) - g_2(s))\big) \underset{H}{+} \xi_2(r)(s)\right).$$

Using the same $H(\mathfrak{m}_A) \hookrightarrow E$ argument (we get $b(rs)\big([r](T) \underset{H}{+} (rg_1(s) - g_2(rs))\big)$ in both cases), we have the commutativity. Thus, we now see that the element in $\mathscr{E}xt_{R,A}$ created by this process is independent of the choice of sections.

(5) Suppose we have a commutative diagram of extensions

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H(\mathfrak{m}) & \longrightarrow & E_1 & \xrightarrow{g_1} & S & \longrightarrow & 0 \\ & & & \searrow & \downarrow{\scriptstyle j} & \nearrow{\scriptstyle g_2} & & & \\ & & & & E_2 & & & & \end{array}$$

If g_1' is a section of g_1 with $g_1'(-s) = -g_1'(s)$, then $g_2' = j \circ g_1'$ is a section of g_2 with $g_2'(-s) = -g_2'(s)$. Moreover, because we identify $H(\mathfrak{m}) \hookrightarrow E_i$, (Ξ, ξ)'s agree for g_1' and g_2'. Thus, clearly the constructed extensions of formal R-modules involving F_1 and F_2 are equivalent.

This finally finishes the tedious checking stage, proving that we have a well-defined process $\mathrm{Ext}_R \to \mathscr{E}xt_{R,A}$.

Next stage is checking that $\mathrm{Ext}_R \to \mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$ is the identity. This essentially follows from our motivation for the construction of F. We will now go through the details. We already know that $H(A) = H(\mathfrak{m})$ and $\mathrm{Spf}_A(A^S) = S$ as R-modules. By the same argument as given in Section A.5, locality of A implies $\mathrm{Spf}_A(A[\![T]\!]^S)(A) = S \times \mathrm{Spf}_A(A[\![T]\!]) = S \times H(\mathfrak{m})$ set-theoretically (where (s, m) corresponds to the projection onto the s-th coordinate and then sending T to m). Using (2.6), the sum of (s, m) and (s', m') in $F(A)$ corresponds to $B \to A$ defined by $b \mapsto b(s + s')(m \underset{H}{+} m' \underset{H}{+} \Xi(s, s'))$, which is the element $(s + s', m + m' + \Xi(s, s')) \in S \times H(\mathfrak{m})$. This agrees with the addition structure put on $S \times H(\mathfrak{m})$ in (4.6). Similarly, using the second diagram of (2.6), we can check that the R actions are the same. It only remains to show that the maps agree. For the first map, the element m (corresponding to the map $A[\![T]\!] \to A$ sending T to m) is sent to $A \leftarrow A[\![T]\!] \leftarrow A[\![T]\!]^S$, defined by projection to the 0-th component followed by sending T to m. Thus, the first map sends m to $(0, m)$, agreeing with (4.6). We can check similarly that the second map agrees, so we have now shown that $\mathrm{Ext}_R \to \mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$ is the identity. In particular, $\mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$ is surjective.

Now we have come to the last stage of the proof. By Proposition 2.3.6, $\mathscr{E}xt_{R,A}(\mathrm{Spf}_A(A^S), H)$ is a group. Moreover, because the group operations on both $\mathscr{E}xt_{R,A}$ and Ext_R are defined by category-theoretic methods of Yoneda Ext, $\mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$ must be a group homomorphism. Therefore, it now suffices to check that the kernel of $\mathscr{E}xt_{R,A} \to \mathrm{Ext}_R$ is 0, i.e. an extension of formal R-modules which splits upon evaluation at A must be a split exact sequence.

So suppose a short exact sequence of formal R-modules $0 \to H \xrightarrow{\alpha} K = \mathrm{Spf}_A(C) \xrightarrow{\beta} \mathrm{Spf}_A(A^S) \to 0$ is such that $0 \to H(\mathfrak{m}) \xrightarrow{f} K(A) \xrightarrow{g} S \to 0$ splits, i.e. there exists an R-module section $g' : S \to K(A)$ (we know from the first stage of the proof that $C \cong A[\![T]\!]^S$, but we won't need this here). By Proposition 2.3.3, there exists a formal R-module homomorphism $\beta' : \mathrm{Spf}_A(A^S) \to K$ such that s-th component $(\beta')^*_s$ of $(\beta')^* : C \to A^S$ is $g'(s)$ for all $s \in S$. To show that β' is a section of β, by the same proposition, it suffices to show that $\beta \circ \beta'$ corresponds to the identity map $S \to \mathrm{Spf}_A(A^S)(A)$. We have $(\beta \circ \beta')^*_s = \beta'^*_s \circ \beta^* = g'(s) \circ \beta^*$, and by definition, $g'(s) \circ \beta^*$ is $g(g'(s)) = s$, so we are done. $\square$

The next stage is adding consideration of level structures. Before going on any further, we will define the concept of 'extension' of a deformation of G^0 to a deformation of G and rigorously establish the connection between classification of such 'extensions' and classifications of deformations with a fixed deformation on the connected component.

As remarked right after the definition of divisible modules, the quotient map part of the connected-étale sequence is not fixed. Let us start from one such $G \longrightarrow \mathrm{Spf}_{\bar{k}}(\bar{k}^S)$. The evaluation at the base $G(\bar{k}) \to \mathrm{Spf}_{\bar{k}}(\bar{k}^S) = S$ is an isomorphism, whose inverse create a formal R-module isomorphism $\mathrm{Spf}_{\bar{k}}(\bar{k}^S) \to \mathrm{Spf}_{\bar{k}}(\bar{k}^S)$ by Proposition 2.3.3. Composing this with the original quotient map, we now have a new quotient map $G \longrightarrow \mathrm{Spf}_{\bar{k}}(\bar{k}^S)$ such that the evaluation at $\bar{k}$ is the identity map. From now on until the end of the proof, we will *always* use this particular short exact sequence $0 \to G^0 \to G \to \mathrm{Spf}_{\bar{k}}(\bar{k}^S) \to 0$ over the residue field.

Now suppose that F is a divisible formal R-module and ι is an isomorphism from $\overline{F}$ to G. Then there exists a *unique* quotient map $F \longrightarrow \mathrm{Spf}_A(A^S)$ such that the induced map makes the diagram

$$\begin{array}{ccc} \overline{F} & \longrightarrow & \mathrm{Spf}_{\bar{k}}(\bar{k}^S) \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ G & \longrightarrow & \mathrm{Spf}_{\bar{k}}(\bar{k}^S) \end{array}$$

commutative. Indeed starting from one quotient map $F \longrightarrow \mathrm{Spf}_A(A^S)$, we obtain every other one by composing an isomorphism $\mathrm{Spf}_A(A^S) \to \mathrm{Spf}_A(A^S)$. Since this isomorphism is uniquely determined by the map on the evaluation at A (Proposition 2.3.3) and since $F(A) \to \mathrm{Spf}_A(A^S)(A) = S$ is same as $F(A) \to \overline{F}(\bar{A}) \to \mathrm{Spf}_{\bar{k}}(\bar{k}^S)(\bar{k}) = S$, we do indeed have the existence and the uniqueness of such quotient map. With this choice of the quotient, we have the commutativity of

$$\begin{array}{ccc} F(A) & \longrightarrow & \mathrm{Spf}_A(A^S)(A) = S \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ \overline{F}(\bar{k}) & \longrightarrow & \mathrm{Spf}_{\bar{k}}(\bar{k}^S)(\bar{k}) = S \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ G(\bar{k}) & \xrightarrow[\mathrm{id}]{} & \mathrm{Spf}_{\bar{k}}(\bar{k}^S)(\bar{k}) \end{array}$$

In particular, with this choice, $F(A) \to \mathrm{Spf}_A(A^S)(A) = S$ is the same map as $F(A) \to \overline{F}(\bar{k}) \xrightarrow{\iota} G(\bar{k}) = S$. This will be extremely useful in our construction of level structure below.

Because there is a well-defined quotient map given F and ι, it is safe to go into the language of 'extensions.'

Definition 4.3.6. Suppose (H, η, ψ) is a deformation of level n over A of G^0. Then a deformation (F, ι, Φ) of (G, ϕ) is called an *extension* of (H, η, ψ) if $F^0 = H$, $\iota|_{F^0} = \eta$, and $\Phi|_{(\pi^{-n}R/R)^h} = \psi$. As discussed above, this set-up gives us a well-defined short exact sequence $0 \to H \to F \to \mathrm{Spf}_A(A^S) \to 0$.

