Displays and Gauges

Dissertation zur Erlangung des Doktorgrades
der Naturwissenschaften (Dr. rer. nat.)
an der Fakultät für Mathematik der Universität Regensburg

vorgelegt von

Marcel Wid

aus Winsen

2012

Universität Regensburg
Fachbereich für Mathematik

Promotionsgesuch eingereicht am 18.04.2012

Die Arbeit wurde angeleitet von Prof. Dr. Uwe Jannsen

Prüfungsausschuss:

Prof. Dr. Helmut Abels (Vorsitzender)

Prof. Dr. Uwe Jannsen (1. Gutachter)

Prof. Dr. Guido Kings (2. Gutachter)

Prof. Dr. Klaus Künnemann (weiterer Prüfer)

Preface

This thesis was written at my time at the university of Regensburg. I want to thank the university of Regensburg for the financial support during the first three years of my studies. The last year, I was supported by the Graduiertenkolleg 1692 “Curvature, Cycles and Cohomology” of the DFG.

The content of this thesis deals with the foundation of a new p-adic cohomology theory in characterstic $p > 0$, which was invented by Jean-Marc Fontaine and Uwe Jannsen. Professor Uwe Jannsen was my supervisor and offered me the opportunity to write this thesis. For that and for the many discussions and comments, I want to thank him heartily.

In december 2010 I visited Prof. Torsten Wedhorn in Bonn to talk to him about the theory of F-zips he introduced together with Prof. Ben Moonen. I want to express my gratitude for this enlightening discussion.

For the nice atmosphere I thank all the other Ph.D. students at the Fakultät für Mathematik at the university of Regensburg. Especially, I thank Tobias Sitte for the fun I had when sharing the office with him and for the uncountable many discussions about mathematics and the english grammar.

Most of all, I thank my wonderful wife, Nicole, for her continous encouragement and patience. Without her support this thesis would not have been completed.

Winsen, February 2012 — Marcel Wid

Contents

Introduction

This thesis is based on the unpublished joint work of Jean-Marc Fontaine and Uwe Jannsen [FJ05]. The motivation for this thesis is twofold. On the one hand we have the following classical theorem of Dieudonné.

Theorem (see [Dem86, Chapter IV, section 8]***).*** — The functor $G \mapsto M(G)$ is an antiequivalence of categories between the category of p-torsion formal groups and the category of Dieudonné modules M such that M is finitely generated as $W(k)$-module.

Recall that a *Dieudonné module* over a perfect field k of characteristic $p > 0$ is a module M over the ring $W(k)$ of Witt vectors with coefficients in k (see chapter 1 section 1) together with two group endomorphisms F_M and V_M satisfying the following relations for all $\lambda \in W(k)$ and $m \in M$:

$$\begin{aligned} F_M(\lambda m) &= \sigma(\lambda) F_M(m) \\ V_M\big(\sigma(\lambda) m\big) &= \lambda V_M(m) \\ F_M V_M = V_M F_M &= p\,\mathrm{id}_M. \end{aligned}$$

Here $\sigma\colon W(k) \to W(k)$ denotes the Frobenius. We can introduce the ring $\mathcal{D} := W(k)[F, V]$, which is a noncommutative polynomial ring over $W(k)$ in two variables F and V satisfying the relations

$$\begin{aligned} F \cdot \lambda &= \sigma(\lambda) \cdot F \\ V \cdot \sigma(\lambda) &= \lambda \cdot V \\ FV = VF &= p. \end{aligned}$$

Using this ring $\mathcal{D}$ we see that a Dieudonné module in the above sense is just a module over the ring $\mathcal{D}$ and each $\mathcal{D}$-module is a Dieudonné module. The drawback of the ring $\mathcal{D}$ is that it is not commutative. One objective of this thesis is to replace the ring $\mathcal{D}$ by a commutative ring D such that each Dieudonné module gives rise to a module over D. Because of the relations the group endomorphisms F_M and V_M must satisfy, we need some more structure on the ring D. This additional structure is motivated by the ring automorphism $\sigma\colon W(k) \to W(k)$. All this leads us to the notion of a φ-ring. We will not give a definition of φ-rings in this introduction, but refer the reader to chapter 5. Actually, we will construct a sheaf of rings on the small syntomic site of a perfect field k of positive characteristic, whose global section over $\mathrm{Spec}(k)$ is the ring D.

The syntomic site was first introduced by Mazur and it was Fontaine and Messing [FM87], who made use of it in p-adic Hodge theory. In their paper Fontaine and Messing argued very sketchy. Nevertheless, all the main ideas in the construction of our sheaf of φ-rings for the syntomic topology can be found in their paper. The first step is to define a sheaf of rings $\mathscr{O}_n^{\text{cris}}$ for the syntomic topology over $\operatorname{Spec}(k)$. This is done using the crystalline site of Berthelot. The main point for us is the fact that this sheaf, considered on the small syntomic site, is flat over $W_n(k)$, where $W_n(k)$ is the ring of Witt vectors of length n. This is stated without proof in [FM87]. We give a full proof of this property here. The restriction to the small syntomic site over a perfect field seems to be important, so this restriction should also be applied in [Sch09], as far as we can see.
The flatness of $\mathscr{O}_n^{\text{cris}}$ implies the exactness of the sequence

$$0 \longrightarrow \mathscr{O}_m^{\text{cris}} \longrightarrow \mathscr{O}_{m+n}^{\text{cris}} \longrightarrow \mathscr{O}_n^{\text{cris}} \longrightarrow 0.$$

This is crucial for everything that follows. We will use this sequence to construct a sheaf of rings denoted $\mathscr{G}_n$ on the small syntomic site of $\operatorname{Spec}(k)$. It turns out that $\mathscr{G}_n$ is a φ-ring and $\mathscr{G}_n(k)$ equals D. Having constructed this fundamental φ-ring we will consider sheaves of modules over $\mathscr{G}_n$. This leads to the notion of φ-modules and φ-gauges and we achieve one of the goals of this thesis, namely to lay the foundations for a new p-adic cohomology theory, which will be developed by Fontaine and Jannsen (see Jannsen's talk [Jan]). It must be noted that Schnellinger [Sch09] also constructed these fundamental sheaves of rings $\mathscr{G}_n$, however there are many details missing and he works on the big syntomic site of an $\mathbf{F}_p$-scheme X, for which there is no proof of flatness of $\mathscr{O}_n^{\text{cris}}$, but he heavily uses this property. We also remark that our strategy of proof differs from his one.
As stated in the beginning, there is a second motivation for this thesis. Instead of working over a perfect field k of positive characteristic and classify p-divisible groups over k, one may ask for a classification of p-divisible groups over a ring R of characteristic p or even over a p-adic ring. This motivated Zink [Zin02] to invent the notion of displays. A display is a projective $W(R)$-module with some additional data. It was Zink who obtained a classification of p-divisible formal groups over R in terms of displays over R under the restriction that R is excellent. Lau extended this result to all p-adic rings R, which are seperated and complete in the p-adic topology. In the joint work [LZ07] Langer and Zink generalized the notion of a display. In many examples there is a display structure on the crystalline cohomology of a smooth and projective scheme. Displays are also connected to so called F-zips, which are objects introduced by Moonen and Wedhorn [MW04]. While displays over a ring R are actually modules over the ring of Witt vectors $W(R)$, an F-zip is a module over R with some additional data. To be more precise, we assume that R is a ring of characteristic $p > 0$. Then a display is a quadruple $(P_i, \eta_i, \alpha_i, \theta_i)_{i\in\mathbf{N}}$ where each P_i is a projective $W(R)$-module. An F-zip is a quadruple $(M, C^i, D_i, \varphi_i)_{i\in\mathbf{Z}}$ where M is a projective R-module. There is a more general notion of F-zip, where R is replaced by an $\mathbf{F}_p$-scheme S and M is a locally free $\mathscr{O}_S$-module. But in this introduction we will stick to the more elementary situation of modules over a ring, since for displays there is no such generalization. In a sense made precise in chapter 2, F-zips are the reduction modulo p of displays. We introduce the notion of F-gauges, which should not be confused with φ-gauges. The main difference between these two objects is that F-gauges can be defined for any sheaf of rings, while φ-gauges are only defined over φ-rings. The notion of F-gauge enables us to clarify the relation between F-zips and displays. An F-gauge over a ring S is a family $(M^r)_{r\in\mathbf{Z}}$ of S-modules together with S-linear maps $f_r\colon M^r \to M^{r+1}$ and $v_r\colon M^r \to M^{r-1}$ satisfying the relations $f_{r-1} \circ v_r = v_{r+1} \circ f_r = p\,\mathrm{id}_{M^r}$. If R is ring of characteristic $p > 0$ then we show

that there is a (fully) faithful functor from displays over R to F-gauges over $W(R)$ and a fully faithful functor from F-zips over R to F-gauges over R. Now if $(M^r)_{r\in\mathbf{Z}}$ is an F-gauge over $W(R)$ we can consider the F-gauge $(M^r/pM^r)_{r\in\mathbf{Z}}$, which is an F-gauge over R. This reduction corresponds to the reduction of a display and thereby establishes the following commutative rectangle

$$\begin{tikzcd}
(\text{displays over } R) \arrow[r] \arrow[d] & (F\text{-gauges over } W(R)) \arrow[d] \\
(F\text{-zips over } R) \arrow[r] & (F\text{-gauges over } R)
\end{tikzcd}$$

Over a perfect field it is an easy consequence of the theory of elementary divisors that the isomorphism classes of displays and F-zips can be described in terms of matrices.
As a final remark let us mention that this thesis has two independent parts, which may be pictured as follows:

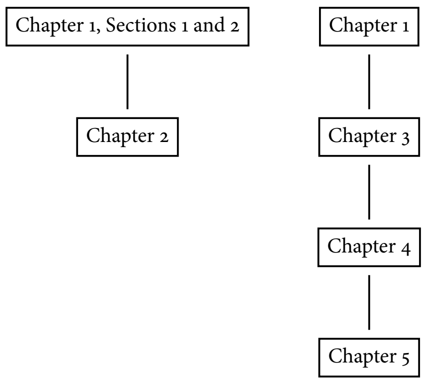

Figure 1: Leitfaden

It must be pointed out that the categories considered in chapter 2 are in general not abelian, while those considered in chapter 5 are abelian, which is an important feature for the cohomology theory to be developed by Jannsen and Fontaine.
We describe the contents of the individual chapters now: Chapter 1 is preliminary and is for the convenience of the reader. There we collect mostly without proofs all facts needed later on. Section 1 gives an overview of the ring of Witt vectors, section 2 deals with semi-linear algebra, section 3 introduces divided powers and proves the existence of divided powers for the ring of Witt vectors and section 4 collects all necessary facts about Grothendieck topologies and sites. We use this chapter also to fix our notation. The reader who is already familiar with these contents should skip this chapter and come back to it when needed.
Chapter 2 contains the first main result of this thesis, which clarifies the connection between displays and F-zips. In section 1 we introduce F-gauges and establish some properties of them. Over a perfect field there is the notion of an F-crystal, which is the content of the second section. Section

3 introduces F-zips. Our definition differs slightly from the one of Moonen and Wedhorn (see remark 2.3.24). Section 4 contains the theory of displays as given by Langer and Zink [LZ07] and we have included some proofs, which were omitted in their paper. In each section we construct functors from the objects considered there to F-gauges and we end up by describing how these functors are related.

Chapter 3 recalls the definitions of syntomic morphisms, the syntomic topology and of the crystalline site. We have also included the notion of p-morphisms and quiet morphisms, which are also interesting classes of morphisms in characteristic p. These are only included for completeness, but we do not use them in the sequel. It should be noted that many results stay valid, if one replaces syntomic by quiet or even p-morphism. One may consult [Sch09, Chapter 3], where it is shown that cohomology of quasi-coherent crystals is independent of the p-topology.

Chapter 4 is the technical main part of this thesis. Here the sheaves $\mathscr{O}_n^{\mathrm{cris}}$ are constructed. This is done in two different ways. First they can be just defined as the sheaves associated to

$$\mathscr{O}_n^{cris}\colon X \longmapsto \mathrm{H}^0\big((X/W_n)_{cris}, \mathscr{O}_{X/W_n}\big)$$

on the syntomic site. We will prove, that these presheaves are already sheaves, i.e. sheafification is unnecessary. The second section gives a different construction using the ring of Witt vectors and divided powers. It is proved, that the two constructions give isomorphic sheaves. The last section in this chapter establishes the flatness of $\mathscr{O}_n^{\mathrm{cris}}$, which is crucial for the construction of the ring $\mathscr{G}_n$ in the last chapter. As has already been pointed out, to prove flatness we have to work on the small syntomic site of a perfect field k.

The last chapter 5 gives the construction of the sheaves of rings $\mathscr{G}_n$ and introduces the notion of φ-gauges, which is the starting point of the theory of Fontaine and Jannsen, which is currently developed. The reader is advised to note the difference of the objects studied in chapter 2 and chapter 5. The difference might be stated by the phrase

$$\sigma\text{-linear isomorphism} \neq \sigma\text{-linear bijective map}.$$

This holds for all rings for which σ is not an automorphism. Chapter 5 finishes by showing that there is an adjoint pair of functors $\Gamma^*_{\mathscr{G}_n}$ and Γ_*. Moreover, we will see that $\Gamma^*_{\mathscr{G}_n}$ is fully faithful.

Notations and Conventions. — We use the usual notations $\mathbf{N}$, $\mathbf{Z}$ and $\mathbf{Q}$ for the natural numbers including 0, the integers and the rational numbers respectively. For a prime p the notation $\mathbf{F}_p$ means a finite field with p elements, i.e. the prime field of characteristic p, which we identify with $\mathbf{Z}/p$ by the natural mapping $1 \mapsto 1$. By ring we always mean commutative ring with unit and a homomorphism of rings always maps 1 to 1. A scheme means a locally ringed space, which is locally isomorphic to the spectrum of a commutative ring. In earlier days, for example by Grothendieck in [Gro60], this was called a prescheme.

The symbol ■ indicates the end of a proof, the symbols ◂ and ◃ indicate the end of a remark and example, respectively.

Chapter

1 Preliminaries

In the first section we briefly recall the theory of Witt vectors without proofs. The second section deals with semi-linear algebra, which is elementary but essential for the rest of this thesis. In the third section divided powers are introduced and it is shown that the maximal ideal of the ring of Witt vectors with coefficients in a perfect field has a canonical structure of divided powers. The last section summarizes the theory of Grothendieck topologies. This chapter also fixes our notations and terminology used throughout this thesis.

§1 The ring of Witt vectors

We fix a prime number $p \in \mathbf{N}$. This section gives a brief overview of the construction of a ring $W(A)$ — the ring of Witt vectors — for any ring A. For details the reader is referred to [Bou06b, chap IX, §1], which we follow closely.

Definition 1.1.1. — For $n \in \mathbf{N}$ define $w_n \in \mathbf{Z}[X_0, \dots, X_n]$ by

$$w_n := \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \dots + p^n X_n.$$

Remark 1.1.2. — We obviously have the relations

$$\begin{aligned} w_0 &= X_0, \\ w_{n+1} &= w_n(X_0^p, \dots, X_n^p) + p^{n+1} X_{n+1}, \\ w_{n+1} &= X_0^{p^{n+1}} + p w_n(X_1, \dots, X_{n+1}). \end{aligned}$$ ◁

Let A be a ring and denote by $A^{\mathbf{N}}$ the product ring with ring structure given componentwise. As a set we define $W(A) := A^{\mathbf{N}}$ and write an element $\mathbf{a} \in W(A)$ as $\mathbf{a} = (a_n)_{n \in \mathbf{N}}$. The Witt polynomials define a map

$$w \colon W(A) \to A^{\mathbf{N}}$$

by

$$(a_n)_{n \in \mathbf{N}} \mapsto \big(w_n(a_0, \dots, a_n)\big)_{n \in \mathbf{N}}.$$

The value $w_n(a_0, \dots, a_n)$ is called the *n-th ghost component* of $\mathbf{a} = (a_n)_{n \in \mathbf{N}}$. The ring structure on $W(A)$ will be such that w becomes a homomorphism of rings. We want $W(A)$ to have two additional operators. In order to construct them, we first introduce their counterparts for the ring $A^{\mathbf{N}}$:

$$\begin{aligned} f&: (a_n)_{n \in \mathbf{N}} \mapsto (a_{n+1})_{n \in \mathbf{N}}, \\ v&: (a_n)_{n \in \mathbf{N}} \mapsto (0, pa_0, pa_1, \dots). \end{aligned}$$

Note that f is an endomorphism of the ring $A^{\mathbf{N}}$, while v is only an endomorphism of additive groups.

Proposition 1.1.3. — *Let A be any ring.*

(i) If p is not a zero divisor in A, then the map w is injective.

(ii) If p is invertible in A, then w is bijective.

(iii) Assume there exists an endomorphism σ of A such that $\sigma(a) = a^p \bmod pA$ for all $a \in A$. Then the image of w is a subring of $A^{\mathbf{N}}$, consisting of those elements $(a_n)_{n \in \mathbf{N}}$ such that $\sigma(a_{n-1}) \equiv a_n \bmod p^n A$ for all $n \in \mathbf{N} \smallsetminus \{0\}$. Moreover, the image of w is stable under the operators f and v.

Let us denote by $\mathfrak{X} = (X_n)_{n \in \mathbf{N}}$ and by $\mathfrak{Y} = (Y_m)_{m \in \mathbf{N}}$ countable sequences of indeterminates and by $R := \mathbf{Z}[\mathfrak{X}, \mathfrak{Y}]$ the polynomial ring in the indeterminates X_n and Y_m. We define an endomorphism σ of the ring R by

$$\begin{aligned} z &\mapsto z && \text{for } z \in \mathbf{Z}, \\ X_n &\mapsto X_n^p && \text{for } n \in \mathbf{N}, \\ Y_m &\mapsto Y_m^p && \text{for } m \in \mathbf{N}. \end{aligned}$$

Since p is not a zero divisor in R it follows from Fermat's little theorem that

$$\sigma(r) \equiv r^p \bmod pR$$

holds for all $r \in R$. The following lemma allows us to define a ring structure on $W(R)$.

Lemma 1.1.4. — *Let $R = \mathbf{Z}[\mathfrak{X}, \mathfrak{Y}]$ and $\sigma\colon R \to R$ be as above. Let $\Phi \in \mathbf{Z}[T_1, T_2]$. Then there exists a unique sequence $\phi = (\varphi_n)_{n \in \mathbf{N}}$ of polynomials with*

$$\varphi_n \in \mathbf{Z}[X_0, \dots, X_n, Y_0, \dots, Y_n] \subset R,$$

i.e. $\phi \in W(R)$ such that $w(\phi) = \Phi(w(\mathfrak{X}), w(\mathfrak{Y}))$.

Applying this lemma to the polynomials $T_1 + T_2$, $T_1 T_2$ and $-T_1$ yields elements $\mathbf{S}, \mathbf{P}, \mathbf{I} \in W(R)$ such that

$$\begin{aligned} w(\mathbf{S}) &= w(\mathfrak{X}) + w(\mathfrak{Y}), \\ w(\mathbf{P}) &= w(\mathfrak{X}) w(\mathfrak{Y}), \\ w(\mathbf{I}) &= -w(\mathfrak{X}). \end{aligned}$$

Example 1.1.5. — We will compute a few polynomials explicitely. First of all, it is easy to see that

$$\begin{aligned} S_0 &= X_0 + Y_0, \\ P_0 &= X_0 Y_0, \\ I_0 &= -X_0. \end{aligned}$$

The polynomial S_1 is determined by

$$w_1(S_0, S_1) = w_1(X_0, X_1) + w_1(Y_0, Y_1).$$

Evaluating gives

$$S_0^p + pS_1 = X_0^p + pX_1 + Y_0^p + pY_1.$$

Inserting $S_0 = X_0 + Y_0$ and manipulating the above equality yields

$$pS_1 = pX_1 + pY_1 - \sum_{i=1}^{p-1} \binom{p}{i} X_i^p Y_i^{p-i}.$$

Now, each $\binom{p}{i}$ is divisible by p for $1 \leq i \leq p-1$ and p is not a zero divisor in $\mathbf{Z}[X_0, X_1, Y_0, Y_1]$, so we obtain

$$S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} p^{-1} \binom{p}{i} X_i^p Y_i^{p-i}.$$

In a similar way, one gets

$$P_1 = pX_1Y_1 + X_0^p Y_1 + X_1 Y_0^p.$$

At last, let us compute I_2. It holds $w_1(I_0, I_1) = I_0^p + I_1 = (-X_0)^p + pI_1$ and $-w_1(X_0, X_1) = -X_0^p - pX_1$. We have to distinguish between $p = 2$ and $p \neq 2$. Hence we obtain

$$I_1 = \begin{cases} -X_1, & \text{if } p \neq 2 \\ -(X_0^2 + X_1), & \text{if } p = 2. \end{cases}$$

Moreover, if $p \neq 2$ we see that $I_n = -X_n$ for all $n \in \mathbf{N}$. ◂

Using these polynomials we can already construct the ring structure on $W(A)$ for any ring A. But as mentioned earlier, we want to have $W(A)$ equipped with two additional operators. Consider the ring $R = \mathbf{Z}[\mathfrak{X}, \mathfrak{Y}]$ again. We know by proposition 1.1.3 (iii) that the image of w is stable under f and v. This means that the element $f(w(\mathfrak{X}))$ is also in the image of w. Hence there is a unique element $\mathbf{F} \in W(A)$ such that $w(\mathbf{F}) = f(w(\mathfrak{X}))$. Explicitely, $\mathbf{F} = (F_n)_{n\in\mathbf{N}}$ is determined by

$$w_n(F_0, \ldots, F_n) = w_{n+1}(X_0, \ldots, X_{n+1}).$$

For example, we have

$$\begin{aligned} F_0 &= X_0^p + pX_1, \\ F_1 &= X_1^p + pX_2 - \sum_{i=0}^{p-1} \binom{p}{i} p^{p-i-1} X_0^{pi} X_1^{p-i}. \end{aligned}$$

Analogously, the element $v(w(\mathfrak{X}))$ is in the image of w and thus there must exist an element $\mathbf{V} \in W(A)$ such that $w(\mathbf{V}) = v(w(\mathfrak{X}))$. It is easy to see that

$$V_n = \begin{cases} 0, & \text{if } n = 0 \\ X_{n-1}, & \text{if } n > 0. \end{cases}$$

Let A be any ring. For $\mathbf{a} = (a_n)_{n\in\mathbf{N}}, \mathbf{b} = (b_n)_{n\in\mathbf{N}} \in W(A)$ we define their sum and product in $W(A)$ by

$$\begin{aligned} \mathbf{a} + \mathbf{b} &:= \mathbf{S}(\mathbf{a}, \mathbf{b}) = (S_n(a_0, \dots, a_n, b_0, \dots, b_n))_{n\in\mathbf{N}}, \\ \mathbf{ab} &:= \mathbf{P}(\mathbf{a}, \mathbf{b}) = (P_n(a_0, \dots, a_n, b_0, \dots, b_n))_{n\in\mathbf{N}}. \end{aligned}$$

The inverse of $\mathbf{a}$ is given by

$$-\mathbf{a} := \mathbf{I}(\mathbf{a}) = (I_n(a_0, \dots, a_n))_{n\in\mathbf{N}}.$$

We have to show that the above laws of composition indeed define a ring structure on $W(A)$. To establish this, we use the map $w: W(A) \to A^{\mathbf{N}}$. By the construction of $\mathbf{S}$ and $\mathbf{P}$ we know that if they define a ring structure on $W(A)$, then w is a homomorphism of rings. If p is not a zero divisor in A, then w is injective and hence defines a bijection between $W(A)$ and $\mathrm{im}(w)$. By slight abuse of notation we denote the inverse by $w^{-1}: \mathrm{im}(w) \to W(A)$. Thus, we get

$$\begin{aligned} \mathbf{a} + \mathbf{b} &= w^{-1}(w(\mathbf{a}) + w(\mathbf{b})), \\ \mathbf{ab} &= w^{-1}(w(\mathbf{a})w(\mathbf{b})), \\ -\mathbf{a} &= w^{-1}(-w(\mathbf{a})). \end{aligned}$$

So we see that in this case $W(A)$ can be given a ring structure by $\mathbf{S}$ and $\mathbf{P}$. To treat the general case, we use the following lemma.

Lemma 1.1.6. — *Let A be any ring. Then there exists a pair (B, ρ) consisting of a ring B and a surjective homomorphism $\rho: B \to A$ such that p is not a zero divisor in B and B has an endomorphism σ satisfying $\sigma(b) \equiv b^p \bmod pB$ for all $b \in B$.*

Proof. — Set $B := \mathbf{Z}[X_a, a \in A]$ and let σ be the idendity on $\mathbf{Z}$ and $\sigma(X_a) := X_a^p$. Then $\sigma(b) \equiv b^p \bmod pB$. The homomorphism ρ is determined by $\rho(X_a) := a$ for $a \in A$. ∎

If $\rho: B \to A$ is a homomorphism of arbitrary rings, we define two maps $\rho^{\mathbf{N}}: B^{\mathbf{N}} \to A^{\mathbf{N}}$ and $W(\rho): W(B) \to W(A)$ by $(b_n)_{n\in\mathbf{N}} \mapsto (\rho(b_n))_{n\in\mathbf{N}}$. The following relations are easily seen to be true for all $\mathbf{b}, \mathbf{b}_1, \mathbf{b}_2 \in W(B)$:

$$\begin{aligned} W(\rho)(\mathbf{b}_1 + \mathbf{b}_2) &= W(\rho)(\mathbf{b}_1) + W(\rho)(\mathbf{b}_2), \\ W(\rho)(\mathbf{b}_1\mathbf{b}_2) &= W(\rho)(\mathbf{b}_1)W(\rho)(\mathbf{b}_2), \\ W(\rho)(-\mathbf{b}) &= -W(\rho)(\mathbf{b}), \\ \rho^{\mathbf{N}}(w_B(\mathbf{b})) &= w_A(W(\rho)(\mathbf{b})). \end{aligned}$$

Here, $w_A: W(A) \to A^{\mathbf{N}}$ and $w_B: W(B) \to B^{\mathbf{N}}$ are the usual ghost component maps.

Theorem 1.1.7. — *Let A be a ring. Then $W(A)$ is again a ring with addition given by $\mathbf{S}$ and multiplication given by $\mathbf{P}$. The additive neutral element is $\mathbf{0} := (0,0,0,\dots)$ and the multiplicative neutral element is $\mathbf{1} := (1,0,0,\dots)$. The additive inverse of an element $\mathbf{a} \in W(A)$ is $\mathbf{I}(\mathbf{a})$.*

Definition 1.1.8. — Let A be a ring. The ring $W(A)$ is called the *ring of Witt vectors of A*.

The ring of Witt vectors of any ring A comes equipped with two mappings denoted F and V respectively. The map $F\colon W(A) \to W(A)$ is defined by

$$F(\mathbf{a}) = \big(F_n(a_0,\dots,a_{n+1})\big)_{n\in\mathbf{N}}$$

and called *Frobenius* and the map $V\colon W(A) \to W(A)$ is given by

$$V(\mathbf{a}) = (0, a_0, a_1, \dots)$$

and called *Verschiebung*. Here F_n denotes the $n+1$-st polynomial (recall our convention $0 \in \mathbf{N}$) in the family $\mathbf{F} = (F_n)_{n\in\mathbf{N}}$ introduced on page 3. To ease notation we will from now on simply write a instead of bold $\mathbf{a}$ for an element of $W(A)$. The interaction between the maps F and V is summarized in the next proposition.

Proposition 1.1.9. — *Let A be a ring.*

(i) The map V is a homomorphism of the additive group of $W(A)$.

(ii) The map F is an endomorphism of the ring $W(A)$.

(iii) For $a \in W(A)$ it holds $F(V(A)) = pa = \sum_{i=1}^{p} a$.

(iv) For $a, b \in W(A)$ it holds

$$V\big(a\cdot F(b)\big) = V(a)\cdot b$$
$$V(a)\cdot V(b) = pV(a\cdot b).$$

(v) For $a \in W(A)$ it holds $V(F(a)) = V(1)\cdot a$.

There is a map $\tau\colon A \to W(A)$ given by $x \mapsto (x, 0, \dots)$. This map is in general not additive but only multiplicative: $\tau(xy) = \tau(x)\cdot\tau(y)$.

Definition 1.1.10. — For $x \in A$ the element $\tau(x) \in W(A)$ is called *the Teichmüller representative of x*.

Witt vectors of finite length. — An element $a = (a_n)_{n\in\mathbf{N}} \in W(A)$ may be decomposed as

$$a = (a_0,\dots,a_{m-1},0,\dots) + (0,\dots,0,a_m,a_{m+1},\dots)$$

for any $m \in \mathbf{N}$. The set of all $a = (a_n)_{n\in\mathbf{N}} \in W(A)$ such that $a_n = 0$ for $0 \le n < m$ is denoted by $V_m(A)$. Let $V^m = V\circ\cdots\circ V$ m-times, then the last proposition yields

$$V^m(a+b) = V^m(a) + V^m(b)$$
$$V^m(a)\cdot b = V^m\big(a\cdot F^m(b)\big)$$

Here F^m denotes the composition of F with itself m-times. Thus we see that $V_m(A)$ is an ideal in $W(A)$.

Definition 1.1.11. — Let A be a ring and $n \in \mathbf{N}$. The quotient $W(A)/V_n(A)$ is denoted by $W_n(A)$ and called the *ring of Witt vectors of length n over A*.

The homomorphism $\pi_n\colon W(A) \to W_n(A)$ is explicitely given by

$$(a_i)_{i\in\mathbf{N}} \longmapsto (a_0, \dots, a_{n-1}).$$

If $m, n \in \mathbf{N}$ are two integers with $1 \le n \le m$ then $V_n(A) \supset V_m(A)$ and there is a canonical map $\pi_{n,m}\colon W_m(A) \to W_n(A)$ explicitely given by

$$(a_0, \dots, a_{m-1}) \longmapsto (a_0, \dots, a_{n-1}).$$

In this way we get a projective system $\big(W_n(A), \pi_{n,m}\big)$ and the map $a = (a_n)_{n\in\mathbf{N}} \mapsto \big(\pi_n(a)\big)$ induces a homomorphism of rings $\pi\colon W(A) \to \varprojlim_{n\in\mathbf{N}} W_n(A)$. It is not hard to see that $W(A)$ is separated and complete with respect to the topology induced by the filtration $\big(V_n(A)\big)_{n\in\mathbf{N}}$. Hence, π is an isomorphism of rings.

Example 1.1.12. — One can show that $W_n(\mathbf{F}_p) \cong \mathbf{Z}/p^n\mathbf{Z}$, which gives an isomorphism $W(\mathbf{F}_p) \cong \mathbf{Z}_p$ with the ring of p-adic integers. ◂

For two natural numbers n, m we have an exact sequence

$$0 \longrightarrow W(A) \xrightarrow{V^n} W(A) \xrightarrow{\pi_n} W_m(A) \longrightarrow 0$$

and by going to the quotient modulo $V_m(A)$ we obtain an additive map $V_m^n\colon W_m(A) \to W_{m+n}(A)$ fitting in the commutative diagram

$$\begin{tikzcd}
W(A) \arrow[r, "V^n"] \arrow[d, "\pi_m"'] & W(A) \arrow[d, "\pi_{m+n}"] \\
W_m(A) \arrow[r, "V_m^n"] & W_{m+n}(A)
\end{tikzcd}$$

This induces the exact sequence

$$0 \longrightarrow W_m(A) \xrightarrow{V_m^n} W_{m+n}(A) \xrightarrow{\pi_{n,m+n}} W_n(A) \longrightarrow 0.$$

Similarly, $F^n\colon W(A) \to W(A)$ induces a homomorphism of rings $F_m^n\colon W_{n+m}(A) \to W_m(A)$ fitting in the commutative diagram

$$\begin{tikzcd}
W(A) \arrow[r, "F^n"] \arrow[d, "\pi_{n+m}"'] & W(A) \arrow[d, "\pi_n"] \\
W_{n+m}(A) \arrow[r, "F_m^n"] & W_m(A)
\end{tikzcd}$$

Witt vectors in characteristic p. — Finally, we turn to the special but very important situation when A is a ring of characteristic $p > 0$. This is equivalent to saying that A has a structure of an $\mathbf{F}_p$-algebra given by the natural map of rings $\mathbf{F}_p \to A$.

Proposition 1.1.13. — *Let A be an $\mathbf{F}_p$-algebra. Then for all $a = (a_n)_{n\in\mathbf{N}}, b \in W(A)$ and all $n, m \in \mathbf{N}$ it holds*

(i) $F(a) = (a_n^p)_{n\in\mathbf{N}}$;

(ii) $pa = VF(a) = FV(a) = (0, a_0^p, a_1^p, \dots)$;

(iii) $V^m(a) \cdot V^n(b) = V^{m+n}\big(F^n(a) \cdot F^m(b)\big)$.

Proposition 1.1.14. — *Let k be a field of characteristic $p > 0$. Then $W(k)$ is a local integral ring with maximal ideal $V_1(k)$ and residue field isomorphic to k. If moreover k is perfect, then $W(k)$ is a discrete valuation ring with maximal ideal $pW(k)$.*

§2 Semi-linear algebra

We collect some basic facts about semi-linear algebra. Let A be a ring and $\sigma\colon A \to A$ an endomorphism. A map $f\colon M \to N$ of A-modules is called *semi-linear with respect to σ* or *σ-linear*, if f is linear as a map of abelian groups and $f(\lambda m) = \sigma(\lambda) f(m)$ for all $\lambda \in A$ and $m \in M$. If we consider A as an A-algebra via the endomorphism $\sigma\colon A \to A$, then we can form the tensor product $M^{(\sigma)} := M \otimes_\sigma A$. To each σ-linear map we can associate its *linearization* $f^\sharp\colon M^{(\sigma)} \to N$ defined by $m \otimes \lambda \mapsto \lambda f(m)$. We say that f is a σ-linear monomorphism, σ-linear epimorphism or σ-linear isomorphism, if its linearization $f^\sharp$ is a monomorphism, epimorphism or isomorphism of A-modules.

The kernel of a σ-linear map is always a submodule, while the image is in general not a submodule. The following lemma gives a characterization of a σ-linear isomorphism, if σ is an automorphism of A.

Lemma 1.2.15. — *Let $\sigma\colon A \to A$ be an automorphism and let $f\colon M \to N$ be a σ-linear map. Then f is a σ-linear isomorphism, if and only if f is bijective.*

Proof. — We first note that every element of $M^{(\sigma)}$ can be written in the form $m \otimes 1$: Since σ is an automorphism, we have $m \otimes \lambda = (\sigma^{-1}(\lambda)m) \otimes 1$. Assume $f^\sharp\colon M^{(\sigma)} \to N$ is an isomorphism. Let $m \in M$ with $f(m) = 0$. Then $f^\sharp(m \otimes 1) = f(m) = 0$, hence $m \otimes 1 = 0$ and so $m = 0$. Let $n \in N$. Then $x := (f^\sharp)^{-1}(n) \in M^{(\sigma)}$ can be written as $x = m \otimes 1$ by the above. It follows $f(m) = n$. For the reverse implication, assume f is bijective. Let $x \in M^{(\sigma)}$, then $x = m \otimes 1$ for some $m \in M$. If $0 = f^\sharp(x) = f(m)$ then $m = 0$ and thus $x = 0$. So $f^\sharp$ is injective. Let $n \in N$ and $m := f^{-1}(n) \in M$. Then $f^\sharp(m \otimes 1) = f(m) = n$ and $f^\sharp$ is surjective. ■

Remark 1.2.16. — If σ is an automorphism and f is a σ-linear bijective map, then the inverse map f^{-1} of f is σ^{-1}-linear. ◁

Example 1.2.17. — The situation we are interested in, is the following: Let R be a ring of characteristic $p > 0$ and $W(R)$ the ring of Witt vectors with coefficients in R. Let $W(R)_{[F]}$ be the scalar restriction by F (see below). The Verschiebung $V\colon W(R)_{[F]} \to W(R)$ is a $W(R)$-linear morphism and the image is the ideal I. Its "inverse" induces a F-linear bijective map $\rho\colon I \to W(R)$, which is not an isomorphism, unless F is an automorphism of $W(R)$, i.e. R is perfect. If R is not perfect, let $\lambda \in W(R) \smallsetminus \mathrm{im}(F)$. Then the element $V(1) \otimes \lambda - V(\lambda) \otimes 1 \in I \otimes_F W(R)$ is a nontrivial element in the kernel of $\rho^\sharp$. ◂

Restriction and extension of scalars. — Let us return to the general setting: A is a ring with an endomorphism σ. For an ideal $I \subset A$, we let $I^{(\sigma)}$ be the ideal in A generated by the image $\sigma(I)$. If $I = (a_1, \dots, a_r)$, then $I^{(\sigma)} = (\sigma(a_1), \dots, \sigma(a_r))$. Note that $\sigma(I)$ is in general not an ideal in A. If M is an A-module, then using σ there are (at least) two possibilities to get a new A-structure on M:

- Restriction of scalars along σ;
- Extension of scalars along σ.

First, we consider restriction of scalars. For an A-module M we denote by $M_{[\sigma]}$ the A-module, which is equal to M as abelian group but the module structure is given by

$$a \cdot m = \sigma(a)m \quad \text{for } a \in A \text{ and } m \in M.$$

In this way we get a functor $\mathcal{R}\colon M \mapsto M_{[\sigma]}$, which is exact, since exactness can be checked on the underlying abelian groups and the group homomorphisms are not changed under this functor. Next we consider extension of scalars. This can be seen as a functor from the category of A-modules to itself and is simply given by the tensor product

$$\mathcal{F}\colon M \mapsto M \otimes_\sigma A,$$

where we view A as an A-algebra via σ. Explicitely, the A-module structure can be described by

$$\lambda(m \otimes a) = m \otimes (\lambda a) \quad \text{and} \quad (\lambda m) \otimes a = m \otimes \big(\sigma(\lambda)a\big)$$

for $\lambda, a \in A$ and $m \in M$. Here are some properties of this functor:

(i) The functor $\mathcal{F}$ is right exact, since tensor product is right exact;

(ii) $\mathcal{F}(A) \cong A$ as A-modules;

(iii) $\mathcal{F}(A/I) \cong A/I^{(\sigma)}$ for any ideal I in A.

Matrices and σ-linear maps. — We want to give a description of σ-linear maps in terms of matrices in the case $A = k$ for a field k of positive characteristic and σ the Frobenius of k. So let V be a finite dimensional k-vector space and $f\colon V \to V$ a σ-linear endomorphism. Choosing a basis $v_1, \dots, v_n$ of V, we can associate a matrix $A_f = (a_{ij})$ to f, where

$$f(v_j) = \sum_{i=1}^{n} a_{ij} v_i.$$

Given a vector $v \in V$ we may write $v = \sum_{i=1}^{n} \alpha_i v_i$ and then we have

$$f(v) = A_f \cdot \begin{pmatrix} \sigma(\alpha_1) \\ \vdots \\ \sigma(\alpha_n) \end{pmatrix}$$

Lemma 1.2.18. — *There is a bijection*

$$\{\sigma\text{-linear maps } f\colon V \to V\} \xleftrightarrow{\sim} \mathrm{Mat}(n, k)$$

The proof is the same as in linear algebra and therefore omitted. For $A = (a_{ij}) \in \mathrm{Mat}(n,k)$ we set $\sigma(A) := \big(\sigma(a_{ij})\big)$. The following identities are true:

- $\sigma(A+B) = \sigma(A) + \sigma(B)$;
- $\sigma(AB) = \sigma(A)\sigma(B)$;
- $\sigma(E_n) = E_n$.

In particular, this yields a group homomorphism

$$\begin{aligned} \sigma\colon \mathrm{GL}_n(k) &\longrightarrow \mathrm{GL}_n(k) \\ A &\longmapsto \sigma(A) \end{aligned}$$

This homomorphism is injective and if $\sigma\colon k \to k$ is bijective (i.e., k is perfect) then this homomorphism is also. Let $v_1, \dots, v_n$ and $w_1, \dots, w_n$ be two bases of V. The base change matrix $B = (b_{ij})$ is defined as usual

$$w_j = \sum_{i=1}^{n} b_{ij} v_i.$$

Lemma 1.2.19. — *Let $f\colon V \to V$ be a σ-linear map, $v_1, \dots, v_n$ and $w_1, \dots, w_n$ be two bases of V and A_f and C_f be the matrices associated to f with respect to $v_1, \dots, v_n$ and $w_1, \dots, w_n$ respectively. Moreover, let B be the base change matrix like above. Then*

$$C_f = B^{-1} A_f \sigma(B).$$

This simple computation is left to the reader. Motivated by this lemma we define the following equivalence relation on $\mathrm{GL}_n(k)$.

Definition 1.2.20. — Two matrices $A, C \in \mathrm{GL}_n(k)$ are called *σ-conjugated*, if there is a matrix $B \in \mathrm{GL}_n(k)$ such that $C = B^{-1} A \sigma(B)$.

