THE DISPLAY OF A FORMAL P-DIVISIBLE GROUP

by

Thomas Zink

Abstract. — We give a new Dieudonné theory which associates to a formal p-divisible group X over an excellent p-adic ring R an object of linear algebra called a display. On the display one can read off the structural equations for the Cartier module of X, and find the crystal of Grothendieck-Messing. We give applications to deformations of formal p-divisible groups.

***Résumé* (Le Display d'un Groupe Formel p-Divisible).** — Nous proposons une nouvelle théorie de Dieudonné qui associe à un groupe formel p-divisible X sur un anneau p-adique excellent R un objet d'algebre linéaire appellé display. Sur le display on peut lire des équations structurelles du module de Cartier de X et aussi trouver directement le cristal de Grothendieck-Messing. Nous donnons des applications au deformations des groupes formels p-divisibles.

Introduction

We fix throughout a prime number p. Let R be a commutative unitary ring. Let $W(R)$ be the ring of Witt vectors. The ring structure on $W(R)$ is functorial in R and has the property that the Witt polynomials are ring homomorphisms:

$$\begin{array}{rccl} \mathbf{w}_n : & W(R) & \longrightarrow & R \\ & (x_0, \ldots x_i, \ldots) & \mapsto & x_0^{p^n} + p x_1^{p^{n-1}} + \ldots + p^n x_n \end{array}$$

Let us denote the kernel of the homomorphism $\mathbf{w}_0$ by I_R. The Verschiebung is a homomorphism of additive groups:

$$\begin{array}{rccl} {}^V : & W(R) & \longrightarrow & W(R) \\ & (x_0, \ldots x_i, \ldots) & \mapsto & (0, x_0, \ldots x_i, \ldots) \end{array}$$

2000 ***Mathematics Subject Classification.*** — 14L05,14F30.
Key words and phrases. — p-divisible groups, crystalline cohomology.

The Frobenius endomorphism ${}^F : W(R) \to W(R)$ is a ring homomorphism. The Verschiebung and the Frobenius are functorial and satisfy the defining relations:

$$\begin{array}{rcll} \mathbf{w}_n({}^F x) & = & \mathbf{w}_{n+1}(x), & \text{for} \quad n \geq 0 \\ \mathbf{w}_n({}^V x) & = & p\mathbf{w}_{n-1}(x), & \text{for} \quad n > 0, \qquad \mathbf{w}_0({}^V x) = 0. \end{array}$$

Moreover the following relations are satisfied:

$${}^F\,{}^V = p, \qquad {}^V({}^F xy) = x\,{}^V y, \quad x, y \in W(R)$$

We note that $I_R = {}^V W(R)$.

Let P_1 and P_2 be $W(R)-$modules. An ${}^F-$linear homomorphism $\phi : P_1 \to P_2$ is a homomorphism of abelian group which satisfies the relation $\phi(wm) = {}^F w\phi(m)$, where $m \in P$, $w \in W(R)$. Let

$$\phi^\sharp : W(R) \otimes_{F,W(R)} P_1 \to P_2$$

be the linearization of ϕ. We will call ϕ an ^{F}-linear epimorphism respectively an ^{F}-linear isomorphism if $\phi^\sharp$ is an epimorphism respectively an isomorphism.

The central notion of these notes is that of a display. The name was suggested by the displayed structural equations for a reduced Cartier module introduced by Norman [N]. In this introduction we will assume that p is nilpotent in R.

Definition 1. — *A $3n-$display over R is a quadruple (P, Q, F, V^{-1}), where P is a finitely generated projective $W(R)-$module, $Q \subset P$ is a submodule and F and V^{-1} are ${}^F-$linear maps $F : P \to P$, $\quad V^{-1} : Q \to P$.*

The following properties are satisfied:

(i) *$I_R P \subset Q \subset P$ and P/Q is a direct summand of the $W(R)-$module $P/I_R P$.*

(ii) *$V^{-1} : Q \longrightarrow P$ is a ^{F}-linear epimorphism.*

(iii) *For $x \in P$ and $w \in W(R)$, we have*

$$V^{-1}({}^V wx) = wFx.$$

If we set $w = 1$ in the relation (iii) we obtain:

$$Fx = V^{-1}({}^V 1x)$$

One could remove F from the definition of a 3n-display. But one has to require that the ${}^F-$linear map defined by the last equation satisfies (iii).

For $y \in Q$ one obtains:

$$Fy = p \cdot V^{-1} y$$

We note that there is no operator V. The reason why we started with V^{-1} is the following example of a 3n-display. Let $R = k$ be a perfect field and let M be a Dieudonné module. It is a finitely generated free $W(k)-$module which is equipped with operators F and V. Since V is injective, there is an inverse operator $V^{-1} : VM \to M$. Hence one obtains a display (M, VM, F, V^{-1}). In fact this defines an equivalence of the category of Dieudonné modules with the category of 3n-displays over k.

Let us return to the general situation. The $W(R)-$module P always admits a direct decomposition

$$P = L \oplus T,$$

such that $Q = L \oplus I_R T$. We call it a normal decomposition. For a normal decomposition the following map is a ${}^F-$linear isomorphism:

$$V^{-1} \oplus F : L \oplus T \longrightarrow P$$

Locally on Spec R the $W(R)$-modules L and T are free. Let us assume that T has a basis $e_1, \ldots, e_d$ and L has a basis $e_{d+1}, \ldots, e_h$. Then there is an invertible matrix (α_{ij}) with coefficients in $W(R)$, such that the following relations hold:

$$\begin{aligned} Fe_j &= \sum_{i=1}^{h} \alpha_{ij} e_i, \quad \text{for} \quad j = 1, \ldots, d \\ V^{-1} e_j &= \sum_{i=1}^{h} \alpha_{ij} e_i \quad \text{for} \quad j = d+1, \ldots, h \end{aligned}$$

Conversely for any invertible matrix (α_{ij}) these relations define a 3n-display.

Let (β_{kl}) the inverse matrix of (α_{ij}). We consider the following matrix of type $(h-d) \times (h-d)$ with coefficients in R/pR :

$$B = (\mathbf{w}_0(\beta_{kl}) \text{ modulo } p)_{k,l=d+1,\ldots,h}$$

Let us denote by $B^{(p)}$ be the matrix obtained from B by raising all coefficients of B to the power p. We say that the $3n-$display defined by (α_{ij}) satisfies the $V-$nilpotence condition if there is a number N such that

$$B^{(p^{N-1})} \cdot \ldots \cdot B^{(p)} \cdot B = 0.$$

The condition depends only on the display but not on the choice of the matrix.

Definition 2. — *A $3n-$display which locally on Spec R satisfies the $V-$ nilpotence condition is called a display.*

The 3n-display which corresponds to a Dieudonné module M over a perfect field k is a display, iff V is topologically nilpotent on M for the p-adic topology. In the covariant Dieudonné theory this is also equivalent to the fact that the $p-$divisible group associated to M has no étale part.

Let S be a ring such that p is nilpotent in S. Let $\mathfrak{a} \subset S$ be an ideal which is equipped with divided powers. Then it makes sense to divide the Witt polynomial $\mathbf{w}_m$ by p^m. These divided Witt polynomials define an isomorphism of additive groups:

$$W(\mathfrak{a}) \longrightarrow \mathfrak{a}^{\mathbb{N}}$$

Let $\mathfrak{a} \subset \mathfrak{a}^{\mathbb{N}}$ be the embedding via the first component. Composing this with the isomorphism above we obtain an embedding $\mathfrak{a} \subset W(\mathfrak{a})$. In fact $\mathfrak{a}$ is a $W(S)$-submodule of $W(\mathfrak{a})$, if $\mathfrak{a}$ is considered as a $W(S)$-module via $\mathbf{w}_0$. Let $R = S/\mathfrak{a}$ be the factor ring. We consider a display $\tilde{\mathcal{P}} = (\tilde{P}, \tilde{Q}, \tilde{F}, \tilde{V}^{-1})$ over S. By base change we obtain a display over R:

$$\tilde{\mathcal{P}}_R = \mathcal{P} = (P, Q, F, V^{-1})$$

By definition one has $P = W(R) \otimes_{W(S)} \tilde{P}$. Let us denote by $\hat{Q} = W(\mathfrak{a})\tilde{P} + \tilde{Q} \subset \tilde{P}$ the inverse image of Q. Then we may extend the operator $\tilde{V}^{-1}$ uniquely to the domain of definition $\hat{Q}$, such that the condition $\tilde{V}^{-1}\mathfrak{a}\tilde{P} = 0$ is fulfilled.

Theorem 3. — *With the notations above let $\tilde{\mathcal{P}}' = (\tilde{P}', \tilde{Q}', \tilde{F}, \tilde{V}^{-1})$ be a second display over S, and $\mathcal{P}' = (P', Q', F, V^{-1})$ the display over R obtained by base change. Assume we are given a morphism of displays $u : \mathcal{P} \to \mathcal{P}'$ over R. Then u has a unique lifting $\tilde{u}$ to a morphism of quadruples:*

$$\tilde{u} : (\tilde{P}, \hat{Q}, \tilde{F}, \tilde{V}^{-1}) \to (\tilde{P}', \hat{Q}', \tilde{F}, \tilde{V}^{-1}).$$

This allows us to associate a crystal to a display: Let R be a ring, such that p is nilpotent in R. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R. Consider a surjection $S \to R$ whose kernel $\mathfrak{a}$ is equipped with a divided power structure. If p is nilpotent in S we call such a surjection a pd-thickening of R. Let $\tilde{\mathcal{P}} = (\tilde{P}, \tilde{Q}, \tilde{F}, \tilde{V}^{-1})$ be any lifting of the display $\mathcal{P}$ to S. By the theorem the module $\widetilde{P}$ is determined up to canonical isomorphism by $\mathcal{P}$. Hence we may define:

$$\mathcal{D}_{\mathcal{P}}(S) = S \otimes_{W(S)} \widetilde{P}$$

This gives a crystal on Spec R if we sheafify the construction.

Next we construct a functor BT from the category of 3n-displays over R to the category of formal groups over R. A nilpotent R-algebra $\mathcal{N}$ is an R-algebra (without unit), such that $\mathcal{N}^N = 0$ for a sufficiently big number N. Let Nil_R denote the category of nilpotent R-algebras. We will consider formal groups as functors from the category Nil_R to the category of abelian groups. Let us denote by $\hat{W}(\mathcal{N}) \subset W(\mathcal{N})$ the subgroup of all Witt vectors with finitely many nonzero components. This is a $W(R)$-submodule. We consider the functor $\mathbf{G}^0_{\mathcal{P}}(\mathcal{N}) = \hat{W}(\mathcal{N}) \otimes_{W(R)} P$ on Nil_R with values in the category of abelian groups. Let $\mathbf{G}^{-1}_{\mathcal{P}}$ be the subgroup functor which is generated by all elements in $\hat{W}(\mathcal{N}) \otimes_{W(R)} P$ of the following form:

$${}^V\xi \otimes x, \quad \xi \otimes y, \qquad \xi \in \hat{W}(\mathcal{N}),\ y \in Q,\ x \in P.$$

Then we define a map:

$$(1) \qquad V^{-1} - \mathrm{id} : \mathbf{G}^{-1}_{\mathcal{P}} \to \mathbf{G}^0_{\mathcal{P}}$$

On the generators above the map $V^{-1} - \mathrm{id}$ acts as follows:

$$(V^{-1} - \mathrm{id})({}^V\xi \otimes x) = \xi \otimes Fx - {}^V\xi \otimes x$$

$$(V^{-1} - \mathrm{id})(\xi \otimes y) = {}^F\xi \otimes V^{-1}y - \xi \otimes y$$

Theorem 4. — *Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a 3n-display over R. The cokernel of the map (1) is a formal group $BT_{\mathcal{P}}$. Moreover one has an exact sequence of functors on Nil_R:*

$$0 \to \mathbf{G}_{\mathcal{P}}^{-1} \xrightarrow{V^{-1}-\mathrm{id}} \mathbf{G}_{\mathcal{P}}^{0} \to BT_{\mathcal{P}} \to 0$$

If $\mathcal{N}$ is equipped with nilpotent divided powers we define an isomorphism:

$$\exp_{\mathcal{P}} : \mathcal{N} \otimes_R P/Q \longrightarrow BT_{\mathcal{P}}(\mathcal{N}),$$

which is called the exponential map. In particular the tangent space of the formal group $BT_{\mathcal{P}}$ is canonically identified with P/Q.

Let $\mathbb{E}_R$ be the local Cartier ring with respect to the prime p. Then $BT_{\mathcal{P}}$ has the following Cartier module:

$$\mathbf{M}(\mathcal{P}) = \mathbb{E}_R \otimes_{W(R)} P/(F \otimes x - 1 \otimes Fx, V \otimes V^{-1}y - 1 \otimes y)_{\mathbb{E}_R},$$

where x runs through all elements of P and y runs through all elements of Q, and $(\quad)_{\mathbb{E}_R}$ indicates the submodule generated by all these elements.

Theorem 5. — *Let $\mathcal{P}$ be a display over R. Then $BT_{\mathcal{P}}$ is a formal p-divisible group of height equal to $\mathrm{rank}_R\, P$.*

The restriction of the functor BT to the category of displays is faithful. It is fully faithful, if the ideal of nilpotent elements in R is a nilpotent ideal.

The following main theorem gives the comparison of our theory and the crystalline Dieudonné theory of Grothendieck and Messing.

Theorem 6. — *Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over a ring R. Then there is a canonical isomorphism of crystals over R:*

$$\mathcal{D}_{\mathcal{P}} \xrightarrow{\sim} \mathbb{D}_{BT_{\mathcal{P}}}$$

Here the right hand side is the crystal from Messing's book [Me]. If $W(R) \to S$ is a morphism of pd−thickenings of R, we have a canonical isomorphism

$$S \otimes_{W(R)} P \cong \mathbb{D}_{BT_{\mathcal{P}}}(S).$$

In this theorem we work with the crystalline site whose objects are pd-thickenings $S \to R$, such that the kernel is a nilpotent ideal. We remark that the crystal $\mathbb{D}_{BT_{\mathcal{P}}}$ is defined in [Me] only for pd-thickenings with nilpotent divided powers. But if one deals with p-divisible groups without an étale part this restriction is not necessary (see corollary 97 below). In particular this shows, that the formal p-divisible group $BT_{\mathcal{P}}$ lifts to a pd-thickening $S \to R$ with a nilpotent kernel, iff the Hodge filtration of the crystal lifts (compare [Gr] p.106).

The functor BT is compatible with duality in the following sense. Assume we are given 3n-displays $\mathcal{P}_1$ and $\mathcal{P}_2$ over a ring R, where p is nilpotent.

Definition 7. — *A bilinear form* (,) *on the pair of 3n-displays* $\mathcal{P}_1, \mathcal{P}_2$ *is a bilinear form of* $W(R)-$*modules:*

$$P_1 \times P_2 \to W(R),$$

which satisfies

$$^V(V^{-1}y_1, V^{-1}y_2) = (y_1, y_2) \quad \textit{for} \quad y_1 \in Q_1,\ y_2 \in Q_2.$$

Let us denote by $\mathrm{Bil}(\mathcal{P}_1, \mathcal{P}_2)$ the abelian group of these bilinear forms. Then we will define a homomorphism:

$$\mathrm{Bil}(\mathcal{P}_1, \mathcal{P}_2) \to \mathrm{Biext}^1(BT_{\mathcal{P}_1} \times BT_{\mathcal{P}_2}, \hat{\mathbb{G}}_m) \tag{2}$$

Here the right hand side denotes the group of biextensions of formal groups in the sense of Mumford [Mu].

To do this we consider the exact sequences for $i = 1, 2$:

$$0 \to \mathbf{G}^{-1}_{\mathcal{P}_i} \overset{V^{-1}-\mathrm{id}}{\longrightarrow} \mathbf{G}^0_{\mathcal{P}_i} \to BT_{\mathcal{P}_i} \to 0$$

To define a biextension in $\mathrm{Biext}^1(BT_{\mathcal{P}_1} \times BT_{\mathcal{P}_2}, \hat{\mathbb{G}}_m)$, it is enough to give a pair of bihomomorphisms (compare [Mu]):

$$\begin{array}{rcl} \alpha_1 : \mathbf{G}^{-1}_{\mathcal{P}_1}(\mathcal{N}) \times \mathbf{G}^0_{\mathcal{P}_2}(\mathcal{N}) & \to & \hat{\mathbb{G}}_m(\mathcal{N}), \\ \alpha_2 : \mathbf{G}^0_{\mathcal{P}_1}(\mathcal{N}) \times \mathbf{G}^{-1}_{\mathcal{P}_2}(\mathcal{N}) & \to & \hat{\mathbb{G}}_m(\mathcal{N}), \end{array}$$

which agree on $\mathbf{G}^{-1}_{\mathcal{P}_1}(\mathcal{N}) \times \mathbf{G}^{-1}_{\mathcal{P}_2}(\mathcal{N})$, if we consider $\mathbf{G}^{-1}_{\mathcal{P}_i}$ as a subgroup of $\mathbf{G}^0_{\mathcal{P}_i}$ via the embedding $V^{-1} - id$, for $i = 1, 2$. To define α_1 and α_2 explicitly we use the Artin-Hasse exponential $\mathrm{hex} : \hat{W}(\mathcal{N}) \to \hat{\mathbb{G}}_m(\mathcal{N})$:

$$\begin{array}{rcll} \alpha_1(y_1, x_2) & = & \mathrm{hex}(V^{-1}y_1, x_2) & \text{for} \quad y_1 \in \mathbf{G}^{-1}_{\mathcal{P}_1}(\mathcal{N}), \quad x_2 \in \mathbf{G}^0_{\mathcal{P}_2}(\mathcal{N}) \\ \alpha_2(x_1, y_2) & = & -\mathrm{hex}(x_1, y_2) & \text{for} \quad x_1 \in \mathbf{G}^0_{\mathcal{P}_1}(\mathcal{N}) \quad y_2 \in \mathbf{G}^{-1}_{\mathcal{P}_2}(\mathcal{N}) \end{array}$$

This completes the definition of the map (2).

Theorem 8. — *Let R be a ring, such that p is nilpotent in R, and such that the ideal of its nilpotent elements is nilpotent. Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be displays over R. Assume that the display $\mathcal{P}_2$ is $F-$nilpotent, i.e. there is a number r such that $F^r P_2 \subset I_R P_2$. Then the map (2) is an isomorphism.*

I would expect that BT induces an equivalence of categories over any noetherian ring. We have the following result:

Theorem 9. — *Let R be an excellent local ring or a ring such that R/pR is an algebra of finite type over a field k. Assume that p is nilpotent in R. Then the functor BT is an equivalence from the category of displays over R to the category of formal $p-$divisible groups over R.*

We will now define the obstruction to lift a homomorphism of displays. Let $S \to R$ be a pd-thickening. Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be displays over S, and let $\bar{\mathcal{P}}_1$ and $\bar{\mathcal{P}}_2$ be their reductions over R. We consider a morphism of displays $\bar{\varphi} : \bar{\mathcal{P}}_1 \to \bar{\mathcal{P}}_2$. Let $\varphi : P_1 \to P_2$ the unique map which exists by theorem 3. It induces a map, which we call the obstruction to lift $\bar{\varphi}$:

$$\operatorname{Obst} \bar{\varphi} : Q_1/I_S P_1 \longrightarrow \mathfrak{a} \otimes_S P_2/Q_2$$

This morphism vanishes iff $\bar{\varphi}$ lifts to a homomorphism of displays $\varphi : \mathcal{P}_1 \to \mathcal{P}_2$.

We will now assume that $pS = 0$ and that $\mathfrak{a}^p = 0$. We equip $S \to R$ with the trivial divided powers. Then $p \operatorname{Obst} \bar{\varphi} = 0$. Therefore $p\bar{\varphi}$ lifts to a homomorphism of displays $\psi : \mathcal{P}_1 \to \mathcal{P}_2$. Let us assume moreover that we are given a second surjection $T \to S$ with kernel $\mathfrak{b}$, such that $\mathfrak{b}^p = 0$, and such that $pT = 0$. Let $\tilde{\mathcal{P}}_1$ and $\tilde{\mathcal{P}}_2$ be two displays, which lift $\mathcal{P}_1$ and $\mathcal{P}_2$. Then we give an easy formula (proposition 73), which computes $\operatorname{Obst} \psi$ directly in terms of $\operatorname{Obst} \bar{\varphi}$. This formula was suggested by the work of Gross and Keating [GK], who considered one-dimensional formal groups. We demonstrate how some of the results in [G] and [K] may be obtained from our formula.

Finally we indicate how p-divisible groups with an étale part may be treated using displays. Let R be an artinian local ring with perfect residue class field k of characteristic $p > 0$. We assume moreover that $2R = 0$ if $p = 2$. The exact sequence

$$0 \longrightarrow W(\mathfrak{m}) \longrightarrow W(R) \xrightarrow{\ \pi\ } W(k) \longrightarrow 0,$$

admits a unique section $\delta : W(k) \to W(R)$, which is a ring homomorphism commuting with ^{F}.

We define as above:

$$\hat{W}(\mathfrak{m}) = \{(x_0, x_1, \dots) \in W(\mathfrak{m}) \quad | \quad x_i = 0 \quad \text{for almost all} \quad i\}$$

Since $\mathfrak{m}$ is a nilpotent algebra, $\hat{W}(\mathfrak{m})$ is a subalgebra stable by F and V. Moreover $\hat{W}(\mathfrak{m})$ is an ideal in $W(R)$.

We define a subring $\hat{W}(R) \subset W(R)$:

$$\hat{W}(R) = \{\xi \in W(R) \quad | \quad \xi - \delta\pi(\xi) \in \hat{W}(\mathfrak{m})\}.$$

Again we have a split exact sequence

$$0 \longrightarrow \hat{W}(\mathfrak{m}) \longrightarrow \hat{W}(R) \xrightarrow{\ \pi\ } W(k) \longrightarrow 0,$$

with a canonical section δ of π. Under the assumptions made on R the subring $\hat{W}(R) \subset W(R)$ is stable by ^{F} and ^{V}. Therefore we may replace in the definition of a 3n-display the ring $W(R)$ by $\hat{W}(R)$. The resulting object will be called a Dieudonné display over R. In a forthcoming publication we shall prove:

***Theorem*:** *Let R be an artinian local ring with perfect residue field k of characteristic $p > 0$. We assume moreover that $2R = 0$ if $p = 2$. Then the category of Dieudonné displays over R is equivalent to the category of p-divisible groups over R.*

I introduced displays after discussions with M.Rapoport on the work of Gross and Keating [GK]. I thank Rapoport for his questions and comments and also for his constant encouragement, which made this work possible. I also thank J. de Jong, G.Faltings, and B.Messing for helpful remarks, and O.Gabber for his helpful questions, which he asked during lectures. The remarks of the referee helped me to correct an error in the first version of this paper. I forgot that Messing [Me] assumes nilpotent divided powers, which is neccesary in the presence of an étale part (see the remarks above). I am very grateful to him. Finally I thank the organizers of the "P-adic Semester" in Paris 1997 for giving me the possibility to present my results there. At this time a preliminary version of this work entitled "Cartier Theory and Crystalline Dieudonné Theory" was distributed.

Note added in March 2001: A proof of the last theorem above is given in [Z3]. The relation of the theory of Ch. Breuil [Br] to the theory given here is explained in [Z4]. A construction of the display associated to an abelian scheme over R is given in [LZ], by means of a de Rham-Witt complex relative to R.

Contents

1. Displays

1.1. Generalities. — Let A and B be commutative rings and $\rho : A \longrightarrow B$ be a homomorphism. If N is a $B-$module, we denote by $N_{[\rho]}$ the $A-$module obtained by restriction of scalars. Let M be a $A-$module. A $\rho-$linear map $\alpha : M \to N$ is an $A-$linear map $\alpha : M \longrightarrow N_{[\rho]}$. It induces a $B-$linear map $\alpha^{\#} : B \otimes_{\rho,A} M \longrightarrow N$. We will say that α is a $\rho-$linear isomorphism (respectively epimorphism), if $\alpha^{\#}$ is an isomorphism (respectively epimorphism).

Let R be a unitary commutative ring, which is a $\mathbb{Z}_{(p)}$-algebra. Let $W(R)$ be the Witt ring with respect to the prime number p. We apply the definitions above to the case where $A = B = W(R)$, and where ρ is the Frobenius endomorphism ${}^F : W(R) \to W(R)$. (For notations concerning the Witt ring we refer to the introduction.) As an example we consider the Verschiebung ${}^V : W(R) \to W(R)$. It induces a $W(R)-$linear isomorphism

$$^V : W(R)_{[F]} \to I_R.$$

Its inverse is a ${}^F-$linear map:

$$^{V^{-1}} : I_R \to W(R)$$

This map is a ${}^F-$linear epimorphism, but it is not a ${}^F-$linear isomorphism (!) unless R is a perfect ring.

We define base change for ${}^F-$linear maps as follows. Let $S \to R$ be a homomorphism of commutative rings. Assume $\alpha : Q \to P$ is a ${}^F-$linear homomorphism of $W(S)-$modules. Then the base change α_R is

$$\begin{array}{cccc} \alpha_R : & W(R) \otimes_{W(S)} Q & \longrightarrow & W(R) \otimes_{W(S)} P. \\ & w \otimes x & \mapsto & {}^F w \otimes \alpha(x) \end{array}$$

We have

$$(\alpha^{\#})_{W(R)} = (\alpha_R)^{\#},$$

where the index $W(R)$ is base change for linear maps.

We are now ready to define the notion of a display.

Definition 1. — *A $3n-$display over R is a quadrupel (P, Q, F, V^{-1}), where P is a finitely generated projective $W(R)-$module, $Q \subset P$ is a submodule and F and V^{-1} are ${}^F-$linear maps $F : P \to P, \quad V^{-1} : Q \to P$.*

The following properties are satisfied:

(i) *$I_R P \subset Q \subset P$ and there exists a decomposition of P into a direct sum of $W(R)-$modules $P = L \oplus T$, such that $Q = L \oplus I_R T$.*

(ii) *$V^{-1} : Q \longrightarrow P$ is a ^{F}-linear epimorphism.*

(iii) *For $x \in P$ and $w \in W(R)$, we have*

$$V^{-1}({}^V wx) = wFx. \tag{1}$$

We make some formal remarks on this definition. The $3n-$displays form an additive category. We are mainly interested in the case, where R is a $\mathbb{Z}_p$-algebra. Then we have $\mathbb{Z}_p \subset W(R)$ and hence the category is $\mathbb{Z}_p-$linear.

The operator F is uniquely determined by V^{-1} because of the relation:

$$V^{-1}({}^V 1x) = Fx, \quad \text{for } x \in P.$$

If we apply this to the case $x = y \in Q$ and apply the ${}^F-$linearity of V^{-1}, we obtain the relation:

$$Fy = p \cdot V^{-1} y. \tag{2}$$

A decomposition $P = L \oplus T$ as required in (i), we will call a normal decomposition. We set $\overline{P} = P/I_R P$ and $\overline{Q} = Q/I_R P$. Then we get a filtration of $R-$modules

$$0 \subset \overline{Q} \subset \overline{P}, \tag{3}$$

whose graded pieces are projective finitely generated R-modules. This is the Hodge filtration associated to a display.

Lemma 2. — *Let R be a $p-$adically complete and separated ring. Let us replace in the definition* 1 *the condition (i) by the weaker condition that $I_R P \subset Q \subset P$ and that the filtration (3) has finitely generated projective R-modules as graded pieces. Then (P, Q, F, V^{-1}) is a 3n-display.*

Before proving the lemma we need a general fact about the Witt ring.

Proposition 3. — *Let R be a p-adic ring, i.e. complete and separated in the p-adic topology. Then the ring $W(R)$ is p-adic. Moreover it is complete and separated in the I_R-adic topology.*

Proof. — We begin to show that $W(R)$ is separated in the p-adic topology. Since $W(R)$ is the projective limit of the rings $W_n(R/p^m R)$ for varying n and m it is enough to show that that p is nilpotent in each of the rings $W_n(R/p^m R)$. To see this we consider a ring $\mathfrak{a}$ without unit such that $p^m \mathfrak{a} = 0$. An easy induction on m shows that p is nilpotent in $W_n(\mathfrak{a})$.

It is enough to prove our assertion for a ring R which has no p-torsion. Indeed in the general case we may choose a surjection $S \to R$ where S is a torsion free p-adic ring. But then we obtain a surjection $W(S) \to W(R)$ from the p-adic ring $W(S)$ to the p-adically separated ring $W(R)$. This implies that $W(R)$ is a p-adic ring.

To treat the case of a p-adic ring we need a few lemmas:

Lemma 4. — *Let S be a ring without p-torsion. Let $x = (x_0, \ldots, x_m) \in W_{m+1}(S)$ be a Witt vector. Then for any fixed number $s \geq 1$ the following conditions are equivalent:*

(i) $p^s \mid x_i$ *for* $i = 0, \ldots, m$

(ii) $p^{n+s} \mid \mathbf{w}_n(x)$ *for* $n = 0, \ldots, m$.

Proof. — The first condition clearly implies the second. Assume the second condition holds. By induction we may assume $p^s \mid x_i$ for $i = 0, \ldots, n-1$. Then we write

$$\mathbf{w}_n(x) = \mathbf{w}_{n-1}(x_0^p \ldots x_{n-1}^p) + p^n x_n.$$

By the obvious implication and by induction the first term on the right hand side is $\equiv 0 \mod p^{(n-1)+ps}$. Since $(n-1) + ps \geq n + s$, we conclude $p^n x_n \equiv 0 \mod p^{n+s} S$. □

Lemma 5. — *Let S be a p-torsion free ring. Let $a \in W_m(S)$ be a given Witt vector. Let u be a number. We assume that the equation*

$$p^u x = a \tag{4}$$

has for each s a solution in the ring $W_m(R/p^s R)$. Then the equation (4) has a solution in $W_m(R)$.

Proof. — Let us consider a fixed s. By assumption there is a $z \in W_m(R)$, such that $p^u z = a$ holds in the ring $W_m(R/p^{s+u} R)$. We let x_s be the image of z in the ring $W_m(R/p^s R)$. Then we claim that x_s is independent of the choice of z.

Indeed, let z' be a second choice and set $\xi = z - z'$. The Witt components of $p^u \xi$ are elements of $p^{s+u} R$. Hence the lemma implies

$$p^{n+s+u} \mid \mathbf{w}_n(p^u \xi) \text{ for } n = 0 \ldots m-1.$$

It follows that $p^{n+s} \mid \mathbf{w}_n(\xi)$. But applying the lemma again we obtain the $p^s \mid \xi_i$ for all Witt components of ξ.

This shows the uniqueness of x_s. We set $x = \varprojlim x_s \in W(R)$ and obtain the desired solution of (4). □

Lemma 6. — *Let S be without p-torsion. We will denote by I_r the ideal ${}^{V^r}W(S) \subset W(S)$. Let $\mathcal{T}$ be the linear topology on $W(S)$, such that the following ideals form a fundamental set of open neighbourhoods of zero:*

$$I_r + W(p^s S) \tag{5}$$

Here, r, s runs through all pairs of numbers.

Then $p^u W(S)$ is for each number u closed in the topology $\mathcal{T}$.

Proof. — We have to show

$$\bigcap_{r,s\in\mathbb{N}} p^u W(S) + I_r + W(p^s S) = p^u W(S) \tag{6}$$

Let x be an element from the left hand side.

We denote for a fixed number r by $\overline{x}$ the image of x in $W_r(S)$. Then the equation

$$p^u z = \overline{x}$$

has a solution z in the ring $W_r(S/p^s S)$ for each number s. By the last lemma we have a solution in $W_r(S)$ too. This shows $x \in p^u W(S) + I_r$.

We take the unique solution $z_r \in W_r(S)$ of $p^u z_r = x$ in $W_r(S)$, and we set $z = \varprojlim z_r$. Hence $x = p^u z \in p^u W(S)$. □

Let S be a torsion free p-adic ring. Clearly the Witt ring $W(S)$ is complete and separated in the topology $\mathcal{T}$. The assertion that $W(S)$ is p-adic is a consequence of the last lemma and the following elementary topological fact (see Bourbaki Topologie III §3 Cor 1):

Lemma 7. — *Let G be an abelian group. Let $\mathcal{A}$ resp. $\mathcal{B}$ be linear topologies on G, which are given by the fundamental systems of neighbourhood of zero $\{A_n\}$ resp. $\{B_n\}$, where A_n and B_n are subgroups.*

We make the following assumptions:

a) *Each A_n is open in the $\mathcal{B}$-topology, i.e. the $\mathcal{B}$ topology is finer.*
b) *Each B_n is closed in the $\mathcal{A}$-topology.*
c) *G is complete and separated in the $\mathcal{A}$-topology.*

Then G is complete and separated in the $\mathcal{B}$-topology.

We omit the easy proof.

We note that in the Witt ring $W(R)$ of any ring we have an equality of ideals for any natural number n:

$$I_R^n = p^{n-1} I_R \tag{7}$$

If R is a p-adic ring the additive group I_R is p-adically complete and separated, because it is by the Verschiebung isomorphic to $W(R)$. This shows that $W(R)$ is then also complete in the I_R-adic topology. This completes the proof of proposition 3. □

Corollary 8. — *Assume that p is nilpotent in R. Then the p-adic and the I_R-adic topology on $W(R)$ coincide. This topology is finer than the V-adic topology, which has the ideals $I_n = {}^{V^n}W(R)$ as a fundamental system of neighbourhoods of zero.*

Proof. — This is clear. □

We turn now to the proof of lemma 2. The proposition 3 implies in particular that $W(R)$ is complete and separated in the I_R-adic topology. We set $A_n = W(R)/I_R^n$. We start with a decomposition $\bar{P} = \bar{L} \oplus \bar{T}$ such that $Q/I_RP = \bar{L}$ over $A_1 = R$ and lift it step by step to a decomposition $A_n \otimes_{W(R)} P = L_n \oplus T_n$ over A_n using the surjections with nilpotent kernel $A_n \to A_{n-1}$. Then we obtain the desired decomposition by taking the projective limit.

Lemma 9. — *Let (P, Q, F, V^{-1}) be a 3n-display over a ring R, and $P = L \oplus T$ be a normal decomposition. Then the map*

$$V^{-1} \oplus F : L \oplus T \longrightarrow P \tag{8}$$

is a ${}^F-$linear isomorphism.

Proof. — Since source and target of $V^{-1} \oplus F$ are projective modules of the same rank, it is enough to show, that we have a ${}^F-$linear epimorphism. Indeed, by the property (ii) of the definition 1 the $W(R)-$module P is generated by $V^{-1}l$, for $l \in L$ and $V^{-1}({}^V wt)$ for $t \in T$ and $w \in W$. The lemma follows, since $V^{-1}({}^V wt) = wFt$. □

Using this lemma we can define structural equations for a 3n-display, whose Hodge filtration (3) has free graded pieces. Let (P, Q, F, V^{-1}) be a 3n-display over R with this property. Then the modules L and T in a a normal decomposition $P = L \oplus T$, are free. We choose a basis $e_1, \dots, e_d$ of T, and basis $e_{d+1} \dots e_h$ of L. Then there are elements $\alpha_{ij} \in W(R), \quad i, j = 1, \dots, h,$, such that the following relations hold.

$$\begin{aligned} Fe_j &= \sum_{i=1}^{h} \alpha_{ij} e_i, \quad \text{for} \quad j = 1, \dots, d \\ V^{-1}e_j &= \sum_{i=1}^{h} \alpha_{ij} e_i \quad \text{for} \quad j = d+1, \dots, h \end{aligned} \tag{9}$$

By the lemma 9 the matrix (α_{ij}) is invertible.

Conversely assume we are given an invertible $h \times h-$matrix (α_{ij}) over the ring $W(R)$ and a number d, such that $0 \leq d \leq h$. Let T be the free $W(R)-$module with basis $e_1, \dots e_d$ and L be the free $W(R)-$module with basis $e_{d+1}, \dots, e_h$. We set $P = L \oplus T$ and $Q = L \oplus I_RT$, and we define the ${}^F-$linear operators F and V^{-1} by the equations (9) and the following equations

$$Fe_j = \sum_{i=1}^{h} p\alpha_{ij}e_i, \quad j = d+1, \dots, h$$
$$V^{-1}({}^V we_j) = \sum_{i=1}^{h} w\alpha_{ij}e_i, \quad j = 1, \dots, d$$

One verifies easily, that this defines a 3n-display over R.

For a 3n-display (P, Q, F, V^{-1}) we do not have an operator V as in Dieudonné or Cartier theory. Instead we have a $W(R)$-linear operator:

$$V^{\sharp} : P \longrightarrow W(R) \otimes_{F,W(R)} P \tag{10}$$

Lemma 10. — *There exists a unique $W(R)-$linear map (10), which satisfies the following equations:*

$$\begin{aligned} V^{\sharp}(wFx) &= p \cdot w \otimes x, \quad \textit{for} \quad w \in W(R), x \in P \\ V^{\sharp}(wV^{-1}y) &= w \otimes y, \quad \textit{for} \quad y \in Q \end{aligned} \tag{11}$$

Moreover we have the identities

$$F^{\sharp}V^{\sharp} = p\,\mathrm{id}_P, \quad V^{\sharp}F^{\sharp} = p\,\mathrm{id}_{W(R)\otimes_{F,W(R)}P}\,. \tag{12}$$

Proof. — Clearly $V^{\sharp}$ is uniquely determined, if it exists. We define the map $V^{\sharp}$ by the following commutative diagram, where $W = W(R)$:

$$\begin{array}{ccc} W \otimes_{F,W} L \oplus W \otimes_{F,W} T & \xrightarrow{(V^{-1}+F)^{\sharp}} & P \\ \Big\downarrow{\scriptstyle \mathrm{id} + p\,\mathrm{id}} & & \Big\downarrow{\scriptstyle V^{\sharp}} \\ W \otimes_{F,W} L \oplus W \otimes_{F,W} T & \longrightarrow & W \otimes_{F,W} P \end{array} \tag{13}$$

Here the lower horizontal map is the identity.

We need to verify (11) with this definition. We write $x = l + t$, for $l \in L$ and $t \in T$.

$$\begin{aligned} V^{\sharp}(wFx) = V^{\sharp}(wFl) + V^{\sharp}(wFt) &= \\ V^{\sharp}(V^{-1}({}^V wl)) + V^{\sharp}(wFt) &= \\ 1 \otimes {}^V wl + pw \otimes t = pw \otimes (l+t) &= pw \otimes x. \end{aligned}$$

Next take y to be of the form $y = l + {}^V ut$.

$$\begin{aligned} V^{\sharp}(wV^{-1}y) &= V^{\sharp}(wV^{-1}l) + V^{\sharp}(wuFt) \\ &= w \otimes l + pwu \otimes t = w \otimes l + w\, {}^{FV}u \otimes t \\ &= w \otimes (l + {}^V ut) = w \otimes y. \end{aligned}$$

The verification of (12) is left to the reader. □

***Remark*:** The cokernel of $V^\sharp$ is a projective $W(R)/pW(R)-$module of the same rank as the $R-$module P/Q.

Let us denote by ${}^{F^i}V^\sharp$ the $W(R)-$linear map

$$\mathrm{id} \otimes_{F^i, W(R)} V^\sharp : W \otimes_{F^i, W} P \longrightarrow W \otimes_{F^{i+1}, W} P,$$

and by $V^{n\sharp}$ the composite ${}^{F^{n-1}}V^\sharp \circ \cdots \circ^F V^\sharp \circ V^\sharp$.

We say that a 3n-display satisfies the nilpotence (or V-nilpotence) condition, if there is a number N, such that the map

$$V^{N\sharp} : P \longrightarrow W(R) \otimes_{F^N, W(R)} P$$

is zero modulo $I_R + pW(R)$. Differently said, the map

$$R/pR \otimes_{\mathbf{w}_0, W(R)} P \longrightarrow R/pR \otimes_{\mathbf{w}_N, W(R)} P \tag{14}$$

induced by $V^{N\sharp}$ is zero.

Definition 11. — *Let p be nilpotent in R. A display (P, Q, F, V^{-1}) is a 3n-display, which satisfies the nilpotence condition above.*

Let us choose a normal decomposition $P = L \oplus T$. It is obvious from the diagram (13) that the map

$$R/pR \otimes_{\mathbf{w}_\circ, W(R)} P \xrightarrow{V^\sharp} R/pR \otimes_{\mathbf{w}_1, W(R)} P \xrightarrow{pr} R/pR \otimes_{\mathbf{w}_1, W(R)} T$$

is zero. Therefore it is equivalent to require the nilpotence condition for the following map:

$$U^\sharp : L \hookrightarrow L \oplus T = P \xrightarrow{V^\sharp} W \otimes_{F, W} P \xrightarrow{pr} W \otimes_{F, W} L$$

Less invariantly but more elementary the nilpotence condition may be expressed if we choose a basis as in (9). Let $(\beta_{k,l})$ be the inverse matrix to $(\alpha_{i,j})$. Consider the following $(h-d) \times (h-d)-$matrix with coefficients in R/pR :

$$B = (\mathbf{w}_0(\beta_{kl}) \text{ modulo } p)_{k,l=d+1,\ldots,h}$$

Let $B^{(p^i)}$ be the matrix obtained by raising the coefficients to the p^i-th power. Then the nilpotence condition says exactly that for a suitable number N :

$$B^{(p^{N-1})} \cdot \ldots \cdot B^{(p)} \cdot B = 0 \tag{15}$$

Corollary 12. — *Assume that p is nilpotent in R. Let (P,Q,F,V^{-1}) be a display over R. Then for any given number n there exists a number N, such that the following map induced by $V^{N\sharp}$ is zero:*

$$W_n(R) \otimes_{W(R)} P \longrightarrow W_n(R) \otimes_{F^N,W(R)} P$$

Proof. — Indeed, by the proof of proposition 3 the ideal $I_R + pW_n(R)$ in $W_n(R)$ is nilpotent. □

We will also consider displays over linear topological rings R of the following type. The topology on R is given by a filtration by ideals:

$$R = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \ldots \supset \mathfrak{a}_n \ldots , \tag{16}$$

such that $\mathfrak{a}_i\mathfrak{a}_j \subset \mathfrak{a}_{i+j}$. We assume that p is nilpotent in $R/\mathfrak{a}_1$ and hence in any ring $R/\mathfrak{a}_i$. We also assume that R is complete and separated with respect to this filtration. In particular it follows that R is a p-adic ring. In the context of such rings we will use the word display in the following sense:

Definition 13. — *Let R be as above. A 3n-display $\mathcal{P} = (P,Q,F,V^{-1})$ over R is called a display, if the 3n-display obtained by base change over $R/\mathfrak{a}_1$ is a display in sense of definition 11.*

Let $\mathcal{P}$ be a display over R. We denote by $\mathcal{P}_i$ the 3n-display over $R/\mathfrak{a}_i$ induced by base change. Then $\mathcal{P}_i$ is a display in the sense of definition 11. There are the obvious transition isomorphisms

$$\phi_i : (\mathcal{P}_{i+1})_{R/\mathfrak{a}_i} \to \mathcal{P}_i \tag{17}$$

Conversely assume we are given for each index i a display $\mathcal{P}_i$ over the discrete ring $R/\mathfrak{a}_i$, and transition isomorphisms ϕ_i as above. Then the system $(\mathcal{P}_i, \phi_i)$ is obtained from a display $\mathcal{P}$ over R. In fact this is an equivalence of the category of systems of displays $(\mathcal{P}_i, \phi_i)$ and the category of displays over R.

If R is for example complete local ring with maximal ideal $\mathfrak{m}$, such that $pR = 0$, we can consider the category of displays over R in the sense of definition 11 but we can also consider the category of displays over the topological ring R, with its $\mathfrak{m}$-adic topology. The last category is in general strictly bigger.

1.2. Examples. — ***Example* 14:** Let $R = k$ be a perfect field. A Dieudonné module over k is a finitely generated free $W(k)$-module M, which is equipped with a ^{F}-linear map $F : M \to M$, and a ${}^{F^{-1}}$-linear map $V : M \to M$, such that:

$$FV = VF = p$$

We obtain a 3n-display by setting $P = M$, $Q = VM$ with the obvious operators $F : M \to M$ and $V^{-1} : VM \to M$. Moreover (P,Q,F,V^{-1}) is a display if the map $V : M/pM \to M/pM$ is nilpotent. The map $V^{\sharp}$ is given by

$$\begin{aligned} V^\sharp \quad : \quad M &\longrightarrow W(k) \otimes_{F,W(k)} M. \\ m &\longmapsto 1 \otimes Vm \end{aligned}$$

In the other direction starting with a display (P, Q, F, V^{-1}) we obtain a Dieudonné module structure on P if we define V as the composite:

$$V : P \xrightarrow{V^\sharp} \begin{array}{ccc} W(k) \otimes_{F,W(k)} P & \to & P \\ w \otimes x & \mapsto & {}^{F^{-1}}w \cdot x \end{array} \tag{18}$$

This makes sense because the Frobenius endomorphism ^{F} is an automorphism of $W(k)$. We see that the category of 3n-displays over a perfect field is naturally equivalent to the category of Dieudonné modules.

More generally let k be a perfect ring of characteristic p. Then ^{F} is an automorphism on $W(k)$ and $pW(k) = I_k$. We call a Dieudonné module k a finitely generated projective $W(k)-$module M equipped with two $\mathbb{Z}-$linear operators

$$F : M \longrightarrow M,$$

$$V : M \longrightarrow M,$$

which satisfy the relation $F(wx) = {}^FwFx,\ V({}^Fwx) = wVx,\ FV = VF = p.$

If we are given a homomorphism of $k \to k'$ of perfect rings, we obtain the structure of a Dieudonné module on $M' = W(k') \otimes_{W(k)} M$.

Since p is injective on $W(R)$, there is an exact sequence of k-modules:

$$0 \to M/FM \xrightarrow{V} M/pM \to M/VM \to 0$$

If we tensorize this sequence with k' we obtain the corresponding sequence for M'. In particular this sequence remains exact. We also see from the sequence that M/VM is of finite presentation. Hence we conclude that M/VM is a finitely generated projective k-module. Therefore we obtain a 3n-display (M, VM, F, V^{-1}).

Proposition 15. — *The category of 3n-displays over a perfect ring k is equivalent to the category of Dieudonné modules over k. Moreover the displays correspond exactly to the Dieudonné modules, such that V is topologically nilpotent for the $p-$adic topology on M.*

The proof is obvious. We remark that a Dieudonné module M, such that V is topologically nilpotent is a reduced Cartier module. The converse is also true by [Z1] Korollar 5.43.

We note that Berthelot [B] associates to any p-divisible group over a perfect ring a Dieudonné module. In the case of a formal p-divisible group his construction gives the Cartier module (compare [Z2] Satz 4.15).

***Example* 16:** The multiplicative display $\mathcal{G}_m = (P, Q, F, V^{-1})$ over a ring R is defined as follows. We set $P = W(R),\ Q = I_R$ and define the maps $F : P \to P,\quad V^{-1} : Q \to P$ by:

$$\begin{aligned} Fw &= {}^F w \qquad \text{for } w \in W(R) \\ V^{-1}({}^V w) &= w \end{aligned}$$

We note that in this case the map $V^\sharp$ is given by:

$$V^\sharp : W(R) \longrightarrow W(R) \otimes_{F,W(R)} W(R) \overset{\kappa}{\cong} W(R)$$

$$V^\sharp w = 1 \otimes {}^V w = pw \otimes 1$$

Hence using the canonical isomorphism κ the map $V^\sharp$ is simply multiplication by p. Therefore we have a display, if p is nilpotent in R, or more generally in the situation of definition 13.

***Example* 17:** To any 3n-display we can associate a dual 3n-display. Assume we are given two 3n-displays $\mathcal{P}_1$ and $\mathcal{P}_2$ over R.

Definition 18. — *A bilinear form of 3n-displays*

$$(\ ,\ ) : \mathcal{P}_1 \times \mathcal{P}_2 \to \mathcal{G}_m$$

is a bilinear form of $W(R)-$modules

$$(\ ,\ ) : P_1 \times P_2 \to W(R),$$

which satisfies the following relation:

$$ {}^V(V^{-1}y_1, V^{-1}y_2) = (y_1, y_2), \quad \textit{for} \quad y_1 \in Q_1,\ y_2 \in Q_2 \tag{19}$$

We will denote the abelian group of bilinear forms by $\mathrm{Bil}(\mathcal{P}_1 \times \mathcal{P}_2, \mathcal{G}_m)$.

The last relation implies the following:

$$\begin{array}{rcll} (V^{-1}y_1, Fx_2) & = & {}^F(y_1, x_2) & \text{for} \quad y_1 \in Q_1, \quad x_2 \in P_2 \\ (Fx_1, Fx_2) & = & p\,{}^F(x_1, x_2) & \text{for} \quad x_1 \in P_1, \\ (Fx_1, V^{-1}y_2) & = & {}^F(x_1, y_2) & \text{for} \quad y_2 \in Q_2, \end{array} \tag{20}$$

Indeed,

$$\begin{array}{rcl} {}^V(V^{-1}y_1, Fx_2) & = & {}^V(V^{-1}y_1, V^{-1}({}^V 1 x_2)) \\ = \ (y_1, {}^V 1 x_2) & = & {}^V 1 (y_1, x_2) \qquad = \ {}^{VF}(y_1, x_2) \end{array}$$

implies the first relation of (20) because ^{V} is injective. The other relations are verified in the same way. We note that $(Q_1, Q_2) \subset I_R$ by (19). Assume we are given a finitely generated projective $W(R)$-module P. Then we define the dual module:

$$P^* = \mathrm{Hom}_{W(R)}(P, W(R))$$

Let us denote the resulting perfect pairing by $(\ ,\ )$:

$$\begin{array}{rcl} P \times P^* & \to & W(R) \\ x \times z & \mapsto & (x, z) \end{array} \tag{21}$$

There is also an induced pairing

$$(\ , \ ) : W(R) \otimes_{F,W(R)} P \times W(R) \otimes_{F,W(R)} P^* \to W(R),$$

which is given by the formula:

$$(w \otimes x, v \otimes z) = wv \ {}^F(x,z), \quad x \in P, \ z \in P^*, \ w, v \in W(R)$$

Let us consider a 3n-display $\mathcal{P} = (P, Q, F, V^{-1})$ over R. We set $\hat{Q} = \{\phi \in P^* \mid \phi(Q) \subset I_R\}$. Then $\hat{Q}/I_R P^*$ is the orthogonal complement of $Q/I_R P$ by the induced perfect pairing:

$$P/I_R P \times P^*/I_R P^* \to R$$

Definition 19. — *There is a unique 3n-display $\mathcal{P}^t = (P^*, \hat{Q}, F, V^{-1})$, such that the operators F and V^{-1} satisfy the following relations with respect to the pairing (21):*

$$\begin{array}{lcll} (V^{-1}x, Fz) & = & {}^F(x,z) & \text{for} \quad x \in Q, \quad z \in P^* \\ (Fx, Fz) & = & p \ {}^F(x,z) & \text{for} \quad x \in P, \quad z \in P^* \\ (Fx, V^{-1}z) & = & {}^F(x,z) & \text{for} \quad x \in P, \quad z \in \hat{Q} \\ {}^V(V^{-1}x, V^{-1}z) & = & (x,z) & \text{for} \quad x \in Q, \quad z \in \hat{Q} \end{array} \tag{22}$$

Hence we have a bilinear form of displays

$$\mathcal{P} \times \mathcal{P}^t \to \mathcal{G}_m$$

We call $\mathcal{P}^t$ the dual 3n-display.

As for ordinary bilinear forms one has a canonical isomorphism:

$$\mathrm{Bil}(\mathcal{P}_1 \times \mathcal{P}_2, \mathcal{G}_m) \to \mathrm{Hom}(\mathcal{P}_2, \mathcal{P}_1^t) \tag{23}$$

From the relations of definition 19 we easily deduce that the $W(R)$-linear maps $F^\sharp$ and $V^\sharp$ for $\mathcal{P}$ respectively $\mathcal{P}^t$ are dual to each other:

$$\begin{array}{lcl} (V^\sharp x, v \otimes z) & = & (x, F^\sharp(v \otimes z)) \\ (F^\sharp(w \otimes x), z) & = & (w \otimes x, V^\sharp z) \end{array} \tag{24}$$

Let us assume that p is nilpotent in R. In terms of the dual 3n-display we may rephrase the nilpotence condition as follows. Iterating the homomorphism $F^\sharp$ for the dual 3n- display we obtain a map:

$$F^{N\,\sharp} : W(R) \otimes_{F^N, W(R)} P^* \to P^* \tag{25}$$

Then the 3n-display $\mathcal{P}$ satisfies the V-nilpotence condition, iff for any number n there exists a number N, such that the following map induced by (25) is zero:

$$F^{N\,\sharp} : W_n(R) \otimes_{F^N, W(R)} P^* \to W_n(R) \otimes_{W(R)} P^*$$

In this case we will also say that $\mathcal{P}^t$ satisfies the F-nilpotence condition.

