$\Gamma(p)$-level structure on p-divisible groups

Thesis by
Andrei Frimu

In Partial Fulfillment of the Requirements for the
Degree of
Doctor of Philosophy

Caltech

CALIFORNIA INSTITUTE OF TECHNOLOGY
Pasadena, California

2019
Defended May 22, 2019

Andrei Frimu
ORCID: 0000-0002-7782-7204

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Prof. Xinwen Zhu, for suggesting the problem and for the continuous support and inspiration he provided. I have learned a lot of beautiful mathematics through his recommendations and conversations.

I would also like to thank Prof. Elena Mantovan, Prof. Dinakar Ramakrishnan and Prof. Matthias Flach for agreeing to be part of my defense committee. I am also grateful to various other faculty and staff of the Caltech Math Department for all the help they provided in the last several years.

Greatest thanks goes to my parents and my sister for their love, support and encouragement throughout all my life.

I am very grateful to Prof. Valeriu Baltag and Prof. Marcel Teleuca for nurturing my passion for mathematics from a young age and guiding me through mathematical contests.

Finally, I thank my friends (currently or formerly) at Caltech, in Pasadena and many other cities around the world, for making my PhD years so enjoyable. Special thanks goes to fellow student Nathan Lawless, whom I met on day one at Caltech and with whom I shared most of the math PhD journey.

ABSTRACT

The main result of the thesis is the introduction of a notion of $\Gamma(p)$-level structure for p-divisible groups. This generalizes the Drinfeld-Katz-Mazur notion of full level structure for 1-dimensional p-divisible groups. The associated moduli problem has a natural forgetful map to the $\Gamma_0(p)$-level moduli problem. Exploiting this map and known results about $\Gamma_0(p)$-level, we show that our notion yields a flat moduli problem. We show that in the case of 1-dimensional p-divisible groups, it coincides with the existing Drinfeld-Katz-Mazur notion.

In the second half of the thesis, we introduce a notion of epipelagic level structure. As part of the task of writing down a local model for the associated moduli problem, one needs to understand commutative finite flat group schemes G of order p^2 killed by p, equipped with an extension structures $0 \to H_1 \to G \to H_2 \to 0$, where H_1, H_2 are finite flat of order p. We investigate a particular class of extensions, namely extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p over $\mathbb{Z}_p$-algebras. These can be classified using Kummer theory. We present a different approach, which leads to a more explicit classification.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 Motivation

The main focus on the thesis is introducing a notion of $\Gamma(p)$-level structure on p-divisible groups. Level structures on abelian varieties or their associated p-divisible groups have long been studied, part of the appeal being that PEL type Shimura varieties have been a rich source of representations of interest to the Langlands program. For example, Harris and Taylor [HT01] establish Langlands correspondence for $GL(n)$ over p-adic fields by studying the (cohomology of the) bad reduction of certain PEL type Shimura varieties which arise as moduli problems of abelian varieties with extra data - a polarization and a Drinfeld-Katz-Mazur level structure on an associated p-divisible group, which is 1-dimensional.

In the above setting, the p-divisible groups under consideration are 1-dimensional (i.e. their Lie algebra is locally free of rank 1). In this case, the Drinfeld-Katz-Mazur notion of $\Gamma(p)$-level (and $\Gamma(p^m)$-level) structure is well-behaved. If G is a p-divisible group of height h, a level p^m-structure is a map of group schemes $\varphi : (\mathbb{Z}/p^m\mathbb{Z})^h \to G[p^m]$ satisfying certain extra properties. These properties have been refined, historically, several times. For example, if G is the p-divisible group associated to an elliptic curve E (so G has height $h = 2$) over some base S where p is invertible, one simply requires φ to be an isomorphism (and one can replace p^m by any integer n invertible on S). When p is not necessarily invertible on S, it can happen that no such isomorphism exists and a remedy is to require that $G[p^m] = \sum_{x\in(\mathbb{Z}/p^m\mathbb{Z})^h} [\varphi(x)]$, where this equality is an equality of Cartier divisors on E. One can check that this implies that φ is an isomorphism if p is invertible.

Katz and Mazur introduce in [KM85] a notion of level structure (which they call "full set of sections," and which we call in this thesis a Drinfeld-Katz-Mazur level structure) that generalizes the above scenarios and does not depend on an ambient curve where an equality of Cartier divisors is to take place. That is the definition used successfully by Harris and Taylor in [HT01]. The moduli space of 1-dimensional p-divisible groups with such level is well-behaved.

The notion of Drinfeld-Katz-Mazur level structure, applies, in principle, to higher-dimensional p-divisible groups (for instance, arising from abelian varieties of dimension > 1), but it is no longer well-behaved. One of the main problems is the fact that points are no longer Cartier divisors - if A is an abelian variety of dimension d, $A[n]$ is a relative Cartier divisor of A only if $d = 1$. Loosely speaking, 1-dimensionality allows us to locally embed our (truncated) p-divisible group G in a curve (see lemma 5.2.1), thus the sections of $G(S)$ in the image of a group homomorphism $(\mathbb{Z}/p^m\mathbb{Z})^h \to G$ correspond to Cartier divisors on this curve, allowing us to make sense of equalities as Cartier divisors, as in the elliptic curve example above. For higher dimensions, among other issues, the arising moduli spaces are no longer flat, as shown for example by Chai and Norman in [CN90]. It is thus an interesting question to define such a notion of ''full'' $\Gamma(p)$ (and $\Gamma(p^m)$)-level structure for higher-dimensional p-divisible groups. We propose such a notion for $\Gamma(p)$-level, show that it agrees with the existing definition for 1-dimensional p-divisible groups, and prove that the arising moduli space is flat over $\mathbb{Z}_p$.

In the second part of the thesis, motivated by the study of epipelagic representations, we introduce a notion of epipelagic level structure. We show that the moduli space of p-divisible groups equipped with this level structure is flat. When trying to write down the local model for the moduli space, a useful gadget would be a classification of commutative finite flat group schemes G of order p^2 killed by p, equipped with an extension structure $0 \to H_1 \to G \to H_2 \to 0$; or at least of such extensions when $H_2 = \mathbb{Z}/p\mathbb{Z}$. We give some partial results in this direction, by explicitly classifying extensions G of $\mathbb{Z}/p\mathbb{Z}$ by μ_p over $\mathbb{Z}_p$-algebras. Locally on the base, it is known that such extensions are classified by $H^1_{\text{fppf}}(S, \mu_p)$ and one can compute this group using Kummer theory. We arrive at the same result without using Kummer theory, but by studying in depth the structure of the affine algebra of G, making use of Oort-Tate theory. We believe that a detailed such study is necessary if one is to write down an explicit moduli problem classifying general extensions $0 \to H_1 \to G \to H_2 \to 0$ as above.

In the third part of the thesis, we present an interpretation of the notion of level structure on p-divisible groups over perfect bases using Dieudonné theory. It is known that over perfect rings there is an anti-equivalence of categories between p-divisible groups (truncated or not) and Dieudonné modules. Thus, the notion of Drinfeld-Katz-Mazur level structure for p-divisible groups should have a corresponding notion in terms of Dieudonné modules. We give such an interpretation.

1.2 Overview of the results

In the first part of the thesis, we introduce the following notion of $\Gamma(p)$-level structure on p-divisible group:

Definition 1.2.1. *A $\Gamma(p)$-level structure on a p-divisible group G of height h is the following data:*

1. *A filtration $0 = H_0 \subset H_1 \subset \ldots \subset H_h = G[p]$ of $G[p]$ by finite flat subgroup schemes.*
2. *Oort-Tate generators (see section 3.1) $\gamma_i : (\mathbb{Z}/p\mathbb{Z}) \to H_i/H_{i-1}$ for $i = 1, \ldots, h$.*
3. *Group homomorphism $\varphi_i : (\mathbb{Z}/p\mathbb{Z})^i \to H_i$ such that the following diagram commutes:*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & \ldots & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{h-1} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^h \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & & & \downarrow{\scriptstyle \varphi_{h-1}} & & \downarrow{\scriptstyle \varphi_h} \\ 0 = H_0 & \longrightarrow & H_1 & \longrightarrow & H_2 & \longrightarrow & \ldots & \longrightarrow & H_{h-1} & \longrightarrow & H_h = G[p] \end{array}$$

so that the induced maps $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-1}$ are the Oort-Tate generators γ_i.

We show that if G is 1-dimensional, the above notion agrees with the (usual) Drinfeld-Katz-Mazur level structure. Our main result is that the moduli space of p-divisible groups with the above notion of $\Gamma(p)$-level structure is flat (for any dimension), which we prove in section 5.3. We establish this by examining the forgetful map to moduli space $\mathcal{M}_{\Gamma_0(p)}$ of p-divisible groups with $\Gamma_0(p)$-level structure, which is known to be flat over $\mathbb{Z}_p$ by [Goe01]. We recall some of the facts about $\mathcal{M}_{\Gamma_0(p)}$ we use in chapter 4. The forgetful map factors through several moduli problems defined by ‘‘intermediate’’ data. We show that each of these intermediate moduli problems is flat over the next one.

In the second part of the thesis, motivated by the study of epipelagic representations, we give a notion of epipelagic level structure and show that the associated moduli space is flat. A useful ingredient in writing down local models for the associated moduli space would be a classification of commutative finite flat group schemes of order p^2 killed by p, equipped with an extension structure of the form

$$0 \to H_1 \to G \to H_2 \to 0$$

where H_1, H_2 are finite flat group schemes of order p. The problem seems hard even when $H_2 = \mathbb{Z}/p\mathbb{Z}$.

A general family of such extensions over any ring R is the following: let $\epsilon \in R$ be a unit and consider the R-algebra

$$B_\epsilon := \bigoplus_{i=0}^{p-1} R[X_i]/(X_i^p - \epsilon^i).$$

This is the Hopf algebra of a group scheme $G_\epsilon := \mathrm{Spec}(B_\epsilon)$. If $S = \mathrm{Spec}\, A$ is a connected R-scheme, then $G_\epsilon(S)$ consists of pairs (t,i) with $t \in A$ such that $t^p = \epsilon^i$. The group law is given by

$$(t,i)\cdot(s,j) = \begin{cases} (st, i+j), \text{ if } i+j < p \\ (st/\epsilon, i+j-p), \text{ if } i+j \geq p \end{cases}$$

We shall prove that locally over a $\mathbb{Z}_p$-algebra R, every extension of $\mathbb{Z}/p\mathbb{Z}$ by μ_p is of the form G_ϵ, for some unit $\epsilon \in R$. One can show that $\mathrm{Ext}^1_S(\mathbb{Z}/p\mathbb{Z}, \mu_p) = H^1_{\mathrm{fppf}}(S, \mu_p)$ and using Kummer theory, the latter group is (locally) isomorphic $R^*/(R^*)^p$. We take a different route and look explicitly at the action of $\mathrm{Hom}(H_2, H_1) = \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mu_p) = \mu_p$ on such groups. Using results of [Tzi17] and [DG70], the action of μ_p on any *scheme* that's nice enough (not necessarily group scheme) can be written quite explicitly. In characteristic p, such actions are in bijection with global derivations D satisfying the relation $D^p = D$. Over a general $\mathbb{Z}_p$-algebra we also obtain a linear map D. It no longer is a derivation, but still has special properties that we can exploit. In both cases, in the presence of $(p-1)$th roots of unity, D is diagonalizable and we can analyze the structure of the (group) schemes acted upon explicitly.

Finally, in the last part, we give an auxiliary result - an interpretation of the notion of Drinfeld-Katz-Mazur level structure using Dieudonné theory. Over a perfect field k of characteristic p, it is classical that p-divisible groups are classified by Dieudonné modules - free $W(k)$-modules with semilinear actions of Frobenius and Verschiebung. In fact, this follows from a more general equivalence: finite flat group schemes of p-power order over k and $W(k)$-modules of finite length with actions of Frobenius and Verschiebung.

This equivalence has more recently been established more generally over any perfect ring R (unpublished results of Gabber, see also [Lau10]). Interpreting a level structure on a p-divisible group G of height h as a group homomorphism between the constant group scheme $(\mathbb{Z}/p^m\mathbb{Z})^h \to G[p^m]$ with certain extra properties (see chapter 7 for a precise statement), it corresponds then to a homomorphism of (truncated) Dieudonné modules with some corresponding properties. The main result is theorem 7.2.1.

1.3 Structure of the thesis

In Chapter II, we recall background material on finite flat group schemes, p-divisible groups and Dieudonné theory. In Chapter III, we introduce various existing notions of level structures and their properties. Chapter IV contains background material regarding moduli spaces of p-divisible groups with $\Gamma_0(p)$ and $\Gamma_1(p)$ level structures.

Chapters V, VI and VII contain our main results. In Chapter V, we introduce our notion of $\Gamma(p)$-level structure and establish its properties. In Chapter VI, we introduce the notion of epipelagic level structure and classify extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p. Chapter VII contains our auxiliary result about interpreting the notion of level structure in the Dieudonné setting.

Chapter 2

PRELIMINARIES

In this chapter, we recall various definitions, examples and results that we will use throughout the thesis. Most of the results are well-known and can be found in a variety of sources, for example [Dem72] or [DG70].

We fix a prime number p. S will typically denote a base scheme. Following the conventions of Messing [Mes72], a *group* G over S is a commutative fppf sheaf of groups on the site Sch/S.

2.1 Finite flat group schemes

Let R be a ring. By a finite flat group scheme of order m over R we mean a commutative group scheme G which is locally free of rank m over R. In this paper m will usually be a power of a fixed prime p. Locally on the base, G is the spectrum of a Hopf algebra A and is endowed with maps describing the group structure: comultiplication $\Delta : A \longrightarrow A \otimes A$, neutral element map $\epsilon : A \longrightarrow R$ and an automorphism $i : A \longrightarrow A$ corresponding to the inverse automorphism. These maps are required to satisfy various conditions which make $G(T)$ into a group for any test scheme T.

The kernel of the map $\epsilon : A \longrightarrow R$ is a locally free ideal called the *augmentation ideal* and has rank $m - 1$ over the base.

Examples

1. Constant group scheme: for any abstract group Γ, the functor associating each connected scheme S the group Γ is representable by the constant group scheme associated to Γ. Its Hopf algebra is $R^{(\Gamma)} = R \times \ldots \times R$, where the factors are indexed by the elements of Γ. This can also be written as $R[e_g]_{g \in \Gamma}$, where e_g are orthogonal idempotents, i.e. $e_g^2 = e_g$ and $e_g e_{g'} = 1$.

   The Hopf algebra structure is given by comultiplication

   $$e_g \mapsto \Delta(e_g) = \sum_{h \in \Gamma} e_h \otimes e_{g-h},$$

   The neutral element map $e_0 \mapsto 1$ and $e_g \mapsto 0$ where 0 is the zero element of Γ. The inverse automorphism is $e_g \mapsto e_{-g}$.

In the section on Oort-Tate theory below, we shall see a different description of $\underline{\mathbb{Z}/p\mathbb{Z}}$ under certain assumptions on the base scheme.

2. μ_m: this represents the functor sending an R-algebra A to the group $\{x \in A|\ x^m - 1 = 0\}$ (under multiplication). The Hopf algebra can be written as $R[Z]/(Z^m - 1)$. Comultiplication sends $Z \mapsto Z \otimes Z$, neutral element sends $Z \mapsto 1$ and inverse $Z \mapsto Z^{-1}$.

   In the section on Oort-Tate theory below, we shall see a different description of μ_p under certain assumptions on the base scheme.

3. α_{p^k}: consider the functor sending an R-algebra A to the set $\{x \in A|\ x^{p^k} = 0\}$. This set is empty if A is reduced. If R is an $\mathbb{F}_p$-algebra, then this set is actually a group and the functor over $\mathbb{F}_p$ is representable. The Hopf algebra is given by $R[X]/(X^{p^k})$ with comultiplication sending $X \mapsto X \otimes 1 + 1 \otimes X$, neutral element $X \mapsto 0$ and inverse element $X \mapsto -X$.

   In the section on Oort-Tate theory below, we shall see another perspective on α_p under certain assumptions on the base scheme.

Cartier duality

If $G = \operatorname{Spec} B$ is a finite flat group scheme over a ring R, then $B^\vee = \operatorname{Hom}_R(B, R)$ has a natural structure of a Hopf algebra. Indeed, using the identification $(B \otimes_R B)^\vee = B^\vee \otimes_R B^\vee$, dualizing the multiplication $m : B \otimes_R B \to B$, comultiplication $c : B \otimes_R B$, inverse map $i : B \to B$, identity section $\epsilon : R \to B$ and structure map $B \to R$ one obtains five ring maps

$$m^\vee : B^\vee \to B^\vee \otimes_R B^\vee$$

$$\Delta^\vee : B^\vee \otimes_R B^\vee \to B^\vee$$

$$i^\vee : B^\vee \to B^\vee$$

$$\epsilon^\vee : R \to B^\vee$$

$$B^\vee \to R$$

One can check that these maps define, in order, comultiplication, multiplication, inverse, structure map and identity section map on $B^\vee$, i.e. endow $B^\vee$ with the structure of a Hopf algebra (which is also finite and flat over R). $\operatorname{Spec}(B^\vee)$ is denoted $G^\vee$ and is called the Cartier dual of G. One can also define $G^\vee$ as

$$G^\vee(S) := \operatorname{Hom}_{\text{group}}(G_S, \mathbb{G}_{\mathrm{m}S}).$$

Cartier duality induces an anti-equivalence from the category of finite flat group schemes to itself.

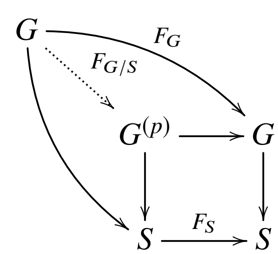
Examples:

The dual of $\mathbb{Z}/p\mathbb{Z}$ is μ_p and the dual of μ_p is $\mathbb{Z}/p\mathbb{Z}$. The group scheme α_p introduced above is self-dual.

