Deformations of p-divisible groups and p-descent on elliptic curves

(Met een samenvatting in het Nederlands)

Proefschrift ter verkrijging van de graad van doctor aan de Universiteit Utrecht op gezag van de Rector Magnificus, Prof. Dr. H. O. Voorma, ingevolge het besluit van het College van Decanen in het openbaar te verdedigen op donderdag 14 september 2000 des ochtends te 10.30 uur

door

Tim Dokchitser

geboren op 12 augustus 1973 te Leningrad.

Promotor: Prof. Dr. F. Oort,
Universiteit Utrecht

Copromotor: Dr. J. Top,
Rijksuniversiteit Groningen

To my first teachers
O. A. Sheptovitskaya and B. M. Bekker

This thesis consists of two independent parts. The first 5 chapters are dedicated to infinitesimal deformation theory and applications to p-divisible groups. The last chapter concerns Kummer maps and p-descent on elliptic curves. Each part has an own introduction, to which we refer for a more detailed description.

I would like to express my deep gratitude to B. Moonen and J. Top for numerous ideas and suggestions. I want also to thank them and E. Schaefer for careful proofreading of the manuscript and many vital corrections. I want to thank J. de Jong, W. van der Kallen, F. Oort and many others for the fruitful discussions related to this work. Finally, I would like to thank Claudia and Fabrizio for their constant support during the writing of this thesis.

Contents

Introduction

The moduli spaces of p-divisible groups with a PEL-type structure have recently attracted considerable attention. One reason for this interest is the search for good integral models of Shimura varieties. Another one is a wish to have a better understanding of the moduli of abelian varieties. This thesis attempts to add to the knowledge of the structure of these moduli spaces.

Our moduli spaces are obtained by looking at those p-divisible groups that possess a given extra structure, which can be a polarization, a ring of endomorphisms and/or a fixed level structure (whence the PEL abbreviation). As Kottwitz has shown ([18], §5), if this extra structure is "prime-to-p", the resulting deformation functors are smooth over the base. If not, the spaces generally become singular. These singularities have been studied in many cases; see for example Deligne-Pappas [6], Rapoport-Zink [33] and Pappas [32] for the ramified ring of endomorphisms, Norman [27], de Jong [17] and Crick [5] for inseparable polarizations and Chai-Norman [4] for the p-level structure.

One of the difficulties in such studies is a lack of deformation theory of p-divisible groups, which would be both general enough to work over an arbitrary base and simple enough to do all the necessary computations. The crystalline approach (Messing [23]; Berthelot, Breen, Messing [2]) and that of Fontaine [10] have a disadvantage that they work only for divided power extensions. Consequently, they directly allow to determine the moduli space only in the cases of not too high ramification (cf. Norman [27]). On the other hand, the Cartier theory or the theory of displays (Norman-Oort [28], Zink [40]) does work over an arbitrary base. However, these theories require computations in σ-linear algebra, which are usually quite difficult.

A possible way out is to use the so-called *local models*. The idea is to find, étale-locally, a *non-canonical* isomorphism between the moduli space that one is interested in and a moduli space of a certain linear algebra problem. This has the advantage of allowing explicit computations. It is the approach used in [6], [17] and [33] for specific moduli problems. The unifying idea is that such an isomorphism is supposed to exist, whenever the deformation data in question is *rigid* on the Dieudonné modules. Our main goal is to give this idea a precise formulation and prove the existence of such an isomorphism (Theorem 4.3.8). To illustrate the possible applications we present some examples in Chapter 5.

Fix a perfect ground field k of characteristic $p>0$ and a complete Noetherian local ring Λ with $\Lambda/m_\Lambda \cong k$. Since we are interested primarily in the "very local" structure of the moduli spaces, we formulate our deformation problems in terms of functors on the category Art_Λ, Artinian local Λ-algebras with residue field k.

For example, let G/k be a p-divisible group and fix a finitely generated $\mathbf{Z}_p$-subalgebra $\mathcal{O} \subset \mathrm{End}(G)$. For simplicity take $\Lambda = W = W(k)$, the ring of Witt vectors of k. One can define the (covariant) functor

$$\mathcal{D}\mathrm{ef}(G,\mathcal{O}) : Art_W \longrightarrow Sets\,,$$

which associates to a ring $A \in Art_W$ the set of pairs $(\mathcal{G}/A, \mathcal{O} \subset \mathrm{End}(\mathcal{G}))$ up to isomorphism. Here $\mathcal{G}/A$ is a deformation of G/k, a p-divisible group given together with an identification $\mathcal{G} \otimes_A k \cong G$. As for the inclusion $\mathcal{O} \subset \mathrm{End}(\mathcal{G})$, we require it to reduce to the chosen one on G. In other words we are interested in those deformations of G which inherit the given $\mathcal{O}$-action. It is not difficult to show that the functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is pro-representable (4.3.5). Since $\mathcal{D}\mathrm{ef}(G)$ is well-known to be pro-represented by the ring $W[[t_1, ..., t_d]]$ with $d = \dim G \dim G^t$, it follows that $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is pro-represented by a ring of the form

$$U = W[[t_1, ..., t_d]]/J$$

for some ideal J. We use here the rigidity of morphisms, which implies that the forgetful map $\mathcal{D}\mathrm{ef}(G, \mathcal{O}) \to \mathcal{D}\mathrm{ef}(G)$ is an inclusion of functors. The question is how to determine the pro-representing ring U.

Associated to deformation $\mathcal{G}/A$ of G/k there is a filtration of the Lie algebra of the universal extension of $\mathcal{G}$ (cf. Messing [23], Chapter IV),

$$V\mathcal{G} \subset M\mathcal{G} \, .$$

The A-modules $V\mathcal{G}$ and $M\mathcal{G}$ are functorial in G and the pair $V\mathcal{G} \subset M\mathcal{G}$ deforms (in the obvious sense) the corresponding pair $VG \subset MG$ for G. Further, if $\mathcal{G}$ admits an $\mathcal{O}$-action, then $V\mathcal{G}$ and $M\mathcal{G}$ are $\mathcal{O}$-modules. So there is a natural transformation of deformation functors (see 4.1.4, 4.3.1 for definitions)

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}) \longrightarrow \mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O}) \, .$$

Thanks to the crystalline theory, we know that the deformation behaviour of the universal extension filtration determines, to a certain extent, that of G. Let us restrict our functors to the category $Art_{W,pd}$ of those $A \in Art_\Lambda$ for which the kernel of the structure map $A \to k$ has nilpotent divided powers. Then the $M\mathcal{G}$'s form a *crystal*; in other words, for any $A \in Art_{W,pd}$ and $\mathcal{G}_1, \mathcal{G}_2/A$ deforming G/k, there are canonical isomorphisms

$$M\mathcal{G}_1 \cong \mathcal{M} \otimes_W A \cong M\mathcal{G}_2,$$

where $\mathcal{M} = \mathbf{D}(G)$ is the covariant Dieudonné module of G. By functoriality, everything is compatible with the $\mathcal{O}$-action. Hence there is a canonical isomorphism of functors

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}) \longrightarrow \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{O}) \, . \tag{1}$$

Here $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{O})$ is the rigidified version of $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O})$; an element of $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{O})(A)$ is an $\mathcal{O}$-stable filtration of finite free A-modules $V_A \subset M_A$ which deforms $VG \subset MG$ and an isomorphism

$$M_A \cong \mathcal{M} \otimes_W A \, ,$$

compatible with the $\mathcal{O}$-action.

Unfortunately, a canonical isomorphism such as (1) does not exist on the full category Art_W(cf. 4.3.10). Still, one can consider the following diagram of natural transformations of functors on Art_W:

$$\begin{array}{ccc} \mathcal{D}\mathrm{ef}(G,\mathcal{O}) & \cdots\cdots> & \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG\subset MG,\mathcal{O}) \\ & {\scriptstyle q_1}\searrow \quad \swarrow{\scriptstyle q_2} & \\ & \mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O}) & \end{array} .$$

Assume that the ring $\mathcal{O}$ has the property that the module $\mathcal{M}$ is *rigid*. By this we mean that any deformation of $\mathcal{M}\otimes_W k$ to a ring $A\in Art_W$ is isomorphic to $\mathcal{M}\otimes_W A$, as an $\mathcal{O}$-module. Then one can expect *every* element of $\mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O})$ to be in the image from $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG\subset MG,\mathcal{O})$. Moreover, by crystalline theory, the same argument should hold for the functor $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$. Indeed, we will show that the transformations q_1 and q_2 are formally smooth (4.3.8, 4.4.1).

The consequence is that there is a non-canonical isomorphism (dotted arrow in the above diagram),

$$\mathcal{D}\mathrm{ef}(G,\mathcal{O}) \;\cong\; \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG\subset MG,\mathcal{O})\,, \tag{2}$$

compatible with the projections to $\mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O})$. This is clear if the functor $\mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O})$ is pro-representable. Then the formal smoothness of q_1 and q_2 implies that both the pro-representing rings of the functors above are formal power series over the pro-representing ring of $\mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O})$. By comparing the tangent spaces (crystalline theory again), it follows that the isomorphism (2) indeed exists. In fact, $\mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O})$ is usually not pro-representable. However, a general comparison theorem (1.5.3) for formally smooth extensions implies the isomorphism (2) exists anyway.

Several comments are in order.

First, one has to determine what is the condition on the ring $\mathcal{O}$ which guarantees the required rigidity. It turns out, that whenever $\mathcal{O}$ is a *hereditary* (e.g. maximal) order in a semi-simple $\mathbf{Q}_p$-algebra, the Dieudonné module $\mathbf{D}(\mathrm{G})$ is a projective $\mathcal{O}\otimes_{\mathbf{Z}_p} W$-module (4.4.1, part 1) and, hence, satisfies the rigidity condition (4.4.1, part 2).

Second remark is that the functor $\mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O})$ is of interest in itself. In fact, let

$$\rho_\tau : \mathcal{O}\longrightarrow \mathrm{End}(TG)$$

be the tangent space representation of $\mathcal{O}$. Then it follows from our rigidity assumption that the natural map

$$\begin{array}{ccc} \mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O}) & \longrightarrow & \mathcal{D}\mathrm{ef}(\rho\tau) \\ V_A\subset M_A & \longmapsto & M_A/V_A \end{array}$$

gives an isomorphism of functors (cf. the proof of Theorem 4.4.1). In view of this, the formal smoothness of q_1 means the following: a necessary and sufficient condition to

deform the pair $(G, \mathcal{O})$ to a ring $A \in Art_W$ is being able to deform the tangent space representation ρ_τ to A. Therefore, the geometric properties of the functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ (flatness, smoothness etc.) can be read off from those of $\mathcal{D}\mathrm{ef}(\rho_\tau)$.

This explains why in the search of good integral models of Shimura varieties, one is bound to restrict the tangent space representation. Indeed, the minimal requirement for these models is that they should be flat over $\mathrm{Spec}\, W$. However, the deformation functor $\mathcal{D}\mathrm{ef}(\rho_\tau)$ is definitely not flat in general; consider for example a supersingular elliptic curve E with $\mathcal{O} = \mathrm{End}(E)$. Then

$$\mathcal{D}\mathrm{ef}(E, \mathcal{O}) \cong \mathrm{Hom}_W(k, -)$$

is not flat over $\mathrm{Spec}\, W$. Kottwitz [18] has formulated a determinantal condition which does imply flatness in certain cases. In fact, Rapoport and Zink [33] have conjectured that under this condition, all local models are flat (in case $\mathcal{O}$ is a maximal order). This was disproved by Pappas [32] in case $\mathcal{O}$ is a quadratic extension of $\mathbf{Z}_p$. He has, moreover, conjectured flatness under a modified version of this condition. In any case, as we have seen above, such a flatness condition can be formulated purely in terms of the tangent space representation. If one provides such a condition and shows that (the hull of) the resulting restricted deformation functor $\mathcal{D}\mathrm{ef}'(\rho_\tau)$ is flat over $\mathrm{Spec}\, W$, the same holds for $\mathcal{D}\mathrm{ef}'(G, \mathcal{O})$.

The final remark is that the proof of the existence of an isomorphism (2) has little to do with the fact that we are looking at the case of endomorphisms. So we can prove the main comparison theorem (4.3.8) for a rather general deformation data.

The structure of the manuscript is as follows. We refer to the introductions of the chapters for a more extended outline.

Chapter 1 is dedicated to the infinitesimal deformation theory in general. It can be read independently of the rest of the thesis. Although infinitesimal methods form a basis of almost every deformation study, the basic statements and even definitions (obstruction space, for instance) seem to have been undocumented until recently (see [9]). So we decided to give a short consistent presentation of the basic results in the theory. We also prove the comparison theorem for formally smooth extensions (Section 1.5) and discuss quotient functors (Sections 1.6–1.7).

Chapters 2,3 form preliminaries needed for the main results in Chapters 4, 5. Chapter 2 is dedicated to the deformation functors of representations of R and of R-stable filtrations (Sections 2.2,2.3). The Hochschild cohomology groups which occur as tangent and obstruction spaces to these functors are recalled in Section 2.1. The ring representation case is similar to Mazur's study of group representations in [22], except that Hochschild cohomology replaces group cohomology.

Chapter 3 recalls the basic structure theorems of maximal and hereditary orders in semisimple algebras over a field K, which is complete with respect to a discrete valuation. We give a simple extension of the result of Janusz [15] on base change of hereditary orders in case of an infinite base extension.

In Chapter 4 we prove the main comparison result for the PEL-type moduli problems of p-divisible groups. To present the result as general as possible, we define the notion of a deformation data (Section 4.2) and formulate the main theorem (Section 4.3) in terms of it. As the theorem only applies when the deformation data is rigid on the Dieudonné modules, there is an obvious question in which situations this condition is satisfied. For the deformation functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ this turns out to be the case whenever $\mathcal{O}$ is a hereditary (e.g. maximal) order in a semi-simple $\mathbf{Q}_p$-algebra (Section 4.4); for the functor deformation functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$ when the order $\mathcal{O}$ is hereditary and λ is principal (Section 4.5). We show also how to reduce the more general deformation problems to the case of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ or $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$ with λ principal (Section 4.6). As an illustration, we consider the case of the "p-chain" of p-divisible groups (Section 4.7).

In Chapter 5 we use the comparison theorem and the relation to the tangent space representation to determine the pro-representing ring of the functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ in some cases. We discuss the following examples:

1. $\mathcal{O}$ unramified.
2. $\mathcal{O}/\mathbf{Z}_p$ quadratic, G arbitrary.
3. $\mathcal{O} = \mathbf{Z}_p[\sqrt[h]{\pi}]$ and G of height $h \leq 4$.
4. $\mathcal{O}$ maximal order in a central division algebra over $\mathbf{Q}_p$ and G arbitrary.
5. $\mathcal{O}$ arbitrary, G one-dimensional.

In case 1 we get the result of Kottwitz; case 3 gives back a local result of Drinfeld ([8], Prop. 4.2) in case $\mathcal{O}$ is commutative. Case 4 generalizes the example of the so-called special formal $\mathcal{O}_D$-modules ([33], 3.69). Finally we discuss the canonical liftability of morphisms (Section 5.5).

Notations. We work over a ground field k which is arbitrary in Chapters 1–2 and perfect of positive characteristic p in Chapters 4, 5. We denote by Λ a fixed complete Noetherian local ring given together with an augmentation isomorphism $\eta_\Lambda : \Lambda/m_\Lambda \xrightarrow{\sim} k$. In Chapter 5 we let $\Lambda = W = W(k)$, the ring of Witt vectors.

A ring by definition contains 1.

To denote the duals, V^* is used for k-vector spaces in Chapters 1–2. From Chapter 4 on, we use the consistent notation G^t, M^t etc. for the Serre duals of p-divisible groups, A-linear duals for finite free A-modules etc.

The symbol Hom_k stands for morphisms in the category of k-vector spaces and Hom_Λ for morphisms in Art_Λ. The set of $m \times n$ matrices over A is denoted by $\mathrm{Mat}_{m\times n}(A)$.

1 Infinitesimal deformation theory

In this chapter we study infinitesimal deformation theory, that is, properties of (covariant) functors of Artin rings. In our applications later, these will be deformation functors of some kind. Let k be an arbitrary ground field and fix a complete Noetherian local ring Λ with $\Lambda/m_\Lambda \cong k$. Following Schlessinger [35], we work on the category Art_Λ of Artinian local Λ-algebras A given together with an isomorphism $A/m_A \cong k$.

There are several points which make infinitesimal deformation theory usually far more accessible than a general moduli study on the full category of rings.

First, any surjection in Art_Λ can be split into a finite sequence of *small surjections*. A surjection $\pi : A \twoheadrightarrow A'$ is small if m_A annihilates $I = \ker \pi$. In this case I is a finite-dimensional k-vector space. So any ring $A \in Art_\Lambda$, however singular and complicated, can be obtained from the ground field k by a finite sequence of extensions by k-vector spaces. This often allows to reduce some questions in the study of (difficult) deformation functors to (hopefully simpler) linear algebra. Consider, for example, a pro-representable functor $\mathcal{F} : Art_\Lambda \to Sets$, and take an element $\xi' \in \mathcal{F}(A')$. Then the size of a fiber of the map $\mathcal{F}(A) \to \mathcal{F}(A')$ above ξ' is controlled by two finite-dimensional k-vector spaces, the obstruction space $O\mathcal{F}$ and the tangent space $T\mathcal{F}$. If $\mathcal{F}$ is a deformation functor of some kind, these are usually some kind of cohomology groups. In practice they can often be determined, yielding some amount of information about the functor in question.

Second, another attractive characteristic of working on Art_Λ is the simple nature of formal smoothness. While there exist plenty of smooth morphisms on the category of rings (or schemes), the analogous infinitesimal notion of formal smoothness is far more restrictive. In fact, any formally smooth natural transformation of pro-representable functors $\mathcal{F} \to \mathcal{G}$ is given in terms of the pro-representing rings by

$$G \longrightarrow G[[t_1, \ldots, t_n]] \cong F$$

for some $n \geq 0$. In particular the only formally smooth pro-representable functors on Art_Λ are the ones whose pro-representing ring is isomorphic to $\Lambda[[t_1, \ldots, t_n]]$ for some n.

Third useful feature of Art_Λ is that it is usually quite easy to determine whether a functor is pro-representable. This is again in constrast with the difficulties of solving the analogous representability questions on the category of rings. Schlessinger's theorem ([35], Theorem 2.11) asserts that $\mathcal{F} : Art_\Lambda \to Sets$ is pro-representable if and only if $\mathcal{F}$ commutes with fibre products,

$$\mathcal{F}(A \times_B C) = \mathcal{F}(A) \times_{\mathcal{F}(B)} \mathcal{F}(C) \tag{3}$$

plus $\mathcal{F}(k)$ consists of one point and the tangent space $T\mathcal{F}$ is finite-dimensional. Moreover, it is enough to test (3) when, say, $C \to B$ is a small surjection. This gives a practically effective criterion to show that a functor is pro-representable.

It should be noted, however, that not all deformation problems give rise to functors which are pro-representable. For example, very often one is led to study the functors

which can be represented as quotients of a pro-representable functor by an action of a formal group, such as $\widehat{GL}_n$ for some n. These are not in general pro-representable, although they do have a weaker property of possessing a hull. Hence it is natural to ask whether the three points mentioned above generalize to a larger class of functors than just that of the pro-representable ones. Roughly speaking, the goal of this chapter is to give some answers to this question.

More precisely, our aim is threefold:

First, we axiomatize the notion of an obstruction space for an arbitrary covariant functor $\mathcal{F}: Art_\Lambda \to Sets$ (Section 1.3). This follows the ideas of Artin ([1], 2.6). We show (1.3.8) that the minimal obstruction space $O\mathcal{F}$ exists when $\mathcal{F}$ commutes with products,

$$\mathcal{F}(A \times_k B) \xrightarrow{\sim} \mathcal{F}(A) \times \mathcal{F}(B)\,.$$

This condition is satisfied for most of the deformation functors which occur in practice, since those can be usually represented as a quotient of a pro-representable functor by a formal group action (1.7.3). In the studies of concrete deformation functors, the technical point of the existence (and functoriality etc.) of an obstruction space is often ignored. Note that very similar results to those presented here have been obtained recently by Fantechi and Manetti [9].

Our second object of study is formally smooth natural transformations $\mathcal{F} \to \mathcal{D}$ where $\mathcal{D}$ is not necessarily pro-representable. More precisely, given a diagram

$$\mathrm{Hom}_\Lambda(F_1, -) = \mathcal{F}_1 \xrightarrow{f} \mathcal{D} \xleftarrow{g} \mathcal{F}_2 = \mathrm{Hom}_\Lambda(F_2, -),$$

with f, g formally smooth, we ask ourselves how are F_1 and F_2 related. For example, if $\mathcal{D}$ is pro-representable, it is clear that one of the rings F_1, F_2 is a formal power series ring over the other. The same statement holds if $\mathcal{D}$ is only assumed to have a tangent space (1.5.5). More generally, for an arbitrary $\mathcal{D}$ we prove a comparison theorem (1.5.3) which relates F_1 and F_2 purely from the tangent space information. This comparison theorem serves as a main tool for our study of deformation functors of p-divisible groups in Chapter 4.

The third part of this chapter addresses a question whether a given functor can be written as a quotient of a pro-representable one by a group action. If Γ is a group which acts on a pro-representable functor $\mathcal{F}$, it is easy to determine whether the question $\mathcal{F}/\Gamma$ has a hull (1.6.2). Conversely, if $\mathcal{D}: Art_\Lambda \to Sets$ has a hull $\mathcal{F} \to \mathcal{D}$, we show that $\mathcal{D}$ can be represented as $\mathcal{F}/\Gamma$ for some Γ if and only if the natural map

$$\mathcal{D}(A \times_B C) \longrightarrow \mathcal{D}(A) \times_{\mathcal{D}(B)} \mathcal{D}(C)$$

is surjective for all $A \to B \leftarrow C$ in Art_Λ (1.6.3). We also conjecture the analogous criterion for quotients by a formal group action (1.7.5).

To keep the presentation self-contained, we recall the basic facts about the category Art_Λ and Schlessinger's criterion (Sections 1.1, 1.2, 1.4).

1.1 Artinian local algebras

Let Λ be a complete Noetherian local ring with residue field k and fix an augmentation isomorphism $\eta_\Lambda : \Lambda/m_\Lambda \to k$. In practice one often has either $\Lambda = k$ (equal characteristics case) or k perfect of positive characteristic and Λ the ring of Witt vectors of k.

Definition 1.1.1. The category Art_Λ consists of Artinian local Λ-algebras A together with an augmentation isomorphism $\eta_A : A/m_A \cong k$. Morphisms in the category are local homomorphisms of Λ-algebras, commuting with the augmentation. The set of such homomorphisms is denoted $\mathrm{Hom}_\Lambda(F, G)$.

Remark. Note that Art_Λ has a final object (k with $\eta_k = \mathrm{id}$). Also note that every surjection $A \twoheadrightarrow A'$ in the category has a nilpotent kernel, so it can be split into a sequence

$$A = A_n \twoheadrightarrow A_{n-1} \twoheadrightarrow \cdots \twoheadrightarrow A_1 \twoheadrightarrow A_0 = A'$$

of small surjections in the sense of [31]:

Definition. A *small surjection* (sometimes called an infinitesimal extension) is a morphism $\pi : A \twoheadrightarrow A'$ in Art_Λ such that $I = \ker \pi$ satisfies $m_A I = 0$.

Remark. The kernel I of a small surjection is a module over $A/m_A = k$. Hence it is a (finite-dimensional) k-vector space. Schlessinger's *small extension* ([35], 1.2) is a small surjection with an additional property that this vector space is one-dimensional. A small surjection (and, hence, any surjection in Art_Λ) can be split into a sequence of small extensions.

To study representability questions, one extends Art_Λ to a larger category $\widehat{Art}_\Lambda$, of which Art_Λ is a full subcategory. The following well-known lemma (cf. [3], Chap. 9, §2, No. 5, Lemme 3b) characterizes the rings of $\widehat{Art}_\Lambda$.

Lemma 1.1.2. *Let F be a complete local Λ-algebra with $F/m_F \cong k$. Then the following conditions are equivalent.*

1. *The vector space $m_F/(m_F^2 + m_\Lambda F)$ is finite-dimensional.*
2. *The ring F is Noetherian.*
3. *For all $n \geq 1$ we have $F/m_F^n \in Art_\Lambda$.*
4. *The algebra F is isomorphic to one of the form $\Lambda[[t_1, ..., t_n]]/J$.*

Proof.
$2 \Rightarrow 1$. If $m_F = (a_1, ..., a_n)F$, then every $x \in m_F$ can be written $x = r_1 a_1 + \cdots + r_n a_n$. Taking r_i modulo m_F and a_i modulo m_F^2, we see that a_i form generators for the F/m_F-vector space $m_F/(m_F^2 + m_\Lambda F)$.
$4 \Rightarrow 2$. Since Λ is Noetherian, $\Lambda[[t_1, ..., t_n]]$ is Noetherian as well.

$1 \Rightarrow 4$. Let $a_1, ..., a_n$ be representatives of a basis for $m_F/(m_F^2 + m_\Lambda F)$. Define a Λ-algebra homomorphism $\Lambda[[t_1, ..., t_n]] \to F$ by letting $t_i \mapsto a_i$. We claim that it is surjective. In other words, for every $x \in F$ there is $f \in \Lambda[[t_1, ..., t_n]]$ with $f(a_1, ..., a_n) = x$. To prove this, we construct inductively a compatible system $f_k \in \Lambda[[t_1, ..., t_n]]$ with total degree of f_k at most k and such that $f_k(a_1, ..., a_n) \equiv x \bmod m_F^{k+1}$. The constant f_0 exists since $\Lambda/m_\Lambda \to F/m_F$ is an isomorphism.

Now assume that f_{k-1} is constructed. Let $y = f_{k-1}(a_1, ..., a_n) - x \in m_F^k$. Firstly, the multiplication map

$$(m_F/m_F^2) \otimes_k \cdots \otimes_k (m_F/m_F^2) \longrightarrow m_F^k/m_F^{k+1}$$

is surjective (by definition of m_F^k). Secondly, m_F/m_F^2 is generated, as a k-vector space, by the a_i and the image of Λ. So there is a homogeneous polynomial $g_k(t_1, ..., t_n)$ of degree k with coefficients in Λ such that $g_k(a_1, ..., a_n) \equiv y \bmod m_F^{k+1}$. Here we again use that the composition $\Lambda \to F \to k$ is surjective. Now $f_k = f_{k-1} + g_k$ satisfies the required property.
$3 \Rightarrow 1$. Use that F/m_F^2 (and hence m_F/m_F^2) has finite length as a Λ-module.
$2 \Rightarrow 3$. The ring F/m_F^n is Noetherian, local and its maximal ideal is nilpotent. It follows that F/m_F^n is Artinian ([26], 9.1). ∎

Definition 1.1.3. The category $\widehat{Art}_\Lambda$ consists of Noetherian local Λ-algebras A given together with an augmentation isomorphism $\eta_A : A/m_A \cong k$. Morphisms in the category are local homomorphisms of Λ-algebras, commuting with the augmentation. Again we denote by $\mathrm{Hom}_\Lambda(F, G)$ the set of such homomorphisms.

Remark. Our Art_Λ is Schlessinger's C_Λ and our $\widehat{Art}_\Lambda$ is $\hat{C}_\Lambda$ ([35], 1). Note that by the above lemma the condition that A is Noetherian in Schlessinger's definition of $\hat{C}_\Lambda$ can be removed, since it follows from the other assumptions.

1.2 Pro-representable functors

This subsection describes the basic properties of pro-representable functors $\mathcal{F} : Art_\Lambda \to Sets$. We define the obstruction space (1.2.4) and show how the behaviour of $\mathcal{F}$ under small surjections is determined by the tangent and the obstruction space (1.2.7). All results presented here are well-known, but we recall them to keep the presentation self-contained and due to the lack of suitable reference.

Remark. Let $\mathcal{F} : Art_\Lambda \to Sets$ be a covariant functor. Then $\mathcal{F}$ can be canonically extended to a functor $\widehat{Art}_\Lambda \to Sets$ by letting

$$\mathcal{F}(G) = \varprojlim \mathcal{F}(G/m_G^n), \qquad G \in \widehat{Art}_\Lambda ,$$

and similarly for morphisms.

Definition 1.2.1. A covariant functor $\mathcal{F}: Art_\Lambda \to Sets$ is said to be *pro-representable* if the extended functor on $\widehat{Art}_\Lambda$ is representable. In other words, $\mathcal{F}$ is pro-representable if there is a complete Noetherian local Λ-algebra F with $F/m_A = k$ and

$$\mathcal{F}(A) = \mathrm{Hom}_\Lambda(F, A)\ , \qquad A \in Art_\Lambda\ ,$$

functorially in A. We will usually denote the pro-representing ring by the corresponding Latin letter.

Definition 1.2.2. For a complete Noetherian local Λ-algebra F with an augmentation, define *the tangent space of F over Λ* to be the k-vector space

$$TF = \left(\frac{m_F}{m_F^2 + m_\Lambda F}\right)^*\ .$$

Here $*$ denotes k-linear dual. Equivalently, $TF = \mathrm{Der}_\Lambda(F, k)$, the set of Λ-linear derivations of F into k ([35], 1.0).

Remark 1.2.3. A homomorphism $\alpha: F \to G$ induces a k-linear map $d\alpha: TG \to TF$. It is easy to show that α is surjective if and only if $d\alpha$ is injective ([35], Lemma 1.1). Note also that TF is finite-dimensional by Lemma 1.1.2.

Definition 1.2.4. Let $F \in \widehat{Art}_\Lambda$. Let $n = \dim TF$ and write $F = S/J$ with $S = \Lambda[[t_1, \ldots, t_n]]$. This is possible by the proof of $(1 \Rightarrow 4)$ of Lemma 1.1.2. Define *the obstruction space OF of F over Λ* to be the k-vector space

$$OF = (J/m_S J)^*\ .$$

Here $*$ denotes k-linear dual.

Remark 1.2.5. It is easy to show that OF does not depend on the choice of a representation of F as S/J. Moreover, OF is contravariantly functorial in F. Note also that $O(F) = 0$ if and only if F is a power series ring over Λ. It is also clear that an inclusion $F \to F[[t_1, \ldots t_m]]$ induces an isomorphism on the obstruction spaces.

Remark 1.2.6. If F is a complete Noetherian local ring and M is an F-module, then $x_1, \ldots, x_n \in M$ generate M if and only if their residue classes generate $M/m_F M$ as a F/m_F-vector space ([26], 5.1). In particular, J is generated by $\dim_k OF$ elements. So $\dim_k TF$ is the smallest number of generators of F as a complete Λ-algebra and $\dim_k OF$ is the smallest number of relations.

The following theorem describes the behaviour of $\mathcal{F} = \mathrm{Hom}_\Lambda(F, -)$ under a small surjection $A \twoheadrightarrow A'$ with kernel I. The vector space $OF \otimes_k I$ contains the obstruction elements to lifting points of $\mathcal{F}$ under a small extension with kernel I. The space $TF \otimes_k I$ measures how many liftings there are, provided the obstruction is zero.

Theorem 1.2.7. *Let $\mathcal{F} \cong \mathrm{Hom}_\Lambda(F, -)$ be a pro-representable functor from Art_Λ to Sets. Let $\pi : A \twoheadrightarrow A'$ be a small surjection in Art_Λ with kernel I. Take $\xi' \in \mathcal{F}(A')$. Then*

1. *There exists an element $\Theta \in OF \otimes_k I$ whose vanishing is necessary and sufficient for the existence of $\xi \in \mathcal{F}(A)$ such that $\pi(\xi) = \xi'$.*

2. *The obstruction element is functorial: assume given a commutative diagram*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\rho} \\ A' & \xrightarrow{\varphi'} & B' \end{array} .$$

   where $B \twoheadrightarrow B'$ is a small surjection with kernel K. Then the obstruction element $\Theta \in OF \otimes_k I$ of $(A \twoheadrightarrow A', \xi')$ is related to the corresponding obstruction element $\Sigma \in OF \otimes_k K$ of $(B \twoheadrightarrow B', \varphi'(\xi'))$ by the formula $\Sigma = (1 \otimes \varphi)\Theta$.

3. *If $\Theta = 0$, then the set of all $\xi \in \mathcal{F}(A)$ with $\pi(\xi) = \xi'$ is a principal homogeneous space under $TF \otimes_k I$.*

Proof. We consider ξ' as a homomorphism $F \to A'$. Choose a surjection $p : S = \Lambda[[t_1, ..., t_n]] \to F$ with kernel J as in Definiton 1.2.4.
1. Define $a_i' \in m_{A'}$ to be the images of t_i under the composite morphism $\xi f_0 : S \to F \to A$. In order to lift ξ' to a homomorphism $\xi : F \to A$, choose arbitrary $a_i \in m_A$ such that $\pi(a_i) = a_i'$. This defines a Λ-homomorphism $\alpha : S \to A$ by letting $t_i \mapsto a_i$.

If $\ker \alpha \supset \ker f_0$, then α descends to a $\xi : F \to A$. In general, however, $\alpha : J \to I$ is non-zero. In any case, α vanishes on $m_S J$, and hence descends to an element $\Theta \in OF \otimes_k I$. Recall that I has a structure of a $A/m_A = k$-vector space by the assumption that $m_A I = 0$. The element Θ does not depend on the choice of a_i. Indeed, a different choice $\tilde{a}_i = a_i + \epsilon_i$ with $\epsilon_i \in I$ gives a map $\tilde{\alpha}$ which is the same on J. This follows from the fact that $Im_A = 0$ (so $a_i a_j = \tilde{a}_i \tilde{a}_j$ etc.) and $J \subset m_S^2 + m_\Lambda S$. The element $\Theta \in OF \otimes_k I$ is the required obstruction.
2. Immediate from the construction.
3. Let $\xi, \tilde{\xi} : F \to A$ be two liftings of $\xi' : F \to A'$. Consider the homomorphism (of Λ-modules) $t = \tilde{\xi} - \xi : F \to A$. Then $\mathrm{Im}\, t \subset I$ and $t(m_\Lambda F) = t(m_F^2) = 0$, since $Im_A = 0$. So $t \in T\mathcal{F} \otimes_k I$. Conversely, given ξ and $t \in T\mathcal{F} \otimes_k I$, the Λ-module map $\tilde{\xi} = \xi + t$ is easily verified to be a Λ-algebra homomorphism $F \to A$. ∎

Remark. In practice, given a functor $\mathcal{F}$, one can often prove that $\mathcal{F}$ is pro-representable (e.g. using Schlessinger's criterion, see Theorem 1.4.3). To determine the pro-representing ring F of $\mathcal{F}$ is, however, generally much harder. It is often possible, though, to determine TF and some vector space V containing OF in terms of $\mathcal{F}$ itself. In some cases, for example if $V = 0$ (and hence $OF = 0$), this suffices to determine the ring F. Otherwise, one has at least the following dimension estimate.

Lemma 1.2.8. *For any* $F \in \widehat{Art}_\Lambda$,

$$\dim \Lambda + \dim_k TF - \dim_k OF \;\leq\; \dim F \;\leq\; \dim \Lambda + \dim_k TF \;. \tag{4}$$

Proof. A Noetherian local ring has finite (Krull) dimension ([26], 9.4–9.6), so all the terms of (4) are finite. The second inequalitity follows from the fact that F can be written as $\Lambda[[t_1, ..., t_n]]/J$ with $n = \dim_k TF$ (cf. 1.1.2). For the first inequality, use that J is generated by $\dim_k OF$ elements (by 1.2.6) and use ([26], 9.7)

$$\dim F/(x) \;\leq\; \dim F \;\leq\; \dim F/(x) + 1, \qquad x \in m_F \;.$$

This proves the lemma. ∎

Finally, let us recall the notion of formal smoothness:

Definition 1.2.9. A natural transformation of functors $\mathcal{F} \to \mathcal{D}$ is said to be *formally smooth* if for every surjection $A \twoheadrightarrow A'$ in Art_Λ, the natural map

$$\mathcal{F}(A) \longrightarrow \mathcal{F}(A') \times_{\mathcal{D}(A')} \mathcal{D}(A)$$

is surjective.

Remark 1.2.10. If both $\mathcal{F}$ and $\mathcal{D}$ are pro-representable, then the formal smoothness of $\mathcal{F} \to \mathcal{D}$ is equivalent to the fact that the corresponding map $D \to F$ of Λ-algebras makes F into a formal power series over D,

$$D \longrightarrow F \cong D[[t_1, \ldots, t_n]] \;.$$

See e.g. [35], Proposition 2.5(i). We will show later (1.5.3) that more generally, whenever $\mathcal{F}_1, \mathcal{F}_2 \to \mathcal{D}$ are formally smooth with $\mathcal{F}_1, \mathcal{F}_2$ pro-representable and $\mathcal{D}$ has a tangent space, one of the pro-representing rings F_1, F_2 is a formal power series ring over the other one.

1.3 The tangent space and the obstruction space

In this section we show how to define the tangent space $T\mathcal{F}$ and an obstruction space $O\mathcal{F}$ of a functor $\mathcal{F}$ which is not necessarily pro-representable. For the tangent space this is well-known (cf. [35], Lemma 2.10). The definition of an obstruction space is suggested by Theorem 1.2.7 and Artin's obstruction theory for a groupoid ([1], 2.6).

If $\mathcal{F}$ happens to be pro-representable, then both the tangent space $T\mathcal{F}$ and the (minimal) obstruction space $O\mathcal{F}$ exist and coincide with those of the pro-representing ring F (1.3.2,1.3.9).

We also show that the (minimal) obstruction space $O\mathcal{F}$ exists when $\mathcal{F}$ commutes with products over k. This applies to most of the deformation functors which come up in practice. Note, however, that the obstruction spaces which one gets in practice (usually some cohomology groups) are rarely minimal. Our result 1.3.8 has been recently obtained independently by Fantechi and Manetti ([9], 2.10, 2.11).

Notation. For a finite-dimensional k-vector space V and $A \in Art_\Lambda$ we let $A[V] \in Art_\Lambda$ denote the ring $A \oplus V$ with $V^2 = m_A V = 0$ and the augmentation determined by that of A. If $A = k$ and $V = k$, we denote the resulting ring by $k[\epsilon]$.

Remark. The association $V \mapsto k[V]$ embeds the category of finite-dimensional k-vector spaces as a full subcategory of Art_Λ.

If V_1 and V_2 are finite-dimensional k-vector spaces, then there are natural projections $k[V_1 \times V_2] \to k[V_1]$ and $k[V_1 \times V_2] \to k[V_2]$. Thus for any $\mathcal{F}$, we have a map

$$\mathcal{F}(k[V_1 \times V_2]) \longrightarrow \mathcal{F}(k[V_1]) \times \mathcal{F}(k[V_2])\,. \tag{5}$$

Remark. If the above map is bijective for any V_1 and V_2, then $\mathcal{F}(k[\epsilon])$ has a structure of a k-vector space given by (cf. [35], Lemma 2.10):

addition: The (k-linear) addition map $k \times k \to k$ induces

$$\alpha : k[\epsilon] \times_k k[\epsilon] \to k[\epsilon]$$

and thus

$$T\mathcal{F} \times T\mathcal{F} = \mathcal{F}(k[\epsilon]) \times \mathcal{F}(k[\epsilon]) = \mathcal{F}(k[\epsilon] \times_k k[\epsilon]) \xrightarrow{\mathcal{F}(\alpha)} \mathcal{F}(k[\epsilon]) = T\mathcal{F}\,.$$

k-action: The action of $a \in k$ on $\mathcal{F}(k[\epsilon])$ is induced by the map $\epsilon \mapsto a\epsilon$ on $k[\epsilon]$.