Frobenius and Flatness. — The last point in this section covers a theorem of Kunz, which gives a connection between the flatness of the Frobenius and the regularity of the ring. If A is a ring of characteristic $p > 0$ and σ is the n-th power of the Frobenius endomorphism, $\sigma\colon a \mapsto a^{p^n}$, then we write A^{p^n} for the image of A under σ. For an ideal I in A we write $I^{(p^n)} := I^{(\sigma)}$. In particular, if $I = (a_1, \dots, a_r)$ then we have $I^{(p^n)} = (a_1^{p^n}, \dots, a_r^{p^n})$. For a prime ideal $\mathfrak{p}$ in A it holds

$$\sigma^{-1}(\mathfrak{p}) = \{a \in A \mid a^{p^n} \in \mathfrak{p}\} = \mathfrak{p}.$$

The following result of Kunz [Mat80, Theorem 107] gives a connection between the regularity of A and the flatness of σ.

Theorem 1.2.21. — *Let A be a Noetherian local ring of characteristic $p > 0$. The following assertions are equivalent:*

(i) A is a regular local ring;

(ii) A is reduced and A is flat over A^{p^n} for every $n > 0$;

(iii) *A is reduced and A is flat over A^{p^n} for some $n > 0$.*

This theorem applies for example to a smooth algebra A over a perfect field k of characteristic $p > 0$, since smoothness is a local property and over a perfect field smoothness is equivalent to regularity (cf. [Mat80, Chapter 11]). We see that in this case the Frobenius $\sigma: A \to A$ is flat. Since $\sigma^{-1}(\mathfrak{p}) = \mathfrak{p}$, the Frobenius is even faithfully flat.

§3 Divided powers

Let A be a commutative ring with unit 1 and let I be an ideal of A.

Definition 1.3.22. — A *divided power structure* (DP-structure) on I is a family $\gamma_n: I \to A$ of maps for $n \in \mathbf{N}$ satisfying

(i) $\gamma_0(x) = 1$ and $\gamma_1(x) = x$ for $x \in I$;

(ii) $\gamma_n(x) \in I$ for $n \geq 1$ and $x \in I$;

(iii) $\gamma_n(x + y) = \sum_{i=0}^{n} \gamma_i(x)\gamma_{n-i}(y)$ for $x, y \in I$;

(iv) $\gamma_n(\lambda x) = \lambda^n \gamma_n(x)$ for $\lambda \in A$ and $x \in I$;

(v) $\gamma_n(x)\gamma_m(x) = \binom{n+m}{n}\gamma_{n+m}(x)$ for $x \in I$ and $n, m \in \mathbf{N}$;

(vi) $\gamma_n(\gamma_m(x)) = \frac{(nm)!}{n!(m!)^n}\gamma_{nm}(x)$ for $x \in I$ and $n, m \in \mathbf{N}$.

Remark 1.3.23. — (i) Note that $\frac{(nm)!}{n!(m!)^n}$ is just the number of partitions of a set with nm elements into n subsets with m elements. Thus, this is an integer.

(ii) It follows from (i) and (v) that $x^n = n!\gamma_n(x)$ for $n \in \mathbf{N}$. Indeed, this is true by (i) for $n = 1$. For $n > 1$ we have $n\gamma_n(x) = \gamma_{n-1}(x)\gamma_1(x)$ by (v) and hence

$$n!\gamma_n(x) = (n-1)!\gamma_{n-1}(x)\gamma_1(x) = x^{n-1}x = x^n.$$

(iii) For $n > 0$ it holds $\gamma_n(0) = 0$ by (iv). ◃

We say that (I, γ) is a DP-ideal in A and that (A, I, γ) is a DP-ring.

Example 1.3.24. — (i) $I = \{0\}$ is a DP-ideal with $\gamma_n(0) = 0$ for all $n \in \mathbf{N}$.

(ii) Let A be a $\mathbf{Q}$-algebra. Then every ideal has a unique DP-structure given by $\gamma_n(x) = x^n/n!$.

(iii) If there exists $0 \neq m \in \mathbf{N}$ with $mA = 0$, then every DP-ideal (I, γ) is a nilideal. In fact, we have for $x \in I$ by the above remark $x^n = n!\gamma_n(x)$ and for $n \geq m$ it follows $x^n = 0$. ◂

We are mainly interested in divided powers on the maximal ideal in the ring of Witt vectors of a perfect field of characteristic $p > 0$. Actually, we can define divided powers in a slightly more general situation. So let A be a ring of characteristic $p > 0$ and $W(A)$ its ring of Witt vectors. Denote the ideal $V(A)$ by I.

Lemma 1.3.25. — *Let $p \in \mathbf{N}$ be a prime and $n > 0$ an integer. Let $n = \sum_{i=0}^{r} a_i p^i$ be the p-adic expansion of n. Then*

$$v_p(n!) = \frac{n - \sum_{i=0}^{r} a_i}{p-1}.$$

Proof. — Denote by $\lfloor x \rfloor$ the largest interger less than or equal to x. We claim that

$$v_p(n!) = \sum_{r=1}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} \left\lfloor \frac{n}{p^r} \right\rfloor.$$

Let $1 \leq m \leq n$ be divisible by p^r. Then $p^r \leq m \leq n$ and $r \leq \left\lfloor \frac{\ln n}{\ln p} \right\rfloor$. Thus

$$v_p(m) = \sum_{\substack{r=1 \\ p^r | m}}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} 1.$$

It follows

$$\begin{aligned} v_p(n!) &= \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{\substack{r=1 \\ p^r | m}}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} 1 \\ &= \sum_{r=1}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} \sum_{\substack{m=1 \\ p^r | m}}^{n} 1 = \sum_{r=1}^{\left\lfloor \frac{\ln n}{\ln p} \right\rfloor} \left\lfloor \frac{n}{p^r} \right\rfloor. \end{aligned}$$

since there are exactly $\left\lfloor \frac{n}{p^r} \right\rfloor$ integers in the interval $[1, n]$, which are divisible by p^r. This proves the claim. Now, if

$$n = a_0 + a_1 p + \cdots + a_r p^r, \quad 0 \leq a_i < p$$

is the p-adic expansion of n, then

$$\begin{aligned} \left\lfloor \frac{n}{p} \right\rfloor &= a_1 + a_2 p + \cdots + a_r p^{r-1} \\ \left\lfloor \frac{n}{p^2} \right\rfloor &= \qquad a_2 + \cdots + a_r p^{r-2} \\ &\vdots \\ \left\lfloor \frac{n}{p^r} \right\rfloor &= \qquad\qquad a_r \end{aligned}$$

Summing up yields

$$\begin{aligned} v_p(n!) &= a_0 \frac{p^0 - 1}{p-1} + a_1 \frac{p^1 - 1}{p-1} + a_2 \frac{p^2 - 1}{p-1} + \cdots + a_r \frac{p^r - 1}{p-1} \\ &= \frac{n - \sum_{i=0}^{r} a_i}{p-1}. \end{aligned}$$

∎

Remark 1.3.26. — The claim in the proof implies

$$v_p(n!) = \begin{cases} 0 & \text{, if } n < p \\ \left\lfloor \frac{n}{p} \right\rfloor + v_p\left(\left\lfloor \frac{n}{p} \right\rfloor ! \right) & \text{, otherwise.} \end{cases}$$

◁

By our assumption, A is an $\mathbf{F}_p$-algebra. The structure morphism $\mathbf{F}_p \to A$ induces a morphism $\mathbf{Z}_p = W(\mathbf{F}_p) \to W(A)$ and we can consider $\mathbf{Z}_p$ as a subring of $W(A)$. For $n \in \mathbf{N}$ with $n \geq 1$ the above lemma implies

$$v_p\left(\frac{p^{n-1}}{n!}\right) = n - 1 - \frac{n - \sum_{i=0}^r a_i}{p-1} > 0.$$

This means that $p^{n-1}/(n!)$ is an element of $\mathbf{Z}_p$ and hence of $W(A)$. Therefore the following definition makes sense.

Definition 1.3.27. — Let A be a ring of characteristic $p > 0$ and $I = V(W(A))$. For $n \in \mathbf{N}$ define $\gamma_n \colon I \to W(A)$ by

$$\gamma_n(V(x)) = \begin{cases} 1 & \text{, if } n = 0 \\ \frac{p^{n-1}}{n!} V(x^n) & \text{, if } n > 0. \end{cases}$$

Lemma 1.3.28. — *The mappings γ_n endow I with a DP-structure.*

Proof. — We verify the properties of definition 1.3.22. Property (i) is obviously true and (ii) follows from the above discussion. To check the remaining properties, we use proposition 1.1.9. For (iii) let $x, y \in W(A)$. We compute

$$\begin{aligned}
\sum_{i=0}^n \gamma_i(V(x))\gamma_{n-i}(V(y)) &= \sum_{i=0}^n \frac{p^{i-1}}{i!} V(x^i) \cdot \frac{p^{n-i-1}}{(n-i)!} V(y^{n-i}) \\
&= \sum_{i=0}^n \frac{p^{n-2}}{i!(n-i)!} \underbrace{V(x^i)V(y^{n-i})}_{=pV(x^i y^{n-i})} \\
&= \sum_{i=0}^n \frac{p^{n-1}}{n!} \cdot \frac{n!}{i!(n-i)!} V(x^i y^{n-i}) \\
&= \frac{p^{n-1}}{n!} \sum_{i=0}^n \binom{n}{i} V(x^i y^{n-i}) \\
&= \frac{p^{n-1}}{n!} V\left(\sum_{i=0}^n \binom{n}{i} x^i y^{n-i} \right) \\
&= \frac{p^{n-1}}{n!} V((x+y)^n) \\
&= \gamma_n(V(x+y)).
\end{aligned}$$

For (iv) let $\lambda \in W(A)$ and $V(x) \in I$. Using $\lambda V(x) = V(F(\lambda)x)$ and that F is a ring homomorphism, this follows immediately from the definition of γ_n. For (v) let $V(x) \in I$. Then

$$\begin{aligned}
\gamma_n\big(V(x)\big)\gamma_m\big(V(x)\big) &= \frac{p^{n-1}}{n!} \cdot \frac{p^{m-1}}{m!} V(x^n)V(x^m) \\
&= \frac{p^{n+m-1}}{n!m!} V(x^{n+m}) \\
&= \frac{(n+m)!}{n!m!} \cdot \frac{p^{n+m-1}}{(n+m)!} V(x^{n+m}) \\
&= \binom{n+m}{n} \gamma_{n+m}\big(V(x)\big).
\end{aligned}$$

For (vi) let $V(x) \in I$. Then

$$\begin{aligned}
\gamma_n\Big(\gamma_m\big(V(x)\big)\Big) &= \gamma_n\left(\frac{p^{m-1}}{m!} V(x^m)\right) \\
&= \gamma_n\left(V\left(F\left(\frac{p^{m-1}}{m!}\right) x^m\right)\right) \\
&= \frac{p^{n-1}}{n!} V\left(F\left(\frac{p^{m-1}}{m!}\right)^n x^{nm}\right) \\
&= \frac{p^{n-1}}{n!} \cdot \frac{p^{nm-n}}{(m!)^n} V(x^{nm}) \\
&= \frac{p^{nm-1}}{n!(m!)^n} V(x^{nm}) \\
&= \frac{(nm)!}{n!(m!)^n} \cdot \frac{p^{nm-1}}{(nm!)} V(x^{nm}) \\
&= \frac{(nm)!}{n!(m!)^n} \gamma_{nm}\big(V(x)\big).
\end{aligned}$$

∎

Since A has characteristic $p > 0$, we have $F\big(V(x)\big) = px = V\big(F(x)\big)$ for any $x \in W(A)$ and in particular $px \in I$. Therefore, it makes sense to calculate

$$\begin{aligned}
\gamma_n(px) &= \gamma_n\Big(V\big(F(x)\big)\Big) \\
&= \frac{p^{n-1}}{n!} V\big(F(x)^n\big) \\
&= \frac{p^{n-1}}{n!} V\big(F(x^n)\big) \\
&= \frac{p^n}{n!} x^n.
\end{aligned}$$

If the ring A is in addition perfect, then $I = pW(A)$ and any $x \in I$ can be written as $x = py$. This implies $\gamma_n(x) = \frac{p^n}{n!} y^n = \frac{x^n}{n!}$. If moreover k is a perfect field, then $W(k)$ is a discrete valuation ring and it follows from remark 1.3.23 (ii) that its maximal ideal $pW(k)$ has a unique DP-structure. We summarize our discussion in the following lemma.

Lemma 1.3.29. — *Let k be a perfect field of characteristic $p > 0$. Then the maximal ideal $pW(k)$ has a unique DP-structure given by $\gamma_n(x) = \frac{x^n}{n!}$ for $x \in pW(k)$.*

Definition 1.3.30. — Let (A, I, γ) and (B, J, δ) be two DP-rings. A *DP-morphism* $f\colon (A, I, \gamma) \to (B, J, \delta)$ is a ring homomorphism $f\colon A \to B$ such that

(i) $f(I) \subset J$;

(ii) $f(\gamma_n(x)) = \delta_n(f(x))$ for all $n \in \mathbf{N}$ and all $x \in I$.

If A is a ring, I an ideal in A and $0 \neq m \in \mathbf{N}$ an integer with $I^m = 0$ such that $(m-1)!$ is invertible in A, then I has a DP-structure given by

$$\gamma_n(x) = \begin{cases} \frac{x^n}{n!} & \text{, if } n < m \\ 0 & \text{, if } n \geq m. \end{cases}$$

But in general there are many different DP-structures on I.
We turn our attention to the truncated ring of Witt vectors $W_m(k)$ of a perfect field k of characteristic $p > 0$. The maximal ideal $pW_m(k)$ has many DP-structures (see [Ber74, Chap. I, 1.2.6] for an example when $k = \mathbf{F}_p$), but there is one which is natural in the sense that it is the one induced from the unique DP-structure on the ideal $pW(k)$ in $W(k)$. This is justified by the next proposition. Before stating this proposition, we need a definition.

Definition 1.3.31. — Let (A, I, γ) be a DP-ring. An ideal $J \subset I$ is called a *sub-DP-ideal* if $\gamma_n(y) \in J$ for all $y \in J$ and $n \in \mathbf{N}$.

Proposition 1.3.32. — *Let (A, I, γ) be a DP-ring.*

(i) Let $J \subset A$ be an ideal. Then there exists a unique DP-structure $\bar{\gamma}$ on $\bar{I} := I/(I \cap J)$ such that the canonical homomorphism $(A, I, \gamma) \to (A/J, \bar{I}, \bar{\gamma})$ is a DP-morphism, if and only if $I \cap J \subset I$ is a sub-DP-ideal.

(ii) Let (J, δ) be a DP-ideal in A. Then IJ is a sub-DP-ideal of I and J and the DP-mappings γ and δ agree on IJ.

Proof. — (i) see [BO78, 3.5], (ii) see [BO78, 3.10]. ∎

Let (A, I, γ) be a DP-ring and B an A-algebra. When do we have a DP-structure on the image IB of I in B?

Definition 1.3.33. — Let (A, I, γ) be a DP-ring and B an A-algebra. We say that γ *extends to* B, if there exists a DP-structure $\overline{\gamma}$ on IB such that the map $(A, I, \gamma) \to (B, IB, \overline{\gamma})$ is a DP-morphism.

Remark 1.3.34. — Assume that γ extends to B. Then $\overline{\gamma}$ is unique. Indeed, let $f\colon (A, I, \gamma) \to (B, IB, \overline{\gamma})$ be the corresponding DP-morphism. Each element of IB may be written as $f(a)b$ with $a \in I$ and $b \in B$. It follows from the definition of divided powers and because f is a DP-morphism that

$$\overline{\gamma}_n(f(a)b) = b^n \overline{\gamma}_n(f(a)) = b^n f(\gamma_n(a)).$$

Thus, the extension $\overline{\gamma}$ is unique if it exists. ◁

Lemma 1.3.35. — *Let (A, I, γ) be a DP-ring and B an A-algebra.*

(i) If I is principal, then γ extends to B.

(ii) If B is a flat A-algebra, then γ extends to B.

Proof. — (i) see [BO78, 3.15], (ii) see [BO78, 3.22]. ∎

There is an analogue of the symmetric algebra of an A-module in the context of divided powers.

Theorem 1.3.36. — *Let A be a ring and M be an A-module. There exists a DP-algebra*

$$(\Gamma_A(M), \Gamma_A^+(M), \gamma)$$

and an A-linear map $\varphi\colon A \to \Gamma_A^+(M)$ satisfying the following universal property: Given any A-DP-algebra (B, J, δ) and A-linear map $\psi\colon M \to J$, there is a unique DP-morphism $\overline{\psi}\colon (\Gamma_A(M), \Gamma_A^+(M), \gamma) \to (B, J, \delta)$ making the diagram

$$\begin{tikzcd} M \arrow[r, "\psi"] \arrow[d, "\varphi"'] & J \\ \Gamma_A^+(M) \arrow[ur, dashed, "\overline{\psi}"'] & \end{tikzcd}$$

commute.

Proof. — See [BO78, 3.9]. ∎

Remark 1.3.37. — (i) The A-algebra $\Gamma_A(M)$ is graded, $\Gamma_A(M) = \bigoplus_{n \in \mathbf{N}} \Gamma_A^n(M)$. We have $\Gamma_A^0(M) = A$, $\Gamma_A^1(M) = M$ and $\Gamma_A^+(M) = \bigoplus_{n \geq 1} \Gamma_A^n(M)$.

(ii) For $x \in M$ we write $x^{[1]} := \varphi(x) \in \Gamma_A^+(M)$ and $x^{[n]} := \gamma_n(\varphi(x)) \in \Gamma_A^n(M)$.

(iii) $\Gamma_A^n(M)$ is generated as A-module by $\{x^{[q]} = x_1^{[q_1]} \cdots x_m^{[q_m]} \mid \sum q_i = n, x_i \in M\}$. In particular, if M is free with basis $\{x_i \mid i \in I\}$, then $\Gamma_A^n(M)$ is free with basis $\{x^{[q]} = x_1^{[q_1]} \cdots x_m^{[q_m]} \mid \sum q_i = n, i \in I\}$. ◃

Given a PD-ring (A, I, γ) and an A-algebra B together with an ideal $J \subset B$, it is sometimes neccessary to construct a DP-ring $(D_{B,\gamma}(J), \overline{J}, \delta)$ with divided powers δ compatible with the divided powers γ. This is the content of the next proposition.

Proposition 1.3.38. — *Let (A, I, γ) be a DP-ring and let J be an ideal in an A-algebra B. Then there exists a B-algebra $D_{B,\gamma}(J)$ with a DP-ideal $(\overline{J}, \delta)$ such that $JD_{B,\gamma}(J) \subset \overline{J}$ and δ is compatible with γ, satisfying the following universal property: For any B-algebra C with DP-ideal (K, ρ) such that $JC \subset K$ and ρ is compatible with γ, there exists a unique DP-morphism $(D_{B,\gamma}(J), \overline{J}, \delta) \to (C, K, \rho)$ making the following diagram commute*

$$\begin{tikzcd} (D_{B,\gamma}(J), \overline{J}, \delta) \arrow[d] \arrow[drr, dashed] & & \\ (B, J) \arrow[rr] & & (C, K, \rho) \\ & (A, I, \gamma) \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Proof. — [BO78, 3.19]. ∎

Example 1.3.39. — Let A be a ring and $B = A[X_1, \dots, X_n]$ be the polynomial algebra over A. Then the DP-envelope $D_{B,0}(J)$ with $J = (X_1, \dots, X_n)$ is just $\Gamma_A(B)$ and will be denoted by $A\langle X_1, \dots, X_n\rangle$ (cf. [BO78, 3.20.5]). It is called the *PD-polynomial algebra* over A. This name is justified by the following universal property: Given any A-DP-algebra (C, K, ρ) and $y_1, \dots, y_n \in K$, there exists a unique A-DP-morphism $A\langle X_1, \dots, X_n\rangle \to (C, K, \rho)$ such that $X_i \mapsto y_i$ for $1 \le i \le n$. ◂

The following proposition will be used in the subsequent chapters.

Proposition 1.3.40. — *Let A be a ring and I an ideal in A generated by a regular sequence. Let (D, J, δ) be the DP-envelope of A with respect to I. Then there is a unique DP-morphism*

$$\bigoplus_{m \in \mathbf{N}} \Gamma^m_{A/I}(I/I^2) \longrightarrow \bigoplus_{m \in \mathbf{N}} J^{[m]}/J^{[m+1]},$$

which is an isomorphism.

Proof. — See [Ber74, Chap. I, 3.4.4]. ∎

§4 Grothendieck topologies, sites and topoi

In this section we recall the main definitions and properties of topoi as needed in the subsequent chapters. In order not to run into any set-theoretical difficulties, we choose once and for all a universe $\mathcal{U}$ and make the agreement that all categories are small with respect to $\mathcal{U}$. For example, if we consider the category of X-schemes, then it is tacitly understood that X is an element of $\mathcal{U}$. Having fixed a universe, we will not mention it in the following anymore, but the reader should remember that there is always a universe in the background. For more details see [SGA72a] and [SGA72b].

Definition 1.4.41. — Let $\mathcal{C}$ be a category. A *Grothendieck topology* on $\mathcal{C}$ consists for each object X of $\mathcal{C}$ of a set $\mathrm{Cov}(X)$ of families of morphisms in $\mathcal{C}$ with fixed target X, called *coverings of* X, satisfying the following properties:

(i) If $V \to X$ is an isomorphism in $\mathcal{C}$, then $\{V \to X\} \in \mathrm{Cov}(X)$;

(ii) if $\{U_i \to X\}_{i \in I} \in \mathrm{Cov}(X)$ and for each $i \in I$ we have $\{V_{ij} \to U_i\}_{j \in J_i} \in \mathrm{Cov}(U_i)$, then the composition $\{V_{ij} \to X\}_{i \in I, j \in J_i}$ is in $\mathrm{Cov}(X)$;

(iii) if $\{U_i \to X\}_{i \in I} \in \mathrm{Cov}(X)$, then for any morphism $V \to X$ in $\mathcal{C}$ the fibre product $U_i \times_X V$ exists in $\mathcal{C}$ for every $i \in I$ and $\{U_i \times_X V \to V\} \in \mathrm{Cov}(V)$.

Remark 1.4.42. — Condition (ii) in the above definition is sometimes referred to as "stable under composition" and condition (iii) as "stable under base change". ◃

Definition 1.4.43. — A *site* is a category endowed with a Grothendieck topology.

Let $(\mathbf{Ab})$ denote the category of abelian groups. If $\mathcal{C}$ is any category, a *presheaf* is a contravariant functor $\mathscr{F}:\mathcal{C} \to (\mathbf{Ab})$. A morphism of presheaves is a morphism of contravariant functors. If $\mathcal{C}$ is a site, then a presheaf $\mathscr{F}$ is called a *sheaf*, if for every U in $\mathcal{C}$ and every covering $\{U_i \to U\}_{i\in I} \in \mathrm{Cov}(U)$ the diagram

$$\mathscr{F}(U) \longrightarrow \prod_i \mathscr{F}(U_i) \rightrightarrows \prod_{i,j} \mathscr{F}(U_i \times_U U_j)$$

is exact in $\mathcal{C}$. Morphisms of sheaves are defined as morphisms of presheaves. The category of (abelian) sheaves on a site $\mathcal{C}$ is denoted by $\mathrm{Sh}(\mathcal{C})$.

Definition 1.4.44. — Let $\mathcal{C}$ and $\mathcal{D}$ be sites. A functor $u:\mathcal{C} \to \mathcal{D}$ is called *continuous*, if for every U in $\mathcal{C}$ and every covering $\{U_i \to U\}_{i\in I} \in \mathrm{Cov}(U)$

(i) $\{u(U_i) \to u(U)\}_{i\in I} \in \mathrm{Cov}(u(U))$;

(ii) for any morphism $V \to U$ in $\mathcal{C}$ the morphism $u(U_i \times_U V) \to u(U_i) \times_{u(U)} u(V)$ is an isomorphism in $\mathcal{D}$.

Lemma 1.4.45. — *Let $u:\mathcal{C} \to \mathcal{D}$ be a continuous functor and $\mathscr{F}$ be a sheaf on $\mathcal{D}$. then $u^s\mathscr{F} := \mathscr{F} \circ u$ is a sheaf on $\mathcal{C}$.*

Proof. — Let $\{U_i \to U\}_{i\in I}$ be a covering in $\mathcal{C}$. By assumption $\{u(U_i) \to u(U)\}_{i\in I}$ is a covering in $\mathcal{D}$ and $u(U_i \times_U U_j) \simeq u(U_i) \times_{u(U)} u(U_j)$. Hence the sheaf condition for $u^s\mathscr{F}$ and the covering $\{U_i \to U\}_{i\in I}$ is equivalent to the sheaf condition for $\mathscr{F}$ and the covering $\{u(U_i) \to u(U)\}_{i\in I}$. ∎

Proposition 1.4.46. — *Let $u:\mathcal{C} \to \mathcal{D}$ be a continuous functor. The functor $u^s: \mathrm{Sh}(\mathcal{D}) \to \mathrm{Sh}(\mathcal{C})$ is left exact and admits a left adjoint $u_s: \mathrm{Sh}(\mathcal{C}) \to \mathrm{Sh}(\mathcal{D})$.*

Proof. — See [Tam94, Ch I 3.6.2]. What Tamme calls a morphism of topologies is in our terminology a continuous functor. ∎

Remark 1.4.47. — Being left adjoint to u^s implies that the functor u_s is right exact. ◁

Definition 1.4.48. — Let $\mathcal{C}$ and $\mathcal{D}$ be sites. A *morphism of sites* $f: \mathcal{D} \to \mathcal{C}$ is given by a continuous functor $u:\mathcal{C} \to \mathcal{D}$ such that u_s is exact.

Note that u and f go in opposite directions. If f is a morphism of sites, we set $f^{-1} := u_s$ and $f_* := u^s$ and call f^{-1} the *inverse image functor* and f_* the *direct image functor*. The following lemma gives a criterion for a continuous functor to induce a morphism of sites.

Lemma 1.4.49. — *Let $u:\mathcal{C} \to \mathcal{D}$ be a continuous functor of sites. Assume that*

(i) $\mathcal{C}$ has a final object X and $u(X)$ is a final object of $\mathcal{D}$;

(ii) in $\mathcal{C}$ all finite fibre products exist and u commutes with them.

Then the functor u_s is exact.

Proof. — See [Tam94, Ch I 3.6.7]. ■

Let U be an object of a site $\mathcal{C}$. We define an additive and left exact functor

$$\Gamma_U\colon \mathrm{Sh}(\mathcal{C}) \to (\mathbf{Ab})$$

by $\Gamma_U(\mathscr{F}) := \mathscr{F}(U)$ (cf. [Tam94, Ch I 3.3]). If $\mathcal{C}$ has a final object X, we call Γ_X the *global section functor*. It is easy to see that in this case we have

$$\mathscr{F}(X) = \Gamma_X(\mathscr{F}) = \mathrm{Hom}_{\mathrm{Sh}(\mathcal{C})}(e, \mathscr{F}),$$

where e denotes the abelian sheaf associated to the constant presheaf $\mathbf{Z}$. For an arbitrary site we define the global section functor Γ by

$$\Gamma(\mathscr{F}) := \mathrm{Hom}_{\mathrm{Sh}(\mathcal{C})}(e, \mathscr{F}).$$

It is well known that the abelian category $\mathrm{Sh}(\mathcal{C})$ of abelian sheaves on a site $\mathcal{C}$ has enough injective objects (cf. [Tam94, Ch I 3.2.2]). This enables us to define cohomology as the right derived functor of Γ.

Definition 1.4.50. — Let $\mathcal{C}$ be a site, U an object of $\mathcal{C}$ and $\mathscr{F}$ an abelian sheaf on $\mathcal{C}$. The *i-th cohomology group* of $\mathscr{F}$ on U is defined by the i-th right derived functor of Γ_U

$$\mathrm{H}^i(U, \mathscr{F}) := \mathrm{R}^i\Gamma_U(\mathscr{F}).$$

The *i-th cohomology group of $\mathscr{F}$ on $\mathcal{C}$* is defined by the i-th right derived functor of Γ

$$\mathrm{H}^i(\mathcal{C}, \mathscr{F}) := \mathrm{R}^i\Gamma(\mathscr{F}).$$

Remark 1.4.51. — In general, a global section s of a sheaf $\mathscr{F}$ is a compatible system $(s_T)_{T\in\mathcal{C}}$, i.e. an element of $\varprojlim_{T\in\mathcal{C}} \Gamma_T(\mathscr{F})$. ◁

Theorem 1.4.52 (Leray spectral sequence). — *Let $u\colon \mathcal{C} \to \mathcal{D}$ be a continuous functor of sites and U be an object of $\mathcal{C}$. Then for any abelian sheaf $\mathscr{F}$ on $\mathcal{D}$ there is a spectral sequence*

$$E_2^{pq} = \mathrm{H}^p(U, \mathrm{R}^q u^s(\mathscr{F})) \Longrightarrow E^{p+q} = \mathrm{H}^{p+q}(u(U), \mathscr{F}),$$

which is functorial in $\mathscr{F}$.

Proof. — See [Tam94, Ch I 3.7.6]. ■

For many Grothendieck topologies cohomological calculations can be done on the big or on the small site of a scheme. This is a consequence of the Leray spectral sequence. To make this more precise, we introduce the notion of a cocontinuous functor between sites. To state the definition, we first need another definition, which is also useful on its own.

Definition 1.4.53. — Let $\mathcal{C}$ be a category and let $\{U_i \to U\}_{i\in I}$ be a family of morphisms in $\mathcal{C}$. A *refinement* of $\{U_i \to U\}_{i\in I}$ is a family $\{V_j \to U\}_{j\in J}$ of morphisms in $\mathcal{C}$ such that there is a map of sets $\varepsilon\colon J \to I$ and for each $j \in J$ there is a morphism $V_j \to U_{\varepsilon(j)}$ in $\mathcal{C}$, which makes the diagram

$$\begin{tikzcd} V_j \arrow[rr] \arrow[dr] & & U_{\varepsilon(j)} \arrow[dl] \\ & U & \end{tikzcd}$$

commutative.

Definition 1.4.54. — Let $\mathcal{C}$ and $\mathcal{D}$ be sites. A functor $u\colon \mathcal{C} \to \mathcal{D}$ is called *cocontinuous*, if for every U in $\mathcal{C}$ and every covering $\{V_j \to u(U)\}_{j\in J}$ in $\mathcal{D}$, there exists a covering $\{U_i \to U\}_{i\in I}$ in $\mathcal{C}$ such that $\{u(U_i) \to u(U)\}_{i\in I}$ is a refinement of $\{V_j \to u(U)\}_{j\in J}$.

Remark 1.4.55. — Note that we do not require the family $\{u(U_i) \to u(U)\}_{i\in I}$ in $\mathcal{D}$ to be a covering. ◃

Proposition 1.4.56. — *Let $u\colon \mathcal{C} \to \mathcal{D}$ be a functor of sites and assume that*

(i) u is continuous;

(ii) u is cocontinuous;

(iii) u is fully faithful.

Then the adjoint morphism $\mathscr{F} \to u^s u_s \mathscr{F}$ is an isomorphism for all sheaves $\mathscr{F}$ on $\mathcal{C}$ and u^s is exact.

Proof. — See [Tam94, Ch I 3.9.2]. ∎

Corollary 1.4.57. — *Let u be as in the proposition. Then we have for all abelian sheaves $\mathscr{F}$ on $\mathcal{C}$ and all abelian sheaves $\mathscr{G}$ on $\mathcal{D}$ functorial isomorphisms*

$$\mathrm{H}^i(\mathcal{C}, \mathscr{F}) \cong \mathrm{H}^i(\mathcal{D}, u_s\mathscr{F}) \quad \textit{and} \quad \mathrm{H}^i(\mathcal{C}, u^s\mathscr{G}) \cong \mathrm{H}^i(\mathcal{D}, \mathscr{G}).$$

Proof. — See [Tam94, Ch I 3.9.3]. ∎

Example 1.4.58. — Let S be a scheme and denote by $(\mathbf{Sch}/S)$ the category of S-schemes with morphisms the S-morphisms of schemes. The big Zariski site of S is the category $(\mathbf{Sch}/S)$ with coverings given for any S-scheme X by surjective families $\{U_i \to X\}_{i\in I}$, where $U_i \to X$ is an open immersion of S-schemes. This site will be denoted by S_{ZAR}. The small Zariski site of S is the full subcategory of $(\mathbf{Sch}/S)$ consisting of all S-schemes X such that the structure morphism $X \to S$ is an open immersion. The coverings of X are the surjective families $\{U_i \to X\}_{i\in I}$, where $U_i \to S$ is an open immersion. This site is denoted by S_{Zar}. The functor $u\colon S_{\mathrm{Zar}} \to S_{\mathrm{ZAR}}$ obviously satisfies all the properties of the proposition and the corollary tells us that it does not matter, if we calculate the cohomology of a sheaf on the big or on the small Zariski site of S. ◂

Let $\mathcal{C}$ be a category and X an object of $\mathcal{C}$. We define the *category of objects over* X, denoted by $\mathcal{C}/X$, as the category with objects the morphisms $Y \to X$ in $\mathcal{C}$. A morphism of two arrows $Y \to X$ and $Y' \to X$ is a morphism in $\mathcal{C}$ such that the diagram

$$\begin{tikzcd} Y \arrow[rr] \arrow[dr] & & Y' \arrow[dl] \\ & X & \end{tikzcd}$$

commutes. The category $\mathcal{C}/X$ has a final object, namely $X \to X$. There is a functor $p_X : \mathcal{C}/X \to \mathcal{C}$, which takes an arrow $Y \to X$ to its source Y. If $\mathcal{C}$ is a site, then we define a Grothendieck topology on $\mathcal{C}/X$ by declaring a family $\{U_i \to U\}_{i \in I}$ of morphisms over X to be a covering in $\mathcal{C}/X$, if it is a covering in $\mathcal{C}$. It is then immediate that the functor p_X is continuous.

Lemma 1.4.59. — *Let $\mathcal{C}$ be a site and X an object of $\mathcal{C}$. The functor $p_X^s : \mathrm{Sh}(\mathcal{C}) \to \mathrm{Sh}(\mathcal{C}/X)$ induced by p_X is exact.*

Proof. — See [Tam94, Ch I 3.8.1]. ■

Corollary 1.4.60. — *Let the notation be as in the lemma. For all abelian sheaves $\mathscr{F}$ on $\mathcal{C}$ there is a functorial isomorphism*

$$\mathrm{H}^i(\mathcal{C}, \mathscr{F}) \cong \mathrm{H}^i(\mathcal{C}/X, p_X^s \mathscr{F}).$$

Proof. — See [Tam94, Ch I 3.8.2]. ■

Let S be a scheme and consider the category $(\mathbf{Sch}/S)$ of all S-schemes with morphisms the morphisms of S-schemes.

Definition 1.4.61. — Let E be a class of morphisms of $(\mathbf{Sch}/S)$, which

(i) contains all isomorphisms;

(ii) is stable under composition, i.e. the composition of two morphisms in E is again in E;

(iii) is stable under base change, i.e. for any morphism of S-schemes, the base change with a morphism in E is again in E.

Then the *big E-site of S* is the category $(\mathbf{Sch}/S)$ with the Grothendieck topology, where the coverings are the surjective families of morphisms in E. The *small E-site of S* is the full subcategory of all X-schemes with structure morphism in E and coverings again the surjective families of E-morphisms.

The items (i) - (iii) ensure that we really get a site, i.e. the axioms for coverings are satisfied. For completeness we close this section with the following definitions.

Definition 1.4.62. —

(i) A category $\mathcal{E}$ is called a *(Grothendieck) topos*, if there exists a site $\mathcal{C}$ such that $\mathcal{E}$ is equivalent to $\mathrm{Sh}(\mathcal{C})$.

(ii) A morphism $f : \mathcal{E}_1 \to \mathcal{E}_2$ of topoi is a pair $f = (f_*, f^{-1})$ of adjoint functors, where f_* is right adjoint to f^{-1} and f^{-1} is exact.

Remark 1.4.63. — There is a more general notion of a topos, see [MLM94]. But our definition is enough for applications in algebraic geometry. ◁

Chapter

2 F-gauges and displays

This chapter contains the first part of the main results of this thesis. The notion of F-gauges is introduced and the connections to F-zips and displays is given. The notion of F-gauges enables us to clarify the relation between F-zips and displays. For a perfect field there is the notion of F-crystals. We also give the relations between all those objects in this case. The last section about displays contains some proofs omitted in the paper by Langer and Zink.

§1 F-gauges

Let $\mathcal{A}$ be an additive category. We denote by $\mathbf{Gr}(\mathcal{A})$ the category of $\mathbf{Z}$-graded objects in $\mathcal{A}$, i.e. an object in $\mathbf{Gr}(\mathcal{A})$ is a family $M = (M^r)_{r\in\mathbf{Z}}$ with each M^r an object in $\mathcal{A}$ and a morphism $\alpha\colon M \to N$ in $\mathbf{Gr}(\mathcal{A})$ is a family of morphisms $\alpha = (\alpha_r)_{r\in\mathbf{Z}}$ such that $\alpha_r\colon M^r \to N^r$ is a morphism in $\mathcal{A}$. If $\mathcal{A}$ is abelian, then the kernel of a morphism α is $(\ker(\alpha_r))_{r\in\mathbf{Z}}$, where $\ker(\alpha_r)$ is the kernel in $\mathcal{A}$. With a similar definition of cokernels, we see that $\mathbf{Gr}(\mathcal{A})$ is again an abelian category if $\mathcal{A}$ is.
For $d \in \mathbf{Z}$ and two objects $(M^r)_{r\in\mathbf{Z}}$ and $(N^r)_{r\in\mathbf{Z}}$ of $\mathbf{Gr}(\mathcal{A})$ we call a family of morphisms $f = (f_r)_{r\in\mathbf{Z}}$ with $f_r\colon M^r \to N^{r+d}$ a morphism in $\mathcal{A}$, a morphism of *degree* $d = \deg(f)$. If M, N, P are objects of $\mathbf{Gr}(\mathcal{A})$ and $f\colon M \to N$ is a family of morphisms of degree d and $g\colon N \to P$ is a family of morphisms of degree e, then the composition $g \circ f\colon M \to P$ with

$$(g \circ f)_r := g_{r+d} \circ f_r\colon M^r \longrightarrow N^{r+d} \longrightarrow P^{r+d+e}$$

has degree $\deg(gf) = \deg(g) + \deg(f) = d + e$. Morphisms of degree 0 are just the morphisms in the category $\mathbf{Gr}(\mathcal{A})$.

Definition 2.1.1. — Let $\mathcal{A}$ be an additive category and $p \in \mathbf{N}$ be a prime number.

(i) The category $\mathbf{FG}(\mathcal{A})$ of F-*gauges* has as objects graded objects $M = (M^r)_{r\in\mathbf{Z}}$ in $\mathbf{Gr}(\mathcal{A})$ together with two families of morphisms $f, v\colon M \to M$ of degrees $\deg(f) = 1$ and $\deg(v) = -1$ satisfying $f_{r-1} \circ v_r = p\mathrm{id}_{M^r} = v_{r+1} \circ f_r$ for all $r \in \mathbf{Z}$. An F-gauge is denoted by the triple (M, f, v). A morphism of F-gauges $\alpha\colon (M, f_M, v_M) \to (N, f_N, v_N)$ is a morphism $\alpha\colon M \to N$

in $\mathbf{Gr}(\mathcal{A})$ such that the diagrams

$$\begin{tikzcd} M^r \arrow[r, "\alpha_r"] \arrow[d, "f_{M,r}"'] & N^r \arrow[d, "f_{N,r}"] \\ M^{r+1} \arrow[r, "\alpha_{r+1}"'] & N^{r+1} \end{tikzcd} \qquad \begin{tikzcd} M^r \arrow[r, "\alpha_r"] \arrow[d, "v_{M,r}"'] & N^r \arrow[d, "v_{N,r}"] \\ M^{r-1} \arrow[r, "\alpha_{r-1}"'] & N^{r-1} \end{tikzcd}$$

commute for all $r \in \mathbf{Z}$.

(ii) Let $s \in \mathbf{Z}$ be an integer. An F-gauge (M, f, v) is called of *level* $\geq s$, if v_r is an isomorphism for $r \leq s$. It is called of *level* $\leq s$, if f_r is an isomorphism for $r \geq s$. The corresponding subcategories are denoted by $\mathbf{FG}^{\geq s}(\mathcal{A})$ and $\mathbf{FG}^{\leq s}(\mathcal{A})$, respectively.

(iii) Let $a, b \in \mathbf{Z}$ be integers with $a \leq b$. The category $\mathbf{FG}^{[a,b]}(\mathcal{A})$ is the subcategory of F-gauges which are of level $\geq a$ and $\leq b$. Such an F-gauge will be called *of finite level*.

