Crystalline comparison theorem for p-divisible groups

Andrea Panontin

Université
de Bordeaux

Università degli Studi
di Padova

Crystalline comparison theorem for p-divisible groups

Supervisor
Prof. Olivier Brinon

Candidate
Andrea Panontin

Master's Degree in Mathematics
Curriculum ALGANT
Academic Year 2020–2021

Contents

Winter kept us warm, covering
Earth in forgetful snow, feeding
A little life with dried tubers.

Introduction

In his renowned paper, [Tat67], Tate proved a very explicit Hodge-like decomposition of the Tate module of a Barsotti-Tate group, when tensored with $\mathbb{C}_p$. In particular, when working over abelian schemes, this granted a "Hodge-Tate" decomposition of the étale cohomology with coefficients in $\mathbb{Q}_p$. It was this paper which started the development of the field that is now known as *p-adic Hodge theory*, following the push from Tate to find analogous decompositions for the étale cohomology tensored with $\mathbb{C}_p$ for schemes admitting a proper and smooth model over a ring of integers of some local field K. This result was achieved by Fontaine employing its so called *period rings*, which allowed him to go even further and obtain finer results in the study of cohomology theories. In particular, when dealing with a variety X over K, admitting a proper smooth model over O_K, tensoring with the period ring B_{cris} grants an isomorphism between étale and crystalline cohomology of the special fiber. In the case of abelian varieties, the first étale cohomology group is just the dual of the Tate module of its associated Barsotti-Tate group, whereas crystalline cohomology is represented by the Dieudonné module of the associated Barsotti-Tate group. The aim of this thesis is to prove a crystalline comparison theorem which grants an isomorphism between the objects we have just mentioned, after tensoring with the period ring B_{cris}. To achieve this goal we will introduce the basic language of group schemes, which will allow the definition of p-divisible groups, also called Barsotti-Tate groups. The notion of sheaves on sites will be also discussed in order to give some extra tools to work with Barsotti-Tate groups and Dieudonné modules. We will define the concept of divided powers with the aim of defining exponentials, hence the crystalline site and crystals on this site. We will then introduce the theory of universal extensions which allows to define some crystals associated to Barsotti-Tate groups, which provide a generalization of the construction of the Dieudonné module. These, together with the theory of deformation of Grothendieck-Messing, will be used to introduce a classification of p-divisible groups over O_K due to Kisin and Breuil. Then, after spending some time to introduce the most relevant period rings for the aim of this work, we will use the above-mentioned results to construct and study the desired comparison isomorphism.

Acknowledgements

I want to dedicate this work to my late aunt and uncle Maria Vittoria e Giovanni, who have always rooted for me and supported my decisions. I wish to thank my family, whose support was vital in these eventful last two years. I have to thank my classmates, who kept reminding me the joy of sharing (be it mathematical ideas, meals or simply life experiences) every day. In particular Giacomo and Stevell, who were always there to give a hand, and Debam and Marco, whose presence coloured study with *playful cleverness*. I need to thank my supervisor, whose guidance was crucial in unravelling the not insignificant amount of information concerning this work and my future studies. Last, but not least, I thank Federica who, in this isolated period, was able to remind me that there is more than just mathematics to life.

Notation and conventions

Each time we will use the letter p it is going to denote a prime number. For convenience sake we can fix it here once and for all. With this in mind we will denote by $\mathbb{F}_q$ the field with q elements, by $\mathbb{Z}$ the ring of integers and by $\mathbb{Q}_p$ and $\mathbb{Z}_p$ respectively the field and ring of p-adic numbers. Then, for an extension $K/\mathbb{Q}_p$, we will denote by O_K the ring of integers of K and by K_0 the maximal unramified subextension of $K/\mathbb{Q}_p$.

With regards to algebraic geometry: for a morphism of schemes $f\colon X \to Y$, we will denote by $f^{\#}\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$ the associated morphism between structure sheaves and, given $y \coloneqq f(x)$, by $f_y^{\#}\colon \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ the induced morphism at the level of stalks. Moreover we denote by $\mathfrak{m}_x$ the maximal ideal of the local ring $\mathcal{O}_{X,x}$ and by $\kappa(x) \coloneqq \mathcal{O}_{X,x}/\mathfrak{m}_x$ the residue field at x. Finally we will say that a topological space is quasi compact iff every open cover admits a finite subcover, whereas we will call it compact if it is also Hausdorff.

With respect to category theory: we will not worry about universes. More precisely we will tacitly assume a universe $\mathbb{U}$ has been chosen and we restrict to categories whose objects lie in $\mathbb{U}$. We will denote categories using a sans serif font and, given a category C, we will denote by C^{op} its opposite category. In particular we will use the following notations: Sch/S for the category of schemes over S, Gp for that of groups, Ab for that of abelian groups, Top for that of topological spaces, and Sets for that of sets. Moreover, by *ring* or *algebra*, we will mean one which is commutative and with unity. Finally we will often use the shorter $X \in \mathsf{C}$ to mean that X is an object of the category C, i.e. that $X \in \mathrm{Ob}\,(\mathsf{C})$.

1 Grothendieck topologies

The aim of this section is to introduce the concept of Grothendieck topology on a category, in order to describe sheaves on such category. The main idea behind this construction is that one can reduce the definition of open coverings to a few formal axioms, translating inclusions with arrows in a category and intersections with fibered products.

Remark 1.1 (Open subsets of a topological space)**.** Let X be a topological space. One can define the category $\mathsf{Op}(X)$ of open subsets of X, whose objects are just open subsets $U \subset X$. Arrows in this category, moreover, are given by:

$$\mathrm{Hom}_{\mathsf{Op}(X)}(U,V) = \begin{cases} \{*\} & \text{if } U \subset V \\ \emptyset & \text{otherwise} \end{cases}.$$

This is the motivating example for the following constructions. In fact arrows in $\mathsf{Op}(X)$ are inclusions and fibered products correspond to intersections.

Definition 1.2: Sites.
Let C be a category. A *pretopology* on C is the assignment, to each object $U \in \mathsf{C}$, of a collection of sets of arrows $\{U_i \to U\}_{i\in I}$, called *coverings* of U, such that the following conditions are satisfied:

1. Given an isomorphism $V \xrightarrow{\sim} U$, the set $\{V \to U\}$ is a covering.
2. Given a covering $\{U_i \to U\}_{i\in I}$ of U and a morphism $V \to U$, then the fibered products $\{U_i \times_U V\}_{i\in I}$ exist and the set of projections $\{U_i \times_U V \to V\}_{i\in I}$ is a covering of V.
3. Given a covering $\{U_i \to U\}_{i\in I}$ and, for each index $i \in I$, a covering $\{U_{ij} \to U_i\}_{j\in J_i}$ of U_i, the set of composite morphisms $\{U_{ij} \to U\}_{i\in I, j\in J_i}$ is a covering of U.

A category with a Grothendieck pretopology is called a *site*.

Remark 1.3. From properties 2 and 3 above it follows that, given two coverings of the same object $\{U_i \to U\}_{i\in I}$ and $\{V_i \to U\}_{j\in J}$, also $\{U_i \times_U V_j \to U\}_{(i,j)\in I\times J}$ is a covering of U.

Before moving on to some examples, we should introduce a concept which plays an important role in the definition of some important pretopologies.

Definition 1.4: Jointly surjective family of morphisms.
For $\mathsf{C} = \mathsf{Sets}$ or $\mathsf{C} = \mathsf{Sch}/S$, for some scheme S, we will say that a family of morphisms $\{U_i \to U\}_{i\in I}$ is *jointly surjective* iff the set-theoretic union of the images is U.

Let's now give some examples.

Example 1.5.

1. The *site of a topological space*. Let X be a topological space, and $\mathsf{Op}(X)$ denote the category of open subsets of X. Then, to each $U \in \mathsf{Op}(X)$, we associate the family of all open coverings of U. Recalling that, given two open subsets $U_1 \hookrightarrow U$ and $U_2 \hookrightarrow U$, their fibered product is just their intersection, i.e. $U_1 \times_U U_2 = U_1 \cap U_2$, one easily checks that this defines a pretopology on $\mathsf{Op}(X)$.
2. The *global classical topology* on Top. Given $U \in \mathsf{Top}$, its coverings are all families of jointly surjective collections of open embeddings $U_i \to U$. Here open embedding means open, continuous, injective map and not only the set theoretic inclusion of a subspace.

Let's now give a couple of examples on Sch/S, for a fixed scheme S.

3. The *global Zariski topology*. A covering $\{U_i \to U\}_{i\in I}$ is a jointly surjective collection of open embeddings.

4. The *global étale topology*. A covering $\{U_i \to U\}_{i\in I}$ is a jointly surjective collection of étale maps.

5. The *fppf topology*. A covering $\{U_i \to U\}_{i\in I}$ is a jointly surjective collection of flat maps locally of finite presentation. The acronym *fppf* stands for "fidèlement plat et de présentation finie".

Proposition 1.6 ([Vis04, §2.3.2])**.** *Let $f\colon X \to Y$ be a surjective morphism of schemes. The following are equivalent.*

1. *Every quasi-compact open subset of Y is the image of a quasi-compact open subset of X.*
2. *There exists a covering $\{V_i\}_{i\in I}$ of Y by open affine subschemes, such that each V_i is the image of a quasi-compact open subset of X.*
3. *Given a point $x \in X$, there exists an open neighbourhood U of x in X, such that the image $f(U)$ is open in Y and the restriction $f|_U$ is a quasi-compact morphism of schemes, i.e. the inverse image of any quasi-compact open subset of $f(U)$ is quasi-compact in U.*
4. *Given a point $x \in X$, there exists an open neighbourhood U of x in X such that the image $f(U)$ is open and affine in Y.*

Definition 1.7: fpqc morphism.
An *fpqc morphism of schemes* is a faithfully flat morphism that satisfies the equivalent conditions of proposition 1.6. The acronym *fpqc* stands for "fidèlement plat et quasi-compact".

Remark 1.8 (fpqc topology)**.** It can be shown, see [Vis04, §2.3.2], that on Sch/S, the data of coverings $\{U_i \to U\}_{i\in I}$, for each $U \in \mathsf{Sch}/S$, such that the induced morphism $\amalg_i U_i \to U$ is *fpqc*, is a pretopology on Sch/S. This pretopology is called the *fpqc topology*.

Let's now investigate the relations between different topologies:

Definition 1.9: Refinement of a covering and subordinate pretopologies.

1. Let C be a category and $\{U_i \to U\}_{i\in I}$ a set of arrows in C. A *refinement* of $\{U_i \to U\}_{i\in I}$ is another set of arrows $\{V_a \to U\}_{a\in A}$, such that, for all $a \in A$, there is some $i \in I$ such that $V_a \to U$ factors through $U_i \to U$.
2. Let now τ and τ' be two pretopologies on C. We say that τ' is *subordinate* to τ iff every covering in τ' has a refinement which is a covering in τ.

The topologies we just introduced are in strong relation between them. In fact each is subordinate to the one we defined afterwards:

Remark 1.10 ([Stacks, Chapter 020K])**.**

1. Any Zariski covering is an étale covering, [Stacks, Lemma 0216]. Hence the Zariski topology is subordinate to the étale one.
2. Any étale covering is an *fppf* covering, [Stacks, Lemma 021N]. Hence the étale topology is subordinate to the *fppf* one.
3. Any *fppf* covering is an *fpqc* covering, [Stacks, Lemma 022C]. Hence the *fppf* topology is subordinate to the *fpqc* one.

1.1 Sheaves

The definition of sheaves on a topological space only depends on the datum of possible open coverings for a given object of the category $\mathsf{Op}(X)$. Then the introduction of pretopologies allows one to define sheaves on sites.

Definition 1.11: Presheaves.
Let C be any category. A *presheaf* on C is just a contravariant functor with values in sets:

$$F\colon \mathsf{C}^{\mathrm{op}} \longrightarrow \mathsf{Sets}.$$

Moreover we define the category of presheaves on C, denoted by $\mathsf{PSh}(\mathsf{C})$ as the category whose objects are presheaves on C and morphisms are natural transformations of functors.

Definition 1.12: Sheaves.
Let C be a *site*, i.e. a category given with a pretopology. Let $F \in \mathsf{PSh}(\mathsf{C})$, we say that

1. F is *separated* iff, given a covering $\{U_i \to U\}_{i\in I}$ and two sections $a, b \in F(U)$ whose pullbacks to each $F(U_i)$ coincide, then $a = b$;
2. F is a *sheaf* iff it satisfies the following condition. Consider any $U \in \mathsf{C}$, any covering $\{U_i \to U\}_{i\in I}$ of U in C and any family of sections $\{a_i\}_{i\in I}$ such that $a_i \in F(U_i)$. Denote

   $$\mathrm{pr}_k^{i_1,i_2}\colon U_{i_1} \times_U U_{i_2} \to U_{i_k}$$

   the projection on the kth component. Assume that, for all i, j, $(\mathrm{pr}_1^{i,j})^* a_i = (\mathrm{pr}_2^{i,j})^* a_j \in F(U_i \times_U U_j)$ then there exists a unique section $a \in F(U)$ whose pullback to $F(U_i)$ is a_i for all $i \in I$.

Moreover we denote by $\mathsf{Sh}(\mathsf{C})$ the full subcategory of $\mathsf{PSh}(\mathsf{C})$ of sheaves on C.

Remark 1.13. Notice that any *sheaf* on C is also a *separated presheaf*.

Remark 1.14. Let's give an equivalent definition of sheaf, for a presheaf F on a site C. Choose $U \in \mathsf{C}$ and a covering $\{U_i \to U\}_{i\in I}$. We denote by $F \to \Pi_{i\in I} F(U_i)$ the map induced by the restriction morphisms $F(U) \to F(U_i)$. Then we define

$$\mathrm{pr}_1^*\colon \prod_{i\in I} F(U_i) \longrightarrow \prod_{i,j\in I\times I} F(U_i \times_U U_j)$$

as the map sending $(a_i) \in \Pi_i F(U_i)$ to $\mathrm{pr}_1^*(a_i) \in \Pi_{i,j} F(U_i \times_U U_j)$, whose component in $F(U_i \times_U U_j)$ is given by $(\mathrm{pr}_1^{i,j})^*(a_i)$, where $\mathrm{pr}_1^{i,j}\colon U_i \times_U U_j \to U_i$ is the projection on the first component. Analogously we define a morphism $\mathrm{pr}_2^*\colon \Pi_i F(U_i) \to \Pi_{i,j} F(U_i \times_U U_j)$. Then the presheaf F is a sheaf iff, for all $U \in \mathsf{C}$ and all coverings $\{U_i \to U\}_{i\in I}$ in C, the following diagram is an equalizer:

$$0 \longrightarrow F(U) \longrightarrow \prod_{i\in I} F(U_i) \underset{\mathrm{pr}_2^*}{\overset{\mathrm{pr}_1^*}{\rightrightarrows}} \prod_{i,j\in I\times I} F(U_i \times_U U_j).$$

Before stating the main result of this section, let's notice a simple fact.

Remark 1.15. If τ' is subordinate to τ, as pretopologies on C, then any sheaf in τ is also a sheaf in τ'. As a consequence, for $\mathsf{C} = \mathsf{Sch}/S$ for some scheme S, any sheaf in fpqc is also a sheaf in fppf, étale and Zariski topologies.

Finally we can state a very important result due to Grothendieck.

Theorem 1.16 ([Vis04, §2.3.6], Grothendieck)**.** *A representable functor on Sch/S is a sheaf in the fpqc topology. In particular it is also a sheaf in the étale and fppf topologies.*

1.2 Morphisms of topoi

The main objects of our future studies will be sheaves on Sch/S taken with the fppf topology. Since we will often be concerned with base change, i.e. pullbacks, of sheaves, we devote this section to define this concept. Essentially we want to generalize the construction of fibered product in the representable case.

Definition 1.17: Topoi.
Let C be a site. The associated *topos* to C is the category $\mathsf{Sh}(\mathsf{C})$ of sheaves on C. A morphism of topoi f from $\mathsf{Sh}(\mathsf{D})$ to $\mathsf{Sh}(\mathsf{C})$ is the data of a pair of functors $f_*\colon \mathsf{Sh}(\mathsf{D}) \to \mathsf{Sh}(\mathsf{C})$ and $f^*\colon \mathsf{Sh}(\mathsf{C}) \to \mathsf{Sh}(\mathsf{D})$ such that, bifunctorially we have

$$\mathrm{Hom}_{\mathsf{Sh}(\mathsf{D})}(f^*G, F) \simeq \mathrm{Hom}_{\mathsf{Sh}(\mathsf{C})}(G, f_*F)$$

and the functor f^* commutes with finite limits, i.e. it is left exact. Moreover, given sites C, D and E and morphisms of topoi $f\colon \mathsf{Sh}(\mathsf{D}) \to \mathsf{Sh}(\mathsf{C})$ and $g\colon \mathsf{Sh}(\mathsf{E}) \to \mathsf{Sh}(\mathsf{D})$, we can define their composition $f \circ g$ as the pair of morphisms $(f \circ g)_* \coloneqq f_* \circ g_*$ and $(f \circ g)^* \coloneqq g^* \circ f^*$.

Definition 1.18: Category over an object.
Consider C a category and $U \in \mathsf{C}$ an object. The *category of objects over* U, denoted by C/U or C_U, is the category whose objects are morphisms $Y \to U$ in C and morphisms are morphisms $Y \to Y'$ in C such that the following (natural) diagram commutes

$$\begin{array}{ccc} Y & \longrightarrow & Y' \\ & \searrow \quad \swarrow & \\ & U. & \end{array}$$

Remark 1.19. If C is also a site we turn C/U into a site by defining the coverings of C/U to be the families of morphisms $\{V_i \to V\}_{i\in I}$ that, viewed as families in C, are coverings for the pretopology on C.

Moreover there is a forgetful functor $f_U\colon \mathsf{C}/U \to \mathsf{C}$ that simply forgets about the morphism. Finally, given a morphism $f\colon U \to V$ there is an induced functor $F\colon \mathsf{C}/U \to \mathsf{C}/V$ given by the composition with f, and $p_V = F \circ p_V$.

Lemma 1.20 ([Stacks, Section 00XZ])**.** *Given a site* C *and* $U \in \mathsf{C}$*, the forgetful functor* $j_U\colon \mathsf{C}/U \to \mathsf{C}$ *induces a morphism of topoi*

$$j_U\colon \mathsf{Sh}(\mathsf{C}/U) \longrightarrow \mathsf{Sh}(\mathsf{C}).$$

given by the functors j_U^* *and* j_{U*}*, whose lengthy definition is left to [Stacks, Chapter 00UZ].*

Definition 1.21: Localization.
Let C be a site and $U \in \mathsf{C}$.

1. We call the site C/U the *localization* of the site C at the object U.
2. The morphism of topoi $j_U\colon \mathsf{Sh}(\mathsf{C}/U) \to \mathsf{Sh}(\mathsf{C})$ is called the *localization morphism*.
3. The functor j_{U*} is called the direct image functor.
4. Taken any sheaf $F \in \mathsf{Sh}(\mathsf{C})$, its image j_U^*F is called the *restriction* of F to C/U.

Remark 1.22 ([Stacks, Section 00XZ])**.** Let C and U be as before. For all $F \in \mathsf{Sh}(\mathsf{C})$, the value of j_U^*F is given by

$$j_U^*F(X/U) = F(X),$$

where X/U denotes any object $X \to U \in \mathsf{C}/U$.

Lemma 1.23 ([Stacks, Lemma 03I4])**.** *Let $g\colon S \to S'$ be a morphism in* Sch*. Let $j\colon \mathsf{Sch}/S \to \mathsf{Sch}/S'$ be the corresponding localization functor, where both categories are taken with the fppf topology. Then, for F' a sheaf of sets on Sch/S', we have*

1. *$j^*F'(T/S) = F'(T/S')$ for any $T \in \mathsf{Sch}/S$, where T/S' means that we view T as an element of Sch/S' via g;*
2. *if F' is representable by $X' \in \mathsf{Sch}/S'$, then j^*F' is representable by $X'_S \coloneqq X' \times_{S'} S$.*

2 Group schemes

In this section we introduce the notion of *group object* in a category, giving all of the definition in the context of group schemes, i.e. group objects over the category of (relative) schemes. In this context we will develop all the important tools which will play a role later in the dissertation, starting from their application in the definition of p-divisible groups.

Definition 2.1: S-Group scheme.
Let $F\colon (\mathsf{Sch}/S)^{\mathrm{op}} \to \mathsf{Gp}$ be a functor. Assume that F is representable by $G \in \mathsf{Sch}/S$, i.e. functorially in $T \in \mathsf{Sch}/S$ we have

$$\iota F(T) \simeq \mathrm{Hom}_{\mathsf{Sch}/S}(T, G),$$

where $\iota\colon \mathsf{Gp} \to \mathsf{Sets}$ is the forgetful functor. We call G a *group scheme* over S or S-group scheme.

Remark 2.2 (T-points of an S-scheme)**.** Let's recall a standard notation: let $T \in \mathsf{Sch}/S$, one defines the *T-points* of $G \in \mathsf{Sch}/S$ as

$$G(T) \coloneqq \mathrm{Hom}_{\mathsf{Sch}/S}(T, G).$$

If we view G, by theorem 1.16, as an fppf sheaf on Sch/S, instead, we will use the notation

$$\Gamma(T, G) \coloneqq G(T)$$

for the sections of G on T. If, in particular, G is a *group scheme* then, by definition, $G(T) = \Gamma(T, G)$ is endowed with group structure for every $T \in \mathsf{Sch}/S$.

Remark 2.3. By definition, an abstract group is a set $G \in \mathsf{Sets}$, endowed with an operation, an inverse map and an identity element satisfying the usual properties. These can be rewritten in terms of commutative diagrams. At first one writes the above as the following maps:

$$\begin{aligned} m\colon G \times G &\longrightarrow G && \text{(multiplication)} \\ \mathrm{inv}\colon G &\longrightarrow G && \text{(inverse)} \\ \varepsilon\colon \{e\} &\longrightarrow G && \text{(unit),} \end{aligned}$$

where $\{e\}$ is the terminal object in Gp. Let's write $\pi\colon G \to \{e\}$ as the unique arrow to the terminal object of Gp and $\Delta\colon G \to G \times G$ the diagonal morphism. Then the group axioms are equivalent to

$$\begin{aligned} m \circ (\mathrm{id}_G \times m) &= m \circ (m \times \mathrm{id}_G), \\ m \circ (\mathrm{id}_G \times \mathrm{inv}) \circ \Delta = m \circ (\mathrm{inv} \times \mathrm{id}_G) \circ \Delta &= \varepsilon \circ \pi, \\ m \circ (\varepsilon \times \mathrm{id}_G) = m \circ (\mathrm{id}_G \times \varepsilon) &= \mathrm{id}_G . \end{aligned} \tag{2.1}$$

Notice that in this last equality we implicitly use the isomorphisms $\{e\} \times G \simeq G \simeq G \times \{e\}$.

Remark 2.4. Given a group scheme $G \in \mathsf{Sch}/S$, Yoneda's lemma allows to translate the group structure of $G(T)$, for all $T \in \mathsf{Sch}/S$, into a group structure on G. In fact, since the universal property of fibered product gives $(G \times_S G)(T) = G(T) \times G(T)$, one obtains that there exist unique maps

$$\begin{aligned} m\colon G \times_S G &\longrightarrow G && \text{(multiplication)} \\ \mathrm{inv}\colon G &\longrightarrow G && \text{(inverse)} \\ \varepsilon\colon S &\longrightarrow G && \text{(unit)} \end{aligned}$$

inducing the group structure on $G(T)$ via Yoneda embedding. Then, again by Yoneda's lemma, also the above maps have to satisfy the properties written in equation (2.1). More explicitly.

1. Associativity of the product

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{\mathrm{id}_G \times_S m} & G \times_S G \\ {\scriptstyle m \times_S \mathrm{id}_G}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow[m]{} & G. \end{array}$$

2. Inverse morphism

$$\begin{array}{ccccc} G \times_S G & \xrightarrow{\mathrm{id}_G \times_S \mathrm{inv}} & G \times_S G \\ {\scriptstyle\Delta}\uparrow & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{\pi} S \xrightarrow{\varepsilon} & G \end{array} \qquad \begin{array}{ccccc} G \times_S G & \xrightarrow{\mathrm{inv} \times_S \mathrm{id}_G} & G \times_S G \\ {\scriptstyle\Delta}\uparrow & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{\pi} S \xrightarrow{\varepsilon} & G \end{array}$$

3. Identity element (again, as with groups, in the following diagrams we use the isomorphisms $S \times_S G \simeq G \simeq G \times_S S$)

$$\begin{array}{ccc} G \times_S G & \xrightarrow{m} & G \\ {\scriptstyle \varepsilon \times_S \mathrm{id}_G}\uparrow & & \uparrow{\scriptstyle \mathrm{id}_G} \\ S \times_S G & \xrightarrow{\sim} & G \end{array} \qquad \begin{array}{ccc} G \times_S G & \xrightarrow{m} & G \\ {\scriptstyle \mathrm{id}_G \times_S \varepsilon}\uparrow & & \uparrow{\scriptstyle \mathrm{id}_G} \\ G \times_S S & \xrightarrow{\sim} & G. \end{array}$$

Definition 2.5: Commutative S-group scheme.
We say that a group scheme $G \in \mathsf{Sch}/S$ is *commutative* iff $G(T)$ is an abelian group for all $T \in \mathsf{Sch}/S$. Using Yoneda's lemma as before, this is equivalent to asking that the following diagram commutes

$$\begin{array}{ccc} G \times_S G & \xrightarrow{(\mathrm{pr}_2, \mathrm{pr}_1)} & G \times_S G \\ & {\scriptstyle m}\searrow \quad \swarrow{\scriptstyle m} & \\ & G. & \end{array}$$

Remark 2.6. One can generalize the definition of group object, from the category of S-schemes, to any category C admitting finite products (hence with final object given by the empty product) in the same manner as above. In fact, being S the final object in Sch/S, one sees that fibered products over S (seen in the category of schemes) are just products in Sch/S.

Definition 2.7: Morphism of group schemes.
Let G, G' be group schemes, a *homomorphism of group schemes*

$$\alpha\colon G \longrightarrow G'$$

is a morphism $G \to G'$ in Sch/S such that, for all $T \in \mathsf{Sch}/S$, the corresponding morphism at the level of T-points is a group homomorphism

$$\begin{aligned} \alpha(T)\colon G(T) &\longrightarrow G'(T) \\ g &\longmapsto \alpha \circ g. \end{aligned}$$

Notice that the identity of a group scheme is clearly a homomorphism of group schemes and compositions of group schemes homomorphisms are still group scheme homomorphisms.

Remark 2.8. Let G, G' be group schemes, representing the functors F, F'. Then, by Yoneda's lemma, giving a homomorphism $\alpha\colon G \to G'$ is equivalent to giving a morphism between the functors they represent.

Again by Yoneda's lemma, one sees that a morphism $\alpha\colon G \to G'$ in Sch/S is a morphism of group schemes iff it preserves products, i.e. iff

$$\alpha \circ m = m' \circ (\alpha, \alpha),$$

for m, m' the product morphisms of G and G' respectively.

Definition 2.9: Category of S-group schemes.
Combining all of the definitions so far, one can define the subcategory Gp/S of Sch/S, of *S-group schemes*, or more simply *S-groups*, whose objects are S-group schemes and morphisms are homomorphisms of S-group schemes.

Remark 2.10 (Kernels and cokernels)**.** As with any category, one defines kernels and cokernels in Gp/S via the usual universal properties.

With regards to kernels, one can use the general construction in a category with zero object, since for a morphism $\alpha\colon G \to G'$ its kernel is just the fibered product of G and 0 over G', i.e.

$$\ker \alpha = \varprojlim \begin{pmatrix} & & 0 \\ & & \downarrow \\ G & \xrightarrow{\alpha} & G' \end{pmatrix} = G \times_{G'} 0.$$

Notice that in Gp/S, since $(G \times_S H)(T) = G(T) \times H(T)$, we can construct fibered products and they coincide with those in Sch/S. Moreover its zero object is S. By definition there is a unique morphism $S \to G'$, which coincides with the unit morphism of G'. Then the following gives rise to a kernel for α in Gp/S

$$G \times_{G'} S \xrightarrow{\ i\ } G,$$

where i is the projection on the first factor. Hence kernels exist in Gp/S.

When it comes to cokernels, instead, one finds difficulties, much like with sheaves of abelian groups. In fact, given a morphism $\alpha\colon G \to G'$, one cannot always find an object $H \in \mathsf{Gp}/S$ representing the functor

$$T \longmapsto \operatorname{coker}(\alpha_T) = G(T)/G'(T).$$

2.1 Affine group schemes

The above definitions have a dual interpretation in the affine case, which is the main topic of this section. Moreover, in the rest of the discussion, we will mostly be concerned by affine group scheme, hence the choice to dedicate a whole section to them. Many of the following results, though, are still valid in a more general setting.

Then, for most of the following section we will fix an affine scheme $S = \operatorname{Spec}(R)$, and focus on affine S-groups.

Remark 2.11. If we consider $G = \mathrm{Spec}(A)$ affine, the arrow-reversing equivalence of categories between affine R-schemes and commutative R-algebras, allows us to translate the structural morphisms of schemes defined in remark 2.4 into appropriate R-algebra morphisms. Then the properties defined by the diagrams in remark 2.4 will translate into properties for these new morphisms.

Recall that the structural morphism $\pi\colon G \to S$ corresponds to a morphism $R \to A$ making A into an R-algebra. Moreover the diagonal morphism $\Delta\colon G \to G \times_S G$ corresponds to the multiplication morphism of the R-algebra A:

$$\begin{aligned} \widetilde{\Delta}\colon A \otimes_R A &\longrightarrow A \\ a \otimes b &\longmapsto a \cdot b. \end{aligned}$$

With this in mind we obtain the following R-algebra morphisms:

$$\begin{aligned} \widetilde{m}\colon A &\longrightarrow A \otimes_R A && \text{(comultiplication)} \\ \widetilde{\mathrm{inv}}\colon A &\longrightarrow A && \text{(antipode)} \\ \widetilde{\varepsilon}\colon A &\longrightarrow R && \text{(counit/augmentation),} \end{aligned}$$

satisfying the duals of the diagrams in remark 2.4.

Definition 2.12: Hopf algebras.
A *Hopf algebra over* R is an R-algebra A endowed with a comultiplication, a couint and an antipode map, respectively:

$$\begin{aligned} \widetilde{m}\colon A &\longrightarrow A \otimes_R A \\ \widetilde{\mathrm{inv}}\colon A &\longrightarrow A \\ \widetilde{\varepsilon}\colon A &\longrightarrow R, \end{aligned}$$

satisfying the conditions obtained by dualizing those of remark 2.4, more explicitly:

$$\begin{aligned} (\widetilde{m} \otimes_R \mathrm{id}_A) \circ \widetilde{m} &= (\mathrm{id}_A \otimes_R \widetilde{m}) \circ \widetilde{m}, \\ (\mathrm{id}_A \otimes_R \widetilde{\varepsilon}) \circ \widetilde{m} &= (\widetilde{\varepsilon} \otimes_R \mathrm{id}_A) \circ \widetilde{m} = \mathrm{id}_A, \\ \widetilde{\Delta} \circ (\mathrm{id}_A \otimes_R \widetilde{\mathrm{inv}}) \circ \widetilde{m} = \widetilde{\Delta} \circ (\widetilde{\mathrm{inv}} \otimes_R \mathrm{id}_A) \circ \widetilde{m} &= (R \to A) \circ \widetilde{\varepsilon}. \end{aligned}$$

Moreover one defines a morphism of Hopf algebras to be an R-algebra morphism preserving the comultiplication morphism. Finally we call $I := \ker \widetilde{\varepsilon}$ the *augmentation ideal* of A.

Remark 2.13. Dualizing the result for groups, one can see that a Hopf algebra homomorphism preserves not only comultiplication, but also counit and antipode morphisms.

Remark 2.14 (Equivalence of categories)**.** Clearly, then, any Hopf algebra over R gives rise to an affine R-group via the aforementioned equivalence of categories. This is actually an anti-equivalence of categories between affine R-group schemes and Hopf algebras over R. In fact the multiplication morphism in a group scheme corresponds to the comultiplication morphism in its associated Hopf algebra, and morphisms in the two categories are defined to preserve such operations.

Definition 2.15: Augmentation ideal.
For a Hopf algebra A over R, the structure morphism $R \to A$ splits the following short exact sequence

$$0 \longrightarrow I \longrightarrow A \xrightarrow{\widetilde{\varepsilon}} R \longrightarrow 0.$$

Hence we have $A = R \cdot 1 \oplus I$, from which we deduce that $A \otimes A = R \oplus (I \otimes 1) \oplus (1 \otimes I) \oplus (I \otimes I)$. Finally it is easy to show that, for all $f \in I$,

$$\widetilde{m}(f) - f \otimes 1 - 1 \otimes f \in I \otimes I.$$

The following results are valid in a more general setting, so let's change the assumption for S: we will assume it is a locally Noetherian scheme.