Definition 1.3.1. We say that $\mathcal{F}$ has a *tangent space* if (5) is bijective for all V_1 and V_2. In that case we call $T\mathcal{F} = \mathcal{F}(k[\epsilon])$ the tangent space of $\mathcal{F}$.

Remark 1.3.2. A pro-representable functor $\mathcal{F} = \mathrm{Hom}_\Lambda(F, -)$, has a finite-dimensional tangent space, since

$$\mathrm{Hom}_\Lambda(F, k[V \times W]) = \mathrm{Hom}_\Lambda(F, k[V]) \times \mathrm{Hom}_\Lambda(F, k[W])$$

and there are canonical k-vector space isomorphisms

$$T\mathcal{F} = \mathrm{Hom}_\Lambda(F, k[\epsilon]) = \mathrm{Hom}_k(m_F/(m_F^2 + m_\Lambda F), k) = TF\,.$$

Definition 1.3.3. Let $\mathcal{F} : Art_\Lambda \to Sets$ be a covariant functor. An *obstruction* Θ is a triple (A, I, ξ') where $A \in Art_\Lambda$ is a ring, $I \subset A$ an ideal for which $m_A I = 0$ and $\xi' \in \mathcal{F}(A/I)$. We say that Θ is *trivial* if there exists $\xi \in \mathcal{F}(A)$ such that $\mathcal{F}(A \to A/I)(\xi) = \xi'$.

Definition 1.3.4. Let $\mathcal{F} : Art_\Lambda \to Sets$ be a covariant functor. We say that (V, o) is an *obstruction space* for $\mathcal{F}$ if V is a k-vector space and

$$(I, A, \xi') = \Theta \longmapsto o(\Theta) \in V \otimes_k I$$

is a rule which associates to an obstruction (I, A, ξ') an element of $V \otimes_k I$, satisfying

1. (functoriality) If $\Theta = (I, A, \xi'_A)$ and $\Sigma = (J, B, \eta'_B)$ and there exists a map $f : A \to B$ with $f(I) \subset J$ and $\mathcal{F}(A/I \to B/J)(\xi') = \eta'$, then
$$(1 \otimes f)\, o(\Theta) = o(\Sigma)\,,$$
2. (vanishing)
$$\Theta \text{ trivial} \iff o(\Theta) = 0\,.$$

We will sometimes denote an obstruction space just by V, dropping o from the notation.

Remark 1.3.5. If (V, o) is an obstruction space and $i : V \hookrightarrow \tilde{V}$ an inclusion of k-vector spaces, then we can let
$$\tilde{o}(\Theta) = (i \otimes 1)(o(\Theta))$$
and thus get an obstruction space $(\tilde{V}, \tilde{o})$. The requirement that i must be injective follows from the vanishing condition of 1.3.4. If we weaken the vanishing condition by replacing " $\iff$ " by "$\Rightarrow$", then any linear map i will do. In defining the notion of a universal obstruction space we allow this larger class of pairs $(\tilde{V}, \tilde{o})$ as test objects. This choice has an advantage that it gives the functoriality in $\mathcal{F}$ for free (cf. 1.3.7).

Definition 1.3.6. We say that the obstruction space (V, o) for $\mathcal{F}$ is *minimal* or *universal* if it satisfies the following universal property: let $(\tilde{V}, \tilde{o})$ satisfy the functoriality condition and the "$\Rightarrow$" part of the vanishing condition of 1.3.4. Then there is a unique k-linear map $V \to \tilde{V}$ which makes $\tilde{o}$ factor via o.

Notation. If a universal obstruction space of $\mathcal{F}$ exists, we denote it by $O\mathcal{F}$. This makes sense as it is clearly unique up to a (canonical) isomorphism.

Theorem 1.3.7. *The association $O : \mathcal{F} \mapsto O\mathcal{F}$ gives a covariant functor from the category of functors $Art_\Lambda \to Sets$ which have a universal obstruction space to the category of vector spaces over k.*

Proof. We have already defined O on objects. To define O on morphisms, let $t : \mathcal{F} \to \mathcal{G}$ be a natural transformation of functors. Denote by $(O\mathcal{F}, o_{\mathcal{F}})$, $(O\mathcal{G}, o_{\mathcal{G}})$ the universal obstruction spaces of $\mathcal{F}$ and $\mathcal{G}$ respectively. Take an obstruction for $\mathcal{F}$,
$$\Theta = \Big(A, I, \xi' \in \mathcal{F}(A/I)\Big)\,.$$
Let
$$l(\Theta) = o_{\mathcal{G}}\Big(A, I, t(\xi') \in \mathcal{G}(A/I)\Big) \in O\mathcal{G} \otimes_k I\,.$$
Clearly $(O\mathcal{G}, l)$ satisfies the functoriality axiom and the "$\Rightarrow$" part of the vanishing axiom of 1.3.4. Define
$$Ot : O\mathcal{F} \longrightarrow O\mathcal{G}$$
to be the factoring map of l which exists and is unique by the universal property of $O\mathcal{F}$. This defines O for morphisms. From the universal property it also follows that O takes composition to composition, so O is a covariant functor. ∎

Remark. Clearly not every functor $\mathcal{F}$ has an obstruction space. The pro-representable ones do (see 1.3.9), but for example the condition that $\mathcal{F}$ has a hull (see 1.4) alone does not guarantee the existence of $O\mathcal{F}$. The functors which arise in practice, however, can be usually written as quotients of a pro-representable functor by a smooth formal group action. Those satisfy the following condition which does imply the existence of $O\mathcal{F}$ (cf. 1.7.2, 1.7.3).

Theorem 1.3.8. *Let $\mathcal{F} : Art_\Lambda \to Sets$ be a covariant functor. Assume that the natural map*

$$\mathcal{F}(A \times_k B) \longrightarrow \mathcal{F}(A) \times \mathcal{F}(B) \tag{6}$$

is bijective for all $A, B \in Art_\Lambda$. Then $\mathcal{F}$ has a universal obstruction space.

Proof. First note that $\mathcal{F}(k)$ consists of one element (take $A = B = k$).

Consider the set S of tuples (A, I, ξ', s) where $\Theta = (A, I, \xi')$ is an obstruction for $\mathcal{F}$ for which $A \to A/I$ is a small surjection and $s : k \cong I$ an isomorphism of W-modules. By abuse of notation, we will denote such a 4-tuple again by Θ. As a set, $O\mathcal{F}$ is supposed to consist of elements of S modulo equivalence, so we define it this way:

Let $\Theta_1 = (A_1, I_1, \xi_1', s_1)$ and $\Theta_2 = (A_2, I_2, \xi_2', s_2)$ be elements of S. Denote $A_1' = A_1/I_1, A_2' = A_2/I_2$. Define the difference $\Theta_1 - \Theta_2 \in S$ as follows. The product map $A_1 \times_k A_2 \longrightarrow A_1' \times_k A_2'$ is a small extension whose kernel is a 2-dimensional k-vector space, generated by $\epsilon_1 = (s_1(1), 0)$ and $\epsilon_2 = (0, s_2(1))$. The map

$$A_1 \times_k A_2/(\epsilon_1 + \epsilon_2) \longrightarrow A_1' \times_k A_2'$$

is a small surjection. Define an isomorphism u between k and the kernel of this small surjection by letting $u(1) = \epsilon_2$. Finally, define $\eta' \in \mathcal{F}(A' \times_k B')$ to be the unique element which maps to (ξ_1', ξ_2') via 6. Let

$$\Theta_1 - \Theta_2 = (A \times_k B/(\epsilon_1 + \epsilon_2), (\epsilon_1), \eta', u)\,.$$

Let

$$\Theta_1 \sim \Theta_2 \quad \Longleftrightarrow \quad \Theta_1 - \Theta_2 \text{ is trivial}\,.$$

It is easy to check that "$\sim$" is an equivalence relation. Moreover, the subtraction operation defined above respects the equivalence and gives the set $S/\sim$ a structure of an abelian group. We let $O\mathcal{F} = S/\sim$ and give it a k-vector space structure by letting

$$\Theta = (A, I, \xi', \beta \mapsto s(\beta)),\ \alpha \in k^* \quad \Rightarrow \quad \alpha \cdot \Theta = (A, I, \xi', \beta \mapsto s(\alpha\beta))\,.$$

It is easy to see that $O\mathcal{F}$ indeed becomes a k-vector space and that it satisfies the required universal property. ∎

Theorem 1.3.9. *Let $\mathcal{F}: Art_\Lambda \to Sets$ be pro-representable. Then the obstruction space OF of the pro-representing ring F is the universal obstruction space for $\mathcal{F}$.*

Proof. Theorem 1.2.7 shows that OF is, indeed, an obstruction space for $\mathcal{F}$. Recall the construction: write $F \cong S/J$,

$$S \cong \Lambda[[t_1, ..., t_n]], \quad J \subset m_S^2 + m_\Lambda S\,.$$

We let $OF = \mathrm{Hom}(J/m_S J, k)$, as a k-vector space. Given $\Theta = (I, A, \xi')$, the element $o(\Theta)$ is constructed as follows. Denote $A' = A/I$ and let $a_i' = \xi'(t_i)$. Then lift a_i' arbitrarily to $a_i \in A$. The homomorphism $S \to A$ defined by $t_i \mapsto a_i$ maps J to I and descends to a linear map $J/m_S J \to I$, hence an element of $OF \otimes_k I$. We denote this element by $f(\Theta)$.

It remains to prove that (OF, o) is universal. Since pro-representable functors commute with fibred products, $\mathcal{F}$ has a universal obstruction space $O\mathcal{F}$. By Remark 1.3.5, the canonical map

$$i : O\mathcal{F} \longrightarrow OF$$

which exists by the universal property, is injective. Hence it suffices to show that it is surjective. Take $\varphi \in OF$, considered as a k-linear form on $J/m_S J$. Let I denote the kernel of the composition of maps of W-modules

$$J \longrightarrow J/m_S J \xrightarrow{\varphi} k\,.$$

Then $I \subset S$ is an ideal and we let $A = S/I$ and $A' = S/J = F$. The natural projection $A \twoheadrightarrow A'$ is a small extension. Finally, the identity map $F \longrightarrow A'$ gives an element $\xi' \in \mathcal{F}(A')$. The triple

$$\Theta = (I, A, \xi')$$

is an obstruction for which $o(\Theta) = \varphi$. Hence $i(\Theta) = \varphi$. This shows that i is surjective. ∎

Remark. In practice, if a $\mathcal{F}$ is a deformation functor of some kind, then often there are (co)homology groups playing a role of tangent and obstruction spaces for $\mathcal{F}$. This is for example the case for deformations of group representations [22], Lie algebras, subschemes of projective space, ring representations (Theorem 2.2.4), filtrations (Theorem 2.3.2), varieties, endomorphisms of p-divisible groups (4.3.4) and in many other situations. Knowing the tangent and an obstruction space either helps to determine the pro-representing ring (or a hull) of a functor itself, or at least to get some estimates on its dimension. It should be noted, however, that one rarely knows that a given obstruction space is actually minimal. So such a computation can be very often used to show that a functor is formally smooth, but does not help much in proving, for example, that a functor is *not* formally smooth.

1.4 Schlessinger's theory

For the sake of completeness, we recall the notion of a fibre product and state Schlessinger's necessary and sufficient conditions for a functor on Art_Λ to be pro-representable and to possess a hull. The results here are taken completely from Schlessinger [35].

Definition 1.4.1. Let $f: A \to B$ and $g: C \to B$ be two morphisms in Art_Λ. Define *the fibre product of A and C over B* to be the ring

$$A \times_B C = \{(x, y) \in A \times C \mid f(x) = g(y)\}$$

with an obvious Λ-structure and augmentation to k.

Remark. The fibre product $A \times_B C$ is the categorical fibre product in Art_Λ. In fact,

$$\mathrm{Hom}_\Lambda(F, A \times_B C) = \mathrm{Hom}_\Lambda(F, A) \times_{\mathrm{Hom}_\Lambda(F,B)} \mathrm{Hom}_\Lambda(F, C)$$

for *any* Λ-algebra F, not necessarily Artinian. In particular, pro-representable functors commute with fibre products, in the sense of the following definition.

Definition 1.4.2. We say that a functor $\mathcal{F}$ *commutes with fibre products* if for any $f: A \to B$ and $g: C \to B$, the natural map

$$\mathcal{F}(A \times_B C) \to \mathcal{F}(A) \times_{\mathcal{F}(B)} \mathcal{F}(C) \tag{7}$$

is bijective.

Remark. If $\mathcal{F}$ commutes with fibre products then, in particular, it has a tangent space (cf. 1.3.1). For a pro-representable $\mathcal{F}$ the tangent space is, moreover, finite-dimensional. The converse to this due to Schlessinger:

Theorem 1.4.3. *A functor $\mathcal{F}: Art_\Lambda \to Sets$ is pro-representable if and only if $\mathcal{F}(k)$ consists of one element, $\mathcal{F}$ commutes with fibre products and has a finite-dimensional tangent space.*

Proof. [35], Theorem 2.11. ∎

Many of the geometrically interesting functors are not pro-representable. For instance, the deformation functors of complete varieties, of group/ring representations and of group schemes are in general not pro-representable. These, however, can often be represented as quotient functors of a pro-representable functor by a group action of a smooth formal group, usually some GL_n. In particular, they satisfy a weaker condition of possessing a hull. (For instance, see Theorem 2.2.4 for the case of ring representations and [35], Prop. 3.10, 3.12 for the case of varieties.)

Theorem 1.4.4. *Assume a functor $\mathcal{F}$ (such that $\mathcal{F}(k)$ has one element) has a finite-dimensional tangent space. The following conditions are equivalent:*

1. *The map (7) is surjective for all $A \to B \leftarrow C$ in Art_Λ (it suffices to check this when $A \twoheadrightarrow B$ is a small extension).*

2. *There is a pro-representable functor $\mathcal{G}$ and a formally smooth map $\mathcal{G} \to \mathcal{F}$ which is an isomorphism on tangent spaces.*

3. *There is a pro-representable functor $\mathcal{G}$ and a formally smooth map $\mathcal{G} \to \mathcal{F}$.*

Proof. $1 \Leftrightarrow 2$ is Schlessinger's theorem [35], Theorem 2.11. $3 \Rightarrow 1$ follows from the fact that the map (7) for $\mathcal{G}$ is surjective and $\mathcal{G}(A) \twoheadrightarrow \mathcal{F}(A)$ for all A. The implication $2 \Rightarrow 3$ is trivial. ∎

Definition. If $\mathcal{F}$ satisfies the equivalent conditions of Theorem 1.4.4, we say that $\mathcal{F}$ has a hull. In fact, a *hull of* $\mathcal{F}$ is a pro-representable functor $\mathcal{G}$ together with a formally smooth map $\mathcal{G} \to \mathcal{F}$ which is an isomorphism on tangent spaces.

Remark. A hull $\mathcal{F}$ of $\mathcal{D}$, if it exists, is unique up to a non-canonical isomorphism ([35], Proposition 2.9). This also follows from Corollary 1.5.4.

1.5 Comparing formally smooth extensions

Suppose a functor $\mathcal{D}$ possesses a hull $g : \mathcal{G} \to \mathcal{D}$ with $\mathcal{G} = \mathrm{Hom}_\Lambda(G, -)$. It turns out that any other formally smooth map $f : \mathrm{Hom}_\Lambda(F, -) = \mathcal{F} \to \mathcal{D}$ factors through $\mathcal{G}$,

$$\begin{array}{ccc} \mathcal{F} & \xrightarrow{\alpha} & \mathcal{G} \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & \mathcal{D} & \end{array} \quad .$$

Moreover the factoring map α is formally smooth, so $F \cong G[[t_1, ..., t_n]]$. In other words, the only rings which can be mapped to $\mathcal{D}$ in a formally smooth way, are formal power series over G. In practice, this can be used to determine the hull of a functor $\mathcal{D}$. Firstly, find *any* formally smooth map $\mathcal{F} \to \mathcal{D}$ with $\mathcal{F}$ pro-representable. For example, $\mathcal{D}$ is often given as a quotient of some $\mathcal{F} = \mathrm{Hom}_\Lambda(F, -)$ by a smooth group action. Secondly, find an isomorphism

$$F \;\cong\; G[[t_1, ..., t_n]], \quad n = \dim_k T\mathcal{F} - \dim_k T\mathcal{D}\,,$$

for some G. Then (combine 1.5.6 with 1.5.7) the ring G pro-represents the hull of $\mathcal{D}$.

The main result of this section is Theorem 1.5.3, which compares formally smooth extensions of a functor $\mathcal{D}$. In order to give a formulation in case $\mathcal{D}$ does not necessarily have a tangent space, we need some preliminary definitions.

Remark. (cf. [35], 2.10) Suppose $\mathcal{G} \cong \mathrm{Hom}_\Lambda(G, -)$ is pro-representable. The cotangent space $T\mathcal{G}^*$ of G over Λ has the property that

$$\mathcal{G}(k[V]) = \mathrm{Hom}_\Lambda(G, k[V]) = \mathrm{Hom}_k(T\mathcal{G}^*, V)$$

for any (finite-dimensional) k-vector space V. In other words, $T\mathcal{G}^*$ represents the functor $V \mapsto \mathcal{G}(k[V])$ on the category of k-vector spaces.

In particular, given another pro-representable functor $\mathcal{F} \cong \mathrm{Hom}_\Lambda(F, -)$, a natural transformation $\mathcal{F} \to \mathcal{G}$ induces a k-linear map $T\mathcal{G}^* \to T\mathcal{F}^*$ and, hence, gives an element of $\mathcal{G}(k[T\mathcal{F}^*])$.

For example, the identity map $\mathcal{G} \to \mathcal{G}$ corresponds to an element which we denote by $1 \in \mathcal{G}(k[T\mathcal{G}^*])$. It is the image of $1 \in \mathcal{G}(G) = \mathrm{Hom}_\Lambda(G, G)$ under the natural projection $G \to k[T\mathcal{G}^*]$.

Definition 1.5.1. Assume given a diagram of natural transformations of functors

$$\begin{array}{ccc} \mathcal{F} & & \mathcal{G} \\ {\scriptstyle f}\searrow & & \swarrow{\scriptstyle g} \\ & \mathcal{D} & \end{array} \tag{8}$$

with $\mathcal{F}$ and $\mathcal{G}$ pro-representable. We say that a k-linear map

$$t : T\mathcal{F} \longrightarrow T\mathcal{G}$$

lies above $\mathcal{D}$, if the corresponding element in $\mathcal{G}(k[T\mathcal{F}^*])$ and the element $1 \in \mathcal{F}(k[T\mathcal{F}^*])$ project via g and f to the same element of $\mathcal{D}(k[T\mathcal{F}^*])$. By a *lift* of such a t, we mean a natural transformation $\alpha : \mathcal{F} \to \mathcal{G}$, which makes (8) commute (i.e. $g\alpha = f$) and which induces t on the tangent spaces.

Remark 1.5.2. Conversely, given $\alpha : \mathcal{F} \to \mathcal{G}$ with $g\alpha = f$, it induces a map $t : T\mathcal{F} \to T\mathcal{G}$ which lies above $\mathcal{D}$, and α is a lift of t. This, perhaps, explains the meaning of these notions.

Remark. If $\mathcal{D}$ has a tangent space, then $t : T\mathcal{F} \to T\mathcal{G}$ lies above $\mathcal{D}$ if and only if it commutes with projections to $T\mathcal{D}$.

Theorem 1.5.3. *Assume given $\mathcal{F} \xrightarrow{f} \mathcal{D} \xleftarrow{g} \mathcal{G}$ with $\mathcal{F}, \mathcal{G}$ pro-representable and a k-linear $t : T\mathcal{F} \to T\mathcal{G}$ which lies above $\mathcal{D}$. Then*

1. *If g is formally smooth then a lift of t exists.*
2. *If f is formally smooth and t is surjective, then any lift of t is formally smooth.*
3. *If f is formally smooth and t is bijective, then any lift of t is an isomorphism of functors.*

Proof. **1.** Constructing a natural transformation $\alpha : \mathcal{F} \to \mathcal{G}$ which lies above $\mathcal{D}$ (i.e. $g\alpha = f$) and induces t on the tangent spaces is equivalent to giving an element $\alpha \in \mathcal{G}(F)$ such that $g(\alpha \in \mathcal{G}[F]) = f(1 \in \mathcal{F}[F]) \in \mathcal{D}(F)$ and such that α maps to an element which corresponds to t under the natural projection $\mathcal{G}(F) \to \mathcal{G}(k[T\mathcal{F}^*])$. In other words, we are looking for a pre-image of $(f(1), t)$ under the map

$$\mathcal{G}(F) \to \mathcal{D}(F) \times_{\mathcal{D}(k[T\mathcal{F}^*])} \mathcal{G}(k[T\mathcal{F}^*]),$$

This map is surjective by the assumption that $g : \mathcal{G} \to \mathcal{D}$ is formally smooth.
2. Let $\alpha : \mathcal{F} \to \mathcal{G}$ induce a surjection $t : T\mathcal{F} \to T\mathcal{G}$. We have to show that given $\pi : A \twoheadrightarrow A'$,

$$\mathcal{F}(A) \twoheadrightarrow \mathcal{F}(A') \times_{\mathcal{G}(A')} \mathcal{G}(A),$$

in other words, given $\varphi' \in \mathcal{F}(A')$ and $\gamma \in \mathcal{G}(A)$ with $\alpha(\varphi') = \pi(\gamma)(= \gamma')$, we have to construct $\varphi \in \mathcal{F}(A)$ with $\pi(\varphi) = \varphi'$ and $\alpha(\varphi) = \gamma$.

By induction over the length, it suffices to consider the case $A \twoheadrightarrow A'$ is a small extension ($\ker \pi = (\epsilon) \neq 0$, $m_A \epsilon = 0$). In other words $(\epsilon) \cong k$ as a Λ-module, and we *fix* such an identification.

Let $\delta \in \mathcal{D}(A), \delta' \in \mathcal{D}(A')$ be the images of γ, γ' under g. Note that $\delta' = f(\varphi')$ and by the formal smoothness of f,

$$\mathcal{F}(A) \twoheadrightarrow \mathcal{F}(A') \times_{\mathcal{D}(A')} \mathcal{D}(A),$$

so there is $\tilde{\varphi} \in \mathcal{F}(A)$ such that $\pi(\tilde{\varphi}) = \varphi'$.

Let $\tilde{\gamma} = \alpha(\tilde{\varphi}) \in \mathcal{G}(A)$. If $\tilde{\gamma} = \gamma$, let $\varphi = \tilde{\varphi}$ and we are done. Otherwise, we adjust $\tilde{\varphi}$ (within the fibre above φ'), using the surjectivity of t as follows:

Both γ and $\tilde{\gamma}$ are ring homomorphisms $G \to A$. Consider them as just homomorphisms of Λ-modules. Then $\tau = \gamma - \tilde{\gamma}$ is a map $G \to A$ of Λ-modules which lands in $(\epsilon) = \ker \pi$. Restrict it to the map $m_G \to (\epsilon)$ and note that it descends to $m_G/(m_G^2 + m_\Lambda G) \to (\epsilon)$, since $(\epsilon) \cong k$ as a Λ-module. Hence τ can be considered as an element of $T\mathcal{G}$.

Now lift τ to an element $\sigma \in T\mathcal{F}$ via the surjection $t : T\mathcal{F} \to T\mathcal{G}$. Extend it to a homomorphism of Λ-modules $F \to (\epsilon) \subset A$ by letting 1 map to 0 and define $\varphi = \tilde{\varphi} + \sigma$. Then one easily checks that φ is a local Λ-algebra homomorphism, $\pi(\varphi) = \varphi'$ and $\alpha(\varphi) = \gamma$ as required.
3. The same argument as in (2.) applies, except that now $t : T\mathcal{F} \to T\mathcal{G}$ is injective, so σ and, therefore, the desired φ is also unique. Hence

$$\mathcal{F}(A) \xrightarrow{\cong} \mathcal{F}(A') \times_{\mathcal{G}(A')} \mathcal{G}(A)$$

whenever $A \twoheadrightarrow A'$. In particular, taking $A' = k$, we see that $\alpha : \mathcal{F}(A) \to \mathcal{G}(A)$ is a bijection for all A. Hence α is an isomorphism of functors. ∎

Corollary 1.5.4. *If $\mathcal{F} \xrightarrow{f} \mathcal{D} \xleftarrow{g} \mathcal{G}$ with $\mathcal{F}, \mathcal{G}$ pro-representable and f, g formally smooth, then $\mathcal{F}$ is isomorphic to $\mathcal{G}$ over $\mathcal{D}$ if and only if the tangent spaces $T\mathcal{F}$ and $T\mathcal{G}$ are isomorphic over $\mathcal{D}$.*

Proof. Follows immediately from the theorem. It should be mentioned, however, that this corollary requires only the (easier) part 1. of the theorem. If $\alpha : \mathcal{F} \to \mathcal{G}$ and $\beta : \mathcal{G} \to \mathcal{F}$ lift the given isomorphisms on the tangent spaces, then $\alpha\beta$ and $\beta\alpha$ are isomorphisms: an endomorphism of a complete Noetherian local Λ-algebra which is identity on the tangent space is an isomorphism. ∎

Corollary 1.5.5. *Assume given $\mathcal{F} \xrightarrow{f} \mathcal{D} \xleftarrow{g} \mathcal{G}$ with $\mathcal{F}, \mathcal{G}$ pro-representable and f, g formally smooth. Assume also that $\mathcal{D}$ has a tangent space. Then one of the pro-representing rings F, G is a formal power series ring over the other one.*

Proof. The tangent space maps $T\mathcal{F} \twoheadrightarrow T\mathcal{D}$ and $T\mathcal{G} \twoheadrightarrow T\mathcal{D}$ are both surjective by formal smoothness. Hence there is either a surjection $T\mathcal{F} \to T\mathcal{G}$ or a surjection $T\mathcal{G} \to T\mathcal{F}$ of k-vector spaces which commutes with the projections to $T\mathcal{D}$. The statement follows from parts 1 and 2 of the theorem. ∎

Corollary 1.5.6. *(Versal property of the hull.) Assume that a functor $\mathcal{D}$ has a hull $\mathcal{G} = \mathrm{Hom}_\Lambda(G, -)$, and let $f : \mathcal{F} \to \mathcal{D}$ be formally smooth with $\mathcal{F} = \mathrm{Hom}_\Lambda(F, -)$. Then*

$$F \;\cong\; G[[t_1, ..., t_n]], \quad n = \dim_k T\mathcal{F} - \dim_k T\mathcal{D}\,,$$

Proof. Since $\mathcal{D}$ has a tangent space and $T\mathcal{G} \cong T\mathcal{D}$ (by definition of a hull), there is a unique map $t : T\mathcal{F} \to T\mathcal{G}$ which lies above $\mathcal{D}$, namely the one induced by f on tangent spaces. ∎

Remark. The corollary often allows to determine a hull G of $\mathcal{D}$, when given a formally smooth map $\mathrm{Hom}_\Lambda(F, -) \to \mathcal{D}$. Indeed, $F \cong G[[t_1, ..., t_n]]$ with $n = \dim T\mathcal{F} - \dim T\mathcal{D}$. So, if one finds a ring G' for which $F \cong G'[[s_1, ..., s_n]]$, then G' is isomorphic to the hull G of $\mathcal{D}$, by the following "cancellation theorem for complete local rings", due to A. J. de Jong.

Proposition 1.5.7. *If $F, G \in \widehat{Art}_\Lambda$ are complete Noetherian local Λ-algebras with an augmentation such that $F[[t]] \cong G[[t]]$, then $F \cong G$.*

Proof. [17], Lemma 4.7. ∎

1.6 Quotients by groups

One often obtains non-pro-representable functors which, nevertheless, possess a hull by taking quotients of pro-representable functors. One can do it either by taking quotients by one group of automorphisms or by taking an action of a formal group instead. The latter way is the one which mostly occurs in practice. This and the next section describe the respective properties of these constructions. In the constant group case we

give necessary and sufficient conditions for a functor which has a hull to be represented as such a quotient (1.6.3). In the formal group case we conjecture the corresponding result (1.7.8).

Definition 1.6.1. Let $\mathcal{F} = \mathrm{Hom}_\Lambda(F, -)$ and let $\Gamma \subset \mathrm{Aut}_\Lambda(F)$ be a subgroup. Then Γ acts on $\mathcal{F}(A)$ for all A by composing a homomorphism $F \to A$ with an element of Γ. Define the *quotient functor* $\mathcal{F}/\Gamma$ by letting $A \mapsto \mathcal{F}(A)/\Gamma$.

Remark. We have let $\Gamma \subset \mathrm{Aut}_\Lambda(F)$ act on $\mathcal{F}(A)$ for all A by composition. Equivalently, one can let an abstract group Γ act on $\mathcal{F}(A)$ for all A, in such a way that for $A \to B$, the maps $\mathcal{F}(A) \to \mathcal{F}(B)$ are Γ-equivariant.

Theorem 1.6.2. *Let $\mathcal{F} = \mathrm{Hom}_\Lambda(F, -)$ and $\Gamma \subset \mathrm{Aut}_\Lambda(F)$. Denote by $\mathcal{D} = \mathcal{F}/\Gamma$ the quotient functor.*

1. *The quotient map $q : \mathcal{F} \to \mathcal{D}$ is formally smooth.*
2. *$\mathcal{D}$ has the property that $\mathcal{D}(A \times_B C) \twoheadrightarrow \mathcal{D}(A) \times_{\mathcal{D}(B)} \mathcal{D}(C)$ for all $A \to B \leftarrow C$.*
3. *$\mathcal{D}$ has a hull if and only if*

$$\Gamma \subset \ker\Big(\mathrm{Aut}_\Lambda(F) \to \mathrm{Aut}_\Lambda(F/m_F^2)\Big) ,$$

   in other words, if Γ acts trivially on the tangent space of F.

4. *$\mathcal{D}$ is pro-representable if and only if $\Gamma = \{1\}$.*

Proof. **1.** Let $\pi : A \twoheadrightarrow B$. We have to show that

$$\mathcal{F}(A) \twoheadrightarrow \mathcal{F}(B) \times_{\mathcal{D}(B)} \mathcal{D}(A) .$$

Take $a \in \mathcal{D}(A)$ and $\tilde{b} \in \mathcal{F}(B)$ such that $\pi(a) = q(\tilde{b})$ in $\mathcal{D}(B)$. Choose a representative $\tilde{a} \in \mathcal{F}(A)$ of a. If $\pi(\tilde{a}) = \tilde{b}$, then we are done. In any case,

$$g \cdot \pi(\tilde{a}) = \tilde{b}$$

for some $g \in \Gamma$. Then $g \cdot \tilde{a}$ is the required lift.
2. Let $\pi : A \to B$ and $\rho : C \to B$ in Art_Λ. Let $a \in \mathcal{D}(A)$ and $c \in \mathcal{D}(C)$ be such that $\pi(a) = \rho(c)$ in $\mathcal{D}(B)$. Choose representatives $\tilde{a} \in \mathcal{F}(A)$ and $\tilde{c} \in \mathcal{F}(C)$ of a and c respectively. The elements $\pi(\tilde{a})$ and $\rho(\tilde{c})$ in $\mathcal{F}(B)$ map to the same element in $\mathcal{D}(B)$, hence there is a $g \in \Gamma$ such that

$$g \cdot \pi(\tilde{a}) = \rho(\tilde{c}) .$$

Replace $\tilde{a}$ by $g \cdot \tilde{a}$. Then $\tilde{a}$ still maps to $a \in \mathcal{D}(A)$, but now we have $\pi(\tilde{a}) = \rho(\tilde{c})$. Since $\mathcal{F}$ commutes with fibre products, there is $\tilde{r} \in \mathcal{F}(A \times_B C)$ which projects to $\tilde{a} \in \mathcal{F}(A)$ and $\tilde{c} \in \mathcal{F}(C)$. Then the image r of $\tilde{r}$ in $\mathcal{D}(A \times_B C)$ is the required lift of (a, c).

3. The "if" part is clear: using part 2. and Schlessinger's criterion, it suffices to prove that $\mathcal{D}$ has a tangent space. But $\mathcal{F}$ has a tangent space and $\mathcal{F}(k[V]) \to \mathcal{D}(k[V])$ is bijective for all k-vector spaces V by our assumption on Γ. Hence $\mathcal{D}$ has a tangent space as well.

For the converse, assume that the action of Γ on TF is non-trivial but the quotient $\mathcal{D} = \mathcal{F}/\Gamma$ has a hull. In particular $\mathcal{D}$ has a tangent space. Let $V = T\mathcal{F} = \mathcal{F}(k[\epsilon])$. Let $k[\epsilon_1, \epsilon_2]$ denote the ring $k[t_1, t_2]/(t_1^2, t_2^2, t_1 t_2)$ and consider the map

$$\pi : \mathcal{D}(k[\epsilon_1, \epsilon_2]) \longrightarrow \mathcal{D}(k[\epsilon]) \times \mathcal{D}(k[\epsilon]).$$

whose components π_1 and π_2 are the natural projections. By assumption $\mathcal{D}$ has a tangent space, so π is a bijection. However,

$$\mathcal{D}(k[\epsilon_1, \epsilon_2]) = \mathcal{F}(k[\epsilon_1, \epsilon_2]/\Gamma = (V \oplus V)/\Gamma \ ,$$

and

$$\mathcal{D}(k[\epsilon]) \times \mathcal{D}(k[\epsilon]) = (V/\Gamma) \times (V/\Gamma) \ .$$

Moreover, the action of Γ on $\mathcal{F}(k[\epsilon_1, \epsilon_2]) = V \oplus V$ is diagonal,

$$g \cdot (v_1, v_2) = (g \cdot v_1, g \cdot v_2), \qquad v_1, v_2 \in V \ , g \in \Gamma \ ,$$

by compatibility of the action with the two inclusions $k[\epsilon] \hookrightarrow k[\epsilon_1, \epsilon_2]$. As we have assumed that the action of G on V is non-trivial, there are $v_1 \neq v_2 \in V$ such that $g \cdot v_1 = v_2$ for some $g \in \Gamma$. Then

$$h \cdot (v_1, v_1) = (h \cdot v_1, h \cdot v_1) \neq (v_1, v_2)$$

for any $h \in \Gamma$. Hence (v_1, v_1) and (v_1, v_2) give two *distinct* elements of $\mathcal{D}(k[\epsilon_1, \epsilon_2])$. However $\pi_1(v_1, v_2) = \pi_2(v_1, v_2)$ as elements of $\mathcal{D}(k[\epsilon]) \times \mathcal{D}(k[\epsilon])$. Hence π is not injective, a contradiction.

4. If $\Gamma = \{1\}$, then $\mathcal{D} = \mathcal{F}$ is pro-representable. Conversely, assume $\mathcal{D}$ is pro-representable. Since, in particular, $\mathcal{D}$ has a hull, $\Gamma \subset \ker(\mathrm{Aut}_\Lambda(F) \to \mathrm{Aut}_\Lambda(F/m_F^2))$ by part 3. of the theorem. Hence $\mathcal{F} \to \mathcal{D}$ is identity on the tangent spaces. Since it is also formally smooth, $\mathcal{F} = \mathcal{D}$ for example by uniqueness of the hull. ∎

Theorem 1.6.3. *Let $\mathcal{D} : Art_\Lambda \to Sets$. The following conditions are equivalent.*

1. *$\mathcal{D}$ possesses a hull and $\mathcal{D}(A \times_B C) \twoheadrightarrow \mathcal{D}(A) \times_{\mathcal{D}(B)} \mathcal{D}(C)$ for all $A \to B \leftarrow C$ (not only in case $C \twoheadrightarrow B$).*

2. *There exists a pro-representable functor $\mathcal{F} = \mathrm{Hom}_\Lambda(F, -)$ and a subgroup*

$$\Gamma \subset \ker\Big(\mathrm{Aut}_\Lambda(F) \to \mathrm{Aut}_\Lambda(F/m_F^2)\Big)$$

such that $\mathcal{D} \cong \mathcal{F}/\Gamma$.

Proof. $2 \Rightarrow 1$ is a part of Theorem 1.6.2. Now we prove $1 \Rightarrow 2$.

Let $\mathcal{F} \cong \mathrm{Hom}_\Lambda(F, -)$ be a hull of $\mathcal{D}$ and $q : \mathcal{F} \to \mathcal{D}$ the defining map. Let $\Gamma \subset \mathrm{Aut}_\Lambda(F)$ consist of those automorphisms g which, considered as elements of $\mathrm{Aut}(\mathcal{F})$ satisfy $qg = q$, as natural transformations. Since q is identity on tangent spaces, $\Gamma \subset \ker\left(\mathrm{Aut}_\Lambda(F) \to \mathrm{Aut}_\Lambda(F/m_F^2)\right)$ as required. It suffices to prove that $\mathcal{D} \cong \mathcal{F}/\Gamma$. Clearly q factors through $\mathcal{F}/\Gamma$ and

$$\mathcal{F}(A)/\Gamma \to \mathcal{D}(A)$$

is surjective for all $A \in Art_\Lambda$, since $\mathcal{F}(A) \twoheadrightarrow \mathcal{D}(A)$ by formal smoothness. To prove injectivity, assume $x, y \in \mathcal{F}(A)$ are such that $q(x) = q(y) \in \mathcal{D}(A)$. We have to prove that there is $g \in \Gamma$ for which $g \cdot x = y$.

Consider x and y as homomorphisms $F \to A$. We first want to reduce to the case that x, y are surjective. Let $A' \subset A$ be the Λ-subalgebra genereated by $\mathrm{Im}\, x$ and $\mathrm{Im}\, y$. Then both x and y factor via A',

$$x, y : F \longrightarrow A' \hookrightarrow A\,.$$

In other words $x, y \in \mathcal{F}(A)$ lie in the image of $\mathcal{F}(A') \hookrightarrow \mathcal{F}(A)$. Let $x', y' \in \mathcal{F}(A')$ be the same homomorphisms, considered as elements of $\mathcal{F}(A')$. We claim that $q(x') = q(y') \in \mathcal{D}(A')$.

We know that $q(x')$ and $q(y')$ have the same image in $\mathcal{D}(A)$. By the second assumption on $\mathcal{D}$, the map

$$\mathcal{D}(A') = \mathcal{D}(A' \times_A A') \to \mathcal{D}(A') \times_{\mathcal{D}(A)} \mathcal{D}(A')$$

is surjective. Equivalently, $\mathcal{D}(A') \hookrightarrow \mathcal{D}(A)$. So $\mathcal{D}$ takes injections to injections. Thus $q(x') = q(y')$. If we can find a $g \in \Gamma$ for which $g \cdot x' = y'$, then $g \cdot x = y$ as required. So we can replace A by A', in other words assume that A is generated by $\mathrm{Im}\, x$ and $\mathrm{Im}\, y$ as a Λ-algebra.

We claim that in this case both x and y have to be surjective.

Indeed, let $B = \mathrm{Im}(x)$ and $C = \mathrm{Im}(y)$. As A is generated by B and C as a Λ-algebra, the cotangent space $V = m_A/(m_A^2 + m_\Lambda A)$ is generated, as a vector space, by $m_B V$ and $m_C V$. Thus, if we show that $m_B V = m_C V$, then it follows that x, y are surjective on cotangent spaces, hence surjective (Remark 1.2.3).

Consider the projection $A \to A/m_A^2$, composed with x and y:

$$F \xrightarrow{x,y} A \twoheadrightarrow A/m_A^2\,.$$

The compositions $\bar{x}$ and $\bar{y}$ define elements $\bar{x}, \bar{y} \in \mathcal{F}(A/m_A^2)$. Since $q(\bar{x}) = q(\bar{y})$, and $q : \mathcal{F} \to \mathcal{D}$ is a bijection on the rings of the form $k[V]$ (such as A/m_A^2), it follows that $\bar{x} = \bar{y}$. Hence $m_B V = m_C V$ and x, y are both surjective.