We say two extensions (F_i, ι_i, Φ_i) of (H, η, ψ) are *equivalent* if there exists a formal R-module homomorphism $\alpha : F_1 \to F_2$ such that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \longrightarrow & F_1 & \longrightarrow & \mathrm{Spf}_A(A^S) & \longrightarrow & 0 \\ & & \| & & {\scriptstyle \alpha}\downarrow & & \| & & \\ 0 & \longrightarrow & H & \longrightarrow & F_2 & \longrightarrow & \mathrm{Spf}_A(A^S) & \longrightarrow & 0 \end{array}$$

commutes, and ι_i's and Φ_i's are compatible via α in an obvious sense (α is then an isomorphism by the same argument as presented immediately before Proposition 2.3.6).

Proposition 4.3.7. *Let (H, ψ, η) be a deformation of level n of G^0 over A. Then the extension classes of (H, ψ, η) to a deformation (F, Φ, ι) of (G, ϕ) over A are naturally classified by the set* $\mathrm{Ext}_R\left((K/\pi^{-n}R)^j, H(\mathfrak{m}_A)\right)$.

Proof. We will give a brief overview of the proof. We will explicitly present two processes, one going from the extension classes of deformations to $\mathrm{Ext}_R((K/\pi^{-n}R)^j, H(\mathfrak{m}))$ and the other going the opposite way. Both processes will use the bijective correspondence given in Proposition 4.3.5. We will then prove that these two processes are indeed inverses of each other.

Let (F, ι, Φ) be an extension of (H, η, ψ) to a deformation of (G, ϕ). By ignoring the level structure information and using the corresponding short exact sequence, Proposition 4.3.5 tells us that this corresponds to an extension of R-modules of the form $0 \longrightarrow H(\mathfrak{m}) \to F(A) \xrightarrow{f} S \to 0$. Using the level structure, we will show that this extension of R-modules is a pull-back of a well-defined element in $\mathrm{Ext}_R((K/\pi^{-n}R)^j, H(\mathfrak{m}))$. In other words, what we need is a commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H(\mathfrak{m}) & \longrightarrow & E' & \longrightarrow & (K/\pi^{-n}R)^j & \longrightarrow & 0 \\ & & \| & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & H(\mathfrak{m}) & \longrightarrow & F(A) & \xrightarrow[f]{} & S & \longrightarrow & 0 \end{array} \tag{4.8}$$

Let $E' = F(A)/\Phi((\pi^{-n}R/R)^j)$. We will now construct $H(\mathfrak{m}) \to E'$ and $E' \to (K/\pi^{-n}R)^j$. As remarked after Definition 4.3.2, the map $g : (\pi^{-n}R/R)^j \xrightarrow{\Phi} F(A) \xrightarrow{f} (\pi^{-n}R/R)^j$ is an isomorphism. This implies $\ker f \cap \Phi((\pi^{-n}R/R)^j) = (0)$, so we have $(\ker f) = H(\mathfrak{m}) \hookrightarrow F(A)/\Phi((\pi^{-n}R/R)^j)$. Moreover, since $f(\Phi((\pi^{-n}R/R)^j))$ lies inside π^n-torsions of S, we have a well-defined R-module homomorphism $E' \longrightarrow (K/\pi^{-n}R)^j$. By construction, the above diagram commutes. We will now check exactness of the top row. $E' \longrightarrow (K/\pi^{-n}R)^j$ is surjective, as f and $S \longrightarrow (K/\pi^{-n}R)^j$ are. The composition $H(\mathfrak{m}) \to E' \to (K/\pi^{-n}R)^j$ is clearly zero. So now let $e' \in E'$ be such that its image in $(K/\pi^{-n}R)^j$ is zero. By taking a lift $\widetilde{e'} \in F(A)$, we must have $f(\widetilde{e'}) \in (\pi^{-n}R/R)^j$. Then $\Phi\left(g^{-1}(f(\widetilde{e'}))\right) \in \widetilde{e'} + \ker f$, but this is also in $\Phi((\pi^{-n}R/R)^j)$, so we conclude $e' \in \ker f \hookrightarrow E'$. Thus we have now constructed a desired element of $\mathrm{Ext}_R((K/\pi^{-n}R)^j, H(\mathfrak{m}))$ corresponding to an extension (F, ι, Φ).

If we start from two equivalent extensions (F_i, ι_i, Φ_i) of (H, η, ψ), then by Proposition 4.3.5, we obtain the same element of $\mathrm{Ext}_R(S, H(\mathfrak{m}))$, and by compatibility of the level structures, $F_1(A) \to F_2(A)$ induces $E_1' \to E_2'$ which fit into a commutative diagram of module extensions, so we can trace through the constructions and conclude that we obtain the same element of $\mathrm{Ext}_R((K/\pi^{-n}R)^j, H(\mathfrak{m}))$.

Conversely, given an extension of R-modules $0 \to H(\mathfrak{m}) \to E' \to (K/\pi^{-n}R)^j \to 0$, we will create an extension (F, ι, Φ) of (H, η, ψ). Pulling back the R-module extension by the quotient map $S \to (K/\pi^{-n}R)^j$, we get an exact sequence $0 \to H(\mathfrak{m}) \to E \to S \to 0$. By Proposition 4.3.5, we get the corresponding short exact sequence of formal R-modules $0 \to H \to F \to \mathrm{Spf}_A(A^S) \to 0$. Because the connected-étale sequence canonically splits over $\bar{k}$ (Proposition 2.3.8), there exists a unique isomorphism $\iota : \overline{F} \to G$ such that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \overline{H} & \longrightarrow & \overline{F} & \longrightarrow & \mathrm{Spf}_{\bar{k}}((\bar{k})^S) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & G^0 & \longrightarrow & G & \longrightarrow & \mathrm{Spf}_{\bar{k}}((\bar{k})^S) & \longrightarrow & 0 \end{array} \tag{4.9}$$

commutes.

By construction, we have commutativity of (4.8) in this case. Therefore $F(A)$ is identified as an R-module as $\{(e', s) \in E' \oplus S : \text{images of } e' \text{ and } s \text{ agree in } (K/\pi^{-n}R)^j\}$. Using this identification, we define

$$\Phi(t_1, t_2) = (\psi(t_1), \phi(t_1, t_2)),$$

where $t_1 \in (\pi^{-n}R/R)^h$ and $t_2 \in (\pi^{-n}R/R)^j$. Note that both $\psi(t_1)$ and $\phi(t_1, t_2)$ vanish in $(K/\pi^{-n}R)^j$, so Φ is indeed a well-defined R-module homomorphism. Since ϕ is a level structure over $\bar{k}$, $\phi(t_1, 0) = 0$, so $\Phi(t_1, 0) = \psi(t_1)$ as required. Moreover, as $(\pi^{-n}R/R)^{h+j} \xrightarrow{\Phi} F(A) \to S$ is ϕ, surjectivity to $(\pi^{-n}R/R)^j$ is also clear. Thus, Φ is a level structure for F. As remarked before, with a choice of ι making (4.9) commute,

$F(A) \to S$ is the same map as $F(A) \to \overline{F}(\overline{A}) \xrightarrow{\iota} G(\bar{k})$, so Φ does reduce to ϕ on G. Hence, we have now created an extension (F, ι, Φ) of (H, η, ψ).

Note that in the above construction of (F, ι, Φ), we had no choice at all after we obtained the short exact sequence for F. Indeed ι must make (4.9) commutative, as $\iota|_H = \eta$ and the constructed short exact sequence $0 \to H \to F \to \mathrm{Spf}_A(A^S) \to 0$ must be the specified one corresponding to F and ι. Once ι is fixed, because Φ must reduce to ϕ (via ι) and $\Phi|_{(\pi^{-n}R/R)^h} = \psi$, we have no choice but to define it as above. This is in fact a key reason for going into the language of extensions to prove Theorem 4.3.4.

If $H(\mathfrak{m}) \hookrightarrow E_i' \twoheadrightarrow (K/\pi^{-n}R)^j$ are equivalent, then their pull-backs to $H(\mathfrak{m}) \hookrightarrow E_i \twoheadrightarrow S$ are equivalent. By Proposition 4.3.5, $H \hookrightarrow F_i \twoheadrightarrow \mathrm{Spf}_A(A^S)$ are equivalent formal R-module extensions. By uniqueness of ι_i as noted above, the isomorphism $F_1 \to F_2$ and ι's are compatible. By the commutativity of the initial diagram of extensions (involving E_i'), the constructed level structures Φ_1 and Φ_2 are compatible.

Now that we have two operations, we will check that these are inverses of each other. The key is the fact that we have no choice for ι and Φ once we have the short exact sequence. Suppose we have an extension (F, Φ, ι). Tracing the construction, we create the exact sequence $0 \to H(\mathfrak{m}) \to F(A) \to S \to 0$ and letting $E' = F(A)/\Phi((\pi^{-n}R/R)^j)$, we get the exact sequence $0 \to H(B) \to E' \to (K/\pi^{-n}R)^j \to 0$. Now to go back, we pull-back, but we can certainly use $0 \to H(\mathfrak{m}) \to F(A) \to S \to 0$. So by Proposition 4.3.5, we can use the original short exact sequence involving F. But by the fact that we have no choice after fixing short exact sequence, the original ι and Φ must be the ones that we get by the construction above.

