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 $\{e_1,\ldots,e_{d'},f_1,\ldots,f_d\}$ 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,

$$\mathcal{U} \;\cong\; \mathcal{U}_1 \,\widehat{\otimes}\, \mathcal{U}_2\,.$$

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

$$\begin{array}{ccc} \{\text{left } S\text{-modules}\} & \longrightarrow & \{\text{left } R\text{-modules}\} \\ N & \longmapsto & \mathrm{Hom}_S(\Delta, N) \cong N^{\oplus n}\,. \end{array} \qquad (33)$$

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

$$\sqrt{\pi}: \quad \left(\begin{array}{ccc|ccc} 0 & I_{r'} & & & & \\ \pi I_{r'} & 0 & & & & \\ & & 0 & I_s & & \\ \hline & & \pi I_s & 0 & & \\ & & & & 0 & I_r \\ & & & & \pi I_r & 0 \end{array}\right) \in \mathrm{End}_W(\mathcal{M}) \,. \tag{34}$$

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 $1 \leq i \leq m$.

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

$$R_A = \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n-1} & a_{1,n} \\ b_{2,1} & a_{2,2} & \cdots & a_{2,n-1} & a_{2,n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ b_{n-1,1} & b_{n-1,2} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n-1} & a_{n,n} \end{pmatrix}, \quad a_{i,j} \in A, b_{i,j} \in pA \right\} . \tag{35}$$

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:

$$e_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \ldots \quad , e_n = \begin{pmatrix} 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

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 $\mathrm{Im}\,\pi^k = \ker \pi^{n-k}$ 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 $M/\pi M$,

$$\pi^k : M/\pi M \xrightarrow{\sim} \pi^k M/\pi^{k+1} M . \tag{41}$$

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

$$V_{i,j} = \pi^j \frac{\pi^{-j}V_{i-j}}{\pi^{-j}V_{i-j} \cap \pi M_{i+1}}, \quad 0 \le j < n,$$

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 $n \ge 1$ 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

$$q_0 \overset{p}{\longleftarrow} v_1 \longleftarrow v_2 \longleftarrow \cdots \longleftarrow v_j \longleftarrow q_{j+1} \longleftarrow \cdots \longleftarrow q_n = q_0\,,$$

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

$$\begin{cases} W, & j = 0 \text{ or } j = n, \\ k, & 1 \le j \le n-1 . \end{cases}$$

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

$$\begin{array}{cl} A_1 A_2 \cdots A_{m-1} A_m & = p \times \text{ identity} \\ A_2 A_3 \cdots A_m A_1 & = p \times \text{ identity} \\ \cdots & \cdots \\ A_m A_1 \cdots A_{m-2} A_{m-1} & = p \times \text{ identity} . \end{array}$$

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

$$\begin{array}{ccccccc} \mathcal{M} = & \mathcal{M}_1 & \oplus & \mathcal{M}_2 & \oplus & \mathcal{M}_3 & \\ & v_1 & \longleftarrow & q_2 & \longleftarrow & q_3 & \xleftarrow{p} & v_1 \\ & v_4 & \longleftarrow & q_5 & \xleftarrow{p} & v_6 & \longleftarrow & v_4 \\ & q_7 & \xleftarrow{p} & v_8 & \longleftarrow & v_9 & \longleftarrow & q_7 \\ & q_{10} & \xleftarrow{p} & v_{11} & \longleftarrow & q_{12} & \longleftarrow & q_{10} . \end{array}$$

Thus $\{v_i\}$ is a basis of V, $\{q_i\}$ gives a basis of M/V and the arrows $\longleftarrow$ resp. $\xleftarrow{p}$ 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.