Remark 2.16 (Finite S-scheme)**.** An S-scheme G is finite and flat over S iff its sheaf of regular functions $\mathcal{O}_G$ is locally-free of finite rank as an $\mathcal{O}_S$-module. More explicitly this means that there exists a cover of S by affine open subschemes on each of which the restriction of the structure morphism is of the form $\mathrm{Spec}(A) \to \mathrm{Spec}(R)$, for A a free R-module of finite rank over R. This is going to be our main interest in what follows.

It is also true that finite flat schemes over affine schemes are themselves affine. We are going to be interested in the case of $S = \mathrm{Spec}(R)$, for R the ring of integers of a local field, and G finite flat over S. In particular S and G will be Noetherian schemes and G, being finite flat over S, is just $\mathrm{Spec}(A)$, for a finite projective R-module A (see, for instance, [Stacks, Lemma 00NX]).

Definition 2.17: Order of a finite flat S-scheme.
Given a finite flat S-scheme G, the rank of $\mathcal{O}_X$ as an $\mathcal{O}_S$-module is a locally constant function with respect to the Zariski topology, with integer values. We call such a function the order of G over S and denote it by $[G : S]$. Moreover we will use the notation $[G : S] = n$ to state that G is finite flat of constant rank n over S.

Proposition 2.18 ([Tat98, §3])**.**

1. *Consider the morphisms of schemes $X \to Y \to S$, with $[X : Y] = m$. Then X is finite and flat over S iff Y is, in which case $[X : S] = [X : Y][Y : S]$ as functions on Y.*
2. *If $[X_i : S] = n_i$ for $i = 1, 2$, then $[X_1 \times_S X_2 : S] = n_1 n_2$.*
3. *If $[X : S] = n$, then $[X \times_S T : T] = n$ for all $T \in \mathsf{Sch}/T$.*

2.2 Examples

In order to compute a few useful examples, let's explicit the relation between multiplication in an S-group and comultiplication in its associated Hopf algebra over R, for $S = \mathrm{Spec}(R)$.

Remark 2.19. As usual let $G \in \mathsf{Gp}/S$. Yoneda tells us that the multiplication map $m \colon G \times_S G \to G$ can be expressed as the product $\mathrm{pr}_1 \mathrm{pr}_2$ of the two projection morphisms, using the group law on $G(G \times_S G)$. Then, in the case of affine schemes $S = \mathrm{Spec}(R)$ and $G = \mathrm{Spec}(A)$, one can translate the above to the corresponding Hopf algebra morphism, using the equivalence of categories. More explicitly one can describe the comultiplication map $\widetilde{m}$ as the product in $\mathrm{Hom}_{R\text{-}\mathsf{Alg}}(A, A \otimes_R A)$ (which has the same group structure as $G(G \times_S G)$) of the embedding morphisms

$$\widetilde{\mathrm{pr}}_1 : a \longmapsto a \otimes_R 1 \qquad \text{and} \qquad \widetilde{\mathrm{pr}}_2 : a \longmapsto 1 \otimes_R a.$$

Example 2.20. In the following examples we will denote $S \coloneqq \mathrm{Spec}(R)$ and $G \coloneqq \mathrm{Spec}(A)$.

1. The *additive group scheme*, given by $\mathbb{G}_a \coloneqq \mathrm{Spec}(R[x])$. It is given on R-schemes by

$$X \longmapsto \Gamma(X, \mathcal{O}_X),$$

in which $\Gamma(X, \mathcal{O}_X)$ is viewed as an additive group. In fact we know that

$$\mathrm{Hom}_{\mathsf{Sch}/S}(X, \mathbb{G}_a) \simeq \mathrm{Hom}_{R\text{-}\mathsf{Alg}}(R[x], \Gamma(X, \mathcal{O}_X)) \simeq \Gamma(X, \mathcal{O}_X),$$

functorially in X. The last isomorphism is determined by $(x \mapsto a) \mapsto a$. The hom set $\mathrm{Hom}_{R\text{-}\mathsf{Alg}}(R[x], A)$ inherits the additive group structure from A. Moreover the embeddings of $R[x]$ in $R[x] \otimes_R R[x]$ are given by

$$\widetilde{\mathrm{pr}}_1(x) = x \otimes_R 1 \qquad \text{and} \qquad \widetilde{\mathrm{pr}}_2(x) = 1 \otimes_R x.$$

Finally, thanks to remark 2.19, we deduce that

$$\widetilde{m}(x) = (\widetilde{\mathrm{pr}}_1(x)) + (\widetilde{\mathrm{pr}}_2(x)) = x \otimes_R 1 + 1 \otimes_R x.$$

Then, from the properties of counit and antipode (see definition 2.12), one deduces

$$\widetilde{\varepsilon}(x) = 0 \qquad \text{and} \qquad \widetilde{\mathrm{inv}}(x) = -x.$$

2. The *multiplicative group scheme* $\mathbb{G}_m \coloneqq \mathrm{Spec}(R[x, x^{-1}])$. It acts on R-schemes by

$$X \longmapsto \Gamma(X, \mathcal{O}_X)^\times,$$

in which $\Gamma(X, \mathcal{O}_X)^\times$ is viewed as a multiplicative group. In fact one checks that

$$\mathrm{Hom}_{\mathsf{Sch}/S}(X, G) \simeq \mathrm{Hom}_{R\text{-}\mathsf{Alg}}\left(R[x, x^{-1}], \Gamma(X, \mathcal{O}_X)\right) \simeq \Gamma(X, \mathcal{O}_X)^\times,$$

functorially in X. Then, reasoning as before, we obtain

$$\widetilde{m}(x) = (\widetilde{\mathrm{pr}}_1(x)) \cdot (\widetilde{\mathrm{pr}}_2(x)) = (x \otimes_R 1) \cdot (1 \otimes_R x) = x \otimes_R x.$$

Finally, from the properties of counit and antipode map (see definition 2.12) one deduces

$$\widetilde{\varepsilon}(x) = 1 \qquad \text{and} \qquad \widetilde{\mathrm{inv}}(x) = x^{-1}.$$

3. The *general linear group scheme* $\mathrm{GL}_n \coloneqq \mathrm{Spec}(R[\mathbf{x}, \mathbf{y}]/J)$, where

$$R[\mathbf{x}, \mathbf{y}] \coloneqq R[x_{11}, x_{12}, \ldots, x_{nn}, y_{11}, \ldots, y_{nn}]$$

and J is the ideal generated by the n^2 entries of the matrix $(x_{ij})_{i,j=1}^n \cdot (y_{ij})_{i,j=1}^n - I$, where I is the identity matrix. It acts on R-schemes by associating to $X \in \mathsf{Sch}/S$ the multiplicative group $\mathrm{GL}_n(X)$ of invertible $n \times n$ matrices with coefficients in $\Gamma(X, \mathcal{O}_X)$. Let's recall that, in $\mathrm{GL}_n(X)$, the product $(x_{i,j})_{i,j=1}^n \cdot (y_{i,j})_{i,j=1}^n$ is given by $(c_{i,j})_{i,j=1}^n$, where

$$c_{i,j} = \sum_{l=1}^{n} x_{i,l} \cdot y_{l,j}.$$

Then, reasoning as before, we can explicitly write the Hopf algebra maps. Indeed they are

$$\widetilde{m}(x_{i,j})_{i,j=1}^n = \sum_{l=1}^{n} x_{i,l} \otimes_R x_{l,j}, \quad \widetilde{\varepsilon}(x_{i,j})_{i,j=1}^n = 1, \quad \widetilde{\mathrm{inv}}(x_{i,j})_{i,j=1}^n = (y_{i,j})_{i,j=1}^n,$$

where $(y_{i,j})_{i,j}$ satisfies $(x_{ij})_{i,j=1}^n \cdot (y_{ij})_{i,j=1}^n = I$.

4. The *group scheme of nth roots of unity*, denoted by μ_n. It is defined to be the kernel of the nth power morphism $\mathbb{G}_m \to \mathbb{G}_m$, corresponding to the R-algebra morphism $\mu\colon x \mapsto x^n$. Then μ_n is represented by $\mathrm{Spec}(\mathrm{coker}\,\mu)$, and the morphism $\mu_n \hookrightarrow \mathbb{G}_m$ is given by the projection

$$R[x, x^{-1}] \twoheadrightarrow R[x, x^{-1}]/(x^n - 1),$$

which is surjective, making μ_n a closed subgroup scheme of $\mathbb{G}_m$. We can also see that μ_n is a finite and flat S-group scheme, since $R[x, x^{-1}]/(x^n - 1)$ is finite and flat over R of order n.

5. The *diagonalizable group schemes*. Let X be an ordinary commutative group, and denote by $R[X] \coloneqq \bigoplus_{x \in X} Rx$ its associated group R-algebra. This is a Hopf algebra whose structural morphisms are given, for every $x \in X$, by

$$\widetilde{m}(x) = x \otimes x, \quad \widetilde{\varepsilon}(x) = 1, \quad \text{and} \quad \widetilde{\mathrm{inv}}(x) = x^{-1}.$$

The above can be checked directly, since we have the identifications, for $G = \mathrm{Spec}(A)$,

$$(D(X))\,(G) \coloneqq \mathrm{Hom}_{R\text{-Alg}}\,(R[X], A) \simeq \mathrm{Hom}_{\mathsf{Ab}}\left(X, A^\times\right),$$

where the last hom set has a natural structure of abelian group. Then we define the *diagonalizable group scheme* $D(X)$ as the commutative R-group $\mathrm{Spec}(R[X])$.

Two important cases are $\mathbb{G}_m \simeq D(\mathbb{Z})$ and $\mu_n \simeq D(\mathbb{Z}/n\mathbb{Z})$. Moreover, if X is finite, $R[X]$ is a free R-module of rank n, making $D(X)$ commutative, finite and flat over R of order n. More generally, for X finitely generated, from the structure theorem for finitely generated abelian groups, X is isomorphic to a finite product of cyclic groups. Hence $D(X)$ is a finite product of copies of $\mathbb{G}_m$ and μ_n, for various n. It is then a closed subgroup scheme of $\mathbb{G}_m^r$, for some r, which again can be seen as the closed subgroup scheme of diagonal matrices of GL_r, explaining the name *diagonalizable*.

6. The *constant group scheme*. Let R be a ring and Γ an ordinary, finite commutative group. We define A to be the R-algebra R^Γ, of set-theoretic functions from Γ to R. A basis for A is given by $\{e_\sigma\}_{\sigma \in \Gamma}$, for $e_\sigma(\gamma) = \delta_{\gamma,\sigma}$, where δ is Kronecker's delta function. Let's define on A the following Hopf algebra structure:

$$\widetilde{m}(e_\rho) \coloneqq \sum_{\gamma\tau=\rho} e_\sigma \otimes e_\tau, \quad \widetilde{\mathrm{inv}}(e_\sigma) \coloneqq e_{\sigma^{-1}}, \quad \widetilde{\varepsilon}(e_\sigma) \coloneqq \begin{cases} 1 & \text{if } \sigma = 1 \in \Gamma \\ 0 & \text{otherwise.} \end{cases}$$

Then A represents an S-group scheme, called the constant group scheme for Γ, which we denote by $\underline{\Gamma}$.

7. The *group scheme of p^rth roots of zero*, if $\mathrm{char}\, R = p$, denoted by α_{p^r}. It is defined to be the kernel of the p^rth power morphism $\mathbb{G}_a \to \mathbb{G}_a$, corresponding to the R-algebra morphism $\alpha\colon x \mapsto x^{p^r}$. Then α_{p^r} is represented by $\mathrm{Spec}(\mathrm{coker}\,\alpha)$. Moreover this is an additive subgroup scheme, since $\mathrm{char}\, R = p$. As for μ_n, it is a closed finite flat subgroup scheme of $\mathbb{G}_a$ of order p^r.

Remark 2.21 (Base change)**.**

1. Let $U, T \in \mathsf{Sch}/S$ be two S-schemes. We use the notation U_T for the base change $U \times_S T$. It is important to notice that, for $V \in \mathsf{Sch}_T$, we have $U_T(V) = U(V)$, where in the last expression we considered V as an S scheme, by $V \to T \to S$.

2. In particular the examples we have developed so far can all be given for $\mathbb{Z}$-group schemes (apart from α_p, which requires a base ring of characteristic p). Then we will use the notation given in the examples to mean the group scheme over $\mathbb{Z}$ (resp. $\mathbb{F}_p$) and take their base change when working in Sch/S for an appropriate S.

2.3 Connected-étale sequence

Quotients and exactness

In order to construct some important short exact sequences we need to tackle the problem of the construction of cokernels, hence of quotient groups. In order to do so we have to start with the concept of group action. Moreover we keep the assumption, from the previous section, that S is a locally Noetherian scheme.

Definition 2.22: Right action.
Let H be an S-group scheme, and take $X \in \mathsf{Sch}/S$. A *right action* of H on X is a morphism

$$a\colon X \times_S H \longrightarrow X$$

such that, for all $T \in \mathsf{Sch}/S$, the induced map $X(T) \times H(T) \to X(T)$ is a right action of the group $H(T)$ on the set $X(T)$. We say that the action is *strictly free* iff the morphism

$$(\mathrm{pr}_1, a)\colon X \times_S H \longrightarrow X \times_S X$$

is a closed immersion.

The next proposition will allow us to construct quotients of S-group schemes by finite, flat closed subgroup schemes. It actually is a consequence of the following, more general result, due to Grothendieck.

Theorem 2.23 ([Tat98, §3.4])**.** *Suppose that H, finite flat over S, acts strictly freely on X of finite type over S in such a way that every orbit is contained in an affine open set. Then there exists $Y \in \mathsf{Sch}/S$ and a morphism $u\colon X \to Y$, constant on orbits, such that for every morphism $v\colon X \to Z$ constant on orbits, there is a unique morphism $f\colon Y \to Z$ such that $v = f \circ u$. We denote Y by X/H, and notice that u has the following properties:*

1. *X is finite flat over X/H and $[X : (X/H)] = [H : S]$;*
2. *for every $T \in \mathsf{Sch}/S$, the following map is injective*

$$X(T)/H(T) \rightarrowtail (X/H)(T).$$

As promised we obtain the following result for group schemes.

Proposition 2.24 ([Tat98, §3.5])**.** *Let G be an S-group scheme and $H \subset G$ a finite flat closed subgroup scheme. Define the action $a\colon G \times_S H \to G$ as the restriction of the group law m on G. Then G/H is the scheme of* left cosets *of H in G.*

Assume, moreover, that G/H is finite and flat over S, with order $[(G/H) : S]$. We will call this the index *of H in G and denote it by $[G : H]$. Then G is finite and flat over S and we have*

$$[G : H][H : S] = [G : S].$$

Finally, in order to take quotients in Gp/S, we need to introduce the notion of normal subgroup.

Definition 2.25: Normal subgroup.
Let G be an S group and H be a subgroup scheme of G, i.e. H is a subscheme of G and the inclusion morphism is a homomorphism of group schemes. We say that H is a *normal subgroup scheme* of G iff, for all $T \in \mathsf{Sch}/S$, the subgroup $H(T)$ of $G(T)$ is a *normal* subgroup.

Remark 2.26 (Short exact sequence)**.** Assume, in the hypothesis of proposition 2.24, that H is also *normal* in G. Then the multiplication on G induces a multiplication morphism on G/H, making it an S-group scheme. Moreover the map $u\colon G \to G/H$ is an S-group homomorphism. In particular this gives rise to the short exact sequence of group schemes

$$1 \longrightarrow H \xrightarrow{\ i\ } G \xrightarrow{\ u\ } G/H \longrightarrow 1,$$

where short exactness also means that i is a closed immersion and u is faithfully flat. Here 1 denotes the constant S-group scheme $\underline{1}$, as seen in item 6 of example 2.20.

Separable algebras and étale group schemes

The study of étale group schemes is strictly related to that of separable algebras, so here are a few interesting results for the latter.

Theorem 2.27 ([Wat79, §6.2])**.** *Let k be a field and denote by $\overline{k}$ and k^s respectively an algebraic and a separable closure of k. Let A be a finite dimensional k-algebra. The following are equivalent:*

1. *$A \otimes_k \overline{k}$ is reduced;*
2. *$A \otimes_k \overline{k} \simeq \overline{k} \times \cdots \times \overline{k}$;*
3. *The number of k-algebra homomorphisms $A \to \overline{k}$ equals the dimension of A over k;*
4. *A is a product of separable field extensions of k;*
5. *$A \otimes_k k^s \simeq k^s \times \cdots \times k^s$.*

If, moreover, k is a perfect field, all of the above are equivalent to

6. *A is reduced.*

Definition 2.28: Separable algebra.
A k-algebra A satisfying the equivalent conditions of theorem 2.27 is called *separable*.

Corollary 2.29 ([Wat79, §6.2])**.** *Subalgebras, quotients, products and tensor products of separable k-algebras are separable. Moreover, given L/k a field extension, A is separable over k iff $A \otimes_k L$ is separable over L.*

For the following definition we will not assume maximal generality, but we will restrict to a case which includes the situation we will be concerned with, i.e. finite flat schemes over a Noetherian affine base.

Definition 2.30: Unramified and étale morphism of schemes.
Let $f\colon X \to S$ be a morphism of finite type between locally Noetherian schemes.

1. We say that f is *unramified* at $x \in X$ iff, for $s \coloneqq f(x)$, the image $f_s^{\#}(\mathfrak{m}_s)$ generates $\mathfrak{m}_x$ in $\mathcal{O}_{X,x}$ and $\kappa(x)/\kappa(s)$ is a finite and separable field extension.
2. We say that f is *étale* at $x \in X$ iff it is flat and unramified at x.

3. We say that f is unramified (resp. étale) iff it is unramified (resp. étale) at every point of X.

4. We say that $X \in \mathsf{Sch}/S$ is unramified (resp. étale) iff its structure morphism is unramified (resp. étale).

In fact we can use this characterization in our context thanks to the following lemmas.

Lemma 2.31 ([Stacks, Lemma 02GL])**.**

1. *A scheme X is étale over a field k iff $X = \mathrm{Spec}(A)$ for a* separable *k-algebra A.*

2. *If $f\colon X \to S$ is an étale morphism of schemes, for every $s \in S$, the fiber at s is given by $X_s = \mathrm{Spec}(A_s)$, for a separable $\kappa(s)$-algebra A_s.*

Lemma 2.32 ([Stacks, Lemma 02GM])**.** *Let $f\colon X \to S$ be a morphism of schemes. Assume, moreover, that f is flat, locally of finite presentation and that, for all $s \in S$, the fiber $X_s := X \times_{\mathrm{Spec}(\kappa(s))} \mathrm{Spec}(\kappa(s))$ is a disjoint union of finite separable extensions of $\kappa(s)$. Then f is étale.*

Finally we to quote an important result which concerns finite étale group schemes over a field.

Definition 2.33: Discrete $\mathscr{G}_k$-groups.
Let k be a field and $\overline{k}$ a fixed separable closure of k. Let $\mathscr{G}_k := \mathrm{Gal}\left(\overline{k}/k\right)$ be the absolute Galois group of k. We define the category of *abstract discrete finite $\mathscr{G}_k$-groups* as the category whose objects are abstract finite groups endowed with the discrete topology and a continuous action of $\mathscr{G}_k$ via group homomorphisms. A morphism of abstract discrete finite $\mathscr{G}_k$-groups is a $\mathscr{G}_k$-equivariant group homomorphism.

Theorem 2.34 ([Mil17, §2.16])**.** *The functor $G \mapsto G(\overline{k})$ is an equivalence of categories between the category of étale group schemes over k and the category of abstract discrete finite $\mathscr{G}_k$-groups.*

Remark 2.35 ([Sha86, §3, example (7)])**.** We can generalize the above result to the case of a base scheme $S := \mathrm{Spec}(R)$, where R is a complete (or more generally Hensel) Noetherian local ring with residue field k. In this case, again, we find an equivalence of categories, this time between the category of abstract discrete finite $\mathscr{G}_k$-groups and that of étale R-group schemes.

Example 2.36. Important examples of étale group schemes are given by constant group schemes over fields. In fact they are represented by the spectrum of a finite product of copies of the base field, hence they are étale by theorem 2.27. More generally, in case the base scheme is a Noetherian discrete valuation ring, we can reduce to the above arguments on the two fibers thanks to lemma 2.32 and obtain the same result. In fact we only need to show that the structure morphism is flat, which corresponds to showing that our algebra is a flat module over the base ring. But this is the case, since as a module it is a finite product of copies of the base ring.

Connected-étale exact sequence

In the following section we will always assume $S = \mathrm{Spec}(R)$ for a henselian local ring R. We will denote by $\mathfrak{m}$ its maximal ideal, by $k := R/\mathfrak{m}$ its residue field and by $s := \mathrm{Spec}(k)$ the closed point of R. Finally by G we will denote a finite and flat S-group scheme.

Theorem 2.37 ([Tat98, §3.7], Connected-étale exact sequence)**.** *Let G^0 be the connected component of the identity in G. Then G^0 is the spectrum of a local R-algebra with residue field $k = R/\mathfrak{m}$ and it is a flat, closed normal subgroup scheme of G. Moreover the quotient $G^{\text{ét}} := G/G^0$, constructed as in proposition 2.24, is étale and gives rise to the short exact sequence*

$$1 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 1,$$

called the connected-étale sequence *for G. In particular it can be characterized by the fact that every homomorphism from G to an étale S-group factorizes through $G \to G^{\text{ét}}$, and G^0 is the kernel of that homomorphism.*

Proposition 2.38 ([Tat98, §3.7])**.**

1. *Assume $\operatorname{char} k = 0$, then $G^0 = S$ and $G = G^{\text{ét}}$. If, instead, $\operatorname{char} k = p > 0$, we have $[G^0 : S] = p^t$ for some t. As a consequence, if $[G : S]$ is invertible in S, then G is étale over S.*
2. *If $R = k$ is a field and $n = [G : S]$, then $x^n = 1$ for all $x \in G(B)$ for any k-algebra B. We say that G is killed by its order.*
3. *If R is a perfect field, then the homomorphism $G \to G^{\text{ét}}$ admits a section. As a consequence $G = G^0 \rtimes G^{\text{ét}}$ can be expressed as a semidirect product.*

2.4 Cartier Duality

In this section we will mainly be concerned with $S = \operatorname{Spec}(R)$ affine and G finite commutative over S, hence affine, let's say $G = \operatorname{Spec}(A)$.

Remark 2.39. In remark 2.16 we recalled that A is a finite projective R-module. Then, still arguing by [Stacks, Lemma 00NX]), A is a finite and locally-free R-module. For an R-module M we define its dual R-module to be $M^D \coloneqq \operatorname{Hom}_R(M, R)$. Hence, for any couple of locally-free R-modules of finite rank M and N, one has the natural isomorphisms

$$M \xrightarrow{\sim} (M^D)^D \qquad \text{and} \qquad M^D \otimes_R N^D \xrightarrow{\sim} (M \otimes_R N)^D .$$

Remark 2.40 (Dual algebra)**.** To the R-algebra A we can associate the R-module

$$A^D \coloneqq \operatorname{Hom}_{R\text{-Mod}}(A, R) .$$

Thanks to the above remark, in case A is given with a cocommutative Hopf algebra structure, one can dualize it to obtain a (cocommutative) Hopf algebra structure on A^D. In particular product and coproduct of A become, respectively, coproduct and product of A^D, as

$$(\widetilde{\Delta})^D \colon A^D \longrightarrow A^D \otimes_R A^D \qquad \text{and} \qquad (\widetilde{m})^D \colon A^D \otimes_R A^D \longrightarrow A^D .$$

More explicitly $(\widetilde{\Delta})^D$ and $(\widetilde{m})^D$ are the transpose maps of $\widetilde{\Delta}$ and $\widetilde{m}$ respectively, i.e.

$$\begin{aligned} (\widetilde{\Delta})^D \coloneqq \operatorname{Hom}_{R\text{-Mod}}(\widetilde{\Delta}, R) \colon \operatorname{Hom}_{R\text{-Mod}}(A, R) &\longrightarrow \operatorname{Hom}_{R\text{-Mod}}(A \otimes_R A, R) \\ f &\longmapsto f \circ \widetilde{\Delta}, \end{aligned}$$

where, since A is a finite projective R-module, on the right hand side we have the isomorphism

$$\operatorname{Hom}_{R\text{-Mod}}(A \otimes_R A, R) \simeq \operatorname{Hom}_{R\text{-Mod}}(A, R) \otimes_R \operatorname{Hom}_{R\text{-Mod}}(A, R) .$$

Analogously one constructs $(\widetilde{m})^D$.

Definition 2.41: Cartier dual.
Given a S and G as before, we define the *dual* of G as the group scheme defined by

$$G^D \coloneqq \operatorname{Spec}(A^D).$$

Theorem 2.42 ([Wat79, §3.7], Cartier duality)**.** *Let G be a finite, commutative R-group scheme. Then the following facts hold true.*

1. *G^D is a finite commutative S-group scheme.*
2. *$(G^D)^D \simeq G$.*
3. *For all $H, G \in \mathsf{Gp}/S$ finite commutative $\mathrm{Hom}_{\mathsf{Gp}/S}(G,H) \simeq \mathrm{Hom}_{\mathsf{Gp}/S}\left(H^D, G^D\right)$.*
4. *Forming G^D commutes with base change.*

Remark 2.43. Duals of finite commutative group schemes inherit some other properties, in fact $[G^D : S] = [G : S]$. Moreover the dual of a short exact sequence is short exact.

One can also interpret duality from a different point of view. Here the relevant notions.

Definition 2.44: Characters of S-groups.
Let G be an S-group scheme. A *character* of G is a homomorphism of S-groups

$$\chi \colon G \longrightarrow \mathbb{G}_{m,S}.$$

Remark 2.45 ([Wat79, §2.4], Dual as hom functor)**.** Characters form a group in the set of morphism of S-schemes between G and $\mathbb{G}_{m,S}$, the base change of $\mathbb{G}_m$ to S. Then one can introduce the contravariant sheaf hom functor, also called internal hom functor, from Sch/S to Ab

$$\mathcal{H}\mathrm{om}_{\mathsf{Gp}/S}(G, \mathbb{G}_{m,S}) : T \longmapsto \mathrm{Hom}_{\mathsf{Gp}/T}(G_T, \mathbb{G}_{m,T}).$$

Then, for a finite, commutative S-group G we have the isomorphism

$$G^D \simeq \mathcal{H}\mathrm{om}_{\mathsf{Gp}/S}(G, \mathbb{G}_{m,S}).$$

This is actually one of the cases in which the above hom functor is representable.

Let's now give a few examples of dual group schemes among the ones we introduced so far:

Example 2.46.

1. The dual algebra of R^Γ is $R[\Gamma]$ and viceversa. Hence diagonalizable finite group schemes are dual to constant commutative group schemes. In particular this yields that μ_n is dual to $\underline{\mathbb{Z}/n\mathbb{Z}}$ and viceversa.

2. One can show that $\alpha_p^D \simeq \alpha_p$. In fact we can view α_p^D as the character group

   $$\mathrm{Hom}_{\mathsf{Gp}/S}(\alpha_{p,S}, \mathbb{G}_{m,S}).$$

   To see this we can reduce to the case where $S = \mathrm{Spec}(\mathbb{F}_p)$. The result holds in general due to compatibility of the construction of dual group scheme with base change. Then, for any $\mathbb{F}_p$-algebra R, we can define the exponential map

   $$\begin{aligned} \exp \colon \alpha_p(R) &\longrightarrow \mathbb{G}_{m,\mathbb{F}_p} \\ r &\longmapsto \exp(r) \coloneqq 1 + r + \tfrac{r^2}{2!} + \cdots + \tfrac{r^{p-1}}{(p-1)!}. \end{aligned}$$

   With this notation it can be shown that, for any $T \in \mathsf{Sch}/\mathbb{F}_p$, self duality is given by

   $$\begin{aligned} \alpha(T) &\xrightarrow{\sim} \mathrm{Hom}_{\mathsf{Gp}/\mathbb{F}_p}\left(\alpha_p, \mathbb{G}_{m,\mathbb{F}_p}\right) \\ \xi &\longmapsto (r \mapsto \exp(\xi \cdot r)). \end{aligned}$$

2.5 Frobenius and Verschiebung

Let's now study a few constructions in characteristic p: let R be a ring with $\operatorname{char} R = p$.

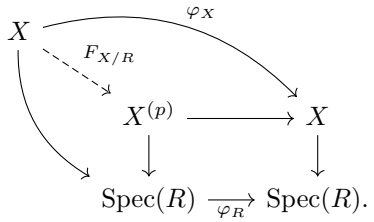
Definition 2.47.
For any R-algebra A, denote by $\varphi_A \colon A \to A$ the morphism acting by $a \mapsto a^p$. It induces $\operatorname{Spec}(\varphi_A) \colon \operatorname{Spec}(A) \to \operatorname{Spec}(A)$, which is the identity at the level of topological spaces. This map, moreover, can be glued for any R-scheme X, giving rise to a map $\varphi_X : X \to X$ such that

1. it is the identity at the level of topological spaces,
2. for any $U \subset X$ open, it induces the p-power map as a ring homomorphism $\mathcal{O}_X(U) \to \mathcal{O}_X(U)$.

We will denote by $X^{(p)}$ the fibered product

$$\begin{array}{ccc} X^{(p)} \coloneqq X \times_R \operatorname{Spec}(R) & \longrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec}(R) & \xrightarrow[\varphi_R]{} & \operatorname{Spec}(R). \end{array}$$

Finally we can construct the map $F_{X/R} \colon X \to X^{(p)}$, which we will denote simply by F_X when the base scheme is clear, as the unique map making the following diagram commute:



Definition 2.48: Frobenius morphism.
For R a ring of characteristic p, and X an R-scheme, we define

1. $\varphi_X : X \to X$ the *absolute Frobenius morphism* of X,
2. $F_X : X \to X^{(p)}$ the *relative Frobenius morphism* of X.

Remark 2.49. Notice that the relative Frobenius F_X is a morphism of R-schemes, for all $X \in \mathsf{Sch}/R$. Instead the absolute Frobenius φ_X, in general, is not.

Notation 2.50.
Given a morphism of R-schemes $f : X \to Y$, we define

$$f^{(p)} \coloneqq f \times \mathrm{id}_R \colon X^{(p)} \longrightarrow Y^{(p)}.$$

Lemma 2.51. *If G is an R-group scheme, for R a ring of characteristic p, the relative Frobenius $F_G \colon G \to G^{(p)}$ is a homomorphism of R-group schemes.*

Definition 2.52: Nilpotent Frobenius.

1. We set, for any $X \in \mathsf{Sch}/S$ and any integer $n \geq 0$, $X^{(0)} \coloneqq X$ and $X^{(p^{n+1})} \coloneqq \left(X^{(p^n)}\right)^{(p)}$. Then we denote by $F_X^n \colon X \to X^{(p^n)}$ the n-fold composition

$$X \xrightarrow{F_X} X^{(p)} \xrightarrow{F_{X^{(p)}}} \cdots \longrightarrow X^{(p^{n-1})} \xrightarrow{F_{X^{(p^{n-1})}}} X^{(p^n)}.$$

2. Assume now that $G \coloneqq X$ is an S-group scheme. By lemma 2.51 F_G^n is a group scheme homomorphism. We say that F_G is *nilpotent* iff there is an integer $n \geq 1$ such that F_G^n is the trivial homomorphism.

The following results hold for group schemes over a field, hence we will replace R by a field k of characteristic $p > 0$.

Proposition 2.53. *Let G be a finite k-group scheme. The following are equivalent:*

1. *G is étale,*
2. $\ker F_G = 1$,
3. *F_G is an isomorphism.*

Proposition 2.54. *Let G be a finite commutative k-group scheme. Then G is connected iff F_G is nilpotent.*

Definition 2.55: Verschiebung.
Let G be a finite, commutative R-group scheme. By theorem 2.42 $(G^{(p)})^D \simeq (G^D)^{(p)}$. One defines the *Verschiebung*, german for "the shift", homomorphism

$$V_G \coloneqq F_{G^D}^D \colon G^{(p)} \longrightarrow G$$

as the dual to $F_{G^D} \colon G^D \to (G^D)^{(p)} \simeq (G^{(p)})^D$, recalling that $((G^{(p)})^D)^D \simeq G^{(p)}$ and $(G^D)^D \simeq G$.

Remark 2.56.

1. By Cartier duality one sees that $F_G^D = V_{G^D}$ and $V_G^D = F_{G^D}$.
2. One constructs V_G^n by successive compositions as for F_G^n. Then we say that V_G is nilpotent iff there exists an integer $n \geq 1$ such that V_G^n is the trivial homomorphism.

Let's briefly quote a result, which is dual to proposition 2.53 and proposition 2.54.

Proposition 2.57. *Let G be a finite commutative k-group scheme. Then the following hold true.*

1. *$\operatorname{coker} V_G = 1$ iff V_G is an isomorphism iff G^D is étale.*
2. *V_G is nilpotent iff G^D is connected.*

We will conclude this section with a famous and useful relation between Frobenius and Verschiebung.

Theorem 2.58 ([Mil17, §11.i])**.** *Let G be a finite commutative k-group scheme. Then the following diagram commutes*

$$\begin{array}{ccccc} G & & \xrightarrow{p\cdot \mathrm{id}_G} & & G \\ & \searrow^{F_G} & & \nearrow_{V_G} & & \searrow^{F_G} \\ & & G^{(p)} & & \xrightarrow[p\cdot \mathrm{id}_{G^{(p)}}]{} & & G^{(p)}, \end{array}$$

where $p \cdot \mathrm{id}_G$ denotes the multiplication by p on G.