Frobenius and Verschiebung

Assume in this subsection that $p = 0$. Any $\mathbb{F}_p$-ring R has a ring endomorphism $F_R : R \to R$ given by $F_R(x) = x^p$, for $x \in R$. If A is an R-algebra, then we can form the F_R-base change $A^{(p)} := A \otimes_{R,F_R} R$. This naturally extends to $\mathbb{F}_p$-schemes. In algebraic-geometric language, starting with a group scheme G over an $\mathbb{F}_p$-scheme S, we can then form the S-scheme $G^{(p)} := G \times_{S,F_S} S$. $G^{(p)}$ is also called the Frobenius twist of G. It is also a group scheme.

We then have an induced map $F_{G/S} : G \to G^{(p)}$, called the *relative Frobenius*, arising from the following diagram:



The relative Frobenius is functorial and commutes with products, so in particular is a group homomorphism. It also commutes with taking Cartier duals.

Let G be a group over a base scheme S over $\mathbb{F}_p$. Then, we can form the relative Frobenius $G^\vee \to (G^\vee)^{(p)} = (G^{(p)})^\vee$. Taking the duals again, one obtains a group homomorphism $G^{(p)} \to G$, called Verschiebung and commonly denoted by V. One can then prove

Proposition 2.1.1. *$V \circ F = p \cdot \mathrm{id}_G$ and $F \circ V = p \cdot \mathrm{id}_{G^{(p)}}$.*

Étale-connected sequence

Let R be a Henselian local ring (for example $R = \mathbb{Z}_p$) and $G = \operatorname{Spec} B$ a finite flat group scheme over R. Then, one has a connected-étale sequence

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

This is obtained as follows: B can be written as a product $B = \prod B_i$ of local rings. One of these local rings, typically denoted B^0, has the property that the identity section $e : S \to G$ lands in $\mathrm{Spec}(B^0)$. Then, $G^0 := \mathrm{Spec}(B^0)$ is called the connected component of the identity in G. One shows that G^0 is actually a (sub)group scheme. Using the hypothesis that R is a Henselian ring, one can show that the quotient G/G^0 exists (as a group scheme) and is étale. It is typically denoted by $G^{\text{ét}}$. One thus has an exact sequence

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

If R is a perfect field, the homomorphism $G \to G^{\text{ét}}$ has a section and thus G can be written as a product $G = G^0 \times G^{\text{ét}}$. This is a very special phenomenon, relying crucially on R being perfect. See, for example, section 6.2 below for a family of finite flat group schemes G_ϵ of order p^2. If the base is a field of characteristic p, then we have an exact sequence

$$0 \to \mu_p \to G_\epsilon \to \mathbb{Z}/p\mathbb{Z} \to 0$$

which only splits if ϵ is a pth power.

2.2 Oort-Tate theory

In this subsection, we review Oort-Tate theory. Finite flat group schemes of prime order p are (relatively) well-understood. Namely, we have the following modern reformulation (see for example, [HR12]) of the results of Oort and Tate in [TO70]:

Theorem 2.2.1. *Let OT be the $\mathbb{Z}_p$-stack of finite flat group schemes of order p. Then*

(i) OT is an Artin stack isomorphic to

$$\left[\left(\mathrm{Spec}\,\mathbb{Z}_p[X,Y]/(XY - w_p)\right)/\mathbb{G}_m\right],$$

where $\mathbb{G}_m$ acts via $\lambda.(X,Y) = (\lambda^{p-1}X, \lambda^{1-p}Y)$. w_p is an explicit element of $p\mathbb{Z}_p^\times$.

(ii) The universal group scheme $\mathcal{G}$ over OT is equal to

$$\mathcal{G} = \left[\left(\mathrm{Spec}_{OT}\,\mathcal{O}[Z]/(Z^p - XZ)\right)/\mathbb{G}_m\right]$$

where $\mathbb{G}_m$ acts via $Z \mapsto \lambda Z$, with zero section $Z = 0$.

In particular, the above theorem classifies finite flat group schemes of order p over $\mathbb{Z}_p$ and $\mathbb{F}_p$. In fact, Oort and Tate classify group schemes of order p over the ring

$\Lambda = \mathbb{Z}\left[\zeta, \frac{1}{p(p-1)}\right] \cap \mathbb{Z}_p$, where ζ is a primitive $(p-1)$th root of unity in $\mathbb{Z}_p$, but for our purposes, this classification over $\mathbb{Z}_p$-algebras suffices. If S is a $\mathbb{Z}_p$-scheme, then finite flat group schemes G of order p over S correspond to morphisms $\varphi : S \to OT$, such that $G = \varphi^*(\mathcal{G})$.

Let $G = \mathrm{Spec}(B)$ be a group scheme of order p over a base S over $\mathrm{Spec}(\mathbb{Z}_p)$. An important idea in Oort and Tate's paper is that the action of $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ on the augmentation ideal decomposes this ideal into a direct sum of invertible modules (this crucially relies on the presence of $p-1$ roots of unity). Indeed, the action allows us to write the augmentation ideal $\mathbf{I}$ of B as a direct sum $\mathbf{I} = \mathbf{I}_1 \oplus \ldots \oplus \mathbf{I}_{p-1}$ of modules $\mathbf{I}_j$. These can be obtained as $\mathbf{I}_j = e_j\,\mathbf{I}$, where e_j are certain idempotents of the group ring $\Lambda[\mathbb{F}_p^*]$. By inspecting what happens at geometric points one then concludes that each $\mathbf{I}_j$ has rank 1. Moreover, $\mathbf{I}_1^j = \mathbf{I}_j$.

Let χ be the Teichmuller character $\chi : \mathbb{F}_p \to \mathbb{Z}_p$. Thus $\chi(0) = 0$ and for $i \neq 0$, $\chi(i)$ is the unique $(p-1)$th root of unity in $\mathbb{Z}_p$ which is congruent to i mod p. We have the following useful description of the modules $\mathbf{I}_j$: $\mathbf{I}_j$ consists of sections f of $\mathbf{I}$ such that $[m]f = \chi^j(m)f$, for every $m \in (\mathbb{Z}/p\mathbb{Z})^\times$.

An important part in the proof of the classification result is the following description of the multiplicative group scheme μ_p over the ring $\Lambda = \mathbb{Z}\left[\zeta, \frac{1}{p(p-1)}\right] \cap \mathbb{Z}_p$ mentioned above. Let $B = \Lambda[z]/(z^p - 1)$ be the Hopf algebra of μ_p over Λ. Define then

$$y_j := (p-1)e_j(1-z).$$

and write $y := y_1$. Extend the indexing to all integers by defining $y_{j+(p-1)k} := y_j$ for any integer k.

Using the above notation, the following properties then hold:

Proposition 2.2.1 ([TO70]). *1.* $\mathbf{I}_1$ *is generated by* y *and* $\mathbf{I}_j$ *is generated by* y^j, *for* $1 \leq j \leq p-1$.

2. *For* $1 \leq j \leq p-1$, *there are constants* w_j *such that* $y^j = w_j y_j$. *We also have*

$$y^p = w_p y,$$

where $w_p = p \cdot$ *unit.*

3.

$$\Delta(y_i) = y_i \otimes 1 + 1 \otimes y_i + \frac{1}{1-p}\sum_{j=1}^{p-1} y_j \otimes y_{i-j}$$

and in particular

$$\Delta(y) = y \otimes 1 + 1 \otimes y + \frac{1}{1-p} \sum_{j=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$$

4. $w_j \equiv j! \pmod{p}$ *for* $1 \leq j \leq p-1$.

5. $z = 1 + \frac{1}{1-p}\left(y + \frac{y^2}{w_2} + \cdots + \frac{y^{p-1}}{w_{p-1}}\right)$.

Examples, revisited

In this subsection, we present how the three examples of finite flat group schemes shown above fit in Oort-Tate theory.

1. Constant group scheme $\mathbb{Z}/p\mathbb{Z}$:

   If $g = \chi(1)e_1 + \ldots + \chi(p-1)e_{p-1}$, where χ is the Teichmuller character described above, then one checks that the affine ring $B = R[e_g]_{g \in \mathbb{Z}/p\mathbb{Z}}/\langle e_g^2 = e_g, e_g e_{g'} = 0\rangle$ of the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ can also be written as

   $$B = R[g]/(g^p - g).$$

   One recovers the e_i's, by factoring $g^p - g$ into linear factors and omitting the ith one. The augmentation ideal is $\mathbf{I} = \oplus g^i R$, and $\mathbf{I}_j = g^j R$.

2. μ_p: This is the content of proposition 2.2.1 above. Note that y is neither z nor $z-1$ (which appear often in description of μ_p).

3. α_p: As mentioned above, this group scheme only exists over $\mathbb{F}_p$-algebras R and has Hopf algebra $R[t]/(t^p)$. The augmentation ideal is $\mathbf{I} = \langle t \rangle$. The invertible modules $\mathbf{I}_j$ in the decomposition $\mathbf{I} = \mathbf{I}_1 \oplus \ldots \oplus \mathbf{I}_{p-1}$ are simply $\mathbf{I}_j = t^j R$.

2.3 p-divisible groups

Definition and basic examples

Definition 2.3.1. *Let S be a base scheme. An S-group G (recall that G is, a priori, an fppf sheaf) is called a* ***p-divisible group*** *on S if it satisfied the following three conditions:*

(i) The morphism $p : G \to G$ *is an epimorphism.*

(ii) G is p-torsion, i.e. $G = \varinjlim_n G[p^n]$, *where* $G[p^n] := \ker(p^n : G \to G)$.

(iii) *The S-groups $G[p^n]$ are representable by finite locally free group schemes over S.*

If S is connected, then the group schemes $G[p^n]$ have constant rank over the base equal to p^{hn}, for some positive integer h not depending on n (only on G). We call h the *height* of G.

Assume now p is locally nilpotent on S. We define the Lie algebra of G as $\operatorname{Lie} G[p^m]$ for m large enough. This is a locally free sheaf on S and we call the rank of $\operatorname{Lie} G$ the *dimension* of G.

Here are some basic examples:

1. The constant p-divisible group $(\mathbb{Q}_p/\mathbb{Z}_p)_S$. The finite flat group scheme $G[p^n]$ is just the constant group scheme $(p^{-n}\mathbb{Z}_p/\mathbb{Z}_p) \simeq (\mathbb{Z}/p^n\mathbb{Z})$ over S. G has height 1 and dimension 0.

2. $G = \mu_{p^\infty}$. This can be defined as $\mathbb{G}_{\mathrm{m}}[p^\infty]$ and we have $G[p^n](S) = \mu_{p^n}(S)$. One can check that G has height 1 and dimension 1.

3. Let A/S be an abelian scheme of dimension g. Then $A[p^\infty]$ is a p-divisible group of height $2g$.

Étale-connected sequence

Let R be a Henselian ring and let G be a p-divisible group over $S = \operatorname{Spec} R$ of height h. Since each $G[p^n]$ is a finite flat group scheme over S, we have étale connected sequences (see section 2.1) for every n:

$$0 \to G^0[p^n] \to G[p^n] \to G^{\text{ét}}[p^n] \to 0.$$

One can show that these sequences maps are compatible between different levels n and m. Moreover, $(G^0[p^n]^0)$ and $(G^{\text{ét}}[p^n])$ are themselves p-divisible groups, typically called the connected and the étale part of G and denoted G^0 and $G^{\text{ét}}$, respectively. If R is a perfect field, then the exact sequence of p-divisible groups

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

splits and one has $G \simeq G^0 \times G^{\text{ét}}$.

Cartier duality

Let G be a p-divisible group over a base scheme S. As each $G[p^n]$ is a finite flat group scheme, one can form the Cartier duals $G[p^n]^\vee$. One can check that these duals also satisfy the conditions in the definition of a p-divisible group. The p-divisible group thus obtained is denote $G^\vee$. It has the same height as G. The dimensions of G and $G^\vee$ are related by the following result:

Proposition 2.3.1. *Let G be a p-divisible group of height h and dimension d. Then $G^\vee$ has dimension $h - d$.*

Common examples are the following: the dual of the constant p-divisible group $(\mathbb{Q}_p/\mathbb{Z}_p)$ is μ_{p^∞}. If G is the p-divisible group arising from an abelian variety A, then $G^\vee$ is the p-divisible group associated to the dual abelian variety $A^\vee$.

Frobenius and Verschiebung

Assume that the base scheme S has characteristic p (i.e. $p\mathcal{O}_S = 0$). From the functoriality of the Frobenius F and Verschiebung V, these maps on each group scheme $G[p^n]$ are compatible (in n). The Frobenius twists then $G[p^n]^{(p)}$ form a p-divisible group which we denote $G^{(p)}$. We thus have isogenies of p-divisible groups $F : G \to G^{(p)}$ and $V : G^{(p)} \to G$. Similar to proposition 2.1.1, we have

Proposition 2.3.2. $F \circ V = p \cdot \mathrm{id}_{G^{(p)}}$ *and* $V \circ F = p \cdot \mathrm{id}_G$.

2.4 Dieudonné theory

In this section, we summarize some results on Dieudonné theory over perfect rings. One can consult [Dem72] or [Fon77] for Dieudonné theory over perfect fields and [Lau10] for Dieudonné theory over perfect rings.

In its classical form, Dieudonné theory gives a contravariant equivalence between the category of p-divisible groups over a perfect field k of characteristic p and the category of Dieudonné modules over the Dieudonné ring $D = W(k)[F, V]$, which we detail below.

Recall first that to any perfect ring R of characteristic p, one can associate, functorially, the ring of Witt vectors $W(R)$. This is a ring of characteristic 0. As a set it is in bijection with $R^{\mathbb{N}}$, but with more complicated addition and multiplication, given by certain Witt polynomials. If R is a perfect field k, then $W(k)$ is a complete discrete valuation ring with maximal ideal (p) and residue field k.

The most common example is $k = \mathbb{F}_p$. Then $W(k) = \mathbb{Z}_p$, the ring of p-adic integers. If $k = \mathbb{F}_{p^r}$, then $W(k)$ is isomorphic to the unique unramified extension of $\mathbb{Z}_p$ of degree r.

The Frobenius automorphism of R lifts to a Frobenius automorphism $W(R)$, usually denoted by σ. On sequences $(a_0, a_1, \ldots)$ it acts by raising each a_i to its $p$the power.

One also has the rings of truncated Witt vectors $W_m(R)$. If R is perfect, these are isomorphic to $W(R)/p^m W(R)$. Its elements can be viewed as finite sequences of length m (but again, not with componentwise addition and multiplication) and are endowed with a Frobenius as well. Note that $W_1(R) \simeq R$.

The Dieudonné ring E_R is defined as the (mildly) non-commutative ring $W(R)[F, V]$ where F and V satisfy the relations:

1. $FV = VF = p$.
2. F is σ-linear, i.e. $Fw = \sigma(w)F$.
3. V is σ^{-1}-linear, i.e. $wV = V\sigma(w)$.

Recall the following definition from [Lau10]:

Definition 2.4.1. *Let R be a perfect ring. A projective Dieudonné module over R is a E_R-module which is a projective $W(R)$-module of finite type. A truncated Dieudonné module of level n is a E_R-module M which is projective over $W_n(R)$ and of finite type; if $n = 1$ we further require that* $\ker F = \operatorname{im} V$, $\operatorname{im} F = \ker V$ *and M/VM is a projective R-module.*

We can now state the anti-equivalence. As we are stating it over perfect rings, we follow [Lau10].

Theorem 2.4.1 (Dieudonné equivalence)**.** *There is an anti-equivalence of categories between that of p-divisible groups over R of height h and projective Dieudonné-modules of rank h. There is an anti-equivalence of categories between the category of truncated p-divisible groups of height h and truncated Dieudonné modules of rank h.*

One can also formulate such an equivalence more generally for finite flat group schemes over R. For a p-divisible group, truncated p-divisible group or finite flat group scheme G over R, we denote by $M(G)$ its associated Dieudonné module.

This equivalence is functorial. For example, the Frobenius map $G \to G^{(p)}$ corresponds to a linear map $M(G^{(p)}) \simeq M(G)^{(p)} \to M(G)$ and analogously for the Verschiebung.

If R is a perfect field k, every finite flat group scheme G fits into the étale-connected sequence:

$$0 \to G^0 \to G \to G^{et} \to 0$$

which splits. In that case, $M(G)$ is the direct sum of its *local* and *etale* part: $M(G) = M(G)_{loc} \oplus M(G)_{\text{ét}}$. Here $M(G)_{loc}$ is the Dieudonné module of G^0 and $M(G)_{loc}$ the Dieudonné module of G^{et}. One also has the following equalities: $M(G)_{loc} = \cap_{n\geq 0} \ker(F^n)$ and $M(G)_{\text{ét}} = \cup_{n\geq 0} F^n M(G)$.

On connected p-divisible groups (truncated or not), the Frobenius is nilpotent and the Verschiebung is an isomorphism. On étale such groups the behavior is reversed: F is an isomorphism, and V is nilpotent.

Examples

Let k be a perfect field, and consider the three examples of finite flat group schemes of order p over k:

1. $G = \mathbb{Z}/p\mathbb{Z}$: Its Dieudonné module is $M(G) = k$, with $F = \sigma$ and $V = 0$. More generally, if H is the constant p-divisible group $(\mathbb{Q}_p/\mathbb{Z}_p)$, then $M(H)$ is just $W(k)$ (as a free rank 1 module over itself) with $F = \sigma$ and $V = 0$.

2. $G = \mu_p$: Its Dieudonné module is $M(G) = k$, with $F = 0$ and $V = \sigma^{-1}$.

3. $G = \alpha_p$: $M(\alpha_p) = k$, with $F = V = 0$.