In summary, we have surjections $x, y : F \to A$ and $q(x) = q(y) \in \mathcal{D}(A)$ if x, y are considered as elements of $\mathcal{F}(A)$. We have to prove that there is a $g \in \Gamma$ for which $g \cdot x = y$.

By the lemma below, there exists a homomorphism $g: F \to F$ such that the corresponding natural transformation $\alpha: \mathcal{F} \to \mathcal{F}$ commutes with q and such that $xg = y$. Since $q\alpha = q$, it follows that g is identity on the tangent space of F. In particular, it is an automorphism of F and $g \in \Gamma$. Also $g \cdot x = y$, as required. ∎

Lemma 1.6.4. *Let $q : \mathcal{F} \to \mathcal{D}$ be formally smooth with $\mathcal{F} \cong \mathrm{Hom}_\Lambda(F, -)$ pro-representable. Let $x, y \in \mathcal{F}(A)$ satisfy $q(x) = q(y)$ and assume that y is surjective, if considered as a homomorphism $F \to A$. Then there exists a natural transformation $\alpha: \mathcal{F} \to \mathcal{F}$ for which*

$$\begin{array}{ccc} \mathcal{F} & \xrightarrow{\alpha} & \mathcal{F} \\ & {\scriptstyle q}\searrow \quad \swarrow{\scriptstyle q} & \\ & \mathcal{D} & \end{array}$$

commutes and such that $\alpha(x) = y$.

Proof. Consider the following commutative diagram:

$$\begin{array}{ccc} \mathcal{F}(F) & \xrightarrow{q} & \mathcal{D}(F) \ni q \\ {\scriptstyle \mathcal{F}(x)}\downarrow & & \downarrow{\scriptstyle \mathcal{F}(x)} \\ y \in \mathcal{F}(A) & \xrightarrow{q} & \mathcal{D}(A) \end{array} .$$

Here q is seen both as a natural transformation and as an element of $\mathcal{D}(F)$. As x is surjective and $\mathcal{F} \to \mathcal{D}$ is formally smooth, there exists a $g \in \mathcal{F}(F)$ lifting (q, y) in the above diagram.

We claim that $g \in \mathrm{Hom}_\Lambda(F, F)$ is a homomorphism which gives the required natural transformation α. Firstly, $q(g) = q$ is the above diagram implies that $q\alpha = q$ as natural transformations. Secondly, $\mathcal{F}(x)(g) = y$ says precisely that $\alpha(x) = y$. ∎

1.7 Quotients by formal groups

Definition 1.7.1. Let $\mathcal{G}$ be a group functor $Art_\Lambda \to Groups$ and $\mathcal{F}: Art_\Lambda \to Sets$. An *action of $\mathcal{G}$ on $\mathcal{F}$* consists of group actions of $\mathcal{G}(A)$ on $\mathcal{F}(A)$ for all $A \in Art_\Lambda$, functorial in A. Recall also that a *formal group* is a formally smooth pro-representable group functor.

Theorem 1.7.2. *Let $\mathcal{F}$ be a pro-representable functor and $\mathcal{G}$ a formal group which acts on $\mathcal{F}$. Then $\mathcal{D} = \mathcal{F}/\mathcal{G}$, defined by $A \mapsto \mathcal{F}(A)/\mathcal{G}(A)$, has a hull.*

Proof. For $A, B \in Art_\Lambda$, the natural maps

$$\mathcal{F}(A \times_k B) \to \mathcal{F}(A) \times \mathcal{F}(B), \quad \mathcal{G}(A \times_k B) \to \mathcal{G}(A) \times \mathcal{G}(B)$$

are isomorphisms, since $\mathcal{F}, \mathcal{G}$ are pro-representable. Hence

$$\mathcal{F}(A \times_k B)/\mathcal{G}(A \times_k B) \longrightarrow \mathcal{F}(A)/\mathcal{G}(A) \times \mathcal{F}(B)/\mathcal{G}(B)$$

is bijective for any A, B. In particular, $\mathcal{F}/\mathcal{G}$ has a tangent space.

Next, we show that the natural map $\mathcal{F} \to \mathcal{F}/\mathcal{G}$ is formally smooth, so

$$\mathcal{F}(A) \twoheadrightarrow \mathcal{F}(B) \times_{\mathcal{F}(B)/\mathcal{G}(B)} \mathcal{F}(A)/\mathcal{G}(A)\,.$$

whenever $\pi : A \twoheadrightarrow B$. Take an element in the right-hand side, represented by a pair $\xi \in \mathcal{F}(B)$, $\eta \in \mathcal{F}(A)$ such that $\pi(\eta) = g_B \cdot \xi$ for some $g_B \in \mathcal{G}(B)$. Since $\mathcal{G}$ is formally smooth, $\mathcal{G}(A) \twoheadrightarrow \mathcal{G}(B)$, so g_B can be lifted to an element $g_A \in \mathcal{G}(A)$. Then $g_A^{-1} \cdot \eta \in \mathcal{F}(A)$ is the required lift.

Hence $\mathcal{D}$ has a hull (cf. definition 1.4). ∎

Remark 1.7.3. From this proof it also follows that $\mathcal{D} = \mathcal{F}/\mathcal{G}$ has a universal obstruction space (Theorem 1.3.8).

Remark. Note that the pro-representability of $\mathcal{G}$ is used *only* to prove that $\mathcal{F}/\mathcal{G}$ has a tangent space and not for the formal smoothness of the quotient map.

Theorem 1.7.4. *Let $\mathcal{G} : Art_\Lambda \to Groups$ be an formally smooth group functor. Assume that $\mathcal{G}$ acts on a pro-representable functor $\mathcal{F}$ in such a way that for every k-vector space V, $\mathcal{G}(k[V])$ acts trivially on $\mathcal{F}(k[V])$. Then $\mathcal{F}/\mathcal{G}$ has a hull, namely $\mathcal{F}$ with the natural quotient map.*

Proof. By the remark above, formal smoothness of $\mathcal{G}$ implies that the quotient map is formally smooth. Since $\mathcal{F}(k[V]) \to (\mathcal{F}/G)(k[V])$ is bijective for all V, the quotient functor has a tangent space and the quotient map is bijective on the tangent spaces. Hence $\mathcal{F}$ is the hull of $\mathcal{F}/\mathcal{G}$. ∎

Remark. Let $\mathcal{G} : Art_\Lambda \to Groups$ be as in the above theorem and let $\Gamma = \mathcal{G}(k)$. For any $A \in Art_\Lambda$ there is a surjective group homomorphism $\mathcal{G}(\eta_A) : \mathcal{G}(A) \to \Gamma$ induced by the augmentation $\eta : A \to k$ (see Definition 1.1.1). Moreover, for any $f : A \to B$ the induced homomorphism $\mathcal{G}(f) : \mathcal{G}(A) \to \mathcal{G}(B)$ commutes with these projections to Γ. So we have a natural transformation of group functors

$$\mathcal{G} \longrightarrow \underline{\Gamma}$$

where $\underline{\Gamma}$ denotes the constant group functor with value Γ on every $A \in Art_\Lambda$ (and taking every morphism in Art_Λ to the identity on Γ). So we get an exact sequence

$$1 \longrightarrow \mathcal{G}^{formal} \longrightarrow \mathcal{G} \longrightarrow \underline{\Gamma} \longrightarrow 1$$

of group functors on Art_Λ, where $\mathcal{G}^{formal}$ denotes the kernel. By definition $\mathcal{G}^{formal}(k)$ consists of one element. So $\mathcal{G}^{formal}$ is close to being a formal group, except that it is not necessary pro-representable. Theorem 1.6.3 characterizes in general quotients by constant groups, but it seems difficult to find to corresponding result for (even pro-representable) formally smooth group functors. Nevertheless, the following conjecture seems feasible.

Conjecture 1.7.5. *Let $\mathcal{D}$ be a functor which has a hull $\mathcal{F}$. Then there exists a formally smooth $\mathcal{G} : Art_\Lambda \to Groups$ (as in Theorem 1.7.4) and an action of $\mathcal{G}$ on $\mathcal{F}$ such that $\mathcal{D} \cong \mathcal{F}/\mathcal{G}$.*

Remark 1.7.6. One might also conjecture that $\mathcal{G}$ can be chosen to be an extension of a formal group by a constant group.

Remark 1.7.7. Let $\mathcal{F}$ be a pro-representable functor and let $\mathcal{G}$ act on $\mathcal{F}$. Assume for simplicity that the action on $\mathcal{F}(k[V])$ is trivial for all V. Let $\mathcal{D} = \mathcal{F}/\mathcal{G}$ and consider the following properties of $\mathcal{D}$:

(1) $\mathcal{D}(A \times_B C) \twoheadrightarrow \mathcal{D}(A) \times_{\mathcal{D}(B)} \mathcal{D}(C)$ for all $A \to B \twoheadleftarrow C$.

(2) $\mathcal{D}(A \times_B C) \xrightarrow{\cong} \mathcal{D}(A) \times_{\mathcal{D}(B)} \mathcal{D}(C)$ for $B = k$, all A, C.

(3) $\mathcal{D}(A \times_B C) \twoheadrightarrow \mathcal{D}(A) \times_{\mathcal{D}(B)} \mathcal{D}(C)$ for all $A \to B \leftarrow C$.

In any case, $\mathcal{D}$ has property (1) by the above theorem. If $\mathcal{G}$ is a constant group functor, then $\mathcal{G}$ satisfies (3) but not (2), unless it is trivial (take $A = C = F$ and $B = k$). If $\mathcal{G}$ is a formal group, then $\mathcal{D}$ satisfies (2) but seemingly never (3), unless again it is trivial. In this respect, the two quotient constructions are complementary to each other. Hence one might conjecture a criterion for quotients by formal groups analogous to Theorem 1.6.3.

Conjecture 1.7.8. *Let $\mathcal{D}$ be a functor which has a hull $\mathcal{F}$. Assume that $\mathcal{D}$ commutes with products,*

$$\mathcal{D}(A \times_k B) \xrightarrow{\sim} \mathcal{D}(A) \times \mathcal{D}(B) .$$

Then $\mathcal{D} \cong \mathcal{F}/\mathcal{G}$ for some formal group $\mathcal{G}$ acting on $\mathcal{F}$.

2 Cohomology of R-R bimodules

It is typical, that tangent spaces and obstruction spaces to moduli functors are certain cohomology groups. For example, the tangent space to the deformation space of a regular variety X/k is $\mathrm{H}^1(X, \tau_X)$ and the obstruction lies in $\mathrm{H}^2(X, \tau_X)$, where τ_X is the tangent sheaf. Deforming a morphism $f : X \to Y$ of (say, regular) varieties gives $\mathrm{H}^0(X, f^*\tau_Y)$ and $\mathrm{H}^1(X, f^*\tau_Y)$ respectively. Mazur's deformation theory of a Galois representation $\rho : G \to \mathrm{Aut}(V)$ gives $\mathrm{H}^1(G, \mathrm{End}(V))$ as the tangent space and $\mathrm{H}^2(G, \mathrm{End}(V))$ as an obstruction space, cf. [22], §1.2, §1.6. Illusie [12] has shown that in general the tangent space of a functor can be identified with a certain Ext^1 and the obstructions lie in Ext^2.

Our primary interest lies in deformations of p-divisible group with an $\mathcal{O}$-action as well as those of ring representations and R-stable filtrations on an R-module. In all three cases the corresponding tangent and obstruction spaces turn out to be the Hochschild cohomology groups.

In Section 2.1 we recall the basic properties of these cohomology groups and prove that $\mathrm{H}^1(R\text{-}R\,, \mathrm{End}_A(R)) = 0$ if the ring R is a finite free A-module (2.1.12). The corollaries (2.1.13, 2.1.14) are used later to show that the deformation functor of a projective module has a trivial tangent space (2.2.5).

Section 2.2 is devoted to the deformation functor $\mathcal{D}\mathrm{ef}(\bar{\rho})$ of a ring representation $\bar{\rho} : R \to \mathrm{End}(V)$ on the category Art_Λ. This basically follows the work of Mazur on deformations of group representations [22]. The deformation functor is pro-representable under the appropriate finiteness condition on R and the tangent space (respectively an obstruction space) is the Hochschild cohomology group $\mathrm{H}^1(R\text{-}R\,, \mathrm{End}(V))$ (respectively $\mathrm{H}^2(R\text{-}R\,, \mathrm{End}(V))$). In case $R = \Lambda[G]$, the group algebra of a group G, we recover Mazur's results. In fact it is easy to see that the Hochschild cohomology groups are isomorphic with the usual group cohomology in this case.

In Section 2.3 we study the case of filtrations. The pro-representability result 2.3.2 serves for us primarily as a tool to study the deformations of p-divisible groups later (Chapter 4).

As in the previous chapter, k is an arbitrary field and Λ is a complete Noetherian local ring given with an augmentation $\eta : \Lambda/m_\Lambda \cong k$. Throughout this chapter R denotes a Λ-algebra which is not necessarily commutative.

2.1 Hochschild cohomology

Throughout this section A is a commutative ring and R a not necessarily commutative A-algebra which is finite and free as an A-module. In particular $A \subset R$. Note that $ar = ra$ for all $a \in A \subset R$ and $r \in R$ (by definition of an A-algebra, see [14], p.44). We recall some basic results on the Hochschild cohomology of R-R bimodules. See [14], Section 6.11 for details. We also prove that $\mathrm{H}^1(R\text{-}R\,, \mathrm{End}_A(R)) = 0$ and deduce some corollaries, which are going to be used later on.

Definition 2.1.1. An R-R bimodule is an abelian group M together with left and right actions of R (denoted $r \cdot m$ and $m \cdot r$) such that for all $r_1, r_2 \in R$, $m \in M$ and $a \in A$,

$$\begin{aligned} r_1 \cdot (m \cdot r_2) &= (r_1 \cdot m) \cdot r_2 \qquad \text{(actions commute)}, \\ a \cdot m &= m \cdot a \qquad\qquad\quad \text{(and coincide on } A). \end{aligned}$$

Example 2.1.2. An R-algebra homomorphism $R \to S$ gives an R-R bimodule structure on S via the left and the right multiplication ($r \cdot s = rs$, $s \cdot r = sr$). In particular, R itself can be considered an R-R bimodule.

Example 2.1.3. If M is a left R-module and N a right R-module, then $M \otimes_A N$ is in a natural way an R-R bimodule.

Example 2.1.4. If M, N are left R-modules, then $\mathrm{Hom}_A(M, N)$ is an R-R bimodule: let $r \cdot f$ and $f \cdot r$ to be $(r \cdot f)(x) = r \cdot f(x)$ and $(f \cdot r)(x) = f(r \cdot x)$. This applies notably to the endomorphism ring of a left R-module.

Definition 2.1.5. A *homomorphism* of R-R bimodules is a homomorphism as abelian groups commuting with both actions. An *exact sequence* is a chain of R-R bimodule homomorphisms which is exact as a sequence of abelian groups (or A-modules).

Remark 2.1.6. To give an R-R bimodule M is equivalent to giving an A-module M together with left R and R^{op} actions. This is equivalent to giving a left $R \otimes_A R^{\mathrm{op}}$ action on M. Hence there is an equivalence of categories

$$\{R\text{-}R \text{ bimodules}\} \;\sim\; \{\text{left } R \otimes_A R^{\mathrm{op}}\text{-modules}\}.$$

Definition 2.1.7. Given an R-R bimodule M, let

$$\mathrm{H}^0(R\text{-}R, M) = \{m \in M \mid r \cdot m = m \cdot r, \text{ all } r \in R\}$$

Note that this an A-submodule of M, although *not* in general an R-module.

Remark 2.1.8. If we let R to be an R-R bimodule via the left and the right multiplication, then for any R-R bimodule M we have a canonical isomorphism of A-modules

$$\mathrm{H}^0(R\text{-}R, M) = \mathrm{Hom}_{R\text{-}R}(R, M)$$

In particular (use Remark 2.1.6), the functor $\mathrm{H}^0(R\text{-}R, -)$ is left exact.

Definition 2.1.9. The right derived functors of $\mathrm{H}^0(R\text{-}R, -)$, denoted $\mathrm{H}^n(R\text{-}R, -)$, are called *Hochschild cohomology groups of R with values in M*.

Example 2.1.10. $A=\mathbf{Z}$, $R=\mathbf{Z}[G]$ with a finite group G. If M is a G-module, define an R-R bimodule structure on M by letting G to act naturally on the left and trivially on the right,

$$g\cdot m = {}^g m$$
$$m\cdot g = m$$

and extending by $\mathbf{Z}$-linearity. Then $H^0(R\text{-}R\,,M)$ becomes the usual 0-th cohomology group,

$$\mathrm{H}^0(R\text{-}R\,,M) = \{m\in M \mid {}^g m = m,\ \text{all } g\in G\} = M^G = \mathrm{H}^0(G,M)\,.$$

Consequently $\mathrm{H}^n(R\text{-}R\,,M)=\mathrm{H}^n(G,M)$.

Example 2.1.11. One can show that $\mathrm{H}^1(R\text{-}R\,,M)\cong \mathrm{Z}^1(R\text{-}R\,,M)/\mathrm{B}^1(R\text{-}R\,,M)$ with

$$\mathrm{Z}^1(R\text{-}R\,,M) = \{\alpha \in \mathrm{Hom}_A(R,M) \mid \alpha(r_1r_2) = r_1\cdot\alpha(r_2)+\alpha(r_1)\cdot r_2\}$$
$$\mathrm{B}^1(R\text{-}R\,,M) = \{\alpha_m \in \mathrm{Hom}_A(R,M) \mid \alpha_m(r) = r\cdot m - m\cdot r,\ \text{for some } m\in M\}\,.$$

Proposition 2.1.12. *Consider R as a left module over itself and define the R-R-bimodule structure on $\mathrm{End}_A(R)$ as in 2.1.4. Then*

$$\mathrm{H}^1(R\text{-}R\,,\mathrm{End}_A(R)) = 0\,.$$

Proof. An element $r\in R$ acts on R via left multiplication. Thus it defines an element in $\mathrm{End}_A(R)$ which we denote by r_l. Let $\alpha\in \mathrm{Z}^1(R\text{-}R\,,\mathrm{End}_A(R))$, so

$$\alpha : R \longrightarrow \mathrm{End}_A(R)$$

is an A-module homomorphism, such that

$$\alpha(rs) = r_l\alpha(s)+\alpha(r)s_l\,.$$

We claim that $\alpha\in \mathrm{B}^1(R\text{-}R\,,\mathrm{End}_A(R))$, so $\alpha=\alpha_\xi$, the coboundary defined by an element $\xi\in\mathrm{End}_A(R)$. Here ξ can be explictly given by

$$\xi(r) = -(\alpha(r))(1)\,,$$

the value of the endomorphism $\alpha(r)\in\mathrm{End}_A(R)$ on $1\in R$. Indeed, for all $r,s\in R$,

$$\begin{aligned}
\alpha_\xi(r)(s) &= (r_l\xi - \xi r_l)(s)\\
&= r_l(\xi(s)) - \xi(r_l(s))\\
&= -r_l(\alpha(s)(1)) + \alpha(rs)(1)\\
&= -r_l(\alpha(s)(1)) + (r_l\alpha(s))(1) + (\alpha(r)s_l)(1)\\
&= \alpha(r)(s)\,.
\end{aligned}$$

Hence $\mathrm{H}^1(R\text{-}R\,,\mathrm{End}_A(R))=0$. ∎

Corollary 2.1.13. *If M is a projective left $R \otimes_A R^{\mathrm{op}}$-module considered as an R-R bimodule, then* $\mathrm{H}^1(R\text{-}R, M) = 0$.

Proof. Since $R \otimes_A R^{\mathrm{op}} \cong \mathrm{End}_A(R)$ as an R-R bimodule, this statement is a reformulation of the above proposition in case M is free of rank 1. For an arbitrary projective M, it follows from the fact that M is a direct summand of a direct sum of free rank 1 modules and the fact that cohomology commutes with direct sums.

Corollary 2.1.14. *If M is a projective left R-module and N a projective right R-module, then* $\mathrm{H}^1(R\text{-}R, M \otimes_A N) = 0$.

2.2 Deforming ring representations

Definition 2.2.1. Let $A \in Art_\Lambda$ and let $\mathcal{V}$ be a finite free A-module. A representation of R on $\mathcal{V}$ is a Λ-algebra homomorphism

$$\wp : R \longrightarrow \mathrm{End}_A(\mathcal{V}) .$$

If $\pi : A \to B$ is a homomorphism in Art_Λ, then $\wp \otimes_A B$ is a representation of R on the B-module $\mathcal{V} \otimes_A B$.

Definition 2.2.2. A representation ρ of R on a finite-dimensional k-vector space V (i.e. in case $A = k$) is called *residual*. Define a *deformation of ρ to $A \in Art_\Lambda$* to be a representation $\wp$ on an A-module $\mathcal{V}$ given together with an isomorphism $i : \wp \otimes_A k \cong \rho$.

Definition 2.2.3. Let $\rho : R \to \mathrm{End}(V)$ be a residual representation. Define the *deformation functor of ρ*,

$$\begin{array}{rccl} \mathcal{D}\mathrm{ef}(\rho) : Art_\Lambda & \longrightarrow & Sets \\ A & \longmapsto & \{\text{deformations of } \rho \text{ to } A\}/\cong \end{array}$$

A representation $\wp : R \to \mathrm{End}_A(\mathcal{V})$ gives an R-R bimodule structure on $\mathrm{End}_A(\mathcal{V})$ via the left and the right multiplication (cf. 2.1.2). The associated Hochschild cohomology groups are responsible for the behaviour of the deformation functor:

Theorem 2.2.4. *Assume R is finitely presented over Λ. Let $\rho : R \to \mathrm{End}(V)$ be a residual representation. Then*

1. $\mathrm{H}^2(R\text{-}R, \mathrm{End}(V))$ *is an obstruction space for* $\mathcal{D}\mathrm{ef}(\rho)$.
2. $\mathrm{H}^1(R\text{-}R, \mathrm{End}(V))$ *is the tangent space of* $\mathcal{D}\mathrm{ef}(\rho)$.
3. $\mathcal{D}\mathrm{ef}(\rho)$ *has a hull.*

Proof. 1. Let $A \twoheadrightarrow A'$ be a surjection with kernel I, such that $m_A I = 0$ Take

$$\wp' : R \longrightarrow \mathrm{End}_{A'}(\mathcal{V}') \,,$$

a deformation of ρ to A'. Choose a basis $v'_1, \ldots, v'_n$ of $\mathcal{V}'/A'$ and let

$$V = Av_1 + \ldots + Av_n$$

be a finite free A-module (so $\mathcal{V} \otimes_A A' = \mathcal{V}'$). We try to lift ρ' to a Λ-homomorphism $\rho : R \to \mathrm{End}(\mathcal{V})$. Denote for every $r \in R$,

$$\alpha'_r = \rho'(r) \in \mathrm{End}(V') = \mathrm{Mat}_{n\times n}(A') \,.$$

Choose a basis $\{r_i\}$ for R over Λ and lift each of the α'_{r_i} to an element $\alpha_{r_i} \in \mathrm{End}(\mathcal{V})$. Defining α_r for all $r \in R$ by linearity results in the map of Λ-modules

$$R \xrightarrow{\alpha} \mathrm{End}(\mathcal{V}) \,.$$

To measure the extent to which α fails to be a ring homomorphism, let

$$\beta_{r,s} = \alpha_{rs} - \alpha_r \alpha_s \,.$$

When all $\beta_{r,s} = 0$, then $\rho(r) = \alpha_r$ is the required deformation. In general, however,

$$\beta_{r,s} = \ker(\mathrm{End}(\mathcal{V}) \twoheadrightarrow \mathrm{End}(\mathcal{V}')) \,.$$

By assumption, the kernel I of $A \twoheadrightarrow A'$ can be considered as a k-vector space, so

$$\beta_{r,s} \in \mathrm{End}(V) \otimes_k I \,.$$

Also, from

$$\begin{aligned} \beta_{rs,t} &= \alpha_{rst} - \alpha_{rs}\alpha_t = \alpha_{rst} - (\alpha_r\alpha_s + \beta_{r,s})\alpha_t \\ \beta_{r,st} &= \alpha_{rst} - \alpha_r\alpha_{st} = \alpha_{rst} - \alpha_r(\alpha_s\alpha_t + \beta_{s,t}) \end{aligned}$$

it follows that

$$\beta_{rs,t} - \beta_{r,st} = \alpha_r\beta_{s,t} - \beta_{r,s}\alpha_t = (\bar\rho(r)\otimes 1)\beta_{s,t} - \beta_{r,s}(\bar\rho(t)\otimes 1) \,.$$

Hence β is an element of $\mathrm{Z}^2(R\text{-}R\,, \mathrm{End}(V)) \otimes_k I$. Replacing α_{r_i} by different lifts $\tilde\alpha_{r_i}$ of α'_{r_i} changes $\beta_{r,s}$ by an element in $\mathrm{B}^2(R\text{-}R\,, \mathrm{End}(V)) \otimes_k I$,

$$\tilde\alpha_r = \alpha_r + m_r \quad \Rightarrow \quad \tilde\beta_{r,s} = \beta_{r,s} + \Big(m_{rs} - (\bar\rho(r)\otimes 1)m_s - m_r(\bar\rho(s)\otimes 1)\Big) \,.$$

Thus, the obstruction to deforming ρ' to A lies in $\mathrm{H}^2(R\text{-}R\,, \mathrm{End}(V)) \otimes_k I$. Since our construction is clearly functorial (Definition 1.3.4), the vector space $\mathrm{H}^2(R\text{-}R\,, \mathrm{End}(V))$ is an obstruction space for $\mathcal{D}\mathrm{ef}(\rho)$.

2. Let $A = k[I] \to k = A'$ for some k-vector space I. In this case there is a section $A' \to A$, so there is a canonical deformation $\wp = \rho \otimes_k k[I]$. It is given by $\alpha_r = \alpha'_r$. Any other deformation is given by

$$\tilde{\alpha}_r = \alpha_r + w_r, \quad w_r \in \mathrm{M}_n(k) \otimes_k I$$

The condition $\tilde{\alpha}_{rs} = \tilde{\alpha}_r \tilde{\alpha}_s$ yields (as in 2.)

$$m_{rs} = \rho(r) m_s + m_r \rho(s) \, .$$

Hence $m \in Z^1(R\text{-}R\,, \mathrm{End}(V)) \otimes_k I$. Moreover, $m^{(1)}$ and $m^{(2)}$ give isomorphic deformations if and only if there is a basis transformation $Q \in \mathrm{M}_n(I)$ which transforms one into the other. This implies that

$$m^{(2)}(r) = m^{(1)}(r) + (\rho(r)Q - Q\rho(r)),$$

i.e. $m^{(2)} - m^{(1)} \in B^1(R\text{-}R\,, \mathrm{End}(V)) \otimes_k I$. It follows that $\mathrm{H}^1(R\text{-}R\,, \mathrm{End}(V))$ is tangent space of the functor $\mathcal{D}\mathrm{ef}(\rho)$.

3. We have already shown that $\mathcal{D}\mathrm{ef}(\rho)$ has a tangent space. The idea is that one can rigidify $\mathcal{D}\mathrm{ef}(\rho)$ by fixing a basis of the module. This yields a pro-representable functor $\mathcal{R}$ of which $\mathcal{D}\mathrm{ef}(\rho)$ is a quotient by a $\widehat{GL}_n$-action. Choose a basis $\{\bar{v}_1, ..., \bar{v}_n\}$ of V and consider the finite free Λ-module

$$\mathcal{V}_\Lambda = \Lambda v_1 + \ldots + \Lambda v_n$$

with an identification $\mathcal{V}_\Lambda \otimes_\Lambda k = V$ given by $v_i \mapsto \bar{v}_i$. For $A \in Art_\Lambda$ let

$$\mathcal{R}(A) = \{\varphi \in \mathrm{Hom}(R, \mathrm{End}(\mathcal{V}_\Lambda \otimes_\Lambda A) \mid \varphi \otimes_A k = \rho\} \, .$$

Here Hom denotes homomorphisms of (non-commutative) Λ-algebras. This gives a functor $\mathcal{R} : Art_\Lambda \to Sets$. Let

$$\widehat{GL}_n(A) = \ker\Big(GL_n(A) \to GL_n(k)\Big)$$

This gives a pro-representable group functor $\widehat{GL}_n$, smooth on n^2 parameters. If we let $\widehat{GL}_n(A)$ act on $\mathrm{End}(\mathcal{V}_\Lambda \otimes_\Lambda A)$ by conjugation, then clearly $\mathcal{D}\mathrm{ef}(\rho) = \mathcal{R}/\widehat{GL}_n$. So, by theorem 1.7.2, it suffices to show that $\mathcal{R}$ is pro-representable. Let $\{x_1, ..., x_m\}$ be the set of generators of R over Λ. Then $\varphi \in \mathcal{R}(A)$ is determined by $\varphi(x_i) \in \mathrm{Mat}_{n\times n}(A)$. Here the isomorphism $\mathrm{End}(\mathcal{V}_\Lambda \otimes_\Lambda A) \cong \mathrm{Mat}_{n\times n}(A)$ is fixed by the choice of the v_i. In other words φ is determined by the coefficients $\alpha_{ijk} \in m_A$ of $\varphi(x_i)$ in the basis $\{v_j \otimes v_k^*\}$ of $\mathrm{End}(\mathcal{V})$. It follows that

$$\mathcal{R} \;\cong\; \mathrm{Hom}(\Lambda[[t_{ijk}]]/J, -)$$

where J is the ideal generated by the relations among the x_i's in R. Hence $\mathcal{R}$ is pro-representable and $\mathcal{D}\mathrm{ef}(\rho)$ has a hull. ∎

Corollary 2.2.5. *Assume that R is finite and free as a Λ-module. Let $\mathcal{V}_\Lambda$ be a projective R-module and $\mathcal{W}_\Lambda$ any R-module which is finite and free over Λ. Then*

$$\mathcal{V}_\Lambda \cong \mathcal{W}_\Lambda \quad \Longleftrightarrow \quad \mathcal{V}_\Lambda \otimes_\Lambda k \cong \mathcal{W}_\Lambda \otimes_\Lambda k \,.$$

Proof. The implication from left to right is trivial. Conversely, assume that $\mathcal{V}_\Lambda \otimes_\Lambda k \cong \mathcal{W}_\Lambda \otimes_\Lambda k$. Then $\mathcal{V}_\Lambda$ and $\mathcal{W}_\Lambda$ are two deformations of the same residual representation. Since $\mathcal{V}_\Lambda$ is R-projective, $V_k = \mathcal{V}_\Lambda \otimes_\Lambda k$ is projective over $R_k = R \otimes_\Lambda k$. By 2.1.13 we have

$$\mathrm{H}^1(R\text{-}R\,, \mathrm{End}(V_k)) \cong \mathrm{H}^1(R_k\text{-}R_k, \mathrm{End}(V_k)) = 0\,.$$

By the above theorem, the deformation functor $\mathcal{D}\mathrm{ef}(\rho : R_A \to \mathrm{End}(V_k))$ has trivial tangent space. It follows that every two deformations of V_k to $A \in Art_\Lambda$ are isomorphic. Thus $\mathcal{V}_\Lambda \cong \mathcal{W}_\Lambda$. ∎

2.3 Deforming filtrations on R-modules

Let $\Lambda \twoheadrightarrow k$ and R be as before. As the proof of Theorem 2.2.4 shows, one way to rigidify the deformation functor of a ring representation $\rho : R \to \mathrm{End}(V)$ is to fix a basis of liftings of V. As we will see in Section 4.4, in case R is a finite free Λ-module, another way is to represent ρ as a quotient representation of a "free representation of R". In this section we study deformations of an R-stable filtration, which are directly related to quotient representations.

The following defines such a deformation functor in general.

Notation. Let $\wp : R \to \mathrm{End}(\mathcal{M})$ be a fixed representation of R on a finite free Λ-module $\mathcal{M}$. Denote $M = \mathcal{M} \otimes_\Lambda k, \rho = \wp \otimes_\Lambda k$ and let

$$V \subset M$$

be an R-stable submodule, i.e. a subrepresentation of ρ.

Definition 2.3.1. For $A \in Art_\Lambda$ denote $\mathcal{M}_A = \mathcal{M} \otimes_\Lambda A$. Let

$$\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)(A) = \{\mathcal{V}_A \subset \mathcal{M}_A \mid \mathcal{V}_A \otimes_A k = V\}\,,$$

the set of direct A-submodules $\mathcal{V}_A$ deforming V in $\mathcal{M}$, such that $\mathcal{V}_A$ is R-stable. We call $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$ *the deformation functor of V in $\mathcal{M}$*. Note that this functor depends on the R-module structure of $\mathcal{M}$, rather than just on V and M.

In the following theorem we consider the k-vector space $\mathrm{Hom}_k(V, M/V)$ an R-R bimodule via 2.1.8.

Theorem 2.3.2. *Assume R is finitely generated over Λ. Then*

1. *$\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$ is pro-representable.*

2. *The tangent space of* $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V{\subset}M,R)$ *is* $\mathrm{H}^0(R\text{-}R\,,\mathrm{Hom}_k(V,M/V))$.

3. $\mathrm{H}^1(R\text{-}R\,,\mathrm{Hom}_k(V,M/V))$ *is an obstruction space for* $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V{\subset}M,R)$.

Proof. 1.

Let $\{e_1,...,e_n,f_1,...,f_m\}$ be a basis of $\mathcal{M}$ over Λ which reduces to bases of V and M/V. This also gives a basis $\{e_1^A,...,e_n^A,f_1^A,...,f_m^A\}$ of $\mathcal{M}_A$ for any $A\in Art_\Lambda$. It is easy to see that any filtration $\mathcal{V}_A\subset\mathcal{M}_A$ which deforms $V\subset M$ has a unique basis of the form

$$\begin{array}{rl} e_1^A & +\,u_{11}f_1^A+\cdots+u_{m1}f_m^A\\ e_2^A & +\,u_{12}f_1^A+\cdots+u_{m2}f_m^A\\ & \vdots\\ e_n^A & +\,u_{1n}f_1^A+\cdots+u_{mn}f_m^A \end{array} \tag{9}$$

with $u_{ij}\in m_A$. Incidentally, this shows that the functor $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V{\subset}M)$ of all (not necessary R-stable) deformations of V in $\mathcal{M}$ is pro-represented by $\Lambda[[t_{ij}]]$ with $1\le i\le n,1\le j\le m$. Clearly $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V{\subset}M,R)\subset\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V{\subset}M)$ is a subfunctor. To show that it is indeed pro-represented by a quotient of $\Lambda[[t_{ij}]]$, we describe explicitly the equations. This computation will be used in chapter 5.

Take $A\in Art_\Lambda$ and a filtration $\mathcal{V}_A\subset\mathcal{M}_A$, described by (9). We put the coefficients u_{ij} into an $n\times m$ matrix U. Thus the basis elements (9) make columns of the block matrix

$$\begin{pmatrix} I\\ U\end{pmatrix}$$

where I denotes the identity matrix ($n\times n$ in this case).

The action of an element $r\in R$ on $\mathcal{M}$ can be described by a block matrix

$$r\quad\mapsto\quad\begin{pmatrix} A_r & B_r\\ C_r & D_r\end{pmatrix}\in\mathrm{End}_\Lambda(\mathcal{M})$$

in the basis $\{e_1,...,e_n,f_1,...,f_m\}$. The condition that r maps the filtration $\mathcal{V}$ into itself is given by

$$\begin{pmatrix} A_r & B_r\\ C_r & D_r\end{pmatrix}\begin{pmatrix} I\\ U\end{pmatrix}=\begin{pmatrix} I\\ U\end{pmatrix}N,\qquad\text{for some } N\in\mathrm{Mat}_{n\times n}(A)$$

This gives two matrix equations, from which we eliminate N and get

$$UA_r+UB_rU-D_rU-C_r=0,\quad 1\le i\le k\,. \tag{10}$$

Note that this equation can be also written in a matrix form,

$$(U\ \ -I)\begin{pmatrix} A_r & B_r\\ C_r & D_r\end{pmatrix}\begin{pmatrix} I\\ U\end{pmatrix}=0\,. \tag{11}$$

Let $\{r_1,...,r_k\}$ be a set of generators of R as a Λ-algebra. Then the conditions (10) for $r=r_1,...,r_k$ are necessary and sufficient for the R-stability of $\mathcal{V}$. Replacing u_{ij} by indeterminants t_{ij} yields exactly the equations (nmk of them) which determine $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V\subset M,R)$. Hence this functor is pro-representable. The pro-representing ring is $\Lambda[[t_{ij}]]/J$ where J is the ideal generated by the above equations.

2. Let $A=k[\epsilon]$. Following the above reasoning, an R-stable filtration $\mathcal{V}_A\subset\mathcal{M}_A$ which deforms V is given by a matrix U for which the equations (10) hold. Since the entries of U lie in m_A and $m_A^2=0$, the term UB_iU vanishes. Also the fact that the original filtration V is R-stable implies $C_i=0$. So the equations read

$$UA_r-D_rU=0,\quad r\in R\,.$$

Write $U=\epsilon\bar{U}$ with $\bar{U}\in\mathrm{Mat}_{n\times m}(k)$. Then this equation can be re-written as

$$\bar{U}\cdot r-r\cdot\bar{U}=0,\quad r\in R\,.$$

Here $\bar{U}$ is considered as an element in $\mathrm{Hom}_k(V,M/V)$ and $r\cdot$ and $\cdot r$ denote the left and the right action of r on this vector space. This identifies the tangent space of $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V\subset M,R)$ with $\mathrm{H}^0(R\text{-}R\,,\mathrm{Hom}_k(V,M/V))$.

3. To simplify the notation, we let $\pi:A\twoheadrightarrow A'$ be a small extension, i.e. assume $\ker\pi\cong k$ as a Λ-module. Let $\mathcal{V}'\in\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V\subset M,R)(A')$ be an R-stable filtration of $\mathcal{M}_{A'}$. We try to deform it to an R-stable filtration of $\mathcal{M}_A$.

Let $\mathcal{V}$ be any filtration of $\mathcal{M}$ which deforms $\mathcal{V}'$. Denote by U and U' the matrices defining $\mathcal{V}$ and $\mathcal{V}'$. To measure the failure of $\mathcal{V}$ being R-stable, consider

$$UA_r+UB_rU-D_rU-C_r=\epsilon E_r\ \in\ \epsilon\cdot\mathrm{Mat}_{n\times m}(k)\,.$$

Here (ϵ) is the kernel of $A\twoheadrightarrow A'$. Consider again $\mathrm{Mat}_{n\times m}(k)=\mathrm{Hom}_k(V,M/V)$ an an R-R bimodule. Then a direct computation shows

$$\begin{aligned}
\epsilon E_{rs} &= (U\ \ -I)\begin{pmatrix}A_r & B_r\\ C_r & D_r\end{pmatrix}\begin{pmatrix}A_s & B_s\\ C_s & D_s\end{pmatrix}\begin{pmatrix}I\\ U\end{pmatrix}\\
&= (U\ \ -I)\begin{pmatrix}A_r & B_r\\ C_r & D_r\end{pmatrix}\begin{pmatrix}I & 0\\ 0 & I\end{pmatrix}\begin{pmatrix}A_s & B_s\\ C_s & D_s\end{pmatrix}\begin{pmatrix}I\\ U\end{pmatrix}\\
&= (U\ \ -I)\begin{pmatrix}A_r & B_r\\ C_r & D_r\end{pmatrix}\left[\begin{pmatrix}I\\ U\end{pmatrix}(I\ \ 0)+\begin{pmatrix}0\\ -I\end{pmatrix}(U\ \ -I)\right]\begin{pmatrix}A_s & B_s\\ C_s & D_s\end{pmatrix}\begin{pmatrix}I\\ U\end{pmatrix} \qquad (12)\\
&= \epsilon E_r(A_s+B_sU)+(-UB_r+D_r)\epsilon E_s\\
&= \epsilon E_rA_s+D_r\epsilon E_s\\
&= \epsilon E_r\cdot s+r\cdot\epsilon E_s\quad .
\end{aligned}$$

The last but one equality uses the fact that the maximal ideal of A is annihilated by ϵ, thus $\epsilon U=0$. So $E:r\mapsto E_r$ is a 1-cocycle for the R-R bimodule cohomology with coefficients in $\mathrm{Hom}_k(V,M/V)$. Also note that $E_r=0$ for all $r\in R$ if and only if the chosen filtration $\mathcal{V}$ is R-stable.