Now we compose these processes in the opposite way. Starting from an exact sequence $0 \to H(\mathfrak{m}) \to E' \to (K/\pi^{-n}R)^j \to 0$, we create the pull-back with middle term E. The level structure Φ put on the corresponding formal R-module is $\Phi(t_1, t_2) = (\psi(t_1), \phi(t_1, t_2))$. Note that under the map $E \to E'$, $\Phi(0, t_2)$ is sent to $\psi(0) = 0$, so we do indeed have a map $E/\Phi((\pi^{-n}R/R)^j) \to E'$. By following the construction of maps $H(\mathfrak{m}) \to E/\Phi((\pi^{-n}R/R)^j)$ and $E/\Phi((\pi^{-n}R/R)^j) \to (K/\pi^{-n}R)^j$, it is clear that these two extensions are equivalent.

Therefore, we get the desired one-to-one correspondence. □

Before finishing the proof of Theorem 4.3.4, we need the following fact:

Proposition 4.3.8. $\mathrm{Ext}_R(K/R, H(\mathfrak{m}_A))$ *is naturally isomorphic to* $H(\mathfrak{m}_A)$. *Therefore, we have a natural (on the second factor) isomorphism between* $\mathrm{Ext}_R((K/\pi^{-n}R)^j, H(\mathfrak{m}_A))$ *and* $H(\mathfrak{m}_A)^j$, *once we fix an isomorphism* $K/R \cong K/\pi^{-n}R$.

Proof. We will prove two things: $H(\mathfrak{m}_A)$ is a π-adically completely R-module, and $\mathrm{Ext}_{R\text{-mod}}(K/R, M) \cong M$ for all π-adically complete R-modules. For the first statement, it suffices to check that $[\pi^m]_H(y) \in \mathfrak{m}_A^{m+1}$ for all m and $y \in \mathfrak{m}_A$, since A is $\mathfrak{m}_A$-adically complete. The $m = 0$ case is clear and if we know it for m, then because $[\pi]_H(X) = \pi X + a_2 X^2 + \cdots$ and $\pi \in \mathfrak{m}_A$, we have

$$[\pi^{m+1}]_H(y) = [\pi]_H\left([\pi^m]_H(y)\right) = \pi\left([\pi^m]_H(y)\right) + a_2\left([\pi^m]_H(y)\right)^2 + \cdots \in \mathfrak{m}_A^{m+2}.$$

For the second statement, we note that $0 \to R \to K \to K/R \to 0$ induces an exact sequence

$$\mathrm{Hom}_R(K, M) \to \mathrm{Hom}_R(R, M) \to \mathrm{Ext}_R(K/R, M) \to \mathrm{Ext}_R(K, M).$$

So it suffices to prove that both the first and the last terms of the above sequence are 0. The first term is zero, since the image of any element of K under such an R-module homomorphism must lie in $\cap \pi^m M$, which is 0 by completeness. For the last term, we need to show that

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} K \longrightarrow 0$$

splits. To create a section g' of g, we need to assign $g'(\pi^{-i})$ for all $i \geq 0$ such that $\pi g'(\pi^{-i-1}) = g'(\pi^{-i})$. Pick $n_i \in N$ such that $g(n_i) = \pi^{-i}$ and let $m_i = n_i - \pi n_{i+1} \in M$. Then by completeness, we can define

$$g'(\pi^{-i}) = n_i - (m_i + \pi m_{i+1} + \pi^2 m_{i+2} + \cdots).$$

for all $i \geq 0$. This is a section of g. □

We will now finish the proof of Theorem 4.3.4. Let $(F_n^{\mathrm{univ}}, \varphi_n^{\mathrm{univ}}, \mathrm{id})$ be the universal deformation of level n of the connected component G^0. Let (F, ι, Φ) be a deformation of (G, ϕ) of level n over A. This is an extension of $(F^0, \iota|_{F^0}, \Phi_{(\pi^{-n}R/R)^h})$, so we have the corresponding element $\mathscr{E}_{(F,\iota,\Phi)} \in \mathrm{Ext}_R((K/\pi^{-n}R)^j, F^0(\mathfrak{m}_A))$ by Proposition 4.3.7. There also exists a unique map $f : D_{h,n} \to A$ of objects in $\mathscr{C}$ such that $(F^0, \iota|_{F^0}, \Phi_{(\pi^{-n}R/R)^h})$ is isomorphic as a deformation of G^0 to $f_*(F_n^{\mathrm{univ}}, \varphi_n^{\mathrm{univ}}, \mathrm{id})$. This isomorphism induces a map

$$\mathrm{Ext}_R((K/\pi^{-n}R)^j,\ F^0(\mathfrak{m}_A)) \to \mathrm{Ext}_R\left((K/\pi^{-n}R)^j,\ \left(f_*(F_n^{\mathrm{univ}})\right)(\mathfrak{m}_A)\right),$$

and let $\mathscr{E}$ be the image of $\mathscr{E}_{(F,\iota,\Phi)}$ under this map. Because equivalent extensions of the same deformation of G^0 are clearly isomorphic as deformations, using Proposition 4.3.7 again, the extension of $f_*(F_n^{\mathrm{univ}}, \varphi_n^{\mathrm{univ}}, \mathrm{id})$ corresponding to $\mathscr{E}$ is isomorphic as a deformation to (F, ι, Φ). Note that because of the way we fixed the quotient map $F \to \mathrm{Spf}_A(A^S)$ (given ι) we force the commutativity of

$$\begin{array}{ccccc} F_1^0 & \longrightarrow & F_1 & \longrightarrow & \mathrm{Spf}_A(A^S) \\ {\scriptstyle\cong}\downarrow & & {\scriptstyle\alpha}\downarrow & & \| \\ F_2^0 & \longrightarrow & F_2 & \longrightarrow & \mathrm{Spf}_A(A^S) \end{array}$$

whenever $\alpha : F_1 \to F_2$ is an isomorphism of deformations. Thus isomorphic deformations are indeed getting sent to the same $\mathscr{E}$ by construction. Using Proposition 4.3.8, $\mathscr{E}$ is naturally sent to an element of $\mathfrak{m}_A^j$. Because isomorphic deformations with the same connected component are certainly equivalent (again because of the way we fix the quotient map) as extensions, different elements of $\mathfrak{m}_A^j$ do correspond to different isomorphism classes of deformations.

Therefore we have now shown that the set of deformations of level n of G over A is naturally in bijection with the set of maps $D_{h,n}[\![\mho_1, \ldots, \mho_j]\!] \to A$ in $\mathscr{C}$. Thus $E_{h,n,j} \cong D_{h,n}[\![\mho_1, \ldots, \mho_j]\!]$, which is a regular local ring of dimension $h + j$ by Theorem 4.2.4. We are finally done with proving Theorem 4.3.4.

In particular note that $E_{h,0,j} \cong \widehat{R}^{\mathrm{nr}}[\![\beth_1, \ldots, \beth_{h-1}, \mho_1, \ldots, \mho_j]\!]$. This is formally smooth over $\widehat{R}^{\mathrm{nr}}$.

Chapter 5

Applications of Deformation Theory

In this chapter we discuss two applications of deformation theory. The first application is that to local class field theory, in particular to the Lubin-Tate theory. It turns out that we can prove the two main propositions of the Lubin-Tate theory by the deformation theory of Chapter 4. Although it is not very difficult to prove these two propositions directly, this approach has the advantage that we can see them as the 'height = 1' special case of the formal module theory.

The second application is Drinfel'd's original purpose of developing this deformation theory of formal R-modules, namely that to the global function fields. Although we will not discuss this application in detail, we will try to give a feeling of how knowledge of various universal deformation rings that we constructed in Chapter 4 is helpful in this application.

5.1 Applications to Local Class Field Theory

In this section, we will consider how Drinfel'd's deformation theory of formal modules can be used to derive Lubin-Tate theory of the local class field theory. We continue the notations of Chapter 4: K for a local field, R for the valuation ring, π a uniformizer of R, $k = R/(\pi)$ is a field with q elements (a power of p), K^{nr} is the maximal unramified extension (after fixing the algebraic closure) with valuation ring R^{nr}, and $\widehat{K}^{\mathrm{nr}}$ is the completion of K^{nr} whiose valuation ring is $\widehat{R}^{\mathrm{nr}}$.