Next we define base change for a 3n-display. Suppose we are given a ring homomorphism $\varphi : S \longrightarrow R$. Let P be a $W(S)-$module. If $\varphi : P \longrightarrow P'$ is a ${}^F-$linear map of $W(S)-$modules, we define the base change $\varphi_{W(R)}$ as follows:

$$\begin{array}{llll} \varphi_{W(R)}: & W(R) \otimes_{W(S)} P & \longrightarrow & W(R) \otimes_{W(S)} P' \\ & w \otimes x & \longmapsto & {}^F w \otimes \varphi(x) \end{array}$$

Then we have $(\varphi_{W(S)})^\sharp = \mathrm{id}_{W(R)} \otimes_{W(S)} \varphi^\sharp$ for the linearizations.

Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a 3n-display over S. Let $\varphi : S \to R$ be any ring morphism. We will now define the 3n-display obtained by base change with respect to φ.

Definition 20. — *We define $\mathcal{P}_R = (P_R, Q_R, F_R, V_R^{-1})$ to be the following quadruple:*

We set $P_R = W(R) \otimes_{W(S)} P$.

We define Q_R to be the kernel of the morphism $W(R) \otimes_{W(S)} P \longrightarrow R \otimes_S P/Q$.

We set $F_R = {}^F \otimes F$.

Finally we let $V_R^{-1} : Q_R \longrightarrow P_R$ be the unique $W(R)$-linear homomorphism, which satisfies the following relations:

$$\begin{aligned} V_R^{-1}(w \otimes y) &= {}^F w \otimes V^{-1} y, \textit{ for } w \in W(R), y \in Q \\ V_R^{-1}({}^V w \otimes x) &= w \otimes Fx, \textit{ for } x \in P \end{aligned} \tag{26}$$

Then $\mathcal{P}_R$ is a 3n-display over R, which is called the 3n-display obtained by base change.

To show that this definition makes sense we have only to prove the existence and uniqueness of V_R^{-1},. The uniqueness is clear. For the existence we choose a normal decomposition $P = L \oplus T$. Then we have an isomorphism:

$$Q_R \simeq W(R) \otimes_{W(S)} L \oplus I_R \otimes_{W(S)} T$$

We define V_R^{-1} on the first summand by the first equation of (26) and on the second direct summand by the second equation. We leave the verification that (26) holds with this definition to the reader.

In the case where φ is surjective the image of the morphism $W(R) \otimes_{W(S)} Q \to W(R) \otimes_{W(S)} P = P_R$, is simply Q_R, but in general this image is strictly smaller than Q_R.

By looking for example at (15) it is clear that $\mathcal{P}_R$ is a display if $\mathcal{P}$ was a display. There is also an obvious converse statement.

Lemma 21. — *Let $\phi : S \to R$ be a ring homomorphism, such that any element in the kernel of ϕ is nilpotent. Then $\mathcal{P}$ is a display if $\mathcal{P}_R$ is a display.*

***Remark*:** Before we turn to the next example, we collect some general facts about the liftings of projective modules. Let $S \to R$ be a surjective ring homomorphism, such that any element in the kernel is nilpotent, or such that S is complete and separated in the adic topology defined by this kernel. Assume we are given a finitely generated projective module P over R. Then P lifts to S, i.e. there is a finitely generated projective S-module $\tilde{P}$ together with an isomorphism $\phi : R \otimes_S \tilde{P} \to P$. By the lemma of Nakayama the pair $(\tilde{P}, \phi)$ is uniquely determined up to isomorphism. The existence follows from the well-known fact that idempotent elements lift with respect the surjection of matrix algebras $\mathrm{End}_S(S^u) \to \mathrm{End}_R(R^u)$, where u is some number (e.g. H.Bass, Algebraic K-Theory, W.A. Benjamin 1968, Chapt. III Prop. 2.10).

Let L be a direct summand of P. A lifting of L to a direct summand of P is obtained as follows. Let $\tilde{L}$ be any lifting of L to S. Let $\tilde{L} \to \tilde{P}$ be any lifting of $L \to P$, whose existence is guaranteed by the universal property of projective modules. In this way $\tilde{L}$ becomes a direct summand of $\tilde{P}$. This is easily seen, if one lifts in the same way a complement T of L in P. Indeed the natural map $\tilde{L} \oplus \tilde{T} \to \tilde{P}$ is by Nakayama an isomorphism.

Let us now assume that the kernel of $S \to R$ consists of nilpotent elements. We also assume that p is nilpotent in S. Let now P denote a projective $W(R)$-module. We set $P_R = R \otimes_{\mathbf{w_0}, W(R)} P$. We have seen that P_R may be lifted to a finitely generated projective S-module $\tilde{P}_S$. Since $W(S)$ is complete and separated in the I_S-adic topology by proposition 3, we can lift $\tilde{P}_S$ to a projective finitely generated $W(S)$-module $\tilde{P}$. We find an isomorphism $W(R) \otimes_{W(S)} \tilde{P} \to P$, because liftings of P_R to $W(R)$ are uniquely determined up to isomorphism. Hence finitely generated projective modules lift with respect to $W(S) \to W(R)$. Since the kernel of the last morphism lies in the radical of $W(S)$, this lifting is again unique up to isomorphism. We also may lift direct summands as described above.

Let $(\tilde{P}, \tilde{Q}, F, V^{-1})$ be a 3n-display over S and (P, Q, F, V^{-1}) be the 3n-display obtained by base change over R. Then any normal decomposition $P = L \oplus T$ may be lifted to a normal decomposition $\tilde{P} = \tilde{L} \oplus \tilde{T}$. Indeed choose any finitely generated projective $W(S)$-modules $\tilde{L}$ and $\tilde{T}$, which lift L and T. Because $\tilde{Q} \to Q$ is surjective, we may lift the inclusion $L \to Q$ to a $W(S)$-module homomorphism $\tilde{L} \to \tilde{Q}$. Moreover we find a $W(S)$-module homomorphism $\tilde{T} \to \tilde{P}$, which lifts $T \to P$. Clearly this gives the desired normal decomposition $\tilde{P} = \tilde{L} \oplus \tilde{T}$.

***Example* 22:** Let $S \to R$ be a surjection of rings with kernel $\mathfrak{a}$. We assume that p is nilpotent in S, and that each element $a \in \mathfrak{a}$ is nilpotent.

Let $\mathcal{P}_0 = (P_0, Q_0, F, V^{-1})$ be a 3n-display over R. A deformation (or synonymously a lifting) of $\mathcal{P}_0$ to S is a 3n-display $\mathcal{P} = (P, Q, F, V^{-1})$ over S together with an isomorphism:

$$\mathcal{P}_R \cong \mathcal{P}_0.$$

Let us fix a deformation $\mathcal{P}$. To any homomorphism

$$\alpha \in \mathrm{Hom}_{W(S)}(P, W(\mathfrak{a}) \otimes_{W(S)} P),$$

we associate another deformation $\mathcal{P}_\alpha = (P_\alpha, Q_\alpha, F_\alpha, V_\alpha^{-1})$ as follows:

We set $P_\alpha = P$, $Q_\alpha = Q$, and

$$\begin{array}{rcll} F_\alpha x & = & Fx - \alpha(Fx), & \text{for} \quad x \in P \\ V_\alpha^{-1} y & = & V^{-1}y - \alpha(V^{-1}y), & \text{for} \quad y \in Q. \end{array} \tag{27}$$

The surjectivity of $(V_\alpha^{-1})^\sharp$ follows the kernel of $W(S) \to W(R)$ is in the radical of $W(S)$ and therefore Nakyama's lemma is applicable.

Since F and F_α respectively V^{-1} and V_α^{-1} are congruent modulo $W(\mathfrak{a})$ the 3n-display $\mathcal{P}_{\alpha,R}$ obtained by base change is canonically isomorphic to $\mathcal{P}_0$.

We note that any deformation is isomorphic to $\mathcal{P}_\alpha$ for a suitable homomorphism α. Indeed, let $\mathcal{P}_1 = (P_1, Q_1, F_1, V_1^{-1})$ be any other deformation of $\mathcal{P}_0$. We find an isomorphism of the pairs (P, Q) and (P_1, Q_1), which reduces to the identity on (P_0, Q_0). Indeed, we fix a normal decomposition $P_0 = L_0 \oplus T_0$ and lift it to a normal decomposition of $\mathcal{P}$ respectively of $\mathcal{P}_1$. Then any isomorphism between the lifted normal decompositions is suitable. Hence we may assume that $(P, Q) = (P_1, Q_1)$. Then we define ^{F}-linear homomorphisms

$$\xi : P \to W(\mathfrak{a}) \otimes_{W(S)} P, \quad \eta : Q \to W(\mathfrak{a}) \otimes_{W(S)} P,$$

by the equations:

$$\begin{array}{rcll} F_1 x & = & Fx - \xi(x) & \text{for} \quad x \in P \\ V_1^{-1} y & = & V^{-1}y - \eta(y) & \text{for} \quad y \in Q. \end{array} \tag{28}$$

Then ξ and η must satisfy the relation:

$$\eta({}^V wx) = w\xi(x), \quad \text{for} \quad x \in P.$$

It is then easily checked that there is a unique homomorphism α as above, which satisfies the relations:

$$\begin{array}{rcll} \alpha(V^{-1}y) & = & \eta(y), & \text{for} \quad y \in Q \\ \alpha(Fx) & = & \xi(x), & \text{for} \quad x \in P \end{array}$$

Then the deformations $\mathcal{P}_\alpha$ and $\mathcal{P}_1$ are isomorphic.

***Example* 23:** Let R be a ring such that $p \cdot R = 0$. Let us denote by $\mathrm{Frob} : R \to R$ the absolute Frobenius endomorphism, i.e. $\mathrm{Frob}(r) = r^p$ for $r \in R$.

Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a 3n-display over R. We denote the 3n-display obtained by base change with respect to Frob by $\mathcal{P}^{(p)} = (P^{(p)}, Q^{(p)}, F, V^{-1})$. More explicitly we have

$$\begin{array}{rcl} P^{(p)} & = & W(R) \otimes_{F,W(R)} P \\ Q^{(p)} & = & I_R \otimes_{F,W(R)} P + \quad \text{Image} \quad (W(R) \otimes_{F,W(R)} Q) \end{array}$$

The operators F and V^{-1} are uniquely determined by the relations:

$$\begin{array}{rcll} F(w \otimes x) & = & {}^F w \otimes Fx, & \text{for} \quad w \in W(R), x \in P \\ V^{-1}({}^V w \otimes x) & = & w \otimes Fx, & \\ V^{-1}(w \otimes y) & = & {}^F w \otimes V^{-1}y, & \text{for} \quad y \in Q. \end{array}$$

(At the first glance it might appear that this explicit definition does not use $p \cdot R = 0$. But without this condition $Q^{(p)}/I_R P^{(p)}$ would not be a direct summand of $P^{(p)}/I_R P^{(p)}$. The elements $1 \otimes {}^V wx = pw \otimes x$ would cause trouble, if ^{F} and ^{V} do not commute.)

The map $V^\# : P \to W(R) \otimes_{F,W(R)} P$ of lemma 1.5 satisfies $V^\#(P) \subset Q^{(p)}$. Using the fact that P is generated as a $W(R)$-module by the elements $V^{-1}y$ for $y \in Q$ a routine calculation shows that $V^{\#}$ commutes with F and V^{-1}. Hence $V^{\#}$ induces a homomorphism of 3n-displays

$$Fr_{\mathcal{P}} : \mathcal{P} \longrightarrow \mathcal{P}^{(p)}, \tag{29}$$

which is called the Frobenius homomorphism of $\mathcal{P}$.

Similiary the map $F^{\#} : W(R) \otimes_{F,W(R)} P \to P$ satisfies $F^{\#}(Q^{(p)}) \subset I_R P$. One can check that $F^{\#}$ commutes with the operators F and V^{-1}. Therefore $F^{\#}$ induces a map of 3n-displays, which is called the Verschiebung.

$$\mathrm{Ver}_{\mathcal{P}} : \mathcal{P}^{(p)} \longrightarrow \mathcal{P}. \tag{30}$$

From the lemma 1.5 we obtain the relations:

$$Fr_{\mathcal{P}} \cdot \mathrm{Ver}_{\mathcal{P}} = p \cdot \mathrm{id}_{\mathcal{P}^{(p)}}, \qquad \mathrm{Ver}_{\mathcal{P}}\, Fr_{\mathcal{P}} = p \cdot \mathrm{id}_{\mathcal{P}}\,. \tag{31}$$

***Example* 24:** We will define displays, which correspond to the Lubin-Tate groups. Let O_K be a complete discrete valuation ring with finite residue class field k, and field of fractions K of characteristic 0. We fix a prime element $\pi \in O_K$. Let R be a $p-$adic ring, which is equipped with a structure $\phi : O_K \to R$ of a O_K-algebra. We set $u = \phi(\pi)$.

The displays we are going to construct are displays $\mathcal{P}$ over the topological ring R with its $p-$adic topology. Moreover they will be equipped with an action $\iota : O_K \to \operatorname{End} \mathcal{P}$ of O_K. This implies an action of the ring $O_K \otimes_{\mathbb{Z}_p} W(R)$ on P. Let us extend the operators ^{F} and ^{V} on the ring $W(R)$ O_K-linearily to the ring $O_K \otimes W(R)$. We need the following easy lemma:

Lemma 25. — *Consider the ring homomorphism:*

$$O_K \otimes_{\mathbb{Z}_p} W(R) \longrightarrow O_K/\pi O_K \otimes R/uR. \tag{32}$$

It is the residue class map on the first factor, and it is the composite of $\mathbf{w}_0$ *with the natural projection* $R \to R/uR$ *on the second factor.*

Then an element in $O_K \otimes W(R)$ *is a unit, iff its image by (32) is a unit.*

Proof. — By proposition 3 the ring $O_K \otimes_{\mathbb{Z}_p} W(R)$ is complete in the I_R -adic topology. Hence an element in this ring is a unit, iff its image in $O_K \otimes_{\mathbb{Z}_p} R$ is a unit. Since this last ring is complete in the p-adic topology, we get easily our result. □

Let us first do the construction of the Lubin-Tate display in a special case:

Proposition 26. — *Let us assume that* $O_K/\pi O_K = \mathbb{F}_p$. *Let* R *be a p-torsion free p-adic ring, with an* O_K*-algebra structure* $\phi : O_K \to R$. *Then there is a unique display* $\mathcal{P}_R = (P_R, Q_R, F, V^{-1})$ *over the topological ring* R*, with the following properties:*

(i) $P_R = O_K \otimes_{\mathbb{Z}_p} W(R)$.
(ii) Q_R *is the kernel of the map* $\phi \otimes \mathbf{w}_0 : O_K \otimes_{\mathbb{Z}_p} W(R) \to R$.
(iii) *The operators* F *and* V^{-1} *are* O_K*-linear.*
(iv) $V^{-1}(\pi \otimes 1 - 1 \otimes [u]) = 1$.

To prove this proposition we need two lemmas:

Lemma 27. — *With the assumptions of proposition 26 we set $e = [O_K : \mathbb{Z}_p]$. Then the element:*

$$\tau = \frac{1}{p}(\pi^e \otimes 1 - 1 \otimes [u^{ep}]) \in K \otimes_{\mathbb{Z}_p} W(R)$$

is a unit in $O_K \otimes_{\mathbb{Z}_p} W(R)$.

Proof. — The statement makes sense because $O_K \otimes_{\mathbb{Z}_p} W(R)$ has no p-torsion. First we prove that the element $\pi^e \otimes 1 - 1 \otimes [u^{ep}]$ is divisible by p. We have $\pi^e = \varepsilon p$ for some unit $\varepsilon \in O_K^*$. Therefore it is enough to show that p divides $1 \otimes [u^{ep}]$. Since $u^{ep} = \phi(\varepsilon)^p p^p$, it is enough to show that p divides $[p^p]$ in $W(R)$. This will follow from the lemma below.

To show that τ is a unit we consider its image by the map $\phi \otimes \mathbf{w}_0 : O_K \otimes_{\mathbb{Z}_p} W(R) \to R$. It is equal to $\frac{1}{p}(u^e - u^{ep})$, which is a unit in R. It follows immediatly from lemma 25 that τ must be a unit too. □

Lemma 28. — *The element $[p^p] \in W(\mathbb{Z}_p)$ is divisible by p.*

Proof. — Let $g_m \in \mathbb{Z}_p$ for $m \geq 0$ be p-adic integers. By a well–known lemma [BAC] IX.3 Proposition 2 there exists a Witt vector $x \in W(\mathbb{Z}_p)$ with $\mathbf{w}_m(x) = g_m$, for all $m \geq 0$, if and only if the following congruences are satisfied:

$$g_{m+1} \equiv g_m \bmod p^{m+1}$$

Hence our assertion follows if we verify the congruences:

$$\frac{(p^p)^{p^{m+1}}}{p} \equiv \frac{(p^p)^{p^m}}{p} \bmod p^{m+1} \quad m = 0, 1, \cdots$$

But both sides of these congruences are zero. □

Proof. — (of proposition 26): Let $L_R \subset P_R$ be the free $W(R)$-submodule of P_R with the following basis

$$\pi^i \otimes 1 - 1 \otimes [u^i], \quad i = 1, \cdots, e-1.$$

Let us denote by $T_R \subset P_R$ the $W(R)$-submodule $W(R)(1 \otimes 1)$. Then $P_R = T_R \oplus L_R$ is a normal decomposition.

To define a display we need to define ^{F}–linear maps

$$\begin{aligned} V^{-1} : L_R &\longrightarrow P_R \\ F : T_R &\longrightarrow P_R, \end{aligned}$$

such that the map $V^{-1} \oplus F$ is an ^{F}-linear epimorphism.

Since we want V^{-1} to be O_K-linear we find by condition (iv) that for $i = 1, \ldots, e-1$:

$$V^{-1}(\pi^i \otimes 1 - 1 \otimes [u^i]) = \frac{\pi^i \otimes 1 - 1 \otimes [u^{ip}]}{\pi \otimes 1 - 1 \otimes [u^p]} = \sum_{k+l=i-1} \pi^k \otimes [u^{lp}]. \tag{33}$$

Here k and l run through nonnegative integers and the fraction in the middle is by definition the last sum. The equation makes sense because by lemma 27 the element $\pi \otimes 1 - 1 \otimes [u^p]$ is not a zero divisor in $O_K \otimes W(R)$.

If we multiply the equation (iv) by p we find

$$F(\pi \otimes 1 - 1 \otimes [u]) = p,$$

and by the required O_K-linearity of F:

$$(\pi \otimes 1 - 1 \otimes [u^p]) \cdot F1 = p.$$

Therefore we are forced to set:

$$F1 = \tau^{-1} \frac{\pi^e \otimes 1 - 1 \otimes [u^{ep}]}{\pi \otimes 1 - 1 \otimes [u^p]} \tag{34}$$

The ^{F}–linear operators $V^{-1} : L_R \to P_R$ and $F : T_R \to P_R$ defined by the equations (33) and (34) may be extended to ^{F}–linear operators

$$V^{-1} : Q_R \to P_R, \quad F : P_R \to P_R$$

using the equations (1) and (2). Then V^{-1} is the restriction of the operator $V^{-1} : P_R[\frac{1}{p}] \to P_R[\frac{1}{p}]$ defined by $V^{-1}x = \frac{{}^F x}{\pi \otimes 1 - 1 \otimes [u^p]}$ and F is the restriction of $pV^{-1} : P_R[\frac{1}{p}] \to P_R[\frac{1}{p}]$. This shows that the operators F and V^{-1} are O_K–linear. Since 1 is in the image of $(V^{-1})^{\#} : W(R) \otimes_{W(R)} Q_R \to P_R$, and since this map is $O_K \otimes W(R)$–linear, we conclude that $(V^{-1})^{\#}$ is an epimorphism. It follows that (P_R, Q_R, F, V^{-1}) is a 3n-display, which satisfies the conditions of the proposition. The uniqueness is clear by what we have said.

It remains to be shown that we obtained a display in the topological sense. By base change it is enough to do this for $R = O_K$. Let us denote by $\bar{\mathcal{P}} = (\bar{P}, \bar{Q}, F, V^{-1})$ the 3n-display over $\mathbb{F}_p$ obtained by base change $O_K \to \mathbb{F}_p$. Then $\bar{P} = O_K$ and F is the O_K–linear map defined by $F\pi = p$. Hence the map V is multiplication by π. Hence $\bar{\mathcal{P}}$ is a display. □

Finally we generalize our construction to the case where the residue class field k of O_K is bigger than $\mathbb{F}_p$. In this case we define for any torsionfree O_K-algebra $\phi : O_K \to R$ a display

$$\mathcal{P}_R = (P_R, Q_R, F, V^{-1}).$$

Again we set

$$P_R = O_K \otimes_{\mathbb{Z}_p} W(R),$$

and we define Q_R to be the kernel of the natural map

$$\phi \otimes \mathbf{w}_0 : O_K \otimes_{\mathbb{Z}_p} W(R) \to R. \tag{35}$$

We identify $W(k)$ with a subring of O_K. The restriction of ϕ to $W(k)$ will be denoted by the same letter:

$$\phi : W(k) \longrightarrow R.$$

Applying the functor W to this last map we find a map (compare (90))

$$\rho : W(k) \longrightarrow W(W(k)) \longrightarrow W(R), \tag{36}$$

which commutes with the Frobenius morphism defined on the first and the third ring of (36) (for a detailed discussion see [Gr] Chapt IV Proposition 4.3).

Let us denote the Frobenius endomorphism on $W(k)$ also by σ. We have the following decomposition in a direct product of rings

$$O_K \otimes_{\mathbb{Z}_p} W(R) = \prod_{i \in \mathbb{Z}/f\mathbb{Z}} O_K \otimes_{\sigma^i, W(k)} W(R). \tag{37}$$

Here f denotes the degree $f = [k : F_p]$ and the tensor product is taken with respect to ρ.

The operators ^{F} and ^{V} on $W(R)$ act via the second factor on the left hand side of (37). On the right–hand side they are operators of degree -1 and $+1$ respectively:

$$\begin{aligned} {}^F : O_K \otimes_{\sigma^i, W(k)} W(R) &\longrightarrow \quad O_K \otimes_{\sigma^{i-1}, W(k)} W(R) \\ {}^V : O_K \otimes_{\sigma^i, W(k)} W(R) &\longrightarrow \quad O_K \otimes_{\sigma^{i+1}, W(k)} W(R). \end{aligned}$$

We obtain from (37) a decomposition of the $O_K \otimes_{\mathbb{Z}_p} W(R)$-module P_R :

$$P_R = \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} P_i, \quad P_i = O_K \otimes_{\sigma^i, W(k)} W(R)$$

Therefore we obtain also a decomposition

$$Q_R = Q_0 \oplus P_1 \oplus \cdots \oplus P_{f-1}.$$

The map (35) factors through

$$O_K \otimes_{W(k)} W(R) \longrightarrow R, \tag{38}$$

and Q_0 is the kernel of (38). The following elements form a basis of P_0 as $W(R)$-module

$$\begin{aligned} \omega_i = &\quad \pi^i \otimes 1 - 1 \otimes [u^i], \qquad i = 1, \cdots, e-1 \\ e_0 = &\quad 1 \otimes 1. \end{aligned}$$

Here u denotes as before the image of π by the map $O_K \to R$, and e is the ramification index $e = [O_K : W(k)]$. Let $T = W(R)e_0 \subset P_0$, and let $L_0 \subset Q_0$ the free $W(R)$ submodule generated by $\omega_1, \cdots \omega_{e-1}$. We have a normal decomposition

$$P_R = T \oplus L,$$

where $L = L_0 \oplus P_1 \oplus \cdots \oplus P_{f-1}$.

Now we may define the O_K-linear operators F and V^{-1}. We set $e_i = 1 \otimes 1 \in P_i$. Then V^{-1} is uniquely defined by the following properties:

$$\begin{array}{lll} V^{-1}\omega_1 & = e_{f-1}, & \\ V^{-1}e_i & = e_{i-1} & \text{for} \quad i \neq 0 \quad i \in \mathbb{Z}/f\mathbb{Z}, \\ V^{-1} \text{ is} & O_K\text{-linear.} & \end{array} \tag{39}$$

Multiplying the first of these equations by p we obtain the following equation in the ring $O_K \otimes_{\sigma^{f-1}, W(k)} W(R)$:

$${}^F\omega_1 F e_0 = p e_{f-1}$$

To see that this equation has a unique solution Fe_0 it suffices to show that:

$$\frac{1}{p}(\pi^e \otimes 1 - 1 \otimes [u^{ep}]) \in O_K \otimes_{\sigma^{f-1}, W(k)} W(R)$$

is a unit. This is seen exactly as before, using that $\frac{1}{p}(1 \otimes [u^{pe}])$ is mapped to zero by the map $W(R) \to R/u$.

Hence we have defined the desired ^{F}-linear operators $F : P_R \to P_R$ and $V^{-1} : Q_R \to P_R$. Again V^{-1} extends to a ^{F}-linear endomorphism of $K \otimes_{\mathbb{Z}_p} W(R)$, which is given by the formula:

$$V^{-1}x = {}^F(\frac{x}{\theta}),$$

where $\theta \in O_K \otimes_{\mathbb{Z}_p} W(R)$ is the element, which has with respect to the decomposition (37) the component ω_1 for $i = 0$ and the component e_i for $i \neq 0$.

As before this proves the following proposition:

Proposition 29. — *Let K be a finite extension of $\mathbb{Q}_p$ with ramification index e and index of inertia f. Let O_K, π, k have the same meaning as before.*

Let R be torsion free O_K-algebra, such that R is p-adically complete and separated. Denote by u the image of π by the structure morphism $\phi : O_K \to R$. Let $\rho : W(k) \to W(R)$ be the homomorphism induced by the structure morphism. Then we have a decomposition

$$O_K \otimes_{\mathbb{Z}_p} W(R) \xrightarrow{\sim} \prod_{i \in \mathbb{Z}/f\mathbb{Z}} O_K \otimes_{\sigma^i, W(k)} W(R)$$

Let $\theta \in O_K \otimes_{\mathbb{Z}_p} W(R)$ be the element, which has the component 1 for $i \neq 0$ and the component $\pi \otimes 1 - 1 \otimes [u]$ for $i = 0$.

Then there is a uniquely defined display $\mathcal{P}_R = (P_R, Q_R, F, V^{-1})$ over the topological ring R, which satisfies the following conditions:

(i) $P_R = O_K \otimes_{\mathbb{Z}_p} W(R)$.

(ii) *Q_R is the kernel of the map $\phi \otimes \mathbf{w}_0 : O_K \otimes_{\mathbb{Z}_p} W(R) \to R$.*

(iii) *The operators F and V^{-1} are O_K-linear.*

(iv) $V^{-1}\theta = 1$.

1.3. Descent.

— We will now study the faithfully flat descent for displays.

Lemma 30. — *Let M be a flat $W(S)-$module, and let $S \to R$ be a faithfully flat ring extension. Then there is an exact sequence*

$$0 \to M \to W(R) \otimes_{W(S)} M \rightrightarrows W(R \otimes R) \otimes_{W(S)} M \overset{\rightarrow}{\underset{\rightarrow}{\rightarrow}} W(R \otimes R \otimes R) \otimes_{W(S)} M \quad \cdots \tag{40}$$

Here the $\otimes$ without index means $\otimes_S$.

Proof. — The arrows are induced by applying the functor W to the usual exact sequence for descent:

$$0 \to S \to R \rightrightarrows R \otimes_S R \overset{\rightarrow}{\underset{\rightarrow}{\rightarrow}} \cdots$$

Since M is a direct limit of free modules, we are reduced to the case $M = W(S)$. In this case any term of the sequence (40) comes with the filtration by the ideals

$I_{R\otimes_S\cdots\otimes_S R,n} \subset W(R\otimes_S \cdots \otimes_S R)$. We obtain by the usual f.p.q.c. descent an exact sequence, if we go to the graded objects. □

Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over S. Then the modules P_R and Q_R obtained by base change fit into an exact sequence

$$0 \to Q_R \to P_R \to R \otimes_S P/Q \to 0$$

Proposition 31. — *Let $S \to R$ be a faithfully flat ring morphism. Consider a display (P, Q, F, V^{-1}) over S. Then we have a commutative diagram with exact rows*

$$\begin{array}{cccccc}
0 \to & P \to & P_R \rightrightarrows & P_{R\otimes_S R} \overset{\to}{\underset{\to}{\to}} & P_{R\otimes_S R\otimes_S R} \overset{\to}{\underset{\to}{\overset{\to}{\to}}} \cdots \\
 & \cup & \cup & \cup & \cup \\
0 \to & Q \to & Q_R \rightrightarrows & Q_{R\otimes_S R} \overset{\to}{\underset{\to}{\to}} & Q_{R\otimes_S R\otimes_S R} \overset{\to}{\underset{\to}{\overset{\to}{\to}}} \cdots
\end{array}$$

Proof. — Indeed, the first row is exact by the lemma. The second row is the kernel of the canonical epimorphism from the first row to:

$$0 \to P/Q \to R \otimes_S P/Q \rightrightarrows R \otimes_S R \otimes_S P/Q \overset{\to}{\underset{\to}{\to}} R \otimes_S R \otimes_S R \otimes P/Q \overset{\to}{\underset{\to}{\overset{\to}{\to}}} \cdots$$

This proves the proposition and more:

Theorem 32. — *(descent for displays): Let $S \to R$ be a faithfully flat ring extension. Let $\mathcal{P} = (P, Q, F, V^{-1})$ and $\mathcal{P}' = (P', Q', F, V^{-1})$ be two displays over S. Then we have an exact sequence*

$$0 \to \operatorname{Hom}(\mathcal{P}, \mathcal{P}') \to \operatorname{Hom}(\mathcal{P}_R, \mathcal{P}'_R) \rightrightarrows \operatorname{Hom}(\mathcal{P}_{R\otimes_S R}, \mathcal{P}'_{R\otimes_S R}).$$

□

Let N be a $W(R)-$module. Then we may define a variant of the usual descent datum relative to $S \to R$.

Let us give names to the morphisms in the exact sequence (40):

$$W(S) \to W(R) \underset{p_2}{\overset{p_1}{\rightrightarrows}} W(R \otimes_S R) \begin{array}{c}\xrightarrow{p_{12}}\\ \xrightarrow{p_{23}}\\ \xrightarrow{p_{13}}\end{array} W(R \otimes_S R \otimes_S R). \tag{41}$$

Here the index of p_{ij} indicates, that the first factor of $R \otimes_S R$ is mapped to the factor i, and the second is mapped to the factor j. The notation p_i is similar. In the context of descent we will often write $\otimes$ instead of $\otimes_S$ We also use the notation

$$p_i^* N = W(R \otimes R) \otimes_{p_i, W(R)} N.$$

We define a $W-$descent datum on N to be a $W(R \otimes R)-$ isomorphism

$$\alpha\colon p_1^*N \longrightarrow p_2^*N,$$

such that the following diagram is commutative (cocycle condition):

$$\begin{array}{ccc} p_{12}^*p_1^*N & \xrightarrow{p_{12}^*\alpha} & p_{12}^*p_2^*N \\ \| & & \| \\ p_{13}^*p_1^*N & & p_{23}^*p_1^*N \\ \downarrow{\scriptstyle p_{13}^*\alpha} & & \downarrow{\scriptstyle p_{23}^*\alpha} \\ p_{13}^*p_2^*N & = & p_{23}^*p_2^*N \end{array} \tag{42}$$

To any descent datum we may associate a sequence of morphisms

$$W(R) \otimes_{W(R)} N \underset{\partial^1}{\overset{\partial^0}{\rightrightarrows}} W(R \otimes R) \otimes_{W(R)} N \overset{\partial^0}{\underset{\partial^2}{\overset{\longrightarrow}{\underset{\longrightarrow}{\overset{\partial^1}{\longrightarrow}}}}} W(R \otimes R \otimes R) \otimes_{W(R)} N \cdots,$$

where the tensor product is always taken with respect to the map $W(R) \to W(R \otimes \cdots \otimes R)$ induced by $a \in R \longmapsto 1 \otimes \cdots \otimes 1 \otimes a \in R \otimes \cdots \otimes R$. The maps $\partial^i\colon W(R^{\otimes n}) \otimes_{W(R)} N \longrightarrow W(R^{\otimes(n+1)}) \otimes_{W(R)} N$, for $i < n$ are simply the tensorproduct with N of the map $W(R^{\otimes n}) \longrightarrow W(R^{\otimes(n+1)})$ induced by

$$a_1 \otimes \cdots \otimes a_n \longmapsto a_1 \otimes \cdots \otimes a_i \otimes 1 \otimes a_{i+1} \otimes \cdots a_n.$$

Finally the map $\partial^n\colon W(R^{\otimes n}) \otimes_{W(R)} N \longrightarrow W(R^{\otimes n+1}) \otimes_{W(R)} N$ is obtained as follows. The descent datum α induces a map $u(x) = \alpha(1 \otimes x)$:

$$u\colon N \longrightarrow W(R \otimes R) \otimes_{W(R)} N,$$

which satisfies $u(rx) = p_1(r)u(x)$. Consider the commutative diagram

$$\begin{array}{ccc} R & \longrightarrow & R \otimes R \\ \downarrow & & \downarrow \\ R^{\otimes n} & \longrightarrow & R^{\otimes n+1} \end{array}$$

The upper horizontal map is $r \mapsto r \otimes 1$ and the lower horizontal map is $r_1 \otimes \cdots \otimes r_n \mapsto r_1 \otimes \cdots \otimes r_n \otimes 1$. The left vertical map is $r \mapsto 1 \otimes \cdots \otimes 1 \otimes r$ and finally the right vertical map is $r_1 \otimes r_2 \mapsto 1 \otimes \cdots \otimes 1 \otimes r_1 \otimes r_2$.

If we apply the functor W we obtain:

$$\begin{array}{ccc} W(R) & \longrightarrow & W(R \otimes R) \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle q_2} \\ W(R^{\otimes n}) & \longrightarrow & W(R^{\otimes(n+1)}) \end{array}$$

Since u is equivariant with respect to the upper horizontal arrow, we may tensorize u by this diagram to obtain

$$W(R^{\otimes n}) \otimes_{q,W(R)} N \longrightarrow W(R^{\otimes n+1}) \otimes_{q_2,W(R\otimes R)} W(R \otimes R) \otimes_{W(R)} N.$$

This is the map we wanted to define.

We set

$$\delta_n = \sum_{i=0}^{n} (-1)^i \delta^i \colon W(R^{\otimes n}) \otimes N \to W(R^{\otimes (n+1)}) \otimes N.$$

The cocycle condition assures that we get a complex:

$$W(R) \otimes_{W(R)} N \xrightarrow{\delta_1} W(R \otimes R) \otimes_{W(R)} N \xrightarrow{\delta_2} W(R \otimes R \otimes R) \otimes_{W(R)} N \cdots \tag{43}$$

Proposition 33. — *Let $S \longrightarrow R$ be a faithfully flat ring homomorphism. Assume that p is nilpotent in S. Let P be a finitely generated projective $W(R)-$module with a $W-$descent datum α relative to $R \longrightarrow S$. Then the complex (43) for $N = P$ is exact. The kernel P_0 of δ_1 is a projective finitely generated $W(S)-$module and the natural map*

$$W(R) \otimes_{W(S)} P_0 \longrightarrow P$$

is an isomorphism.

We prove this a little later.

Corollary 34. — *The functor which associates to a finitely generated projective $W(S)-$module P_0 the $W(R)-$module $P = W(R) \otimes_{W(S)} P_0$ with its canonical descent datum is an equivalence of categories.*

Proposition 35. — *: The following conditions for a W(R)-module P are equivalent:*

(i) *P is finitely generated and projective.*

(ii) *P is separated in the topology defined by the filtration I_nP for $n \in \mathbb{N}$ (same notation as in the proof of proposition 3), and for each n the $W_n(R)-$module P/I_nP is projective and finitely generated.*

(iii) *P is separated as above, and there exist elements $f_1, \ldots, f_m \in R$, which generate the unit ideal, and such that for each $i = 1, \ldots, m$ $W(R_{f_i})-$module $W(R_{f_i}) \otimes_{W(R)} P$ is free and finitely generated.*

Proof. — For any number n and any $f \in R$ we have a natural isomorphism $W_n(R_f) \cong W_n(R)_{[f]}$. This fact shows, that (iii) implies (ii). Next we assume (ii) and show that (i) holds. We find elements $u_1, \ldots, u_h$, which generate P/IP as an $R-$module. They define a map $L = W(R)^h \to P$. Since L is complete in the topology defined by the ideals I_n this map is surjective and P is complete. By the lemma below we find for each number n a section σ_n of $L/I_nL \to P/I_nP$, such that σ_{n+1} reduces to σ_n. The projective limit of these sections is a section of the $W(R)$-module homomorphism $L \to P$. For the proof of the implication (i) implies (iii), we may assume that

$R \otimes_{W(R)} P$ is free. But then the same argument as above shows that any basis of $R \otimes_{W(R)} P$ lifts to a basis of P. □

Lemma 36. — *Let $S \to R$ be a surjective ring homomorphism. Let $\pi : P_1 \to P_2$ be a surjective $S-$module homomorphism. Suppose that P_2 is a projective $S-$module. Let $\bar{\pi} : \bar{P}_1 \to \bar{P}_2$ be the $R-$module homomorphism obtained by tensoring π by $R \otimes_S$. Then any section $\bar{\sigma} : \bar{P}_2 \to \bar{P}_1$ lifts to a section $\sigma : P_1 \to P_2$.*

Proof. — Let us denote by K the kernel of π, and set $\bar{K} = R \otimes_S K$. Let τ be any section of π. Consider the morphism $\bar{\sigma} - \bar{\tau} : \bar{P}_2 \to \bar{K}$. This lifts to a S-module homomorphism $\rho : P_2 \to K$, because P_2 is projective. We set $\sigma = \tau + \rho$. □

Proof. — (of proposition 33): We begin to prove the statement on the exactness of (43) under the additional assumption that $p \cdot S = 0$. On each term of the sequence (43) we consider the filtration by $I_{R^{\otimes n},m} \otimes_{W(R)} P$. Since P is projective the associated graded object is

$$I_{R,m}/I_{R,m+1} \otimes_{W(R)} P \to (I_{R\otimes R,m}/I_{R\otimes R,m+1}) \otimes_{W(R)} P \to \cdots$$

Applying the assumption $p \cdot R = 0$ we may rewrite this as

$$R \otimes_{p^m,R} P/I_R P \rightrightarrows R \otimes_S R \otimes_{p^m,R} P/I_R P \substack{\to \\ \to \\ \to} \cdots$$

The symbol p^m indicates, that the tensor product is taken with respect to the m-th power of the Frobenius endomorphism. The last sequence comes from a usual descent datum on $R \otimes_{p^m,R} P/I_R P$ and is therefore exact, except for the first place. Now we will get rid of the assumption $p \cdot S = 0$. We consider any ideal $\mathfrak{a} \subset S$ such that $p \cdot \mathfrak{a} = 0$. Let us denote by a bar the reduction modulo p (i.e. $\overline{R} = R/pR$ etc.), and by a dash the reduction modulo $\mathfrak{a}$.

We have an exact sequence

$$\begin{aligned} 0 \to \mathfrak{a} \otimes R \otimes R \cdots \otimes R &\longrightarrow R \otimes R \otimes \cdots \otimes R \to R' \otimes_{S'} R' \otimes \cdots_{S'} \otimes R' \to 0 \\ a \otimes r_1 \otimes \cdots \otimes r_n &\longmapsto ar_1 \otimes \cdots \otimes r_n \end{aligned}$$

An obvious modification of the complex (43) yields a complex

$$W(\mathfrak{a} \otimes R) \otimes_{W(R)} P \xrightarrow{\delta_1} W(\mathfrak{a} \otimes R \otimes R) \otimes_{W(R)} P \xrightarrow{\delta_2} \cdots, \tag{44}$$

where the factor $\mathfrak{a}$ is untouched in the definition of δ_i.

We set $\overline{P} = W(\overline{R}) \otimes_{W(R)} P$. Then the complex (44) identifies with the complex

$$W(\mathfrak{a} \otimes_{\overline{S}} \overline{R}) \otimes_{W(\overline{R})} \overline{P} \xrightarrow{\delta_1} W(\mathfrak{a} \otimes_{\overline{S}} \overline{R} \otimes_{\overline{S}} \overline{R}) \otimes_{W(\overline{R})} \overline{P} \xrightarrow{\delta_2} \cdots \tag{45}$$

given by the induced descent datum on $\overline{P}$. Since $p \cdot \mathfrak{a} = p \cdot \overline{S} = p \cdot \overline{R} = 0$ the argument before applies to show that (45) is exact except for the first place. Now an easy induction argument using the exact sequence of complexes

$$0 \to W(\mathfrak{a} \otimes_{\overline{S}} \overline{R}^{\otimes n}) \otimes_{W(\overline{R})} \overline{P} \to W(R^{\otimes n}) \otimes_{W(R)} P \to W(R'^{\otimes n}) \otimes_{W(R')} P' \to 0$$

proves the exactness statement for the complex in the middle.

In fact our method gives slightly more namely that we have also exactness of the complex of the augmentation ideals

$$I_{R^{\otimes n},m} \otimes_{W(R)} P$$

for each m.

Now we set $P_0 = \ker \delta_1 \colon (P \to W(R \otimes R) \otimes_{W(R)} P)$ and $P_0^1 = P_0 \cap I_R P$. By the exact cohomology sequence we have a diagram with exact rows and columns.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 \to & & P_0^1 & \to & I_R \otimes_{W(R)} P & \to & I_{R\otimes R} \otimes_{W(R)} P & \to & I_{R\otimes R\otimes R} \otimes_{W(R)} P \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 \to & & P_0 & \to & W(R) \otimes_{W(R)} P & \to & W(R \otimes R) \otimes_{W(R)} P & \to & W(R \otimes R \otimes R) \otimes_{W(R)} P \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 \to & & P_0/P_0^1 & \to & P/I_R P & \to & R \otimes R \otimes_R P/I_R P & \to & R \otimes R \otimes R \otimes_R P/I_R P \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0 & & 0
\end{array}$$

By the usual descent P_0/P_0^1 is a finitely generated projective $S-$module. We may lift it to a projective $W(S)-$module F, by lifting it step by step with respect to the surjection $W_{n+1}(S) \to W_n(S)$ and then taking the projective limit. By the projectivity of F we obtain a commutative diagram

$$\begin{tikzcd}
F \arrow[rr] \arrow[dr] & & P_0 \arrow[dl] \\
 & P_0/P_0^1 &
\end{tikzcd}$$

From the upper horizontal arrow we obtain a map $W(R) \otimes_{W(S)} F \to P$, which may be inserted into a commutative diagram

$$\begin{array}{ccc}
W(R) \otimes_{W(S)} F & \longrightarrow & P \\
\Big\downarrow & & \Big\downarrow \\
R \otimes_S P_0/P_0^1 & \xrightarrow{\sim} & P/IP
\end{array}$$

Since the lower horizontal arrow is an isomorphism by usual descent theory we conclude by Nakayama that the upper horizontal arrow is an isomorphism. Comparing the exact sequence (40) for $M = F$ with the exact sequence (43) for $N = P$, we obtain that $F \to P_0$ is an isomorphism. Since also the graded sequence associated to (40) is exact, we obtain moreover that $P_0^1 = IP_0$. Hence the proof of the proposition 33 is complete. $\square$

We may define a descent datum for 3n-displays. Let S be a ring, such that p is nilpotent in S and let $S \to R$ be a faithfully flat morphism of rings. We consider the usual diagram (compare (41)):

$$R \underset{q_2}{\overset{q_1}{\rightrightarrows}} R \otimes_S R \overset{\xrightarrow{q_{12}}}{\underset{\xrightarrow{q_{23}}}{\xrightarrow{q_{13}}}} R \otimes_S R \otimes_S R$$

Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a 3n-display over R. We denote the 3n-displays obtained by base change by $q_1^* \mathcal{P}$ etc.. Then a descent datum on $\mathcal{P}$ relative to $R \to S$ is an isomorphism of 3n-displays

$$\alpha \colon q_1^* \mathcal{P} \longrightarrow q_2^* \mathcal{P},$$

such that the cocycle condition holds, i.e. the diagram (42) is commutative if the letter p is replaced by q and the letter N is replaced by $\mathcal{P}$. Clearly for any 3n-display $\mathcal{P}_0$ over S we have a canonical descent datum $\alpha_{\mathcal{P}_0}$ on the base change $\mathcal{P}_{0,R}$ over R.

Theorem 37. — *The functor $\mathcal{P}_0 \mapsto (\mathcal{P}_{0,R}, \alpha_{\mathcal{P}_0})$ from the category of displays over S to the category of displays over R equipped with a descent datum relative to $S \to R$ is an equivalence of categories. The same assertion holds for the category of 3n-displays.*

Proof. — Let $(\mathcal{P}, \alpha)$ be a display over R with a descent datum relative to $S \to R$. We define a $W(S)-$module P_0 and a $S-$module K_0, such that the rows in the following diagram are exact

$$\begin{array}{ccccccc} 0 & \longrightarrow & P_0 & \longrightarrow & P & \xrightarrow{\delta} & W(R \otimes_S R) \otimes_{W(R)} P \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & K_0 & \longrightarrow & P/Q & \xrightarrow{\delta} & R \otimes_S R \otimes_R P/Q \end{array} \tag{46}$$

Here the maps δ are given by the descent datum α as explained above. That we have also a descent datum on P/Q follows just from our assumption that α is an isomorphism of displays and therefore preserves Q. We claim that the map $P_0 \to K_0$ is surjective. Indeed, since $R \to S$ is faithfully flat, it suffices to show that $R \otimes_S P_0 / I_S P_0 \to R \otimes_S K_0$ is surjective. But this can be read of from the commutative diagram:

$$\begin{array}{ccccc} W(R) \otimes_{W(S)} P_0 & \twoheadrightarrow & R \otimes_S P_0 / I P_0 & \longrightarrow & R \otimes_S K_0 \\ \downarrow & & \downarrow & & \downarrow \\ P & \twoheadrightarrow & P/IP & \twoheadrightarrow & P/Q \end{array}$$

Note that the vertical arrows are isomorphisms by proposition 33 or the usual descent theory.

Let us denote by Q_0 the kernel of the surjection $P_0 \to K_0$. Then we obtain a commutative diagram with exact rows and columns:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & Q_0 & \longrightarrow & Q & \longrightarrow & Q_2 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & P_0 & \longrightarrow & P & \longrightarrow & W(R \otimes_S R) \otimes_{W(R)} P = p_2^* P \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & P_0/Q_0 & \longrightarrow & P/Q & \longrightarrow & R \otimes_S R \otimes_R (P/Q) = q_2^*(P/Q) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
\end{array}$$

Here Q_2 and $p_2^* P$ are parts of the display $q_2^* \mathcal{P} = (p_2^* P, Q_2, F, V^{-1})$ which is obtained by base change.

To get a display $\mathcal{P}_0 = (P_0, Q_0, F, V^{-1})$ we still have to define the operators F and V^{-1}. First since α commutes with F by assumption we have a commutative diagram

$$\begin{array}{ccc}
P & \xrightarrow{\delta} & p_2^* P \\
{\scriptstyle F}\downarrow & & \downarrow{\scriptstyle F} \\
P & \xrightarrow{\delta} & p_2^* P
\end{array}$$

This shows that F induces a map on the kernel of δ:

$$F \colon P_0 \longrightarrow P_0$$

Secondly α commutes with V^{-1}, i.e. we have a commutative diagram

$$\begin{array}{ccc}
Q_1 & \xrightarrow[\sim]{\alpha} & Q_2 \\
{\scriptstyle V^{-1}}\downarrow & & \downarrow{\scriptstyle V^{-1}} \\
p_1^* P & \xrightarrow{\alpha} & p_2^* P
\end{array}$$

Recalling the definition of δ one obtains a commutative diagram

$$\begin{array}{ccc}
Q & \xrightarrow{\delta} & Q_2 \\
{\scriptstyle V^{-1}}\downarrow & & \downarrow{\scriptstyle V^{-1}} \\
P & \xrightarrow{\delta} & p_2^* P = W(R \otimes_S R) \otimes_{W(R)} P.
\end{array}$$

Hence we obtain $V^{-1} \colon Q_0 \longrightarrow P_0$ as desired. Finally we need to check the nilpotence condition. Since the maps V^{-1} and F are compatible with $P_0 \hookrightarrow P$, the same is true for $V^{\#}$ by the characterization of lemma 10. Hence we have a commutative diagram

$$\begin{array}{ccc} P_0 & \longrightarrow & P \\ {\scriptstyle V^{\#}}\downarrow & & \downarrow{\scriptstyle V^{\#}} \\ W(S)\otimes_{F,W(S)} P_0 & \longrightarrow & W(R)\otimes_{F,W(R)} P \end{array}$$

The nilpotence follows now from the injectivity of the map

$$S/pS \otimes_{\mathbf{w}_n,W(S)} P_0 \longrightarrow R/pR \otimes_{\mathbf{w}_n,W(R)} P$$

and the form (14) of the nilpotence condition. □

1.4. Rigidity. — Our next aim is a rigidity theorem for displays in the sense of rigidity for p-divisible groups. Let S be a ring, such that p is nilpotent in S. Assume we are given an ideal $\mathfrak{a} \subset S$ with a divided power structure γ_n ([BO] 3.1). We set $\alpha_{p^n}(a) = (p^n - 1)!\gamma_{p^n}(a)$. We may "divide" the $n-th$ Witt polynomial $\mathbf{w}_n(X_0, \cdots, X_n)$ by p^n:

$$\mathbf{w}'_n(X_0, \cdots, X_n) = \alpha_{p^n}(X_0) + \alpha_{p^{n-1}}(X_1) + \cdots + X_n. \tag{47}$$

Let us denote by $\mathfrak{a}^{\mathbb{N}}$ the additive group $\prod_{i\in\mathbb{N}} \mathfrak{a}$. We define a $W(S)-$module structure on $\mathfrak{a}^{\mathbb{N}}$:

$$\xi[a_0, a_1 \cdots] = [\mathbf{w}_0(\xi)a_0, \mathbf{w}_1(\xi)a_1, \cdots], \quad \text{where } \xi \in W(S),\ [a_0, a_1, \cdots] \in \mathfrak{a}^{\mathbb{N}}.$$

The $\mathbf{w}'_n$ define an isomorphism of $W(S)-$modules:

$$\begin{aligned} \log : W(\mathfrak{a}) &\longrightarrow \mathfrak{a}^{\mathbb{N}} \\ \underline{a} = (a_0, a_1, a_2 \cdots) &\longmapsto [\mathbf{w}'_0(\underline{a}), \mathbf{w}'_1(\underline{a}), \cdots] \end{aligned} \tag{48}$$

We denote the inverse image $\log^{-1}[\mathfrak{a}, 0, \cdots, 0, \cdots]$ simply by $\mathfrak{a} \subset W(\mathfrak{a})$. Then $\mathfrak{a}$ is an ideal of $W(S)$.

By going to a universal situation it is not difficult to compute what multiplication, Frobenius homomorphism, and Verschiebung on the Witt ring induce on the right hand side of (48):

$$\begin{aligned} [a_0, a_1, \ldots][b_0, b_1, \ldots] &= [a_0b_0, pa_1b_1, \ldots, p^i a_i b_i, \ldots] \\ {}^F[a_0, a_1, \ldots] &= [pa_1, pa_2, \ldots .pa_i, \ldots] \\ {}^V[a_0, a_1, \ldots] &= [0, a_0, a_1, \ldots, a_i, \ldots] \end{aligned} \tag{49}$$

The following fact is basic:

Lemma 38. — *Let (P, Q, F, V^{-1}) be a display over S. Then there is a unique extension of the operator V^{-1}:*

$$V^{-1} \colon W(\mathfrak{a})P + Q \longrightarrow P,$$

such that $V^{-1}\mathfrak{a}P = 0$.

Proof. — Choose a normal decomposition

$$P = L \oplus T.$$

Then $W(\mathfrak{a})P + Q = \mathfrak{a}T \oplus L \oplus I_S T$. We define V^{-1} using this decomposition. To finish the proof we need to verify that $V^{-1}\mathfrak{a}L = 0$. But ${}^F\mathfrak{a} = 0$, since the Frobenius map on the right hand side of (48) is

$${}^F[u_0, u_1, \ldots] = [pu_1, pu_2, \ldots].$$

□

Lemma 39. — *Let S be a ring, such that p is nilpotent in S. Let $\mathfrak{a} \subset S$ be an ideal with divided powers. We consider two displays $\mathcal{P} = (P, Q, F, V^{-1})$ and $\mathcal{P}' = (P', Q', F, V^{-1})$ over S. Then the natural map*

$$\operatorname{Hom}(\mathcal{P}, \mathcal{P}') \longrightarrow \operatorname{Hom}(\mathcal{P}_{S/\mathfrak{a}}, \mathcal{P}'_{S/\mathfrak{a}}) \tag{50}$$

is injective. Moreover let M be a natural number, such that $a^{p^M} = 0$ for any $a \in \mathfrak{a}$. Then the group $p^M \operatorname{Hom}(\mathcal{P}_{S/\mathfrak{a}}, \mathcal{P}'_{S/\mathfrak{a}})$ lies in the image of (50).