A more interesting application is the classification of group schemes of order p^2, killed by p, over a perfect field k of characteristic p. This is done in [Buz12], by classifying instead the corresponding Dieudonné modules, which are just 2-dimensional vector spaces over k with various actions of F and V. There are 9 such group schemes: direct products of any two of $\mathbb{Z}/p\mathbb{Z}$, α_p and μ_p, and also three non-split extensions of α_p by α_p: α_{p^2}, its Cartier dual and a third one, which is self-dual and on which F and V are both nilpotent but nonzero.

Chapter 3

LEVEL STRUCTURES

The notion of level structure was originally introduced by Drinfeld in [Dri74]. It was later generalized by Katz and Mazur and, in that formulation, among other applications, was used by Harris and Taylor to establish local Langlands correspondence for $\mathbf{GL}_n$.

Historically, the notion has been refined several times. In one of its more basic instances, for an elliptic curve E over a base scheme S over $\mathbb{Z}[1/n]$, a level-n structure, or $\Gamma(n)$-structure, is simply an isomorphism $(\mathbb{Z}/n\mathbb{Z})^2_S \xrightarrow{\sim} E[n]$. Two further notions of level can be defined: $\Gamma_1(n)$-level which is a homomorphism of group schemes $\mathbb{Z}/n\mathbb{Z} \to E[n](S)$, and $\Gamma_0(n)$-level structure which is a finite flat subgroup scheme of $E[n]$ locally isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Here *locally* means for the étale topology. These three notions of level structure give rise to three moduli problems (for schemes S over $\mathbb{Z}[1/n]$). By Katz-Mazur [KM85], Theorem 3.7.1 each of these moduli problems are relatively representable and finite étale.

For an elliptic curve over an arbitrary scheme S, where n need not be invertible, there may not exist an isomorphism $(\mathbb{Z}/n\mathbb{Z})^2_S \xrightarrow{\sim} E[n]$. To fix this problem, one introduces the notion of ''full level-n structure'' as the data of two points P, Q of order n (equivalently, a group homomorphism $(\mathbb{Z}/n\mathbb{Z})^2_S \to E[n]$) so that we have the following equality of *Cartier divisors* inside E:

$$E[n] = \sum_{i,j \in (\mathbb{Z}/n\mathbb{Z})^2} [iP + jQ].$$

Over $\mathbb{Z}[1/n]$ this notion coincides with the previous level-n structure notion. When n is not invertible, this ''correctly'' counts the zero section with correct multiplicity.

A mild generalization, introduced in [KM85] is the following:

Definition 3.0.1. *Let C/S be a smooth commutative group scheme over S of relative dimension one. Let A be a finite group (in the usual sense). A homomorphism of abstract groups $\varphi : A \to C(S)$ is said to be an A-structure on C/S if the effective Cartier divisor of degree $\#A$ defined by*

$$D = \sum_{i \in A} [\varphi(i)]$$

is a subgroup G of C/S.

A disadvantage of all above notions is that, given a finite flat group scheme G, it is not clear how to define a level structure on G intrinsically, i.e. without embedding G in a curve as a Cartier divisor. All the above notions depend on such an ambient curve where we can make sense of Cartier divisors. Katz and Mazur in [KM85] generalize the above definitions to an intrinsic notion of level structure that, i.e. not restricted to groups embeddable in a curve. In what follows, we call this level structure a Drinfeld-Katz-Mazur level structure, or sometimes ''full set of sections.''

Before we introduce the definition, let's recall a few basic facts from commutative algebra. Let S be a scheme and Z/S a finite flat S-scheme of finite presentation and rank $N \geq 1$ (typically N will be a power of a prime p). Reducing to the noetherian case, one can equivalently assume that Z/S is finite locally free over S of rank $N \geq 1$. For every affine S-scheme $\mathrm{Spec}(R) \to S$, the base change $Z_R/\mathrm{Spec}(R)$ is then the spectrum of an algebra B, locally free over R as an R-module. Thus, for every global section $f \in B$, one can view f as an R-linear endomorphism of B, and we can speak of the characteristic polynomial of f:

$$\det(T - f) = T^N - \mathrm{trace}(f)T^{n-1} + \ldots + (-1)^N \mathrm{norm}(f).$$

We are now ready to introduce Katz and Mazur's notion of full set of sections:

Definition 3.0.2 (Full set of sections)**.** *Let $P_1, \ldots, P_N \in Z(S)$ be N points (not necessarily distinct). One says that they form a* ***full set of sections*** *if for every affine S-scheme $\mathrm{Spec}(R) \to S$ and for every $f \in H^0(Z_R, \mathcal{O}_{Z_R})$, we have the equality of polynomials in $R[T]$:*

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

Here, we can interpret each P_i as a map of schemes $\mathrm{Spec}(R) \to Z_R$, or, as a ring homomorphism $H^0(Z_R, \mathcal{O}_{Z_R}) \to R$, and $f(P_i)$ denotes the image of f under the aforementioned ring homomorphism.

An equivalent statement of the determinant condition above is to require for any affine S-scheme $\mathrm{Spec}(R)$ and $f \in \mathcal{O}_{Z_R}$ the following equality in R:

$$\mathrm{norm}(f) = \prod_{i=1}^{N} f(P_i).$$

In the case that Z is embeddable in a curve C as a closed subscheme, which is finite flat of finite presentation over S, and we are given N not necessarily distinct points $P_1, \ldots, P_N$ of $C(S)$, then Katz and Mazur show in theorem 1.10.1 [KM85] that the condition $Z = \sum_{i=1}^{N}[P_i]$ is equivalent to the P_i's forming a full set of sections of Z/S.

Example: Consider the zero map $\mathbb{Z}/p\mathbb{Z} \to \mu_p$ over an $\mathbb{F}_p$-scheme S. Write μ_p as $\mu_p = \operatorname{Spec} B$ with $B = O_S[t]/(t^p - 1)$. Since we are in characteristic p, one can also write $B = O_S[z]/z^p$, where $z = t - 1$ and $z^p = 0$. The zero section sends $z \mapsto 0$. Let R be an O_S-algebra and $f \in B$. Write $f(z) = a_0 + a_1 z + \ldots + a_{p-1} z^{p-1}$. Since $z^p = 0$, multiplication by f is upper triangular with respect to the basis $\{1, z, \ldots, z^{p-1}\}$ with diagonal entries all equal to a_0 and thus $\det(T - f) = (T - a_0)^p = (T - f(0))^p$, showing that the zero map is a full set of sections. We shall see below another way to analyze full sets of sections on μ_p using Oort-Tate theory.

Note that the zero map is *not* a full set of sections for μ_p over R if $pR \neq 0$. One can show this computationally or otherwise embed μ_p in $\mathbb{G}_{\mathrm{m}}$ and then test whether the zero map is a level structure using Cartier divisors. If it were, we would have the equality $(X - 1)^p = X^p - 1$ in $R[X]$, which is false if $p \neq 0$ on R.

We shall need the following result from [KM85] (proposition 1.11.3 in *loc. cit.*):

Lemma 3.0.1. *Let S be an arbitrary scheme and consider a short exact sequence*

$$0 \to G_1 \to G \to G_2 \to 0$$

of finite flat commutative S-group-schemes of finite presentation, and ranks N_1, N and N_2 respectively.

Suppose give a short exact sequence

$$0 \to A_1 \to A \to A_2 \to 0$$

of (abstract) finite abelian groups of orders N_1, N and N_2 respectively.

Consider a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & A & \longrightarrow & A_2 & \longrightarrow & 0 \\ & & \downarrow \phi_1 & & \downarrow \phi & & \downarrow \phi_2 & & \\ 0 & \longrightarrow & G_1(S) & \longrightarrow & G(S) & \longrightarrow & G_2(S) & & \end{array}$$

If for $i = 1, 2$ the homomorphisms ϕ_i are Drinfeld-Katz-Mazur level structures for G_i/S, then ϕ is a Drinfeld-Katz-Mazur level structure for G.

Proof of lemma: Indeed, let B_2, B, B_1 be the affine rings of G_2, G and G_1 respectively. For $a \in A_1, A$ and A_2 respectively, denote by $\phi_{1,a}$, ϕ_a and $\phi_{2,a}$ the ring maps $B_1 \to R$, $B \to R$ and $B_2 \to R$ corresponding to the section that is the image of a in $G_1(S), G(S)$ and $G_2(S)$ respectively.

We want to show that if $f \in B$, then

$$N_{B/R}(f) = \prod_{a \in A} \phi_a(f).$$

By transitivity of the norm, the left hand side equals

$$N_{B_2/R}(N_{B/B_2}(f)) = \prod_{b \in A_2} \phi_{2,b}(N_{B/B_2}(f)),$$

since ϕ_2 is a level structure.

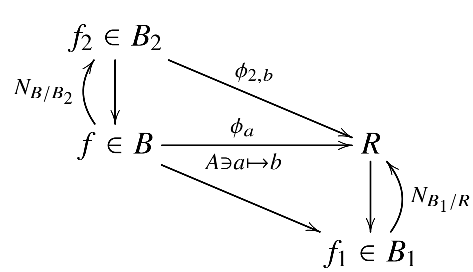
Denote $f_2 := N_{B/B_2}(f)$. It suffices then to show that

$$\phi_{2,b}(f_2) = \prod_{A \ni a \mapsto b \in A_2} \phi_a(f).$$

Note that the base change via $\phi_{2,b} : S \to G_2$ of $G \to G_2$ is just $G_1 \to S$. Thus, the norm from G to G_2 can be computed as the norm from G_1 to S. In other words, $N_{B/B_2}(f) = N_{B_1/R}(f_1)$, where f_1 is the image of f in B_1 under the ring homomorphism $B \to B_1$, corresponding to the above fiber product. Note that $B \to B_1$, and thus f_1, depends on $\phi_{2,b}$. Thus,

$$\phi_{2,b}(f_2) = \phi_{2,b}(N_{B/B_2}(f)) = N_{B_1/B}(f_1).$$

Since $A_1 \to G_1(S)$ is a level structure, the right hand side equals $\prod_{a \in A_1} \phi_{1,a}(f_1)$. But $\phi_{1,a}(f_1) = \phi_{a'}(f)$, for a unique $a' \in A$ which maps to b. Taking the product over all $a \in A_1$ and corresponding a's, the conclusion follows. One can refer to the diagram below, where the parallelogram is cartesian and the triangles are commutative.



■

3.1 Oort-Tate generators

In this section, we introduce the notion of Oort-Tate generators and show that they coincide with Drinfeld-Katz-Mazur level structures for finite flat group schemes of order p. Our main reference is [HR12].

Recall from Section 2.2 that these are classified by the $\mathbb{Z}_p$-stack $OT = \operatorname{Spec} \mathbb{Z}_p[X,Y]/(XY - w_p)/\mathbb{G}_m$ with the universal group scheme $\mathcal{G} = \operatorname{Spec}_{OT} \mathcal{O}[Z]/(Z^p - XZ)/\mathbb{G}_m$ of order p. Inside $\mathcal{G}$ we define the *scheme of generators* $\mathcal{G}^\times$: it is the closed subscheme of $\mathcal{G}$ cut out by $Z^{p-1} - X$. The morphism $\mathcal{G}^\times \to OT$ is relatively representable and finite flat of degree $p-1$. Thus if G is a finite flat group scheme over a $\mathbb{Z}_p$-scheme S corresponding to a map $\varphi : S \to OT$ then $G = \varphi^*(\mathcal{G})$ and the *subscheme of generators* of G is $G^\times = \varphi^*(\mathcal{G}^\times)$.

Let's show that this notion is the same as Drinfeld-Katz-Mazur level structure. We check that if $\alpha \in G(S)$, then $\alpha \in G^\times(S)$ if and only if α has exact order p in the sense of Katz-Mazur, or, in other words, if and only if $\{0, \alpha, \ldots, (p-1)\alpha\}$ is a full set of sections of G/S:

Lemma 3.1.1. *Let $\alpha \in G^\times(S)$ be an Oort-Tate generator. Then $\{0, \alpha, \ldots, (p-1)\alpha\}$ is a full set of sections of G/S.*

Proof of lemma: As mentioned above, G corresponds to $\varphi : S \to OT$ via $G = \varphi^*(\mathcal{G})$. By localizing, we reduce to the affine case, so we can take $S = \operatorname{Spec} R$. Then $G = \operatorname{Spec} R[Z]/(Z^p - aZ)$, where a has the property that there exists $b \in R$ so that $ab = w_p$. (Note that in [HR12], a mistake seems to have been made, and a is assumed to be in pR).

Since α is a section in $G(S)$, it arises from a ring map $R[Z]/(Z^p - aZ) \to R$, i.e. is given by an element $c \in R$ such that $c^p = ac$. Note that Z has the property that $[m]Z = \chi(m)Z$, for every $1 \le m \le p-1$. Thus (see also [HR12]) that the group of sections $\{0, \alpha, \ldots, (p-1)\alpha\}$ corresponds to $\{0, c, \zeta c, \ldots, \zeta^{p-2}c\}$, where ζ is a primitive $p-1$th root of unity in R.

Then α defines a Drinfeld-Katz-Mazur level structure (i.e. full set of sections) if

$$Z^p - aZ = Z(Z - \zeta c)(Z - \zeta^2 c) \cdot \ldots \cdot (Z - \zeta^{p-2} c)$$

which is easily seen to be equivalent to $a = c^{p-1}$, hence $\alpha \in G^\times(S)$. ∎

Chapter 4

VARIOUS MODULI PROBLEMS

4.1 Moduli problems

In this chapter, we recall the definitions and basic properties of several moduli problems of p-divisible groups with different level structures. We do not use standard notation for these moduli problems. We largely follow the exposition of [HR12].

Denote by $\mathcal{M}_{\Gamma_1}$ the stack of p-divisible groups defined as follows: as a fibered category, if S is a scheme over $\mathbb{Z}_p$, then $\mathcal{M}_{\Gamma_1}(S)$ consists of (isomorphism classes) of p-divisible groups over S.

The moduli problem $\mathcal{M}_{\Gamma_0(p)}$ classifies p-divisible groups G with the following extra data: a filtration $0 = H_0 \subset H_1 \subset \cdots \subset H_h = G[p]$, where H_i is a finite flat group scheme of rank p^i and h is the height of G (compare with the $\Gamma_0(n)$-level in the introduction to the previous chapter). An equivalent datum is a chain of isogenies of p-divisible groups

$$G \to G_1 \to G_2 \ldots \to G_{h-1} \to G,$$

each of degree p and whose composition is $p \cdot \mathrm{id}_G$.

Let S be a scheme over $\mathbb{Z}_p$ and consider an S-point of $\mathcal{M}_{\Gamma_0(p)}$, corresponding to a p-divisible group G over S with a filtration H_i as above. Denote $X_i := H_i/H_{i-1}$. The X_i's are finite flat group schemes of order p.

Recall from 2.2 that OT denotes the $\mathbb{Z}_p$-stack of finite flat group schemes of order p and that over OT we have the universal finite flat group scheme of order p, denoted by $\mathcal{G}$. Inside $\mathcal{G}$ we have a closed subscheme $\mathcal{G}^\times$ - the scheme of generators of $\mathcal{G}$. From the definition of $\mathcal{M}_{\Gamma_0(p)}$ there is thus a map $\mathcal{M}_{\Gamma_0(p)} \to OT \times_{\mathbb{Z}_p} \ldots \times_{\mathbb{Z}_p} OT$ sending $(G, (H_i)) \mapsto (X_1, \ldots, X_h)$.

The moduli problem $\mathcal{M}_{\Gamma_1(p)}$ is then defined as the 2-fiber product

$$\begin{array}{ccc} \mathcal{M}_{\Gamma_1(p)} & \longrightarrow & \mathcal{G}^\times \times \ldots \times \mathcal{G}^\times \\ \downarrow & & \downarrow \\ \mathcal{M}_{\Gamma_0(p)} & \longrightarrow & OT \times \ldots \times OT. \end{array}$$

In other words, if S is a $\mathbb{Z}_p$-scheme, an S-point of $\mathcal{M}_{\Gamma_1(p)}$ is given by a p-divisible group G over S, with a filtration $0 = H_0 \subset H_1 \subset \cdots \subset H_h = G[p]$ as above and with Oort-Tate generators for each quotient H_i/H_{i-1}, which are finite flat of order p (compare with the $\Gamma_1(n)$-level in the introduction to the previous chapter).

Note that we have forgetful morphisms $\mathcal{M}_{\Gamma_1(p)} \to \mathcal{M}_{\Gamma_0(p)} \to \mathcal{M}_{\Gamma_1}$.

It follows from [Goe01] that $\mathcal{M}_{\Gamma_0(p)}$ is flat over $\mathrm{Spec}(\mathbb{Z}_p)$. In loc. cit. Gortz also writes down local model equations. From the 2-fiber product defining $\mathcal{M}_{\Gamma_1(p)}$ and the fact that $\mathcal{G}^\times$ is flat over OT (or from [Sha15]) it follows that $\mathcal{M}_{\Gamma_1(p)}$ is flat over $\mathcal{M}_{\Gamma_0(p)}$ and is thus flat over $\mathrm{Spec}(\mathbb{Z}_p)$.

Let's also introduce the moduli space $\mathcal{M}_{\Gamma(p)^{\mathrm{DKM}}}$. For any $\mathbb{Z}_p$-scheme S, $\mathcal{M}_{\Gamma(p)^{\mathrm{DKM}}}(S)$ will consist of (isomorphism classes of) p-divisible groups G equipped with a Drinfeld-Katz-Mazur level structure on $G[p]$.