If we change the filtration $\mathcal{V}$ by a different lifting $\tilde{\mathcal{V}}$ of $\mathcal{V}'$, then we can write

$$\tilde{U} = U + N, \quad N \in \epsilon \operatorname{Mat}_{n\times m}(k)\,.$$

Then the relation between the cocycles $\tilde{E}$ and E is given by

$$\tilde{E}_r = E_r + (r \cdot N - N \cdot r)\,.$$

Hence a different choice of $\mathcal{V}$ changes the cocycle E by a 1-coboundary. Thus the obstruction to the existence of an R-stable filtration $\mathcal{V}$ lies in the cohomology group $\mathrm{H}^1(R\text{-}R\,, \operatorname{Hom}(V, M/V))$, as asserted.

If $A \twoheadrightarrow A'$ is an arbitrary small surjection with kernel I, an identical argument (everything has to be tensored with I) shows that the corresponding obstruction lies in $\mathrm{H}^1(R\text{-}R\,, \operatorname{Hom}(V, M/V)) \otimes_k I$. Moreover, our construction is clearly functorial in the sense of Definition 1.3.4. Hence $\mathrm{H}^1(R\text{-}R\,, \operatorname{Hom}(V, M/V))$ is an obstruction space for $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$, as asserted. ∎

3 Modules over maximal orders

In this chapter we recall the basic structure theorems for maximal and hereditary orders in (not necessarily commutative) semisimple algebras. These results are used in Section 4.4.

More specifically let G/k be a p-divisible group. Assume k is perfect and denote by $W = W(k)$ its Witt vector ring. If $\mathcal{O} \subset \mathrm{End}(G)$ is a $\mathbf{Z}_p$-subalgebra, we will need to single out the situations when the representation of $\mathcal{O}$ on the Dieudonné module $\mathbf{D}(G[p])$ has a trivial deformation functor. Using the results of the previous section, we show that this is the case whenever the Dieudonné module $\mathbf{D}(G)$ is $\mathcal{O} \otimes_{\mathbf{Z}_p} W(k)$-projective. This turns out to be the case whenever $\mathcal{O}$ is a *maximal* order in a semi-simple $\mathbf{Q}_p$-subalgebra of $\mathrm{End}(G)$. Indeed, maximal orders over a complete field are *hereditary*, so torsion-free modules over them are projective (3.2.9). In order to prove that if $\mathcal{O}$ is hereditary then so is $\mathcal{O} \otimes_{\mathbf{Z}_p} W(k)$, we show that hereditary orders stay hereditary after an unramified base ring extension (3.2.11). This is a simple extension of [15], Theorem 1.

All algebras considered in this chapter are *finite-dimensional* and *separable* over a field K. In our applications (Chapter 4) K will be the fraction field of $W(k)$, hence separability will be automatic. The word module stands for a left module. We refer to Reiner [34] for the proofs of most of the statements.

3.1 Semi-simple algebras

In this section the ground field K is arbitrary.

Definition 3.1.1. A K-algebra D is *simple* if D has no non-trivial two-sided ideals. A K-algebra whose radical (intersection of all maximal left ideals) is zero is called *semisimple*. A K-algebra D is called *central* if the center $Z(D)$ equals K.

Example. A finite field extension L of K is a simple K-algebra (non-central, unless $L = K$). A finite-dimensional division algebra D over K is simple. A matrix ring $\mathrm{Mat}_{n\times n}(K)$ and, more generally, a matrix ring $\mathrm{Mat}_{n\times n}(D)$ over a (central) division K-algebra D is a (central) simple K-algebra.

These are in fact the only examples:

Structure Theorem 3.1.2. *A semisimple K-algebra D decomposes as a product of matrix algebras over division algebras,*

$$D = \mathrm{Mat}_{n_1\times n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_k\times n_k}(D_k)\,.$$

Each of the D_i's is central over a finite field extension K_i of K.

Proof. [34], Theorems 7.1,7.4.

If D is a (semi)simple K-algebra and L/K a finite field extension, then $D \otimes_K L$ is easily seen to be a (semi)simple L-algebra. Moreover, central K-algebras become central L-algebras after such a base change. It is not true, however, that division algebras stay

division. For example if a division algebra D/K contains a non-trivial field extension L/K, then $D \otimes_K L$ contains $L \otimes_K L$, which has zero divisors. If, moreover, $L \subset D$ is maximal commutative, then $D \otimes_K L \cong \mathrm{Mat}_{n\times n}(L)$. The converse to this is the following theorem.

Theorem 3.1.3. *Let D be a division algebra, central over K and L/K a finite field extension. Then*

1. *$D \otimes_K L$ is a division algebra if and only if L/K and D/K have no isomorphic intermediate subfields (except for K itself).*

2. *$D \otimes_K L \cong \mathrm{Mat}_{n\times n}(L)$ if and only if L can be embedded into D as a maximal commutative subalgebra.*

Proof. [14], Theorem 4.8; [34], Theorem 7.15. ∎

Definition 3.1.4. In the situation of (2.) we say that L *splits* D.

Finally, we discuss the structure of (left) modules over semisimple algebras.

Theorem 3.1.5. *Let D be a semisimple K-algebra. Then every finitely generated D-module is projective.*

Proof. If D is a division algebra over K, then every finitely generated D-module is free (easy induction argument, using that D has no two-sided ideals). If D is a matrix algebra over a division algebra, the result follows from Morita equivalence. Finally, if D is a product of simple K-algebras, every D-module decomposes as a direct sum of modules over the factors of D and, hence, is projective. ∎

3.2 Maximal and hereditary orders

Throughout this section K is a field, which is complete with respect to a discrete valuation v and A its valuation ring. Again, K-algebras are assumed to be separable and finite-dimenional.

Definition 3.2.1. Let D be a semi-simple K-algebra. An *order of D* is a finitely generated A-subring $\mathcal{O}$ of D such that $\mathcal{O} \otimes_A K = D$.

Definition 3.2.2. An order $\mathcal{O}$ of D is said to be *maximal* if there is no order $\mathcal{O}'$ of D which strictly contains $\mathcal{O}$.

Over a complete field, the structure of maximal orders in a semi-simple K-algebra is summarized in the following theorems ([34], Theorems 12.8, 17.3, 10.5).

Theorem 3.2.3. *Let D/K be a division algebra (*recall that K is complete by assumption*). Then D has a unique maximal order, the integral closure of A in D.*

Theorem 3.2.4. *Let $D = \mathrm{Mat}_{n\times n}(D_0)$, a matrix ring over a division algebra D_0. Denote the unique maximal order of D_0 by $\mathcal{O}_0$. Then $\mathrm{Mat}_{n\times n}(\mathcal{O}_0)$ is a maximal order of D and every other maximal order of D is conjugate to it.*

Theorem 3.2.5. *Every maximal order of a product $D = D_1 \times \cdots \times D_n$ of simple K-algebras is conjugate to a product of (some) maximal orders of the D_i's.*

Remark 3.2.6. Let $L \supset K$ be a finite field extension. Denote by B the integral closure of A in L. We have already remarked that if D is a central semi-simple K-algebra, then $D \otimes_K L$ is central semi-simple. It is also clear that if $\mathcal{O} \subset D$ is an order, then $\mathcal{O} \otimes_R S \subset D \otimes_K L$ is again an order. However, if $\mathcal{O}$ is maximal, this does *not* imply that $\mathcal{O} \otimes_A B$ is maximal, even if L/K is unramified. Consider the following example:

Example 3.2.7. Let $p \neq 2$ be a prime, $K = \mathbf{Q}_p$ and L the unique unramified quadratic extension of K. Let $A = \mathbf{Z}_p$, $B = \mathbf{Z}_p \oplus \mathbf{Z}_p\xi$ be the rings of integers of K and L respectively. Denote by σ the unique non-trivial automorphism of L over K. Consider

$$\mathcal{O} = \left\{ \mathbf{Z}_p \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \mathbf{Z}_p \begin{pmatrix} \xi & 0 \\ 0 & \xi^\sigma \end{pmatrix} + \mathbf{Z}_p \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} + \mathbf{Z}_p \begin{pmatrix} 0 & \xi^\sigma \\ \xi p & 0 \end{pmatrix} \right\} \subset \mathrm{Mat}_{2\times 2}(L)\,.$$

It is easy to see that $D = \mathcal{O} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a division algebra, in fact the unique quaternion algebra over $\mathbf{Q}_p$. The subring $\mathcal{O} \subset D$ is the maximal order of D. The field L splits D. (L is contained in D as a maximal commutative subfield.) Consider the order

$$O \otimes_A B \subset D \otimes_K L \cong \mathrm{Mat}_{2\times 2}(L)$$

It is easy to see by looking at the given generators that

$$O \otimes_A B \;\cong\; \left\{ \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \;\middle|\; a, b, c, d \in B \right\}\,,$$

which is *not* a maximal order in $D \otimes_K L$, as it is contained in $\mathrm{Mat}_{2\times 2}(B)$. It is fortunate for the applications in Chapter 4 that the orders which can be obtained by a base change from a maximal order by an unramified ring extension do inherit the following important property of maximal orders:

Definition 3.2.8. An order $\mathcal{O}$ of D is *(left) hereditary* if every $\mathcal{O}$-module, which is finitely generated and free as an A-module is $\mathcal{O}$-projective.

Theorem 3.2.9. *([34], 18.1) A maximal order in a K-algebra D is hereditary.*

Theorem 3.2.10. *(Structure theorem; [34], 39.14)*

1. *A division algebra D/K has a unique hereditary order, namely the maximal order of D.*

2. *Let D/K be a division algebra. Let $\mathcal{O}$ denote the unique maximal order of D_0 and r denote the radical of $\mathcal{O}_0$. Let $E \cong \mathrm{Mat}_{n\times n}(D)$. Then for every hereditary order H of E, there are positive integers $\{n_1, ..., n_k\}$ with sum n and an identification $E = \mathrm{Mat}_{n\times n}(D)$, such that H takes the form*

$$H = \begin{pmatrix} \mathrm{Mat}_{n_1\times n_1}(\mathcal{O}) & \mathrm{Mat}_{n_1\times n_2}(\mathcal{O}) & \mathrm{Mat}_{n_1\times n_3}(\mathcal{O}) & \cdots & \mathrm{Mat}_{n_1\times n_k}(\mathcal{O}) \\ \mathrm{Mat}_{n_2\times n_1}(r) & \mathrm{Mat}_{n_2\times n_2}(\mathcal{O}) & \mathrm{Mat}_{n_2\times n_3}(\mathcal{O}) & \cdots & \mathrm{Mat}_{n_2\times n_k}(\mathcal{O}) \\ \mathrm{Mat}_{n_3\times n_1}(r) & \mathrm{Mat}_{n_3\times n_2}(r) & \mathrm{Mat}_{n_3\times n_3}(\mathcal{O}) & \cdots & \mathrm{Mat}_{n_3\times n_k}(\mathcal{O}) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \mathrm{Mat}_{n_k\times n_1}(r) & \mathrm{Mat}_{n_k\times n_2}(r) & \mathrm{Mat}_{n_k\times n_3}(r) & \cdots & \mathrm{Mat}_{n_k\times n_k}(\mathcal{O}) \end{pmatrix}.$$

   Conversely, every order of this form is hereditary.

3. *If D is semi-simple with simple components D_i, then the hereditary orders of D are exactly the direct sums of hereditary orders in the D_i.*

Theorem 3.2.11. *Let D/K be a (finite-dimensional) semi-simple algebra and $\mathcal{O} \subset D$ a hereditary order. Let L/K be an unramified extension of complete fields and let B denote the ring of integers of L. Then $\mathcal{O} \otimes_A B$ is a hereditary order in $D \otimes_K L$.*

Proof. In case $[L:K] < \infty$ this is Janusz [15], Theorem 1. Now let L/K be arbitrary. Using the Structure theorem 3.2.10, one reduces to the case D is division. In this case $\mathcal{O} \subset D$ is the maximal order. If $D \otimes_K L$ happens to be a division algebra, then $\mathcal{O} \otimes_A B$ is easily seen to be the maximal order of $D \otimes_K L$, hence it is hereditary. If $D \otimes_K L$ is not division, then there is a finite extension K_1 of K in L such that already $D \otimes_K L$ is not division. Let B_1 denote the ring of integers of K_1. Replace K by K_1, D by $D_1 = D \otimes_K K_1$ and $\mathcal{O}$ by $O_1 = O \otimes_A B$. The order O_1 is hereditary in D_1 (again Janusz [15], Theorem 1) and we can apply the same procedure until on some step $D_n \otimes_{K_n} L$ is a division algebra. This happens necessarily after finitely many ($< rk_L D$) steps. ∎

Remark. We will use this theorem in 4.4.1 with $A = \mathbf{Z}_p$ and $B = W(k)$, the ring of Witt vectors of a perfect field k of characteristic p. We show namely that the Dieudonné module $D(G)$ of a p-divisible group G/k is $\mathcal{O} \otimes_{\mathbf{Z}_p} W(k)$-projective whenever $\mathcal{O} \subset \mathrm{End}(G)$ is a hereditary order in a semi-simple $\mathbf{Q}_p$-algebra.

4 Formal moduli of p-divisible groups

In this chapter we are going to study deformation functors of p-divisible groups with extra structure, such as a ring action and/or a principal quasi-polarization. From here on the ground field k is assumed to be perfect. As usual we work on the category Art_Λ where Λ is a fixed complete Noetherian local ring with $\Lambda/m_\Lambda = k$.

To illustrate our approach, consider a p-divisible group G/k and fix a $\mathbf{Z}_p-$subalgebra $\mathcal{O} \subset \mathrm{End}(G)$. Let $\mathcal{G}/A$ be a deformation of G to a ring $A \in Art_\Lambda$ and assume that the $\mathcal{O}$-action lifts to $\mathcal{G}$. Associated to $\mathcal{G}$ there is a filtration on the Lie algebra of the universal extension of $\mathcal{G}$,

$$V\mathcal{G} \subset M\mathcal{G} .$$

Here $M\mathcal{G}$ is a finite free A-module of rank equal to the height of G and $V\mathcal{G}$ is a direct summand. Moreover, by functoriality, the ring $\mathcal{O}$ acts on $V\mathcal{G}$ and $M\mathcal{G}$. So $V\mathcal{G} \subset M\mathcal{G}$ can be considered as a deformation of $VG \subset MG$ on the category of filtered modules with an $\mathcal{O}$-action. This gives a natural transformation of deformation functors (see 4.1.4, 4.3.1 for definitions)

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}) \longrightarrow \mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O}) . \tag{13}$$

We are going study how the two functors are related.

We appeal to the Grothendieck-Messing deformation theory of p-divisible groups ([23], Ch. IV). Let $\mathcal{G}'/A'$ be a p-divisible group. If $A \twoheadrightarrow A'$ is a surjection in Art_Λ, whose kernel has a nilpotent divided power structure, one can relate deformations of $\mathcal{G}'$ to A to the deformations of the universal extension filtration. This relies, in particular, on the "crystalline" nature of MG. Namely, for any two deformations $\mathcal{G}_1/A, \mathcal{G}_2/A$ of $\mathcal{G}'/A'$, there is a *canonical* isomorphism

$$M\mathcal{G}_1 \cong M\mathcal{G}_2$$

which reduces to the identity on $M\mathcal{G}'$. It follows that there is a universal A-module $M_A\mathcal{G}'$, which can be canonically identified with every $M\mathcal{G}$ for $\mathcal{G}/A$ deforming $\mathcal{G}'/A'$. Hence, associated to $\mathcal{G}/A$ there is a deformation of the filtration $V\mathcal{G}' \subset M\mathcal{G}'$ to a filtration $V\mathcal{G}$ of a *fixed* A-module, namely $M_A\mathcal{G}'$. By the result of Messing ([23], V, 1.6) this association is a bijection.

This is a powerful method of studying deformations of p-divisible groups with extra data. For example if $\mathcal{G}'/A'$ admits an $\mathcal{O}$-action, then $M_A\mathcal{G}'$ is an $\mathcal{O}$-module (by functoriality) and the deformations G/A which inherit the $\mathcal{O}$-action correspond precisely to the $\mathcal{O}$-stable filtrations of $M_A\mathcal{G}'$. One does need to know, however, what is the structure of $M_A\mathcal{G}'$ as an $\mathcal{O}$-module. The difficulty is that although $M\mathcal{G}$ "does not change" over divided power extensions, it does change over arbitrary extensions $A \to k$. It is easy to give an example of rings $A \twoheadrightarrow A' \twoheadrightarrow k$ and two deformations $\mathcal{G}'_1/A', \mathcal{G}'_2/A'$ of G/k such that $M_A\mathcal{G}'_1$ and $M_A\mathcal{G}'_2$ are not isomorphic as $\mathcal{O}$-modules. So it is much easier to study a

functor such as $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ on the category $Art_{W,pd}$ of divided power extensions $A \to k$ than on the full category Art_Λ.

The idea is to target the situations when MG is "rigid" as an $\mathcal{O}$-module, meaning that for any $A \in Art_\Lambda$ any two deformations M_1, M_2 of MG to A are isomorphic as $\mathcal{O} \otimes_{\mathbf{Z}_p} A$-modules. In this case for any deformation $\mathcal{G}/A$ there is an $\mathcal{O} \otimes_{\mathbf{Z}_p} A$-module isomorphism

$$M\mathcal{G} \cong \mathbf{D}(G) \otimes_{W(k)} A\,.$$

Here $\mathbf{D}(G)$ is a covaraint Dieudonné module of G, which is a finite free $W(k)$-module with an $\mathcal{O}$-action. In such a "rigid" situation it turns out that the natural transformation (13) is formally smooth: any deformation of the pair $VG \subset MG$ is induced by that of G. Note that this implies that the functor $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ can be determined in terms of pure linear algebra. It is namely pro-represented by a formal power series ring over the hull of $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O})$.

As it seems difficult to actually determine the hull of $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O})$, we are going to appeal instead to the strategy described in Section 1.5. Namely, we are going to produce another formally smooth natural transformation $\mathcal{F} \to \mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O})$ with $\mathcal{F}$ pro-representable and one which can be calculated explicitly. We get a diagram

$$\begin{array}{ccc} \mathcal{F} & & \mathcal{D}\mathrm{ef}(G,\mathcal{O}) \\ & \searrow \quad \swarrow & \\ & \mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O}) & \end{array}\,.$$

If the tangent spaces of $\mathcal{F}$ and $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ happen to be of the same dimension, then the two functors are isomorphic by 1.5.4. There is in fact a natural candidate for $\mathcal{F}$. We can rigidify $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O})$ by studying deformations $\mathcal{V} \subset \mathcal{M}$ over A given *together* with an isomorphism $\mathcal{M} \cong \mathbf{D}(G) \otimes_W A$ of $\mathcal{O} \otimes_{\mathbf{Z}_p} A$-modules. Then the corresponding deformation functor $\mathcal{D}\mathrm{ef}_{\mathbf{D}(G)}(VG \subset MG)$ is easily seen to be pro-representable (cf. 2.3.2) and formally smooth over $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{O})$. Moreover, its tangent space is isomorphic to that of $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ by crystalline theory. Hence

$$\mathcal{D}\mathrm{ef}(G,\mathcal{O}) \cong \mathcal{D}\mathrm{ef}_{\mathbf{D}(G)}(VG \subset MG)\,.$$

This gives a way to determine $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ explicitly, provided the rigidity assumption on MG is satisfied.

The structure of this chapter is as follows:

First we recall the basic facts concerning p-divisible groups: rigidity of homomorphisms, duality and deformation theory (Section 4.1). For a subring $\mathcal{O} \subset \mathrm{End}(G)$ and a principal quasi-polarization $\lambda : G \xrightarrow{\sim} G^t$ we define the deformation functors $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ and $\mathcal{D}\mathrm{ef}(G,\mathcal{O},\lambda)$.

In Section 4.2 we define the notion of *deformation data* $\mathcal{D}$, in order to generalize our method to any situation when the rigidity of MG applies. We also define deformation functors $\mathcal{D}\mathrm{ef}(G,\mathcal{D})$ of p-divisible groups with a given deformation data and the notion of rigidity in this context.

In Section 4.3 we prove the pro-representability of the functors $\mathcal{D}\mathrm{ef}(G,\mathcal{D})$ in general (4.3.5) and the main comparison theorem (4.3.8). We also present an example to illustrate that such a comparison result does not hold if the rigidity assumption is omitted (4.3.10).

Then we apply the result to the functors $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ and $\mathcal{D}\mathrm{ef}(G,\mathcal{O},\lambda)$ (Sections 4.4, 4.5). In order to do that, it is necessary to determine for which $\mathcal{O}\subset\mathrm{End}(G)$ the $\mathcal{O}$-module MG is rigid. This turns out to hold whenever $\mathcal{O}$ is a *hereditary* (e.g. maximal) order in a semi-simple subalgebra of $\mathrm{End}(G)$ (Theorems 4.4.1,4.5.3). An interesting by-product is that in the case of a hereditary order the deformation functor $\mathcal{D}\mathrm{ef}(VG\subset MG,\mathcal{O})$ is isomorphic to the deformation functor of the tangent space representation $\rho_\tau:\mathcal{O}\longrightarrow\mathrm{End}(TG)$. In view of the formal smoothness of (13), a necessary and sufficient condition of deforming the pair $(G,\mathcal{O})$ to some $A\in Art_\Lambda$ is being able to deform this tangent space representation. This generalizes some known results on deformations with a restricted tangent space representation (cf. [8], [18], [33]).

Finally, we show that a deformation functor $\mathcal{D}\mathrm{ef}(G,\mathcal{D})$ with an arbitrary deformation data is isomorphic to a functor of the form $\mathcal{D}\mathrm{ef}(H,\mathcal{O},\lambda)$ for some p-divisible group H, a subring $\mathcal{O}\subset\mathrm{End}(G)$ (not necessarily a maximal order) and a principal quasi-polarization λ on H. This explains why in Chapter 5 we consider only deformation problems with one p-divisible group G/k.

As an illustration, we present another standard example, namely that of a chain of maps between p-divisible groups,

$$G_0\longrightarrow G_1\longrightarrow\cdots\longrightarrow G_{n-1}\longrightarrow G_n=G_0,$$

whose composition is multiplication by p (Section 4.7). The required rigidity condition is also satisfied in this case (but not, for example, if the composition is p^2) and our comparison theorem applies.

Our references for the deformation theory of p-divisible groups are Messing [23] (Chapters IV, V) and Berthelot, Breen, Messing [2] (especially 3.3, 4.2 and 5.3). We have chosen to follow the *covariant* Dieudonné module convention, as in the Cartier theory.

4.1 Deformations of p-divisible groups

For the definition of p-divisible groups and Serre duality we refer to [38], 2.1, 2.3. We work on the category Art_Λ of Artinian local Λ-algebras with residue field k, perfect of characteristic p. By G/k we denote a p-divisible group over k and $\mathcal{G}/A$ or $\mathcal{G}_A/A$ denotes a p-divisible group over $A\in Art_\Lambda$. We use $\mathcal{G}^t$ for the Serre dual of $\mathcal{G}$ and similarly for morphisms. Recall that $G\cong G^{tt}$ canonically, as follows from the corresponding result for finite group schemes.

In order to study the deformations of p-divisible groups, we rely on the Grothendieck-Messing approach ([23], Ch. IV).

Notation. For a p-divisible group $\mathcal{G}/A$ denote

$T\mathcal{G}$ — the tangent space (or the Lie algebra) of $\mathcal{G}$,
$M\mathcal{G}$ — the Lie algebra of the universal extension of $\mathcal{G}$,
$V\mathcal{G}$ — the canonical filtration on $M\mathcal{G}$.

There is an exact sequence (of finite free A-modules)

$$0 \longrightarrow V\mathcal{G} \longrightarrow M\mathcal{G} \longrightarrow T\mathcal{G} \longrightarrow 0, \tag{14}$$

Moreover, $T\mathcal{G}, M\mathcal{G}, V\mathcal{G}$ and the above sequence are compatible with base change and are functorial in $\mathcal{G}$. We have

$$\dim_A T\mathcal{G} = n, \quad \dim_A M\mathcal{G} = h, \quad \dim_A V\mathcal{G} = n' .$$

where n, n' denote the dimensions of $\mathcal{G}$ and $\mathcal{G}^t$ and $h = n + n'$ is the height. The sequence (14) for $\mathcal{G}^t$ is canonically isomorphic to the (A-linear) dual of the corresponding sequence for $\mathcal{G}$.

Finally, for G/k there are canonical isomorphisms ([2], 4.2.14)

$$MG = \mathbf{D}(G[p]) = \mathbf{D}(G) \otimes_{W(k)} k ,$$

functorial in G. Here $\mathbf{D}(-)$ denotes the covariant Dieudonné module.

We need the following rigidity result for morphisms of p-divisible groups:

Theorem 4.1.1. *Let $\mathcal{G}, \mathcal{H}$ be p-divisible groups over A and $A \to B$ a ring homomorphism in Art_Λ. Then*

$$\mathrm{Hom}(\mathcal{G}, \mathcal{H}) \hookrightarrow \mathrm{Hom}(\mathcal{G} \otimes_A B, \mathcal{H} \otimes_A B) .$$

Proof. Compose the map $A \to B$ with the augmentation to k,

$$A \longrightarrow B \longrightarrow k .$$

To show that $\mathrm{Hom}(\mathcal{G}, \mathcal{H}) \to \mathrm{Hom}(\mathcal{G} \otimes_A B, \mathcal{H} \otimes_A B)$ is injective, it suffices to verify that the composition $\mathrm{Hom}(\mathcal{G}, \mathcal{H}) \to \mathrm{Hom}(\mathcal{G} \otimes_A k, \mathcal{H} \otimes_A k)$ is injective. In other words we can reduce to the case of a map $A \to k$. From here we can also reduce to the case when $A \twoheadrightarrow B$ is a small extension, in particular an extension with divided powers.

Thus let $A \twoheadrightarrow B$ be a divided power extension. Then the Grothendieck-Messing theory identifies $\mathrm{Hom}(\mathcal{G}, \mathcal{H})$ with a *subset* of $\mathrm{Hom}(\mathcal{G} \otimes_A B, \mathcal{H} \otimes_A B)$ of those homomorphisms which preserve the filtrations. Hence the injectivity follows.

Definition 4.1.2. A *quasi-polarization* on a p-divisible group $\mathcal{G}_A/A$ is an isogeny

$$\lambda : \mathcal{G}_A \longrightarrow \mathcal{G}_A^t$$

which satisfies $\lambda^t = -\lambda$. We say that the quasi-polarization is *principal* if λ is an isomorphism.

Remark. It follows from 4.1.1 that a morphism $\lambda : \mathcal{G}_A \to \mathcal{G}_A^t$ is a (principal) quasi-polarization on $\mathcal{G}_A$ if and only if $\lambda \otimes_A k$ is a (principal) quasi-polarization on $\mathcal{G}_A \otimes_A k$.

Our primary goal is to study the structure of the following deformation functors:

Definition 4.1.3. Let $A \twoheadrightarrow A'$ be a morphism in Art_Λ and $\mathcal{G}'/A'$ a p-divisible group. A *deformation* of $\mathcal{G}'$ to A is a p-divisible group $\mathcal{G}/A$ together with an isomorphism

$$i : \mathcal{G} \otimes_A A' \cong \mathcal{G}' . \tag{15}$$

Definition 4.1.4. Let G/k be a p-divisible group. Define the deformation functor of G,

$$\begin{array}{rccc} \mathcal{D}\mathrm{ef}(G): & Art_\Lambda & \longrightarrow & Sets \\ & A & \longmapsto & \left\{ \begin{array}{c} \text{deformations} \\ \text{of } G \text{ to } A \end{array} \right\} / \cong \end{array} .$$

Given a subring $j : \mathcal{O} \hookrightarrow \mathrm{End}(G)$, we let

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}) : Art_\Lambda \longrightarrow Sets$$

to be the functor of deformations $\mathcal{G}/A$ together with the action of $\mathcal{O}$ which reduces to j on G (under (15)). Similarly, given a subring $\mathcal{O} \subset \mathrm{End}(G)$ and a quasi-polarization λ on G, we define

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda) : Art_\Lambda \longrightarrow Sets$$

to be the functor of deformations $\mathcal{G}/A$ together with the action of $\mathcal{O}$ and a quasi-polarization which reduce to those of G.

Remark. It is well-known that $\mathcal{D}\mathrm{ef}(G)$ is pro-representable and

$$\mathcal{D}\mathrm{ef}(G) \cong \mathrm{Hom}_\Lambda(\Lambda[[t_1, ..., t_d]], -), \quad d = \dim G \cdot \dim G^t .$$

From the rigidity theorem (4.1.1) it follows that $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ and $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$ are subfunctors of $\mathcal{D}\mathrm{ef}(G)$. These subfunctors are pro-representable (4.3.5 below), so the pro-representing rings are of the form

$$\Lambda[[t_1, ..., t_d]]/J .$$

These rings are often singular and our goal is to describe them in some cases.

4.2 Deformation data

In order to generalize 4.1.4 to a potentially larger class of situations, we define the notion of a deformation data. Such a deformation data can be of the form "an object with an action of a ring $\mathcal{O}$" or "an object with an action of a ring $\mathcal{O}$ and a quasi-polarization" or, most generally, a finite collection of objects together with certain morphisms between them and their duals. For such a deformation data $\mathcal{D}$, it is clear how to define a $\mathcal{D}$-object of pDiv_A or any other additive $\mathbf{Z}_p$-linear category with duality (such as finite free modules over a given $\mathbf{Z}_p$-algebra). We also define deformation functors of $\mathcal{D}$-objects and give the examples that we have in mind.

Notation 4.2.1. For $A \in Art_\Lambda$ let $\mathcal{C} = \mathcal{C}_A$ denote one of the following categories:

1. The category pDiv_A of p-divisible groups $\mathcal{G}_A$ over A.
2. The category Mod_A of finite free A-modules $\mathcal{M}_A$.
3. The category FMod_A of filtrations $\mathcal{F}_A \subset \mathcal{M}_A$, where $\mathcal{M}_A$ is a finite free A-module and $\mathcal{F}_A$ a direct A-summand.

In each case $\mathcal{C}_A$ is an additive $\mathbf{Z}_p$-linear category with a duality, an anti-equivalence of categories $t : \mathcal{C}_A^\circ \to \mathcal{C}_A$. We have namely the Serre duality for p-divisible groups, the A-linear duals for modules over A and

$$(F \subset M) \longmapsto ((M/F)^t \subset M^t)$$

for the filtrations. In any case, we denote the dual object of X by X^t and similarly for morphisms.

A morphism $A \to A'$ in Art_Λ induces a $\mathbf{Z}_p$-linear "base change" functor

$$- \otimes_A A' : \mathcal{C}_A \longrightarrow \mathcal{C}_{A'} .$$

There are also some obvious forgetful functors, such as

$$\mathrm{FMod}_A \longrightarrow \mathrm{Mod}_A \qquad \text{(forget the filtration)} .$$

These are $\mathbf{Z}_p$-linear, commute with base change and preserve duality.

Definition 4.2.2. An arbitrary self-dual $\mathbf{Z}_p$-linear category $\mathcal{D}$ is called a *deformation data* if it has finitely many objects and all $\mathrm{Hom}(X, Y)$ are finitely generated $\mathbf{Z}_p$-modules.

In the following list of basic definitions, let $\mathcal{C} = \mathcal{C}_A$ be as in 4.2.1 and $\mathcal{D}$ a deformation data. The term functor will refer to a $\mathbf{Z}_p$-linear duality-preserving functor.

Definition 4.2.3. A *$\mathcal{D}$-object* X_A of a category $\mathcal{C}$ is a covariant functor $X_A : \mathcal{D} \to \mathcal{C}$. By a *morphism* $X \to Y$ of $\mathcal{D}$-objects we mean a natural transformation as functors.

Notation 4.2.4. For a functor $\mathcal{F} : \mathcal{C} \to \mathcal{C}'$ and a $\mathcal{D}$-object X of $\mathcal{C}$ we let $\mathcal{F}(X)$ to be the $\mathcal{D}$-object of $\mathcal{C}'$ given by the composition $\mathcal{F}(X) = \mathcal{F} \circ X$. In particular, this defines the base change of $\mathcal{D}$-objects (let $\mathcal{F} = - \otimes_A A' : \mathcal{C}_A \to \mathcal{C}_{A'}$).

Remark. With the notations of Section 4.1, the following associations give duality-preserving $\mathbf{Z}_p$-linear covariant functors (cf. [2], 5.3.6).

$$\begin{array}{rccc}
U : & \mathrm{pDiv}_A & \longrightarrow & \mathrm{FMod}_A \\
 & \mathcal{G} & \longmapsto & (V\mathcal{G} \subset M\mathcal{G}) \\
\mathbf{D}(-) : & \mathrm{pDiv}_k & \longrightarrow & \mathrm{Mod}_{W(k)} \\
 & G & \longmapsto & \mathbf{D}(G) \\
\mathbf{D}(-[p]) : & \mathrm{pDiv}_k & \longrightarrow & \mathrm{Mod}_k \\
 & G & \longmapsto & \mathbf{D}(G[p])
\end{array}$$

Following 4.2.4, for a deformation data $\mathcal{D}$ and a $\mathcal{D}$-object $\mathcal{G}_A$ of pDiv_A we can speak of $U(\mathcal{G}_A)$. In case $A = k$ and G/k we can also define $\mathbf{D}(G)$ and $\mathbf{D}(G[p])$.

Definition 4.2.5. Let $A \twoheadrightarrow A'$ be a homomorphism in Art_Λ. Given a $\mathcal{D}$-object $X_{A'}$ of $\mathcal{C}_{A'}$, a *deformation* of $X_{A'}$ to $\mathcal{C}_A$ is a $\mathcal{D}$-object X_A of $\mathcal{C}_A$ given together with an isomorphism

$$X_A \otimes_A A' \;\cong\; X_{A'} \,.$$

For a $\mathcal{D}$-object X_k of $\mathcal{C}_k$, let the *deformation functor of* X_k to be

$$\begin{array}{rccc} \mathcal{D}\mathrm{ef}(X_k,\mathcal{D}): & Art_\Lambda & \longrightarrow & Sets \\ & A & \longmapsto & \{\text{deformations of } X_k \text{ to } \mathcal{C}_A\}/\cong \end{array} \,.$$

Keeping in mind the deformation functors that we are interested in (cf. 4.1.4), we have the following examples:

Example 4.2.6. (Endomorphisms.) Let $\mathcal{O}$ be a $\mathbf{Z}_p$-algebra. Let $\mathcal{D}$ consist of two objects, X and its dual X^t with

$$\mathrm{End}(X) = \mathcal{O}, \quad \mathrm{End}(X^t) = \mathcal{O}^{\,\mathrm{op}}, \quad \mathrm{Hom}(X, X^t) = 0, \quad \mathrm{Hom}(X^t, X) = 0 \,.$$

We let duality interchange X and X^t and act as identity $\mathrm{End}(X) \to \mathrm{End}(X^t)$. Then $\mathcal{D}$ defines the data "an object with an $\mathcal{O}$-action". For instance, a $\mathcal{D}$-object of pDiv_A can be identified with a p-divisible group $\mathcal{G}_A/A$ together with an action of $\mathcal{O}$. In particular, for a $\mathcal{D}$-object G/k we have (cf. 4.1.4)

$$\mathcal{D}\mathrm{ef}(G,\mathcal{D}) \cong \mathcal{D}\mathrm{ef}(G,\mathcal{O}) \,.$$

Example 4.2.7. (Endomorphisms, principal quasi-polarization.) Let $\mathcal{O}$ be a $\mathbf{Z}_p$-algebra with a $\mathbf{Z}_p$-linear anti-involution $r : \mathcal{O} \cong \mathcal{O}^{\,\mathrm{op}}$. Again take $\mathcal{D} = \{X, X^t\}$ and let

$$\mathrm{End}(X) = \mathcal{O}, \quad \mathrm{End}(X^t) = \mathcal{O}^{\,\mathrm{op}}, \quad \mathrm{Hom}(X, X^t) = \mathbf{Z}_p\lambda, \quad \mathrm{Hom}(X^t, X) = \mathbf{Z}_p\lambda^{-1} \,.$$

Here λ and λ^{-1} are formal symbols and

$$\lambda\lambda^{-1} = id = \lambda^{-1}\lambda, \qquad \lambda^t = -\lambda, \qquad \lambda^{-1} o^t \lambda = r(o) \;\; (o \in \mathcal{O}) \,.$$

Then $\mathcal{D}$ defines the data "an object with an $\mathcal{O}$-action and a principal quasi-polarization". For instance, a $\mathcal{D}$-object of pDiv_A is a p-divisible group $\mathcal{G}_A/A$ together with an action of $\mathcal{O}$ and a self-dual isomorphism $\lambda : G \to G^t$ whose Rosati involution on $\mathcal{O}$ is r. So for a $\mathcal{D}$-object G/k we have (cf. 4.1.4)

$$\mathcal{D}\mathrm{ef}(G,\mathcal{D}) \cong \mathcal{D}\mathrm{ef}(G,\mathcal{O},\lambda) \,.$$

Example 4.2.8. (p-chain.) Take $n \geq 1$. Let $\mathcal{D}$ consist of objects X_i indexed by $i \in \mathbf{Z}/n\mathbf{Z}$ and their duals X_i^t. Let

$$\mathrm{Hom}(X_i, X_{i+1}) = \mathbf{Z}_p f_i, \quad \mathrm{Hom}(X_{i+1}^t, X_i^t) = \mathbf{Z}_p f_i^t$$

and define the compositions of all the f_i to be multiplication by p,

$$f_{i-1}f_{i-2}\cdots f_{i-n} = p \in \mathbf{Z}_p = \mathrm{End}(X_i), \qquad i \in \mathbf{Z}/n\mathbf{Z}\,.$$

As in 4.2.6 we let all the homomorphisms between X_i and X_j^t to be 0. Then $\mathcal{D}$ defines the data "p-chain of length n". For instance, a $\mathcal{D}$-object of pDiv_A is a collection of p-divisible groups $\mathcal{G}_i/A$ (with $i \in \mathbf{Z}/n\mathbf{Z}$) and maps $f_i : G_i \to G_{i+1}$ every of whose cyclic compositions equals p. In particular this forces the G_i to have the same height and the f_i to be isogenies.