3 p-divisible groups

The aim of this section is to introduce, from two different points of view, the notions of *formal Lie group* and of *p-divisible group*, and to show how the two concepts are related to one another. Before doing so, though, we need to introduce a new notion, that of formal scheme.

3.1 Formal schemes

These definitions are meant to allow to capture infinitesimal information which is not present in the construction of schemes. We will not have time to discuss such interpretation, and will only restrict to stating the definitions and results which will be needed in what follows. This section is strongly inspired from [Stacks, Section 0AHY], which in turn bases itself on [EGA, Chapter I, §10]. Let's start by recalling a few useful algebra definitions.

Definition 3.1: Topological rings and modules.

1. We say that a ring R is a *topological ring* iff it is a ring endowed with a topology such that both addition and multiplication are continuous maps $R \times R \to R$, where $R \times R$ is taken with the product topology.
2. We say that an R-module M, where R is a topological ring, is a *topological module* iff M is endowed with a topology such that addition and scalar multiplication are both continuous, again with their sources taken with the product topology.
3. We say that R is *linearly topologized* iff 0 has a fundamental system of neighbourhoods consisting of ideals. Analogously M is *linearly topologized* iff 0 has a fundamental system of neighbourhood consisting of submodules.
4. If R is linearly topologized, we say that the ideal $I \triangleleft R$ is an *ideal of definition* iff I is open and every neighbourhood of 0 contains I^n for an appropriate $n \in \mathbb{N}$.
5. $\mathscr{R}$ is *admissible* iff it has an ideal of definition and it is *complete*.

Definition 3.2: Completed tensor product.
Let R be a topological ring and M, N be linearly topologized R-modules. Let $M_\mu \triangleleft M$ and $N_\nu \triangleleft N$ run through fundamental systems of open submodules of M and N respectively. We endow the tensor product of M and N with the linear topology defined by the fundamental system of open submodules

$$\mathrm{im}\{M_\mu \otimes_R N + M \otimes_R N_\nu \longrightarrow M \otimes_R N\}.$$

Then we define the *completed tensor product* as the completion of the tensor product with respect to the topology we just defined, i.e. as

$$M \widehat{\otimes}_R N \coloneqq \varprojlim \frac{M \otimes_R N}{M_\mu \otimes_R N + M \otimes_R N_\nu} = \varprojlim M/M_\mu \otimes_R N/N_\nu.$$

Remark 3.3. In the case where R is a complete topological ring, $M = R[\![X_1, \dots, X_n]\!]$ and $N = R[\![Y_1, \dots, Y_m]\!]$, one obtains the isomorphism

$$R[\![X_1, \dots, X_n]\!] \widehat{\otimes}_R R[\![Y_1, \dots, Y_m]\!] \simeq R[\![S_1, \dots, S_n, T_1 \dots, T_m]\!].$$

Above we denoted by $S_j \coloneqq X_j \otimes 1$ and by $T_j \coloneqq 1 \otimes Y_j$.

Definition 3.4: Pseudo-discrete sheaves.
A sheaf $\mathcal{F}$ of topological rings (resp. topological modules, topological groups, etc) is called *pseudo-discrete* iff $\mathcal{F}(U)$ is endowed with the discrete topology, for all open $U \subset X$.

Definition 3.5: Associated pseudo-discrete sheaf.
Let X be a topological space with a basis of the topology consisting of quasi compact open subsets (for example $\mathrm{Spec}(R)$ for a ring R). Given any sheaf $\mathcal{F}$ of rings (resp. modules, groups, etc) we define the *associated pseudo-discrete sheaf*, still denoted by $\mathcal{F}$, as the sheaf of *topological* rings (resp. topological modules, topological groups, etc) with topologies defined as follows. To each $U \subset X$ open and quasi compact we endow $\mathcal{F}(U)$ with the discrete topology. For an arbitrary open $U = \cup_{i\in I} U_i$, where U_i are all quasi compact open, we endow $\mathcal{F}(U)$ with the induced topology from $\Pi_{i\in I}\mathcal{F}(U_i)$, via the inclusion in the definition of sheaf, which comes from the exact sequence in remark 1.14.

Remark 3.6. In the above one should verify good definition of the topology. For questions of space we will leave these verifications to [Stacks, Section 0AHY] and [EGA, Chapter I, §10].

Definition 3.7: Locally topologically ringed spaces.
We define a *locally topologically ringed space*, for short *ltrs*, to be a pair $(X, \mathcal{O}_X)$ consisting of a topological space X and a sheaf of topological rings $\mathcal{O}_X$, whose stalks are local rings. A *morphism of locally topologically ringed spaces* $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a pair $\left(f, f^{\#}\right)$, where $f\colon X \to Y$ is a continuous map and $f^{\#}\colon \mathcal{O}_Y \to f_*\mathcal{O}_X$ is a morphism of sheaves such that, for all $V \subset Y$ open, the map

$$f_V^{\#}\colon \mathcal{O}_X(V) \longrightarrow \mathcal{O}_X(f^{-1}(V))$$

is continuous and, for all $x \in X$, the induced map at the level of stalks

$$f_x^{\#}\colon \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$$

is a local homomorphism of local rings (here we forget about topology). We define the category of locally topologically ringed spaces, denoted by ltrs, as the category whose objects and morphism have just been described.

We now have enough basic definitions to give that of formal scheme. Let's notice that this construction follows that of [EGA, Chapter I, §10], hence all of the verifications can be checked there.

Definition 3.8: Affine formal scheme.

1. Let $\mathscr{A}$ be an *admissible ring*, with fundamental system of neighbourhoods $\{I_\lambda\}_{\lambda\in\Lambda}$. We define
$$\mathrm{Spf}(\mathscr{A}) \coloneqq \{\mathfrak{p} \lhd \mathscr{A} \mid \mathfrak{p} \text{ is open and prime}\} \subset \mathrm{Spec}(\mathscr{A}),$$
and endow $\mathrm{Spf}(\mathscr{A})$ with the subset topology. For each $\lambda \in \Lambda$, one can associate, as in definition 3.5, to the structure sheaf $\mathcal{O}_{\mathrm{Spec}(\mathscr{A}/I_\lambda)}$ of $\mathrm{Spec}(\mathscr{A}/I_\lambda)$, a pseudo-discrete sheaf, which we will denote by $\mathcal{O}_\lambda$. One should also notice that, since $\mathscr{A}$ is admissible, $\mathrm{Spec}(\mathscr{A}/I_\lambda)$ has indeed the same topological space as $\mathrm{Spf}(\mathscr{A})$ for all I_λ. Moreover, for $I_\lambda \subset I_\mu$, one has an induced homomorphism
$$\mathrm{Spec}(\mathscr{A}/I_\mu) \longrightarrow \mathrm{Spec}(\mathscr{A}/I_\lambda),$$
which gives rise to a compatible system. Then one defines
$$\mathcal{O}_{\mathrm{Spf}(\mathscr{A})} \coloneqq \varprojlim_{\lambda\in\Lambda} \mathcal{O}_\lambda,$$
where the limit is taken in the category of sheaves of topological rings. Finally one defines the pair $(\mathrm{Spf}(\mathscr{A}), \mathcal{O}_{\mathrm{Spf}(\mathscr{A})})$ to be the *formal spectrum* of $\mathscr{A}$.

2. A *locally topologically ringed space* is said to be an *affine formal scheme* iff it is isomorphic, in ltrs, to the spectrum of an admissible ring. A morphism of affine formal schemes is just a morphism of the underlying locally topologically ringed spaces.

Remark 3.9. As in the definition of associated pseudo-discrete sheaf, in the above there are many details to be checked and filled in. Again we will leave them to [EGA, Chapter I, §10].

Remark 3.10. One can prove that, much like with affine schemes, the category of affine formal schemes is anti-equivalent to that of admissible topological rings. In particular we have

$$\mathrm{Hom}_{\mathsf{ltrs}}\left(\mathrm{Spf}(\mathscr{B}), \mathrm{Spf}(\mathscr{A})\right) \simeq \mathrm{Hom}_{\mathrm{cont}}\left(\mathscr{A}, \mathscr{B}\right),$$

where in the right hand side we considered only continuous morphisms of rings, i.e. morphisms in the category of admissible topological rings.

Definition 3.11: Formal scheme.
A *formal scheme* is a locally topologically ringed space $(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ such that every point has an open neighbourhood isomorphic, in ltrs, to an *affine formal scheme*. A morphism of formal schemes is just a morphism of the underlying locally topologically ringed spaces.

Remark 3.12. Following the construction of associated pseudo-discrete sheaf, one can associate to any sheaf a formal sheaf. This actually gives rise to a fully faithful embedding of the category of schemes in that of formal schemes.

To ease the transition to the study of p-divisible groups let's also recall a couple of results with these objects.

Remark 3.13. Since it will be our main interest, let's restrict to the affine case. Given an admissible ring $\mathscr{A}$, with fundamental system of ideals $\{I_\lambda\}_{\lambda\in\Lambda}$, we have

$$\mathrm{Spf}(\mathscr{A}) \simeq \varinjlim_{\lambda\in\Lambda} \mathrm{Spec}(\mathscr{A}/I_\lambda)$$

in the category of formal schemes. In fact, as can be seen in [EGA, Chapter I, §10.6], one can do a similar construction with formal schemes. Hence we can view these last as inductive limits of ordinary schemes.

Remark 3.14. Moreover, with regards to the construction of p-divisible groups and formal Lie groups, we will follow [Sha86, §5] for the point of view of formal schemes. Then, as we will remark again, we will fix $\mathscr{R}$ a local admissible ring and $S \coloneqq \mathrm{Spec}(\mathscr{R})$. Moreover we will mainly deal with formal affine schemes over S which are given by inductive limits of what Shatz defines *very finite* schemes over S. There, we read that an S-schemes T is very finite iff it satisfies:

1. T is *finite and flat* over S (hence affine) and
2. the $\mathscr{R}$-module $\Gamma\left(T, \mathcal{O}_T\right)$ is of finite length.

Specializing remark 3.10 to the case of this family of formal affine schemes over S, i.e. those which are given by inductive limits of *very finite* S schemes, we obtain an anti-equivalence of categories with the category of profinite $\mathscr{R}$-algebras. This is the setting in which we will state most results in the formal scheme setting in the following sections.

3.2 Formal groups and formal Lie groups

In this section we will define the concept of *formal Lie group*, generalizing that of Lie group, i.e. that of group in the category of complex analytic manifolds, without the restriction of convergence of the series defining the group operation.

Starting from this section we will define concepts both in terms of formal schemes, borrowing from [Sha86], and in terms of fppf sheaves, borrowing from [Mes72].

Formal schemes point of view

As anticipated in remark 3.14, we fix $\mathscr{R}$ a local admissible ring, $S \coloneqq \mathrm{Spec}(\mathscr{R})$ and we work only with inductive limits of *very finite* S-schemes.

Definition 3.15: Formal group schemes.
A *formal group scheme* is just a group object, as defined in remark 2.6, in the category of formal schemes. Analogously a *formal S-group scheme* is a group object in the category of formal schemes over S.

Remark 3.16. As with the case of group schemes, in the affine case $G = \mathrm{Spf}(\mathscr{A})$, one defines, on $\mathscr{A}$, comultiplication, antipode and counit morphisms with the usual properties of definition 2.12. One should note, though, that in the category of profinite R-algebras, the coproduct is given by the completed tensor product, hence the comultiplication is a morphism

$$\widetilde{m}\colon \mathscr{A} \longrightarrow \mathscr{A}\widehat{\otimes}_R\mathscr{A}.$$

One can generalize the results of theorem 2.37 to this new setting.

Theorem 3.17 ([Sha86, §5])**.** *Let G be a formal group scheme over S. Then there is a canonical short exact sequence*

$$1 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{\text{ét}} \longrightarrow 1,$$

in which G^0 is a connected normal formal subgroup of G and $G^{\text{ét}}$ is an étale formal group.

The following definition is not the most general one, but the right one in our context.

Definition 3.18: Formal Lie variety.

1. A formal S-scheme G is said to be *smooth* iff G^0, as defined in theorem 3.17, is the formal spectrum of a power series ring over $\mathscr{R}$.
2. A *formal Lie variety* over S is a smooth, connected formal S-scheme.

Definition 3.19: Formal Lie group.
A *formal Lie group* is a group object in the category of formal Lie varieties. More explicitly it is $\Gamma \coloneqq \mathrm{Spf}\,(\mathscr{A})$, where $\mathscr{A} \coloneqq \mathscr{R}[\![X_1, \ldots, X_n]\!]$. Then n is its dimension.

Remark 3.20. As stated in remark 3.16, since a formal Lie group is an affine formal scheme, one gets a Hopf algebra structure on $\mathscr{A}$. As formal Lie groups are often introduced giving focus only on the comultiplication morphism and its axioms, we will recall them here, with names which can be found in the literature. More explicitly comultiplication of the formal Lie group $\mathrm{Spf}(\mathscr{A})$ is a morphism of topological rings

$$f\colon \mathscr{A} \longrightarrow \mathscr{A}\widehat{\otimes}_{\mathscr{R}}\mathscr{A} = \mathscr{R}[\![X_1, \ldots, X_{2n}]\!],$$

satisfying the following conditions:

1. *ε axiom:* $X = f(X, 0) = f(0, X)$;
2. *coassociativity:* $f(X, f(Y, Z)) = f(f(X, Y), Z)$;
3. *commutativity:* $f(X, Y) = f(Y, X)$.

Notice that any such morphism f is just the data of $(f_i(Y,Z))_{i=1}^n$, power series in $2n$ variables, where f_i is the image of X_i via f. Again, as is often found in the literature, one denotes the image of comultiplication by

$$X * Y \coloneqq f(X,Y).$$

One can also prove that these axioms are enough to grant the existence of the inverse for any element of Γ, hence they suffice to give Γ a formal group scheme structure.

Finally a note on the terminology and the axioms. At first one can notice that we have never explicitly asked a formal Lie group to be commutative, but we have added the axiom here. In fact, much like the choice of introducing them via the explicit description of the group law, this is a choice which brings this definition closer to the analogous concept of Lie groups over complex analytic manifolds. Moreover, in the future, we will mainly concentrate on Lie groups related to p-divisible groups, which are assumed to be commutative.

Definition 3.21: p-divisible formal Lie group.
We define the map multiplication by p on $\Gamma \coloneqq \mathrm{Spf}(\mathscr{A})$ as the map $p\colon \Gamma \to \Gamma$ associated to

$$\begin{aligned} \psi\colon \mathscr{A} &\longrightarrow \mathscr{A} \\ X &\longmapsto X * \cdots * X \quad (p \text{ times}). \end{aligned}$$

If, moreover, Γ is a formal Lie group, it is said to be *p-divisible* iff the map p is an isogeny, i.e. it is surjective and has finite kernel. This means that $\mathscr{A}$ is a *free* module of finite rank over itself.

fppf sheaves point of view

In the following part we will always write groups over S, or S-group, to mean an fppf sheaf of commutative groups on the site $(\mathsf{Sch}/S)_{\mathrm{fppf}}$. Also the schemes $X, Y \in \mathsf{Sch}/S$ will be viewed, via the associated functor of points, as sheaves on S for the fppf topology. Recall that, for $Y \in \mathsf{Sch}/S$, sections on $T \in \mathsf{Sch}/S$ of Y are just T-points and, as usual with sheaves, we denote them by

$$\Gamma(T,Y) \coloneqq Y(T).$$

Notation 3.22.
To differentiate the above definition of S-group, which does not require representability, from that of definition 2.9, we will denote the category of group schemes as fppf sheaves by Gr/S, as opposed to Gp/S.

Remark 3.23. Since the category of commutative groups, i.e. Ab, is abelian we see that Gr/S inherits two important properties. First of all, as proved in [Stacks, Lemma 03CN], Gr/S is an abelian category. Moreover, as proved in [Stacks, Theorem 01DP], it has enough injectives.

Remark 3.24. Since the category Gr/S does not require representability, to define the pullback for a morphism of schemes $f\colon S \to S'$ we need to use the localization morphism of topoi, as defined in definition 1.21.

Definition 3.25: kth infinitesimal neighbourhood.
Let $Y \hookrightarrow X$ be a monomorphism of fppf sheaves on Sch/S. We define $\mathrm{Inf}_Y^k(X)$ as the subsheaf of X whose sections over an S-scheme T are given as follows. The sections $\Gamma(T, \mathrm{Inf}_Y^k(X))$ consist of all $t \in \Gamma(T,X)$ such that there is an fppf covering $\{T_i \to T\}_{i\in I}$ of T and, for each i, a closed subscheme T_i' of T_i, defined by an ideal whose $(k+1)$ power is (0), with the property that every element $t|_{T_i'} \in \Gamma(T_i', X)$ is already an element of $\Gamma(T_i', Y)$.

Notation 3.26.
Let X be a sheaf on S, with a section $e_X : S \to X$. If this section is clear from context, e.g. in case we have (X, e_X) a pointed sheaf on S, i.e. a sheaf on S given with a section $e_X : S \hookrightarrow X$, we will write $\mathrm{Inf}^k(X)$ instead of $\mathrm{Inf}^k_S(X)$.

Remark 3.27. Notice that, when $G = X$ is an S-group, it is canonically a pointed sheaf (G, e_G) on S, with immersion $e_G : S \to G$ given by the unit section, i.e. the unique section whose image is the unit of the group G. In the following we will implicitly assume this, and write only G to denote the pointed sheaf (G, e_G).

Notation 3.28.
For a scheme S and an S-group $G \in \mathsf{Gr}/S$, we introduce the notation

$$\overline{G} \coloneqq \varinjlim_{k \in \mathbb{N}} \inf^k(G),$$

where the limit is taken with respect to the natural inclusion morphisms.

Definition 3.29: Ind-infinitesimal sheaf.
A pointed sheaf (X, e_X) is called *ind-infinitesimal* iff, as an *fppf sheaf*, $X = \overline{X}$.

Right now we need to introduce a couple more concepts from algebraic geometry to make sense of the definitions which are at the heart of this section.

Definition 3.30: Conormal sheaf of an immersion.
Let $\iota : Z \to X$ be a closed immersion of schemes. Let $\mathcal{I} \subset \mathcal{O}_X$ be the corresponding quasi-coherent sheaf of ideals. Then the sheaf $\mathcal{I}/\mathcal{I}^2$ is annihilated by $\mathcal{I}$, hence it corresponds to a sheaf on Z. This last sheaf, denoted with ω_ι, is called the *conormal sheaf* of Z in X, or the conormal sheaf of the immersion ι. In case we are given (X, e_X), a pointed sheaf on S, we will denote the conormal sheaf of the immersion e_X simply by ω_X.

Definition 3.31: Symmetric and exterior powers.
Let $(X, \mathcal{O}_X)$ be a ringed space and $\mathcal{F}$ be an $\mathcal{O}_X$-module.

1. We define the *tensor algebra* of $\mathcal{F}$ to be the sheaf of noncommutative $\mathcal{O}_X$-algebras

$$\mathrm{T}(\mathcal{F}) = \mathrm{T}_{\mathcal{O}_X}(\mathcal{F}) \coloneqq \bigoplus_{n \geq 0} \mathrm{T}^n(\mathcal{F}),$$

   where $\mathrm{T}^0(\mathcal{F}) \coloneqq \mathcal{O}_X$, $\mathrm{T}^1(\mathcal{F}) \coloneqq \mathcal{F}$ and, for all $n \geq 2$,

$$\mathrm{T}^n(\mathcal{F}) \coloneqq \mathcal{F} \otimes_{\mathcal{O}_X} \cdots \otimes_{\mathcal{O}_X} \mathcal{F} \quad (n \text{ times}).$$

2. We define the *exterior algebra* of $\mathcal{F}$, denoted by $\bigwedge \mathcal{F}$, to be the quotient of $\mathrm{T}(\mathcal{F})$ by the two sided ideal generated by local sections of the form $s \otimes s$ of $\mathrm{T}^2(\mathcal{F})$, where s is a local section of $\mathcal{F}$.

3. We define the *symmetric algebra* of $\mathcal{F}$, denoted by $\mathrm{Sym}(\mathcal{F})$, to be the quotient of $\mathrm{T}(\mathcal{F})$ by the two-sided ideal generated by local sections of the form $s \otimes t - t \otimes s$ of $\mathrm{T}^2(\mathcal{F})$, where s and t are local sections of $\mathcal{F}$.

Remark 3.32.

1. Both $\bigwedge \mathcal{F}$ and $\mathrm{Sym}(\mathcal{F})$ are graded $\mathcal{O}_X$-algebras, whose grading is inherited from $\mathrm{T}(\mathcal{F})$. Moreover $\mathrm{Sym}(\mathcal{F})$ is commutative, whereas $\bigwedge \mathcal{F}$ is graded-commutative.

2. If $\mathcal{F}$ is a *quasi-coherent* (resp. *locally-free*) sheaf of $\mathcal{O}_X$-modules, then each of $T(\mathcal{F})$, $\bigwedge \mathcal{F}$ and $\mathrm{Sym}(\mathcal{F})$ are *quasi-coherent* (resp. *locally-free*), see [Stacks, Lemma 01CL].

And now back to our interests.

Definition 3.33: Formal Lie variety.
A pointed sheaf (X, e_X) on S is said to be a *formal Lie variety* iff it satisfies the following:

1. X is ind-infinitesimal, i.e. $X = \overline{X} = \varinjlim \mathrm{Inf}^k(X)$, and $\mathrm{Inf}^k(X)$, viewed as a sheaf in the fppf topology, is representable for all $k \geq 0$;
2. $\omega_X \simeq e_X^*\left(\Omega^1_{X/S}\right) \simeq e_X^*\left(\Omega^1_{\mathrm{Inf}^k(X)/S}\right)$, for any $k \in \mathbb{N}$, is *locally-free of finite type*;
3. Denoting by $\mathrm{gr}^{\mathrm{inf}}(X)$ the unique graded $\mathcal{O}_S$-algebra such that $\mathrm{gr}_i^{\mathrm{inf}}(X) = \mathrm{gr}_i(\mathrm{Inf}^i(X))$, we have an isomorphism

$$\mathrm{Sym}\left(\omega_X\right) \xrightarrow{\sim} \mathrm{gr}^{\mathrm{inf}}(X)$$

induced by the canonical mapping $\omega_X \xrightarrow{\sim} \mathrm{gr}_1^{\mathrm{inf}}(X)$.

Remark 3.34 ([Mes72, Chapter II, §1])**.** From this definition it follows that X, locally on S, is isomorphic to $\mathcal{O}_S[\![T_1, \ldots, T_n]\!]$. In particular, following the assumptions made for the formal scheme point of view, it grants that X is given by $R[\![T_1, \ldots, T_n]\!]$, where $S = \mathrm{Spec}(R)$.

Definition 3.35: Formal Lie group.
A *formal Lie group* over S is a group object G in the category of formal Lie varieties over S.

In the following we will always assume that a formal Lie group G is commutative. Moreover, for these last results, we will assume that our base scheme S is of characteristic $p > 0$.

Remark 3.36 (Frobenius and Verschiebung)**.** One can generalize the definitions given for finite commutative group scheme in section 2.5. In fact, looking at how they act on S-points, these definitions can be generalized to any contravariant functor from Sch/S to Sets. Then one defines, on any sheaf of groups G, a Frobenius morphism, denoted again by $F_G \colon G \to G^{(p)}$, and a Verschiebung morphism, denoted by $V_G \colon G^{(p)} \to G$. Moreover, as in definition 2.52, we denote by $F_G^n \colon G \to G^{(p^n)}$ the n-fold composition of the Frobenius morphism.

Definition 3.37.

1. We denote by $G[n] \coloneqq \ker F_G^n$, the kernel of the n-fold composition of the Frobenius morphism.
2. A sheaf of groups G on S is said to be of *F-torsion* iff $G = \varinjlim_{n \in \mathbb{N}} G[n]$.
3. A sheaf of groups G on S is said to be *F-divisible* iff $F_G \colon G \to G^{(p)}$ is an epimorphism.

With this in mind we can more easily characterize the formal Lie groups over S of characteristic p.

Theorem 3.38 ([Mes72, Chapter II, §2, theorem 2.1.7])**.** *In order for a sheaf of groups G on S to be a formal Lie group, it is necessary and sufficient that the following conditions hold:*

1. *G is of F-torsion;*
2. *G is F-divisible;*

3. the $G[n]$ are finite and locally-free S-group schemes.

For the following result assume that the base scheme $S = \mathrm{Spec}(A)$ is the affine scheme associated to an admissible ring with ideal of definition I. Assume moreover that I/I^2 is of finite type over A/I and set $S_n \coloneqq \mathrm{Spec}(A/I^{n+1})$.

Lemma 3.39 ([Mes72, Chapter 2, §4, lemma 4.13])**.** *The natural functor associating to a formal Lie variety over S a family of formal Lie varieties over S_n is an* equivalence of categories*. In particular it induces an equivalence of categories between formal Lie groups on S and the inverse limit of the categories of formal Lie groups on the various S_ns.*

Remark 3.40 (Comparison of the two points of view)**.** We can see, thanks to theorem 3.38, remark 3.34, and definition 3.19, that the two definitions of formal Lie group coincide, over $S = \mathrm{Spec}(R)$, where R is a local admissible ring. In fact from the definition as an fppf sheaf of groups, we obtain that G is F-torsion. As a consequence every $G[n]$, up to base change to the residue field, satisfies conditions of proposition 2.54, which grants connectedness. Moreover we see that G is given by a ring of formal power series, hence it is smooth. For the converse we recall theorem 1.16, remark 3.14 and theorem 2.58 and then have to argue following [Tat67, proposition 1], see also [Mes72, Chapter II, §2, theorem 2.1.7] for some more details.

3.3 p-divisible groups

As in the previous section, we will define p-divisible groups from two different points of view: that of formal schemes and that of fppf sheaves.

Formal scheme point of view

In this section we will follow the construction of [Tat67, §2] and of [Sha86, §6]. In particular we will see a p-divisible group as a formal group satisfying certain important properties. As before, sticking to the convention of [Sha86], we will denote by $\mathscr{R}$ an admissible local ring (and often assume that it also has residue characteristic p).

Definition 3.41: p-divisible group.
A *p-divisible group* over $\mathscr{R}$ of height $h \in \mathbb{N}_+$ is an inductive system

$$G \coloneqq (G_v, i_v)_{v\in\mathbb{N}}\,,$$

satisfying:

1. for each $v \in \mathbb{N}$, G_v is a finite, flat and commutative group scheme over $\mathscr{R}$ of order p^{vh};
2. for each $v \in \mathbb{N}$, there is an exact sequence

$$0 \longrightarrow G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1},$$

where the second map is the multiplication by p^v in G_{v+1}, hence the first is a closed immersion which identifies G_v with the kernel of p^v on G_{v+1}.

Remark 3.42. Recalling remark 3.14 we see that the inductive system $(G_v, i_v)_{v\in\mathbb{N}}$ defines a formal group

$$G \coloneqq \varinjlim_{v\in\mathbb{N}} G_v.$$

Even though this remark allows to associate an object to a p-divisible group, we will mostly work directly with the inductive system.

As of now the reason behind the name *p-divisible* is still not clear. The following proposition and remark will clarify it.

Proposition 3.43. *A p-divisible group over $\mathscr{R}$ is a p-torsion commutative formal group G over $\mathscr{R}$, for which $p\colon G \to G$ is an* isogeny.

Proof. Since, for all $v \in \mathbb{N}$, i_v is a monomorphism, the following diagram shows that G_v is the kernel of p^v on G_{v+2} via the iterated immersion $i_{v+1} \circ i_v$. Inductively this holds for G_{v+t}, where $t \geq 1$:

$$\begin{array}{ccccccc} & & & & G_{v+2} & \xrightarrow{p^v} & G_{v+2} & \xrightarrow{p} & G_{v+2} \\ & & & & \uparrow{\scriptstyle i_{v+1}} & & \uparrow{\scriptstyle i_{v+1}} & & \\ 0 & \longrightarrow & G_v & \xrightarrow[i_v]{} & G_{v+1} & \xrightarrow[p^v]{} & G_{v+1}. & & \end{array}$$

As a consequence G_v is the kernel of p^v on G, hence G is p-torsion (it is $\varinjlim G_v$). To simplify the discussion we will introduce the notation $i_{v,t} \coloneqq i_v \circ \cdots \circ i_{v+t}\colon G_v \to G_{v+t}$. Then we analyze the following diagram to obtain that p is an isogeny:

$$\begin{array}{ccccc} G_{v+t+1} & \xrightarrow{\quad p^t \quad} & G_{v+t+1} & \xrightarrow{p^v} & G_{v+t+1} \\ \uparrow{\scriptstyle i_{v+t}} & \nearrow{\scriptstyle i_{v,t+1}} & & & \uparrow{\scriptstyle i_{v+t}} \\ & G_v & & & \\ & {\scriptstyle j_{t,v}}\nearrow & \searrow{\scriptstyle i_{v,t}} & & \\ G_{v+t} & & \xrightarrow[p^t]{} & & G_{v+t}. \end{array} \tag{3.1}$$

In fact the big square commutes and condition 2 of the definition of p-divisible group, applied to G_{v+t}, implies that $p^t \circ i_{v+t}$ factors through the kernel of p^v on G_{v+t+1}. As seen above this is G_v, granting the existence of the dashed arrow $j_{t,v}$. Moreover we obtain the commutativity of the right triangle by definition of inductive system. As a consequence, since i_{v+t} is a monomorphism, also the lower triangle commutes, granting $i_{v,t} \circ j_{t,v} = p^t$. Then, as also $i_{v,t}$ is a monomorphism, $\ker j_{t,v}$ coincides with the kernel of p^t on G_{v+t}, which is G_t by the above discussion. Then, by property 1 of p-divisible groups, the order of G_{v+t} is the product of the orders of G_v and G_t. Then, by arguments of order, the following is a short exact sequence of abelian S-group schemes

$$0 \longrightarrow G_t \xrightarrow{i_{t,v}} G_{v+t} \xrightarrow{j_{t,v}} G_v \longrightarrow 0. \tag{3.2}$$

Let's remark that these computation do not depend on the chosen $t \geq 1$ nor on the chosen v. Hence the above sequence is exact for all v and t. In particular, fixing $t = 1$ and letting v vary, we obtain that $p\colon G \to G$ is an isogeny, i.e. it is onto and has kernel given by a finite group scheme over S. ∎

Remark 3.44. This proposition actually has an inverse. In fact, starting from a p-torsion commutative formal group G over $\mathscr{R}$, for which $p\colon G \to G$ is an isogeny, we can recover a p-divisible group as in definition 3.41. In fact setting $G_v \coloneqq \ker p^v$, as seen in proposition 3.43, and i_v the inclusion of one kernel into the next gives an inductive system. The height h is given by the exponent in the order of $\ker p$, and one checks that the order of $\ker p^v$ is p^{vh}. Finally $G = \varinjlim_{v\in\mathbb{N}} G_v$ since it is p-torsion.

Example 3.45.

1. In the case of ordinary abelian groups this definition only allows $G_v = (\mathbb{Z}/p^v\mathbb{Z})^h$, hence it just gives rise to the p-divisible group
$$G = \varinjlim G_v = (\mathbb{Q}_p/\mathbb{Z}_p)^h .$$

2. Let $G_v \coloneqq (\mu_{p^v})_{\mathscr{R}}$ be the kernel of multiplication by p^v in $(\mathbb{G}_m)_{\mathscr{R}}$. We can form an inductive system from these objects, which defines the p-divisible group

$$\mu_{p^\infty} = \mathbb{G}_m(p) \coloneqq \varinjlim_{v\in\mathbb{N}} \mu_{p^v},$$

called the *p-divisible group of* $\mathbb{G}_m$. In particular it is of height 1.

3. Denote by $\underline{\mathbb{Z}/p^v\mathbb{Z}}$ the base change to $\mathscr{R}$ of the constant group scheme associated to the group $\Gamma \coloneqq \mathbb{Z}/p^v\mathbb{Z}$, see example 2.20 of item 6. We can form an inductive system from these objects, defining the p-divisible group

$$\underline{\mathbb{Q}_p/\mathbb{Z}_p} \coloneqq \varinjlim_{v\in\mathbb{N}} \underline{\mathbb{Z}/p^v\mathbb{Z}},$$

generalizing to the setting of group schemes example of item 1. As the one before, this p-divisible group is of height 1.

4. In case we are given an n-dimensional commutative formal Lie group Γ over $\mathscr{R}$, we clearly have to require that it is p-divisible, as defined in definition 3.21. Then multiplication by p is an isogeny. In case, moreover, $\mathscr{R}$ is complete and has residue characteristic p, one can define a p-divisible group of height h over $\mathscr{R}$, starting from Γ, by the inductive system

$$\Gamma(p) \coloneqq \left(\Gamma_{p^\nu}, i_{p^\nu}\right)_\nu.$$

In the above Γ_{p^ν} is the kernel of the multiplication by p^ν in Γ. Then one can prove that $\ker p$ is connected and, since p is an isogeny, it is also finite. By proposition 2.38 this implies that the order of $\ker p$ is a power of p. Then flatness allows us to base change to the residue field and invoke theorem 2.58, with which one can extend this result to $\ker p^v$ for all $v \geq 1$. It follows that the construction of $\Gamma(p)$ gives rise to a connected p-divisible group.