The moduli space $\mathcal{M}_{\Gamma(p)^{\mathrm{DKM}}}$ is *not* well-behaved for higher-dimensional p-divisible groups. For example, it is not even flat, as Chai and Norman show in [CN90]. This contradicts for example the flatness conjectures of Rapoport and Zink [RZ96]. The non-flatness suggests that the Drinfeld-Katz-Mazur notion of level structure is inadequate for higher-dimensional p-divisible groups. Another example of this phenomenon is presented in [CN90], where the authors show, that the scheme S of all $(\mathbb{Z}/p\mathbb{Z})^2$-level structures on $\mu_p \times \mu_p$ over $\mathbb{Z}_{(p)}$ is not flat by computing the dimensions of its special and of its generic fibers and showing they are distinct.

Note that $\mu_p \times \mu_p$ is a truncated two-dimensional p-divisible group. We shall see the case of $\mu_p \times \mu_p$ again in the next chapter, as a non-example for the notion of level structure we are going to introduce.

Chapter 5

Γ(P)-LEVEL STRUCTURE

Let S be a scheme over $\mathbb{Z}_p$ and G a p-divisible group of height h and dimension d over S. We introduce the following notion of $\Gamma(p)$-level structure on G:

Definition 5.0.1. *A $\Gamma(p)$-level structure on G is the following data:*

1. *A filtration $0 = H_0 \subset H_1 \subset \ldots \subset H_h = G[p]$ of $G[p]$ by finite flat subgroup schemes, so that the rank of H_i is p^i.*
2. *Oort-Tate generators $\gamma_i : (\mathbb{Z}/p\mathbb{Z}) \to H_i/H_{i-1}$.*
3. *Group homomorphism $\varphi_i : (\mathbb{Z}/p\mathbb{Z})^i \to H_i$ such that the following diagram commutes:*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & \ldots & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{h-1} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^h \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & & & \downarrow{\scriptstyle \varphi_{h-1}} & & \downarrow{\scriptstyle \varphi_h} \\ 0 = H_0 & \longrightarrow & H_1 & \longrightarrow & H_2 & \longrightarrow & \ldots & \longrightarrow & H_{h-1} & \longrightarrow & H_h = G[p] \end{array}$$

so that the induced maps $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-1}$ are the Oort-Tate generator γ_i. We denote it succinctly by $\varphi := (\varphi_i) = (\varphi_1, \ldots, \varphi_h)$.

Note that data 1 defines a $\Gamma_0(p)$ level structure and G. Data 1 and 2 define a $\Gamma_1(p)$ level on $G[p]$.

Consider the functor which to an $\mathbb{Z}_p$-scheme S associated the set of p-divisible groups of height h and dimension d together with a $\Gamma(p)$-level structure, up to isomorphism. This is relatively representable by $\mathcal{M}_{\Gamma(p)}$ which has a natural map to $\mathcal{M}_{\Gamma_1(p)}$ obtained by ''forgetting'' the (vertical) group homomorphism in the above diagram. Sometimes, to emphasize that we are using our new definition, we write $\mathcal{M}_{\Gamma(p)^{\mathrm{new}}}$ instead of $\mathcal{M}_{\Gamma(p)}$.

Let's establish some basic properties of this new notion of level structure. We first see that $(\mathbb{Z}/p\mathbb{Z})^h \to G[p]$ forms a full set of sections i.e. is a Drinfeld-Katz-Mazur level structure. In fact, we show:

Lemma 5.0.1. *Let $\varphi = (\varphi_1, \ldots, \varphi_h)$ be a $\Gamma(p)$-level structure on a p-divisible group G. Then each φ_i is a Drinfeld-Katz-Mazur level structure on H_i. In particular, φ_h is a Drinfeld-Katz-Mazur level structure on $G[p]$.*

Proof of lemma: We use induction on i. For $i = 1$, it is part of the *definition* of a $\Gamma(p)$-level structure that $\varphi_1 : \mathbb{Z}/p\mathbb{Z} \to H_1$ is an Oort-Tate generator, which by lemma 3.1.1 means that φ_1 is a Drinfeld-Katz-Mazur level structure.

For the induction step, apply Lemma 3.0.1 to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{i-1} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{i} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_{i-1}} & & \downarrow{\scriptstyle \varphi_i} & & \downarrow & & \\ 0 & \longrightarrow & H_{i-1}(S) & \longrightarrow & H_i(S) & \longrightarrow & (H_i/H_{i-1})(S). & & \end{array}$$

The left vertical arrow is a Drinfeld-Katz-Mazur level structure by induction and the right one by definition. Lemma 3.0.1 then implies that φ_i also is a Drinfeld-Katz-Mazur level structure. ■

The content of Lemma 5.0.1 and the forgetful maps mentioned above and in the previous chapter can be summarized in the following diagram:

$$\begin{array}{ccc} & & \mathcal{M}_{\Gamma(p)^{\mathrm{new}}} \\ & \swarrow & \downarrow \\ & & \mathcal{M}_{\Gamma_1(p)} \\ & & \downarrow \\ \mathcal{M}_{\Gamma(p)^{\mathrm{DKM}}} & & \mathcal{M}_{\Gamma_0(p)} \\ & \searrow & \downarrow \\ & & \mathcal{M}_{\Gamma_1} \end{array}$$

5.1 A (non-)example

In this section, we will see that our notion of $\Gamma(p)$-level structure is different from than of Drinfeld-Katz-Mazur level structure. We give an example of a p-divisible group and a Drinfeld-Katz-Mazur level structure which does not arise as a $\Gamma(p)$-level structure. In a later section, we prove that for 1-dimensional p-divisible groups our notion of $\Gamma(p)$-level structure does agree with the Drinfeld-Katz-Mazur one, so the smallest (non-)example should arise from a p-divisible group of dimension at least 2.

Let G be the p-divisible group $\mu_{p^\infty} \times \mu_{p^\infty}$ over $S = \mathrm{Spec}(\mathbb{Z}/p^2\mathbb{Z})$. This is a p-divisible group of height 2 and dimension 2. Let $H := G[p] = \mu_p \times \mu_p$. Consider the map $\alpha : (\mathbb{Z}/p\mathbb{Z})^2 \to G(S)$ given by sending every element to the zero section.

We check that this is a Drinfeld-Katz-Mazur level structure. The argument is presented in Katz and Mazur [KM85], as a counter-example for a *converse* of Lemma 3.0.1. It also serves the purpose of an example of a Drinfeld-Katz-Mazur level structure which is not a $\Gamma(p)$-level structure, as introduced by us. For completeness, we present the argument from [KM85] here.

The Hopf algebra of H is $B = (\mathbb{Z}/p^2\mathbb{Z})[X,Y]/(X^p - 1, Y^p - 1)$. The zero section on B corresponds to the ring homomorphism sending X and Y to 1. Thus the p^2 sections P_i in the definition of full set of sections, on the level of rings, do the following: for any $\mathbb{Z}/p^2\mathbb{Z}$-algebra R and $f \in R \otimes_{\mathbb{Z}/p^2\mathbb{Z}} B = R[X,Y]/(X^p - 1, Y^p - 1)$ it sends $f \mapsto f(1,1) \in R$. Thus, to check that α is a Drinfeld-Katz-Mazur level structure, we need to verify the following: if R is a $\mathbb{Z}/p^2\mathbb{Z}$-algebra, and $f \in R \otimes_{\mathbb{Z}/p^2\mathbb{Z}} B = R[X,Y]/(X^p - 1, Y^p - 1)$, then

$$\det(T - f) = (T - f(1,1))^{p^2}$$

or, equivalently, that

$$\mathrm{norm}(f) = f(1,1)^{p^2}$$

In other words, it suffices to check that if R is *any* algebra, then

$$\mathrm{norm}(f) \equiv f(1,1)^{p^2} \pmod{p^2}.$$

By transitivity of the norm, it factors as $R[X,Y]/(X^p-1, Y^p-1) \xrightarrow{N_X} R[Y]/(Y^p-1) \xrightarrow{N_Y} R$. Since the zero map is a full set of sections for μ_p in characteristic p (as seen above), it follows that

$$N_X(f) = f(1,Y)^p + p \cdot g(Y),$$

for some polynomial $g \in R[Y]/(Y^p - 1)$.

Note now that $N_Y(h + pg) \equiv N_Y(h) \mod p^2$. Indeed, consider more generally the norm map $N_Y(h + Tg) : R[T][Y]/(Y^p - 1) \to R[T]$ for an indeterminate T and express this as a polynomial in T:

$$N_Y(h + Tg) = N_Y(h) + T^p N_Y(g) + \sum_{i=1}^{p-1} T^i Q_i(h,g).$$

Since mod p the zero map is a full set of sections, $N_Y(h + Tg)$ mod p is just $(h(1) + Tg(1))^p = h(1)^p + T^p g(1)^p$. This implies that $Q_i(h,g) \equiv 0 \pmod{p}$ for every

i. Thus, $N_Y(h+Tg) \equiv N_Y(h) \pmod{pT, T^p}$. Taking $T = p$ yields $N_Y(h+pg) \equiv N_Y(h) \pmod{p^2}$, as claimed.

Thus,

$$\begin{aligned} N(f) &= N_Y\left(f(1,Y)^p + p \cdot g(Y)\right) \equiv N_Y\left(f(1,Y)^p\right) \pmod{p^2} = \\ &= (N_Y(f(1,Y)))^p = (f(1,1)^p + p \cdot \alpha)^p \pmod{p^2} \equiv f(1,1)^{p^2} \pmod{p^2}, \end{aligned}$$

as wanted.

We then check that this does not arise as a $\Gamma(p)$-level structure as in our definition. Indeed, it suffices to verify that the zero map $\mathbb{Z}/p\mathbb{Z} \to \mu_p$ does not form a full set of sections over the base $S = \mathrm{Spec}(\mathbb{Z}/p^2\mathbb{Z})$. Indeed, we have already seen this in Chapter 3, the example following the definition of full set of sections - the zero map $\mathbb{Z}/p\mathbb{Z} \to \mu_p$ is not a full set of sections unless $p = 0$.

5.2 1-dimensional p-divisible groups

In this subsection, we show that if G is 1-dimensional (i.e. $d = 1$) then our new notion of $\Gamma(p)$-level structure agrees with the existing notion of Drinfeld-Katz-Mazur level structure, as used for example in [HT01].

Using Lemma 5.0.1, we saw that given a $\Gamma(p)$-level structure $\varphi = (\varphi_i)$ as in our definition gives a Drinfeld-Katz-Mazur level structure, namely φ_h. This holds true for any dimension d. This gives us a morphism $\mathcal{M}_{\Gamma(p)^{\mathrm{new}}} \to \mathcal{M}_{\Gamma(p)^{\mathrm{DKM}}}$.

We show that a Drinfeld-Katz-Mazur level structure on a 1-dimensional p-divisible group G (over a base scheme $S/\mathbb{Z}_p$) gives us a $\Gamma(p)$-level structure and these two associations are inverse to each other, in other words our notion of $\Gamma(p)$-level structure coincides with the existing notion of ‘‘full level structure’’ for 1-dimensional p-divisible groups.

We shall need a preliminary lemma, sketched in [HT01]:

Lemma 5.2.1. *Let G be a 1-dimensional p-divisible group over a locally noetherian base scheme S. Then, for any i, locally on S, $G[p^i]$ is embeddable in a smooth curve C/S.*

Proof of lemma: As we are working locally on the base, we can assume that S is affine. Let $S = \mathrm{Spec}\, A$ and $G[p^i] = \mathrm{Spec}\, R$. Our goal is to find a surjection $A[T] \twoheadrightarrow R$. It suffices to find, for each maximal ideal $\mathfrak{m}$ of A and each $f \in A - \mathfrak{m}$ a surjection $A_f[T] \twoheadrightarrow R_f$. Using Nakayama's lemma, it suffices then to find a surjection $(A/\mathfrak{m})[T] \twoheadrightarrow R/\mathfrak{m}$, i.e. we have reduced to the case where the base S is the spectrum of a field.

In fact, we can assume that this field is algebraically closed. Indeed, let $N = p^{ih}$ be the rank of R over A as a module. The map $A[T] \to R$ is surjective if and only if the images $1, T, \ldots, T^{N-1}$ are linearly independent (so the image of $A[T] \to R$ has full rank and is thus all of R). All these images are determined by the image of T. If $T \mapsto \sum t_j e_j$, where (e_j) is some basis of R over A, then linear independence is equivalent to a certain polynomial in the t_j's being nonzero. This condition stays invariant when passing to algebraic closure.

We have thus reduced the setup of the lemma to a 1-dimensional p-divisible group G over an algebraically closed field A. Recall that over perfect fields, we have a (split) connected-étale sequence (see section 2.3 in chapter 2), hence $G[p^i]$ is a disjoint union of copies of $G^0[p^i]$ and thus we reduce to the case where G is connected. But in this case we know that $G[p^i] = \operatorname{Spec} R$ for a ring R of the form $A[[T]]/(T^{p^{hi}})$, and the map $A[T] \to A[[T]] \twoheadrightarrow R$ is the desired surjective map. ∎

Proposition 5.2.1. *Let S be a base scheme over $\mathbb{Z}_p$ and let G be a 1-dimensional p-divisible group over S. Consider a Drinfeld-Katz-Mazur level structure $\varphi : (\mathbb{Z}/p\mathbb{Z})^h \to G[p]$ on G. Then there is a unique filtration $0 = H_0 \subset H_1 \subset \ldots \subset H_h = G[p]$ of $G[p]$, so that each H_i has rank p^i, φ restricted to $(\mathbb{Z}/p\mathbb{Z})^i$ factors through H_i and is a Drinfeld level structure for H_i and the induced maps $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-1}$ for each i are Oort-Tate generators.*

Proof. We follow and elaborate on details of the proof of Lemma II.4.1 in [HT01]. Note that we do not need to assume that S is locally Noetherian and has a dense set of points with residue field algebraic over $\mathbb{F}_p$ - we can always reduce to this case using standard results from EGA (see also [Wed00], page 306).

By the lemma above, we are justified in applying Corollary I.10.3 in [KM85], which says that there is a unique closed *subscheme* H_i of $G[p]$, locally free over S, for which $\varphi|_{(\mathbb{Z}/p\mathbb{Z})^i} \to H_i$ is a Drinfeld level structure for H_i. We have to check that H_i is a *subgroup* of $G[p]$.

The condition of H_i being a subgroup and the conditions imposed on the quotients H_i/H_{i-1}, are both closed conditions, defined in fact by finitely many relations and generators. There is thus a closed subscheme $S' \subset S$ so that for any scheme T/S, $H_i \times_S T \hookrightarrow G[p] \times_S T$ has the required properties if and only if $T \to S$ factors though S'.

Our goal is then to prove that $S' = S$.

We establish this via a series of reductions. The first one is to the case where $S = \operatorname{Spec} A$ for an Artinian local ring A. Indeed, to check equality of two closed subschemes, it suffices to do so at the local rings of a dense set of points. We then reduce to the Artinian local case and thus look at $A = \mathcal{O}_{S,s}/\mathfrak{m}_s^i$ as s runs through a dense set of points and $i \in \mathbb{Z}_{\geq 0}$, A having residue field k algebraic over $\mathbb{F}_p$ (recall that we can assume S has these properties, e.g. [Wed00], page 306). Recall that if R is any perfect ring of characteristic p, then $W(R)$ is flat over $\mathbb{Z}_p$. Since checking equality of two closed subschemes (defined by certain ideals) can be done after a flat base change, we can tensor with $W\left(\overline{k}\right)$ over $\mathbb{Z}_p$ and it suffices to check $S' = S$ after this base change. In other words, we can assume $S = \operatorname{Spec} A$ where A is a local Artinian ring with algebraically closed residue field $\overline{\mathbb{F}_p}$.

But a p-divisible group H/A with a Drinfeld-Katz-Mazur level structure is obtained by pullback from the universal deformation on $H \times \operatorname{Spec}(\overline{\mathbb{F}_p})$, together with its level structure. This deformation has been studied explicitly by Drinfeld and Harris and Taylor, and we have thus reduced to proving $S = S'$ in the case of a p-divisible group H over a complete Noetherian local ring R, together with its level structure. This ring is flat over $\mathcal{O}_{\hat{\mathbb{Q}}_p^{\text{unr}}}$, and thus after another flat base change, it suffices to check our assertion over $\operatorname{Spec}(R) \times \operatorname{Spec}(\mathbb{Q}_p)$, which is dense in $\operatorname{Spec}(R)$. In this case, H is étale, the level structure is an isomorphism and the existence of the filtration as claimed is clear: for example, embed H in a curve, and take the H_i's as sum of Cartier divisors: $H_i := \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^i} [\varphi(x)]$, viewed as a closed subscheme of $H[p^m]$.

□

5.3 Flatness

The goal of this section is to prove that

Theorem 5.3.1. *$\mathcal{M}_{\Gamma(p)^{\text{new}}}$ is flat over $\mathbb{Z}_p$.*

Recall from the previous chapter that the maps $\mathcal{M}_{\Gamma_1(p)} \to \mathcal{M}_{\Gamma_0(p)}$ and $\mathcal{M}_{\Gamma_0(p)} \to \mathbb{Z}_p$ are flat. We will verify that $\mathcal{M}_{\Gamma(p)^{\text{new}}}$ is flat over $\mathcal{M}_{\Gamma_0(p)}$. Since the latter is flat over $\mathbb{Z}_p$, our result will follow.

Theorem 5.3.2. *$\mathcal{M}_{\Gamma(p)^{\text{new}}}$ is flat over $\mathcal{M}_{\Gamma_0(p)}$.*

Proof. We will construct a tower of moduli spaces $\mathcal{M}_i$ for $i = 0, 1, \ldots, h-1, h$, so that $\mathcal{M}_0 = \mathcal{M}_{\Gamma_0(p)}$, $\mathcal{M}_h = \mathcal{M}_{\Gamma(p)^{\mathrm{new}}}$ and such that $\mathcal{M}_i$ is flat over $\mathcal{M}_{i-1}$ for every $i = 1, \ldots, h$.