4.3 The comparison theorem

Notation. Let G be a $\mathcal{D}$-object of pDiv_k. Let $\mathcal{M} = \mathbf{D}(G) \otimes_W \Lambda$, which is a $\mathcal{D}$-object of Mod_Λ. Denote by $VG \subset MG$ the $\mathcal{D}$-object $U(G)$. Thus, canonically, $MG = \mathcal{M} \otimes_\Lambda k$. Following 4.2.2, we can define the deformation functors $\mathcal{D}\mathrm{ef}(G, \mathcal{D})$ and $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{D})$. We also define the "rigidified" version of the latter deformation functor, $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{D})$:

Definition 4.3.1. Let $\mathcal{N}$ be a deformation of MG to Λ. Define

$$\mathcal{D}\mathrm{ef}_{\mathcal{N}}(VG \subset MG, \mathcal{D}) : Art_\Lambda \longrightarrow Sets$$

to be the covariant functor which associates to a ring $A \in Art_\Lambda$ the set of isomorphism classes of elements $(\mathcal{V}_A \subset \mathcal{M}_A) \in \mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{D})$ given together with an isomorphism $\mathcal{M}_A \cong \mathcal{N} \otimes_\Lambda A$.

Lemma 4.3.2. *Let $\mathcal{D}$ be a deformation data and G a $\mathcal{D}$-object of* pDiv_k. *For any deformation $\mathcal{N}$ of the $\mathcal{D}$-object MG to Λ, the functor $\mathcal{D}\mathrm{ef}_{\mathcal{N}}(VG \subset MG, \mathcal{D})$ is pro-representable.*

Proof. Apply the same argument as in the proof of Theorem 2.3.2. It is easy to see that the $\mathbf{Z}_p$-generators of the $\mathrm{Hom}(X, Y)$ for varying $X, Y \in \mathcal{D}$ plus the duality constraints give finitely many equations for the deformation functor.

Remark 4.3.3. The crystalline theory establishes a canonical bijection

$$\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{D})(A) = \mathcal{D}\mathrm{ef}(G, \mathcal{D})(A)$$

for every k-algebra $A \in Art_\Lambda$ whose augmentation $A \to k$ is a divided power extension. In particular, this applies to $A = k[V]$ for any finite-dimensional k-vector space V. So the tangent spaces of the two functors are isomorphic. In particular, $\mathcal{D}\mathrm{ef}(G, \mathcal{D})$ does have a (finite-dimensional) tangent space.

Example 4.3.4. Let G/k be a p-divisible group and $\mathcal{O} \subset \mathrm{End}(G)$ a $\mathbf{Z}_p$-subalgebra. Then the tangent space to $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ equals to the Hochschild cohomology group $\mathrm{H}^1(\mathcal{O} - \mathcal{O}, TG \otimes_k TG^t)$ as it is the tangent space to the deformation functor of the filtration (Theorem 2.3.2).

Lemma 4.3.5. *Let $\mathcal{D}$ be a deformation data and G a $\mathcal{D}$-object of* pDiv_k. *Then the functor $\mathcal{D}\mathrm{ef}(G, \mathcal{D}) : Art_\Lambda \to Sets$ is pro-representable.*

Proof. We apply the Schlessinger's criterion (Theorem 1.4.3). By 4.3.3, $\mathcal{D}\mathrm{ef}(G, \mathcal{D})$ has a finite-dimensional tangent space. So it suffices to prove that

$$\mathcal{D}\mathrm{ef}(G, \mathcal{D})(A \times_{A'} B') \longrightarrow \mathcal{D}\mathrm{ef}(G, \mathcal{D})(A) \times_{\mathcal{D}\mathrm{ef}(G,\mathcal{D})(A')} \mathcal{D}\mathrm{ef}(G, \mathcal{D})(B') \tag{16}$$

is a bijection whenever $A \twoheadrightarrow A'$ is a small extension and $B' \to A'$ a morphism in Art_Λ. Let $\mathcal{G}_{B'} \in \mathcal{D}\mathrm{ef}(G, \mathcal{D})(B')$ be a deformation of G to B'.

Associated to $\mathcal{G}_{B'}$ there is a universal extension filtration $V\mathcal{G}_{B'} \subset M\mathcal{G}_{B'}$. Moreover, since

$$B = A \times_{A'} B' \twoheadrightarrow B'$$

is a small (in particular, a divided power) extension, we can also define $M_B\mathcal{G}_{B'}$, the value of the universal extension crystal of $\mathcal{G}_{B'}$ on the ring B. This is a $\mathcal{D}$-object of Mod_B. Moreover, by Grothendieck-Messing, there is a bijection between the deformations of $\mathcal{G}_{B'}$ to B (as a $\mathcal{D}$-object) and deformations of the filtration $V\mathcal{G}_{B'} \subset M\mathcal{G}_{B'}$ to a filtration of $M_B\mathcal{G}_{B'}$ (again, as a $\mathcal{D}$-object). However, the functor

$$\mathcal{F} = \mathcal{D}\mathrm{ef}_{M_B\mathcal{G}_{B'}}(VG \subset MG) : Art_B \longrightarrow Sets$$

is pro-representable by Lemma 4.3.2. In particular, it commutes with fibre products, so

$$\mathcal{F}(A \times_{A'} B') \longrightarrow \mathcal{F}(A) \times_{\mathcal{F}(A')} \mathcal{F}(B')$$

is a bijection. It follows that (16) is a bijection as well. ∎

Remark. In order to prove the pro-representability of $\mathcal{D}\mathrm{ef}(G, \mathcal{D})$ we have used the Grothendieck-Messing theory together with the pro-representability of $\mathcal{D}\mathrm{ef}_{\mathcal{N}}(VG \subset MG, \mathcal{D})$ for various choices of $\mathcal{N}$. However, non-isomorphic p-divisible groups over A might have non-isomorphic $M\mathcal{G}$'s, as $\mathcal{D}$-objects. Consequently, one should not expect the full deformation functor $\mathcal{D}\mathrm{ef}(G, \mathcal{D})$ to be isomorphic to $\mathcal{D}\mathrm{ef}_{\mathcal{N}}(VG \subset MG, \mathcal{D})$ for any particular choice of $\mathcal{N}$. In some cases, however, the $\mathcal{D}$-object MG is "rigid" in the sense that it can be uniquely deformed to any $A \in Art_\Lambda$. Then $\mathcal{D}\mathrm{ef}(G, \mathcal{D})$ could be expected to be (non-canonically) isomorphic to $\mathcal{D}\mathrm{ef}_{\mathcal{M}_\Lambda}(VG \subset MG, \mathcal{D})$ where $\mathcal{M}_\Lambda$ is the unique deformation of M to Λ. Such a non-canonical isomorphism in fact exists, as we show in 4.3.8 below.

Definition 4.3.6. Let $\mathcal{C}$ be as in 4.2.1 and let $\mathcal{D}$ be a deformation data. A $\mathcal{D}$-object X_k of $\mathcal{C}_k$ is said to be *rigid* if there is a "universal" $\mathcal{D}$-object X_Λ of $\mathcal{C}_\Lambda$ such that

$$\mathcal{D}\mathrm{ef}(X_k, \mathcal{D})(A) = \{X_\Lambda \otimes_\Lambda A\}, \qquad A \in Art_\Lambda\,,$$

and such that the automorphism functor

$$\mathcal{A}ut(X_\Lambda): \ A \longmapsto \mathrm{Aut}(X_\Lambda \otimes_\Lambda A)$$

is formally smooth.

Remark 4.3.7. It is not difficult to show that a $\mathcal{D}$-object X_k of $\mathcal{C}_k$ is rigid if and only if the following holds. First, X_k can be deformed to any $A \in Art_\Lambda$. Second, given a surjection $A \twoheadrightarrow A'$ in Art_Λ and a deformation $\mathcal{X}_{A'}$ of X_k to A', any two deformations $\mathcal{X}_A^{(1)}, \mathcal{X}_A^{(2)}$ of $\mathcal{X}_{A'}$ to A are isomorphic *over* $\mathcal{X}_{A'}$. In other words, there is an isomorphism of $\mathcal{D}$-objects $\mathcal{X}_A^{(1)} \cong \mathcal{X}_A^{(2)}$ which becomes identity on $\mathcal{X}_{A'}$ after applying $\otimes_A A'$.

Theorem 4.3.8. *Let $\mathcal{D}$ be a deformation data and G a $\mathcal{D}$-object of* pDiv_k. *Let $\mathcal{M} = \mathbf{D}(G) \otimes_{W(k)} \Lambda$. Consider a diagram of functors*

$$\begin{array}{ccc} \mathcal{D}\mathrm{ef}(G,\mathcal{D}) & & \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{D}) \\ & {\scriptstyle q_1}\searrow \quad \swarrow{\scriptstyle q_2} & \\ & \mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{D}) & \end{array} \,. \tag{17}$$

Assume that the $\mathcal{D}$-object $\mathcal{M} \otimes_\Lambda k = \mathbf{D}(G[p])$ of Mod_k *is rigid. Then q_1 and q_2 are formally smooth and there is a (non-canonical) isomorphism of functors $i : \mathcal{D}\mathrm{ef}(G,\mathcal{D}) \to \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{D})$ which makes (17) commute.*

Proof. The strategy is to apply the comparison theorem 1.5.4. First note that both $\mathcal{D}\mathrm{ef}(G,\mathcal{D})$ and $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{D})$ are pro-representable (4.3.2, 4.3.5). Moreover, their tangent spaces are isomorphic by 4.3.3 and this isomorphism commutes with the projections to $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{D})$. In order to conclude that the two functors are isomorphic over $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{D})$ it suffices to prove that the projections q_1 and q_2 are formally smooth. We begin with q_2.

Let $A \twoheadrightarrow A'$ be a surjection in Art_Λ. Let $\mathcal{V}_{A'} \subset \mathcal{M}_{A'} = \mathcal{M} \otimes_\Lambda A'$ be a $\mathcal{D}$-object of $\mathrm{FMod}_{A'}$, considered as an element of $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{D})(A')$. Assume that we are given a deformation $\mathcal{V}_A \subset \mathcal{M}_A$ of this element to A. In particular, $\mathcal{M}_A$ is a deformation of $\mathcal{M}_{A'}$. However, $\mathcal{M} \otimes_\Lambda A$ is also a deformation of $\mathcal{M}_{A'}$. So, by the rigidity assumption, this two deformations are isomorphic. Moreover, by 4.3.7, we can choose as identification $\mathcal{M}_A = \mathcal{M} \otimes_\Lambda A$ which reduces to the identity map on $\mathcal{M}_{A'}$. Then $\mathcal{V}_A \subset \mathcal{M}_A = \mathcal{M} \otimes_\Lambda A$ is a required deformation.

To show that q_1 is formally smooth we apply a similar argument. Let $A \twoheadrightarrow A'$ be a small extension in Art_Λ. Let $\mathcal{G}_{A'} \in \mathcal{D}\mathrm{ef}(G,\mathcal{D})(A')$. Denote by $\mathcal{V}_{A'} \subset \mathcal{M}_{A'}$ the associated universal filtration object and let $\mathcal{V}_A \subset \mathcal{M}_A^{(1)}$ be a deformation of it to A (as a $\mathcal{D}$-object of $\mathrm{FMod}_{A'}$). Since $A \twoheadrightarrow A'$ has divided powers, we can also define the value of

the universal extension crystal of $\mathcal{G}_{A'}$ on A. Denote it by $\mathcal{M}_A^{(2)}$. Both $\mathcal{M}_A^{(1)}$ and $\mathcal{M}_A^{(2)}$ are deformations of $\mathcal{M}_{A'}$. Hence, by rigidity, they are isomorphic over $\mathcal{M}_{A'}$. Using such as isomorphism, $\mathcal{V}_{A'}$ can be considered as a filtration on $\mathcal{M}_A^{(2)}$. An application of crystalline theory shows that this filtration comes from a $\mathcal{D}$-object $\mathcal{G}_A$ of pDiv_A. Then $\mathcal{G}_A$ is a required deformation of $\mathcal{G}_{A'}$ to A. Hence q_2 is formally smooth. ∎

Remark 4.3.9. The isomorphisms established in Theorems 4.3.8 are in no way canonical. For example, we do not claim that they are functorial in G. The following example shows that such a functorial isomorphism can not exist in general, even in the case $\mathcal{O} = \mathbf{Z}_p$.

Example 4.3.10. Let $k = \mathbf{F}_p$ and G be the p-divisible group of an ordinary elliptic curve over k. Assume for a moment that for any $A \in Art_\Lambda$ and any deformation $\mathcal{G}/A$ of G/k, there is a canonical isomorphism

$$\mathbf{D}(G) \otimes_\Lambda A = M\mathcal{G},$$

which is compatible with base change, functorial in $\mathcal{G}$ and which coincides with the Grothendieck-Messing isomorphism at least when $A = k[W]$ for a finite-dimensional k-vector space W. Construct a natural transformation of functors

$$\mathcal{D}\mathrm{ef}(G) \longrightarrow \mathcal{D}\mathrm{ef}_{\mathbf{D}(G)}(VG \subset MG)$$

by letting

$$\mathcal{G}/A \longmapsto V\mathcal{G} \subset E\mathcal{G} = \mathbf{D}(G) \otimes_\Lambda A\,.$$

This natural transformation is in fact an isomorphism, since both functors are pro-represented by the ring $\Lambda[[t]]$ and the map is an isomorphism on the tangent spaces. Moreover, by functoriality, we get an induced inclusion of functors,

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}) \hookrightarrow \mathcal{D}\mathrm{ef}_{\mathbf{D}(G)}(VG \subset MG, R),$$

for an *arbitrary* subring $\mathcal{O} \subset \mathrm{End}(G)$ and $R = \mathcal{O} \otimes_{\mathbf{Z}_p} \Lambda$. Now denote by $\varphi \in \mathrm{End}(G)$ the (geometric) Frobenius on G and let

$$\mathcal{O}_n = \mathbf{Z}_p[p^n\varphi] \subset \mathrm{End}(G), \quad n \geq 0\,.$$

From the Serre-Tate theory, it follows that

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}_n) \cong \mathrm{Hom}_\Lambda\Big(W[[t]]/((1+t)^{p^n} - 1), -\Big)\,.$$

However, it is easy to see that

$$\mathcal{D}\mathrm{ef}_{\mathbf{D}(G)}(VG \subset MG, R) \cong \mathrm{Hom}_\Lambda\Big(W[[t]]/(p^n t), -\Big)\,.$$

Remark. In Chapter 5 we compute the functors $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ and $\mathcal{D}\mathrm{ef}(G,\mathcal{O},\lambda)$ in some cases using the above isomorphisms. Recall the basic steps of our method to determine the above functors.

Say we are interested in $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$. Then firstly, we have found a functor (not necessarily pro-representable) over which $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ is formally smooth. Then we have rigidified this functor to get a pro-representable functor ($\mathcal{D}\mathrm{ef}_{\mathbf{D}(G)}(VG\subset MG,R)$ in this case) which is relatively easy to compute. Then we have applied the comparison theorem.

It might be interesting to apply the same method in a different setting. For example, a theorem of Grothendieck-Illusie ([13], Thm. 4.4) asserts that

$$q : \mathcal{D}\mathrm{ef}(G) \longrightarrow \mathcal{D}\mathrm{ef}(G[p])$$

is formally smooth. Here $\mathcal{D}\mathrm{ef}(G[p])$ is the deformation functor of the p-torsion of G as a truncated p-divisible group. Suppose we could rigidify this functor to get

$$r : \mathcal{F} \longrightarrow \mathcal{D}\mathrm{ef}(G[p])$$

with r formally smooth as well. Assume also that $\mathcal{F}$ is pro-representable and explicit enough. By "explicit enough" we mean that one can determine, say, the filtrations of $\mathcal{F}$ determined by the p-rank filtration on $\mathcal{D}\mathrm{ef}(G[p])$. Then using the comparison theorem as in the theorems above, one could deduce the corresponding information about the deformation functor of G.

4.4 The maximal order case

To discuss the applications of our results, we consider the case of a p-divisible group G with an action of a ring $\mathcal{O}$. We show that in this case, the rigidity required for 4.3.8 is satisfied if the Dieudonné module $\mathbf{D}(G)$ is $\mathcal{O}\otimes_{\mathbf{Z}_p} W(k)$-projective. This, in turn, is true whenever $\mathcal{O}$ is a hereditary (e.g. maximal) order in a semi-simple $\mathbf{Q}_p$-algebra.

We fix the following notations. Let G/k be a p-divisible group over a perfect field of characteristic p and $\mathcal{O}\subset\mathrm{End}(G)$ a $\mathbf{Z}_p$-subalgebra. Let $\mathcal{D}$ be the deformation data of Example 4.2.6 with $\mathcal{O}$ as the acting ring. We let $R=\mathcal{O}\otimes_{\mathbf{Z}_p}\Lambda$ and

$$\rho_\tau : R \longrightarrow \mathrm{End}(TG)$$

denote the tangent space representation. Note that TG is a $\mathcal{D}$-object and (cf. 2.2.3)

$$\mathcal{D}\mathrm{ef}(TG,\mathcal{D}) \cong \mathcal{D}\mathrm{ef}(\rho_\tau)\,.$$

Let $VG\subset MG=\mathbf{D}(G[p])$ as usual denote the universal extension filtration. We let $\mathcal{M}$ denote $\mathbf{D}(G)\otimes_W\Lambda$. Clearly (cf. 2.3.1)

$$\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG\subset MG,\mathcal{D}) \cong \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG\subset MG,R)\,.$$

Finally, by 4.2.6 we have $\mathcal{D}\mathrm{ef}(G,\mathcal{O})=\mathcal{D}\mathrm{ef}(G,\mathcal{D})$. This is a subfunctor of $\mathcal{D}\mathrm{ef}(G)$, the full deformation functor of the p-divisible group G.

Theorem 4.4.1. *Let G/k be a p-divisible group. Let $\mathcal{O} \subset \mathrm{End}(G)$ be a $\mathbf{Z}_p$-subalgebra which is isomorphic to a hereditary order in a semi-simple $\mathbf{Q}_p$-algebra. Consider the diagram of functors*

$$\begin{array}{ccc} \mathcal{D}\mathrm{ef}(G,\mathcal{O}) & & \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, R) \\ & {\scriptstyle q_1}\searrow \quad \swarrow{\scriptstyle q_2} & \\ & \mathcal{D}\mathrm{ef}(\rho_\tau) & \end{array} \tag{18}$$

Here q_1 and q_2 are the obvious maps given by $\mathcal{G}_A \mapsto T\mathcal{G}_A$ and $(V_A \subset M_A) \mapsto (M_A/V_A)$. Then

1. *$\mathbf{D}(G)$ is a projective $R = \mathcal{O} \otimes_{\mathbf{Z}_p} W(k)$-module.*
2. *$\mathbf{D}(G[p])$ is rigid as a $\mathcal{D}$-object of Mod_k.*
3. *q_1 and q_2 are formally smooth.*
4. *There is a (non-canonical) isomorphism of functors $i : \mathcal{D}\mathrm{ef}(G,\mathcal{O}) \to \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, R)$ which completes (18) to a commutative diagram.*

Proof. 1. Since hereditary orders stay hereditary after an unramified base change over a complete field (Theorem 3.2.11), R is a hereditary order in a semi-simple algebra over the fraction field of $W(k)$. Thus (by definition, cf. 3.2.8), every R-module which is free over W is projective.
2. From the first part of the theorem it follows that $\mathcal{M}$ is a projective R-module. The assertion follows from the fact that projective modules satisfy the rigidity condition (cf. 2.2.5).
3, 4. This follows from Theorem 4.3.8 once we show that

$$\begin{array}{ccc} \mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{D}) & \longrightarrow & \mathcal{D}\mathrm{ef}(\rho_\tau) \\ V_A \subset M_A & \longmapsto & M_A/V_A \end{array} \tag{19}$$

is an isomorphism. We start with surjectivity. Let $A \in Art_\Lambda$ and $\wp_A \in \mathcal{D}\mathrm{ef}(\rho_\tau)(A)$,

$$\wp_A : R \longrightarrow \mathrm{End}_A(\mathcal{T}_A)\,.$$

Here $\mathcal{T}_A$ is a finite free A-module and $\mathcal{T}_A \otimes_A k = TG$. Let $\mathcal{M}_A = \mathcal{M} \otimes_\Lambda A$. We have a diagram of $R \otimes_\Lambda A$-modules,

$$\begin{array}{ccccc} \mathcal{M}_A & \xrightarrow{\otimes k} & MG & \twoheadrightarrow & TG \\ & & & & \uparrow \otimes k \\ & & & & \mathcal{T}_A \end{array} \tag{20}$$

where the map $MG \twoheadrightarrow TG$ comes from the canonical isomorphism $MG/VG \cong TG$. Since $\mathcal{M}_A$ is a projective $R \otimes_\Lambda A$-module, there exists a $R \otimes_\Lambda A$-module map $\mathcal{M}_A \to \mathcal{T}_A$

which makes (20) commute. It is surjective by Nakayama's lemma and its kernel $\mathcal{V}_A \subset \mathcal{M}_A$ is the required deformation of the filtration $VG \subset MG$.

It remains to show that (19) is injective. Let $\mathcal{V}_{1,A} \subset \mathcal{M}_{1,A}$ and $\mathcal{V}_{2,A} \subset \mathcal{M}_{2,A}$ be two elements of $\mathcal{D}\mathrm{ef}(VG \subset MG, \mathcal{D})(A)$. Suppose

$$\mathcal{M}_{1,A}/\mathcal{V}_{1,A} \cong \mathcal{T}_A \cong \mathcal{M}_{2,A}/\mathcal{V}_{2,A} \,. \tag{21}$$

as $R \otimes_\Lambda A$-modules. By the second part of the theorem, there are isomorphisms

$$\mathcal{M}_{1,A} \cong \mathcal{M} \otimes_\Lambda A \cong \mathcal{M}_{2,A} \,.$$

In particular, $\mathcal{M}_{i,A}$ are projective $R \otimes_\Lambda A$-modules. We have to show that there is an isomorphism $\mathcal{M}_{1,A} \cong \mathcal{M}_{2,A}$ which reduces to the identity map on MG and which takes $\mathcal{V}_{1,A}$ to $\mathcal{V}_{2,A}$.

Consider the set $\mathcal{T}_A \times_{TG} MG$. It can be naturally given an $R \otimes_\Lambda A$-module structure (via that of its components). We have the following diagram of $R \otimes_\Lambda A$-modules

$$\begin{array}{ccc} \mathcal{M}_{1,A} & \dashrightarrow & \mathcal{M}_{2,A} \\ {\scriptstyle \pi_1}\searrow & & \swarrow{\scriptstyle \pi_2} \\ & \mathcal{T}_A \times_{TG} MG & \end{array} \tag{22}$$

Here π_i have the maps induced by (21) as their first components and the natural projections $\mathcal{M}_{1,A} \to MG$ as their second components. In particular π_2 (and π_1) is surjective. By projectivity of $\mathcal{M}_{1,A}$, there exists a dotted map which makes (22) commute. Such a map has both of the required properties (look at its components). ∎

4.5 The polarized maximal order case

Our next case is that of a p-divisible group G with a fixed subring $\mathcal{O} \subset \mathrm{End}(G)$ and given together with a principal quasi-polarization, an isomorphism

$$\lambda : G \longrightarrow G^t$$

which is anti-symmetric, $\lambda^t = -\lambda$. We assume that $\mathcal{O}$ is stable under the Rosati involution

$$\varphi \longmapsto i(\varphi) = \lambda^{-1}\varphi^t\lambda, \quad \varphi \in \mathrm{End}(G) \,.$$

To simplify our considerations, we only study the case $p \neq 2$. So we use the blanket assumption $\mathrm{char}\, k \neq 2$ is used throughout this section.

Notation 4.5.1. Denote $R = \mathcal{O} \otimes_{\mathbf{Z}_p} \Lambda$ and $\mathcal{M} = \mathbf{D}(G) \otimes_{W(k)} \Lambda$ as in the previous section. The quasi-polarization induces an isomorphism, which we also denote by λ,

$$\lambda : \mathcal{M} \longrightarrow \mathcal{M}^t \,.$$

This is an isomorphism of (left) R-modules if we give $\mathcal{M}^t$ the left R-module structure via the Rosati involution,

$$(r \cdot f)(x) = f(i(r) \cdot x), \quad f \in \mathcal{M}^t \,. \tag{23}$$

Notation 4.5.2. Denote by $\mathcal{D}$ the deformation data of Example 4.2.7 with our given ring $\mathcal{O}$ and the involution i induced by λ. Note that (G, G^t) becomes a $\mathcal{D}$-object of pDiv_k. By abuse of notation we will denote this object just by G. Hence we will also refer to $VG \subset MG$ as a $\mathcal{D}$-object of FMod_k and adopt similar notations for the deformations $\mathcal{G}_A$ of G to some $A \in Art_\Lambda$.

Remark. The deformation functor $\mathcal{D}\mathrm{ef}(G, \mathcal{D})$ is canonically isomorphic to the one defined in 4.1.4 (cf. 4.2.7),

$$\mathcal{D}\mathrm{ef}(G, \mathcal{D}) = \mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda) \,.$$

Denote also

$$\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, R, \lambda) = \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{D}) \,.$$

Remark. An element of $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)(A)$ is thus a p-divisible group $\mathcal{G}_A/A$ deforming G, which admits an $\mathcal{O}$-action and a principal quasi-polarizations reducing to those of G. An element of $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, R, \lambda)(A)$ is an $\mathcal{O}$-stable (eqivalently R-stable) totally isotropic filtration $\mathcal{V}_A \subset \mathcal{M}_A = \mathcal{M} \otimes_\Lambda A$ which reduces to $VG \subset MG$.

Theorem 4.5.3. *Let $\lambda : G \to G^t$ be a principal quasi-polarization. Let $\mathcal{O} \subset \mathrm{End}(G)$ be a Rosati-invariant $\mathbf{Z}_p$-subalgebra which is isomorphic to a hereditary order in a semi-simple $\mathbf{Q}_p$-algebra. Then there is a (non-canonical) isomorphism*

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda) \cong \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, R, \lambda) \,.$$

Proof. Let $\mathcal{D}$ be as above (see 4.5.2). We show that

$$\mathcal{D}\mathrm{ef}(G, \mathcal{D}) \cong \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{D})$$

by applying the main comparison theorem (4.3.8) to this situation. In order to do this, it suffices to prove that $MG = \mathbf{D}(G[p])$ is rigid as a $\mathcal{D}$-object. Let $A \twoheadrightarrow A'$ be a surjection in Art_Λ and $\mathcal{M}_{A'}$ a deformation of MG to A' as a $\mathcal{D}$-object. Hence $\mathcal{M}_{A'}$ is a finite free A'-module with an R-action and given together with a self-dual (left) R-module isomorphism $\mathcal{M}_{A'} \cong \mathcal{M}_{A'}^t$ (as in 4.5.1).

Let $\mathcal{M}_A^{(1)}$ and $\mathcal{M}_A^{(2)}$ be two deformations of $\mathcal{M}_{A'}$ to A (as a $\mathcal{D}$-object). We claim that they are isomorphic. Let

$$\Lambda^{(1)} : \mathcal{M}_A^{(1)} \longrightarrow (\mathcal{M}_A^{(1)})^t, \qquad \Lambda^{(2)} : \mathcal{M}_A^{(2)} \longrightarrow (\mathcal{M}_A^{(2)})^t \quad .$$

be the quasi-polarizations. By 2.2.5, there is an R-module isomorphism $\varphi : \mathcal{M}_A^{(1)} \to \mathcal{M}_A^{(2)}$ which reduces to the identity map on $\mathcal{M}_{A'}$. If, moreover, φ commutes with the Λ's,

that is, if $\Lambda^{(1)} = \varphi^t \Lambda^{(2)} \varphi$, then $\mathcal{M}_A^{(1)}$ and $\mathcal{M}_A^{(2)}$ are indeed isomorphic as $\mathcal{D}$-objects, as required. Otherwise, consider the maps

$$\varphi \qquad \text{and} \qquad (\Lambda^{(2)})^{-1}(\varphi^t)^{-1}\Lambda^{(1)} .$$

Both are R-module isomorphisms $\mathcal{M}_A^{(1)} \to \mathcal{M}_A^{(2)}$ which reduce to the identity on $\mathcal{M}_{A'}$. Hence their "average",

$$\psi = \frac{1}{2}\left(\varphi + (\Lambda^{(2)})^{-1}(\varphi^t)^{-1}\Lambda^{(1)}\right)$$

is also an R-module map which reduces to the identity on $\mathcal{M}_{A'}$. In particular (Nakayama's lemma), it is an isomorphism as well. Using the self duality of $\Lambda^{(1)}$ and $\Lambda^{(2)}$, it is easy to check that $\Lambda^{(1)} = \psi^t \Lambda^{(2)} \psi$. Hence ψ is the required isomorphism of $\mathcal{D}$-objects. This completes the proof. ∎

Remark. Given a triple $(G, \mathcal{O}, \lambda)$, it might be interesting to compare the structure of the deformation functors $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ and $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$. One can describe the latter functor as a fibre product functor

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda) = \mathcal{D}\mathrm{ef}(G, \mathcal{O}) \times_{\mathcal{D}\mathrm{ef}(G)} \mathcal{D}\mathrm{ef}(G, \lambda),$$

which presents the pro-representing ring of $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$ as a (completed) tensor product of the corresponding rings. Here $\mathcal{D}\mathrm{ef}(G)$ is the full deformation functor of the p-divisible group G, pro-represented by the formal power series ring $\Lambda[[t_1, \ldots t_{n^2}]]$ with $n = \dim G$. The functor $\mathcal{D}\mathrm{ef}(G, \lambda)$ of deformations of G which respect λ is pro-represented by $\Lambda[[t_1, \ldots t_{n(n+1)/2}]]$. Note however, that knowing abstractly the pro-representing ring of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ does not by itself give that of $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$. In fact, one needs to know how exactly the subfunctors $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ and $\mathcal{D}\mathrm{ef}(G, \lambda)$ "intersect" inside $\mathcal{D}\mathrm{ef}(G)$. For example assume that $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is formally smooth, i.e. it is pro-represented by a formal power series ring (in some number of variables) over Λ. It is not clear then that $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$ is formally smooth as well, as two regular subschemes of a regular scheme can have a singular intersection. Surprisingly, the formal smoothness of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ does imply that of $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$, as we show in the theorem below. The proof makes use of the fact that $\mathcal{O}$ is Rosati invariant (although not the actual involution on $\mathcal{O}$) and the "averaging" trick used in the proof of 4.5.3.

Theorem 4.5.4. *Let $\lambda : G \to G^t$ be a principal quasi-polarization. Let $\mathcal{O} \subset \mathrm{End}(G)$ be a Rosati-invariant $\mathbf{Z}_p$-subalgebra and assume that $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is formally smooth. Then $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$ is formally smooth as well.*

Proof. Let $A \twoheadrightarrow A'$ be a small extension in Art_Λ and $\mathcal{G}_{A'} \in \mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)(A')$. Hence $\mathcal{G}_{A'}/A'$ a deformation of G/k to which the quasi-polarization and the ring action lift. We have to show that there is a $\mathcal{G}_A \in \mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)(A)$ which deforms $\mathcal{G}_{A'}$. The formal smoothness of $\mathcal{D}\mathrm{ef}(G, \lambda)$ implies the existence of a deformation $\mathcal{G}_A^\lambda/A$ of $\mathcal{G}_{A'}$ which inherits the quasi-polarization. On the other hand, by formal smoothness of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$

there is also (another) deformation $\mathcal{G}_A^{\mathcal{O}}/A$ of $\mathcal{G}_{A'}$ to which the $\mathcal{O}$-action lifts. We are going to use the relation between λ and $\mathcal{O}$ (namely, the Rosati invariance) to show that there is a third lifting, $\mathcal{G}_A = \mathcal{G}_A^{\mathcal{O},\lambda}/A$ to which both λ and $\mathcal{O}$-action lift. In some sense, $\mathcal{G}_A^{\mathcal{O},\lambda}$ is going to be a combination of $\mathcal{G}_A^{\mathcal{O}}$ and $\mathcal{G}_A^{\lambda}$.

As in the proof of pro-representability 4.3.5, we use the results of Grothendieck-Messing. Associated to $\mathcal{G}_{A'}$ there is a universal extension filtration $V\mathcal{G}_{A'} \subset M\mathcal{G}_{A'}$. Since $A \twoheadrightarrow A'$ has divided powers, we can also define $M_A\mathcal{G}_{A'}$, the value of the universal extension crystal of $\mathcal{G}_{A'}$ on the ring A. This is a $\mathcal{D}$-object of Mod_A. There is a bijection between the deformations of $\mathcal{G}_{A'}$ to A (as a $\mathcal{D}$-object) and deformations of the filtration $V\mathcal{G}_{A'} \subset M\mathcal{G}_{A'}$ to a filtration of $M_A\mathcal{G}_{A'}$ (again, as a $\mathcal{D}$-object).

Fix an identification of Λ-modules $\ker(A \twoheadrightarrow A') \cong k$. By Theorem 2.3.2, the set of all deformations of $V\mathcal{G}_{A'} \subset M\mathcal{G}_{A'}$ to a filtration of $M_A\mathcal{G}_{A'}$ is a principal homogeneous space under $TG \otimes TG^t$. Thus, for any $\mathcal{G}_A$ deforming $\mathcal{G}_{A'}$, we can formally write

$$\mathcal{G}_A = \mathcal{G}_A^{\lambda} + \xi \tag{24}$$

for some $\xi \in TG \otimes TG^t$. Since it is easy to characterize the filtrations to which either λ or the $\mathcal{O}$-action lifts, the same is true for the deformations $\mathcal{G}_A$ of $\mathcal{G}_{A'}$ to A. Consider the composition s of the maps

$$TG \otimes TG^t \quad \overset{d\lambda \otimes d\lambda^{-1}}{\longrightarrow} \quad TG^t \otimes TG \quad \overset{i}{\longrightarrow} \quad TG \otimes TG^t \,.$$

Here i interchanges the two factors and $d\lambda : TG \longrightarrow TG^t$ is induced by $\lambda : G \to G^t$ on the tangent spaces. Then λ lifts to the deformation $\mathcal{G}_A$ as in 24 if and only if ξ is symmetric under s,

$$s(\xi) = \xi \,.$$

On the other hands, the liftings $\mathcal{G}_A$ which inherit the $\mathcal{O}$-action can be written as

$$\mathcal{G}_A = \mathcal{G}_A^{\mathcal{O}} + \eta, \qquad \eta \in \mathrm{H}^0(R\text{-}R\,, TG \otimes TG^t) \subset TG \otimes TG^t \,.$$

Write

$$\mathcal{G}_A^{\mathcal{O}} = \mathcal{G}_A^{\lambda} + \theta, \qquad \theta \in TG \otimes TG^t$$

From the relation 23, it follows that

$$s(\theta) - \theta \in \mathrm{H}^0(R\text{-}R\,, TG \otimes TG^t) \subset TG \otimes TG^t \,.$$

Thus both $\mathcal{G}_A^{\lambda} + \theta$ and $\mathcal{G}_A^{\lambda} + s(\theta)$ give deformations which inherit the $\mathcal{O}$-action. Hence so does

$$\mathcal{G}_A^{\mathcal{O},\lambda} = \mathcal{G}_A^{\lambda} + \frac{\xi + s(\xi)}{2}$$

It is also clear that $(\xi + s(\xi))/2$ is symmetric under s, so $\mathcal{G}_A^{\mathcal{O},\lambda}$ inherits both λ and the $\mathcal{O}$-action, as asserted. ∎

4.6 Non-rigid deformation problems

Let G/k be a p-divisble group. We have studied the deformation functors of G with an action of a maximal order $\mathcal{O}$ and/or a principal quasi-polarization λ. In many applications to abelian varieties, such as the study of CM-liftings or construction of abelian varieties with a given endomorphism ring, one is led to study a more general situation. This leads to consider a functor of the type

$$\mathcal{D} = \mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda_1, ..., \lambda_n, \mu_1, ..., \mu_m), \quad \lambda_i : G \to G^t,\ \mu_j : G^t \to G \tag{25}$$

where $\mathcal{O} \subset \mathrm{End}(G)$ is an arbitrary subring and λ_i, μ_j are quasi-polarizations, not necessarily principal. It is possible to reduce the study of such functors to a simpler case. Namely, there is an isomorphism

$$\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda_1, ..., \lambda_n, \mu_1, ..., \mu_m) \ \cong\ \mathcal{D}\mathrm{ef}(H, \mathcal{O}_H, \lambda_H) \tag{26}$$

for a certain choice of $H, \mathcal{O}_H$ and λ_H. In fact, take $H = G \times G^t$ and let i be the map $H = G \times G^t \to G^t \times G = H^t$ which interchanges the two factors. Then $\lambda_H = i \circ (1, -1)$ is a (principal) quasi-polarization on H. If the subring $\mathcal{O}_H \subset \mathrm{End}(H)$ happens to be a hereditary order in a semi-simple $\mathbf{Q}_p$-algebra, we can apply our previous results. Unfortunately, this is far from the case in general.

The ring $\mathcal{O}_H$ and the isomorphism (26) are established as follows. Let $\mathcal{D}$ be as in (25). Let $H = G \times G^t$ and decompose

$$\mathrm{End}(H) = \left(\begin{array}{c|c} \mathrm{End}(G) & \mathrm{Hom}(G, G^t) \\ \hline \mathrm{Hom}(G^t, G) & \mathrm{End}(G^t) \end{array}\right)$$

Define $\mathcal{O}_H \subset \mathrm{End}(H)$ to be

$$\mathcal{O}_H = \left\langle p_G, p_{G^t}, \left(\begin{array}{c|c} \varphi & 0 \\ \hline 0 & \varphi^t \end{array}\right)_{\varphi \in \mathcal{O}}, \left(\begin{array}{c|c} 0 & \lambda_i \\ \hline 0 & 0 \end{array}\right)_{1 \le i \le n}, \left(\begin{array}{c|c} 0 & 0 \\ \hline \mu_j & 0 \end{array}\right)_{1 \le j \le m} \right\rangle .$$

In other words, $\mathcal{O}_H$ is generated by the data defining $\mathcal{D}$ plus the projections p_G and p_{G^t} of H on the two factors. Take λ_H as above and consider

$$\mathcal{F} = \mathcal{D}\mathrm{ef}(H, \mathcal{O}_H, \lambda_H) .$$

We claim that $\mathcal{D} \cong \mathcal{F}$. Clearly a deformation $\mathcal{G} \in \mathcal{D}(A)$ for some $A \in Art_\Lambda$ gives also an element of $\mathcal{F}(A)$.

Conversely, take $\mathcal{H} \in \mathcal{F}(A)$. Define

$$\mathcal{G}_1 = \ker(p_G : \mathcal{H} \to \mathcal{H}), \quad \mathcal{G}_2 = \ker(p_{G^t} : \mathcal{H} \to \mathcal{H}) .$$

These are p-divisible groups over A which deform G and G^t. Since $p_G, p_{G^t} \in \mathrm{End}(\mathcal{H})$ are orthogonal idempotents, $\mathcal{H} \cong \mathcal{G}_1 \times \mathcal{G}_2$.

From the relation

$$p_{G^t} = \lambda_H^{-1} p_G^t \lambda_H$$

it follows that the lift of λ_H to a principal quasi-polarization on $\mathcal{H}$ identifies $\mathcal{G}_1^t$ with $\mathcal{G}_2$. So $H \cong \mathcal{G}_1 \times \mathcal{G}_1^t$.

Finally, from the commutation relation of the elements of $\mathcal{O}_H$ with the projections p_G, p_{G^t} it follows that every $\varphi \in \mathcal{O}$ lifts indeed to an endomorphism of $\mathcal{G}_1$, rather than just an endomorphism of $\mathcal{H}$. The same hold for λ_i and μ_j. So $\mathcal{G}_1 \in \mathcal{D}(A)$ as asserted.