Proof. — As explained above the map $V^{-1} : Q' \longrightarrow P'$ extends to the map $V^{-1} : W(\mathfrak{a})P' + Q' \longrightarrow P'$, which maps $W(\mathfrak{a})P'$ to $W(\mathfrak{a})P'$. Let $u : \mathcal{P} \longrightarrow \mathcal{P}'$ be a map of displays, which is zero modulo $\mathfrak{a}$, i.e. $u(P) \subset W(\mathfrak{a})P'$. We claim that the following diagram is commutative:

$$\begin{array}{ccc} P & \xrightarrow{u} & W(\mathfrak{a})P' \\ {\scriptstyle V^{\#}}\big\downarrow & & \big\uparrow{\scriptstyle (V^{-1})^{\#}} \\ W(S) \otimes_{F,W(S)} P & \xrightarrow{1 \otimes u} & W(S) \otimes_{F,W(S)} W(\mathfrak{a})P' \end{array} \tag{51}$$

Indeed, since $P = W(S)V^{-1}Q$, it is enough to check the commutativity on elements of the form $wV^{-1}l$, where $l \in Q$. Since $V^{\#}(wV^{-1}l) = w \otimes l$. the commutativity is readily checked. Let us denote by $1 \otimes_{F^N} u : W(R) \otimes_{F^N, W(R)} P \longrightarrow W(R) \otimes_{F^N, W(R)} W(\mathfrak{a})P'$ the map obtained by tensoring. Iterating the diagram (51) we obtain

$$(V^{-N})^{\#}(1 \otimes_{F^N} u)(V^{N\#}) = u \tag{52}$$

By the nilpotence condition for each number$M$, there exists a number N, such that

$$V^{N\#}(P) \subset I_{S,M} \otimes_{F^N, W(S)} P.$$

But since $I_{S,M} \cdot W(\mathfrak{a}) = 0$ for big M, we obtain that the left hand side of (52) is zero. This proves the injectivity.

The last assertion is even true without the existence of divided powers. Indeed, it follows from the assumption that $p^M W(\mathfrak{a}) = 0$. Let now $\overline{u} : \mathcal{P}_{S/\mathfrak{a}} \longrightarrow \mathcal{P}'_{S/\mathfrak{a}}$ be a morphism of displays.

For $x \in P$ let us denote by $\overline{x} \in W(S/\mathfrak{a}) \otimes_{W(S)} P$ its reduction modulo $\mathfrak{a}$. Let $y \in P'$ be any lifting of $u(\overline{x})$. Then we define

$$v(x) = p^M \cdot y.$$

Since $p^M W(\mathfrak{a}) = 0$ this is well–defined. One checks that v is a morphism of displays $\mathcal{P} \to \mathcal{P}'$, and that $\overline{v} = p^M \overline{u}$. □

Proposition 40. — *Let S be a ring such that p is nilpotent in S. Let $\mathfrak{a} \subset S$ be a nilpotent ideal, i.e. $\mathfrak{a}^N = 0$ for some integer N. Let $\mathcal{P}$ and $\mathcal{P}'$ be displays over S. The the natural map*

$$\operatorname{Hom}(\mathcal{P}, \mathcal{P}') \longrightarrow \operatorname{Hom}(\mathcal{P}_{S/\mathfrak{a}}, \mathcal{P}'_{S/\mathfrak{a}})$$

is injective, and the cokernel is a p-torsion group.

Proof. — By induction one restricts to the case, where $\mathfrak{a}^p = 0$. Then we have a unique divided power structure on $\mathfrak{a}$, such that $\gamma_p(a) = 0$ for $a \in \mathfrak{a}$. One concludes by the lemma. □

Corollary 41. — *Assume again that p is nilpotent in S and that the ideal generated by nilpotent elements is nilpotent. Then the group* $\operatorname{Hom}(\mathcal{P}, \mathcal{P}')$ *is torsionfree.*

Proof. — By the proposition we may restrict to the case where the ring S is reduced. Then the multiplication by p on $W(S)$ is the injective map:

$$(s_0, s_1, s_2 \dots) \longmapsto (0, s_0^p, s_1^p \dots)$$

Therefore the multiplication by p on P' is also injective, which proves the corollary. □

2. Lifting Displays

In this chapter we will consider a surjective homomorphism of rings $S \to R$. The kernel will be denoted by $\mathfrak{a}$. We assume that the fixed prime number p is nilpotent in S.

To a display over R we will associate the crystal, which controls the deformation theory of this display in a way which is entirely similiar to the deformation theory of Grothendieck and Messing for $p-$divisible groups.

2.1. The main theorem. — We begin by a lemma which demonstrates what we are doing in a simple situation.

Lemma 42. — *Let $S \to R$ be as above and assume that there is a number N, such that $a^N = 0$ for any $a \in \mathfrak{a}$. Let (P_i, F_i) for $i = 1, 2$ be projective finitely generated $W(S)-$modules P_i, which are equipped with ${}^F-$linear isomorphisms $F_i : P_i \to P_i$. We set $\overline{P}_i = W(R) \otimes_{W(S)} P_i$ and define ${}^F-$linear isomorphisms $\overline{F}_i : \overline{P}_i \to \overline{P}_i$, by $\overline{F}_i(\xi \otimes x) = {}^F\xi \otimes F_i x$, for $\xi \in W(R), x \in P_i$.*

Then any homomorphism $\overline{\alpha} : (\overline{P}_1, \overline{F}_1) \to (\overline{P}_2, \overline{F}_2)$ admits a unique lifting $\alpha : (P_1, F_1) \to (P_2, F_2)$.

Proof. — First we choose a lifting $\alpha_0 : P_1 \to P_2$, which does not necessarily commute with the F_i. We look for a $W(S)$-linear homomorphism $\omega \in \mathrm{Hom}_{W(S)}(P_1, W(\mathfrak{a})P_2)$, such that

$$F_2(\alpha_0 + \omega) = (\alpha_0 + \omega)F_1. \tag{53}$$

Since $\overline{\alpha}$ commutes with $\overline{F}_1$ the ^{F}−linear map $\eta = F_2\alpha_0 - \alpha_0 F_1$ maps P_1 to $W(\mathfrak{a})P_2$. The equation (53) becomes

$$\omega F_1 - F_2\omega = \eta,$$

or equivalently

$$\omega - F_2^{\#}(W(S) \otimes_{F,W(S)} \omega)(F_1^{\#})^{-1} = \eta^{\#}(F_1^{\#})^{-1}. \tag{54}$$

We define now a $\mathbb{Z}_p$−linear endomorphism U of $\mathrm{Hom}_{W(S)}(P_1, W(\mathfrak{a})P_2)$ by

$$U\omega = F_2^{\#}(W(S) \otimes_{F,W(S)} \omega)(F_1^{\#})^{-1}.$$

Then U is nilpotent. Indeed for this it suffices to show that F_2 is nilpotent on $W(\mathfrak{a})P_2$. Clearly we need only to show that the Frobenius ^{F} is nilpotent on $W(\mathfrak{a})$. Since p is nilpotent an easy reduction reduces this statement to the case, where $p \cdot \mathfrak{a} = 0$. It is well–known that in this case the Frobenius on $W(\mathfrak{a})$ takes the form

$${}^F(a_0, a_1, \ldots, a_i, \ldots) = (a_0^p, a_1^p, \ldots, a_i^p, \ldots).$$

Since this is nilpotent by assumption the operator U is nilpotent, too.

Then the operator $1 - U$ is invertible, and therefore the equation (54)

$$(1 - U)\omega = \eta^{\#}(F_1^{\#})^{-1}$$

has a unique solution. □

Corollary 43. — *Assume that we are given an ideal $\mathfrak{c} \subset W(\mathfrak{a})$, which satisfies ${}^F\mathfrak{c} \subset \mathfrak{c}$ and a $W(S)$−module homomorphism $\alpha_0 : P_1 \to P_2$, which satisfies the congruence*

$$F_2\alpha_0(x) \equiv \alpha_0(F_1 x) \mod \mathfrak{c}P_2.$$

Then we have $\alpha \equiv \alpha_0 \mod \mathfrak{c}P_2$.

Proof. — One starts the proof of the lemma with α_0 given by the assumption of the corollary and looks for a solution $\omega \in \mathrm{Hom}_{W(S)}(P_1, \mathfrak{c}P_2)$ of the equation (53). □

Theorem 44. — *Let $S \to R$ be a surjective homomorphism of rings, such that p is nilpotent in S. Assume the kernel $\mathfrak{a}$ of this homomorphism is equipped with divided powers. Let $\mathcal{P}$ be a display over R and let $\mathcal{P}_1$ and $\mathcal{P}_2$ be liftings to S. Let us denote by $\hat{Q}_i$ the inverse image of Q by the map $P_i \to P$ for $i = 1, 2$. Let $V^{-1} : \hat{Q}_i \to P_i$ be the extension of the operator $V^{-1} : Q_i \to P_i$ given by the divided powers. Then there is a unique isomorphism $\alpha : (P_1, \hat{Q}_1, F, V^{-1}) \to (P_2, \hat{Q}_2, F, V^{-1})$, which lifts the identity of $\mathcal{P}$.*

Proof. — The uniqueness follows from the proof of lemma 39. Indeed one has only to observe that the commutative diagram (51) still makes sense. By assumption we have $p^M \cdot \mathfrak{a} = 0$ for some number M. We make an induction on the number N to show the following assertion:

There exists a $W(S)-$linear lifting $\alpha : P_1 \to P_2$ of the identity such that

$$\begin{aligned} F\alpha(x) &= \alpha(Fx) \mod p^N W(\mathfrak{a}) \quad \text{for} \quad x \in P_1 \\ V^{-1}\alpha(y) &= \alpha(V^{-1}y) \mod p^N W(\mathfrak{a}) \quad \text{for} \quad y \in \hat{Q}_1. \end{aligned} \tag{55}$$

We note that the divided powers give us an isomorphism $\prod_n \mathbf{w'}_n : W(\mathfrak{a}) \simeq \mathfrak{a}^{\mathbb{N}}$. From this we see that

$$^F W(\mathfrak{a}) \subset pW(\mathfrak{a}), \qquad I_S \cdot W(\mathfrak{a}) \subset pW(\mathfrak{a}).$$

In order to have a start for our induction, we consider the equations (55) to be fulfilled in the case $N = 0$ for any $W(S)-$linear lifting α. Hence we may assume that we have already constructed a $W(S)-$linear homomorphism α_N, which lifts the identity and satisfies (55). To prove the theorem we have to construct a $W(S)-$ linear lifting α' of the identity, which satisfies (55) with N replaced by $N+1$. We choose a normal decomposition $P_1 = L_1 \oplus T_1$ and we put $L_2 = \alpha_N(L_1)$ and $T_2 = \alpha_N(T_1)$. Then $P_2 = L_2 \oplus T_2$ will in general not be a normal decomposition for the display $\mathcal{P}_2$. But we can replace the display $\mathcal{P}_2$ by the display $(P_2, L_2 + I_S T_1, F, V^{-1})$, which is defined because $L_2 + I_S T_1 \subset \hat{Q}_2$. Hence we may assume without loss of generality that $P_2 = L_2 + T_2$ is a normal decomposition.

For $i = 1, 2$ we consider the $^F-$linear isomorphisms

$$U_i = V_i^{-1} + F_i : L_i \oplus T_i \longrightarrow P_i.$$

Then we define α to be the unique $W(S)-$linear map $P_1 \to P_2$, lifting the identity which satisfies

$$\alpha(U_1 x) = U_2 \alpha(x), \qquad \text{for} \quad x \in P_1. \tag{56}$$

One readily verifies that α_N satisfies this equation modulo $p^N W(\mathfrak{a})$. By the corollary to the lemma 42 we obtain:

$$\alpha \equiv \alpha_N \mod p^N W(\mathfrak{a}) \tag{57}$$

We will verify that α commutes with F modulo $p^{N+1} W(\mathfrak{a})$. We verify this for elements $l_1 \in L_1$ and $t_1 \in T_1$ separately. We write $\alpha(l_1) = l_2 + t_2$, where $l_2 \in L_2$ and $t_2 \in T_2$. Since $\alpha_N(l_1) \in L_2$ we conclude from the congruence (57) that $t_2 \equiv 0 \mod p^N W(\mathfrak{a})$. Therefore we obtain

$$Ft_2 \equiv 0 \mod p^{N+1} W(\mathfrak{a}).$$

Also since $V^{-1}(W(\mathfrak{a})P_2) \subset W(\mathfrak{a})P_2$, we find

$$V^{-1} t_2 \equiv 0 \mod p^N W(\mathfrak{a}).$$

Now we can compute:

$$\begin{aligned}\alpha(V^{-1}l_1)= &\ \alpha(U_1 l_1) = U_2\alpha(l_1) = V^{-1}l_2 + Ft_2 \\ &\equiv V^{-1}l_2 = V^{-1}\alpha(l_1) - V^{-1}t_2 \mod p^{N+1}W(\mathfrak{a}).\end{aligned} \tag{58}$$

If we multiply the last equation by p, we obtain

$$\alpha(Fl_1) \equiv F\alpha(l_1) \quad \text{modulo} \quad p^{N+1}W(\mathfrak{a}), \quad \text{for} \quad l_1 \in L_1.$$

To treat the elements in T_1 we write $\alpha(t_1) = l'_2 + t'_2$. The same argument as before now yields $l'_2 \equiv 0 \mod p^N W(\mathfrak{a})$. Since our operator V^{-1} is ${}^F-$linear on $\hat{Q}_2$ and since l'_2 is a sum of elements of the form $\xi \cdot y$, where $\xi \in p^N W(\mathfrak{a})$ and $y \in L'_2$, we obtain

$$V^{-1}l'_2 \equiv 0 \mod p^{N+1}W(\mathfrak{a}).$$

Now we compute as above:

$$\alpha(Ft_1) = \alpha(U_1 t_1) = U_2\alpha(t_1) = V^{-1}l'_2 + Ft'_2$$

$$\equiv Ft'_2 = F\alpha(t_1) - Fl'_2 \equiv F\alpha(t_1) \mod p^{N+1}W(\mathfrak{a}).$$

Alltogether we have proved

$$\alpha(Fx) \equiv F\alpha(x) \mod p^{N+1}W(\mathfrak{a}), \quad \text{for} \quad x \in P_1. \tag{59}$$

From this equation we conclude formally

$$\alpha(V^{-1}y) \equiv V^{-1}\alpha(y) \mod p^{N+1}W(\mathfrak{a}) \quad \text{for} \quad y \in I_S P_1. \tag{60}$$

Indeed, it is enough to check this congruence for y of the form ${}^V\xi \cdot x$. Since $V^{-1}({}^V\xi x) = \xi Fx$, we conclude easily by 59. The following equation holds because both sides are zero:

$$\alpha(V^{-1}y) = V^{-1}\alpha(y) \quad \text{for} \quad y \in \mathfrak{a} \cdot P_1. \tag{61}$$

The equation (58) shows that α does not necessarily commute with V^{-1} on L_1 modulo $p^{N+1}W(\mathfrak{a})$. Indeed, the map $L_1 \xrightarrow{\alpha} L_2 \oplus T_2 \xrightarrow{pr} T_2$ factors through $p^N W(\mathfrak{a})T_2$. Let us denote by η the composite:

$$\eta : L_1 \longrightarrow p^N W(\mathfrak{a})T_2 \xrightarrow{V^{-1}} p^N W(\mathfrak{a})P_2$$

Then we may rewrite the formula (58) as

$$\alpha(V^{-1}l_1) \equiv V^{-1}\alpha(l_1) - \eta(l_1) \mod p^{N+1}W(\mathfrak{a}). \tag{62}$$

We look for a solution α' of our problem, which has the form

$$\alpha' = \alpha + \omega,$$

where ω is a $W(S)-$linear map

$$\omega : P_1 \longrightarrow p^N W(\mathfrak{a})P_2. \tag{63}$$

First of all we want to ensure that the equation (59) remains valid for α'. This is equivalent with

$$\omega(Fx) = F\omega(x) \mod p^{N+1}W(\mathfrak{a}) \quad \text{for} \quad x \in P_1.$$

But the right hand side of this equation is zero $\mod p^{N+1}W(\mathfrak{a})$. Hence α' satisfies (59), if

$$\omega(Fx) \equiv 0 \mod p^{N+1}W(\mathfrak{a}).$$

We note that any $W(S)-$linear map (63) satisfies trivially $\omega(FL_1) = \omega(pV^{-1}L_1) = p\omega(V^{-1}L_1) \equiv 0 \mod p^{N+1}W(\mathfrak{a})$. Hence α' commutes with $F \mod p^{N+1}W(\mathfrak{a})$, if ω mod $p^{N+1}W(\mathfrak{a})$ belongs to the $W(S)-$module

$$\mathrm{Hom}(P_1/W(S)FT_1,\ p^N W(\mathfrak{a})/p^{N+1}W(\mathfrak{a}) \otimes_{W(S)} P_2). \tag{64}$$

Moreover α' commutes with $V^{-1} \mod p^{N+1}W(\mathfrak{a})$, if ω satisfies the following congruence

$$\omega(V^{-1}l_1) - V^{-1}\omega(l_1) = \eta(l_1) \mod p^{N+1}W(\mathfrak{a}), \quad \text{for } l_1 \in L_1. \tag{65}$$

Indeed, we obtain from (65)

$$\alpha'(V^{-1}y) = V^{-1}\alpha'(y) \mod p^{N+1}W(\mathfrak{a}), \quad \text{for} \quad y \in \hat{Q}_1,$$

because of (62) for $y \in L_1$ and because of (60) and (61) for $y \in I_S P_1 + \mathfrak{a}P_1$. Hence our theorem is proved if we find a solution ω of the congruence (65) in the $W(S)-$module (64).

The map V^{-1} induces an ${}^F-$linear isomorphism

$$V^{-1} : L_1 \longrightarrow P_1/W(S)FT_1.$$

Hence we may identify the $W(S)-$module (64) with

$$\mathrm{Hom}_{F-\mathrm{linear}}(L_1,\ p^N W(\mathfrak{a})/p^{N+1}W(\mathfrak{a}) \otimes_{W(S)} P_2), \tag{66}$$

by the map $\omega \longmapsto \omega V^{-1}$.

We rewrite now the congruence (65) in terms of $\tilde{\omega} = \omega V^{-1}$. The map $V^{-1}\omega$ is in terms of $\tilde{\omega}$ the composite of the following maps:

$$\begin{array}{ccccccc} L_1 & \overset{\iota}{\hookrightarrow} & P_1 & \overset{pr}{\to} & W(S)V^{-1}L_1 & \xrightarrow{V^{\#}} & W(S) \otimes_{F,W(S)} L_1 \\ &&&&&& \downarrow{\scriptstyle\tilde{\omega}^{\#}} \\ & & p^N W(\mathfrak{a})/p^{N+1}W(\mathfrak{a}) \otimes_{W(S)} P_2 & & \xleftarrow{V^{-1}} & & p^N W(\mathfrak{a})/p^{N+1}W(\mathfrak{a}) \otimes_{W(S)} P_2 \end{array} \tag{67}$$

The map ι in this diagram is the canonical injection. The map pr is the projection with respect to the following direct decomposition

$$P_1 = W(S)V^{-1}L_1 \oplus W(S)FT_1.$$

Finally the lower horizontal ${}^F-$linear map V^{-1} is obtained as follows. The divided powers provide an isomorphism (compare (48)):

$$p^N W(\mathfrak{a})/p^{N+1}W(\mathfrak{a}) \xrightarrow{\sim} (p^N\mathfrak{a}/p^{N+1}\mathfrak{a})^{\mathbb{N}}.$$

Using the notation $[a_0, a_1, \ldots, a_n, \ldots]$ for a vector of $(p^N\mathfrak{a}/p^{N+1}\mathfrak{a})^{\mathbb{N}}$, the map V^{-1} is given by:

$$V^{-1}[a_0, a_1, \ldots] \otimes x \quad = \quad [a_1, a_2, \ldots] \otimes Fx.$$

Let us denote by $B = V^{\#} \circ pr \circ \iota$ the composite of the upper horizontal maps in the diagram (67). Then we may write

$$V^{-1}\omega = V^{-1}\tilde{\omega}^{\#}B.$$

We define a $\mathbb{Z}-$linear operator U on the space

$$\mathrm{Hom}_{F-\mathrm{linear}}(L_1, p^N W(\mathfrak{a})/p^{N+1}W(\mathfrak{a})^{\otimes}_{W(S)} P_2), \tag{68}$$

by

$$U\tilde{\omega} = V^{-1}\tilde{\omega}^{\#}B. \tag{69}$$

Hence the equation (65) which we have to solve now reads as follows:

$$(1-U)\tilde{\omega} = \eta \quad \mathrm{mod}\ p^{N+1}W(\mathfrak{a}).$$

Here 1 denotes the identity operator on the group (68) and $\tilde{\omega}$ and η are considered as elements of this group. Clearly this equation has a solution $\tilde{\omega}$ for any given η, if the operator U is nilpotent on (68).

To see the nilpotency we rewrite the space (68). We set $D_i = P_i/I_S P_i + pP_i = S/pS \otimes_{w_0, W(S)} P_i$, and we denote the image of Q_i in this space by D_i^1. Then our group (68) is isomorphic to

$$\mathrm{Hom}_{\mathrm{Frobenius}}(D_1^1, p^N W(\mathfrak{a})/p^{N+1}W(\mathfrak{a}) \otimes_{S/pS} D_2),$$

where Hom denotes the Frobenius linear maps of $S/pS-$modules. Now the operator U is given by the formula (69) modulo $pW(S) + I_S$. But then locally on Spec S/pS, the operator B, is just given by the matrix B of (15). Hence the nilpotency follows from (15). $\square$

2.2. Triples and crystals. — Let R be a ring such that p is nilpotent in R, and let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R. Consider a pd-thickening $S \to R$ with kernel $\mathfrak{a}$, i.e. by definition that p is nilpotent in S and that the ideal $\mathfrak{a}$ is equipped with divided powers. In particular this implies that all elements in $\mathfrak{a}$ are nilpotent. We will now moreover assume that the divided powers are compatible with the canonical divided powers on $p\mathbb{Z}_p \subset \mathbb{Z}_p$.

A $\mathcal{P}$-triple $\mathcal{T} = (\tilde{P}, F, V^{-1})$ over S consists of a projective finitely generated $W(S)$-module $\widetilde{P}$, which lifts P, i.e. is equipped with an isomorphism $W(R) \otimes_{W(S)} \widetilde{P} \simeq P$. Hence we have a canonical surjection $\widetilde{P} \to P$ with kernel $W(\mathfrak{a})\widetilde{P}$. Let us denote by $\hat{Q}$ the inverse image of Q. Moreover a triple consists of two ^{F}-linear operators of $W(S)$-modules $F : \widetilde{P} \to \widetilde{P}$ and $V^{-1} : \hat{Q} \to \widetilde{P}$. The following relations are required:

$$V^{-1}({}^V wx) = wFx, \quad \text{for} \quad w \in W(S), w \in \widetilde{P}.$$

$$V^{-1}(\mathfrak{a}\widetilde{P}) = 0$$

Here $\mathfrak{a} \subset W(S)$ is the ideal given by the divided powers (48).

There is an obvious notion of a morphism of triples. Let $\alpha : \mathcal{P}_1 \to \mathcal{P}_2$ be a morphism of displays. Let $\mathcal{T}_1$ respectively $\mathcal{T}_2$ be a $\mathcal{P}_1$-triple respectively a $\mathcal{P}_2$-triple over S. An α-morphism $\widetilde{\alpha} : \widetilde{P}_1 \to \widetilde{P}_2$ is a homomorphism of $W(S)$-modules which lifts α and which commutes with F and V^{-1}. We note that $\widetilde{\alpha}(\hat{Q}_1) \subset \hat{Q}_2$. Therefore the requirement that $\widetilde{\alpha}$ commutes with V^{-1} makes sense. With this definition the $\mathcal{P}$-triples over S form a category, where $\mathcal{P}$ is allowed to vary in the category of displays over R. We call it the category of triples relative to $S \to R$.

Let us now define base change for triples. Let $\varphi : R \to R'$ be a ring homomorphism. Let $S \to R$ respectively $S' \to R'$ be pd-thickenings. Assume that we are given a homomorphism of pd-thickenings:

$$\begin{array}{ccc} S & \xrightarrow{\psi} & S' \\ \downarrow & & \downarrow \\ R & \xrightarrow[\varphi]{} & R' \end{array} \tag{70}$$

Let $\mathcal{T}$ be a $\mathcal{P}$-triple over S as before. Let $\mathcal{P}_{R'}$ be the display obtained by base change from $\mathcal{P}$. Then we define a $\mathcal{P}_{R'}$-triple $\mathcal{T}_{S'}$ over S' as follows. We set $\mathcal{T}_{S'} = (W(S') \otimes_{W(S)} \widetilde{P}, F, V^{-1})$ with the following definition of F and V^{-1}. The operator F is simply the ^{F}-linear extension of $F : \widetilde{P} \to \widetilde{P}$. The operator V^{-1} on $\hat{Q}'$ is uniquely determined by the equations:

$$\begin{aligned} V^{-1}(w \otimes y) &= {}^F w \otimes V^{-1} y, \quad \text{for} \quad y \in \hat{Q}, w \in W(S') \\ V^{-1}({}^V w \otimes x) &= w \otimes Fx, \qquad \text{for} \quad x \in \widetilde{P} \\ V^{-1}(a \otimes x) &= 0, \qquad \text{for} \quad a \in \mathfrak{a}' \subset W(\mathfrak{a}'). \end{aligned}$$

Here $\mathfrak{a}'$ is the kernel of $S' \to R'$ with its pd-structure.

Let $S \to R$ be a pd-thickening and $\mathcal{P}$ be a display over R. Let $\mathcal{T}$ be a $\mathcal{P}$-triple over S. By theorem 44 it is determined up to unique isomorphism. We can construct all liftings of $\mathcal{P}$ to a display over S as follows. We consider the Hodge filtration of $\mathcal{P}$.

$$Q/I_R P \quad \subset \quad P/I_R P \tag{71}$$

Let L be a direct summand of $\widetilde{P}/I_S\widetilde{P}$, such that the filtration of S-modules

$$L \quad \subset \widetilde{P}/I_S\widetilde{P} \tag{72}$$

lifts the filtration (71). We call this a lifting of the Hodge filtration to $\mathcal{T}$. If we denote by $\widetilde{Q}_L \subset \widetilde{P}$ the inverse image of L by the projection $\widetilde{P} \to \widetilde{P}/I_S\widetilde{P}$ we obtain a display $(\widetilde{P}, \widetilde{Q}_L, F, V^{-1})$. By theorem 44 we conclude:

Proposition 45. — *The construction above gives a bijection between the liftings of the display $\mathcal{P}$ to S and the liftings of the Hodge filtration to $\mathcal{T}$.*

We will now formulate an enriched version of theorem 44.

Theorem 46. — *Let $\alpha : \mathcal{P}_1 \to \mathcal{P}_2$ be a morphism of displays over R. Let $S \to R$ be a pd-thickening and consider for $i = 1, 2$ a $\mathcal{P}_i$-triple $\mathcal{T}_i$ over S. Then there is a unique α-morphism of triples $\widetilde{\alpha} : \mathcal{T}_1 \to \mathcal{T}_2$.*

Proof. — To prove the uniqueness we may assume $\alpha = 0$. Then we consider the diagram 51 with P respectively P' replaced by $\widetilde{P}_1$ respectively $\widetilde{P}_2$ and u replaced by $\widetilde{\alpha}$. There is a map $V^{\#}$ on $\widetilde{P}$ which is uniquely determined by

$$V^{\#}(wV^{-1}y) = w \otimes y, \quad \text{for} \quad w \in W(S), y \in \hat{Q}.$$

Its existence follows by choosing a lifting of the Hodge filtration of $\mathcal{P}$ to $\mathcal{T}$. With these remarks the arguments of lemma 39 apply, and show the uniqueness. To show the existence we first consider the case where α is an isomorphism. By choosing liftings $\widetilde{\mathcal{P}}_1$ respectively $\widetilde{\mathcal{P}}_2$ of $\mathcal{P}_1$ respectively $\mathcal{P}_2$ to S this case is easily reduced to theorem 44. The general case is reduced to the first case by considering the isomorphism of displays:

$$\begin{array}{rcl} \mathcal{P}_1 \oplus \mathcal{P}_2 & \longrightarrow & \mathcal{P}_1 \oplus \mathcal{P}_2 \quad , \\ (x, y) & \longmapsto & (x, \alpha(x) + y) \end{array}$$

where $x \in \mathcal{P}_1$ and $y \in \mathcal{P}_2$. □

Remark: This theorem extends trivially to the case where S is a topological ring as in definition 13. More precisely let R be as in the last theorem, and let $S \to R$ be any surjection, such that the kernel $\mathfrak{a}$ is equipped with divided powers. If p is not nilpotent in S this is not a pd-thickening in our sense (compare section 2.2). Assume that there is a sequence of sub pd-ideals $\ldots \mathfrak{a}_n \supset \mathfrak{a}_{n+1} \ldots$, such that p is nilpotent in $S/\mathfrak{a}_n$ and such that S in complete and separated in the linear topology defined by the ideals $\mathfrak{a}_n$. Then the theorem above is true for the surjection $S \to R$. We note that S is a p-adic ring. We will call $S \to R$ a topological pd-thickening. We are particularly interested in the case where S has no p-torsion.

Let us fix $S \to R$ as before. To any display $\mathcal{P}$ we may choose a $\mathcal{P}$-triple $\mathcal{T}_{\mathcal{P}}(S)$. By the theorem $\mathcal{P} \mapsto \mathcal{T}_{\mathcal{P}}(S)$ is a functor from the category of displays to the category of triples. It commutes with arbitrary base change in the sense of (70). If we fix $\mathcal{P}$ we may view $S \mapsto \mathcal{T}_{\mathcal{P}}(S)$ as a crystal with values in the category of triples. We deduce from it two other crystals.

Let X be a scheme, such that p is locally nilpotent in $\mathcal{O}_X$. Then we will consider the cystalline site, whose objects are triples (U, T, δ), where $U \subset X$ is an open subscheme, $U \to T$ is a closed immersion defined by an ideal $\mathcal{J} \subset \mathcal{O}_T$, and δ is a divided power structure on $\mathcal{J}$. We assume that p is locally nilpotent on T, and that the divided powers δ are compatible with the canonical divided power structure on the ideal $p\mathbb{Z}_p \subset \mathbb{Z}_p$. The reason for this last condition, which was not necessary in theorem 46 will become apparent later. Let $W(\mathcal{O}_X^{\mathrm{crys}})$ be the sheaf on the crystalline site, which associates to a pd-thickening $U \to T$ the ring $W(\Gamma(T, \mathcal{O}_T))$. A crystal in $W(\mathcal{O}_X^{\mathrm{crys}})$-modules will be called a Witt crystal.

Sometimes we will restrict our attention to the crystalline site which consists of pd-thickenings (U, T, δ), such that the divided power structure is locally nilpotent in the sense of [Me] Chapt. III definition 1.1. We call this the nilpotent crystalline site.

Let $\mathcal{P}$ be a display over R. Then we define a Witt crystal $\mathcal{K}_{\mathcal{P}}$ on $\operatorname{Spec} R$ as follows. It is enough to give the value of $\mathcal{K}_{\mathcal{P}}$ on pd-thickenings of the form $\operatorname{Spec} R' \to$

$\operatorname{Spec} S'$, where $\operatorname{Spec} R' \hookrightarrow \operatorname{Spec} R$ is an affine open neighbourhood. The triple over S' associated to $\mathcal{P}'_R$ is of the form

$$\mathcal{T}_{\mathcal{P}_{R'}}(S') = (\widetilde{P}, F, V^{-1}).$$

We define

$$\mathcal{K}_{\mathcal{P}}(\operatorname{Spec} R' \to \operatorname{Spec} S') = \widetilde{P}. \tag{73}$$

For the left hand side we will also write $\mathcal{K}_{\mathcal{P}}(S')$.

Definition 47. — *The sheaf $\mathcal{K}_{\mathcal{P}}$ on the crystalline situs of* $\operatorname{Spec} R$ *is called the Witt crystal associated to $\mathcal{P}$. We also define a crystal of $\mathcal{O}^{\mathrm{crys}}$-modules on* $\operatorname{Spec} R$ *by*

$$\mathcal{D}_{\mathcal{P}}(S') = \mathcal{K}_{\mathcal{P}}(S')/I_{S'}\mathcal{K}(S').$$

$\mathcal{D}_{\mathcal{P}}$ is called the (covariant) Dieudonné crystal.

More generally we may evaluate these crystals for any topological pd-thickening in the sense of the last remark. If $(S, \mathfrak{a}_n)$ is a topological pd-thickening we set:

$$\begin{aligned} \mathcal{K}_{\mathcal{P}}(S) &= \varprojlim_n \mathcal{K}_{\mathcal{P}}(R/\mathfrak{a}_n) \\ \mathcal{D}_{\mathcal{P}}(S) &= \varprojlim_n \mathcal{D}_{\mathcal{P}}(R/\mathfrak{a}_n) \end{aligned} \tag{74}$$

The Witt crystal and the Dieudonné crystal are compatible with base change. This means that for an arbitrary homomorphism of pd-thickenings (70) we have canonical isomorphisms:

$$\begin{aligned} \mathcal{K}_{\mathcal{P}_{\mathcal{R}'}}(S') &\simeq W(S') \otimes_{W(S)} \mathcal{K}_{\mathcal{P}}(S) \\ \mathcal{D}_{\mathcal{P}_{\mathcal{R}'}}(S') &\simeq S' \otimes_S \mathcal{D}_{\mathcal{P}}(S). \end{aligned} \tag{75}$$

This follows from the definition of the $\mathcal{P}_{R'}$-triple $\mathcal{T}_{S'}$. The R-module $\mathcal{D}_{\mathcal{P}}(R)$ is identified with $P/I_R P$ and therefore inherits the Hodge filtration

$$\mathcal{D}^1_{\mathcal{P}}(R) \subset \mathcal{D}_{\mathcal{P}}(R). \tag{76}$$

The proposition 45 may be reformulated in terms of the Dieudonné crystal.

Theorem 48. — *Let $S \to R$ be a pd-thickening. Consider the category $\mathcal{C}$ whose objects are pairs $(\mathcal{P}, E)$, where $\mathcal{P}$ is a display over R, and E is a direct summand of the S-module $\mathcal{D}_{\mathcal{P}}(S)$, which lifts the Hodge filtration (76). A morphism $\phi : (\mathcal{P}, E) \to (\mathcal{P}', E')$ in the category $\mathcal{C}$ is a morphism of displays $\phi : \mathcal{P} \to \mathcal{P}'$, such that the induced morphism of the associated Dieudonné crystals (definition 47) maps E to E'. Then the category $\mathcal{C}$ is canonically equivalent to the category of displays over S.*

The description of liftings of a display $\mathcal{P}$ over R is especially nice in the following case: Let $S \to R$ be surjection with kernel $\mathfrak{a}$, such that $\mathfrak{a}^2 = 0$. Then we consider the abelian group:

$$\operatorname{Hom}(\mathcal{D}^1_{\mathcal{P}}(R), \mathfrak{a} \otimes_R (\mathcal{D}_{\mathcal{P}}(R)/\mathcal{D}^1_{\mathcal{P}}(R))) \tag{77}$$

We define an action of this group on the set of liftings of $\mathcal{P}$ to S as follows. Two liftings correspond by theorem 48 to two liftings E_1 and E_2 of the Hodge filtration. We need to define their difference in the group (77). Consider the natural homomorphism:

$$E_1 \subset \mathcal{D}_{\mathcal{P}}(S) \to \mathcal{D}_{\mathcal{P}}(S)/E_2$$

Since E_1 and E_2 lift the same module $\mathcal{D}^1_{\mathcal{P}}(R)$ the last map factors through

$$E_1 \to \mathfrak{a}(\mathcal{D}_{\mathcal{P}}(S)/E_2). \tag{78}$$

The right hand side is canonically isomorphic to $\mathfrak{a} \otimes_R (\mathcal{D}_{\mathcal{P}}(R)/\mathcal{D}^1_{\mathcal{P}}(R))$, since $\mathfrak{a}^2 = 0$. Hence the map (78) may be identified with a map:

$$u : \mathcal{D}^1_{\mathcal{P}}(R) \to \mathfrak{a} \otimes_R \mathcal{D}_{\mathcal{P}}(R)/\mathcal{D}^1_{\mathcal{P}}(R)$$

We define $E_1 - E_2 = u$. It follows immediately that:

$$E_2 = \{e - \widetilde{u(e)} | e \in E_1\}, \tag{79}$$

where $\widetilde{u(e)} \in \mathfrak{a}\mathcal{D}_{\mathcal{P}}(S)$ denotes any lifting of $u(e)$. This proves the following

Corollary 49. — *Let $\mathcal{P}$ be a display over R. Let $S \to R$ be a surjective ring homomorphism with kernel $\mathfrak{a}$, such that $\mathfrak{a}^2 = 0$. The action of the group* (77) *on the set of lifings of $\mathcal{P}$ to a display over S just defined is simply transitive. If $\mathcal{P}_0$ is a lifting of $\mathcal{P}$ and u an element in* (77) *we denote the action by $\mathcal{P}_0 + u$.*

Using example 1.17 it is easy to give a description of $\mathcal{P}_0 + u$ in the situation of the last corollary. Let $\mathfrak{a} \subset W(\mathfrak{a})$ be the subset of all Teichmüller representatives of elements of $\mathfrak{a}$. If we equip $\mathfrak{a}$ with the divided powers $\alpha_p(\mathfrak{a}) = 0$ this agrees with our definition after equation (48). We restrict our attention to homomorphisms $\alpha : P_0 \to \mathfrak{a}P_0 \subset W(\mathfrak{a})P_0$ and consider the display defined by (27):

$$\begin{array}{rcll} F_\alpha x & = & Fx - \alpha(Fx), & \text{for} \quad x \in P_0 \\ V_\alpha^{-1} y & = & V^{-1}y - \alpha(V^{-1}y), & \text{for} \quad y \in Q_0. \end{array} \tag{80}$$

Then there is an element u in the group (77) such that:

$$\mathcal{P}_\alpha = \mathcal{P}_0 + u \tag{81}$$

It is easily described: There is a natural isomorphism $\mathfrak{a}P_0 \cong \mathfrak{a} \otimes_R P/I_RP$. Hence α factors uniquely through a map:

$$\bar{\alpha} : P/I_RP \to \mathfrak{a} \otimes_R P/I_RP.$$

Conversely any R-module homomorphism $\bar{\alpha}$ determines uniquely a map α. Let u be the composite of the following maps:

$$u : Q/I_RP \subset P/I_RP \xrightarrow{\bar{\alpha}} \mathfrak{a} \otimes_R P/I_RP \to \mathfrak{a} \otimes_R P/Q. \tag{82}$$

Then the equation (81) holds. To see this consider the isomorphism :

$$\tau : (P_0, \hat{Q}_0, F_\alpha, V_\alpha^{-1}) \to (P_0, \hat{Q}_0, F, V^{-1}),$$

which exists by theorem 46 . Using the relations:

$$F\mathfrak{a}P_0 = V^{-1}\mathfrak{a}P_0 = 0, \quad \alpha^2 = 0,$$

it is easily verified that $\tau(x) = x + \alpha(x)$ for $x \in P_0$. It follows that $\mathcal{P}_\alpha$ is isomorphic to the display $(P_0, \tau(Q_0), F, V^{-1})$. Since

$$\tau(Q_0) = \{x + \alpha(x) | x \in Q_0\}$$

the equation (81) follows with the u defined above (82).

Next we define the universal deformation of a display. Let $S \to R$ be a surjection of rings, such that the kernel is a nilpotent ideal $\mathfrak{a}$. For a display $\mathcal{P}$ over R, we define the functor of deformations of $\mathcal{P}$:

$$\mathrm{Def}_{\mathcal{P}}(S)$$

as the set of isomorphism classes of pairs $(\tilde{\mathcal{P}}, \iota)$, where $\tilde{\mathcal{P}}$ is a display over S and $\iota : \mathcal{P} \to \tilde{\mathcal{P}}_R$ is an isomorphism with the display obtained by base change.

We will consider the deformation functor on the following categories $\mathrm{Aug}_{\Lambda\to R}$. Let Λ be a topological ring of type (16). The ring R is equipped with the discrete topology. Suppose we are given a continous surjective homomorphism $\varphi : \Lambda \to R$.

Definition 50. — *Let* $\mathrm{Aug}_{\Lambda\to R}$ *be the category of morphisms of discrete* Λ*-algebras* $\psi_S : S \to R$, *such that* ψ_S *is surjective and has a nilpotent kernel. If* $\Lambda = R$, *we will denote this category simply by* Aug_R.

A nilpotent R-algebra $\mathcal{N}$ is an R-algebra (without unit), such that $\mathcal{N}^N = 0$ for a sufficiently big number N. Let Nil_R denote the category of nilpotent R-algebras. To a nilpotent R-algebra $\mathcal{N}$ we associate an object $R|\mathcal{N}|$ in Aug_R. As an R-module we set $R|\mathcal{N}| = R \oplus \mathcal{N}$. The ring sructure on $R|\mathcal{N}|$ is given by the rule:

$$(r_1 \oplus n_1)(r_2 \oplus n_2) \quad = \quad (r_1 r_2 \oplus r_1 n_2 + r_2 n_1 + n_1 n_2) \quad \text{for } n_i \in \mathcal{N},\ r_i \in R.$$

It is clear that this defines an equivalence of the categories Nil_R and Aug_R. An R-module M is considered as an element of Nil_R by the multiplication rule: $M^2 = 0$. The corresponding object in Aug_R is denoted by $R|M|$. We have natural fully faithful embeddings of categories

$$(R - \text{modules}) \subset \mathrm{Aug}_R \subset \mathrm{Aug}_{\Lambda\to R}$$

Let F be a set-valued functor on $\mathrm{Aug}_{\Lambda\to R}$. The restriction of this functor to the category of R-modules is denoted by $\mathbf{t}_F$ and is called the tangent functor. If the functor $\mathbf{t}_F$ is isomorphic to a functor $M \mapsto M \otimes_R t_F$ for some R-module t_F, we call t_F the tangent space of the functor F (compare [Z1] 2.21).

Let T be a topological Λ-algebra of type (16) and $\psi_T : T \to R$ be a surjective homomorphism of topological Λ-algebras. For an object $S \in \mathrm{Aug}_{\Lambda\to R}$, we denote by $\mathrm{Hom}(T, S)$ the set of continous Λ-algebra homomorphisms, which commute with the augmentations ψ_T and ψ_S. We obtain a set-valued functor on $\mathrm{Aug}_{\Lambda\to R}$:

$$\mathrm{Spf}\, T(S) = \mathrm{Hom}(T, S) \tag{83}$$

If a functor is isomorphic to a functor of the type $\mathrm{Spf}\, T$ it is called prorepresentable.

We will now explain the prorepresentability of the functor $\mathrm{Def}_{\mathcal{P}}$. Let us first compute the tangent functor. Let M be an R-module. We have to study liftings of our fixed display $\mathcal{P}$ over R with respect to the homomorphism $R|M| \rightarrow R$. The corollary 49 applies to this situation. We have a canonical choice for $\mathcal{P}_0$:

$$\mathcal{P}_0 = \mathcal{P}_{R|M|}.$$

Let us denote by $\mathrm{Def}_{\mathcal{P}}(R|M|)$ the set of isomorphism classes of liftings of $\mathcal{P}$ to $R|M|$. Then we have an isomorphism :

$$\mathrm{Hom}_R(Q/I_R P, M \otimes_R P/Q) \rightarrow \mathrm{Def}_{\mathcal{P}}(R|M|), \tag{84}$$

which maps a homomorphism u to the display $\mathcal{P}_0 + u$. Hence the functor $\mathrm{Def}_{\mathcal{P}}$ has a tangent space, which is canonically isomorphic to the finitely generated projective R-module $\mathrm{Hom}_R(Q/I_R P, P/Q)$. Consider the dual R-module $\omega = Hom_R(P/Q, Q/I_R P)$. Then we may rewrite the isomorphism (84):

$$\mathrm{Hom}_R(\omega, M) \rightarrow \mathrm{Def}_{\mathcal{P}}(R|M|)$$

Hence the identical endomorphism of ω defines a morphism of functors:

$$\mathrm{Spf}\, R|\omega| \rightarrow \mathrm{Def}_{\mathcal{P}} \tag{85}$$

We lift ω to a projective finitely generated Λ-module $\tilde{\omega}$. We consider the symmetric algebra $\mathcal{S}_\Lambda(\tilde{\omega})$. Its completion A with respect to the augmentation ideal is a topological Λ-algebra of type (16), which has a natural augmentation $A \rightarrow \Lambda \rightarrow R$. Since the deformation functor is smooth, i.e. takes surjections $S_1 \rightarrow S_2$ to surjective maps of sets, the morphism (85) may be lifted to a morphism:

$$\mathrm{Spf}\, A \rightarrow \mathrm{Def}_{\mathcal{P}} \tag{86}$$

It is not difficult to show, that this is an isomorphism using the fact that it induces by construction an isomorphism on the tangent spaces (compare [CFG]). It is easy to describe the universal display over $\mathcal{P}^{univ}$ over A. Let $u : Q/I_R P \rightarrow \omega \otimes_R P/Q$ the map induced by the identical endomorphism of ω. Let $\alpha : P \rightarrow \omega \otimes_R P/Q$ be any map, which induces u as described by (82). The we obtain a display $\mathcal{P}_\alpha$ over $R|\omega|$. For $\mathcal{P}^{univ}$ we may take any lifting of $\mathcal{P}_\alpha$ to A.

Let us assume that the display $\mathcal{P}$ is given by the equations (9). In this case the universal deformation is as follows. We choose an arbitrary lifting $(\tilde{\alpha_{ij}}) \in Gl_h(W(\Lambda))$ of the matrix (α_{ij}). We choose indeterminates (t_{kl}) for $k = 1, \ldots d,\ l = d+1, \ldots h$. We set $A = \Lambda[\![t_{kl}]\!]$. For any number n we denote by E_n the unit matrix. Consider the following invertible matrix over $Gl_h(A)$:

$$\begin{pmatrix} E_d & [t_{kl}] \\ 0 & E_{h-d} \end{pmatrix} \quad (\alpha_{ij}) \tag{87}$$

As usual $[t_{kl}] \in W(A)$ denotes the Teichmüller representative. This matrix defines by (9) display $\mathcal{P}^{univ}$ over the topological ring A. The the pair $(A, \mathcal{P}^{univ})$ prorepresents the functor $\mathrm{Def}_{\mathcal{P}}$ on the category $\mathrm{Aug}_{\Lambda \rightarrow R}$.

2.3. Witt and Dieudonné crystals. — Our next aim is to explain how the Witt crystal may be reconstructed from the Dieudonné crystal.

The ideal $I_R \subset W(R)$ will be equipped with the divided powers (see [Gr] Chapt. IV 3.1):

$$\alpha_p({}^V w) = p^{p-2}\ {}^V(w^p), \qquad \text{for} \quad w \in W(R). \tag{88}$$

The morphism $\mathbf{w}_0 : W(R) \to R$ is a topological pd-thickening, in the sense of the remark after theorem 46, because (88) defines a pd-thickenings $\mathbf{w}_0 : W_n(R) \to R$. We note that the last pd-thickenings are nilpotent, if $p \neq 2$.

If we evaluate a crystal on $\operatorname{Spec} R$ in $W(R)$ we have the topological pd-structure above in mind (compare (74)).

More generally we may consider a pd-thickening $S \to R$, where we assume p to be nilpotent in S. Let $\mathfrak{a} \subset S$ be the kernel. The divided powers define an embedding $\mathfrak{a} \subset W(S)$, which is an ideal of $W(S)$ equipped with the same divided powers as $\mathfrak{a} \subset S$. The kernel of the composite $W(S) \overset{\mathbf{w}_0}{\to} S \to R$ is the orthogonal direct sum $I_S \oplus \mathfrak{a}$. Since we have defined divided powers on each direct summand, we obtain a pd-structure on the kernel of:

$$W(S) \longrightarrow R. \tag{89}$$

Again this induces pd-thickenings $W_m(S) \to R$. Therefore me may consider (89) as a topological pd-thickening, and evaluate crystals in $W(S)$.

In the case $p \neq 2$ the divided powers on the kernel of $W_m(S) \to R$ are nilpotent, if the divided powers on the ideal $\mathfrak{a}$ were nilpotent.

Proposition 51. — *Let $S \to R$ be a pd-thickening. There is a canonical isomorphism*

$$\mathcal{K}_{\mathcal{P}}(S) \cong \mathcal{D}_{\mathcal{P}}(W(S)).$$

This will follow from the more precise statement in proposition 53.

For later purposes it is useful to note that this proposition makes perfect sense if we work inside the nilpotent crystalline site.

To define the isomorphism of proposition 51 we need the following ring homomorphism defined by Cartier:

$$\triangle : W(R) \longrightarrow W(W(R)). \tag{90}$$

It is defined for any commutative ring R. In order to be less confusing we use a hat in the notation, if we deal with the ring $W(W(R))$.

The homomorphism $\triangle$ is functorial in R and satisfies

$$\hat{\mathbf{w}}_n(\triangle(\xi)) = {}^{F^n}\xi, \qquad \xi \in W(R). \tag{91}$$

As usual these properties determine $\triangle$ uniquely. We leave the reader to verify that the equation:

$$W(\mathbf{w}_n)(\triangle(\xi)) = {}^{F^n}\xi, \tag{92}$$

holds too.

Lemma 52. — *The following relations hold:*

$$\triangle({}^{F}\xi) = {}^{\hat{F}}(\triangle(\xi)) = W({}^{F})(\triangle(\xi)),$$

$$\triangle({}^{V}\xi) -^{\hat{V}} (\triangle(\xi)) = \left[{}^{V}\xi, 0, 0, \cdots\right] \in W(I_R)$$

Here on the right hand side we have used logarithmic coordinates with respect to the divided powers on I_R.

Proof. — We use the standard argument. By functoriality we may restrict to the case where R is torsion free (as $\mathbb{Z}$-module). Then $W(R)$ is torsion free too. Hence it is enough to show that for each integer $n \geq 0$ the equations of the lemma hold after applying $\hat{\mathbf{w}}_n$. This is readily verified. $\square$

Proposition 53. — *Let $S \to R$ be a pd-thickening with kernel $\mathfrak{a}$, and let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R. Let $\mathcal{T} = (\widetilde{P}, F, V^{-1})$ be the unique (up to canonical isomorphism) $\mathcal{P}$-triple over S. Consider the pd-thickening $W(S) \to R$ with kernel $I_S \oplus \mathfrak{a}$. Let $\overline{\mathcal{T}}$ denote the unique $\mathcal{P}$-triple related to this pd-thickening. Then $\overline{\mathcal{T}}$ is of the form*

$$\overline{\mathcal{T}} = (W(W(S)) \otimes_{\triangle, W(S)} \widetilde{P}, F, V^{-1}),$$

where the operators F and V^{-1} are uniquely determined by the following properties:

$$\begin{aligned} F(\hat{\xi} \otimes x) &= {}^{\hat{F}}\hat{\xi} \otimes Fx, \qquad \hat{\xi} \in W(W(S)), x \in \widetilde{P} \\ V^{-1}(\hat{\xi} \otimes y) &= {}^{\hat{F}}\hat{\xi} \otimes V^{-1}y, \quad y \in \hat{Q} \\ V^{-1}({}^{\hat{V}}\hat{\xi} \otimes x) &= \hat{\xi} \otimes Fx. \end{aligned} \tag{93}$$

Here as usual $\hat{Q}$ denotes the inverse image of Q by the morphism $\widetilde{P} \to P$.

The triple $\overline{\mathcal{T}}$ provides the isomorphism of proposition 51:

$$\mathcal{K}_{\mathcal{P}}(S) = \tilde{P} = W(S) \otimes_{\hat{\mathbf{w}}_0} (W(W(S)) \otimes_{\triangle, W(S)} \tilde{P}) = \mathcal{D}_{\mathcal{P}}(W(S)) \tag{94}$$

Proof. — Let $\alpha : W(S) \to R$ be the pd-thickening (89). It follows that from (92) that $W(W(S)) \otimes_{\triangle, W(S)} \widetilde{P} = \overline{P}$ is a lifting of P relative to α. We have homomorphisms

$$\overline{P} \xrightarrow{\pi} \widetilde{P} \longrightarrow P,$$

where the first arrow is induced by $W(\mathbf{w}_0) : W(W(S)) \to W(S)$. Let $\hat{Q}$ be the inverse image of Q in $\widetilde{P}$.