5. Let X be an *abelian scheme* of relative dimension d over S. Denote by $X(v)$ the kernel of multiplication by p^v in X. It is known that $X(v)$ is a finire flat and commutative group scheme over S of order p^{2dv}. As a consequence the inductive system $(X(v), i_v)$, where i_v is the natural inclusion, gives rise to a p-divisible group, denoted by $X(p)$, of height $2d$. We call $X(p)$ the p-divisible group of of the abelian scheme S.

Remark 3.46. Even though the above, in item 4, is just a sketch of the construction, of which more details are available at [Sha86, §6], we felt it was useful to quote it in view of the following section.

fppf sheaves point of view

As before, in the following part we will write group over S, or S-group, to mean an fppf sheaf of commutative groups on the site $(\mathsf{Sch}/S)_{\mathrm{fppf}}$. Moreover, following [Mes72], we will call p-divisible groups *Barsotti-Tate groups*.

Lemma 3.47 ([Mes72, Chapter I, §1, lemma 1.1])**.** *Let G be an S-group such that $p^n G = 0$. The following conditions are equivalent:*

1. *G is a flat $\mathbb{Z}/p^n\mathbb{Z}$-module,*
2. *$\ker(p^{n-i}) = \mathrm{im}(p^i)$, for $i = 0, \ldots, n$.*

Definition 3.48: Truncated Barsotti-Tate group of level n.
Consider $n \geq 2$, a *truncated Barsotti-Tate group* of level n is an S-group G such that

1. G is a finite and locally-free group scheme and
2. G is killed by p^n and satisfies the equivalent conditions of lemma 3.47.

Definition 3.49.
If G is a group, we write $G(n)$ for the kernel of p^n. Then, if G is killed by p^n, we write $G = G(n)$.

Lemma 3.50 ([Mes72, Chapter I, §1, lemma 1.5])**.**

1. *If $G(n)$ is a flat $\mathbb{Z}/p^n\mathbb{Z}$-module, then $G(n)$ is a finite, locally-free group scheme iff $G(1)$ is. In such case all the $G(i)$, for $1 \leq i \leq n$, are also finite and locally-free.*
2. *If $G(n)$ is finite and locally-free, then*

$$p^i \colon G(n) \longrightarrow G(n-i)$$

is an epimorphism iff it is faithfully flat.

Definition 3.51: p-torsion and p-divisible groups.
Let S be a scheme and G be an S-group. Denote by $G(n)$ the kernel of the multiplication by p^n on G. The group G is said to be of *p-torsion* iff $\varinjlim_{n\in\mathbb{N}} G(n) = G$. Similarly G is said to be *p-divisible* iff $p \colon G \to G$ is an epimorphism.

Definition 3.52: Barsotti-Tate group.
An S group G is called *Barsotti-Tate* iff it satisfies

1. G is of p-torsion;
2. G is p-divisible;
3. $G(1)$ is a finite, locally-free S-group.

We denote by BT/S the full subcategory of Gr/S whose objects are Barsotti-Tate groups over S.

Remark 3.53. The category BT/S is not abelian: it does not admit kernels. In fact the kernel of the morphism $p \colon G \to G$ of multiplication by p must be killed by p, hence cannot be a Barsotti-Tate group (unless $G = 0$).

Remark 3.54 ([Mes72, Chpater I, §2.4.1])**.** Let $f \colon S' \to S$ be an arbitrary morphism of schemes. Consider BT/S as a subcategory of sheaves of abelian groups on $(\mathsf{Sch}/S)_{\mathrm{fppf}}$ and define, as in definition 1.21, the pullback functor between the appropriate categories of sheaves. Then, for any $G \in \mathsf{BT}/S$, the pullback f^*G, is a Barsotti-Tate group on S'. Moreover we call *lift* of $G \in \mathsf{BT}/S'$ via f any $H \in \mathsf{BT}/S$ such that $f^*H \simeq G$.

Lemma 3.55 ([Mes72, Chapter II, §3, lemma 3.3.18])**.** *Let p be locally nilpotent of S and G be a* Barsotti-Tate *group on S. Then $\overline{G} \coloneqq \varinjlim_{k\in\mathbb{N}} \mathrm{Inf}^k(G)$ is a* formal Lie group*.*

Definition 3.56: Conormal sheaf of a Barsotti-Tate group.
Given a Barsotti-Tate group G over a scheme S, on which p is locally nilpotent, we define the conormal sheaf of G by $\omega_G \coloneqq \omega_{\overline{G}}$ where, as above, $\overline{G} \coloneqq \varinjlim_k \mathrm{Inf}^k(G)$.

Remark 3.57 ([Mes72, Chapter II, §3, remark 3.3.20])**.** In the above hypothesis, thanks to definition 3.33, the sheaf ω_G is locally-free of finite type. Moreover, locally on S, $\omega_G = \omega_{G(m)}$ for m sufficiently large. Finally, if p^N kills S, we have $\omega_G = \omega_{G(N)}$.

As in the section regarding formal Lie varieties, for the following result we will consider the base scheme $S = \mathrm{Spec}(A)$, where A is an admissible ring with ideal of definition I. Assume moreover that I/I^2 is of finite type over A/I and set $S_n \coloneqq \mathrm{Spec}(A/I^{n+1})$.

Lemma 3.58 ([Mes72, Chapter 2, §4, lemma 4.13])**.** *The natural functor associating to a Barsotti-Tate group over S a family of Barsotti-Tate groups over S_n is an* equivalence of categories*. Moreover this equivalence of categories is compatible with extensions.*

Remark 3.59 (Comparison of the two points of view)**.** We will follow [Mes72, Chapter I, §2, remark 2.3 and Chapter II, §3, theorem 2.1.7] to show that the two points of view define the same objects over $S = \mathrm{Spec}(R)$, for an admissible local ring R. Let's start by considering $G \in \mathsf{BT}/S$. Let's denote by $i_{v,t} \colon G(v) \to G(v+t)$ the natural inclusion morphisms. By definition we have $G(v) = G(v+t)(v)$ for all $t \geq 1$. Then, denoting by $i_v \coloneqq i_{v,1}$, this means that $(G_v, i_v)_{v\in\mathbb{N}}$ is an inductive system. Moreover it also means that $G(v)$ is the kernel of multiplication by p^v on G_{v+t} for all t. As a consequence we obtain that the following sequence is exact:

$$0 \longrightarrow G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1}.$$

Hence $(G_v, i_v)_{v\in\mathbb{N}}$ satisfies condition 2 of definition 3.41. Then, since G is p-divisible, i.e. multiplication by p is an epimorphism on G we have that, for any $0 \leq i \leq v$, p^{v-i} induces an epimorphism $G(v) \twoheadrightarrow G(i)$. Combining this with the above remark we obtain the exactness of

$$0 \longrightarrow G(v-i) \xrightarrow{i_{v-i,i}} G(v) \xrightarrow{p^{v-i}} G(i) \longrightarrow 0. \tag{3.3}$$

From the theory of finite group schemes over a field one obtains that the rank of the fiber of $G(1)$ at a point $s \in S$ is of the form $p^{h(s)}$ for a function h which is locally constant on S. Then, from equation (3.3) and multiplicativity of ranks in short exact sequences, see proposition 2.24, we obtain that the rank of the fiber of $G(n)$ at s is $p^{nh(s)}$. As a consequence our inductive system satisfies also 1 of definition 3.41.

Starting from a p-divisible group $(G_v, i_v)_{v\in\mathbb{N}}$, instead, we set $G \coloneqq \varinjlim_{v\in\mathbb{N}} G_v$ and invoke proposition 3.43 to conclude that $G \in \mathsf{BT}/S$.

To end this section we will state a result which relates the concepts introduced in the last couple of sections: that of formal Lie group and of p-divisible group.

Proposition 3.60 ([Tat67, §2, proposition 1])**.** *Let $\mathscr{R}$ be a complete Noetherian local ring whose residue field k is of characteristic $p > 0$. Then the functor $\Gamma \mapsto \Gamma(p)$, constructed as in item 4 of example 3.45, is an equivalence of categories between the category of p-divisible commutative formal Lie groups over $\mathscr{R}$ and the category of connected p-divisible groups over $\mathscr{R}$.*

3.4 Cartier duality

In this section we want to extend the concept of duality introduced in section 2.4 to p-divisible groups. We will do so in the setting of formal schemes, i.e. viewing a p-divisible group as an inductive system of finite, flat and commutative group schemes. In fact we will follow [Sha86, §6] and [Tat67, §2.3] and, again, $\mathscr{R}$ will denote an admissible local ring.

Remark 3.61. Let's notice that for $t = 1$, thanks to remark 2.43, equation (3.2) dualizes to the exact sequence

$$0 \longrightarrow G_v^D \xrightarrow{j_v^D} G_{v+1} \xrightarrow{i_v^D} G_1 \longrightarrow 0.$$

Moreover we see that $\left(G_v^D, j_v^D\right)_{v\in\mathbb{N}}$ defines an inductive system, by construction of j_v (using the universal property defining it). Then, still by remark 2.43, we obtain that it satisfies condition 1 of definition 3.41. Moreover, since $i_{1,v}$ is injective, commutativity of the lower triangle in equation (3.1) shows that $j_v = \mathrm{coker}\, i_{1,v} = \mathrm{coker}\,(p^v \colon G_{v+1} \to G_{v+1})$. But then, since duality is exact, this implies that the inductive system satisfies also property 2 of definition 3.41, hence it defines a p-divisible group.

Definition 3.62: Cartier dual of a p-divisible group.
Let $G \coloneqq (G_v, i_v)_{v\in\mathbb{N}}$ be a p-divisible group over $\mathscr{R}$. Let $G^D \coloneqq \left(G_v^D, j_v^D\right)_{v\in\mathbb{N}}$ be the inductive system defined in remark 3.61. This last inductive system defines a p-divisible group over $\mathscr{R}$ which is called the *Cartier dual* of G.

Remark 3.63. By theorem 2.42, for finite commutative group scheme, the formation of Cartier duals commutes with base change. Since we see a p-divisible group as an inductive limit of finite, flat and commutative group schemes, this also means that taking duals of p-divisible groups commutes with base change.

Example 3.64. Borrowing from example 3.45 we can notice that $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$ is dual to $\mathbb{G}_m(p)$ and viceversa. In fact, by example 2.46, we know that $\underline{\mathbb{Z}/p^n\mathbb{Z}}$ is dual to $\underline{\mu_{p^n}}$ for all $n \in \mathbb{N}$.

It now makes sense to introduce one more definition for p-divisible groups, that of dimension.

Remark 3.65. In the case of p-divisible groups over $\mathscr{R}$, for each $v \in \mathbb{N}$, one obtains the exact connected-étale sequence

$$0 \longrightarrow G_v^0 \longrightarrow G_v \longrightarrow G_v^{\text{ét}} \longrightarrow 0.$$

Moreover one can notice that the inductive system $G^0 \coloneqq \left(G_v^0, i_v^0\right)_{v\in\mathbb{N}}$, where $i_v^0 \coloneqq i_v|_{G_v^0}$, defines a p-divisible group. Then theorem 3.17 gives a short exact sequence in which the first term, G^0, is a connected p-divisible group. By proposition 3.60 we see that $G^0 = \mathrm{Spf}(\mathscr{A})$, for $\mathscr{A} = \mathscr{R}[\![X_1, \ldots, X_n]\!]$ the ring of formal power series in n variables.

Definition 3.66: Dimension of a p-divisible group.
Let $G \coloneqq (G_v, i_v)_{v\in\mathbb{N}}$ be a p-divisible group over $\mathscr{R}$. Consider the connected-étale sequence

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

obtained by theorem 3.17. Thanks to remark 3.65 we see that $G^0 = \mathrm{Spf}(\mathscr{A})$, where $\mathscr{A} = \mathscr{R}[\![X_1, \ldots, X_n]\!]$. We define n to be the *dimension* of the p-divisible group G.

Proposition 3.67 ([Tat67, §2.3, proposition 3])**.** *Let G be a p-divisible group over $\mathscr{R}$ and G^D its dual p-divisible group. Denote by n and n^D their respective dimensions. Then the heights of the two p-divisible groups coincide and the common value, h, satisfies*

$$h = n + n^D.$$

3.5 Tate Modules

In this section we will introduce the Tate module associated to a p-divisible group. This is one of the central objects which will play a role in the comparison morphism. In fact, as stated in the introduction, this object, in the context of abelian varieties, is the dual of the first étale cohomology group.

Then, for this section, we will fix the following notation. Let $K/\mathbb{Q}_p$ be a finite extension and denote by $k \coloneqq O_K/\pi O_K$ the residue field, where π is a uniformizer of K. Let L be the completion of an algebraic extension of K and, as usual, O_L be the ring of integers of L. In particular let's denote by $\overline{K}$ a fixed algebraic closure of K, and by $\mathscr{G}_K = \mathrm{Gal}\left(\overline{K}/K\right)$ the absolute Galois group of K. Let, finally, $G \coloneqq (G_v, i_v)_{v\in\mathbb{N}}$ be a Barsotti-Tate group over O_K.

Definition 3.68.
We define the group of points of G with values in O_L as

$$G(O_L) \coloneqq \varprojlim_{i\in\mathbb{N}} G(O_L/\mathfrak{m}^i O_L),$$

where $\mathfrak{m}$ is the maximal ideal of O_K and where

$$G(O_L/\mathfrak{m}^i O_L) = \varinjlim_{v\in\mathbb{N}} G_v(O_L/\mathfrak{m}^i O_L).$$

Remark 3.69. Let G be a p-divisible group over O_K as in definition 3.41. Then G_v is finite and flat over O_K, for all $v \in \mathbb{N}$. In particular this means that it is proper over O_K, hence that we can apply the valuative criterion of properness, see [Har77, Chapter II, theorem 4.7]. As a consequence we see that, for every $v \in \mathbb{N}$, we have $G_v(L) \simeq G_v(O_L)$. Notice, moreover, that given M/K an infinite algebraic extension and L the p-acid completion of M, then $O_L = \varprojlim_{n\in\mathbb{N}} O_M/\mathfrak{m}^n O_M$ and, for each n, we have

$$O_L/\mathfrak{m}^n O_L = O_M/\mathfrak{m}^n O_M.$$

As a consequence, by definition 3.68, we see that $G(L) = G(O_L) = G(O_M) = G(M)$. In particular the above holds for $M = \overline{K}$ and $L = \mathbb{C}_K$.

Definition 3.70: Tate module.
To the Barsotti-Tate group $G \in \mathsf{BT}/O_K$ we associate the group

$$T_p(G) \coloneqq \varprojlim_{v\in\mathbb{N}} G_v(\overline{K}),$$

called the *Tate module* of G. Here notice that the projective limit is taken over the maps

$$j_v(\overline{K})\colon G_v(\overline{K}) \longrightarrow G_{v-1}(\overline{K}),$$

where j_v corresponds to $j_{1,v}$ constructed in equation (3.1), from proposition 3.43.

Remark 3.71. The module $T_p(G)$ is a free $\mathbb{Z}_p$-module of rank h, where h is the height of G. Moreover it is endowed with a continuous action of $\mathscr{G}_K$. To see how it acts, notice that

$$T_p(G) = \varprojlim_{v\in\mathbb{N}} G_v(\overline{K}) = \varprojlim_{v\in\mathbb{N}} \mathrm{Hom}_{\mathsf{Sch}/O_K}\left(\mathrm{Spec}(\overline{K}), G_v\right) \simeq \varinjlim_{v\in\mathbb{N}} \mathrm{Hom}_{O_K\text{-}\mathsf{Alg}}\left(A_v, \overline{K}\right),$$

where $G_v = \mathrm{Spec}(A_v)$ is affine, being finite over O_K. Here the action of $\mathscr{G}_K$ is the usual action on hom groups, i.e. it is given by

$$(g \cdot f)(x) = g \cdot f(x)$$

for all $g \in \mathscr{G}_K$, $x \in A_v$ and $f \in \mathrm{Hom}_{O_K\text{-}\mathsf{Alg}}\left(A_v, \overline{K}\right)$.

Proposition 3.72. *Consider $G \in \mathsf{BT}/O_K$. Then*

$$T_p(G) \simeq \mathrm{Hom}_{\mathsf{BT}/O_{\overline{K}}}\left(\underline{\mathbb{Q}_p/\mathbb{Z}_p}, G_{O_{\overline{K}}}\right),$$

where $\underline{\mathbb{Q}_p/\mathbb{Z}_p} \coloneqq \varinjlim_{v\in\mathbb{N}} \underline{\mathbb{Z}/p^n\mathbb{Z}}$, as constructed in example 3.45 item 3 with $\mathscr{R} = O_{\overline{K}}$.

Proof. For this proof we will recall definition 3.41 and write $G = \varinjlim_v G_v$. The proof consists of the following isomorphisms.

$$T_p(G) = \varprojlim_{v\in\mathbb{N}} G_v(\overline{K}) \overset{1}{\simeq} \varprojlim_{v\in\mathbb{N}} G_{v,O_{\overline{K}}}(O_{\overline{K}}) \overset{2}{\simeq} \varprojlim_{v\in\mathbb{N}} \mathrm{Hom}_{\mathsf{Gr}/O_{\overline{K}}}\left(\underline{\mathbb{Z}/p^v\mathbb{Z}}, G_{v,O_{\overline{K}}}\right)$$
$$\overset{3}{\simeq} \mathrm{Hom}_{\mathsf{BT}/O_{\overline{K}}}\left(\varinjlim_{v\in\mathbb{N}} \underline{\mathbb{Z}/p^v\mathbb{Z}}, G_{O_{\overline{K}}}\right) \simeq \mathrm{Hom}_{\mathsf{BT}/O_{\overline{K}}}\left(\underline{\mathbb{Q}_p/\mathbb{Z}_p}, G_{O_{\overline{K}}}\right).$$

Let's explain why these isomorphisms hold. Isomorphism 1 is just the valuative criterion of properness, (see [Har77, Chapter II, theorem 4.7]), as seen in remark 3.69. Isomorphism 2 follows from the fact that G_v is a flat $\mathbb{Z}/p^v\mathbb{Z}$-module, by definition 3.52 and lemmas 3.47 and 3.50. Finally isomorphism 3 holds since G_v is exactly the subgroup of G of p^v-torsion. ∎

Notation 3.73: Tate twist.
Let us define a $\mathscr{G}_K$-module to be a $\mathbb{Z}_p$-module endowed with an action of $\mathscr{G}_K$. Let $\chi\colon \mathscr{G}_K \to \mathbb{Z}_p^\times$ denote the cyclotomic character, i.e. the map such that, for all $\zeta_{p^n} \in \overline{K}$ primitive p^nth roots of unity and all $g \in \mathscr{G}_K$,

$$g(\zeta_{p^n}) = \zeta_{p^n}^{\chi(g)}.$$

We define the $\mathscr{G}_K$-module $\mathbb{Z}_p(1)$ to be $\mathbb{Z}_p$ on which $\mathscr{G}_K$ acts multiplicatively by χ. More explicitly the $\mathscr{G}_K$-action on $\mathbb{Z}_p(1)$ is given by

$$g \cdot x \coloneqq \chi(g)x$$

for all $x \in \mathbb{Z}_p(1)$ and all $g \in \mathscr{G}_K$. Let's now denote $\mathbb{Z}_p(-1) \coloneqq \mathrm{Hom}_{\mathbb{Z}_p\text{-}\mathsf{Mod}}(\mathbb{Z}_p(1), \mathbb{Z}_p)$, where the action is the usual action on the hom group. More explicitly it is given, for all $f \in \mathrm{Hom}_{\mathbb{Z}_p\text{-}\mathsf{Mod}}(\mathbb{Z}_p(1), \mathbb{Z}_p)$ and $g \in \mathscr{G}_K$, by

$$(g \cdot f)(x) \coloneqq f(g^{-1}x),$$

since the action of $\mathscr{G}_K$ on $\mathbb{Z}_p$ is trivial. Then, for all $n \in \mathbb{Z}$, we define the following modules

$$\mathbb{Z}_p(n) \coloneqq \begin{cases} \mathbb{Z}_p(1)^{\otimes n} & \text{if } n > 0, \\ \mathbb{Z}_p & \text{if } n = 0, \\ \mathbb{Z}_p(-1)^{\otimes -n} & \text{if } n < 0. \end{cases}$$

Here by $\mathbb{Z}_p(1)^{\otimes n}$ we mean the n-fold tensor product of $\mathbb{Z}_p(1)$ with itself. Then it is clear that $\mathbb{Z}_p(n) = \mathrm{Hom}_{\mathbb{Z}_p\text{-}\mathsf{Mod}}(\mathbb{Z}_p(-n), \mathbb{Z}_p)$ for all $n < 0$. More explicitly we see that $\mathbb{Z}_p(n)$ coincides, as a module, with $\mathbb{Z}_p$, but the action of $\mathscr{G}_K$ has been twisted by an appropriate power of the cyclotomic character, i.e.

$$g \cdot x = (\chi(g))^n\, x.$$

With this notation in mind we can twist the action on any $\mathscr{G}_K$-module M. To do so we define

$$M(n) \coloneqq M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(n),$$

where the action on the tensor product is given by the diagonal one. Here notice that, since $\mathbb{Z}_p$ is clearly free and of finite rank as a $\mathbb{Z}_p$-module, for $n < 0$ we have

$$M(n) \simeq \mathrm{Hom}_{\mathbb{Z}_p\text{-}\mathsf{Mod}}(\mathbb{Z}_p(-n), M).$$

To conclude we can give an explicit description of the twisted action on $M(n)$. It is given, for all $m \in M$ and all $g \in \mathscr{G}_K$, by

$$g * m = (\chi(g))^n (g \cdot m),$$

where $g*m$ denotes the new modified action, whereas $g\cdot m$ the old one on M and $(\chi(g))^n(g\cdot m)$ is just scalar multiplication.

Proposition 3.74. *Let $G \in \mathsf{BT}/O_K$, then*

$$T_p(G^D) \simeq T_p(G)^\vee(1).$$

Proof. We need to notice that

$$\begin{aligned} T_p(G^D) = \varprojlim_{v\in\mathbb{N}} G_v^D(\overline{K}) &\overset{1}{\simeq} \varprojlim_{v\in\mathbb{N}} \mathrm{Hom}_{\mathsf{Gp}/\overline{K}}\left(G_{v,\overline{K}}, \mathbb{G}_{m,\overline{K}}\right) \\ &\overset{2}{\simeq} \varprojlim_{v\in\mathbb{N}} \mathrm{Hom}_{\mathsf{Gp}/\overline{K}}\left(G_{v,\overline{K}}, \mathbb{G}_m(p)_{\overline{K}}\right) \simeq \mathrm{Hom}_{\mathsf{Gp}/\overline{K}}\left(G_{\overline{K}}, \mathbb{G}_m(p)_{\overline{K}}\right) \\ &\overset{3}{\simeq} \mathrm{Hom}_{\mathsf{Gp}}\left(G(\overline{K}), \mathbb{G}_m(p)(\overline{K})\right) \overset{4}{\simeq} \mathrm{Hom}_{\mathsf{Gp}}\left(G(\overline{K}), \mathbb{Z}_p(1)\right) \\ &\overset{5}{\simeq} \mathrm{Hom}_{\mathsf{Gp}}\left(G(\overline{K}), \mathbb{Z}_p\right)(1) = T_p(G)^\vee(1). \end{aligned}$$

Let's explain why these isomorphisms hold. Isomorphism 1 holds by remark 2.45, whereas isomorphism 2 holds since the image of G_v sits in the p^v-torsion points of $\mathbb{G}_m$. Isomorphism 3 holds since, by proposition 2.38, our group schemes are étale, being over a field of characteristic 0. Moreover, by theorem 2.34, there is an equivalence of categories between étale group schemes over a field and finite groups with an action of the absolute Galois group of the field, which in our case is trivial. Since the equivalence is given taking $\overline{K}$-points, the isomorphism follows. For isomorphism 4 notice that $\mathbb{G}_m(p)(\overline{K})$ consists of all p^nth roots of unity in $\overline{K}$, on which $\mathscr{G}_K$ acts via the cyclotomic character. As a group this is isomorphic to $\mathbb{Z}_p$ (viewed in multiplicative notation), though the action of $\mathscr{G}_K$ differs, since it is trivial on $\mathbb{Z}_p$ (being contained in K). Then it is clear that $\mu_{p^\infty}(\overline{K}) \simeq \mathbb{Z}_p(1)$. Finally isomorphism 5 holds, since the action of $\mathscr{G}_K$ on $\mathrm{Hom}_{\mathsf{Gp}}\left(G(\overline{K}), \mathbb{Z}_p\right)$ is given by $(g\cdot f)(x) = gf(g^{-1}x)$ for all $g \in \mathscr{G}_K$, $f \in \mathrm{Hom}_{\mathsf{Gp}}\left(G(\overline{K}), \mathbb{Z}_p\right)$ and $x \in G(\overline{K})$. ■

4 Divided powers, exponentials and crystals

The aim of this section is to introduce the crystalline site on a scheme, on which we will define the notion of crystal. In order to do so we will need to develop some theory for extensions and prolongations, which will be studied via the exponential map. To introduce this map we need to define divided power structures, which allow to make sense of expressions like $x^n/n!$, hence of exponentials.

4.1 Divided powers

Definition 4.1: Ideal with divided powers.
Let A be a ring, and $I \triangleleft A$ an ideal of A. We say that I is equipped with *divided powers*, equivalently it is given a *divided power structure*, iff it is given with a family of maps $\{\gamma_n\}_{n\geq 1}$, where $\gamma_n : I \to A$ for all $n \in \mathbb{N}$, satisfying, for all $\lambda \in A$ and $x, y \in I$, the following conditions:

1. $\gamma_0(x) = 1, \gamma_1(x) = x$ and $\gamma_n(x) \in I$ for all $n \geq 2$;
2. $\gamma_n(\lambda x) = \lambda^n \gamma_n(x)$;
3. $\gamma_n(x)\cdot\gamma_m(x) = \frac{(m+n)!}{m!n!}\gamma_{m+n}(x)$;
4. $\gamma_n(x+y) = \sum_{i=0}^n \gamma_{n-i}(x)\gamma_i(y)$;
5. $\gamma_m(\gamma_n(x)) = \frac{(mn)!}{(n!)^m m!}\gamma_{mn}(x)$.

Given such a system, we say that (I, γ) is an *ideal with divided powers*, where we denoted $\gamma := \{\gamma_n\}_{n\in\mathbb{N}}$. Moreover we might sometimes use the notation $x^{[n]} := \gamma_n(x)$. Finally, to stress the ring we are working in, we might write (A, I, γ) to denote $I \triangleleft A$ an ideal with divided powers given by γ, and we will refer to it as a *ring with divided powers* or as a *divided power ring*. Borrowing from the literature we may use the shorter *P.D. ring* (analogously *P.D. structure* or *P.D. ideal*), where P.D. stands for "puissances divisées", french for "divided powers".

Definition 4.2: Nilpotent divided powers.
Given (A, I, γ) as before, we say that the divided powers are *nilpotent* iff there is an $N \in \mathbb{N}$ such that, for all $i_1 + \cdots + i_k \geq N$, the ideal generated by elements of the form

$$\gamma_{i_1}(x_1) \cdot \cdots \cdot \gamma_{i_k}(x_k),$$

for all $x_1, \ldots, x_k \in I$, is zero.

Remark 4.3. Let's now notice the following immediate consequences of the definitions.

1. Axiom 2 of definition 4.1 implies that $\gamma_n(0) = 0$ for all $n \in \mathbb{N}$.
2. Via an easy induction argument, axioms 1 and 3 tell us that $n!\gamma_n(x) = x^n$.
3. Reasoning by induction one can show that

$$\frac{(mn)!}{(n!)^m\, m!} = \prod_{k=1}^{m-1} \frac{(kn+n-1)!}{(kn)!(n-1)!},$$

   which implies that it is an integer. In fact it can be interpreted as the number of partitions of a set with mn elements into m subsets of n elements each.
4. In definition 4.2, if we take $k = N$ and $i_1 = \cdots = i_N = 1$, then, thanks to axiom 1 of definition 4.1, the ideal I is nilpotent. In particular $I^N = (0)$.

Example 4.4.

1. Given any ring A, (0) is an ideal with divided powers, with $\gamma_n(0) = 0$ for all $n \in \mathbb{N}$. This is called the *trivial* divided power structure.
2. If A is a $\mathbb{Q}$-algebra, every ideal has a unique divided power structure, given by $x^n/n! =: \gamma_n(x)$.
3. Suppose that $(m-1)!$ is invertible in A and $I^m = (0)$. Then I has a (not necessarily unique) divided power structure, given by

$$x^{[n]} := \begin{cases} \frac{x^n}{n!} & \text{if } n < m, \\ 0 & \text{if } n \geq m. \end{cases}$$

   In particular, whenever $I^2 = 0$, we can give I a divided power structure by setting $\gamma_n(x) = 0$ for all $x \in I$ and all $n \geq 2$.
4. If V is a discrete valuation ring of unequal characteristic p and uniformizer π, we can write $p = u\pi^e$, where u an invertible element and e the absolute ramification index of V. Then (π) has a divided power structure iff $e \leq p-1$. In such case, since V is an integral domain, γ is unique, determined by $x^n/n! =: \gamma_n(x)$. In fact it is known that, denoted by ν_p the valuation of $\mathbb{Z}_p$ normalized to have value group $\mathbb{Z}$, then

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1},$$

where $s_p(n) \coloneqq a_0 + \cdots + a_k$ is the sum of the digits of n in base p. In other words it is the sum of the coefficients of $n = a_0 + \cdots + a_k p^k$, the p-adic expansion of n in $\mathbb{Z}_p$. Then, in order for all γ_n to have values in (π) we need that $\nu(\gamma_n(x)) > 0$ for all $x \in (\pi)$ and all n. By axiom 2 of definition 4.1 it is enough to check it for π. Then, assuming ν is normalized to have values in $\mathbb{Z}$, we have

$$\nu(\gamma_n(\pi)) = \nu(\pi^n/n!) = n - e \cdot \nu_p(n!) = n \cdot \frac{p-1-e}{p-1} + e \cdot \frac{s_p(n)}{p-1}.$$

It is clear that $\nu(\gamma_n(\pi)) > 0$ for all $n \in \mathbb{N}$ iff $p - 1 - e \geq 0$, i.e. iff $e \leq p - 1$.

Since divided power structures need not be unique, we are pushed to introduce the following definition.

Definition 4.5: Morphism of divided power rings.
A *morphism of divided power rings*, denoted by

$$u\colon\ (A, I, \gamma) \longrightarrow (B, J, \delta)\,,$$

is a ring homomorphism $u\colon A \to B$ such that $u(I) \subset J$ and $u(\gamma_n(x)) = \delta_n(u(x))$ for all $x \in I$ and all $n \in \mathbb{N}$.

Definition 4.6.
Given a divided power ring (A, I, γ) and a ring homomorphism $f\colon A \to B$, we say that γ extends to B iff there exists a divided power structure $\overline{\gamma}$ on IB such that

$$f\colon\ (A, I, \gamma) \to (B, IB, \overline{\gamma})$$

is a morphism of divided power rings.

Definition 4.7: Sub-P.D. ideal.
Let (A, I, γ) a P.D. ring and $J \subset I$ the ideal of A generated by a subset $S \subset I$. We say that J is a sub-P.D. ideal of I iff $\gamma_n(s) \in J$ for all $s \in S$ and all $n \geq 1$.

Let's now state a few criteria which allow to extend an existing divided power structure.

Lemma 4.8 ([Stacks, Lemma 07H1])**.** *Let (A, I, γ) be a divided power ring and $A \to B$ a ring homomorphism. If γ extends to B, then it extends uniquely. Assume moreover that any of the following conditions holds*

1. *$IB = 0$,*
2. *I is* principal *or*
3. *$A \to B$ is a* flat *morphism,*

then γ extends to B.

Proposition 4.9 ([BO78, §3, proposition 3.12])**.** *Suppose that (I, γ) and (J, δ) are P.D. ideals of a ring A. Suppose that $I \cap J$ is a sub-P.D. ideal of both I and J and that γ and δ agree on $I \cap J$. Then there is a unique P.D. structure on $I + J$ such that both I and J are sub-P.D. ideals of $I + J$.*

We will also need to work with p-adic completions, so we wish to extend divided powers also in this case.

Lemma 4.10 ([Stacks, Lemma 07KD])**.** *Let (A, I, γ) be a divided power ring and assume that p is nilpotent on A/I. Then*

1. *the p-adic completion $\widehat{A} = \varprojlim_{n\in\mathbb{N}} A/p^n A$ surjects onto A/I,*
2. *the kernel of this map is the p-adic completion $\widehat{I}$ of I and*
3. *each γ_n is continuous for the p-adic topology and extends to a continuous map $\widehat{\gamma}_n \colon \widehat{I} \to \widehat{I}$, defining a divided power structure on $\widehat{I}$.*

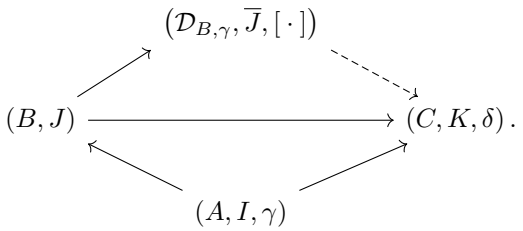
Let's now introduce the analogous of the symmetric algebra, first, and of the formal completion, later, in the context of divided powers.