(iv) An F-gauge is called *bounded below* (resp. *bounded above*), if it is of level $\geq a$ for some $a \in \mathbf{Z}$ (resp. of level $\leq b$ for some $b \in \mathbf{Z}$). It is called *bounded*, if it is bounded below and above. The corresponding subcategories are denoted by $\mathbf{FG}^{+}(\mathcal{A})$, $\mathbf{FG}^{-}(\mathcal{A})$ and $\mathbf{FG}^{\flat}(\mathcal{A})$ respectively.

(v) An F-gauge of level ≥ 0 is called *effective*, one of level ≤ 0 is called *coeffective*.

Remark 2.1.2. — Let (M, f, v) be an F-gauge in $\mathbf{FG}^{[a,b]}(\mathcal{A})$. Then (M, f, v) is simply given by a finite diagram of the form

$$M^a \underset{v_{a-1}}{\overset{f_a}{\rightleftarrows}} \cdots \underset{v_{r-1}}{\overset{f_{r-2}}{\rightleftarrows}} M^{r-1} \underset{v_r}{\overset{f_{r-1}}{\rightleftarrows}} M^r \underset{v_{r+1}}{\overset{f_r}{\rightleftarrows}} M^{r+1} \underset{v_{r+2}}{\overset{f_{r+1}}{\rightleftarrows}} \cdots \underset{v_b}{\overset{f_{b-1}}{\rightleftarrows}} M^b.$$

Indeed, consider for example the relation $f_{r-1} \circ v_r = p$ for $r \leq a$. Then v_r is an isomorphism and hence f_{r-1} is uniquely determined by $f_{r-1} = p v_r^{-1}$. Similarly, f_r is an isomorphism for $r \geq b$ and hence $v_{r+1} = p f_r^{-1}$ is uniquely determined by f_r. We see that there is a natural isomorphism of F-gauges, where the upper row is the given F-gauge and the lower row is the F-gauge corresponding to the finite diagram above:

$$\begin{tikzcd} \cdots \arrow[r, shift left, "f_{a-2}"] & M^{a-1} \arrow[l, shift left, "v_{a-1}"] \arrow[r, shift left, "f_{a-1}"] \arrow[d, "v_a^{-1}"'] & M^a \arrow[l, shift left, "v_a"] \arrow[r, shift left, "f_a"] \arrow[d, equal] & \cdots \arrow[l, shift left, "v_{a+1}"] \arrow[r, shift left, "f_{b-1}"] & M^b \arrow[l, shift left, "v_b"] \arrow[r, shift left, "f_b"] \arrow[d, equal] & M^{b+1} \arrow[l, shift left, "v_{b+1}"] \arrow[r, shift left, "f_{b+1}"] \arrow[d, "f_b^{-1}"] & \cdots \arrow[l, shift left, "v_{b+2}"] \\ \cdots \arrow[r, shift left, "p"] & M^a \arrow[l, shift left, "="] \arrow[r, shift left, "p"] & M^a \arrow[l, shift left, "="] \arrow[r, shift left, "f_a"] & \cdots \arrow[l, shift left, "v_{a+1}"] \arrow[r, shift left, "f_{b-1}"] & M^b \arrow[l, shift left, "v_b"] \arrow[r, shift left, "="] & M^b \arrow[l, shift left, "p"] \arrow[r, shift left, "="] & \cdots \arrow[l, shift left, "p"] \end{tikzcd}$$

This means that all the information is contained in the interval $[a, b]$. In the same way we see that to give a morphism of F-gauges in $\mathbf{FG}^{[a,b]}(\mathcal{A})$ amounts just to give a morphism of the corresponding finite diagrams. ◃

If $\mathcal{A}$ is an abelian category, then as already remarked earlier $\mathbf{Gr}(\mathcal{A})$ is an abelian category and the category $\mathbf{FG}(\mathcal{A})$ and all its subcategories are abelian too. For an arbitrary additive category $\mathcal{A}$ we have the forgetful functor $\mathbf{FG}(\mathcal{A}) \to \mathbf{Gr}(\mathcal{A})$, which is faithful but in general not full.

To an object A of $\mathcal{A}$ we can associate an F-gauge $A(0)$ in $\mathbf{FG}^{[0,0]}(\mathcal{A})$, where $A(0)$ is the F-gauge concentrated in degree 0

$$\begin{tikzcd} \mathrm{deg}: & & -1 & & 0 & & 1 & \\ \cdots \arrow[r, shift left, "p"] & \arrow[l, shift left, "="] & A \arrow[r, shift left, "p"] \arrow[l, phantom] & \arrow[l, shift left, "="] & A \arrow[r, shift left, "="] & \arrow[l, shift left, "p"] & A \arrow[r, shift left, "="] & \arrow[l, shift left, "p"] \cdots \end{tikzcd}$$

It is left to the reader to check that this establishes an equivalence of categories $\mathcal{A} \to \mathbf{FG}^{[0,0]}(\mathcal{A})$. In our applications the category $\mathcal{A}$ is either the category of modules over a ring or the category of sheaves of $\mathscr{O}_S$-modules over a scheme S. In these cases, $\mathcal{A}$ is abelian and so is $\mathbf{FG}(\mathcal{A})$.

Filtered modules and F-gauges. — One of the main examples of F-gauges comes from filtered modules. We first give a precise definition of what we mean by filtered module and then construct a functor to F-gauges.

Definition 2.1.3. — Let A be an object of an abelian category $\mathcal{A}$.

(i) A *decreasing filtration on* A is a family $\{\mathrm{Fil}^i A\}_{i\in I}$, where each $\mathrm{Fil}^i A \subset A$ is a subobject of A and $\mathrm{Fil}^{i+1} A \subset \mathrm{Fil}^i A$ for all $i \in I$.

(ii) An *increasing filtration on* A is a family $\{\mathrm{Fil}^i A\}_{i\in I}$, where each $\mathrm{Fil}^i A \subset A$ is a subobject of A and $\mathrm{Fil}^{i+1} A \supset \mathrm{Fil}^i A$ for all $i \in I$.

Instead of writing $\{\mathrm{Fil}^i A\}_{i\in I}$ we will also denote this family simply by $\mathrm{Fil}^\bullet A$. Actually, we are interested in filtrations with some additional properties.

Definition 2.1.4. — A filtration $\{\mathrm{Fil}^i A\}_{i\in I}$ on an object A of an additive category $\mathcal{A}$ is called

(i) *separated*, if $\bigcap_{i\in I} \mathrm{Fil}^i A = 0$;

(ii) *exhaustive*, if $\bigcup_{i\in I} \mathrm{Fil}^i A = A$.

Moreover, if $p \in \mathbf{N}$ is a prime number and A is p-torsion free, then the filtration is called *p-adapted*, if it is decreasing and $p\mathrm{Fil}^i A \subset \mathrm{Fil}^{i+1} A$ for all $i \in I$.

We denote by $\mathbf{Fil}(\mathcal{A})$ the category of pairs $(A, \mathrm{Fil}^\bullet A)$, where A is an object of $\mathcal{A}$ and $\mathrm{Fil}^\bullet A$ is a decreasing, separated and exhaustive filtration on A indexed by $\mathbf{Z}$. A morphism in this category $\alpha\colon (A, \mathrm{Fil}^\bullet A) \to (B, \mathrm{Fil}^\bullet B)$ is a morphism $\alpha\colon A \to B$ in $\mathcal{A}$ such that $\alpha(\mathrm{Fil}^i A) \subset \mathrm{Fil}^i B$ for all $i \in \mathbf{Z}$. The subcategory of all p-adapted filtrations is denoted by $\mathbf{Fil}_{p-\mathrm{sep}}(\mathcal{A})$. We note that the category $\mathbf{Fil}(\mathcal{A})$ is additive but in general not abelian.

Example 2.1.5. — Let k be a field and consider the category $\mathbf{Vec}_k$ of finite dimensional vector spaces over k. By a *filtered vector space* we mean an object in the category $\mathrm{Fil}_k := \mathrm{Fil}(\mathbf{Vec}_k)$. If $(V, \mathrm{Fil}^\bullet V)$ is a filtered vector space, then the condition that the filtration is separated just means that $\mathrm{Fil}^i V = 0$ for $i \gg 0$ and that the filtration is exhaustive just means that $\mathrm{Fil}^i V = V$ for $i \ll 0$. Here we used the finite dimensionality. Let $f\colon (V, \mathrm{Fil}^\bullet V) \to (W, \mathrm{Fil}^\bullet W)$ be a morphism of filtered vector spaces. The kernel of f is given by the *subspace filtration*

$$\mathrm{Fil}^i \ker(f) = \ker(f) \cap \mathrm{Fil}^i V$$

and the cokernel of f is given by the *quotient filtration*

$$\mathrm{Fil}^i \mathrm{coker}(f) = \left(\mathrm{Fil}^i W + \mathrm{im}(f)\right)/\mathrm{im}(f).$$

It is left to the reader to check that these kernels and cokernels indeed satisfy the universal properties of kernels and cokernels. But it may happen that $\ker(f) = \mathrm{coker}(f) = 0$ and nevertheless f may not be invertible in Fil_k. Consider for example a vector space V with the trivial filtration

$$\mathrm{Fil}^i V = \begin{cases} V, & \text{if } i \leq 0 \\ 0, & \text{if } i > 0 \end{cases}$$

On the other hand consider $W = V$ with the filtration

$$\mathrm{Fil}^i W = \begin{cases} W, & \text{if } i \leq 1 \\ 0, & \text{if } i > 1 \end{cases}$$

Then the idendity induces a map of filtered vector spaces $V \to W$, whose kernel and cokernel vanish, but there is no inverse in the category Fil_k. ◂

Example 2.1.6. — The category $\mathrm{Fil}_{p-\mathrm{sep}}(\mathcal{A})$ is in general not abelian. For example let W be the ring of Witt vectors of a perfect field k. Let $M = N = W$ and consider the two filtrations

$$\mathrm{Fil}^i M = \begin{cases} p^i W, & \text{if } i > 0 \\ W, & \text{if } i \leq 0 \end{cases} \quad \text{and} \quad \mathrm{Fil}^i N = \begin{cases} p^i W, & \text{if } i > 1 \\ W, & \text{if } i \leq 1 \end{cases}$$

Then $(M, \mathrm{Fil}^\bullet M) \subset (N, \mathrm{Fil}^\bullet N)$, but the filtration on the quotient N/M is given by

$$\mathrm{Fil}^i\left(N/M\right) = \left(\mathrm{Fil}^i N\right)/\left(\mathrm{Fil}^i M\right),$$

which is obviously not p-adapted. ◂

There is one last definition, which is useful in the context of filtrations. This definition is similar to definition 1.1 in [Ogu01].

Definition 2.1.7. — Let $a, b \in \mathbf{Z}$ be integers with $a \leq b$. The full subcategory $\mathbf{Fil}^{[a,b]}_{p-\mathrm{sep}}(\mathcal{A})$ consists of pairs $(A, \mathrm{Fil}^\bullet A)$, where $\mathrm{Fil}^a A = \mathrm{Fil}^i A$ for all $i \leq a$ and $p\mathrm{Fil}^i A = \mathrm{Fil}^{i+1} A$ for all $i \geq b$. In this case the filtration is called of *level* $[a, b]$.

Example 2.1.8. — Let k be a perfect field of characteristic $p > 0$ and W be the ring of Witt vectors of k. For a free W-module A we define the p-adic filtration on A by

$$\mathrm{Fil}^i A := \begin{cases} p^i A, & \text{if } i > 0 \\ A, & \text{if } i \leq 0. \end{cases}$$

This filtration is of level $[0, 0]$ and p-adapted. ◂

Fix a prime $p \in \mathbf{N}$. In order to define a functor from the full subcategory $\mathbf{Fil}_{p-\mathrm{sep}}(\mathcal{A})$ of p-adapted objects of the category $\mathbf{Fil}(\mathcal{A})$ to the category $\mathbf{FG}(\mathcal{A})$, let $(A, \mathrm{Fil}^\bullet A)$ be p-seperated. We set

$$M^r := \mathrm{Fil}^r A \quad \text{for } r \in \mathbf{Z}.$$

The map $v_r \colon M^r \to M^{r-1}$ is given by the inclusion $\mathrm{Fil}^r A \subset \mathrm{Fil}^{r-1} A$ and the map $f_r \colon M^r \to M^{r+1}$ is given by p-multiplication, which is well defined since the filtration is p-adapted. If $\alpha \colon (A, \mathrm{Fil}^\bullet A) \to (B, \mathrm{Fil}^\bullet B)$ is a morphism in $\mathbf{Fil}(\mathcal{A})$, then α obviously induces a morphism between the associated F-gauges, since $\alpha(\mathrm{Fil}^i A) \subset \mathrm{Fil}^i B$ by definition of a morphism in $\mathbf{Fil}(\mathcal{A})$. We denote this functor by $\mathfrak{Fg} \colon \mathbf{Fil}_{p-\mathrm{sep}}(\mathcal{A}) \to \mathbf{FG}(\mathcal{A})$.

Proposition 2.1.9. — *The functor $\mathfrak{Fg}$ is fully faithful. Moreover, for integers $a \le b$ the restriction of $\mathfrak{Fg}$ to $\mathbf{Fil}^{[a,b]}_{p-\mathrm{sep}}(\mathcal{A})$ has image in $\mathbf{FG}^{[a,b]}(\mathcal{A})$.*

Proof. — We have to show that for two objects $(A, \mathrm{Fil}^\bullet A)$ and $(B, \mathrm{Fil}^\bullet B)$ of $\mathbf{Fil}_{p-\mathrm{sep}}(\mathcal{A})$ and $M := \mathfrak{Fg}(A, \mathrm{Fil}^\bullet A)$ and $N := \mathfrak{Fg}(B, \mathrm{Fil}^\bullet B)$ the induced map

$$\mathrm{Hom}_{\mathbf{Fil}(\mathcal{A})}\big((A, \mathrm{Fil}^\bullet A), (B, \mathrm{Fil}^\bullet B)\big) \longrightarrow \mathrm{Hom}_{\mathbf{FG}(\mathcal{A})}(M, N)$$

is bijective. To show surjectivity, let $\beta \colon M \to N$ be a morphism in $\mathbf{FG}(\mathcal{A})$. This means that we have a family $\beta = (\beta_r)_{r \in \mathbf{Z}}$ with $\beta_r \colon M^r \to N^r$ and that the diagrams

$$\begin{tikzcd} M^r \arrow[r, "\beta_r"] \arrow[d, "f_{M,r}"'] & N^r \arrow[d, "f_{N,r}"] \\ M^{r+1} \arrow[r, "\beta_{r+1}"'] & N^{r+1} \end{tikzcd} \qquad \begin{tikzcd} M^r \arrow[r, "\beta_r"] \arrow[d, "v_{M,r}"'] & N^r \arrow[d, "v_{N,r}"] \\ M^{r-1} \arrow[r, "\beta_{r-1}"'] & N^{r-1} \end{tikzcd}$$

commute for all $r \in \mathbf{Z}$. We set $\widetilde{M} := \bigcup_{r \in \mathbf{Z}} M^r$ and $\widetilde{N} := \bigcup_{r \in \mathbf{Z}} N^r$. Then $\widetilde{M} = A$ and $\widetilde{N} = B$ are objects of $\mathcal{A}$ since the filtrations are exhaustive and we can define a morphism $\alpha \colon \widetilde{M} \to \widetilde{N}$ by the following rule: If $m \in \widetilde{M}$, then there exists a minimal $r \in \mathbf{Z}$ with $m \in M^r$, since the filtration is separated, and we set $\alpha(m) := \beta_r(m)$. The filtrations are simply given by $\mathrm{Fil}^i \widetilde{M} := M^i$ and similarly for $\widetilde{N}$. Hence $M^i = \mathrm{Fil}^i A$ and $N^i = \mathrm{Fil}^i B$. By the definition of α and the above commutative diagram on the right hand side it follows that $\alpha(\mathrm{Fil}^i A) \subset \mathrm{Fil}^i B$. It is clear from the construction that $\mathfrak{Fg}(\alpha) = \beta$. To show injectivity, let $\alpha \colon (A, \mathrm{Fil}^\bullet A) \to (B, \mathrm{Fil}^\bullet B)$ be a morphism in $\mathrm{Fil}(\mathcal{A})$ such that $(\beta_r)_{r \in \mathbf{Z}} = \mathfrak{Fg}(\alpha) = 0$. This means that each β_r is zero. Thus the induced map $\bigcup_{r \in \mathbf{Z}} M^r \to \bigcup_{r \in \mathbf{Z}} N^r$ is zero and since the filtrations are exhaustive, α must be zero. The second statement in the proposition is clear. ∎

Corollary 2.1.10. — *Assume that $\mathcal{A}$ is an additive category such that each object in $\mathcal{A}$ is p-torsion free and that direct and inverse limits indexed by $\mathbf{N}$ exist. Then the functor $\mathfrak{Fg}$ gives an equivalence of categories from $\mathbf{Fil}_{p-\mathrm{sep}}(\mathcal{A})$ to the full subcategory of $\mathbf{FG}(\mathcal{A})$ of objects $(M^r)_{r \in \mathbf{Z}}$ with $\varprojlim_{f_r} M^r = 0$.*

Proof. — Obviously, the image of $\mathfrak{Fg}$ lies in the required subcategory. By the proposition it remains to show that $\mathfrak{Fg}$ is essentially surjective. So let $M = (M^r)_{r \in \mathbf{Z}}$ be an object of $\mathbf{FG}(\mathcal{A})$ with $\varprojlim_{f_r} M^r = 0$. By assumption each M^r is p-torsion free, i.e. p-multiplication on M^r is injective. The relation $f_{r-1} v_r = v_{r+1} f_r = p$ on M^r implies the injectivity of v_r. We define

$$A := \varinjlim_{r \in \mathbf{N}} M^{-r},$$

where the transition maps are given by the inclusions $v_r\colon M^r \to M^{r-1}$. We obtain a filtration on A by setting $\mathrm{Fil}^i A$ the image of M^i via the composition of the v_r in $A = \varinjlim_{r\in\mathbf{N}} M^{-r}$. This gives an object $(A, \mathrm{Fil}^\bullet A)$ of $\mathbf{Fil}(\mathcal{A})$. Note that we have an isomorphism $v_r^\infty\colon M^r \to \mathrm{Fil}^r A$ by the injectivity of the v_r. Since for $m \in M^r$ it holds $pm = v_{r+1}(f_r(m))$, we get $p\mathrm{Fil}^r A \subset \mathrm{Fil}^{r+1} A$ for all $r \in \mathbf{Z}$. Hence $(A, \mathrm{Fil}^\bullet A)$ is actually an object of $\mathbf{Fil}_{p-\mathrm{sep}}(\mathcal{A})$. The simple calculation

$$\begin{aligned} v_{r+1}^\infty(m) &= v_r^\infty\Big(v_{r+1}\big(f_r(m)\big)\Big) \\ &= v_r^\infty(pm) \\ &= pv_r^\infty(m) \end{aligned}$$

for $m \in M^r$ shows that the diagram

$$\begin{tikzcd} M^r \arrow[r, shift left, "f_r"] \arrow[d, "v_r^\infty"'] & M^{r+1} \arrow[l, shift left, "v_{r+1}"] \arrow[d, "v_{r+1}^\infty"] \\ \mathrm{Fil}^r A \arrow[r, shift left, "p"] & \mathrm{Fil}^{r+1} A \arrow[l, shift left, "\supset"] \end{tikzcd}$$

commutes for all $r \in \mathbf{Z}$. This means that the F-gauges $(M^r)_{r\in\mathbf{Z}}$ and $\mathfrak{Fg}(A, \mathrm{Fil}^\bullet A)$ are isomorphic via the family $(v_r^\infty)_{r\in\mathbf{Z}}$. ■

§2 F-crystals

Let k be a perfect field of positive characteristic p and denote by $W := W(k)$ the ring of Witt verctors of k. Moreover, let $B := B(k) := \mathrm{Quot}(W(k))$ be the quotient field of W. The Frobenius of k, W and B is denoted by the letter σ. If $\phi\colon M \to M$ is a σ-linear map of W-modules, then the linearization of ϕ is defined by

$$\phi^\sharp\colon M^{(p)} := M \otimes_\sigma W \longrightarrow M, \qquad m \otimes \lambda \longmapsto \lambda\phi(m).$$

Definition 2.2.11. — An *F-crystal over k* is a pair (M, ϕ), where M is a finitely generated free W-module and $\phi\colon M \to M \otimes_W B$ is a σ-linear injective map.

Example 2.2.12. — Let X be a proper and smooth scheme over k. Then the absolute Frobenius F_{abs} on X induces a σ-linear map $\phi\colon \mathrm{H}^i(X/W) \to \mathrm{H}^i(X/W)$ on the crystalline cohomology groups of X. If T is the torsion submodule of $\mathrm{H}^i(X/W)$, then $(\mathrm{H}^i(X/W)/T, \phi)$ is an F-crystal. In particular, if $i = 1$, then $\mathrm{H}^1(X/W)$ is torsion free and $(\mathrm{H}^1(X/W), \phi)$ is an F-crystal, the Dieudonnè module of the p-divisible group associated to the Albanese variety of X (see [BM90, II 3.11].). ◂

Definition 2.2.13. — A *morphism of F-crystals* $\alpha\colon (M, \phi) \to (N, \psi)$ is a homomorphism $\alpha\colon M \to N$ of W-modules such that the diagram

$$\begin{tikzcd} M \arrow[r, "\phi"] \arrow[d, "\alpha"'] & M \otimes_W B \arrow[d, "\alpha\otimes\mathrm{id}_B"] \\ N \arrow[r, "\psi"] & N \otimes_W B \end{tikzcd}$$

commutes.

With these definitions we get the category of F-crystals over k. This is an additive category, which is not abelian since cokernels do not exist in general.
If (M, ϕ) is an F-crystal, then the natural map $M \to M \otimes_W B, m \mapsto m \otimes 1$ identifiues M with a lattice in $M \otimes_W B$. Since M is finitely generated, the B-vector space $M \otimes_W B$ is finite dimensional and it follows that there are $a, b \in \mathbf{Z}$ such that $p^b M \subset \phi(M) \subset p^a M$.

Definition 2.2.14. — An F-crystal (M, ϕ) over k is called *effective*, if $\phi(M) \subset M$.

Remark 2.2.15. — Some authors define F-crystals as what we call an effective F-crystal and use the term *virtual* F-crystal for an F-crystal in our sense. ◁

***F*-crystals and elementary divisors.** — Since W is a discrete valution ring (cf. proposition 1.1.14), we can apply the theory of elementary divisors (see [Lan02, III Theorem 7.8 and 7.9]) and conclude that there is a pair bases $e_1, \dots, e_h$ and $f_1, \dots, f_h$ of M such that the W-linear injective map $\phi^\sharp \colon M^{(p)} \to M \otimes_W B$ is given by a matrix of the form

$$\begin{pmatrix} p^{\mu_1} & 0 & \cdots & 0 \\ 0 & p^{\mu_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & p^{\mu_h} \end{pmatrix}$$

with $\mu_j \in \mathbf{Z}$ and $\mu_1 \leq \cdots \leq \mu_h$.

Definition 2.2.16. — The *height* of an F-crystal (M, ϕ) is the dimension of the B-vector space $M \otimes_W B$.

We want to give a classification of F-crystals of height h in terms of matrices. Therefor, let $\alpha \colon (M, \phi) \to (N, \psi)$ be an isomorphism of F-crystals. This actually implies that (M, ϕ) and (N, ψ) must have the same height h and that M and N are both abstractly isomorphic to W^h as W-modules. The W-linear isomorphism α induces an isomorphism of vector spaces $\alpha_B := \alpha \otimes \mathrm{id}_B$, hence the diagram

$$\begin{tikzcd} M \otimes_W B \arrow[r, "\phi_B"] \arrow[d, "\alpha_B"'] & M \otimes_W B \arrow[d, "\alpha_B"] \\ N \otimes_W B \arrow[r, "\psi_B"] & N \otimes_W B \end{tikzcd}$$

commutes or put it differently that we have

$$\phi_B = \alpha_B^{-1} \circ \psi_B \circ \alpha_B.$$

Thus ϕ_B is uniquely determined by ψ_B. By the above considerations we can choose a basis of M such that the σ-linear map ϕ is given by a matrix of the form

$$A := \begin{pmatrix} p^{\mu_1} & 0 & \cdots & 0 \\ 0 & p^{\mu_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & p^{\mu_h} \end{pmatrix}$$

with $\mu_j \in \mathbf{Z}$ and $\mu_1 \leq \cdots \leq \mu_h$. The relation $\phi_B = \alpha_B^{-1} \circ \psi_B \circ \alpha_B$ implies that the represanting matrices are σ-conjugated. We obtain the following classification of F-crystals of height h. For shortness we set $GL_h := GL_h(W)$.

Theorem 2.2.17. — *Let k be a perfect field of characteristic $p > 0$. Then there is a bijection of sets*

$$\left\{ \begin{array}{c} F\text{-crystals of height } h \\ \text{with elementary divisors} \\ \mu_1 \leq \cdots \leq \mu_h \end{array} \right\} \Big/ \cong \xleftrightarrow{\sim} \mathrm{GL}_h \begin{pmatrix} p^{\mu_1} & & 0 \\ & \ddots & \\ 0 & & p^{\mu_h} \end{pmatrix} \mathrm{GL}_h \Big/ \sim_\sigma$$

with $\mu_i \in \mathbf{Z}$.

F-crystals and F-gauges. — The connection to F-gauges is given by the following construction: Let (M, ϕ) be an F-crystal over k. We define an F-gauge $(M^r)_{r\in\mathbf{Z}}$ by setting

$$M^r := \{m \in M \mid \phi(m) \in p^r M\}$$

for $r \in \mathbf{Z}$. The map v is given by the inclusion $M^r \subset M^{r-1}$ and f is given by multiplication with p. It is clear that this gives an F-gauge and that the construction is functorial. But there is some additional structure on such F-gauges, which arises from F-crystals. Namely, the map $\phi \colon M \to M \otimes_W B$ induces σ-linear maps

$$\varphi_r \colon M^r \longrightarrow M$$

defined by $\varphi_r(m) := p^{-r}\phi(m)$. This makes sense, since by definition of M^r we have $\phi(m) \in p^r M$ and W is torsion free. So, $\varphi_r(m)$ is a well defined element of M. Moreover, we have $pm \in M^{r+1} \subset M^r$ for $m \in M^r$ and hence by the σ-linearity

$$\varphi_{r+1}\big(f_r(m)\big) = \varphi_{r+1}(pm) = p\varphi_r(m).$$

We have two projective systems $(M^r, f_r)_{r\in\mathbf{N}}$ and $(M^{-r}, v_{-r})_{r\in\mathbf{N}}$ and we set

$$M^{+\infty} := \varinjlim_{f_r} M^r \quad \text{and} \quad M^{-\infty} := \varinjlim_{v_{-r}} M^{-r}.$$

In our case we can identify these W-modules to

$$M^{+\infty} \cong M^b \quad \text{and} \quad M^{-\infty} \cong M^a,$$

where $p^b M \subset \phi(M) \subset p^a M$ for suitable $a, b \in \mathbf{Z}$. Moreover, we see that $M^a = \bigcup_{r\in\mathbf{Z}} M^r = M$, because v_r is the inclusion. Using these informations we get a diagram

$$\begin{tikzcd} M^r \arrow[rr, "f_r"] \arrow[dr] \arrow[ddr, bend right, "\varphi_r"'] & & M^{r+1} \arrow[dl] \arrow[ddl, bend left, "\varphi_{r+1}"] \\ & \varinjlim_{f_r} M^r \arrow[d, dashed, "\varphi"] & \\ & M & \end{tikzcd}$$

This implies that there exists a unique σ-linear map $\varphi\colon M^b \to M$ making the diagram commute. The maps φ_r are injective, since ϕ is by definition injective. Hence φ is injective. On the other hand we have $\varphi_b(M^b) = M$ and this shows that φ is surjective. Thus φ is a σ-linear bijective map, which by lemma 1.2.15 is the same as a σ-linear isomorphism. This motivates the following definition.

Definition 2.2.18. — Let S be a scheme and σ be an endomorphism of sheaves of rings of $\mathscr{O}_S$. A φ-F-gauge over $\mathscr{O}_S$ is an F-gauge $(M^r)_{r\in\mathbf{Z}}$ over $\mathscr{O}_S$, where each M^r is a quasi-coherent $\mathscr{O}_S$-module such that there is a σ-linear isomorphism of $\mathscr{O}_S$-modules

$$\varphi\colon \varinjlim_{f_r} M^r \longrightarrow \varinjlim_{v_r} M^r.$$

A morphism of φ-F-gauges is a morphism of F-gauges compatible with φ. The category of φ-F-gauges over $\mathscr{O}_S$ is denoted by $\mathbf{FG}^{\varphi,\sharp}(\mathscr{O}_S)$.

The following definition will be useful in the sequel.

Definition 2.2.19. — Let S be a scheme over $\mathbf{F}_p$. An F-gauge $(M^r)_{r\in\mathbf{Z}}$ over $\mathscr{O}_S$ is called

(i) *strict*, if the map $(f_r^\infty, v_r^\infty)\colon M^r \to M^{+\infty} \oplus M^{-\infty}$ is injective for all $r \in \mathbf{Z}$;

(ii) *quasi-rigid*, if the sequence

$$M^r \xrightarrow{f_r} M^{r+1} \xrightarrow{v_{r+1}} M^r \xrightarrow{f_r} M^{r+1}$$

is exact for all $r \in \mathbf{Z}$;

(iii) *rigid*, if it is strict and quasi-rigid.

If $S = \operatorname{Spec}(A)$ for a ring A and σ is an endomorphism of A, then the category $\mathbf{FG}^{\varphi,\sharp}(\mathscr{O}_S)$ is equivalent to the category of F-gauges over A such that there is a σ-linear isomorphism $\varphi\colon M^{+\infty} \to M^{-\infty}$ of A-modules. This equivalence is just given by the well-known equivalence of the category of quasi-coherent $\mathscr{O}_S$-modules and the category of A-modules. Using this equivalence we will denote the category of φ-F-gauges over A by $\mathbf{FG}^{\varphi,\sharp}(A)$. In particular, if $A = W(k)$ is the ring of Witt vectors of a perfect field k of charactetristic $p > 0$ and σ is the Frobenius on A, then our discussion above shows that we have a functor from the category of F-crystals over A to the category of φ-F-gauges over A. It is not hard to see that this functor is fully faithful, but it is not essential surjective. For details see section 5.3.

Reduction of F-gauges. — Although the following considerations are true in more generality, we focus only on the case needed in the sequel. So let k be a perfect field of positive characteristic p and W be the ring of Witt vectors of k. For a natural number $n \in \mathbf{N}$ we consider multiplication by p^n on W. This map is injective and its cokernel is isomorphic to $W_n \cong W/p^nW$. Given an F-gauge $(M^r)_{r\in\mathbf{Z}}$ over W, we get an F-gauge $(M^r/p^nM^r)_{r\in\mathbf{Z}}$ over W_n by reducing everything mod p^n. For $n = 1$ we get F-gauges over k with the relations $fv = vf = 0$, since p operates as 0 on k. The same is true for φ-F-gauges over W.

Lemma 2.2.20. — *Let $(M^r)_{r\in\mathbf{Z}}$ be a φ-F-gauge over W and $n \in \mathbf{N}$ be an integer. Then the reduction mod p^n of $(M^r)_{r\in\mathbf{Z}}$ is a φ-F-gauge over W_n.*

Proof. — The only thing to note is that direct limits commute with tensor products and hence we have $\varinjlim_{f_r} M^r \otimes_W W/p^n W \cong \varinjlim_{f_r} \left(M^r/p^n M^r\right)$ as W_n-modules. ∎

We can now define the notion of strictness also for F-gauges over W.

Definition 2.2.21. — Let k be a perfect field of characteristic $p > 0$ and W be the ring of Witt vectors of k.

(i) An F-gauge $M = (M^r)_{r\in\mathbf{Z}}$ over W is called of *finite type*, if M is of finite level and each M^r is of finte type over W.

(ii) An F-gauge $M = (M^r)_{r\in\mathbf{Z}}$ over W is called *strict*, if its reduction mod p is strict.

§3 F-zips

Let S be a scheme over $\mathbf{F}_p$. For a $\mathscr{O}_S$-module $\mathscr{M}$ we set

$$\mathscr{M}^{(p)} := F^*_{\mathrm{abs}}\mathscr{M} = \mathscr{M} \otimes_{F_{\mathrm{abs}}} \mathscr{O}_S$$

where $F_{\mathrm{abs}}: X \to X$ is the absolute Frobenius on X that is it is the idendity on the underlying topological space and maps a section a of $\mathscr{O}_S$ to a^p. We set $\sigma := F_{\mathrm{abs}}$. Note that σ is a ring endomorphism of $\mathscr{O}_S$, but in general it is not an automorphism. Hence there is a difference between σ-linear isomorphisms and bijective σ-linear maps!

Definition 2.3.22. — Let $\mathscr{M}$ be an $\mathscr{O}_S$-module.

(i) A *descending filtration* on $\mathscr{M}$ is a family $(C^i)_{i\in\mathbf{Z}}$ of $\mathscr{O}_S$-submodules of $\mathscr{M}$, which are locally direct summands and
   - $C^i \supset C^{i+1}$ for all $i \in \mathbf{Z}$;
   - $\bigcup_{i\in\mathbf{Z}} C^i = \mathscr{M}$;
   - $\bigcap_{i\in\mathbf{Z}} C^i = 0$.

(ii) An *ascending filtration* on $\mathscr{M}$ is a family $(D_i)_{i\in\mathbf{Z}}$ of $\mathscr{O}_S$-submodules of $\mathscr{M}$, which are locally direct summands and
   - $D_i \subset D_{i+1}$ for all $i \in \mathbf{Z}$;
   - $\bigcup_{i\in\mathbf{Z}} D_i = \mathscr{M}$;
   - $\bigcap_{i\in\mathbf{Z}} D_i = 0$.

Definition 2.3.23. — Let S be a scheme over $\mathbf{F}_p$. An *F-zip* over S is a quadrupel

$$\mathcal{M} = (\mathscr{M}, C^\bullet, D_\bullet, \varphi_\bullet),$$

where

- $\mathscr{M}$ is a locally free $\mathscr{O}_S$-module of finite rank;
- $C^\bullet = (C^i)_{i\in\mathbf{Z}}$ is a descending filtration on $\mathscr{M}^{(p)}$;
- $D_\bullet = (D_i)_{i\in\mathbf{Z}}$ is an ascending filtration on $\mathscr{M}$;
- $\varphi_\bullet = (\varphi_i)_{i\in\mathbf{Z}}$ is a family of $\mathscr{O}_S$-linear isomorphisms

$$\varphi_i\colon C^i/C^{i+1} \longrightarrow D_i/D_{i-1}.$$

Remark 2.3.24. — Our definition of F-zip differs from the definition of Moonen and Wedhorn [MW04]. We use the definition given by Wedhorn in [Wed08]. By lemma 1.2.15, the two definitions are equivalent, if S is the spectrum of a perfect ring. ◁

Fix a scheme S over $\mathbf{F}_p$ and let $\mathcal{A}$ be the category of quasi-coherent $\mathscr{O}_S$-modules. This is an abelian category and hence $\mathbf{FG}(\mathcal{A})$ is also abelian.

***F*-zips and *F*-gauges.** — To any F-zip $\mathcal{M} = (\mathscr{M}, C^\bullet, D_\bullet, \varphi_\bullet)$ over $\mathscr{O}_S$ we will associate an F-gauge by the following construction: First we define $\mathscr{O}_S$-modules $\mathrm{gr}^i_C := C^i/C^{i+1}$ and $\mathrm{gr}^D_i := D_i/D_{i-1}$. Moreover, we let $\mathrm{gr}^D := \bigoplus_{i\in\mathbf{Z}} \mathrm{gr}^D_i$. With this notation, the maps φ_i are just the linear isomorphisms $\mathrm{gr}^i_C \to \mathrm{gr}^D_i$. Using the canonical projections $\mathrm{pr}_{C^i}\colon C^i \to \mathrm{gr}^i_C$ and $\mathrm{pr}_{D_i}\colon D_i \to \mathrm{gr}^D_i$, we set

$$M^r := C^r \times_{\mathrm{gr}^D_r} D_r.$$

By this we mean the fibre product in the category of $\mathscr{O}_S$-modules, i.e. the following diagram is a cartesian square:

$$\begin{tikzcd} C^r \times_{\mathrm{gr}^D_r} D_r \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & D_r \arrow[d, "\mathrm{pr}_{D_r}"] \\ C^r \arrow[r, "\varphi_r\circ\mathrm{pr}_{C^r}"] & \mathrm{gr}^D_r \end{tikzcd}$$

The $\mathscr{O}_S$-module M^r may be identified with

$$M^r \cong \ker\Big(C^r \oplus D_r \longrightarrow \mathrm{gr}^D_r,\, (c,d) \longmapsto \varphi_r\big(\mathrm{pr}_{C^r}(c)\big) - \mathrm{pr}_{D_r}(d)\Big).$$

To get an F-gauge we must define maps f and v, which satisfy the relation $fv = vf = 0$. For $r \in \mathbf{Z}$ there is a $\mathscr{O}_S$-linear map

$$C^r \oplus D_r \longrightarrow C^{r+1} \oplus D_{r+1}, \qquad (c,d) \longmapsto (0,d)$$

given by the inclusion $D_r \subset D_{r+1}$. The restriction of this map to M^r has obviously image in M^{r+1} and we let f_r be this map. Similarly, there is an $\mathscr{O}_S$-linear map

$$C^{r+1} \oplus D_{r+1} \longrightarrow C^r \oplus D_r, \qquad (c,d) \longmapsto (c,0)$$

given by the inclusion $C^{r+1} \subset C^r$. The restriction of this map to M^{r+1} obviously has image in M^r and we let v_{r+1} be this map. It is clear that the relation $fv = vf = 0$ holds. Hence we have associated an F-gauge to an F-zip.

We are going to show that the F-gauge associated to an F-zip is rigid. First, the map

$$M^r \longrightarrow M^{r+1} \oplus M^{r-1}$$

is given by $(c,d) \mapsto \big((0,d),(c,0)\big)$ which is obviously injective. It follows that the map (f_r^∞, v_r^∞) is also injective and hence the associated F-gauge is strict. Second, we show $\ker(v_{r+1}) = \operatorname{im}(f_r)$. The inclusion $\operatorname{im}(f_r) \subset \ker(v_{r+1})$ is clear from the relation $vf = 0$. Let $m \in M^r$ be such that $v_{r+1}(m) = 0$. Writing $m = (c,d)$ with $c \in C^{r+1}$ and $d \in D_{r+1}$, we must have $c = 0$ and hence $m = (0,d)$. But M^{r+1} may be identified with the kernel of the map $C^{r+1} \oplus D_{r+1} \to \mathrm{gr}^D_{r+1}$ which in our case means that it actually holds $d \in D_r$. Setting $n := (0,d) \in M^r$ we find $f_r(n) = m$. The equality $\ker(f_r) = \operatorname{im}(v_{r+1})$ is shown in a similar fashion. Thus, the associated F-gauge is also quasi-rigid and in total it is rigid. As a last step we show that there is also a σ-linear isomorphism $M^{+\infty} \to M^{-\infty}$. Therefor, we compute both $\mathscr{O}_S$-modules. We have

$$\begin{aligned} M^{+\infty} &= \varinjlim_{f_r} M^r \\ &\cong \varinjlim_{f_r} \ker(C^r \oplus D_r \to \mathrm{gr}^D_r) \\ &\cong \bigcup_{r\in\mathbf{Z}} D_r \\ &= \mathscr{M}. \end{aligned}$$

Here we used that f_r annihilates C^r and that $D_r = D_{r+1}$ for $r \ll 0$. Analogously, we find

$$\begin{aligned} M^{-\infty} &= \varinjlim_{v_r} M^r \\ &\cong \varinjlim \ker(C^r \oplus D_r \to \mathrm{gr}^D_r) \\ &\cong \bigcup_{r\in\mathbf{Z}} C^r \\ &= \mathscr{M}^{(p)}. \end{aligned}$$

We define a σ-linear map $\varphi\colon M^{+\infty} \to M^{-\infty}$ by using the above $\mathscr{O}_S$-linear isomorphism and the natural map

$$\mathscr{M} \longrightarrow \mathscr{M}^{(p)} = \mathscr{M} \otimes_\sigma \mathscr{O}_S.$$

This is apparently a σ-linear isomorphism.
Next, we construct a quasi-inverse functor from the category of those rigid φ-F-gauges over $\mathscr{O}_S$, which are locally free, to the category of F-zips. Let $(M^r)_{r\in\mathbf{Z}}$ be a rigid φ-F-gauge such that all M^r are locally free $\mathscr{O}_S$-modules. The associated F-zip is obtained in the following manner:

$$\begin{aligned} \mathscr{M} &:= M^{+\infty} \\ C^i &:= \operatorname{im}\big((\varphi^\sharp)^{-1} \circ v_i^\infty\big) \subset \mathscr{M}^{(p)} \\ D_i &:= \operatorname{im}\big(f_i^\infty\big) \subset \mathscr{M} \end{aligned}$$

In order to construct the isomorphisms $\varphi_i\colon \mathrm{gr}^i_C \to \mathrm{gr}^D_i$, some work is needed. We claim that for each $r \in \mathbf{Z}$ there is an exact sequence

$$M^{r-1} \oplus M^{r+1} \xrightarrow{(f_{r-1}, v_{r+1})} M^r \xrightarrow{\mathrm{pr}_{D_r} \circ f_r^\infty} \mathrm{gr}^D_r \longrightarrow 0$$

of $\mathscr{O}_S$-modules. Clearly, the second map is surjective. Let $m \in M^{r-1}$ and $n \in M^{r+1}$. Then it holds

$$\begin{aligned} f_r^\infty\big(f_{r-1}(m) + v_{r+1}(n)\big) &= f_{r-1}^\infty(m) + f_r^\infty\big(v_{r+1}(n)\big) \\ &= f_{r-1}^\infty(m) \end{aligned}$$

again because of the relation $fv = 0$. Moreover, we have $f_{r-1}^\infty(m) \in D_{r-1} \subset D_r$ by definition of D_{r-1}, hence $\mathrm{pr}_{D_r}\big(f_{r-1}^\infty(m)\big) = 0$. Now let $m \in M^r$ with $\mathrm{pr}_{D_r}\big(f_r^\infty(m)\big) = 0$. Since $\ker(\mathrm{pr}_{D_r}) = D_{r-1}$, this implies $f_r^\infty(m) = f_{r-1}^\infty(n)$ for some $n \in M^{r-1}$. We find $f_r^\infty\big(m - f_{r-1}(m)\big) = 0$, which means $m - f_{r-1}(n) \in \ker(f_r^\infty)$. But by rigidity we have $\ker(f_r^\infty) = \ker(f_r) = \mathrm{im}(v_{r+1})$. This yields

$$m \in \mathrm{im}(f_{r-1}) + \mathrm{im}(v_{r+1}).$$

A similar argument shows that there is for each $r \in \mathbf{Z}$ an exact sequence

$$M^{r-1} \oplus M^{r+1} \xrightarrow{(f_{r-1}, v_{r+1})} M^r \xrightarrow{\mathrm{pr}_{C^r} \circ (\varphi^\sharp)^{-1} \circ v_r^\infty} \mathrm{gr}_C^r \longrightarrow 0.$$

From these two exact sequences we obtain a commutative diagram

$$\begin{tikzcd} M^{r-1} \oplus M^{r+1} \arrow[r] \arrow[d, equal] & M^r \arrow[r] \arrow[d, equal] & \mathrm{gr}_C^r \arrow[r] \arrow[d, dashed, "\varphi_r"] & 0 \\ M^{r-1} \oplus M^{r+1} \arrow[r] & M^r \arrow[r] & \mathrm{gr}_r^D \arrow[r] & 0 \end{tikzcd}$$

which defines the $\mathscr{O}_S$-linear isomorphism $\varphi_i \colon \mathrm{gr}_C^i \to \mathrm{gr}_i^D$. The connection between F-gauges and F-zips is summarized in the next proposition.