We choose a normal decomposition $P = L \oplus T$, and we lift it to a decomposition $\widetilde{P} = \widetilde{L} \oplus \widetilde{T}$. Then we have the decomposition

$$\hat{Q} = \widetilde{L} \oplus I_S \widetilde{T} \oplus \mathfrak{a} \widetilde{T}. \tag{95}$$

The divided power structure on the ideal $I_S \oplus \mathfrak{a} \subset W(S)$ induces an embedding of this ideal in $W(W(S))$. We will denote the images of I_S respectively $\mathfrak{a}$ by $\hat{I}_S$ respectively $\hat{\mathfrak{a}}$. The analogue of the decomposition (95) for the pd-thickening $W(S) \to R$ gives for the inverse image of Q:

$$\pi^{-1}(\hat{Q}) = W(W(S)) \otimes_{\triangle, W(S)} \widetilde{L} \oplus I_{W(S)} \otimes_{\triangle, W(S)} \widetilde{T} \oplus \hat{I}_S \otimes_{\triangle, W(S)} \widetilde{T} \oplus \hat{\mathfrak{a}} \otimes_{\triangle, W(S)} \widetilde{T}. \tag{96}$$

By the definition of $\overline{\mathcal{T}}$ the operator V^{-1} must be defined on $\pi^{-1}(\hat{Q})$ and it must be a lifting of V^{-1} on $\widetilde{P}$.

Let us assume for a moment that V^{-1} exists as required in the proposition. We claim that this implies that V^{-1} vanishes on the last two direct summands on (96). To see that V^{-1} vanishes on $\hat{I}_S \otimes_{\triangle, W(S)} \widetilde{T}$, we remark that by lemma 52 any element of $\hat{I}_S$ may be written in the form $\triangle({}^V\xi) -^{\hat{V}} \triangle(\xi)$, for $\xi \in W(S)$. Hence it suffices to show that for $t \in \widetilde{T}$

$$V^{-1}(\triangle({}^V\xi) - {}^{\hat{V}}\triangle(\xi) \otimes t) = 0.$$

But this follows from the equation (93).

Let $a \in \mathfrak{a} \subset W(S)$ be an element. The same element considered as element of $\hat{\mathfrak{a}} \subset W(W(S))$ will be denoted by $\hat{a}$. We have the following lemma, which we prove later.

Lemma 54. — *We have* $\triangle(a) = \hat{a}$.

Hence $V^{-1}(\hat{a} \otimes t) = V^{-1}(1 \otimes at) = 1 \otimes V^{-1}at = 0$, by the second equation of (93) for $y = at$. Now we see from the decomposition (96) that the operator V^{-1} from the triple $\overline{\mathcal{T}}$ is uniquely determined by the requirements (93). Moreover we can check now that V^{-1} (if it exists) is a lift of $V^{-1} : \hat{Q} \to \widetilde{P}$ relative to $W(\mathbf{w}_0) : W(W(S)) \to W(S)$. In fact our proof of the uniqueness shows that $\pi^{-1}(\hat{Q})$ is generated by all elements of the form $\hat{\xi} \otimes y$, for $\hat{\xi} \in W(W(S))$ and $y \in \hat{Q}$ and of the form ${}^{\hat{V}}\hat{\xi} \otimes x$, for $x \in \widetilde{P}$. Since $W(\mathbf{w}_0)$ commutes with ^{F} and ^{V}, we see from (93) that V^{-1} is indeed a lift. It remains to show the existence of a V^{-1} as asserted in the proposition.

To prove the existence of V^{-1}, we define an ^{F}-linear operator V^{-1} on $\pi^{-1}(\hat{Q})$. On the first direct summand of (96) it will be defined by the second equation of (93), and on the second direct summand by the third equation of (93). On the last two direct summands of (96) we set V^{-1} equal to zero. We only have to check, that the last two equations of (93) hold with this definition. We will write down here only some parts of this routine calculation. Let us verify for example that the second equation of (93) holds for $y \in I_S\widetilde{T}$. We may assume that y is of the form $y =^V \eta t$, where $\eta \in W(S)$ and $t \in \widetilde{T}$. Then we have to decompose $\hat{\xi} \otimes^V \eta t$ according to the decomposition (93):

$$\begin{array}{c} \hat{\xi} \otimes^V \eta t \quad = \quad \triangle({}^V\eta) \cdot \hat{\xi} \otimes t \quad = \\ \left(\triangle\left({}^V\eta\right) - {}^{\hat{V}}\triangle(\eta)\right) \cdot \hat{\xi} \otimes t + {}^{\hat{V}}\triangle(\eta)\hat{\xi} \otimes t \end{array}$$

Here the first summand is in the third direct summand of (96) and the second summand is in the second direct summand of the decomposition (96). The definition of V^{-1} therefore gives:

$$\begin{aligned} V^{-1}\left(\hat{\xi} \otimes y\right) &= V^{-1}\left({}^{\hat{V}}\triangle(\eta) \cdot \hat{\xi} \otimes t\right) \\ &= V^{-1}\left({}^{\hat{V}}\left(\triangle(\eta)^{\hat{F}}\hat{\xi}\right) \otimes t\right) = \triangle(\eta)^{\hat{F}}\hat{\xi} \otimes Ft \\ &= {}^{\hat{F}}\hat{\xi} \otimes \eta F t = {}^{\hat{F}}\hat{\xi} \otimes V^{-1}\left({}^V\eta t\right) = {}^{\hat{F}}\hat{\xi} \otimes V^{-1}y \end{aligned}$$

Hence the second equation of (93) holds with the given definition of V^{-1} for $y \in I_S\widetilde{T}$. For $y \in \widetilde{L}$ this second equation is the definition of V^{-1} and for $y \in \mathfrak{a}\widetilde{T}$ the lemma 54 shows that both sides of the equation

$$V^{-1}\left({}^{\hat{F}}\hat{\xi} \otimes y\right) \quad = \quad \hat{\xi} \otimes Fy$$

are zero. Because we leave the verification of the third equation (93) to the reader we may write modulo the lemma 54: □

Let us now prove the lemma 54. The ideal $W(\mathfrak{a}) \subset W(S)$ is a pd-ideal, since it is contained in the kernel $\mathfrak{a} \oplus I_S$ of (89). One sees that $W(\mathfrak{a})$ inherits a pd-structure from this ideal. One checks that in logarithmic coordinates on $W(\mathfrak{a})$ this pd-structure has the form:

$$\alpha_p[a_0, a_1, \dots] = [\alpha_p(a_0), p^{(p-1)}\alpha_p(a_1), \dots, p^{i(p-1)}\alpha_p(a_i), \dots]$$

where $\alpha_p(a_i)$ for $a_i \in \mathfrak{a}$ denotes the given pd-structure on $\mathfrak{a}$.

On $W(\mathfrak{a})$ the operator F^n becomes divisible by p^n. We define an operator $\frac{1}{p^n}F^n$ on $W(\mathfrak{a})$ as follows:

$$\begin{aligned} \frac{1}{p^n}F^n : \qquad & W(\mathfrak{a}) \longrightarrow W(\mathfrak{a}) \\ & [a_0, a_1, a_2 \dots] \longmapsto [a_n, a_{n+1}, a_{n+2}, \dots] \end{aligned}$$

Since $W(\mathfrak{a}) \subset W(S)$ is a pd-ideal, we have the divided Witt polynomials

$$\hat{\mathbf{w}}'_n : W(W(\mathfrak{a})) \longrightarrow W(\mathfrak{a})$$

If $a \in \mathfrak{a} \subset W(\mathfrak{a})$ the element $\hat{a} \in \hat{\mathfrak{a}} \subset W(W(\mathfrak{a}))$ used in the lemma 54 is characterized by the following properties

$$\hat{\mathbf{w}}'_0(\hat{a}) = a, \quad \hat{\mathbf{w}}'_n(\hat{a}) = 0 \quad \text{for} \quad n > 0.$$

Therefore the lemma 54 follows from the more general fact:

Lemma 55. — *Let S be a $\mathbb{Z}_p$-algebra and $\mathfrak{a} \subset S$ be a pd-ideal. Then the canonical homomorphism*

$$\triangle : W(\mathfrak{a}) \longrightarrow W(W(\mathfrak{a}))$$

satisfies

$$\hat{\mathbf{w}}'_n\left(\triangle\left(\underline{a}\right)\right) = \frac{1}{p^n}\ {}^{F^n}\underline{a}, \quad \textit{for} \quad \underline{a} \in W(\mathfrak{a}), n \geq 0.$$

Proof. — One may assume that S is the pd-polynomial algebra in variables $a_0, a_1, \dots$ over $\mathbb{Z}_p$. Since this ring has no p-torsion the formula is clear from (91) □

Corollary 56. — *Under the assumptions of proposition 53 let $\varphi : W(R) \to S$ be a homomorphism of pd-thickenings. Then the triple $\mathcal{T} = (\tilde{P}, F, V^{-1})$ may be described as follows: Let δ be the composite of the homomorphisms*

$$\delta : W(R) \xrightarrow{\triangle} W(W(R)). \xrightarrow{W(\varphi)} W(S) \tag{97}$$

This is a ring homomorphism, which commutes with ^{F}.

We define $\tilde{P} = W(S) \otimes_{\delta, W(R)} P$. Then $\tilde{P}$ is a lifting of P with respect to the morphism $S \to R$. For the operator F on $\tilde{P}$ we take the ^{F}-linear extension of the operator F on P. Let $\hat{Q} \subset \tilde{P}$ be the inverse image of Q. Finally we define $V^{-1} : \hat{Q} \to \tilde{P}$ to be the unique ^{F}-linear homomorphism, which satisfies the following relations.

$$\begin{aligned} V^{-1}(w \otimes y) &= {}^F w \otimes V^{-1} y, && w \in W(S), y \in Q \\ V^{-1}({}^V w \otimes x) &= w \otimes Fx, && w \in W(S), x \in P \\ V^{-1}(a \otimes x) &= 0 && a \in \mathfrak{a} \subset W(S). \end{aligned} \tag{98}$$

In particular we obtain the following isomorphisms:

$$\begin{aligned} \mathcal{K}_{\mathcal{P}}(S) &\cong W(S) \otimes_{W(R)} \mathcal{K}_{\mathcal{P}}(R) \\ \mathcal{D}_{\mathcal{P}}(S) &\cong \ S \otimes_{W(R)} \mathcal{K}_{\mathcal{P}}(R). \end{aligned}$$

Proof. — We apply propositon 53 to the trivial pd-thickening $R \to R$, to obtain the triple $\bar{\mathcal{T}}$. Then we make base change with respect to $\varphi : W(R) \to S$. □

We will now see that the isomorphism of proposition 51 (compare (94)) is compatible with Frobenius and Verschiebung.

Let R be a ring such that $p \cdot R = 0$. For a display $\mathcal{P}$ over R we have defined Frobenius and Verschiebung.

$$\mathcal{F}r_{\mathcal{P}} : \mathcal{P} \longrightarrow \mathcal{P}^{(p)} \quad \mathrm{Ver}_{\mathcal{P}} : \mathcal{P}^{(p)} \longrightarrow \mathcal{P}$$

They induce morphisms of the corresponding Witt and Dieudonné crystals:

$$Fr_{\mathcal{D}_{\mathcal{P}}} : \mathcal{D}_{\mathcal{P}} \longrightarrow \mathcal{D}_{\mathcal{P}^{(p)}}, \quad Fr_{\mathcal{K}_{\mathcal{P}}} : \mathcal{K}_{\mathcal{P}} \longrightarrow \mathcal{K}_{\mathcal{P}^{(p)}} \tag{99}$$

$$\mathrm{Ver}_{\mathcal{D}_{\mathcal{P}}} : \mathcal{D}_{\mathcal{P}^{(p)}} \longrightarrow \mathcal{D}_{\mathcal{P}}, \quad \mathrm{Ver}_{\mathcal{K}_{\mathcal{P}}} : \mathcal{K}_{\mathcal{P}^{(p)}} \longrightarrow \mathcal{K}_{\mathcal{P}} \tag{100}$$

Let us make the morphisms more explicit. We set $\mathcal{P} = (P, Q, F, V^{-1})$. Let $S \to R$ be a pd-thickening, such that p is nilpotent in S. We denote by $\mathcal{T} = (\widetilde{P}, F, V^{-1})$ the unique $\mathcal{P}$-triple over S. The unique $\mathcal{P}^{(p)}$-triple over S is given as follows

$$\mathcal{T}^{(p)} = \left(W(S) \otimes_{F, W(S)} \widetilde{P}, F, V^{-1} \right),$$

where F and V^{-1} will now be defined:

$$F(\xi \otimes x) = {}^F \xi \otimes Fx, \quad \text{for} \quad \xi \in W(S), x \in \widetilde{P}.$$

The domain of definition of V^{-1} is the kernel $\hat{Q}^{(p)}$ of the canonical map

$$W(S) \otimes_{F, W(S)} \widetilde{P} \longrightarrow R \otimes_{\mathrm{Frob}, R} P/Q,$$

which is induced by $W(S) \xrightarrow{w_0} S \longrightarrow R$. The operator V^{-1} on $\hat{Q}^{(p)}$ is uniquely determined by the following formulas

$$\begin{aligned} V^{-1}(\xi \otimes y) &= {}^F\xi \otimes V^{-1}y, \quad \text{for} \quad \xi \in W(S), y \in \hat{Q} \\ V^{-1}\left({}^V\xi \otimes x\right) &= \xi \otimes Fx \quad , \qquad x \in \widetilde{P} \\ V^{-1}\left(\mathfrak{a} \otimes_{F,W(S)} \widetilde{P}\right) &= 0. \end{aligned} \tag{101}$$

Even though it makes the text long, we do not leave the verification of the existence of V^{-1} to the reader: We take a normal decomposition $\widetilde{P} = \widetilde{L} \oplus \widetilde{T}$. Then we obtain the decompositions

$$\hat{Q} = \widetilde{L} \oplus I_S\widetilde{T} \oplus \mathfrak{a}\widetilde{T}$$

$$\hat{Q}^{(p)} = W(S) \otimes_{F,W(S)} \widetilde{L} \oplus I_S \otimes_{F,W(S)} \widetilde{T} \oplus \mathfrak{a} \otimes_{F,W(S)} \widetilde{T}$$

We define the operator V^{-1} on $\hat{Q}^{(p)}$ by taking the first formula of (101) as a formula on the first direct summand, the second formula on the second direct summand and so on. Then we have to verify that V^{-1} defined on this way satisfies (101). To verify the first formula (101) it is enough to check the cases $y \in \widetilde{L}, y \in I_S\widetilde{T}$ and $y \in \mathfrak{a}\widetilde{T}$ separately. For $y \in \widetilde{L}$ the assertion is the definition of V^{-1} and for $y \in \mathfrak{a}\widetilde{T}$ both sides of the equation become zero. Therefore we may assume $y = {}^V\eta x, \quad \text{for} \quad \eta \in W(S)$ and $x \in \widetilde{T}$. We have

$$\xi \otimes {}^V\eta x \quad = \quad p\xi\eta \otimes x.$$

Now in the ring $W(\mathbb{Z}_p) = W(W(\mathbb{F}_p))$ we have the equation

$$p - [p, 0, 0 \cdots] = \triangle({}^V1) - [{}^V1, 0 \cdots 0] = {}^V\triangle 1 = {}^V1.$$

Since $\mathbb{Z}_p \to S$ is a pd-morphism the same equation holds in $W(S)$. We obtain

$$p\xi\eta \otimes x = \left([p, 0 \cdots 0] + {}^V1\right)\xi\eta \otimes x.$$

Since $[p, 0 \cdots 0]\xi\eta \otimes x \in \mathfrak{a} \otimes \widetilde{T}$ we obtain by the definition of V^{-1}

$$V^{-1}(p\xi\eta \otimes x) = V^{-1}\left({}^V1 \cdot \xi\eta \otimes x\right)$$

$$= V^{-1}\left({}^{VF}(\xi\eta) \otimes x\right) = {}^F(\xi\eta) \otimes Fx = {}^F\xi \otimes \eta Fx$$

$$= {}^F\xi \otimes V^{-1}\left({}^V\eta x\right).$$

This proves the assertion. The verification of the last two equations of (101) is done in the same way, but much easier.

Hence we have proved the existence of V^{-1}. It follows that $\mathcal{T}^{(p)}$ is a $\mathcal{P}^{(p)}$-triple.

To the triple $\mathcal{T} = (\widetilde{P}, F, V^{-1})$ there is by lemma 1.5 an associated $W(S)$-linear map

$$V^{\#} : \widetilde{P} \longrightarrow W(S) \otimes_{F,W(S)} \widetilde{P}, \tag{102}$$

which satisfies the relations

$$\begin{aligned} V^{\#}(wV^{-1}y) &= w \otimes y, \qquad \text{for} \quad y \in \hat{Q}, w \in W(S) \\ V^{\#}(wFx) &= p \cdot w \otimes x. \end{aligned}$$

Indeed, to conclude this from lemma 1.5 we complete $\mathcal{T}$ to a display $(\widetilde{P}, \widetilde{Q}, F, V^{-1})$ and note that $\hat{Q} = \widetilde{Q} + \mathfrak{a}\widetilde{P}$.

Then we claim that (102) induces a map of triples:

$$Fr_{\mathcal{T}} : \mathcal{T} \longrightarrow \mathcal{T}^{(p)} \tag{103}$$

We have to verify that the morphism (102) commutes with F and V^{-1}. Let us do the verification for V^{-1}. The assertion is the commutativity of the following diagram:

$$\begin{tikzcd} \hat{Q} \arrow[r, "V^{\#}"] \arrow[d, "V^{-1}"'] & \hat{Q}^{(p)} \subset W(S) \otimes_{F,W(S)} \widetilde{P} \arrow[d, "V^{-1}"] \\ \widetilde{P} \arrow[r, "V^{\#}"] & W(S) \otimes_{F,W(S)} \widetilde{P} \end{tikzcd}$$

We take any $y \in \hat{Q}$ and we write it in the form

$$y = \sum_{i=1}^{m} \xi_i V^{-1} z_i,$$

for $\xi_i \in W(S)$ and $z_i \in \hat{Q}$. Then we compute

$$V^{\#}(V^{-1}y) = 1 \otimes y$$

$$V^{-1}(V^{\#}y) = V^{-1}\left(\sum_{i=1}^{m} \xi_i \otimes z_i\right) = \sum_{i=1}^{m} {}^{F}\xi_i \otimes V^{-1} z_i = 1 \otimes y$$

We leave to the reader the verification that

$$F^{\#} : W(S) \otimes_{F,W(S)} \widetilde{P} \longrightarrow \widetilde{P}$$

induces a morphism of triples

$$\mathrm{Ver}_{\mathcal{T}} : \mathcal{T}^{(p)} \longrightarrow \mathcal{T}$$

Then $Fr_{\mathcal{T}}$ and $\mathrm{Ver}_{\mathcal{T}}$ are liftings of $Fr_{\mathcal{P}}$ and $\mathrm{Ver}_{\mathcal{P}}$ and may therefore be used to compute the Frobenius and the Verschiebung on the Witt crystal and the Dieudonné crystal:

Proposition 57. — *Let R be a ring, such that $p \cdot R = 0$. Let $\mathcal{P}$ be a display over R. We consider a $\mathcal{P}$-triple $\mathcal{T} = (\widetilde{P}, F, V^{-1})$ relative to a pd-thickening $S \to R$. Then the Frobenius morphism on the Witt crystal $Fr_{\mathcal{K}_{\mathcal{P}}}(S) : \mathcal{K}_{\mathcal{P}} \to \mathcal{K}_{\mathcal{P}^{(p)}}(S)$ is canonically identified with the map $V^{\#} : \widetilde{P} \to W(S) \otimes_{F,W(S)} \widetilde{P}$, and the Verschiebung morphism $\mathrm{Ver}_{\mathcal{K}_{\mathcal{P}}}(S) : \mathcal{K}_{\mathcal{P}^{(p)}}(S) \to \mathcal{K}_{\mathcal{P}}(S)$ is canonically identified with $F^{\#} : W(S) \otimes_{F,W(S)} \widetilde{P} \to \widetilde{P}$. The Frobenius and Verschiebung on the Dieudonné crystal are obtained by taking the tensor product with $S \otimes_{\mathbf{w}_0, W(S)}$.*

This being said we formulate a complement to the proposition 53.

Corollary 58. — *Let us assume that $p \cdot R = 0$. Then for any pd-extension $S \to R$ the isomorphism of the proposition 53:*

$$\mathcal{K}_{\mathcal{P}}(S) \xrightarrow{\sim} \mathcal{D}_{\mathcal{P}}(W(S))$$

is compatible with the Frobenius and the Verschiebung on these crystals.

Proof. — We will check this for the Frobenius. The commutativity of the following diagram is claimed:

$$\begin{tikzcd}
\mathcal{K}_{\mathcal{P}}(S) \arrow[r] \arrow[d, "Fr_{\mathcal{K}_{\mathcal{P}}}"'] & \mathcal{D}_{\mathcal{P}}(W(S)) \arrow[d, "Fr_{\mathcal{D}_{\mathcal{P}}}"] \\
\mathcal{K}_{\mathcal{P}^{(p)}}(S) \arrow[r] & \mathcal{D}_{\mathcal{P}^{(p)}}(W(S)).
\end{tikzcd}$$

Now we take a $\mathcal{P}$-triple $(\widetilde{P}, F, V^{-1})$ over S. Taking the proposition 57 into account, we may rewrite the last diagram as follows:

$$\begin{tikzcd}
\widetilde{P} \arrow[dd, "V^{\#}"'] & W(S) \otimes_{\mathbf{w}_0} (W(W(S)) \otimes_{\triangle, W(S)} \widetilde{P}) \arrow[l] \arrow[d, "1 \otimes V^{\#}"] \\
& W(S) \otimes_{\mathbf{w}_0} (W(W(S)) \otimes_{\hat{F}, W(W(S))} W(W(S)) \otimes_{\triangle, W(S)} \widetilde{P}) \arrow[d, equal] \\
W(S) \otimes_{F, W(S)} \widetilde{P} & W(S) \otimes_{\mathbf{w}_0} (W(W(S)) \otimes_{\triangle, W(S)} W(S) \otimes_{F, W(S)} \widetilde{P}) \arrow[l]
\end{tikzcd}$$

It is enough to check the commutativity of this diagram on elements of the form $1 \otimes V^{-1}(\hat{\xi} \otimes y), \hat{\xi} \in W(W(S)) y \in \hat{Q}$ and $V^{-1}({}^{\hat{V}}\hat{\xi} \otimes x), x \in \widetilde{P}$. This is easy. □

We will now study the functor which associates to a display its Dieudonné crystal over a base R of characteristic p. In this case the Dieudonné crystal is equipped with the structure of a filtered F-crystal. We will prove that the resulting functor from displays to filtered F-crystals is almost fully faithful.

Let R be a ring, such that $p \cdot R = 0$, and let $\mathcal{P}$ be a display over R. The inverse image of the Witt crystal $\mathcal{K}_{\mathcal{P}}$ by the Frobenius morphism $\mathrm{Frob} : R \to R$ may be identified with $\mathcal{K}_{\mathcal{P}^{(p)}}$. To see this we look at the commutative diagram:

$$\begin{tikzcd}
W(S) \arrow[r, "F"] \arrow[d] & W(S) \arrow[d] \\
R \arrow[r, "\mathrm{Frob}"] & R
\end{tikzcd}$$

The vertical map is a pd-thickening by (89) and ^{F} is compatible with the pd-structure. This diagram tells us ([BO] Exercise 6.5), that

$$\mathrm{Frob}^* \mathcal{K}_{\mathcal{P}}(W(S)) = W(W(S)) \otimes_{W(F), W(W(S))} \mathcal{K}_{\mathcal{P}}(W(S)).$$

The pd-morphism $w_0 : W(S) \to S$ gives an isomorphism

$$W(S) \otimes_{W(w_0), W(W(S))} \mathrm{Frob}^* \mathcal{K}_{\mathcal{P}}(W(S)) = \mathrm{Frob}^* \mathcal{K}_{\mathcal{P}}(S)$$

Combining the last two equations we get as desired identification:

$$\text{Frob}^* \mathcal{K}_{\mathcal{P}}(S) = W(S) \otimes_{F,W(S)} \mathcal{K}_{\mathcal{P}}(S) = \mathcal{K}_{\mathcal{P}^{(p)}}(S). \tag{104}$$

From this we also deduce:

$$\text{Frob}^* \mathcal{D}_{\mathcal{P}}(S) = \mathcal{D}_{\mathcal{P}^{(p)}}(S)$$

Remark: This computation of $\text{Frob}^* \mathcal{D}_{\mathcal{P}}$ may be carried out inside the nilpotent crystalline site, if $p \neq 2$. The point is that we need that $W(S) \to R$ is a topological nilpotent pd-thickening, if S is a nilpotent pd-thickening. The result is the same.

Definition 59. — *Let X be a scheme, such that $p \cdot \mathcal{O}_X = 0$. Let us denote by* $\text{Frob} : X \to X$ *the absolute Frobenius morphism. A filtered F-crystal on X is a triple $(\mathcal{D}, G, Fr)$, where $\mathcal{D}$ is a crystal in $\mathcal{O}_X^{\text{crys}}$-modules $G \subset \mathcal{D}_X$ is an $\mathcal{O}_X$-submodule of the $\mathcal{O}_X$-module $\mathcal{D}_X$ associated to $\mathcal{D}$, such that G is locally a direct summand. Fr is a morphism of crystals*

$$Fr : \mathcal{D} \longrightarrow \text{Frob}^* \mathcal{D} = \mathcal{D}^{(p)}.$$

We also define a filtered F-Witt crystal as a triple $(\mathcal{K}, Q, Fr)$, where $\mathcal{K}$ is a crystal in $W(\mathcal{O}_X^{\text{crys}})$-modules, $Q \subset \mathcal{K}_X$ is a $W(\mathcal{O}_X)$-submodule, such that $I_X\mathcal{K}_X \subset Q$ and $Q/I_X\mathcal{K}_X \subset \mathcal{O}_X \otimes_{\mathbf{w}_0, W(\mathcal{O}_X)} \mathcal{K}_X$ is locally a direct summand as $\mathcal{O}_X$-module. Fr is a morphism of $W(\mathcal{O}_X^{\text{crys}})$-crystals

$$Fr : \mathcal{K} \longrightarrow \mathcal{K}^{(p)} = \text{Frob}^* \mathcal{K}.$$

With the same definition we may also consider fitered F-crystals (resp. F-Witt crystals), if $p \neq 2$.

The same argument which leads to (104) shows that for any pd-thickening $T \leftarrow U \hookrightarrow X$ there is a a canonical isomorphism:

$$\mathcal{K}^{(p)}(T) = W(\mathcal{O}_T) \otimes_{F,W(\mathcal{O}_T)} \mathcal{K}(T)$$

From a filtered F-Witt crystal we get a filtered F-crystal by taking the tensor product $\mathcal{O}_X^{\text{crys}} \otimes_{W(\mathcal{O}_X^{\text{crys}})}$. Let R be a ring such that $p \cdot R = 0$ and $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R as above. Then we give the Witt crystal $\mathcal{K}_{\mathcal{P}}$ the structure of a filtered F-Witt crystal, by taking the obvious Q, and by defining $Fr : \mathcal{K}_{\mathcal{P}} \to \mathcal{K}_{\mathcal{P}}{}^{(p)}$ as the map (99). By taking the tensor product $\mathcal{O}_X^{\text{crys}} \otimes_{\mathbf{w}_0, W(\mathcal{O}_X^{\text{crys}})}$ we also equip the Dieudonné crystal $\mathcal{D}_{\mathcal{P}}$ with the structure of a filtered F crystal.

We will say that a pd-thickening (resp. nilpotent pd-thickening) $S \to R$ is liftable, if there is a morphism of topological pd-thickenings (resp. topological nilpotent pd-thickenings) $S' \to S$ of the ring R, such that S' is a torsionfree p-adic ring. We prove that the functors $\mathcal{K}$ and $\mathcal{D}$ are "fully faithful" in the following weak sense:

Proposition 60. — *Let R be a $\mathbb{F}_p$-algebra. Assume that there exists a topological pd-thickening $S \to R$, such that S is a torsionfree p-adic ring.*

Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be displays over R. We denote the filtered F-crystal associated to $\mathcal{P}_i$ by $(\mathcal{D}_i, G_i, Fr_i)$ for $i = 1, 2$ and by $(\mathcal{K}_i, Q_i, Fr_i)$ the filtered F-Witt crystal.

Let $\alpha : (\mathcal{D}_1, G_1, Fr_1) \to (\mathcal{D}_2, G_2, Fr_2)$ be a morphism of filtered F-crystals. Then there is a morphism $\varphi : \mathcal{P}_1 \to \mathcal{P}_2$ of displays, such that the morphism of filtered

F-crystals $\mathcal{D}(\varphi) : (\mathcal{D}_1, G_1, Fr_1) \to (\mathcal{D}_2, G_2, Fr_2)$, which is associated to φ has the following property:

For any liftable pd-thickening $S' \to R$, we have

$$\alpha_{S'} = \mathcal{D}(\varphi)_{S'}. \tag{105}$$

The similar statement for the filtered F-Witt crystals is also true.

***Remark*:** The result will later be used to show that the functor BT of the introduction is fully faithful under the assumptions of the proposition. In fact we will use the following variant of the proposition: Assume that $p \neq 2$ and that we are given a topological nilpotent pd-thickening, such that S is a torsionfree p-adic ring. Then it is enough to have a morphism α on the nilpotent crystalline site to conclude the existence of φ, such that for any liftable nilpotent pd-thickening $S' \to R$ the equality (105) holds.

Proof. — First we prove the result for the filtered F-Witt crystals. Let $(\widetilde{P}_i, F, V^{-1})$ be the $\mathcal{P}_i$-triple over S for $i = 1, 2$. We may identify $\mathcal{K}_i(S)$ with $\widetilde{P}_i$ and $Fr_i(S)$ with the morphism $V^{\#} : \widetilde{P}_i \to W(S) \otimes_{F,W(S)} \widetilde{P}_i$. Then we may regard α_S as a homomorphism of $W(S)$-modules

$$\alpha_S : \widetilde{P}_1 \longrightarrow \widetilde{P}_2,$$

which commutes with $V^{\#}$:

$$V^{\#}\alpha_S = (1 \otimes \alpha_S)V^{\#}. \tag{106}$$

Since α_R respects the filtrations Q_1 and Q_2, we get

$$\alpha_S(\hat{Q}_1) \subset \hat{Q}_2.$$

Because the ring S is torsionfree we conclude from the equations $F^{\#} \cdot V^{\#} = p$ and $V^{\#} \cdot F^{\#} = p$, which hold for any display, that the maps $F^{\#} : W(S) \otimes_{F,W(S)} \widetilde{P}_i \to \widetilde{P}_i$ and $V^{\#} : \widetilde{P}_i \to W(S) \otimes_{F,W(S)} \widetilde{P}_i$ are injective. Hence the equation

$$F^{\#}(1 \otimes \alpha_S) = \alpha_S F^{\#} \tag{107}$$

is verified by multiplying it from the left by $V^{\#}$ and using (106). We conclude that α_S commutes with F. Finally α_S also commutes with V^{-1} because we have $pV^{-1} = F$ on $\hat{Q}$.

We see from the following commutative diagram

$$\begin{array}{ccc} \widetilde{P}_1 & \xrightarrow{\alpha_S} & \widetilde{P}_2 \\ \downarrow & & \downarrow \\ P_1 & \xrightarrow{\alpha_R} & P_2 \end{array},$$

that α_R induces a homomorphism of displays and that α_S is the unique lifting of α_R to a morphism of triples. This proves the proposition in the case of filtered F-Witt crystals. Finally a morphism $\beta : \mathcal{D}_1 \to \mathcal{D}_2$ of the filtered F-crystals also provides a morphism $\alpha : \mathcal{K}_1 \to \mathcal{K}_2$ of the Witt crystals by the proposition (53), which commutes with Fr by the corollary (58). It is clear that α also respects the filtrations. Hence the assertion of the theorem concerning filtered F-crystals is reduced to the case of filtered F-Witt crystals. □

2.4. Isodisplays. — Let R be a ring and let $\mathfrak{a} \subset R$ be an ideal, such that p is nilpotent in $R/\mathfrak{a}$. We assume that R is complete and separated in the $\mathfrak{a}-$adic topology. In this section we will consider displays over the topological ring R with its $\mathfrak{a}$-adic topology (see definition 13).

We consider the ring $W_{\mathbb{Q}}(R) = W(R) \otimes_{\mathbb{Z}} \mathbb{Q}$. The Frobenius homomorphism ^{F} and the Verschiebung ^{V} extend from $W(R)$ to $W_{\mathbb{Q}}(R)$.

Definition 61. — *An isodisplay over R is a pair $(\mathcal{I}, F)$, where $\mathcal{I}$ is a finitely generated projective $W_{\mathbb{Q}}(R)-$module and*

$$F : \mathcal{I} \longrightarrow \mathcal{I}$$

is an ${}^F-$linear isomorphism.

Let us assume for a moment that R is torsionfree (as an abelian group). Then we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_R & \longrightarrow & W(R) & \longrightarrow & R & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I_R \otimes \mathbb{Q} & \longrightarrow & W_{\mathbb{Q}}(R) & \longrightarrow & R \otimes \mathbb{Q} & \longrightarrow & 0, \end{array}$$

where the vertical maps are injective. In particular $W(R) \cap I_R \otimes \mathbb{Q} = I_R$.

Definition 62. — *Let R be torsionfree. A filtered isodisplay over R is a triple $(\mathcal{I}, E, F)$, where $(\mathcal{I}, F)$ is an isodisplay over R and $E \subset \mathcal{I}$ is a $W_{\mathbb{Q}}(R)$ submodule, such that*

(i) $I_R\mathcal{I} \subset E \subset \mathcal{I}$
(ii) $E/I_R\mathcal{I} \subset \mathcal{I}/I_R\mathcal{I}$ *is a direct summand as $R \otimes \mathbb{Q}-$module.*

Example 63: Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a 3n-display over R. Obviously F extends to an ${}^F-$linear homomorphism $F : P \otimes \mathbb{Q} \to P \otimes \mathbb{Q}$.

The pair $(P \otimes \mathbb{Q}, F)$ is an isodisplay. Indeed, to see that F is an ${}^F-$linear isomorphism we choose a normal decomposition $P = L \oplus T$. We present $F : P \to P$ as a composite of two morphisms

$$L \oplus T \xrightarrow{p\,\mathrm{id}_L \oplus \mathrm{id}_T} L \oplus T \xrightarrow{V^{-1} \oplus F} L \oplus T.$$

The last morphism is already an ${}^F-$linear isomorphism and the first morphism becomes an ${}^F-$linear isomorphism, if we tensor by $\mathbb{Q}$.

Example 64: If R is torsionfree, we get a filtered isodisplay $(P \otimes \mathbb{Q}, Q \otimes \mathbb{Q}, F)$.

Example 65: Let $\mathfrak{a} \subset R$ be an ideal, such that R is complete and separated in the $\mathfrak{a}$-adic topology. We assume that $pR \subset \mathfrak{a} \subset R$.

Let k be a perfect field, such that $k \subset R/\mathfrak{a}$. Then we find by the universality of Witt vectors a commutative diagram

$$\begin{array}{ccc} W(k) & \xrightarrow{\rho} & R \\ \downarrow & & \downarrow \\ k & \longrightarrow & R/\mathfrak{a} \end{array} \tag{108}$$

The map $\delta : W(k) \xrightarrow{\triangle} W(W(k)) \xrightarrow{W(\rho)} W(R)$ commutes with ^{F}. Hence if we are given an isodisplay (N, F) over k, we obtain an isodisplay $(\mathcal{I}, F)$ over R if we set

$$\mathcal{I} = W_{\mathbb{Q}}(R) \otimes_{\delta, W_{\mathbb{Q}}(k)} N, \quad F(\xi \otimes x) = {}^F\xi \otimes Fx.$$

We will write $(\mathcal{I}, F) = W_{\mathbb{Q}}(R) \otimes_{\delta, W_{\mathbb{Q}}(k)} (N, F)$.

Let $Qisg_R$ be the category of displays over R up to isogeny. The objects of this category are the displays over R and the homomorphisms are $\mathrm{Hom}_{Qisg}(\mathcal{P}, \mathcal{P}') = \mathrm{Hom}(\mathcal{P}, \mathcal{P}') \otimes \mathbb{Q}$. We note that the natural functor $(\mathrm{Displays})_R \to Qisg_R$ is by corollary 41 faithful if the nilradical of R/pR is nilpotent. It is clear that the construction of example 2.22 provides a functor:

$$Qisg_R \longrightarrow (\mathrm{Isodisplays})_R \tag{109}$$

Proposition 66. — *If p is nilpotent in R, the functor (109) is fully faithful*

Proof. — The faithfulness means that for any morphism of displays $\alpha : \mathcal{P} \to \mathcal{P}'$, such that the induced map $\alpha_{\mathbb{Q}} : P_{\mathbb{Q}} \to P'_{\mathbb{Q}}$ is zero, there is a number N, such that $p^N \alpha = 0$. This is obvious. To prove that the functor is full, we start with a homomorphism of isodisplays $\alpha_0 : (P_{\mathbb{Q}}, F) \to (P'_{\mathbb{Q}}, F)$. Let $\mathrm{Im}P'$ be the image of the map $P' \to P'_{\mathbb{Q}}$. Since we are allowed to multiply α_0 with a power of p, we may assume that α_0 maps $\mathrm{Im}P$ to $\mathrm{Im}P'$. Since P is projective we find a commutative diagram:

$$\begin{array}{ccc} P_{\mathbb{Q}} & \xrightarrow{\alpha_0} & P'_{\mathbb{Q}} \\ \uparrow & & \uparrow \\ P & \xrightarrow{\alpha} & P' \end{array} \tag{110}$$

Since $F\alpha - \alpha F$ is by assumption in the kernel of $P' \to P'_{\mathbb{Q}}$, we find a number N, such that $p^N(F\alpha - \alpha F) = 0$. Multiplying α and α_0 by p^N, we may assume without loss of generality that α commutes with F. Moreover, since p is nilpotent in $P'/I_R P'$ we may assume that $\alpha(P) \subset I_R P'$ and hence a fortiori that $\alpha(Q) \subset Q'$. Finally since $pV^{-1} = F$ on Q it follows that $p\alpha$ commutes with V^{-1}. Therefore we have obtained a morphism of displays. □

Let us now consider the case of a torsionfree ring R. Then we have an obvious functor

$$Qisg_R \longrightarrow (\text{filtered Isodisplays})_R. \tag{111}$$

Proposition 67. — *Let R be torsiofree. Then the functor (111) is fully faithful.*

Proof. — Again it is obvious that this functor is faithful. We prove that the functor is full.

Let $\mathcal{P}$ and $\mathcal{P}'$ be displays over R. Assume that we are given a morphism of the corresponding filtered isodisplays

$$\alpha_0 : (P_{\mathbb{Q}}, Q_{\mathbb{Q}}, F) \longrightarrow (P'_{\mathbb{Q}}, Q'_{\mathbb{Q}}, F).$$

We have to show that α_0, if we replace it possibly by $p^N\alpha_0$, is induced by a homomorphism

$$\alpha : (P, Q, F, V^{-1}) \longrightarrow (P', Q', F, V^{-1}).$$

The proof of proposition 66 works except for the point where the inclusion $\alpha(Q) \subset Q'$ is proved. But this time we already know that $\alpha(Q) \subset Q'_{\mathbb{Q}}$. We choose finitely many elements $x_1, \ldots, x_M \in Q$, whose images generate the $R-$module $Q/I_R P$. Since it suffices to show that $\alpha(x_i) \in Q'$, if we possibly multiply α by p^N we are done. □

Definition 68. — *An isodisplay (resp. filtered isodisplay) is called effective, if it is in the image of the functor (109) (resp. (111)).*

Proposition 69. — *Let R be torsionfree. Let $\mathfrak{a} \subset R$ be an ideal, such that there exists a number N, such that $\mathfrak{a}^N \subset pR$ and $p^N \in \mathfrak{a}$. Let $(\mathcal{I}_1, F)$ and $(\mathcal{I}_2, F)$ be effective isodisplays over R. Then any homomorphism $\overline{\alpha}_0 : (\mathcal{I}_1, F)_{R/\mathfrak{a}} \to (\mathcal{I}_2, F)_{R/\mathfrak{a}}$ lifts uniquely to a homomorphism $\alpha_0 : (\mathcal{I}_1, F) \to (\mathcal{I}_2, F)$.*

Proof. — We choose displays $\mathcal{P}_1$ and $\mathcal{P}_2$ over R together with isomorphisms of isodisplays $(P_{i,\mathbb{Q}}, F) \simeq (\mathcal{I}_i, F)$ for $i = 1, 2$. By the proposition 66 we may assume that $\overline{\alpha}_0$ is induced by a morphism of displays $\overline{\alpha} : \mathcal{P}_{1,R/\mathfrak{a}} \to \mathcal{P}_{2,R/\mathfrak{a}}$. Indeed, to prove the proposition it is allowed to multiply $\overline{\alpha}_0$ by a power of p.

Next we remark, that for the proof we may assume that $\mathfrak{a} = p \cdot R$. Indeed, let $S \to T$ be a surjection of rings with nilpotent kernel and such that p is nilpotent in S. Then the induced map $W_{\mathbb{Q}}(S) \to W_{\mathbb{Q}}(T)$ is an isomorphism and hence an isodisplay on S is the same as an isodisplay on T. Applying this remark to the diagram

$$R/\mathfrak{a}R \longrightarrow R/\mathfrak{a} + pR \longleftarrow R/pR,$$

we reduce our assertion to the case, where $\mathfrak{a} = pR$.

Since $pR \subset R$ is equipped canonically with divided powers the morphism of displays $\overline{\alpha} : \mathcal{P}_{1,R/pR} \to \mathcal{P}_{2,R/pR}$ lifts by theorem 46 uniquely to a morphism of triples $(P_1, F, V^{-1}) \to (P_2, F, V^{-1})$ which gives a morphism of isodisplays $\alpha_0 : (P_{1,\mathbb{Q}}, F) \to (P_{2,\mathbb{Q}}, F)$. This shows the existence of α_0.

To prove the uniqueness we start with any lifting $\alpha_0 : (\mathcal{I}_1, F) \to (\mathcal{I}_2, F)$ of $\overline{\alpha}_0$. Since it is enough to show the uniqueness assertion for $p^N\overline{\alpha}_0$ and some number N, we may assume that $\alpha_0(P_1) \subset P_2$. Since P_1 and P_2 are torsionfree as abelian groups it follows that α_0 commutes with F and with V^{-1}, which is defined on $\hat{Q}_1 \subset P_1$ resp. $\hat{Q}_2 \subset P_2$ taken with respect to $R \to R/pR$. Hence α_0 is a morphism of triples $(P_1, F, V^{-1}) \to (P_2, F, V^{-1})$, which is therefore uniquely determined by the morphism of displays $\overline{\alpha} : \mathcal{P}_{1,R/pR} \to \mathcal{P}_{2,R/pR}$. □

We will now explain the period map. Let us fix an effective isodisplay (N,F) over a perfect field k. We consider the diagram (108) and make the additional assumption that $\mathfrak{a}^t \subset pR$ for some number t. We consider the category $\mathcal{M}(R)$ of pairs $(\mathcal{P},r)$, where $\mathcal{P} \in Qisg_R$ and r is an isomorphism $r : \mathcal{P}_{R/\mathfrak{a},\mathbb{Q}} \to (N,F)_{R/\mathfrak{a}}$ in the category of isodisplays over $R/\mathfrak{a}$. By the proposition 69 any homomorphism between pairs $(\mathcal{P},r)$ is an isomorphism and there is at most one isomorphism between two pairs.

The period map will be injection from the set of isomorphism classes of pairs $(\mathcal{P},r)$ to the set $\mathrm{Grass}_{W_{\mathbb{Q}}(k)}N(R\otimes\mathbb{Q})$, where $\mathrm{Grass}_{W_{\mathbb{Q}}(k)}N$ is the Grassmann variety of direct summands of the $W_{\mathbb{Q}}(k)-$module N.

The definition is as follows. The lemma below will show that the isodisplay $W_{\mathbb{Q}}(R) \otimes_{\delta,W_{\mathbb{Q}}(k)} (N,F)$ is effective. Hence by the proposition 69 there is a unique isomorphism of isodisplays, which lifts r

$$\tilde{r} : (P_{\mathbb{Q}},F) \longrightarrow W_{\mathbb{Q}}(R) \otimes_{\delta,W_{\mathbb{Q}}(k)} (N,F).$$

The map

$$W_{\mathbb{Q}}(R) \otimes_{\delta,W_{\mathbb{Q}}(k)} N \xrightarrow{\tilde{r}^{-1}} P_{\mathbb{Q}} \longrightarrow P_{\mathbb{Q}}/Q_{\mathbb{Q}}$$

factors through the map induced by $\mathbf{w}_0$

$$W_{\mathbb{Q}}(R) \otimes_{\delta,W_{\mathbb{Q}}(k)} N \longrightarrow R_{\mathbb{Q}} \otimes_{\delta,W_{\mathbb{Q}}(k)} N.$$

Hence we obtain the desired period:

$$R_{\mathbb{Q}} \otimes_{\delta,W_{\mathbb{Q}}(k)} N \twoheadrightarrow P_{\mathbb{Q}}/Q_{\mathbb{Q}} \tag{112}$$

Hence if $\mathrm{Iso}\,\mathcal{M}(R)$ denotes the set of isomorphism classes in $\mathcal{M}(R)$ we have defined a map

$$\mathrm{Iso}\,\mathcal{M}(R) \longrightarrow \quad \mathrm{Grass}_{W_{\mathbb{Q}}(k)}N(R_{\mathbb{Q}}).$$

This map is injective by the proposition 67.

Now we prove the missing lemma.

Lemma 70. — *Let (N,F) be an effective isodisplay over a perfect field k (i.e. the slopes are in the interval [0,1]). Then in the situation of the diagram (108) the isodisplay $W_{\mathbb{Q}}(R) \otimes_{\delta,W_{\mathbb{Q}}(k)} (N,F)$ is effective.*

Proof. — One can restrict to the case $R = W(k)$ and $\rho = \mathrm{id}$. Indeed, if we know in the general situation that $W_{\mathbb{Q}}(W(k)) \otimes_{\triangle,W_{\mathbb{Q}}(k)} (N,F)$ is the isocrystal of a display $\mathcal{P}_0$, then $\rho_*\mathcal{P}_0$ is a display with isodisplay $W_{\mathbb{Q}}(R) \otimes_{\delta,W_{\mathbb{Q}}(k)} (N,F)$. In the situation $\rho = \mathrm{id}$ let$(M,\overline{Q},F,V^{-1})$ be a display with the isodisplay (N,F). Then the associated triple with respect to the pd-thickening $W(k) \to k$ is the form $(W(W(k)) \otimes_{\triangle,W(k)} M,F,V^{-1})$, where V^{-1} is given by (93). This triple gives the desired display if we take some lift of the Hodge-filtration of M/pM to M. The isodisplay of this display is $(W_{\mathbb{Q}}(W(k)) \otimes_{\triangle,W_{\mathbb{Q}}(k)} N,F)$. $\square$

Finally we want to give an explicit formula for the map (112). The map $\tilde{r}^{-1}$ is uniquely determined by the map:

$$\rho : N \longrightarrow P_{\mathbb{Q}}, \tag{113}$$

which is given by $\rho(m) = \tilde{r}^{-1}(1 \otimes m)$, for $m \in N$. This map ρ may be characterized by the following properties:

(i) ρ is equivariant with respect to the ring homomorphism $\delta : W_{\mathbb{Q}}(k) \to W_{\mathbb{Q}}(R)$.

(ii) $\rho(Fm) = F\rho(m)$, for $m \in N$

(iii) The following diagram is commutative:

$$\begin{tikzcd} P_{\mathbb{Q}} \arrow[r] & W_{\mathbb{Q}}(R/\mathfrak{a}) \otimes_{W_{\mathbb{Q}}(k)} N \\ & N \arrow[u] \arrow[ul, "\rho"'] \end{tikzcd} \tag{114}$$

We equip $P_{\mathbb{Q}}$ with the p-adic topology, i.e. with the linear topology, which has as a fundamental system of neighbourhoods of zero the subgroups p^iP. Because $W(R)$ is a p-adic ring, P is complete for this linear topology.

Proposition 71. — *Let $\rho_0 : N \to P$ be any δ-equivariant homomorphism, which makes the diagram (114) commutative. Then the map ρ is given by the following p-adic limit:*

$$\rho = \lim_{i \to \infty} F^i \rho_0 F^{-i}.$$

Proof. — We use ρ to identify $P_{\mathbb{Q}}$ with $W_{\mathbb{Q}}(R) \otimes_{\delta, W_{\mathbb{Q}}(k)} N$, i.e. the map ρ becomes $m \mapsto 1 \otimes m$, for $m \in N$. We write $\rho_0 = \rho + \alpha$. Clearly it is enough to show that:

$$\lim_{i \to \infty} F^i \alpha F^{-i}(m) = 0, \quad \text{for } m \in N. \tag{115}$$

Since ρ and ρ_0 make the diagram (114) commutative, we have $\alpha(N) \subset W_{\mathbb{Q}}(\mathfrak{a}) \otimes_{\delta, W_{\mathbb{Q}}(k)} N$. We note that $W_{\mathbb{Q}}(\mathfrak{a}) = W_{\mathbb{Q}}(pR)$.

We choose a $W(k)$-lattice $M \subset N$, which has a $W(k)-$module decomposition $M = \oplus M_j$, and such that there exists nonnegative integers $s, r_j \in \mathbb{Z}$ with $F^s M_j = p^{r_j} M_j$. We take an integer a, such that

$$\alpha(M) \subset p^a W(pR) \otimes_{\delta, W(k)} M.$$

It suffices to prove (115) for elements $m \in M_j$. We compute for any number u:

$$F^{us}\alpha(F^{-us}m) \in p^{-ur_j} F^{us}\alpha(M_j) \subset p^{a-ur_j} F^{us}(W(pR) \otimes_{\delta, W(k)} M). \tag{116}$$

But using the logarithmic coordinates for the pd-ideal pR we find:

$${}^{F}W(pR) = W(p^2R) = pW(pR).$$

This shows that the right hand side of (116) is included in

$$p^{a-ur_j+us} W(pR) \otimes_{\delta, W(k)} M.$$

Since N is an effective isodisplay we conclude $s > r_j$ for each j. This proves that $F^{us}\alpha F^{-us}(m)$ converges to zero if u goes to ∞.

More generally we can consider the limit (115), where i runs through a sequence $i = us + q$ for some fixed number q. By the same argument we obtain that this limit is zero too. $\square$

2.5. Lifting homomorphisms. — Consider a pd-thickening $S \to R$ with kernel $\mathfrak{a}$. We assume that p is nilpotent in S.

We consider two displays $\mathcal{P}_i = (P_i, Q_i, F, V^{-1})$ for $i = 1, 2$ over S. The base change to R will be denoted by $\overline{\mathcal{P}}_i = \overline{\mathcal{P}}_{i,R} = (\overline{P}_i, \overline{Q}_i, F, V^{-1})$. Let $\overline{\varphi} : \overline{\mathcal{P}}_1 \to \overline{\mathcal{P}}_2$ be a morphism of displays. It lifts to a morphism of triples:

$$\varphi : (P_1, F, V^{-1}) \longrightarrow (P_2, F, V^{-1}) \tag{117}$$

We consider the induced homomorphism:

$$\operatorname{Obst} \overline{\varphi} : Q_1/I_S P_1 \hookrightarrow P_1/I_S P_1 \xrightarrow{\varphi} P_2/I_S P_2 \longrightarrow P_2/Q_2$$

This map is zero modulo $\mathfrak{a}$, because $\overline{\varphi}(\overline{Q}_1) \subset \overline{Q}_2$. Hence we obtain a map:

$$\operatorname{Obst} \overline{\varphi} : Q_1/I_S P_1 \to \mathfrak{a} \otimes_S P_2/Q_2 \tag{118}$$

Clearly this map is zero, iff $\overline{\varphi}$ lifts to a morphism of displays $\mathcal{P}_1 \to \mathcal{P}_2$

Definition 72. — *The map* $\operatorname{Obst} \overline{\varphi}$ *above (118) is called the obstruction to lift* $\overline{\varphi}$ *to* S.

This depends on the divided powers on $\mathfrak{a}$ by the definition of φ.