Theorem 4.11 ([BO78, §3, theorem 3.9])**.** *Let M be an A-module. Then there exists a divided power A-algebra $\left(\Gamma_A(M), \Gamma_A^+(M), \gamma\right)$ and an A-linear map $\varphi \colon M \to \Gamma_A^+(M)$ with the following universal property: given any other divided power A-algebra (B, J, δ) and any A-linear map $\psi \colon M \to J$, then there is a unique divided power morphism $\overline{\psi} \colon \Gamma_A(M) \to B$ such that $\overline{\psi} \circ \varphi = \psi$. Moreover the divided power A-algebra $\Gamma_A(M)$ has the following properties.*

1. *Denote by $x^{[1]} \coloneqq \varphi(x)$ and $x^{[n]} \coloneqq \gamma_n(\varphi(x)) \in \Gamma_A^n(M)$, following notation of definition 4.1. Then the A-module $\Gamma_A^n(M)$ is generated by*
$$\left\{ x_1^{[q_1]} \cdots x_k^{[q_k]} \;\middle|\; q_1 + \cdots + q_k = n \right\}.$$
Moreover, if $\{x_i\}_{i\in I}$ is a basis for M, then $\{x_i^{[n]}\}_{I\in I}$ is a basis for $\Gamma_A^n(M)$, for all $n \geq 1$.
2. *$\Gamma_A(M)$ is a graded algebra, with $\Gamma_A^0(M) = A$, $\Gamma_A^1(M) = M$ and $\Gamma_A^+(M) = \oplus_{i\geq 1}\Gamma_A^i(M)$.*
3. *The functor $M \mapsto \Gamma_A(M)$ is compatible with:*
   (a) base change*: given any A-algebra A', we have*
   $$\Gamma_{A'}(M \otimes_A A') \simeq A' \otimes_A \Gamma_A(M),$$
   (b) filtered direct limits*: given any directed system of A-modules $\{M_\lambda\}_{\lambda\in\Lambda}$, we have*
   $$\Gamma_A(\varinjlim_\lambda M_\lambda) \simeq \varinjlim_\lambda \Gamma_A(M_\lambda),$$
   (c) coproducts*: given any pair of A-modules M, N, we have*
   $$\Gamma_A(M \oplus N) \simeq \Gamma_A(M) \otimes_A \Gamma_A(N).$$

To make notation cleaner, when the base A is clear, we will write $\Gamma(M)$ for $\Gamma_A(M)$.

Theorem 4.12 ([BO78, §3, theorem 3.19], divided power envelope)**.** *Let (A, I, γ) a ring with divided powers, B an A-algebra and $J \lhd B$ an ideal. There exists a B-algebra $\mathcal{D}_{B,\gamma}(J)$ with a divided power ideal $\left(\overline{J}, [\,\cdot\,]\right)$, such that $J\mathcal{D}_{B,\gamma} \subset \overline{J}$, the divided power structure $[\,\cdot\,]$ is compatible with γ, and which satisfies the following universal property: for any B-algebra C containing an ideal K which contains JC and has a divided power structure δ compatible with γ, there is a unique divided power morphism $\left(\mathcal{D}_{B,\gamma}, \overline{J}, [\,\cdot\,]\right) \to (C, K, \delta)$ making the following diagram commute*



Remark 4.13. Though we will not include the proof for the above theorem, we think it is useful to outline the construction of the divided power envelope since it is going to be used quite prominently in the following sections. One starts by replacing J with $J + IB$, so that $I \subset J$. Then, denoting by $\varphi\colon J \to \Gamma_B^1(J)$ the universal map of theorem 4.11 and by f the map $A \to B$, we define the ideal $\mathcal{J} \lhd \Gamma_B(J)$ whose generators are given by

1. $\varphi(x) - x$ for all $x \in J$ and
2. $\varphi(f(y))^{[n]} - \varphi(f(\gamma_n(y)))$ for $y \in I$.

Then, after checking some compatibility conditions, one finds that $\mathcal{D} \coloneqq \Gamma_B(J)/\mathcal{J}$ has an induced divided power structure, that it is a B-algebra and that it satisfies the desired universal property.

The point of introducing all of these definitions is to allow one to define the following inverse maps, of which we will construct some generalizations later on.

Definition 4.14.
Let (A, I, γ) be a nilpotent divided power ring. Then we can define two maps

$$\exp\colon I \longrightarrow (1+I)^{\times}$$
$$\log\colon (1+I)^{\times} \longrightarrow I,$$

given by $\exp(x) \coloneqq \sum_{n\geq 0} \gamma_n(x)$ and $\log(1+x) \coloneqq \sum_{n\geq 1} (-1)^{n-1}\,(n-1)!\gamma_n(x)$. Let's notice that these maps are well defined. In fact we assumed I with nilpotent divided powers, hence $\gamma_n = 0$ for n big enough, which implies that these are actually finite sums. Then, as outlined in [Mes72, Chapter III, §1.6], one checks that these maps are inverses to each other by reducing to the universal case $\widehat{\Gamma_{\mathbb{Z}}(\mathbb{Z})}$.

Remark 4.15. Notice that lemma 4.8 allows one, starting from a divided power ring (A, I, γ), to give a structure of divided power ring to $A_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec}(A) =: S$, since localization is a flat morphism. Moreover the structures we defined above are all compatible with localization, by construction. This pushes us to expand the notion of divided powers to the sheaf $\mathcal{O}_S$. Actually one can be even more general, giving the following definition.

Definition 4.16: Scheme with divided powers.
Let S be a scheme and $\mathcal{I}$ a quasi-coherent sheaf of ideals of $\mathcal{O}_S$. A *divided power structure* on $\mathcal{I}$ is the data, for all $U \subset S$ open, of divided powers $\gamma(U)$ of $\Gamma(U, \mathcal{I})$ in which restriction maps are given by morphisms of divided power rings. Then we will call one triple $(S, \mathcal{I}, \gamma)$ a *scheme with divided powers*, or equivalently a *divided power scheme* or a *P.D. scheme*.

Let now $(S, \mathcal{I}, \gamma)$ and $(S', \mathcal{I}', \gamma')$ be schemes with divided powers. A *morphism of divided power schemes*

$$f\colon (S, \mathcal{I}, \gamma) \to (S', \mathcal{I}', \gamma')$$

is a morphism of schemes $f\colon S \to S'$ such that $f^{-1}(\mathcal{I}')\mathcal{O}_S \subset \mathcal{I}$ and, for all $U' \subset S'$ open,

$$f^{\#}(U')\colon (\mathcal{O}_{S'}(U'), \mathcal{I}'(U'), \gamma'(U')) \longrightarrow \big(\mathcal{O}_S(f^{-1}U'), \mathcal{I}(f^{-1}U'), \gamma(f^{-1}U')\big)$$

is a morphism of divided power rings.

Definition 4.17: Locally nilpotent sheaf of ideals with divided powers.
We say that the divided powers on the sheaf of ideals $\mathcal{I}$ of $\mathcal{O}_S$ are *locally nilpotent* iff, locally on S, they satisfy the conditions in definition 4.2.

In order to generalize the other constructions of the section we need the following result.

Proposition 4.18 ([BO78, Remark 3.20, proposition 3.21])**.** *Let (A, I, γ) be a divided power ring, B an A-algebra with J an ideal of B.*

1. *Consider a surjective morphism of divided power rings $(A, I, \gamma) \to (A', I', \gamma')$, $B' \coloneqq A' \otimes_A B$ and $J' = JB'$. Then the following canonical map is an isomorphism*

$$A' \otimes_A \mathcal{D}_{B,\gamma}(J) \xrightarrow{\sim} \mathcal{D}_{B',\gamma'}(J').$$

2. *Suppose $J \triangleleft A$ is an ideal and B' is a B-algebra. Then there is a natural map*

$$\mathcal{D}_{B,\gamma}(J) \otimes_B B' \longrightarrow \mathcal{D}_{B',\gamma}(JB'),$$

which is an isomorphism if B' is a flat *B-algebra.*

Remark 4.19. Finally one can generalize the construction of theorems 4.11 and 4.12 to the case of $\mathcal{M}$ an quasi-coherent $\mathcal{O}_S$-algebra. Indeed the divided power algebra $\Gamma(\mathcal{M})$ is defined as the sheaf associated to the presheaf $U \mapsto \Gamma_{\mathcal{O}_S(U)}(\mathcal{M}(U))$.

For the divided power envelope let's consider the following situation. Take a closed immersion of schemes $X \to Y$, with a morphism $Y \to S$, where S is equipped with a structure of divided powers via γ. Then, one defines the divided power envelope $\mathcal{D}_{X,\gamma}(Y)$, to be the scheme corresponding to the divided power envelope of X in Y, compatible with γ. More explicitly $\mathcal{D}_{X,\gamma}(Y)$ is locally given by the spectrum of the divided power envelope of $\mathcal{O}_Y$ at the ideal defining X, compatible with γ. As already remarked we can carry out this construction thanks to proposition 4.18.

4.2 Cospec and Lie algebras

The aim of the following section is to give some vocabulary to be able to work with exponentials, in a more general context than the previous section, and to introduce the construction of Lie algebra. The notation of this section will follow that of [Mes72, Capther III]. This means that it might not be consistent with our previous exposition.

Definition 4.20: Quasi-coherent (co-)algebra.
Let S be a scheme.

1. We say that $\mathcal{U}$ is an *$\mathcal{O}_S$-algebra* iff it is an $\mathcal{O}_S$-module which is also endowed with an $\mathcal{O}_S$-algebra structure.

2. We say that $\mathcal{U}$ is an *$\mathcal{O}_S$ co-algebra* iff it is an $\mathcal{O}_S$-modules, endowed with morphisms of $\mathcal{O}_S$-modules $\Delta \colon \mathcal{U} \to \mathcal{U} \otimes_{\mathcal{O}_S} \mathcal{U}$ and $\eta \colon \mathcal{U} \to \mathcal{O}_S$ satisfying the properties of Hopf algebra structure morphisms, as defined in definition 2.12.

3. Let $\sigma : \mathcal{U} \otimes \mathcal{U} \to \mathcal{U} \otimes \mathcal{U}$ be the map which, on sections, acts as $s \otimes t \mapsto t \otimes s$. We say that an $\mathcal{O}_S$ co-algebra $\mathcal{U}$ is *co-commutative* iff $\sigma \circ \Delta = \Delta$.

If, moreover, the (co-)algebra $\mathcal{U}$ is quasi-coherent as an $\mathcal{O}_S$-module, we say that it is a *quasi-coherent* $\mathcal{O}_S$ (co-)algebra.

Remark 4.21. The definition of $\mathcal{O}_S$ co-algebra is the categorical dual to that of $\mathcal{O}_S$-algebra. In particular, given a finite locally-free $\mathcal{O}_S$-module $\mathcal{A}$, we can define its dual $\mathcal{O}_S$-module $\mathcal{A}^\vee \coloneqq \mathcal{H}\mathrm{om}_{\mathcal{O}_S}(\mathcal{A}, \mathcal{O}_S)$, defined as in definition 4.25, which is again a finite locally-free $\mathcal{O}_S$-module.

Then, if $\mathcal{A}$ is given an $\mathcal{O}_S$-algebra structure, following remark 2.40, we can endow $\mathcal{A}^\vee$ with an $\mathcal{O}_S$ co-algebra structure (here again the hypothesis of local freeness and finiteness are indeed of vital importance). Vice-versa, given a finite locally-free $\mathcal{O}_S$ co-algebra $\mathcal{B}$, its dual $\mathcal{O}_S$-module $\mathcal{B}^\vee$ can be given an $\mathcal{O}_S$-algebra structure.

Notation 4.22.
In order to stay consistent with [Mes72] we will use the following notation. Let S be a scheme, $\mathcal{U}$ an $\mathcal{O}_S$-module and S' a scheme, with a morphism $f\colon S' \to S$. We denote the pullback of $\mathcal{U}$ along f by

$$\mathcal{U}_{S'} \coloneqq f^*\mathcal{U} = f^{-1}\mathcal{U} \otimes_{f^{-1}\mathcal{O}_S} \mathcal{O}_{S'},$$

where $f^{-1}\mathcal{U}$ is the usual inverse image of sheaves and $f^{-1}\mathcal{O}_S \to \mathcal{O}_{S'}$ is defined from $f^\#$.

Definition 4.23.
Let S be a scheme and $\mathcal{U}$ a co-commutative $\mathcal{O}_S$ co-algebra. We define the functor

$$\begin{aligned} \mathrm{Cospec}(\mathcal{U})\colon \mathsf{Sch}/S &\longrightarrow \mathsf{Sets} \\ S' &\longmapsto \{y \in \Gamma(S', \mathcal{U}_{S'}) \mid \eta(y) = 1, \Delta(y) = y \otimes y\}. \end{aligned}$$

Remark 4.24 ([Mes72, Chapter 3, §2.1])**.** The functor $\mathrm{Cospec}(\mathcal{U})$ is a sheaf for the fpqc topology for any co-commutative $\mathcal{O}_S$ co-algebra $\mathcal{U}$. As a consequence we obtain a covariant functor $\mathcal{U} \mapsto \mathrm{Cospec}(\mathcal{U})$ from the category of co-commutative $\mathcal{O}_S$ co-algebras to that of fpqc sheaves on S. Moreover this functor is compatible with inverse images.

Let's now investigate the relation between Cospec and Spec. We need some preliminary definitions first.

Definition 4.25: Internal hom of $\mathcal{O}_X$-modules.
Let X be a scheme, and $\mathcal{F}, \mathcal{G}$ be two $\mathcal{O}_X$-modules. We define their internal hom as

$$\begin{aligned} \mathcal{H}\mathrm{om}_{\mathcal{O}_X\text{-}\mathsf{Mod}}(\mathcal{F}, \mathcal{G})\colon \mathsf{Op}(X)^{\mathrm{op}} &\longrightarrow \mathcal{O}_X\text{-}\mathsf{Mod} \\ U &\longmapsto \mathrm{Hom}_{\mathcal{O}_X|_U\text{-}\mathsf{Mod}}(\mathcal{F}|_U, \mathcal{G}|_U), \end{aligned}$$

which is a sheaf of abelian groups (see [Stacks, Section 00AK]). Moreover it carries an $\mathcal{O}_X$-module structure given as follows. Fixed any $U \subset X$ open, $\varphi \in \mathrm{Hom}_{\mathcal{O}_X|_U\text{-}\mathsf{Mod}}(\mathcal{F}|_U, \mathcal{G}|_U)$ and $f \in \mathcal{O}_X(U)$, we can define $f\varphi \in \mathrm{Hom}_{\mathcal{O}_X|_U\text{-}\mathsf{Mod}}(\mathcal{F}|_U, \mathcal{G}|_U)$ either by precomposing φ with multiplication by f on $\mathcal{F}|_U$ or by postcomposing φ with multiplication by f on $\mathcal{G}|_U$.

Remark 4.26. We start out giving the following useful identification. Let $\mathcal{U}$ be a quasi-coherent $\mathcal{O}_S$ co-algebra, then we have a one to one correspondence

$$\Gamma(S', \mathrm{Cospec}(\mathcal{U})) \simeq \mathrm{Hom}_{\mathcal{O}_{S'}\text{-}\mathsf{co\text{-}alg}}(\mathcal{O}_{S'}, \mathcal{U}_{S'}),$$

where $\mathcal{O}_S$ is given the co-algebra structure of the multiplicative group scheme, as seen in item 2 of example 2.20, and the right hand side denotes the morphisms of $\mathcal{O}_{S'}$ co-algebras which are morphisms of $\mathcal{O}_{S'}$-modules preserving the morphisms Δ and η. More explicitly this identification associates $\varphi\colon \mathcal{O}_{S'} \to \mathcal{U}_{S'}$ to $\varphi(S')(1) \in \Gamma(S', \mathcal{U}_{S'})$. Finally it is clear that the above identification is functorial in S'.

In order to investigate more in detail the notion of Cospec we need to be able to construct schemes starting from quasi-coherent $\mathcal{O}_S$-algebras or $\mathcal{O}_S$-modules.

Definition 4.27: Relative spectrum and Vector bundles.
Let's fix a scheme S.

1. Assume that $\mathcal{A}$ is a quasi-coherent $\mathcal{O}_S$-algebra. We define the *relative spectrum* of $\mathcal{A}$, denoted by $\underline{\mathrm{Spec}}_S(\mathcal{A})$, as the gluing of $\mathrm{Spec}(\Gamma(U,\mathcal{A}))$, where U ranges over all affine open subsets of S.

2. Let $\mathcal{E}$ be a quasi-coherent sheaf of $\mathcal{O}_S$-modules. Denote by $\mathrm{Sym}(\mathcal{E})$ the symmetric algebra associated to $\mathcal{E}$ (which, thanks to item 2 of remark 3.32 is quasi-coherent). We define the *vector bundle* associated to E as

$$\mathbf{V}(\mathcal{E}) \coloneqq \underline{\mathrm{Spec}}_S(\mathrm{Sym}(\mathcal{E})).$$

Remark 4.28.

1. Notice that the constructions outlined above can actually be carried out, as can be checked at [Stacks, Section 01LL] and [Stacks, Section 01M1].

2. Let $\mathcal{A}$ be an $\mathcal{O}_S$-algebra. Then, as proved in [Stacks, Lemma 01LP], $\underline{\mathrm{Spec}}_S(\mathcal{A})$, is canonically an S-scheme. In fact there is a morphism of schemes

$$\pi\colon \underline{\mathrm{Spec}}_S(\mathcal{A}) \longrightarrow S,$$

   where, for all $U \subset S$ affine open, $\pi^{-1}(U) \simeq \mathrm{Spec}(\mathcal{A}(U))$.

3. $\mathbf{V}(\mathcal{E})$ is endowed with some extra structure: it inherits the grading of $\mathrm{Sym}(\mathcal{E})$ thanks to

$$\pi_*\mathcal{O}_{\mathbf{V}(\mathcal{E})} = \bigoplus_{n\geq 0} \mathrm{Sym}^n(\mathcal{E}).$$

   Then $\pi_*\mathcal{O}_{\mathbf{V}(\mathcal{E})}$ is a graded $\mathcal{O}_S$-algebra and $\mathcal{E}$ is just the degree 1 part of this.

Remark 4.29. For a finite locally-free $\mathcal{O}_S$-algebra $\mathcal{A}$, we can see that $\mathrm{Cospec}(\mathcal{A}^\vee)$, as an fppf sheaf, is representable by $\underline{\mathrm{Spec}}_S(\mathcal{A})$ and the category of finite locally-free S-schemes is equivalent to the category of finite locally-free co-commutative $\mathcal{O}_S$ co-algebras, as shown in [Mes72, Chapter III, remark 2.1.2].

Indeed, given $\mathcal{A}$ as above, its dual $\mathcal{A}^\vee$ can be endowed with the structure of co-algebra, as seen in remark 4.21. Then, invoking remark 4.26, we can construct our desired isomorphism: let $S' \in \mathsf{Sch}/S$

$$\begin{aligned}\Gamma(S', \mathrm{Cospec}(\mathcal{A}^\vee)) &\simeq \mathrm{Hom}_{\mathcal{O}_{S'}\text{-}\mathsf{co\text{-}alg}}(\mathcal{O}_{S'}, \mathcal{A}^\vee_{S'}) \simeq \mathrm{Hom}_{\mathcal{O}_{S'}}(\mathcal{A}_{S'}, \mathcal{O}_{S'}) \\ &\simeq \Gamma(S', \underline{\mathrm{Spec}}_S(\mathcal{A})),\end{aligned}$$

where the last isomorphism holds by [Stacks, Lemma 01LV]. In fact we can conclude thanks to functoriality of the above isomorphisms.

Remark 4.30 ([Mes72, Chapter III, §2.1.3])**.** The above construction can be generalized to filtered direct limits. Let $\mathcal{U} = \varinjlim_i \mathcal{U}_i$ be a filtered direct limit of co-commutative $\mathcal{O}_S$ co-algebras. One obtains an isomorphism

$$\varinjlim_i \mathrm{Cospec}(\mathcal{U}_i) \xrightarrow{\sim} \mathrm{Cospec}(\mathcal{U}).$$

Let's now consider filtered direct limits of finite S-schemes with structure sheaves $\mathcal{A}_i$, finite and locally-free $\mathcal{O}_S$-algebras, and denote $\mathcal{U}_i \coloneqq \mathcal{A}_i^\vee$ as above. Then $\varinjlim_i \mathcal{U}_i$ is a limit of finite locally-free co-commutative $\mathcal{O}_S$ co-algebras. In particular, given a *Barsotti-Tate group* or a *formal Lie variety* over S, one can write it as $\mathrm{Cospec}(\mathcal{U})$ for an appropriate co-commutative $\mathcal{O}_S$ co-algebra $\mathcal{U}$, constructed as just outlined.

Definition 4.31: fppf sheaf associated to an $\mathcal{O}_S$-module.
Let S be a scheme and $\mathcal{V}$ be an $\mathcal{O}_S$-module. We will denote by $\mathbf{W}(\mathcal{V})$ the functor

$$\begin{aligned}\mathbf{W}(\mathcal{V})\colon (\mathsf{Sch}/S)^{\mathrm{op}} &\longrightarrow \mathsf{Gp}\\ S' &\longmapsto \Gamma(S', \mathcal{V}_{S'}),\end{aligned}$$

where $\mathcal{V}_{S'}$, as usual, denotes the pullback of $\mathcal{V}$ to S'.

Remark 4.32 ([SGA3-1, propositiona 4.6.2 and 4.6.5])**.**

4.6.2: The functor $\mathbf{W}$ commutes with base changes, so that $\mathbf{W}(\mathcal{V})_{S'} \simeq \mathbf{W}(\mathcal{V}_{S'})$, where the subscript S' denotes respectively the base change and the pullback along $S' \to S$.

4.6.5: If $\mathcal{V}$ is also locally-free and of finite rank, we have the canonical isomorphism

$$\mathbf{W}(\mathcal{V}) \simeq \mathrm{Hom}_{\mathcal{O}_S\text{-}\mathsf{Mod}}\left(\mathbf{W}(\mathcal{V}^\vee), \mathcal{O}_S\right) \simeq \underline{\mathrm{Spec}}_S(\mathrm{Sym}(\mathcal{V}^\vee)).$$

This gives a representative in Sch/S for $\mathbf{W}(\mathcal{V})$, making it not only an object of Gr/S, as defined in notation 3.22, but also of Gp/S.

Notation 4.33.
To be more consistent with [Mes72], we will introduce a lighter notation to denote the same object. Let S be a scheme and $\mathcal{M}$ a quasi-coherent sheaf of $\mathcal{O}_S$-modules. Then we will write $\underline{\mathcal{M}} \coloneqq \mathbf{W}(\mathcal{M})$ for an $\mathcal{O}_S$-module. In particular $\mathcal{O}_S$ itself is an $\mathcal{O}_S$-module, hence we will denote by $\underline{\mathcal{O}_S} \coloneqq \mathbf{W}(\mathcal{O}_S)$ and say that $\underline{\mathcal{M}}$ is an $\underline{\mathcal{O}_S}$-module.

Definition 4.34: Vector S-group.
Let S be a scheme and $\mathcal{V}$ a quasi-coherent locally-free $\mathcal{O}_S$-module of finite rank. We define the *vector S-group* of $\mathcal{V}$ to be $\underline{\mathcal{V}} = \mathbf{W}(\mathcal{V})$, as of definition 4.31. Thanks to remark 4.32 $\underline{\mathcal{V}} \in \mathsf{Gp}/S$, since it is represented by $\underline{\mathrm{Spec}}_S(\mathrm{Sym}(\mathcal{V}^\vee))$.

Proposition 4.35 ([Stacks, Proposition 03DX])**.** *Let S be a scheme. The functor $\mathcal{M} \mapsto \underline{\mathcal{M}}$ is fully faithful.*

Remark 4.36. As a consequence, in what follows, we can follow [Mes72] and switch between morphisms of sheaves of $\mathcal{O}_S$-modules and morphism between the associated sheaves of $\underline{\mathcal{O}_S}$-modules without problem.

Definition 4.37.
Let $\mathcal{U}$ be a co-commutative $\mathcal{O}_S$ co-algebra.

1. We say that a section x of $\mathcal{U}$ is *primitive* iff $\Delta(x) = x \otimes 1 + 1 \otimes x$.
2. We denote by $\mathrm{Lie}(\mathcal{U})$ the sheaf of $\mathcal{O}_S$-modules whose sections on $T \subset S$ open are given by primitive sections of $\mathcal{U}$ on T.
3. We denote by $\underline{\mathrm{Lie}}(\mathcal{U})$ the sheaf of $\underline{\mathcal{O}_S}$-modules associated to $\mathrm{Lie}(\mathcal{U})$ as in notation 4.33.

Moreover consider $G \in \mathsf{Gr}/S$ for which there exists a co-algebra $\mathcal{U}$ for which $G = \mathrm{Cospec}(\mathcal{U})$ as fppf sheaves (which in particular include *formal Lie groups* and *Barsott-Tate groups*). Then we define $\mathrm{Lie}(G) \coloneqq \mathrm{Lie}(\mathcal{U})$.

Remark 4.38 ([Mes72, Chapter III, example 2.2.2])**.** Let $\mathcal{U}$ be a finite and locally-free $\mathcal{O}_S$-module, where S is a scheme. Then we have the following isomorphism $(\mathcal{U}^\vee)^\vee \simeq \mathcal{U}$. If, moreover, $\mathcal{U}$ is a co-commutative $\mathcal{O}_S$ co-algebra, we have $X = \mathrm{Cospec}(\mathcal{U}) \simeq \underline{\mathrm{Spec}}_S(\mathcal{U}^\vee)$. Let's, moreover,

define ω_X with respect to the section $e\colon S \to X$ associated to the counit $\eta\colon \mathcal{U} \to \mathcal{O}_S$ via the identification

$$\mathrm{Hom}_{\mathcal{O}_S}(\mathcal{U}_S, \mathcal{O}_S) \simeq \Gamma(S, \underline{\mathrm{Spec}}_S(\mathcal{U}^\vee)).$$

It can be viewed as the dual of the tangent space at the origin of our group X. Analogously the requirements that sections of $\underline{\mathrm{Lie}}(\mathcal{U})$ be primitive, can be seen as a formal version of Leibnitz rule, so that these sections can be paired with left invariant derivations, i.e. elements of the tangent space at the origin. All in all, the above can be expanded to obtain an isomorphism

$$\underline{\mathrm{Lie}}(X) = \underline{\mathrm{Lie}}(\mathcal{U}) \simeq \underline{\mathcal{H}\mathrm{om}}_{\mathcal{O}_S}(\omega_X, \mathcal{O}_S) = \underline{\omega_X}^\vee.$$

4.3 Exponentials and prolongations

Here we generalize the concept of exponential, seen in definition 4.14, to groups on S and see how this construction relates to prolongations. Let A be a ring, $I \lhd A$ an ideal with nilpotent divided powers and $A_0 \coloneqq A/I$. Denote by $S \coloneqq \mathrm{Spec}(A)$ and by $S_0 \coloneqq \mathrm{Spec}(A/I)$ its closed subscheme defined by the ideal I.

Exponentials

For this section we will interested in V a locally-free A-module of finite rank and $G = \mathrm{Spec}(B)$ a finite locally-free group scheme over S. Consider the S-group $\underline{V} \times_S G$, whose ring is $C \coloneqq \mathrm{Sym}(V^\vee) \otimes_A B$ and H an S-group isomorphic to $\underline{V} \times_S G$ as pointed schemes (but not necessarily as group objects). Here we want to extend the theory of exponentials to H.

Remark 4.39. Since $\underline{V} \times_S G$ is isomorphic to H as pointed schemes, we have $\omega_H \simeq \omega_{\underline{V} \times_S G}$, locally-free of finite type, which implies that $\mathrm{Lie}(H)$ is also locally-free.

Definition 4.40: [Mes72, Chapter III, §2.6.8].
Let $\mathcal{W}$ be a locally-free $\mathcal{O}_S$-module of finite rank. Denote by $\mathcal{W}_0$ and H_0 the restrictions of $\mathcal{W}$ and H to S_0 (i.e. their pullback along the closed immersion $S_0 \hookrightarrow S$). Then we will denote

$$\mathrm{Hom}_{\mathsf{Gr}/S}(\underline{\mathcal{W}}, H) \longrightarrow \mathrm{Hom}_{\mathsf{Gr}/S_0}\left(\underline{\mathcal{W}_0}, H_0\right)$$

the map induced by the pullback functor on hom groups. Here one can define a morphism

$$\exp\colon \mathrm{Hom}_{\mathcal{O}_S\text{-}\mathsf{Mod}}(\mathcal{W}, I \cdot \mathrm{Lie}(H)) \hookrightarrow \ker\left[\mathrm{Hom}_{\mathsf{Gr}/S}(\underline{\mathcal{W}}, H) \longrightarrow \mathrm{Hom}_{\mathsf{Gr}/S_0}\left(\underline{\mathcal{W}_0}, H_0\right)\right]$$

by setting, on sections, $\exp(\theta)(x) \coloneqq \exp(\theta(x))$. More precisely, to $\theta\colon \mathcal{W} \to I \cdot \mathrm{Lie}(H)$, we associate the map $\exp(\theta)\colon \Gamma(\mathcal{W}) \to C^\vee$, given on sections by

$$\exp(\theta)(x) = \exp(\theta(x)) \coloneqq \sum_{n \geq 0} (\theta(x))^{[n]},$$

for all sections x of $\mathcal{W}$. Notice that, by theorem 4.11, $\exp(\theta)$ maps $\Gamma^+(\mathcal{W})$ in $I \cdot \mathrm{Lie}(H)$. This last has nilpotent divided powers, hence for N sufficiently large, $(\theta(x))^{[n]} = 0$ for all $n \geq N$. Then the above sum is finite and the map is well defined. Taking the transpose of such a map we obtain a mapping $(C^\vee)^\vee \simeq C \to \mathrm{Sym}(\mathcal{W}^\vee)$, which corresponds to an S-group homomorphism $\underline{\mathcal{W}} \to G$. Then one can check that it actually sits in the desired kernel following [Mes72, Chapter III, §2.4, §2.6].

Prolongations

Let's now concentrate our efforts on lifting homomorphisms. Consider S, S_0 as before and H an S-group given as a vector S-group, i.e. $H = \underline{\mathcal{V}}$, where $\mathcal{V}$ is a locally-free $\mathcal{O}_S$-module of finite rank. As usual, denote by $\mathcal{V}_0$ and H_0 the restriction of the above to S_0.

Remark 4.41 ([Mes72, Chapter III, §2.7])**.** In order to study prolongations of homomorphisms it is useful to notice that the above construction can be carried out in the following case. Let's assume that $G \in \mathsf{Gr}/S$ is a filtering direct limit of representable subgroups G_α. Assume that $\mathrm{Inf}^1(G) = \mathrm{Inf}^1(G_\alpha)$ for some α, so that $\mathrm{Lie}(G) = \mathrm{Lie}(G_\alpha)$. Then one can define the exponential map in this case, giving rise to

$$\exp\colon \mathrm{Hom}_{\mathcal{O}_S\text{-}\mathsf{Mod}}\left(\mathcal{V}, I\cdot\mathrm{Lie}(G)\right) \hookrightarrow \ker\left[\mathrm{Hom}_{\mathsf{Gr}/S}\left(H,G\right) \longrightarrow \mathrm{Hom}_{\mathsf{Gr}/S_0}\left(H_0,G_0\right)\right]$$

where, as before, $\mathcal{V}_0$ and G_0 are the pullback of $\mathcal{V}$ and G along $S_0 \hookrightarrow S$. In particular, thanks to [Mes72, Chapter II, Corollary 3.3.16], the above conditions are satisfied by Barsotti-Tate groups over a base scheme S on which p is nilpotent.

Definition 4.42: Linearly compatible prolongations.
Let $u_0\colon H_0 \to G_0$ be a homomorphism of S-groups. We say that two lifts $u', u''\colon H \to G$ of u_0 are *linearly compatible* iff their difference is in the image of

$$\exp\colon \mathrm{Hom}_{\mathcal{O}_S\text{-}\mathsf{Mod}}\left(\mathcal{V}, I\cdot\mathrm{Lie}(G)\right) \hookrightarrow \ker\left[\mathrm{Hom}_{\mathsf{Gr}/S}\left(H,G\right) \longrightarrow \mathrm{Hom}_{\mathsf{Gr}/S_0}\left(H_0,G_0\right)\right].$$

Remark 4.43. The above is an equivalence relation on the set of lifts of u_0.

Let's now study better this relation with the exponential map in the context of

$$u_0\colon \underline{\mathcal{V}_0} \hookrightarrow G_0$$

a monomorphism with image $H_0 \subset G_0$. We want to study the set of lifts of H_0 to subgroups H of G that are flat over S, together with the structure of locally-free module on H, lifting that of H_0.