Proposition 2.3.25. — *Let S be a scheme over $\mathbf{F}_p$. The above construction establishes an equivalence of categories between the category of F-zips over $\mathscr{O}_S$ and the category of rigid φ-F-gauges over $\mathscr{O}_S$, which are locally free.*

Proof. — This is straightforward (see [Sch09]). ∎

***F*-zips over perfect fields**. — Let us consider the special case, where $S = \mathrm{Spec}(k)$ for a perfect field k of characteristic $p > 0$. To any F-crystal over k we have constructed a φ-F-gauge over $W := W(k)$. We will now see that there is a commutatice square

$$\begin{tikzcd} F\text{-crystals} \arrow[r, "\mathfrak{F}_W"] \arrow[d, "\mathfrak{Z}"'] & \mathbf{FG}^{\varphi,\sharp}(W) \arrow[d, "\mathrm{mod}\ p"] \\ F\text{-zips} \arrow[r, "\mathfrak{F}\mathfrak{g}"] & \mathbf{FG}^{\varphi,\sharp}(k) \end{tikzcd}$$

We already know three of the four functors. The functor $\mathfrak{Z}$ is constructed in the following way: Let (M, ϕ) be an F-crystal over k. Thus, M is a free W-module of finite rank and $\phi \colon M \to M \otimes_W B$ is a σ-linear injective map, where B is the quotient field of W. In order to associate an F-zip to (M, ϕ), we proceed in two steps: First, we set

$$\begin{aligned} \widetilde{C}^i &:= \{m \in M^{(p)} \mid \phi^\sharp(m) \in p^i M\} \\ \widetilde{\varphi}_i &:= p^{-i}\phi^\sharp|_{\widetilde{C}^i} \colon \widetilde{C}^i \to M \\ \widetilde{D}_i &:= \mathrm{im}\big(\widetilde{\varphi}_i\big). \end{aligned}$$

Second, we define

$$\begin{aligned}
\overline{M} &:= M/pM \\
C^i &:= \operatorname{im}\big(\widetilde{C}^i \to M^{(p)}/pM^{(p)}\big) \subset \overline{M}^{(p)} \\
D_i &:= \operatorname{im}\big(\widetilde{D}_i \to M/pM\big) \subset \overline{M}
\end{aligned}$$

To define the k-linear isomorphism φ_i we use the theory of elementary divisors (see [Lan02, III Theorem 7.8 and 7.9]). Since W is a discrete valution ring, we can apply the theory of elementary divisors and conclude that we can choose a basis $e_1, \ldots, e_n$ of M such that the W-linear injective map $\phi^\sharp \colon M^{(p)} \to M \otimes_W B$ is given with respect to the basis $e_1^{(p)}, \ldots, e_n^{(p)}$ of $M^{(p)}$ and $e_1, \ldots, e_n$ of M by a matrix of the form

$$\begin{pmatrix} p^{\mu_1} & 0 & \cdots & 0 \\ 0 & p^{\mu_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & p^{\mu_n} \end{pmatrix}$$

with $\mu_j \in \mathbf{Z}$ and $\mu_1 \leq \cdots \leq \mu_n$. In terms of this representation, we can quite explicitely describe the submodules $\widetilde{C}^i$ of $M^{(p)}$ and $\widetilde{D}_i$ of M. The W-module $\widetilde{C}^i$ has basis

$$\begin{cases} e_1^{(p)}, \ldots, e_n^{(p)}, & \text{if } i \leq \mu_1 \\ p^{i-\mu_1} e_1^{(p)}, \ldots, p^{i-\mu_j} e_j^{(p)}, e_{j+1}^{(p)}, \ldots, e_n^{(p)}, & \text{if } \mu_j < i \leq \mu_{j+1} \\ p^{i-\mu_1} e_1^{(p)}, \ldots, p^{i-\mu_n} e_n^{(p)}, & \text{if } i > \mu_n \end{cases}$$

If we denote the k-basis of $\overline{M}^{(p)}$ by $\overline{e}_1^{(p)}, \ldots, \overline{e}_n^{(p)}$, then C^i has basis

$$\begin{cases} \overline{e}_1^{(p)}, \ldots, \overline{e}_n^{(p)}, & \text{if } i \leq \mu_1 \\ \overline{e}_{j+1}^{(p)}, \ldots, \overline{e}_n^{(p)}, & \text{if } \mu_j < i \leq \mu_{j+1} \\ \varnothing, & \text{if } i > \mu_n \end{cases}$$

The k-vector space D_i has basis

$$\begin{cases} \varnothing, & \text{if } i < \mu_1 \\ \overline{e}_1, \ldots, \overline{e}_j, & \text{if } \mu_j \leq i < \mu_{j+1} \\ \overline{e}_1, \ldots, \overline{e}_n, & \text{if } i \geq \mu_n \end{cases}$$

From this description it is now obvious that $\varphi_i \colon C^i/C^{i+1} \to D_i/D_{i-1}$ is just given by mapping $\overline{e}_l^{(p)}$ to $\overline{e}_l$, if $\overline{e}_l^{(p)}$ is a basis vector of $\overline{M}^{(p)}$. This completes the construction of $\mathfrak{Z}$.

Example 2.3.26. — Set $M := W \oplus W$ with basis $\{e_1, e_2\}$ and define $\phi \colon M \to M \otimes_W B$ by

$$\begin{aligned} e_1 &\longmapsto p^{-1} e_1 \\ e_2 &\longmapsto p e_2 \end{aligned}$$

Let $e_j^{(p)} := e_j \otimes 1 \in M^{(p)} = M \otimes_\sigma W$. We compute

$$\begin{aligned}
\widetilde{C}^{-1} &= M^{(p)} \\
\widetilde{C}^{0} &= pW^{(p)} \oplus W^{(p)} \\
\widetilde{C}^{1} &= p^2W^{(p)} \oplus W^{(p)} \\
\widetilde{C}^{2} &= p^3W^{(p)} \oplus pW^{(p)}
\end{aligned}$$

and

$$\begin{aligned}
\widetilde{D}_{-2} &= pW \oplus p^3W \\
\widetilde{D}_{-1} &= W \oplus p^2W \\
\widetilde{D}_{0} &= W \oplus pW \\
\widetilde{D}_{1} &= M
\end{aligned}$$

This yields the following filtrations

$$\begin{aligned}
C^{-1} &= \overline{M}^{(p)} = k^{(p)} \oplus k^{(p)} \\
C^{0} &= 0 \oplus k^{(p)} \\
C^{1} &= 0 \oplus k^{(p)} \\
C^{2} &= 0
\end{aligned}$$

and

$$\begin{aligned}
D_{-2} &= 0 \\
D_{-1} &= k \oplus 0 \\
D_{0} &= k \oplus 0 \\
D_{1} &= \overline{M}
\end{aligned}$$

Denoting $\overline{e}_j^{(p)}$ and $\overline{e}_j$ the basis vectors of $\overline{M}^{(p)}$ and $\overline{M}$ respectively, the k-linear ismorphisms φ_i are given by

$$\varphi_{-1}\colon \overline{e}_1^{(p)} \longmapsto \overline{e_1}$$

$$\varphi_{1}\colon \overline{e}_2^{(p)} \longmapsto \overline{e_2}$$

and zero otherwise. ◂

Lemma 2.3.27. — *Let $\mathcal{M} = (\overline{M}, C^\bullet, D_\bullet, \varphi_\bullet)$ be an F-zip over k. Then there exists an F-crystal (M, ϕ) over k such that $\mathfrak{Z}(M, \phi) \cong \mathcal{M}$.*

Proof. — Let the support of the type of $\mathcal{M}$ be $\{d_1 < \cdots < d_s\}$. For $j = 1, \dots, s$ we set $n_j := \tau(d_j)$. Choose a basis $\overline{e}_1^s, \dots, \overline{e}_{n_s}^s$ of $C^{d_s} = C^{d_s}/C^{d_s+1}$. Since we have the ascending chain

$$C^{d_s} \subset C^{d_{s-1}} \subset C^{d_{s-2}} \subset \cdots \subset C^{d_2} \subset C^{d_1} = \overline{M}^{(p)},$$

we can extend this basis to a basis $\overline{e}_1^{s-1}, \dots, \overline{e}_{n_{s-1}}^{s-1}, \overline{e}_1^s, \dots, \overline{e}_{n_s}^s$ of $C^{d_{s-1}}$. Repeating this process, we get finally a basis $\overline{e}_1^1, \dots, \overline{e}_{n_1}^1, \dots, \overline{e}_1^s, \dots, \overline{e}_{n_s}^s$ of $\overline{M}^{(p)}$.
Next we observe that it follows right from the definition

$$D_{d_j} \simeq D_{d_j}/D_{d_j-1} \oplus D_{d_j-1}.$$

The images of the basis $\overline{e}_1^s, \dots, \overline{e}_{n_s}^s$ under the isomorphism φ_{d_s} are linearly independent and can thus be considered as part of a basis of D_{d_j} by the above identification. We denote this part of a basis of D_{d_s} by $\overline{f}_1^s, \dots, \overline{f}_{n_s}^s$. Since $D_{d_s} \subset D_{d_{s-1}-1} \subset D_{d_{s-1}}$, we obtain in a similar way a part $\overline{f}_1^{s-1}, \dots, \overline{f}_{n_{s-1}}^{s-1}$ of a basis of $D_{d_{s-1}}$ and $\overline{f}_1^{s-1}, \dots, \overline{f}_{n_{s-1}}^{s-1}, \overline{f}_1^s, \dots, \overline{f}_{n_s}^s$ are linearly independent. Proceeding in that way, we obtain a second basis $\overline{f}_1^1, \dots, \overline{f}_{n_1}^1, \dots, \overline{f}_1^s, \dots, \overline{f}_{n_s}^s$ of $\overline{M}$.
Let $M := \bigoplus_{i=1}^n W$ be a free W-module of rank $n = \sum_{j=1}^s n_j$. We can lift the k-basis $\overline{f}_1^1, \dots, \overline{f}_{n_s}^s$ to a W-basis $f_1^1, \dots, f_{n_1}^1, \dots, f_1^s, \dots, f_{n_s}^s$ of M. Similarly, we can lift the k-basis $\overline{e}_1^1, \overline{e}_{n_s}^s$ of $\overline{M}^{(p)}$ to a W-basis $e_1^1, \dots, e_{n_1}^1, \dots, e_1^s, \dots, e_{n_s}^s$ of $M^{(p)}$.
At last, we have to define a σ-linear injective map $\phi\colon M \to M \otimes_W B$. This is achieved by the rule

$$e_{i_j}^j \mapsto p^{d_i} f_{i_j}^j$$

for $j = 1, \dots, s$ and $i_j = 1, \dots, n_j$. By construction it is clear that this F-crystal induces an F-zip isomorphic to the given one. ∎

§4 Displays

This section is based on the article [LZ07] by Langer and Zink. We proof some simple facts, which were omitted in this paper.

The Category of Predisplays. — Let R be a ring of characteristic $p > 0$. We denote by $W(R)$ the ring of Witt vectors of R and σ denotes the Frobenius on R and on $W(R)$. Let $I := V(W(R))$, then we have $pW(k) \subseteq I$, but in general this is not an equality since the Frobenius-endomorphism need not to be surjective. If $\phi\colon M \to N$ is a σ-linear homomorphism of $W(R)$-modules, we define a σ-linear homomorphism $\widetilde{\phi}$ by

$$\begin{aligned} \widetilde{\phi}\colon I \otimes_{W(R)} M &\longrightarrow N \\ V(\xi) \otimes m &\longmapsto \xi\phi(m), \end{aligned} \tag{2.4.1}$$

where $V\colon W(R) \to W(R)$ denotes the Verschiebung, which is an injective homomorphism of additive groups. With these preliminaries we can define the notion of a predisplay.

Definition 2.4.28. — A *predisplay over R* consists of the following data:

(i) A chain of morphisms of $W(R)$-modules

$$\cdots \longrightarrow P_{i+1} \xrightarrow{\eta_i} P_i \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\eta_0} P_0.$$

(ii) For each $i \geq 0$ a $W(R)$-linear map

$$\alpha_i : I \otimes_{W(R)} P_i \to P_{i+1}.$$

(iii) For each $i \geq 0$ a σ-linear map

$$\theta_i : P_i \to P_0.$$

These data are subjected to the following axioms:

(D1) For each $i \geq 1$ the following diagram is commutative and its diagonal is the multiplication.

$$\begin{tikzcd}
I \otimes P_i \arrow[r, "\alpha_i"] \arrow[d, "\mathrm{id}_I \otimes \eta_{i-1}"'] & P_{i+1} \arrow[d, "\eta_i"] \\
I \otimes P_{i-1} \arrow[r, "\alpha_{i-1}"] & P_i
\end{tikzcd}$$

For $i = 0$ the following map is the multiplication:

$$I \otimes P_0 \xrightarrow{\alpha_0} P_1 \xrightarrow{\eta_0} P_0$$

(D2) For each $i \geq 0$

$$\theta_{i+1}\alpha_i = \widetilde{\theta}_i : I \otimes P_i \longrightarrow P_0,$$

where $\widetilde{\theta}_i$ is defined by (2.4.1).

We denote a predisplay over $W(R)$ by $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i \in \mathbf{N}}$.

Definition 2.4.29. — Let $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i \in \mathbf{N}}$ and $\mathcal{Q} = (Q_i, \rho_i, \beta_i, \tau_i)_{i \in \mathbf{N}}$ be two predisplays. A *morphism*

$$X : \mathcal{P} \longrightarrow \mathcal{Q}$$

of predisplays is a family of morphism of $W(R)$-modules $\chi_i : P_i \to Q_i$, such that for all $i \in \mathbf{N}$ each diagram

(i)

$$\begin{tikzcd}
P_{i+1} \arrow[r, "\eta_i"] \arrow[d, "\chi_{i+1}"'] & P_i \arrow[d, "\chi_i"] \\
Q_{i+1} \arrow[r, "\rho_i"] & Q_i
\end{tikzcd}$$

(ii)

$$\begin{tikzcd}
I \otimes P_i \arrow[r, "\alpha_i"] \arrow[d, "\mathrm{id}_I \otimes \chi_i"'] & P_{i+1} \arrow[d, "\chi_{i+1}"] \\
I \otimes Q_i \arrow[r, "\beta_i"] & Q_{i+1}
\end{tikzcd}$$

(iii)

$$\begin{tikzcd} P_i \arrow[r, "\theta_i"] \arrow[d, "\chi_i"'] & P_0 \arrow[d, "\chi_0"] \\ Q_i \arrow[r, "\tau_i"] & Q_0 \end{tikzcd}$$

commutes.

With these definitions we get a category $(\mathbf{Pdis}/R)$ of predisplays over R. A predisplay $\mathcal{Q}$ is called a *subpredisplay* of a predisplay $\mathcal{P}$, if for all $i \in \mathbf{N}$ the $W(R)$-module Q_i is a submodule of the module P_i and the maps ρ_i, β_i and τ_i are the restrictions of η_i, α_i and θ_i, respectively, to Q_i.
Our next task is to show that $(\mathbf{Pdis}/R)$ is an abelian category. Let $\mathcal{P}$ and $\mathcal{Q}$ be two predisplays over R. We define the direct sum

$$\mathcal{P} \oplus \mathcal{Q} = (P_i \oplus Q_i, \eta_i \oplus \rho_i, \alpha_i \oplus \beta_i, \theta_i \oplus \tau_i)_{i \in \mathbf{N}}.$$

It is clear from the definition of the direct sum that $\mathcal{P} \oplus \mathcal{Q}$ is also a predisplay over R.
Now, we define kernels and cokernels. Let

$$\Xi : \mathcal{P} \longrightarrow \mathcal{Q}$$

be a morphism of predisplays. We consider the following diagram

$$\begin{tikzcd} & 0 \arrow[d] & 0 \arrow[d] & & 0 \arrow[d] & 0 \arrow[d] \\ \cdots \arrow[r, dashed] & \ker \chi_{i+1} \arrow[r, dashed, "\mu_i"] \arrow[d] & \ker \chi_i \arrow[r, dashed] \arrow[d] & \cdots \arrow[r, dashed] & \ker \chi_1 \arrow[r, dashed, "\mu_0"] \arrow[d] & \ker \chi_0 \arrow[d] \\ \cdots \arrow[r] & P_{i+1} \arrow[r, "\eta_i"] \arrow[d, "\chi_{i+1}"'] & P_i \arrow[r] \arrow[d, "\chi_i"'] & \cdots \arrow[r] & P_1 \arrow[r, "\eta_0"] \arrow[d, "\chi_1"'] & P_0 \arrow[d, "\chi_0"'] \\ \cdots \arrow[r] & Q_{i+1} \arrow[r, "\rho_i"] & Q_i \arrow[r] & \cdots \arrow[r] & Q_1 \arrow[r, "\rho_0"] & Q_0 \end{tikzcd}$$

The maps $\mu_i : \ker \chi_{i+1} \to \ker \chi_i$ are given by restricting η_i to $\ker \chi_{i+1}$. In this way, we get a predisplay

$$\ker \Xi = (\ker \chi_i, \mu_i, \gamma_i, \sigma_i)_{i \in \mathbf{N}}$$

where γ_i and σ_i are the restrictions of α_i and θ_i, respectively. That $\ker \Xi$ fulfills the axioms (D1) and (D2) is obvious from the definition of the maps μ_i, γ_i and σ_i.
Cokernels are defined in a similar way.
Summing up, we get the following proposition.

Proposition 2.4.30. — *The category* $(\mathbf{Pdis}/R)$ *of predisplays over R is abelian.*

Properties of Predisplays. — Let $\mathcal{P}$ be a predisplay. Then we have a commutative diagram

$$\begin{tikzcd} P_{i+1} \arrow[r, "\theta_{i+1}"] \arrow[d, "\eta_i"'] & P_0 \arrow[d, "p"] \\ P_i \arrow[r, "\theta_i"] & P_0 \end{tikzcd} \tag{2.4.2}$$

where the righthand arrow is multiplication by p. Indeed, let $x \in P_{i+1}$ and consider the commutative diagram obtained from (D1)

$$\begin{tikzcd} I \otimes P_{i+1} \arrow[r, "\alpha_{i+1}"] \arrow[d, "\mathrm{id}_I \otimes \eta_i"'] & P_{i+2} \arrow[d, "\eta_{i+1}"] \\ I \otimes P_i \arrow[r, "\alpha_i"] & P_{i+1} \end{tikzcd}$$

Since the diagonal is multiplication, we have

$$\alpha_i(V(1) \otimes \eta_i(x)) = (V(1))x.$$

Now applying θ_{i+1} to this equation and using (D2) yields

$$\theta_i(\eta_i(x)) = p\theta_{i+1}(x).$$

The commutative diagram (2.4.2) induces a unique map from P_{i+1} to the fibre product

$$\begin{tikzcd} P_{i+1} \arrow[dr, dashed, "\delta_i"] \arrow[drr, bend left, "\theta_{i+1}"] \arrow[ddr, bend right, "\eta_i"'] & & \\ & P_i \times_{P_0} P_0 \arrow[r] \arrow[d] & P_0 \arrow[d, "p"] \\ & P_i \arrow[r, "\theta_i"] & P_0 \end{tikzcd}$$

Definition 2.4.31. — A predisplay $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i \in \mathbf{N}}$ is called *separated*, if the maps $\delta_i \colon P_{i+1} \to P_i \times_{P_0} P_0$ are injective for all $i \in \mathbf{N}$.

Proposition 2.4.32. — *Let $\mathcal{P}$ be a predisplay. Then there exists a separated predisplay $\mathcal{P}^{\mathrm{sep}}$ and a canonical surjection $\mathcal{P} \to \mathcal{P}^{\mathrm{sep}}$.*

Proof. — We set $P_0^{\mathrm{sep}} := P_0$ and $\theta_0^{\mathrm{sep}} := \theta_0$. For $i \geq 0$ we define P_{i+1}^{sep} as the image of P_{i+1} under the map to the fibre product

$$\begin{tikzcd} P_{i+1} \arrow[dr, dashed] \arrow[drr, bend left, "\theta_{i+1}"] \arrow[ddr, bend right] & & \\ & P_i^{\mathrm{sep}} \times_{P_0} P_0 \arrow[r] \arrow[d] & P_0 \arrow[d, "p"] \\ & P_i^{\mathrm{sep}} \arrow[r, "\theta_i^{\mathrm{sep}}"] & P_0 \end{tikzcd}$$

where

$$P_{i+1} \xrightarrow{\eta_i} P_i \longrightarrow P_i^{\mathrm{sep}}$$

is the lefthand map. The map η_i^{sep} is given by the commative diagram

$$\begin{tikzcd} P_{i+1} \arrow[r] \arrow[d, "\eta_i"'] & P_{i+1}^{\mathrm{sep}} \arrow[d, dashed, "\eta_i^{\mathrm{sep}}"] \\ P_i \arrow[r] & P_i^{\mathrm{sep}} \end{tikzcd}$$

and the map α_i^{sep} is defined by the commutative diagram

$$\begin{tikzcd} I \otimes P_i \arrow[r, "\alpha_i"] \arrow[d] & P_{i+1} \arrow[d] \\ I \otimes P_i^{\mathrm{sep}} \arrow[r, dashed, "\alpha_i^{\mathrm{sep}}"] & P_{i+1}^{\mathrm{sep}} \end{tikzcd}$$

To show that $\mathcal{P}^{\mathrm{sep}}$ satisfies axiom (D1), we consider the diagram

$$\begin{tikzcd} I \otimes P_i \arrow[rrr, "\alpha_i"] \arrow[ddd, "\mathrm{id}_I \otimes \eta_{i-1}"'] \arrow[dr] & & & P_{i+1} \arrow[ddd, "\eta_i"] \arrow[dl] \\ & I \otimes P_i^{\mathrm{sep}} \arrow[r, "\alpha_i^{\mathrm{sep}}"] \arrow[d, "\mathrm{id}_I \otimes \eta_{i-1}^{\mathrm{sep}}"'] & P_{i+1}^{\mathrm{sep}} \arrow[d, "\eta_i^{\mathrm{sep}}"] & \\ & I \otimes P_{i-1}^{\mathrm{sep}} \arrow[r, "\alpha_{i-1}^{\mathrm{sep}}"] & P_i^{\mathrm{sep}} & \\ I \otimes P_{i-1} \arrow[rrr, "\alpha_{i-1}"] \arrow[ur] & & & P_i \arrow[ul] \end{tikzcd}$$

From the definitions of the maps α_i^{sep} and η_i^{sep} it follows that this diagram is commutative. Hence, axiom (D1) is satisfied. Axiom (D2) is even easier to prove. That $\mathcal{P}^{\mathrm{sep}}$ is really separated and that the map $\mathcal{P} \to \mathcal{P}^{\mathrm{sep}}$ is surjective is an immediate consequence of the construction of $\mathcal{P}^{\mathrm{sep}}$. ■

***Remark* 2.4.33**. — The functor $\mathcal{P} \mapsto \mathcal{P}^{\mathrm{sep}}$ is left adjoint to the forgetful functor, but it is not exact.◁

Recall that the Verschiebung $V\colon W(R) \to W(R)$ is injective.

Definition 2.4.34. — Let $n \in \mathbf{N}$. The map

$$\begin{aligned} v^{(n)}\colon \qquad I^{\otimes n} &\longrightarrow I \\ V(\xi_1) \otimes \cdots \otimes V(\xi_n) &\longmapsto V(\xi_1 \cdots \xi_n) \end{aligned}$$

is called *Verjüngung*.

For a predisplay $\mathcal{P}$ we form the iteration of the maps α_i by picking up the last factor of $I^{\otimes}$:

$$\gamma_i^{(n)} \colon I^{\otimes n} \otimes P_i \xrightarrow{\alpha_i} I^{\otimes n-1} \otimes P_{i+1} \xrightarrow{\alpha_{i+1}} \cdots \xrightarrow{\alpha_{i+n-1}} P_{i+n} \tag{2.4.3}$$

Proposition 2.4.35. — *For a separated predisplay $\mathcal{P}$ the iteration (2.4.3) factors uniquely through the Verjüngung $v^{(n)}$. To be more precise, there is for any $i, n \in \mathbf{N}$ a unique map $\alpha_i^{(n)}$ such that the following diagram is commutative:*

$$\begin{tikzcd}
I^{\otimes n} \otimes P_i \arrow[r, "\gamma_i^{(n)}"] \arrow[d, "v^{(n)} \otimes \mathrm{id}_{P_i}"'] & P_{i+n} \\
I \otimes P_i \arrow[ur, "\alpha_i^{(n)}"'] &
\end{tikzcd}$$

Proof. — For $n = 1$ the map $\alpha_i^{(1)}$ must be α_i. For arbitrary n, we define the map $\alpha_i^{(n)}$ by

$$(V(\xi) \otimes x) \mapsto \gamma_i^{(n)}\big(\underbrace{V(1) \otimes \cdots \otimes V(1)}_{n-1 \text{ times}} \otimes V(\xi) \otimes x\big)$$

Assume we have proved the uniqueness of $\alpha_i^{(n)}$. Then consider the diagram

$$\begin{tikzcd}
I \otimes P_i \arrow[dr, "\alpha_i^{(n+1)}"] \arrow[drrr, bend left, "\widetilde{\theta}_i"] \arrow[ddrr, bend right, "V(1)\cdot\alpha_i^{(n)}"'] & & & \\
& P_{i+n+1} \arrow[dr, "\delta_{i+n}"] \arrow[drr, bend left, "\theta_{i+n+1}"] \arrow[dr, bend right, "\eta_{i+n}"'] & & \\
& & P_{i+n} \times_{P_0} P_0 \arrow[r] \arrow[d] & P_0 \arrow[d, "p"] \\
& & P_{i+n} \arrow[r, "\theta_{i+n}"] & P_0
\end{tikzcd}$$

It is easy to see that this diagram is commutative. Thus the map $\delta_{i+n} \circ \alpha_i^{(n+1)}$ is unique by the universal property of the fibre product. But the predisplay is separated, so δ_{i+n} is injective. It follows that $\alpha_i^{(n+1)}$ is also unique with respect to the imposed properties. ∎

Remark 2.4.36. — The last proposition shows that forming the iteration $\gamma_i^{(n)}$ is independent of the factor I of $I^{\otimes m}$ we choose. ◁

For a separated predisplay we have the following lemma.

Lemma 2.4.37. — *Let $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i \in \mathbf{N}}$ be a separated predisplay. Then the maps α_i are uniquely determined by the other data.*

Proof. — We have a commutative diagram

$$\begin{tikzcd}
I \otimes P_i \arrow[dr, "\alpha_i"] \arrow[drrr, bend left, "\widetilde{\theta}_i"] \arrow[ddrr, bend right] & & & \\
& P_{i+1} \arrow[dr, "\delta_i"] \arrow[drr, bend left, "\theta_{i+1}"] \arrow[dr, bend right, "\eta_i"'] \arrow[dd, phantom] & & \\
& & P_i \times_{P_0} P_0 \arrow[r] \arrow[d] & P_0 \arrow[d, "p"] \\
& & P_i \arrow[r, "\theta_i"] & P_0
\end{tikzcd}$$

Since $\mathcal{P}$ is separated, the maps δ_i are injective. By the universal property of the fibre product the uniqueness of α_i follows. ∎

Let $d \in \mathbf{N}$ be an integer. Assume that we are given data

$$P_0, \ldots, P_d, \eta_0, \ldots, \eta_{d-1}, \alpha_0, \ldots, \alpha_{d-1}, \theta_0, \ldots, \theta_d$$

satisfying the axioms for a predisplay. We have a commutative diagram of solid arrows

$$\begin{tikzcd}
I \otimes P_d \arrow[dr, dashed] \arrow[drr, bend left, "\widetilde{\theta}_d"] \arrow[ddr, bend right, "\alpha_{d-1}\circ(\mathrm{id}_I \otimes \eta_{d-1})"'] & & \\
& P_d \times_{P_0} P_0 \arrow[r] \arrow[d] & P_0 \arrow[d, "p"] \\
& P_d \arrow[r, "\theta_d"] & P_0
\end{tikzcd}$$

There is a unique map $\alpha_d \colon I \otimes P_d \to P_d \times_{P_0} P_0$ making the whole diagram commutative. Let P_{d+1} be the image of α_d. Let η_d be the restriction of the first projection and θ_{d+1} be the restriction of the second projection to P_{d+1}. Inductively we get a predisplay associated to these data. In fact, all the axioms are trivially satisfied by construction. This shows that a set of data satisfying the predisplay axioms may be extended in a canonical way to a predisplay.

Definition 2.4.38. — A predisplay is of *degree* d (or a d*-predisplay*), if for all $i \geq d$ the map α_i is surjective and $d \in \mathbf{N}$ is minimal with this property. If no such d exists, the degree is ∞.

Remark 2.4.39. — From Lemma 2.4.37 and the above discussion it follows that a separated predisplay of degree d is uniquely determined by the data

$$P_0, \ldots, P_d, \eta_0, \ldots, \eta_{d-1}, \alpha_0, \ldots, \alpha_{d-1}, \theta_0, \ldots, \theta_d. \qquad \triangleleft$$

We end this subsection by showing that every $W(R)$-module gives rise to a predisplay.

Lemma 2.4.40. — *The category* $(\mathbf{Pdis}/R)$ *of predisplays over* R *contains the category of* $W(R)$*-modules as a full subcategory.*

Proof. — Let M be a $W(R)$-module. We define a predisplay over R by

$$P_i := \begin{cases} M, & \text{for } i = 0, \\ I \otimes M, & \text{for } i > 0. \end{cases}$$

Let $\eta_0\colon I \otimes M \to M$ be multiplication $\xi \otimes x \mapsto \xi x$ and let $\eta_i\colon I \otimes M \to I \otimes M$ be multiplication by p for all $i > 0$. The maps $\alpha_i\colon I \otimes P_i \to P_{i+1}$ are given by

$$\alpha_i := \begin{cases} \mathrm{id}_{I\otimes M}, & \text{for } i = 0, \\ v \otimes \mathrm{id}_M, & \text{for } i > 0, \end{cases}$$

where $v = v^{(2)}$ is the Verjüngung. The σ-linear maps θ_i are all identically zero. This defines a predisplay. If $f\colon M \to N$ is a homomorphism of $W(R)$-modules and $\mathcal{M}$ and $\mathcal{N}$ are the associated predisplays, then we get a morphism $\Xi\colon \mathcal{M} \to \mathcal{N}$ by $\chi_0 := f$ and $\chi_i := \mathrm{id}_I \otimes f$ for all $i > 0$. By construction of the functor from the category of $W(R)$-modules to $(\mathbf{Pdis}/R)$ it is clear that this functor is faithfull. Now, let M and N be two $W(R)$-modules and let $\Xi\colon \mathcal{M} \to \mathcal{N}$ be a morphism of the associated predisplays. Then $f := \chi_0\colon M \to N$ is a homomorphism of $W(R)$-modules. By property (ii) in the definition of a morphism of predisplays we have a commutative diagram

$$\begin{tikzcd} I \otimes M \arrow[r, "\alpha_0"] \arrow[d, "\mathrm{id}_I\otimes\chi_0"'] & I \otimes M \arrow[d, "\chi_1"] \\ I \otimes N \arrow[r, "\beta_0"] & I \otimes N \end{tikzcd}$$

Since $\alpha_0 = \mathrm{id}_{I\otimes M}$ and $\beta_0 = \mathrm{id}_{I\otimes N}$ it follows that $\chi_1 = \mathrm{id}_I \otimes f$. Considering the above commutative diagram for arbitrary $i > 0$

$$\begin{tikzcd} I \otimes I \otimes M \arrow[r, "\alpha_i"] \arrow[d, "\mathrm{id}_I\otimes\chi_i"'] & I \otimes M \arrow[d, "\chi_{i+1}"] \\ I \otimes I \otimes N \arrow[r, "\beta_i"] & I \otimes N \end{tikzcd}$$

and assuming that $\chi_i = \mathrm{id}_I \otimes f$ we find

$$\begin{aligned} \chi_{i+1}(V(\xi) \otimes x) &= \chi_{i+1}(\alpha_i(V(1) \otimes V(\xi) \otimes x)) \\ &= \beta_i(\mathrm{id}_I \otimes \chi_i(V(1) \otimes V(\xi) \otimes x)) \\ &= \beta_i(V(1) \otimes \chi_i(V(\xi) \otimes x)) \\ &= \beta_i(V(1) \otimes V(\xi) \otimes f(x)) \\ &= V(\xi) \otimes f(x). \end{aligned}$$

Thus, we see that $\chi_{i+1} = \mathrm{id}_I \otimes f$. The assertion follows now by induction. ∎

The Category of Displays. — We are mainly interested in predisplays with some additional structure. Such predisplays will be called displays and we are now going to define them.

Definition 2.4.41. — Let $d \in \mathbf{N}$ and let R be a ring of characteristic $p > 0$. A *set of standard data for a display of degree d* is

(i) a sequence $L_0, \dots, L_d$ of finitely generated projective $W(R)$-modules and

(ii) a sequence of σ-linear maps

$$\phi_i\colon L_i \to L_0 \oplus \cdots \oplus L_d,$$

such that the map $\Phi := \bigoplus_{i=0}^d \phi_i$ is a σ-linear automorphism of the $W(R)$-module $L_0 \oplus \cdots \oplus L_d$.

To a set of standard data we associate a predisplay in the following way: For $i \geq 0$ set

$$P_i := (I \otimes L_0) \oplus \cdots \oplus (I \otimes L_{i-1}) \oplus L_i \oplus \cdots \oplus L_d.$$

Note that $P_i = P_{d+1}$ for $i > d$, but this identification is not part of the predisplay structure we are going to define.
We denote by $\mu_i\colon I \otimes L_i \to L_i$ the multiplication. The map $\eta_i\colon P_{i+1} \to P_i$ is given by the following diagram

$$\begin{array}{ccccccccc}
(I \otimes L_0) & \oplus \cdots \oplus & (I \otimes L_{i-1}) & \oplus & (I \otimes L_i) & \oplus & L_{i+1} & \oplus \cdots \oplus & L_d \\
\downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle \mu_i} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} \\
(I \otimes L_0) & \oplus \cdots \oplus & (I \otimes L_{i-1}) & \oplus & L_i & \oplus & L_{i+1} & \oplus \cdots \oplus & L_d
\end{array}$$

The map $\alpha_i\colon I \otimes P_i \to P_{i+1}$ is given by the next diagram

$$\begin{array}{ccccccccccc}
(I \otimes (I \otimes L_0)) & \oplus \cdots \oplus & (I \otimes (I \otimes L_{i-1})) & \oplus & (I \otimes L_i) & \oplus & (I \otimes L_{i+1}) & \oplus \cdots \oplus & (I \otimes L_d) \\
\downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mu_{i+1}} & & \downarrow{\scriptstyle \mu_d} \\
(I \otimes L_0) & \oplus \cdots \oplus & (I \otimes L_{i-1}) & \oplus & (I \otimes L_i) & \oplus & L_{i+1} & \oplus \cdots \oplus & L_d
\end{array}$$

where $\nu = \nu^{(2)}$ is the Verjüngung.
The σ-linear map $\theta_i\colon P_i \to P_0$ is given by

$$\begin{array}{ccccccc}
(I \otimes L_0) & \oplus\cdots\oplus & (I \otimes L_{i-1}) & \oplus & L_i & \oplus & L_{i+1} \oplus\cdots\oplus L_d \\
\searrow{\scriptstyle \widetilde{\phi}_0} & & \searrow{\scriptstyle \widetilde{\phi}_{i-1}} & & \downarrow{\scriptstyle \phi_i} & & \swarrow{\scriptstyle p\phi_{i+1}} \quad \swarrow{\scriptstyle p^{d-i}\phi_d} \\
 & & & & L_0 \oplus \cdots \oplus L_d & &
\end{array}$$

Remark 2.4.42. — If R is a reduced ring, then the maps η_i in the above construction are injective. Indeed, we always have $p = F \circ V$ and V injective as a homomorphism of additive groups. Now, F is injective as an endomorphism of $W(R)$ if and only if the underlying ring R is reduced. It follows that for a reduced ring R the predisplay just constructed is separated. ◃

Actually, the predisplay constructed from standard data is always separated.