Remark 4.6.1. The above argument clearly generalizes to a deformation problem with an arbitrary deformation data (cf. 4.2.2). Thus, given a deformation data $\mathcal{D}$ and a $\mathcal{D}$-object G of pDiv_k, there is an isomorphism

$$\mathcal{D}\mathrm{ef}(G, \mathcal{D}) \cong \mathcal{D}\mathrm{ef}(H, \mathcal{O}_H, \lambda_H)$$

for some p-divisible group H/k, a subring $\mathcal{O} \subset \mathrm{End}(H)$ and a principal quasi-polarization λ_H on H. This is, however, mostly of theoretical interest, as the deformation functors $\mathcal{D}\mathrm{ef}(H, \mathcal{O}_H, \lambda_H)$ can be extremely complicated in case $\mathcal{O}_H$ is not a maximal order.

4.7 The p-chain case

Although our computations in Chapter 4 concern primarily the deformation functors $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ and $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$, it is interesting to give an example of a slightly different kind. Here is a well-known deformation problem which involves more than one p-divisible group.

Let $\mathcal{D}$ be the deformation data of 4.2.8, a "p-chain of length n". As we already remarked, a $\mathcal{D}$-object of pDiv_A can be identified with a collection of p-divisible groups $\{\mathcal{G}_i/A\}$ indexed by $i \in \mathbf{Z}/n\mathbf{Z}$ and maps $f_i : \mathcal{G}_i \to \mathcal{G}_{i+1}$, such that

$$f_{i-1} f_{i-2} \cdots f_{i-n} = p \in \mathrm{End}(\mathcal{G}_i), \qquad i \in \mathbf{Z}/n\mathbf{Z}\,. \tag{27}$$

In particular, f_i are isogenies. We claim that in this situation the comparison theorem 4.3.8 applies:

Proposition 4.7.1. *Let G be a $\mathcal{D}$-object of* pDiv_k. *Then $\mathbf{D}(G[p])$ is a rigid $\mathcal{D}$-object of* Mod_k. *There is a non-canonical isomorphism of functors*

$$\mathcal{D}\mathrm{ef}(G, \mathcal{D}) \;\cong\; \mathcal{D}\mathrm{ef}_{\mathcal{M}}(VG \subset MG, \mathcal{D})\,.$$

Proof. Let G_i denote the p-divisible groups which form the p-chain and $f_i : G_i \to G_{i+1}$ the connecting maps. As usual, let $\mathcal{M}_i = \mathbf{D}(G_i)$ and $M_i = \mathbf{D}(G_i[p]) = \mathcal{M}_i \otimes_W k$. For any $i \in \mathbf{Z}/n$ choose a subspace $K_i \subset M_i$ such that $M_i = f_{i-1} M_{i-1} \oplus K_i$. The compositions

$$f_{i-1} \cdots f_{i-j} : \;\; M_{i-j} \longrightarrow M_i$$

map K_{i-j} injectively into M_i for $1 \le j < n$. Letting $f_{i-1} \cdots f_{i-j}$ denote the identity map for $j = 0$, we have

$$M_i = \bigoplus_{j=0}^{n-1} f_{i-1} \cdots f_{i-j} K_{i-j} \ .$$

If $\{\mathcal{M}_i\}$ is a deformation of M to $A \in Art_\Lambda$ as a $\mathcal{D}$-object, one obtains a similar decomposition: let $\mathcal{K}_i \subset \mathcal{M}_i$ be a finite free A-module which lifts $K_i \subset M_i$. Then, using Nakayama's lemma, one shows that

$$\mathcal{M}_i = \bigoplus_{j=0}^{n-1} f_{i-1} \cdots f_{i-j} \mathcal{K}_{i-j} \ .$$

It follows that every two $\mathcal{D}$-deformations of M to A are isomorphic. The second assertion of the proposition follows from Theorem 4.3.8. ∎

Remark 4.7.2. It is interesting to note that the condition (27) is essential for the rigidity. In fact, if one takes a chain of p-divisible groups (G_i, f_i) with, for instance, $\prod f_j = p^2$ instead, the corresponding deformation data is not rigid and the statement corresponding to 4.7.1 does not hold.

Remark 4.7.3. Proposition 4.7.1 allows to write down equations for the deformation functor $\mathcal{D}\mathrm{ef}(G, \mathcal{D})$ of a p-chain of p-divisible groups. There is, however, a different approach to study this functor. As in the previous section, it is possible to find an isomorphism

$$\mathcal{D}\mathrm{ef}(G, \mathcal{D}) \cong \mathcal{D}\mathrm{ef}(H, \mathcal{O}) \tag{28}$$

for certain p-divisible group H and a hereditary order $\mathcal{O} \subset \mathrm{End}(H)$.

Namely, let the p-chain in question be given by

$$G_n \xrightarrow{f_n} G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} G_{n-1} \xrightarrow{f_{n-1}} G_n \ .$$

Define $H = G_1 \oplus \cdots \oplus G_n$. Let $e_i \in \mathrm{End}(H)$ be the projector on the i-th factor and $f = (f_1, ..., f_n) \in \mathrm{End}(H)$. Let $\mathcal{O} \subset \mathrm{End}(H)$ be the $\mathbf{Z}_p$-subalgebra generated by the e_i and f. Then (28) holds.

The structure of $\mathcal{O}$ can be also easily determined. It is isomorphic to the subring of $\mathrm{Mat}_{n\times n}(\mathbf{Z}_p)$ given by

$$\mathcal{O} = \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ b_{2,1} & a_{2,2} & \dots & a_{2,n-1} & a_{2,n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ b_{n-1,1} & b_{n-1,2} & \dots & a_{n-1,n-1} & a_{n-1,n} \\ b_{n,1} & b_{n,2} & \dots & b_{n,n-1} & a_{n,n} \end{pmatrix}, \quad a_{i,j} \in \mathbf{Z}_p, b_{i,j} \in p\mathbf{Z}_p \right\} \ . \tag{29}$$

We refer to Section 5.3 for the proof of this statement (cf. 5.3.1) and a study of the deformation problem $\mathcal{D}\mathrm{ef}(H, \mathcal{O})$. There we discuss the case of a p-divisible group with an action of a maximal order a central division algebra over $\mathbf{Q}_p$, which leads to the same functor. In fact, these considerations also give an alternative proof of 4.7.1.

5 Computing the moduli

We are going to consider the deformation functor $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ in detail and present some examples. Throughout this chapter G is a p-divisible group over a perfect ground field k of characteristic p and $\mathcal{O}\subset\mathrm{End}(G)$ a hereditary order in a semi-simple $\mathbf{Q}_p$-subalgebra of $\mathrm{End}(G)\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$.

Let d,d',h denote the dimension of G, the dimension of the dual G^t and the height of G respectively. Thus $h=d+d'$.

Let $\Lambda=W=W(k)$ be the ring of Witt vectors of k. Thus the category Art_W is the category of all Artin local rings with residue field k. We let $R=\mathcal{O}\otimes_{\mathbf{Z}_p}W$.

Let $\mathcal{M}=\mathbf{D}(G)$ be the (covariant) Dieudonné module of G and let $V=VG$ and $M=MG$ denote the terms of the filtration on the Lie algebra of the universal extension,

$$0\longrightarrow VG\longrightarrow MG\longrightarrow TG\longrightarrow 0\,. \tag{30}$$

The representation of R on the tangent space G is denoted by ρ_τ.

Recall that our assumption on $\mathcal{O}$ implies that $\mathcal{M}$ is a projective R-module (Theorem 4.4.1). The functors $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V\subset M,R)$ and $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ are pro-representable (2.3.2,4.3.5). The projections

$$\mathcal{D}\mathrm{ef}(G,\mathcal{O})\to\mathcal{D}\mathrm{ef}(\rho_\tau),\qquad \mathcal{D}\mathrm{ef}_{\mathcal{M}}(V\subset M,R)\to\mathcal{D}\mathrm{ef}(\rho_\tau)$$

are formally smooth and there is a non-canonical isomorphism (Theorem 4.4.1)

$$\mathcal{D}\mathrm{ef}(G,\mathcal{O})\cong\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V\subset M,R)$$

which commutes with these projections.

Denote by $\mathcal{U}$ the pro-representing ring of $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V\subset M,R)$ (and hence of $\mathcal{D}\mathrm{ef}(G,\mathcal{O})$ as well). Our goal is to compute $\mathcal{U}$ in some cases.

Note that the proof of Theorem 2.3.2 gives the equations of the moduli space for any hereditary order $\mathcal{O}$, provided the action of $\mathcal{O}$ on the Dieudonné module of G is known. We state this result explictly as follows.

Theorem 5.0.4. *Let G/k be a p-divisible group and $\mathcal{O}\subset\mathrm{End}(G)$ a subring, which is a hereditary order in a semisimple $\mathbf{Q}_p$-algebra. Choose a basis $\{e_1,\dots,e_{d'},f_1,\dots,f_d\}$ of the Dieudonné module $\mathcal{M}=\mathbf{D}(G)$ over W, which lifts the respective bases of $V=VG$ and TG of the filtration on $M=MG=\mathcal{M}\otimes_W k$,*

$$0\longrightarrow V\longrightarrow M\longrightarrow TG\longrightarrow 0\,.$$

Write the action of $R=\mathcal{O}\otimes_{\mathbf{Z}_p}W$ on $\mathcal{M}$ in a block matrix form with the respect to this basis,

$$R\ni r\ \longmapsto\ \left(\begin{array}{c|c}A_r & B_r\\ \hline C_r & D_r\end{array}\right)\in\mathrm{End}(\mathcal{M})\,.$$

Let U be a $d \times d'$ matrix, whose entries u_{ij} are indeterminants. Then the pro-representing ring of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is

$$\mathcal{U} \cong W[[u_{ij}]]/J\ ,$$

where J is the ideal generated by the equations

$$UA_r + UB_rU - D_rU - C_r = 0, \quad r \in R\,. \tag{31}$$

Remark. An analogous result holds in the principally polarized case. The equations defining the functor $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R, \lambda)$ are (31) together with the symmetry equations $u_{ij} = u_{ji}$ if the basis is properly chosen.

Before we give the examples of computations, we state some simple reductions (Section 5.1) which allow to assume that the ring $\mathcal{O}$ has a relatively simple form. Then we determine the pro-representing ring in case $\mathcal{O}$ is the ring of integers in a quadratic extension of $\mathbf{Q}_p$ and give some higher-dimensional computations as well (Section 5.2). Then we look at the case of a maximal order in a division algebra with unramified center (Section 5.3), the case of one-dimensional p-divisible groups (Section 5.4) and the so-called canonical liftings (Section 5.5).

5.1 Preliminary reductions

Let W^0 be the fraction field of W and $R^0 = R \otimes_W W^0$. Since R^0 is a semisimple W^0-algebra, by the structure theorem (3.1.2) we have

$$R^0 \cong \mathrm{Mat}_{n_1 \times n_1}(S_1^0) \times \cdots \times \mathrm{Mat}_{n_k \times n_k}(S_k^0), \tag{32}$$

a product of matrix rings over division rings S_i^0. Each of the S_i^0 is central over a finite extension of W^0.

Reduction to the case of simple R

Assume that $R \cong R_1 \times R_2$. Then every R-module decomposes as a direct sum of an R_1-module and an R_2-module. In particular this applies to $\mathcal{M}, M, V$ and, similarly, to $\mathcal{M} \otimes_W A, \mathcal{V}_A$ for all A. Thus,

$$\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)(A) = \mathcal{D}\mathrm{ef}_{\mathcal{M}}(V_1 \subset M_1, R)(A) \times \mathcal{D}\mathrm{ef}_{\mathcal{M}}(V_2 \subset M_2, R)(A)\,.$$

On the level of the pro-representing rings,

$$\mathcal{U} \ \cong\ \mathcal{U}_1 \mathbin{\hat{\otimes}} \mathcal{U}_2\,.$$

Thus, we can assume that R^0 is simple rather than semi-simple. In view of the decomposition (32), this means that R^0 is a matrix ring over a division algebra.

Remark. Even if the original order $\mathcal{O} \subset \mathrm{End}(G)$ is simple, $R = \mathcal{O} \otimes_{\mathbf{Z}_p} W$ might not stay simple. In fact it is simple if and only if the center $Z(\mathcal{O}^0)$ stays a field after tensoring with W^0. This is equivalent to requiring that the field extensions $Z(\mathcal{O}^0)/\mathbf{Q}_p$ and $W^0/\mathbf{Q}_p$ have no isomorphic intermediate subfields (except $\mathbf{Q}_p$ itself).

Reduction to the case of a totally ramified center

Let W' be the maximal étale extension of R in the center $Z(R)$,

$$W \subset W' \subset Z(R)\,.$$

Then $\mathcal{M}, V, V_A$ etc. can be all naturally considered as W' modules. The ring W' is the ring of Witt vectors of some finite separable field extension k' of k.

Consider $\mathcal{M}$ a finite free W'-module and

$$\mathcal{M}_A = \mathcal{M} \otimes_W A = \mathcal{M} \otimes_{W'} W' \otimes_W A = \mathcal{M} \otimes_{W'} (A \otimes_W W')$$

as a base change of $\mathcal{M}$ to the ring $A \otimes_W W'$. Then an element $\{V_A \subset M \otimes_W A\}$ of $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)(A)$ is a filtration of $A \otimes_W W'$-modules which reduces to $\{V \subset M\}$. Thus, $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$ becomes a composition of functors

$$Art_W \longrightarrow Art_{W'} \longrightarrow Sets$$

Here the first functor is the base change $A \mapsto A \otimes_W W'$. The second one is $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$ but with $R, \mathcal{M}, V$ etc. considered over W'. If we denote its pro-representing ring by $\mathcal{U}'$, then

$$\mathcal{U} = \mathcal{U}' \otimes_W W'$$

Moreover, since W' was chosen as maximal étale, the center of R is totally ramified over W'. By this reduction we can assume that $Z(R)$ is totally ramified over W^0.

Remark. If k is algebraically closed, then every finite extension of W^0 is totally ramified and the discussion above becomes vacuous.

Reduction from $\mathrm{Mat}_{n\times n}(R)$ to R

Assume that $R \cong \mathrm{Mat}_{n\times n}(S)$, so R is a full matrix ring over another ring S. In particular this applies when S^0 is a division algebra and $R \subset R^0$ is a maximal order (rather than just hereditary).

Let Δ be a free S-module of rank n. The Morita equivalence ([34], 16.9, 16.16) gives an equivalence of categories

$$\begin{array}{ccc} \{\text{left } S\text{-modules}\} & \longrightarrow & \{\text{left } R\text{-modules}\} \\ N & \longmapsto & \mathrm{Hom}_S(\Delta, N) \cong N^{\oplus n}\,. \end{array} \tag{33}$$

Here R acts on $\mathrm{Hom}_S(\Delta, N)$ on the left via its natural linear action on Δ.

Now let $\mathcal{M}$ be an R-module (finite and free over W as above) and $V \subset M = \mathcal{M} \otimes_W k$ an R-stable filtration. Then there is an S-module $\mathcal{M}^S$ and a S-submodule V^S of M^S, which induce $\mathcal{M}$ and V respectively, via (33). Moreover, a deformation of V to a ring A

(as an R-module) is induced by a unique deformation of $\mathcal{V}^S$ to A (as an S-module). Hence

$$\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R) \;\cong\; \mathcal{D}\mathrm{ef}_{\mathcal{M}}(V^S \subset M^S, S)\,.$$

So the problem of determining the pro-representing ring $\mathcal{U}$ for $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$ reduces to a similar problem for the ring S.

As an application of the above reductions, we get a result of Kottwitz ([18], §5) on formal smoothness in the unramified case.

Theorem 5.1.1. *Let G/k be a p-divisible group and let $\mathcal{O} \subset \mathrm{End}(G)$ be of the form*

$$\mathcal{O}^0 \cong \mathrm{Mat}_{n_1 \times n_1}(\mathcal{O}_1) \times \cdots \times \mathrm{Mat}_{n_k \times n_k}(\mathcal{O}_k),$$

where $\mathcal{O}_i$ are maximal orders in (finite) unramified field extensions of $\mathbf{Q}_p$. Then $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is formally smooth over W. Moreover, if λ is a principal quasi-polarization on G whose Rosati involution stabilizes $\mathcal{O}$, then $\mathcal{D}\mathrm{ef}(G, \mathcal{O}, \lambda)$ is formally smooth over W as well.

Proof. The functor $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M)$ (no extra data) is formally smooth for any finite free W-module $\mathcal{M}$ and any filtration $V \subset M = \mathcal{M} \otimes_W k$. Thus, the formal smoothness of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ follows from the above reductions. The quasi-polarized case follows from 4.5.4. ∎

Remark 5.1.2. It follows that the pro-representing ring of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is

$$\mathcal{U} \cong W[[t_1, ..., t_n]], \quad n = \dim_k H^1(R\text{-}R\,, TG \otimes_k TG^t)\,.$$

Indeed, $\mathcal{D}\mathrm{ef}(G, \mathcal{O}) \cong \mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$ and the dimension of the tangent space of the latter functor is given by 2.3.2.

5.2 The commutative case

In this section we give some computation in case $\mathcal{O} \subset \mathrm{End}(G)$ is commutative. By the results of the previous section, $\mathcal{O}$ can be taken to be the maximal order in a field extension of $\mathbf{Q}_p$ in this case.

We have seen that the deformation functor Def(G,$\mathcal{O}$) is formally smooth in case $\mathcal{O}/\mathbf{Z}_p$ is unramified.

If $\mathcal{O}$ is ramified, the moduli space is usually highly singular. We illustrate this with two specific examples. First we look at the case of a maximal order in a quadratic field. Here it is possible to determine the equations of the deformation functor in all cases. The other example is the case $\mathcal{O} \cong W[\sqrt[h]{p}]$. Here we list some computations in low dimensions.

Example 5.2.1. Maximal order in a quadratic field.

Assume for simplicity that $\mathrm{char}\, k \neq 2$. Let $[K : \mathbf{Q}_p] = 2$ and $\mathcal{O} \subset K$ be the valuation ring of K. Let G be a p-divisible group over k with an $\mathcal{O}$-action. Take $R = \mathcal{O} \otimes_{\mathbf{Z}_p} W$ with $W = W(k)$. The following cases are possible.

Case 1. $R \cong W \times W$.

Index the components $W \cong W^{(1)} \times W^{(2)}$. Decompose $V = V^{(1)} \oplus V^{(2)}$ and $T = M/V$ as $T^{(1)} \oplus T^{(2)}$ correspondingly. The deformation functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is formally smooth and

$$\mathcal{U} \cong W[[t_1, ..., t_n]], \quad n = \dim V^{(1)} \dim T^{(1)} + \dim V^{(2)} \dim T^{(2)} .$$

Case 2. R is local and R/W is unramified.

In this case $\mathcal{M}$ is a free R-module and M, V and M/V free $l = R \otimes_W k$-modules. So $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is formally smooth and

$$\mathcal{U} \cong W[[t_1, ..., t_n]], \quad n = \frac{d}{2}\frac{d'}{2} .$$

Case 3. R is local and R/W is ramified.

Write $R = W[\sqrt{\pi}]$ with with $(\pi) = m_W$. The module $\mathcal{M}$ is free of rank $(d + d')/2$ over R. The action of $\sqrt{\pi}$ on $\mathcal{M}$ can be therefore described by a matrix

$$\sqrt{\pi}: \quad \begin{pmatrix} 0 & I \\ \pi I & 0 \end{pmatrix} \in \mathrm{End}_W(\mathcal{M})$$

in some basis. Here I is the identity matrix of size $(d + d')/2$. However, we have to take into account the filtration $V \subset M$. It is easy to see that there a basis $\{e_1, ..., e_{d'}, f_1, ..., f_d\}$ of $\mathcal{M}$ (as in the Theorem 5.0.4) in which the action of $\sqrt{\pi}$ takes the form

$$\sqrt{\pi}: \quad \left(\begin{array}{cc|cc|cc} 0 & I_{r'} & & & & \\ \pi I_{r'} & 0 & & & & \\ \hline & & 0 & I_s & & \\ & & \pi I_s & 0 & & \\ \hline & & & & 0 & I_r \\ & & & & \pi I_r & 0 \end{array}\right) \in \mathrm{End}_W(\mathcal{M}) . \tag{34}$$

Here I_x denotes the $x \times x$ identity matrix. We have

$$d = 2r + s, \quad d' = 2r' + s .$$

The equations which decribe the moduli space are (31) applied to $\sqrt{\pi} \in R$. Thus let $A_{\sqrt{\pi}}, B_{\sqrt{\pi}}, C_{\sqrt{\pi}}$ and $D_{\sqrt{\pi}}$ be the blocks of (34) separated by the boldface lines. Computation shows that the solutions of (31) are given in a block matrix form by the matrices

$$\begin{array}{c} \\ s \\ r \\ r \end{array} \begin{array}{c} \begin{array}{ccc} r' & r' & s \end{array} \\ \begin{pmatrix} -U_{13}U_{12} & U_{12} & U_{13} \\ U_{32} - U_{23}U_{12} & U_{22} & U_{23} \\ \pi U_{22} - U_{23}U_{13}U_{12} & U_{32} & U_{23}U_{13} \end{pmatrix} \end{array} = U ,$$

where $U_{12}, U_{22}, U_{23}, U_{32}$ are arbitrary and U_{13} satisfies $U_{13}^2 = \pi I_s$. Hence the pro-representing ring of the deformation functor is given by

$$\mathcal{U} \cong W[[t_1, ..., t_n]]\,[[u_{ij}]]/J, \quad n = rs + 2rr' + r's, \quad 1 \le i, j \le s$$

where J is the ideal expressing the matrix relation $\{u_{ij}\}^2 = \pi I_s$.

Note the two particular instances of this example:

If $s = 0$ then the deformation functor is formally smooth of dimension $\frac{d}{2}\frac{d'}{2}$ over W, as in the unramified case.

On the other hand, if $d = d'$ and $r = r' = 0$, then the defining equations are just $\{u_{ij}\}^2 = \pi I_s$ with $1 \le i, j \le d$. This is for example the case when a (ramified at p) quadratic field acts diagonally on a product of elliptic curves. Note also that in this case the pro-representing ring is highly singular. Indeed, the tangent space of $\mathcal{U}$ is n^2-dimensional (i.e. maximal possible), while the dimension of the ring itself is actually much smaller.

Example 5.2.2. $\mathcal{O} = \mathbf{Z}_p[\sqrt[h]{\pi}]$)

Take $\mathcal{O} = \mathbf{Z}_p[\sqrt[h]{\pi}]$ with $\pi \in m_W$ and $R = \mathcal{O} \otimes_{\mathbf{Z}_p} W$. Let G/k be a p-divisible group of height $h = d + d'$ with an $\mathcal{O}$-action. This is a "complex multiplication" case, in a sense that $\mathcal{O} \subset \mathrm{End}(G)$ has a largest possible rank (namely h) for a commutative subring.

We sketch the results of our computations. The tangent space to $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ has dimension $\min(d, d')$. The functor is formally smooth if and only if $d = 0$ or $d' = 0$, in which case the pro-representing ring is W. Some of the low-dimensional examples are presented in the following table.

Note that, by duality, we can reduce to the case $d \le d'$.

d	d'	Pro-representing ring of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$
1	any	$W[x]/\left(x^{d'} - \pi \right)$
2	2	$W[x,y]/\left(2xy + y^3, x^2 + xy^2 - \pi \right)$
2	3	$W[x,y]/\left(x^2 + 3xy^2 + y^4, 2x^2y + xy^3 - \pi \right)$
2	4	$W[x,y]/\left(3x^2y + 4xy^3 + y^5, x^3 + 3x^2y^2 + xy^4 - \pi \right)$
3	3	$W[x,y,z]/\left(yz^3 + 2y^2z + 2xy + xz^2, z^4 + 3yz^2 + 2xz + y^2, xz^3 + 2xyz + x^2 - \pi \right)$

5.3 Maximal order in a division algebra with unramified center

We keep the notations of the introduction to this chapter. In this section we study the case when $\mathcal{O}$ is the maximal order in a division algebra D whose center is a (finite) unramified extension $K/\mathbf{Q}_p$.

We begin with the structure of $R = \mathcal{O} \otimes_{\mathbf{Z}_p} W$ in this case.

An arbitrary finite extension $K/\mathbf{Q}_p$ can be filtered by intermediate subfields

$$\mathbf{Q}_p \subset K^W \subset K^{\mathrm{un}} \subset K$$

where K^{un} is the maximal unramified extension of $\mathbf{Q}_p$ inside K and K^W is the maximal subfield of K which is isomorphic to a subfield of $W^0 = W \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Note that $W^0/\mathbf{Q}_p$ is unramified, whence the inclusion $K^W \subset K^{\mathrm{un}}$. Let $\Omega^W, \Omega^{\mathrm{un}}$ and Ω denote the rings of integers of K^W, K^{un} and K respectively.

First, we can reduce the computation of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ to the case $K^W = K^{\mathrm{un}}$. This can be achieved by replacing $W = W(k)$ by a $W' = W(k')$ for a finite extension k'/k as described in Section 5.1.

Second, since Ω^W is contained in $\mathcal{O}$, the base changed ring $\mathcal{O} \otimes_{\mathbf{Z}_p} \Omega^W$ is isomorphic to a product of $m = [K^W : \mathbf{Q}_p]$ copies of $\mathcal{O}$. Hence

$$\begin{aligned} R &= \mathcal{O} \otimes_{\mathbf{Z}_p} W = (\mathcal{O} \otimes_{\mathbf{Z}_p} \Omega^W) \otimes_{\Omega^W} W = (\mathcal{O} \times \cdots \times \mathcal{O}) \otimes_{\Omega^W} W \\ &= (\mathcal{O} \otimes_{\Omega^W} W) \times \cdots \times (\mathcal{O} \otimes_{\Omega^W} W)\,. \end{aligned}$$

The p-divisible group G decomposes $G = G_1 \oplus \cdots \oplus G_m$ and the study of the deformation functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ can be reduced to that of $\mathcal{D}\mathrm{ef}(G_i, \mathcal{O})$ for $1 \le i \le m$.

Thus assume that $\mathbf{Q}_p = K^W = K^{\mathrm{un}}$. To justify the title of this section, assume further that $K/\mathbf{Q}_p$ is unramified, $K^{\mathrm{un}} = K$. In summary, we assume that D is a finite-dimensional central $\mathbf{Q}_p$-algebra and $\mathcal{O} \subset D$ the maximal order.

By Theorem 4.4.1, the functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is isomorphic to the deformation functor of the universal filtration $\mathcal{D}\mathrm{ef}(VG \subset MG, R)$ where $R = \mathcal{O} \otimes_{\mathbf{Z}_p} W$. The Dieudonné module $\mathbf{D}(G)$ is an R-module and $VG \subset MG = \mathbf{D}(G) \otimes_W k$ is an $R \otimes_W k$-filtration. So we need to know the structure of these rings to study $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$. The ring $R = R_W$ has the following shape ([34]):

Notation. Let $A \in Art_W$. Denote by R_A the A-algebra of matrices

$$R_A = \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ b_{2,1} & a_{2,2} & \dots & a_{2,n-1} & a_{2,n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ b_{n-1,1} & b_{n-1,2} & \dots & a_{n-1,n-1} & a_{n-1,n} \\ b_{n,1} & b_{n,2} & \dots & b_{n,n-1} & a_{n,n} \end{pmatrix}, \quad a_{i,j} \in A, b_{i,j} \in pA \right\}. \tag{35}$$

Denote by Mod_{R_A} the category of R_A-modules which are finite and free over A. Note that $R_A \cong R_W \otimes_W A$. In order to study the structure of the R_A-modules, we introduce further the following basic elements:

$$e_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \ \dots \ , e_n = \begin{pmatrix} 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

and

$$\pi = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ p & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

To ease the notation (cf. (37) below), we will think of the indices of the e_i as being in $\mathbf{Z}/n\mathbf{Z}$, so we let $e_{n+1} = e_1$ etc.

Clearly e_i are orthogonal idempotents,

$$e_i^2 = e_i, \qquad e_i e_j = 0 \quad (i \neq j), \qquad \sum_{i=1}^{n} e_i = 1\,. \tag{36}$$

Further

$$\pi^n = p \qquad \text{and} \qquad e_i \pi = \pi e_{i+1}\,. \tag{37}$$

The ring R_A is generated (as an A-algebra) by the e_i and π subject to (36) and (37). This allows to describe the structure of R_A-modules as follows.

Lemma 5.3.1. *Let $M \in \mathrm{Mod}_{R_A}$ be an R_A-module. Then M decomposes as a direct sum of A-modules,*

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n, \qquad M_i = e_i M\,.$$

The element $e_i \in R_A$ acts as identity on M_i and as zero on M_j for $j \neq i$. The element $\pi \in R_A$ maps M_i to M_{i-1}, so we get a sequence of A-modules and A-module maps:

$$M_n \xleftarrow{\pi_1} M_1 \xleftarrow{\pi_2} M_2 \xleftarrow{\pi_3} \cdots \xleftarrow{\pi_{n-1}} M_{n-1} \xleftarrow{\pi_n} M_n\,. \tag{38}$$

The cyclic composition $\pi_{i+1}\pi_{i+2}\cdots\pi_{i-1}\pi_i$ is multiplication by p on M_i. Conversely, given A-modules M_i for $i \in \mathbf{Z}/n\mathbf{Z}$ and maps $\pi_i : M_i \to M_{i-1}$ every of whose cyclic compositions equals p, there is a unique R_A-module M which gives this data.

Remark 5.3.2. The above lemma can be also formulated in the form of an equivalence of categories between Mod_{R_A} and the category of data $\{M_i, \pi_i\}$ satisfying the above conditions.

Proof of 5.3.1. The decomposition (38) is a consequence of the fact that e_i are orthogonal idempotents, so they generate a subring of R_A isomorphic to $A \times A \times \cdots \times A$.

To find the action of π on the M_i, we use the relation $e_i\pi = \pi e_{i+1}$. Since $e_i \pi e_j = \pi e_{i+1} e_j$ which is zero for $j \neq i+1$, it follows that $e_i \pi = 0$ on M_j for $j \neq i+1$. So π

maps M_k to M_{k-1} for all k. The assertion on the cyclic composition follows from the fact that $\pi^n = p$.

Conversely, suppose given finite free A-modules M_i and A-module maps $\pi_i : M_i \to M_{i-1}$ whose cyclic compositions equal p. Let $M = M_1 \oplus \cdots \oplus M_n$ and define the R_A-module structure on M as follows.

Let $e_i \in R_A$ act as identity on M_i and as zero on M_j for j different from i. Let π act as π_i on M_i. Extend by linearity to an action of π and the e_i on the whole of M. It is easy to check that the relations (36) and (37) are satisfied, so we obtain indeed an R_A-action. Remark 5.3.2 is obvious. ∎

Example. Let $M \cong R_A$, a free R_A-module of rank 1. Then M decomposes as a direct sum of R_A-modules $M = S_A^{(1)} \oplus \cdots \oplus S_A^{(n)}$. Namely, let $S^{(i)} = S_A^{(i)}$ consist of those matrices of (35) which are zero outside the i-th column. Applying the decomposition of (5.3.1) to $S^{(i)}$, we find that the components $S_j^{(i)}$ are all one-dimensional and the maps

$$S_n^{(i)} \xleftarrow{\pi_1} S_1^{(i)} \xleftarrow{\pi_2} S_2^{(i)} \xleftarrow{\pi_3} \cdots \xleftarrow{\pi_{n-1}} S_{n-1}^{(i)} \xleftarrow{\pi_n} S_n^{(i)} . \tag{39}$$

are all identity except π_i, which is multiplication-by-p. It follows that $S^{(i)}$ are indecomposable. Further, $S^{(i)}$ are R_A-projective, as they are direct summands of a free R_A-module. In fact, every projective R_A-module is a sum of the $S^{(i)}$:

Proposition 5.3.3. *Every projective R_A-module M is a direct sum of $S_A^{(i)}$. An R_A-module M is projective if and only if $M \otimes_A k$ is R_k-projective.*

Proof. First assume $A = k$.

We claim that every (finitely generated) projective R_k-module M is a direct sum of the $S_k^{(i)}$.

It is easy to see that M is free over the subring P of R_k,

$$P = k[\pi] \cong k[t]/t^n .$$

Decompose $M = M_1 \oplus \cdots \oplus M_n$ as in 5.3.1. Filter each of the M_i by letting $F_i = \ker \pi_i \subset M_i$. Finally choose $e_{ij} \in M_i, 1 \le j \le k_i$ such that $\{e_{ij}\}_{1 \le j \le k_i}$ reduces to a basis of M_i/F_i as a k-vector space. It is then not difficult see that $R_k e_{ij} \subset M$ is a submodule isomorphic to S_i and that

$$M = \sum_{i,j} R_k e_{ij}$$

is a direct sum (see the proof of 5.3.5, parts 1 and 2 for a detailed proof).

Now let $A \in Art_W$ be arbitrary. If an R_A-module M is projective, then it is a direct summand of a free R_A-module. Tensoring with k shows that $M \otimes_A k$ is a direct summand of a free R_k-module, hence projective.

Conversely, assume that $M \otimes_A k$ is projective. Then

$$M \otimes_A k \cong \sum (S_k^{(i)})^{n_i}, \qquad \text{some } n_i \in \mathbf{Z} .$$

Let

$$M' = \sum (S_A^{(i)})^{n_i}$$

Then M' is a (projective) R_A-module and $M' \otimes_A k \cong M \otimes_A k$. From Corollary 2.2.5, it follows that $M \cong M'$. ∎

Remark 5.3.4. Let $A = W = W(k)$. Since R_W is a hereditary order, every R_W-module, which is finite and free as W-module, is R_W-projective. In particular, this applies to the Dieudonné module $\mathcal{M} = \mathbf{D}(G)$. It follows from the above proposition, that one can find a basis $\{e_j\}_{j\in J}$ of $\mathcal{M}$ over W, such that every πe_j is either equal to e_k or pe_k for some $k \in J$. Such a basis, therefore, respects

(1) The action of π on $\mathcal{M}$.

(2) The decomposition $\mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_n$, i.e. the action of e_i on $\mathcal{M}$.

On the other hand, the module $\mathcal{M}$ comes with a filtration $V \subset M = \mathcal{M} \otimes_W k$. So it is desirable to be able to choose a basis $\{e_j\}_{j\in J}$ as above, but with the additional property that $J = J_V \amalg J_{M/V}$ and $\{e_j\}_{j\in J_V}$ and $\{e_j\}_{j\in J_{M/V}}$ reduce to bases of V and M/V respectively. In other words, this basis is also supposed to respect

(3) The filtration $V \subset M = \mathcal{M} \otimes_W k$.

In fact such a basis exists (5.3.5 below). This allows, for instance, to classify the possible equations of the moduli space of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$, at least in the low-dimensional cases.

Theorem 5.3.5. *There is a basis $\{e_j\}_{j\in J}$ of $\mathcal{M}$ as a W-module which respects (1), (2) and (3) of 5.3.4 as described above.*

Proof. We proceed in three steps, adding an extra condition on each step. We start by describing those bases of $\mathcal{M}$ which satisfy just the condition (1) of 5.3.4.

1. Consider the action of π on M. For any $0 \le k \le n$, we have $\operatorname{Im}\pi^k = \ker \pi^{n-k}$ on M (with $\pi^0 = \mathrm{id}_M$). This follows immediately from the fact that this equality is true for finite free R_k modules (by inspection), and hence for projective ones as well. Consequently, the natural filtrations of M by the images and the kernels of π^k coincide,

$$\begin{array}{ccccccccccc} 0 = & \pi^n M & \subset & \pi^{n-1} M & \subset & \cdots & \subset & \pi M & \subset & \pi^0 M & = M \\ & \| & & \| & & & & \| & & \| & \\ 0 = & \ker \pi^0 & \subset & \ker \pi & \subset & \cdots & \subset & \ker \pi^{n-1} & \subset & \ker \pi^n & = M \end{array} \tag{40}$$

It follows that the consecutive quotients in this filtration are all isomorphic to $M/\pi M$,

$$\pi^k : M/\pi M \quad \xrightarrow{\sim} \quad \pi^k M/\pi^{k+1} M \,. \tag{41}$$

Indeed, the above map is injective,

$$\pi^k x \in \pi^{k+1} M \iff \pi^k x \in \ker \pi^{n-k-1} \iff x \in \ker \pi^{n-1} \iff x \in \pi M \,.$$

We can now construct a W-basis of $\mathcal{M}$ which satisfies (1) of 5.3.4, starting with a similar k-basis of M. Take an arbitrary k-basis $\{\bar\rho_j\}_j$ of $M/\pi M$ and choose representatives $\rho_j \in M$ of $\bar\rho_j$. Then for any $0 \le k < n$, the set $\{\pi^k \rho_j\}_j$ gives a basis of $\pi^k M/\pi^{k+1}M$, thanks to the isomorphism (41). It follows that $B = \{\pi^k \rho_j\}_{j,0\le k<n}$ is a k-basis of M. Moreover, for any $v \in B$ either $\pi v \in B$ or $\pi v = 0$.

Finally, lift ρ_j to arbitrary elements $\varrho_j \in \mathcal{M}$. Then $\{\pi^k \varrho_j\}_{j,0\le k<n}$ is easily seen to be a W-basis of $\mathcal{M}$ which satisfies the condition (1) of 5.3.4. Conversely, every such basis is easily seen to come from our construction.

2. As a second step, we show how to determine those bases which satisfiy both (1) and (2) of 5.3.4. By 5.3.1, M decomposes as $M = M_1 \oplus \cdots \oplus M_n$ with respect to the action of the idempotents $e_i \in R_k$. Every R_k-submodule $N \subset M$ also decomposes $N = N_1 \oplus \cdots \oplus N_n$ with $N_i \subset M_i$. This applies to the steps of the filtration (40). Indeed, $\ker \pi^k|_M$ is an R_k-submodule of M, as immediately follows from the defining equations (36) and (37). Hence $M/\pi M$ also decomposes as a direct sum,

$$M/\pi M = M_1/\pi M_2 \oplus M_2/\pi M_3 \oplus \cdots \oplus M_n/\pi M_1 \,. \tag{42}$$

(Note that $\pi M \cap M_i = \pi M_{i+1}$, which is used to obtain this decomposition.) Now we apply the construction of the first step of the proof. Instead of starting from an arbitrary k-basis of $M/\pi M$, we choose a basis $\{\bar\rho_j\}_j$ of $M/\pi M$ which respects (42). Also we do not lift $\bar\rho_j \mapsto \rho_j$ and $\rho_j \mapsto \varrho_j$ arbitrarily, but preserving the decompositions $M = \bigoplus_i M_i$ and $\mathcal{M} = \bigoplus_i \mathcal{M}_i$. Then $\{\pi^k \varrho_j\}_{j,0\le k<n}$ is easily seen to be a W-basis of $\mathcal{M}$ which satisfies the conditions (1) and (2) of 5.3.4.

Note also that $\{\rho_j\}_j$ is a basis of M as a $W[\pi]$-module and that the submodules

$$R_k\rho_j = \langle \rho_j, \pi\rho_j, \ldots, \pi^{n-1}\rho_j \rangle$$

are isomorphic to $S_W^{(i_j+1)}$ where i_j are the indices such that $\rho_j \in M_{i_j}$. This provides the promised detailed proof of 5.3.3. (We only used that M is a projective R_k-module in this construction).