The obstruction has the following functorial property: Assume we are given a morphism $\alpha : \mathcal{P}_2 \to \mathcal{P}_3$ of displays over S. Let $\overline{\alpha} : \overline{\mathcal{P}}_2 \to \overline{\mathcal{P}}_3$ be its reduction over R. Then $\operatorname{Obst} \overline{\alpha}\overline{\phi}$ is the composite of the following maps:

$$Q_1/I_S P_1 \xrightarrow{\operatorname{Obst} \overline{\varphi}} \mathfrak{a} \otimes_S P_2/Q_2 \xrightarrow{1 \otimes \alpha} \mathfrak{a} \otimes_S P_3/Q_3$$

We will denote this fact by:

$$\operatorname{Obst} \bar{\alpha}\bar{\varphi} = \alpha \operatorname{Obst} \overline{\varphi} \tag{119}$$

In the case $\mathfrak{a}^2 = 0$ we have an isomorphism $\mathfrak{a} \otimes_S P_2/Q_2 \cong \mathfrak{a} \otimes_R \overline{P}_2/\overline{Q}_2$. Hence the obstruction may be considered as a map:

$$\operatorname{Obst} \overline{\varphi} : \overline{Q}_1/I_R \overline{P}_1 \to \mathfrak{a} \otimes_R \overline{P}_2/\overline{Q}_2 \tag{120}$$

In this case the equation (119) simplifies:

$$\operatorname{Obst} \bar{\alpha}\bar{\varphi} = \bar{\alpha} \operatorname{Obst} \bar{\varphi} \tag{121}$$

Let S be a ring, such that $p \cdot S = 0$ for our fixed prime number p. Let $S \to R$ be a surjective ring homomorphism with kernel $\mathfrak{a}$. We assume that $\mathfrak{a}^p = 0$. In this section we will use the trivial divided powers on $\mathfrak{a}$, i.e. $\alpha_p(a) = 0$ for $a \in \mathfrak{a}$.

Let us consider a third ring $\widetilde{S}$, such that $p \cdot \widetilde{S} = 0$. Let $\widetilde{S} \to S$ be a surjection with kernel $\mathfrak{b}$, such that $\mathfrak{b}^p = 0$. Again we equip $\mathfrak{b}$ with the trivial divided powers.

Assume we are given liftings $\widetilde{\mathcal{P}}_i$ over $\widetilde{S}$ of the displays $\mathcal{P}_i$ over S for $i = 1, 2$. The morphism $p\overline{\varphi} : \overline{\mathcal{P}}_1 \to \overline{\mathcal{P}}_2$ lifts to the morphism $p\varphi : \mathcal{P}_1 \to \mathcal{P}_2$ of displays. Hence we obtain an obstruction to lift $p\varphi$ to a homomorphism of displays $\widetilde{\mathcal{P}}_1 \to \widetilde{\mathcal{P}}_2$:

$$\operatorname{Obst}(p\varphi) : \widetilde{Q}_1/I_S \widetilde{P}_1 \longrightarrow \widetilde{P}_2/\widetilde{Q}_2.$$

We will compute this obstruction in terms of $\mathrm{Obst}\,\overline{\varphi}$. For this we need to define two further maps: The operator V^{-1} on $\widetilde{P}_1$ induces a surjection

$$(V^{-1})^{\#} : \widetilde{S} \otimes_{\mathrm{Frob},\widetilde{S}} \widetilde{Q}_1/I_{\widetilde{S}}\widetilde{P}_1 \longrightarrow \widetilde{P}_1/I_{\widetilde{S}}\widetilde{P}_1 + W(\widetilde{S})F\widetilde{P}_1. \tag{122}$$

Here we denote by Frob the Frobenius endomorphism of $\widetilde{S}$. The map (122) is an isomorphism. To see this it is enough to verify that we have on the right hand side a projective $\widetilde{S}-$module of the same rank as on the left hand side. Let $\widetilde{P} = \widetilde{L} \oplus \widetilde{T}$ be a normal decomposition. Because $p\widetilde{S} = 0$, we have $W(\widetilde{S})F\widetilde{L} \subset pW(\widetilde{S})\widetilde{P} \subset I_{\widetilde{S}}\widetilde{P}$. Since we have a decompositon $\widetilde{P} = W(\widetilde{S})V^{-1}\widetilde{L} \oplus W(\widetilde{S})F\widetilde{T}$, one sees that the right hand side of (122) is isomorphic to $W(\widetilde{S})V^{-1}\widetilde{L}/I_{\widetilde{S}}V^{-1}\widetilde{L}$. This is indeed a projective $\widetilde{S}-$module of the right rank.

The ideal $\mathfrak{b}$ is in the kernel of Frob. Therefore the left hand side of (122) may be written as $\widetilde{S} \otimes_{\mathrm{Frob},S} Q_1/I_S P_1$. We consider the inverse of the map (122)

$$V^{\#} : \widetilde{P}_1/I_{\widetilde{S}}\widetilde{P}_1 + W(\widetilde{S})F\widetilde{P}_1 \longrightarrow \widetilde{S} \otimes_{\mathrm{Frob},S} Q_1/I_S P_1,$$

which we will also consider as a homomorphism of $W(\widetilde{S})$-modules

$$V^{\#} : \widetilde{P}_1 \longrightarrow \widetilde{S} \otimes_{\mathrm{Frob},S} Q_1/I_S P_1. \tag{123}$$

Now we define the second homomorphism. Since $\mathfrak{b}^p = 0$, the operator F on $\widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2$ factors as follows:

$$\begin{tikzcd}
\widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2 \arrow[rr, "F"] \arrow[dr] & & \widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2 \\
& P_2/I_S P_2 \arrow[ur, "F^b"'] &
\end{tikzcd}$$

The module $\widetilde{Q}_2/I_{\widetilde{S}}\widetilde{P}_2$ is in the kernel of F. Hence we obtain a Frobenius linear map

$$F^b : P_2/Q_2 \longrightarrow \widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2,$$

whose restriction to $\mathfrak{a}(P_2/Q_2)$ induces

$$F^b : \mathfrak{a}(P_2/Q_2) \longrightarrow \mathfrak{b}(\widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2).$$

If we use our embedding $\mathfrak{b} \subset W(\mathfrak{b})$, we may identify the target of F^b with $\mathfrak{b} \cdot \widetilde{P}_2 \subset W(\mathfrak{b})\widetilde{P}_2$. Let us denote the linearization of F^b simply by

$$F^{\#} : \quad \widetilde{S} \otimes_{\mathrm{Frob},S} \mathfrak{a}(P_2/Q_2) \longrightarrow \mathfrak{b}\widetilde{P}_2 \tag{124}$$

Proposition 73. — *The obstruction to lift $p\varphi : \mathcal{P}_1 \to \mathcal{P}_2$ to a homomorphism of displays $\widetilde{\mathcal{P}}_1 \to \widetilde{\mathcal{P}}_2$ is given by the composition of the following maps:*

$$\begin{tikzcd}
\widetilde{Q}_1/I_S\widetilde{P}_1 \arrow[r, "V^{\#}"] & \widetilde{S} \otimes_{\mathrm{Frob},S} Q_1/I_S P_1 \arrow[r, "\widetilde{S}\otimes \mathrm{Obst}\,\overline{\varphi}"] & \widetilde{S} \otimes_{\mathrm{Frob},S} \mathfrak{a}(P_2/Q_2) \arrow[d, "F^{\#}"] \\
& & \mathfrak{b}(\widetilde{P}_2/\widetilde{Q}_2)
\end{tikzcd}$$

Here the horizontal map is induced by the restriction of the map (123) to $\widetilde{Q}_1/I_{\widetilde{S}}\widetilde{P}_1$*, and the map* $F^{\#}$ *is the map (124) followed by the factor map* $\mathfrak{b}\widetilde{P}_2 \to \mathfrak{b}(\widetilde{P}_2/\widetilde{Q}_2)$.

Before giving the proof, we state a more precise result, which implies the proposition.

Corollary 74. — *The morphism of displays* $p\varphi : \mathcal{P}_1 \to \mathcal{P}_2$ *lifts by theorem 46 to a morphism of triples* $\widetilde{\psi} : (\widetilde{P}_1, F, V^{-1}) \to (\widetilde{P}_2, F, V^{-1})$*. This morphism may be explicitly obtained as follows. We define* $\omega : \widetilde{P}_1 \to \mathfrak{b}\widetilde{P}_2 \subset W(\mathfrak{b})\widetilde{P}_2$ *to be the composite of the following maps*

$$\widetilde{P}_1 \xrightarrow{V^{\#}} \widetilde{S} \otimes_{\mathrm{Frob},S} Q_1/I_S P_1 \xrightarrow{\widetilde{S}\otimes \mathrm{Obst}\,\overline{\varphi}} \widetilde{S} \otimes_{\mathrm{Frob},S} \mathfrak{a}(P_2/Q_2) \xrightarrow{F^{\#}} \mathfrak{b}\widetilde{P}_2.$$

Then we have the equation

$$\widetilde{\psi} = p\widetilde{\varphi} + \omega,$$

where $\widetilde{\varphi} : \widetilde{P}_1 \to \widetilde{P}_2$ *is any* $W(\widetilde{S})-$*linear map, which lifts* $\varphi : P_1 \to P_2$.

We remark that $p\widetilde{\varphi}$ depends only on φ and not on the particular lifting $\widetilde{\varphi}$.

Proof. — It is clear that the proposition follows from the corollary. Let us begin with the case, where $\bar{\varphi}$ is an isomorphism. We apply the method of the proof of theorem 44 to $p\widetilde{\varphi}$.

We find that $p\widetilde{\varphi}$ commutes with F.

$$F(p\widetilde{\varphi}) = (p\widetilde{\varphi})F \tag{125}$$

Indeed, since φ commutes with F, we obtain

$$F\widetilde{\varphi}(x) - \widetilde{\varphi}(Fx) \in W(\mathfrak{b})\widetilde{P}_2.$$

Since $p \cdot W(\mathfrak{b}) = 0$, we obtain (125). We have also that $p\widetilde{\varphi}(Q_1) \subset Q_2$.

We need to understand how much the commutation of $p\widetilde{\varphi}$ and V^{-1} fails. For this purpose we choose normal decompositions as follows. Let $\overline{P}_1 = \overline{L}_1 \oplus \overline{T}_2$ be any normal decomposition. We set $\overline{L}_2 = \overline{\varphi}(\overline{L})$ and $\overline{T}_2 = \overline{\varphi}(\overline{T}_1)$. Since $\overline{\varphi}$ is an isomorphism we have the normal decomposition $\overline{P}_2 = \overline{L}_2 \oplus \overline{T}_2$. We take liftings of these decompositions to normal decompositions

$$P_1 = L_1 \oplus T_1 \qquad \text{and} \qquad P_2 = L_2 \oplus T_2.$$

Finally we lift the last decomposition further to normal decompositions

$$\widetilde{P}_1 = \widetilde{L}_1 \oplus \widetilde{T}_1 \qquad \text{and} \qquad \widetilde{P}_2 = \widetilde{L}_2 \oplus \widetilde{T}_2.$$

We write the restriction of φ to L_1 as follows:

$$\varphi(l_1) = \lambda(l_1) + \mu(l_1), \quad \lambda(l_1) \in L_2,\ \mu(l_1) \in W(\mathfrak{a})T_2$$

Since $\mathfrak{a}^p = 0$, we have $I_S \cdot W(\mathfrak{a}) = 0$ and the Witt addition on $W(\mathfrak{a})$ is the usual addition of vectors. Let us denote by $\mathfrak{a}_n$ the $S-$module obtained from $\mathfrak{a}$ via restriction of scalars by $\mathrm{Frob}^n : S \to S$. Then we have a canonical isomorphism of $S-$modules

$$W(\mathfrak{a})T_2 \simeq \prod_{n\geq 0} \mathfrak{a}_n \otimes_S T_2/I_2T_2$$

Hence μ is a map

$$\mu : L_1/I_S L_1 \longrightarrow \prod_{n\geq 0} \mathfrak{a}_n \otimes_S T_2/I_S T_2.$$

We denote by μ_n its $n-th$ component. Then

$$\mu_0 : L_1/I_S L_1 \longrightarrow \mathfrak{a} \otimes_S T_2/I_S T_2$$

may be identified with the obstruction $\eta = \operatorname{Obst} \overline{\varphi}$.

Since φ commutes with V^{-1} we have

$$\varphi(V^{-1}l_1) = V^{-1}\lambda(l_1) + V^{-1}\mu(l_1). \tag{126}$$

Let us denote by $\mathfrak{c}$ the kernel of the map $\widetilde{S} \to R$. We choose any lifting $\widetilde{\tau}\cdot\widetilde{L}_1 \to W(\mathfrak{c})\widetilde{P}_2$ of the Frobenius linear map:

$$V^{-1}\mu : L_1 \longrightarrow W(\mathfrak{a})T_2 \xrightarrow{V^{-1}} W(\mathfrak{a})P_2.$$

We write the restriction of $\widetilde{\varphi}$ to $\widetilde{L}_1$ in the form

$$\widetilde{\varphi} = \widetilde{\lambda} + \widetilde{\mu},$$

where $\widetilde{\lambda} : \widetilde{L}_1 \to \widetilde{L}_2$ and $\widetilde{\mu} : \widetilde{L}_1 \to W(\mathfrak{a})\widetilde{T}_2$. Then we obtain from the equation (126) that

$$\widetilde{\varphi}(V^{-1}\widetilde{l}_1) - (V^{-1}\widetilde{\lambda}(\widetilde{l}_1) + \widetilde{\tau}(\widetilde{l}_1)) \in W(\mathfrak{b})\widetilde{P}_2, \quad \text{for} \quad \widetilde{l}_1 \in \widetilde{L}_1.$$

Since $pW(\mathfrak{b}) = 0$, we deduce the equation

$$p\widetilde{\varphi}(V^{-1}\widetilde{l}_1) = pV^{-1}\widetilde{\lambda}(\widetilde{l}_1) + p\widetilde{\tau}(\widetilde{l}_1). \tag{127}$$

On the other hand we have obviously

$$V^{-1}p\widetilde{\varphi}(\widetilde{l}_1) = pV^{-1}\widetilde{\lambda}(\widetilde{l}_1) + F\widetilde{\mu}(\widetilde{l}_1).$$

If we substract this form (127), we get an information on the commutation of $p\widetilde{\varphi}$ and V^{-1} :

$$p\widetilde{\varphi}(V^{-1}\widetilde{l}_1) - V^{-1}p\widetilde{\varphi}(\widetilde{l}_1) = (p\widetilde{\tau} - F\widetilde{\mu})(\widetilde{l}_1). \tag{128}$$

We set $\mu' = \mu - \mu_0$, with the map μ_0 defined above and consider it as a map $\mu' : L_1 \to {}^V W(\mathfrak{a})T_2$. We choose any lifting of μ' to a $W(\widetilde{S})-$linear map

$$\widetilde{\mu}' : \widetilde{L}_1 \longrightarrow {}^V W(\mathfrak{c})\widetilde{T}_2.$$

Then $V^{-1}\widetilde{\mu}'$ is defined and is a lifting of $V^{-1}\mu$, since by definition $V^{-1}\mu_0 = 0$. Therefore we may take $\tau = V^{-1}\widetilde{\mu}'$. Hence we may rewrite the right hand side of (128):

$$p\tau - F\widetilde{\mu} = F(\widetilde{\mu}' - \widetilde{\mu}). \tag{129}$$

Then $\widetilde{\mu} - \widetilde{\mu}'$ is a lifting of the map

$$\mu_0 : L_1 \longrightarrow \mathfrak{a} \otimes_S (T_2/I_S T_2) \subset W(\mathfrak{a})T_2,$$

to a map

$$\widetilde{\mu}_0 : \widetilde{L}_1 \longrightarrow W(\mathfrak{c})\widetilde{T}_2.$$

In fact the expression $F\widetilde{\mu}_0$ is independent of the particular lifting $\widetilde{\mu}_0$ of μ_0. Therefore we may rewrite the formula (128)

$$V^{-1}p\widetilde{\varphi}(\widetilde{l}_1) - p\widetilde{\varphi}(V^{-1}\widetilde{l}_1) = F\widetilde{\mu}_0(\widetilde{l}_1). \tag{130}$$

Let $\mathfrak{u} \subset W(\mathfrak{c})$ be the kernel of the following composite map:

$$W(\mathfrak{c}) \longrightarrow W(\mathfrak{a}) = \prod_{n\geq 0} \mathfrak{a}_n \xrightarrow{pr} \prod_{n\geq 1} \mathfrak{a}_n.$$

$\mathfrak{u}$ is the ideal consisting of vectors in $W(\mathfrak{c})$, whose components at places bigger than zero are in $\mathfrak{b}$. We see that ${}^F\mathfrak{u} \subset \mathfrak{b} = \mathfrak{b}_0 \subset W(\mathfrak{b})$. We find:

$$F\widetilde{\mu}_0(\widetilde{l}_1) \in \mathfrak{b}(\widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2) \subset W(\mathfrak{b})\widetilde{P}_2.$$

More invariantly we may express $F\widetilde{\mu}_0$ as follows.

We have a factorization:

$$\begin{tikzcd} F : \widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2 \arrow[rr] \arrow[dr] & & \widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2 \\ & P_2/I_S P_2 \arrow[ur, "F^b"'] & \end{tikzcd}$$

Then F^b induces by restriction a map

$$F^b : \mathfrak{a}(P_2/I_S P_2) \longrightarrow \mathfrak{b}(\widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2).$$

The map $F\widetilde{\mu}_0$ is the following composite map.

$$\widetilde{L}_1 \longrightarrow L_1 \xrightarrow{\mu_0} \mathfrak{a}(T_2/I_S T_2) \xrightarrow{F^b} \mathfrak{b}(\widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2).$$

By a slight abuse of notation we may write

$$F\widetilde{\mu}_0 = F^b\mu_0.$$

We obtain the final form of the commutation rule

$$V^{-1}p\widetilde{\varphi}(\widetilde{l}_1) - p\widetilde{\varphi}(V^{-1}\widetilde{l}_1) = F^b\mu_0(\widetilde{l}_1). \tag{131}$$

We want to know the map of triples

$$\widetilde{\psi} : (\widetilde{P}_1, F, V^{-1}) \longrightarrow (\widetilde{P}_2, F, V^{-1}),$$

which lifts $p\varphi$.

As in the proof of 2.2 we write $\widetilde{\psi} = p\widetilde{\varphi} + \omega$, where $\omega : \widetilde{P}_1 \to W(\mathfrak{b})\widetilde{P}_2$ is a $W(\widetilde{S})-$linear map. The condition that $\widetilde{\psi}$ should commute with F is equivalent to $\omega(W(\widetilde{S})F\widetilde{T}_1) = 0$. We consider only these ω. To ensure that V^{-1} and $\widetilde{\psi}$ commute is enough to ensure

$$V^{-1}\widetilde{\psi}(\widetilde{l}_1) = \widetilde{\psi}(V^{-1}\widetilde{l}_1) \quad \text{for} \quad \widetilde{l}_1 \in \widetilde{L}_1. \tag{132}$$

On $I_{\widetilde{S}}\widetilde{T}_1$ the commutation follows, because $\widetilde{\psi}$ already commutes with F. Using (131) we see that the equality (132) is equivalent with:

$$\omega(V^{-1}\widetilde{l}_1) - V^{-1}\omega(\widetilde{l}_1) = F^b\mu_0(\widetilde{l}_1) \tag{133}$$

We look for a solution of this equation in the space of $W(\widetilde{S})$- linear maps

$$\omega : \widetilde{P}_1/W(\widetilde{S})F\widetilde{T}_1 \longrightarrow \mathfrak{b}_0 \otimes_{\widetilde{S}} \widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2 \subset W(\mathfrak{b})\widetilde{P}_2$$

Then we have $V^{-1}\omega(\widetilde{l}_1) = 0$, by definition of the extended V^{-1}. Hence we need to find ω, such that

$$\omega(V^{-1}\widetilde{l}_1) = F^b\mu_0(\widetilde{l}_1). \tag{134}$$

We linearize this last equation as follows. The operator V^{-1} induces an isomorphism

$$(V^{-1})^{\#} : W(\widetilde{S}) \otimes_{F,W(\widetilde{S})} \widetilde{L}_1 \longrightarrow \widetilde{P}_1/W(\widetilde{S})F\widetilde{T}_1,$$

whose inverse will be denoted by $V^{\#}$.

We will also need the tensor product μ_0' of μ_0 with the map $w_0 : W(\widetilde{S}) \to \widetilde{S}$:

$$\mu_0' : W(\widetilde{S}) \otimes_{F,W(S)} L_1 \longrightarrow \widetilde{S} \otimes_{\mathrm{Frob},S} \mathfrak{a}(T_2/I_S T_2).$$

Finally we denote the linearization of F^b simply by $F^{\#}$:

$$F^{\#} : \widetilde{S} \otimes_{\mathrm{Frob},S} \mathfrak{a}(P_2/I_S P_2) \longrightarrow \mathfrak{b}(\widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2).$$

Noting that we have a natural isomorphism $W(\widetilde{S}) \otimes_{F,W(\widetilde{S})} \widetilde{L}_1 \cong W(\widetilde{S}) \otimes_{W(S)} L_1$, we obtain the following equivalent linear form of the equation (134):

$$\omega(V^{-1})^{\#} = F^{\#}\mu_0'.$$

It follows that the unique lifting of $p\varphi$ to a homomorphism of triples is

$$\widetilde{\psi} = p\widetilde{\varphi} + F^{\#}\mu_0' V^{\#}.$$

In this equation $V^{\#}$ denotes the composite map

$$\widetilde{P}_1 \longrightarrow \widetilde{P}_1/W(\widetilde{S})F\widetilde{T}_1 \longrightarrow W(\widetilde{S}) \otimes_{F,W(S)} \widetilde{L}_1.$$

This map $\widetilde{\varphi}$ induces the obstruction to lift $p\varphi$:

$$\tau : \widetilde{Q}_1/I_{\widetilde{S}}\widetilde{P}_1 \hookrightarrow \widetilde{P}_1/I_{\widetilde{S}}\widetilde{P}_1 \xrightarrow{\widetilde{\psi}} \widetilde{P}_2/I_{\widetilde{S}}\widetilde{P}_2 \to \widetilde{P}_2/\widetilde{Q}_2.$$

Since $p\widetilde{\varphi}$ maps $\widetilde{Q}_1$ to $\widetilde{Q}_2$, we may replace $\widetilde{\psi}$in the definition of the obstruction τ by $F^{\#}\mu_0' V^{\#}$. This proves the assertion of the corollary in the case where $\overline{\varphi}$ is an isomorphism.

If $\overline{\varphi}$ is not an isomorphism we reduce to the case of an isomorphism by the standard construction: Consider in general a homomorphism $\psi : \mathcal{P}_1 \to \mathcal{P}_2$ of displays over S. Then we associate to it the isomorphism

$$\begin{aligned} \psi_1 : \mathcal{P}_1 \oplus \mathcal{P}_2 &\longrightarrow \quad \mathcal{P}_1 \oplus \mathcal{P}_2 \\ x \oplus y \ &\longmapsto z \oplus y + \psi(x) \end{aligned}$$

If $\mathcal{P}_1$ and $\mathcal{P}_2$ are liftings to $\widetilde{S}$ as in the lemma, we denote by $\widetilde{\psi} : (\widetilde{P}_1, F, V^{-1}) \to (\widetilde{P}_2, F, V^{-1})$ the unique lifting to a homomorphism of triples. Then

$$\widetilde{\psi}_1(\tilde{x} \oplus \tilde{y}) = \tilde{x} \oplus (\tilde{y} + \widetilde{\psi}(\tilde{x})), \quad \tilde{x} \in \widetilde{P}_1, \quad \tilde{y} \in \widetilde{P}_2.$$

It follows that $\operatorname{Obst}\psi_1$ is the map

$$0 \oplus \operatorname{Obst}\widetilde{\psi} : \widetilde{Q}_1/I_{\widetilde{S}}\widetilde{P}_1 \oplus \widetilde{Q}_2/I_{\widetilde{S}}\widetilde{P}_2 \longrightarrow \widetilde{P}_1/\widetilde{Q}_1 \oplus \widetilde{P}_2/\widetilde{Q}_2.$$

Applying these remarks the reduction to the case of an isomorphism follows readily. $\square$

We will now apply the last proposition to obtain the following result of Keating:

Proposition 75. — *Let k be an algebraically closed field of characteristic $p > 2$. Let $\mathcal{P}_0$ be the display over k of dimension 1 and height 2. The endomorphism ring O_D of $\mathcal{P}_0$ is the ring of integers in a quaternion division algebra D with center $\mathbb{Q}_p$. Let $\alpha \mapsto \alpha^*$ for $\alpha \in O_D$ be the main involution. We fix $\alpha \in O_D$, such that $\alpha \notin \mathbb{Z}_p$ and we set $i = \operatorname{ord}_{O_D}(\alpha - \alpha^*)$. We define $c(\alpha) \in \mathbb{N}$:*

$$c(\alpha) = \begin{cases} p^{i/2} + 2p^{(i/2-1)} + 2p^{(i/2-2)} + \cdots + 2 & \text{for } i \text{ even} \\ 2p^{\frac{i-1}{2}} + 2p^{\left(\frac{i-1}{2}-1\right)} + \cdots + 2 & \text{for } i \text{ odd} \end{cases}$$

Let $\mathcal{P}$ over $k[\![t]\!]$ be the universal deformation of $\mathcal{P}_0$ in equal characteristic. Then α lifts to an endomorphism of $\mathcal{P}$ over $k[\![t]\!]/t^{c(\alpha)}$ but does not lift to an endomorphism of $\mathcal{P}$ over $k[\![t]\!]/t^{c(\alpha)+1}$.

Proof. — The display $\mathcal{P}_0 = (P_0, Q_0, F, V^{-1})$ is given by the structural equations

$$\begin{array}{rcl} Fe_1 & = & e_2 \\ V^{-1}e_2 & = & e_1. \end{array}$$

For any $a \in W(\mathbb{F}_{p^2})$ we have an endomorphism φ_a of $\mathcal{P}_0$, which is given by

$$\varphi_a(e_1) = ae_1 \qquad \varphi_a(e_2) = \sigma(a)e_2 \tag{135}$$

Here σ denotes the Frobenius endomorphism $W(\mathbb{F}_{p^2})$, and a is considered as an element of $W(k)$ with respect to a fixed embedding $\mathbb{F}_{p^2} \subset k$.

We denote by Π the endomorphism of $\mathcal{P}_0$ defined by

$$\Pi e_1 = e_2 \qquad \Pi e_2 = pe_1. \tag{136}$$

The algebra O_D is generated by Π and the φ_a. The following relations hold:

$$\Pi^2 = p\ , \qquad \Pi\varphi_a = \varphi_{\sigma(a)}\Pi.$$

The display $\mathcal{P}^u = (P^u, Q^u, F, V^{-1})$ of X over $k[\![t]\!]$ is given by the structural equations

$$Fe_1 = [t]e_1 + e_2 \qquad , \quad V^{-1}e_2 = e_1.$$

To prove our assertion on the liftability of α it is enough to consider the following cases:

$$\begin{array}{lll} \alpha = \varphi_a p^s\ , & a \not\equiv \sigma(a) \mod p\ , & s \in \mathbb{Z}, s \geq 0 \\ \alpha = \varphi_a p^s \Pi;\ , & a \in W(\mathbb{F}_{p^2})^*\ , & s \in \mathbb{Z}\ , s \geq 0 \end{array} \tag{137}$$

Let us begin by considering the two endomorphisms α for $s = 0$. The universal deformation $\mathcal{P}^u$ induces by base change $k[\![t]\!] \to k[\![t]\!]/t^p$ a display $\mathcal{P} = (P, Q, F, V^{-1})$. Then α induces an obstruction to the liftability to $S = k[\![t]\!]/t^p$:

$$\begin{array}{rcl} \operatorname{Obst}\alpha : Q/I_S P & \longrightarrow & t(P/Q), \\ e_2 & \longrightarrow & o(\alpha)\cdot e_1 \end{array} \tag{138}$$

where $o(\alpha) \in tk[\![t]\!]/t^p$. To compute the obstruction, we need to find the extension of α to a morphism of triples

$$\widetilde{\alpha} : \quad (P, F, V^{-1}) \longrightarrow (P, F, V^{-1}).$$

Let $\tilde{e}_1, \tilde{e}_2 \in P$ be defined, by

$$\tilde{e}_1 = e_1 \qquad \text{and} \qquad \tilde{e}_2 = [t]e_1 + e_2.$$

This is a basis of P and the extended operator V^{-1} is defined on $\tilde{e}_2$. We find the equations

$$F\tilde{e}_1 = \tilde{e}_2, \qquad V^{-1}\tilde{e}_2 = \tilde{e}_1.$$

Then obviously $\widetilde{\alpha}$ is given by the same equations as α:

$$\widetilde{\alpha}(\tilde{e}_1) = a\tilde{e}_1, \quad \widetilde{\alpha}(\tilde{e}_2) = \sigma(a)\tilde{e}_2, \tag{139}$$

respectively

$$\widetilde{\alpha}(\tilde{e}_1) = \sigma(a)\tilde{e}_2, \quad \widetilde{\alpha}(\tilde{e}_2) = ap\tilde{e}_1. \tag{140}$$

For the first endomorphism α of (137) we find

$$\begin{array}{rcl} \widetilde{\alpha}(e_2) & = & \widetilde{\alpha}(\tilde{e}_2 - [t]\tilde{e}_1) = \sigma(a)\tilde{e}_2 + [t]a\tilde{e}_1 \\ & = & \sigma(a)e_2 + [t](\sigma(a) - a)e_1 \end{array}$$

Hence the obstruction to lift α to $k[\![t]\!]/t^p$ is $o(\varphi_a) = o(\alpha) = (\sigma(a) - a)t \in tk[\![t]\!]/t^p$. For the second endomorphism α of (137) we find

$$\begin{array}{rcl} \widetilde{\alpha}(e_2) & = & \widetilde{\alpha}(\tilde{e}_2 - [t]\tilde{e}_1) = ap\tilde{e}_1 - [t]\sigma(a)\tilde{e}_2 \\ & = & ape_1 - [t]\sigma(a)\left([t]e_1 + e_2\right). \end{array}$$

Hence we obtain the obstruction

$$o\left(\varphi_a\Pi\right) = o(\alpha) = -t^2\sigma(a) \in tk[\![t]\!]/t^p.$$

Now we consider the first endomorphism of (137) for $s = 1$. It lifts to an endomorphism over $k[\![t]\!]/t^p$. We compute the obstruction to lift it to $k[\![t]\!]/t^{p^2}$. We can apply the lemma to the situation

$$\begin{array}{ccccc} k & \longleftarrow & k[\![t]\!]/t^p & \longleftarrow & k[\![t]\!]/t^{p^2} \\ \| & & \| & & \| \\ R & & S & & \widetilde{S} \end{array}$$

We set $\overline{\varphi} = \varphi_a$ and $\widetilde{\mathcal{P}} = \mathcal{P}^u_{\widetilde{S}}$. Then we have the following commutative diagram of obstructions

$$
\begin{tikzcd}
\widetilde{Q}/I_{\widetilde{S}}\widetilde{P} \arrow[r] \arrow[drr, "\mathrm{Obst}(p\varphi_a)"'] & \widetilde{S} \otimes_{\mathrm{Frob},S} Q/I_S P \arrow[r, "\widetilde{S}\otimes \mathrm{Obst}(\varphi_a)"] & \widetilde{S} \otimes_{\mathrm{Frob},S} t(P/Q) \arrow[d, "F^{\#}"] \\
 & & t^p(\widetilde{P}/\widetilde{Q})
\end{tikzcd}
\tag{141}
$$

The first horizontal map here is computed as follows:

$$
\begin{array}{ccccc}
\widetilde{Q}/I_{\widetilde{S}}\widetilde{P} & \longrightarrow & \widetilde{P}/I_{\widetilde{S}}\widetilde{P} + W(\widetilde{S})F\widetilde{P} & \xleftarrow{(V^{-1})^{\#}} & \widetilde{S} \otimes_{\mathrm{Frob},S} Q/I_S P \\
e_2 & \longmapsto & e_2 = -te_1 & & \\
 & & -te_1 & \longleftarrow\!\!\shortmid & -t \otimes e_2
\end{array}
$$

We obtain that the maps in the diagram (141) are as follows

$$
e_2 \longmapsto -t \otimes e_2 \longmapsto -t \otimes t\,(\sigma(a) - a)\, e_1 \longmapsto -t \cdot t^p\,(-\sigma(a) + a)\, Fe_1
$$

Therefore we obtain for $\mathrm{Obst}(p\varphi_a)$:

$$
\mathrm{Obst}\, p\varphi_a = t^{p+1}\,(\sigma(a) - a)\, Fe_1 = \quad t^{p+2}(\sigma a - a)e_1 \in t^p\left(\widetilde{P}/\widetilde{Q}\right).
$$

With the same convention as in (138) we write $o(p\varphi_a) = (\sigma(a) - a)t^{p+2}$. Then we prove by induction that $p^s\varphi_a$ lifts to $k[\![t]\!]/t^{p^2} + 2(p^{s-1} + \cdots + 1)$ and that the obstruction to lift it to $k[\![t]\!]/t^{p^{s+1}}$ is $(\sigma(a) - a) \cdot t^{p^s + 2(p^{s-1} + \cdot + 1)}$. For the induction step we apply our lemma to the situation

$$
\begin{array}{ccccc}
k[\![t]\!]/t^{p^s+2(p^{s-1}+\cdots+1)} & \longleftarrow & k[\![t]\!]/t^{p^{s+1}} & \longleftarrow & k[\![t]\!]/t^{p^{s+2}} \\
\| & & \| & & \| \\
R & & S & & \widetilde{S}
\end{array}
$$

We set $\overline{\varphi} = p^s\varphi_a$ over R and $\widetilde{\mathcal{P}} = \mathcal{P}^u_{\widetilde{S}}$. Then the maps in the diagram (141) are as follows

$$
\begin{array}{l}
e_2 \longmapsto -t \otimes e_2 \longmapsto -t \otimes (\sigma(a) - a)t^{p^s+2(p^{s-1}+\cdots+1)}e_1 \\
\qquad\qquad\qquad\qquad \downarrow \\
\qquad\qquad\qquad -t\,(a - \sigma(a))\, t^{p\left(p^s+2\left(p^{s-1}+\cdots+1\right)\right)} Fe_1
\end{array}
$$

This gives the asserted obstruction for $p^{s+1}\varphi_a$:

$$
\mathrm{Obst}\left(p^{s+1}\varphi_a\right) = \sigma(a) - a)t^{p^{s+1}+2(p^s+\cdots+p)+1} \cdot te_1.
$$

Next we consider the case of the endomorphisms $p^s\varphi_a\Pi$. In the case $s=1$ we apply the lemma to the situation

$$\begin{tikzcd} k & k[\![t]\!]/t^p \arrow[l] & k[\![t]\!]/t^{p^2}, \arrow[l] \\ R \arrow[u, equal] & S \arrow[l] \arrow[u, equal] & \widetilde{S} \arrow[l] \arrow[u, equal] \end{tikzcd}$$

and the endomorphism $\overline{\varphi} = \varphi_a\Pi$. Then the maps in the diagram (141) are as follows:

$$\begin{tikzcd} e_2 \arrow[r, mapsto] & -t\otimes e_2 \arrow[r, mapsto] & -t\otimes -t^2\sigma(a)e_1 \arrow[d, mapsto] \\ & & tt^{2p}aFe_1 \end{tikzcd}$$

This gives $\mathrm{Obst}(p\varphi_a\Pi) = t^{2p+2}a$. Now one makes the induction assumtion that for even s the obstruction to lift $p^s\varphi_a\Pi$ from $k[\![t]\!]/t^{2(p^s+\cdots+1)}$ to $k[\![t]\!]/t^{p^{s+1}}$ is $-t^{2(p^s+\cdots+1)}\cdot\sigma(a)$ and for odd s is $t^{2(p^s+\cdots+1)}\cdot a$. We get the induction step immediately from the lemma applied to the situation

$$k[\![t]\!]/t^{2(p^s+\cdots+1)} \longleftarrow k[\![t]\!]/p^{s+1} \longleftarrow k[\![t]\!]/p^{s+2}.$$

$\square$

We finish this section with a result of B.Gross on the endomorphism ring of the Lubin-Tate groups. Let A be a $\mathbb{Z}_p$-algebra. Let S be an A-algebra.

Definition 76. — *A A-display over S is a pair $(\widetilde{\mathcal{P}},\iota)$, where $\widetilde{\mathcal{P}}$ is a display over S, and $\iota : A\to \mathrm{End}\,\widetilde{\mathcal{P}}$ is a ring homomorphism, such that the action of A on $\widetilde{P}/\widetilde{Q}$ deduced from ι coincides with the action coming from the natural S-module structure on $\widetilde{P}/\widetilde{Q}$ and the homomorphism $A\to S$ giving the A-algebra structure.*

Let $a\in A$ be a fixed element. We set $R=S/a$ and $R_i = S/a^{i+1}$. Then we have a sequence of surjections

$$S\to\ldots\to R_i\to R_{i-1}\to\cdots\to R=R_0$$

Let $\widetilde{\mathcal{P}}_1$ and $\widetilde{\mathcal{P}}_2$ be displays over S. They define by base change displays $\mathcal{P}_1^{(i)}$ and $\mathcal{P}_2^{(i)}$ over R_i. We set $\mathcal{P}_1=\mathcal{P}_1^{(0)}$ and $\mathcal{P}_2=\mathcal{P}_2^{(0)}$.

Assume we are given a morphism $\varphi:\mathcal{P}_1\to\mathcal{P}_2$, which lifts to a morphism $\varphi^{(i-1)}:\mathcal{P}_1^{(i-1)}\to\mathcal{P}_2^{(i-1)}$. The obstruction to lift $\varphi^{(i-1)}$ to a morphism $\mathcal{P}_1^{(i)}\to\mathcal{P}_2^{(i)}$ is a homomorphism:

$$\mathrm{Obst}\,\varphi^{(i-1)} : Q_1^{(i)}/I_{R_i}P_1^{(i)} \longrightarrow (a^i)/(a^{i+1})\otimes_{R_i} P_2^{(i)}/Q_2^{(i)}.$$

Clearly $\mathrm{Obst}\,\varphi^{(i-1)}$ factors through a homomorphism:

$$\mathrm{Obst}_i\,\varphi : Q_1/I_RP_1 \longrightarrow (a^i)/(a^{i+1})\otimes_R P_2/Q_2.$$

Proposition 77. — *Assume that $(\widetilde{\mathcal{P}}_2, \iota)$ is an A-display over S. Let $\varphi : \mathcal{P}_1 \to \mathcal{P}_2$ be a morphism of displays, which lifts to a morphism $\mathcal{P}_1^{(i-1)} \to \mathcal{P}_2^{(i-1)}$. Then $\iota(a)\varphi$ lifts to a homomorphism $\mathcal{P}_1^{(i)} \to \mathcal{P}_2^{(i)}$ and moreover we have a commutative diagram if $i \geq 2$ or $p > 2$:*

$$\begin{tikzcd} Q_1/I_R P_1 \arrow[r, "\mathrm{Obst}_i\,\varphi"] \arrow[dr, "\mathrm{Obst}_{i+1}(\iota(a)\varphi)"'] & (a^i)/(a^{i+1}) \otimes_R P_2/Q_2 \arrow[d, "a\otimes \mathrm{id}"] \\ & (a^{i+1})/(a^{i+1}) \otimes_R P_2/Q_2 \end{tikzcd} \tag{142}$$

Loosely said we have $\mathrm{Obst}_{i+1}(\iota(a)\varphi) = a\,\mathrm{Obst}_i(\varphi)$.

Proof. — We consider the surjection $R_{i+1} \to R_{i-1}$. The kernel $a^i R_{i+1}$ has divided powers if $i \geq 2$ or $p > 2$. Hence the obstruction to lift $\varphi^{(i-1)}$ to $R^{(i+1)}$ is defined:

$$\mathrm{Obst}\,\varphi^{(i-1)} : Q_1^{(i+1)}/I_{R_{i+1}} P_1^{(i+1)} \to (a^i)/(a^{i+2}) \otimes_{R_{i+1}} P_2^{(i+1)}/Q_2^{(i+1)}$$

is defined. Since $\iota(a)$ induces on the tangent space $P^{(i+1)}/Q^{(i+1)}$ the multiplication by a we obtain

$$\mathrm{Obst}\,\iota(a)\varphi^{(i-1)} = a\,\mathrm{Obst}\,\varphi^{(i-1)}$$

This proves the proposition. □

We will now apply this proposition to the case of a Lubin–Tate display. Let $K/\mathbb{Q}_p$ be a totally ramified extension of degree $e \geq 2$. We consider the ring of integers $A = O_K$. The rôle of the element a in the proposition will be played by a prime element $\pi \in O_K$. For S we take the ring $S = O_K \otimes_{\mathbb{Z}_p} W(\overline{\mathbb{F}}_p)$. Now we take a notational difference between π and its image in S, which we denote by a.

Let $\widetilde{\mathcal{P}} = (\widetilde{P}, \widetilde{Q}, F, V^{-1})$ be the Lubin–Tate display over S. We recall that $\widetilde{P} = O_K \otimes_{\mathbb{Z}_p} W(S)$, $\widetilde{Q} = \mathrm{kernel} \quad (O_K \otimes_{\mathbb{Z}_p} W(S) \to S)$, and $V^{-1}(\pi \otimes 1 - 1 \otimes [a]) = 1$.

Let $\mathcal{P}$ be the display obtained by base change over $R = S/aS = \overline{\mathbb{F}}_p$. The operator V^{-1} of $\mathcal{P}$ satisfies

$$V^{-1}\pi^i = \pi^{i-1},$$

where $\pi = \pi \otimes 1 \in O_K \otimes_{\mathbb{Z}_p} W(R)$. (One should not be confused by the fact that this ring happens to be S). We note that $Q = \pi P$.

We consider an endomorphism $\varphi : \mathcal{P} \to \mathcal{P}$, and compute the obstruction to lift φ to $R_1 = S/a^2 S$:

$$\mathrm{Obst}_1(\varphi) : Q/I_R P \longrightarrow (a)/(a^2) \otimes_R P/Q.$$

The endomorphism φ induces an endomorphism on P/Q, which is the multiplication by some element $\mathrm{Lie}\,\varphi \in \overline{\mathbb{F}}_p$. Let us denote by σ the Frobenius endomorphism of $\overline{\mathbb{F}}_p$.

Lemma 78. — $\mathrm{Obst}_1(\varphi)$ *is the composition of the following maps:*

$$\begin{tikzcd} Q/I_R P = Q/pP \arrow[r, "1/\pi"] & P/\pi P = P/Q \arrow[r, "\sigma^{-1}(\mathrm{Lie}\,\varphi)-\mathrm{Lie}\,\varphi"] & P/Q \arrow[d, "a"] \\ & & (a)/(a^2)\otimes_R P/Q \end{tikzcd}$$

Proof. — We write

$$\varphi(1) = \xi_0 + \xi_1\pi + \cdots + \xi_{e-1}\pi^{e-1}, \quad \xi_i \in W(\overline{\mathbb{F}}_p).$$

Applying the operator V we obtain:

$$\varphi(\pi^i) =^{F^{-i}} \xi_0^{\pi^i} +^{F^{-i}} \xi_1\pi^{i+1} + \dots, \quad \text{for} i = 0, 1 \dots \tag{143}$$

By theorem 46 this φ admits a unique extension to an endomorphism of the triple $(P^{(1)}, F, V^{-1})$, where $P^{(1)} = O_K \otimes_{\mathbb{Z}_p} W(R_1)$. For the definition of the extension $\widetilde{\varphi}$ we use here the obvious divided powers on the ideal $aR_1 \subset R_1 = S/a^2S$ given by $\alpha_p(a) = 0$. Then we have $V^{-1}[a]P^{(1)} = 0$, for the extended V^{-1}. Hence we find for the triple $(P^{(1)}, F, V^{-1})$ the equations:

$$V^{-1}\pi^i = \pi^{i-1}, \quad \text{for} \quad i \geq 1, \qquad F1 = \frac{p}{\pi}.$$

The last equation follows because the unit τ of lemma 27 specialise in R_1 to π^e/p. Hence we can define $\widetilde{\varphi}$ on $P^{(1)}$ by the same formulas (143) as φ. In other words:

$$\widetilde{\varphi} = \varphi \otimes_{W(\overline{\mathbb{F}}_P)} W(R_1). \tag{144}$$

This formula may also be deduced from the fact that $\widetilde{\varphi}$ is an endomorphism of the display $\mathcal{P}_{R_1}$ obtained by base change via the natural inclusion $R \to R_1$.

The map $\widetilde{\varphi}$ induces an $O_K \otimes_{\mathbb{Z}_p} R_1$-module homomorphism

$$Q^{(1)}/I_{R_1}P^{(1)} \longrightarrow P^{(1)}/Q^{(1)}. \tag{145}$$

By definition the module on the left hand side has the following basis as an R_1-module:

$$\pi - a, \quad \pi^2 - a^2, \dots, \pi^{e-1} - a^{e-1},$$

where we wrote π for $\pi \otimes 1 \in O_K \otimes_{\mathbb{Z}_p} R_1$ and a for $1 \otimes a$. We note that $\pi^i \in Q^{(1)}$ for $i \geq 2$, because $a^2 = 0$ in R_1 and because $Q^{(1)}$ is an O_K-module. By (144) and (143) we find

$$\begin{aligned} \widetilde{\varphi}(\pi - a) &= {}^{F^{-1}}\xi_0\pi + {}^{F^{-1}}\xi_1\pi^2 + \cdots - a(\xi_0 + \xi_1\pi + \cdots) \\ &\equiv \left({}^{F^{-1}}\xi_0 - \xi_0\right)a \qquad \mathrm{mod}\ Q^{(1)} \end{aligned}$$

Since $\widetilde{\varphi}$ is an $O_K \otimes_{\mathbb{Z}_p} W(R_1)$-module homomorphism we have $\widetilde{\varphi}(\pi^i) = 0 \mod Q^{(1)}$. This gives the result for $\mathrm{Obst}_1\,\varphi$ because $\xi_0 \mod p = \mathrm{Lie}\,\varphi$. □

We can obtain a result of B.Gross [G] in our setting:

Proposition 79. — *Let us assume that $p > 2$. Assume that K is a totally ramified extension of $\mathbb{Q}_p$, which has degree $e = [K : \mathbb{Q}_p]$. We fix a prime element $\pi \in O_K$. Let $\widetilde{\mathcal{P}}$ be the corresponding Lubin–Tate display over O_K. Let $\mathcal{P} = \widetilde{\mathcal{P}}_{\overline{\mathbb{F}}_p}$ the display obtained by base change via $O_K \to \mathbb{F}_p \subset \overline{\mathbb{F}}_p$. Let $O_D = \operatorname{End}\mathcal{P}$ be the endomorophism ring. Let $\breve{K}$ be the completion of the maximal unramified extension of K with residue class field $\overline{\mathbb{F}}_p$. Then we have*

$$\operatorname{End}\widetilde{\mathcal{P}}_{O_{\breve{K}}/(\pi^{m+1})} = O_K + \pi^m O_D \quad m \geq 0.$$

Proof. — We use the notation of proposition 77, and set $R_i = O_{\breve{K}}/(\pi^{+1})$. Let $\varphi \in O_D$ be an endomorphism of $\mathcal{P}$. It follows from the formula (2.61) that $\pi^m\varphi$ lifts to an endomorphism of $\widetilde{\mathcal{P}}$ over $O_{\breve{K}}/\pi^{m+1}$. From (77) we obtain by induction:

$$\operatorname{Obst}_{m+1} \pi^m\varphi = \pi^m \operatorname{Obst}_1 \varphi,$$

where π^m on the right hand side denotes the map

$$\pi^m : (\pi)/(\pi^2) \otimes_R P/Q \longrightarrow (\pi^{m+1})/(\pi^{m+2}) \otimes_R P/Q.$$

We recall that $R = R_0 = \overline{\mathbb{F}}_p$ by definition.

Now assume we are given an endomorphism

$$\psi \in (O_K + \pi^m O_D) - (O_K + \pi^{m+1} O_D).$$

Since π is a prime element of O_D we have the expansion

$$\psi = [a_0] + \lfloor a_1 \rceil \pi + \cdots + [a_m]\pi^m + \cdots, \quad \text{where} \quad a_i \in F_{p^e}.$$

We have $a_i \in \mathbb{F}_p$ for $i < m$ and $a_m \notin \mathbb{F}_p$ since $\psi \notin O_K + \pi^{m+1}O_D$. Then we find

$$\operatorname{Obst}^{m+1} \psi = \operatorname{Obst}_{m+1} ([a_m]\pi^m + \cdots) = \pi^m \operatorname{Obst}_1 ([a_m]] + \pi[a_{m+1}] + \cdots)$$

Since $\sigma(a_m) \neq a_m$ the obstruction $\operatorname{Obst}_1 (\lfloor a_m \rceil + \pi \lfloor a_{m+1} \rceil \cdots)$ does not vanish. Hence $\operatorname{Obst}_{m+1} \psi$ does not vanish. □

3. The p–divisible group of a display

3.1. The functor BT. — Let R be a unitary commutative ring, such that p is nilpotent in R. Consider the category Nil_R introduced after definition 50. We will consider functors $F : \operatorname{Nil}_R \to \text{Sets}$, such that $F(0)$ consists of a singe point denoted by 0 and such that F commutes with finite products. Let us denote this category by $\mathcal{F}$. If $\mathcal{N}^2 = 0$, we have homomorphism in Nil_R:

$$\mathcal{N} \times \mathcal{N} \xrightarrow{\text{addition}} \mathcal{N}, \quad \mathcal{N} \xrightarrow{\tau} \mathcal{N}, \quad \text{where} \quad \tau \in R.$$

The last arrow is multiplied by τ. Applying F we obtain a R-module structure on $F(\mathcal{N})$. A R-module M will be considered as an object of Nil_R by setting $M^2 = 0$. We write $t_F(M)$ for the R-module $F(M)$.

We view a formal group as a functor on Nil_R (compare [Z1]).

Definition 80. — *A (finite dimensional) formal group is a functor $F : \operatorname{Nil}_R \to$ (abelian groups), which satisfies the following conditions.*

(i) *F(0) =0.*

(ii) *For any sequence in* Nil_R
$$0 \longrightarrow \mathcal{N}_1 \longrightarrow \mathcal{N}_2 \longrightarrow \mathcal{N}_3 \longrightarrow 0,$$
which is exact as a sequence of R-modules the corresponding sequence of abelian groups
$$0 \longrightarrow F(\mathcal{N}_1) \longrightarrow F(\mathcal{N}_2) \longrightarrow F(\mathcal{N}_3) \longrightarrow 0$$
is exact.

(iii) *The functor* t_F *commutes with infinite direct sums.*

(iv) $t_F(R)$ *is a finitely generated projective R-module.*

Our aim is to associate a formal group to a 3n-display.

Let us denote by $\hat{W}(\mathcal{N}) \subset W(\mathcal{N})$ the subset of Witt vectors with finitely many non–zero components. This is a $W(R)$-subalgebra.

Let us fix $\mathcal{N}$ and set $S = R|\mathcal{N}| = R \oplus \mathcal{N}$. Then we introduce the following $W(R)$-modules

$$\begin{aligned} P_{\mathcal{N}} &= W(\mathcal{N}) \otimes_{W(R)} P \subset P_S \\ Q_{\mathcal{N}} &= (W(\mathcal{N}) \otimes_{W(R)} P) \cap Q_S \\ \hat{P}_{\mathcal{N}} &= \hat{W}(\mathcal{N}) \otimes_{W(R)} P \subset P_S \\ \hat{Q}_{\mathcal{N}} &= \hat{P}_{\mathcal{N}} \cap Q_S \end{aligned}$$

We will denote by $I_{\mathcal{N}} \subset W(\mathcal{N})$ resp. $\hat{I}_{\mathcal{N}} \subset \hat{W}(\mathcal{N})$ the $W(R)$-submodules ${}^V W(\mathcal{N})$ and ${}^V \hat{W}(\mathcal{N})$. We note that ^{F} and ^{V} act also on $\hat{W}(\mathcal{N})$. Hence the restriction of the operators $F : P_S \to P_S$ and $V^{-1} : Q_S \to P_S$ define operators

$$\begin{aligned} F : P_{\mathcal{N}} &\longrightarrow P_{\mathcal{N}} & \qquad V^{-1} : Q_{\mathcal{N}} &\longrightarrow P_{\mathcal{N}} \\ F : \hat{P}_{\mathcal{N}} &\longrightarrow \hat{P}_{\mathcal{N}} & \qquad V^{-1} : \hat{Q}_{\mathcal{N}} &\longrightarrow \hat{P}_{\mathcal{N}}. \end{aligned}$$

If we choose a normal decomposition
$$P = L \oplus T,$$
we obtain:

$$\begin{aligned} Q_{\mathcal{N}} &= W(\mathcal{N}) \otimes_{W(R)} L \oplus I_{\mathcal{N}} \otimes_{W(R)} T \\ \hat{Q}_{\mathcal{N}} &= \hat{W}(\mathcal{N}) \otimes_{W(R)} L \oplus \hat{I}_{\mathcal{N}} \otimes_{W(R)} T \end{aligned} \tag{146}$$

Theorem 81. — *Let* $\mathcal{P} = (P, Q, F, V^{-1})$ *be a 3n-display over R. Then the functor from* Nil_R *to the category of abelian groups, which associates to an object* $\mathcal{N} \in \mathrm{Nil}_R$ *the cokernel of the homomorphism of additive groups:*
$$V^{-1} - \mathrm{id} : \hat{Q}_{\mathcal{N}} \longrightarrow \hat{P}_{\mathcal{N}},$$
is a finite dimensional formal group. Here id *is the natural inclusion* $\hat{Q}_{\mathcal{N}} \subset \hat{P}_{\mathcal{N}}$. *We denote this functor be* $BT_{\mathcal{P}}$. *One has an exact sequence:*

$$0 \longrightarrow \hat{Q}_{\mathcal{N}} \xrightarrow{V^{-1}-\mathrm{id}} \hat{P}_{\mathcal{N}} \longrightarrow BT_{\mathcal{P}}(\mathcal{N}) \longrightarrow 0. \tag{147}$$

We will give the proof of this theorem and of the following corollary later in this section.