$\mathcal{M}_i$ will be moduli space representing the following moduli problem:

For a base scheme $S/\mathbb{Z}_p$, we consider the moduli problem classifying p-divisible groups of height h over S, together with a filtration $0 = H_0 \subset H_1 \subset \ldots \subset H_h = G[p]$ together with i compatible group homomorphisms $\varphi_1, \ldots, \varphi_i$ such that the induced maps $\mathbb{Z}/p\mathbb{Z} \to H_j/H_{j-1}$, $1 \leq j \leq i$ are Oort-Tate generators:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & \ldots & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{i-1} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^i \\
 & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & & & \downarrow{\scriptstyle \varphi_{i-1}} & & \downarrow{\scriptstyle \varphi_i} \\
H_0 = 0 & \longrightarrow & H_1 & \longrightarrow & H_2 & \longrightarrow & \ldots & \longrightarrow & H_{i-1} & \longrightarrow & H_i
\end{array}$$

Note that $\mathcal{M}_0$ is just $\mathcal{M}_{\Gamma_0(p)}$ and $\mathcal{M}_h = \mathcal{M}_{\Gamma(p)^{\mathrm{new}}}$. There is a natural map $\mathcal{M}_i \to \mathcal{M}_{i-1}$ obtained by forgetting φ_i and the Oort-Tate generator $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-1}$. We will show that $\mathcal{M}_i$ is flat over $\mathcal{M}_{i-1}$ for each i. It will follow that $\mathcal{M}_{\Gamma(p)^{\mathrm{new}}} = \mathcal{M}_h$ is flat over $\mathcal{M}_0 = \mathcal{M}_{\Gamma_0(p)}$, as desired.

The case $i = 1$ is slightly different from the others, and we treat it first:

Let $i = 1$. By definition, $\mathcal{M}_1$ represents the functor over $\mathcal{M}_{\Gamma_0(p)}$ whose S-points are given by a p-divisible group G/S together with a filtration (H_i) as in the definition of $\Gamma_0(p)$-level, together with an Oort-Tate generator of H_1. This means that $\mathcal{M}_1$ is the 2-fiber product of the following diagram:

$$\begin{array}{ccc}
\mathcal{M}_1 & \longrightarrow & \mathcal{G}^{\times} \\
\downarrow & & \downarrow \\
\mathcal{M}_0 = \mathcal{M}_{\Gamma_0(p)} & \longrightarrow & OT
\end{array}$$

where the bottom arrow extracts H_1.

Since $\mathcal{G}^{\times}$ is flat over OT (see 3.1), it follows that $\mathcal{M}_1$ is flat over $\mathcal{M}_{\Gamma_0(p)}$.

Assume now that $2 \leq i \leq h$ and let's show that $\mathcal{M}_i$ is flat over $\mathcal{M}_{i-1}$.

Note that the forgetful map $\mathcal{M}_i \to \mathcal{M}_{i-1}$ factors through $\mathcal{M}_{i-1} \times_{OT} \mathcal{G}^{\times}$. Indeed, this corresponds to forgetting φ_i, but not the induced Oort-Tate generator $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-1}$. By a similar argument as in the $i = 1$ case, $\mathcal{M}_{i-1} \times_{OT} \mathcal{G}^{\times} \to \mathcal{M}_{i-1}$ is flat. It thus suffices to establish flatness of $\mathcal{M}_i \to \mathcal{M}_{i-1} \times_{OT} \mathcal{G}^{\times}$.

We show that $\mathcal{M}_i$ is in fact a fppf torsor over $\mathcal{M}_{i-1} \times_{OT} \mathcal{G}^\times$ under H_{i-1} and thus flat. Consider the diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{i-1} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{i} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_{i-1}} & & \vdots & & \downarrow{\scriptstyle \gamma_i} & & \\
0 & \longrightarrow & H_{i-1} & \longrightarrow & H_i & \longrightarrow & H_i/H_{i-1} & \longrightarrow & 0
\end{array}$$

Observe that since φ_{i-1} is a Drinfeld-Katz-Mazur level structure and $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-1}$ is an Oort-Tate generator, Lemma 3.1.1 implies that any group homomorphism, if it exists, completing the diagram as above is automatically a Drinfeld-Katz-Mazur level structure.

Group homomorphisms $\varphi_i : (\mathbb{Z}/p\mathbb{Z})^i \to H_i$ yielding the above diagram commutative, if they exist, are classified by $\mathcal{H} := \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, H_{i-1}) = H_{i-1}$. We claim that $\mathcal{M}_i$ is a H_{i-1}-torsor over $\mathcal{M}_{i-1} \times_{OT} \mathcal{G}^\times$. For that we need to verify that locally, the above diagram can be completed with a dotted arrow.

Any extension filling in the above diagram arises in the following form:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{i-1} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{i} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_{i-1}} & & \downarrow & & \| & & \\
0 & \longrightarrow & H_{i-1} & \longrightarrow & ?_1 & \longrightarrow & (\mathbb{Z}/p\mathbb{Z}) & \longrightarrow & 0 \\
 & & \| & & \vdots & & \| & & \\
0 & \longrightarrow & H_{i-1} & \longrightarrow & ?_2 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow{\scriptstyle \gamma_i} & & \\
0 & \longrightarrow & H_{i-1} & \longrightarrow & H_i & \longrightarrow & H_i/H_{i-1} & \longrightarrow & 0
\end{array}$$

where the second row is the pushout under $\varphi_i : (\mathbb{Z}/p\mathbb{Z})^{i-1} \to H_{i-1}$ and the third row is the pull-back under $\gamma_i : \mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-1}$. We thus need to verify that a dotted arrow such as above exists, locally on the base.

Note that the top row $0 \to (\mathbb{Z}/p\mathbb{Z})^{i-1} \to (\mathbb{Z}/p\mathbb{Z})^i \to \mathbb{Z}/p\mathbb{Z} \to 0$ is a split extension, and thus corresponds to the trivial element in the corresponding Ext group. Thus the extension

$$0 \longrightarrow H_{i-1} \longrightarrow ?_1 \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

is trivial, as it is obtained by pushout from a trivial extension. A dotted arrow as above then exists if and only if the class of

$$0 \longrightarrow H_{i-1} \longrightarrow ?_2 \longrightarrow (\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

in the Ext group is trivial, i.e. if the sequence splits locally. Note that $?_2$ is the fiber product $H_i \times_{H_i/H_{i-1}} (\mathbb{Z}/p\mathbb{Z})$. Since H_i (and $\mathbb{Z}/p\mathbb{Z}$) are killed by p (see [TO70]), $?_2$ is also killed by p. We then invoke following lemma:

Lemma 5.3.1. *Let G be a commutative finite flat group scheme killed by p. Every short exact sequence*

$$0 \to H \to G \to (\mathbb{Z}/p\mathbb{Z}) \to 0$$

splits locally in the fppf topology.

Proof of lemma: If S is our base scheme, then any section in $(\mathbb{Z}/p\mathbb{Z})_S(S)$ has, fppf locally, a preimage in G. Say $T \to S$ is such a scheme, i.e. $1 \in (\mathbb{Z}/p\mathbb{Z})(T)$ acquires a preimage. But $G(T)$, by assumption is killed by p.

Note that $G(T)$, as an abstract group, could be infinite (for example $G = \alpha_p \times \alpha_p$ over an infinite field k of characteristic p and $T = k[\epsilon]/(\epsilon^p)$). However, *any* pre-image of $1 \in (\mathbb{Z}/p\mathbb{Z})(T)$ gives a splitting, as $G(T)$ is killed by p. In other words, every exact sequence of (abstract) abelian groups

$$0 \to A \to G(T) \to \mathbb{Z}/p\mathbb{Z} \to 0,$$

where A and $G(T)$ are killed by p, splits. ∎

□

Chapter 6

EPIPELAGIC LEVEL AND CERTAIN GROUP SCHEMES OF ORDER P^2

6.1 Epipelagic level structure

In this section, we discuss yet another notion of level structure on p-divisible groups. The motivation comes from the study of epipelagic representations. Just like our notion of $\Gamma(p)$-level, it ''lives'' over $\mathcal{M}_{\Gamma_1(p)}$, however it is not ''comparable'' to it. To introduce the moduli problem on p-divisible groups, we first define:

Definition 6.1.1. *Let S be a scheme over $\mathbb{Z}_p$ and G be a p-divisible group of height h over S. An epipelagic level structure on G is the data consisting of*

1. *A filtration $0 = H_0 \subset H_1 \subset \ldots \subset H_h = G[p]$ of $G[p]$ by finite flat group schemes H_i of rank p^i. Note that the isomorphism $G[p^2]/G[p] \xrightarrow{\simeq} G[p]$ induced by multiplication by p allows us to extend this filtration to the right $H_{h-1} \subset H_h = G[p] = H_{h+1} \subset \ldots \subset G[p^2]$, such that $H_{h+1}/G[p] \simeq H_1$.*

2. *Oort-Tate generators γ_i for the quotients H_i/H_{i-1} (which are finite flat of rank p), for $i = 1, \ldots, h+1$ such that $\gamma_{h+1} = \gamma_1$.*

3. *For $2 \leq i \leq h+1$, group homomorphisms $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-2}$ such that the composition $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-2} \twoheadrightarrow H_i/H_{i-1}$ is the Oort-Tate generator $\gamma_i : \mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-1}$.*

Denote by $\mathcal{M}_{I_{++}}$ the set-valued functor on $\mathrm{Sch}/\mathbb{Z}_p$ whose values on S are given by p-divisible groups with an epipelagic level structure. Note that we have a natural map $\mathcal{M}_{I_{++}} \to \mathcal{M}_{\Gamma_1(p)}$ by forgetting the group homomorphisms $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-2}$.

We now show that $\mathcal{M}_{I_{++}}$ is flat over $\mathbb{Z}_p$ by showing that it flat over $\mathcal{M}_{\Gamma_1(p)}$, which is flat over $\mathbb{Z}_p$ (see chapter 4). In fact we prove that

Proposition 6.1.1. *$\mathcal{M}_{I_{++}}$ is a torsor over $\mathcal{M}_{\Gamma_1(p)}$ under $\prod_{i=2}^{h+1} H_i/H_{i-1}$.*

Proof. The data of a map $\mathbb{Z}/p\mathbb{Z} \to H_i/H_{i-2}$ such that the composition with $H_i/H_{i-2} \to H_i/H_{i-1}$ is the Oort-Tate generator γ_i is the same as a dotted group homomorphism making the following diagram commute:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma_{i-1}} & & \vdots & & \downarrow{\scriptstyle \gamma_i} & & \\ 0 & \longrightarrow & H_{i-1}/H_{i-2} & \longrightarrow & H_i/H_{i-2} & \longrightarrow & H_i/H_{i-1} & \longrightarrow & 0 \end{array}$$

If a group homomorphism completing the above exists, then all such group homomorphisms are classified by $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, H_{i-1}/H_{i-2}) = H_{i-1}/H_{i-2}$. The argument for $i = 2$ used in the proof of flatness for $\Gamma(p)$-level structures shows that existence is indeed satisfied. □

Corollary 6.1.1. *$\mathcal{M}_{I_{++}}$ is flat over $\mathbb{Z}_p$.*

We now take a different turn. Recall that in writing down the local models of Shimura varieties for $\Gamma_1(p)$-level structure, a crucial gadget was the classification of group schemes of order p due to Oort-Tate and level structures on them (see [Sha15] and [HR12]). Similarly, when trying to write down the local model for the moduli space of p-divisible groups with epipelagic level structure, a useful gadget would be a classification of group schemes G of order p^2, killed by p, equipped with an extension structure $0 \to H_1 \to G \to H_2 \to 0$, or at least of such extensions when $H_2 = \mathbb{Z}/p\mathbb{Z}$.

We will give a partial result in this direction, giving an explicit classification of extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p over $\mathbb{Z}_p$-algebras R. Note that one can compute (abstractly) the group $\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ as $H^1_{\mathrm{fppf}}(\mathrm{Spec}(R), \mu_p)$. Using Kummer theory, the latter is (locally) isomorphic to $R^*/(R^*)^p$. We will arrive at this result from a different direction, by analyzing in detail what happens on the level of Hopf algebras, using Oort-Tate theory along the way. It is our hope that such an approach can be generalized to classify other extensions.

6.2 Certain group schemes of order p^2

Let R be any algebra and $\epsilon \in R^\times$ a unit. Consider the following group schemes, which we denote by G_ϵ, introduced in [KM85]. The affine ring of G_ϵ is

$$B_\epsilon := \bigoplus_{i=0}^{p-1} R[X_i]/(X_i^p - \epsilon^i).$$

For any R-algebra A with connected spectrum $T = \mathrm{Spec}\, A$, we have

$$G_\epsilon(T) = \{(t, i) |\ t^p = \epsilon^i,\ 0 \le i \le p-1\}$$

Addition is defined as

$$(t,i)\cdot(s,j)=\begin{cases}(st,i+j), \text{ if } i+j<p\\ (st/\epsilon,i+j-p), \text{ if } i+j\geq p\end{cases}$$

Comultiplication is given by

$$X_i=(0,\dots,0,X_i,0,\dots,0)\mapsto\sum_{j=0}^{i}X_j\otimes X_{i-j}+\sum_{j=i+1}^{p-1}\frac{X_j\otimes X_{p+i-j}}{\epsilon}$$

and

$$e_i=(0,\dots,0,1,0,\dots,0)\mapsto\sum_{j+k=i \pmod p}e_j\otimes e_k,$$

as is usual for constant group schemes. Here we view e_i and X_i as elements in the ith component $R[X_i]/(X_i^p-\epsilon^i)$. The augmentation ideal has rank p^2-1 and equals $\langle X_0-1\rangle\oplus R[X_1]/(X_1^p-\epsilon)\oplus\cdots\oplus R[X_{p-1}]/(X_{p-1}^p-\epsilon^{p-1})$.

Projection onto the first factor $B\twoheadrightarrow R[X_0]/(X_0^p-1)$ and the map sending $X_i\to 0$ for every i (on functor of points, this sends $(a,i)\mapsto i$) induces a short exact sequence of group schemes

$$0\to\mu_p\to G_\epsilon\to\mathbb{Z}/p\mathbb{Z}\to 0$$

This sequence splits if and only if ϵ is a pth power of a unit in R.

6.3 Extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p in characteristic p

In this section we prove that in characteristic p, locally on the base, the group schemes G_ϵ defined above are the only finite flat extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p. Let R be a (connected) $\mathbb{F}_p$-algebra. Since $\mathbb{Z}/p\mathbb{Z}$, as a scheme over $S=\operatorname{Spec}(R)$, has p disjoint components, an extension G of $\mathbb{Z}/p\mathbb{Z}$ by μ_p is of the form $G_0\coprod S_1\coprod\dots\coprod S_{p-1}$, where $G_0=\mu_p$ and S_i are schemes, flat over $S=\operatorname{Spec}(R)$ of rank p.

For each $i=1,\dots,p-1$ we have an action $G_0\times S_i\to S_i$. Let us investigate this action. We need to use certain results about μ_p actions from [Tzi17]. That paper studies actions of α_p and μ_p on schemes and the result we need is only proved for α_p, so we prove it for μ_p here:

Lemma 6.3.1. *Let X be a scheme of finite type over a ring R of characteristic $p>0$. X admits a nontrivial μ_p action if and only if X has a nontrivial global vector field D such that $D^p=D$.*

Before we begin the proof, let us summarize the results of Proposition 2.2.1 in characteristic p:

Proposition 6.3.1 ([TO70])**.** *Let R be a ring of characteristic p and consider the Hopf algebra $B = R[z]/(z^p - 1)$ of $\mu_p/\operatorname{Spec} R$. Then, there is an element y such that:*

1. *$\mathbf{I}_1$ is generated by y and $\mathbf{I}_j$ is generated by y^j, for $1 \leq j \leq p-1$ (notation from chapter II).*
2. *For $1 \leq j \leq p-1$, we have $y^j = j!y_j$. We denote $w_j := j!$. Moreover*
$$y^p = w_p y = 0,$$
for some $w_p \in \mathbb{Z}_p$ equal to $p \cdot (unit)$.
3. $$\Delta(y_i) = y_i \otimes 1 + 1 \otimes y_i + \sum_{j=1}^{p-1} y_j \otimes y_{i-j}$$
and in particular
$$\Delta(y) = y \otimes 1 + 1 \otimes y + \sum_{j=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$$
4. $z = 1 + y + \dfrac{y^2}{2!} + \cdots + \dfrac{y^{p-1}}{(p-1)!}$.

Let us go back now to the proof of the Lemma 6.3.1.

Proof. Suppose first that X has a nontrivial vector field D such that $D^p = D$. Let y be the element in the Hopf algebra of μ_p described above (so the Hopf algebra of μ_p is $\operatorname{Spec} R[y]/(y^p - w_p y) = \operatorname{Spec} R[y]/(y^p)$; however y is *not* $z - 1$ in the traditional representation of μ_p as $R[z]/(z^p - 1)$).

Consider the map $\Phi : \mathcal{O}_X \to \mathcal{O}_X[y]/(y^p)$ by setting
$$\Phi(a) = \sum_{m=0}^{p-1} \frac{D^{(m)}(a)}{m!} y^m$$

Let's check that this defines an action of μ_p on X. Recall that the comultiplication $\Delta : R[y]/(y^p) \to R[y]/(y^p) \otimes R[y]/(y^p)$ sends $y \mapsto y \otimes 1 + 1 \otimes y + \sum_{i=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$.