3. Finally, we show how to choose a basis which satisfies (1), (2) and (3). The filtration $V \subset M$ is R_k-stable, so it also decomposes

$$V = \bigoplus_i V_i \;\subset\; \bigoplus_i M_i = M \,.$$

Consider the subsets $\pi^{-k}V_{i-k}$ of M_i,

$$\pi^{-k}V_{i-k} = \{v \in M_i \mid \pi^k v \in V_{i-k}\} \,.$$

Then M_i becomes filtered,

$$0 \subset V_i \subset \pi^{-1}V_{i-1} \subset \pi^{-2}V_{i-2} \subset \cdots \subset \pi^{-n}V_{i-n} = M_i \,. \tag{43}$$

This induces a filtration on $M_i/\pi M_{i+1}$,

$$0 \subset \frac{V_i+\pi M_{i+1}}{\pi M_{i+1}} \subset \frac{\pi^{-1}V_{i-1}+\pi M_{i+1}}{\pi M_{i+1}} \subset \cdots \subset \frac{\pi^{-n}V_{i-n}+\pi M_{i+1}}{\pi M_{i+1}} = \frac{M_i}{\pi M_{i+1}} ,$$

which can be also written as

$$0 \subset \frac{V_i}{V_i \cap \pi M_{i+1}} \subset \frac{\pi^{-1}V_{i-1}}{\pi^{-1}V_{i-1} \cap \pi M_{i+1}} \subset \cdots \subset \frac{\pi^{-n}V_{i-n}}{\pi^{-n}V_{i-n} \cap \pi M_{i+1}} = \frac{M_i}{\pi M_{i+1}} .$$

Choose a basis of $M_i/\pi M_{i+1}$ which respects this filtration and lift it to M_i using the natural surjections from (43). Combining these vectors for various i, we get a subset $\{\rho_j\}_j$ of M. Finally, as described in part 2 of the proof, lift these elements to a subset $\{\varrho_j\}_j$ of $\mathcal{M}$, respecting $\mathcal{M} = \bigoplus_i \mathcal{M}_i$. We get a basis of $\mathcal{M}$ as a W-module which satisfies (1) and (2) of 5.3.4. We claim that the condition (3) is fulfilled as well. Indeed, each V_i is a direct sum of subspaces

$$V_{i,j} = \pi^j \frac{\pi^{-j}V_{i-j}}{\pi^{-j}V_{i-j} \cap \pi M_{i+1}}, \quad 0 \leq j < n,$$

each of which is spanned by a subset of $\{\rho_j\}_j$ of M. This completes the proof. ∎

The existence of a basis as in Theorem 5.3.5 allows to determine the possible moduli spaces of the type that we are considering for a given W-rank of $\mathcal{M}$. To give an impression of the kind of equations that one obtains, we present some general and some low-dimensional examples. We denote by U the pro-representing ring of $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$.

Example 5.3.6. If $V = \{0\}$ or $V = M$, then $U \cong W$. In fact, if G/k is an étale-local or a local-étale p-divisible group, then G can be uniquely deformed to any $A \in Art_W$ and all endomorphisms of G lift to these unique deformations.

Example 5.3.7. Recall that $V = \oplus_i V_i$ with $V_i \subset M_i$. If $\dim_k V_i \neq \dim_k V_j$ for some i, j, then $\mathcal{D}\mathrm{ef}(G, \mathcal{O})(A) = \emptyset$ for any A in which $p \neq 0$. So a necessary condition for $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ to have non-characteristic-p points is that $\dim_k V_i = \dim_k V_j$ for all i, j. This is the so-called Kottwitz determinant condition in our case.

Example 5.3.8. If V is a projective R_k-module, then $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is formally smooth. This follows from 4.4.1 since the deformation functor of the tangent space representation is trivial in this case. In other words, U is a formal power series ring over W.

Example 5.3.9. Let $m = 1$ and $n \geq 1$ be arbitrary. After renumbering the M_i if necessary, we can assume that $\pi M_1 = 0$ and $\pi M_i = M_{i-1}$ for $i \neq 1$. The corresponding picture of the basis elements of 5.3.5 is then

$$q_0 \xleftarrow{p} v_1 \longleftarrow v_2 \longleftarrow \cdots \longleftarrow v_j \longleftarrow q_{j+1} \longleftarrow \cdots \longleftarrow q_n = q_0 ,$$

where $j = \dim_k F$ and $\{v_i\}$ resp. $\{q_i\}$ denote the parts of the basis as in 5.3.5 which reduce to the basis of V resp. the basis of M/V. The pro-representing ring U of $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$ is given by

$$\begin{cases} W, & j = 0 \text{ or } j = n, \\ k, & 1 \leq j \leq n-1 . \end{cases}$$

This illustrates both 5.3.6 and 5.3.7.

Example 5.3.10. Another example, the so-called Drinfeld case, is given in [33], Chapter 3. In fact, in [33] it is assumed that the division algebra in question has a Brauer invariant $1/n$. However, the answer does not depend on the Brauer invariant, since the structure of R is independent of it.

Let $\dim_k V_i = 1$ for all i. For any i either $\pi V_i = 0$ or $\pi V_i = V_{i-1}$. Let r be the number of $i \in \mathbf{Z}/n\mathbf{Z}$ for which $\pi V_i = 0$, i.e. the number of *critical indices*. Then

$$U \cong W[[t_1, ..., t_m]]/(\prod t_i - p) .$$

By condidering higher-dimensional analogues of this example, it is easy to construct examples with

$$U \cong W[[A_1, ..., A_m]]/J . \tag{44}$$

where A_j are (not necessarily square) matrices which consist of indeterminants and J is the ideal which expresses the relations

$$\begin{aligned} A_1 A_2 \cdots A_{m-1} A_m &= p \times \text{ identity} \\ A_2 A_3 \cdots A_m A_1 &= p \times \text{ identity} \\ \cdots &\quad \cdots \\ A_m A_1 \cdots A_{m-2} A_{m-1} &= p \times \text{ identity} . \end{aligned}$$

Example 5.3.11. Not every filtration with $\dim_k V_i = \dim_k V_j$ for $i, j \in \mathbf{Z}/n\mathbf{Z}$. gives a deformation problem of the type described in the previous example. For instance, let $n = 3$, $\dim_k M = 12$. Let the filtration $V \subset M$ and the action of π on M be given by

$$\begin{array}{ccccccccc} \mathcal{M} & = & \mathcal{M}_1 & & \oplus & & \mathcal{M}_2 & & \oplus & & \mathcal{M}_3 \\ & & v_1 & \longleftarrow & q_2 & \longleftarrow & q_3 & \overset{p}{\longleftarrow} & v_1 \\ & & v_4 & \longleftarrow & q_5 & \overset{p}{\longleftarrow} & v_6 & \longleftarrow & v_4 \\ & & q_7 & \overset{p}{\longleftarrow} & v_8 & \longleftarrow & v_9 & \longleftarrow & q_7 \\ & & q_{10} & \overset{p}{\longleftarrow} & v_{11} & \longleftarrow & q_{12} & \longleftarrow & q_{10} . \end{array}$$

Thus $\{v_i\}$ is a basis of V, $\{q_i\}$ gives a basis of M/V and the arrows $\longleftarrow$ resp. $\overset{p}{\longleftarrow}$ indicate that the given basis element is mapped to the following basis element resp. p times the following basis element. A computation shows that the pro-representing ring of $\mathcal{D}\mathrm{ef}_{\mathcal{M}}(V \subset M, R)$ is given by

$$U \cong W[[A, B, C, D, E, F, G]]/(AF + BE, BC - p, FG + FAD - p, AC + EG + EAD) .$$

This is clearly not isomorphic to a ring of the form (44) for any choice of the A_i.

5.4 One-dimensional formal groups

We keep the notations of the introduction to this chapter. We assume further that the p-divisible group G is one-dimensional. Let R denote $\mathcal{O} \otimes_{\mathbf{Z}_p} W$, as usual.

The representation ρ_τ of R on the tangent space of G is simply a homomorphism

$$\rho_\tau : R \longrightarrow k \, . \tag{45}$$

Moreover a deformation of ρ_τ to a ring A is just a deformation of this homomorphism to a homomorphism (of W-algebras) $R \to A$. Thus $\mathcal{D}\mathrm{ef}(\rho_\tau)$ is pro-represented by R itself or, rather, by the following ring:

Notation. Write the abelianization $R/[R,R]$ as a product of local factors,

$$R/[R,R] \cong S_1 \times S_2 \times \cdots \times S_k \, .$$

Let $R^{(c)}$ denote the unique factor which has a non-zero image under (45).

Remark. Clearly $R^{(c)} \in \widehat{Art}_W$ if we let the augmentation $R^{(c)} \to k$ to be induced by (45). Moreover,

$$\mathrm{Hom}_W(R, -) \cong \mathrm{Hom}_W(R^{(c)}, -)$$

as functors on Art_W.

Theorem 5.4.1. *Let G/k be a one-dimensional p-divisible group and $\mathcal{O} \subset \mathrm{End}(G)$ a hereditary order in a finite-dimensional semisimple $\mathbf{Q}_p$-algebra. Then $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is pro-represented by a ring of the form*

$$\mathcal{U} \;\cong\; R^{(c)}[[t_1, ..., t_m]] \, .$$

Proof. This is an application of Theorem 4.4.1. ∎

Remark 5.4.2. In case $\mathcal{O}$ is commutative, this result is due to Lubin-Tate [19]; see also Drinfeld [8], Prop. 4.2.

5.5 Canonical liftings

In this section we present a computation of slightly different kind. Here we use the explicit structure of the tangent and the obstruction space to $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$, which is independent of the fact whether or not $\mathcal{O}$ is a maximal order.

Let G/k be p-divisible group over a perfect field and $\varphi \in \mathrm{End}_k G$ an arbitrary endomorphism.

Definition 5.5.1. We say that φ is *canonically liftable* if for any $A \in Art_W$ there is a unique lifting of (G, φ) to A, that is, a p-divisible group $\mathcal{G}/A$ and $\Phi \in \mathrm{End}_A(\mathcal{G})$, such that $\mathcal{G} \otimes_A k = G$ and $\Phi \otimes_A k = \varphi$.

Remark. In terms of the deformation functor,

$$\varphi \text{ is canonically liftable} \quad \Longleftrightarrow \quad \mathcal{D}\mathrm{ef}(G, \mathbf{Z}_p[\varphi]) \cong \mathrm{Hom}_W(W, -)\,.$$

Theorem 5.5.2. *The pair (G, φ) is canonically liftable if and only if the linear operators induced by φ*

$$\varphi^* \in \mathrm{End}_k(TG^t) \quad \text{and} \quad \varphi_* \in \mathrm{End}_k(TG)$$

do not have a common eigenvalue over $\bar{k}$.

Proof. Let V denote the k-vector space $TG \otimes TG^t$. The condition that φ_* and φ^* have distinct eigenvalues over $\bar{k}$ is equivalent to requiring the operator

$$\varphi^* \otimes 1 - 1 \otimes \varphi_* \in \mathrm{End}_k(V)$$

to be a bijection. To see this, first note that being a bijection is stable under a base field change, so we can assume that k is algebraically closed. Choose bases $\{e_i\}$ for T_G and $\{f_i\}$ for T_{G^t} such that φ_* and φ^* get into an upper-triangular form,

$$\varphi_* = \begin{pmatrix} \lambda_1 & * & \dots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & \lambda_n \end{pmatrix}, \qquad \varphi^* = \begin{pmatrix} \mu_1 & * & \dots & * \\ 0 & \mu_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & \mu_n \end{pmatrix}.$$

Then $\varphi^* \otimes 1 - 1 \otimes \varphi_*$ is upper-triangular in the basis $\{e_i \otimes f_j\}$ with $\lambda_i - \mu_j$ on the diagonal. It is invertible if and only the diagonal entries are non-zero or, equivalently, if λ_i and μ_j are pairwise distinct.

Now it suffices to prove that φ is canonically liftable if and only if $\varphi^* \otimes 1 - 1 \otimes \varphi_*$ is a bijection on V. Let $\mathcal{O}$ denote the ring $\mathbf{Z}_p[\varphi]$ and $R = \mathcal{O} \otimes_{\mathbf{Z}_p} W$.

The tangent space to the functor $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is isomorphic to $\mathrm{H}^0(R\text{-}R\,, TG \otimes TG^t)$ by 4.3.4. Clearly a necessary condition for φ to be canonically liftable is that this tangent space is zero, for otherwise the pair (G, φ) is not uniquely liftable to $k[\epsilon]$.

So $\mathrm{H}^0(R\text{-}R\,, TG \otimes TG^t) = 0$. Since R is generated by φ over W, we have

$$\mathrm{H}^0(R\text{-}R\,, V) = \{ v \in V \mid (\varphi^* \otimes 1 - 1 \otimes \varphi_*)v = 0 \}\,.$$

This group is trivial if and only if $\varphi^* \otimes 1 - 1 \otimes \varphi_*$ is injective (equivalently, bijective). This proves the "only if" part of the theorem.

For the "if" part, it suffices to show that both the tangent space and the obstruction space to $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ are 0, provided $\varphi^* \otimes 1 - 1 \otimes \varphi_*$ is bijective. As we have seen, its injectivity gives the vanishing of the tangent space. As for the obstruction space, we unravel the definition of $\mathrm{H}^1(R\text{-}R\,, TG \otimes TG^t)$,

$$\mathrm{H}^1(R\text{-}R\,, TG \otimes TG^t) = V / \mathrm{Im}(\varphi^* \otimes 1 - 1 \otimes \varphi_*)\,.$$

This group is 0 since $\varphi^* \otimes 1 - 1 \otimes \varphi_*$ is surjective. Hence $\mathcal{D}\mathrm{ef}(G, \mathcal{O})$ is formally smooth of dimension 0, as required. ∎

Example 5.5.3. Let $k = \mathbf{F}_q$ be finite, X/k an *ordinary* abelian variety and $\varphi = F_q$ be the geometric Frobenius ($F_q : x \mapsto x^q$). Let $G = X[p^\infty]$ be the associated p-divisible group. Then $F_{q,*} = 0$ on TG and F_q^* is a bijection on TG^t. Hence F_q is canonically liftable. In fact the unique liftings $(\mathcal{G}, \Phi)$ of (G, φ) obtained in this case are exactly the Serre-Tate canonical liftings. This perhaps explains the terminology "canonical liftings" which we use.

Example 5.5.4. If $k = \mathbf{F}_q$ is finite, $\varphi = F_q$ and X/k is *non-ordinary*, then $(X[p^\infty], F_q)$ is not canonically liftable, since $F_{q,*}$ is zero while F_q^* is not bijective and thus has also at least one zero eigenvalue. So the geometric Frobenius is canonically liftable *if and only if* X is ordinary.

Remark 5.5.5. If φ is canonically liftable, then $\mathcal{D}\mathrm{ef}(G, \mathbf{Z}_p[\varphi])$ is formally smooth (of dimension 0 over W). Let λ be a principal quasi-polarization on G whose Rosati involution stabilizes $\mathbf{Z}_p[\varphi]$. By Theorem 4.5.4, $\mathcal{D}\mathrm{ef}(G, \mathbf{Z}_p[\varphi], \lambda)$ is formally smooth as well. Hence $\mathcal{D}\mathrm{ef}(G, \mathbf{Z}_p[\varphi], \lambda)$, being also a subfuctor of $\mathcal{D}\mathrm{ef}(G, \mathbf{Z}_p[\varphi])$, equals $\mathcal{D}\mathrm{ef}(G, \mathbf{Z}_p[\varphi])$. In other words, λ lifts to all the canonical liftings.

Remark. Even if φ has small degree over $\mathbf{Z}_p$ compared to the height of G, it might happen that φ is canonically liftable. For example let $p > 2$ and $\mathbf{Z}[\varphi] = \mathbf{Z}[\sqrt{-d}]$ with $(d, p) = 1$. Let E be an ellptic curve over k with $\mathbf{Z}[\varphi] \subset \mathrm{End}(E)$. Then we can let $\mathbf{Z}_p[\varphi]$ act diagonally on the product (any number of times) $G = E[p^\infty] \times \cdots \times E[p^\infty]$. Then φ on G is canonically liftable.

References

[1] M. Artin, "Versal deformations and algebraic stacks", Inv. Math. **27** (1974), 165–189.

[2] P. Berthelot, L. Breen, W. Messing, "Théorie de Dieudonné cristalline II", Lecture Notes in Math. **930**, Springer-Verlag, Heidelberg, 1982.

[3] N. Bourbaki, "Commutative Algebra", Hermann, Paris.

[4] C. L. Chai, P. Norman, "Singularities of the $\Gamma_0(p)$-level structure", J. Alg. Geometry **1** (1992), 251–277.

[5] S. E. Crick, "Local moduli of abelian varieties", Am. Journ. Math. **97** (1975), 851–861.

[6] P. Deligne, G.Pappas, "Singularites des espaces de modules de Hilbert, en les caractéristiques divisants le discriminant", Compositio Math. **90** (1994), 59–79.

[7] M. Demazure, "Lectures on p-divisible groups", Lecture Notes in Math. **302**, Springer-Verlag, 1972.

[8] V. G. Drinfeld, "Elliptic modules", Mat. Sbornik **94** (136) (1974), No. 4., 561–592.

[9] B. Fantechi, M. Manetti, "Obstruction calculus for functors of Artin rings, I", J. of Algebra **202** (1998), No. 2, 541–576.

[10] J.-M. Fontaine, "Groupes p-divisibles sur les corps locaux", Astérisque 47–48 (1977).

[11] B. H. Gross, "On canonical and quasi-canonical liftings", Invent. Math. **84** (1986), 321–326.

[12] L. Illusie, "Complexe cotangent et déformations, I, II", Lecture Notes in Math. **239**, **283**, Springer-Verlag, 1971, 1972.

[13] L. Illusie, "Déformations de groupes de Barsotti-Tate", Exp. VI in: Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell (Ed. L. Szpiro), Astérisque **127** (1985), Soc. Math. France.

[14] N. Jacobson, "Basic algebra II", second ed., Freeman, 1985.

[15] G. Janusz, "Tensor products of orders", J. London Math. Soc. (Series 2) **20** (1979), 186–192.

[16] A. J. de Jong, "The moduli spaces of polarized abelian varieties", Math. Ann. **295** (1993), 485–503.

[17] A. J de Jong, "The moduli spaces of principally polarized abelian varieties with $\Gamma_0(p)$-level structure", Journal of Alg. Geometry **2** (1993), 667–688.

[18] R. Kottwitz, "Points on some Shimura varieties over finite fields", Journal of the AMS **5** (1992), 373–444.

[19] J. Lubin, J. Tate, "Formal moduli for one-parameter formal Lie groups", Bull. Soc. Math. France **49** (1966), 49–60.

[20] S. Lichtenbaum, M. Schlessinger, "The cotangent complex of a morphism", Trans. Amer. Math. Soc. **128** (1967), 41–70.

[21] J. Lubin, J-P. Serre, J.Tate, "Elliptic curves and formal groups", Lecture Notes Summer Inst. Algebraic Geeometry, Woods Hole (1964).

[22] B. Mazur, "Deforming Galois representations", Galois groups over **Q** (Eds. Y. Ihara, K. Ribet, J.-P. Serre), Math. Sciences Research Institute Publications, Springer-Verlag, New York, 1989, 385–437.

[23] W. Messing, "The crystals associated to Barsotti-Tate groups: with applications to abelian schemes", Lecture Notes in Math. **264**, Springer-Verlag, 1972.

[24] D. Mumford, "Abelian varieties", Tata Inst. Fund. Res., Oxford Univ. Press, 1970.

[25] D. Mumford, J. Fogarty, "Geometric invariant theory", Springer-Verlag, Heidelberg, 1982.

[26] M. Nagata, "Local rings", Interscience tracts in pure in applied mathematics no. 13, Interscience publishers, 1962.

[27] P. Norman, "Lifting abelian varieties", Invent. Math. **64** (1981), 431–443.

[28] P. Norman, F. Oort, "Moduli of abelian varieties", Ann. Math. **112** (1980), 413–439.

[29] T. Oda, "The first De Rham cohomology group and Dieudonné modules", Ann. Sc. Ecole Norm. Sup. **2** (1969), 63–135.

[30] F. Oort, "CM-liftings of abelian varieties", J. Alg. Geom. **1** (1992), 131–146.

[31] F. Oort, "Finite group schemes, local moduli for abelian varieties, and lifting problems", Algebraic geometry, Oslo 1970 (Ed. F. Oort), Wolters-Noordhof 1972, 223–254.

[32] G. Pappas, "Local structure of arithmetic moduli for PEL Shimura varieties", preprint.

[33] M. Rapoport, T. Zink, "Period spaces for p-divisible groups", Annals of Math. Studies **141**, Princeton University Press, 1996.

[34] I. Reiner, "Maximal orders", Academic Press, London, 1975.

[35] M. Schlessinger, "Functors of Artin rings", Trans. Amer. Math. Soc. **130** (1968), 208–222.

[36] M. Schlessinger, "On rigid singularities", Rice University Studies **59** (1973), 147–162.

[37] G. Shimura, "On analytic families of polarized abelian varieties and automorphic functions", Ann. Math. **78** (1963), 149–192.

[38] J. Tate, "p-divisible groups", Proc. Conf. on Local Fields, Driebergen, 1966 (T. Springer, ed.), Springer-Verlag, 1967, 158–183.

[39] J.-K. Yu, "On the moduli of quasi-canonical liftings", preprint.

[40] T. Zink, "Cartiertheorie kommutativer formaler Gruppen", Teubner-Texte zur Mathematik, Band 68.

6 p-descent on elliptic curves

6.1 Introduction

Classically, a 2-descent is the most widely used method to bound the rank of the Mordell-Weil group of an elliptic curve E over a number field. Originally, these methods required the existence of rational torsion points or a rational isogeny on E. In [2], Brumer and Kramer presented a method which works independently of the structure of the 2-torsion. As one of the applications, they have produced examples of cubic extensions of $\mathbf{Q}$ whose class group has large 2-torsion.

In some cases, the existence of the 2-part of the Tate-Shafarevich group makes it difficult to determine the rank exactly. It is then helpful to be able to use a prime $p>2$ in the descent computations. The goal of this chapter is to show that the basic ingredient for this, namely the injectivity of the Kummer map, holds in a large class of situations.

Let E/K be an elliptic curve and fix a prime $p \neq \mathrm{char}\,(K)$. Take a field L with $K \subset L \subset \bar{K}$ over which there is a non-trivial p-torsion point $T \in E(L)[p]$. There is a *Kummer map* associated to T (cf. 6.2.1 below),

$$\alpha = \alpha_{T,L} : \ E(K)/pE(K) \longrightarrow L^*/L^{*p} .$$

If all of the p-torsion of E is already rational over $K=L$, the associated Kummer pairing

$$\alpha_{*,K} : \ E[p] \times E(K)/pE(K) \longrightarrow K^*/K^{*p}$$

is non-degenerate on the left. If K is a number field, the standard local methods give a bound for the size of the image of the Kummer pairing in L^*/L^{*p}. This gives the corresponding bound on $E(K)/pE(K)$ and, hence, on the Mordell-Weil rank of E.

In practice, however, the points of $E[p]=E(\bar{K})[p]$ are rarely defined over K. In fact, for a fixed non-CM elliptic curve, the Galois group $G_{\bar{K}/K}$ acts *irreducibly* on $E(\bar{K})[p]$ for all but finitely many primes p. Our main result is that precisely in this situation, the Kummer map is injective (Theorems 6.3.1, 6.4.2):

Theorem. *Let E/K be an elliptic curve, $p \neq \mathrm{char}\, K$ a prime and $T \in E[p]$ a non-zero torsion point. Assume that $E[p]$ is an irreducible $G_{\bar{K}/K}$-module. Then for any intermediate field $K(T) \subset L \subset K(E[p])$,*

$$\alpha_{T,L} : \ E(K)/pE(K) \longrightarrow L^*/L^{*p}$$

is injective.

This result extends [13], Exercise 10.9 where the Kummer map is defined and its properties are outlined. Note that the assumption $[L:K]=m^2-1$ of the exercise suggests that m is prime.

The outline of this chapter is as follows. We start by recalling both the cohomological definition of the Kummer map and the more practical geometric definition (Section 6.2).

It is also possible to give a yet equivalent description, in terms of $H^0(C, \mathcal{O}_C^*/\mathcal{O}_C^{*p})$ which makes sense for a non-singular projective curve C of arbitrary genus.

Then we turn to injectivity of the Kummer map starting with the case $L = K(E[p])$ (Section 6.3) and then deducing the general case as a corollary (Section 6.4).

In Section 6.5 we show that in many cases the image of the Kummer map is contained in the kernel of the norm map $N_{L/K}$. This can be used to bound the potential size of this image.

We also discuss the local properties of the image of $\alpha_{T,L}$ in case K is a number field (Section 6.6). The primary question we are interested in here is when for a given prime l of L, the image of α is "trivial at l". Using this one shows that in some cases there is a large part of $E(K)/pE(K)$ which maps into the subgroup of L^*/L^{*p} which corresponds to the p-part of the class group of L.

An example which illustrates our results is presented in Section 6.7.

Notation. The ground field K is assumed to be perfect. We let p denote a prime of $\mathbf{Q}$ different from $\operatorname{char} K$. We denote by $E[p]$ the p-torsion of an elliptic curve E/K over the algebraic closure $\bar{K}$. For a point $T \in E(\bar{K})$ we denote by $K(T)$ the field extension of K inside $\bar{K}$ which is obtained by adjoining the coordinates of T. Similarly, $K(E[p])$ stands for the compositum of $K(T)$ for $T \in E[p]$. This is a finite Galois extension of K. The Galois group of a field extension L/K is denoted by $G_{L/K}$.

Remark. Results similar to those presented here have been obtained independently by Djabri, Schaefer and Smart [3]. The slight difference is that they study the algebra A obtained by adjoining the coordinates of a "generic p-torsion point" rather than the field $L = K(T)$. Thus they are able to prove the injectivity on the Kummer map without using the irreducibility assumption. An advantage of our method, however, is that it is possible to "vary L", which is useful in applying the results of Section 6.5, see Remark 6.5.4.

6.2 The Kummer map

Let E be an elliptic curve over a field K. Fix a prime $p \neq \operatorname{char}(K)$. We recall the well-known cohomological description of $E(K)/pE(K)$. We refer to [13], Ch. X for details. Consider the exact sequence of $G_{\bar{K}/K}$-modules

$$0 \longrightarrow E[p] \longrightarrow E(\bar{K}) \xrightarrow{[p]} E(\bar{K}) \longrightarrow 0\,.$$

Taking $G_{\bar{K}/K}$-cohomology yields a long exact sequence, from which we extract

$$0 \longrightarrow E(K)/pE(K) \hookrightarrow H^1(G_{\bar{K}/K}, E[p]) \longrightarrow H^1(G_{\bar{K}/K}, E(\bar{K}))[p] \longrightarrow 0\,. \qquad (46)$$

What interests us here is the first injection. Tracing through the definition of the connecting homomorphism, one can produce the explicit description of this map:

Let $P \in E(K)$. Choose any $Q \in E(\bar{K})$ with $pQ = P$. Then

$$E(K)/pE(K) \ni P \quad \longmapsto \quad (\sigma \mapsto Q^\sigma - Q) \in H^1(G_{\bar{K}/K}, E[p]) \, .$$

Note that a different choice of Q affects the cocycle $\sigma \mapsto Q^\sigma - Q$ by a 1-coboundary, so the map is well-defined.

We do a similar computation for the multiplicative group in place of the group of points of E. Take the $G_{\bar{K}/L}$-cohomology of

$$1 \longrightarrow \mu_p \longrightarrow \bar{K}^* \xrightarrow{[p]} \bar{K}^* \longrightarrow 1$$

(here $[p]$ is the p-th power map) and in the same way as above extract

$$1 \longrightarrow L^*/L^{*p} \longrightarrow H^1(G_{\bar{K}/L}, \mu_p) \longrightarrow H^1(G_{\bar{K}/L}, \bar{K}^*) \longrightarrow 1 \, .$$

By the Hilbert '90 theorem, the group $H^1(G_{\bar{K}/L}, \bar{K}^*)$ is trivial. So $H^1(G_{\bar{K}/L}, \mu_p) \cong L^*/L^{*p}$.

Now take a point $T \in E[p]$ of order p. Choose an intermediate field $K \subset L \subset \bar{K}$ over which T is defined. Then the Weil pairing on $E[p]$ gives a homomorphism of $G_{\bar{K}/L}$-modules $E[p] \to \mu_p$,

$$E[p] \ni S \quad \longmapsto \quad e_p(S, T) \in \mu_p \, .$$

It induces the map on cohomology,

$$H^1(G_{\bar{K}/K}, E[p]) \longrightarrow H^1(G_{\bar{K}/L}, \mu_p) \, ,$$

given explicitly by $\xi \mapsto (\sigma \mapsto e_p(\xi(\sigma), T))$.

The above maps can be combined to (cf. [13], Exc. 10.9)

$$E(K)/pE(K) \longrightarrow H^1(G_{\bar{K}/K}, E[p]) \xrightarrow{\text{Res}} H^1(G_{\bar{K}/L}, E[p]) \longrightarrow H^1(G_{\bar{K}/L}, \mu_p) \cong L^*/L^{*p} \, .$$

Here Res denotes the restriction homomorphism.

Definition 6.2.1. The *Kummer map* $\alpha_{T,L}$ is the composition of the above maps,

$$\alpha_{T,L} : \; E(K)/pE(K) \longrightarrow L^*/L^{*p} \, .$$

It is defined for any point $T \in E[p]$ of order p and a field L which contains $K(T)$.

There is a different description of the Kummer map, which is more geometric in nature and more suitable for actual computations. In case $p = 2$, it was already used by Mordell in the proof of his finiteness theorem ([5]; [6], Ch. 16). Start again with E/K and a non-trivial torsion point $T \in E(K)[p]$. The divisor

$$D = p(T) - p(O)$$

is principal, so there is a rational function $f \in K(E)$ which represents it. The evaluation map

$$e : E(K) \ni \ P \longmapsto f(P) \ \in K^*$$

is defined outside T and O and can be extended by linearity to

$$\mathrm{Div}' E(K) \longrightarrow K^* \ .$$

Here Div' stands for divisors whose support does not contain T or O. Moreover, by Weil reciprocity

$$f(\mathrm{div}\, g) = g(\mathrm{div}\, f) = g(p(T) - p(O)) = g((T)-(O))^p \in K^{*p}$$

for any g for which $\mathrm{div}\, g \in \mathrm{Div}'$. This allows to get rid of "$'$" in Div' and get a well-defined map which we still denote by e,

$$e : \mathrm{Pic}\, E(K) \longrightarrow K^*/K^{*p} \ .$$

It also follows that e is a group homomorphism. Finally, using the explicit definition of the Weil pairing, one can show that the map induced by e,

$$E(K)/pE(K) \longrightarrow K^*/K^{*p} \ ,$$

coincides with the Kummer map $\alpha_{T,K}$. For instance, this follows from [11], Theorem 2.3. It is also stated in [13], Exc. 10.9(a).

Also note that the above construction can be generalized to curves of arbitrary genus (see [8], Section 5 and [11], Lemma 2.1).

As an example, consider the $p=2$ case. Let E be an elliptic curve over a field K with $\mathrm{char}\, K \neq 2$. Assume that E has a rational 2-torsion point over K and put E in the form

$$Y^2 = (X - t_1)(X - t_2)(X - t_3), \qquad t_1 \in K, \ t_2, t_3 \in \bar{K} \ .$$

Let $T = (t_1, 0)$. The function $X - t_1$ has the correct properties, so the Kummer map associated to T is given by

$$\begin{array}{rccc} e : & E(K) & \longrightarrow & K^*/K^{*2} \\ & (x,y) & \longmapsto & x - t_1 \end{array} \tag{47}$$

for $(x,y) \neq T$ and $\neq O$. It is easy to check that $e(O) = 1$ and $e(T) = (t_1 - t_2)(t_1 - t_3)$. This description is used in the actual computation for 2-descent.

The exceptional values $e(T)$ and $e(O)$ can be made less exceptional: in fact e is given on the whole of E *locally* by invertible regular functions. The functions

$$\begin{array}{lll} f_1 = & X - t_1 & \text{on } \ U_1 = E \setminus \{(t_1,0), O\} \\ f_2 = & \dfrac{1}{(X-t_2)(X-t_3)} & \text{on } \ U_2 = E \setminus \{(t_2,0), (t_3,0)\} \end{array}$$

have the property that

$$f_1(P) = f_2(P) \ \in K^*/K^{*2}$$

for every $P \in E(K)$ which lies in $U_1 \cap U_2$, since

$$f_1/f_2 = Y^2 \ .$$

In general, for a non-singular projective curve C/K and a prime p one might ask which maps

$$C(K) \longrightarrow K^*/K^{*p}$$

are locally given by invertible regular functions, defined over K and which differ by p-th powers on the intersections. We can make this precise (after all $C(K)$ might be empty) as follows.

Definition. Let C be a non-singular projective curve over a field K. A *p-map* is a global section of the sheaf $\mathcal{O}_C^*/\mathcal{O}_C^{*p}$. Here $\mathcal{O}_C$ denotes the structure sheaf.

Note that a p-map can be given by an open covering $\{U_i\}$ of C and invertible regular functions f_i on U_i with the property that $f_i/f_j \in H^0(U_i \cap U_j, \mathcal{O}_C^{*p})$.

It turns out that for an elliptic curve $C = E$ the p-maps are exactly the Kummer maps given by some K-rational p-torsion point $T \in E(K)[p]$. More generally, for a curve C of arbitrary genus the p-maps are classified by K-rational p-torsion points in the Picard group of C:

Proposition 6.2.2. *Let C be a non-singular projective curve over a perfect field K. Then*

$$H^0(C, \mathcal{O}_C^*/\mathcal{O}_C^{*p}) \ \cong \ \mathrm{Pic}\, C(K)[p] \ . \tag{48}$$

Proof. First assume K is algebraically closed. A short exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_X^*/\mu_p \longrightarrow \mathcal{O}_X^* \longrightarrow \mathcal{O}_X^*/\mathcal{O}_X^{*p} \longrightarrow 0$$

where the left map is taking a function to its p-th power gives a long cohomology sequence

$$0 \longrightarrow K^*/\mu_p \xrightarrow{\cong} K^* \longrightarrow H^0(C, \mathcal{O}_C^*/\mathcal{O}_C^{*p}) \longrightarrow H^1(C, \mathcal{O}_C^*/\mu_p) \longrightarrow H^1(C, \mathcal{O}_C^*) \ .$$

The sheaf μ_p on C is constant, hence flasque (Zariski topology), hence acyclic. Thus

$$0 \longrightarrow H^0(\mathcal{O}_C^*/\mathcal{O}_C^{*2}) \longrightarrow \mathrm{Pic}C \xrightarrow{[p]} \mathrm{Pic}C$$

which gives (48). The case of arbitrary K is obtained by taking $G_{\bar{K}/K}$-invariants. ∎

Example 6.2.3. As an illustration, consider the case $p = 3$. Assume that E/K is given by an equation

$$E: \ y^2 = x^3 + ax + b\,.$$

Let $T = (x_T, y_T) \in E[p]$ be a non-trivial 3-torsion point and let $L = K(T)$. Thus x_T is a root of the 3-division equation,

$$x_T^4 + 2ax_T^2 + 4bx_T - \frac{a^2}{3} = 0$$

and the extension $L/K(x_T)$ is given by

$$y_T^2 - (x_T^3 + ax_T + b) = 0\,.$$

It is easy to find a function on E which has the divisor $3(T) - 3(O)$. Namely T is an inflection point of E so a linear function which defines the tangent line to T has the required properties. The Kummer map $\alpha_{T,L}$ is thus given (outside T and O) by

$$\alpha_{T,L}: \ E(K)/pE(K) \ni (X,Y) \ \longmapsto \ (Y - y_T) - \frac{3x_T^2 + a}{2y_T}(X - x_T) \ \in L^*/L^{*3}\,.$$

This is in agreement with the formula given in [14], p.309.

6.3 The case of an irreducible action on p-torsion points

Theorem 6.3.1. *Let E/K be an elliptic curve, $p \neq \mathrm{char}(K)$ a prime, $L = K(E[p])$ and $T \in E(\bar{K})$ a point of exact order p. Assume that $G_{\bar{K}/K}$ acts irreducibly on $E[p]$. Then the Kummer map*

$$\alpha_{T,L}: \ E(K)/pE(K) \longrightarrow L^*/L^{*p}$$

is injective.

Proof. First note that $E[p]$ is an irreducible $G_{\bar{K}/K}$-module means that $E[p]$ has no non-trivial $G_{\bar{K}/K}-$invariant subspace. Equivalently, $E[p]$ has no non-trivial $G_{L/K}-$invariant subspace. It is also equivalent to saying that E does not admit a $p-$isogeny defined over K.

The sequence (46) and the corresponding one for $G_{\bar{K}/L}$-cohomology fit into the commutative diagram

$$\begin{array}{ccccc} & & \Phi & & \\ & & \downarrow & & \\ E(K)/pE(K) & \hookrightarrow & H^1(G_{\bar{K}/K}, E[p]) & \twoheadrightarrow & H^1(G_{\bar{K}/K}, E(\bar{K}))[p] \\ \downarrow & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ E(L)/pE(L) & \hookrightarrow & H^1(G_{\bar{K}/L}, E[p]) & \twoheadrightarrow & H^1(G_{\bar{K}/L}, E(\bar{K}))[p] \end{array}\,.$$

In particular, $\alpha_{T,L}$ also equals the composition

$$E(K)/pE(K) \longrightarrow E(L)/pE(L) \longrightarrow H^1(G_{\bar{K}/L}, E[p]) \longrightarrow H^1(G_{\bar{K}/L}, \mu_p) \cong L^*/L^{*p} .$$

Thus an obvious necessary condition for $\alpha_{T,L}$ to be injective is $\Phi = 0$ or, in other words

$$E(K) \cap pE(L) = pE(K) .$$

The fact that this is necessary is of course clear anyway: if $P \in E(K) \cap pE(L)$ then one can choose $Q \in E(L)$ with $pQ = P$, so

$$e_p(Q^\sigma - Q, T) = 1 \quad \text{for all} \quad \sigma \in G_{\bar{K}/L}$$

as $Q^\sigma = Q$ for all σ. Hence P is in the kernel of α. If $P \notin pE(K)$, then α is not injective.

Apply the snake lemma to the diagram above:

$$\begin{array}{ccccc}
\Phi & & H^1(G_{L/K}, E[p]) & & H^1(G_{L/K}, E(L))[p] \\
\downarrow & & \downarrow \text{Inf} & & \downarrow \text{Inf} \\
E(K)/pE(K) & \hookrightarrow & H^1(G_{\bar{K}/K}, E[p]) & \twoheadrightarrow & H^1(G_{\bar{K}/K}, E(\bar{K}))[p] \\
\downarrow & & \downarrow \text{Res} & & \downarrow \text{Res} \\
E(L)/pE(L) & \hookrightarrow & H^1(G_{\bar{K}/L}, E[p]) & \twoheadrightarrow & H^1(G_{\bar{K}/L}, E(\bar{K}))[p] \\
\downarrow & & \downarrow & & \downarrow \\
E(L)/pE(L)+E(K) & & C_1 & & C_2
\end{array} .$$

The kernels form an exact sequence

$$0 \longrightarrow \Phi \hookrightarrow H^1(G_{L/K}, E[p]) \longrightarrow H^1(G_{L/K}, E(L))[p] .$$

So the natural constraint which would imply $\Phi = 0$ is $H^1(G_{L/K}, E[p]) = 0$. This is indeed the case since $G_{L/K}$ acts faithfully and irreducibly on $E[p] \cong \mathbf{F}_p \oplus \mathbf{F}_p$:

Lemma 6.3.2. *Let p be a prime and let $G \subset GL_2(\mathbf{F}_p)$ act irreducibly on a two-dimensional vector space V over $\mathbf{F}_p$ (via the natural action of GL_2). Then $H^1(G, V) = 0$.*

Proof. (cf. [3], Proposition 1). First note that if G does not contain an element of order p then $H^1(G, V)$ is automatically zero as it is annihilated both by $|G|$ and p. Thus assume this is not the case.