There are two fundamental theorems in local class field theory: the isomorphism theorem which states $\mathrm{Gal}(L/K) \cong K^*/N_{L/K}(L^*)$ for every abelian extension L/K of local fields, and the existence theorem which states that every open and finite-indexed subgroup of K^* is $N_{L/K}(L^*)$ for some abelian extension L/K. By these, we have a one-to-one correspondence between the abelian extensions of K and open and finite-indexed subgroups of K^*. The problem is, though, if we start from an open and finite-indexed subgroup of K^*, it is often extremely difficult to construct the corresponding abelian extension of K. Neither the cohomology method (as in [25] or [26]) nor the character-theoretic method (as in [23]) gives us these concrete constructions of abelian extensions.

To fix this problem, the Lubin-Tate theory was developed [18]. With this theory, we can explicitly construct abelian extensions K_π^n of K corresponding to the norm subgroup $\langle \pi \rangle \times U_K^{(n)}$, where $U_K^{(n)}$ is the n-th higher unit group. From this, we can show $\left(\bigcup K_\pi^n\right) K^{\mathrm{nr}}$ is the maximal abelian extension of K, thus obtaining a satisfactory explicit description of the maximal abelian extension. Moreover, Lubin-Tate theory also gives an explicit description of the Artin reciprocity map.

For construction of K_π^n and proof of the above properties, Lubin and Tate exploits a general principle of class field theory, which is to establish a connection between prime elements and Frobenius maps. This connection is done through the notion of formal R-modules, as follows:

Proposition 5.1.1. *If $f \in R[\![X]\!]$ such that $f \equiv \pi X \pmod{\text{poly. deg. } 2}$ and $f \equiv X^q \pmod{\pi}$, then there exists a unique formal R-module F_f over R such that $[\pi]_{F_f}(X) = f$.*

f satisfying the conditions in the above proposition is called a **Lubin-Tate series**, and the set of all such series is denoted by $\mathcal{F}_\pi$. The proofs of Lubin-Tate theory are essentially done by using one Lubin-Tate series, namely $f = \pi X + X^q$, but in specific examples (such as over $\mathbb{Q}_p$, we would want to use $(1+X)^p - 1$ to get the cyclotomic field), it is useful to be able to choose from $\mathcal{F}_\pi$.

For construction of the Artin reciprocity map, we need to know that the construction does not depend on the choice of the uniformizer. The following is the essential:

Proposition 5.1.2. *Let σ be the continuous extension of the Frobenius automorphism of $\mathrm{Gal}(K^{\mathrm{nr}}/K)$ to $\widehat{K}^{\mathrm{nr}}$. Let π, ω be two uniformizers of R such that $\omega = \pi u$, and let $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\omega$. Then there exists an isomorphism $\alpha \in \widehat{R}^{\mathrm{nr}}[\![X]\!]$ from F_f to F_g of formal R-modules such that $\sigma_*(\alpha) = \alpha \circ [u]_{F_f}$.*

These are the two main propositions of the Lubin-Tate theory. The usual method of proving these use successive approximation together with surjectivity of $u \mapsto \frac{\sigma(u)}{u}$ in $U_{\widehat{K}^{\mathrm{nr}}}$ ([22], [25]). We will now give the proof of these propositions using Drinfel'd's theory of deformation of formal R-modules.

Proof of Proposition 5.1.1. By Proposition 3.3.2, a normal formal R-module over $\bar{k}$ of height 1 corresponds to some $R[\Upsilon_1, \ldots] \to \mathbb{F}_q$, so by lifting image of each Υ_i, we get a formal R-module F_2 over R such that

$$[\pi]_{F_2}(X) \equiv f \pmod{\text{poly. deg. } 2}, \quad \text{and} \quad [\pi]_{F_2}(X) \equiv X^q \pmod{\pi}.$$

Suppose we have constructed up to F_n such that

$$[\pi]_{F_n}(X) \equiv f \pmod{\text{poly. deg. } n} \quad \text{and} \quad [\pi]_{F_n}(X) \equiv X^q \pmod{\pi}.$$

The image $F_{n+1,r}$ of F_n via the isomorphism $\varphi = (X + rX^n)^{-1}$ with $r \in R$ has the property that $[\pi]_{F_{n+1,r}}(X) \equiv X^q \pmod{\pi}$ and $[\pi]_{F_{n+1,r}}(X) \equiv [\pi]_{F_n}(X) + (r\pi - r\pi^n)X^n \pmod{\text{poly. deg. } n+1}$, so $f \equiv [\pi]_{F_n} \pmod{\pi}$ from the inductive hypothesis gives us the suitable r to continue induction. We are done by taking limit of the formal R-modules F_n.

Uniqueness is successive application of Proposition 3.3.4 and the fact that R is an integral domain. □

Proof of Proposition 5.1.2. Both $\overline{F_f}$ and $\overline{F_g}$ are height 1 formal R-modules over $\bar{k}$, so by Theorem 3.3.11, there exists an isomorphism $\overline{\alpha} : \overline{F_f} \to \overline{F_g}$. Thus, $(F_f, \overline{\alpha})$ and (F_g, id) are both deformations of $\overline{F_g}$ in the sense of Definition 4.1.1, so by Theorem 4.1.7 applied to $h = 1$, there must exist an isomorphism of formal R-modules $\alpha : F_f \to F_g$ over $\widehat{R}^{\mathrm{nr}}$ which reduces to $\overline{\alpha}$ modulo $\mathfrak{m}_{\widehat{R}^{\mathrm{nr}}}$. Clearly, $\alpha \circ [u]_{F_f}$ defines a formal R-module homomorphism from F_f to F_g, and because σ fixes all elements of R and F_f is defined over R, it follows that $\sigma_*(\alpha)(F_f(X,Y)) = \sigma_*(\alpha(F_f(X,Y))) = \sigma_*(F_g(\alpha(X), \alpha(Y))) = F_g(\sigma_*(\alpha)(X), \sigma_*(\alpha)(Y))$. Similarly, $\sigma_*(\alpha)([r]_{F_f}(X)) = [r]_{F_g}(\sigma_*(\alpha)(X))$, so $\sigma_*(\alpha)$ is a formal R-module homomorphism from F_f to F_g. On the residue field, we have

$$\overline{\sigma_*(\alpha)}(X^q) = (\overline{\alpha}(X))^q = \overline{[\omega]}_{F_g}(\overline{\alpha}(X)) = \overline{\alpha}(\overline{[\omega]}_{F_f}) = \overline{\alpha}(\overline{[u]}_{F_f}(X^q)),$$

so $\overline{\sigma_*(\alpha)}(X) = \overline{\alpha \circ [u]}_{F_f}(X)$ on the residue field, so by Proposition 4.1.3, we obtain $\sigma_*(\alpha) = \alpha \circ [u]_{F_f}$. □

Once we have these two propositions, we can simply follow [22] and [25], as below. Let us denote $\mathfrak{m} = \mathfrak{m}_{\overline{K}}$. Since we have R-modules $F_f(\mathfrak{m}_L)$ for each finite extension L/K in a compatible manner, $M_f = F_f(\mathfrak{m})$ is also an R-module. Let E_f^n denote the *π^n-division points* of the module M_f, i.e.

$$E_f^n = \{\lambda \in \mathfrak{m} : [\pi^n]_{F_f}(\lambda) = 0\},$$

and let $K_f^n = K(E_f^n)$. By Proposition 5.1.2 applied with $\omega = \pi$, for $f, g \in \mathcal{F}_\pi$, there is an isomorphism α of formal R-modules F_f and F_g over $\mathscr{O}_{\widehat{K}^{\mathrm{nr}}}$ with $\sigma_*(\alpha) = \alpha$ (so α has coefficients in R). Thus, α sends π^n-division points of F_f to that of F_g, so we see $K_f^n = K_g^n$. We will denote this common field by K_π^n. Using the two propositions above, we have

Theorem 5.1.3. (a) $E_f^n \cong R/(\pi^n)$ *as* R*-modules. So we have* $\mathrm{Aut}(E_f^n) \cong U_K/U_K^{(n)}$.
(b) K_π^n *is a totally ramified abelian extension of* K*. If* f *is of the form* $X^q + \pi(a_{q-1}X^{q-1} + \cdots + a_2X^2) + \pi X$*, every element in* $E_f^n \backslash E_f^{n-1}$ *is a prime element of* K_π^n *whose minimal polynomial is an Eisenstein polynomial*

$$g_n = \frac{f^{(n)}(X)}{f^{(n-1)}(X)} = (f^{(n-1)}(X))^{q-1} + \pi\left(a_{q-1}(f^{(n-1)}(X))^{q-2} + \cdots + a_2(f^{(n-1)}(X))\right) + \pi \in \mathscr{O}_K[X],$$

where $f^{(n)}(X) = f \circ \cdots \circ f$ n *times. Moreover,* $\mathrm{Gal}(K_\pi^n/K) \cong \mathrm{Aut}(E_f^n)$ *by the natural restriction map.*
(c) $N_{K_\pi^n/K}((K_\pi^n)^*)$ *contains* $\langle\pi\rangle \times U_K^{(n)}$.