Remark 4.44 ([Mes72, Chapter III, §2.7.3])**.** In case H is a solution to this problem, it is given by $\underline{\mathcal{V}}$, where $\mathcal{V}$ is a finite, locally-free $\mathcal{O}_S$-module. Any such $\mathcal{V}$ is determined up to a (non-unique) isomorphism. Fixed one such $\mathcal{V}$, giving H is equivalent to giving a morphism $u\colon \underline{\mathcal{V}} \to G$ lifting u_0, modulo identifying two such morphisms if they differ by an $\mathcal{O}_S$-automorphism of $\mathcal{V}$ which reduces to the identity on $\mathcal{V}_0$.

Lemma 4.45 ([Mes72, Chapter III, lemma 2.7.4])**.** *Let $u_0, \underline{\mathcal{V}}, G, \underline{\mathcal{V}_0}, G_0$ be as above. Any homomorphism $u\colon \underline{\mathcal{V}} \to G$ lifting $u_0\colon \underline{\mathcal{V}_0} \hookrightarrow G_0$ is a monomorphism.*

Definition 4.46: Congruent lifts.
Two lifts $u, u'\colon \underline{\mathcal{V}} \to G$ of u_0 are said to be *congruent* iff the differ by an $\mathcal{O}_S$-linear automorphism of $\underline{\mathcal{V}}$ reducing to the identity on $\underline{\mathcal{V}_0}$.

Remark 4.47. By remark 4.44 it is clear that two lifts of u_0 are congruent iff they define the same solution H to the problem of lifting subgroups of G_0 to subgroups of G.

Lemma 4.48 ([Mes72, Chapter III, lemma 2.7.6])**.** *If u and u' are congruent lifts of u_0, then they are linearly compatible.*

Remark 4.49. Let's notice that this proposition allows to transfer the equivalence relation, via the exponential map, from lifts of u_0 to solutions of the problem of lifting the subgroup H_0. In particular we can rephrase it in terms of subgroups of $\mathrm{Lie}(G)$. More explicitly let $\mathfrak{h} \subset \mathrm{Lie}(G)$ be a locally-free submodule of $\mathrm{Lie}(G)$ lifting $\mathfrak{h}_0 := \mathrm{Lie}(H_0)$. Then the following proposition holds.

Proposition 4.50 ([Mes72, Chapter III, proposition 2.7.7])**.** *In each linear equivalence class of solutions of the problem of lifting the subgroup H_0 there is exactly one H with $\mathrm{Lie}(H) = \mathfrak{h}$.*

4.4 Crystals

Here we finally give the definition of crystalline site and, then, of crystal on such a site. This concept was introduced by A. Grothendieck, who described his choice of terminology saying: « *Un crystal possède deux propriétés caractéristiques : la rigidité, et la faculté de croître, dans un voisinage approprié. Il y a des cristaux de toute espèce de substance : des cristaux de soude, de soufre, de modules, d'anneaux, de schémas relatifs, etc.* »[1]

Crystalline site

In order to introduce crystals we need to first define the crystalline site. Here, as a start, we will introduce the basic terminology needed to give some meaning to our objects.

Definition 4.51: Thickening.
Let X be a scheme. We say that a scheme X' is a *thickening* of X iff X is a closed subscheme of X' and their underlying topological spaces are equal. More generally, given a scheme S and $X, X' \in \mathsf{Sch}/S$, we say that X' is a *thickening of X over S* iff the closed immersion $X \hookrightarrow X'$ is a morphism over S.

Remark 4.52. For thickenings, the closed embedding $f\colon X \to X'$ gives a homeomorphism of the underlying topological spaces. Recall, moreover, that closed immersions $X \hookrightarrow X'$ in Sch are in one to one correspondence with quasi-coherent sheaves of ideals $\mathcal{I}$ of $\mathcal{O}_{X'}$, see [Stacks, Section 01QN] for more details. More in general, to a closed immersion $X \hookrightarrow X'$ in Sch/S, one can associate a quasi-coherent sheaf of ideals $\mathcal{I}$ of $\mathcal{O}_{X'}$. Then the ideal associated to a thickening X' of X is *locally nilpotent*. Moreover, if the ideal sheaf $\mathcal{I}$ associated to the thickening $X \hookrightarrow X'$ is globally nilpotent, i.e. there exists $n \in \mathbb{N}$ such that $\mathcal{I}^{n+1} = 0$, we say that $X \hookrightarrow X'$ is a *finite order thickening*.

Definition 4.53: Divided power thickening.
Let U be a scheme. A *divided power thickening* of U is the datum of $(U \hookrightarrow T, \gamma)$, where $U \hookrightarrow T$ is a thickening defined by a locally nilpotent sheaf of ideals $\mathcal{I}$ on $\mathcal{O}_T$ equipped with a divided power structure defined by γ.

Remark 4.54. Thanks to remark 4.52, the datum of a divided power thickening of U is equivalent to the datum of a scheme T with divided powers, i.e. $(T, \mathcal{J}, \delta)$, as in definition 4.16, in which $\mathcal{J}$ is a locally nilpotent sheaf of ideals and is associated to the closed immersion $U \hookrightarrow T$.

Definition 4.55: Relative divided powers.
Consider a base scheme with divided powers $(S, \mathcal{I}, \gamma)$, and a divided power scheme $(T, \mathcal{J}, \delta)$. We call it

1. a *divided power scheme over* $(S, \mathcal{I}, \gamma)$ iff it is given with a morphism $T \to S$ of divided power schemes;

[1] A crystal has two characteristic properties: rigidity and ability to grow in appropriate neighbourhoods. There are crystals of every kind of substance: crystals of soda, of sulfur, of modules, of rings, of relative schemes, etc.

2. a *divided power thickening over* $(S, \mathcal{I}, \gamma)$ iff it is a divided power thickening endowed with a morphism of divided power schemes $T \to S$.

If the divided powers of S are clear from context we will simply write divided power scheme (resp. thickening) over S.

Definition 4.56: Crystalline site on X over $(S, \mathcal{I}, \gamma)$.
Let $(S, \mathcal{I}, \gamma)$ be a divided power base scheme and $X \in \mathsf{Sch}/S$ be an S-scheme on which p is locally nilpotent. The *crystalline site* on X over $(S, \mathcal{I}, \gamma)$, denoted by $\mathsf{Crys}(X/S, \mathcal{I}, \gamma)$ or simply $\mathsf{Crys}(X/S)$ if the divided power structure of S is clear from context, is given as follows. The objects of $\mathsf{Crys}(X/S)$ are divided power thickenings $(U \hookrightarrow T, \delta)$ over S with an open immersion $U \hookrightarrow X$ of S-schemes. A morphism $f\colon (U \hookrightarrow T, \gamma) \to (U' \hookrightarrow T', \delta)$ in $\mathsf{Crys}(X/S)$ is given by a commutative diagram

$$\begin{array}{ccc} U & \hookrightarrow & T \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \overline{f}} \\ U' & \hookrightarrow & T', \end{array} \tag{4.1}$$

such that $U \hookrightarrow U'$ is an open immersion (corresponds to an inclusion of open S-subschemes of X) and $\overline{f}\colon T \to T'$ is a divided power morphism. Finally we endow this category with the pretopology induced by the Zariski topology. More explicitly

$$\{(U_i \hookrightarrow T_i, \gamma_i) \longrightarrow (U \hookrightarrow T, \gamma)\}_{i \in I}$$

is a covering iff, for all i, the map $T_i \hookrightarrow T$ is an open immersion and the family $\{T_i \to T\}_{i \in I}$ is jointly surjective. Then, since U_i and T_i have the same underlying topological space, we also obtain that $\cup_{i \in I} U_i = U$ as sets.

Notation 4.57.
In case we consider the base scheme $S = \mathrm{Spec}(\mathbb{Z})$ with trivial divided powers (given by the zero sheaf of ideals), we obtain the category $\mathsf{Crys}(X/S)$, which we simply denote by $\mathsf{Crys}(X)$ since there is no restriction imposed by S. The following constructions are carried out over $\mathbb{Z}$ to keep notation cleaner, but can be generalized to the general case $\mathsf{Crys}(X/S)$.

Remark 4.58 (Sheaves on the crystalline site on X)**.** Let's remark that a sheaf $\mathcal{F}$ on $\mathsf{Crys}(X)$, for every object $(U \hookrightarrow T, \gamma)$, gives rise by restriction to a Zariski sheaf $\mathcal{F}_T$ on the scheme T by the rule

$$\mathcal{F}_T(W) \coloneqq \mathcal{F}(U \cap W \hookrightarrow W, \delta|_W),$$

where $W \subset T$ is an open subscheme. Moreover a morphism $f\colon (U \hookrightarrow T, \delta) \to (U' \hookrightarrow T', \delta')$ in $\mathsf{Crys}(X)$ gives rise to a canonical comparison map

$$c_f\colon f^{-1}\mathcal{F}_{T'} \longrightarrow \mathcal{F}_T.$$

More explicitly, for all open $W' \subset T'$, one defines the restriction

$$f|_{f^{-1}W'} : (U \cap f^{-1}W' \hookrightarrow f^{-1}W', \delta|_{f^{-1}W'}) \longrightarrow (U' \cap W' \hookrightarrow W', \delta'|_{W'})\,.$$

This defines a morphism $(f|_{f^{-1}W'})^*$ which, in turn, induces a map $\mathcal{F}_{T'}(W') \to \mathcal{F}_T(f^{-1}W')$ and finally, by adjunction, this gives the desired morphism c_f. Moreover we can notice that if, in equation (4.1), $\overline{f}$ is an open immersion, then c_f is an isomorphism, since $\mathcal{F}_{T'}$ is just the restriction of $\mathcal{F}_T$ to T'.

Conversely, using a standard argument for gluing of sheaves, see [Stacks, Section 07IN], one can define a sheaf on the crystalline site from the following data.

1. A family of Zariski sheaves $\mathcal{F}_T$, indexed by all objects $(U \hookrightarrow T, \delta) \in \mathsf{Crys}(X)$.

2. A family of morphisms $\rho_u \colon u^{-1}\mathcal{F}_{T'} \to \mathcal{F}_T$, indexed by morphisms u of $\mathsf{Crys}(X)$, satisfying the usual cocycle condition, i.e. such that the following diagram commutes

$$\begin{array}{ccc} u^{-1}v^{-1}\mathcal{F}_{T''} & \xrightarrow{v^{-1}\rho_u} & v^{-1}\mathcal{F}_{T'} \\ \downarrow \wr & & \downarrow \rho_v \\ (u \circ v)^{-1}\,\mathcal{F}_{T''} & \xrightarrow{\rho_{u\circ v}} & \mathcal{F}_T \end{array}$$

   where $u \colon (U \hookrightarrow T, \delta) \to (U' \hookrightarrow T', \delta')$, and $v \colon (U' \hookrightarrow T', \delta') \to (U'' \hookrightarrow T'', \delta'')$ range over all morphisms of $\mathsf{Crys}(X)$.

Example 4.59 (Structure sheaf)**.** The above remark allows one to define a canonical structure sheaf on $\mathsf{Crys}(X)$, denoted by $\mathcal{O}_{\mathsf{Crys}(X)}$, given by the family of structure sheaves $\mathcal{O}_T$ indexed by the objects $(U \hookrightarrow T, \delta) \in \mathsf{Crys}(X)$.

Crystals

We can finally focus our attention on crystals and their pullback.

Definition 4.60: Sheaf of modules.
We say that a sheaf on $\mathsf{Crys}(X)$ is a *sheaf of modules* iff it is a sheaf of $\mathcal{O}_{\mathsf{Crys}(X)}$-modules.

Remark 4.61. We can remark that a sheaf on $\mathsf{Crys}(X)$ is a sheaf of modules iff it induces, as in remark 4.58, a family $\{\mathcal{M}_T\}_T$ of $\mathcal{O}_T$-modules $\mathcal{M}_T$, indexed by $(U \hookrightarrow T, \delta) \in \mathsf{Crys}(X)$.

Moreover, given a sheaf of modules $\mathcal{M}$ on $\mathsf{Crys}(X)$, the morphism $\rho_u \colon u^{-1}\mathcal{M}_{T'} \to \mathcal{M}_T$, where $u \colon (U \hookrightarrow T, \delta) \to (U' \hookrightarrow T', \delta')$ is a morphism in $\mathsf{Crys}(X)$, induces a morphism

$$\sigma_u \colon u^*\mathcal{M}_{T'} \longrightarrow \mathcal{M}_T. \tag{4.2}$$

Definition 4.62.
We say that a sheaf of modules $\mathbb{M}$ is *special* iff, for all morphisms in $\mathsf{Crys}(X)$, the induced morphism in equation (4.2) is an isomorphism. Moreover we say that $\mathbb{M}$ is *quasi-coherent* iff it is special and, for all $(U \hookrightarrow T, \delta) \in \mathsf{Crys}(X)$, the $\mathcal{O}_T$-module $\mathbb{M}_T$ is quasi-coherent.

Remark 4.63. Usually, when dealing with special sheaves of modules, we will omit the isomorphism σ_u and assume that there is a literal equality. In particular, given a special sheaf of modules $\mathbb{F}$, we will write $u^*\mathbb{F}_{T'} = \mathbb{F}_T$.

Definition 4.64: Crystals of modules.
We say that a sheaf of modules on $\mathsf{Crys}(X)$ is a *crystal of modules* iff it is special. Moreover, following notation of [Mes72], we will denote them using a blackboard bold typeface.

Remark 4.65. This is just a special case of a more general notion of C-crystal, where C is a category fibered over Sch. In fact, given C, one defines C-crystals as cartesian sections of the fibered category $\mathsf{C} \times_{\mathsf{Sch}} \mathsf{Crys}(X)$, where $\mathsf{Crys}(X) \to \mathsf{Sch}$ is given by $(U \hookrightarrow T, \delta) \mapsto T$.

We can now end this section by outlining the construction of inverse images of crystals.

Remark 4.66. Since crystals are sheaves we can define them locally, given that we satisfy the necessary compatibility conditions. In particular, given a crystal of modules $\mathbb{F}$ on $\mathsf{Crys}(Y)$, where $Y \in \mathsf{Sch}$, and a morphism of schemes $\varphi \colon X \to Y$, we want to define a crystal $\varphi^*\mathbb{F}$ on $\mathsf{Crys}(X)$. To do so we will concentrate only on objects $(U \hookrightarrow T, \delta) \in \mathsf{Crys}(X)$ such that U (hence also T) is affine and $\varphi(U)$ is contained in an affine subset V of Y.

Definition 4.67: [Mes72, Chapter III, §3.8], pullback of crystals.
Consider $X, Y \in \mathsf{Sch}$, $\varphi\colon X \to Y$ a morphism of schemes and $\mathbb{F}$ a crystal of modules on Y. Fix U and V as in the last remark and set $T = \mathrm{Spec}(A), U = \mathrm{Spec}(A/I)$ and $V = \mathrm{Spec}(B)$. Consider the following pullback of rings, also known as fibered product or amalgamated product,

$$\begin{array}{ccc} A/I & \twoheadleftarrow & A \\ \uparrow & & \uparrow \\ B & \twoheadleftarrow & B \times_{A/I} A. \end{array}$$

By construction (fibered products of commutative rings commute with $\mathrm{for}\colon \mathsf{CRings} \to \mathsf{Sets}$) the morphism $B \times_{A/I} A \twoheadrightarrow B$ is surjective with kernel $J \coloneqq (0) \times I$. Since I is nilpotent, also J is. Moreover one can define divided powers on $\big(B \times_{A/I} A, J\big)$ by setting $\gamma_n(0, i) \coloneqq (0, \delta_n(i))$, making $B \times_{A/I} A \to A$ a divided power morphism. Setting $W \coloneqq \mathrm{Spec}(B \times_{A/I} A)$ and translating everything into the category of schemes, we obtain the following cartesian diagram

$$\begin{array}{ccc} U & \hookrightarrow & T \\ {\scriptstyle \varphi|_U}\downarrow & & \downarrow{\scriptstyle \widetilde{\varphi}} \\ V & \hookrightarrow & W, \end{array}$$

where $(V \hookrightarrow W, \gamma)$ is an object of $\mathsf{Crys}(Y)$ and $\widetilde{\varphi}\colon T \to W$ is a morphism of divided power schemes. We finally define $(\varphi^*\mathbb{F})_{(U \hookrightarrow T, \delta)} \coloneqq \widetilde{\varphi}^*\mathbb{F}_{(V \hookrightarrow W, \gamma)}$ and use remark 4.58 to glue these sheaves together and obtain $\varphi^*\mathbb{F}$ a crystal on $\mathsf{Crys}(X)$.

Proposition 4.68. *The construction carried out in definition 4.67 is well defined. More explicitly the definition of $\widetilde{\varphi}^*\mathbb{F}_{(V \hookrightarrow W, \gamma)}$ does not depend on the chosen affine V containing $\varphi(U)$.*

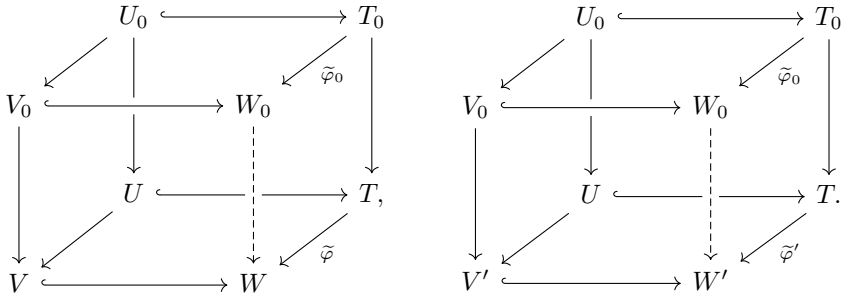
Proof. Let's keep notation as in definition 4.67 and consider another open affine V' in Y containing $\varphi(U)$. As above we construct $(V' \hookrightarrow W', \gamma') \in \mathsf{Crys}(Y)$, where $W' \coloneqq V' \amalg_U T$ and has divided powers defined as for W. Denote by $\widetilde{\varphi}'\colon T \to W'$ the morphism defined in the same way as $\widetilde{\varphi}$, then we need to show

$$\widetilde{\varphi}^*\mathbb{F}_{(V \hookrightarrow W, \gamma)} = \widetilde{\varphi}'^*\mathbb{F}_{(V' \hookrightarrow W', \gamma')}.$$

Again we are working with sheaves, hence it suffices to check equality locally. Let $U_0 \subset U$ be an open affine subset such that $\varphi(U_0) \subset V_0 \subset V \cap V'$, where V_0 is again open affine. Finally we define $T_0 \subset T$ the open subscheme of T induced by the immersion $U_0 \hookrightarrow U$. Repeating the construction with the amalgamated product we obtain the diagram

$$\begin{array}{ccc} U_0 & \hookrightarrow & T_0 \\ \downarrow & & \downarrow{\scriptstyle \widetilde{\varphi}_0} \\ V_0 & \hookrightarrow & W_0. \end{array}$$

Moreover this construction is such that the following diagrams both commute



Then, by universal property of amalgamated coproduct, we obtain the existence and uniqueness of the dashed arrows. Now we can conclude, since $\mathbb{F}$ is a crystal and commutativity of the above diagrams implies

$$(\widetilde{\varphi}^*\mathbb{F}_{(V\hookrightarrow W,\gamma)})\big|_{T_0} = \widetilde{\varphi}_0^*\mathbb{F}_{(V_0\hookrightarrow W_0,\gamma_0)} = (\widetilde{\varphi}'^*\mathbb{F}_{(V'\hookrightarrow W',\gamma')})\big|_{T_0}\,.$$

Then, by sheaf properties, the definition of $\widetilde{\varphi}^*$ does not depend on the chosen V. ■

5 The crystals associated to Barsotti-Tate groups

In this section we want to associate to certain Barsotti-Tate groups a few crystals. In particular, as hinted at in the introduction, we will give the definition of $\mathbb{D}^*$, the crystal whose aim is to generalize the Dieudonné module associated to a Brasotti-Tate group. In order to do so we need to discuss universal extensions, which will be the basis for the definitions of such crystals.

5.1 Universal extensions

Before studying the case of our interest, let's recall the necessary definitions and notations with regards to extensions in general.

Extensions

Here we will usually assume C to be an abelian category on which we can compute the $\mathrm{Ext}^n_{\mathsf{C}}$ functors. Let's recall already remark 3.23, which states that Gr/S satisfies the above requirements.

Definition 5.1: Extension.
Let C be an abelian category and $A, B \in \mathsf{C}$. We define an *extension* X of A by B to be a short exact sequence

$$(\zeta) \qquad 0 \longrightarrow B \longrightarrow X \longrightarrow A \longrightarrow 0,$$

where $X \in \mathsf{C}$. We might also denote the extension by ζ. Moreover, given two extensions ζ and ζ' of A by B, respectively given by X and X', we say that a *morphism of extensions* of A by B is a morphism $f\colon X \to X'$ that makes the following diagram commute

$$\begin{array}{lccccccc} (\zeta) & 0 & \longrightarrow & B & \longrightarrow & X & \longrightarrow & A & \longrightarrow & 0 \\ & & & \| & & \downarrow{\scriptstyle f} & & \| & & \\ (\zeta') & 0 & \longrightarrow & B & \longrightarrow & X' & \longrightarrow & A & \longrightarrow & 0. \end{array}$$

Finally we introduce the notation $\mathrm{E}(A, B)$ for the set of all extensions of A by B, and the notation $\mathrm{Hom}\,(\zeta, \zeta')$ to denote the set of morphisms $f\colon X \to X'$ inducing a morphism of extensions.

Remark 5.2. Notice that, thanks to the five lemma, all $f \in \mathrm{Hom}\,(\zeta, \zeta')$ are isomorphisms in C.

Definition 5.3: Pullback and pushout.

1. Given a morphism $\gamma\colon A' \to A$ and an extension X of A by B, we define $X' \coloneqq X \times_A A'$, so that we have the following morphism of short exact sequences

$$\begin{array}{lccccccc} (\zeta\gamma) & 0 & \longrightarrow & B & \longrightarrow & X' & \longrightarrow & A' & \longrightarrow & 0 \\ & & & \| & & \downarrow & & \downarrow{\scriptstyle \gamma} & & \\ (\zeta) & 0 & \longrightarrow & B & \longrightarrow & X & \longrightarrow & A & \longrightarrow & 0. \end{array}$$

   The extension X' of A' by B is called the *pullback* of X via $\gamma\colon A' \to A$. Moreover, if we denote with ζ the extension X of A by B, then $\zeta\gamma$ will denote its pullback via γ.

2. Given a morphism $\beta\colon B \to B'$ and an extension X of A by B, we define $X' \coloneqq B' \amalg_A X$, so that we have the following morphism of short exact sequences

$$\begin{array}{lccccccc} (\xi) & 0 & \longrightarrow & B & \longrightarrow & X & \longrightarrow & A & \longrightarrow & 0 \\ & & & {\scriptstyle \beta}\downarrow & & \downarrow & & \| & & \\ (\beta\xi) & 0 & \longrightarrow & B' & \longrightarrow & X' & \longrightarrow & A & \longrightarrow & 0. \end{array}$$

   The extension X' of A by B' is called the *pushout* of X via $\beta\colon B \to B'$. Moreover, if we denote with ξ the extension X of A by B, then $\beta\xi$ will denote its pushout via β.

Remark 5.4. Given an extension

$$(\zeta) \qquad 0 \longrightarrow M \xrightarrow{\ \iota\ } E \xrightarrow{\ \pi\ } G \longrightarrow 0,$$

we can construct an isomorphism

$$\begin{aligned} \mathrm{Hom}_{\mathsf{Gr}/S}\,(G, M) &\xrightarrow{\ \sim\ } \mathrm{Aut}(\zeta) \\ u &\longmapsto \mathrm{id}_E + \iota \circ u \circ \pi, \end{aligned}$$

where we denoted by $\mathrm{Aut}(\zeta) \coloneqq \mathrm{Hom}\,(\zeta, \zeta)$. The construction of the inverse morphism follows naturally from the universal properties of kernel and cokernel, since $M = \ker \pi$ and $G = \operatorname{coker} \iota$.

Remark 5.5. We define an equivalence relation on the set $\mathrm{E}(A, B)$ by saying that $\zeta \sim \zeta'$ iff $\mathrm{Hom}\,(\zeta, \zeta') \neq 0$, i.e. iff there is a commutative diagram

$$\begin{array}{lccccccc} (\zeta) & 0 & \longrightarrow & B & \longrightarrow & X & \longrightarrow & A & \longrightarrow & 0 \\ & & & \| & & \downarrow{\scriptstyle \wr} & & \| & & \\ (\zeta') & 0 & \longrightarrow & B & \longrightarrow & X' & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

connecting the two extensions. Assume now that we can compute $\mathrm{Ext}^n_{\mathsf{C}}(A, B)$ for all $A, B \in \mathsf{C}$ and all $n \in \mathbb{N}$. Then we can define a map $\theta\colon \mathrm{E}(A, B) \to \mathrm{Ext}^1_{\mathsf{C}}(A, B)$ as follows. Fix an

extension $\zeta \in \mathrm{E}(A,B)$, given by X, and denote by h^B the Yoneda embedding defined, for all $X \in \mathsf{C}$, by $h^B(X) \coloneqq \mathrm{Hom}_{\mathsf{C}}(X,B)$. We apply the right derived functor $\left\{R^n h^B\right\}_{n\in\mathbb{N}}$ of h^B, to the short exact sequence

$$(\zeta) \qquad 0 \longrightarrow B \longrightarrow X \longrightarrow A \longrightarrow 0,$$

corresponding to the extension ζ. This gives rise to the exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathsf{C}}(A,B) \longrightarrow \mathrm{Hom}_{\mathsf{C}}(X,V) \longrightarrow \mathrm{Hom}_{\mathsf{C}}(B,B) \xrightarrow{\partial} \mathrm{Ext}^1_{\mathsf{C}}(A,B).$$

Then we define $\theta(\zeta) \coloneqq \partial(\mathrm{id}_B) \in \mathrm{Ext}^1_{\mathsf{C}}(A,B)$.

Lemma 5.6 ([Wei94, §3.4, Porism 3.4.2])**.** *Let C be an abelian category on which we can compute $\mathrm{Ext}^n_{\mathsf{C}}(A,B)$ for all $A,B \in \mathsf{C}$ and all $n \in \mathbb{N}$. Let $\zeta \sim \zeta'$ be equivalent extensions of A by B. Then $\theta(\zeta) = \theta(\zeta')$, hence θ defines a map*

$$\theta\colon \frac{\mathrm{E}(A,B)}{\sim} \longrightarrow \mathrm{Ext}^1_{\mathsf{C}}(A,B).$$

Theorem 5.7 ([Wei94, §3.4, Thoerem 3.4.3])**.** *Let C be an abelian category on which we can compute $\mathrm{Ext}^n_{\mathsf{C}}(A,B)$ for all $A,B \in \mathsf{C}$ and all $n \in \mathbb{N}$. Then θ induces a bijective correspondence*

$$\frac{\mathrm{E}(A,B)}{\sim} \xleftrightarrow{\ \theta\ } \mathrm{Ext}^1_{\mathsf{C}}(A,B).$$

Universal extensions

For this section we fix S a scheme and G a finite locally-free S-group. For the first proposition it is not necessary, but for the rest of the section we will often assume that p^N is zero on S. We recall that, thanks to remark 3.23, we can apply the results of last section to Gr/S.

Proposition 5.8 ([Mes72, Chapter IV, proposition 1.3])**.** *The functor acting, on quasi-coherent $\mathcal{O}_S$-modules, by*

$$\mathcal{M} \longmapsto \mathrm{Hom}_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}})$$

is corepresented by $\underline{\omega}_{G^D}$, where G^D is the Cartier dual of G.

Remark 5.9. The proposition implies that there is a homomorphism $\alpha\colon G \to \underline{\omega}_{G^D}$ with the property that, for all $\beta\colon G \to \underline{\mathcal{M}}$, there is a unique linear $u\colon \underline{\omega}_{G^D} \to \underline{\mathcal{M}}$ such that $\beta = u \circ \alpha$. Moreover, following [Mes72, Chapter IV, remark 1.6], one can check that the isomorphism

$$\mathrm{Hom}_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}) \xrightarrow{\ \sim\ } \mathrm{Hom}_{\mathsf{Gr}/S}(\underline{\omega}_{G^D}, \underline{\mathcal{M}})$$

is functorial in G. Thus, given a morphism of finite locally-free S-groups $u\colon G \to H$, we have a commutative diagram whose lower horizontal arrow is induced by the Cartier dual of u

$$\begin{array}{ccc} G & \xrightarrow{\ u\ } & H \\ {\scriptstyle\alpha_G}\downarrow & & \downarrow{\scriptstyle\alpha_H} \\ \underline{\omega}_{G^D} & \longrightarrow & \underline{\omega}_{H^D}. \end{array} \tag{5.1}$$

Lemma 5.10. *Let S be a scheme killed by p^N, G a Barsotti-Tate group on S and $\mathcal{M}$ a quasi-coherent $\mathcal{O}_S$-module. Then any extension ζ of G by $\underline{\mathcal{M}}$ is uniquely determined by $\theta(\zeta) \in \mathrm{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}})$.*

Proof. Since p^N kills S, multiplication by p^N is the trivial map on $\mathcal{M}$. As a consequence, for all $f \in \mathrm{Hom}_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}})$, we obtain the following commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & \underline{\mathcal{M}} \\ {\scriptstyle p^N}\downarrow & \searrow^{0} & \downarrow{\scriptstyle p^n} \\ G & \xrightarrow[f]{} & \underline{\mathcal{M}}. \end{array}$$

But this means that $f \circ p^N = 0$ and, since multiplication by p^N on G is an epimorphism, that $f = 0$. This proves that $\mathrm{Hom}_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}) = 0$. Thanks to remark 5.4, this implies that the only automorphism of ζ is the identity. Let's now recall remark 3.23, which states that Gr/S is an abelian category with enough injectives. This allows us to apply theorem 5.7. Then the above implies that ζ is uniquely determined by $\theta(\zeta) \in \mathrm{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}})$, since its equivalence class is reduced to ζ itself. ∎

Definition 5.11: Universal extension.
Let S be a scheme, $G \in \mathsf{BT}/S$ and $\underline{\mathcal{V}}(G)$ a vector S-group, as in definition 4.34. We say that an extension $\zeta \in \mathrm{E}(G, \underline{\mathcal{V}}(G))$, given by $E(G)$, is *universal* iff, given any extension

$$(\xi) \qquad 0 \longrightarrow \underline{\mathcal{M}} \longrightarrow (*) \longrightarrow G \longrightarrow 0$$

of G by a vector S-group $\underline{\mathcal{M}}$, where also $\mathcal{M}$ is a quasi-coherent $\mathcal{O}_S$-module, there is a unique map $\varphi\colon \underline{\mathcal{V}}(G) \to \underline{\mathcal{M}}$ such that $\varphi\zeta = \xi$, i.e. the pushout of $E(G)$ by φ is the given extension ξ.

Remark 5.12. Let's consider again the case where p is nilpotent on the base scheme S. By rigidity of extensions of Barsotti-Tate groups by quasi-coherent modules, i.e. lemma 5.10, we see that $\varphi\zeta = \xi$ is actually an equality, and not just an isomorphism.