We need to verify that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{O}_X & \xrightarrow{\Phi} & \mathcal{O}_X \otimes_R R[y]/(y^p) \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi\otimes 1} \\ \mathcal{O}_X \otimes_R R[y]/(y^p) & \xrightarrow{1\otimes\Delta} & \mathcal{O}_X \otimes_R R[y]/(y^p) \otimes_R R[y]/(y^p) \end{array}$$

Indeed, a section $a \in \mathcal{O}_X$ gets sent to $\sum_{m,n=0}^{p-1} \frac{D^{(m+n)}(a)}{m!n!} y^m \otimes y^n$ under the above-diagonal composition of the above diagram. The below-diagonal composition sends

$$a \mapsto \sum_{m=0}^{p-1} \frac{D^{(m)}(a)}{m!} \Delta(y^i)$$

Since

$$\Delta(y^i) = \Delta(w_i y_i) = w_i \Delta(y_i) = w_i \left(y_i \otimes 1 + 1 \otimes y_i + \sum_{j=1}^{p-1} y_j \otimes y_{i-j} \right) =$$

$$= w_i \left(\frac{1}{w_i} y^i \otimes 1 + \frac{1}{w_i} 1 \otimes y^i + \sum_{j=1}^{p-1} \frac{y^j}{w_j} \otimes \frac{y^{i-j}}{w_{i-j}} \right)$$

we can see that the coefficients of $y^n \otimes y^m$ is equal to

$$\frac{D^{(m+n)}(a)}{(m+n)!} \cdot w_{m+n} \cdot \left(\frac{1}{w_n} \otimes \frac{1}{w_m} \right),$$

if $m + n < p$ and

$$\frac{D^{(m+n-p+1)}(a)}{(m+n)!} \cdot w_{m+n} \cdot \left(\frac{1}{w_n} \otimes \frac{1}{w_m} \right),$$

if $m + n \geq p$ respectively. The result then follows since $w_i = i! \pmod p$ for $1 \leq i \leq p-1$ and $D^p = D$.

Assume now X admits a non-trivial μ_p-action given by $\alpha : \mu_p \times X \to X$. This corresponds to a co-action map

$$\alpha^* : \mathcal{O}_X \to \mathcal{O}_X \otimes_R R[y]/(y^p).$$

By definition, we then have the commutative diagram:

$$\begin{array}{ccc} \mathcal{O}_X & \xrightarrow{\alpha^*} & \mathcal{O}_X \otimes_R R[y]/(y^p) \\ \downarrow{\scriptstyle \alpha^*} & & \downarrow{\scriptstyle \alpha^*\otimes 1} \\ \mathcal{O}_X \otimes_R R[y]/(y^p) & \xrightarrow{1\otimes\Delta} & \mathcal{O}_X \otimes_R R[y]/(y^p) \otimes_R R[y]/(y^p) \end{array}$$

Write

$$\alpha^*(a) = a \otimes 1 + \Phi_1(a) \otimes y + \sum_{j=2}^{p-1} \Phi_j(a) \otimes y^j.$$

It is clear that the Φ_i's are R-linear. Since $y^p = 0$ and α^* is a ring homomorphism, the relation $\alpha^*(ab) = \alpha^*(a)\alpha^*(b)$ implies that $\Phi_1(ab) = a\Phi_1(b) + b\Phi_1(a)$, i.e. that Φ_1 is a derivation. We now prove by induction that $\Phi_i = \frac{\Phi_1^{(i)}}{i!}$.

Indeed, the coefficient of $y \otimes y^i$ under the above-diagonal compositions is $\Phi_1(\Phi_i(a))$. Under the below-diagonal composition, this is

$$\frac{w_{i+1}\Phi_{i+1}(a)}{w_i w_1}.$$

By induction, $\Phi_i(a) = \frac{\Phi_1^{(i)}(a)}{i!}$, thus $\Phi_{i+1}(a) = \frac{\Phi_1^{(i+1)}(a)}{(i+1)!}$ since $w_i = i!$ for every i.

Finally, equating the coefficients of $y \otimes y^{p-1}$ under the two compositions, one obtains $D^p = D$, proving the lemma.

We will also need the following result (mild generalization of lemma 4.1 in [Tzi17]):

Lemma 6.3.2. *Let A be an $\mathbb{Z}_p$-algebra and M and A-module. Let $\Phi : M \to M$ be an A-module homomorphism such that $\Phi^p = \Phi$. Then $M = \oplus_{i=0}^{p-1} M_i$, where $M_i = \{m \in M | \Phi(m) = \chi(i)m\}$, where $\chi : \mathbb{F}_p \to \mathbb{Z}_p$ is the Teichmuller character defined in section 2.2.*

We remark that this lemma is a purely algebraic result, similar to the one used in [TO70] to decompose the augmentation ideal of a group scheme of order p into a direct sum of $p-1$ modules. The only prerequisite is the presence of $p-1$ roots of unity. Note that the proof referenced in [Tzi17] is for the case of $\mathbb{F}_p$-algebras, and is based on Lemma 1, A.V. 104 in [Bou03]. The $\mathbb{Z}_p$ case is nearly identical to the $\mathbb{F}_p$ case: while in loc. cit., over $\mathbb{F}_p$ one has the identity $1 = \sum P_i(x)$, where $P_i(x) = \frac{X - X^p}{X - \chi(i)}$; over $\mathbb{Z}_p$ the sum is still a unit in $\mathbb{Z}_p[X]/(X^p - X)$, so the argument of loc. cit. goes through. Indeed, one has the identity $\left(1 + \frac{p}{1-p} X^{p-1}\right) \sum P_i(x) = 1$.

Returning to our problem, the action of μ_p on $S_i = \mathrm{Spec}(A_i)$ thus gives R-derivations D_i on A_i such that $D_i^p = D_i$. Using the above lemma, we decompose each R_i as a direct sum of p submodules $M_{i,j}$, $j = 0, \ldots, p-1$. We shall analyze these derivations and decompositions. Because we repeat this process for every A_i, we drop (temporarily) the subscript i and thus write A, D, M_j instead of A_i, D_i and $M_{i,j}$ respectively.

We check that each M_j is locally free of rank 1. Indeed, it suffices to prove that at every geometric point x, the vector space $(M_j)_x$ is 1-dimensional. But at geometric points all extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p are split and thus the schemes S_i are actually copies of $\mu_p = \operatorname{Spec} k[X]/(X^p - 1)$, where k is an algebraically closed field. In this case one checks that M_i is spanned by y^i, where y is, as usual, the generating Oort-Tate section in the Oort-Tate description of μ_p (see Proposition 6.3.1).

Thus M_1 is free of rank 1 and let f be a generating section of M_1. Then $D(f) = f$ by definition and an easy induction shows that $D(f^i) = if^i$. In fact because the image of f^i at geometric points is nonzero, it follows that $f^i \neq 0$. Moreover, because the decomposition of $\mathcal{O}_{S_i}$ as a sum of eigenspaces of D is *direct*, it follows that the f^is are linearly independent for $0 \leq i \leq p-1$ (compare also Lemma 2 on page 9 of [TO70]). Since however S_i is finite flat of rank p over $S = \operatorname{Spec}(R)$, the section f satisfies a monic polynomial of degree p (e.g. the characteristic polynomial), and this polynomial is killed by D. On the other hand, $D(f^i) = if^i$ for $0 \leq i \leq p-1$. It follows that the only possible polynomial relation must be of the form $f^p = \epsilon$, where ϵ is some constant in R.

Thus each S_i of the form $\operatorname{Spec} R[X]/(X^p - \epsilon_i)$. Note that we don't know yet ϵ_i are units in R. However, we have also not fully used the fact that G is a group scheme of order p^2 - we have only exploited the action of μ_p on the S_i's. We will now use the ''global'' group structure to conclude that each ϵ_i is a unit and in fact $\epsilon_i = \epsilon_1^i \cdot u_i^p$ where the u_i are some units (i.e. $\epsilon_i = \epsilon^i$ up to multiplication by pth power of units).

Denote by α_i the action map $\mu_p \times S_i \longrightarrow S_i$. The group structure on G induces further actions $\alpha_{ij} : S_i \times S_j \longrightarrow S_{i+j}$ if $i + j < p$ and actions $\alpha_{ij} : S_i \times S_j \longrightarrow S_{i+j-p}$ if $i + j \geq p$. All these actions commute with the $S_0 = G_0 = \mu_p$ action. In other words, we have, for $i + j < p$, a commutative diagram

$$\begin{array}{ccc} G_0 \times S_i \times S_j & \xrightarrow{\mathrm{id} \times \alpha_{ij}} & G_0 \times S_{i+j} \\ \downarrow{\scriptstyle \alpha_i \times \mathrm{id}} & & \downarrow \\ S_i \times S_j & \xrightarrow{\alpha_{ij}} & S_{i+j} \end{array}$$

Let's analyze the ring maps induced by the above diagram:

$$\begin{array}{ccc} R[y]/(y^p) \otimes R[X_i]/(X_i^p - \epsilon_i) \otimes R[X_j]/(X_j^p - \epsilon_j) & \xleftarrow{\mathrm{id} \times \alpha_{ij}} & R[y]/(y^p) \otimes R[X_{i+j}]/(X_{i+j}^p - \epsilon_{i+j}) \\ \uparrow{\scriptstyle \alpha_i^* \times \mathrm{id}} & & \uparrow{\scriptstyle \alpha_{i+j}^*} \\ R[X_i]/(X_i^p - \epsilon_i) \otimes R[X_j]/(X_j^p - \epsilon_j) & \xleftarrow[\alpha_{ij}]{} & R[X_{i+j}]/(X_{i+j}^p - \epsilon_{i+j}) \end{array}$$

Note that we can write the maps α_i^* explicitly. They are determined by derivations D_i on Spec $R[X_i]/(X_i^p - \epsilon_i)$ such that $D_i(X_i^k) = kX_i^k$. An easy induction shows that $D_i^m(X_i^k) = k^m X_i^k$. Thus the co-actions α_i^* satisfy:

$$\alpha_i^*(X_i^k) = \sum_{m=0}^{p-1} \frac{D_i^m(X_i^k)}{m!} \otimes y^m = \sum_{m=0}^{p-1} \frac{k^m X_i^k}{m!} \otimes y^m.$$

Fix some indices i and j. Assume $\alpha_{ij}(X_{i+j}) = \sum_{kl} c_{kl} X_i^k \otimes X_j^l$. Let's look at what happens to X_{i+j} in the above commutative diagram. Its image in the top-left ring is a sum of monomials $X_i^k \otimes X_j^l \otimes y^m$ with various coefficients. For each k, l, m, equating these coefficients from the two compositions yields

$$c_{kl} \cdot \frac{k^m}{m!} = \frac{c_{kl}}{m!}.$$

Since this is true for any k, l, m, we conclude that $c_{kl} = 0$ if $k \neq 1$. By symmetry $c_{kl} = 0$ if $l \neq 1$. Thus $\alpha_{ij}(X_{i+j}) = c_{11} X_i \otimes X_j$. Since $X_i^p = \epsilon_i$, this implies

$$\epsilon_{i+j} = c_{11}^p \epsilon_i \epsilon_j.$$

Recall that the indices were fixed and c_{11} depends on the pair (i, j). A straightforward induction then shows that $\epsilon_i = \epsilon_1^i \cdot u_i^p$, for some $u_i \in R$.

It remains to check that ϵ_i are units. By the above, we can assume that $\epsilon_i = \epsilon^i$ where $\epsilon = \epsilon_1$.

Note that for every $1 \leq i \leq p-1$ we also have maps $\beta_i : S_i \times S_{p-i} \to G_0 = \mu_p$. These commute with the actions of G_0 on the S_i's, making the following diagram commutative:

$$\begin{array}{ccc} G_0 \times S_i \times S_{p-i} & \xrightarrow{\mathrm{id} \times \beta_i} & G_0 \times G_0 \\ \downarrow{\scriptstyle \alpha_i \times \mathrm{id}} & & \downarrow{\scriptstyle m} \\ S_i \times S_{p-i} & \xrightarrow{\beta_i} & G_0 \end{array}$$

The induced maps on rings are

$$\begin{array}{ccc}
R[z]/(z^p-1)\otimes R[X_i]/(X_i^p-\epsilon^i)\otimes R[X_{p-i}]/(X_{p-i}^p-\epsilon^{p-i}) & \xleftarrow{\ \mathrm{id}\times\beta_i\ } & R[z]/(z^p-1)\otimes R[z]/(z^p-1) \\
\Big\uparrow{\scriptstyle \alpha_i^*\times\mathrm{id}} & & \Big\uparrow{\scriptstyle \Delta} \\
R[X_i]/(X_i^p-\epsilon^i)\otimes R[X_{p-i}]/(X_{p-i}^p-\epsilon^{p-i}) & \xleftarrow[\ \beta_i\ ]{} & R[z]/(z^p-1)
\end{array}$$

Note that we have switched, for computational convenience, to the presentation $R[z]/(z^p-1)$ of μ_p, rather than $R[y]/(y^p-w_py)$. The relations between y and z are given in proposition 2.2.1.

Assume $\beta_i(z)=\sum_{k,l} d_{kl}X_i^k\otimes X_{p-i}^l$.

Then the image of z in the top-left ring under the above-diagonal composition is

$$\sum_{k,l} d_{kl}z\otimes X_i^k\otimes X_{p-i}^l.$$

Recall that $\alpha_i^*(X_i^k)=\sum_{m\geq 0} y^m\otimes \dfrac{D^{(m)}(X_i^k)}{m!}=\sum_{m\geq 0}\dfrac{k^m}{m!}y^m\otimes X_i^k$.

Thus, the image of z under the below-diagonal composition is

$$\sum_{k,l} d_{kl}\alpha_i^*(X_i^k)\otimes X_{p-i}^l=\sum_{k,l,m}\left(d_{kl}\cdot\frac{k^m}{m!}\right)y^m\otimes X_i^k\otimes X_{p-i}^l.$$

Equating the coefficients of $X_i^k\otimes X_{p-i}^l$, we obtain

$$d_{kl}z=d_{kl}\sum_{m\geq 0}\frac{k^m}{m!}y^m.$$

On the other hand, from 2.2.1, $z=\sum_{m\geq 0}\dfrac{1}{m!}y^m$. Thus, if $k\neq 1$, we must have $d_{kl}=0$. By symmetry (i.e. letting G_0 act on S_{p-i} instead of S_i), we obtain that $d_{kl}=0$ if $l\neq 1$. Thus $\beta_i(z)=d_{11}X_i\otimes X_{p-i}$. Since $z^p=1$, we must have $d_{11}^p\epsilon^i\cdot\epsilon^{p-i}=1$, and thus ϵ is a unit, as wanted. □

6.4 Extensions of $\mathbb{Z}/p\mathbb{Z}$ by μ_p over any $\mathbb{Z}_p$-algebra

Most of the above results go through, with minor modifications which we explain here. We still have the commutative diagram:

$$\begin{array}{ccc}
O_X & \xrightarrow{\ \alpha^*\ } & O_X\otimes_R R[y]/(y^p) \\
\Big\downarrow{\scriptstyle \alpha^*} & & \Big\downarrow{\scriptstyle \alpha^*\otimes 1} \\
O_X\otimes_R R[y]/(y^p) & \xrightarrow{\ 1\otimes\Delta\ } & O_X\otimes_R R[y]/(y^p)\otimes_R R[y]/(y^p)
\end{array}$$

Write

$$\alpha^*(a) = a \otimes 1 + \Phi_1(a) \otimes y + \sum_{j=2}^{p-1} \Phi_j(a) \otimes y^j.$$

We show that

$$\Phi_i(a) = \frac{\Phi_1^{(i)}(a)(1-p)^{i-1}}{w_i}.$$

When $p = 0$, we recover the formula $\Phi_i(a) = \dfrac{\Phi_1^i(a)}{i!}$. The proof is nearly identical to the characteristic p case - one looks at the coefficient of $y \otimes y^{i-1}$. One picks up an extra $(1-p)$ because it is present in the comultiplication rule for y (see 2.2.1). By looking at the coefficient of $y \otimes y^{p-1}$, we deduce that

$$\Big(D(1-p)\Big)^p = D(1-p).$$

Thus in the presence of $p-1$ roots of unity, we still have a nice decomposition of O_X into eigenspaces of $D(1-p)$, with eigenvalues $0, \chi(1) = 1, \chi(2), \ldots, \chi(p-1)$. In our case $X = S_1$ is of rank p and looking at geometric points just as in the characteristic p case, since every extension of $\mathbb{Z}/p\mathbb{Z}$ by μ_p splits, one sees that these are all of rank 1.

A difference from the case when $p = 0$ is that $\alpha^*(ab) = \alpha^*(a)\alpha^*(b)$ no longer implies that $D = \Phi_1$ is a derivation. However we see below that it still has strong properties. The relation $\alpha^*(ab) = \alpha^*(a)\alpha^*(b)$ together with $y^p = w_p y$ then implies

$$\begin{aligned} D(ab) &= aD(b) + bD(a) + w_p \sum_{j=1}^{p-1} \Phi_j(a)\Phi_{p-j}(a) \\ &= aD(b) + bD(a) + w_p \sum_{j=1}^{p-1} \frac{(1-p)^{p-2} D^{(j)}(a) D^{(p-j)}(a)}{w_j w_{p-j}}. \end{aligned}$$

Let f generate the invertible module corresponding to eigenvalue 1, so $(1-p)D(f) = f$. Using the above relation, we show that $(1-p)D(f) = f$ implies $(1-p)D(f^2) = \chi(2)f$ and more generally $(1-p)D(f^i) = \chi(i)f^i$.

Indeed, $(1-p)D(f) = f$ implies $(1-p)^i D^{(i)}(f) = f$, thus $D^{(j)}(f)D^{(p-j)}(f) = \dfrac{1}{(1-p)^p} f^2$. Thus, plugging $a = b = f$ in the above relation yields:

$$D(f^2) = f^2 \left(\frac{2}{1-p} + \frac{w_p}{(1-p)^2} \sum_{j=1}^{p-1} \frac{1}{w_j w_{p-j}} \right)$$

This implies that $(1-p)D(f^2) = c_2 f^2$ for some constant c_2. Since $(1-p)D$ is fully diagonalizable with a full set of distinct eigenvalues $0, \chi(1), \ldots, \chi(p-1)$, it follows that c_2 is one of those. Since $w_p = p \cdot \text{unit}$, we have $c_2 \equiv 2 \pmod{p}$, thus c_2 must be $\chi(2)$. In fact, an easy induction then shows that there are constants c_i, congruent to i mod p, such that $D(f^i) = c_i f^i$ and then a similar argument shows that $c_i = \chi(i)$.