Lemma 2.4.43. — *The above construction yields a separated predisplay.*

Proof. — We first prove axiom (D1). The commutativity of the diagram

$$\begin{tikzcd} I \otimes P_i \arrow[r, "\alpha_i"] \arrow[d, "\mathrm{id}_I \otimes \eta_{i-1}"'] & P_{i+1} \arrow[d, "\eta_i"] \\ I \otimes P_{i-1} \arrow[r, "\alpha_{i-1}"] & P_i \end{tikzcd}$$

is readily read off from the definitions of the involved maps. We must show that the diagonal is multiplication. To prove that $\eta_i \circ \alpha_i$ is multiplication, it is enough to prove this for each component of the direct sum. It is clear that this holds for the j-th component for every $j \geq i$. So we just have to prove that pv is multiplication. Let $x \in L_j$, and $\xi_1, \xi_2 \in W(k)$. The map pv is given by

$$\begin{array}{ccccc} I \otimes I \otimes L_j & \xrightarrow{\quad v \quad} & I \otimes L_j & \xrightarrow{\quad p \quad} & I \otimes L_j \\ V(\xi_1) \otimes V(\xi_2) \otimes x & \longmapsto & V(\xi_1\xi_2) \otimes x & \longmapsto & p(V(\xi_1\xi_2) \otimes x) \end{array}$$

But by proposition 1.1.9 (iv) we have $pV(\xi_1\xi_2) = V(\xi_1)V(\xi_2)$, so that

$$p(V(\xi_1\xi_2) \otimes x) = V(\xi_1)(V(\xi_2) \otimes x).$$

Axiom (D2) is also proved componentwise. For $j < i$ let $x \in L_j$ and $\xi_1, \xi_2 \in W(k)$. It is

$$\widetilde{\phi}_j(v(V(\xi_1) \otimes V(\xi_2) \otimes x)) = \widetilde{\phi}_j(V(\xi_1\xi_2) \otimes x) = \xi_1\xi_2\phi_j(x)$$

and

$$\widetilde{\widetilde{\phi}}_j(V(\xi_1) \otimes (V(\xi_2) \otimes x)) = \xi_1\widetilde{\phi}_j(V(\xi_2) \otimes x) = \xi_1\xi_2\phi_j(x).$$

The case $j = i$ is trivial. For $j > i$ let $x \in L_j$ and $\xi \in W(k)$. We have

$$p^{j-i}\widetilde{\phi}_j(V(\xi) \otimes x) = p^{j-i}\xi\phi_j(x).$$

and

$$p^{j-i-1}\phi_j(\mu_j(V(\xi) \otimes x)) = p^{j-i-1}\phi_j(V(\xi)x) = p^{j-i}\xi\phi_j(x)$$

Here we used $F(V(\xi)) = p\xi$. Note that ϕ_j is σ-linear.
To show that this predisplay is separated, we just have to look at the definitions of the involved maps. By the construction of the fibre product in the category of $W(R)$-modules we have

$$P_i \times_{P_0} P_0 = \ker\big(P_i \oplus P_0 \longrightarrow P_0 \mid (a, b) \longmapsto \theta_i(a) - pb\big).$$

The map $P_{i+1} \to P_i \times_{P_0} P_0$ is given by $x \mapsto \big(\eta_i(x), \theta_{i+1}(x)\big)$. Writing $P_0 = L_0 \oplus \cdots \oplus L_d$, then

$$P_{i+1} = (I \otimes L_0) \oplus \cdots \oplus (I \otimes L_i) \oplus L_{i+1} \oplus \cdots \oplus L_d$$

and we can write $x = x_0 + \cdots + x_d$ according to this decomposition. Now assume that

$$\big(\eta_i(x), \theta_{i+1}(x)\big) = (0, 0).$$

Then by definition of η_i we have $x_{i+1} = \cdots = x_d = 0$. On the other hand, $\theta_{i+1}(x) = 0$ implies $\sum_{j=0}^{i} \widetilde{\phi}_j(x_j) = 0$ and since $\bigoplus_{i=0}^{d} \phi_i$ is a σ-linear automorphism, it follows $x_0 = \cdots = x_i = 0$, thus $x = 0$. ∎

Definition 2.4.44. — A predisplay is called a *display*, if it is isomorphic to a predisplay associated to a set of standard data. A *morphism* of displays is a morphism of predisplays.

If $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)$ is a display given by standard data (L_i, ϕ_i), then we call the decomposition $P_0 = L_0 \oplus \cdots \oplus L_d$ a *normal decomposition* for $\mathcal{P}$. With these definitions we get a category $(\mathbf{Dis}/R)$ of displays over R. This category is obviously a full subcategory of the category of predisplays. But in contrast to the category of predisplays, the category of displays is not abelian, since the quotient of two displays is not a display in general.
Let $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)$ be a display of degree d given by standard data $(L_i, \phi_i)_{i=0,\dots,d}$ and let $\mathcal{Q} = (Q_i, \rho_i, \beta_i, \tau_i)$ be a predisplay. Assume we are given maps $\lambda_i \colon L_i \to Q_i$. Then we define maps

$$\chi_i \colon P_i = (I \otimes L_0) \oplus \cdots \oplus (I \otimes L_{i-1}) \oplus L_i \oplus \cdots \oplus L_d \to Q_i$$

by the following rules: On the summand $I \otimes L_{i-k}$ for $1 \le k \le i$ the map χ_i is the composition

$$I \otimes L_{i-k} \xrightarrow{\mathrm{id}_I \otimes \lambda_{i-k}} I \otimes Q_{i-k} \xrightarrow{\beta_{i-k}^{(k)}} Q_i,$$

and on the summand L_{i+k} for $0 \le k \le d-i$ the map χ_i is the composite

$$L_{i+k} \xrightarrow{\lambda_{i+k}} Q_{i+k} \xrightarrow{\rho_i^{(k)}} Q_i,$$

where $\rho_i^{(k)}$ is the composition of the ρ_j for $j = i, \dots, i+k-1$.

Proposition 2.4.45. — *The above defined maps χ_i induce a morphism of predisplays if and only if the diagram*

$$\begin{tikzcd} L_i \arrow[r, "\lambda_i"] \arrow[d, "\phi_i"'] & Q_i \arrow[d, "\tau_i"] \\ P_0 \arrow[r, "\chi_0"] & Q_0 \end{tikzcd}$$

is commutative for every $i \in \mathbf{N}$.

Proof. — If the χ_i induce a morphism of predisplays, then we have for every $i \in \mathbf{N}$ obviously a commutative diagram

$$\begin{tikzcd} L_i \arrow[r] \arrow[rr, bend left, "\lambda_i"] \arrow[dr, "\phi_i"'] & P_i \arrow[r, "\chi_i"] \arrow[d, "\theta_i"] & Q_i \arrow[d, "\tau_i"] \\ & P_0 \arrow[r, "\chi_0"] & Q_0 \end{tikzcd}$$

For the "if" part we must prove that the three diagrams in the definition of a morphism of predisplays commute. We start with diagram (i):

$$\begin{tikzcd} P_{i+1} \arrow[r, "\eta_i"] \arrow[d, "\chi_{i+1}"'] & P_i \arrow[d, "\chi_i"] \\ Q_{i+1} \arrow[r, "\rho_i"] & Q_i \end{tikzcd}$$

Because all the maps involed are defined componentwise, it suffices to prove the commutativity in each component. Therefor fix an $i \in \mathbf{N}$. We destinguish three cases:
Case (1) — $0 \leq k < i$: Let $V(\xi) \otimes x \in I \otimes L_k \subset P_{i+1}$. Then the following equalities hold:

$$\begin{aligned} \chi_i(\eta_i(V(\xi) \otimes x)) &= \chi_i(pV(\xi) \otimes x) \\ &= \beta_k^{(i-k)}(\mathrm{id}_I \otimes \lambda_k(pV(\xi) \otimes x)) \\ &= \beta_k^{(i-k)}(pV(\xi) \otimes \lambda_k(x)). \end{aligned}$$

On the other hand we have

$$\begin{aligned} \rho_i(\chi_{i+1}(V(\xi) \otimes x)) &= \rho_i(\beta_k^{(i-k+1)}(\mathrm{id}_I \otimes \lambda_k(V(\xi) \otimes x))) \\ &= \rho_i(\beta_k^{(i-k+1)}(V(\xi) \otimes \lambda_k(x))) \\ &= \rho_i(\beta_i(\mathrm{id}_I \otimes \gamma_k^{(i-k)}(V(1) \otimes \cdots \otimes V(1) \otimes V(\xi) \otimes \lambda_k(x)))) \\ &= \rho_i(\beta_i(V(1) \otimes \beta_k^{(i-k)}(V(\xi) \otimes \lambda_k(x)))) \\ &= V(1)\beta_k^{(i-k)}(V(\xi) \otimes \lambda_k(x)). \end{aligned}$$

Now using the fact that $V(1) = p$ (this holds by proposition 1.1.13 (ii) since R is of characteristic p) and $\beta_k^{(i-k)}$ being linear, we see that the two sides agree. Here we used the definition of the map $\beta_k^{(i-k)}$ and the commutativity of the following diagram for all $n \in \mathbf{N}$

$$\begin{tikzcd} I \otimes I^{(n)} \otimes Q_k \arrow[r, "\mathrm{id}_I \otimes \gamma_k^{(n)}"] \arrow[rr, bend left, "\gamma_k^{(n+1)}"] \arrow[d, "\mathrm{id}_I \otimes \nu^{(n)} \otimes \mathrm{id}_{Q_k}"'] & I \otimes Q_{k+n} \arrow[r, "\beta_{k+n}"] & Q_{k+n+1} \\ I \otimes I \otimes Q_k \arrow[ur, "\mathrm{id}_I \otimes \beta_k^{(n)}"'] \arrow[d, "\nu^{(2)} \otimes \mathrm{id}_{Q_k}"'] & & \\ I \otimes Q_k \arrow[uurr, "\beta_k^{(n+1)}"'] & & \end{tikzcd}$$

Note that the vertical arrow on the left is just $\nu^{(n+1)} \otimes \mathrm{id}_{Q_k}$.
Case (2) — $k = i$: This follows easily from the commutative diagram below. Just note that $\rho_i \circ \beta_i$ is multiplication by axiom (D2) of a predisplay.

$$\begin{tikzcd} P_{i+1} \arrow[r, phantom, "\supset"] \arrow[d, "\eta_i"'] & I \otimes L_i \arrow[r, "\mathrm{id}_i \otimes \lambda_i"] \arrow[d, "\mu_i"'] & I \otimes Q_i \arrow[r, "\beta_i"] & Q_{i+1} \arrow[d, "\rho_i"] \\ P_i \arrow[r, phantom, "\supset"] & L_i \arrow[rr, "\lambda_i"] & & Q_i \end{tikzcd}$$

Case (3) — $i < k \leq d$: This case is also easy and left to the reader.
The commutativity of the diagram

$$\begin{tikzcd} I \otimes P_i \arrow[r, "\alpha_i"] \arrow[d, "\mathrm{id}_I \otimes \chi_i"'] & P_{i+1} \arrow[d, "\chi_{i+1}"] \\ I \otimes Q_i \arrow[r, "\beta_i"] & Q_{i+1} \end{tikzcd}$$

follows along the same lines as above and is also left to the reader.
There is still the commutativity of the following diagram to prove.

$$\begin{tikzcd} P_i \arrow[r, "\theta_i"] \arrow[d, "\chi_i"'] & P_0 \arrow[d, "\chi_0"] \\ Q_i \arrow[r, "\tau_i"] & Q_0 \end{tikzcd}$$

Case (1) — $k = i$: This is just our hypothesis.
Case (2) — $k < i$: From our hypothesis we get a commutative diagram

$$\begin{tikzcd} I \otimes L_k \arrow[r, "\widetilde{\phi}_k"] \arrow[d, "\mathrm{id}_I \otimes \lambda_k"'] & P_0 \arrow[d, "\chi_0"] \\ I \otimes Q_k \arrow[r, "\widetilde{\tau}_k"] & Q_0 \end{tikzcd}$$

On the other hand it follows easily from the predisplay axiom (D2) that

$$\widetilde{\tau}_k = \tau_i \circ \beta_k^{(i-k)}.$$

Combining these two facts, we arrive at the desired commutative diagram

$$\begin{tikzcd} I \otimes L_k \arrow[r, "\widetilde{\phi}_k"] \arrow[d, "\mathrm{id}_I \otimes \lambda_k"'] & P_0 \arrow[d, "\chi_0"] \\ I \otimes Q_k \arrow[r, "\widetilde{\tau}_k"] \arrow[d, "\beta_k^{(i-k)}"'] & Q_0 \\ Q_i \arrow[ur, "\tau_i"'] & \end{tikzcd}$$

Case (3) — $k > i$: This case is again left to the reader. ∎

Displays and F-zips. — The connection between F-zips and displays is given by the following construction: Let R be a ring of characteristic $p > 0$ and $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i \in \mathbf{N}}$ be a display over R. We set

$$M := P_0 \big/ IP_0$$

and define two filtrations $C^\bullet$ and $D_\bullet$ by

$$C^i := \mathrm{im}\Big(P_i \xrightarrow{\quad \eta^i \quad} P_0 \longrightarrow M\Big) \otimes_\sigma R$$

$$D_i := \mathrm{im}\Big(P_i \otimes_\sigma W(R) \xrightarrow{\theta_i^\sharp} P_0 \xrightarrow{\qquad} M\Big)$$

Here, η^i denotes the composition $\eta_0 \circ \cdots \circ \eta_{i-1} \colon P_i \to P_0$. The R-linear isomorphisms $\varphi_i \colon C^i / C^{i+1} \to D_i / D_{i-1}$ are induced by the maps $\theta_i^\sharp$. In fact, we choose a normal decomposition $P_0 = L_0 \oplus \cdots \oplus L_d$ and obtain identifications

$$C^i \big/ C^{i+1} \cong L_i^{(p)} \big/ IL_i^{(p)} \quad \text{and} \quad D_i \big/ D_{i-1} \cong \theta_i^\sharp\big(L_i^{(p)}\big) \big/ I\theta_i^\sharp\big(L_i^{(p)}\big).$$

From these descriptions it is obvious that $\theta_i^\sharp$ induces an R-linear isomorphism $\varphi_i\colon C^i/C^{i+1} \to D_i/D_{i-1}$. Hence we get an F-zip $\mathcal{M} = (M, C^\bullet, D_\bullet, \varphi_\bullet)$ over R.

Displays and F-gauges. — We can also construct an F-gauge out of a predisplay. Therefor, let $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i\in\mathbf{N}_0}$ be a predisplay over R. We set

$$M^r := \begin{cases} P_r, & \text{if } r \geq 0,\\ P_0, & \text{if } r < 0,\end{cases} \quad \text{and} \quad \nu_{r+1} := \begin{cases} \eta_r, & \text{if } r \geq 0,\\ \mathrm{id}_{M^0}, & \text{if } r < 0.\end{cases}$$

We define a map $P_r \to I \otimes P_r$ by $x \mapsto p \otimes x$. For $r \geq 0$ let $f_r\colon M^r \to M^{r+1}$ be the composition of the map $P_r \to I \otimes P_r$ followed by α_r and for $r < 0$ let f_r be multiplication by p. We have to verify that $f_{r-1} \circ \nu_r = \nu_{r+1} \circ f_r = p$ holds. Let $x \in M^r$. By definition of f_r we have

$$\nu_{r+1}\big(f_r(x)\big) = \nu_{r+1}\big(\alpha_r(p \otimes x)\big) = \eta_r\big(\alpha_r(p\otimes x)\big) = px,$$

since by the predisplay axiom (D1) the map $\eta_r \circ \alpha_r$ is multiplication. For the second identity let $x \in M^{r+1}$. Then

$$f_{r-1}\big(\nu_r(x)\big) = \alpha_r\big(p \otimes \eta_r(x)\big) = px,$$

which also follows from (D1) by considering the commutative diagram

$$\begin{tikzcd} I \otimes M^{r+1} \arrow[r, "\alpha_{r+1}"] \arrow[d, "\mathrm{id}_I \otimes \eta_r"'] & M^{r+2} \arrow[d, "\eta_{r+1}"] \\ I \otimes M^r \arrow[r, "\alpha_r"] & M^{r+1} \end{tikzcd}$$

where the diagonal is multiplication. Since $M^r = M^0$ for $r \leq 0$, we have $M^{-\infty} = M^0$. This gives an F-gauge $(M^r)_{r\in\mathbf{Z}}$ over $W(R)$. There is also a σ-linear map

$$\varphi\colon M^{+\infty} = \varinjlim_{f_r} M^r \to \varinjlim_{\nu_r} M^r,$$

but this map is of some different nature (it is not a σ-linear isomorphism) as we will see later. Note that $M^0 \cong \varinjlim_{\nu_r} M^r$ and let

$$\varphi_r := \begin{cases} \theta_r, & \text{if } r \geq 0,\\ \theta_0, & \text{if } r < 0.\end{cases}$$

Because the maps θ_r are σ-linear, the maps φ_r are also. By the definition of f_r and the predisplay axiom (D2) we have for $x \in M^r$

$$\varphi_{r+1}\big(f_r(x)\big) = \varphi_{r+1}\big(\alpha_r(p\otimes x)\big) = \widetilde{\varphi}_r(p \otimes x) = \varphi_r(x),$$

which means that $\varphi_r = \varphi_{r+1} \circ f_r$. Thus, the maps φ_r induce a unique σ-linear map

$$\varphi\colon \varinjlim_{f_r} M^r \to M^0,$$

such that

$$\varphi_r = \varphi \circ \iota_r,$$

where $\iota_r\colon M^r \to \varinjlim M^s$ is induced by the natural inclusion $M^r \to \coprod M^s$. In this way we get an F-gauge $\mathfrak{M}(\mathcal{P})$ together with a σ-linear map φ associated to the predisplay $\mathcal{P}$.
Now, we have to define $\mathfrak{M}$ on morphisms. So let $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i\in\mathbf{N}}$ and $\mathcal{Q} = (Q_i, \rho_i, \beta_i, \tau_i)_{i\in\mathbf{N}}$ be two predisplays and let

$$X\colon \mathcal{P} \to \mathcal{Q}$$

be a morphism of predisplays. By the above construction we get two φ-modules

$$\mathcal{R} := \mathfrak{M}(\mathcal{P}) = (M^r, f_r, v_r, \varphi)_{r\in\mathbf{Z}} \quad \text{and} \quad \mathcal{S} := \mathfrak{M}(\mathcal{Q}) = (N^r, g_r, w_r, \psi)_{r\in\mathbf{Z}}.$$

Let

$$E := \mathfrak{M}(\Xi)\colon \mathcal{R} \to \mathcal{S}$$

be a map associated to Ξ by setting

$$\varepsilon_r := \begin{cases} \chi_r, & \text{if } r \geq 0 \\ \chi_0, & \text{if } r < 0. \end{cases}$$

To show that E is a morphism of F-gauges, we let $x \in M^r$. Then by definition of f_r and since X is a morphism of predisplays we have

$$\varepsilon_{r+1}\big(f_r(x)\big) = \chi_{r+1}\big(\alpha_r(p\otimes x)\big) = \beta_r\big(p\otimes \chi_r(x)\big) = g_r\big(\varepsilon_r(x)\big).$$

Therefore, the diagram

$$\begin{tikzcd} M^r \arrow[r, "f_r"] \arrow[d, "\varepsilon_r"'] & M^{r+1} \arrow[d, "\varepsilon_{r+1}"] \\ N^r \arrow[r, "g_r"] & N^{r+1} \end{tikzcd}$$

is commutative. The commutativity of the diagram

$$\begin{tikzcd} M^r \arrow[d, "\varepsilon_r"'] & M^{r+1} \arrow[l, "v_r"'] \arrow[d, "\varepsilon_{r+1}"] \\ N^r & N^{r+1} \arrow[l, "w_r"'] \end{tikzcd}$$

is obvious. Actually, these maps commute with φ and ψ, i.e. the diagram

$$\begin{tikzcd} M^{+\infty} \arrow[r, "\varphi"] \arrow[d, "\varepsilon_{+\infty}"'] & M^{-\infty} \arrow[d, "\varepsilon_{-\infty}"] \\ N^{+\infty} \arrow[r, "\psi"] & N^{-\infty} \end{tikzcd}$$

also commutes. First note that $M^{-\infty} = M^0$ and $N^{-\infty} = N^0$, so that $\varepsilon_{-\infty} = \varepsilon_0$. By the construction of φ_r and ψ_r and the fact that X is a morphism of predisplays, we have for all $r \in \mathbf{Z}$ a commutative diagram

$$\begin{tikzcd} M^r \arrow[r, "\varphi_r"] \arrow[d, "\varepsilon_r"'] & M^0 \arrow[d, "\varepsilon_0"] \\ N^r \arrow[r, "\psi_r"] & N^0 \end{tikzcd}$$

Thus, the induced diagram

$$\begin{tikzcd} M^{+\infty} \arrow[r, "\varphi"] \arrow[d, "\varepsilon_{+\infty}"'] & M^0 \arrow[d, "\varepsilon_0"] \\ N^{+\infty} \arrow[r, "\psi"] & N^0 \end{tikzcd}$$

commutes, too.

Summing up, we have constructed a functor $\mathfrak{M}\colon (\mathbf{Pdis}/R) \to \mathbf{FG}\big(W(R)\big)$ from the category of predisplays over R to the category of F-gauges over $W(R)$, which are equipped with a σ-linear map φ.

Example 2.4.46. — Consider the display defined by

$$P_i = \begin{cases} W(R), & \text{if } i = 0 \\ I, & \text{if } i > 0 \end{cases}$$

with η_0 the natural inclusion $I \subset W(R)$ and η_i multiplication by p for all $i > 0$. The map $\alpha_0\colon I \otimes W(R) \to W(R)$ is multiplication and the map $\alpha_i\colon I \otimes I \to I$ is given by the Verjüngung $\nu^{(2)}$ for $i > 0$. The σ-linear maps $\theta_i\colon I \to W(R)$ for $i > 0$ are given by $V^{-1}\colon I \to W(R)$, $V(\xi) \mapsto \xi$ (cf. 1.2.17). The map θ_0 is the Frobenius on $W(R)$. This display is called the *unit display*. The associated F-gauges is given by the diagram

$$\begin{tikzcd} W(R) \arrow[r, shift left, "p"] & W(R) \arrow[l, shift left, "="] \arrow[r, shift left, "p"] & I \arrow[l, shift left, "\supset"] \arrow[r, shift left, "="] & I \arrow[l, shift left, "p"] \end{tikzcd}$$

Here we have $M^{+\infty} = I$ and $M^{-\infty} = W(R)$ and the map φ is defined by $V(\xi) \mapsto \xi$. This is a σ-linear bijective map, hence in particular it is surjective (see also 1.2.17). ◂

We introduce a new category $\mathbf{FG}^{\varphi}\big(W(R)\big)$ with objects pairs (M, φ_M), where M is an F-gauge over $W(R)$ and $\varphi_M\colon M^{+\infty} \to M^{-\infty}$ is a σ-linear map. The morphisms in this category are the morphisms in $\mathbf{FG}(W(R))$, which are also compatible with φ. The subcategory of $\mathbf{FG}^{\varphi}(W(R))$ of all F-gauges equipped with a σ-linear surjective map $\varphi_M\colon M^{+\infty} \to M^{-\infty}$ is denoted by $\mathbf{FG}^{\varphi,\natural}\big(W(R)\big)$. For two $W(R)$-modules M and N and a σ-linear map $\phi\colon M \to N$, we have defined a σ-linear map

$$\begin{aligned} \widetilde{\phi}\colon I \otimes_{W(R)} M &\longrightarrow N \\ V(\xi) \otimes m &\longmapsto \xi\phi(m) \end{aligned}$$

Lemma 2.4.47. — *Let M and N be two $W(R)$-modules and $\phi\colon M \to N$ a σ-linear isomorphism. Then $\widetilde{\phi}$ is a σ-linear surjective map.*

Proof. — Apparently, the map $\widetilde{\phi}$ is σ-linear. Let $n \in N$ and consider the preimage $(\phi^{\sharp})^{-1}(n) = \sum \alpha_i \otimes m_i \in M \otimes_\sigma W(R)$. We set $m := \sum V(\alpha_i) \otimes m_i \in I \otimes_{W(R)} M$. Then it holds

$$\begin{aligned} \widetilde{\phi}(m) &= \sum \alpha_i \phi(m_i) \\ &= \phi^{\sharp}\Big(\sum \alpha_i \otimes m_i\Big) \\ &= n \end{aligned}$$

and $\widetilde{\phi}$ is surjective. ∎

Let $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i\in\mathbf{N}}$ be a display. In particular, $\mathcal{P}$ is a predisplay. We define a functor $\mathfrak{G}$ as the restriction of the functor $\mathfrak{M}$ to $(\mathbf{Dis}/R)$.

Lemma 2.4.48. — *For a display $\mathcal{P}$, the F-gauge $\mathfrak{G}(\mathcal{P})$ lies in $\mathbf{FG}^{\varphi,\natural}(W(R))$.*

Proof. — Without loss of generality we can assume that $\mathcal{P}$ is the display of degree d associated to the standard data $L_0, \dots, L_d$ with σ-linear maps ϕ_i. We already know that $\mathfrak{G}(\mathcal{P})$ is an F-gauge. It only remains to show that the map $\varphi\colon I\otimes_{W(R)} M^{+\infty} \to M^0$ is surjective. We first show that f_r is the identity if $r \geq d+1$. For $r \geq d+1$ the map α_r is given in each component by the Verjüngung $v^{(2)}$. Therefore the map $f_r\colon M^r \to M^{r+1}$ is given by

$$\begin{aligned}(V(\xi_0)\otimes x_0)\oplus\cdots\oplus(V(\xi_d)\otimes x_d) &\mapsto \\ p\otimes\big((V(\xi_0)\otimes x_0)\oplus\cdots\oplus(V(\xi_d)\otimes x_d)\big) &\mapsto \\ (V(\xi_0)\otimes x_0)\oplus\cdots\oplus(V(\xi_d)\otimes x_d)&,\end{aligned}$$

since $p = V(1)$. It follows that $\varinjlim M^r \cong M^{d+1}$. The map $\varphi = \varphi_{d+1}$ is given by $\bigoplus \widetilde{\phi}_i$. The map $\Phi = \bigoplus \phi_i$ is by definition a σ-linear automorphism of M_0. Now $M^{d+1} = (I\otimes_{W(R)} L_0)\oplus\cdots\oplus(I\otimes_{W(R)} L_d)$ is canonically isomorphic to $I\otimes_{W(R)} M^0$. Using this isomorphism we get a commutative diagram of abelian groups

$$\begin{tikzcd} M^{d+1} \arrow[r, "\varphi"] \arrow[d] & M^0 \\ I\otimes_{W(R)} M^0 \arrow[ur, "\widetilde{\Phi}"'] & \end{tikzcd}$$

The above lemma now implies the surjectivity of $\widetilde{\Phi}$ and hence φ is also surjective. ∎

The last Lemma implies that $\mathfrak{G}$ is a functor from the category of displays over R to the category of gauges over R.

The Main Theorem. — We are now going to prove the main theorem about the functors $\mathfrak{M}$ and $\mathfrak{G}$. Here we must assume, that R is perfect.

Theorem 2.4.49. — *Let R be a perfect ring. The functor $\mathfrak{M}\colon(\mathbf{Pdis}/R) \to \mathbf{FG}^{\varphi}(W(R))$ is fully faithful.*

Proof. — From the construction of $\mathfrak{M}$ it follows trivially that $\mathfrak{M}$ is faithful. So, we only have to show that $\mathfrak{M}$ is full. Let $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i\in\mathbf{N}}$ and $\mathcal{Q} = (Q_i, \rho_i, \beta_i, \tau_i)_{i\in\mathbf{N}}$ be two predisplays and let

$$E\colon \mathfrak{M}(\mathcal{P}) \to \mathfrak{M}(\mathcal{Q})$$

be a morphism of F-gauges, which is compatible with φ and ψ. For $i\in\mathbf{N}$ we set

$$\chi_i := \varepsilon_i.$$

In this way, we get a map $X\colon \mathcal{P} \to \mathcal{Q}$. To show that $\mathfrak{M}$ is full, it must be verified that X is a morphism of predisplays and that $\mathfrak{M}(X) = E$. We have only to show the first assertion, since the second is then obvious. The commutativity of the diagram

$$\begin{tikzcd} P_{i+1} \arrow[r, "\eta_i"] \arrow[d, "\chi_{i+1}"'] & P_i \arrow[d, "\chi_i"] \\ Q_{i+1} \arrow[r, "\rho_i"] & Q_i \end{tikzcd}$$

is clear. Now consider the following diagram

$$\begin{tikzcd} P_i \arrow[r] \arrow[d, "\chi_i"'] \arrow[rr, bend left, "f_i"] & I \otimes P_i \arrow[r, "\alpha_i"] \arrow[d, "\mathrm{id}_I \otimes \chi_i"'] & P_{i+1} \arrow[d, "\chi_{i+1}"] \\ Q_i \arrow[r] \arrow[rr, bend right, "g_i"'] & I \otimes Q_i \arrow[r, "\beta_i"] & Q_{i+1} \end{tikzcd}$$

Let $\zeta \otimes x \in I \otimes P_i$. Since $I = pW(R)$, we can write $\zeta = p\xi$, so that $\zeta \otimes x = p \otimes \xi x$. We have

$$\chi_{i+1}\big(\alpha_i(\zeta \otimes x)\big) = \chi_{i+1}\big(f_i(\xi x)\big).$$

On the other hand we have

$$\beta_i\big(\zeta \otimes \chi_i(x)\big) = g_i\big(\chi_i(\xi x)\big).$$

The whole diagram above is commutative, so we obtain

$$\chi_{i+1}\big(\alpha_i(\zeta \otimes x)\big) = \beta_i\big(\zeta \otimes \chi_i(x)\big),$$

which means that the righthand square is also commutative. At last, consider the diagram

$$\begin{tikzcd} P_i \arrow[r] \arrow[d, "\chi_i"'] \arrow[rr, bend left, "\varphi_i"] & P^{+\infty} \arrow[r, "\varphi"] \arrow[d, "\varepsilon_{+\infty}"'] & P_0 \arrow[d, "\chi_0"] \\ Q_i \arrow[r] \arrow[rr, bend right, "\psi_i"'] & Q^{+\infty} \arrow[r, "\psi"] & Q_0 \end{tikzcd}$$

All the four small squares commute by construction. Hence, the whole diagram commutes. Just note that $\varphi_i = \theta_i$ and $\psi_i = \tau_i$. This completes the proof. ∎

Since the inclusion functor $(\mathbf{Dis}/R) \to (\mathbf{Pdis}/R)$ is by the definition of a morphism of displays full and $\mathfrak{G}$ is the composition of this inclusion functor with $\mathfrak{M}$, which is fully faithful by the theorem, we obtain the following corollary.

Corollary 2.4.50. — *The functor $\mathfrak{G}\colon (\mathbf{Dis}/R) \to \mathbf{FG}^{\varphi,\natural}\big(W(R)\big)$ is fully faithful.*

In particular we see that if an φ-F-gauge over $W(R)$ comes from a display over R, then its reduction mod $I = V\big(W(R)\big)$ even belongs to $\mathbf{FG}^{\varphi,\sharp}(R)$.

Summing up, we have established the following figure:

$$\begin{tikzcd} (\mathrm{Dis/R}) \arrow[r] \arrow[d] & \mathrm{FG}^{\varphi,\natural}\big(W(R)\big) \arrow[r] & \mathrm{FG}^{\varphi}\big(W(R)\big) \arrow[d] \\ (F\text{-zips/R}) \arrow[r] & \mathrm{FG}^{\varphi,\sharp}(R) \arrow[r] & \mathrm{FG}^{\varphi}(R) \end{tikzcd}$$

Figure 2.1: Connection between display, F-zips and F-gauges for a ring R with $\mathrm{char}(R) = p > 0$

Displays over perfect fields. — Let k be a perfect field of characteristic $p > 0$, W be the ring of Witt vectors of k and σ be the Frobenius on k and W. Then W is a discrete valuation ring with maximal ideal pW (see proposition 1.1.14). We claim that in this situation a display $\mathcal{P} = (P_i, \eta_i, \alpha_i, \theta_i)_{i\in\mathbf{N}}$ is uniquely determined by P_0 and θ_0, i.e. by the effective F-crystal (P_0, θ_0). Indeed, let B be the quotient field of W and by abuse of notation denote the Frobenius on B again by σ. The σ-linear map $\theta_0\colon P_0 \to P_0$ induces a σ-linear map $\theta_0 \otimes B\colon P_0 \otimes_W B \to P_0 \otimes_W B$. By definition the W-module P_0 is projective and hence it is even free, since W is a principal ideal domain. Thus, $\theta_0 \otimes B$ is a σ-linear map of finite dimensional B-vector spaces, which in this situation must be an isomorphism, since by definition displays come from standard data. Using the natural inclusion $P_0 \hookrightarrow P_0 \otimes_W B$ we identify P_0 with a lattice in $P_0 \otimes_W B$. The preimage of this lattice P_0 under $\theta_0 \otimes B$ is again a lattice, which contains P_0, i.e. $P_0 \subset (\theta_0 \otimes B)^{-1}(P_0)$. Using the theory of elementary divisors ([Lan02, III Theorem 7.8 and 7.9]) we find a decomposition $P_0 = L_0 \oplus \cdots \oplus L_d$ such that

$$(\theta_0 \otimes B)^{-1}(P_0) = L_0 \oplus p^{-1}L_1 \oplus \cdots \oplus p^{-d}L_d.$$

The restriction of $p^{-i}\theta_0$ to L_i defines a σ-linear map $\phi_i\colon L_i \to P_0$ such that $\bigoplus \phi_i$ is a σ-linear bijective map (cf. lemma 1.2.15). This gives standard data for the display $\mathcal{P}$. This discussion establishes the following lemma.

Lemma 2.4.51. — *There is a bijection*

$$\{\textit{displays over } k\}/\cong \;\xleftrightarrow{\sim}\; \{\textit{effective } F\textit{-crystals over } k\}/\cong$$

given by $(P_i, \eta_i, \alpha_i, \theta_i)_{i\in\mathbf{N}} \mapsto (P_0, \theta_0)$.

Using this lemma in conjuction with theorem 2.2.17 we obtain the following classification of displays in terms of matrices. The height of a display is just the rank of the free W-module P_0, which in turn is the height of the associated F-crystal.

Theorem 2.4.52. — *Let k be a perfect field of characteristic $p > 0$. Then there is a bijection of sets*

$$\left\{\begin{array}{c} \textit{displays of height } h \\ \textit{with elementary divisors} \\ \mu_1 \le \cdots \le \mu_h \end{array}\right\}\Big/\cong \;\xleftrightarrow{\sim}\; \mathrm{GL}_h \begin{pmatrix} p^{\mu_1} & & 0 \\ & \ddots & \\ 0 & & p^{\mu_h} \end{pmatrix} \mathrm{GL}_h \Big/ \sim_\sigma$$

with $\mu_i \in \mathbf{N}$.

Chapter 3

Topologies in positive characteristic

This short chapter recalls the definition and some simple properties of syntomic morphisms. We also introduce some other classes of morphisms in characteristic p. The second section gives the definition of the crystalline category and describes the syntomic topology on that category.

§1 Syntomic morphisms

A syntomic morphism is a morphism, which is flat, locally of finite presentation and locally a complete intersection. We recall what it means for a morphism to be a locally complete intersection. This notion is related to the notion of a regular immersion. The definition of a regular immersion in [Gro67, 16.9.2] is not well-behaved for non Noetherian schemes. Therefore, we use the definition in [SGA71, Exp. VII], which is the right one in the general situation and agrees with the one in [Gro67] in the locally Noetherian case (cf. [Gro67, 19.5.1]).
Let R be a ring. A sequence $x_1, \dots, x_r \in R$ is called *regular*, if

- the ideal $(x_1, \dots, x_r) \subsetneq R$ is proper;
- the image of x_{i+1} in $R/(x_1, \dots, x_i)$ is a nonzerodivisor.

If R is a Noetherian local ring, it is well known that any permutation of a regular sequence is again regular. This may fail in the non Noetherian case. For a general discussion of different notions of regularity and counterexamples see [Kab71].

Definition 3.1.1. — Let R be a ring and $\mathbf{x} = (x_1, \dots, x_r)$ a sequenece in R. The sequence $\mathbf{x}$ is called *Koszul-regular*, if the associated Koszul-complex is acyclic in degrees ≥ 1.

Remark 3.1.2. — A regular sequence is always Koszul-regular, but in general not conversely. See [Gro67, 19.5.1] for the first part and [Kab71, Section 3 Example 3] for a counterexample. ◁

Definition 3.1.3. — Let $f\colon X \to Y$ be an immersion of schemes and choose an open subset $U \subset Y$ such that $f\colon X \to U$ is a closed immersion. Let $\mathcal{J}$ be the quasi-coherent ideal sheaf in $\mathcal{O}_U$, which defines this closed immersion. Then f is called a *regular immersion*, if for each $x \in \operatorname{Supp}(\mathcal{O}_U/\mathcal{J})$ there is an affine open neighbourhood $V = \operatorname{Spec} A$ of x such that $\mathcal{J}|_U = \widetilde{I}$ for some ideal I of A, which can be generated by a Koszul-regular sequence $g_1, \dots, g_r \in A$.

***Remark* 3.1.4.** — This definition is obviously independent of the open set U chosen. ◁

Definition 3.1.5. — Let $f: X \to Y$ be a morphism of schemes. We call f *a locally complete intersection morphism*, if for each $x \in X$ there is an open neighbourhood $U \subset X$ of x and a smooth Y-scheme V such that $f|_U$ factors as

$$\begin{tikzcd} U \arrow[r, "i"] \arrow[dr, "f|_U"'] & V \arrow[d, "h"] \\ & Y \end{tikzcd}$$

where $i: U \to V$ is a regular closed immersion and $h: V \to Y$ is smooth.

Since the class of locally complete intersection morphisms is only stable under base change for flat morphisms, we cannot use it to define a Grothendieck topology. But if we add a flatness hypothesis, we get a good class of morphisms.

Definition 3.1.6. — A morphism of schemes is called *syntomic*, if it is flat, locally of finite presentation and a locally complete intersection morphism.

Locally, a syntomic morphism $f: X \to Y$ is of the form

$$\operatorname{Spec} A[x_1, \ldots, x_n]/(g_1, \ldots, g_r) \to \operatorname{Spec} A$$

for a regular sequence $g_1, \ldots, g_r$, where the map

$$A \to A[x_1, \ldots, x_n]/(g_1, \ldots, g_r)$$

is flat (cf. [Gro66, 11.3.8]). Moreover, by [Gro67, 19.2] we can assume $g_1, \ldots, g_r$ to be *transversally regular*, i.e. $g_1, \ldots, g_r$ is a regular sequence and $A[x_1, \ldots, x_n]/(g_1, \ldots, g_i)$ is a flat A-algebra for each $1 \leq i \leq r$.
Syntomic morphisms have the following properties.

Proposition 3.1.7. —

(i) *An open immersion is syntomic.*

(ii) *The composition of syntomic morphisms is syntomic.*

(iii) *Any base change of a syntomic morphism is syntomic.*

Proof. — This follows from [SGA71, Exp. VIII, Prop. 1.4] and [Gro67, 19.3.9]. ∎

These properties enable us to define a Grothendieck topology on the category of X-schemes. So let X be a scheme and consider the category $(\mathbf{Sch}/X)$ of all X-schemes with morphisms the X-morphisms. A covering of a X-scheme U is a surjective family $\{f_i: U_i \to U\}_{i \in I}$ of syntomic morphisms, i.e. $U = \bigcup_{i \in I} f_i(U_i)$ and each f_i is a syntomic X-morphism. We denote the coresponding site by X_{SYN} and call it the *big syntomic site of* X. Analoguously, one defines the big Zariski site X_{ZAR} of X. The *small syntomic site of* X, denoted by X_{syn} is the full subcategory of X_{SYN} of all syntomic

X-schemes with coverings again the surjective families of syntomic morphisms. The small Zariski site is denoted by X_{Zar}. In contrast to the small Zariski site, the fibre product of two objects of the small syntomic site does in general not exists. The problem is, that a morphism in X_{syn} is in general not syntomic. But for cohomological considerations we can use both the big or the small syntomic site: The natural functor $u: X_{syn} \to X_{\mathrm{SYN}}$ is obviously continuous, cocontinuous and fully faithful. By corollary 1.4.57 the cohomology groups of an abelian sheaf are canonically isomorphic.

Remark 3.1.8. — It is an immediate consequence of Delign's theorem (see [SGA72b, expose VI, 9. appendice]) that the big syntomic site over a noetherian base has enough points. The main step is to show that each covering has a finite subcovering. This is almost literally the same as in [Tam94, Ch II 3.1.1]. Note that one cannot use Delign's theorem to show that the small syntomic site has enough points, since the fibre product of two syntomic schemes is in general not syntomic. ◁

Although we will work in this paper only with the syntomic topology, there are some coarser topologies in positive characteristic which one could also use. To deal with inseparable extensions of fields in characteristic $p > 0$, one has to enlarge the class of étale morphism. What one needs is to treat extensions given by a polynomial of the form $x^p - a$.

Definition 3.1.9. —

(i) A morphism $f: \mathrm{Spec} B \to \mathrm{Spec} A$ is called an *extraction of p-th roots*, if the corresponding ring homomorphism can be written as a chain

$$A_0 = A \to A_1 \to \cdots \to A_n = B,$$

such that $A_{i+1} \cong A_i[x]/(x^p - a_i)$ for some $a_i \in A_i$.

(ii) A morphism $f: X \to Y$ of schemes is said to be a *p-morphism*, if for every $x \in X$ there is an affine open neighbourhood $U \subset X$ of x and an affine open neighbourhood $V \subset Y$ of $f(x)$ such that $f(U) \subset V$ and $f|_U: U \to V$ is an extraction of p-th roots.

Remark 3.1.10. — The case $n = 0$ is allowed in part (i). Hence the identity is an extraction of p-th roots. ◁

Now, to be able to handle arbitrary finite field extensions in positive characteristic, we combine the notion of an étale morphism with that of a p-morphism. The leading example is the classical statement, that an algebraic field extension E/k can be decomposed into $E \supset F \supset k$, where F/k is separable and E/F is purely inseparable (see [Lan02, V §6 Prop. 6.5]).

Definition 3.1.11. — Let $f: X \to Y$ be a morphism of schemes. We call f a *quasi-étale* morphism, *quiet* for short, if for any $x \in X$ there is an affine open neighbourhood $U \subset X$ of x and an étale affine Y-scheme V such that the diagram

$$\begin{tikzcd} U \arrow[r, "g"] \arrow[d] & V \arrow[d] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

commutes and $g: U \to V$ is an extraction of p-th roots.