Proposition 5.13. *Let S be a scheme killed by p^N and G a Barsotti-Tate group on S. Then there is a universal extension of G by a vector group, which we denote by*

$$0 \longrightarrow \underline{\mathcal{V}}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0.$$

Proof. Let's start by noticing that we are in the same situation of lemma 5.10. Consider now the short exact sequence

$$(\zeta') \qquad 0 \longrightarrow G(N) \xrightarrow{\iota_G} G \xrightarrow{p^N} G \longrightarrow 0.$$

Let's fix a quasi-coherent $\mathcal{O}_S$-module $\mathcal{M}$. Applying, as in remark 5.5, the right derived functor $\left\{R^n h^{\underline{\mathcal{M}}}\right\}_{n\in\mathbb{N}}$, we obtain the long exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathsf{Gr}/S}(G(N), \underline{\mathcal{M}}) \xrightarrow{\partial} \mathrm{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}) \xrightarrow{p^N} \mathrm{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}),$$

where we used $\mathrm{Hom}_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}) = 0$, as seen in lemma 5.10. Moreover Ext^1 is a bifunctor, which implies that the map $p^N\colon \mathrm{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}) \to \mathrm{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}})$ comes from multiplication by p^N in $\underline{\mathcal{M}}$. By additivity of Ext, this is 0, which implies that ∂ is an isomorphism. Clearly this argument is functorial in $\underline{\mathcal{M}}$. Moreover, by proposition 5.8, we see that the source of ∂ is

represented by $\underline{\omega}_{G(N)^D}$. Let $\alpha\colon G(N) \to \underline{\omega}_{G(N)^D}$ be as in remark 5.9 and define $\zeta \coloneqq \alpha\zeta'$, as in the following commutative diagram

$$\begin{array}{lccccccccc}
(\zeta') & 0 & \longrightarrow & G(N) & \xrightarrow{\iota_G} & G & \xrightarrow{p^N} & G & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \| & & \\
(\alpha\zeta') & 0 & \longrightarrow & \underline{\omega}_{G(N)^D} & \longrightarrow & E(G) & \longrightarrow & G & \longrightarrow & 0,
\end{array}$$

where we denoted by $E(G) \coloneqq \underline{\omega}_{G(N)^D} \amalg_{G(N)} G$. Then, by rigidity of extensions of G by vector groups (lemma 5.10) any extension ξ of G by a vector group is uniquely determined by its class $\theta(\xi) \in \operatorname{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}})$. By the above this corresponds to a morphism $u\colon G(N) \to \underline{\mathcal{M}}$ which, thanks to remark 5.9, factors through α as $u = \alpha \circ \beta$. Finally, thanks to naturality of the connecting morphism ∂, we obtain the following commutative diagram, obtained from the pushout of the extension ζ via β:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \operatorname{Hom}_{\mathsf{Gr}/S}(P, \underline{\mathcal{M}}) & \longrightarrow & \operatorname{Hom}_{\mathsf{Gr}/S}(\underline{\mathcal{M}}, \underline{\mathcal{M}}) & \xrightarrow{\partial_1} & \operatorname{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}) \\
 & & \downarrow & & \downarrow{\scriptstyle \operatorname{Hom}_{\mathsf{Gr}/S}(\,\cdot\,,\beta)} & & \| \\
0 & \longrightarrow & \operatorname{Hom}_{\mathsf{Gr}/S}(E(G), \underline{\mathcal{M}}) & \longrightarrow & \operatorname{Hom}_{\mathsf{Gr}/S}(\underline{\omega}_{G(N)^D}, \underline{\mathcal{M}}) & \xrightarrow{\partial_2} & \operatorname{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}) \\
 & & \downarrow & & \downarrow{\scriptstyle \operatorname{Hom}_{\mathsf{Gr}/S}(\,\cdot\,,\alpha)} & & \| \\
0 & \longrightarrow & 0 & \longrightarrow & \operatorname{Hom}_{\mathsf{Gr}/S}(G(N), \underline{\mathcal{M}}) & \xrightarrow{\partial_3} & \operatorname{Ext}^1_{\mathsf{Gr}/S}(G, \underline{\mathcal{M}}),
\end{array}$$

where the extension $\beta\zeta$ of G by $\underline{\mathcal{M}}$ is given by P. By definition of θ the rightmost rectangle acts on elements as

$$\begin{array}{ccc}
\mathrm{id}_{\underline{\mathcal{M}}} & \xmapsto{\partial_1} & \theta(\beta\zeta) \\
{\scriptstyle \beta^* \circ \alpha^*}\downarrow & & \| \\
u & \xmapsto{\partial_3} & \theta(\xi).
\end{array}$$

Commutativity of this diagram implies that $\theta(\beta\zeta) = \theta(\xi)$. Then rigidity of the extensions grants that $\xi = \beta\zeta$, i.e. that ζ is universal. ■

Remark 5.14 ([Mes72, Chapter III, remark 1.11])**.** Notice that in the above proposition one could substitute N with any $n \geq N$ and still obtain a universal extension. The unique isomorphism comes from the commutative diagram of equation (5.1) which, setting $H = G(N)$ and $G = G(N+i)$, becomes

$$\begin{array}{ccc}
G(N+i) & \xrightarrow{p^i} & G(N) \\
{\scriptstyle \alpha_{G(N+i)}}\downarrow & & \downarrow{\scriptstyle \alpha_{G(N)}} \\
\underline{\omega}_{G(N+i)^D} & \xrightarrow{\sim} & \underline{\omega}_{G(N)^D}.
\end{array}$$

Here the fact that the bottom arrow is an isomorphism is remark 3.57. Then, thanks to universal property of pushout it's easy to construct a morphism of extensions, which is clearly an isomorphism thanks to the five lemma.

Definition 5.15.
Given S and G as before, for n sufficiently big, we define $\underline{\mathcal{V}}(G) \coloneqq \underline{\omega}_{G(n)^D}$ and $E(G) \coloneqq \underline{\mathcal{V}}(G) \amalg_{G(n)} G$. Then the extension

$$(\zeta) \qquad 0 \longrightarrow \underline{\mathcal{V}}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0$$

is universal. Moreover $E(G)$ is an fppf sheaf of groups on S, determined up to unique isomorphism.

Now that we have finally defined it, let's see a few results concerning this universal extension.

Lemma 5.16 ([Mes72, Chapter IV, lemma 1.13])**.** *The universal extension*

$$0 \longrightarrow \underline{\mathcal{V}}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0$$

commutes with base change.

Lemma 5.17 ([Mes72, Chapter IV, corollary 1.14])**.** *Assume that p is only locally nilpotent on S and consider G a Barsotti-Tate group on S. Then there is a universal extension, which we denote by*

$$0 \longrightarrow \underline{\mathcal{V}}(G) \longrightarrow E(G) \longrightarrow G \longrightarrow 0,$$

of G by the vector group $\underline{\mathcal{V}}(G) \coloneqq \underline{\omega}_{G^D}$.

Proposition 5.18 ([Mes72, Chapter IV, proposition 1.15])**.** *Let p be locally nilpotent on S and G, H be two Barsotti-Tate groups on S, with a homomorphism $u\colon G \to H$. Then there is a unique homomorphism $E(u)\colon E(G) \to E(H)$ inducing the morphism of extensions*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{\mathcal{V}}(G) & \longrightarrow & E(G) & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \underline{\mathcal{V}}(u)} & & \downarrow{\scriptstyle E(u)} & & \downarrow{\scriptstyle u} & & \\ 0 & \longrightarrow & \underline{\mathcal{V}}(H) & \longrightarrow & E(H) & \longrightarrow & H & \longrightarrow & 0, \end{array}$$

where $\underline{\mathcal{V}}(u)$ is induced by the Cartier dual of u.

Recall that, in notation 3.28, we introduced the notation $\overline{G} \coloneqq \varinjlim_{k\in\mathbb{N}} \mathrm{Inf}^k(G)$, for $G \in \mathsf{Gr}/S$.

Proposition 5.19 ([Mes72, Chapter IV, proposition 1.19])**.** *Let $G \in \mathsf{BT}/S$ and S be as before, then $\overline{E(G)}$ is a* formal Lie group*.*

Definition 5.20.
Let S be a scheme where p is locally nilpotent and G a Barsotti-Tate group on S. Denote by $E(G)$ the universal extension of G, then we define $\mathrm{Lie}(E(G)) \coloneqq \mathrm{Lie}(\overline{E(G)})$.

Remark 5.21. Notice that $\mathrm{Lie}(E(G))$ is a locally-free $\mathcal{O}_S$-module of finite rank.

Let's end with a couple of results, still with the same notation and hypothesis as before.

Proposition 5.22 ([Mes72, Chapter IV, proposition 1.21])**.** *The following sequence is exact*

$$0 \longrightarrow \overline{\underline{\mathcal{V}}(G)} \longrightarrow \overline{E(G)} \longrightarrow \overline{G} \longrightarrow 0.$$

Proposition 5.23 ([Mes72, Chapter IV, proposition 1.22])**.** *The following sequence is exact*

$$0 \longrightarrow \underline{\mathcal{V}}(G) \longrightarrow \underline{\mathrm{Lie}}(E(G)) \longrightarrow \underline{\mathrm{Lie}}(G) \longrightarrow 0.$$

5.2 Crystals associated to Barsotti-Tate groups

Here we can finally make use of the above results to define the desired crystals associated to Barsotti-Tate groups. Since it will be used in what follows, we start by introducing the following notation.

Notation 5.24.
Let S be a scheme and $\mathcal{I}$ a quasi-coherent sheaf of ideals of $\mathcal{O}_S$. We write $\mathbb{V}(\mathcal{I})$ to denote the unique closed subscheme of S induced by the sheaf of ideals $\mathcal{I}$. Notice that, in the affine case $S = \mathrm{Spec}(A)$, the sheaf $\mathcal{I}$ corresponds to an ideal $I \triangleleft A$ and $\mathbb{V}(I) \simeq \mathrm{Spec}(A/I)$.

Remark 5.25. This section follows [Mes72, Chpater IV, §2], in which the author introduces a new notation. He denotes by $\mathsf{BT}'(S_0)$ the subcategory of locally infinitesimally liftable Barsotti-Tate groups, i.e. which can be locally lifted along finite order thickenings. At the same time, in the introduction to his work, Messing acknowledges that it has been shown that all objects $G_0 \in \mathsf{BT}/S_0$ satisfy this condition. For this reason we chose to differentiate our notation from that of [Mes72]. Still, since it is used to define our crystals, here is the precise lifting requirements asked by Messing. Let S_0 be a scheme with p locally nilpotent on it. We say that G_0 is *locally infinitesimally liftable* iff there is an affine open cover $\{U_i\}_{i\in I}$ of S_0, which depends on G_0, on which, for all i and all finite order thickening $U_i \hookrightarrow U$, there is a $G \in \mathsf{BT}/U$ such that $G|_{U_i} = G_0|_{U_i}$.

Theorem 5.26 ([Mes72, Chapter IV, theorem 2.2])**.** *Let $S = \mathrm{Spec}(A)$ such that $p^N \cdot 1_S = 0$ and $S_0 \coloneqq \mathbb{V}(I) \subset S$, where I is an ideal of A with nilpotent divided powers. Consider $G, H \in \mathsf{BT}/S$ and a homomorphism $u_0 \colon G_0 \to H_0$ between the respective restrictions to S_0. By proposition 5.18 u_0 defines a morphism of extensions $v_0 \coloneqq E(u_0) \colon E(G_0) \to E(H_0)$, making the diagram commute:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{\mathcal{V}}(G_0) & \longrightarrow & E(G_0) & \longrightarrow & G_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \underline{\mathcal{V}}(u_0)} & & \downarrow{\scriptstyle v_0} & & \downarrow{\scriptstyle u_0} & & \\ 0 & \longrightarrow & \underline{\mathcal{V}}(H_0) & \longrightarrow & E(H_0) & \longrightarrow & H_0 & \longrightarrow & 0. \end{array}$$

Then there is a unique morphism of S-groups $v \colon E(G) \to E(H)$, which is not necessarily a morphism of extensions, that satisfies the following properties.

1. *v is a lift of v_0.*
2. *Denote the inclusions by $i \colon \underline{\mathcal{V}}(H) \to E(H)$ and by $j \colon \underline{\mathcal{V}}(G) \to E(G)$. Given $w \colon \underline{\mathcal{V}}(G) \to \underline{\mathcal{V}}(H)$ a lift of $\underline{\mathcal{V}}(u_0)$ such that $d \coloneqq (i \circ w - v \circ j) \colon \underline{\mathcal{V}}(G) \to E(H)$ induces the zero morphism on S_0, then d is an exponential.*

Remark 5.27 ([Mes72, Chapter IV, remark 2.3])**.** The morphism v is independent of the choice of w in theorem 5.26. In fact, chosen another lift w' of $\underline{\mathcal{V}}(u_0)$, we can write $w' = w + h$, where h, thanks to lemma 4.48 is an exponential. So, defining d' corresponding to w' in the above construction, we obtain $d' = d + i \circ h$. But then it is easy to show that $i \circ h$ is itself an exponential, hence that d' is an exponential iff d is.

As shown by the following corollaries, the construction of the lift v is functorial in G.

Corollary 5.28 ([Mes72, Chapter IV, corollary 2.4.1])**.** *Let $G, H, K \in \mathsf{BT}/S$ as before and consider another homomorphism $u_0' \colon H_0 \to K_0$, where K_0 again denotes the restriction of K to S_0. Denote by $E_S(u_0)$ the morphism v whose existence is granted by theorem 5.26. Then $E_S(u_0' \circ u_0) = E_S(u_0') \circ E_S(u_0)$.*

Corollary 5.29 ([Mes72, Chapter IV, corollary 2.4.2])**.** *If, in the above notation, $G = H$ and $u_0 = \mathrm{id}_{G_0}$, then $E_S(u_0) = \mathrm{id}_G$.*

Corollary 5.30 ([Mes72, Chapter IV, corollary 2.4.3])**.** *Let G, H, u_0 as in theorem 5.26, with u_0 an isomorphism. Then $E_S(u_0)$ is an isomorphism too.*

Corollary 5.31 ([Mes72, Chapter IV, corollary 2.4.4])**.** *Suppose we are given a commutative diagram*

$$\begin{array}{ccc} S_0 & \hookrightarrow & S \\ \uparrow & & \uparrow \\ S_0' & \hookrightarrow & S', \end{array}$$

where $S_0 \hookrightarrow S$ and $S_0' \hookrightarrow S'$ are nilpotent immersions with divided powers, as in the statement of theorem 5.26. Write $S_0' = \mathbb{V}(I')$ and $S_0 = \mathbb{V}(I)$ and assume that $S' \to S$ is a divided powers morphism. Consider $G, H \in \mathsf{BT}/S$ and $u_0 \colon G_0 \to H_0$ as before. Then the construction of $E_S(u_0)$ is compatible with the base change $S' \to S$. More explicitly we have

$$E_{S'}(u_{0_{S_0'}}) = (E_S(u_0))_{S'} = v_{S'}.$$

Thanks to the above results we are ready to define the crystals we hinted at above.

Remark 5.32 ([Mes72, Chapter IV, §2.5])**.** Let S_0 be a scheme, on which p is locally nilpotent, and $G_0 \in \mathsf{BT}/S_0$. Let's start by recalling that, since crystals are sheaves on $\mathsf{Crys}(S_0)$, it suffices to define them locally. More specifically we are going to define their evaluation on objects $(U_0 \hookrightarrow U, \delta) \in \mathsf{Crys}(S_0)$ with the property that U_0 is affine with p nilpotent on U_0 and $G_0|_{U_0}$ can be lifted to U.

Moreover, by corollaries 5.28 to 5.30, we can see that, fixing one such object of $\mathsf{Crys}(S_0)$, $E(G)$ is independent of the chosen lift of $G_0|_{U_0}$. Also, given $f \colon (V_0 \hookrightarrow V, \delta) \to (U_0 \hookrightarrow U, \gamma)$, a morphism in $\mathsf{Crys}(S_0)$ inducing the diagram

$$\begin{array}{ccc} U_0 & \hookrightarrow & U \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle \overline{f}} \\ V_0 & \hookrightarrow & V, \end{array}$$

then f is an open immersion. Hence $u_0 \colon f^*\, G_0|_{U_0} \to G_0|_{V_0}$ is an isomorphism. Then, applying corollary 5.30 to G_U a lift of $G_0|_{U_0}$ to U and G_V of $G_0|_{V_0}$ to V, we obtain a canonical isomorphism

$$\overline{f}^*\,(E(G_U)) \xrightarrow{\sim} E(G_V).$$

Definition 5.33.

1. In the above notation, we define the crystal $\mathbb{E}(G_0)$ by setting its value on $(U_0 \hookrightarrow U, \delta)$, as considered before, to be $E(G)$ for any lift of $G_0|_{U_0}$.

2. In the same way we define, for any morphism $u_0 \colon G_0 \to H_0$ of Barsotti-Tate groups on S_0, a morphism between the associated crystals. In particular, on "sufficiently small" open subsets $U_0 \hookrightarrow U$ as before, we set $\mathbb{E}(u_0) \coloneqq E(u_0)$.

3. Finally, for an arbitrary morphism of schemes $f \colon T_0 \to S_0$, we can define the *pullback* of the crystal $\mathbb{E}(G_0)$, denoted by $f^*\,(\mathbb{E}(G_0))$, on "sufficiently small" open sets in the crystalline site of T_0. Here we say that $V_0 \hookrightarrow V$ is sufficiently small iff

(a) $f(V_0) \subset U_0$ and $G_0|_{U_0}$ can be lifted to infinitesimal neighbourhoods,

(b) V_0 is affine.

Remark 5.34 ([Mes72, Chapter IV, §2.5])**.** Since we are in the affine case we can use the construction of amalgamated sum of schemes to obtain the diagram

$$\begin{array}{ccc} U_0 & \hookrightarrow & U \coloneqq U_0 \amalg_{V_0} V \\ {\scriptstyle f}\uparrow & & \uparrow \\ V_0 & \hookrightarrow & V. \end{array}$$

Then, as seen in remark 5.32, for a lifting G_U of $G_0|_{U_0}$ to U, we have

$$\overline{f}^* \left(E(G_U)\right) = E(G_V) = \mathbb{E}\left(f^*(G_0)\right)_{V_0 \hookrightarrow V}.$$

As a consequence $f^*\left(\mathbb{E}(G_0)\right) = \mathbb{E}\left(f^*(G_0)\right)$. Let's now notice that we write the above as equalities following remark 4.63; more properly these equalities should be considered as isomorphisms. Then a more precise statement would be that the following diagram commutes up to a *unique natural equivalence*:

$$\begin{array}{ccc} \mathsf{BT}/S_0 & \xrightarrow{\mathbb{E}} & \{\text{Crystals in } \mathsf{Gr}/S_0\} \\ {\scriptstyle f^*}\downarrow & & \downarrow{\scriptstyle f^*} \\ \mathsf{BT}/T_0 & \xrightarrow{\mathbb{E}} & \{\text{Crystals in } \mathsf{Gr}/T_0\}, \end{array}$$

where by "Crystals in Gr/S" we mean sheaves $\mathbb{F}$ on $\mathsf{Crys}(S)$ which, for each $(U_0 \hookrightarrow U, \gamma) \in \mathsf{Crys}(S)$, induce a sheaf $\mathbb{F}_{(U_0 \hookrightarrow U,\gamma)} \in \mathsf{Gr}/S$ and are special, as in definition 4.62.

Definition 5.35.

1. We define the functor $\overline{\mathbb{E}}$, associating to any $G_0 \in \mathsf{BT}/S_0$ a crystal in Gr/S_0 setting, for any $(U_0 \hookrightarrow U, \delta) \in \mathsf{Crys}(S_0)$,
$$\overline{\mathbb{E}}(G_0)_{(U_0 \hookrightarrow U,\delta)} \coloneqq \overline{\left(\mathbb{E}(G_0)_{(U_0 \hookrightarrow U,\delta)}\right)}.$$
2. We define the functor $\mathbb{D}$, associating to any $G_0 \in \mathsf{BT}/S_0$ a crystal in Gr/S_0 setting, for any $(U_0 \hookrightarrow U, \delta) \in \mathsf{Crys}(S_0)$,
$$\mathbb{D}(G_0)_{(U_0 \hookrightarrow U,\delta)} \coloneqq \mathrm{Lie}\left(\overline{\mathbb{E}}(G_0)_{(U_0 \hookrightarrow U,\delta)}\right).$$
3. We define the functor $\mathbb{D}^*$, associating to any $G_0 \in \mathsf{BT}/S_0$ a crystal in Gr/S_0 setting, for any $(U_0 \hookrightarrow U, \delta) \in \mathsf{Crys}(S_0)$,
$$\mathbb{D}^*(G_0)_{(U_0 \hookrightarrow U,\delta)} \coloneqq \mathrm{Lie}\left(\overline{\mathbb{E}}(G_0^D)_{(U_0 \hookrightarrow U,\delta)}\right).$$

Remark 5.36. It is clear that all functors, $\mathbb{E}$, $\overline{\mathbb{E}}$, $\mathbb{D}$ and $\mathbb{D}^*$ are additive.

Remark 5.37. Let's summarise the above constructions. Consider $S_0 \hookrightarrow S$ a nilpotent divided power immersion. Assume that $G_0 \in \mathsf{BT}/S_0$ can be lifted to $G \in \mathsf{BT}/S$. Notice that, by remark 3.63, G^D is a lift of G_0^D. Then, up to canonical isomorphisms, we have

1. $\mathbb{E}(G_0)_{S_0 \hookrightarrow S} = E(G)$,
2. $\overline{\mathbb{E}}(G_0)_{S_0 \hookrightarrow S} = \overline{E(G)}$,
3. $\mathbb{D}(G_0)_{S_0 \hookrightarrow S} = \mathrm{Lie}(E(G))$,
4. $\mathbb{D}^*(G_0)_{S_0 \hookrightarrow S} = \mathrm{Lie}(E(G^D))$.

5.3 Grothendieck-Messing deformation theory

In this section we present the main result of [Mes72, Chapter V]. It is going to be of fundamental importance in the theory of Breuil and Kisin of classification of Barsotti-Tate groups over O_K, the ring of integers of a local field. In particular this result will allow us to lift Barsotti-Tate groups over a divided powers thickening, in a way which is uniquely determined by a certain filtration on its associated crystal.

Notation 5.38.
Let S be a scheme on which p is locally nilpotent, $\mathcal{I}$ be a quasi-coherent sheaf of ideals on $\mathcal{O}_S$ endowed with locally nilpotent divided powers. Let $S_0 \coloneqq \mathbb{V}(\mathcal{I})$, so that $S_0 \hookrightarrow S$ is an object of the crystalline site of S_0.

Remark 5.39. It is worth quoting remark 5.25, since also for [Mes72, Chapter V] Messing introduces a new notion of liftable Barsotti-Tate groups. Again, we will not follow his notation $\mathsf{BT}'(S_0)$, since all $G \in \mathsf{BT}/S_0$ can be lifted locally (in the Zariski topology) along $S_0 \hookrightarrow S$, which allows us to carry along the following construction and proofs.

Notation 5.40.
In this section we are mainly interested in the values of crystals on a specific object of $\mathsf{Crys}(S_0)$, given by the closed immersion $S_0 \hookrightarrow S$ Hence we introduce the following notation. Let $G_0 \in \mathsf{BT}/S_0$ and $\mathbb{F}$ a crystal on $\mathsf{Crys}(S)$, we denote by $\mathbb{F}_S$ the Zariski sheaf $\mathbb{F}_{(S_0 \hookrightarrow S, \mathcal{I})}$. In particular, for the crystals defined in the previous section, we have

1. $\mathbb{E}(G_0)_S \coloneqq \mathbb{E}(G_0)_{S_0 \hookrightarrow S} = E(G)$,
2. $\overline{\mathbb{E}}(G_0)_S \coloneqq \overline{\mathbb{E}}(G_0)_{S_0 \hookrightarrow S} = \overline{E(G)}$,
3. $\mathbb{D}(G_0)_S \coloneqq \mathbb{D}(G_0)_{S_0 \hookrightarrow S} = \mathrm{Lie}(E(G))$.
4. $\mathbb{D}^*(G_0)_S \coloneqq \mathbb{D}^*(G_0)_{S_0 \hookrightarrow S} = \mathrm{Lie}(E(G^D))$.

Definition 5.41: Admissible filtration.
Consider $G_0 \in \mathsf{BT}/S_0$. A filtration $\mathrm{Fil}^1 \subset \mathbb{D}(G_0)_S$ is said to be *admissible* iff Fil^1 is a locally-free vector subgroup with locally-free quotient which, on S_0, reduces to (the morphisms of sheaves on S_0 associated to)

$$\underline{\mathcal{V}}(G_0) \hookrightarrow \underline{\mathrm{Lie}}(E(G_0)).$$

Definition 5.42.
Let's fix $S_0 \hookrightarrow S$ as before. We define the category BF/S_0 whose objects are pairs (G_0, Fil^1), where $G_0 \in \mathsf{BT}/S_0$ and Fil^1 is an *admissible* filtration on $\mathbb{D}(G_0)_S$ and whose morphisms are defined to be pairs (u_0, ξ), where $u_0 \colon G_0 \to H_0$ and ξ is a morphism of filtered objects, i.e. a commutative diagram

$$\begin{array}{ccc} \mathrm{Fil}^1 & \hookrightarrow & \mathbb{D}(G_0)_S \\ \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \mathbb{D}(u_0)_S} \\ \mathrm{Fil}^1 & \hookrightarrow & \mathbb{D}(H_0)_S \end{array}$$

which, on S_0, reduces to

$$\begin{array}{ccc} \underline{\mathcal{V}}(G_0) & \hookrightarrow & \underline{\mathrm{Lie}}(E(G_0)) \\ \downarrow{\scriptstyle \underline{\mathcal{V}}(u_0)_{S_0}} & & \downarrow{\scriptstyle \underline{\mathrm{Lie}}(E(u_0))} \\ \underline{\mathcal{V}}(H_0) & \hookrightarrow & \underline{\mathrm{Lie}}(E(H_0)) \end{array}$$

(or, more precisely, to the associated Zariski sheaves on S_0).

This definition allows to state the following theorem:

Theorem 5.43 ([Mes72, Chapter V, theorem 1.6])**.** *Let $S \hookrightarrow S_0$ as before. The following functor defines an equivalence of categories*

$$\begin{aligned} \mathsf{BT}/S &\longrightarrow \mathsf{BF}/S_0 \\ G &\longmapsto (G_0, \underline{\mathcal{V}}(G) \hookrightarrow \underline{\mathrm{Lie}}(E(G)))\,, \end{aligned}$$

where we denoted by G_0 the restriction of G to S_0 and we recall that $\mathbb{D}(G_0)_S = \mathrm{Lie}(E(G))$.

Remark 5.44.

1. Consider $G_0 \in \mathsf{BT}/S_0$. We define a Zariski sheaf of sets on S, denoted by $\mathscr{L}$, as follows. Let $U \subset S$ be an affine open subscheme of S. We define $\Gamma(U, \mathscr{L})$ to be the set of all linearly compatible prolongations, as in definition 4.42, of

   $$\underline{\mathcal{V}}(G_0)|_{U_0} \longhookrightarrow E(G_0)|_{U_0}$$

   to a vector subgroup $\underline{\mathcal{V}}' \hookrightarrow \mathbb{E}(G_0)_S|_U$. Clearly this defines a sheaf on the affine open subsets of S. Since affine open subschemes form a basis for the topology of S, the definition of $\mathscr{L}$ can be extended to that of a sheaf on S.

2. By construction of $\mathbb{E}(G_0)_S$ we can define a canonical section $\Theta \in \Gamma(S, \mathscr{L})$. By sheaf properties it is enough to define it on sufficiently small affine open subschemes U of S and then check compatibility of all these sections. In particular we assume that U is affine and p is nilpotent on U. Then, we define $\Theta|_U$ to be the equivalence class of $\underline{\mathcal{V}}(G)$, where G is any lift of $G_0|_{U_0}$ to U. In order to check compatibility we pick U_1, U_2, G_1 and G_2 as above and $V \subset U_1 \cap U_2$ affine with p nilpotent on it. Then we require that the restrictions of the two lifts to V, which we still denote by G_1 and G_2, lie in the same equivalence class. Here we can apply proposition 5.18 and obtain the following square

   $$\begin{array}{ccc} \underline{\mathcal{V}}(G_1) & \overset{j}{\longhookrightarrow} & E(G_1) \\ \downarrow{\scriptstyle w} & & \downarrow{\scriptstyle v} \\ \underline{\mathcal{V}}(G_1) & \overset{i}{\longhookrightarrow} & E(G_2), \end{array}$$

   where $i \circ w - v \circ j$ is an exponential. Since $\mathbb{E}(G_0)_S|_V = E(G_2)$, this is exactly the requirement of definition 4.42 to state that the two lifts lie in the same equivalence class.

3. If G is a global lift of G_0, then we have the canonical isomorphism $E(G) \simeq \mathbb{E}(G_0)_S$. Hence $\underline{\mathcal{V}}(G)$ gives an element $\Theta \in \Gamma(S, \mathscr{L})$, i.e. a distinguished vector subgroup in the linear equivalence class of prolongations of $\underline{\mathcal{V}}(G_0)$.

4. Notice that, by proposition 4.50, the datum of $\underline{\mathcal{V}} \hookrightarrow \mathbb{E}(G_0)_S$ which belongs to Θ is equivalent to the datum of an *admissible* filtration $\mathrm{Fil}^1 \hookrightarrow \mathbb{D}(G_0)_S$. In particular the knowledge of the map $\underline{\mathcal{V}}(G) \hookrightarrow \mathbb{E}(G_0)_S$, for G a global lift of G_0, is equivalent to the knowledge of $\underline{\mathcal{V}}(G) \hookrightarrow \mathbb{D}(G_0)_S$. Finally, from the definition of universal extension and of the crystal $\mathbb{E}(G_0)$, we can reconstruct

   $$G \simeq \mathbb{E}(G_0)_S / \underline{\mathcal{V}}(G).$$

   Essentially the above, modulo checking that the quotient defines a Barsotti-Tate group (verification which is carried out in [Mes72, Chapter V, theorem 1.6]), states that, from the datum of an admissible filtration of $\mathbb{D}(G_0)_S$, one can recover the global lift G of G_0. This is indeed the main idea used to construct the quasi-inverse to the functor of theorem 5.43.

6 Classification of p-divisible groups over O_K

In this section we will review the classification of p-divisible groups over O_K of Breuil and Kisin, from [Kis07, Appendix A]. In fact we will introduce some technical lemmas and use them to generalize the classification of Barsotti-Tate groups over a perfect field of characteristic p to that of Barsotti-Tate groups over the ring of integers of a local field.

6.1 Witt vectors

In order to work over a finite extension $K/\mathbb{Q}_p$ it is convenient to have some familiarity with the formalism of Witt vectors, so we will dedicate some space to recall the basic definitions and results. As a typographical convention, in the following sections, we will denote vectors using a boldface character.

Remark 6.1 (Motivation)**.** Consider $K/\mathbb{Q}_p$ a finite and unramified extension. Denote by $k \coloneqq O_K/pO_K$ the residue field of K and by $q \coloneqq |k|$ its cardinality. Then there is a multiplicative map $[\,\cdot\,]\colon k \to O_K$, called the Teichmüller lift, with image $\mu_{q-1}(O_K)$, the $(q-1)$st root of unity of O_K. In particular it is well known that any element $a \in O_K$ can be uniquely written via a Teichmüller expansion

$$a = \sum_{n\in\mathbb{N}} [c_n]p^n,$$

with $c_n \in k$ for all $n \in \mathbb{N}$. The theory of Witt vectors allows the explicit computation of sums and products between Teichmüller expansions, using only algebraic operations on the sequences of elements of k. Clearly its interest doesn't stop there, so we will highlight some other properties of the construction.

Moreover we wish to remark that the following constructions can be carried out for any ring A, though the most interesting results for us will be in case A is a perfect $\mathbb{F}_p$-algebra, i.e. an $\mathbb{F}_p$-algebra on which the map $x \mapsto x^p$ is an automorphism. The results we will introduce in this section revolve around this assumption, but we will highlight when it is not strictly necessary.

Definition 6.2: Witt polynomials.
We define a family of polynomials $\{w_n(\mathbf{x})\}_{n\in\mathbb{N}} \subset \mathbb{Z}[\mathbf{x}] = \mathbb{Z}[x_i]_{i\in\mathbb{N}}$ by

$$\begin{aligned} w_0(\mathbf{x}) &\coloneqq w_0(x_0) \coloneqq x_0, \\ w_1(\mathbf{x}) &\coloneqq w_1(x_0, x_1) \coloneqq x_0^p + px_1, \\ &\vdots \\ w_n(\mathbf{x}) \coloneqq w_n(x_0,\dots,x_n) &\coloneqq \sum_{i=0}^{n} p^i x_i^{p^{n-i}} = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^{n-1}x_{n-1}^p + p^n x_n. \end{aligned}$$

Lemma 6.3 ([SG80, Chapter II, §6, theorem 6])**.** *For every $\phi \in \mathbb{Z}[x,y]$ there exists a unique sequence $\{\varphi_n\}_{n\in\mathbb{N}} \subset \mathbb{Z}[\mathbf{x},\mathbf{y}]$, where $\mathbf{x} = \{x_n\}_{n\in\mathbb{N}}$ and $\mathbf{y} = \{y_n\}_{n\in\mathbb{N}}$, such that, for all $n \in \mathbb{N}$,*

$$w_n(\varphi_0,\dots,\varphi_n) = \phi\left(w_n(x_0,\dots,x_n), w_n(y_0,\dots,y_n)\right).$$

Notation 6.4.
Denote by $\{S_n\}_{n\in\mathbb{N}}$ and $\{P_n\}_{n\in\mathbb{N}}$ the polynomials associated by lemma 6.3 to $\phi(x,y) = x+y$ and $\phi(x,y) = x\cdot y$ respectively. Then we define, for $\mathbf{a},\mathbf{b} \in A^{\mathbb{N}}$ the following composition laws:

$$\begin{aligned} \mathbf{a}+\mathbf{b} &\coloneqq (S_n(\mathbf{a},\mathbf{b}))_{n\in\mathbb{N}} \\ \mathbf{a}\cdot\mathbf{b} &\coloneqq (P_n(\mathbf{a},\mathbf{b}))_{n\in\mathbb{N}}. \end{aligned}$$

Theorem 6.5 ([SG80, Chapter II, §6, theorem 7])**.** *The composition laws on $A^{\mathbb{N}}$ defined in notation 6.4 make it into a commutative unitary ring.*

Definition 6.6: Ring of Witt vectors.
We define the *ring of Witt vectors* with coefficients in A, denoted by $W(A)$, to be the commutative unitary ring $A^{\mathbb{N}}$ endowed with the composition laws defined in notation 6.4.

Remark 6.7. By definition, the map

$$\begin{aligned} W\colon W(A) &\longrightarrow A^{\mathbb{N}} \\ \mathbf{a} &\longmapsto (w_n(\mathbf{a}))_{n\in\mathbb{N}} \end{aligned}$$

is a ring homomorphism. Moreover it is easy to check that it is a monomorphism if p is not a zero divisor and an isomorphism as soon as p is invertible.