Alternatively, to show directly $D(f^2) = \dfrac{\chi(2)}{1-p} f^2$, it suffices to verify the identity:

$$\chi(2) = 2 + \frac{w_p}{1-p} \sum_{j=1}^{p-1} \frac{1}{w_j w_{p-j}}.$$

A series of similar identities can be derived for each $\chi(i)$, $2 \le i \le p-1$.

Computing then $D(f^p)$ (for example from $\alpha^*(f^p) = \alpha^*(f)\alpha^*(f^{p-1})$), one finds that it vanishes (even if we are not in characteristic p and D is not a derivation!). Thus, any polynomial relation involving f must be of the form $f^p = \epsilon$ as before.

Thus, $S_i = \operatorname{Spec}(R[X_i]/(X_i^p - \epsilon_i))$. The rest of the argument in the characteristic p case goes through unchanged, and we deduce that $\epsilon_i = \epsilon_1^i \cdot u_i^p$ for some unit u_i. Moreover, the global group structure implies, by a nearly identical argument, that ϵ_1 is a unit. The only changes are the appearance of $(1-p)$ factors in the formulas, the replacement of $m!$ by w_m throughout the formulas and $D^{(m)}(X_i^k) = k^m X_i^k$ is replaced by $\dfrac{\chi(k)^m}{(1-p)^m} X_i^k$.

Thus G is isomorphic to a group scheme of the form G_ϵ, as we wanted to show.

Chapter 7

LEVEL STRUCTURES ON DIEUDONNÉ MODULES

In this chapter, we present an auxiliary result about interpreting Drinfeld-Katz-Mazur level structures using (contravariant) Dieudonné theory. Gabber (unpublished) and Eike Lau [Lau10] have shown the Dieudonné equivalence over perfect bases. We briefly recalled this equivalence in Section 2.4. Thus, the notion of Drinfeld-Katz-Mazur level structure should have a (semi-)linear algebraic analogue. We restrict our attention to a perfect base schemes S, locally given by $S = \operatorname{Spec} R$, where R is a perfect ring (over $\mathbb{F}_p$). The goal of this chapter is to give an interpretation of the notion of Drinfeld-Katz-Mazur level structure in the Dieudonnś setting.

We will use some results of [HT01] but to simplify the exposition, we will work with (usual) p-divisible groups instead of Barsotti-Tate $\mathcal{O}_K$-modules as is done in [HT01] (so $K = \mathbb{Q}_p$ and $\mathcal{O}_K = \mathbb{Z}_p$). Let thus S be a base scheme over $\mathbb{Z}_p$ and H/S a p-divisible group of height h endowed with an embedding $\mathbb{Z}_p \hookrightarrow \operatorname{End}(H)$. We do not assume H is 1-dimensional.

Recall that a Drinfeld-Katz-Mazur p^m-level structure on H/S is then a morphism of $\mathbb{Z}_p$-modules:

$$\alpha : (\mathbb{Z}/p^m\mathbb{Z})^{\oplus h} \simeq (p^{-m}\mathbb{Z}_p/\mathbb{Z}_p)^{\oplus h} \to H[p^m](S)$$

so that the set of $\alpha(x)$ for $x \in (\mathbb{Z}/p^m\mathbb{Z})^h$ forms a full set of sections of $H[p^m]$.

Note that, from the definition of endomorphisms of p-divisible groups, $\mathbb{Z}_p$ acts on each ''level'' $H[p^m]$, i.e. $H[p^m](T)$ is a $\mathbb{Z}_p$-module for any scheme T over S.

By embedding $\mathbb{Z}_p$ into $\operatorname{End}(H)$, we embed $\mathbb{Z}_p$ into $\operatorname{End}(M_H)$, hence the Dieudonné module M_H of H becomes itself a $\mathbb{Z}_p$-module. Then an abstract group homomorphism $(\mathbb{Z}/p^m\mathbb{Z})^h \to H[p^m](S)$ is a homomorphism of $\mathbb{Z}_p$-modules if and only if the induced homomorphism of Dieudonné modules $M_H = W_m(R)^h \to M_{const} = W_m(R)^h$ is a $\mathbb{Z}_p$-module homomorphism.

7.1 A commutative diagram

Let H be a p-divisible group as above, $m \geq 1$ an integer and $G := H[p^m]$.

Consider a group homomorphism $f : (p^{-m}\mathbb{Z}/\mathbb{Z})^{\oplus h} \to G$. This must commute with the action of Frobenius (and Verschiebung), so we have the following diagram:

$$\begin{array}{ccc} (p^{-m}\mathbb{Z}/\mathbb{Z})^{\oplus h} & \longrightarrow & G \\ \simeq \big\downarrow \text{Frob} & & \big\downarrow \text{Frob} \\ (p^{-m}\mathbb{Z}/\mathbb{Z})^{\oplus h\ (p)} & \longrightarrow & G^{(p)} \end{array} \tag{7.1}$$

Locally on S, the Dieudonné module of H is free of rank h over $W(R)$ (and thus the Dieudonné module of G is free of rank h over $W_m(R)$). Choose a basis. The corresponding diagram of contravariant Dieudonné modules is

$$\begin{array}{ccc} W_m(R)^{\oplus h} & \longleftarrow & W_m(R)^{\oplus h} \\ \text{Frob} \big\uparrow \simeq & & B \big\uparrow \text{Frob} \\ W_m(R)^{\oplus h} & \xleftarrow{A} & W_m(R)^{\oplus h} \end{array} \tag{7.2}$$

Note that the left side of the diagram are the Dieudonné modules of the constant group and the ones on the right those of G.

The diagram can be interpreted and used in two (equivalent) ways: we either view the bottom two Dieudonné modules as identical to the ones above, and the vertical maps are *semi-linear* maps; or the vertical maps are *linear* and the modules on the bottom row are Frobenius twists of the ones above. We will mainly work in the linear setting.

Here A and B are $h \times h$ matrix with entries in $W_m(R)$. The condition for the map to ‘‘commute’’ with the Frobenius is

$$\operatorname{Frob} A = AB,$$

where $\operatorname{Frob} A$ is obtained by raising *each* entry of A to the pth power. To see this one can take a basis $e_1, \ldots, e_h$ of the Dieudonné module corresponding to G (which is free over $W_m(R)$) and look at the action of each map.

Let's make this a bit more explicit as follows: write M_G for the Dieudonné module of G and M_{const} for that of $(p^{-m}\mathbb{Z}/\mathbb{Z})^h_S$. Then, in the *semi-linear* point of view, we have:

$$\begin{array}{ccc} M_{const} & \xleftarrow{A} & M_G \\ \text{Frob} \big\uparrow \simeq & & B \big\uparrow \text{Frob} \\ M_{const} & \xleftarrow{A} & M_G \end{array}$$

In the *linear* viewpoint, we have

$$\begin{array}{ccc} M_{const} & \xleftarrow{\quad A \quad} & M_G \\ {\scriptstyle \mathrm{Frob}}\uparrow{\scriptstyle \simeq \mathrm{id}} & & {\scriptstyle B}\uparrow{\scriptstyle \mathrm{Frob}} \\ M_{const} \otimes_{W(R),\sigma} W(R) & \xleftarrow{\ A\otimes 1\ } & M_G \otimes_{W(R),\sigma} W(R) \end{array}$$

Note that in the *linear* case, the matrix of $A \otimes 1$ is obtained by applying the Frobenius automorphism of $W(R)$ to each entry of A (note that the entries are of the matrices are elements of $W_m(R)$). So we do indeed get, as matrices

$$\mathrm{Frob}\, A = AB,$$

as maps from $M_G^{(p)} \to M_{const}$. Note that id corresponds to the identity matrix but not the identity homomorphism, as the modules are different.

7.2 Level structures

A Drinfeld-Katz-Mazur level structure is, in particular, a group homomorphism, so the commutativity conditions in Section 7.1 hold (in the category of Dieudonné modules). The goal is to further translate what does it mean to be a ‘‘full set of sections’’ into a condition involving A and B.

Let $B^{(i)}$ denote the linear homomorphism corresponding to the Frobenius $F : G^{(p^{i-1})} \to G^{(p^i)}$, i.e. $B^{(i)}$ is a linear map $M_G \otimes_{W(R),\sigma^i} W(R) \to M_G \otimes_{W(R),\sigma^{i-1}} W(R)$. Note that $B = B^{(1)}$. Denote by $\mathcal{N}_i(B)$ the composition $B^{(i)} \circ B^{(i-1)} \circ \ldots \circ B^{(1)}$. This is a linear map $M_G \otimes_{W(R),\sigma^i} W(R) \to M_G$.

Let $s = mh$ be a large enough integer. Consider the diagram of *linear* maps.

$$\begin{array}{ccc} W_m(R)^{\oplus h} & \xleftarrow{\quad A \quad} & W_m(R)^{\oplus h} \\ {\scriptstyle \mathrm{id}}\uparrow{\scriptstyle \simeq} & & \uparrow{\scriptstyle \mathcal{N}_s(B)} \\ W_m(R)^{\oplus h} \otimes_{W(R),\sigma^s} W(R) & \xleftarrow{\mathrm{Frob}^s A} & W_m(R)^{\oplus h} \otimes_{W(R),\sigma^s} W(R) \end{array}$$

Since the vertical arrow on the left is an isomorphism, it follows that we *always* have $i : \ker \mathcal{N}_s(B) \hookrightarrow \ker(\mathrm{Frob}^s A)$ for any group homomorphism $(\mathbb{Z}/p\mathbb{Z})^h \to G$, not from a level structure.

We will prove the following result:

Theorem 7.2.1. *Let R be a perfect ring and H be a p-divisible group of height h over $S = \mathrm{Spec}\, R$. Consider a group homomorphism $\alpha : (p^{-m}\mathbb{Z}/\mathbb{Z})^h \to H[p^m]$. Let A be the corresponding homomorphism of associated Dieudonné modules. Then α is a level structure on H if and only if the inclusion i is an isomorphism, i.e. if and only if* $\ker \mathcal{N}_s(B) = \ker(\mathrm{Frob}^s A)$.

7.3 The case $S = \mathrm{Spec}(k)$, where k is a perfect field

Both to motivate our guess and as an aid for the general proof, let's prove the main theorem 7.2.1 when R is a perfect field k. We shall need parts 4 and 5 of a lemma from Harris-Taylor [HT01]:

Lemma 7.3.1 (II.2.1)**.** *Let S be an $\mathbb{Z}_p$-scheme and H/S a Barsotti-Tate $\mathbb{Z}_p$-module of constant height h.*

4. *Suppose that S is connected and that over S there is an exact sequence of p-divisible groups*
$$0 \to H^0 \to H \to H^{ét} \to 0$$
with H^0 formal and $H^{ét}$ ind-étale. Then
$$\alpha : (\mathbb{Z}/p^m\mathbb{Z})^h \to H[p^m](S)$$
is a Drinfeld p^m-level structure if and only if there is a direct summand of $M \subset (\mathbb{Z}/p^m\mathbb{Z})^h$ such that:
    1. *$\alpha|_M : M \to H^0[p^m](S)$ is a Drinfeld p^m-structure.*
    2. *α induces an isomorphism*
    $$\alpha : ((\mathbb{Z}/p^m\mathbb{Z})^h/M)_S \xrightarrow{\simeq} H^{ét}[p^m].$$
5. *Suppose that S is reduced, connected and that $p = 0$ on S. Suppose also that there is an exact sequence of p-divisible groups*
$$(0) \to H^0 \to H \to H^{ét} \to (0),$$
over S with H^0 formal and $H^{ét}$ ind-etale. If H/S admits a Drinfeld p^m-level structure (with $m \geq 1$) then there is a unique splitting
$$H[p^m] \simeq H^0[p^m] \times H^{ét}[p^m]$$
over S. On the other hand if there is a splitting $H[p^m] \simeq H^0[p^m] \times H^{ét}[p^m]/S$ then to give a Drinfeld p^m-structure $\alpha : (\mathbb{Z}/p^m\mathbb{Z})^h \to H[p^m](S)$ is the same as giving a direct summand $M \subset (\mathbb{Z}/p^m\mathbb{Z})^h$ and an isomorphism
$$\left((\mathbb{Z}/p^m\mathbb{Z})^h/M\right)_S \xrightarrow{\simeq} H^{ét}[p^m].$$

Our goal is thus to establish:

Theorem 7.3.1 (Field case)**.** *Let k be a perfect field and H be a p-divisible group of height h over $S = \operatorname{Spec} k$. Consider a group homomorphism $\alpha : (\mathbb{Z}/p^m\mathbb{Z})^h \to H[p^m]$. Let A be the corresponding homomorphism of associated Dieudonné modules. Then α is a level structure on H if and only if $i : \ker \mathcal{N}_s(B) \hookrightarrow \ker(\operatorname{Frob}^s A)$ is an isomorphism, i.e. if and only if* $\ker \mathcal{N}_s(B) = \ker(\operatorname{Frob}^s A)$ *(see discussion before this subsection).*

Proof. Over a perfect field k, H (and $H[p^m]$) has a connected-étale sequence that splits (Demazure [Dem72], page 34). Note that such an exact sequence exists over any field k, but only splits over a perfect field k. Write $G := H[p^m]$ and consider

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

Note that G^0 and G^{et} are truncated BT groups. The Dieudonné module M_G of G can be written as a direct sum $M_{\text{ét}} \oplus M_{loc}$ (see Fontaine [Fon77]). In fact, $M_{\text{ét}} = \cap_{n\geq 1} F^n M$ and $M_{loc} = \cup_{n\geq 1} \ker F^n$. Since the Frobenius commutes with the $\mathbb{Z}_p$-action, it is easy to see that $M_{\text{ét}}$ and M_{loc} are $\mathbb{Z}_p$-modules. Recall from [Dem72] that a high enough power of the Frobenius kills M_{loc} (in the semi-linear setting; if we work in the linear setting, this statement says that $\mathcal{N}_i(B)$ kills $M_{loc} \otimes_{W(R),\sigma^i} W(R)$ for large enough i). Moreover, the Frobenius is an isomorphism on $M_{\text{ét}}$. In fact, the high enough exponent that suffices is $i = mh =: s$ works. Thus $\ker \mathcal{N}_s(B) = \left(M_G \otimes_{W(R),\sigma^s} W(R)\right)_{loc}$.

Assume first that $\ker \mathcal{N}_s(B) = \ker(\operatorname{Frob}^s A) = \left(M_G \otimes_{W(R),\sigma^s} W(R)\right)_{loc}$. We want to show that α is a level structure. Note that A is injective on the étale part. Consider the image P of $M_{\text{ét}}$, under A, sitting inside $M_{const} = W_m(R)^h$. Note that P is stable under Frobenius, hence P is *a* Dieudonné submodule of M_{const}. Moreover P is a $\mathbb{Z}_p$-module (because $M_{\text{ét}}$ is). The inclusion $P \hookrightarrow M_{const}$ corresponds thus a quotient map $(\mathbb{Z}/p^m\mathbb{Z})^h_S \to ((\mathbb{Z}/p^m\mathbb{Z})^h/N)_S$ for a subgroup N of $(\mathbb{Z}/p^m\mathbb{Z})^h$.

The restriction of A to $M_{\text{ét}}$ gives an isomorphism between $M_{\text{ét}}$ and P, hence it corresponds to an isomorphism $((\mathbb{Z}/p^m\mathbb{Z})^h/N)_S \simeq G^{\text{ét}}$. This shows that $((\mathbb{Z}/p^m\mathbb{Z})^h/N)_S$ is not killed by p^{m-1} (because $G^{\text{ét}}$ is not). Together with the quotient being constant, we get that N cannot be an arbitrary subgroup of $(\mathbb{Z}/p^m\mathbb{Z})^h$ (i.e. there are restrictions), in fact it has to be a direct summand (and also a $\mathbb{Z}_p$-module as noticed above).

Thus we can use Lemma 7.3.1 (II.2.1 part (5) of Harris-Taylor [HT01]) to conclude that α is a level structure (keep in mind the clash of notation between the theorem and the lemma).

Assume now that α is a level structure. Invoking again lemma 7.3.1 (II.2.1 part 4 in [HT01]) we see that there is a summand N of $(\mathfrak{p}^{-m}/O_K)^{\oplus h}$ so that α induces an isomorphism $\alpha|N : ((\mathfrak{p}^{-m}/O_K)^h/N)_S \to G = H^{\text{ét}}[\mathfrak{p}^m]$ and $\alpha|N : N \to H^0[\mathfrak{p}_K^m](S)$ is a level structure. But since $S = \operatorname{Spec} R$ is reduced, part 3 of the same lemma implies that the latter condition simply means that $\alpha|N$ is the zero homomorphism $N \to H(S)$.

Thus, the matrix A is an isomorphism from $M_{\text{ét}}$ to a Dieudonné O_K-submodule of $M_{const} = W_m(R)^{\oplus h}$ and vanishes on M_{loc} which gives us $\ker(\mathrm{Frob}^s A) = \ker \mathcal{N}_s(B)$ (both equal to M_{loc}), as wanted. □

7.4 Integral domain base

Let now R be an perfect integral domain of characteristic p. Denote $K := \mathrm{Frac}(R)$ and η the generic point of $S = \operatorname{Spec} R$. The ring R injects into K. Moreover $W(R)$ is an integral domain which injects into $W(K)$ ([Shi14], Lemma 3.7).