Corollary 82. — *Let $\mathcal{P}$ be a 3n-display, such that there is a number N with the property $F^N P \subset I_R P$. Then we have an exact sequence compatible with (147):*

$$0 \longrightarrow Q_{\mathcal{N}} \xrightarrow{V^{-1}-\mathrm{id}} P_{\mathcal{N}} \longrightarrow BT_{\mathcal{P}}(\mathcal{N}) \longrightarrow 0$$

***Remark*:** The F-nilpotence condition $F^N P \subset I_R P$ is equivalent to the condition that $F : P \to P$ induces a nilpotent (Frobenius linear) map $R/pR \otimes_{\mathbf{w}_0} P \to R/pR \otimes_{\mathbf{w}_0} P$ of R/pR-modules.

Assume that $\mathcal{N}$ is equipped with divided powers, i.e. the augmentation ideal of the augmented R-algebra $R|\mathcal{N}|$ is equipped with divided powers. Then the divided Witt polynomials define an isomorphism:

$$\prod \mathbf{w'}_n : W(\mathcal{N}) \longrightarrow \prod_{i \geq 0} \mathcal{N} \tag{148}$$

This induces a homomorphism:

$$\begin{array}{rcl} \hat{W}(\mathcal{N}) & \longrightarrow & \bigoplus_{i \geq 0} \mathcal{N} \\ (n_0, n_1, n_2, \cdots) & \longmapsto & [\mathbf{w'}_0(n_0), \mathbf{w'}_1(n_0, n_1), \cdots]. \end{array} \tag{149}$$

To see that the homomorphism (148) takes $\hat{W}(\mathcal{N})$ to the direct sum, it is enough to check, that for a fixed element $n \in \mathcal{N}$ the expression $\alpha_{p^k}(n) ='' \frac{n^{p^k}}{p^k}''$ becomes zero, if k is big enough. But in terms of the divided powers γ_m on $\mathcal{N}$ this expression is $\frac{(p^k)!}{p^k} \gamma_{pk}(n)$. Since the exponential valuation $\mathrm{ord}_p(\frac{p^k!}{p^k})$ tends with k to infinity, we conclude that (149) is defined.

If we assume moreover that the divided powers on $\mathcal{N}$ are nilpotent in the sense that $\gamma_{p^k}(n)$ is zero for big k, for a fixed $n \in \mathcal{N}$, the homomorphism (149) is an isomorphism. Indeed, for the surjectivity of (149) it is enough to verify that elements of the form $[x, 0, \cdots, 0, \cdots]$ lie in the image, because the morphism (148) is compatible with Verschiebung. To prove the surjectivity of (149) we may moreover restrict to the case where $p \cdot \mathcal{N} = 0$. Indeed $p\mathcal{N} \subset \mathcal{N}$ is a pd-subalgebra, which is an ideal in $\mathcal{N}$. Hence $\mathcal{N}/p\mathcal{N}$ is equipped with nilpotent divided powers. Therefore an induction with the order of nilpotence of p yields the result. If $p \cdot \mathcal{N} = 0$, we see that any expression $''\frac{n^{p^k}}{p^k}''$ is zero for $k \geq 2$ because $\frac{(p^k)!}{p^k}$ is divisible by p. But then the assertion, that $[x, 0, 0, \cdots 0]$ is in the image of (149) means that there is $(n_0, n_1, \cdots) \in \hat{W}(\mathcal{N})$ satisfies the equations

$$x = n_0, \quad \alpha_p(n_0) + n_1 = 0, \quad \alpha_p(n_1) + n_2 = 0, \quad \alpha_p(n_2) + n_3 = 0 \cdots .$$

We have to show that the solutions of these equations:

$$n_k = (-1)^{1+p+\cdots p^{k-1}} \alpha_p(\cdots \alpha_p(x)) \cdots) \quad k \geq 1,$$

where α_p is iterated k-times, become zero if k is big. It is easy to see from the definition of divided powers that $\alpha_p(\cdots(\alpha_p(x))\cdots)$ and $\gamma_{p^k}(x)$ differ by a unit in

$\mathbb{Z}_{(p)}$. Hence we find a solution in $\hat{W}(\mathcal{N})$, if $\gamma_{p^k}(x)$ is zero for big k. Hence (149) is an isomorphism in the case of nilpotent divided powers. Assume we are given divided powers on $\mathcal{N}$. They define the embedding

$$\begin{aligned} \mathcal{N} &\longrightarrow \quad W(\mathcal{N}), \\ n &\longmapsto \quad [n, 0 \cdots 0 \cdots] \end{aligned} \tag{150}$$

where we have used logarithmic coordinates on the right hand side. If we have nilpotent divided powers the image of the map (150) lies in $\hat{W}(\mathcal{N})$. Then we obtain the direct decomposition $\hat{W}(\mathcal{N}) = \mathcal{N} \oplus {}^V\hat{W}(\mathcal{N})$.

By lemma 38 the operator $V^{-1} : Q_S \to P_S$ extends to the inverse image of Q, if $\mathcal{N}$ has divided powers. This gives a map

$$V^{-1} : W(\mathcal{N}) \otimes_{W(R)} P \longrightarrow W(\mathcal{N}) \otimes_{W(R)} P. \tag{151}$$

If the divided powers on $\mathcal{N}$ are nilpotent, we obtain a map

$$V^{-1} : \hat{W}(\mathcal{N}) \otimes_{W(R)} P \longrightarrow \hat{W}(\mathcal{N}) \otimes_{W(R)} P. \tag{152}$$

In fact the nilpotent divided powers are only needed for the existence of this map.

Lemma 83. — *If $\mathcal{N}$ has nilpotent divided powers the map (152) is nilpotent. If $\mathcal{N}$ has only divided powers but if we assume moreover that $F^N P \subset I_R P$ for some number N, the map (151) is nilpotent.*

Proof. — From the isomorphism (146) we get an isomorphim

$$W(\mathcal{N}) \otimes_{W(R)} P \cong \prod_{i \geq 0} \mathcal{N} \otimes_{\mathbf{w}_i, W(R)} P \tag{153}$$

We describe the action of the operator V^{-1} on the right hand side. Let us denote by F_i the following map

$$\begin{aligned} F_i : \mathcal{N} \otimes_{\mathbf{w}_i, W(R)} P \quad &\longrightarrow \quad \mathcal{N} \otimes_{\mathbf{w}_{i-1}, W(R)} P, \quad i \geq 1. \\ a \otimes x \quad &\longmapsto \quad a \otimes Fx \end{aligned}$$

If we write an element from the right hand side of (153) in the form $[u_0, u_1, u_2, \cdots], u_i \in \mathcal{N} \otimes_{\mathbf{w}_i, W(R)} P$, the operator V^{-1} looks as follows:

$$V^{-1}[u_0, u_1, \cdots] = [F_1 u_1, F_2 u_2, \cdots, F_i u_i \cdots]. \tag{154}$$

In the case where the divided powers on $\mathcal{N}$ are nilpotent, we have an isomorphism

$$\hat{W}(\mathcal{N}) \otimes_{W(R)} P \longrightarrow \bigoplus_{i \geq 0} \mathcal{N} \otimes_{\mathbf{w}_i, W(R)} P. \tag{155}$$

Since V^{-1} on the right hand side is given by the formula (154), the nilpotency of V^{-1} is obvious in this case.

To show the nilpotency of V^{-1} on (153), we choose a number r, such that $p^r \cdot R = 0$. Then we find $\mathbf{w}_i(I_r) \cdot \mathcal{N} \subset p^r \mathcal{N} = 0$, for any $i \in \mathbb{N}$. By our assumption we find a number M, such that $F^M P \subset I_r P$. This implies $F_{i+1} \cdot \ldots \cdot F_{i+M} = 0$ and hence the nilpotency of V^{-1}. $\square$

Corollary 84. — *Let $\mathcal{P}$ be a 3n-display over R. For any nilpotent algebra $\mathcal{N} \in \mathrm{Nil}_R$ the following map is injective*

$$V^{-1} - \mathrm{id} : \hat{Q}_{\mathcal{N}} \longrightarrow \hat{P}_{\mathcal{N}}.$$

Proof. — We remark that the functors $\mathcal{N} \mapsto \hat{P}_{\mathcal{N}}$ and $\mathcal{N} \mapsto \hat{Q}_{\mathcal{N}}$ are exact in the sense of definition (80) (ii). For $\hat{Q}_{\mathcal{N}}$ this follows from the decomposition (146).

Since any nilpotent $\mathcal{N}$ admits a filtration

$$0 = \mathcal{N}_0 \subset \mathcal{N}_1 \subset \cdots \subset \mathcal{N}_\tau = \mathcal{N},$$

such that $\mathcal{N}_i^2 \subset \mathcal{N}_{i-1}$, we may by induction reduce to the case $\mathcal{N}^2 = 0$. Since in this case $\mathcal{N}$ may be equipped with nilpotent divided powers, we get the injectivity because by the lemma (83) the map $V^{-1} - \mathrm{id} : \hat{W}(\mathcal{N}) \otimes P \to \hat{W}(\mathcal{N}) \otimes P$ is an isomorphism. $\square$

Corollary 85. — *Let $\mathcal{P}$ be a 3n-display over R, such that $F^N P \subset I_R P$ for some number N, then the map*

$$V^{-1} - \mathrm{id} : Q_{\mathcal{N}} \longrightarrow P_{\mathcal{N}}$$

is injective.

The proof is the same starting from lemma (83).

Proof. — (theorem (81) and its corollary). For any 3n-display $\mathcal{P}$ we define a functor $\hat{G}$ on Nil_R by the exact sequence:

$$0 \longrightarrow \hat{Q}_{\mathcal{N}} \xrightarrow{V^{-1}-\mathrm{id}} \hat{P}_{\mathcal{N}} \longrightarrow \hat{G}(\mathcal{N}) \longrightarrow 0.$$

If $\mathcal{P}$ satisfies the assumption of corollary (85) we define a functor G by the exact sequence:

$$0 \longrightarrow Q_{\mathcal{N}} \xrightarrow{V^{-1}-\mathrm{id}} P_{\mathcal{N}} \longrightarrow G(\mathcal{N}) \longrightarrow 0.$$

We verify that the functors G and $\hat{G}$ satisfy the conditions (i) – (iv) of the definition (80). It is obvious that the conditions (i) and (ii) are fulfilled, since we already remarked that the functors $\mathcal{N} \mapsto Q_{\mathcal{N}}$ (resp. $\hat{Q}_{\mathcal{N}}$) and $\mathcal{N} \mapsto P_{\mathcal{N}}$ (resp. $\hat{P}_{\mathcal{N}}$) are exact.

All what remains to be done is a computation of the functors t_G and $t_{\hat{G}}$. We do something more general.

Let us assume that $\mathcal{N}$ is equipped with nilpotent divided powers. Then we define an isomorphism, which is called the exponential map

(156) $$\exp_{\mathcal{P}} : \mathcal{N} \otimes_R P/Q \longrightarrow \hat{G}(\mathcal{N}).$$

It is given by the following commutative diagram.

(157) $$\begin{tikzcd} 0 \arrow[r] & \hat{Q}_{\mathcal{N}} \arrow[r] \arrow[d, equal] & \hat{P}_{\mathcal{N}} \arrow[r] \arrow[d, "V^{-1}-\mathrm{id}"] & \mathcal{N} \otimes_R P/Q \arrow[r] \arrow[d, "\exp"] & 0 \\ 0 \arrow[r] & \hat{Q}_{\mathcal{N}} \arrow[r, "V^{-1}-\mathrm{id}"] & \hat{P}_{\mathcal{N}} \arrow[r] & \hat{G}(\mathcal{N}) \arrow[r] & 0. \end{tikzcd}$$

If $\mathcal{N}^2 = 0$, we can take the divided powers $\gamma_k = 0$ for $i \geq 2$. Then the exponential map provides an isomorphism of the functor $t_{\hat{G}}$ with the functor $M \mapsto M \otimes_R P/Q$ on the category of $R-$modules. Hence the conditions (iii) and (iv) of definition 80 are fulfilled. If the display $\mathcal{P}$ satisfies the condition $F^N \cdot P \subset I_R P$ for some number $\mathcal{N}$, we may delete the hat in diagram (157), because the middle vertical arrow remains an isomorphism by lemma (83). In fact in this case we need only to assume that $\mathcal{N}$ has divided powers. We get an isomorphism

$$\exp : \mathcal{N} \otimes P/Q \longrightarrow G(\mathcal{N}). \tag{158}$$

It follows again that $G(\mathcal{N})$ is a finite dimensional formal group. The obvious morphism $\hat{G}(\mathcal{N}) \to G(\mathcal{N})$ is a homomorphism of formal groups, which is by (156) and (158) an isomorphism on the tangent functors $t_{\hat{G}} \to t_G$. Hence we have an isomorphism $\hat{G} \cong G$, which proves the theorem 81 completely. □

Corollary 86. — *The functor $\mathcal{P} \mapsto BT_{\mathcal{P}}$ commutes with base change. More pecisely if $\alpha : R \to S$ is a ring homomorphism base change provides us with a display $\alpha_* \mathcal{P}$ and a formal group $\alpha_* BT_{\mathcal{P}}$ over S. Then we assert that there is a canonical isomorphism:*

$$\alpha_* BT_{\mathcal{P}} \cong BT_{\alpha_* \mathcal{P}}$$

Proof. — In fact for $\mathcal{M} \in \mathrm{Nil}_S$ we have the obvious isomorphism:

$$\hat{W}(\mathcal{M}) \otimes_{W(R)} P \cong \hat{W}(\mathcal{M}) \otimes_{W(S)} W(S) \otimes_{W(R)} P = \hat{W}(\mathcal{M}) \otimes_{W(S)} \alpha_* P$$

This provides the isomorphism of the corollary. □

Proposition 87. — *Let R be a ring, such that $pR = 0$, and let $\mathcal{P}$ be a display over R. Then we have defined a Frobenius endomorphism (29):*

$$Fr_{\mathcal{P}} : \mathcal{P} \to \mathcal{P}^{(p)}. \tag{159}$$

Let $G = BT_{\mathcal{P}}$ be the formal group we have associated to $\mathcal{P}$. Because the functor BT commutes with base change we obtain from (159) a homomorphism of formal groups:

$$BT(Fr_{\mathcal{P}}) : G \to G^{(p)}. \tag{160}$$

Then the last map (160) is the Frobenius homomorphism Fr_G of the formal group G.

Proof. — Let $\mathcal{N} \in \mathrm{Nil}_R$ be a nilpotent $R-$algebra. Let $\mathcal{N}_{[p]} \in \mathrm{Nil}_R$ be the nilpotent $R-$algbra obtained by base change via the absolute Frobenius $\mathrm{Frob} : R \to R$. Taking the p-th power gives an $R-$algebra homomorphism

$$Fr_{\mathcal{N}} : \mathcal{N} \to \mathcal{N}_{[p]}. \tag{161}$$

The Frobenius of any functor is obtained by applying it to (161). In particular the Frobenius for the functor $\hat{W}$ is just the usual operator ^{F}:

$${}^F : \hat{W}(\mathcal{N}) \to \hat{W}(\mathcal{N}_{[p]}) = \hat{W}(\mathcal{N}).$$

From this remark we obtain a commutative diagram:

$$
\begin{tikzcd}
\hat{W}(\mathcal{N}) \otimes_{W(R)} P \arrow[r] \arrow[d, "{}^{F}\otimes id_P"'] & G(\mathcal{N}) \arrow[d, "Fr_G"] \\
\hat{W}(\mathcal{N}_{[p]}) \otimes_{W(R)} P \arrow[r] & G(\mathcal{N}_{[p]})
\end{tikzcd}
\tag{162}
$$

The left lower corner in this diagram may be identified with $\hat{W}(\mathcal{N}) \otimes_{F,W(R)} P \cong \hat{W} \otimes_{W(R)} P^{(p)}$. All we need to verify is that for $\xi \in \hat{W}(\mathcal{N})$ and $x \in P$ the elements ${}^{F}\xi \otimes x \in \hat{W}(\mathcal{N}) \otimes_{F,W(R)} P$ and $\xi \otimes V^{\#}x \in \hat{W}(\mathcal{N}) \otimes_{W(R)} P^{(p)}$ have the same image by the lower horizontal map of (162). Since P is generated as an abelian group by elements of the form $uV^{-1}y$, where $y \in Q$ and $u \in W(R)$, it is enough to verify the equality of the images for $x = uV^{-1}y$. But in $\hat{W}(\mathcal{N}) \otimes_{F,W(R)} P$ we have the equalities:

$$ {}^{F}\xi \otimes uV^{-1}y = {}^{F}(\xi u) \otimes V^{-1}y = V^{-1}(\xi u \otimes y) $$

The last element has the same image in $G(\mathcal{N}_{[p]})$ as $\xi u \otimes y$, by the exact sequence (147). Hence our proposition follows from the equality:

$$ \xi \otimes V^{\#}(uV^{-1}y) = \xi u \otimes y $$

We note that here the left hand side is considered as an element of $\hat{W} \otimes_{W(R)} P^{(p)}$, while the right hand side is considered as an element of $\hat{W} \otimes_{F,W(R)} P$. □

Proposition 88. — *Let R be a ring, such that $pR = 0$. Let $\mathcal{P}$ be a display over R. Then there is a number N and a morphism of displays $\gamma : \mathcal{P} \to \mathcal{P}^{(p^N)}$ such that the following diagram becomes commutative:*

$$
\begin{tikzcd}
\mathcal{P} \arrow[r, "p"] \arrow[d, "Fr^N_{\mathcal{P}}"'] & \mathcal{P} \arrow[dl, "\gamma"'] \\
\mathcal{P}^{(p^N)} &
\end{tikzcd}
$$

Proof. — By (29) $Fr_{\mathcal{P}}$ is induced by the homomorphism $V^{\#} : P \to W(R) \otimes_{F,W(R)} P$. First we show that a power of this map factors through multiplication by p. By the definition of a display there is a number M, such that $V^{M\#}$ factors through:

$$ V^{M\#} : P \to I_R \otimes_{F^M,W(R)} P \tag{163} $$

Hence the homomorphism $V^{(M+1)\#}$ is given by the composite of the following maps:

$$
\begin{tikzcd}
P \arrow[r, "V^{\#}"] & W(R) \otimes_{F,W(R)} P \arrow[r, "W(R)\otimes V^{M\#}"] & W(R) \otimes_{F,W(R)} I_R \otimes_{F^M,W(R)} P \arrow[d] \\
 & & W(R) \otimes_{F^{M+1},W(R)} P
\end{tikzcd}
\tag{164}
$$

Here the vertical arrow is induced by the map $W(R) \otimes_{F,W(R)} I_R \to W(R)$ such that $\xi \otimes \zeta \mapsto \xi\, {}^{F}\zeta$. We note that this map is divisible by p., because there is also the map $\kappa : W(R) \otimes_{F,W(R)} I_R \to W(R)$ given by $\xi \otimes {}^{V}\eta \mapsto \xi\eta$. Composing the horizontal maps in the diagram (164) with κ we obtain a map $\gamma_0 : P \to W(R) \otimes_{F^{M+1},W(R)} P$, such that $\gamma_0 p = V^{(M+1)\#}$. For any number m we set $\gamma_m = V^{m\#}\gamma_0$. Then we have $\gamma_m p = V^{(M+m+1)\#}$.

Secondly we claim that for a big number m the homomorphism γ_m induces a homomorphism of displays. It follows from the factorization (163) that γ_M respects the Hodge filtration. We have to show that for $m \geq M$ big enough the following ^{F}-linear maps are zero:

$$F\gamma_m - \gamma_m F, \quad V^{-1}\gamma_m - \gamma_m V^{-1} \tag{165}$$

These maps become 0, if we multiply them by p. But the kernel of multiplication by p on $W(R) \otimes_{F^m,W(R)} P$ is $W(\mathfrak{a}) \otimes_{F^m,W(R)} P$, where $\mathfrak{a}$ is the kernel of the absolute Frobenius homomorphism Frob : $R \to R$. Because $W(\mathfrak{a})I_R = 0$, we conclude that the composite of the following maps induced by (163) is zero:

$$W(\mathfrak{a}) \otimes_{F^m,W(R)} P \to W(\mathfrak{a}) \otimes_{F^m,W(R)} I_R \otimes_{F^M,W(R)} P \to W(R) \otimes_{F^{M+m},W(R)} P$$

Hence γ_{2M} commutes with F and V^{-1} and is therefore a morphism of displays. This is the morphism γ we were looking for. □

Applying the functor BT to the diagram in the proposition we get immediately that $BT_{\mathcal{P}}$ is a p-divisible group. If p is nilpotent in R a formal group over R is p-divisible, iff its reduction mod p is p-divisible. Hence we obtain:

Corollary 89. — *Let p be nilpotent in R, and let $\mathcal{P}$ be a display over R. Then $BT_{\mathcal{P}}$ is a p-divisible group.*

We will now compute the Cartier module of the formal group $BT_{\mathcal{P}}$. By definition the Cartier ring $\mathbb{E}_R$ is the ring opposite to the ring $\mathrm{Hom}(\hat{W}, \hat{W})$. Any element $e \in \mathbb{E}_R$ has a unique representation:

$$e = \sum_{n,m \geq 0} V^n [a_{n,m}] F^m,$$

where $a_{n,m} \in R$ and for any fixed n the coefficients $a_{n,m} = 0$ for almost all m. We write the action $e : \hat{W}(\mathcal{N}) \to \hat{W}(\mathcal{N})$ as right multiplication. It is defined by the equation:

$$ue = \sum_{m,n \geq 0} {}^{V^m}([a_{n,m}]({}^{F^n}u)) \tag{166}$$

One can show by reducing to the case of a $\mathbb{Q}-$algebra that ${}^{F^n}u = 0$ for big n. Hence this sum is in fact finite.

Let G be a functor from Nil_R to the category of abelian groups, such that $G(0) = 0$. The Cartier module of G is the abelian group:

$$\mathbf{M}(G) = \mathrm{Hom}(\hat{W}, G), \tag{167}$$

with the left $\mathbb{E}_R-$module structure given by:

$$(e\phi)(u) = \phi(ue), \quad \phi \in \mathbf{M}(G),\ u \in \hat{W}(\mathcal{N}),\ e \in \mathbb{E}_R$$

Let P be a projective finitely generated $W(R)-$module. Let us denote by $\mathbf{G}_P$ the functor $\mathcal{N} \mapsto \hat{W}(\mathcal{N}) \otimes_{W(R)} P$. Then we have a canonical isomorphism :

$$\mathbb{E}_R \otimes_{W(R)} P \to \operatorname{Hom}(\hat{W}, \mathbf{G}_P) = \mathbf{M}(\mathbf{G}_P) \tag{168}$$

An element $e \otimes x$ from the left hand side is mapped to the homomorphism $u \mapsto ue \otimes x \in \hat{W}(\mathcal{N}) \otimes_{W(R)} P$.

Proposition 90. — *Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a 3n-display over R. By definition (147) we have a natural surjection of functors $\mathbf{G}_P \to BT_{\mathcal{P}}$. It induces a surjection of Cartier modules:*

$$\mathbb{E}_R \otimes_{W(R)} P \to \mathbf{M}(BT_{\mathcal{P}}) \tag{169}$$

The kernel of this map is the $\mathbb{E}_R$-submodule generated by the elements $F \otimes x - 1 \otimes Fx$, for $x \in P$, and $V \otimes V^{-1}y - 1 \otimes y$, for $y \in Q$.

Proof. — We set $\mathbf{G}^0_{\mathcal{P}} = \mathbf{G}_P$ and we denote by $\mathbf{G}^{-1}_{\mathcal{P}}$ the subfunctor $\mathcal{N} \mapsto \hat{Q}_{\mathcal{N}}$. Let us denote the corresponding Cartier modules by $\mathbf{M}^0_{\mathcal{P}}$ respectively $\mathbf{M}^{-1}_{\mathcal{P}}$. By the first main theorem of Cartier theory, we obtain from (147) an exact sequence of Cartier modules:

$$0 \to \mathbf{M}^{-1}_{\mathcal{P}} \xrightarrow{\rho_{\mathcal{P}}} \mathbf{M}^0_{\mathcal{P}} \to \mathbf{M}(BT_{\mathcal{P}}) \to 0 \tag{170}$$

We have to compute $\rho_{\mathcal{P}}$ explicitly. Using a normal decomposition $P = L \oplus T$ we may write:

$$\mathbf{G}^{-1}_{\mathcal{P}}(\mathcal{N}) = \hat{W}(\mathcal{N}) \otimes_{W(R)} L \oplus \hat{I}_{\mathcal{N}} \otimes_{W(R)} T$$

The Cartier module of the last direct summand may be written as follows:

$$\begin{array}{ccc} \mathbb{E}_R F \otimes_{W(R)} T & \to & \operatorname{Hom}(\hat{W}, \hat{I} \otimes_{W(R)} T) \\ eF \otimes t & \mapsto & (u \mapsto ueF \otimes t) \end{array} \tag{171}$$

From this we easily see that $\mathbf{M}^{-1}_{\mathcal{P}} \subset \mathbf{M}^0_{\mathcal{P}}$ is the subgroup generated by all elements $eF \otimes x$, where $e \in \mathbb{E}_R$ and by all elements $e \otimes y$, where $e \in \mathbb{E}_R$ and $y \in Q$.

The map $V^{-1} : \mathbf{G}^{-1}_{\mathcal{P}} \to \mathbf{G}^0_{\mathcal{P}}$ is defined by the equations:

$$\begin{array}{lcll} V^{-1}(u \otimes y) & = & uV \otimes V^{-1}y, & u \in \hat{W},\ (\mathcal{N})\ y \in Q \\ V^{-1}(uF \otimes x) & = & u \otimes Fx, & x \in P \end{array} \tag{172}$$

Hence on the Cartier modules $V^{-1} - id$ induces a map $\rho_{\mathcal{P}} : \mathbf{M}^{-1}_{\mathcal{P}} \to \mathbf{M}^0_{\mathcal{P}}$, which satisfies the equations:

$$\begin{array}{lcll} \rho_{\mathcal{P}}(eF \otimes x) & = & e \otimes Fx - eF \otimes x, & x \in P \\ \rho_{\mathcal{P}}(e \otimes y) & = & eV \otimes V^{-1}y - e \otimes y, & y \in Q \end{array} \tag{173}$$

This proves the proposition. □

3.2. The universal extension. — Grothendieck and Messing have associated to a $p-$divisible group G over R a crystal $\mathbb{D}_G$, which we will now compare with the crystal $\mathcal{D}_{\mathcal{P}}$, if $\mathcal{P}$ is a display with associated formal $p-$divisible group $G = BT(\mathcal{P})$.

Let us first recall the theory of the universal extension [Me] in terms of Cartier theory [Z2].

Let S be a $\mathbb{Z}_p-$algebra and L an $S-$module. We denote by $C(L) = \prod_{i=0}^{\infty} V^i L$, the abelian group of all formal power series in the indeterminate V with coefficients in L. We define on $C(L)$ the structure of an $\mathbb{E}_S-$module by the following equations

$$\begin{aligned}
\xi\left(\sum_{i=0}^{\infty} V^i l_i\right) &= \sum_{i=0}^{\infty} V^i w_n(\xi) l_i \quad , \quad for \quad \xi \in W(S), l_i \in L \\
V\left(\sum_{i=0}^{\infty} V^i l_i\right) &= \sum_{i=0}^{\infty} V^{i+1} l_i \\
F\left(\sum_{i=0}^{\infty} V^i l_i\right) &= \sum_{i=1}^{\infty} V^{i-1} p l_i
\end{aligned}$$

The module $C(L)$ may be interpreted as the Cartier module of the additive group of L :

Let $\hat{L}^+$ be the functor on the category Nil_S of nilpotent $S-$algebras to the category of abelian groups, which is defined by

$$\hat{L}^+(\mathcal{N}) = (\mathcal{N} \otimes_S L)^+.$$

Then one has a functor isomorphism:

$$\begin{array}{ccc}
\mathcal{N} \otimes_S L & \cong & \hat{W}(\mathcal{N}) \otimes_{\mathbb{E}_S} C(L) \\
n \otimes l & \mapsto & [n] \otimes V^0 l
\end{array}$$

Consider a $pd-$thickening $S \to R$ with kernel $\mathfrak{a}$. Let G be a $p-$divisible formal group over R and $M = M_G = \mathbf{M}(G)$ be its Cartier module (167), which we will regard as an $\mathbb{E}_S-$module.

Definition 91. — *An extension (L, N) of M by the $S-$module L is an exact sequence of $\mathbb{E}_S-$modules*

$$0 \to C(L) \to N \to M \to 0, \tag{174}$$

such that N is a reduced $\mathbb{E}_S-$module, and $\mathfrak{a}N \subset V^0 L$, where $\mathfrak{a} \subset W(S) \subset \mathbb{E}_S$ is the ideal in $W(S)$ defined after (48).

***Remark*:** We will denote $V^0 L$ simply by L and call it the submodule of exponentials of $C(L)$ respectively N. A morphism of extensions $(L, N) \to (L', N')$ consists of a morphism of $S-$modules $\varphi : L \to L'$ and a homomorphism of $\mathbb{E}_S-$modules

$u : N \to N'$ such that the following diagram is commutative

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C(L) & \longrightarrow & N & \longrightarrow & M & \longrightarrow & 0 \\ & & {\scriptstyle C(\varphi)}\big\downarrow & & \big\downarrow{\scriptstyle u} & & \big\| & & \\ 0 & \longrightarrow & C(L') & \longrightarrow & N' & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

More geometrically an extension as in definition 91 is obtained as follows. Let $\widetilde{G}$ be a lifting of the $p-$divisible formal group G to a $p-$divisible formal group over S, which may be obtained by lifting the display $\mathcal{P}$ to S. Let $\mathbb{W}$ be the vector group associated to a locally free finite $S-$module W. Consider an extension of f.p.p.f. sheaves over $\mathrm{Spec}S$:

$$0 \to \mathbb{W} \to E \to \widetilde{G} \to 0 \tag{175}$$

The formal completion of (175) is an exact sequence of formal groups (i.e. a sequence of formal groups, such that the corresponding sequence of Lie algebras is exact). Hence we have an exact sequence of Cartier modules.

$$0 \to C(W) \to M_{\hat{E}} \to M_{\widetilde{G}} \to 0,$$

$\hat{E}$ being the formal completion of E.

We have $\mathfrak{a}M_{\hat{E}} \simeq \mathfrak{a} \otimes_S \mathrm{Lie}E$. We let $L = W + \mathfrak{a}\mathrm{Lie}E$ as submodule of $\mathrm{Lie}E$ or equivalently of $M_{\hat{E}}$. Since L is killed by F we obtain an exact sequence

$$0 \to C(L) \to M_{\hat{E}} \to M_G \to 0,$$

which is an extension in the sense of definition 91. Conversely we can start with a sequence (174). We choose a lifting of M/VM to a locally free $S-$module P. Consider any map ρ making the following diagram commutative.

$$\begin{array}{ccc} N/VN & \longrightarrow & M/VM \\ & {\scriptstyle\rho}\searrow & \big\uparrow \\ & & P \end{array} \tag{176}$$

Let $W = \ker \rho$. Then $L = W + \mathfrak{a}(N/VN)$ as a submodule of $\mathrm{Lie}N$. The quotient of N by $C(W)$ is a reduced $\mathbb{E}_S-$module and hence the Cartier module of a formal group $\widetilde{G}$ over S, which lifts G. We obtain an extension of reduced $\mathbb{E}_S-$modules

$$0 \longrightarrow C(W) \longrightarrow N \longrightarrow M_{\widetilde{G}} \longrightarrow 0,$$

and a corresponding extension of formal groups over S

$$0 \longrightarrow \hat{W}^+ \longrightarrow \hat{E} \longrightarrow \widetilde{G} \longrightarrow 0.$$

Then the push–out by the natural morphism $\hat{W}^+ \longrightarrow \mathbb{W}$ is an extension of f.p.p.f. sheaves (175).

These both constructions are inverse to each other. Assume we are given two extensions $(\mathbb{W}, E, \widetilde{G})$ and $(\mathbb{W}_1, \mathbb{E}_1, \widetilde{G}_1)$ of the form (175). Then a morphism between the corresponding extensions of Cartier modules in the sense of definition 91 may be geometrically described as follows. The morphism consists of a pair (u, v_R), where u :

$E \longrightarrow E_1$ is a morphism of f.p.p.f. sheaves and $v_R : \mathbb{W}_R \longrightarrow \mathbb{W}_{1,R}$ a homomorphism of vector groups over R. The following conditions are satisfied.

1) We have a commutative diagram for the reductions over R:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{W}_R \arrow[r] \arrow[d, "v_R"] & E_R \arrow[r] \arrow[d, "u"] & G \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & \mathbb{W}_{1,R} \arrow[r] & E_{1,R} \arrow[r] & G_1 \arrow[r] & 0 \end{tikzcd}$$

2) For any lifting $\widetilde{v} : \mathbb{W} \to \mathbb{W}_1$ of v_R to a homomorphism of vector groups the map:

$$\widetilde{v} - u_{|\hat{\mathbb{W}}} : \hat{\mathbb{W}}. \longrightarrow \hat{E}_1$$

factors through a linear map $W \to \mathfrak{a} \otimes \mathrm{Lie} E_1$:

$$\hat{\mathbb{W}} \longrightarrow (\mathfrak{a} \otimes \mathrm{Lie} E_1)^\wedge \xrightarrow{\exp} \hat{E}_1.$$

Here the second map is given by the natural inclusion of Cartier modules $C(\mathfrak{a} M_{\hat{E}_1}) \subset M_{\hat{E}_1}$ or equivalently by the procedure in Messing's book [Me] (see [Z2]). This dictionary between extensions used by Messing and extensions of Cartier modules in the sense of definition 91, allows us to use a result of Messing in a new formulation:

Theorem 92. — *Let $S \to R$ be a pd-thickening with nilpotent divided powers. Let G be a formal $p-$divisible group over R. Then there exists a universal extension $(L^{\mathrm{univ}}, N^{\mathrm{univ}})$ of G by a $S-$module L^{univ}.*

Then any other extension (L, N) in sense of definition 91 is obtained by a unique $S-$module homomorphism $L^{\mathrm{univ}} \to L$.

Proof. — This is [Me] Chapt. 4 theorem 2.2. □

***Remark*:** The definition of the universal extension over S is based on the exponential map

$$\exp : (\mathfrak{a} \otimes \mathrm{Lie} E)^\wedge \longrightarrow E^\wedge,$$

which we simply defined using Cartier theory and the inclusion $\mathfrak{a} \subset W(S)$ given by the divided powers on $\mathfrak{a}$. In the case of a formal p-divisible group it makes therefore sense to ask whether Messing's theorem 92 makes sense for any pd-thickening and not just nilpotent ones. We will return to this question in proposition 96

Since we consider p-divisible groups without an étale part, this theorem should be true without the assumption that the divided powers are nilpotent. This would simplify our arguments below. But we don't know a reference for this.

The crystal of Grothendieck and Messing deduced from this theorem is defined by

$$\mathbb{D}_G(S) = \mathrm{Lie} N^{\mathrm{univ}}.$$

Lemma 93. — *Let $S \to R$ be a pd$-$thickening with nilpotent divided powers. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over R. By proposition 44 there exist up to canonical isomorphism a unique triple $(\widetilde{P}, F, V^{-1})$, which lifts (P, F, V^{-1}), such that V^{-1} is defined on the inverse image $\hat{Q} \subset \widetilde{P}$ of Q.*

Then the universal extension of $BT(\mathcal{P})$ is given by the following exact sequence of $\mathbb{E}_S-$*modules*

$$0 \to C(\hat{Q}/I_S\widetilde{P}) \to \mathbb{E}_S \otimes_{W(S)} \widetilde{P}/(F \otimes x - 1 \otimes Fx)_{x\in\widetilde{P}} \to M(\mathcal{P}) \to 0, \tag{177}$$

where the second arrow maps $y \in \hat{Q}$ to $V \otimes V^{-1}y - 1 \otimes y$, and the third arrow is given by the canonical map $\widetilde{P} \longrightarrow P$.

Proof. — By [Z1] the $\mathbb{E}_S-$module N in the middle of the sequence (177) is a reduced Cartier module, and the canonical map $\widetilde{P} \longrightarrow \mathbb{E}_S \otimes_{W(S)} \tilde{P}, x \longmapsto 1 \otimes x$ provides an isomorphism $\widetilde{P}/I_S\widetilde{P} \simeq N/VN$.

Let us verify that the arrow $C(\hat{Q}/I_S\widetilde{P}) \to N$ in the sequence (177) is well-defined. Clearly $y \longmapsto V \otimes V^{-1}y - 1 \otimes y$ is a homomorphism of abelian groups $\hat{Q} \longrightarrow N$. The subgroup $I_S\widetilde{P}$ is in the kernel:

$$V \otimes V^{-1}\ {}^Vwx - 1 \otimes\ {}^Vwx = V \otimes wFx - 1 \otimes\ {}^Vwx =$$

$$VwF \otimes x - 1 \otimes\ {}^Vwx =\ {}^Vwx - 1 \otimes\ {}^Vwx = 0,$$

for $w \in W(S), x \in \widetilde{P}$.

Moreover one verifies readily that $F(V \otimes V^{-1}y - 1 \otimes y) = 0$ in N. Then the image of $\hat{Q} \longrightarrow N$ is in a natural way an $S-$module, $\hat{Q}/I_S\widetilde{P} \to N$ is an $S-$module homomorphism, and we have a unique extension of the last map to a $\mathbb{E}_S-$module homomorphism

$$C(\hat{Q}/I_S\widetilde{P}) \longrightarrow N.$$

We see that (177) is a complex of $V-$reduced $\mathbb{E}_S-$modules. Therefore it is enough to check the exactness of the sequence (177) on the tangent spaces, which is obvious.

We need to check that (177) is an extension in the sense of definition 91, i.e. $\mathfrak{a} \cdot N \subset \hat{Q}/I_S\widetilde{P}$, where $\hat{Q}/I_S\widetilde{P}$ is regarded as a subgroup of N by the second map of (177) and $\mathfrak{a} \subset W(S)$ as an ideal.

Indeed, let $a \in \mathfrak{a}$, $x \in \widetilde{P}$ and $\xi = \sum V^i[\xi_{ij}i]F^j \in \mathbb{E}_S$. Then $a\xi \otimes x = a\sum_j [\xi_{0j}]F^j \otimes x = 1 \otimes a\sum [\xi_{0j}]F^jx$. Hence it is enough to verify that an element of the form $1 \otimes ax$ is in the image of $\hat{Q} \to N$. But we have

$$V \otimes V^{-1}ax - 1 \otimes ax = -1 \otimes ax.$$

It remains to be shown that the extension (177) is universal. Let

$$0 \to C(L^{\text{univ}}) \to N^{\text{univ}} \to M(\mathcal{P}) \to 0$$

be the universal extension. For any lifting of $M(\mathcal{P})$ to a reduced Cartier module $\widetilde{M}$ over S, There is a unique morphism $N^{\text{univ}} \longrightarrow M$, which maps L^{univ} to $\mathfrak{a} \cdot \widetilde{M}$. Let $\widetilde{L}$ be the kernel of $L^{\text{univ}} \longrightarrow \mathfrak{a}\widetilde{M}$. Then it is easy to check that

$$0 \longrightarrow C(\widetilde{L}) \longrightarrow N^{\text{univ}} \longrightarrow \widetilde{M} \longrightarrow 0 \tag{178}$$

is the universal extension of $\widetilde{M}$. Hence conversely starting with a universal extension (178) of $\widetilde{M}$, we obtain the universal extension of M over S as

$$0 \longrightarrow C(\widetilde{L} + \mathfrak{a}N^{\mathrm{univ}}) \longrightarrow N^{\mathrm{univ}} \longrightarrow M \longrightarrow 0,$$

where the sum $\widetilde{L} + \mathfrak{a}N^{\mathrm{univ}}$ is taken in $\mathrm{Lie}N^{\mathrm{univ}}$.

Now let $\widetilde{Q} \subset \hat{Q}$ be an arbitrary $W(S)-$submodule, such that $\widetilde{\mathcal{P}} = (\widetilde{P}, \widetilde{Q}, F, V^{-1})$ is a display. By the consideration above it suffices to show that

$$0 \longrightarrow C(\widetilde{Q}/I_S\widetilde{P}) \longrightarrow N \longrightarrow M(\widetilde{\mathcal{P}}) \longrightarrow 0 \tag{179}$$

is the universal extension of $M(\widetilde{\mathcal{P}})$ over S. In other words, we may assume $R = S$.

Starting from the universal extension (178) for $\widetilde{M} = M(\widetilde{\mathcal{P}})$, we get a morphism of finitely generated projective modules $\widetilde{L} \longrightarrow \widetilde{Q}/I_S\widetilde{P}$. To verify that this is an isomorphism it suffices by the lemma of Nakayama to treat the case, where $S = R$ is a perfect field. In this case we may identify $M(\widetilde{\mathcal{P}})$ with $\widetilde{P}$. The map $\widetilde{P} \longrightarrow \mathbb{E}_S \otimes_{W(S)} \widetilde{P}, \quad x \mapsto 1 \otimes x$ induces the unique $W(S)[F]-$linear section σ of

$$\begin{tikzcd} 0 \arrow[r] & C(\widetilde{Q}/I_S\widetilde{P}) \arrow[r] & N \arrow[r] & \widetilde{P} \arrow[l, bend right, "\sigma"'] \arrow[r] & 0, \end{tikzcd}$$

such that $V\sigma(x) - \sigma(Vx) \in \widetilde{Q}/I_S\widetilde{P}$ (compare [Z1], 2, 2.5 or [Ra-Zi] 5.26). The extension is classified up to isomorphism by the induced map $\sigma : \widetilde{P} \longrightarrow N/VN$. Since this last map is $\widetilde{P} \longrightarrow \widetilde{P}/I_S\widetilde{P}$ the extension is clearly universal. $\square$

Our construction of the universal extension (177) makes use of the existence of the triple $(\widetilde{P}, F, V^{-1})$. If we have a pd-morphism $\varphi : W(R) \longrightarrow S$, we know how to write down this triple explicity (corollary 56). Hence we obtain in this case a complete description of the universal extension over S only in terms of (P, Q, F, V^{-1}). Indeed, let $\overline{Q}_\varphi$ be the inverse image of Q/IP be the map

$$S \otimes_{W(R)} P \longrightarrow R \otimes_{W(R)} P.$$

Then the universal extension is given by the sequence

$$0 \longrightarrow C(\overline{Q}_\varphi) \longrightarrow \mathbb{E}_S \otimes_{W(R)} P/(F \otimes x - 1 \otimes Fx)_{x \in P} \longrightarrow M(\mathcal{P}) \longrightarrow 0, \tag{180}$$

where the tensor product with $\mathbb{E}_S$ is given by $\delta_\varphi : W(R) \longrightarrow W(S)$ (compare (97)). The second arrow is defined as follows. For an element $\bar{y} \in \bar{Q}_\phi$ we choose a lifting $y \in Q_\phi \subset W(S) \otimes_{W(R)} P$. Then we write:

$$1 \otimes y \in \mathbb{E}_S \otimes_{W(S)} (W(S) \otimes_{W(R)} P) = \mathbb{E}_S \otimes_{W(R)} P$$

With this notation the image of $\bar{y}$ by the second arrow of (180) is $V \otimes V_\varphi^{-1}y - 1 \otimes y$.

One may specialize this to the case of the $pd-$thickening $S = W_m(R) \rightarrow R$, and then go to the projective limit $W(R) = \varprojlim_m W_m(R)$. Then the universal extension over $W(R)$ takes the remarkable simple form:

$$
\begin{aligned}
0 \longrightarrow C(Q) \longrightarrow \mathbb{E}_{W(R)} \otimes_{W(R)} P/(F \otimes x - 1 \otimes Fx)_{x \in P} &\longrightarrow M(\mathcal{P}) \longrightarrow 0 \\
y \longmapsto \quad V \otimes V^{-1}y - 1 \otimes y &
\end{aligned} \tag{181}
$$

3.3. Classification of p-divisible formal groups. — The following main theorem gives the comparison between Cartier theory and the crystalline Dieudonné theory of Grothendieck and Messing.

Theorem 94. — *Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a display over a ring R, such that p is nilpotent in R. Let $G = BT(\mathcal{P})$ be the associated formal $p-$divisible group. Then there is a canonical isomorphism of crystals on the crystalline site of nilpotent pd-thickenings over* Spec R*:*

$$\mathcal{D}_{\mathcal{P}} \xrightarrow{\ \sim\ } \mathbb{D}_G$$

It respects the Hodge filtration on $\mathcal{D}_{\mathcal{P}}(R)$ respectively $\mathbb{D}_G(R)$.

Let $S \to R$ be a pd-thickening with nilpotent divided powers. Assume we are given a morphism $W(R) \longrightarrow S$ of topological pd-thickenings of R. Then there is a canonical isomorphism:

$$S \otimes_{W(R)} P \cong \mathbb{D}_G(S).$$

Remark: We will remove the restriction to the nilpotent crystalline site below (corollary 97).

Proof. — In the notation of lemma 93 we find $\mathcal{D}_{\mathcal{P}}(S) = \widetilde{P}/I_S\widetilde{P}$ and this is also the Lie algebra of the universal extension of G over S, which is by definition the value of the crystal $\mathbb{D}_G$ at S. □

Corollary 95. — *Let $S \to R$ be a surjective ring homomorphsim with nilpotent kernel. Let $\mathcal{P}$ be a display over R and let G be the associated formal p-divisible group. Let $\tilde{G}$ be a formal p-divisible group over S, which lifts G. Then there is a lifting of $\mathcal{P}$ to a display $\tilde{\mathcal{P}}$ over S, and an isomorphism $BT(\tilde{\mathcal{P}}) \to \tilde{G}$, which lifts the identity $BT(\mathcal{P}) \to G$.*

Moreover let $\mathcal{P}'$ be a second display over R, and let $\alpha : \mathcal{P} \to \mathcal{P}'$ be a morphism. Assume we are given a lifting $\tilde{\mathcal{P}}'$ over S of $\mathcal{P}'$. We denote the associated formal p-divisible groups by $\tilde{G}'$ respectively G'. Then the morphism α lifts to a morphism of displays $\tilde{\mathcal{P}} \to \tilde{\mathcal{P}}'$, iff $BT(\alpha) : G \to G'$ lifts to a homomorphsim of formal p- divisible groups $\tilde{G} \to \tilde{G}'$.

Proof. — Since $S \to R$ may be represented as a composition of nilpotent pd-thickenings, we may assume that $S \to R$ itself is a nilpotent pd-thickening. Then the left hand side of the isomorphism of theorem 94 classifies liftings of the display $\mathcal{P}$ by theorem 48 and the right hand side classifies liftings of the formal p-divisible group G by Messing [Me] Chapt V theorem (1.6). Since the constructions are functorial in $\mathcal{P}$ and G the corollary follows: □

Proposition 96. — *Let $\mathcal{P}$ be a display over R. Let $S \to R$ be a pd-thickening with nilpotent kernel $\mathfrak{a}$. Then the extension of lemma 93 is universal (i.e. in the sense of the remark after Messing's theorem 92).*

Proof. — We denote by G the formal p-divisible group associated to $\mathcal{P}$. Any lifting $\tilde{G}$ of G to S gives rise to an extension of M_G in the sense of definition 91:

$$0 \to C(\mathfrak{a}M_{\tilde{G}}) \to M_{\tilde{G}} \to M_G \to 0$$

With the notation of the proof of lemma 93 we claim that there is a unique morphism of extensions $N \to M_{\tilde{G}}$. Indeed, the last corollary shows that $\tilde{G}$ is the p-divisible group associated to a display $\tilde{\mathcal{P}}(\tilde{G})$ which lifts the display $\mathcal{P}$. Hence $\tilde{\mathcal{P}}(\tilde{G})$ is of the form $(\tilde{P}, \tilde{Q}, F, V^{-1})$, where $(\tilde{P}, F, V^{-1})$ is the triple in the formulation of lemma 93. But then the description of the Cartier module $M_{\tilde{G}}$ in terms of the display gives immediately a canonical morphism of Cartier modules $N \to M_{\tilde{G}}$. Its kernel is $C(L)$, where L is the kernel of the map $\tilde{P}/I_S\tilde{P} \to \operatorname{Lie}\tilde{G}$, i.e. the Hodge filtration determined by $\tilde{G}$. This shows the uniquenes of $N \to M_{\tilde{G}}$.

Now let us consider any extension:

$$0 \to C(L_1) \to N_1 \to M(\mathcal{P}) \to 0$$

Using the argument (176), we see that there is a lifting $\tilde{G}$ of G, such that the extension above is obtained from

$$0 \to C(U_1) \to N_1 \to M_{\tilde{G}} \to 0.$$

Let $\tilde{Q} \subset \tilde{P}$ be the display which corresponds to $\tilde{G}$ by the last corollary. Then by lemma 93 the universal extension of $M_{\tilde{G}}$ is :

$$0 \to C(\tilde{Q}/I_S\tilde{P}) \to N \to M_{\tilde{G}} \to 0$$

This gives the desired morphism $N \to N_1$. It remains to show the uniqueness. But this follows because for any morphism of extensions $N \to N_1$ the following diagram is commutative:

$$\begin{array}{ccc} N & \longrightarrow & N_1 \\ \downarrow & & \downarrow \\ M_{\tilde{G}} & \longrightarrow & M_{\tilde{G}} \end{array}$$

Indeed we have shown, that the morphism of extensions $N \to M_{\tilde{G}}$ is unique. □

***Remark*:** Let $\mathcal{P}$ be the display of a p-divisible formal group G. Then we may extend the definition of the crystal $\mathbb{D}_G$ to all pd-thickenings $S \to R$ (not necessarily nilpotent) whose kernel is a nilpotent ideal, by setting:

$$\mathbb{D}_G(S) = \operatorname{Lie} E_S,$$

where E_S is the universal extension of G over S, which exist by the proposition above.

This construction is functorial in the following sense. Let $\mathcal{P}'$ be another display over R and denote the associated formal p-divisible group by G'. Then any homomorphism

$a : G \rightarrow G'$ induces by the universality of the universal extension a morphism of crystals:

$$\mathbb{D}(a) : \mathbb{D}_G \rightarrow \mathbb{D}_{G'}.$$

Corollary 97. — *If we extend $\mathbb{D}_G$ to the whole crystalline site as above, the theorem 94 continues to hold, i.e. we obtain a canonical isomorphism of crystals:*

$$\mathcal{D}_{\mathcal{P}} \longrightarrow \mathbb{D}_G \tag{182}$$

Proof. — This is clear. □

Proposition 98. — *The functor BT from the category of displays over R to the category of formal $p-$divisible groups over R is faithful, i.e. if $\mathcal{P}$ and $\mathcal{P}'$ are displays over R, the map*

$$\mathrm{Hom}(\mathcal{P}, \mathcal{P}') \longrightarrow \mathrm{Hom}(BT(\mathcal{P}), BT(\mathcal{P}'))$$

is injective.

Proof. — Let $\mathcal{P} = (P, Q, F, V^{-1})$ and $\mathcal{P}' = (P', Q', F, V^{-1})$ be the displays and G and G' the associated $p-$divisible groups. Assume $\alpha : \mathcal{P} \longrightarrow \mathcal{P}'$ is a morphism of displays. It induces a morphism $a : G \longrightarrow G'$.

But the last corollary gives α back if we apply to a the functor $\mathbb{D}$:

$$\mathbb{D}_G(W(R)) \longrightarrow \mathbb{D}_{G'}(W(R))$$

□

Proposition 99. — *Let p be nilpotent in R and assume that the set of nilpotent elements in R form a nilpotent ideal. Then the functor BT of proposition 98 is fully faithful.*

We need a preparation before we can prove this.