Proof. For (a) and (b), see [22] or [25]. For (c), see [14, Lemma 5.15]. □

Using the isomorphism theorem and counting degrees, we now see that $N_{K_\pi^n/K}((K_\pi^n)^*) = \langle\pi\rangle \times U_K^{(n)}$. Using this and $N_{K_n/K}(K_n^*) = \langle\pi^n\rangle$ for the unramified extension K_n/K of degree n, corollaries of the isomorphism and existence theorems (such as $N(L_1 \cdot L_2) = N(L_1) \cap N(L_2)$) show that $(\bigcup K_\pi^n)\, K^{\mathrm{nr}}$ is the maximal abelian extension K^{ab} of K (see [22, Corollary V.5.7] for details).

We can also express the Artin reciprocity map in terms of K_π^n. Note that $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{\mathrm{nr}}/K)$, where $K_\pi = \bigcup K_\pi^n$. For any f satisfying the conditions of Theorem 5.1.3 (b), let $[u]_f$ denote the unique element of $\mathrm{Gal}(K_\pi/K)$ whose restriction to E_f^n agrees with $[u]_{F_f}$ for all n. We can now define a well-defined group homomorphism $r_f : K^* \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ by
(1) $r_f(\pi) = \mathrm{id}$ on K_π and Frobenius σ on K^{nr},
(2) For $u \in U_K$, $r_f(u) = [u^{-1}]_f$ on K_π and id on K^{nr}.
We will now check that if we use another uniformizer $\omega = \pi u$ and $g \in \mathcal{F}_\omega$, $r_f = r_g$. Since uniformizers generate K^*, it suffices to check $r_f(\omega) = r_g(\omega)$. Thus we need to show $r_f(\omega) = \mathrm{id}$ on K_ω, so let $\lambda \in E_g = \bigcup E_g^n$. Letting α be the formal R-module isomorphism over $\widehat{R}^{\mathrm{nr}}$ from F_f to F_g obtained from Proposition 5.1.2, we know that $\lambda = \alpha(\mu)$ for some $\mu \in E_f$. So what we need to check is $r_f(\omega)(\alpha(\mu)) = \alpha(\mu)$. But since α has coefficients in $\widehat{R}^{\mathrm{nr}}$, we have

$$r_f(\omega)(\alpha(\mu)) = \sigma_*(\alpha)(r_f(\omega)(\mu)) = \sigma_*(\alpha)(r_f(\pi) \circ r_f(u)(\mu)) = \sigma_*(\alpha)([u^{-1}]_f(\mu)) = \alpha(\mu).$$

So indeed, $r_f = r_g$, and because of the property that $r(\pi)$ is identity on corresponding K_π and Frobenius on K^{nr} for each uniformizer π, this must agree with the reciprocity map.

Remark. If we did not assume the isomorphism and existence theorems of local class field theory, we could actually *prove* them using K_π^n ([12], [14]). After establishing Theorem 5.1.3, we can obtain $N(K_\pi^n) = \langle\pi\rangle \times U_K^{(n)}$ by Coleman's Norm operator [14] or by 'denseness' of separable polynoamials [12]. We can also prove the Hasse-Arf theorem by elementary congruences as in [24]. Then using $\mathrm{Gal}(K_\pi^n/K)^n = \{1\}$ as in [9] and a general fact that $\mathrm{Gal}(L/K)^n = \{1\} \Longrightarrow |\,\mathrm{Gal}(L/K)_0| \leq q^{n-1}(q-1)$ for an abelian extension L/K, we can show that any finite abelian extension is contained in $K_\pi K^{\mathrm{nr}}$. From these information, we can prove the two fundamental theorems of local class field theory, using the above description of the Artin reciprocity map ([14, Chapter VI]).

5.2 Applications to the Arithmetic of Function Fields

Now we will briefly discuss Drinfel'd's original purpose for developing the deformation theory of formal R-modules, namely the study of global function fields. As discussed in the introduction, Drinfel'd was interested in proving the analogues of the fundamental theorem of Complex Multiplication and the Langlands Conjecture for a global function field K. For this, Drinfel'd introduces the notion of **elliptic $\mathscr{O}_K$-modules** of rank d over a scheme S (now in the literature, these are called **Drinfel'd modules**). Further, Drinfel'd defines a **level structure** for each ideal $I \subseteq \mathscr{O}_K$, and defines a **modular variety** M_I^d to be the one which represents (i.e. 'parametrizes') the functor $S \rightsquigarrow$ the set of Drinfel'd $\mathscr{O}_K$-modules (up to isomorphism) of rank d with structure of level I over S.

Since it is hard to directly study the modular variety (which contains information about 'all' the Drinfel'd modules simultaneously), it is helpful to study locally at first at Drinfel'd modules which are 'close' to a given one. The local analysis of Drinfel'd $\mathscr{O}_K$-modules leads to studying deformations of divisible formal $(\mathscr{O}_K)_v$-modules for each $v \in \operatorname{Spec} \mathscr{O}_K$ (here each v is viewed as a place), which have already been discussed in detail in Section 4.3. In essence, any 'local' properties of the modular varieties that one wants to prove can be proved using the local deformation theory. For example, as smoothness and flatness are local properties, the proof of the smoothness of M_I^d over $\operatorname{Spec} A - V(I)$ (where $V(I)$ as usual denotes primes which contain I) and flatness of $M_J^d \to M_I^d$ for $J \subseteq I$ do reduce to the nice properties of the universal deformation ring that we have obtained in Theorem 4.3.4 ([5, Corollary of Proposition 5.4]). Furthermore, using a similar reduction process to the local deformation theory, Drinfel'd defines a group action on the (global) modular variety locally by using Proposition 4.2.7. So the local deformation theory lies at the foundation of Drinfel'd's study of global function fields.

As discussed in [10], the arithmetic of function fields developed dramatically since this Drinfeld's paper. It was particularly influential in the explicit class field theory for the function fields which Hayes and others developed. Moreover, even outside the strict realm of global function fields, Drinfel'd's ideas of the 'full level structures' over a general scheme gave a new interpretation to reduction modulo p of the moduli space of elliptic curves with N-level structure where $p \mid N$, and in fact, [16] uses this idea of level structures to the study of moduli spaces of elliptic curves.

Thus, [5] is an extremely important paper, proving analogues of theorems of number fields in the equi-characteristic global function fields case, and significantly contributing to the development of study of function fields and other areas of math. At the basis of this is the local deformation theory of formal R-modules which has been presented in detail in the previous chapters, and it is the author's hope that both beauty and the importance of this theory have been conveyed to the reader.

Appendix A

Profinite Modules and Commutative Formal Group Schemes

In this appendix, we will briefly discuss some properties and proof techniques concerning profinite modules and commutative formal group schemes. We will omit many proofs here. Since we pick out only things that are needed for this thesis, this is not necessarily the best approach to take (for instance, many of the following hold in more generality, where proofs are simplified). For complete proofs and for a more coherent and thorough approach, see [3] (which is based on SGA3).

A.1 Preliminary

Suppose A is a topological ring which has a base of opens around 0 consisting of ideals. We define $\widehat{A} = \varprojlim A/\mathfrak{a}$, where $\mathfrak{a}$ runs through all the open ideals with the directed system being the reverse inclusion. Such an A is said to be **pseudocompact** if the natural continuous map $A \longrightarrow \widehat{A}$ is a topological isomorphism and $A/\mathfrak{a}$ is an artinian ring for all open ideals $\mathfrak{a}$. Similarly, given a topological A-module M with base of opens around 0 given by A-submodules, we define $\widehat{M} = \varprojlim M/M'$, where M' runs through all the open A-submodules. We say such an M is **profinite** if the natural continuous map $M \longrightarrow \widehat{M}$ is a topological isomorphism and each M/M' is a finite-length A-module. We denote the category of profinite A-modules by PF_A. We call an A-algebra B **profinite** if B is profinite as an A-module; the category of all such A-algebras is denoted by $\mathcal{PA}_A$.

From now on, A will denote a pseudocompact ring, and all modules are assumed to be profinite. The aim of the notion of pseudocompactness is to preserve some nice properties of artin rings in a framework which is stable under formation of inverse limits. Therefore, properties which hold for artin rings usually hold for pseudocompact rings if we insert the word 'open' in the appropriate places. For instance, every open prime of a pseudocompact ring is maximal. On the other hand, pseudocompact rings are often huge (such as arbitrary products of complete noetherian local rings with the product topology). Such rings naturally arise in the context of étale formal groups.