Lemma 7.4.1. *K is flat over R and $W(K)$ is flat over $W(R)$.*

Proof of lemma: The first part is basic commutative algebra. The second part is more subtle. From [Shi14], Proposition 5.2 it follows that $W(K)$ is flat over $W(R)$. Indeed, Proposition 5.2 in loc. cit. says that

$$W(K) \simeq \left(W(B)_{(p)}\right)^{\wedge}$$

The proof of this proposition shows that $W(B)_{(p)}$ is Noetherian. Thus, $W(K)$ is obtained via a localization and a completion of a Noetherian ring, and both these operations are flat. ■

Lemma 7.4.2. *If $R \to S$ is a flat ring homomorphism of perfect $\mathbb{F}_p$-rings, then $W_m(R) \to W_m(S)$ is flat for any $m \geq 1$.*

Proof of lemma: We apply Theorem 1 in Bourbaki, Alg. com., III, §5 [Bou85]. We reproduce below the part we need. We have to verify that we are justified in applying the result.

Using the notation of the Bourbaki lemma, we have $A = W_m(R)$, $M = W_m(S)$ and $\mathfrak{J} = (p)$. Since the rings are perfect $\mathfrak{J}$ is indeed nilpotent. $M/\mathfrak{J}M = W_m(S)/pW_m(S) \simeq S$ and $A/\mathfrak{J} = W_m(R)/pW_m(R) \simeq R$. By assumption $R \to S$ is flat, thus $M/\mathfrak{J}M$ is flat over $A/\mathfrak{J}$.

Finally $\mathrm{gr}_i(A) = p^i W_m(R)/p^{i+1}W_m(R) \simeq R$, since R is perfect. Similarly, $\mathrm{gr}_i(M) = p^i W_m(S)/p^{i+1}W_m(S) \simeq S$. Thus, the requirement $\mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \longrightarrow \mathrm{gr}(M)$ being bijective is indeed met, as it simply says that $R \otimes_R S \longrightarrow S$ is bijective. ■

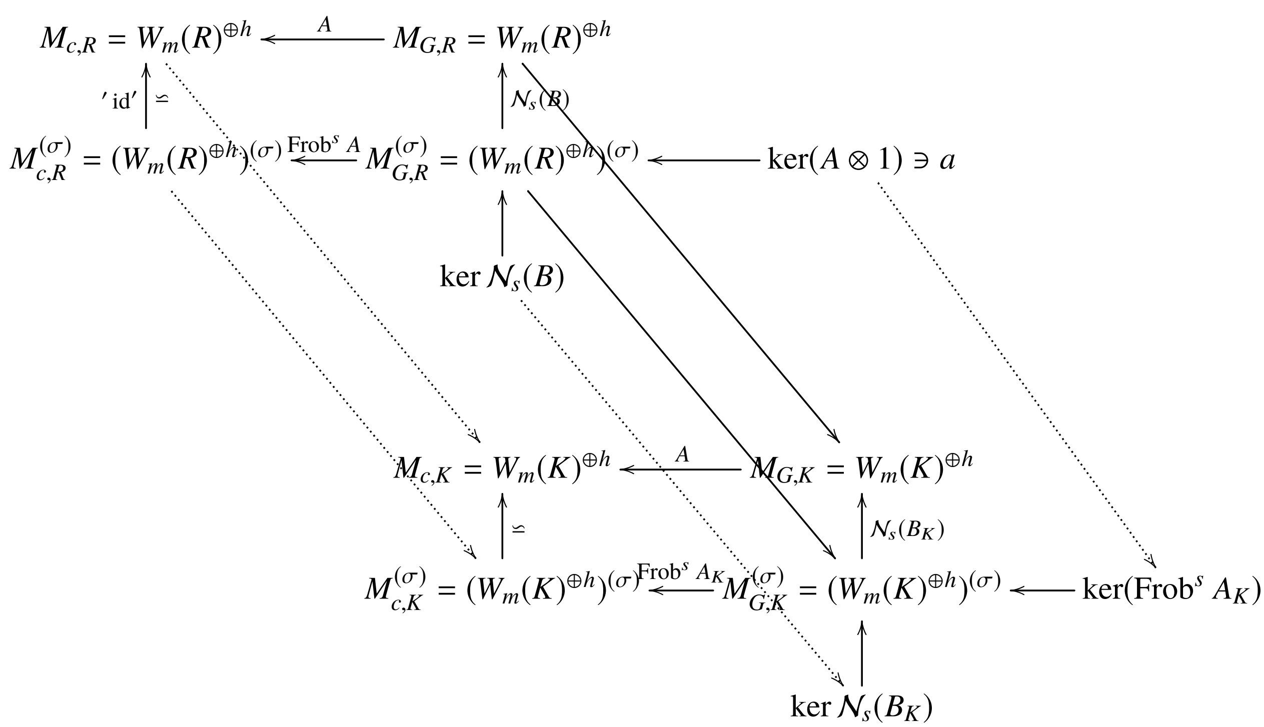
Lemma 7.4.3 (Bourbaki ACIII§5, Th.1)**.** *Let A be a commutative ring, $\mathfrak{I}$ an ideal of A, and M an A-module. Consider the following properties:*

(i) M is a flat A-module.

(iv) $M/\mathfrak{I}M$ is a flat $A/\mathfrak{I}$-module, and the canonical homomorphism $\mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \longrightarrow \mathrm{gr}(M)$ *is bijective.*

Then (i) implies (iv). If moreover $\mathfrak{I}$ is nilpotent, then (i) and (iv) are equivalent.

Taking truncations we have $W_m(R) \hookrightarrow W_m(K)$ (since at the level of sets, this is just $R^m \hookrightarrow K^m$). Consider the diagram (the subscript c stands for constant):



The bottom-right part of the diagram is obtained by base-changing to the generic point, i.e. using the morphism $\mathrm{Spec}\, K \longrightarrow \mathrm{Spec}\, R$. The vertical maps are *linear*. All parallelograms in the diagram are commutative (by functoriality of the Frobenius, Dieudonné module and base change).

Assume first that α is a level structure. We want to show that $\ker\left(\mathrm{Frob}^s(A)\right) = \ker \mathcal{N}_s(B)$.

Let $a \in \ker \mathrm{Frob}^s A$. Then the image $\widetilde{a}$ of a in $W_m(K)^{\oplus h(\sigma)}$ is in the kernel of $\mathrm{Frob}^s A_K$. Since α_K is a level structure for the truncated p-divisible group G_K over $\operatorname{Spec} K$, from the main theorem in the case where the base is a field, proved above, we have $\ker(\mathrm{Frob}^s A_K) = \ker \mathcal{N}_s(B_K)$. So $\tilde{a} \in \ker \mathcal{N}_s(B_K)$. But the map $W_m(R)^{\oplus h} \to W_m(K)^{\oplus h}$ is injective because it is simply induced by the inclusion $R \hookrightarrow K$ (so on the level of sets is just $R^m \hookrightarrow K^m$). Thus $a \in \ker \mathcal{N}_s(B)$, and thus $\ker \mathrm{Frob}^s A = \ker \mathcal{N}_s(B)$.

Assume now that $\ker \mathrm{Frob}^s A = \ker \mathcal{N}_s(B)$. We want to prove that α is a level structure.

We shall need the following simple result from commutative algebra:

Lemma 7.4.4. *Given a module homomorphism $f : M \to N$ of R-modules and a flat R-algebra S, then* $(\ker f) \otimes_R S = \ker(f \otimes 1_S)$.

Proof of lemma: Let M' be the kernel of f, N' the image and P the cokernel. We then have a diagram

$$\begin{array}{ccc} 0 \longrightarrow M' \longrightarrow M & \longrightarrow & N \longrightarrow P \longrightarrow 0 \\ & \searrow \quad \nearrow & \\ & 0 \longrightarrow N' \longrightarrow 0 & \end{array}$$

The top row is exact, and the two arising short exact sequences are exact. Tensoring with S, the short exact sequences stay exact. If a tensor w in $M \otimes_R S$ goes to 0 in $N \otimes_R S$ under $f \otimes 1_S$, then from the injectivity of $N' \otimes_R S \to N \otimes_R S$ it follows that it goes to zero in $N' \otimes_R S$. Thus, $\ker(f \otimes 1) = \ker(M \otimes_R S \to N' \otimes_R S) = M' \otimes S = (\ker f) \otimes_R S$, as wanted. ■

Since $W(K)$ is flat over $W(R)$ (and $W_m(K)$ flat over $W_m(R)$), it follows the maps induced by base change: $\mathcal{N}_s(B_K)$ and $\mathrm{Frob}^s A_K$ have kernels equal to $\ker(\mathcal{N}_s(B)) \otimes_{W(R)} W(K)$ and $\ker \mathrm{Frob}^s A \otimes_{W(R)} W(K)$ respectively. By assumption, $\ker \mathrm{Frob}^s A = \ker \mathcal{N}_s(B)$, hence $\ker \mathcal{N}_s(B_K) = \ker \mathrm{Frob}^s A_K$. But our main theorem over a perfect field precisely says that this equality is equivalent to the group homomorphism $\alpha_K : (p^{-m}\mathbb{Z}/\mathbb{Z})^h_K \to G_K$ induced by α begin a level structure.

Thus the condition $\ker \mathrm{Frob}^s A = \ker \mathcal{N}_s(B)$ implies that α_K is a level structure on G_K. It will suffice then to prove the following statement:

Proposition 7.4.1. *Let $\alpha : (\mathbb{Z}/p^m\mathbb{Z})^h_S \to G$ be a homomorphism of group schemes over $S =$ Spec R, with R a perfect integral domain. Let K be the fraction field of*

R and α_K the homomorphism obtained by base-change to Spec K*. If α_K is a level structure on G_K, then α is a level structure on G.*

In other words, the above proposition says that being a level structure is a closed condition. In fact, we can replace $(\mathbb{Z}/p^m\mathbb{Z})^h$ by an *arbitrary* (abstract) finite abelian group $\mathcal{H}$ and view $\alpha : \mathcal{H}_S \to G$ as a set of $|\mathcal{H}|$ sections. Moreover, G need not be a truncated p-divisible group. We keep, however, the essential assumption that R is a (perfect) *integral domain*.

Proof. Let $G = \operatorname{Spec} B$ for a locally free R-algebra B. We can assume that B is free over R, of rank N. Choose a basis $b_1, \ldots, b_N$. Then $b_1 \otimes 1, \ldots, b_N \otimes 1$ form a basis for $B \otimes_R K$ over K.

Let $\varphi_1, \ldots, \varphi_N : S \to G$ be a set of sections, corresponding to ring homomorphisms $f_1, \ldots, f_N : B \to R$. By assumption, $(\varphi_i)_K$ form a full set of sections for G_K over K. This is equivalent to the fact (see [KM85], page 38), that the ‘‘universal’’ element $Z_0 = \sum T_i(b_i \otimes 1) \in (B \otimes_R K) \otimes_K K[T_1, \ldots, T_N]$ satisfies

$$\operatorname{Norm}(Z_0) = \prod (f_i)_K(Z_0) \tag{7.3}$$

as an equality in $(B \otimes_R K)[T_1, \ldots, T_N]$.

Now $\varphi_1, \ldots, \varphi_N$ form a full set of sections for G over R if and only if the ‘‘universal’’ element $Z = \sum T_i b_i \in B \otimes_R R[T_1, \ldots, T_N]$ satisfies

$$\operatorname{Norm}(Z) = \prod f_i(Z). \tag{7.4}$$

So the proposition comes down to checking the equivalence of (7.3) and (7.4).

The proposition then follows because $Z_0 = Z \otimes 1$, so the linear map that is multiplication by Z_0 has the ‘‘same’’ matrix (with respect to basis $\{b_i \otimes 1\}$) as multiplication by Z does with respect to basis $\{b_i\}$, so has the same norm / characteristic polynomial. □

7.5 From integral domain to general case

We proceed as follows: Let $\mathfrak{q}$ be a minimal prime of R. A basic but key point (from commutative algebra) is that $\operatorname{Frac}(R/\mathfrak{q}) = R_{\mathfrak{q}}$. This helps because localization is exact, hence the composition map $R \to R/\mathfrak{q} \to \operatorname{Frac}(R/\mathfrak{q})$ is flat (even if $R \to R/\mathfrak{q}$ isn't!). Thus $W_m(R) \to W_m(\operatorname{Frac}(R/\mathfrak{q}))$ is flat (by Lemma 7.4.2).

Assume α is a level structure. We want to show $\ker(\mathrm{Frob}^s A) = \ker \mathcal{N}_s(B)$. As usual, we have $\ker(\mathrm{Frob}^s A) \supset \ker \mathcal{N}_s(B)$. Let $a \in \ker(\mathrm{Frob}^s A)$ and assume $a \notin \ker \mathcal{N}_s(B)$. Recall that the (twisted or not) Dieudonné module of G is free over $W_m(R)$ of rank h. Consider the *image* of a under $\mathcal{N}_s(B)$ (by assumption it is nonzero) and write it as $\sum_{i=1}^{h} a_i e_i$, with $a_i \in W_m(R)$. Since R is reduced, there is a minimal prime $\mathfrak{q}$ so that *not all* a_i's are in the ideal $W_m(\mathfrak{q})$ of $W_m(R)$. This means that under the map $W_m(R)^h \longrightarrow W_m(R/\mathfrak{q})^h \hookrightarrow W_m(F)^h$, the image of $\mathcal{N}_s(B)(a)$ is *not* zero. But via flatness, we know that kernels are preserved when passing from R to F. This means that $\ker \mathrm{Frob}^s A_F \neq \ker \mathcal{N}_s(B_F)$, which is a contradiction because α_F is a level structure on the generic point.

Assume now $\ker \mathrm{Frob}^s A = \ker \mathcal{N}_s(B)$. Let $\mathfrak{q}$ be a minimal prime and $F = \mathrm{Frac}(R/\mathfrak{q})$. Passing to the generic point of the irreducible component corresponding to $\mathfrak{q}$, and using the flatness of $W_m(R) \longrightarrow W_m(F)$ we have $\ker(\mathrm{Frob}^s A_F) = \ker(\mathcal{N}_s(B_F))$. Thus, from the field case, α_F is a level structure on G_F. By the argument in the integral domain case, α is a level structure on the whole irreducible component corresponding to $\mathfrak{q}$. In particular, α induces a level structure at every geometric point of every irreducible component, i.e. at every geometric point of $S = \mathrm{Spec}\, R$. From corollary 1.9.2 of Katz-Mazur, this implies that α is a level structure.

BIBLIOGRAPHY

[Bou03] N. Bourbaki. *Algebra II, Chapter 4-7*. Springer, 2003.

[Bou85] N. Bourbaki. *Éléments de Mathématique: Algebre Commutative*. Springer, 1985.

[Buz12] Kevin Buzzard. *Group schemes of order p^2*. 2012. URL: http://wwwf.imperial.ac.uk/~buzzard/maths/research/notes/group_schemes_of_order_p_squared.pdf.

[CN90] Ching-Li Chai and Peter Norman. ''Bad Reduction of the Siegel Moduli Scheme of Genus Two with $\Gamma(p)$-Level Structure.'' In: *American Journal of Mathematics* 112.6 (1990), pp. 1003–1071. ISSN: 00029327, 10806377. URL: http://www.jstor.org/stable/2374734.

[Dem72] M. Demazure. *Lectures on p-divisible groups*. 1972.

[DG70] M. Demazure and P. Gabriel. *Groupes Algébriques Tome I*. Masson, 1970.

[Dri74] V.G. Drinfeld. ''Elliptic Modules.'' In: *Mat. Sb. (N.S.)* (1974).

[Fon77] J-M Fontaine. *Groupes p-divisibles sur les corps locaux*. 1977.

[Goe01] Ulrich Goertz. ''On the flatness of models of certain Shimura varieties of PEL-type.'' In: *Mathematische Annalen* 321 (Nov. 2001), pp. 689–727. DOI: 10.1007/s002080100250.

[HR12] Thomas Haines and Michael Rapoport. ''Shimura varieties with $\Gamma_1(p)$-level via Hecke algebra isomorphisms: the Drinfeld case.'' In: *Annales Scientifiques de l'École Normale Supérieure* 45 (Sept. 2012), pp. 719–785. DOI: 10.24033/asens.2177.

[HT01] M. Harris and R. Taylor. *The Geometry and Cohomology of Some Simple Shimura Varieties*. Annals of Mathematics Studies, Princeton University Press, 2001.

[KM85] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Annals of Mathematics Studies, Princeton University Press, 1985.

[Lau10] E. Lau. *Smoothness of the truncated display functor*. 2010. URL: https://arxiv.org/pdf/1006.2723.pdf.

[Mes72] W. Messing. *The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes*. Vol. 264. Lecture Notes in Mathematics, 1972.

[RZ96] M. Rapoport and Th. Zink. *Period Spaces for "p"-divisible Groups (AM-141)*. Princeton University Press, 1996. ISBN: 9780691027814. URL: http://www.jstor.org/stable/j.ctt1b7x72g.

[Sha15] R. Shadrach. *Integral models of certain PEL-Shimura varieties with $\Gamma_1(p)$-type level structure*. 2015. URL: https://arxiv.org/abs/1309.3485.

[Shi14] K. Shimomoto. *On The Witt Vectors Of Perfect Rings In Positive Characteristic*. 2014. URL: https://arxiv.org/abs/1404.5147.

[TO70] J Tate and Frans Oort. ''Group scheme of Prime Order.'' In: *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série* 3 (Jan. 1970).

[Tzi17] N. Tziolas. ''Quotients of schemes by α_p or μ_p actions in characteristic $p > 0$.'' In: *Manuscripta Mathematica* (2017). URL: https://arxiv.org/pdf/1412.7941.pdf.

[Wed00] Torsten Wedhorn. ''The local Langlands correspondence for GL(n) over p-adic fields.'' In: (Dec. 2000). URL: http://users.ictp.it/~pub_off/lectures/lns021/Wedhorn/Wedhorn.pdf.