Remark 3.1.12. — It is a classical result that each finite group scheme over a field k of characteristic 0 is étale (see [Wat79, section 11.4]). This yields an equivalence of categories between the category of finite group schemes over k and the category of étale sheaves over $\mathrm{Spec}(k)$. If k has characteristic $p > 0$ then by the structure theorem for finite group schemes over k (see [Wat79, section 14.4]) one gets an equivalence of categories between the category of finite group schemes over k and the quiet sheaves over $\mathrm{Spec}(k)$, which are representable. ◃

It is not hard to show that p-morphisms and quiet morphisms are stable under composition and base change. For quiet morphisms one can use the topological invariance of étale morphisms [SGA72b, Exp. VIII, 1.1] to show stability of composition. Here are some examples of classes of morphisms in characteristic $p > 0$.

Example 3.1.13. — We have the following inclusions of classes of morphisms in characteristic $p > 0$:

$$\begin{tikzcd}
\{\text{open immersions}\} \arrow[r, hook] \arrow[d, hook] & \{\text{étale morphisms}\} \arrow[r, hook] \arrow[d, hook] & \{\text{fppf morphisms}\} \\
\{p\text{-morphisms}\} \arrow[r, hook] & \{\text{quiet morphisms}\} \arrow[r, hook] & \{\text{syntomic morphisms}\} \arrow[u, hook]
\end{tikzcd}$$

Figure 3.1: Morphisms in positive characteristic

In this paper, we will only work with syntomic morphisms. But many results carry over without difficulty to other classes of morphisms and the Grothendieck topology they generate. In positive characteristic this is especially the case for the classes in the lower line of the above figure.

§2 The crystalline-syntomic site

We will define the big and small crystalline-syntomic site on the category $\mathrm{CRIS}(X/S)$. In our applications X will be the spectrum of a perfect field k and S the ring of truncated Witt vectors of length n of k. Before we proceed, we recall the definition of the crystalline category.

Definition 3.2.14. — Let S be a scheme, $(\mathscr{J}, \gamma)$ a quasi-coherent sheaf of ideals in $\mathscr{O}_S$ with divided powers and X be an S-scheme such that

- p is locally nilpotent in X;
- the divided powers γ extend to X.

The category $\mathrm{CRIS}(X/S, \mathscr{J}, \gamma)$ has as objects quadrupels (U, T, i, δ), where

(i) U is an X-scheme;

(ii) T is an S-schemes such that p is locally nilpotent in T;

(iii) $i: U \hookrightarrow T$ is a closed S-immersion;

(iv) δ is a DP-structure on the ideal in $\mathscr{O}_T$ defined by the closed immersion i and compatible with γ.

A morphism $(u,v)\colon (U',T',i',\delta') \to (U,T,i,\delta)$ in $\mathrm{CRIS}(X/S,\mathscr{J},\gamma)$ is a commutative diagram

$$\begin{tikzcd} U' \arrow[r, hook, "i'"] \arrow[d, "u"'] & T' \arrow[d, "v"] \\ U \arrow[r, hook, "i"] & T \end{tikzcd}$$

where u is an X-morphism and v is a DP-morphism over S.

Remark 3.2.15. — (i) If the ideal $\mathscr{J}$ is locally principal, then the DP-structure γ always extends to any S-scheme (cf. 1.3.35). In particular, if k is a perfect field, $S = \operatorname{Spec} W_n(k)$ and $\mathscr{J} = (p)$ with its canonical DP-structure, then the above conditions are satisfied.

(ii) For any object (U,T,i,δ) in $\mathrm{CRIS}(X/S,\mathscr{J},\gamma)$, the closed immersion $i\colon U \hookrightarrow T$ is a nil-immersion, because p is locally nilpotent in T and the DP-structure δ is required to be compatible with γ (cf. 1.3.24 (iii)). ◁

To topologize this category we use syntomic morphisms. Actually, by replacing "syntomic" in the following definition by any class E like in 3.1.13, we get a Grothendieck topology on $\mathrm{CRIS}(X/S,\mathscr{J},\gamma)$.

Definition 3.2.16. — Let (U,T,i,δ) be an object of $\mathrm{CRIS}(X/S,\mathscr{J},\gamma)$. A covering of (U,T,i,δ) is a family $(U_\alpha,T_\alpha,i_\alpha,\delta_\alpha)$ of objects of $\mathrm{CRIS}(X/S,\mathscr{J},\gamma)$ together with morphisms

$$(u_\alpha,v_\alpha)\colon (U_\alpha,T_\alpha,i_\alpha,\delta_\alpha) \to (U,T,i,\delta)$$

such that the diagram

$$\begin{tikzcd} U_\alpha \arrow[r, hook, "i_\alpha"] \arrow[d, "u_\alpha"'] & T_\alpha \arrow[d, "v_\alpha"] \\ U \arrow[r, hook, "i"] & T \end{tikzcd}$$

is cartesian and $\{v_\alpha\colon T_\alpha \to T\}$ is a surjective family of syntomic morphisms.

Remark 3.2.17. — Since the above diagram is required to be cartesian, we have $U_\alpha \cong U \times_T T_\alpha$ and the map $U_\alpha \to U$ is also syntomic, for syntomic morphisms being stable under base change. ◁

The *big crystalline-syntomic site* of X/S is the category $\mathrm{CRIS}(X/S,\mathscr{J},\gamma)$ with the just defined Grothendieck topology. This site is denoted $\mathrm{CRIS}(X/S,\mathscr{J},\gamma)_{\mathrm{SYN}}$ and the associated topos by $(X/S,\mathscr{J},\gamma)_{\mathrm{CRIS-SYN}}$. In the sequel we will write $\mathrm{CRIS}(X/S)$ for the category $\mathrm{CRIS}(X/S,\mathscr{J},\gamma)$ when the DP-structure is clear from the context and for objects we will write (U,T) instead of (U,T,i,δ). If $S = \operatorname{Spec} A$ is affine, we will write $\mathrm{CRIS}(X/A)$ instead of $\mathrm{CRIS}(X/S)$. There is also a *small crystalline-syntomic site*. It is the full subcategory of $\mathrm{CRIS}(X/S)$ of objects (U,T), where U is a syntomic X-scheme and the coverings are the surjective families $\{(U_\alpha,T_\alpha) \to (U,T)\}$ of syntomic morphisms like above. It follows from the general theory (1.4.57) that cohomological calculations can be done on either site. The small crystalline-syntomic site will be denoted by $\mathrm{CRIS}(X/S)_{\mathrm{syn}}$ and the associated topos by $(X/S)_{\mathrm{cris-syn}}$. In the sequel we also have to use the crystalline category with the Zariski topology. This site (called *big crystalline-Zariski site*) is denoted by $\mathrm{CRIS}(X/S)_{\mathrm{ZAR}}$ and the associated topos by $(X/S)_{\mathrm{CRIS}}$. For the small variants we use the notations $\mathrm{CRIS}(X/S)_{\mathrm{Zar}}$ and $(X/S)_{\mathrm{cris}}$ repsectively. For more details about the crystalline-syntomic site the reader is referred to [**Bau92**] and [**BM90**], where the crystalline category is endowed with different topologies and many of the results there carry over to the crystalline-syntomic site.

Chapter

4 The sheaves $\mathscr{O}_n^{\text{cris}}$

This chapter contains the definition and the technical most important facts about the syntomic sheaf $\mathscr{O}_n^{\text{cris}}$. Section one gives the basic definition of these sheaves and section two describes an alternative way of constructing these sheaves using the ring of Witt vectors and divided powers. This is used in the third section to show flatness of these sheaves.

§1 Definition of $\mathscr{O}_n^{\text{cris}}$

Many of the results proved in this chapter can be found in [Bre96] for the log-syntomic setting and our presentation will follow this paper in many places.

Let k be a perfect field and $W_n := W_n(k)$ the truncated ring of Witt vectors of k of length n. The Frobenius on k and W_n will be denoted by the same letter σ. We define a presheaf $\mathscr{O}_n^{\text{cris}}$ on $(\operatorname{Spec} k)_{\text{SYN}}$ by

$$\mathscr{O}_n^{cris}\colon X \longmapsto \mathrm{H}^0\big((X/W_n)_{cris}, \mathscr{O}_{X/W_n}\big)$$

This assignment is in fact functorial, since for any map $f\colon X \to Y$ of k-schemes there is a morphism of ringed topoi

$$f_{\text{CRIS}}\colon \big(X/W_n, \mathscr{J}, \gamma\big)_{\text{CRIS-SYN}} \longrightarrow \big(Y/W_n, \mathscr{J}, \gamma\big)_{\text{CRIS-SYN}},$$

i.e. there is a map of sheaves $\mathscr{O}_{Y/W_n} \to f_{\text{CRIS},*}\mathscr{O}_{X/W_n}$ [BBM82, 1.1.10]. From this morphism and the edge morphism of the Leray spectral sequence we obtain the desired map

$$\mathrm{H}^0\big(Y/W_n, \mathscr{O}_{Y/W_n}\big) \longrightarrow \mathrm{H}^0\big(Y/W_n, f_{\text{CRIS},*}\mathscr{O}_{X/W_n}\big) \longrightarrow \mathrm{H}^0\big(X/W_n, \mathscr{O}_{X/W_n}\big).$$

Obviously, the cohomology group $\mathrm{H}^0\big((X/W_n)_{\text{cris}}, \mathscr{O}_{X/W_n}\big)$ is a W_n-module and the absolute Frobenius F_{abs} on X induces by functoriality a σ-linear homomorphism of rings

$$F_{\text{abs}}^*\colon \mathrm{H}^0\big((X/W_n)_{\text{cris}}, \mathscr{O}_{X/W_n}\big) \longrightarrow \mathrm{H}^0\big((X/W_n)_{\text{cris}}, \mathscr{O}_{X/W_n}\big)$$

Hence we obtain a σ-linear map

$$\varphi\colon \mathscr{O}_n^{\text{cris}} \longrightarrow \mathscr{O}_n^{\text{cris}},$$

which is a homomorphism of sheaves of rings. This map φ is called the *Frobenius* on $\mathscr{O}_n^{\mathrm{cris}}$. In order to show that the presheaf $\mathscr{O}_n^{\mathrm{cris}}$ is actually a sheaf, we need the following lemmas.

Lemma 4.1.1. — *Let $s\colon A \to B$ be a surjective homomorphism of rings with nilpotent kernel. Let $C = B[x_1,\dots,x_n]/(g_1,\dots,g_r)$ be an B-algebra for a transversally regular sequence $g_1,\dots,g_r \in B[x_1,\dots,x_n]$. Choose preimages $\widehat{g}_i \in A[x_1,\dots,x_n]$ of g_i under the natural surjection induced by s. Then the sequence $\widehat{g}_1,\dots,\widehat{g}_r$ is transversally regular in the A-algebra $A[x_1\dots,x_n]$.*

Proof. — This is a special case of [Bou06a, Théorème 1, chap. III §5 No. 2]. Fix $1 \le i \le r$ and apply the equivalence of (i) and (iii) of this theorem with I the kernel of $A[x_1,\dots,x_n]/(\widehat{g}_1,\dots,\widehat{g}_i) \to B[x_1,\dots,x_n]/(g_1,\dots,g_i)$, which is nilpotent since $\ker(s)$ is nilpotent by hypothesis. ∎

Lemma 4.1.2. — *Let $X \hookrightarrow Y$ be an object of $\mathrm{CRIS}(\mathrm{Spec}k/W_n)$ and $V \to X$ a syntomic morphism. Then each $x \in V$ posesses a Zariski-open neighborhood U_x such that there exists a syntomic Y-schemes T_x, which is a DP-thickening of U_x and the family $\{U_x \hookrightarrow T_x\}_{x\in V}$ is a syntomic covering of $\{X \hookrightarrow Y\}$.*

Proof. — Since the question is local, we can assume that $X = \mathrm{Spec}B$ and $Y = \mathrm{Spec}A$ and $V = \mathrm{Spec}C$ with $C \cong B[x_1,\dots,x_n]/(g_1,\dots,g_r)$ for a transversally regular sequence $g_1,\dots,g_r \in B[x_1,\dots,x_n]$. Denote by $s\colon A \to B$ the surjection with nilpotent kernel and let $\widehat{g}_1,\dots,\widehat{g}_r \in A[x_1,\dots,x_n]$ be preimages of $g_1,\dots,g_r$ under the natural map $A[x_1,\dots,x_n] \to B[x_1,\dots,x_n]$ induced by s. Set $D := A[x_1\dots,x_n]/(\widehat{g}_1,\dots,\widehat{g}_r)$ and let $\widehat{s}\colon D \to C$ be the natural surjection. Then $\ker(\widehat{s})$ is nilpotent and $C \cong B \otimes_A D$. By the previous lemma, the sequence $\widehat{g}_1,\dots,\widehat{g}_r$ is transversally regular and D is a flat A-algebra. Hence, $\mathrm{Spec}D \to \mathrm{Spec}A$ is syntomic and the divided powers of $\ker(s)$ extend to $\ker(\widehat{s})$ by 1.3.35 (ii). ∎

Proposition 4.1.3. — *The presheaf $\mathscr{O}_n^{\mathrm{cris}}$ is already a sheaf on $(\mathrm{Spec}k)_{\mathrm{SYN}}$.*

Proof. — Let U be an object of $(\mathrm{Spec}k)_{\mathrm{SYN}}$ and $\{U_i \to U\}$ be a syntomic covering of U. We have to show that the sequence

$$0 \longrightarrow \mathscr{O}_n^{\mathrm{cris}}(U) \longrightarrow \prod_i \mathscr{O}_n^{\mathrm{cris}}(U_i) \longrightarrow \prod_{i,j} \mathscr{O}_n^{\mathrm{cris}}(U_i \times_U U_j)$$

is exact. Let $s \in \mathscr{O}_n^{\mathrm{cris}}(U) = \mathrm{H}^0(U/W_n, \mathscr{O}_{U/W_n})$. By the definition of the global section functor $s = (s_T)$ for a compatible family (s_T) of sections $s_T \in \Gamma(T, \mathscr{O}_T)$, where $V \hookrightarrow T$ is an object of $\mathrm{CRIS}(U/W_n)$. Assume s maps to 0 in $\prod_i \mathscr{O}_n^{\mathrm{cris}}(U_i)$. Let $V \hookrightarrow T$ be an object of $\mathrm{CRIS}(U/W_n)$ and set $V_i := U_i \times_U V$. Then the projection on the second factor $V_i \to V$ is syntomic since $U_i \to U$ is syntomic and syntomic morphisms are stable under base extension. By lemma 4.1.2 we can find a syntomic covering $\{W_l \hookrightarrow T_l\}$ of $V \hookrightarrow T$ such that the diagram

$$\begin{tikzcd}
W_l \arrow[r] \arrow[d] & T_l \arrow[dd] \\
V_i \arrow[d] & \\
V \arrow[r] & T
\end{tikzcd}$$

is cartesian. Since $(s_T) \mapsto 0$ in $\prod_i \mathscr{O}_n^{\mathrm{cris}}(U_i)$, we have in particular $\mathrm{res}_{T_l,T}(s_T) = 0$ for all l. But $\mathscr{O}_T$ is a syntomic sheaf and T_l a syntomic covering of T, hence $s_T = 0$. This holds for all objects $V \hookrightarrow T$ of $\mathrm{CRIS}(U/W_n)$ and we deduce $s = 0$. A similar argument shows exactness at the second node. ∎

For any k-scheme X, the sheaf $\mathscr{O}_n^{\mathrm{cris}}$ can also be considered as a sheaf on X_{SYN} by using the inverse image functor $f^{-1}\colon (\mathrm{Spec}\,k)_{\mathrm{SYN}} \to X_{\mathrm{SYN}}$ induced by the structure morphism $f\colon X \to \mathrm{Spec}\,k$.
We will now construct morphisms from the crystalline-syntomic topos to the (big) syntomic topos and to the crystalline-Zariski topos. It will be shown that the syntomic sheaf $\mathscr{O}_n^{\mathrm{cris}}$ "computes" the crystalline cohomology of the crystalline structure sheaf. The next two lemmas are true for every pair X/S satisfying the requirements in the definition of the crystalline category 3.2.14.

Lemma 4.1.4. — *There is a morphism of topoi*

$$u\colon (X/S)_{\mathrm{CRIS-SYN}} \longrightarrow X_{\mathrm{SYN}}$$

given by

- $u_*\mathscr{F}(U) := \mathrm{H}^0((U/S)_{\mathrm{CRIS-SYN}}, \mathscr{F})$ *for an abelian sheaf* $\mathscr{F}$ *on* $\mathrm{CRIS}(X/S)_{\mathrm{SYN}}$ *and an object* U *of* $\mathrm{SYN}(X)$.
- $u^*\mathscr{G}(U, T, \delta) := \mathscr{G}(U)$ *for an abelian sheaf* $\mathscr{G}$ *on* $\mathrm{SYN}(X)$ *and an object* (U, T, δ) *of* $\mathrm{CRIS}(X/S)_{\mathrm{SYN}}$.

Proof. — See [Bau92, Proposition 1.10]. ∎

Remark 4.1.5. — Note that u is not a morphism ringed topoi, if we consider both topoi with their natural structure sheaves. But if we let $S = \mathrm{Spec}(W_n)$ and X be a k-scheme, then we can view X_{SYN} as a ringed topos with the sheaf associated to the constant presheaf with value W_n (abusively also denoted by W_n) as ring sheaf. For (U, T) an object of $(X/W_n)_{\mathrm{CRIS-SYN}}$ we have by definition $\mathscr{O}_{X/W_n}(U, T) = \Gamma(T, \mathscr{O}_T)$ and this is a W_n-algebra. Hence we have a map $u^{-1}W_n \to \mathscr{O}_{X/W_n}$ of sheaves or by adjunction $W_n \to u_*\mathscr{O}_{X/W_n}$. ◁

Example 4.1.6. — Let $X = \mathrm{Spec}\,k$ for a perfect field k of characteristic $p > 0$ and $S = \mathrm{Spec}(W_n)$. Then we have $\mathscr{O}_n^{\mathrm{cris}} = u_*\mathscr{O}_{\mathrm{Spec}\,k/W_n}$. ◀

Lemma 4.1.7. — *There is a morphism of topoi*

$$v\colon (X/S)_{\mathrm{CRIS-SYN}} \longrightarrow (X/S)_{\mathrm{CRIS}}$$

given by

- $v_*\mathscr{F}(U, T, \delta) := \mathscr{F}(U, T, \delta)$ *for an abelian sheaf* $\mathscr{F}$ *on* $\mathrm{CRIS}(X/S)_{\mathrm{SYN}}$ *and an object* (U, T, δ) *of* $\mathrm{CRIS}(X/S)_{\mathrm{ZAR}}$.
- $v^*\mathscr{G}$ *is the sheaf associated to the presheaf* $(U, T, \delta) \mapsto \mathscr{G}(U, T, \delta)$ *for an abelian sheaf* $\mathscr{G}$ *on* $\mathrm{CRIS}(X/S)_{\mathrm{ZAR}}$ *and an object* (U, T, δ) *of* $\mathrm{CRIS}(X/S)_{\mathrm{SYN}}$.

Proof. — This is evident, since open immersions are syntomic. ∎

Lemma 4.1.8. — *For all $i \geq 1$ we have*

$$\mathrm{R}^i u_* \mathscr{O}_{X/S} = 0 \quad \text{and} \quad \mathrm{R}^i v_* \mathscr{O}_{X/S} = 0.$$

Proof. — For the first part see [Bau92, Proposition 1.17] and for the second part see [BBM82, 1.1.18 and 1.1.19]. ∎

Corollary 4.1.9. — *Let X be an object of* $\mathrm{SYN}(\mathrm{Spec}k)$. *Then there is for any $i \geq 0$ a canonical isomorphism*

$$\mathrm{H}^i(X_{\mathrm{SYN}}, \mathscr{O}_n^{\mathrm{cris}}) \cong \mathrm{H}^i((X/W_n)_{\mathrm{CRIS-ZAR}}, \mathscr{O}_{X/W_n})$$

compatible with Frobenius.

Proof. — See [FM87, II 1.3]. ∎

§2 Witt vectors and $\mathscr{O}_n^{\mathrm{cris}}$

In this section we will construct an isomorphism from the sheaf $\widetilde{W}_n^{DP,\mathrm{cris}}$ associated to the divided power envelope of the ring of Witt vectors of length n to the sheaf $\mathscr{O}_n^{\mathrm{cris}}$ on the site $(\mathrm{Spec}k)_{\mathrm{SYN}}$. If A is a ring of characteristic $p > 0$ such that the Frobenius is surjective on A, then we get an isomorphism $W_n^{DP}(A) \to \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A)$. This enables us to compute the value of $\mathscr{O}_n^{\mathrm{cris}}$ for special coverings. We keep the notation of the last section: k is a perfect field of characteristic $p > 0$. We write W_n for the ring of Witt vectors of k of length n. For a k-algebra A we view $W_n(A)$ as a W_n-algebra via the map

$$W_n \xrightarrow{F^{-n}} W_n \longrightarrow W_n(A),$$

where F is the Frobenius on W_n (which is an isomorphism since k is perfect) and $W_n \to W_n(A)$ is the canonical map induced by $k \to A$. Note that $W_n(A)$ as W_n-algebra in the above sense can be identified with $W_n(A) \otimes_{F^n} W_n$ via the isomorphism $a \otimes \lambda = F^{-n}(\lambda)a \otimes 1 \mapsto F^{-n}(\lambda)a$.
We consider the following commutative diagram in the category $\mathrm{CRIS}(\mathrm{Spec}k/W_n)$.

$$\begin{tikzcd} \mathrm{Spec}A \arrow[r, hook] \arrow[d] & \mathrm{Spec}B \arrow[d] \\ \mathrm{Spec}k \arrow[r, hook] & \mathrm{Spec}W_n \end{tikzcd}$$

The nilimmersion $\mathrm{Spec}A \hookrightarrow \mathrm{Spec}B$ is induced by a surjection $s\colon B \twoheadrightarrow A$. The kernel $\ker(s)$ has divided powers compatible with the natural divided powers on pW_n by the definition of the crystalline category. Define a homomorphism of rings by

$$\sigma_n\colon W_n(A) \to A, \quad (a_0, \dots, a_{n-1}) \mapsto a_0^{p^n}.$$

For $a \in A$ we denote by $\widehat{a} \in B$ a preimage of a under the map s and define a map by

$$\widehat{\sigma}_n\colon W_n(A) \to B, \quad (a_0, \dots, a_{n-1}) \mapsto \widehat{a}_0^{p^n} + p\widehat{a}_1^{p^{n-1}} + \cdots + p^{n-1}\widehat{a_{n-1}}^p.$$

The next two lemmas show that this is a well-defined homomorphism of W_n-algebras.

Lemma 4.2.10. — *The map $\widehat{\sigma}_n$ is well-defined.*

Proof. — Two preimages of $a \in A$ differ by an element $\alpha \in \ker(s)$. Let $(a_0, \dots, a_{n-1}) \in W_n(A)$ and $\widehat{a_i}, \widehat{b_i} \in B$ two preimages of a_i. There exists $\alpha_i \in \ker(s)$ such that $\widehat{a_i} = \widehat{b_i} + \alpha_i$. We compute

$$\begin{aligned} p^i \widehat{a_i}^{p^{n-i}} &= p^i (\widehat{b_i} + \alpha_i)^{p^{n-i}} \\ &= p^i \widehat{b_i}^{p^{n-i}} + \sum_{j=1}^{p^{n-i}} p^i \binom{p^{n-i}}{j} \widehat{b_i}^{p^{n-i}-j} \alpha^j. \end{aligned}$$

Since the ideal $\ker(s)$ has divided powers γ, we can write $\alpha^j = j! \gamma_j(\alpha)$. The following elementary lemma says that the p-valuation of $\binom{p^{n-i}}{j}$ is $p^{n-i} - v_p(j)$. Thus we have

$$v_p\left(p^i \cdot \binom{p^{n-i}}{j} \cdot j!\right) = i + n - i - v_p(j) + v_p(j!) \geq n$$

for $0 < j \leq p^{n-i}$. But B is as W_n-algebra annihilated by p^n. Hence, all the coefficients in the sum are zero, which completes the proof. ∎

Lemma 4.2.11. — *Let $p \in \mathbf{N}$ be prime and $e \geq 1$ be an integer. Then for all $0 < j \leq p^e$ one has*

$$v_p\left(\binom{p^e}{j}\right) = e - v_p(j).$$

Proof. — We use induction over j. For $j = 1$ the assertion is true. Let $j > 1$. Then

$$\begin{aligned} v_p\left(\binom{p^e}{j}\right) &= v_p\left(\binom{p^e}{j-1} \cdot \frac{p^e - (j-1)}{j}\right) \\ &= v_p\left(\binom{p^e}{j-1}\right) + v_p(p^e - (j-1)) - v_p(j) \\ &= e - v_p(j-1) + v_p(p^e - (j-1)) - v_p(j). \end{aligned}$$

In the last line we used the induction hypothesis. But $v_p(p^e - (j-1))$ is equal to $v_p(j-1)$ and this implies the lemma. ∎

Lemma 4.2.12. — *The map $\widehat{\sigma}_n \colon W_n(A) \to B$ is a homomorphism of W_n-algebras.*

Proof. — The surjective map $s \colon B \twoheadrightarrow A$ induces a surjective ring homomorphism $W_n(s) \colon W_n(B) \twoheadrightarrow W_n(A)$. The commutative diagram

$$\begin{tikzcd} W_n(B) \arrow[d, "W_n(s)"'] \arrow[dr, "w_n"] & \\ W_n(A) \arrow[r, "\widehat{\sigma}_n"] & B \end{tikzcd}$$

now shows that $\widehat{\sigma}_n$ is a ring homomorphism. Next note that $W_n(B)$ is a $W_n(W_n)$-algebra, since B is a W_n-algebra. The following diagram on the left hand side gives the commutative diagram on the right hand side:

$$\begin{tikzcd} A & B \arrow[l, "s"'] \\ k \arrow[u] & W_n \arrow[l] \arrow[u] \end{tikzcd} \qquad \begin{tikzcd} W_n(A) & W_n(B) \arrow[l, "W_n(s)"'] \\ W_n \arrow[u] & W_n(W_n) \arrow[l] \arrow[u] \end{tikzcd}$$

Let $(\alpha_0,\ldots,\alpha_{n-1}) \in W_n$. Because we view $W_n(A)$ as a W_n-algebra via F^{-n} it follows

$$(\alpha_0,\ldots,\alpha_{n-1})\cdot(1,0,\ldots,0) = \left(\alpha_0^{p^{-n}},\ldots,\alpha_{n-1}^{p^{-n}}\right) \in W_n(A).$$

The element $\alpha := \left((\alpha_0^{p^{-n}},0,\ldots,0),\ldots,(\alpha_{n-1}^{p^{-n}},0,\ldots,0)\right)$ is a preimage of $\left(\alpha_0^{p^{-n}},\ldots,\alpha_{n-1}^{p^{-n}}\right)$ in $W_n(B)$. For $(b_0,\ldots,b_{n-1}) \in W_n(B)$ we have

$$\begin{aligned} w_n\big(\alpha\cdot(b_0,\ldots,b_{n-1})\big) &= w_n(\alpha)w_n\big((b_0,\ldots,b_{n-1})\big) \\ &= \left(\sum_{i=0}^{n-1} p^i(\alpha_i^{p^{-n}},0,\ldots,0)^{p^{n-i}}\right)\cdot\left(\sum_{i=0}^{n-1} p^i\widehat{a}_i^{\,p^{n-i}}\right) \end{aligned}$$

where $s(b_i) = \widehat{a}_i$. We compute $p^i\left(\alpha_i^{p^{-n}},0,\ldots,0\right)^{p^{n-i}} \in W_n$. First,

$$\left(\alpha_i^{p^{-n}},0,\ldots,0\right)^{p^{n-i}} = \left(\alpha_i^{p^{-i}},0,\ldots,0\right)$$

and second $p^i = V^iF^i$, which yields

$$p^i\left(\alpha_i^{p^{-i}},0,\ldots,0\right) = (0,\ldots,0,\alpha_i,0,\ldots,0).$$

Finally, we get $\sum_{i=0}^{n-1} p^i\left(\alpha_i^{p^{-n}},0,\ldots,0\right)^{p^{n-i}} = (\alpha_0,\ldots,\alpha_{n-1})$. ■

Since A is a k-algebra, multiplication by p is zero and we obtain a commutative diagram of rings

$$\begin{tikzcd} W_n(A) \arrow[r, "\sigma_n"] \arrow[d, "\widehat{\sigma}_n"'] & A \arrow[d, equal] \\ B \arrow[r, "s"] & A \end{tikzcd}$$

We set

$$W_n^{\mathrm{cris}}(\mathrm{Spec}A) := W_n(A).$$

Consider the morphism $\sigma_n \colon W_n^{\mathrm{cris}}(\mathrm{Spec}A) \to A$. Its kernel is

$$I_A := \left\{(a_0,\ldots,a_{n-1}) \in W_n^{\mathrm{cris}}(\mathrm{Spec}A) \,\middle|\, a_0^{p^n} = 0\right\}.$$

Let $W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A)$ be the divided power envelope of $W_n^{\mathrm{cris}}(\mathrm{Spec}A)$ with respect to I and compatible with the canonical DP-structure on pW_n (cf. proposition 1.3.38). The next step is to construct a canonical morphism $W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A) \to \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A)$. Therefor let A' be a syntomic A-algebra and $\mathrm{Spec}A' \hookrightarrow \mathrm{Spec}B'$ be a W_n-DP-thickening:

$$\begin{tikzcd} \mathrm{Spec}A' \arrow[r, hook] \arrow[d] & \mathrm{Spec}B' \\ \mathrm{Spec}A & \end{tikzcd}$$

We define a map $W_n^{\mathrm{cris}}(\mathrm{Spec}A) \to B'$ of W_n-algebras as the composition

$$W_n^{\mathrm{cris}}(\mathrm{Spec}A) \longrightarrow W_n^{\mathrm{cris}}(\mathrm{Spec}A') \longrightarrow B'.$$

This gives a commutative diagram

$$\begin{tikzcd} W_n^{\mathrm{cris}}(\mathrm{Spec}A') \arrow[r, "\widehat{\sigma}_n'"] & B' \arrow[r, "s'"] & A' \\ W_n^{\mathrm{cris}}(\mathrm{Spec}A) \arrow[u] \arrow[rr, "\sigma_n"] & & A \arrow[u] \end{tikzcd}$$

The commutativity implies that the image of $I_A = \ker(\sigma_n)$ in B' is contained in $\ker(s')$. Moreover, the DP-structure δ' on $\ker(s')$ is compatible with the canonical DP-structure on pW_n. By the universal property of the DP-envelope (see proposition 1.3.38) we get a unique map $W_n^{DP}(A) \to B'$ of W_n-DP-algebras making the diagram commute:

$$\begin{tikzcd} (W_n^{DP}(A), I_A, \gamma) \arrow[dr, dashed] & \\ (W_n(A), I_A) \arrow[u] \arrow[r] & (B', \ker(s'), \delta') \end{tikzcd}$$

Given two W_n-DP-thickenings $\mathrm{Spec}A_i \hookrightarrow \mathrm{Spec}B_i$ for $i = 1, 2$, where A_1 is a syntomic A-algebra and A_2 is a syntomic A_1-algebra, and a W_n-DP-morphism $\mathrm{Spec}B_2 \to \mathrm{Spec}B_1$ such that the diagram

$$\begin{tikzcd} \mathrm{Spec}A_2 \arrow[r, hook] \arrow[d] & \mathrm{Spec}B_2 \arrow[d] \\ \mathrm{Spec}A_1 \arrow[r, hook] & \mathrm{Spec}B_1 \end{tikzcd}$$

commutes, we get with the same reasoning as above for $i = 1, 2$ a unique map of W_n-DP-algebras

$$W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A) \longrightarrow B_i.$$

From the uniqueness of these two maps it follows that the triangle of W_n-algebra homomorphisms

$$\begin{tikzcd} & W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A) \arrow[dl] \arrow[dr] & \\ B_1 \arrow[rr] & & B_2 \end{tikzcd}$$

commutes. Since the sections $\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A)$ may be computed as the inverse limit over all diagrams

$$\begin{tikzcd} \mathrm{Spec}A' \arrow[r, hook] \arrow[d] & \mathrm{Spec}B' \\ \mathrm{Spec}A & \end{tikzcd}$$

where A' is a syntomic A-algebra and B' is a W_n-DP-thickening, there is a unique map of W_n-algebras to this inverse limit and we obtain our desired canonical W_n-algebra homomorphism

$$W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A) \longrightarrow \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A).$$

To show functoriality in the category of affine k-schemes, let $f\colon \mathrm{Spec}A \to \mathrm{Spec}B$ be a morphism of k-schemes. Then f induces obviously two morphisms

$$W_n^{DP,\mathrm{cris}}(\mathrm{Spec}B) \longrightarrow W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A)$$

$$\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}B) \longrightarrow \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A)$$

Our construction above gives a commutative square

$$\begin{tikzcd} W_n^{\mathrm{cris}}(\mathrm{Spec}B) \arrow[r] \arrow[d] & W_n^{\mathrm{cris}}(\mathrm{Spec}A) \arrow[d] \\ \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}B) \arrow[r] & \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A) \end{tikzcd}$$

and the universal property of DP-envelopes implies the commutativity of the square

$$\begin{tikzcd} W_n^{DP,\mathrm{cris}}(\mathrm{Spec}B) \arrow[r] \arrow[d] & W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A) \arrow[d] \\ \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}B) \arrow[r] & \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A) \end{tikzcd}$$

After having defined the presheaf $W_n^{DP,\mathrm{cris}}$ on the category of affine k-schemes it is straightforward to extend this definition to the category $(\mathrm{Spec}k)_{\mathrm{SYN}}$: Let $\mathscr{O}$ be the structure sheaf of $(\mathrm{Spec}k)_{\mathrm{SYN}}$. For an object X of $(\mathrm{Spec}k)_{\mathrm{SYN}}$ we set

$$W_n^{\mathrm{cris}}(X) := W_n\big(\mathscr{O}(X)\big).$$

If I_X denotes the kernel of the map $\widehat{\sigma}_n\colon W_n^{\mathrm{cris}}(X) \to W_n(\mathscr{O}(X))$, we define $W_n^{DP,\mathrm{cris}}(X)$ as the DP-envelope of $W_n^{\mathrm{cris}}(X)$ with respect to I_X and compatible with the canonical DP-structure on pW_n. Obviously, this construction is functorial and we get a presheaf of W_n-algebras

$$X \longmapsto W_n^{DP,\mathrm{cris}}(X)$$

on $(\mathrm{Spec}k)_{\mathrm{SYN}}$. To construct a morphism of presheaves $W_n^{DP,\mathrm{cris}} \to \mathscr{O}_n^{\mathrm{cris}}$ just note the description of $\mathscr{O}_n^{\mathrm{cris}}(X)$ as a projective limit like in the proof of 4.1.3. Exactly the same arguments as in the affine case establish now the canonical morphism of presheaves of W_n-algebras $W_n^{DP,\mathrm{cris}} \to \mathscr{O}_n^{\mathrm{cris}}$. This morphism gives rise to a morphism of sheaves of W_n-algebras on $(\mathrm{Spec}k)_{\mathrm{SYN}}$

$$\widetilde{W}_n^{DP,\mathrm{cris}} \longrightarrow \mathscr{O}_n^{\mathrm{cris}},$$

where $\widetilde{W}_n^{DP,\mathrm{cris}}$ is the syntomic sheafification of $W_n^{DP,\mathrm{cris}}$. Our goal is now to show that this morphism is actually an isomorphism of sheaves. In order to proof this, we first proof a proposition, which is also useful for computing global sections of $\mathscr{O}_n^{\mathrm{cris}}$ for k-algebras with surjective Frobenius.

Proposition 4.2.13. — *Let A be a k-algebra and assume that the Frobenius endomorphism of A is surjective. Then we have a canonical isomorphism*

$$W_n^{DP}(A) \xrightarrow{\sim} \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A).$$

Proof. — The main point is to observe that

$$\mathrm{Spec}A \hookrightarrow \mathrm{Spec}\big(W_n^{DP}(A)\big)$$

is an object of $\mathrm{CRIS}(\mathrm{Spec}k/W_n)$: Since the Frobenius is assumed to be surjective, the map

$$W_n(A) \xrightarrow{\sigma_n} A$$

is surjective as well with kernel I_A and forming the DP-envelope gives a map of DP-rings

$$(W_n^{DP}(A), \overline{I}_A, \delta) \longrightarrow (A, \{0\}, 0).$$

The W_n-algebra $W_n^{DP}(A)$ is annihilated by p^n and hence the DP-ideal $\overline{I}_A$ is a nilideal by example 1.3.24. This shows that

$$\mathrm{Spec}A \hookrightarrow \mathrm{Spec}\big(W_n^{DP}(A)\big)$$

is an object of $\mathrm{CRIS}(\mathrm{Spec}k/W_n)$. Moreover, this object is a W_n-DP-thickening of $\mathrm{Spec}A$. Let ϕ denote the canonical map of W_n-algebras

$$\phi\colon W_n^{DP}(A) \longrightarrow \mathscr{O}_n^{\mathrm{cris}}\big(\mathrm{Spec}A\big).$$

The sheaf $\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A)$ is the inverse limit over all W_n-DP-thickenings of $\mathrm{Spec}A$. Let

$$\psi\colon \mathscr{O}_n^{\mathrm{cris}}\big(\mathrm{Spec}A\big) \longrightarrow W_n^{DP}(A)$$

be the projection to the component $\mathrm{Spec}A \hookrightarrow \mathrm{Spec}(W_n^{DP}(A))$. We claim that ϕ and ψ are inverse to each other. By the universal property of the inverse limit, we must have

$$\phi \circ \psi = \mathrm{id}.$$

On the other hand, the equality $\psi \circ \phi = \mathrm{id}$ is clear by the construction of the map ϕ. This completes the proof. ∎

***Remark* 4.2.14.** — If A is a k-algebra with surjective Frobenius, then the object

$$\big(\mathrm{Spec}A, \mathrm{Spec}(W_n^{DP}(A))\big)$$

is a final object in the category $\mathrm{CRIS}(\mathrm{Spec}A/W_n)$. This follows from the universal property of the DP-envelope of $W_n(A)$. ◃

Corollary 4.2.15. — *Let R be a perfect ring of characteristic $p > 0$. Then there is a canonical isomorphism*

$$W_n(R) \xrightarrow{\sim} \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}R).$$

Proof. — The kernel of $\sigma_n\colon W_n(R) \to R$ is

$$I_R = \big\{(a_0, \dots, a_{n-1}) \in W_n(R) \bigm| a_0^{p^n} = 0\big\}.$$

But a perfect ring is reduced and we see that $I_R = V\big(W_n(R)\big)$. This ideal already has divided powers compatible with the canonical divided powers on pW_n. Therefore, the DP-envelope of $W_n(R)$ with respect to I_R is $W_n(R)$ itself and the result follows from the proposition, for the Frobenius being by assumption an isomorphism and in particular surjective on R. ∎

Now we are ready to state the main theorem of this section.

Theorem 4.2.16. — *Let k be a perfect field of characteristic $p > 0$. Then the canonical morphism defined above*

$$\widetilde{W}_n^{DP,\mathrm{cris}} \longrightarrow \mathscr{O}_n^{\mathrm{cris}}$$

is an isomorphism of sheaves on $(\mathrm{Spec}k)_{\mathrm{SYN}}$.