For a profinite A-module M and an element m of an open submodule M', $0 \cdot m \in M'$ implies that there exists an open ideal $\mathfrak{a}$ of A such that $\mathfrak{a} \cdot m \subseteq M'$. Since M/M' is a finite A-module, by taking a finite intersection of such $\mathfrak{a}$'s, we conclude that there exists an open ideal $\mathfrak{b}$ such that $\mathfrak{b}M \subseteq M'$. Thus, each quotient of M by an open submodule is finite over an artinian ring (thus it is artinian). By this argument, we see that every object of $\mathcal{PA}_A$ is pseudocompact.

In general, inverse limits are only left-exact. But if $\{M_\alpha\} \longrightarrow \{N_\alpha\}$ is a map between two systems of A-modules such that $M_\alpha \longrightarrow N_\alpha$ is surjective with kernel an artinian module for each α, we can show that $\varprojlim M_\alpha \longrightarrow \varprojlim N_\alpha$ is also surjective by the use of Zorn's lemma (this is one of the places where the artinian assumption is crucial, as it ensures a kind of "Mittag-Leffler" property). From this, it follows that given any closed submodule N of $M \in \mathrm{PF}_A$, N and M/N are in PF_A with the subspace and quotient topologies,

respectively. Further, any map between objects in PF_A is closed and PF_A is an abelian category where monomorphisms are injective maps and epimorphisms are surjective maps ([3, Theorem 1.2.2] for all of the above).

Since $A \cong \widehat{A}$ implies that the intersection of all open ideals is (0), when A is artinian, it follows that (0) is open (i.e. the topology is discrete). We would like to have a localization which behaves well topologically, so it makes sense to define localization of an artinian ring as the algebraic localization with the discrete topology and to define localization of a psueudocompact ring as their inverse limit. In other words, for a pseudocompact ring A and an open maximal ideal $\mathfrak{m}$, we define

$$\widetilde{A_{\mathfrak{m}}} = \varprojlim (A/\mathfrak{a})_{\mathfrak{m}/\mathfrak{a}},$$

where the limit is taken over all open ideals $\mathfrak{a} \subseteq \mathfrak{m}$. Since the inverse limit of profinite A-algebras is again a profinite A-algebra ([3, Corollary 1.2.3]), $\widetilde{A_{\mathfrak{m}}}$ is a profinite A-algebra (thus, it is pseudocompact). Moreover, using the structure theorem of artinian rings, it follows that A is isomorphic to $\prod \widetilde{A_{\mathfrak{m}}}$ where the product is taken over open maximals. Moreover, by the universal property (and using that $\widetilde{A_{\mathfrak{m}}}$ is local), it follows that $\widetilde{A_{\mathfrak{m}}}$ is the algebraic localization $A_{\mathfrak{m}}$ if we ignore the topology ([3, Theorem 1.2.5]). From now on, we will write $A_{\mathfrak{m}}$ for the topological localization as well. This isomorphism $A \cong \prod A_{\mathfrak{m}}$ enables us to reduce many proofs to the local case. Using this decomposition, we can show that the set τ of **topological nilpotents** ($a \in A$ with $a^n \to 0$) satisfy $A/\tau \cong \prod A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$ where the product is over the open maximals ([3, Corollary 1.2.6]).

For any topological A-modules M, N, we can define **completed tensor product**

$$M \widehat{\otimes}_A N = \varprojlim (M/M') \otimes_A (N/N')$$

where triples of opens $\{(\mathfrak{a}, M', N') : \mathfrak{a}M \subseteq M', \mathfrak{a}N \subseteq N'\}$ are made into a directed system by reverse inclusion. $\widehat{\otimes}$ has the usual universal property (with the additional continuity assumption). $\widehat{\otimes}$ also has the usual base change properties: for a pseudocompact ring A, a pseudocompact A-algebra B, a pseudocompact B-algebra C, and $M, N \in \mathrm{PF}_A$, we have $M \widehat{\otimes}_A N \in \mathrm{PF}_A$, $M \widehat{\otimes}_A B \in \mathrm{PF}_B$, $(M \widehat{\otimes}_A B) \widehat{\otimes}_B C \cong M \widehat{\otimes}_A C$ ([3, Theorem 1.1.8 and Corollary 1.3.8]). As we expect, the functor $M \widehat{\otimes}_A : \mathrm{PF}_A \to \mathrm{PF}_A$ is right-exact and we have natural isomorphisms

$$M \widehat{\otimes}_A \left(\prod_{i \in I} N_i \right) \cong \prod_{i \in I} \left(M \widehat{\otimes}_A N_i \right), \qquad M \widehat{\otimes}_A \left(\varprojlim N_i \right) \cong \varprojlim (M \widehat{\otimes}_A N_i),$$

$$M \cong \prod (M \widehat{\otimes}_A A_{\mathfrak{m}}), \quad \text{and} \quad \mathrm{Hom}_{\mathrm{PF}_A}(M, N) \cong \prod \mathrm{Hom}_{\mathrm{PF}_{A_{\mathfrak{m}}}}(M \widehat{\otimes}_A A_{\mathfrak{m}}, N \widehat{\otimes}_A A_{\mathfrak{m}}),$$

where the product in the last line is over all open maximals of A ([3, Theorem 1.3.1]). When $B \in \mathcal{PA}_A$ is used instead of M, we get the similar decomposition of $\mathrm{Hom}_{\mathcal{PA}_A}$. This shows that $M \widehat{\otimes}_A A_{\mathfrak{m}}$ is the algebraic localization as modules (by universal property). All of these results are crucial, since they enable us to analyze each local part separately.

One advantage of going to the local case, as in the usual commutative ring case, is Nakayama's lemma. For a pseudocompact local A with the unique (thus, open by $A \cong \widehat{A}$) maximal ideal $\mathfrak{m}$, $\overline{\mathfrak{m}M} = M$ implies $M = 0$ for a profinite A-module ([3, Theorem 1.3.2]). Thus, $M \widehat{\otimes}_A (A/\mathfrak{m}) \cong M/\overline{\mathfrak{m}M} = 0$ implies $M = 0$. This is a powerful tool which allows us to analyze our situation over formal closed fiber. For instance, if $M \to N$ is a map of PF_A with N a projective object and the induced map $M \widehat{\otimes}_A (A/\mathfrak{m}) \to N \widehat{\otimes}_A (A/\mathfrak{m})$ is an isomorphism, then $M \cong N$ ([3, the proof of Theorem 1.3.6]). Also, if B is a local ring which is a profinite A-algebra, then the inverse image in A of $\mathfrak{m}_B$ is an open prime in A, so the map $A \to B$ is local, and $B/\mathfrak{m}_B$ is a finite extension field of $A/\mathfrak{m}_A$.

We say $M \in \mathrm{PF}_A$ is **topologically free** if $M \cong \prod Ae_i$, M is **topologically flat** if $M \widehat{\otimes}_A$ is exact on PF_A, and M is **topologically faithfully flat** if a sequence of PF_A is exact if and only if the sequence $\widehat{\otimes}_A M$ is exact. Using the above properties of $\widehat{\otimes}$ together with Nakayama/projectivity arguments and Zorn's lemma, we can show that $M \in \mathrm{PF}_A$ is a projective object $\iff$ M is topologically flat $\iff$ $M_{\mathfrak{m}}$ is topologically free over $A_{\mathfrak{m}}$ for each open maximal $\mathfrak{m}$ ([3, Theorem 1.3.6]). Further, M is topologically faithfully flat if and

only if it is topologically flat and $M_{\mathfrak{m}} \neq 0$ for all open maximals; in particular, $B \in \mathcal{PA}_A$ is topologically faithfully flat over A if and only if it is topologically flat and the map $A \to B$ is injective ([3, Corollary 1.3.7]). Thus, these conditions can be checked locally. We can also show by the usual method that $B \in \mathcal{PA}_A$ is topologically faithfully flat if and only if it is topologically flat and $B \widehat{\otimes}_A M = 0$ implies $M = 0$ for every $M \in \mathrm{PF}_A$. Finally, using the Nakayama/projectivity argument, we can prove the 'fiber-by-fiber' criterion for topological flatness ([3, Theorem 2.3.2]):

Theorem A.1.1. *A map $B_1 \longrightarrow B_2$ between topologically flat profinite A-algebras is topologically flat if and only if it is topologically flat on the formal fiber over all open maximals of A (i.e. after applying $\widehat{\otimes}_A(A/\mathfrak{m})$ for all open maximals $\mathfrak{m}$).*