Lemma 100. — *Let $\mathcal{P}$ and $\mathcal{P}'$ be displays over R. Let $a : G \rightarrow G'$ be a morphism of the associated $p-$divisible groups over R. Assume that there is an injection $R \longrightarrow S$ of rings, such that $a_S : G_S \longrightarrow G'_S$ is induced by a morphism of displays $\beta : \mathcal{P}_S \longrightarrow \mathcal{P}'_S$. Then a is induced by a morphism of displays $\alpha : \mathcal{P} \longrightarrow \mathcal{P}'$.*

Proof. — The morphism $W(R) \rightarrow R$ is a pd-thickening. By the corollary 97 a induces a map $\alpha : P \longrightarrow P'$, namely the map induced on the Lie algebras of the universal extensions (181). Therefore α maps Q to Q'. By assumption the map $\beta = W(S) \otimes_{W(R)} \alpha : W(S) \otimes_{W(R)} P \longrightarrow W(S) \otimes_{W(R)} P'$ commutes with F and V^{-1}. Then the same is true for α because of the inclusions $P \subset W(S) \otimes_{W(R)} P$, $P' \subset W(S) \otimes_{W(R)} P'$. Hence α is a morphism of displays. By proposition 98 $BT(\alpha)$ is a. □

Proof. — (of the proposition): If $R = K$ is a perfect field, the proposition is true by classical Dieudonné theory. For any field we consider the perfect hull $K \subset K^{\mathrm{perf}}$ and apply the last lemma. Next assume that $R = \prod_{i \in I} K_i$ is a product of fields. We denote the base change $R \longrightarrow K_i$ by an index i. A morphism of $p-$divisible groups

$G \longrightarrow G'$, is the same thing as a family of morphisms of $p-$divisible groups $G_i \longrightarrow G'_i$ over each K_i. Indeed, one can think of G in terms of systems of finite locally free group schemes. Then one needs only to observe that any finitely generated projective module L over R is of the form $\prod L_i$, since it is a direct summand of R^n. Next one observes that the same statements are true for morphisms of displays $\mathcal{P} \longrightarrow \mathcal{P}'$, because $W(R) = \prod W(K_i)$ etc. Hence the case where R is a product of fields is established. Since a reduced ring may be embedded in a product of fields we may apply the lemma to this case. The general case follows from corollary 95 if we divide out the nilpotent ideal of nilpotent elements. □

We now give another criterion for the fully faithfulness of the functor BT, which holds under slightly different assumptions.

Proposition 101. — *Let R be an $\mathbb{F}_p$-algebra. We assume that there exists a topological pd-thickening $(S, \mathfrak{a}_n)$ of R, such that the kernels of $S/\mathfrak{a}_n \to R$ are nilpotent, and such that S is a p-adic torsion free ring.*

Then the functor BT from the category of displays over R to the category of p-divisible formal groups is fully faithful.

Proof. — Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be displays over R, and let G_1 and G_2 be the p-divisible formal groups associated by the functor BT. We show that a given homomorphism of p-divisible groups $a : G_1 \to G_2$ is induced by a homomorphism of displays $\mathcal{P}_1 \to \mathcal{P}_2$.

The homomorphism a induces a morphism of filtered F-crystals $a_{\mathcal{D}} : \mathbb{D}_{G_1} \to \mathbb{D}_{G_2}$ on the crystalline site. Since we have identified (corollary 97) the crystals $\mathbb{D}$ and $\mathcal{D}$ on this site, we may apply proposition 60 to obtain a homomorphism $\phi : \mathcal{P}_1 \to \mathcal{P}_2$ of displays. We consider the triples $(\tilde{P}_1, F, V^{-1})$ and $(\tilde{P}_2, F, V^{-1})$, which are associated to $\mathcal{P}_1$ and $\mathcal{P}_2$, and the unique lifting of ϕ to a homomorphism $\tilde{\phi}$ of these triples. Then $\mathbb{D}_{G_i}(S)$ is identified with $\tilde{P}_i/I_S\tilde{P}_i$ for $i = 1, 2$. Let $\mathbb{E}_{1,S}$ and $\mathbb{E}_{2,S}$ be the universal extensions of G_1 and G_2 over S. By the proposition loc.cit. the homomorphism $a_{\mathcal{D}}(S) : \mathrm{Lie}\ \mathbb{E}_{1,S} \to \mathrm{Lie}\ \mathbb{E}_{2,S}$ coincides with the identifications made, with the homomorphism induced by $\tilde{\phi}$:

$$\tilde{\phi} : \tilde{P}_1/I_S\tilde{P}_1 \to \tilde{P}_2/I_S\tilde{P}_2$$

Let us denote by $b : G_1 \to G_2$ the homomorphism $BT(\phi)$. Then by theorem 94 b induces on the crystals the same morphism as ϕ.

The two maps $\mathbb{E}_{1,S} \to \mathbb{E}_{2,S}$ induced by a and b coincide therefore on the Lie algebras. But then these maps coincide because the ring S is torsionfree. Hence we conclude that a and b induce the same map $\mathbb{E}_{1,R} \to \mathbb{E}_{2,R}$, and finally that $a = b$. □

Proposition 102. — *Let k be a field. Then the functor BT from the category of displays over k to the category of formal p-divisible groups over k is an equivalence of categories.*

Proof. — By proposition 99 we know that the functor BT is fully faithful. Hence we have to show that any p-divisible formal group X over k is isomorphic to $BT(\mathcal{P})$ for some display $\mathcal{P}$ over k. Let ℓ be the perfect closure of k. Let $\bar{X} = X_\ell$ be the formal p-divisible group obtained by base change. By Cartier theory we know that $\bar{X} = BT(\bar{\mathcal{P}})$ for some display $\bar{\mathcal{P}}$ over ℓ.

Now we apply descent with respect to the inclusion $q : k \to \ell$. Let q_1 and q_2 be the two natural maps $\ell \to \ell \otimes_k \ell$. Let $\bar{X}_i$ respectively $\bar{\mathcal{P}}_i$ be the objects obtained by base change with respect to q_i for $i = 1, 2$. Our result would follow if we knew that the functor BT is fully faithful over $\ell \otimes_k \ell$. Indeed in this case the descent datum $\bar{X}_1 \cong \bar{X}_2$ defined by X would provide an isomorphism $\bar{\mathcal{P}}_1 \cong \bar{\mathcal{P}}_2$. This isomorphism would be a descent datum (i.e. satisfy the cocycle condition) because by proposition 98 the functor BT is faithful. Hence by theorem 37 it would give the desired display $\mathcal{P}$ over k.

By proposition 101 it is enough to find a topological pd-thickening $S \to \ell \otimes_k \ell$, such that S is a torsion free p-adic ring. We choose a Cohen ring C of k and embedding $C \to W(\ell)$ [AC] IX, §2, 3. Then we consider the natural surjection:

$$W(\ell) \otimes_C W(\ell) \longrightarrow \ell \otimes_k \ell \tag{183}$$

The ring $A = W(\ell) \otimes_C W(\ell)$ is torsionfree because $W(\ell)$ is flat over C. The kernel of (183) is pA. We define S as the p-adic completion:

$$S = \varprojlim_n A/p^n A.$$

Then S is a torsionfree p-adic ring, such that $S/pS \cong \ell \otimes_k \ell$. this follows by going to the projective limit in the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A/p^nA & \xrightarrow{p} & A/p^{n+1}A & \longrightarrow & A/pA & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{=} & & \\
0 & \longrightarrow & A/p^{n-1} & \xrightarrow{p} & A/p^nA & \longrightarrow & A/pA & \longrightarrow & 0
\end{array}$$

But with the canonical divided powers on pS the topological pd-thickening $S \to \ell \otimes_k \ell$ is the desired object. □

Theorem 103. — *Let R be an excellent local ring or a ring such that R/pR is of finite type over a field k. Then the functor BT is an equivalence from the category of displays over R to the category of formal $p-$divisible groups over R.*

Proof. — We begin to prove this for an Artinian ring R. Since BT is a fully faithful functor, we need to show that any $p-$divisible group G over R comes from a display $\mathcal{P}$. Let $S \to R$ be a pd-thickening. Since we have proved the theorem for a field, we may assume by induction that the theorem is true for R. Let G be a $p-$divisible group over R with $BT(\mathcal{P}) = G$. The liftings of G respectively of $\mathcal{P}$ correspond functorially to the liftings of the Hodge filtration to

$$\mathcal{D}_{\mathcal{P}}(S) = \mathbb{D}_G(S).$$

Hence the theorem is true for S.

More generally if $S \to R$ is surjective with nilpotent kernel the same reasoning shows that the theorem is true for S, if it is true for R.

Next let R be a complete noetherian local ring. We may assume that R is reduced. Let $\mathfrak{m}$ be the maximal ideal of R. We denote by G_n the $p-$divisible group $G_{R/\mathfrak{m}^n}$

obtained by base change from G. Let $\mathcal{P}_n$ be the display over $R/\mathfrak{m}^n$, which correspond to G_n. Then $\mathcal{P} = \varprojlim \mathcal{P}_n$ is a 3n-display over R. Consider the formal group H over R which belongs to the reduced Cartier module $M(\mathcal{P})$. Since $\mathcal{P}_n$ is obtained by base change from $\mathcal{P}$ and consequently $M(\mathcal{P}_n)$ from $M(\mathcal{P})$ too, we have canonical isomorphisms $H_n \cong G_n$. Hence we may identify H and G. Clearly we are done, if we show the following assertion. Let $\mathcal{P} = (P, Q, F, V^{-1})$ be a 3n-display over R, such that $M(\mathcal{P})$ is the Cartier module of a $p-$divisible formal group of height equal to the rank of P. Then $\mathcal{P}$ is nilpotent.

Indeed, it is enough to check the nilpotence of $\mathcal{P}_S$ over an arbitrary extension $S \supset R$, such that $p \cdot S = 0$ (compare (15)). Since R admits an injection into a finite product of algebraically closed fields, we are reduced to show the assertion above in the case, where R is an algebraically closed field. In this case we have the standard decomposition

$$\mathcal{P} = \mathcal{P}^{\text{nil}} \oplus \mathcal{P}^{\text{et}}$$

where $\mathcal{P}^{\text{nil}}$ is a display and $\mathcal{P}^{\text{et}}$ is a 3n-display with the structural equations

$$V^{-1}e_i = e_i, \qquad \text{for} \quad i = 1 \cdots h.$$

Then

$$M(\mathcal{P}^{\text{et}}) = \bigoplus_{i=1}^{h} \mathbb{E}_R e_i/(Ve_i - e_i),$$

is zero, because $V - 1$ is a unit in $\mathbb{E}_R$. We obtain $M(\mathcal{P}) = M(\mathcal{P}^{\text{nil}}) = P^{\text{nil}}$. Hence the height of the $p-$divisible group G is $\operatorname{rank}_R P^{\text{nil}}$. Our assumption $\text{height}G = \operatorname{rank}_R P$ implies $P = P^{\text{nil}}$. This finishes the case, where R is a complete local ring.

Next we consider the case, where the ring R is an excellent local ring. As above we may assume R is reduced. Then the completion $\hat{R}$ is reduced. Since the geometric fibres of $\operatorname{Spec}\hat{R} \to \operatorname{Spec}R$, are regular, for any $R-$algebra L, which is a field, the ring $\hat{R} \otimes_R L$ is reduced. Hence if R is reduced, so is $\hat{R} \otimes_R \hat{R}$. Consider the diagram:

$$R \xrightarrow{\ p\ } \hat{R} \ \underset{p_2}{\overset{p_1}{\rightrightarrows}}\ \hat{R} \otimes_R \hat{R}$$

Let G be a $p-$divisible formal group over R. It gives a descent datum on $p^*G = G_{\hat{R}}$:

$$a : p_1^* G_{\hat{R}} \longrightarrow p_2^* G_{\hat{R}}.$$

We find a display $\hat{\mathcal{P}}$ over $\hat{R}$, such that $BT(\hat{\mathcal{P}}) = G_{\hat{R}}$. Since the functor BT is fully faithful over $\hat{R} \otimes_R \hat{R}$ by proposition 99 the isomorphism a is induced by an isomorphism

$$\alpha : p_1^* \hat{\mathcal{P}} \longrightarrow p_2^* \hat{\mathcal{P}}$$

From the corollary 98 it follows that α satisfies the cocycle condition. By theorem 37 there is a display $\mathcal{P}$ over R, which induces $(\hat{\mathcal{P}}, \alpha)$. Since the application of the functor BT gives us the descent datum for G, it follows by the usual descent theory for $p-$divisible groups, that $BT(\mathcal{P}) = G$.

Finally we consider the case of a finitely generated $W(k)-$algebra R. We form the faithfully flat $R-$algebra $S = \prod R_{\mathfrak{m}}$, where $\mathfrak{m}$ runs through all maximal ideals of R. Then we will apply the same reasoning as above to the sequence

$$R \longrightarrow S \quad \underset{p_2}{\overset{p_1}{\rightrightarrows}} \quad S \otimes_R S.$$

We have seen, that it is enough to treat the case, where R is reduced. Assume further that Spec$R$ is connected, so that G has constant height.

We see as in the proof of proposition 99, that to give a $p-$divisible group of height h over $\prod R_{\mathfrak{m}}$ is the same thing as to give over each $R_{\mathfrak{m}}$ a $p-$divisible group of height h. The same thing is true for displays. (One must show that the order N of nilpotence in (15) is idenpendent of $\mathfrak{m}$. But the usual argument in linear algebra shows also in $p-$linear algebra that $N = h - d$ is enough.) Since each ring $R_{\mathfrak{m}}$ is excellent with perfect residue field, we conclude that $G_S = BT(\widetilde{\mathcal{P}})$ for some display $\widetilde{\mathcal{P}}$ over S. We may apply descent if we prove that the ring $S \otimes_R S$ is reduced. This will finish the proof. Let us denote by $Q(R)$ the full ring of quotients. Then we have an injection

$$\left(\prod R_{\mathfrak{m}}\right) \otimes_R \left(\prod R_{\mathfrak{m}}\right) \hookrightarrow \left(\prod Q\left(R_{\mathfrak{m}}\right)\right) \otimes_{Q(R)} \left(\prod Q\left(R_{\mathfrak{m}}\right)\right)$$

The idempotent elements in $Q(R)$ allows to write the last tensor product as

$$\bigoplus_{\substack{\mathfrak{p} \in \operatorname{Spec} R \\ \mathfrak{p} \text{ minimal}}} \left(\left(\prod\nolimits_{\mathfrak{m}} Q\left(R_{\mathfrak{m}}/\mathfrak{p}R_{\mathfrak{m}}\right)\right) \otimes_{Q(R/\mathfrak{p}R)} \left(\prod\nolimits_{\mathfrak{m}} Q\left(R_{\mathfrak{m}}/\mathfrak{p}R_{\mathfrak{m}}\right)\right)\right)$$

We set $K = Q(R/gR)$. Then we have to prove that for any index set I the tensor product

$$\left(\prod_{i \in I} K\right) \otimes_K \left(\prod_{i \in I} K\right).$$

But any product of separable (= geometrically reduced) $K-$algebras is separable, because $\prod$ commutes with the tensor product by a finite extension E of K. $\square$

4. Duality

4.1. Biextensions. — Biextensions of formal group were introduced by Mumford [Mu]. They may be viewed as a formalization of the concept of the Poincaré bundle in the theory of abelian varieties. Let us begin by recalling the basic definitions (loc.cit.).

Let A, B, C be abelian groups. An element in $\operatorname{Ext}^1(B \otimes^{\mathbb{L}} C, A)$ has an interpretation, which is similiar to the usual interpretation of $\operatorname{Ext}^1(B, A)$ by Yoneda.

Definition 104. — *A biextension of the pair B, C by the abelian group A consists of the following data:*

1) *A set G and a surjective map*

$$\pi : G \longrightarrow B \times C$$

2) *An action of A on G, such that G becomes a principal homogenous space with group A and base $B \times C$.*

3) *Two maps*

$$+_B : G \times_B G \longrightarrow G \quad +_C : G \times_C G \longrightarrow G,$$

where the map $G \to B$ used to define the fibre product, is the composite of π with the projection $B \times C \to B$, and where $G \to C$ is defined in the same way.

One requires that the following conditions are verified:

(i) *The maps of 3) are equivariant with respect to the morphism $A \times A \to A$ given by the group law.*

(ii_B) *The map $+_B$ is an abelian group law of G over B, such that the following sequence is an extension of abelian groups over B:*

$$\begin{array}{ccccccc} 0 \to & B \times A & \longrightarrow & G & \xrightarrow{\pi} & B \times C & \to 0 \\ & b \times a & \mapsto & a + 0_B(b) & & & \end{array}$$

Here $0_B : B \to G$ denotes the zero section of the group law $+_B$ and $a + 0_B(b)$ is the given action of A on G.

(ii_C) *The same condition as (ii_B) but for C.*

(iii) *The group laws $+_B$ and $+_C$ are compatible in the obvious sense:*

Let $x_{i,j} \in G, 1 \leq i, j \leq 2$ be four elements, such that $pr_B(x_{i,1}) = pr_B(x_{i,2})$ and $pr_C(x_{1,i}) = pr_C(x_{2,i})$ for $i = 1, 2$. Then

$$(x_{11} +_B x_{12}) +_C (x_{21} +_B x_{22}) = (x_{11} +_C x_{21}) +_B (x_{12} +_C x_{22}).$$

Remark: The reader should prove the following consequence of these axioms:

$$0_B(b_1) +_C 0_B(b_2) = 0_B(b_1 + b_2)$$

The biextension of the pair B, C by A form a category which will be denoted by $\mathrm{BIEXT}^1(B \times C, A)$. If $A \to A'$ respectively $B' \to B$ and $C' \to C$ are homomorphism of abelian groups, one obtians an obvious functor

$$\mathrm{BIEXT}^1(B \times C, A) \longrightarrow \mathrm{BIEXT}^1(B' \times C', A').$$

Any homomorphism in the category $\mathrm{BIEXT}^1(B \times C, A)$ is an isomorphism. The automorphism group of an object G is canonically isomorphic of the set of bilinear maps

$$\mathrm{Bihom}(B \times C, A). \tag{184}$$

Indeed if α is a bilinear map in (184), the corresponding automorphism of G is given by $g \mapsto g + \alpha(\pi(g))$.

If $b \in B$, we denote by G_b or $G_{b \times C}$ the inverse image of $b \times C$ by π. Then $+_B$ induces on G_b the structure of an abelian group, such that

$$0 \longrightarrow A \longrightarrow G_b \longrightarrow C \longrightarrow 0$$

is a group extension. Similiarily one defines G_c for $c \in C$.

A trivialization of a biextension G is a "bilinear" section $s : B \times C \to G$, i.e. $\pi \circ s = \mathrm{id}_{B \times C}$, and $s(b, -)$ for each $b \in B$ is a homomorphism $C \to G_b$, and $s(-, c)$ for each $c \in C$ is a homomorphism $B \to G_C$. A section s defines an isomorphism of G with the trivial biextension $A \times B \times C$.

We denote by $\mathrm{Biext}^1(B \times C, A)$ the set of isomorphism classes in the category $\mathrm{BIEXT}^1(B \times C, A)$. It can be given the structure of an abelian group (using cocycles or Baer sum). The zero element is the trivial biextension.

An exact sequence $0 \to B_1 \to B \to B_2 \to 0$ induces an exact sequence of abelian groups

$$0 \to \mathrm{Bihom}(B_2 \times C, A) \to \mathrm{Bihom}(B \times C, A) \to \mathrm{Bihom}(B_1 \times C, A) \xrightarrow{\delta}$$
$$\mathrm{Biext}^1(B_2 \times C, A) \to \mathrm{Biext}^1(B \times C, A) \to \mathrm{Biext}^1(B_1 \times C, A)$$

The connecting homomorphism δ is obtained by taking the push–out of the exact sequence

$$0 \to B_1 \times C \to B \times C \to B_2 \times C \to 0,$$

by a bilinear map $\alpha : B_1 \times C \to A$. More explicitly this push-out is the set $A \times B \times C$ modulo the equivalence relation:

$$(a, b_1 + b, c) \equiv (a + \alpha(b_1, c), b, c), \quad a \in A,\ b \in B\ c \in C, b_1 \in B_1$$

If $0 \to A_1 \to A \to A_2 \to 0$ is an exact sequence of abelian groups, one obtains an exact sequence:

$$0 \to \mathrm{Bihom}(B \times C, A_1) \to \mathrm{Bihom}(B \times C, A) \to \mathrm{Bihom}(B \times C, A_2) \xrightarrow{\delta}$$
$$\mathrm{Biext}^1(B \times C, A_1) \to \mathrm{Biext}^1(B \times C, A) \to \mathrm{Biext}^1(B \times C, A_2)$$

We omit the proof of the following elementary lemma:

Lemma 105. — *If B and C are free abelian groups, one has*

$$\mathrm{Biext}^1(B \times C, A) = 0.$$

This lemma gives us the possibility to compute Biext^1 by resolutions:

Proposition 106. — *(Mumford) Assume we are given exact sequences $0 \to K_1 \to K_0 \to B \to 0$ and $0 \to L_1 \to L_0 \to C \to 0$. Then one has an exact sequence of abelian groups*

$$\mathrm{Bihom}(K_0 \times L_0, A) \to \mathrm{Bihom}(K_0 \times L_1, A) \times_{\mathrm{Bihom}(K_1 \times L_1, A)} \mathrm{Bihom}(K_1 \times L_0, A)$$
$$\to \mathrm{Biext}^1(B \times C, A) \to \mathrm{Biext}^1(K_0 \times L_0, A)$$

Proof. — One proves more precisely that to give a biextension G of $B \times C$ together with a trivialization over $K_0 \times L_0$:

$$\begin{tikzcd} G \arrow[r] & B \times C \\ & K_0 \times L_0 \arrow[ul, "s"] \arrow[u] \end{tikzcd}$$

is the same thing as to give bilinear maps $\xi : K_0 \times L_1 \to A$ and $\mu : K_1 \times L_0 \to A$, which have the same restriction on $K_1 \times L_1$. We denote this common restriction by $\varphi : K_1 \times L_1 \to A$.

Using the splitting 0_B of the group extension

$$0 \longrightarrow A \longrightarrow G_{B\times 0} \longrightarrow B \longrightarrow 0,$$

we may write

$$s(k_0, l_1) = 0_B(b_0) + \xi(k_0, l_1), \quad \text{for} \quad k_0 \in K_0, l_1 \in L_1, \tag{185}$$

where b_0 is the image of k_0 in B and $\xi(k_0, l_1) \in A$. This defines the bilinear map ξ. Similiarly we define μ:

$$s(k_1, l_0) = 0_C(c_0) + \mu(k_1, l_0), \tag{186}$$

for $k_1 \in K_1$ and $l_0 \in L_0$, where $c_0 \in C$ is the image of l_0. Clearly these maps are bilinear, since s is bilinear. Since $0_B(0) = 0_C(0)$ their restrictions to $K_1 \times L_1$ agree.

Conversely if ξ and μ are given, one considers in the trivial biextension $A \times K_0 \times L_0$ the equivalence relation

$$(a, k_0 + k_1, l_0 + l_1) \equiv (a + \xi(k_0, l_1) + \mu(k_1, l_0) + \xi(k_1, l_1), k_0, l_0).$$

Dividing out we get a biextension G of $B \times C$ by A with an obvious trivialization. $\square$

The following remark may be helpful. Let $l_0 \in L_0$ be an element with image $c \in C$. We embed $K_1 \to A \times K_0$ by $k_1 \mapsto (-\mu(k_1, l_0), k_1)$. Then the quotient $(A \times K_0)/K_1$ defines the group extension $0 \to A \to G_c \to B \to 0$.

Corollary 107. — *There is a canonical isomorphism:*

$$\mathrm{Ext}^1(B \otimes^{\mathbb{L}} C, A) \longrightarrow \mathrm{Biext}^1(B \times C, A).$$

Proof. — If B and C are free abelian groups one can show that any biextension is trivial (see (105)). One considers complexes $K_\bullet = \ldots 0 \to K_1 \to K_0 \to 0 \ldots$ and $L_\bullet = \ldots 0 \to L_1 \to L_0 \to 0 \ldots$ as in the proposition, where K_0 and L_0 are free abelian groups. In this case the proposition provides an isomorphism

$$H^1(\mathrm{Hom}(K_\bullet \otimes L_\bullet, A)) = \mathrm{Biext}^1(K \times L, A). \tag{187}$$

Let $T_\bullet = \ldots 0 \to T_2 \to T_1 \to T_0 \to 0 \ldots$ be the complex $K_\bullet \otimes L_\bullet$. Then the group (187) above is simply the cokernel of the map

$$\mathrm{Hom}(T_0 A) \longrightarrow \mathrm{Hom}(T_1/\mathrm{Im}T_2, A). \tag{188}$$

Let $\ldots P_i \to \cdots \to P_1 \twoheadrightarrow K_1 \to 0$ be any free resolution. We set $P_0 = K_0$ and consider the complex $P_\bullet = \cdots \to P_i \to \ldots P_1 \to P_0 \to 0$. The same process applied to the $L's$ yields $Q_\bullet = \cdots \to Q_1 \to \cdots \to Q_1 \to Q_0 \to 0$. Let $\widetilde{T} = P_\bullet \otimes Q_\bullet$. Then the complex

$$\ldots 0 \to \widetilde{T}_1/\mathrm{Im}\widetilde{T}_2 \to \widetilde{T}_0 \to \ldots$$

is identical with the complex

$$\ldots 0 \to T_1/\mathrm{Im}T_2 \to T_0 \to \ldots$$

Therefore the remark (188) yields an isomorphism

$$H^1(\mathrm{Hom}(K_\bullet \otimes L_\bullet, A)) \simeq H^1(\mathrm{Hom}(P_\bullet \otimes Q_\bullet, A)) = \mathrm{Ext}^1(B \otimes^{\mathbb{L}} C, A).$$

□

The notion of a biextension has an obvious generalization to any topos. This theory is developped in $SGA7$. We will consider the category Nil_R with the flat topology. To describe the topology it is convenient to consider the isomorphic category Aug_R (see definition 50). Let $(B, \epsilon) \in \mathrm{Aug}_R$ be an object, i.e. a morphism $\epsilon : B \to R$ of R-algebras. We write $B^+ = \mathrm{Ker}\,\epsilon$ for the augmentation ideal. We will often omit the augmentation from the notation, and write B instead of (B, ϵ).

If we are given two morphisms $(B, \varepsilon) \to (A_i, \varepsilon_i)$ for $i = 1, 2$, we may form the tensorproduct:

$$(A_1, \varepsilon_1) \otimes_{(B,\varepsilon)} (A_2, \varepsilon_2) = (A_1 \otimes_{B_1} A_2, \varepsilon_1 \otimes \varepsilon_2).$$

This gives a fibre product in the opposite category $\mathrm{Aug}_R^{\mathrm{opp}}$:

$$\mathrm{Spf}\, A_1 \times_{\mathrm{Spf}\, B} \mathrm{Spf}\, A_2 = \mathrm{Spf}(A_1 \otimes_B A_2).$$

Via the Yoneda embedding we will also consider $\mathrm{Spf}\, B$ as a functor on Nil_R:

$$\mathrm{Spf}\, B(\mathcal{N}) = \mathrm{Hom}_{\mathrm{Nil}\, R}(B^+, \mathcal{N}).$$

We equip $\mathrm{Aug}_R^{\mathrm{opp}}$ with a Grothendieck topology. A covering is simply a morphism $\mathrm{Spf}\, A \to \mathrm{Spf}\, B$, such that the corresponding ring homomorphism $B \to A$ is flat. We note that in our context flat morphisms are automatically faithfully flat. We may define a sheaf on $\mathrm{Aug}_R^{\mathrm{opp}}$ as follows.

Definition 108. — *A functor $F : \mathrm{Aug}_R \to \mathrm{Sets}$ is called a sheaf, if for any flat homomorphism $B \to A$ in Aug_R the following sequence is exact.*

$$F(B) \to F(A) \rightrightarrows F(A \otimes_B A).$$

Recall that a left exact functor $G : \mathrm{Nil}_R \to (\mathrm{Sets})$ is a functor, such that $G(0)$ consists of a single point, and such that each exact sequence in Nil_R

$$0 \to \mathcal{N}_1 \to \mathcal{N}_2 \to \mathcal{N}_3 \to 0$$

induces an exact sequence of pointed sets

$$0 \to G(\mathcal{N}_1) \to G(\mathcal{N}_2) \to G(\mathcal{N}_3),$$

i.e. $G(\mathcal{N}_1)$ is the fibre over the point $G(0) \subset G(\mathcal{N}_3)$. It can be shown that such a functor respects fibre products in Nil_R. We remark that any left exact functor on Nil_R is a sheaf.

A basic fact is that an exact abelian functor on Nil_R has trivial Čech cohomology.

Proposition 109. — *Let $F : \mathrm{Nil}_R \to (Ab)$ be a functor to the category of abelian groups, which is exact. Then for any flat morphism $B \to A$ in Aug_R the following complex of abelian groups is exact*

$$F(B) \to F(A) \rightrightarrows F(A \otimes_B A) \substack{\to \\ \to \\ \to} F(A \otimes_B A \otimes_B A) \substack{\to \\ \to \\ \to \\ \to} \cdots$$

Proof. — Let $\mathcal{N}$ be a nilpotent B-algebra and $B \to C$ be a homomorphism in Aug_R. then we define simplicial complexes:

$$(189)\qquad \begin{gathered}(C^n(\mathcal{N}, B \to A), \theta_i^n)\\ (C^n(C, B \to A), \theta_i^n)\end{gathered}$$

for $n \geq 0$.

We set

$$C^n(\mathcal{N}, B \to A) = \mathcal{N} \otimes_B A \otimes_B \cdots \otimes_B A$$

$$C^n(C, B \to A) = C \otimes_B A \otimes_B \cdots \otimes_B A,$$

where in both equations we have $n+1$ factors on the right hand side. The operators $\theta_i^n : C^{n-1} \to C^n$ for $i = 0, \cdots, n$ are defined by the formulas:

$$\theta_i^n(x \otimes a_0 \otimes \cdots \otimes a_{n-1}) = (x \otimes a_0 \otimes \cdots \otimes a_{i-1} \otimes 1 \otimes a_i \cdots \otimes a_{n-1}),$$

where $x \in \mathcal{N}$ or $x \in C$.

One knows that the associated chain complexes with differential $\delta^n = \sum(-1)^i\theta_i^n$ are resolutions of $\mathcal{N}$ respectively C, if either $B \to A$ is faithfully flat or $B \to A$ has a section $s : A \to B$. In the latter case one defines

$$s^n : C^n \to C^{n-1}, s^n(x \otimes a_0 \otimes \cdots \otimes a_n) = xa_0 \otimes a_1 \otimes \cdots \otimes a_n.$$

If one sets $C^{-1} = \mathcal{N}$ respectively $C^{-1} = C$ and $\theta_0^0 : C^{-1} \to C^0, \theta_0^0(x) = x \otimes 1$, one has the formulas:

$$(190)\qquad s^n\theta_i^n = \begin{cases} \mathrm{id}_{C^{n-1}} & , \text{ for } \quad i = 0 \\ \theta_{i-1}^{n-1}s^{n-1} & , \text{ for } \quad i > 0 \quad \text{and} \quad n \geq 1. \end{cases}$$

Let us extend the chain complex (C^n, δ^n) by adding zeros on the left:

$$(191)\qquad 0 \to \cdots \to 0 \to C^{-1} \xrightarrow{\theta_0^0 = \delta^0} C^0 \xrightarrow{\delta^1} C^1 \xrightarrow{\delta^2} C^2 \to \cdots$$

Since by (190) we have $s^n\delta^n + \delta^{n-1}s^{n-1} = \mathrm{id}_{C^{n-1}}$, we have shown that this complex is homotopic to zero.

If $F : \mathrm{Nil}_R \to (Ab)$ is a functor we can apply F to the simplicial complexes (189), because θ_i^n are R-algebra homomorphisms. The result are simplicial complexes, whose associated simple complexes will be denoted by

$$(192)\qquad C^n(\mathcal{N}, B \to A, F) \quad \text{respectively} \quad C^n(C, B \to A, F).$$

Let us assume that $B \to A$ has a section. Then the extended complexes $C^n(F), n \in \mathbb{Z}$ are homotopic to zero by the homotopy $F(s^n)$, since we can apply F to the relations (190).

Let now F be an exact functor and assume that $B \to A$ is faithfully flat. If $\mathcal{N}^2 = 0$, each algebra $C^n(\mathcal{N}, B \to A)$ has square zero. In this case the δ^n in (191) are algebra homomorphisms. Therefore we have the right to apply F to (191). This sequence is an exact seuqence in Nil_R, which remains exact, if we apply F. Hence the extended complex $C^n(\mathcal{N}, B \to A, F), n \in \mathbb{Z}$ is acyclic if $\mathcal{N}^2 = 0$.

Any exact sequence $0 \to \mathcal{K} \to \mathcal{M} \to \mathcal{N} \to 0$ is Nil_B, gives an exact sequence of complexes.

$$0 \to C^n(\mathcal{K}, B \to A, F) \to C^n(\mathcal{M}, B \to A, F) \to C^n(\mathcal{N}, B \to A, F) \to 0.$$

Hence $C^n(\mathcal{N}, B \to A, F)$ is acyclic for any $\mathcal{N} \in \mathrm{Nil}_B$. Finally let $\mathfrak{a} \subset B$ be the kernel of the augmentation $B \to R$. Then one has an exact sequence of complexes:

$$0 \to C^n(\mathfrak{a}, B \to A, F) \to C^n(B, B \to A, F) \to C^n(B/\mathfrak{a}, B/\mathfrak{a} \to A/\mathfrak{a}, F) \to 0 \tag{193}$$

The augmentation of A induces a section of $B/\mathfrak{a} = R \to A/\mathfrak{a}$. Hence the last complex in the sequence (193) is acyclic. Since we have shown $C^n(\mathfrak{a}, B \to A, F)$ to be acyclic, we get that $C^n(B, B \to A, F)$ is acyclic. This was our assertion. $\square$

We reformulate the result in the language of sheaf theory.

Corollary 110. — *An exact functor $F : \mathrm{Nil}_R \to Ab$ is a sheaf on the Grothendieck topology $\mathcal{T} = \mathrm{Aug}_R^{\mathrm{opp}}$. For each covering $T_1 \to T_2$ in $\mathcal{T}$ the Čech cohomology groups $\check{H}^i(T_1/T_2, F)$ are zero for $i \geq 1$. In particular an F-torsor over an object of $\mathcal{T}$ is trivial.*

By *SGA*7 one has the notion of a biextension in the category of sheaves. If F, K, L are abelian sheaves a biextension in $\mathrm{BIEXT}^1(K \times L, F)$ is given by an F-torsor G over $K \times L$ and two maps $t_K : G \times_K G \to G$ and $t_L : G \times_L G \to G$, which satisfy some conditions, which should now be obvious. If F is moreover an exact functor, then any F torsor is trivial. Hence in this case we get for any $\mathcal{N} \in \mathrm{Nil}_R$, that $G(\mathcal{N})$ is a biextension of $K(\mathcal{N})$ and $L(\mathcal{N})$ is the category of abelian groups. This is the definition Mumford [Mu] uses.

4.2. Two propositions of Mumford. — We will now update some proofs and results in Mumford's article. We start with some general remarks. Let F be an exact functor. Let $G \xrightarrow{\pi} H$ be any F-torsor is the category of sheaves on $\mathcal{T}$. If $H = \mathrm{Spf}\, A$ is representable we know that π is trivial and hence smooth because F is smooth. (The word smooth is used in the formal sense [Z1] 2.28.) If H is not representable, π is still smooth since the base change of G by any $\mathrm{Spf}\, A \to H$ becomes smooth.

More generally any F-torsor over H is trivial if H is prorepresentable in the following sense:

There is a sequence of surjections in $\mathrm{Aug}\, R$:

$$\to \cdots \to A_{n+1} \to A_n \cdots \to A_1,$$

such that

$$H = \varinjlim \mathrm{Spf}\, A_i. \tag{194}$$

Then π has a section because it has a section over any $\mathrm{Spf}\, A_i$ and therefore over H as is seen by the formula:

$$\mathrm{Hom}(H, G) = \varprojlim \mathrm{Hom}(\mathrm{Spf}\, A_i, G)$$

Hence we have shown:

Lemma 111. — *Let $F : \mathrm{Nil}_R \to (Ab)$ be an exact functor. Then any F-torsor over a prorepresentable object H is trivial.*

For some purposes it is useful to state the first main theorem of Cartier theory in a relative form. From now on R will be a $\mathbb{Z}_{(p)}$-algebra.

Let B be an augmented nilpotent $R-$algebra. In order to avoid confusion we will write $\mathrm{Spf}_R\, B$ instead of $\mathrm{Spf}\, B$ in the following. Let $G : \mathrm{Nil}_R \to (\mathrm{Sets})$ be a left exact functor. There is an obvious functor $\mathrm{Nil}_B \to Nil_R$. The composite of this functor with G is the base change G_B.

Assume we are given a morphism $\pi : G \to \mathrm{Spf}_R\, B$, which has a section $\sigma : \mathrm{Spf}_R\, B \to G$. Then we associate to the triple (G, π, σ) a left exact functor on Nil_B:

Let $\mathcal{L} \in \mathrm{Nil}_B$ and let $B|\mathcal{L}| = B \oplus \mathcal{L}$ be the augmented B-algebra associated to it. Then $B|\mathcal{L}|$ is also an augmented R-algebra, with augmentation ideal $B^+ \oplus \mathcal{L}$. Then we define the restriction $\mathrm{Res}_B\, G(\mathcal{L})$ of G to be the fibre over σ of the following map

$$\mathrm{Hom}_{\mathrm{Spf}_R\, B}(\mathrm{Spf}_R\, B|\mathcal{L}|, G) \to \mathrm{Hom}_{\mathrm{Spf}_R\, B}(\mathrm{Spf}_R\, B, G).$$

The functor $G \mapsto \mathrm{Res}_B\, G$ defines an equivalence of the category of triples (G, π, σ) with the category of left exact funtors on Nil_B. We will call the triple (G, π, σ) a pointed left exact functor over Spf_B. It is useful to explain this formalism a little more.

Let us start with a left exact functor F on Nil_R. Then $F \times \mathrm{Spf}\, B \xrightarrow{\mathrm{pr}} \mathrm{Spf}\, B$ is naturally a pointed functor over $\mathrm{Spf}\, B$. The restriction of this pointed functor is F_B:

$$\mathrm{Res}_B(F \times \mathrm{Spf}\, B) = F_B.$$

Suppose that the B-algebra structure on $\mathcal{L}$ is given by a morphism $\varphi : B^+ \to \mathcal{L}$. Then we have also a map of augmented R-algebras $B|\mathcal{L}| \to R|\mathcal{L}|$, which is on the augmentation ideals $\varphi + \mathrm{id}_{\mathcal{L}} : B^+ \oplus \mathcal{L} \to \mathcal{L}$.

Lemma 112. — *Let $\varphi : B^+ \to \mathcal{L}$ be a morphism in Nil_R. Via φ we may consider $\mathcal{L}$ as an element of Nil_B. Then $\mathrm{Res}_B\, G(\mathcal{L})$ may be identified with the subset of elements of $G(\mathcal{L})$, which are mapped to φ by the morphism*

$$\pi_{\mathcal{L}} : G(\mathcal{L}) \longrightarrow \mathrm{Hom}(B^+, \mathcal{L}).$$

Proof. — Consider the two embeddings of nilpotent algebras $\iota_{\mathcal{L}} : \mathcal{L} \to B^+ \oplus \mathcal{L} = B|\mathcal{L}|^+, \iota_{\mathcal{L}}(l) = 0 \oplus l$ and $\iota_{B^+} : B^+ \to B^+ \oplus \mathcal{L} = B|\mathcal{L}|^+, \iota_{B^+}(b) = b \oplus 0$. Let us denote by $G_\sigma(B^+ \oplus \mathcal{L}) \subset G(B^+ \oplus \mathcal{L}) = \mathrm{Hom}(\mathrm{Spf}_R\, B|\mathcal{L}|, G)$ the fibre at σ of the map

$$\mathrm{Hom}(\mathrm{Spf}_R\, B|\mathcal{L}|, G) \to \mathrm{Hom}(\mathrm{Spf}_R\, B, G) \tag{195}$$

We have an isomorphism in Nil_R:

$$\begin{array}{ccc} B^+ \bigoplus \mathcal{L} & \xrightarrow{\sim} & B^+ \times \mathcal{L} \\ b \oplus l & \longmapsto & b \times (\varphi(b) + l) \end{array} \tag{196}$$

Let $G(B^+ \oplus \mathcal{L}) \to G(\mathcal{L})$ be the map induced by $B^+ \oplus \mathcal{L} \to \mathcal{L}, b \oplus l \to \varphi(b) + l$. It follows from the isomorphism (196) and the left exactness of G, that this map induces a bijection $G_\sigma(B^+ \oplus \mathcal{L}) \xrightarrow{\sim} G(\mathcal{L})$. Hence we have identified $G(\mathcal{L})$ with the fibre of (195) at σ. It remains to determine, which subset of $G(\mathcal{L})$ corresponds to $\mathrm{Hom}_{\mathrm{Spf}\, B}(\mathrm{Spf}\, B|\mathcal{L}|, G)$. But looking at the following commutative diagram

$$\begin{array}{ccc} G(B^+ \oplus \mathcal{L}) & \longrightarrow & G(\mathcal{L}) \\ {\scriptstyle \pi_{B^+\oplus\mathcal{L}}}\downarrow & & \downarrow{\scriptstyle \pi_{\mathcal{L}}} \\ \mathrm{Hom}(B^+, B^+ \oplus \mathcal{L}) & \longrightarrow & \mathrm{Hom}(B^+, \mathcal{L}) \end{array}$$

$$\iota_{B^+} \longmapsto \varphi$$

we see that this subset is exactly the fibre of $\pi_{\mathcal{L}}$ at φ. ☐

Conversely given a functor $H : \mathrm{Nil}_B \to (\mathrm{Sets})$, such that $H(0) = \{\mathrm{point}\}$. Then we obtain a functor $G : \mathrm{Nil}_R \to (\mathrm{Sets})$ by:

$$G(\mathcal{N}) = \bigsqcup_{\varphi: B^+ \to \mathcal{N}} H(\mathcal{N}_\varphi) \quad , \quad \mathcal{N} \in \mathrm{Nil}_R,$$

where $\mathcal{N}_\varphi$ is $\mathcal{N}$ considered as a B-algebra via φ. Then we have a natural projection $\pi : G(\mathcal{N}) \to \mathrm{Hom}(B^+, \mathcal{N})$, which maps $H(\mathcal{N}_\varphi)$ to φ. The distinguished point in each $H(\mathcal{N}_\varphi)$ defines a section σ of π.

In particular our remark shows that a group object in the category of arrows $G \to \mathrm{Spf}\, B$, such that G is a left exact functor on Nil_R is the same thing as a left exact functor $H : \mathrm{Nil}_B \to (Ab)$.

In Cartier theory one considers the following functors on Nil_R:

$$D(\mathcal{N}) = \mathcal{N}, \qquad \hat{\Lambda}(\mathcal{N}) = (1 + t\mathcal{N}[t])^\times, \quad \text{for } \mathcal{N} \in \mathrm{Nil}_R\,.$$

Here t is an indeterminate. The functor D is considered as a set valued functor, while $\hat{\Lambda}$ takes values in the category (Ab) of abelian groups. We embed D into $\hat{\Lambda}$ by the map $n \mapsto (1 - nt)$ for $n \in \mathcal{N}$.

Theorem 113. — *(Cartier): Let $G \xrightarrow{\pi} H$ be a morphism of functors on* Nil_R*. Assume that G is left exact and has the structure of an abelian group object over H. The embedding $D \subset \hat{\Lambda}$ induces a bijection.*

$$\mathrm{Hom}_{groups/H}(\hat{\Lambda} \times H, G) \longrightarrow \mathrm{Hom}_{pointed\ functors/H}\,(D \times H, G)\,.$$

Proof. — If H is the functor $H(\mathcal{N}) = \{\mathrm{point}\}$, $\mathcal{N} \in \mathrm{Nil}_R$ this is the usual formulation of Cartier's theorem [Z1]. To prove the more general formulation above, one first reduces to the case $H = \mathrm{Spf}\, B$. Indeed to give a group homomorphism $\hat{\Lambda} \times H \to G$ over H is the same thing as to give for any morphism $\mathrm{Spf}\, B \to H$ a morphism $\hat{\Lambda} \times \mathrm{Spf}\, B \to \mathrm{Spf}\, B \times_H G$ of groups over $\mathrm{Spf}\, B$.

Secondly the case $H = \mathrm{Spf}\, B$ is reduced to the usual theorem using the equivalence of pointed left exact functors over $\mathrm{Spf}\, B$ and left exact functors on Nil_B. ☐

The following map is a homomorphism of abelian functors:

$$\begin{array}{ccc} \hat{\Lambda}(\mathcal{N}) & \longrightarrow & \hat{W}(\mathcal{N}), \\ \prod(1 - x_i t^i) & \longmapsto & (x_{p^0}, x_{p^1}, \cdots, x_{p^k} \cdots) \end{array} \tag{197}$$

If we compose this with $D \subset \hat{\Lambda}$, we obtain an inclusion $D \subset \hat{W}$.

Let R be a $\mathbb{Q}$-algebra. Then the usual power series for the natural logarithm provides an isomorphism of abelian groups:

$$\log : \hat{\Lambda}(\mathcal{N}) = (1 + t\mathcal{N}[t])^+ \longrightarrow t\mathcal{N}[t]$$

The formula $\varepsilon_1 \left(\sum_{i \geq 1} n_i t^i \right) = \sum n_{p^k} t^{p^k}$. defines a projector $\varepsilon_1 : t\mathcal{N}[t] \to t\mathcal{N}[t]$. Then Cartier has shown that ε_1 induces an endomorphism of $\hat{\Lambda}$ over any $\mathbb{Z}_{(p)}$-algebra. Moreover the homomorphism (197) induces an isomorphism:

$$\epsilon_1 \hat{\Lambda} \cong \hat{W}.$$

We use this to embed $\hat{W}$ into $\hat{\Lambda}$.

Mumford remarked that Cartier's theorem provides a section κ of the natural inclusion

$$\mathrm{Hom}_{\mathrm{groups}/H}(\hat{W} \times H, G) \longrightarrow \mathrm{Hom}_{\text{pointed functors /H}}(\hat{W} \times H, G). \tag{198}$$

Indeed, let $\alpha : \hat{W} \times H \to G$ be a map of pointed set-valued functors. We define $\tilde{\kappa}(\alpha) : \hat{\Lambda} \times H \to G$ to be the unique group homomorphism, which coincides with α on $D \times H$ (use theorem 113). We get $\kappa(\alpha)$ as the composition of $\tilde{\kappa}(\alpha)$ with the inclusion $\hat{W} \times H \subset \hat{\Lambda} \times H$.

Proposition 114. — *Let $F : \mathrm{Nil}_R \to (Ab)$ be an exact functor. Then*

$$\mathrm{Ext}^1(\hat{W}, F) = 0,$$

where the Ext*-group is taken in the category of abelian sheaves on $\mathcal{T}$.*

Proof. — By the remark (194) a short exact sequence $0 \to F \to G \to \hat{W} \to 0$ has a set–theoretical section $s : \hat{W} \to G$. Then $\kappa(s)$ splits the sequence. □

***Remark*:** It is clear that this proposition also has a relative version. Namely in the category of abelian sheaves over any prorepresentable sheaf H in $\mathcal{T}$. we have:

$$\mathrm{Ext}^1_{\mathrm{groups}/H}(\hat{W} \times H, F \times H) = 0,$$

if H is prorepresentable. Indeed consider an extension

$$0 \to F \times H \to G \xrightarrow{\pi} \hat{W} \times H \to 0. \tag{199}$$

Then G is an F torsor over $\hat{W} \times H$ and hence trivial. Let σ be any section of π. Let us denote by $\iota : H \to \hat{W} \times H$ and $s_G : H \to G$ the zero sections of the group laws relative to H. We obtain a morphism $s_G - \sigma\iota : H \to F$. Let $\mathrm{pr}_2 : \hat{W} \times H \to H$ be the projection. Then we define a new section of π by

$$\sigma_{\mathrm{new}} = \sigma + (s_G - \sigma\iota)\,\mathrm{pr}_2\,. \tag{200}$$

Then σ_{new} is a morphism of pointed functors over H, i.e. it respects the sections s_G and ι. Hence we may apply the section κ of (198) to σ_{new}. This gives the desired section of (199).

If $G : \mathrm{Nil}_R \to Ab$ is any functor, we set

$$G^+(\mathcal{N}) = \operatorname{Ker}(G(\mathcal{N}) \longrightarrow G(0)). \tag{201}$$

Because of the map $0 \to \mathcal{N}$ we obtain a functorial decomposition

$$G(\mathcal{N}) = G^+(\mathcal{N}) \oplus G(0),$$

which is then respected by morphisms of functors. If G is in the category of abelian sheaves we find:

$$\operatorname{Ext}^1_{Ab}(\hat{W}, G) = \operatorname{Ext}^1_{Ab}(\hat{W}, G^+),$$

which vanishes if G^+ is exact.

Cartier's theorem applies to an abelian functor G, such that G^+ is left exact:

$$\operatorname{Hom}(\hat{\Lambda}, G) \simeq \operatorname{Hom}(\hat{\Lambda}, G^+) \simeq G^+(XR[\![X]\!]),$$

where the Hom are taken in the category of abelian functors on Nil_R. If F, G are abelian sheaves on $\mathcal{T}$, the sheaf of local homomorphisms is defined as follows:

$$\begin{aligned} \underline{\operatorname{Hom}}(F,G)(A^+) &= \operatorname{Hom}(F_A, G_A), \quad A \in \operatorname{Aug} R. \\ \underline{\operatorname{Hom}}(F,G)^+(A^+) &= \operatorname{Ker}(\operatorname{Hom}(F_A, G_A) \longrightarrow \operatorname{Hom}(F_R, G_R)). \end{aligned} \tag{202}$$

Cartier's theorem tells us that for a left exact functor G:

$$\begin{aligned} \underline{\operatorname{Hom}}(\hat{\Lambda}, G)(A^+) &= G(XA[\![X]\!]) \\ \underline{\operatorname{Hom}}^+(\hat{\Lambda}, G)(A^+) &= G(XA^+[\![X]\!]) \end{aligned} \tag{203}$$

In particular the last functor $\underline{\operatorname{Hom}}^+(\hat{\Lambda}, G)$ is exact if G is exact. Using the projector ϵ_1 we see that $\underline{\operatorname{Hom}}^+(\hat{W}, G)$ is also exact.

Proposition 115. — *(Mumford): Let F be an exact functor. Then*

$$\operatorname{Biext}^1(\hat{W} \times \hat{W}, F) = 0.$$

Proof. — We strongly recommend to read Mumford's proof, but here is his argument formulated by the machinery of homological algebra. We have an exact sequence (SGA7):

$$0 \to \operatorname{Ext}^1(\hat{W}, \underline{\operatorname{Hom}}(\hat{W}, F)) \to \operatorname{Biext}^1(\hat{W} \times \hat{W}, F) \to \operatorname{Hom}(\hat{W}, \underline{\operatorname{Ext}}^1(\hat{W}, F)).$$

The outer terms vanish, by proposition (114) and because the functor $\underline{\operatorname{Hom}}^+(\hat{W}, F)$ is exact. $\square$

Our next aim is the computation of $\operatorname{Bihom}(\hat{W} \times \hat{W}, \hat{\mathbb{G}}_m)$. Let us start with some remarks about endomorphisms of the functors W and $\hat{W}$.

Let R be any unitary ring. By definition the local Cartier ring $\mathbb{E}_R$ relative to p acts from the right on $\hat{W}(\mathcal{N})$. Explicitly this action is given as follows. The action of $W(R)$:

$$\hat{W}(\mathcal{N}) \times W(R) \longrightarrow \hat{W}(\mathcal{N}), \tag{204}$$

is induced by the multiplication in the Witt ring $W(R|\mathcal{N}|)$. The action of the operators $F, V \in \mathbb{E}_R$ is as follows

$$\underline{n}F = {}^{V}\underline{n}, \quad \underline{n}V = {}^{F}\underline{n}, \tag{205}$$

where on the right hand side we have the usual Verschiebung and Frobenius on the Witt ring. An arbitrary element of $\mathbb{E}_R$ has the form $\sum_{i=0}^{\infty} V^i \xi_i + \sum_{j=1}^{\infty} \mu_j F^j$, $\xi_i, \mu_j \in W(R)$, where $\lim \mu_j = 0$ in the V-adic topology on $W(R)$ (see corollary 8). We may write such an element (not uniquely) in the form: $\sum V^n \alpha_n$, where $\alpha_n \in W(R)[F]$.