Proof. — Let $\mathscr{P}\mathscr{K}$ be the kernel and $\mathscr{P}\mathscr{C}$ be the cokernel of the map of presheaves $W_n^{DP,\mathrm{cris}} \to \mathscr{O}_n^{\mathrm{cris}}$. Denote the associated sheaves by $\mathscr{K}$ and $\mathscr{C}$ respectively. We have to show that $\mathscr{K}(X) = 0 = \mathscr{C}(X)$ for every k-scheme X. It is actually enough to show this for affine schemes $X = \mathrm{Spec}A_0$. So let A_0 be a k-algebra. Consider the set

$$J := \{\text{finite subsets of } A_0\} \times \mathbf{N}$$

with the partial order

$$(\mathcal{E}_1, n_1) \le (\mathcal{E}_2, n_2) :\Longleftrightarrow \mathcal{E}_1 \subset \mathcal{E}_2 \quad \text{and} \quad n_1 \le n_2.$$

For $j = (\mathcal{E}, n) \in J$ we construct a A_0-algebra

$$A_j := A_0[X_a \mid a \in \mathcal{E}]\big/(X_a^{p^n} - a \mid a \in \mathcal{E}).$$

If $j_1 \le j_2$ then there is an obvious morphism $\mathrm{Spec}A_{j_2} \to \mathrm{Spec}A_{j_1}$. This morphism is actually a syntomic covering, since it is a successive extraction of p-th roots. We set $A := \varinjlim_{j\in J} A_j$. By construction, the Frobenius is surjective on A. Since J is partially ordered, the direct limit is filtered and thus exact. The idea of the proof is now to show that given a section $s \in \mathscr{P}\mathscr{K}(\mathrm{Spec}A_0)$, the restriction of s to some $\mathrm{Spec}A_j$ vanishes. But first we compute $\varinjlim_{j\in J}\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A_j)$. By definition we have

$$\varinjlim_{j\in J}\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A_j)=\varinjlim_{j\in J}\mathrm{H}^0(\mathrm{Spec}A_j/W_n,\mathscr{O}_{\mathrm{Spec}A_j/W_n}).$$

It follows from the general theory of [SGA72b, Exp. VI, 8.1 - 8.7] that

$$\varinjlim_{j\in J}\mathrm{H}^0(\mathrm{Spec}A_j/W_n,\mathscr{O}_{\mathrm{Spec}A_j/W_n})\cong\mathrm{H}^0(\mathrm{Spec}A/W_n,\mathscr{O}_{\mathrm{Spec}A/W_n})$$

and we finally get

$$\varinjlim_{j\in J}\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A_j)\cong\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A).$$

On the other hand we have

$$\varinjlim_{j\in J}W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A_j)\cong W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A),$$

since taking divided power envelopes commutes with direct limits by [Ber74, Chap. I, 2.4.1]. Therefore, there is an exact sequence

$$0\longrightarrow\varinjlim_{j\in J}\mathscr{P}\mathscr{K}(\mathrm{Spec}A_j)\longrightarrow W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A)\longrightarrow\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A)\longrightarrow\varinjlim_{j\in J}\mathscr{P}\mathscr{C}(\mathrm{Spec}A_j)\longrightarrow 0$$

But the Frobenius is surjective on A and it follows from proposition 4.2.13 that

$$W_n^{DP,\mathrm{cris}}(\mathrm{Spec}A)\longrightarrow\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec}A)$$

is an isomorphism. Thus,

$$\varinjlim_{j\in J}\mathscr{P}\mathscr{K}(\mathrm{Spec}A_j)=0=\varinjlim_{j\in J}\mathscr{P}\mathscr{C}(\mathrm{Spec}A_j).$$

Hence there exists a $j\in J$ such that $\mathrm{res}_{\mathrm{Spec}A_j,\mathrm{Spec}A_0}(s)=0$. This implies that the associated sheaf $\mathscr{K}$ of the presheaf $\mathscr{P}\mathscr{K}$ is zero. The same argument shows that $\mathscr{C}=0$. ∎

§3 Flatness of $\mathscr{O}_n^{\mathrm{cris}}$

From now on we work on the small syntomic site $(\mathrm{Spec}k)_{syn}$. By abuse of notation we denote the restriction of $\mathscr{O}_n^{\mathrm{cris}}$ to the small site again by $\mathscr{O}_n^{\mathrm{cris}}$. In this situation we can show that the sheaves $\mathscr{O}_n^{\mathrm{cris}}$ on $(\mathrm{Spec}k)_{syn}$ are flat W_n-modules. From this result we derive a very important short exact sequence of sheaves

$$0\longrightarrow\mathscr{O}_m^{\mathrm{cris}}\longrightarrow\mathscr{O}_{m+n}^{\mathrm{cris}}\longrightarrow\mathscr{O}_n^{\mathrm{cris}}\longrightarrow 0,$$

which is crucial for the construction of the gauges $\mathscr{G}_n$ in the next chapter.

The following criterion of flatness is well known (at least in the case of modules over a ring). We state and proof it in the form which will be used in the sequel.

Lemma 4.3.17. — *Let k be a perfect field of characteristic $p > 0$ and let $n \in \mathbf{N}$ be an integer. For a sheaf $\mathscr{F}$ of W_n-modules on the small syntomic site of* $\operatorname{Spec} k$ *the following are equivalent:*

(i) $\mathscr{F}$ is a flat sheaf of W_n-modules;

(ii) $\ker(p^i) = \operatorname{im}(p^{n-i})$ for all $0 \le i \le n$.

Proof. — The proof follows closely [Mes72, Chapter I, Lemma 1.1]. We first show (i) implies (ii). We have the exact sequence

$$W_n \xrightarrow{p^{n-i}} W_n \xrightarrow{p^i} W_n$$

and applying $- \otimes \mathscr{F}$ yields by (i) the exact sequence

$$\mathscr{F} \xrightarrow{p^{n-i}} \mathscr{F} \xrightarrow{p^i} \mathscr{F},$$

which gives (ii). For the converse we use the following criterion of [Bou06a, Thm. 1 and Prop. 1, chap. III §5 No. 2] which holds with the same proof also for sheaves of modules:
The following are equivalent:

(i) $\mathscr{F}$ is a flat sheaf of W_n-modules;

(ii) a) $\mathscr{F}/p\mathscr{F}$ is a flat sheaf of k-modules;
b) $\operatorname{Tor}_1^{W_n}(W_m, \mathscr{F}) = 0$ for all $m \ge 0$.

Since k is a field, (a) is trivial. To show (b), we consider the exact sequence

$$0 \longrightarrow W_{n-i} \xrightarrow{p^i} W_n \longrightarrow W_i \longrightarrow 0$$

and obtain by applying $- \otimes \mathscr{F}$ the exact sequence

$$0 \longrightarrow \operatorname{Tor}_1^{W_n}(W_i, \mathscr{F}) \longrightarrow \mathscr{F}/p^{n-i}\mathscr{F} \xrightarrow{p^i} \mathscr{F} \longrightarrow \mathscr{F}/p^i\mathscr{F} \longrightarrow 0$$

But our assumption $\ker(p^i) = \operatorname{im}(p^{n-i})$ tells us that $p^i \colon \mathscr{F}/p^{n-i}\mathscr{F} \to \mathscr{F}$ is injective and we must thus have $\operatorname{Tor}_1^{W_n}(W_i, \mathscr{F}) = 0$. ∎

To show that the sheaves $\mathscr{O}_n^{\mathrm{cris}}$ are flat W_n-modules, we introduce the notion of a *perfection* of a ring A of characteristic $p > 0$.

Definition 4.3.18. — Let A be a ring of characteristic $p > 0$. The *perfection* of A is a perfect ring $A^{p^{-\infty}}$ of characteristic $p > 0$ together with a map $i \colon A \to A^{p^{-\infty}}$ satisfying the following universal property: Given any perfect ring B and a homomorphism of $j \colon A \to B$, there exists a unique homomorphism $\varphi \colon A^{p^{-\infty}} \to B$ making the diagram

$$\begin{tikzcd} A \arrow[r, "j"] \arrow[d, "i"'] & B \\ A^{p^{-\infty}} \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

commute.

Obviously, the perfection of A is unique (up to unique isomorphism) if it exists. To construct the perfection, let us denote the Frobenius endomorphism $a \mapsto a^p$ of A be σ. We consider the diagram

$$A \xrightarrow{\sigma} A \xrightarrow{\sigma} A \xrightarrow{\sigma} A \xrightarrow{\sigma} \cdots$$

and set $A^{p^{-\infty}}$ the direct limit over this diagram. It is easy to see, that this ring satisfies the requiered properties. The details may also be found in [Bou07b, Chap. V §1 No. 4]. The map $i\colon A \to A^{p^{-\infty}}$ is the natural map of A to this direct limit and the kernel of i consists of the nilpotent elements of A.

Example 4.3.19. — Let k be a field of characteristic $p > 0$. Then $k^{p^{-\infty}}$ is the inseparable closure of k. ◂

Example 4.3.20. — Let $A := k[X_1, \dots, X_m]$ be the polynomial ring over a perfect field of characteristic $p > 0$. The perfection of A is denoted by $A^{p^{-\infty}} := k[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}]$. This means that for $1 \leq i \leq m$ and every $s \in \mathbf{N}$ there exists an element $Y \in k[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}]$ with $Y^{p^s} = X_i$. This element Y will be denoted by $X_i^{p^{-s}}$. Hence, the perfection of A may be described as a polynomial ring over k (since k is assumed to be perfect, the perfection of k is k itself) in infinite many variables

$$X_1, \dots, X_m, X_1^{p^{-1}}, \dots, X_m^{p^{-1}}, X_1^{p^{-2}}, \dots, X_m^{p^{-1}}, \dots$$

modulo the obvious relations. Note that the perfection of a polynomial ring is not Noetherian. ◂

We set for $B = k[X_1, \dots, X_m]$

$$B_i := k[X_1^{p^{-i}}, \dots, X_n^{p^{-i}}].$$

Then $B^{p^{-\infty}} = B_\infty := \varinjlim_{i\in\mathbf{N}} B_i$ with the injective maps $B_i \to B_{i+1}$ induced by $X_j^{p^{-i}} \mapsto (X_j^{p^{-i-1}})^p$. We note that

$$B_i \cong B[Y_1, \dots, Y_m]/(Y_1^{p^i} - X_1, \dots, Y_m^{p^i} - X_m).$$

Thus the maps $B_i \to B_{i+1}$ are faithfully flat p-th roots. Since any syntomic k-algebra can locally (for the Zariski topology) be written as $A = k[X_1, \dots, X_m]/(f_1, \dots, f_r)$ for a (transversally) regular sequence $f_1, \dots, f_r$, we set

$$A_i = k[X_1^{p^{-i}}, \dots, X_m^{p^{-i}}]/(f_1, \dots, f_r)$$

and still have injective maps $A_i \to A_{i+1}$ given by $X_j^{p^{-i}} \mapsto (X_j^{p^{-i-1}})^p$. Using these maps we define $A_\infty = \varinjlim_{i\in\mathbf{N}} A_i$. This is not the perfection of A, but the Frobenius on A_∞ is surjective and this is all we need. Moreover, the maps $A_i \to A_{i+1}$ are faithfully flat syntomic morphisms. In particular each A_i is a faithfully flat syntomic k-algebra. The next easy lemma is a technical key step in proving the flatness of $\mathcal{O}_n^{\mathrm{cris}}$ over W_n.

Lemma 4.3.21. — *Let $A = k[X_1, \dots, X_m]/(f_1, \dots, f_r)$ for a regular sequence $f_1, \dots, f_r$ and let A_i and A_∞ be as above. Let $\mathscr{F} \to \mathscr{G} \to \mathscr{H}$ be a sequence of sheaves on $(\mathrm{Spec} k)_{syn}$. Then the sequence*

$$0 \longrightarrow \mathscr{F} \longrightarrow \mathscr{G} \longrightarrow \mathscr{H} \longrightarrow 0$$

is exact, if the sequence

$$0 \longrightarrow \mathscr{F}(\mathrm{Spec} A_\infty) \longrightarrow \mathscr{G}(\mathrm{Spec} A_\infty) \longrightarrow \mathscr{H}(\mathrm{Spec} A_\infty) \longrightarrow 0$$

is exact, where $\mathscr{F}(\mathrm{Spec} A_\infty) := \varinjlim_{i\in\mathbf{N}} \mathscr{F}(\mathrm{Spec} A_i)$ and the same for $\mathscr{G}$ and $\mathscr{H}$.

Proof. — This is immediate from the fact that $\mathrm{Spec} A_{i+1} \to \mathrm{Spec} A_i$ is a faithfully flat syntomic morphism. ∎

Remark 4.3.22. — Since the perfection of a Notherian ring A is in general not Noetherian, we cannot evaluate a sheaf $\mathscr{F}$ on $(\mathrm{Spec} k)_{syn}$ in $A^{p^{-\infty}}$, because this may not be an object of our site. That is the reason for the convention $\mathscr{F}(\mathrm{Spec} A_\infty) := \varinjlim_{i\in\mathbf{N}} \mathscr{F}(\mathrm{Spec} A_i)$ in the lemma. ◁

Proposition 4.3.23. — *Let the notations be as above. Then the W_n-algebra $\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec} A_\infty)$ is flat.*

Proof. — *Step 1:* We first show the W_n-linear isomorphism

$$\mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec} A_\infty) \cong (W_n(A_\infty) \otimes_{F^n} W_n)^{DP},$$

where the DP-envelope is with repsect to the kernel of the W_n-linear map $\sigma_n\colon W_n(A_\infty) \otimes_{F^n} W_n \to A_\infty$ of section 2 page 64. Let us compute

$$\begin{aligned}\varinjlim_{i\in\mathbf{N}} \mathscr{O}_n^{\mathrm{cris}}(\mathrm{Spec} A_i) &= \varinjlim_{i\in\mathbf{N}} \mathrm{H}^0((\mathrm{Spec} A_i/W_n)_{\mathrm{CRIS}}, \mathscr{O}_{\mathrm{Spec} A_i/W_n}) \\ &\cong \mathrm{H}^0((\mathrm{Spec} A_\infty/W_n)_{\mathrm{CRIS}}, \mathscr{O}_{\mathrm{Spec} A_\infty/W_n}) \\ &\cong (W_n(A_\infty) \otimes_{F^n} W_n)^{DP}.\end{aligned}$$

The first isomorphism follows from [SGA72b, Exp. VI, 8.1 - 8.7] (compare the proof of theorem 4.2.16), and the second follows from proposition 4.2.13 or the remark following that proposition, since the Frobenius is surjective on A_∞.
Step 2: By step 1 it is enough to show that $(W_n(A_\infty) \otimes_{F^n} W_n)^{DP}$ is flat over W_n. Therefor, consider $k[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}]$, the perfection of the polynomial ring over k. The image of the regular sequence $f_1, \dots, f_r \in k[X_1, \dots, X_m]$ in the perfection is again regular and is still denoted by $f_1, \dots, f_r$. Using lemma 4.1.1 we can lift this sequence to a regular sequence $\widehat{f_1}, \dots, \widehat{f_r}$ in $W_n[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}]$, since the kernel of the natural surjection is (p), which is a nilpotent ideal. We get a natural surjection

$$s\colon W_n[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}] \longrightarrow k[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}]/(f_1, \dots, f_r) = A_\infty$$

with kernel $I = (p, \widehat{f_1}, \dots, \widehat{f_r})$. Let $(W_n[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}])^{DP}$ be the DP-envelope with respect to I and compatible with the canonical divided powers on pW_n.
Step 3: There is a canonical isomorphism

$$(W_n(A_\infty) \otimes_{F^n} W_n)^{DP} \longrightarrow (W_n[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}])^{DP}.$$

First, the canonical surjection $k[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}] \to A_\infty$ gives a canonical surjection

$$s'\colon W_n(k[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}]) \to W_n(A_\infty).$$

Let $(W_n(k[X_1^{p^{-\infty}}, \dots, X_m^{p^{-\infty}}]) \otimes_{F^n} W_n)^{DP}$ be the DP-envelope with respect to $\ker(\sigma_n \circ (s' \otimes_{F^n} \mathrm{id}_{W_n}))$. The DP-envelope of an algebra (B, J) is by construction a quotient of $\Gamma_B(J)$ and the image of $\ker(s' \otimes_{F^n} \mathrm{id} W_n)$ in $(W_n(k[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}]) \otimes_{F^n} W_n)^{DP}$ is zero. Applying [BO78, 3.20.7], we obtain an isomorphism

$$(W_n(k[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}]) \otimes_{F^n} W_n)^{DP} \longrightarrow (W_n(A_\infty) \otimes_{F^n} W_n)^{DP}.$$

On the other hand, there is a canonical isomorphism

$$(W_n(k[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}])) \otimes_{F^n} W_n \longrightarrow W_n[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}]$$

induced by $(g_0, \ldots, g_{n-1}) \mapsto \sum_{i=0}^{n-1} p^i \widehat{g}_i^{p^{n-i}}$, where $\widehat{g}_i$ is a lifting of g_i to $W_n[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}]$ (compare page 64). Since the ideal (p) is nilpotent and has divided powers, this map is well-defined. The composition $\sigma_n \circ (s' \otimes_{F^n} \mathrm{id}_{W_n})$ now factors as

$$\begin{tikzcd}
(W_n(k[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}])) \otimes_{F^n} W_n \arrow[r, "\sim"] \arrow[d, "\sigma_n \circ (s' \otimes_{F^n} \mathrm{id}_{W_n})"'] & W_n[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}] \arrow[dl, "s"] \\
A_\infty &
\end{tikzcd}$$

Hence we get the desired isomorphism

$$((W_n(k[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}])) \otimes_{F^n} W_n)^{DP} \longrightarrow (W_n[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}])^{DP}$$

Step 4: Let us set $B := W_n[X_1^{p^{-\infty}}, \ldots, X_m^{p^{-\infty}}]$ and $\widehat{f}_0 := p$. Then $I = (\widehat{f}_0, \ldots, \widehat{f}_r)$ is the kernel of the surjection $s \colon B \to A_\infty$ (Step 2). We consider the ring

$$C := \left(B \otimes_{W_n} W_n[T_0, \ldots, T_m]/(T_0^{p^n}, \ldots, T_m^{p^n})\right) \Big/ (T_0 - \widehat{f}_0, \ldots, T_m - \widehat{f}_m).$$

The canonical map $B \to C$ is surjective and gives an isomorphism $B^{DP} \cong C^{DP}$, where B^{DP} is the DP-envelope of B with respect to I and C^{DP} the DP-envelope of C with respect to the image of I in C. The image of I in C is equal to the ideal $(T_0, \ldots, T_m)$.
Step 5: By the criterion of flatness of a regular sequence it follows that C is flat over

$$S := W_n[T_0, \ldots, T_m]/(T_0^{p^n}, \ldots, T_m^{p^n}).$$

Now [BO78, 3.21] yields an isomorphism

$$C^{DP} \cong C \otimes_S W_n\langle T_0, \ldots, T_m\rangle.$$

It follows that C^{DP} is flat over $W_n\langle T_0, \ldots, T_m\rangle$. Since $W_n\langle T_0, \ldots, T_m\rangle$ is by construction a free W_n-module, it is flat over W_n and so C^{DP} is flat over W_n. Combining the isomorphism above with the isomorphisms obtained in the previous steps, we finally get

$$(W_n(A_\infty) \otimes_{F^n} W_n)^{DP} \cong C \otimes_S W_n\langle T_0, \ldots, T_m\rangle.$$

Thus, $(W_n(A_\infty) \otimes_{F^n} W_n)^{DP}$ is flat over W_n. ∎

Corollary 4.3.24. — *The sheaf $\mathscr{O}_n^{\mathrm{cris}}$ on $(\operatorname{Spec} k)_{syn}$ is flat over W_n and we have an exact sequence*

$$0 \longrightarrow \mathscr{O}_m^{\mathrm{cris}} \xrightarrow{\pi} \mathscr{O}_{m+n}^{\mathrm{cris}} \xrightarrow{\nu} \mathscr{O}_n^{\mathrm{cris}} \longrightarrow 0.$$

Remark 4.3.25. — In terms of the ring of Witt vectors one should think of the exact sequenece in the following way: Consider the exact sequnece

$$W_{m+n} \xrightarrow{p^n} W_{m+n} \xrightarrow{p^m} W_{m+n}.$$

It is very easy to check that we have a commutative diagram with exact rows

$$\begin{tikzcd}
 & W_{m+n} \arrow[r, "p^n"] \arrow[d] & W_{m+n} \arrow[r, "p^m"] \arrow[d, "\mathrm{id}"] & W_{m+n} \arrow[d] & \\
0 \arrow[r] & W_m \arrow[r, "\pi"] & W_{m+n} \arrow[r, "\nu"] & W_n \arrow[r] & 0
\end{tikzcd}$$

where $\pi\colon W_m \to W_{m+n}$ is given by $(a_0, \dots, a_{m-1}) \mapsto (0, \dots, 0, a_0^{p^n}, \dots, a_{m-1}^{p^n})$ and $\nu\colon W_{m+n} \to W_n$ by $(a_0, \dots, a_{m+n-1}) \mapsto (a_0^{p^m}, \dots, a_{n-1}^{p^m})$. The vertical maps are the natural truncations

$$(a_0, \dots, a_{m+n-1}) \mapsto (a_0, \dots, a_{m-1}).$$

◁

Chapter

5 Gauges

This chapter contains the second part of the main theorem of this thesis. After first introducing the notion of φ-rings and φ-gauges, we construct in the second section a sheaf of rings on the small syntomic site of a perfect field, which is the fundamental object in the theory of Fontaine and Jannsen. We proof some important facts about this sheaf of rings. The last section deals with the connection between p-torsion W-modules and p-torsion syntomic sheaves. We show that there is a pair of adjoint functors. It is most important to note that the objects in chapter two and in this chapter are quite different although they might seem to be quite similar. The difference is that we required in chapter two the map φ to be a semi-linear isomorphism, while in this chapter we require the map to be semi-linear and bijective.

§1 φ-rings, φ-modules and φ-gauges

This sections contains the main definitions of the new objects introduced by Fontaine and Jannsen.

Graded modules. — A graded ring $R = \bigoplus_{r\in\mathbf{Z}} R^r$ is a commutative graded ring with graduation indexed by $\mathbf{Z}$. A *graded R-module M* is a module such that there is a decomposition into abelian groups $M = \bigoplus_{r\in\mathbf{Z}} M^r$ and it holds $R^s \cdot M^r \subset M^{s+r}$. A homomorphism of graded R-modules $f\colon M \to N$ is a homomorphism of modules in the usual sense such that $f(M^r) \subset N^r$. The category of graded R-modules is obviously R^0-linear and abelian.

Tensor product of graded modules. — Let R be a graded ring and M and N be graded R-modules. Under the canonical inclusion $R^0 \to R$ the modules M and N can be considered as R^0-modules. We set $(M \otimes_{R^0} N)^r := \bigoplus_{i+j=r} M^i \otimes_{R^0} N^j$ for $r \in \mathbf{Z}$ and denote by $L^r \subset (M \otimes_{R^0} N)^r$ the subgroup generated by $\lambda x \otimes y - x \otimes \lambda y$ for $\lambda \in R^k$, $x \in M^l$ and $y \in N^s$ with $k + l + s = r$. By the construction of a tensor product we have

$$M \otimes_R N = \bigoplus_{r\in\mathbf{Z}} (M \otimes_R N)^r$$

with $(M \otimes_R N)^r = (M \otimes_{R^0} N)^r / L^r$ (see [Bou07a, Chap. III, §4 No. 8]).

Tate twists. — Let $i \in \mathbf{N}$ be an integer. For a graded R-module M we define the *i-th Tate twist* of M to be the graded R-module $M(i)$ with $M(i)^r := M^{i+r}$. The functor $M \mapsto M(1)$ from the category of graded R-modules to itself is an equivalence of categories with quasi-inverse given by $N \mapsto N(-1)$. We have the following rules:

- $M(0) = M$;
- $M(i)(j) = M(i+j)$ for all $i, j \in \mathbf{Z}$;
- $M(i) \cong R(i) \otimes_R M$ for all $i \in \mathbf{Z}$.

Definition 5.1.1. — A graded R-module M is called *free of rank* 1, if there is an isomorphism $M \cong R(i)$ of graded R-modules for some $i \in \mathbf{Z}$. A graded R-module is called *free*, if it is isomorphic to a direct some of free graded R-modules of rank 1.

φ-rings. — Let $R = \bigoplus_{r \in \mathbf{Z}} R^r$ be a $\mathbf{Z}$-graded commutative ring and $f \in R^1$ and $v \in R^{-1}$ be two homogeneous elements. We set

$$R^{+\infty} := R/(f-1) \quad \text{and} \quad R^{-\infty} := R/(v-1).$$

This notation is justified by the simple fact that we have a canonical isomorphism of R^0-modules

$$R^{+\infty} \cong \varinjlim_{r \mapsto +\infty} R^r \quad \text{and} \quad R^{-\infty} \cong \varinjlim_{r \mapsto -\infty} R^r,$$

where the transition maps are given by $f\colon R^r \to R^{r+1}$ and $v\colon R^r \to R^{r-1}$, respectively.

Definition 5.1.2. — A *φ-ring* is a quadruple (R, f, v, φ), where R is a $\mathbf{Z}$-graded commutative ring, $f \in R^1$ and $v \in R^{-1}$ are homogeneous elements and $\varphi\colon R^{+\infty} \to R^{-\infty}$ is an isomorphism of rings.

The following example of a φ-ring is one of the most important examples and will be treated in detail in section 3. Section 2 is devoted to the construction of another fundamental example of a φ-ring.

Example 5.1.3. — Let k be a perfect field of characteristic $p > 0$ and W be the ring of Witt vectors of k. We set $R := W[S,T]/(ST - p)$, where S is an indetermined in degree 1 and T is an indetermined in degree −1. Let f be the image of S in R and v be the image of T in R. Then R is a $\mathbf{Z}$-graded ring with $R^0 = W$, $f \in R^1$, $v \in R^{-1}$ and $fv = vf = p$. Since p-multiplication is injective in W, we see from the relation of f and v that multiplication with f respectively v is injective. Hence we get identifications $R/(f-1) \cong W$ and $R/(v-1) \cong W$ as W-modules. Using this identification, we get the structure of a φ-ring by letting $\varphi\colon R^{+\infty} \to R^{-\infty}$ be the Frobenius on W, which is a ring isomorphism since k is assumed to be perfect. Replacing k by any perfect ring yields obviously also an example of a φ-ring. ◂

φ-modules. — Let (R, f, v, φ) be a φ-ring. To avoid confusion we will denote the map $\varphi\colon R^{+\infty} \to R^{-\infty}$ by φ_R in the sequel. For a $\mathbf{Z}$-graded R-module M we can consider the $R^{+\infty}$-module $M^{+\infty}$ and $R^{-\infty}$-module $M^{-\infty}$, where

$$M^{+\infty} := R^{+\infty} \otimes_R M \quad \text{and} \quad M^{-\infty} := R^{-\infty} \otimes_R M.$$

Here, $R^{+\infty}$ is considered as R-module via the canonical map $R \to R/(f-1)$ and similarly for $R^{-\infty}$. Hence, we may also write

$$M^{+\infty} = M/(f-1)M \quad \text{and} \quad M^{-\infty} = M/(v-1)M.$$

As R^0-modules we get also an identification

$$M^{+\infty} \cong \varinjlim_{r \mapsto +\infty} M^r \quad \text{and} \quad M^{-\infty} \cong \varinjlim_{r \mapsto -\infty} M^r.$$

Definition 5.1.4. — A *φ-R-module* is a pair (M, φ_M), where M is a $\mathbf{Z}$-graded R-module and $\varphi_M\colon M^{+\infty} \to M^{-\infty}$ is a homomorphism of groups such that

$$\varphi_M(\lambda m) = \varphi_R(\lambda)\varphi_M(m)$$

for $\lambda \in R^{+\infty}$ and $m \in M^{+\infty}$.

We define a morphism of φ-R-modules $\alpha\colon (M, \varphi_M) \to (N, \varphi_N)$ to be a morphism of graded R-modules $\alpha\colon M \to N$ (i.e. $\alpha(M^r) \subset N^r$ for all $r \in \mathbf{Z}$) such that for $\alpha^{+\infty} := \mathrm{id}_{R^{+\infty}} \otimes \alpha\colon R^{+\infty} \otimes_R M \to R^{+\infty} \otimes_R N$ and $\alpha^{-\infty} := \mathrm{id}_{R^{-\infty}} \otimes \alpha$ the induced diagram

$$\begin{tikzcd} M^{+\infty} \arrow[r, "\alpha^{+\infty}"] \arrow[d, "\varphi_M"'] & N^{+\infty} \arrow[d, "\varphi_N"] \\ M^{-\infty} \arrow[r, "\alpha^{-\infty}"] & N^{-\infty} \end{tikzcd}$$

commutes. Here, $\alpha^{+\infty}$ is a morphism of $R^{+\infty}$-modules and $\alpha^{-\infty}$ is a morphism of $R^{-\infty}$-modules. With these definitions we get a category $\mathcal{M}(R, f, v, \varphi)$ of φ-R-modules over the φ-ring (R, f, v, φ).

Lemma 5.1.5. — *The category $\mathcal{M}(R, f, v, \varphi)$ is abelian.*

Proof. — Let (M, φ_M) and (N, φ_N) be two φ-modules. The direct sum is given by $(M \oplus N, \varphi_M \oplus \varphi_N)$ and is easily seen to satisfy the universal property of a direct sum in $\mathcal{M}(R, f, v, \varphi)$. Let $\alpha\colon (M, \varphi_M) \to (N, \varphi_N)$ be a morphism of φ-R-modules. Let $K := \ker(\alpha)$ be the kernel of $\alpha\colon M \to N$ in the category of R-modules. Then obviously K is again a $\mathbf{Z}$-graded R-module. For each $r \in \mathbf{Z}$ we have an exact sequence of R^0-modules (and thus of the underlying abelian groups, which suffices for exactness questions)

$$0 \longrightarrow K^r \longrightarrow M^r \xrightarrow{\alpha} N^r$$

and taking the direct limit, which is an exact functor, yields the commutative diagram (of abelian groups) with exact rows

$$\begin{tikzcd} 0 \arrow[r] & K^{+\infty} \arrow[r] \arrow[d, dashed, "\varphi_K"] & M^{+\infty} \arrow[r, "\alpha^{+\infty}"] \arrow[d, "\varphi_M"] & N^{+\infty} \arrow[d, "\varphi_N"] \\ 0 \arrow[r] & K^{-\infty} \arrow[r] & M^{-\infty} \arrow[r, "\alpha^{-\infty}"] & N^{-\infty} \end{tikzcd}$$

A trivial diagram chase now shows that this gives a map $\varphi_K\colon K^{+\infty} \to K^{-\infty}$ with the desired properties. The existence of cokernels is even easier to prove. ∎

φ-gauges. — Again, (R, f, v, φ) denotes a φ-ring.

Definition 5.1.6. — A *φ-R-gauge* is a φ-R-module (M, φ_M) such that

$$\varphi_M \colon M^{+\infty} \to M^{-\infty}$$

is an isomorphism of groups.

A morphism of φ-R-gauges is just a morphism of φ-R-modules. We denote the category of φ-R-gauges by $\mathcal{G}(R, f, v, \varphi)$. This is by definition a full subcategory of $\mathcal{M}(R, f, v, \varphi)$.

Proposition 5.1.7. — *The category $\mathcal{G}(R, f, v, \varphi)$ is abelian.*

Proof. — We show that $\mathcal{G}(R, f, v, \varphi)$ is stable under forming kernels. The other properties are proved similarly. So let $\alpha \colon (M, \varphi_M) \to (N, \varphi_N)$ be a morphism of φ-R-gauges and (K, φ_K) be the kernel of α in the category of φ-R-modules. We must show that (K, φ_K) is actually a φ-R-gauge, i.e. the φ_R-linear map $\varphi_K \colon K^{+\infty} \to K^{-\infty}$ is an isomorphism of groups. But since φ_M and φ_N are isomorphisms of abelian groups, the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & K^{+\infty} \arrow[r] \arrow[d, dashed, "\varphi_K"] & M^{+\infty} \arrow[r, "\alpha^{+\infty}"] \arrow[d, "\varphi_M"] & N^{+\infty} \arrow[d, "\varphi_N"] \\
0 \arrow[r] & K^{-\infty} \arrow[r] & M^{-\infty} \arrow[r, "\alpha^{-\infty}"] & N^{-\infty}
\end{tikzcd}$$

implies that φ_K is also an isomorphism of abelian groups. ∎

Tensor product and Tate twists. — If (M, φ_M) and (N, φ_N) are two φ-R-modules, we have

$$(M \otimes_R N)^{+\infty} = M^{+\infty} \otimes_{R^{+\infty}} N^{+\infty} \quad \text{and} \quad (M \otimes_R N)^{-\infty} = M^{-\infty} \otimes_{R^{-\infty}} N^{-\infty}$$

and thus $\varphi_M \otimes \varphi_N$ endows $M \otimes_R N$ with the structure of a φ-R-module. If (M, φ_M) and (N, φ_N) are even φ-R-gauges, then $M \otimes_R N$ is also a φ-R-gauge.
Since it holds $M(i)^{+\infty} = M^{+\infty}$ and $M(i)^{-\infty} = M^{-\infty}$ for all $i \in \mathbf{Z}$, we can extend the definition of Tate twists to φ-R-modules and φ-R-gauges.

§2 The φ-ring $\mathscr{G}_n$

We consider the small syntomic site over k with associated topos $(\operatorname{Spec} k)_{syn}$. The sheaves $\mathscr{O}_n^{cris}$ are flat W_n-modules and we have the exact sequence (see corollary 4.3.24)

$$0 \longrightarrow \mathscr{O}_m^{cris} \xrightarrow{\pi} \mathscr{O}_{m+n}^{cris} \xrightarrow{v} \mathscr{O}_n^{cris} \longrightarrow 0,$$

This sequence will be called the *fundamental exact sequence* in the sequel. The goal is to construct a graded sheaf of rings $\mathscr{G}_n$ on $(\operatorname{Spec} k)_{syn}$ for each $n \in \mathbf{N}$. Therefor, let $r \in \mathbf{Z}$. If $r \leq 0$ we set

$$\mathscr{G}_n^r := \mathscr{O}_n^{cris}.$$

The subring $\bigoplus_{r\leq 0}\mathcal{G}_n^r$ is just the polynomial ring in one variable v with coefficients in $\mathcal{O}_n^{cris}$, i.e. for each syntomic k-scheme X the sheaf $\mathcal{G}_n^r(X)$ is a free $\mathcal{O}_n^{cris}(X)$-module of rank one with basis v^{-r}. The isomorphism is given by

$$\mathcal{O}_n^{cris} \ni 1 \longmapsto v^{-r} \in \mathcal{G}_n^r.$$

Under this identification, v may be identified with the section $1 \in \mathcal{O}_n^{cris} = \mathcal{G}_n^{-1}$. The degree of v is therefore -1.
Now let $m, r \in \mathbf{N}$ with $m \geq r$ and set

$$\widehat{\mathcal{G}}_m^r := \ker\left(\mathcal{O}_m^{cris} \xrightarrow{\varphi} \mathcal{O}_m^{cris} \xrightarrow{v} \mathcal{O}_r^{cris}\right).$$

Lemma 5.2.8. — *Let X be a syntomic k-scheme and $a \in \widehat{\mathcal{G}}_m^r(X)$ be a section. Then there is a syntomic covering $\{U_i \to X\}$ and sections $b_i \in \mathcal{O}_m^{cris}(U_i)$ such that $\mathrm{res}_{U_i,X}(a) = p^r b_i$.*

Proof. — By definition of $\widehat{\mathcal{G}}_m^r$ we have $\varphi(x) \in \ker(v)$. The fundamental exact sequence implies $\ker(v) = \mathrm{im}(\pi)$ and we know that $\mathrm{im}(\pi) = \mathrm{im}(p^m\colon \mathcal{O}_m^{cris} \to \mathcal{O}_m^{cris})$. This gives by the very definition of the image sheaf the lemma. ∎

Informally, the lemma just says that $\widehat{\mathcal{G}}_m^r$ is the set of section of $\mathcal{O}_m^{cris}$, for which the Frobenius is locally (for our topology) divisible by p^r:

$$\widehat{\mathcal{G}}_m^r = \left\{a \in \mathcal{O}_m^{cris} \mid \varphi(a) \in p^r\mathcal{O}_m^{cris}\right\}$$

Since for fixed r the sheaves $\widehat{\mathcal{G}}_m^r$ depend on m, we fix $n \in \mathbf{N}$ and define for $m \geq n + r$

$$\mathcal{G}_n^r := \mathrm{coker}\left(\widehat{\mathcal{G}}_m^r \xrightarrow{p^n} \widehat{\mathcal{G}}_m^r\right).$$

This is easily seen to be independent of m.

Lemma 5.2.9. — *Let $n, r \in \mathbf{N}$. The definition of*

$$\mathcal{G}_n^r = \mathrm{coker}\left(\widehat{\mathcal{G}}_m^r \xrightarrow{p^n} \widehat{\mathcal{G}}_m^r\right)$$

does not depend on $m \geq n + r$.

Proof. — First note that $\mathcal{G}_n^r = \widehat{\mathcal{G}}_m^r \otimes_{W_m} W_m/p^n$ by flatness of $\mathcal{O}_m^{cris}$. Now let $s \geq r$ be an integer. It obviously holds $p^{n+r}\mathcal{O}_{n+s}^{cris} \subset \widehat{\mathcal{G}}_{n+s}^r$ and we have an exact sequence

$$\mathcal{O}_{n+s}^{cris} \xrightarrow{p^{n+r}} \mathcal{O}_{n+s}^{cris} \longrightarrow \mathcal{O}_{n+r}^{cris} \longrightarrow 0.$$

These two facts yield the exact sequence of W_{n+s}-modules

$$\mathcal{O}_{n+s}^{cris} \xrightarrow{p^{n+r}} \widehat{\mathcal{G}}_{n+s}^r \longrightarrow \widehat{\mathcal{G}}_{n+r}^r \longrightarrow 0.$$

Applying $-\otimes_{W_{n+s}} W_{n+s}/p^n$ to this sequence and noting that $p^{n+r}\mathcal{O}_{n+s}^{cris} \subset p^n \cdot p^r\mathcal{O}_{n+s}^{cris} \subset p^n\widehat{\mathcal{G}}_{n+r}^r$ we finally obtain the isomorphism

$$\widehat{\mathcal{G}}_{n+s}^r \otimes_{W_{n+s}} W_{n+s}/p^n \cong \widehat{\mathcal{G}}_{n+r}^r \otimes_{W_{n+s}} W_{n+s}/p^n.$$ ∎

The next step is to define a ring structure on $\bigoplus_{r\in\mathbf{Z}}\mathscr{G}_n^r$. So let X be a syntomic k-scheme and $n,m,r,s\in\mathbf{N}$ with $m\geq\max\{n,r+s\}$. For $a\in\widehat{\mathscr{G}}_m^r(X)$ and $b\in\widehat{\mathscr{G}}_m^s(X)$ it holds: Locally $\varphi(a)$ is divisible by p^r and $\varphi(b)$ by p^s. Hence we might find a covering of X such that ab restricted to each member of this covering is divisible by p^{r+s}, i.e. $ab\in\widehat{\mathscr{G}}_m^{r+s}(X)$. By going to the quotient modulo p^n we get a well-defined multiplication $\mathscr{G}_n^r\times\mathscr{G}_n^s\to\mathscr{G}_n^{r+s}$. For negative s the same as just said applies with the only difference that b need not be divisible by p, which does not matter, since the degree drops and the product is divisible by p^r since a is. Because multiplication in $\mathscr{O}_m^{cris}$ is commutative the same is true with r and s interchanged. It remains only to define multiplication with $v:\mathscr{G}_n^r\to\mathscr{G}_n^{r-1}$ for $r\geq 1$: It is induced by the inclusion $\widehat{\mathscr{G}}_m^r\subset\widehat{\mathscr{G}}_m^{r-1}$. For $r\leq 0$ multiplication has already been defined above. Summing up, we have constructed a graded sheaf of rings

$$\mathscr{G}_n:=\bigoplus_{r\in\mathbf{Z}}\mathscr{G}_n^r$$

on $(\operatorname{Spec}k)_{syn}$.

Proposition 5.2.10. — *For all $n\in\mathbf{N}$ the sheaf $\mathscr{G}_n^r$ is flat over W_n for any $r\in\mathbf{N}$.*

Proof. — It is enough to show that the map $\mathscr{G}_m^r\to\mathscr{G}_n^r$ induced by $p^{n-m}:\mathscr{G}_n^r\to\mathscr{G}_n^r$ is injective for $0\leq m\leq n$. We have the exact sequence

$$\mathscr{O}_{n+r}^{\text{cris}}\xrightarrow{p^{m+r}}\mathscr{O}_{n+r}^{\text{cris}}\xrightarrow{p^{n-m}}\mathscr{O}_{n+r}^{\text{cris}},$$

which yields the exact sequence

$$\mathscr{O}_{n+r}^{\text{cris}}\xrightarrow{p^{m+r}}\widehat{\mathscr{G}}_{n+r}^r\xrightarrow{p^{n-m}}\widehat{\mathscr{G}}_{n+r}^r$$

since $p^{m+r}\mathscr{O}_{n+r}^{\text{cris}}\subset\widehat{\mathscr{G}}_{n+r}^r$. Moreover, it holds

$$p^{m+r}\mathscr{O}_{n+r}^{\text{cris}}\subset p^m\cdot p^r\mathscr{O}_{n+r}^{\text{cris}}\subset p^m\widehat{\mathscr{G}}_{n+r}^r$$

and this implies that the map $\mathscr{G}_m^r\to\mathscr{G}_n^r$ induced by $p^{n-m}:\mathscr{G}_n^r\to\mathscr{G}_n^r$ is injective. ∎

Corollary 5.2.11. — *There is for all $m,n\in\mathbf{N}$ an exact sequence*

$$0\longrightarrow\mathscr{G}_m\xrightarrow{\pi}\mathscr{G}_{m+n}\xrightarrow{v}\mathscr{G}_n\longrightarrow 0.$$

In order to get on $\mathscr{G}_n$ the structure of a φ-ring, we have to define the global sections $f\in\mathscr{G}_n^1(k)$ and $v\in\mathscr{G}_n^{-1}(k)=\mathscr{O}_n^{\text{cris}}(k)$ and a morphism of sheaves of rings

$$\varphi:\mathscr{G}_n^{+\infty}\longrightarrow\mathscr{G}_n^{-\infty}.$$

The section v has already been constructed above. For all $m\in\mathbf{N}$ we have $\mathscr{O}_m^{\text{cris}}(k)=W_m$ and $p\in W_m$. For $n\in\mathbf{N}$ and $m\geq n+1$ the image of p belongs to $\widehat{\mathscr{G}}_m^1(k)$ and we define f as the image of p in $\mathscr{G}_n^1(k)$. Then we have $fv=vf=p$. Now we define the map φ: By construction we have $\mathscr{G}_n^{-\infty}=\mathscr{O}_n^{\text{cris}}$. Let $r\in\mathbf{N}$ and U be a syntomic k-scheme. For $x\in\mathscr{G}_n^r(U)=\left(\widehat{\mathscr{G}}_m^r\,/\,p^n\widehat{\mathscr{G}}_m^r\right)(U)$ and some $m\geq n+r$ there is a syntomic U-scheme V and a $y\in\widehat{\mathscr{G}}_m^r(V)$ such that $x|_V=\bar{y}$, where $\bar{y}\equiv y \bmod p^n$. Moreover, we can find a syntomic V-scheme W and a $z\in\mathscr{O}_m^{\text{cris}}(W)$ such that $\varphi_{\mathscr{O}_m^{\text{cris}}}(y|_W)=p^rz$. The existance of such coverings follows by unwinding the definitions. Let $z'\in\mathscr{O}_n^{\text{cris}}(W)$ be the image of $z\in\mathscr{O}_m^{\text{cris}}(W)$ under the map $v:\mathscr{O}_m^{\text{cris}}\to\mathscr{O}_n^{\text{cris}}$.