A.2 Formal Schemes

Let $\mathcal{F}_A$ be the category of profinite A-algebras which are artinian as a ring (this is the 'finite quotient part' of $\mathcal{PA}_A$). Given a covariant functor $X : \mathcal{F}_A \to \mathbf{Set}$, by letting $X'(B) = \varprojlim X(B/\mathfrak{b})$ where inverse limit runs through all open ideals of $B \in \mathcal{PA}_A$, we obtain a functor $X' : \mathcal{PA}_A \to \mathbf{Set}$. We can show ([3, Theorem 1.4.2]) that this functor commutes with inverse limits (i.e. $X'(\varprojlim B_i) = \varprojlim X'(B_i)$ for every inverse systems of elements in $\mathcal{PA}_A$). This $X \rightsquigarrow X'$ defines an equivalence between the category of covariant functors $\mathcal{F}_A \to \mathbf{Set}$ and the category of covariant functors $\mathcal{PA}_A \to \mathbf{Set}$ which are 'continuous' in the sense that they commute with inverse limits, where the inverse process is given by the restriction (in both categories, the morphisms are the natural transformations). Note that the representable functors $\mathrm{Hom}_{\mathcal{PA}_A}(B, -)$ are 'continuous'. We define a **formal scheme over** A to be a covariant functor $\mathrm{Spf}_A(B) : \mathcal{F}_A \to \mathbf{Set}$, which is the restriction of $\mathrm{Hom}_{\mathcal{PA}_A}(B, -)$ to $\mathcal{F}_A$ for some $B \in \mathcal{PA}_A$. In other words, a formal scheme is a functor on $\mathcal{F}_A$ which is representable by a *pro*finite object. The above discussion together with Yoneda's lemma shows that $\mathrm{Hom}_{\mathcal{PA}_A}(B_2, B_1)$ is naturally isomorphic to $\mathrm{Hom}(\mathrm{Spf}_A(B_1), \mathrm{Spf}_A(B_2))$. By the universal property of completed tensor product and Yoneda's lemma, $\mathrm{Spf}_A(B_1) \times \mathrm{Spf}_A(B_2)$ is naturally isomorphic to the functor $\mathrm{Spf}_A(B_1 \widehat{\otimes}_A B_2)$, and for $A' \in \mathcal{PA}_A$, the restriction of the functor $\mathrm{Spf}_A(B)$ to $\mathcal{F}_{A'}$ is naturally isomorphic to the functor $\mathrm{Spf}_{A'}(A' \widehat{\otimes}_A B)$. Thus, the formal schemes over A form a "category" in which products and the final object (i.e. $\mathrm{Spf}_A(A)$) exist.

One of the reasons for wanting to deal with profinite objects (with large index set) is to have the following nice representability theorem of Grothendieck. We won't need this, but mention it in passing ([3, Theorem 1.4.7]).

Theorem A.2.1. *A covariant functor $X : \mathcal{F}_A \to \mathbf{Set}$ is a formal scheme over A if and only if it is left exact and commutes with products.*

A.3 Duality and Commutative Group Schemes

We will first talk about the duality of profinite modules. Suppose A is an artin local ring (which is pseudocompact with the discrete topology) with maximal ideal $\mathfrak{m}$ and M is a topologically flat profinite A-module. Since $A = A_{\mathfrak{m}}$, M must be topologically free (see section A.1), so $M \cong \prod Ae_i$. For any element $\varphi \in \mathrm{Hom}_{\mathrm{PF}_A}(M, A)$, $\varphi^{-1}(0)$ is open, so φ factors through a finite product of A's. Hence, if we write $M^D = \mathrm{Hom}_{\mathrm{PF}_A}(M, A)$, then M^D is an A-module which is the direct sum of A's with the same index set as the original product for M. Conversely, starting from a free A-module N, we can define $N^D = \mathrm{Hom}_A(N, A)$, where we define open submodules to be the annihilators of finite-length submodules of N. This makes $N^D \cong \prod Ae_i$ with the same index set as that for N, so N^D is an object of PF_A which is topologically free. Because free objects in the category of A-modules (resp. topologically flat objects in PF_A) are projective in their respective categories (see Section A.1), every exact sequence splits in each category. Moreover, (resp. completed) tensor product commutes with direct sums (resp. products). Hence, we have the following ([3, Theorem 1.3.4]):

Theorem A.3.1. *Assume A is an artin local ring. For a topologically flat $M \in \mathrm{PF}_A$ and a free A-module N, $M \longrightarrow M^{DD}$ and $N \longrightarrow N^{DD}$ are natural isomorphisms. Moreover, the functors $(-)^D$ take exact sequences of free A-modules (resp. topologically flat profinite A-modules) to exact sequences of topologically*

flat profinite A-modules (resp. free A-modules). $(-)^D$ also interchange direct products with direct sums. Further, $(M')^D \otimes_A M^D \longrightarrow (M' \widehat{\otimes}_A M)^D$ and $(N')^D \widehat{\otimes}_A N^D \longrightarrow (N' \otimes_A N)^D$ are natural isomorphisms.

As a consequence of this duality, we can prove that the functors $(-)^D$ take commutative group objects which are free (resp. topologically flat) to commutative group objects which are topologically flat (resp. free) by the same argument as in the proof of Cartier duality ([31, page 17]).

When $A = k$ is a field, we call a commutative group object in the category of affine (resp. formal) schemes over k to be a **commutative affine** (resp. **formal**) **group scheme**. This is the simplest case, and the questions about group objects over more general A will often be reduced to the case over fields by base change, so it is fortunate that we have the following theorem ([3, Theorem 2.1.4]):

Theorem A.3.2. *The category of affine (resp. formal) commutative group schemes is abelian, with monomorphisms being the surjections on rings and epimorphisms being the (resp. topologically) faithfully flat maps on rings.*

Now, we assume that A is a pseudocompact *local* ring, with the maximal ideal $\mathfrak{m}$. This is more complicated than the field case, since in general we will not be able to conclude that the category is abelian. But we do want to have a concept of a short exact sequence, so we will now define this with a bit more care. Note that in our discussion of duality, having flatness was important. So we actually define **commutative formal group scheme** over A to be a commutative group object in the category of formal schemes such that it is also *topologically flat* over A. We then say that a sequence of commutative formal group schemes

$$0 \to \mathrm{Spf}_A(B_1) \to \mathrm{Spf}_A(B_2) \to \mathrm{Spf}_A(B_3) \to 0 \tag{A.1}$$

is a **short exact sequence** if the composition of the two maps is zero, $\mathrm{Spf}_A(B_1) \to \mathrm{Spf}_A(B_2)$ is a closed immersion (i.e. $B_1 \leftarrow B_2$ is surjective), $\mathrm{Spf}_A(B_2) \to \mathrm{Spf}_A(B_3)$ is topologically faithfully flat, and $\mathrm{Spf}_A(B_1)$ is the kernel of $\mathrm{Spf}_A(B_2) \to \mathrm{Spf}_A(B_3)$ (i.e. $B_1 \leftarrow B_2 \widehat{\otimes}_{B_3} A$ is an isomorphism).

We will now show that (A.1) is a short exact sequence if and only if the composition of the two maps is zero and it is a short exact sequence modulo the maximal ideal $\mathfrak{m}$ (i.e. after applying $\widehat{\otimes}_A(A/\mathfrak{m})$, where we are now working inside an abelian category). The formal Nakayama shows that $\mathrm{Spf}_A(B_1) \to \mathrm{Spf}_A(B_2)$ is a closed immersion if and only if it is so over the closed fiber. If $B_2 \leftarrow B_3$ is topologically faithfully flat, then so is the map over the closed fiber. Conversely, by Theorem A.1.1, we know topological flatness of $B_2 \leftarrow B_3$ knowing topological flatness over the closed fiber, so we just need to show that $B_2 \widehat{\otimes}_{B_3} M = 0$ implies $M = 0$ for $M \in \mathrm{PF}_{B_3}$. But this follows from $0 = (A/\mathfrak{m}) \widehat{\otimes}_A B_2 \widehat{\otimes}_{B_3} M \cong \left((A/\mathfrak{m}) \widehat{\otimes}_A B_2\right) \widehat{\otimes}_{A/\mathfrak{m} \widehat{\otimes}_A B_3} \left(A/\mathfrak{m} \widehat{\otimes}_A M\right)$ and Nakayama's lemma. Finally, because B_1 is topologically flat, Nakayama/projectivity argument shows that $B_1 \leftarrow B_2 \widehat{\otimes}_{B_3} A$ is an isomoprphism if and only if it is so over the closed fiber. Hence by Theorem A.3.2, we have now proved the equivalence of these two notions of a short exact sequence of commutative formal group schemes. We will use the more convenient definition for each occasion in this thesis.