By the following lemma we may extend the actions (204) and (204) to a right action of $\mathbb{E}_R$ on $\hat{W}(\mathcal{N})$.

Lemma 116. — *For any $\underline{n} \in \hat{W}(\mathcal{N})$ there exists a number r such that ${}^{F^r}\underline{n} = 0$.*

Proof. — Since $\underline{n}$ is a finite sum of elements of the form ${}^{V^s}[n]$, $n \in \mathcal{N}$ it suffices to show the lemma for $\underline{n} = [n]$. This is trivial. $\square$

We note that in the case, where p is nilpotent in R there is a number r, such that ${}^{F^r}W(\mathcal{N}) = 0$. Hence in this case the Cartier ring acts from the right on $W(\mathcal{N})$.

We write the opposite ring to $\mathbb{E}_R$ in the following form:

$$ {}^t\mathbb{E}_R = \left\{ \sum_{i=1}^{\infty} V^i \xi_i + \sum_{j=0}^{\infty} \mu_j F^j \mid \xi_i, \mu_j \in W(R), \lim \xi_i = 0 \right\} \tag{206}$$

The limit is taken in the V-adic topology. The addition and multiplication is defined in the same way as in the Cartier ring, i.e. we have the relations:

$$\begin{aligned} FV &= p \\ V\xi F &= {}^{V}\xi \\ F\xi &= {}^{F}\xi F \\ \xi V &= V {}^{F}\xi \end{aligned} \tag{207}$$

Then we have the antiisomorphism

$$t : \mathbb{E}_R \longrightarrow {}^t\mathbb{E}_R,$$

which is defined by $t(F) = V$, $t(V) = F$ and $t(\xi) = \xi$ for $\xi \in W(R)$. The ring ${}^t\mathbb{E}_R$ acts from the left on $\hat{W}(\mathcal{N})$:

$$F\underline{n} = {}^{F}\underline{n} \quad , \quad V\underline{n} = {}^{V}\underline{n}.$$

It is the endomorphism ring of $\hat{W}$ by Cartier theory.

We define $\bar{\mathbb{E}}_R$ to be the abelian group of formal linear combinations of the form:

$$\bar{\mathbb{E}}_R = \left\{ \sum_{i=1}^{\infty} V^i \xi_i + \sum_{j=0}^{\infty} \mu_j F^j . \right\} \tag{208}$$

There is in general no ring structure on $\bar{\mathbb{E}}_R$, which satisfies the relations (207). The abelian group ${}^t\mathbb{E}_R$ is a subgroup of $\bar{\mathbb{E}}_R$ by regarding an element from the right hand side of (206) as an element from the right hand side of (208). Obviously the left action of ${}^t\mathbb{E}_R$ on $\hat{W}(\mathcal{N})$ extends to a homomorphism of abelian groups

$$\bar{\mathbb{E}}_R \longrightarrow \operatorname{Hom}(\hat{W}, W). \tag{209}$$

We will write this homomorphism as

$$\underline{n} \longmapsto u\underline{n}$$

since it extends the left action of ${}^t\mathbb{E}_R$. We could also extend the right action of $\mathbb{E}_R$:

$$\underline{n} \longmapsto \underline{n}u.$$

Of course we get the formula

$$\underline{n}u = {}^t u\underline{n}.$$

The first theorem of Cartier theory tells us again that (209) is an isomorphism. By the remark after lemma (116), it is clear that in the case where p is nilpotent in R the homomorphism (209) extends to a homomorphism:

$$\bar{\mathbb{E}}_R \longrightarrow \operatorname{End}(W) \tag{210}$$

The reader can verify that there exists a ring structure on $\bar{\mathbb{E}}_R$ that satisfies (207), if p is nilpotent in R. In this case the map $t : \mathbb{E}_R \to {}^t\mathbb{E}_R$ extends to an antiinvolution of the ring $\bar{\mathbb{E}}_R$. Then (210) becomes a homomorphism of rings.

By Cartier theory we have an exact sequence:

$$0 \longrightarrow \hat{W}(\mathcal{N}) \xrightarrow{\cdot(F-1)} \hat{W}(\mathcal{N}) \xrightarrow{\text{hex}} \hat{\mathbb{G}}_m(\mathcal{N}) \longrightarrow 0 \tag{211}$$

The second arrow is the right multiplication by $(F-1) \in \mathbb{E}_R$, and hex is the so called Artin-Hasse exponential. For the following it is enough to take (211) as a definition of $\hat{\mathbb{G}}_m$. But we include the definition of hex for completeness. It is the composition of the following maps (compare (197)):

$$\hat{W}(\mathcal{N}) \xrightarrow{\sim} \varepsilon_1 \hat{\Lambda}(\mathcal{N}) \subset \hat{\Lambda}(\mathcal{N}) = (1 + t\mathcal{N}[t])^{\times} \xrightarrow{t=1} (1+\mathcal{N})^{\times}. \tag{212}$$

It is easy to produce a formula for hex but still easier if one does not know it. The verification of the exactness of (211) is done by reduction to the case of a $\mathbb{Q}$-algebra $\mathcal{N}$. We will skip this.

Proposition 117. — *The Artin-Hasse exponential defines an isomorphism of abelian groups:*

$$\varkappa : W(R) \longrightarrow \operatorname{Hom}(\hat{W}, \hat{\mathbb{G}}_m) \tag{213}$$

An element $\xi \in W(R)$ corresponds to the following homomorphism $\varkappa_\xi : \hat{W} \to \hat{\mathbb{G}}_m$. If $u \in \hat{W}(\mathcal{N})$, we have:

$$\varkappa_\xi(u) = \mathrm{hex}(\xi \cdot u).$$

Proof. — This is a well–known application of the first main theorem of Cartier theory of p-typical curves. Let $[X] = (X, 0 \cdots 0 \cdots)$ be the standard p-typical curve in $\hat{W}(XK[\![X]\!])$. We have to show that $\mathrm{hex}(\xi \cdot [X])$ gives exactly all p-typical curves of $\hat{\mathbb{G}}_m$ if ξ runs through $W(R)$. We set $\gamma_m = \mathrm{hex}([X])$. This is the standard p-typical curve in $\hat{\mathbb{G}}_m$. It satisfies $F\gamma_m = \gamma_m$ by (211). By definition of the action of the Cartier ring on the p-typical curves of $\hat{\mathbb{G}}_m$ we have:

$$\mathrm{hex}(\xi\lfloor X\rceil) = \xi\gamma_m.$$

If $\xi = \sum V^i[\xi_i]F^i$ as elements of $\mathbb{E}_R$ we obtain:

$$\xi\gamma_m = \sum_{i=0}^{\infty} V^i[\xi_i]\gamma_m.$$

These are exactly the p-typical curves of $\hat{\mathbb{G}}_m$. □

From (201) we deduce the following sheafified version of the proposition:

Corollary 118. — *The homomorphism (213) gives rise to an isomorphism of functors on* Nil_R*:*

$$\varkappa : W(\mathcal{N}) \longrightarrow \underline{\mathrm{Hom}}(\hat{W}, \hat{\mathbb{G}}_m)^+(\mathcal{N}).$$

We are now ready to classify the bilinear forms $\mathrm{Bihom}(\hat{W} \times \hat{W}, \hat{\mathbb{G}}_m)$. To each $u \in \bar{\mathbb{E}}_R$ we associate the bilinear form β_u :

$$\begin{array}{ccccccc} \hat{W}(\mathcal{N}) \times \hat{W}(\mathcal{N}) & \longrightarrow & W(\mathcal{N}) \times \hat{W}(\mathcal{N}) & \xrightarrow{\text{mult.}} & \hat{W}(\mathcal{N}) & \xrightarrow{\text{hex}} & \hat{\mathbb{G}}_m(\mathcal{N}) \\ \xi \times \eta & \longmapsto & \xi u \times \eta & \longmapsto & (\xi u)\eta & & \end{array}$$

Proposition 119. — *We have the relations:*

$$\beta_u(\xi, \eta) = \beta_{{}^t u}(\eta, \xi)$$
$$\mathrm{hex}(\xi u)\eta = \mathrm{hex}\,\xi(u\eta).$$

Proof. — Clearly the second relation implies the first one. For $u \in W(R)$ we have $(\xi u)\eta = \xi(u\eta)$. Hence the assertion is trivial.

First we do the case $u = F$:

$$\mathrm{hex}(\xi F)\eta = \mathrm{hex}\ {}^V\xi\eta = \mathrm{hex}\ {}^V(\xi^F\eta) =$$
$$\mathrm{hex}(\xi^F\eta)F = \mathrm{hex}\,\xi\ {}^F\eta = \mathrm{hex}\,\xi(F\eta).$$

The fourth equation holds because:

$$\mathrm{hex}(\hat{W}(\mathcal{N})(F-1)) = 0$$

Secondly let $u = V$:

$$\mathrm{hex}(\xi V)\eta = \mathrm{hex}\ {}^F\xi\eta = \mathrm{hex}\ {}^V({}^F\xi\eta) = \mathrm{hex}\,\xi\ {}^V\eta = \mathrm{hex}\,\xi(V\eta).$$

Finally we have to treat the general case $u = \sum_{i=1}^{\infty} V^i w_i + \sum_{i=0}^{\infty} w_{-i} F^i$. For a finite sum there is no problem. The general case follows from the following statement:

For given $\xi, \eta \in \hat{W}(\mathcal{N})$ there is an integer m_0, such that for any $w \in W(R)$:

$$\operatorname{hex}(\xi w F^m)\eta = 0, \qquad \operatorname{hex}(\xi V^m w)\eta = 0.$$

Indeed, this is an immediate consequence of lemma 116. $\square$

Proposition 120. — *(Mumford) The map:*

$$\begin{aligned} \bar{\mathbb{E}}_R &\longrightarrow \operatorname{Bihom}(\hat{W} \times \hat{W}, \hat{\mathbb{G}}_m), \\ u &\longmapsto \beta_u(\xi, \eta) = \operatorname{hex}(\xi u)\eta \end{aligned} \tag{214}$$

is an isomorphism of abelian groups.

Proof. — One starts with the natural isomorphism.

$$\operatorname{Bihom}(\hat{W} \times \hat{W}, \hat{\mathbb{G}}_m) \simeq \operatorname{Hom}(\hat{W}, \underline{\operatorname{Hom}}^+(\hat{W}, \mathbb{G}_m)).$$

The sheaf $\underline{\operatorname{Hom}}^+(\hat{W}, \hat{\mathbb{G}}_m)$ is easily computed by the first main theorem of Cartier theory: Let $A = R \oplus \mathcal{N}$ be an augmented nilpotent R-algebra. Then one defines a homomorphism:

$$W(\mathcal{N}) \longrightarrow \underline{\operatorname{Hom}}^+(\hat{W}, \hat{\mathbb{G}}_m)(\mathcal{N}) \subset \operatorname{Hom}(\hat{W}_A, \hat{\mathbb{G}}_{m_A}), \tag{215}$$

as follows. For any nilpotent A-algebra $\mathcal{M}$ the multiplication $\mathcal{N} \times \mathcal{M} \to \mathcal{M}$ induces on the Witt vectors the multiplication:

$$W(\mathcal{N}) \times \hat{W}(\mathcal{M}) \longrightarrow \hat{W}(\mathcal{M}).$$

Hence any $\omega \in W(\mathcal{N})$ induces a morphism $\hat{W}(\mathcal{M}) \to \hat{\mathbb{G}}_m(\mathcal{M}), \xi \mapsto \operatorname{hex} \omega\xi$. Since by the first main theorem of Cartier theory:

$$W(A) \longrightarrow \operatorname{Hom}(\hat{W}_A, \hat{\mathbb{G}}_{m_A}),$$

is an isomorphism. One deduces easily that (215) is an isomorphism. If we reinterprete the map (214) in terms of the isomorphism (215) just described, we obtain:

$$\begin{array}{ccc} \bar{\mathbb{E}}_R & \longrightarrow & \operatorname{Hom}(\hat{W}, W) \\ u & \longmapsto & (\xi \mapsto \xi u) \end{array} \tag{216}$$

But this is the isomorphism (209). $\square$

4.3. The biextension of a bilinear form of displays. — After this update of Mumford's theory we come to the main point of the whole duality theory: Let $\mathcal{P}$ and $\mathcal{P}'$ be 3n-displays over R. We are going to define a natural homomorphism:

$$\operatorname{Bil}(\mathcal{P} \times \mathcal{P}', \mathcal{G}_m) \longrightarrow \operatorname{Biext}^1(BT_{\mathcal{P}} \times BT_{\mathcal{P}'}.\hat{\mathbb{G}}_m) \tag{217}$$

Let $(\quad,\quad) : P \times P' \to W(R)$ be a bilinear form of 3n-displays (18). For $\mathcal{N} \in \operatorname{Nil}_R$ this induces a pairing

$$(\quad,\quad) : \hat{P}_{\mathcal{N}} \times \hat{P}'_{\mathcal{N}} \longrightarrow \hat{W}(\mathcal{N}), \tag{218}$$

(Compare chapter 3 for the notation). More precisely, if $x = \xi \otimes u \in \hat{P}_{\mathcal{N}} = \hat{W}(\mathcal{N}) \otimes_{W(R)} P$ and $x' = \xi' \otimes u' \in \hat{P}'_{\mathcal{N}} = \hat{W}(\mathcal{N}) \otimes_{W(R)} P'$, we set $(x', x) = \xi\xi'(u, u') \in \hat{W}(\mathcal{N})$, where the product on the right hand side is taken in $W(R|\mathcal{N}|)$.

To define the biextension associated to (218), we apply a sheafified version proposition 106 to the exact sequences of functors on Nil_R:

$$0 \longrightarrow \hat{Q}_{\mathcal{N}} \xrightarrow{V^{-1}-\mathrm{id}} \hat{P}_{\mathcal{N}} \longrightarrow BT_{\mathcal{P}}(\mathcal{N}) \longrightarrow 0$$
$$0 \longrightarrow \hat{Q}'_{\mathcal{N}} \xrightarrow{V^{-1}-\mathrm{id}} \hat{P}'_{\mathcal{N}} \longrightarrow BT_{\mathcal{P}'}(\mathcal{N}) \longrightarrow 0.$$

The proposition 106 combined with proposition 115, tells us that any element in $\mathrm{Biext}^1(BT_{\mathcal{P}} \times BT_{\mathcal{P}'}, \hat{\mathbb{G}}_m)$ is given by a pair of bihomomorphisms

$$\begin{aligned} \alpha_1 : \hat{Q}_{\mathcal{N}} \times \quad \hat{P}'_{\mathcal{N}} &\longrightarrow \quad \hat{\mathbb{G}}_m(\mathcal{N}) \\ \alpha_2 : \hat{P}_{\mathcal{N}} \times \quad \hat{Q}'_{\mathcal{N}} &\longrightarrow \quad \hat{\mathbb{G}}_m(\mathcal{N}), \end{aligned}$$

which agree on $\hat{Q}_{\mathcal{N}} \times \hat{Q}'_{\mathcal{N}}$.

In the following formulas an element $y \in \hat{Q}_{\mathcal{N}}$ is considered as an element of $\hat{P}_{\mathcal{N}}$ by the natural inclusion id. We set

$$\begin{aligned} \alpha_1(y, x') &= \mathrm{hex}(V^{-1}y, x'), \quad \text{for} \quad y \in \hat{Q}_{\mathcal{N}}, x' \in \hat{P}'_{\mathcal{N}}. \\ \alpha_2(x, y') &= -\mathrm{hex}(x, y'), \quad \text{for} \quad x \in \hat{P}_{\mathcal{N}}, y \in \hat{Q}'_{\mathcal{N}}. \end{aligned} \tag{219}$$

We have to verify that α_1 and α_2 agree on $\hat{Q}_{\mathcal{N}} \times \hat{Q}'_{\mathcal{N}}$, i.e. that the following equation holds:

$$\alpha_1(y, V^{-1}y' - y') = \alpha_2(V^{-1}y - y, y').$$

This means that:

$$\mathrm{hex}(V^{-1}y, V^{-1}y' - y') = -\mathrm{hex}(V^{-1}y - y, y'),$$

which is an immediate consequence of (1.14):

$$\mathrm{hex}(V^{-1}y, V^{-1}y') = \mathrm{hex}\ {}^V(V^{-1}y, V^{-1}y') = \mathrm{hex}(y, y').$$

We define the homomorphism (217) to be the map which associates to the bilinear form $(\ \ ,\ \ ) \in \mathrm{Bil}(\mathcal{P} \times \mathcal{P}', \mathcal{G})$ the biextension given by the pair α_1, α_2.

***Remark*:** Consider the biextension defined by the pair of maps $\beta_1 : \hat{Q}_{\mathcal{N}} \times \hat{P}'_{\mathcal{N}} \to \hat{W}(\mathcal{N})$ and $\beta_2 : \hat{P}_{\mathcal{N}} \times \hat{Q}'_{\mathcal{N}} \to \hat{W}_{\mathcal{N}}$ defined as follows:

$$\begin{aligned} \beta_1(y, x') &= \quad \mathrm{hex}(y, x'), \quad y \in \hat{Q}_{\mathcal{N}}, x' \in \hat{P}'_{\mathcal{N}} \\ \beta_2(x, y') &= -\mathrm{hex}(x, V^{-1}y'), x \in \hat{P}_{\mathcal{N}} y \in \hat{Q}'_{\mathcal{N}}. \end{aligned} \tag{220}$$

We claim that the biextension defined by (220) is isomorphic to the biextension defined by (219). Indeed by the proposition 106 we may add to the pair (β_1, β_2) the bihomomorphism

$$\mathrm{hex}(\ \ ,\ \ ) : \hat{P}_{\mathcal{N}} \times \hat{P}'_{\mathcal{N}} \longrightarrow \hat{\mathbb{G}}_m(\mathcal{N})$$

obtained from (218). One verifies readily:

$$\beta_1(y,x') + \mathrm{hex}(V^{-1}y - y, x') = \alpha_1(y,x')$$

$$\beta_2(x,y') + \mathrm{hex}(x, V^{-1}y' - y') = \alpha_2(y,y').$$

***Remark*:** Let $G \xrightarrow{\pi} B \times C$ be a biextension by an abelian group A, with the relative group laws $+_B$ and $+_C$. Let $s : B \times C \to C \times B,\ (b,c) \mapsto (c,b)$ be the switch of factors, and set $\pi^s = s \circ \pi$. Then $(G, \pi^s, +_C, +_B)$ is an object in $\mathrm{BIEXT}(C \times B, A)$. We will denote this biextension simply by G^s. Let us suppose that $B = C$. Then we call a biextension G symmetric if G and G^s are isomorphic.

Let us start with the bilinear form

$$(\quad,\quad) : \mathcal{P} \times \mathcal{P}' \longrightarrow \mathcal{G}_m.$$

We denote by G the biextension, which corresponds to the pair (219) of bihomomorphisms α_1 and α_2. Clearly the biextension G^s corresponds to the pair of bihomomorphisms $\alpha_1^s : \hat{Q}'_{\mathcal{N}} \times \hat{P}_{\mathcal{N}} \to \hat{W}(\mathcal{N})$ and $\alpha_2^s : \hat{P}'_{\mathcal{N}} \times \hat{Q}_{\mathcal{N}} \to \hat{W}(\mathcal{N})$, which are defined by the equations:

$$\begin{array}{lclcl} \alpha_1^s(y',x) & = & \alpha_2(x,y') & = & -\mathrm{hex}(x,y') \\ \alpha_2^s(x',y) & = & \alpha_1(y,x') & = & \mathrm{hex}(Vy,x') \end{array} \tag{221}$$

If we define a bilinear form:

$$(\quad,\quad)_s : \mathcal{P}' \times \mathcal{P} \longrightarrow \mathcal{G}_m,$$

by $(x',x)_s = (x,x')$, we see by the previous remark that the biextension defined by (221) corresponds to the bilinear form $-(x',x)_s$. We may express this by the commutative diagram:

$$\begin{array}{ccc} \mathrm{Bil}(\mathcal{P} \times \mathcal{P}', \mathcal{G}) & \longrightarrow & \mathrm{Biext}^1(BT_{\mathcal{P}} \times BT_{\mathcal{P}'}, \hat{\mathbb{G}}_m) \\ {\scriptstyle -s}\downarrow & & \downarrow{\scriptstyle s} \\ \mathrm{Bil}(\mathcal{P}' \times \mathcal{P}, \mathcal{G}) & \longrightarrow & \mathrm{Biext}^1(BT_{\mathcal{P}'} \times BT_{\mathcal{P}}, \hat{\mathbb{G}}_m) \end{array}$$

Let $\mathcal{P} = \mathcal{P}'$ and assume that the bilinear form $(\quad,\quad)$ is alternating, i.e. the corresponding bilinear form of $W(R)$-modules $P \times P \to W(R)$ is alternating. Then it follows that the corresponding biextension G in $\mathrm{Biext}^1(BT_{\mathcal{P}} \times BT_{\mathcal{P}}, \hat{\mathbb{G}}_m)$ is symmetric.

4.4. The duality isomorphism. — Assume we are given a bilinear form $(\quad,\quad) : \mathcal{P} \times \mathcal{P}' \to \mathcal{G}_m$ as in definition 18. Let $G = BT_{\mathcal{P}}$ and $G' = BT_{\mathcal{P}'}$ be the formal groups associated by theorem 81. The Cartan isomorphism $\mathrm{Biext}^1(G \times G', \hat{\mathbb{G}}_m) = \mathrm{Ext}^1(G \otimes^{\mathbb{L}} G', \hat{\mathbb{G}}_m) \xrightarrow{\sim} \mathrm{Ext}^1(G, R\underline{\mathrm{Hom}}(G', \hat{\mathbb{G}}_m))$ provides a canonical homomorphism

$$\mathrm{Biext}^1(G \times G', \hat{\mathbb{G}}_m) \longrightarrow \mathrm{Hom}(G, \underline{\mathrm{Ext}}^1(G', \hat{\mathbb{G}}_m)). \tag{222}$$

Let us describe the element on the right hand side, which corresponds to the biextension defined by the pair of bihomomorphisms α_1 and α_2 given by (219). For this purpose we denote the functor $\mathcal{N} \mapsto \hat{P}_{\mathcal{N}}$ simply by $\hat{P}$, and in the same way we define functors $\hat{Q}, \hat{P}', \hat{Q}'$. We obtain a diagram of sheaves:

(223)
$$\begin{tikzcd} & \underline{\mathrm{Hom}}(\hat{P}', \hat{\mathbb{G}}_m) \arrow[r, "(V^{-1}-\mathrm{id})^*"] & \underline{\mathrm{Hom}}(\hat{Q}', \hat{\mathbb{G}}_m) \arrow[r] & \underline{\mathrm{Ext}}^1(G', \hat{\mathbb{G}}_m) \arrow[r] & 0 \\ 0 \arrow[r] & \hat{Q} \arrow[u, "\alpha_1"] \arrow[r, "(V^{-1}-\mathrm{id})"] & \hat{P} \arrow[u, "\alpha_2"'] \arrow[r] & G \arrow[r] & 0 \end{tikzcd}$$

Hence $(V^{-1}-\mathrm{id})^*$ is the homomorphism obtained from $V^{-1}-\mathrm{id} : \hat{Q}' \to \hat{P}'$ by applying the functor $\underline{\mathrm{Hom}}(-, \hat{\mathbb{G}}_m)$. The horizontal rows are exact. The square is commutative because the restiction of α_1 to $\hat{Q} \times \hat{Q}'$ agrees with the restriction of α_2 in the sense of the inclusions defined by $V^{-1} - \mathrm{id}$. Hence (223) gives the desired $G \to \underline{\mathrm{Ext}}^1(G', \hat{\mathbb{G}}_m)$.

The functors in the first row of (222) may be replaced by their $^+$-parts (see (201)). Then we obtain a diagram with exact rows:

(224)
$$\begin{tikzcd} & \underline{\mathrm{Hom}}(\hat{P}', \hat{\mathbb{G}}_m)^+ \arrow[r] & \underline{\mathrm{Hom}}(\hat{Q}', \hat{\mathbb{G}}_m)^+ \arrow[r] & \underline{\mathrm{Ext}}^1(G', \hat{\mathbb{G}}_m)^+ \arrow[r] & 0 \\ 0 \arrow[r] & \hat{Q} \arrow[u] \arrow[r] & \hat{P} \arrow[u] \arrow[r] & G \arrow[u] \arrow[r] & 0 \end{tikzcd}$$

The first horizontal arrow in this diagram is injective, if $\mathcal{P}'$ is a display. Indeed, the group G' is p-divisible and by the rigidity for homomorphisms of p-divisible groups:

(225)
$$\underline{\mathrm{Hom}}(G', \hat{\mathbb{G}}_m)^+ = 0.$$

***Remark*:** Let $\mathcal{P}'$ be a display. The following proposition 121 will show that the functor $\underline{\mathrm{Ext}}^1(G', \hat{\mathbb{G}}_m)^+$ is a formal group. We will call it the dual formal group. The isomorphism (227) relates it to the dual display.

By the corollary 118 one obviously obtains an isomorphism

(226)
$$W(\mathcal{N}) \otimes_{W(R)} P^t \longrightarrow \underline{\mathrm{Hom}}(\hat{P}, \hat{\mathbb{G}}_m)^+(\mathcal{N}).$$

Here $P^t = \mathrm{Hom}_{W(R)}(P, W(R))$ is the dual $W(R)$-module. Therefore the functor $\underline{\mathrm{Hom}}(\hat{P}', \hat{\mathbb{G}}_m)^+$ is exact, and the first row of (224) is by proposition 109 exact in the sense of presheaves, if $\mathcal{P}'$ is a display.

Proposition 121. — *Let $\mathcal{P}$ be a display and $\mathcal{P}^t$ be the dual 3n-display. By definition 19 we have a natural pairing*

$$<,>: \mathcal{P}^t \times \mathcal{P} \longrightarrow \mathcal{G},$$

which defines by (217) a biextension in $\mathrm{Biext}^1(BT_{\mathcal{P}^t} \times BT_{\mathcal{P}}, \hat{\mathbb{G}}_m)$*. By (222) this biextension defines a homomorphism of sheaves*

(227)
$$BT_{\mathcal{P}^t} \longrightarrow \underline{\mathrm{Ext}}^1(BT_{\mathcal{P}}, \hat{\mathbb{G}}_m)^+.$$

The homomorphism (227) is an isomorphism.

Proof. — In our situation (224) gives a commutative diagram with exact rows in the sense of presheaves:

$$\begin{tikzcd} 0 \arrow[r] & \underline{\mathrm{Hom}}(\hat{P}, \hat{\mathbb{G}}_m)^+ \arrow[r] & \underline{\mathrm{Hom}}(\hat{Q}, \hat{\mathbb{G}}_m)^+ \arrow[r] & \underline{\mathrm{Ext}}^1(G, \hat{\mathbb{G}}_m)^+ \arrow[r] & 0 \\ 0 \arrow[r] & \hat{Q}^t \arrow[r] \arrow[u] & \hat{P}^t \arrow[r] \arrow[u] & G^t \arrow[r] \arrow[u] & 0. \end{tikzcd} \tag{228}$$

Here we use the notation $G = BT_{\mathcal{P}},\ G^t = BT_{\mathcal{P}^t}$. Let us make the first commutative square in (228) more explicit.

The bilinear pairing

$$\begin{array}{llll} W(\mathcal{N}) \otimes_{W(R)} P^t \times & \hat{W}(\mathcal{N}) \otimes_{W(R)} P & \longrightarrow \hat{\mathbb{G}}_m(\mathcal{N}), \\ \xi \otimes x^t \quad \times & u \otimes x & \longmapsto \mathrm{hex}(\xi u < x^t, x >) \end{array} \tag{229}$$

provides by the corollary 118 an isomorphism of functors

$$W(\mathcal{N}) \otimes_{W(R)} P^t \longrightarrow \underline{\mathrm{Hom}}(\hat{P}, \hat{\mathbb{G}}_m)^+(\mathcal{N}). \tag{230}$$

In order to express $\underline{\mathrm{Hom}}(\hat{Q}, \hat{\mathbb{G}}_m)^+$ in a similiar way, we choose a normal decomposition $P = L \oplus T$. Let us denote by $L^* = \mathrm{Hom}_{W(R)}(L, W(R))$ and $T^* = \mathrm{Hom}_{W(R)}(T, W(R))$ the dual modules. In terms of the chosen normal decomposition the dual 3n-display $\mathcal{P}^t = (P^t, Q^t, F, V^{-1})$ may be described as follows.

We set $P^t = P^*, Q^t = T^* \oplus I_R L^*$. Then we have a normal decomposition

$$P^t = L^t \oplus T^t,$$

where $L^t = T^*$ and $T^t = L^*$. To define F and V^{-1} for $\mathcal{P}^t$ it is enough to define ^{F}-linear maps:

$$V^{-1} : L^t \longrightarrow P^t \quad F : T^t \longrightarrow P^t.$$

We do this using the direct decomposition

$$P = W(R)V^{-1}L \oplus W(R)FT.$$

For $x^t \in L^t = T^*$ we set:

$$\begin{array}{rcl} < V^{-1}x^t, wFy >= & w^F < x^t, y >, & w \in W(R), y \in T \\ < V^{-1}x^t, wV^{-1}x >= & 0, & x \in L \end{array}$$

For $y^t \in T^t = L^*$ we set:

$$\begin{array}{rcl} < Fy^t, wFy >= & 0, & y \in T \\ < Fy^t, wV^{-1}x >= & w^F <^t y, x >, & x \in L. \end{array}$$

The bilinear pairing:

$$\begin{array}{rcl} W(\mathcal{N}) \otimes_{F,W(R)} T^* & \times & \hat{W}(\mathcal{N}) \otimes_{F,W(R)} T \to \hat{\mathbb{G}}_m(\mathcal{N}) \\ \xi \otimes x^t & \times & u \otimes y \quad \mapsto \mathrm{hex}(\xi u \ {}^F < x^t, y >) \end{array}$$

defines a morphism

$$W(\mathcal{N}) \otimes_{F,W(R)} T^* \longrightarrow \underline{\mathrm{Hom}}(\hat{W} \otimes_{F,W(R)} T, \hat{\mathbb{G}}_m)^+(\mathcal{N}), \tag{231}$$

where $\hat{W} \otimes_{F,W(R)} T$ denotes the obvious functors on Nil_R. The right hand side of (231) may be rewritten by the isomorphism:

$$\begin{aligned} \hat{I}_{\mathcal{N}} \otimes_{W(R)} T &\longrightarrow \hat{W}(\mathcal{N}) \otimes_{F,W(R)} T \\ {}^V u \otimes y &\longmapsto u \otimes y \end{aligned} \tag{232}$$

The pairing (229) induces an isomorphism:

$$W(\mathcal{N}) \otimes_{W(R)} L^* \longrightarrow \underline{\mathrm{Hom}}(\hat{W} \otimes_{W(R)} L, \hat{\mathbb{G}}_m)^+(\mathcal{N}) \tag{233}$$

Taking the isomorphisms (231), (232) and (233) together, we obtain an isomorphism of functors

$$\begin{aligned} \underline{\mathrm{Hom}}(\hat{Q}, \hat{\mathbb{G}}_m)^+(\mathcal{N}) &\cong W(\mathcal{N}) \otimes_{F,W(R)} T^* \oplus W(\mathcal{N}) \otimes_{W(R)} L^* \\ &= W(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus W(\mathcal{N}) \otimes_{W(R)} T^t. \end{aligned} \tag{234}$$

We use the decomposition $P^t = W(R)V^{-1}L^t \oplus W(R)FT^t$ to rewrite the isomorphism (230)

$$\begin{aligned} \underline{\mathrm{Hom}}(\hat{P}, \hat{\mathbb{G}}_m)^+(\mathcal{N}) &\cong W(\mathcal{N}) \otimes_{W(R)} W(R)V^{-1}L^t \oplus W(\mathcal{N}) \otimes_{W(R)} W(R)FT^t \\ &\simeq W(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus W(\mathcal{N}) \otimes_{F,W(R)} T^t. \end{aligned} \tag{235}$$

Here an element $\xi \otimes x^t \oplus \eta \otimes y^t$ from the last module of (237) is mapped to $\xi V^{-1}x^t \oplus \eta F y^t$ from the module in the middle.

We rewrite the first square in (228) using the isomorphism (234) and (235):

$$\begin{array}{ccc} W(\mathcal{N}) \otimes_{F,} L^t \oplus W(\mathcal{N}) \otimes_{F,} T^t & \xrightarrow{(V^{-1}-\mathrm{id})^*} & W(\mathcal{N}) \otimes_{F,} L^t \oplus W(\mathcal{N}) \otimes T^t \\ \tilde{\alpha}_1 \uparrow & & \tilde{\alpha}_2 \uparrow \\ \hat{W}(\mathcal{N}) \otimes L^t \oplus \hat{W}(\mathcal{N}) \otimes_{F,} T^t & \xrightarrow{V^{-1}-\mathrm{id}} & \hat{W}(\mathcal{N}) \otimes L^t \oplus \hat{W}(\mathcal{N}) \otimes T^t \end{array} \tag{236}$$

In this diagram all tensor products are taken over $W(R)$. We have to figure out what are the arrows in this diagram explicitly. We will first say what the maps are and then indicate how to verify this.

$$\begin{aligned} \widetilde{\alpha}_2 &= -\left({}^F \otimes \mathrm{id}_{L^t} \oplus \mathrm{id}_{W(\mathcal{N}) \otimes_{W(R)} T^t} \right) \\ \widetilde{\alpha}_1 &= {}^F \otimes \mathrm{id}_{L^t} \oplus \mathrm{id}_{W(\mathcal{N}) \otimes_{F,W(R)} T^t} \end{aligned} \tag{237}$$

The upper horizontal map in (236) is the map $(V^{-1} - \mathrm{id})^* = \underline{\mathrm{Hom}}(V^{-1} - \mathrm{id}, \hat{\mathbb{G}}_m)$: $\underline{\mathrm{Hom}}(\hat{P}, \hat{\mathbb{G}}_m) \to \underline{\mathrm{Hom}}(\hat{Q}, \hat{\mathbb{G}}_m)$. We describe the maps $(V^{-1})^* = \underline{\mathrm{Hom}}(V^{-1}, \hat{\mathbb{G}}_m)$ and $\mathrm{id}^* = \underline{\mathrm{Hom}}(\mathrm{id}, \hat{\mathbb{G}}_m)$. Let $\xi \otimes x^t \oplus \eta \otimes y^t \in W(\mathcal{N}) \otimes_{F,W} L^t \oplus W(\mathcal{N}) \otimes_{F,W} T^t$ be an element. Then we have:

$$(V^{-1})^*(\xi \otimes x^t \oplus \eta \otimes y^t) = \xi \otimes x^t \oplus {}^V\eta \otimes y^t. \tag{238}$$

Finally the map id^* is the composite of the map $(V^{-1})^\# \oplus F^\# : W(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus W(\mathcal{N}) \otimes_{F,W(R)} T^t \to W(\mathcal{N}) \otimes_{W(R)} P^t$ with the extension of $-\tilde{\alpha}_2$ to the bigger domain $W(\mathcal{N}) \otimes_{W(R)} P^t = W(\mathcal{N}) \otimes_{W(R)} L^t \oplus W(\mathcal{N}) \otimes_{W(R)} T^t$. We simply write:

$$\mathrm{id}^* = -\widetilde{\alpha}_2 \left((V^{-1})^\# \oplus F^\# \right). \tag{239}$$

If one likes to be a little imprecise, one could say $(V^{-1})^* = \mathrm{id}$ and $(\mathrm{id})^* = V^{-1}$.

Let us now verify these formulas for the maps in (238). $\widetilde{\alpha}_1$ is by definition (219) the composition of $V^{-1} : \hat{Q}^t_{\mathcal{N}} \rightarrow \hat{P}^t_{\mathcal{N}}$ with the inclusion $\hat{P}^t_{\mathcal{N}} \subset W(\mathcal{N}) \otimes_{W(R)} P^t = \underline{\mathrm{Hom}}(\hat{P}, \mathbb{G}_m)^+(\mathcal{N})$. Hence by the isomorphism (235) which was used to define the diagram (236) the map $\widetilde{\alpha}_1$ is:

$$\widetilde{\alpha}_1 : \hat{Q}^t_{\mathcal{N}} \xrightarrow{V^{-1}} W(\mathcal{N}) \otimes_{W(R)} P^t \xleftarrow[\sim]{(V^{-1})^{\#} \oplus F^{\#}} W(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus W(\mathcal{N}) \otimes_{F,W(R)} T^t$$

Clearly this is the map given by (237).

Consider an element $u \otimes x^t \in \hat{W}(\mathcal{N}) \otimes_{W(R)} L^t$. This is mapped by $\tilde{\alpha}_2$ to an element in $\underline{\mathrm{Hom}}(\hat{Q}, \hat{\mathbb{G}}_m)^+(\mathcal{N}) = \underline{\mathrm{Hom}}(\hat{I} \otimes_{W(R)} T, \hat{\mathbb{G}}_m)^+(\mathcal{N}) \oplus \underline{\mathrm{Hom}}(\hat{W} \otimes_{W(R)} L, \hat{\mathbb{G}}_m)^+(\mathcal{N})$, whose component in the second direct summand is zero and whose component in the first direct summand is given by the following bilinear form $\overline{\alpha}_2$:

$$\overline{\alpha}_2(u \otimes x^t,\ {}^V u' \otimes y) = -\operatorname{hex}\ {}^V u' u < x^t, y >= -\operatorname{hex} u'\ {}^F u\ {}^F <^t x, y > .$$

Hence the image in the first direct summand is equal to the image of ${}^F u \otimes x^t$ by the homomorphism (231).

Next we compute the map:

$$(V^{-1})^* : W(\mathcal{N}) \otimes_{W(R)} P^t \simeq \underline{\mathrm{Hom}}(\hat{P}, \hat{\mathbb{G}}_m)^+(\mathcal{N}) \rightarrow \underline{\mathrm{Hom}}(\hat{Q}, \hat{\mathbb{G}}_m)^+(\mathcal{N}).$$

Let use denote by $(\quad,\quad)_D$ the bilinear forms induced by the homomorphism (231) respectively (233). Let $\theta \otimes z^t \in W(\mathcal{N}) \otimes_{W(R)} P^t$ be an element, and let $\theta \otimes x \oplus v \otimes y \in \hat{W}(\mathcal{N}) \otimes_{W(R)} L \oplus \hat{W}(\mathcal{N}) \otimes_{F,W(R)} T \simeq \hat{W}(\mathcal{N}) \otimes_{W(R)} L \oplus \hat{I}_{\mathcal{N}} \otimes_{W(R)} T = \hat{Q}_{\mathcal{N}}$. Then we have by definition of $(V^{-1})^*$:

$$\begin{gathered}\big((V^{-1})^*(\theta \otimes z^t), u \otimes x + v \otimes y\big)_D = \\ \operatorname{hex} \theta^F u < z^t, V^{-1} x > + \operatorname{hex} \theta v < z^t, F y > .\end{gathered} \tag{240}$$

Since we use the isomorphism (235) we have to write $\theta \otimes z^t$ in the form $\xi \otimes V^{-1} x^t + \eta \otimes F y^t$, where $\xi, \eta \in W(\mathcal{N}), x^t \in L^t, y^t \in T^t$. Then we find for the right hand side of (240):

$$\begin{gathered}\operatorname{hex} \xi^F u < V^{-1} x^t, V^{-1} x > + \operatorname{hex} \xi v < V^{-1} x^t, F y > \\ + \operatorname{hex} \eta^F u < F y^t, V^{-1} x > + \operatorname{hex} \eta v < F y^t, F y >\end{gathered} \tag{241}$$

By definition of the dual 3n-display the first and the last summand of (241) vanish. Using (20) we obtain for (241):

$$\begin{gathered}\operatorname{hex} \xi v^F < x^t y > + \operatorname{hex} \eta\ {}^F u\ {}^F < y^t, x >= \\ \operatorname{hex} \xi v^F < x^t, y > + \operatorname{hex}\ {}^V \eta u < y^t, x > .\end{gathered}$$

Since this is equal to the left hand side of (241), we see that $(V^{-1})^*(\xi \otimes V^{-1} x^t + \eta \otimes F y^t)$ is the element in $\underline{\mathrm{Hom}}(\hat{Q}, \hat{\mathbb{G}}_M)^+(\mathcal{N})$ induced by:

$$\xi \otimes x^t +\ {}^V \eta \otimes y^t \in \hat{W}(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus \hat{W}(\mathcal{N}) \otimes_{W(R)} T^t$$

This is the assertion (238).

Finally we compute id^*. By the isomorphisms (230) and (234) the map id^* identifies with a map

$$\mathrm{id}^* : W(\mathcal{N}) \otimes_{W(R)} P^t \longrightarrow W(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus W(\mathcal{N}) \otimes_{W(R)} T^t \tag{242}$$

The assertion of (239) is that this map is the extension of $-\widetilde{\alpha}_2$, if we identify the left hand side of (242) with $W(\mathcal{N}) \otimes_{W(R)} L^t \oplus W(\mathcal{N}) \otimes_{W(R)} T^t$ using our normal decomposition.

Let $\xi \otimes x^t \oplus \eta \otimes y^t \in W(\mathcal{N}) \otimes_{W(R)} L^t \oplus W(\mathcal{N}) \otimes_{W(R)} T^t$ and $u \otimes x \oplus {}^V v \otimes y \in \hat{W}(\mathcal{N}) \otimes_{W(R)} L \oplus \hat{I}_{\mathcal{M}} \otimes_{W(R)} T = \hat{Q}_{\mathcal{M}}$ for some $\mathcal{N}$-algebra $\mathcal{M}$. We obtain:

$$\begin{aligned} &\mathrm{id}^*(\xi \otimes x^t \oplus \eta \otimes y^t)(u \otimes x \oplus {}^V v \otimes y) \\ &= \mathrm{hex}(\xi\, {}^V v < x^t, y > + \mathrm{hex}\, \eta u < y^t, x > \\ &= \mathrm{hex}\, v\, {}^F\xi\, {}^F < x^t, y > + \mathrm{hex}\, \eta u < y^t, u >, \end{aligned}$$

which proves that

$$\mathrm{id}^*(\xi \otimes x^t + \eta \otimes y^t) = {}^F\xi \otimes x^t + \eta \otimes y^t.$$

Alltogether we have verified that the diagram (236) with the maps described coincides with the first square in (228). We may now write the first row of the diagram (228) as follows:

$$\begin{array}{c} 0 \to W \otimes_{F,W(R)} L^t \oplus I \otimes_{W(R)} T^t \xrightarrow{(V^{-1})^* - \mathrm{id}^*} W \otimes_{F,W(R)} L^t \oplus W \otimes_{W(R)} T^t \\ \hfill \downarrow \hfill \\ \hfill \underline{\mathrm{Ext}}^1(G, \hat{\mathbb{G}}_m)^+ \hfill \\ \hfill \downarrow \hfill \\ \hfill 0 \hfill \end{array} \tag{243}$$

Here we wrote W and I for the functors $\mathcal{N} \mapsto W(\mathcal{N})$ and $\mathcal{N} \mapsto I_{\mathcal{N}}$. We also used the isomorphism (232) to replace $W \otimes_{F,W(R)} T^t$ by $I \otimes_{W(R)} T^t$. The map $(V^{-1})^*$ is just the natural inclusion.

We know from (228), that $\underline{\mathrm{Ext}}^1(G, \hat{\mathbb{G}}_m)^+$ is an exact functor on Nil_R. We will now compute the tangent space of this functor.

Let us assume that $\mathcal{N}$ is equipped with a pd-structure. Then the logarithmic coordinates (48) define an isomorphism of $W(R)$-modules

$$\mathcal{N} \oplus I_{\mathcal{N}} \simeq W(\mathcal{N}).$$

Hence we have an isomorphism of abelian groups:

$$\mathcal{N} \otimes_{W(R)} T^t \oplus I_{\mathcal{N}} \otimes_{W(R)} T^t \xrightarrow{\sim} W(\mathcal{N}) \otimes_{W(R)} T^t.$$

We extend id^* to an endomorphism of $W(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus W(\mathcal{N}) \otimes_{W(R)} T^t$ by setting:

$$\mathrm{id}^*(\mathcal{N} \otimes_{W(R)} T^t) = 0.$$

We claim that id^* is then a nilpotent endomorphism. First we verify this in the case, where $p \cdot \mathcal{N} = 0$. Then we have ${}^F W(\mathcal{N}) = 0$ and therefore the map $\widetilde{\alpha}_2$

is zero on the first component. It follows from (239) that the image of id^* lies in $0 \oplus W(\mathcal{N}) \otimes_{W(R)} T^t \subset W(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus W(\mathcal{N}) \otimes_{W(R)} T^t$. Via the natural inclusion and projection id^* induces an endomorphism

$$\mathrm{id}^*_{22} : W(\mathcal{N}) \otimes_{W(R)} T^t \longrightarrow W(\mathcal{N}) \otimes_{W(R)} T^t.$$

By what we have said it is enough to show that id^*_{22} is nilpotent. The endomorphism

$$F : P^t = L^t \oplus T^t \longrightarrow P^t = L^t \oplus T^t,$$

induces via inclusion and projection an endomorphism

$$\varphi : T^t \longrightarrow T^t.$$

By the formula (239) we find for id^*_{22}:

$$\mathrm{id}^*_{22}\left((n + {}^V\xi) \otimes y^t\right) = \xi \otimes \varphi(y^t),$$

where $n \in \mathcal{N}, \xi \in W(\mathcal{N})$, and $y^t \in T^t$. But since $\mathcal{P}$ is a display the 3n-display $\mathcal{P}^t$ is F-nilpotent, i.e. there is an integer r, such that $\varphi^r(T^t) \subset I_R T^t$. Since $W(\mathcal{N}) \cdot I_R = 0$ it follows that $(\mathrm{id}^*_{22})^r = 0$. In the case where $p\mathcal{N}$ is not necessarily zero, we consider the filtration by pd-ideals

$$0 = p^r\mathcal{N} \subset p^{r-1}\mathcal{N} \subset \cdots \subset \mathcal{N}.$$

Since the functors of (243) are exact on Nil_R an easy induction on r yields the nilpotency of id^* in the general case. This proves our claim that id^* is nilpotent if $p \cdot \mathcal{N} = 0$. Since $(V^{-1})^*$ is the restriction of the identity of

$$W(\mathcal{N}) \otimes_{F,W(R)} L^t \oplus W(\mathcal{N}) \otimes_{W(R)} T^t$$

it follows that $(V^{-1})^* - \mathrm{id}^*$ induces an automorphism of the last group. One sees easily (compare (157) that the automorphism $(V^{-1})^* - \mathrm{id}^*$ provides an isomorphism of the cokernel of $(V^{-1})^*$ with the cokernel of $(V^{-1})^* - \mathrm{id}^*$. Therefore we obtain for a pd-algebra $\mathcal{N}$ that the composition of the following maps:

$$\mathcal{N} \otimes_{W(R)} T^t \hookrightarrow W(\mathcal{N}) \otimes_{W(R)} T^t \to \underline{\mathrm{Ext}}^1(G, \hat{\mathbb{G}}_m)^+(\mathcal{N})$$

is an isomorphism. This shows that the $\underline{\mathrm{Ext}}^1(G, \hat{\mathbb{G}}_m)^+$ is a formal group with tangent space $T^t/I_R T^t$ by definition 80. Moreover

$$G^t \longrightarrow \underline{\mathrm{Ext}}^1(G, \hat{\mathbb{G}}_m)^+$$

is an isomorphism of formal groups because it induces an isomorphism of the tangent spaces. This proves the proposition. □

Let $\mathcal{P}$ be a 3n-display and let $\mathcal{P}'$ be a display. We set $G = BT_{\mathcal{P}}$, $G' = BT_{\mathcal{P}'}$, and $(G')^t = BT_{(\mathcal{P}')^t}$. If we apply the proposition 121 to (222) we obtain a homomorphism:

$$\mathrm{Biext}^1(G \times G', \hat{\mathbb{G}}_m) \longrightarrow \mathrm{Hom}(G, (G')^t) \tag{244}$$

We note that this map is always injective, because the kernel of (222) is by the usual spectral sequence $\mathrm{Ext}^1(G, \underline{\mathrm{Hom}}(G', \hat{\mathbb{G}}_m))$. But this group is zero, because $\underline{\mathrm{Hom}}(G', \hat{\mathbb{G}}_m)^+ = 0$ (compare (225)). A bilinear form $\mathcal{P} \times \mathcal{P}' \to \mathcal{G}$ is clearly the same thing as a homomorphism $\mathcal{P} \to (\mathcal{P}')^t$. It follows easily from the diagram (224) that the injection (244) inserts into a commutative diagram:

$$\begin{array}{ccc} \mathrm{Bil}(\mathcal{P} \times \mathcal{P}', \mathcal{G}) & \xrightarrow{\sim} & \mathrm{Hom}(\mathcal{P}, (\mathcal{P}')^t) \\ \downarrow & & \downarrow{\scriptstyle BT} \\ \mathrm{Biext}^1(G \times G', \hat{\mathbb{G}}_m) & \longrightarrow & \mathrm{Hom}(G, (G')^t) \end{array} \tag{245}$$

Theorem 122. — *Let R be a ring, such that p is nilpotent in R, and such that the set of nilpotent elements in R are a nilpotent ideal. Let $\mathcal{P}$ and $\mathcal{P}'$ be displays over R. We assume that $\mathcal{P}'$ is F-nilpotent, i.e. the dual 3n-display $(\mathcal{P}')^t$ is a display. Then the homomorphism (217) is an isomorphism:*

$$\mathrm{Bil}(\mathcal{P} \times \mathcal{P}', \mathcal{G}) \longrightarrow \mathrm{Biext}^1(BT_{\mathcal{P}} \times BT_{\mathcal{P}'}, \hat{\mathbb{G}}_m).$$

Proof. — By proposition 99 the right vertical arrow of the diagram (245) becomes an isomorphism under the assumptions of the theorem. Since we already know that the lower horizontal map is injective every arrow is this diagram must be an isomorphism. □

References

[BAC] Bourbaki,N.: Algébre Commutative, Chapt. 8 et 9, Masson 1983.

[B] Berthelot, P.: Théorie Dieudonné sur un anneau de valuation parfait, Ann. Scient. Éc. Norm. Sup. 13, 225-268, (1980).

[Br] Breuil, Ch.: Groupes p-divisibles, groupes finis et modules filtrés, Ann. Math. 152 (2000), 489-549.

[BO] Berthelot,P., Ogus,A.: Notes on crystalline cohomology, Princeton 1978.

[C] Cartier,P.: Relèvement des groupes formels commutatifs, Sém. Bourbaki 1968/69, exp. 359, Springer LNM 179, Berlin 1971.

[Gr] Grothendieck, A.: Groupes de Barsotti-Tate et cristaux de Dieudonné, Sém. Math. Sup. **45**, Presses de l'Univ. de Montreal, 1970.

[G] Gross, B.H., On canonical and quasicanonical liftings, Invent.math. 84, 321-326, (1986).

[GK] Gross,B.H., Keating, K., On the intersection of modular correspondences, Invent.math. 112, 225-245, (1993)

[K] Keating, K., Lifting endomorphisms of formal A-modules, Compos. Math. 67, 211-239, (1988).

[LZ] Langer, A., Zink, Th.: De Rham-Witt cohomology for a proper and smooth morphism. http://www. mathematik.uni-bielefeld.de/˜zink

[Me] Messing, W.: The crystals associated to Barsotti-Tate groups, LNM **264**, Springer 1972.

[Mu] Mumford, D.: Bi-extensions of formal groups, in: Algebraic Geometry, Oxford University Press 1969, pp. 307 -322.

[N] Norman, P.: An algorithm for computing local moduli of abelian varieties, Ann. Math. **101**, 499 -509 (1975).

[RZ] Rapoport, M., Zink, Th.: Period spaces for p–divisible groups, Annals of Mathematics Studies **141**, Princeton 1996.

[SGA7] Groupes de Monodromie en Géometrie algebrique, Séminaire Géométrie Algébrique, dirigé par A.Grothendieck, Springer Lecture Notes in Mathematics 288, Berlin 1972.

[Z1] Zink, Th.: Cartiertheorie kommutativer formaler Gruppen, Teubner Texte zur Mathematik **68**, Leipzig 1984.

[Z2] Zink, Th.: Cartiertheorie über perfekten Ringen, I, II, Preprints, Akademie der Wissenschaften Berlin 1986.

[Z3] Zink, Th.: A Dieudonné theory of p-divisible groups, in: Class Field Theory, Its Centenary and Prospect pp.1-22, Advanced Studies in Pure Mathematics, Tokyo 2000

[Z4] Windows for displays of p-divisible groups, http://www. mathematik.uni-bielefeld.de/˜zink, to appear in: Proceedings of a Conference on Texel Island 1999.

Thomas Zink, Faculty of Mathematics · University of Bielefeld · POB 100131 · D-33501 Bielefeld
E-mail : `zink@mathematik.uni-bielefeld.de`