Lemma 5.2.12. — *The element $z' \in \mathscr{O}_n^{\mathrm{cris}}(W)$ is independent of all choices made.*

Proof. — *Step 1:* It follows from lemma 5.2.9 that z' is independent of $m \geq n + r$.
Step 2: We show that z' is independent of $y \in \widehat{\mathscr{G}}_m^r(V)$. Choosing $y_1, y_2 \in \widehat{\mathscr{G}}_m^r(V)$ such that $\bar{y}_1 = x|_V = \bar{y}_2$ means that $y_1 = y_2 + p^n a$ for some $a \in \widehat{\mathscr{G}}_m^r(V)$. Then

$$\varphi(y_1|_W) = \varphi(y_2|_W) + p^n \varphi(a|_W)$$

and we see that $\varphi(y_1|_W) \equiv \varphi(y_2|_W) \bmod p^n$.
Step 3: Let V_1 and V_2 two syntomic U-schemes with the required properties. Then $V_1 \coprod V_2$ is a common refinement and we may assume that V_2 is a syntomic V_1-scheme. Since $x|_{V_2} = (x|_{V_1})|_{V_2}$ we get the independence of the chosen coverings. A similar argument shows the indepence of W. ■

Since z' is independent of all choices, it follows that z' actually belongs to $\mathscr{O}_n^{\mathrm{cris}}(U)$ for $x \in \mathscr{G}_n^r(U)$. In this way we obtain a map $\phi_r : \mathscr{G}_n^r \to \mathscr{O}_n^{\mathrm{cris}}$ by $x \mapsto z'$. For $x \in \mathscr{G}_n^r$ it obviously holds $\phi_r(x) = \phi_{r+1}(fx)$. Thus, these maps ϕ_r induces a map

$$\varphi : \varinjlim_{f} \mathscr{G}_n^r \longrightarrow \mathscr{O}_n^{\mathrm{cris}}$$

and we are done. The main theorem will be proved in a forthcomming paper by Fontaine and Jannsen.

Theorem 5.2.13. — *The map $\varphi : \mathscr{G}_n^{+\infty} \to \mathscr{G}_n^{-\infty}$ is an isomorphism of rings.*

With this theorem the construction of the φ-ring $\mathscr{G}_n$ is complete.

§3 φ-Gauges over perfect fields

Now k is a perfect field of characteristic $p > 0$ and W the ring of Witt vectors of k. For a natural number $n \in \mathbf{N}$ the ring of Witt vectors of length n is as usual denoted by W_n. We will compute the global sections of the sheaf $\mathscr{G}_n$ over $\operatorname{Spec} k$. We already know that $\mathscr{O}_n^{\mathrm{cris}}(\operatorname{Spec} k) \cong W_n$ by corollary 4.2.15. This is an isomorphism of W_n-algebra, but we are only interested in it as an isomorphism of rings. By construction we have

$$\widehat{\mathscr{G}}_m^r := \ker\left(\mathscr{O}_m^{cris} \xrightarrow{\varphi} \mathscr{O}_m^{cris} \xrightarrow{v} \mathscr{O}_r^{cris}\right)$$

for $m, r \in \mathbf{N}$ with $m \geq r$. Since the Frobenius is an automorphism of W_n we obtain

$$\widehat{\mathscr{G}}_m^r(\operatorname{Spec} k) \cong W_{m-r}.$$

Using $W_{m-r}/p^n \cong W_n$ for $n \leq m - r$ it follows immediately

$$\mathscr{G}_n^r(\operatorname{Spec} k) \cong W_n.$$

Under this identification the map $\varphi : \mathscr{G}_n^{+\infty} \to \mathscr{G}_n^{-\infty}$ is just the usual Frobenius on W_n. So we are led to consider the following φ-ring D.

φ-W-**Gauges**. — Consider the graded ring $W[S,T]$, where $\deg S = 1$ and $\deg T = -1$. The ideal $(ST - p)$ is homogenous and we get a graded ring $D := W[S,T]/(ST-p)$. The images of S and T are denoted by f and v respectively. Sometimes we may also write $D = W[f,v]$, where $\deg f = 1$, $\deg v = -1$ and $fv = vf = p$. We turn D into a φ-ring by observing $D^{+\infty} = D^{-\infty} = W$ and defining the map $\varphi\colon W \to W$ to be the Frobenius, which is an isomorphism of rings, since k is perfect.

Definition 5.3.14. — A *D-module* is a finitely generated graded module over D.

Let $M = \bigoplus_{r\in\mathbf{Z}} M^r$ be a D-module. Then we may view M as a diagram

$$\cdots \underset{v_{r-1}}{\overset{f_{r-2}}{\rightleftarrows}} M^{r-1} \underset{v_r}{\overset{f_{r-1}}{\rightleftarrows}} M^r \underset{v_{r+1}}{\overset{f_r}{\rightleftarrows}} M^{r+1} \underset{v_{r+2}}{\overset{f_{r+1}}{\rightleftarrows}} \cdots,$$

where $f_r\colon M^r \to M^{r+1}$ is the map induced by $m \mapsto f\cdot m$ and analogously for v_r. Moreover, we must have $v_{r+1}\circ f_r = f_{r-1}\circ v_r = p$ for all $r \in \mathbf{Z}$. Since M is assumed to be finitely generated, we may choose generators $m_1,\dots,m_s$ and assume without lost of generality that m_i is homogeneous of degree d_i. Then there is a surjection $\bigoplus_{i=1}^s D(-d_i) \to M$ mapping 1 in $D(-d_i)$ to m_i. Let $n_1,\dots,n_l$ be homogeneous generators of the kernel of this map. Then for $r \geq \max\{\deg n_i, d_j \mid 1\leq i\leq l, 1\leq j\leq s\}$ the maps f_r are isomorphisms and for $r \leq \min\{-\deg n_i, -d_j \mid 1\leq i\leq l, 1\leq j\leq s\}$ the maps v_r are isomorphisms. Thus, a D-module can actually be viewed as a finite diagram

$$M^a \underset{v_{a-1}}{\overset{f_a}{\rightleftarrows}} \cdots \underset{v_{r-1}}{\overset{f_{r-2}}{\rightleftarrows}} M^{r-1} \underset{v_r}{\overset{f_{r-1}}{\rightleftarrows}} M^r \underset{v_{r+1}}{\overset{f_r}{\rightleftarrows}} M^{r+1} \underset{v_{r+2}}{\overset{f_{r+1}}{\rightleftarrows}} \cdots \underset{v_b}{\overset{f_{b-1}}{\rightleftarrows}} M^b,$$

since we have $f_{r-1} = p\cdot v_r^{-1}$ for $r \leq a$ and $v_{r+1} = p\cdot f_r^{-1}$ for $r \geq b$ und hence there is no new information in these degrees.

Definition 5.3.15. — A D-module is called *effective*, if it can be given by a finite diagram as above with $a \geq 0$.

For a W-algebra A we introduce the following D-module $A(-i)$:

$$\begin{array}{ccccccccc} \deg: & & i-1 & & i & & i+1 & & \\ \cdots & \underset{=}{\overset{p}{\rightleftarrows}} & A & \underset{=}{\overset{p}{\rightleftarrows}} & A & \underset{p}{\overset{=}{\rightleftarrows}} & A & \underset{p}{\overset{=}{\rightleftarrows}} & \cdots \end{array}$$

Here, p denotes multiplication by p.

Definition 5.3.16. — A D-module M is called *free*, if $M \simeq \bigoplus_{i=0}^d D(-d_i)$ for some $d_i \in \mathbf{Z}$.

The proof of the next lemma is easy and left to the reader.

Lemma 5.3.17. — *Let $M = \bigoplus_{i=0}^d W(-d_i)$ be a D-module for some $d_i \in \mathbf{Z}$.*

(i) M is a free D-module isomorphic to $\bigoplus_{i=0}^d D(-d_i)$.

(ii) M is effective, if and only if $d_i \geq 0$ for all $i = 0,\dots,d$.

For the convenience of the reader we give the definition of a φ-modules and a φ-gauge in this context, since we use a slightly different terminology compared with the general setting.

Definition 5.3.18. —

(i) A *φ-W-module M* is a D-module together with a σ-linear map $\varphi\colon M^{+\infty} \to M^{-\infty}$.

(ii) A *φ-W-gauge M* is a φ-W-module such that the induced map

$$\varphi\colon M^{+\infty} \longrightarrow M^{-\infty}$$

is an isomorphism of groups.

Remark 5.3.19. — By lemma 1.2.15 we know that in this special case, a σ-linear bijective map is the same as a σ-linear isomorphism. ◁

We note that there are φ-W-gauges, which are equal as D-modules, but not as φ-W-gauges.

Example 5.3.20. — Let $M = D(0) \oplus D(0)$ be a free D-module with basis e_1, e_2. Let $\varphi_1\colon M^{+\infty} = We_1 \oplus We_2 \to M^{-\infty} = We_1 \oplus We_2$ be the idendity on the underlying abelian groups and let φ_2 be the map interchanging e_1 and e_2. We get two different W-gauges (M, φ_1) and (M, φ_2), which are equal as D-modules. ◂

We have seen in chapter 2 that to every F-crystal over k we can associate an φ-F-gauge over W. The last remak tells us that φ-F-gauges are the same as φ-W-gauges. But one has to be very careful, since in general these two notions are different.
Let $\mathfrak{C}$ be the functor from chapter 2, which assigns to an F-crystal over k a φ-W-gauge.

Proposition 5.3.21. — *Let (M, ϕ) be an F-crystal over k. Then the φ-W-gauge $\mathfrak{C}(M, \phi)$ is free as D-module.*

Proof. — Since W is a discrete valuation ring with maximal ideal (p), the theory of elementary divisors apply and we can choose a W-basis $e_1^1, \dots, e_{n_1}^1, \dots, e_1^s, \dots, e_{n_s}^s$ of $M^{(F)}$ and a W-basis $f_1^1, \dots, f_{n_1}^1, \dots, f_1^s, \dots, f_{n_s}^s$ of M such that $\Phi^\sharp$ is given with respect to these bases by the diagonal matrix

$$\begin{pmatrix} p^{d_1} \cdot I_{n_1} & & \\ & \ddots & \\ & & p^{d_s} \cdot I_{n_s} \end{pmatrix},$$

where I_n is the idendity matrix of rank n and $d_i \in \mathbf{Z}$ with $d_i < d_j$ for $i < j$. It follows that we can write

$$M^r = \begin{cases} \bigoplus_{j=1}^s \bigoplus_{i=1}^{n_j} W^{(F)} e_i^j, & \text{for } r < d_1, \\ \bigoplus_{j=1}^s \bigoplus_{i=1}^{n_j} p^{\max\{p^{r-d_j},0\}} W^{(F)} e_i^j, & \text{for } r \geq d_1. \end{cases}$$

Fix j for the moment and consider for $r > d_j$ the W-module

$$\bigoplus_{i=1}^{n_j} p^{r-d_j} W^{(F)} e_i^j.$$

We have an isomorphism

$$\bigoplus_{i=1}^{n_j} W^{(F)} e_i^j \to \bigoplus_{i=1}^{n_j} p^{r-d_j} W^{(F)} e_i^j$$

induced by p-multiplication. Using these isomorphisms, it is easily seen that the gauge $\mathfrak{Ig}(M,\Phi)$ is as D-module isomorphic to

$$\bigoplus_{j=1}^{s} \bigoplus_{i=1}^{n_j} W^{(F)}(-d_j).$$

Freeness follows from Lemma 5.3.17. ∎

Reduction of φ-W-gauges. — Given a φ-W-gauge M and an integer $n \in \mathbf{N}$, we consider the graded D-module $\overline{M} := M/p^n := \bigoplus_{r\in\mathbf{Z}} M^r/p^n M^r$. The maps $\overline{f}_r$ and $\overline{v}_r$ are the induced ones. Since $\varinjlim$ commutes with $\otimes$, we have $\overline{M}^{-\infty} = M^{-\infty}/p^n M^{-\infty}$ and $\overline{M}^{+\infty} = M^{+\infty}/p^n M^{+\infty}$. Hence the σ-linear isomorphism φ induces a σ-linear isomorphism $\overline{\varphi}\colon \overline{M}^{-\infty} \to \overline{M}^{+\infty}$. This is an isomorphism of $W_n := W/p^n$-modules. Let us denote by D_n the reduction of D modulo p^n. Then we can define D_n-modules and φ-W_n-gauges just analogously to D-modules and φ-W-gauges. Our discussion shows that the reduction of a φ-W-gauge M modulo p^n yields a φ-W_n-gauge $\overline{M}$.

***Example* 5.3.22.** — Consider the σ-W-gauge $W(-i)$. The reduction modulo p^n is then the gauge

$$\begin{array}{cccccccc} \deg: & & i-1 & & i & & i+1 & \\ \cdots & \underset{=}{\overset{p}{\rightleftarrows}} & W_n & \underset{=}{\overset{p}{\rightleftarrows}} & W_n & \underset{p}{\overset{=}{\rightleftarrows}} & W_n & \underset{p}{\overset{=}{\rightleftarrows}} \cdots \end{array}$$

where p denotes the map given by $1 \mapsto p\cdot 1$. This gauge is denoted by $W_n(-i)$. ◂

***Remark* 5.3.23.** — In the above example, the map p is actually the same as p-multiplication. But in general one has to be carefull. For example consider the D-module

$$\cdots \underset{\supset}{\overset{p}{\rightleftarrows}} W \underset{\supset}{\overset{p}{\rightleftarrows}} pW \underset{\supset}{\overset{p}{\rightleftarrows}} p^2W \underset{\supset}{\overset{p}{\rightleftarrows}} \cdots$$

and reduce modulo p. We get

$$\cdots \underset{\supset}{\overset{p}{\rightleftarrows}} W/p \underset{\supset}{\overset{p}{\rightleftarrows}} pW/p^2 \underset{\supset}{\overset{p}{\rightleftarrows}} p^2W/p^3 \underset{\supset}{\overset{p}{\rightleftarrows}} \cdots$$

Now, the map $p\colon W/p \to pW/p^2$ is not multiplication by p (which is zero), but the map induced by p-multiplication on W, namely $1 \bmod p \mapsto p\cdot 1 \bmod p^2$. This is actually an isomorphism of W_1-modules. On the other hand, the map " $\supset$ ": $pW/p^2 \to W/p$ is the zero map. But this is exactly what one expects, since the given D-module is isomorphic to $W(-i)$ for some i and hence one exspects the reduction to be isomorphic to $W_n(-i)$. ◃

Rigid D_n-modules. — Fix an integer $n \in \mathbf{N}$.

Definition 5.3.24. —

(i) A D_n-module M is called *strict*, if the map

$$(f_r^\infty, v_r^\infty)\colon M^r \to M^{+\infty} \oplus M^{-\infty}$$

is injective for all $r \in \mathbf{Z}$.

(ii) A D_n-module M is called *quasi-rigid*, if

$$\ker(f_r^n) = \mathrm{im}(v_{r+n}^n) \quad \text{and} \quad \ker(v_r^n) = \mathrm{im}(f_{r-n}^n)$$

holds for all $r \in \mathbf{Z}$.

(iii) A D_n-module is called *rigid*, if it is strict and quasi-rigid.

Lemma 5.3.25. —

(i) If M is a strict D_n-module, then $\ker(f_r^n) = \ker(f_r^\infty)$ *and* $\ker(v_r^n) = \ker(v_r^\infty)$ *for all* $r \in \mathbf{Z}$.

(ii) A D_n-module M is strict, if and only if

$$\ker(f_r^n) \cap \ker(v_r^n) = 0$$

for all $r \in \mathbf{Z}$.

Proof. — (i) We clearly have $\ker(f_r^n) \subset \ker(f_r^\infty)$. Let $x \in \ker(f_r^\infty)$. Then

$$\begin{aligned}\big(f_{r+n}^\infty, v_{r+n}^\infty\big)\big(f_r^n(x)\big) &= \big(f_r^\infty(x), p^n v_r^\infty(x)\big)\\ &= 0,\end{aligned}$$

and hence $f_r^n(x) = 0$, for M is strict. The proof for v is similar.
(ii) By (i) neccessity is clear. For the converse we show that

$$\ker(f_r^{kn}) \cap \ker(v_r^{ln}) = 0$$

for all $k, l \in \mathbf{N}$. For $k = l = 1$ this is our assumption. Suppose, we have already shown that

$$\ker(f_r^{kn}) \cap \ker(v_r^n) = 0$$

for some $k \in \mathbf{N}$. Let $x \in \ker(f_r^{(k+1)n}) \cap \ker(v_r^n)$. Then

$$\big(f_{r+kn}^n, v_{r+kn}^n\big)\big(f_r^{kn}(x)\big) = 0$$

and thus $f_r^{kn}(x) = 0$ by assumption. This yields $x \in \ker(f_r^{kn}) \cap \ker(v_r^n) = 0$. Now fix $k \in \mathbf{N}$ and a similar induction over l shows

$$\ker(f_r^{kn}) \cap \ker(v_r^{ln}) = 0.$$

Since a D_n-module is by definition finitely generated, the maps f_r and v_{-r} are isomorphisms for $r \gg 0$. Thus, $\ker(f_r^\infty) = \ker(f_r^{kn})$ for $k \gg 0$ and $\ker(v_r^\infty) = \ker(v_r^{ln})$ for $l \gg 0$. ∎

Lemma 5.3.26. —

(i) If M is a strict D_n-module such that all M^r are free W_n-modules, then the reduction $M/p^s M$ is again a strict D_s-module for all $1 \le s \le n-1$.

(ii) If M is a quasi-rigid D_n-module, then the reduction $M/p^s M$ is a quasi-rigid D_s-module for all $1 \le s \le n-1$.

(iii) Let M be a quasi-rigid D_n-module. Then we have $\ell(M^r) = \ell(M^{r+1})$ for all $r \in \mathbf{Z}$, where $\ell(-)$ denotes the length of a W_n-module.

Proof. — (i) Let $r \in \mathbf{Z}$ and $x \in M^r$ with $f^s x = p^s y$ and $v^s x = p^s z$ for some $y \in M^{r+s}$ and $z \in M^{r-s}$. Then $f^n v^{n-s} x = f^s p^{n-s} x = 0$ and similarly $v^s p^{n-s} x = 0$. By strictness of M it follows $p^{n-s} x = 0$. But M^r is a free W_n-module and hence we must have $x = p^s a$ for some $a \in M^r$.
(ii) Let $r \in \mathbf{Z}$ and $x \in M^r$ with $f_r^s(x) = p^s y$ for some $y \in M^{r+s}$. Writing $p^s = f_r^s \circ v_{r+s}^s$ we get $f_r^s\big(x - v_{r+s}^s(y)\big) = 0$ and in particular $x - v_{r+s}^s(y) \in \ker(f_r^n)$, since $s \le n$. But M is quasi-rigid, so there is an $z \in M^{r+n}$ with $x - v_{r+s}^s(y) = v_{r+n}^n(z)$. This yields $x = v_{r+s}^s\big(y - v_{r+n}^{n-s}(z)\big)$.
(iii) For $r \in \mathbf{Z}$ there are by quasi-rigidity exact sequences

$$0 \longrightarrow \operatorname{im}(f_r^n) \longrightarrow M^{r+n} \longrightarrow \operatorname{im}(v_{r+n}^n) \longrightarrow 0$$

$$0 \longrightarrow \operatorname{im}(v_{r+n}^n) \longrightarrow M^{r} \longrightarrow \operatorname{im}(f_r^n) \longrightarrow 0$$

of W_n-modules. This implies by the additivity of the length

$$\ell\big(M^r\big) = \ell\big(M^{r+n}\big)$$

for all $r \in \mathbf{Z}$. But M is finitely generated as D_n-module. Hence it holds $M^r = M^{r+1}$ for $r \gg 0$, which gives the claim. ∎

Lifting φ-W-Gauges. — Let M be a φ-W-gauge, which is free as D-module. We claim that under one mild restriction there is an F-crystal $(\widetilde{M}, \phi)$ such that $\mathfrak{C}(\widetilde{M}, \Phi)$ is isomorphic to M as φ-W-gauge.

Definition 5.3.27. — A D-module M is called *strict*, if the reduction modulo p is strict.

***Example* 5.3.28.** — We consider the D-module

$$W \underset{p}{\overset{=}{\rightleftarrows}} W \underset{=}{\overset{p}{\rightleftarrows}} W$$

and its reduction mod p

$$k \underset{0}{\overset{=}{\rightleftarrows}} k \underset{=}{\overset{0}{\rightleftarrows}} k.$$

This D-module is not strict. ◂

Proposition 5.3.29. — *Every free D-module is strict.*

Proof. — The reduction of the D-module $W(-i)$ is

$$\begin{array}{ccccccccc} \deg: & & i-1 & & i & & i+1 & & \\ \cdots & \underset{=}{\overset{0}{\rightleftarrows}} & W_1 & \underset{=}{\overset{0}{\rightleftarrows}} & W_1 & \underset{0}{\overset{=}{\rightleftarrows}} & W_1 & \underset{0}{\overset{=}{\rightleftarrows}} & \cdots \end{array}$$

which is clearly strict. Since every free D-module is a finite direct sum of modules of the above type, the proposition follows. ■

We call a gauge strict, if the underlying module is strict.

Corollary 5.3.30. — *Let (M, ϕ) be an F-crystal over k. Then $\mathfrak{C}(M, \Phi)$ is a strict free φ-W-gauge.*

Proof. — We have already seen in Proposition 5.3.21 that $\mathfrak{C}(M, \phi)$ is free and hence the claim follows from the proposition. ■

The main theorem of this section is the following.

Theorem 5.3.31. — *Let M be a free φ-W-gauge. Then there is an F-rystal $(\widetilde{M}, \phi)$ such that $\mathfrak{C}(\widetilde{M}, \phi) = M$ as φ-W-gauge.*

Proof. — The W-module $M^{-\infty}$ is free and we define $\widetilde{M} := M_F^{-\infty}$. Since M is free as D-module, we can write

$$M = \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{n_j} W(-d_j).$$

In particular, $M^{-\infty}$ is a free W-module of rank $\sum_{j=1}^{s} n_j$. Choose a basis $e_1^1, \ldots, e_{n_1}^1, \ldots, e_1^s, \ldots, e_{n_s}^s$ of $M^{-\infty}$. Then, we let $\Phi(e_i^j) := p^{d_j}\varphi(e_i^j)$ be the Frobenius-linear injective map $\Phi\colon \widetilde{M} \to \widetilde{M} \otimes_F B$. This yields an isocrystal $(\widetilde{M}, \phi)$, and one verifies immediately that this F-crystal induces the given gauge. ■

We end this section by giving another characterization of free D-modules.

Lemma 5.3.32. — *Let M be a D-module such that each M^r is torsion free. Then the reduction mod p^n of M is quasi-rigid. In particular, the reduction of a free D-module is quasi-rigid.*

Proof. — Every torsion free module over a principal ideal domain is free. Thus, every M^r is a free W-module. Since p-multiplication is injective on free W-modules, we see that the maps f_r and v_r are all injective. We denote by $\overline{}$ the reduction map. Let $\overline{x} \in \ker(\overline{f}_r^n)$. This means that $f_r^n(x) \in p^n M^{r+n}$. Thus, there is a $y \in M^{r+n}$ such that $f_r^n(x) = p^n y$. This implies

$$f_r^n(x) = p^n y = f_r^n(v_{r+n}^n(y)),$$

and because of the injectivity of f_r we have $x = v_{r+n}^n(y)$, i.e. $\overline{x} \in \operatorname{im}(\overline{v}_{r+n}^n)$. The reverse inclusion $\operatorname{im}(\overline{v}_{r+n}^n) \subset \ker(\overline{f}_r^n)$ is clear. The equality $\ker(\overline{v}_{r+n}^n) = \operatorname{im}(\overline{f}_r^n)$ is shown similarly. ■

Theorem 5.3.33. — *A D-module M is free, if and only if M is strict and every M^r is torsionfree as W-module.*

Proof. — Neccessity is clear by Proposition 5.3.29. For the converse consider the reduction mod p of M. By our assumption, M/pM is strict and the above lemma implies that M/pM is actually rigid. By Lemma 5.3.26 all M^r a finite dimensional k-vector spaces of the same dimension. By strictness, we can write

$$M^r = \ker(f_r) \oplus \ker(v_r) \oplus B^r,$$

where B^r is zero for all but finite many $r \in \mathbf{Z}$, since M is finitely generated. Let $d_1, \cdots, d_s$ be these integers, for which $B^r \neq 0$. Letting $n_j := \dim B^{d_j}$, we have

$$M/pM \simeq \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{n_j} D_1(-d_j).$$

This can be lifted and we obtain

$$M \simeq \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{n_j} D(-d_j).$$

■

§4 The adjoint functors $\Gamma^*_{\mathscr{G}_n}$ and Γ_*

Again, k denotes a perfect field of characteristic $p > 0$ and W the ring of Witt vectors of k. We consider the topos $(\operatorname{Spec} k)_{\text{syn}}$ associated to the small syntomic site of $\operatorname{Spec} k$. The small Zariski site of $\operatorname{Spec} k$ gives the trivial topos. The morphism of topoi

$$\Gamma = (\Gamma_*, \Gamma^{-1}) \colon (\operatorname{Spec} k)_{\text{syn}} \longrightarrow (\operatorname{Spec} k)_{\text{Zar}}$$

can thus be described as follows: If $\mathscr{F}$ is an abelian sheaf on $\operatorname{syn}(\operatorname{Spec} k)$, then $\Gamma_*(\mathscr{F}) = \mathscr{F}(k)$ is an abelian group, and if M is any abelian group, then $\Gamma^{-1}(M)$ is the constant sheaf associated to M. Recall that we have $\mathscr{O}_n^{\text{cris}}(k) = W_n(k)$ by corollary 4.2.15.

Definition 5.4.34. — Let $\mathscr{R} = (\mathscr{R}_n)_{n\in\mathbf{N}}$ be a family of sheaves of rings on $(\operatorname{Spec} k)_{\text{syn}}$ such that for all $n \in \mathbf{N}$ we have an isomorphism of sheaves of rings $\mathscr{R}_{n+1}/p^n \cong \mathscr{R}_n$. Then $\mathscr{R}$ is called a *p-adic ring*.

***Example* 5.4.35.** — We know by the exact sequence in corollary 4.3.24 that $\mathscr{O}^{\text{cris}} = (\mathscr{O}_n^{\text{cris}})_{n\in\mathbf{N}}$ is a p-adic ring. Moreover, corollary 5.2.11 tells us that $\mathscr{G} = (\mathscr{G}_n)_{n\in\mathbf{N}}$ is also a p-adic ring. ◂

Definition 5.4.36. — Let $\mathscr{R} = (\mathscr{R}_n)_{n\in\mathbf{N}}$ be a p-adic ring on $(\operatorname{Spec} k)_{\text{syn}}$. Then $\mathscr{R}$ is called *flat*, if there is an exact sequence

$$\mathscr{R}_n \xrightarrow{p} \mathscr{R}_n \xrightarrow{p^{n-1}} \mathscr{R}_n$$

for all $n \in \mathbf{N}$.

***Example* 5.4.37.** — Corollary 4.3.24 tells us that $\mathscr{O}^{\text{cris}}$ is flat and proposition 5.2.10 tells us that $\mathscr{G}$ is flat. ◂

Definition 5.4.38. — Let $\mathscr{R} = (\mathscr{R}_n)_{n\in\mathbf{N}}$ be a p-adic ring on $(\operatorname{Spec}k)_{\mathrm{syn}}$. A *$p$-torsion $\mathscr{R}$-module* on $(\operatorname{Spec}k)_{\mathrm{syn}}$ is a p-torsion abelian sheaf $\mathscr{M}$ on $(\operatorname{Spec}k)_{\mathrm{syn}}$ such that for all $n\in\mathbf{N}$ the kernel of p^n-multiplication $\mathscr{M}_n$ has a structure of $\mathscr{R}_n$-module and the diagram

$$\begin{tikzcd} \mathscr{R}_{n+1}\times\mathscr{M}_{n+1} \arrow[r] \arrow[d] & \mathscr{M}_{n+1} \arrow[d] \\ \mathscr{R}_n\times\mathscr{M}_n \arrow[r] & \mathscr{M}_n \end{tikzcd}$$

commutes. A *morphism* of p-torsion $\mathscr{R}$-modules is a morphism of the underlying abelian sheaves, which satisfies the obvious compatibility conditions. The category of p-torsion $\mathscr{R}$-modules is denoted by $\mathcal{G}_{p-\mathrm{tor}}(\mathscr{R})$.

Since W is a discrete valuation ring with maximal ideal pW, torsion W-modules and p-torsion W-modules are the same in this case. Let M be a torsion W-module. Then we can write $M = \varinjlim_{n\in\mathbf{N}} M_n$. We want to associate a $\mathscr{O}^{\mathrm{cris}}$-module to M. First assume that M is killed by p^n for some $n\in\mathbf{N}$. Then $M = M_n$ and we set $\Gamma^*_{W_n}(M) = \Gamma^{-1}(M_n)\otimes_{W_n}\mathscr{O}^{\mathrm{cris}}_n$, i.e. the sheafification of the presheaf

$$U \longmapsto \Gamma^{-1}(M_n)\otimes_{W_n}\mathscr{O}^{\mathrm{cris}}_n(U).$$

Obviously, the functor $\Gamma^*_{W_n}$ is left adjoint to Γ_*, since this is true for the functor Γ^{-1} and the statement follows from that like in the classical case. Actually, if $\mathscr{M}$ is an $\mathscr{O}^{\mathrm{cris}}_n$-module, then $\Gamma_*(\mathscr{M}) = \mathscr{M}(\operatorname{Spec}k)$ is a W_n-module. For an arbitrary torsion W-module M we set

$$\Gamma^*_W(M) := \varinjlim_{n\in\mathbf{N}}\bigl(\Gamma^{-1}(M_n)\otimes_{W_n}\mathscr{O}^{\mathrm{cris}}_n\bigr).$$

Hence we get a functor $\Gamma^*_W\colon \mathcal{G}_{p-\mathrm{tor}}(W)\to\mathcal{G}_{p-\mathrm{tor}}(\mathscr{O}^{\mathrm{cris}})$. It is clear that the functor Γ^*_W is left adjoint to Γ_*.
Let $D = W[f,v]$ with the relation $fv = vf = p$ and the isomorphism of rings $D^{+\infty} = W \to W = D^{-\infty}$ given by the Frobenius on W. This is a φ-ring and by reduction we have the φ-rings $D_n = D/p^n$. The canonical isomorphism $D = \varprojlim_{n\in\mathbf{N}} D_n$ implies that D is a flat p-adic ring. If M is a D_n-module, we define $\Gamma^*_{D_n}(M) := \Gamma^{-1}(M)\otimes_{D_n}\mathscr{G}_n$, i.e. the sheafification of

$$U \longmapsto \Gamma^{-1}(M_n)\otimes_{D_n}\mathscr{G}_n(U).$$

The discussion above immediately shows that $\Gamma^*_{D_n}$ is left adjoint to Γ_*. Moreover, if $\mathscr{M}$ is a $\mathscr{G}_n$-module, then $\Gamma_*(\mathscr{M})$ is a D_n-module. If M is any p-torsion D-module, we can write $M = \varinjlim_{n\in\mathbf{N}} M_n$, where M_n is the kernel of p^n-multiplication on M, and set

$$\Gamma^*_D(M) := \varinjlim_{n\in\mathbf{N}}\bigl(\Gamma^{-1}(M_n)\otimes_{D_n}\mathscr{G}_n\bigr).$$

We finally obtain a functor

$$\Gamma^*_D\colon \mathcal{G}_{p-\mathrm{tor}}(D)\to\mathcal{G}_{p-\mathrm{tor}}(\mathscr{G}).$$

Theorem 5.4.39. — *The functor Γ^*_D is fully faithful. The restriction of the global section functor Γ_* to the essential image of Γ^*_D is a quasi-inverse.*

Proof. — Fix $n \in \mathbf{N}$. The adjointness of Γ_* and $\Gamma^*_{D_n}$ gives

$$\mathrm{Hom}_{\mathscr{G}_n}\big(\Gamma^*_{D_n}(M), \mathscr{N}\big) \xrightarrow{\simeq} \mathrm{Hom}_{D_n}\big(M, \Gamma_*(\mathscr{N})\big).$$

If $\mathscr{N}$ is in the essential image of $\Gamma^*_{D_n}$, then there exists a D_n-module N such that

$$\mathscr{N} \cong \Gamma^*_{D_n}(N).$$

By the construction of our functors Γ_* and $\Gamma^*_{D_n}$ and since $(\mathrm{Spec}\, k)_{\mathrm{Zar}}$ is trivial we have

$$\Gamma_*\big(\Gamma^*_{D_n}(N)\big) \cong N.$$

Using this together with the adjointness property yields an isomorphism

$$\mathrm{Hom}_{\mathscr{G}_n}\big(\Gamma^*_{D_n}(M), \Gamma^*_{D_n}(N)\big) \cong \mathrm{Hom}_{D_n}\big(M, N\big).$$

Taking the direct limit over all $n \in \mathbf{N}$ proves the theorem. ∎

Remark 5.4.40. — The proof of the theorem is actually a special case of the following formal fact about adjoint pairs: Let $\mathcal{C}$ and $\mathcal{D}$ be categories and let

$$\mathcal{C} \underset{R}{\overset{L}{\rightleftarrows}} \mathcal{D}$$

be a pair of adjoint functors, where L is left adjoint to R. Then there exists a morphism of functors

$$\varepsilon\colon \mathrm{id}_{\mathcal{C}} \longrightarrow R \circ L$$

called the unit of the adjunction. Then L is fully faithful if and only if $\varepsilon\colon R \circ L$ is an isomorphism (see [KS06, proposition 1.5.6 (ii)]). ◃

As an immediate consequence of the theorem we obtain the following corollary.

Corollary 5.4.41. —

(i) If M is a φ-module over D, then $\Gamma^*_D(M)$ is a φ-module over $\mathscr{G}$ and the restriction of Γ^*_D to φ-modules is fully faithful.

(ii) If M is a φ-gauge over D, then $\Gamma^*_D(M)$ is a φ-module over $\mathscr{G}$ and the restriction of Γ^*_D to φ-gauges is fully faithful.

Bibliography

[Bau92] W. Bauer – "On the conjecture of Birch and Swinnerton-Dyer for abelian varieties over function fields in characteristic $p > 0$", *Invent. Math.* **108** (1992), no. 2, p. 263–287.

[BBM82] P. Berthelot, L. Breen & W. Messing – *Théorie de Dieudonné cristalline. II*, Lecture Notes in Mathematics, vol. 930, Springer-Verlag, Berlin, 1982.

[Ber74] P. Berthelot – *Cohomologie cristalline des schémas de caractéristique* $p > 0$, Lecture Notes in Mathematics, Vol. 407, Springer-Verlag, Berlin, 1974.

[BM90] P. Berthelot & W. Messing – "Théorie de Dieudonné cristalline. III. Théorèmes d'équivalence et de pleine fidélité", The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, p. 173–247.

[BO78] P. Berthelot & A. Ogus – *Notes on crystalline cohomology*, Princeton University Press, Princeton, N.J., 1978.

[Bou06a] N. Bourbaki – *Éléments de mathématique. Algèbre commutative. Chapitres 1 à 4*, Springer-Verlag, Berlin, 2006, Reprint of the 1985 original.

[Bou06b] — , *Éléments de mathématique. Algèbre commutative. Chapitres 8 et 9*, Springer-Verlag, Berlin, 2006, Reprint of the 1983 original.

[Bou07a] — , *Éléments de mathématique. Algèbre. Chapitres 1 à 3*, Springer-Verlag, Berlin, 2007, Reprint of the 1970 original.

[Bou07b] — , *Éléments de mathématique. Algèbre. Chapitres 4 à 7*, Springer-Verlag, Berlin, 2007, Reprint of the 1981 original.

[Bre96] C. Breuil – "Topologie log-syntomique, cohomologie log-cristalline et cohomologie de Čech", *Bull. Soc. Math. France* **124** (1996), no. 4, p. 587–647.

[Dem86] M. Demazure – *Lectures on p-divisible groups*, Lecture Notes in Mathematics, vol. 302, Springer-Verlag, Berlin, 1986, Reprint of the 1972 original.

[FJ05] J. Fontaine & U. Jannsen – "Some p-torsion sheaves in chrarcteristic p", unpublished, 2005.

[FM87] J.-M. Fontaine & W. Messing – "p-adic periods and p-adic étale cohomology", Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, p. 179–207.

[Gro60] A. Grothendieck – "Éléments de géométrie algébrique. I. Le langage des schémas", *Inst. Hautes Études Sci. Publ. Math.* (1960), no. 4, p. 228.

[Gro66] — , "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III", *Inst. Hautes Études Sci. Publ. Math.* (1966), no. 28, p. 255.

[Gro67] — , "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV", *Inst. Hautes Études Sci. Publ. Math.* (1967), no. 32, p. 361.

[Jan] U. Jannsen – "A new p-adic cohomology theory in characteristic p", Talk given at the conference "Arithmetic and Motivic Algebraic Geometry" (Regensburg, 17 February 2011).

[Kab71] T. Kabele – "Regularity conditions in nonnoetherian rings", *Trans. Amer. Math. Soc.* **155** (1971), p. 363–374.

[KS06] M. Kashiwara & P. Schapira – *Categories and sheaves*, Grundlehren der Mathematischen Wissenschaften, vol. 332, Springer-Verlag, Berlin, 2006.

[Lan02] S. Lang – *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[LZ07] A. Langer & T. Zink – "De Rham-Witt cohomology and displays", *Doc. Math.* **12** (2007), p. 147–191 (electronic).

[Mat80] H. Matsumura – *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[Mes72] W. Messing – *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, Vol. 264, Springer-Verlag, Berlin, 1972.

[MLM94] S. Mac Lane & I. Moerdijk – *Sheaves in geometry and logic*, Universitext, Springer-Verlag, New York, 1994, A first introduction to topos theory, Corrected reprint of the 1992 edition.

[MW04] B. Moonen & T. Wedhorn – "Discrete invariants of varieties in positive characteristic", *Int. Math. Res. Not.* (2004), no. 72, p. 3855–3903.

[Ogu01] A. Ogus – "Frobenius and the Hodge spectral sequence", *Adv. Math.* **162** (2001), no. 2, p. 141–172.

[Sch09] F. Schnellinger – "Rigid gauges and F-zips, and the fundamental sheaf of gauges G_n", Ph.D. Thesis, University of Regensburg, 2009, http://epub.uni-regensburg.de/12290/.

[SGA71] *Théorie des intersections et théorème de Riemann-Roch* – Lecture Notes in Mathematics, Vol. 225, Springer-Verlag, Berlin, 1971, Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967 (SGA 6), Dirigé par P. Berthelot, A. Grothendieck et L. Illusie. Avec la collaboration de D. Ferrand, J. P. Jouanolou, O. Jussila, S. Kleiman, M. Raynaud et J. P. Serre.

[SGA72a] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos* – Lecture Notes in Mathematics, Vol. 269, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[SGA72b] *Théorie des topos et cohomologie étale des schémas. Tome 2* – Lecture Notes in Mathematics, Vol. 270, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[Tam94] G. Tamme – *Introduction to étale cohomology*, Universitext, Springer-Verlag, Berlin, 1994, Translated from the German by Manfred Kolster.

[Wat79] W. C. Waterhouse – *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979.

[Wed08] T. Wedhorn – "De Rham cohomology of varieties over fields of positive characteristic", Higher-dimensional geometry over finite fields, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16, IOS, Amsterdam, 2008, p. 269–314.

[Zin02] T. Zink – "The display of a formal p-divisible group", *Astérisque* (2002), no. 278, p. 127–248, Cohomologies p-adiques et applications arithmétiques, I.