Of course, to justify the terminology 'short exact sequence,' we need to prove several properties. For example, we can extend a closed immersion $\mathrm{Spf}_A(B_1) \to \mathrm{Spf}_A(B_2)$ of commutative formal group schemes to a short exact sequence. To construct the quotient, we first observe that we only have to do this over artin local rings, since we can define the quotient as the inverse limit of the quotients over $A/\mathfrak{a}$'s in general. When A is an artin local ring, we have the duality. In particular, we can show that $B_1^D \to B_2^D$ is faithfully flat by the fiber-by-fiber criterion, so we can base change by the identity section to obtain a faithfully flat affine commutative group scheme over A. The Cartier dual of this is the quotient formal commutative group scheme $\left(\mathrm{Spf}_A(B_2)\right) / \left(\mathrm{Spf}_A(B_1)\right)$ (for justification, see [3, page 54]).

We can also extend a topologically faithfully flat $\mathrm{Spf}_A(B_2) \to \mathrm{Spf}_A(B_3)$ to a short exact sequence, simply by taking the kernel (which is a commutative formal group scheme over A). This notion of short exact sequence also satisfies stability under products and stability under base change. We will not need all of these properties, but what we will need is proven in Section 2.3, together with important examples.

A.4 Formal Étaleness

Given a pseudocompact *local* ring A, and $R \in \mathcal{PA}_A$, we can have the notion of the topologized **module of differentials**. Specifically, we let I_R be the closed ideal $\ker(R \widehat{\otimes}_A R \to R)$, and define $\widehat{\Omega}^1_{R/A}$ to be

$I_R/\overline{I_R^2}$. We can show the usual properties of the module of differentials in this setting by the same proof, taking care with continuity: we have first and the second fundamental sequences, a natural isomorphism $\widehat{\Omega}_{R/A}\widehat{\otimes}_A A' \cong \widehat{\Omega}^1_{R\widehat{\otimes}_A A'/A'}$ whenever $A \to A'$ a (continuous) map of pseudocompact rings, and $\widehat{\Omega}^1_{R\widehat{\otimes}_A S/A} \cong \widehat{\Omega}^1_{R\widehat{\otimes}_A S/R} \oplus \widehat{\Omega}^1_{R\widehat{\otimes}_A S/S}$ for $R, S \in \mathcal{PA}_A$ ([3, Theorem 1.5.7]). We say a profinite A-algebra R is **formally étale** if R is topologically flat over A and $\widehat{\Omega}^1_{R/A} = 0$. We immediately see that taking completed tensor product of two formally étale algebras is again formally étale, and that étaleness is preserved via base change. By analyzing what happens for each artinian quotient, we can prove the following useful theorem ([3, Theorem 1.5.9]):

Theorem A.4.1. *For $R \in \mathcal{PA}_A$, R is formally étale if and only if R is topologically flat over A and $R\widehat{\otimes}_A(A/\mathfrak{m})$ is a product of finite separable field extensions of $A/\mathfrak{m}$.*

Because a pseudocompact local ring is henselian (page 27), it follows that for $B \in \mathcal{PA}_A$ which is topologically flat, there exists a *unique* maximal formally étale closed A-subalgebra $B^{\text{ét}}$. By construction, the map $B^{\text{ét}} \hookrightarrow B$ is topologically faithfully flat and $(\prod B_i)^{\text{ét}} = \prod {B_i}^{\text{ét}}$ ([3, Theorem 1.5.10]). By reducing to the analysis of non-formal étaleness of artin local rings, we can also show that for a local map of pseudocompact local rings $A \to A'$, $B^{\text{ét}}\widehat{\otimes}_A A' \hookrightarrow B\widehat{\otimes}_A A'$ is the maximal étale subalgebra ([3, Theorem 1.5.12]) and ${B_1}^{\text{ét}}\widehat{\otimes}_A {B_2}^{\text{ét}} \hookrightarrow B_1\widehat{\otimes}_A B_2$ is the maximal étale subalgebra ([3, Theorem 1.5.11]). Moreover, any map from a formally étale A-algebra to B factors through $B^{\text{ét}}$.

A.5 Formal Smoothness

Again, for simplicity, let us assume that A is a *local* pseudocompact ring with maximal ideal $\mathfrak{m}$. Let $B \in \mathcal{PA}_A$. Then B is said to be **formally smooth** over A if for every profinite artinian A-algebra R and an ideal $I \subseteq R$ with $I^2 = 0$, the map $\mathrm{Spf}_A(B)(R) \to \mathrm{Spf}_A(B)(R/I)$ is surjective. Because we can write $R = \prod R_{\mathfrak{n}}$ where $\mathfrak{n}$ runs through open maximals of R and $(R/I)_{\mathfrak{n}} \cong R_{\mathfrak{n}}/I_{\mathfrak{n}}$, it suffices to check the above condition for artin *local* R with the maximal ideal $\mathfrak{n}$. If $\varphi \in \mathrm{Spf}_A(\prod B_i)(R)$, then $\varphi^{-1}(\mathfrak{n})$ is an open prime, so it is an open maximal by pseudocompactness. But the only idempotent inside $\mathfrak{n}$ is 0 by locality of R, so φ factors through one of B_i's. Hence,

$$\mathrm{Spf}_A(\prod B_i)(R) = \coprod \mathrm{Spf}_A(B_i)(R). \tag{A.2}$$

Thus, it is now clear that $\prod B_i$ is formally smooth over A if and only if each B_i is formally smooth over A. In particular, B is formally smooth over A if and only if localization of B at each of the open maximals is formally smooth over A.

So now the important question about formal smoothness is determination of all the *local* profinite A-algebras which are formally smooth. We have the following result to this effect, but we won't need it: if B is a local profinite A-algebra such that $A/\mathfrak{m} \cong B/\mathfrak{m}_B$ by the structure map, then B is formally smooth if and only if $B \cong A[\![X_i]\!]$ for some index set ([3, Theorem 1.5.15]).

Bibliography

[1] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Perseus Books, 1969.

[2] R. Coleman, *Course Notes from Spring 1999*, available at http://www.math.berkeley.edu/~coleman/Courses/Course-Spring99/.

[3] B. Conrad, *Background Notes on p-divisible Groups over Local Fields*, available at http://www-math.mit.edu/~dejong/.

[4] ———, *Notes on Ext.*

[5] V. G. Drinfel'd, *Elliptic modules*, Math. USSR Sb. **23** (1974), 561–592.

[6] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, 1995.

[7] P. Freyd, *Abelian categories: An introduction to the theory of functors*, Harper & Row Publishers, 1964.

[8] A. Frölich, *Formal groups*, Lecture Notes in Mathematics, no. 74, Springer-Verlag, 1968.

[9] R. Gold, *Local class field theory via lubin-tate groups*, Indiana Univ. Math. Jour. **30** (1981), 795–798.

[10] D. Goss, *Basic structures of function field arithmetic*, Springer, 1996.

[11] R. Hartshorne, *Algebraic geometry*, Springer, 1977.

[12] M. Hazewinkel, *Local class field theory is easy*, Advances in Math. **18** (1975), 148–181.

[13] ———, *Formal groups and applications*, Academic Press, 1978.

[14] K. Iwasawa, *Local class field theory*, Oxford University Press, 1986.

[15] N. Jacobson, *Basic algebra II*, W. H. Freeman and Company, 1989.

[16] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, Princeton University Press, 1985.

[17] H. Koch, *Algebraic number theory*, Springer, 1997.

[18] J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. Math. **81** (1965), 380–387.

[19] ———, *Formal moduli for one parameter formal lie groups*, Bull. Soc. Math. France **94** (1966), 49–60.

[20] S. MacLane and G. Birkhoff, *Algebra*, Chelsea Publishing Company, 1988.

[21] H. Matsumura, *Commutative ring theory*, Cambridge studies in advanced mathematics, no. 8, Cambridge University Press, 1986.

[22] J. Neukirch, *Algebraic number theory*, Springer, 1999.

[23] S. Saito, *Number theory*, Kyōritsu-Shuppan, 1997, in Japanese.

[24] S. Sen, *On automorphisms of local fields*, Ann. of Math. **90** (1969), 33–46.

[25] J-P Serre, *Local class field theory*, Algebraic number theory (J. W. S. Cassels and A. Frölich, eds.), Academic Press, 1967.

[26] ———, *Local fields*, GTM, no. 67, Springer-Verlag, 1979.

[27] S. S. Shatz, *Group schemes, formal groups, and p-divisible groups*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer, 1986.

[28] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, 1986.

[29] J. Tate, *Finite flat group schemes*, Modular Forms and Fermat's Last Theorem (J. H. Silverman G. Cornell and G. Stevens, eds.), Springer, 1997.

[30] R. Taylor, *Lecture notes*, 1999.

[31] W. C. Waterhouse, *Introducdtion to affine group schemes*, Springer, 1979.