First assume $p = 2$. Then $GL_2(V) \cong S_3$ and the action is the usual action of S_3 on the set of 3 elements $V - \{0\}$. Since G acts irreducibly on V (so it has no fixed points on $V - \{0\}$) and it contains an element of order 2, the only possibility is $G = S_3$. The inflation-restriction sequence for the normal subgroup $A_3 \subset S_3$ reads:

$$H^1(S_3/A_3, V^{A_3}) \xrightarrow{\text{Inf}} H^1(S_3, V) \xrightarrow{\text{Res}} H^1(A_3, V) .$$

Since A_3 has no non-zero invariants on V (so that the group on the left is trivial) and $H^1(A_3, V)$ is trivial as well (being annihilated both by 2 and by 3), we see that $H^1(S_3, V) = 0$ as required.

Now let p be an odd prime. Since G acts irreducibly on V and G has an element of order p, a result of Serre ([12], 2.4, Proposition 15) asserts that G contains $SL_2(\mathbf{F}_p)$, thus $\{\pm 1\} \subset G$. We apply the inflation-restriction sequence for this (normal) subgroup:

$$H^1(G/\pm 1, V^{\pm 1}) \xrightarrow{\text{Inf}} H^1(G,V) \xrightarrow{\text{Res}} H^1(\pm 1, V)\,.$$

Again $\{\pm 1\}$ has no invariants on V and also $H^1(\pm 1, V)=0$ being annihilated both by p and by 2. So $H^1(G,V)=0$. ∎

We continue with the proof of the theorem. The map $\alpha_{T,L}$ becomes the composition

$$E(K)/pE(K) \hookrightarrow E(L)/pE(L) \longrightarrow H^1(G_{\bar{K}/L}, \mu_p)\,.$$

So it remains to show that the second map here is injective. This means that

$$e_p(Q^\sigma - Q, T) = 1 \quad \text{for all} \quad \sigma \in G_{\bar{K}/L}$$

implies $Q \in E(L)$. In other words, it can not happen that for some $Q \notin E(L)$,

$$Q^\sigma - Q \;\in\; <T> \;\subset E[p] \quad \text{for all} \quad \sigma \in G_{\bar{K}/L}\,.$$

If this would be the case, the set $V = \{Q^\sigma - Q \mid \sigma \in G_{\bar{K}/L}\}$ would form a proper non-trivial subspace of $E[p]$. However, the following lemma applied with

$$G = G_{\bar{K}/K}, \quad H = G_{\bar{K}/L}, \quad A = E[p] \quad \text{and} \quad \xi(\sigma) = Q^\sigma - Q$$

shows that V is $G_{L/K}$-invariant. This contradicts the irreducibility assumption. ∎

Lemma 6.3.3. *Let a group G act on an abelian group A, and let $H \lhd G$ act trivially on A. Then for any $\xi \in H^1(G,A)$, the subgroup of A*

$$V = V_\xi = \{\xi(h) \mid h \in H\}$$

is invariant under G (or G/H).

Proof. First note that $\text{Res}(\xi) \in H^1(H,A) = \text{Hom}(H,A)$, so ξ defines a homomorphism $H \to A$, whose image is V (in particular V is a subgroup of A). If we let G act on H by

$$g \cdot h = ghg^{-1}$$

then H becomes a G-module and the important thing is that the map $\xi : H \to A$ becomes a G-homomorphism (it commutes with this action of G). Clearly ξ factors as

$$\xi : \quad H \twoheadrightarrow V \hookrightarrow A\,.$$

Thus to show that V is invariant under G, take $v \in V \subset A$, take $h \in H$ such that $\xi(h) = v$. Then

$$g \cdot v = \xi(g \cdot h) \in V$$

as required. ∎

Remark. By a theorem of Serre ([12], 4.2, Théorème 2), for a curve E without complex multiplication, there are only finitely many primes p for which $G_{\bar{K}/K}$ does not act irreducibly on $E[p]$. Indeed, the theorem asserts that $G_{\bar{K}/K} \to \mathrm{Aut}(E[p])$ $(\cong GL_2(\mathbf{F}_p))$ is surjective for almost all primes. Thus the condition of Theorem 6.3.1 is satisfied for all but finitely many primes provided E has no CM.

6.4 A generalization for subfields of $K(E[p])$

Proposition 6.4.1. *Let E/K be an elliptic curve, p a prime different from $\mathrm{char}\, K$ and $T \in E[p]$ a non-trivial point of order p. Let $K(T) \subset L_1 \subset L_2 \subset \bar{K}$ be fields. Then the associated Kummer map α_{T,L_2} factors*

$$\alpha_{T,L_2} : \; E(K)/pE(K) \xrightarrow{\alpha_{T,L_1}} L_1^*/L_1^{*p} \longrightarrow L_2^*/L_2^{*p} \; .$$

Here the second map is induced by the inclusion $L_1 \hookrightarrow L_2$.

Proof. The defining map for α_{T,L_2}

$$E(K)/pE(K) \longrightarrow H^1(G_{\bar{K}/K}, E[p]) \xrightarrow{\mathrm{Res}} H^1(G_{\bar{K}/L_2}, E[p]) \longrightarrow H^1(G_{\bar{K}/L_2}, \mu_p) \cong L_2^*/L_2^{*p}$$

factors as (look at the explicit definition of $\alpha_{T,L}$)

$$\begin{aligned} E(K)/pE(K) \longrightarrow H^1(G_{\bar{K}/K}, E[p]) &\xrightarrow{\mathrm{Res}} H^1(G_{\bar{K}/L_1}, E[p]) \longrightarrow \\ &\longrightarrow H^1(G_{\bar{K}/L_1}, \mu_p) \xrightarrow{\mathrm{Res}} H^1(G_{\bar{K}/L_2}, \mu_p) \cong L_2^*/L_2^{*p} \; . \end{aligned}$$

It remains to remark that $H^1(G_{\bar{K}/L_1}, \mu_p) \cong L_1^*/L_1^{*p}$ and that the restriction map from $H^1(G_{\bar{K}/L_1}, \mu_p)$ to $H^1(G_{\bar{K}/L_2}, \mu_p)$ is indeed equivalent to the natural map $L_1^*/L_1^{*p} \to L_2^*/L_2^{*p}$ induced by the inclusion $L_1 \hookrightarrow L_2$. ∎

A direct corollary of this proposition is the following generalization of Theorem 6.3.1 to the subfields M of $L = K(E[p])$ over which α can still be defined.

Theorem 6.4.2. *Let E/K be an elliptic curve, p a prime different from $\mathrm{char}\, K$ and $T \in E[p]$ a non-trivial point of order p. Let $L = K(E[p])$ and let M be a subfield of L which contains $K(T)$. Assume that $G_{\bar{K}/K}$ acts irreducibly on $E[p]$. Then the Kummer map*

$$\alpha_{T,M} : \; E(K)/pE(K) \longrightarrow M^*/M^{*p}$$

is injective.

Proof. By the proposition above, $\alpha_{T,L}$ factors as

$$\alpha_{T,L} : \quad E(K)/pE(K) \longrightarrow M^*/M^{*p} \longrightarrow L^*/L^{*p} \; .$$

Since the composition is injective, the first map (which is $\alpha_{T,M}$) is injective as well. ∎

6.5 The norm map on the image of the Kummer map

Let E/K be an elliptic curve, $T \in E[p]$ a point of (exact) order p and L a subfield of $K(E[p])$ over which T is defined. We have defined the Kummer map

$$\alpha_{T,L} : \quad E(K)/pE(K) \hookrightarrow L^*/L^{*p}$$

and proved that it is injective under the irreducibility assumption. In this section we show that in many cases the image of $\alpha_{T,L}$ is contained in the kernel of the norm map

$$N_{L/K} : L^*/L^{*p} \longrightarrow K^*/K^{*p} .$$

In the next section we study the local behaviour of the image in case of a number field.

We start by describing the action of Galois on the target of the Kummer map.

Lemma 6.5.1. *Let $E/K, p$ and L be as above. For $\tau \in G_{\bar{K}/K}$ the composition*

$$E(K)/pE(K) \quad \stackrel{\alpha_{T,L}}{\longrightarrow} \quad L^*/L^{*p} \quad \stackrel{\tau}{\longrightarrow} \quad \tau(L)^*/\tau(L)^{*p} \tag{49}$$

is equal to the Kummer map $\alpha_{T^\tau,\tau(L)}$.

Proof. Recall the geometric description of the Kummer map. The map $\alpha_{T,L}$ is given (locally on E) by invertible regular functions f_i which are defined over L,

$$f_i : E(K) \supset U_i \ni P \longmapsto f(P) \in L^* .$$

The composition (49) is then given by the functions f_i^τ. Clearly these also form an element of $H^0(E, \mathcal{O}_E^*/\mathcal{O}_E^{*p})$. Moreover, the principal divisors (f_i^τ) are the conjugates $(f_i)^\tau$. It follows that $\{f_i^\tau\}$ corresponds to the Kummer map defined by T^τ, as required. ∎

Corollary 6.5.2. *Let $E/K, p$ and L be as above. Assume that $E[p](K) = \{O\}$. Then the image of $\alpha_{T,L}$ is contained in the kernel of the norm map (cf. [13], Exc. 10.9(b))*

$$N_{L/K} : L^*/L^{*p} \longrightarrow K^*/K^{*p} .$$

Proof. Extend each of the possible embeddings $\bar{\tau}_i : L \to \bar{K}$ to an automorphism $\tau_i \in G_{\bar{K}/K}$. Let $\alpha_{T,L}$ be given by a cocycle $\{f_i\} \in H^0(E, \mathcal{O}_E^*/\mathcal{O}_E^{*p})$. Then $N_{L/K}(\alpha_{T,L})$ is given by a cocycle $\{\prod_\tau f_i^\tau\}$. However this cocycle is defined over K, and hence corresponds to a Kummer map given by some p-torsion point $N \in E[p](K)$. The assumption that E has no non-trivial p-torsion defined over K gives $N = O$, so this Kummer map is trivial. ∎

Example 6.5.3. We continue Example 6.2.3, that is, the $p = 3$ case. Assume for simplicity that the Galois group of $K(E[3])/K$ is isomorphic to the full group $GL_2(\mathbf{F}_3)$. (This is the case for general $E/\mathbf{Q}$.) The chain of subfields

$$K \quad \stackrel{4}{\subset} \quad K(x_T) \quad \stackrel{2}{\subset} \quad K(x_T, y_T) = L \quad \stackrel{6}{\subset} \quad K(E[3])$$

corresponds (via Galois theory) to the chain

$$\begin{pmatrix} * & * \\ * & * \end{pmatrix} \quad \stackrel{4}{\supset} \quad \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \quad \stackrel{2}{\supset} \quad \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \quad \stackrel{6}{\supset} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of subgroups of $GL_2(\mathbf{F}_3)$. The field $K(x_T)$ is the unique non-trivial intermediate field of the field extension L/K. More generally, every proper subgroup of $GL_2(\mathbf{F}_p)$ which contains $\left(\begin{smallmatrix}1 & * \\ 0 & *\end{smallmatrix}\right)$ is of the form $\left(\begin{smallmatrix}H & * \\ 0 & *\end{smallmatrix}\right)$ with H a subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$. This follows from Serre [12], 2.4, Proposition 15.

Clearly $E[p](K(x_T)) = 0$. So an application of 6.5.2 shows that the Kummer map $\alpha_{T,L}$ lands into the kernel of the norm map

$$N_{L/K(x_T)} : \ L^*/L^{*3} \ \longrightarrow \ K(x_T)^*/K(x_T)^{*p} \ .$$

In fact, this can be verified explicitly. The unique non-trivial automorphism of the (quadratic Galois) extension $L/K(x_T)$ sends $T = (x_T, y_T)$ to $-T = (x_T, -y_T)$. The product $\alpha_{T,L}\alpha_{-T,L}$ maps

$$(X,Y) \ \longmapsto \ \left[(Y-y_T)-\frac{3x_T^2+a}{2y_T}(X-x_T)\right]\left[(Y+y_T)-\frac{3x_T^2+a}{-2y_T}(X-x_T)\right] \ = \ (X-x_T)^3 \ .$$

The last equality is an easy symbolic computation. Clearly the map lands into $K(x_T)^{*3}$.

Remark 6.5.4. The result of 6.5.2 can be used to bound the size of the potential image of the Kummer map. More precisely, the image of $\alpha_{T,L}$ is contained in the intersection of the kernels of the norm maps $N_{L/K'}$ where K' varies through all the intermediate fields of the extension L/K over which E has no non-trivial p-torsion. This allows to decrease the amount of computation necessary to compute this image.

6.6 Local analysis of the image of $\alpha_{T,L}$

Let K be a number field, E/K an elliptic curve and $T \in E[p]$ a point of order p. Let L be any subfield of $K(E[p])$ containing $K(T)$. We have defined a map

$$\alpha_{T,L} : \quad E(K)/pE(K) \hookrightarrow L^*/L^{*p}$$

and proved that it is injective in certain cases. Now we study the image of this map. We start with recalling the result that for almost all primes l of L, this image is "trivial at l", i.e. it lands into

$$\{a \in L^*/L^{*p} \ \mid \ \mathrm{ord}_l(a) = 0 \ \mathrm{mod} \ p\} \ .$$

This is well-known, see for instance [8], Prop. 12.4.

Let L_l be the completion of L at l and K_v the completion of K at the unique prime v of K which l divides. Denote by L_l^{un} and K_v^{un} their unramified closures; thus L_l^{un} contains K_v^{un} and L and is their compositum. By $\mathbf{F}_v$ we will denote the residue field of K_v. We use $\mathcal{O}_v^{\mathrm{un}}$ and m_v^{un} to denote the ring of integers of K_v^{un} and its maximal ideal respectively. Finally, Δ_v denotes the minimal discriminant of E at v.

The Kummer maps for E/K_v and E/K_v^{un} fit into a commutative diagram

$$\begin{array}{ccc} E(K)/pE(K) & \longrightarrow & L^*/L^{*p} \\ \downarrow & & \downarrow \\ E(K_v)/pE(K_v) & \longrightarrow & L_l^*/L_l^{*p} \\ \downarrow & & \downarrow \\ E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}}) & \longrightarrow & L_l^{\mathrm{un}*}/L_l^{\mathrm{un}*p} \end{array} .$$

Assume that for our chosen prime v of K, either $E(K_v)/pE(K_v)$ is trivial or that $E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}})$ is trivial. Then, by the commutativity of the diagram, for any $P \in E(K)/pE(K)$, the image $\alpha_{T,L}(P)$ in L is in $L_l^{\mathrm{un}*p}$. This implies that (and for $l \not| p$ is equivalent to)

$$\mathrm{ord}_l(\alpha_{T,L}(P)) = 0 \mod p .$$

Even if the groups $E(K_v)/pE(K_v)$ and $E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}})$ are not trivial, a bound on the size of either of them gives a lower bound on the size of the subgroup of $E(K)/pE(K)$ which lands into $L_l^{\mathrm{un}*p}$. More precisely, we have the following result.

Theorem 6.6.1. *Let K be a number field, E/K an elliptic curve and p a prime. For a prime v of K denote*

$$\delta_v = \min\Big(\dim_{\mathbf{F}_p} E(K_v)/pE(K_v), \dim_{\mathbf{F}_p} E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}})\Big) .$$

Let $\delta = \sum_v \delta_v$. Then there is a subgroup $H \subset E(K)/pE(K)$ of $\mathbf{F}_p$-codimension at most δ which lands via the Kummer map

$$\alpha_{T,L} : \quad E(K)/pE(K) \longrightarrow L^*/L^{*p}$$

into the subgroup

$$\{a \in L^*/L^{*p} \mid \mathrm{ord}_l(a) = 0 \mod p \text{ for all } l\} .$$

Proof. Clear. ∎

Let us investigate the groups $E(K_v)/pE(K_v)$ and $E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}})$. It turns out that the former group is useful for the primes above p while the latter gives a better estimate for the primes not dividing p.

For the standard structure results for the group of points of an elliptic curve over a complete field we refer to [13], Chapters IV, VII. Let E be defined by a minimal Weierstrass equation at v. There is a reduction map (which we denote by "~")

$$E(K_v) \longrightarrow \tilde{E}(\mathbf{F}_v) .$$

Here $\tilde{E}/\mathbf{F}_v$ is the reduced curve. It might be singular or not depending on whether E has good or bad reduction at v. In any case let

$$\tilde{E}_{\mathrm{ns}}(\mathbf{F}_v) = \{R \in \tilde{E}(\mathbf{F}_v) \mid R \text{ is non-singular}\}$$

and

$$E_0(K_v) = \{P \in E(K_v) \mid \tilde{P} \in \tilde{E}_{\rm ns}(\mathbf{F}_v)\} .$$

Then the following sequences are exact ([13], VII.2.1, VII.2.2)

$$\begin{aligned} 0 \longrightarrow \hat{E}(m_v) \longrightarrow E_0(K_v) \longrightarrow \tilde{E}_{\rm ns}(\mathbf{F}_v) \longrightarrow 0 \\ 0 \longrightarrow \hat{E}(m_v^{\rm un}) \longrightarrow E_0(K_v^{\rm un}) \longrightarrow \tilde{E}_{\rm ns}(\bar{\mathbf{F}}_v) \longrightarrow 0 \ . \end{aligned} \tag{50}$$

Here $\hat{E}$ is the group associated to the formal group of E over K_v. To compare E with E_0, we will also make use of the exact sequences

$$\begin{aligned} 0 \longrightarrow E_0(K_v) \longrightarrow E(K_v) \longrightarrow E(K_v)/E_0(K_v) \longrightarrow 0 \\ 0 \longrightarrow E_0(K_v^{\rm un}) \longrightarrow E(K_v^{\rm un}) \longrightarrow E(K_v^{\rm un})/E_0(K_v^{\rm un}) \longrightarrow 0 \ . \end{aligned} \tag{51}$$

Finally, the size of the quotient E/E_0 is determined by the Kodaira-Néron theorem.

Theorem (Kodaira, Néron). Let E/K_v be an elliptic curve over a local field. If E has split multiplicative reduction, then $E(K_v)/E_0(K_v)$ is a cyclic group of order $\mathrm{ord}_v(\Delta_v)=-\mathrm{ord}_v(j)$. In all other cases, $E(K_v)/E_0(K_v)$ is a finite group of order at most 4.

Proof. [7], §III.17. ∎

The two propositions below give estimates on the sizes of $E(K_v)/E_0(K_v)$ for arbitrary v and of $E(K_v^{\rm un})/E_0(K_v^{\rm un})$ for $v \not| p$.

Proposition 6.6.2. *Let E/K_v be an elliptic curve over a local field. Then*

$$\dim_{\mathbf{F}_p} E(K_v)/pE(K_v) = \dim_{\mathbf{F}_p} E(K_v)[p] + \begin{cases} v(p)\dim_{\mathbf{F}_p} \mathbf{F}_v, & v|p \\ 0, & v \not| p \end{cases} .$$

Proof. Let A be an abelian group for which $[p]: A \to A$ has finite kernel and finite cokernel. Define

$$P(A) = \dim_{\mathbf{F}_p} A/pA - \dim_{\mathbf{F}_p} A[p] .$$

For an exact sequence of abelian groups

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 , \tag{52}$$

an application of the snake lemma to the multiplication by p map on (52) shows that

$$P(B) = P(A) + P(C) ,$$

provided $P(A)$ and $P(C)$ are defined. Note also that $P(C) = 0$ if C is finite. Hence $P(B) = P(A)$ whenever $B \subset A$ is of finite index and $P(B)$ (equivalently $P(A)$) is defined.

For the group of points $A = E(K_v)$ we have a filtration by subgroups of finite index

$$\cdots \subset \hat{E}(m_v^r) \subset \cdots \subset \hat{E}(m_v^2) \subset \hat{E}(m_v) \subset E_0(K_v) \subset E(K_v)\,.$$

Indeed, the subgroup $E_0(K_v) \subset E(K_v)$ is of finite index by the Kodaira-Néron theorem, $E_0(K_v)/\hat{E}(K_v) \cong \tilde{E}_{\rm ns}(\mathbf{F}_v)$ is finite since $\mathbf{F}_v$ is finite and (cf. [13], IV.3.2a)

$$\hat{E}(m_v^r)/\hat{E}(m_v^{r+1}) \cong m_v^r/m_v^{r+1} \cong \mathbf{F}_v, \quad r \geq 1\,.$$

By [13], IV.6.4 there is an integer $r \geq 1$ for which

$$\hat{E}(m_v^r) \cong \hat{\mathbf{G}}_a(m_v^r) \cong (\mathcal{O}_v, +)\,.$$

Hence

$$P(E(K_v)) = P(\mathcal{O}_v) = \dim_{\mathbf{F}_p} \mathcal{O}_v/p\mathcal{O}_v - 0$$

which equals $v(p)\dim_{\mathbf{F}_p} \mathbf{F}_v$ if $v|p$ and zero otherwise. This gives the assertion of the proposition. ∎

Note that the above result is well-known. Our proof in a more general setting can be found in [9], Lemma 3.8 and Prop. 3.9. For an alternative proof, see [8], Lemma 12.10.

Remark 6.6.3. Clearly $\dim_{\mathbf{F}_p} E(K_v)[p] \leq 2$. Moreover, in case $K_v = \mathbf{Q}_p$ and $p \neq 2$, this dimension is at most 1, since $\mu_p \not\subset \mathbf{Q}_p$. So

$$\dim_{\mathbf{F}_p} E(\mathbf{Q}_p)/pE(\mathbf{Q}_p) \leq 2$$

in this case.

Remark 6.6.4. The rough estimate $\dim_{\mathbf{F}_p} E(K_v)[p] \leq 2$ can often be improved. For example, one can apply the multiplication-by-p map to the exact sequences (50) and (51) and look at the kernels. One obtains

$$\dim_{\mathbf{F}_p} E(K_v)[p] \leq \dim_{\mathbf{F}_p} \hat{E}(m_v)[p] + \dim_{\mathbf{F}_p} \tilde{E}_{\rm ns}(\mathbf{F}_v)[p] + \dim_{\mathbf{F}_p}(E(K_v)/E_0(K_v))[p]\,.$$

For example if $K_v = \mathbf{Q}_p$ and $p \neq 2$, then $\hat{E}(m_v)$ has no p-torsion ([13], IV.6.1.1). If moreover, p is a prime of good reduction for E, then E/E_0 is trivial as well, so for such primes $p > 2$ one finds

$$\dim_{\mathbf{F}_p} E(K_v)[p] \leq \dim_{\mathbf{F}_p} \tilde{E}_{\rm ns}(\mathbf{F}_v)[p] = \begin{cases} 0, & \tilde{E} \text{ supersingular,} \\ 1, & \tilde{E} \text{ ordinary.} \end{cases}$$

Lemma 6.6.5. *Assume that $v \not| p$. Then $E_0(K_v^{\rm un})/pE_0(K_v^{\rm un})$ is trivial.*

Proof. Apply the multiplication-by-p map to the second sequence of (50). We get a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{E}(m_v^{\rm un}) & \longrightarrow & E_0(K_v^{\rm un}) & \longrightarrow & \tilde{E}_{\rm ns}(\bar{\mathbf{F}}_v) & \longrightarrow & 0 \\ & & \downarrow [p] & & \downarrow [p] & & \downarrow [p] & & \\ 0 & \longrightarrow & \hat{E}(m_v^{\rm un}) & \longrightarrow & E_0(K_v^{\rm un}) & \longrightarrow & \tilde{E}_{\rm ns}(\bar{\mathbf{F}}_v) & \longrightarrow & 0 \end{array}\,.$$

From the kernel-cokernel sequence extract an exact sequence of cokernels:

$$\hat{E}(m_v^{\mathrm{un}})/p\hat{E}(m_v^{\mathrm{un}}) \longrightarrow E_0(K_v^{\mathrm{un}})/pE_0(K_v^{\mathrm{un}}) \longrightarrow \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v)/p\tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v)\,. \tag{53}$$

The assumption $\mathrm{char}\,\mathbf{F}_v \neq p$ implies that the multiplication-by-p map is an isomorphism $\hat{E}(m_v^{\mathrm{un}}) \to \hat{E}(m_v^{\mathrm{un}})$. So it suffices to show that

$$[p]: \quad \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \longrightarrow \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v)$$

is surjective. We distinguish the following possibilities of reduction:

- Good reduction. In this case $\tilde{E}/\mathbf{F}_v$ is an elliptic curve, $\tilde{E}_{\mathrm{ns}} = \tilde{E}$ and $[p]$ is surjective on $\bar{\mathbf{F}}_v-$valued points, as it is a non-constant morphism of algebraic curves.
- Multiplicative reduction. Here

  $$\tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \cong (\bar{\mathbf{F}}_v^*, *)$$

  and $[p]$ is the p-th power map on $\bar{\mathbf{F}}_v^*$, thus surjective.
- Additive reduction. Here

  $$\tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \cong (\bar{\mathbf{F}}_v, +)$$

  and $[p]$ is the multiplication-by-p map on $\bar{\mathbf{F}}_v$, again surjective (note that $\mathrm{char}\,\mathbf{F}_v \neq p$).

This proves the lemma. ∎

Proposition 6.6.6. *Assume that $v \not| p$. Let C denote $E(K_v^{\mathrm{un}})/E_0(K_v^{\mathrm{un}})$ and let Δ_v denote the minimal discriminant of E at v. Then $\dim_{\mathbf{F}_p} E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}}) = \dim_{\mathbf{F}_p} C/pC$ and*

$$\dim_{\mathbf{F}_p} C/pC \begin{cases} = 0, & E \text{ has good reduction at } v, \\ \leq 2, & p = 2, \\ \leq 1, & p = 3, \\ = 1, & p > 3,\ p|\mathrm{ord}_v\Delta_v > 0 \text{ and } E \text{ has multiplicative reduction}, \\ = 0, & p > 3,\ p \not| \mathrm{ord}_v\Delta_v > 0 \text{ or } E \text{ has additive reduction}. \end{cases}$$

Proof. Apply the multiplication-by-p map to the short exact sequence

$$0 \longrightarrow E_0(K_v^{\mathrm{un}}) \longrightarrow E(K_v^{\mathrm{un}}) \longrightarrow E(K_v^{\mathrm{un}})/E_0(K_v^{\mathrm{un}}) \longrightarrow 0$$

and look at the cokernels. Then

$$E_0(K_v^{\mathrm{un}})/pE_0(K_v^{\mathrm{un}}) = 0 \longrightarrow E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}}) \longrightarrow C/pC \longrightarrow 0\,. \tag{54}$$

The first equality of the lemma follows. The second equality is a direct consequence of the Kodaira-Néron theorem. ∎

6.7 An example

We give an example which illustrates our results. The following elliptic curve was found by Fermigier [4] and has rank ≥ 22 over $K = \mathbf{Q}$.

$$E_{22}: \; y^2 + xy + y = x^3 - 940299517776391362903023121165864\,x \\ + 1070736307071974303342529551544927453465112501136 2\,. \qquad (55)$$

In order to apply our results, let us first collect the standard local information. The given model of E_{22} is minimal at all primes and

$$\Delta(E_{22}) = 2^2 3^9 5^2 7^6 13^6 17^4 37^3\, 47293\, p_1\, p_2$$

with

$$p_1 = 270704849145149791,$$
$$p_2 = 607946578788643377756647126742313704271227343809 97\,.$$

We would like to thank Herman te Riele for producing the above factorization. The curve E_{22} is semi-stable at all primes except 17. The reduction types are

$$2{:}I_2,\; 3{:}I_9,\; 5{:}I_2,\; 7{:}I_6,\; 13{:}I_6,\; 17{:}IV,\; 37{:}I_3,\; 47293{:}I_1,\; p_1{:}I_1,\; p_2{:}I_1\,.$$

A computation (as in Serre [12], Example 5.9.4) shows that the Galois group of $\bar{\mathbf{Q}}/\mathbf{Q}$ acts on $E[p]$ via the full group $GL_2(\mathbf{F}_p)$ for all p. For a non-trivial point $T \in E[p]$ consider the field $L = \mathbf{Q}(T)$. The degree $[L : \mathbf{Q}]$ is $p^2 - 1$, that is maximal possible. The injectivity theorem 6.4.2 applies for every p and the local result 6.6.1 immediately implies the following:

Proposition 6.7.1. *Let p be a prime and $T \in E_{22}[p]$ a non-trivial point of order p. Let $L = \mathbf{Q}(T)$ and define*

$$C_p = \{a \in L^*/L^{*p} \mid \mathrm{ord}_l(a) = 0 \mod p, \text{ all } l\} \cong (\mathbf{Z}/p\mathbf{Z})^{c_p}\,.$$

Then

$$c_p \geq \begin{cases} 16, & p = 2, \\ 15, & p = 3, \\ 19, & p = 17, \\ 20, & p \neq 2, 3, 17. \end{cases}$$

It is interesting to note that such an elliptic curve $E/\mathbf{Q}$ with a large Mordell-Weil rank can be used to produce number fields whose class group has a large p-part. Such examples have been studied in detail for $p = 2$ (see [2]) and for $p = 3$ in case E possesses a rational 3-isogeny (see [14]). The group

$$C_p = \{a \in L^*/L^{*p} \mid \mathrm{ord}_l(a) = 0 \mod p, \text{ all } l\} \cong (\mathbf{Z}/p\mathbf{Z})^{c_p}\,.$$

fits into an exact sequence

$$0 \longrightarrow U_L/U_L^p \longrightarrow C_p \longrightarrow H_L[p] \longrightarrow 0$$

where U_L is the group of units of L and H_L is the class group. Hence a lower bound on the size of C_p combined with the knowledge of the size of U_L gives a lower bound on the size of $H_L[p]$.

In our chosen example, this can be done as follows. The field L has 3 real embeddings for $p=2$ and $p-1$ real embeddings for an odd prime p. Moreover, L^* has no p-torsion for odd p. This follows from the fact the the Galois group acts via the full $GL_2(\mathbf{F}_p)$. We have by the Dirichlet unit theorem

$$\dim_{\mathbf{F}_p} U_L/U_L^p = \begin{cases} 3, & p=2, \\ (p^2+p-4)/2, & p>2. \end{cases}$$

A combination of this with the above proposition gives the following bounds for small primes p:

p	2	3	5	7
c_p	≥ 16	≥ 15	≥ 20	≥ 20
$\dim_{\mathbf{F}_p} U_L/U_L^p$	3	4	13	26
$\dim_{\mathbf{F}_p} H_L[p]$	≥ 13	≥ 11	≥ 7	—

These rough estimates become useless for primes $p \geq 7$. However, a more careful analysis on the possible image of the Kummer map, notably the use of 6.5.2, can be used to produce sharper bounds.

For example, take an intermediate field $\mathbf{Q} \subset K \subset L$ such that $E[p](K) = 0$. By 6.5.2, the image of the Kummer map lands into the kernel of the norm map $N_{L/K} : L^*/L^{*p} \to K^*/K^{*p}$. In particular, the intersection of this image with the unit part U_L/U_L^p is actually contained in the kernel of

$$N_{L/K} : \ U_L/U_L^p \longrightarrow U_K/U_K^p \ . \tag{56}$$

In this way one can produce better lower bounds on the size of $H_L[p]$. Note, however, that the obvious idea to take $K=\mathbf{Q}$ works only for $p=2$, since U_K/U_K^p is trivial for $p>2$. So one has to consider different fields, such as for instance $K=\mathbf{Q}(x_T)$.

In our chosen example, this works as follows. Let $p>2$ and take $K=\mathbf{Q}(x_T)$ which is a subfield of $L=\mathbf{Q}(T)$ of degree 2. Since $E[p](K)$ is trivial, the image of the Kummer map inside the units is contained in the kernel of (56). The field K has $p-1$ real embeddings for an odd prime p. By the Dirichlet unit theorem,

$$\dim_{\mathbf{F}_p} U_K/U_K^p = \frac{1}{4}(p^2+2p-7) \ .$$

The norm map (56) is surjective. Indeed, consider the map $i : U_K/U_K^p \to U_L/U_L^p$ induced by the inclusion $K \to L$. Then the composition $N_{L/K} \circ i$ is multiplication by $[L:K]=2$, hence an isomorphism ($p>2$).

A combination of these considerations with Proposition 6.7.1 gives the following bounds for small primes p:

p	2	3	5	7	11
c_p	≥ 16	≥ 15	≥ 20	≥ 20	≥ 20
$\dim_{\mathbf{F}_p} U_L/U_L^p$	3	4	13	26	64
$\dim_{\mathbf{F}_p} U_K/U_K^p$	3	2	7	14	34
$\dim_{\mathbf{F}_p} H_L[p]$	≥ 13	≥ 13	≥ 14	≥ 8	—

A similar argument can also be applied to bound the part of the Kummer map which lands outside the unit group. In this way it is possible to improve the bounds even further.

For instance, consider the family of elliptic curves over $\mathbf{Q}$

$$E_n: \ y^2 = x^3 + nx, \qquad n \in \mathbf{Z}\,.$$

Let $p=3$, take a non-zero point $T \in E[3]$ and take $L_n = \mathbf{Q}(T)$ (a degree 8 extension of $\mathbf{Q}$). It is not difficult to show that

$$\dim_{\mathbf{F}_3} H_{L_n}[3] \geq \operatorname{rank}_{\mathbf{Q}}(E_n) - 1\,. \tag{57}$$

This gives a non-trivial estimate already for those $E_n/\mathbf{Q}$ whose Mordell-Weil rank is at least 2. For instance, there are six E_n of rank 2 with $|n| \leq 50$, namely the ones with

$$n = -17, 14, 33, 34, 39, 46.$$

For each of these we have $H_{L_n}[3] \cong \mathbf{Z}/3\mathbf{Z}$, so in these cases the estimate (57) is in fact an equality.

References

[1] J. P. Buhler, B. H. Gross, D. B. Zagier, On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3, Math. Comp. **44** (1985), 473–481.

[2] A. Brumer, K. Kramer, The rank of elliptic curves, Duke Math. J. **44** (1977), 715–743.

[3] Z. Djabri, E. F. Schaefer, N. P. Smart, Computing the p-Selmer group of an elliptic curve, to appear in Trans. Amer. Math. Soc.

[4] S. Fermigier, An elliptic curve over $\mathbf{Q}$ of rank ≥ 22, www.fermigier.com.

[5] L. J. Mordell, On the rational solutions of the indeterminate equations of the 3rd and 4th degrees, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

[6] L. J. Mordell, Diophantine equations, Academic Press, London and New York, 1969.

[7] A. Néron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, IHES Publ. Math., **21** (1964), 361–482.

[8] B. Poonen, E. F. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, J. reine und angew. Math. **488** (1997), 141–188.

[9] E. F. Schaefer, Class groups and Selmer groups, J. Number theory **56** (1996), 79–114.

[10] E. F. Schaefer, 2-Descent on the Jacobians of hyperelliptic curves, J. Number Th. **51** (1995), 219–232.

[11] E. F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve, Math. Ann. **310** (1998), 447–471.

[12] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math. **15** (1972), 259–331.

[13] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Math. **106**, Springer-Verlag, New York, 1986.

[14] J. Top, Descent by 3-isogeny and the 3-rank of quadratic fields, In: Advances in number theory (ed. by F. Q. Gouvea and N. Yui), Clarendon Press, Oxford 1993, 303–317.

Samenvatting in het Nederlands

Dit proefschrift bestaat uit twee onafhankelijke delen. Het eerste deel (hoofdstuk 1–5) is gewijd aan infinitesimale deformatietheorie en toepassingen op p-deelbare groepen.

De moduliruimtes van p-deelbare groepen met een PEL-type structuur zijn recent sterk in de belangstelling gekomen. Een reden hiervoor is dat men op zoek is naar goede modellen voor Shimura-variëteiten. Een andere reden is dat ze kunnen helpen een beter begrip te verkrijgen van de moduli van abelse variëteiten. Het eerste deel van dit proefschrift probeert iets toe te voegen aan de kennis van de structuur van deze moduliruimtes. Ze zijn vaak zeer singulier en deze singulariteiten zijn in specifieke gevallen bestudeerd.

Een van de problemen in het bestuderen van deze moduliruimtes is het ontbreken van een deformatietheorie van p-deelbare groepen die algemeen genoeg is om over een willekeurige basisruimte te werken en tegelijkertijd eenvoudig genoeg is om berekeningen uit te kunnen voeren. Een mogelijke oplossing hiervoor zou zijn om de zogenaamde lokale modellen te gebruiken. Het idee is dan om, étale-lokaal, een niet-canoniek isomorfisme te vinden tussen de moduliruimte waar men in geïnteresseerd is en een moduliruimte van een lineair algebraïsch probleem. Onder andere Deligne en Pappas, de Jong en Rapoport en Zink hebben dit idee gebruikt in bepaalde gevallen van een PEL-type structuur moduliruimtes. Het algemene idee is dat zo'n isomorfisme wordt verondersteld te bestaan wanneer de deformatiedata rigide is op de Dieudonné-modulen. We zullen dit idee preciezer formuleren en een bewijs geven van het bestaan van dit isomorfisme.

Een van de moduliruimtes waar ons resultaat op van toepassing is, is die van een p-deelbare groep G met een werking van een maximale order $\mathcal{O}$. In dit geval laten we zien dat de corresponderende modulifunctor formeel glad is over de deformatiefunctor van de raakruimtevoorstelling ρ_τ van $\mathcal{O}$ op G. Dus een noodzakelijke en voldoende voorwaarde om $(G, \mathcal{O})$ te kunnen deformeren is dat men ρ_τ kan deformeren. Dit verklaart de rol van de raakruimtevoorstelling in de studie van Kottwitz, Pappas en anderen naar de platheid van lokale modellen.

De indeling van dit deel van het proefschrift is als volgt. In hoofdstuk 1 wordt de algemene infinitesimale deformatietheorie behandeld. Wij geven de basisresultaten van de theorie, bewijzen een stelling die formele gladde uitbreidingen vergelijkt en bespreken quotiëntfunctoren. In hoofdstuk 2 en 3 geven wij de voorbereidingen voor de hoofdresultaten in hoofdstuk 4, waar wij de isomorfiestelling bewijzen voor de PEL-type moduliproblemen. We passen die toe op het bovengenoemde geval van een p-deelbare groep met een ringwerking en op het geval waarin we een hoofdpolarizatie hebben.

In het tweede deel van dit proefschrift (hoofdstuk 6) houden we ons bezig met de Kummerafbeelding en p-descent op elliptische krommen. Klassiek is 2-descent de meest gebruikte methode om een bovengrens te bepalen van de rang van de Mordell-Weil groep van een elliptische kromme E over een getallenlichaam K. In sommige gevallen maakt de 2-torsie van de Tate-Shafarevich groep het moeilijk om de rang precies te bepalen.

Men zou dan een priemgetal $p > 2$ willen gebruiken in het afdalingsproces, mits men weet dat de Kummerafbeelding nog steeds injectief is. In dit hoofdstuk bewijzen wij dat dit het geval is wanneer de kromme E geen rationale p-isogenie heeft over K. Dit maakt het mogelijk om p-descent toe te passen in deze gevallen. Ook beschrijven wij met standaardmethoden de lokale beelden van de Kummerafbeelding en geven een voorbeeld ter illustratie.

Curriculum vitae

Tim Dokchitser was born on August 12, 1973 in Leningrad, USSR (now St. Petersburg, Russia). He studied in two secondary schools, from September 1980 to June 1990, the last two years in the specialized physical-technical school of St. Petersburg. In September 1990 he started with undergraduate studies in mathematics and computer science at the University of Lund, Sweden. He received his B. Sc. (cum laude) in May 1992 and went on with graduate studies in mathematics. In the year 1994/95 he attended the Master Class program "Arithmetic and Algebraic Geometry" in The Netherlands. In September 1995 he obtained a M. Sc. in mathematics at Lund, specializing in number theory. At the same time he started his Ph. D. studies in the University of Utrecht, The Netherlands, resulting in this thesis.