Definition 6.8: Frobenius and Verschiebung.
Since A is of characteristic p we can define on $W(A)$ the following two maps

$$\begin{aligned} V\colon W(A) &\longrightarrow W(A) \\ (a_0, a_1, \ldots) &\longmapsto (0, a_0, a_1, \ldots) \end{aligned} \qquad \text{and} \qquad \begin{aligned} F\colon W(A) &\longrightarrow W(A) \\ (a_0, a_1, \ldots) &\longmapsto (a_0^p, a_1^p, \ldots). \end{aligned}$$

It can be easily shown that the first map, called *Verschiebung* (which we recall is the german word for *shift*), is additive, whereas the second, called *Frobenius*, is a ring homomorphism.

Definition 6.9: (Strict) p-ring.
A ring B is called *p-ring* iff it is separated and complete for the topology induced by a decreasing collection of ideals $\{\mathfrak{b}_i\}_{i\geq 1}$ such that $\mathfrak{b}_n\mathfrak{b}_m \subset \mathfrak{b}_{n+m}$ for all $n, m \geq 1$ and $B/\mathfrak{b}_1$ is a perfect $\mathbb{F}_p$-algebra (hence $p \in \mathfrak{b}_1$).

We say that B is a *strict p-ring* iff it is a p-ring and $\mathfrak{b}_i = p^i B$ for all $i \geq 1$ and $p\colon B \to B$ is an injective map.

Remark 6.10. Notice that a strict p-ring is a p-adically separated and complete ring such that B/pB is a perfect $\mathbb{F}_p$-algebra.

Remark 6.11. Since A is of characteristic p we have the identities $VF = FV = p$. Moreover, in case A is perfect, we see that $p^n W(A) = V^n W(A)$, since $p \cdot (a_0, a_1, \ldots) = (0, a_0^p, a_1^p, \ldots)$. This means that the p-adic topology of $W(A)$ corresponds to its natural product topology. This means that $W(A) \simeq \varprojlim_{n\in\mathbb{N}} W(A)/(p^n)$. Then, since $W(A)/(p) \simeq A$, this also means that $W(A)$ is a strict p-ring.

Lemma 6.12 ([BC09, Lemma 4.2.2])**.** *Let B be a p-ring. There is a unique set theoretic section $r_B\colon B/\mathfrak{b}_1 \to B$ to the reduction map such that $r_B(x^p) = r_B(x)^p$ for all $x \in B/\mathfrak{b}_1$. Moreover r_B is multiplicative and $r_B(1) = 1$.*

Definition 6.13: Teichmüller lift.
For a ring A, we can define the following section to the reduction map

$$\begin{aligned} [\,\cdot\,]\colon A &\longrightarrow W(A) \\ a &\longmapsto [a] \coloneqq (a, 0, 0, \ldots)\,, \end{aligned}$$

where $[a]$ is called the *Teichmüller lift* of a.

Remark 6.14.

1. Reducing to an appropriate universal case it is easy to prove that

$$(x_0, x_1, x_2, \ldots) \cdot (y_0, 0, 0 \ldots) = (x_0 y_0, x_1^p y_0, x_2^{p^2} y_0, \ldots)$$

in $W(A)$. Hence $[\,\cdot\,]$ is a multiplicative map and satisfies conditions of lemma 6.12.

2. If B is a strict p-ring endowed with the p-adic topology, each $b \in B$ can be written as

$$b = \sum_{n \in \mathbb{N}} r_B(b_n) p^n$$

with $b_n \in B/\mathfrak{b}_1 = B/pB$. Let's recall that B is complete and separated with respect to the p-adic topology. As a consequence the above series converges and the expansion is unique.

3. Let A be a perfect $\mathbb{F}_p$-algebra, then any element $\mathbf{x} \in W(A)$ can be uniquely written as

$$\mathbf{x} = \sum_{n \in \mathbb{N}} [c_n] p^n,$$

where $c_n \in A$. We will refer to this expansion as the *Teichmüller expansion* in the future. Moreover, given $\mathbf{x} = (a_n)_{n \in \mathbb{N}}$, one can also write it as

$$\mathbf{x} = \sum_{n \in \mathbb{N}} V^n([a_n]).$$

Then, since A is perfect, F is invertible on $W(A)$ too and we obtain $V^n = p^n F^{-n}$. Then we can rewrite the above sum as

$$\mathbf{x} = \sum_{n \in \mathbb{N}} p^n F^{-n}([a_n]) = \sum_{n \in \mathbb{N}} [a_n^{p^{-n}}] p^n.$$

All combined we can explicitly compute the coefficients of the Teichmüller expansion of $\mathbf{x} = (a_n)_{n \in \mathbb{N}}$, via $[c_n] = [a_n^{p^{-n}}]$.

Proposition 6.15 ([BC09, Proposition 4.2.3])**.** *If A is a perfect $\mathbb{F}_p$-algebra and B is a p-ring, then the natural "reduction" map*

$$\mathrm{Hom}\,(W(A), B) \xrightarrow{\sim} \mathrm{Hom}\,(A, B/\mathfrak{b}_1)$$

is an isomorphism. More generally, for any strict p-ring $\mathcal{B}$, the natural map

$$\mathrm{Hom}\,(\mathcal{B}, B) \xrightarrow{\sim} \mathrm{Hom}\,(\mathcal{B}/(p), B/\mathfrak{b}_1)$$

is bijective for every p-ring B.

Remark 6.16.

1. Let's notice that, by the previous comments, we have $W(A)/(p) = A$, which allows the definition of the first map above. Moreover the above shows that $\mathcal{B}$ and $W(\mathcal{B}/p\mathcal{B})$ satisfy the same universal property in the category of p-rings. As a consequence all strict p-rings are isomorphic to $W(A)$ for a perfect $\mathbb{F}_p$-algebra A.

2. The inverse to the second bijection has the following form. Let $h \in \mathrm{Hom}\,(\mathcal{B}/(p), B/\mathfrak{b}_1)$ and write an element $x \in \mathcal{B}$ using its expansion via $r_{\mathcal{B}}$. The induced map on $\mathcal{B}$ acts by

$$x = \sum_{n\in\mathbb{N}} r_{\mathcal{B}}(x_n)p^n \longmapsto \sum_{n\in\mathbb{N}} r_B(h(x_n))p^n.$$

3. Using the above proposition we can recover the theory of maximal unramified extensions for finite extensions $K/\mathbb{Q}_p$. Fix K and let $k \coloneqq O_k/(\pi_K)$ be its residue field. In fact O_K is a p-ring, when considered with the filtration given by $\left\{\pi_K^i\right\}_{i\geq 1}$. Then there is a unique map of rings $\alpha\colon W(k) \to O_K$ lifting the isomorphism $W(k)/(p) \simeq k \simeq O_K/(\pi_K)$. Since p has image in the maximal ideal of O_K, the map α is local and injective. This means that $O_K/(p)$ is a $W(k)/(p) = k$ vector space with basis $(1, \pi_K, \dots, \pi_K^e)$, where $e = e(K/\mathbb{Q}_p)$ is the absolute ramification index of K. Since O_K is complete and separated with respect to the p-adic topology, by successive approximations, we see that the above is a $W(k)$-basis of O_K, which is then a free $W(k)$-module of rank e. As a consequence also $K = O_K[1/p]$ is a $W(k)[1/p] =: K_0$ vector space of dimension e. Then K/K_0 is a field extension of degree e, which is totally ramified since the two fields have isomorphic residue fields. Then we see that the Witt vector construction allows one to construct K_0 the *maximal unramified subextension* of any finite extension of $\mathbb{Q}_p$.

4. We can finally notice that the isomorphism $W(k) \simeq O_{K_0}$ preserves Teichmüller lifts. Hence, recalling the motivational remark at the beginning of the section, we can use the definition of sum and product via Witt polynomials on $W(k)$ to compute the operations on Teichmüller expansions on O_{K_0}.

6.2 Classification of p-divisible groups over O_K

This section will follow [Kis07, Appendix A]. Fix k a perfect field of characteristic p and denote by $W \coloneqq W(k)$ its ring of Witt vectors and by $K_0 \coloneqq W[1/p]$ its field of fractions. Finally fix K/K_0 a finite totally ramified extension. We denote by π a fixed uniformizer of K and by $E(u) \in W[u]$ its (Eisenstein) minimal polynomial.

Remark 6.17. Let T be a scheme and $G \in \mathsf{BT}/T$. The formation of $\mathbb{D}(G)$ and $\mathbb{D}^*(G)$ is compatible with all base changes. In particular, if $p = 0$ on T, we can pull G back by the Frobenius φ on T. Then the relative Frobenius on G gives a map $G \to \varphi^*(G)$ hence a map of crystals

$$\varphi^*(\mathbb{D}^*(G)) \xrightarrow{\sim} \mathbb{D}^*(\varphi^*(G)) \longrightarrow \mathbb{D}^*(G),$$

where the first is an isomorphism since, as seen above, the formation of $\mathbb{D}^*(G)$ commutes with base change.

Notation 6.18.
In the following we will mainly be interested in the evaluation of crystals on objects. In particular, given schemes $T_0, G_0 \in \mathsf{BT}/T_0$ and $T_0 \hookrightarrow T \in \mathsf{Crys}(T_0)$, we will be interested in the evaluation $\mathbb{D}^*(G_0)_T(T) = \mathbb{D}^*(G_0)_{T_0\hookrightarrow T}(T)$, where $\mathbb{D}^*(G_0)_T$ is defined in notation 5.40 and its evaluation in remark 4.58. Hence we introduce the shorter $\mathbb{D}^*(G_0)(T) \coloneqq \mathbb{D}^*(G_0)_T(T)$. Moreover, if $T = \mathrm{Spec}(A)$ is affine, we introduce the notation $\mathbb{D}^*(G)(A)$ for $\mathbb{D}^*(G)(T)$. Finally we can notice that, fixed G, the functor $\mathbb{D}^*(G)$, induced by a sheaf on $\mathsf{Crys}(T_0)$, is contravariant when evaluated on schemes, but covariant on rings.

Remark 6.19. Suppose that T_0 is a scheme over W and that $p = 0$ on T_0. Consider $G_0 \in \mathsf{BT}/T_0$ and $T_0 \hookrightarrow T \in \mathsf{Crys}(T_0/W)$ an object on which p is locally nilpotent, and G a lift of G_0 to T.

By construction of $\mathbb{D}^*$ we have an isomorphism

$$\mathbb{D}^*(G_0)(T) \xrightarrow{\sim} \mathbb{D}^*(G)(T).$$

Moreover, recalling proposition 5.23, the O_T-module $\mathbb{D}^*(G)(T)$ sits in an exact sequence

$$0 \longrightarrow (\mathrm{Lie}(G))^\vee \longrightarrow \mathbb{D}^*(G)(T) \longrightarrow \mathrm{Lie}(G^D) \longrightarrow 0.$$

We recall that elements of $\mathsf{Crys}(X/S)$ are defined by locally nilpotent sheaves of ideals. In what follows, though, we want to evaluate crystals on surjections of p-adically complete rings, whose kernels are endowed with divided powers (not necessarily nilpotent).

Definition 6.20.
Let $A \twoheadrightarrow A_0$ be a surjective homomorphism of p-adically complete and separated $\mathbb{Z}_p$-algebras whose kernel is equipped with divided powers, compatible with those on $p\mathbb{Z}_p$. Take $G \in \mathsf{BT}/A_0$. Denote by G_n the restriction of G to A_0/p^nA_0. Then we define

$$\mathbb{D}^*(G)(A) \coloneqq \varprojlim_{n\in\mathbb{N}} \mathbb{D}^*(G_1)(A/p^nA).$$

Remark 6.21. Notice that, in the above definition, $A/p^nA \twoheadrightarrow A_0/p^nA_0$ has kernel equipped with divided powers. In fact it is the projection of the kernel of $A \twoheadrightarrow A_0/p^nA_0$, over p^nA. This ideal has divided powers since pA and $\ker(A \to A_0)$ have compatible divided powers. Analogously we see that the kernel of $A/p^nA \twoheadrightarrow A_0/p^mA_0$ has divided powers for all $m \leq n$. Now, combining this remark with remark 6.19, we see that the above definition could have easily been swapped out with

$$\mathbb{D}^*(G)(A) \coloneqq \varprojlim_{n\geq m} \mathbb{D}^*(G_m)(A/p^nA)$$

by cofinality of the family $n \geq m$ in $\mathbb{N}$. Moreover we can notice that, in case p is not nilpotent on A_0, the theory of Messing (see definition 5.33), doesn't suffice to define the crystal $\mathbb{D}^*(G)$. Though, for our purpose, it is enough to define the valuation $\mathbb{D}^*(G)(A)$, for which it suffices to have the crystal associated to G_1. In particular we can notice that the crystal can be constructed for $G \in \mathsf{BT}/A_0$ if A_0 is p-adically complete, as above.

Remark 6.22. We will now introduce some technical lemmas, which will play a crucial role in the proof of the main result of this section, proposition 6.37. In fact these lemmas allow, in combination with theorem 5.43, to lift not only a Barsotti-Tate group along a thickening with divided powers, but also some additional structure, i.e. a Frobenius morphism and a filtration, on the evaluation of $\mathbb{D}^*$. Iin fact, this extra semi-linear algebra structure is going to be of vital importance in the proof.

Lemma 6.23 ([Kis07, Lemma A.2])**.** *Let $A \twoheadrightarrow A_0$ be a surjection of p-adically complete and separated local $\mathbb{Z}_p$-algebras with residue field k and kernel $\mathrm{Fil}^1 A$ equipped with divided powers. Suppose moreover that*

1. *A is p-torsion-free and it is equipped with an endomorphism $\varphi\colon A \to A$ lifting the Frobenius endomorphism on A/pA;*
2. *the following map, induced on the pullback, is surjective*

$$\mathrm{id}_A \otimes \varphi/p\colon \varphi^*(\mathrm{Fil}^1 A) \twoheadrightarrow A.$$

If $G \in \mathsf{BT}/A_0$ we write $\operatorname{Fil}^1 \mathbb{D}^*(G)(A) \subset \mathbb{D}^*(G)(A)$ for the preimage of $(\operatorname{Lie}(G))^\vee$ inside $\mathbb{D}^*(G)(A_0)$. Then the restriction of $\varphi\colon \mathbb{D}^*(G)(A) \to \mathbb{D}^*(G)(A)$ to $\operatorname{Fil}^1 \mathbb{D}^*(G)(A)$ is divisible by p and the following induced map is a surjection

$$1 \otimes \varphi/p\colon \varphi^* \operatorname{Fil}^1 \mathbb{D}^*(G)(A) \longrightarrow\!\!\!\!\!\rightarrow \mathbb{D}^*(G)(A).$$

Remark 6.24. Here are the main ingredients of the proof.

1. Given an ideal $I \triangleleft A$ with divided powers, then $\varphi(I) \subset pA$. In fact
$$\varphi(x) = x^p = \gamma_p(x) \cdot p! \in pA.$$
2. Let $\widetilde{G}$ be a lift of G to A, then we have
$$\operatorname{Fil}^1 \mathbb{D}^*(\widetilde{G})(A) = (\operatorname{Lie} \widetilde{G})^\vee + \operatorname{Fil}^1 A \cdot \mathbb{D}^*(\widetilde{G})(A).$$
3. Let $H \in \mathsf{BT}/\operatorname{Spec}(W(k))$. Denote by H_0 the restriction of H to k and by V the Verschiebung morphism. Then $W(k) \twoheadrightarrow k$ satisfies the hypothesis of our lemma, and the kernel $\operatorname{Fil}^1(W(k)) = (p)$ is equipped with divided powers by item 4 of example 4.4. Then, using the theory of Dieudonné modules, one can see that
$$(\operatorname{Lie} H)^\vee + p\mathbb{D}^*(H)(W(k)) = V\mathbb{D}^*(H)(W(k)),$$
i.e. that $V\mathbb{D}^*(H)(W(k)) = \operatorname{Fil}^1 \mathbb{D}^*(H)(W(k))$.

Definition 6.25: Special ring.
A *special ring* A is a p-adically complete, separated, p-torsion-free, local $\mathbb{Z}_p$-algebra equipped with an endomorphism φ lifting the Frobenius on A/pA. Moreover we call *map of special rings* a morphism of $\mathbb{Z}_p$-algebras between special rings which is also compatible with φ.

Definition 6.26.
Let A be a special ring. We define the category C_A whose objects are finite, free A-modules M equipped with a semilinear Frobenius map $\varphi\colon M \to M$ and an A-submodule $M_1 \subset M$ such that $\varphi(M_1) \subset pM$ and such that the map
$$\mathrm{id}_A \otimes \varphi/p\colon \varphi^*(M_1) \longrightarrow\!\!\!\!\!\rightarrow M$$
is surjective. Its morphisms are morphisms of A-modules compatible with the Frobenius and submodules.

Remark 6.27. Notice that lemma 6.23 allows to endow, for $G \in \mathsf{BT}/A_0$ and $A \twoheadrightarrow A_0$ as in the hypothesis, the module $\mathbb{D}^*(G)(A)$ with the structure of an object in C_A.

Definition 6.28.
Consider a map of special rings $A \to B$ and $M \in \mathsf{C}_A$. Then $M \otimes_A B \in \mathsf{C}_B$, when equipped with the induced Frobenius and setting $(M \otimes_A B)_1$ to be the image of $M_1 \otimes_A B$ in $M \otimes_A B$.

Lemma 6.29 ([Kis07, Lemma A.4])**.** *Let $h\colon A \twoheadrightarrow B$ be a surjection of special rings with kernel J. Suppose that, for all $i \geq 1$, $\varphi^i(J) \subset p^{i+j_i} J$, where $\{j_i\}_{i\geq 1}$ is a sequence of integers such that $\lim_{i\to\infty} j_i = \infty$. Consider $M, M' \in \mathsf{C}_A$ and*
$$\theta_B\colon M \otimes_A B \xrightarrow{\sim} M' \otimes_A B$$
an isomorphism in C_B. Then there exists a unique isomorphism of A-modules $\theta_A\colon M \to M'$ lifting θ_B and compatible with φ.

Remark 6.30. As before we will only present the main idea behind the proof. In this case, starting from any lift $\theta_0 \colon M \to M'$ of θ_B, we deform iteratively the map

$$\varphi^*(M_1) \xrightarrow{\varphi^*(\theta_i|_{M_1})} \varphi^*(M_1') \xrightarrow{1\otimes\varphi/p} M'$$

obtaining a succession of maps θ_i whose successive difference has image lying in $p^{j_i}M'$. The fact that $j_i \to \infty$ allows to obtain a well defined limit.

In order to apply the above results to the proof of the main theorem of the section we still need some remarks and definitions. Let's start by defining the ring which allows to overcome the problem of definition of divided powers on the maximal ideal of O_K for a ramified extension, see item 4 of example 4.4.

Definition 6.31.
Consider W as a divided power ring, endowing the maximal ideal (p) with the divided power structure defined in item 4 of example 4.4. Consider $W[u]$ as a W-algebra, and take $\mathcal{D}_{W[u]}(E(u))$ its divided powers envelope, constructed in theorem 4.12. Let's notice that, as outlined in remark 4.13, we can take $\overline{J} \lhd \mathcal{D}_{W[u]}(E(u))$ as the ideal generated by $E(u), p$ and their divided powers, also called the P.D. ideal generated by $E(u)$ and p. We denote by S the p-adic completion of $\mathcal{D}_{W[u]}(E(u))$ and by $\mathrm{Fil}^1 S \subset S$ the closure of the ideal generated by $E(u)$ and its divided powers.

Remark 6.32. The ring S is equipped with an endomorphism φ lifting that on S/pS. It is, in fact, induced by the Frobenius on $W[u]$ which acts naturally on W and by $u \mapsto u^p$. In order to lift it we use the universal property of the divided powers envelope. In particular we need to notice that this map sends $(E(u))$ into $\overline{J}$ which, as stated before,contains p. But this is clear, since F sends $pW[u]$ to $pW[u]$ and, since the P.D. ideal generated by $E(u)$ in $\mathcal{D}_{W[u]}(E(u))$ contains divided powers, it sends $E(u)$ in the P.D. ideal generated by $E(u)$ and p. Then, by universal property of divided powers envelope, we obtain the desired lift φ as the unique map making the following diagram commute

$$\begin{array}{ccc} & & \mathcal{D}_{W[u]}(E(u)) \\ & \nearrow & \vdots\ \varphi \\ (W[u],(E(u),p)) & \xrightarrow{\quad F \quad} & (W[u],(E(u),p)) \subset \mathcal{D}_{W[u]}(E(u)). \end{array}$$

Then this extends to S by continuity with respect to p-adic topology and it lifts the Frobenius defined on $S/pS = \mathcal{D}_{W[u]}(E(u))/(p)$.

Notation 6.33.
Thanks to lemma 4.10, the ideal $\mathrm{Fil}^1(S)$ is equipped with divided powers. Then, as seen in remark 6.24, we have $\varphi(\mathrm{Fil}^1 S) \subset pS$, which allows us to define $\varphi_1 \coloneqq \varphi/p \colon \mathrm{Fil}^1 S \to S$.

Remark 6.34. We will apply lemma 6.29 in the situation where J is equipped with divided power structure and there exists a finite set of elements $x_1, \ldots, x_n \in J$ such that J, in the p-adic topology, is topologically generated by the x_i and their divided powers and such that $\varphi(x_i) = x_i^p$ for all i. Then the integers j_i of lemma 6.29 can be taken to be $\nu_p((p-1)!) - 1$. Since φ is a continuous endomorphism in the p-adic topology, it suffices to prove the statement for elements of the type

$$x \coloneqq x^{[m_1]} \cdot \cdots \cdot x_n^{[m_n]},$$

for arbitrary $m_1, \dots, m_n \in \mathbb{N}$. Here we can notice that $\varphi(x_i^{[m_i]}) = (x_i^p)^{[m_i]}$ for all i. Hence

$$\varphi^i(x) = \prod_{k=1}^{n} \varphi^i\Big(\big(x_k\big)^{[m_k]}\Big) = \prod_{k=1}^{n} \big(\varphi^i(x_k)\big)^{[m_k]}.$$

Let's now fix a k with $m_k > 0$. Since J is equipped with divided powers we have

$$\varphi^i(x_k) = x_k^{p^i} = x_k \cdot \gamma_{p^i-1}(x_k) \cdot (p^i - 1)!.$$

Now, from condition 2 of definition 4.1, we obtain

$$\big(\varphi^i(x_k)\big)^{[m_k]} = \Big(x_k^{[p^i-1]}\Big)^{m_k} \big((p^i-1)!\big)^{m_k} \cdot x_k^{[m_k]}.$$

Since x_k and all its divided powers are in J, we see that $(\varphi^i(x_k))^{[m_k]} \in p^{\nu_p((p^i-1)!)}J$. As a consequence this claim holds for any $x = x_1^{[m_1]} \cdot \dots \cdot x_k^{[m_k]}$, hence for all $x \in J$.

Definition 6.35.
We denote by $\mathsf{BT}^{\varphi}_{/S}$ the category whose objects are finite free S-modules M equipped with an S-submodule $\mathrm{Fil}^1 M$ and a φ-semilinear map $\varphi_1 \colon \mathrm{Fil}^1 M \to M$ such that

1. $\mathrm{Fil}^1 S \cdot M \subset \mathrm{Fil}^1 M$ and the quotient $M/\mathrm{Fil}^1 M$ is a free O_K-module;
2. the map $\mathrm{id}_S \otimes \varphi_1 \colon \varphi^*\left(\mathrm{Fil}^1 M\right) \to M$ is surjective.

Remark 6.36. Notice that any $M \in \mathsf{BT}^{\varphi}_{/S}$ is equipped with a φ-semilinear map $\varphi \colon M \to M$ defined by

$$\varphi(x) \coloneqq \varphi_1\left(E(u)\right)^{-1} \varphi_1(E(u)x).$$

In fact $\varphi_1(E(u))$ is invertible in S. To show this we recall that, by definition, φ_1 is φ-semilinear on $W[u]$, and that $W[u]$ embeds in S. More explicitly we need to show that the element

$$\varphi_1(E(u)) = \underbrace{\frac{u^{ep}}{p} + \varphi_1(a_{e-1})u^{(e-1)p} + \dots + \varphi_1(a_1)u^p}_{x} + \varphi_1(a_0)$$

is invertible in S. To do so it suffices to show that $\varphi_1(a_1) \in S^\times$ and that x is nilpotent modulo p. In fact, in such case, since S is complete with respect to the p-adic topology, we can compute an inverse of $\varphi_1(E(u))$ in S via successive approximations (essentially in the same way one proves this for power series). Let's start with x. We want to prove that a certain power x^n of x is in $\mathrm{Fil}^1 S$, which has divided powers, from which we would deduce $x^{np} = p!\gamma_p(x^n) \in pS$. Let's recall that we defined $\mathrm{Fil}^1 S$ as the topological closure of the P.D. ideal $(E(u), p) \triangleleft \mathcal{D}_{W[u]}(E(u))$, i.e. the ideal topologically generated by $E(u), p$ and their divided powers. Notice, moreover, that $u^e \in \mathrm{Fil}^1 S$, since $E(u)$ is Eisenstein. Then we can also notice that each term of x^e is either divided by a power of u^{ep}/p or a power of u^e. But $u^{ep}/p = (p!/p)\gamma_p(u^e) = (p-1)!\gamma_p(u^e)$. Then this means that

$$x^e \in (\gamma_p(u^e), u^e) \subset \mathrm{Fil}^1 S$$

since $\mathrm{Fil}^1 S$ contains u^e and its divided powers. With regards to $\varphi_1(a_0)$ we need to show that it is invertible modulo p. But this is true, since $\varphi(p) = p$ on W, hence on S, and $a_0 = p \cdot \alpha$, for $\alpha \in W^\times$. In fact this grants that $\varphi_1(a_0) = \varphi(p\alpha)/p = \varphi(\alpha)$. Since $\alpha \in W$ and φ lifts the Frobenius on W, which itself lifts the Frobenius on k, we see that the image of α is invertible in $W/pW \simeq k$, and $\varphi(\alpha)$ too, which allows us to conclude.

Proposition 6.37 ([Kis07, Proposition A.6])**.** *There is an exact contravariant functor*

$$\begin{aligned} M\colon \mathsf{BT}/O_K &\longrightarrow \mathsf{BT}^{\varphi}_{/S} \\ G &\longmapsto \mathbb{D}^*(G)(S) =: M(G). \end{aligned}$$

If $p > 2$ this functor is an anti-equivalence, whereas if $p = 2$ it induces an anti-equivalence of the corresponding isogeny categories.

Proof. We start by showing that this functor actually takes values in $\mathsf{BT}^{\varphi}_{/S}$. We need to show that $M(G) = \mathbb{D}^*(G)(S)$ has a structure of object in $\mathsf{BT}^{\varphi}_{/S}$, for which it is enough to check that $S \twoheadrightarrow O_K$ satisfies the hypothesis of lemma 6.23. Notice that the map $S \to O_K$ is induced by $W[u] \twoheadrightarrow O_K$ which is a surjection, as remarked before. Then, by construction, we see that $S \twoheadrightarrow O_K$ is surjective too. It is also clear that both S and O_K are p-adically complete, separated, local $\mathbb{Z}_p$-algebras. Moreover, by definition, $\ker(W[u] \to O_K) = (E(u))$. Then, by construction of S and completeness of O_K, we see that $\mathrm{Fil}^1 S$, the kernel of $S \twoheadrightarrow O_K$, as seen in notation 6.33, is the P.D. ideal topologically generated by $E(u)$, hence it is equipped with divided powers. Moreover, by construction, it is clear that S is p-torsion-free and, thanks to remark 6.32, that it is equipped with an endomorphism lifting the Frobenius on S/pS. Finally we are left to prove that the map

$$\mathrm{id}_S \otimes \varphi/p\colon \varphi^*(\mathrm{Fil}^1 S) \longrightarrow\!\!\!\!\!\rightarrow S$$

is surjective. Here, thanks to the argument in remark 6.36, we easily conclude. In fact we see that, for all $s \in S$,

$$s \cdot (\varphi_1(E(u)))^{-1} \otimes E(u) \longmapsto s.$$

The construction of the quasi-inverse $M \mapsto G(M)$ is definitely more tricky and we will concentrate only on the case $p > 2$, leaving the rest of the proof to [Kis07]. It will require the use of classical Dieudonné theory to construct a Barsotti-Tate group over k associated to a module $M \in \mathsf{BT}^{\varphi}_{/S}$ and then to iteratively lift it from $k = O_K/\pi O_K$ to O_K. This difficulty is due to the fact that, in general, the maximal ideal of O_K, i.e. the kernel of $O_K \twoheadrightarrow k$, does not admit divided powers. Then the only hope to lift the classical construction is to proceed iteratively, reducing the above projection to a sequence of smaller projections, whose kernels all have nilpotent divided power structures. And for this process the choice of the right ring, i.e. S, will be crucial. In particular those lifting steps will make use of Grothendieck-Messing deformation theory to lift the Barsotti-Tate group, and of the previous technical lemmas to lift the structure of module in $\mathsf{BT}^{\varphi}_{/S}$ associated to the p-divisible group via the crystal $\mathbb{D}^*(G)$.

Let's now start the proof by introducing the necessary notation: let i vary in $1, \dots, e$ and set $R_i \coloneqq W[u]/(u^i)$. Clearly R_i is equipped with a Frobenius endomorphism φ given by the usual one on W and $u \mapsto u^p$ on the indeterminate. These are all S-algebras. In fact, by universal property of divided powers envelope we have a ring homomorphism $S \to R_i$ given by the unique map associated to

$$\begin{aligned} W[u] &\longrightarrow R_i \\ u &\longmapsto u \\ u^{ej}/j! &\longmapsto 0. \end{aligned}$$

This map is compatible with φ and, by uniqueness, also the induced map on S is. Moreover also $O_K/(\pi^i)$ is an R_i-algebra by $u \mapsto \pi$, seeing $W = O_{K_0} \subset O_K$. As one can check

writing the elements of O_K in Teichmüller expansion, the map $R_i \twoheadrightarrow O_K/(\pi^i)$ is a surjection with kernel pR_i, which is equipped with divided powers by lemma 4.8. Then, given a p-divisible group $G_i \in \mathsf{BT}/(O_K/\pi^i O_K)$, we can consider its evaluation $\mathbb{D}^*(G_i)(R_i)$ by definition 6.20. Following the notation of lemma 6.23 we denote by $\mathrm{Fil}^1\,\mathbb{D}^*(G_i)(R_i)$ the preimage of $(\mathrm{Lie}\,G_i)^\vee \subset \mathbb{D}^*(G_i)(O_K/\pi^i O_K)$ in $\mathbb{D}^*(G_i)(R_i)$.

We define the module $M_i \coloneqq M \otimes_S R_i$, which is a restriction of scalars of our original one and it is also equipped with the diagonal action of φ. We set $\mathrm{Fil}^1 M_i \subset M_i$ to be the image of $\mathrm{Fil}^1 M$ in M_i, which is a submodule by surjectivity of $S \twoheadrightarrow R_i$. Notice that the above corresponds to defining $\mathrm{Fil}^1 M_i \coloneqq \mathrm{Fil}^1 M \otimes_S R_i$. Then, by right exactness of tensor product,

$$\mathrm{id}_S \otimes \varphi_1 \colon \varphi^*(\mathrm{Fil}^1 M) \longrightarrow M$$

induces a surjective map $\varphi^*(\mathrm{Fil}^1 M_i) \twoheadrightarrow M_i$ for all i. In other words we have just seen that $M_i \in \mathsf{C}_{R_i}$ for all $i \in [1, e]$.

With all this in mind we can start with the lifting process.

1. At first we need to construct, using classical Dieudonné theory, a Barsotti-Tate group G_1 on $k = O_K/\pi O_k$ from M_1. Let's denote by $F \colon M_1 \to M_1$ the map induced by $\varphi \colon M \to M$. Then we see that both sides of the surjective map $\varphi^*(\mathrm{Fil}^1 M_1) \to M_1$ are free W-modules of the same (finite) rank, as can be seen by base changing to k, which means that the map is an isomorphism. Now we consider the composition

$$M_1 \xrightarrow{\sim} \varphi^*(\mathrm{Fil}^1 M) \longrightarrow \varphi^*(M_1) \xrightarrow{\sim} M_1,$$

   where the first arrow is just the inverse of the above isomorphism, the second map is induced by the inclusion $\mathrm{Fil}^1 M \hookrightarrow M$ and the third one is given by $a \otimes m \mapsto \varphi^{-1}(a)m$. This composition gives a φ^{-1}-semilinear map $V \colon M_1 \to M_1$ such that $FV = VF = p$. Let's denote by G_1 the Barsotti-Tate group on k associated to this Dieudonné module, see e.g. [BC09, Proposition 7.2.6] for a reference. In particular the isomorphism

$$\mathbb{D}^*(G_1)(W) \xrightarrow{\sim} M_1$$

   is compatible with Frobenius. Moreover, thanks to remark 6.24, $\mathrm{Fil}^1\,\mathbb{D}^*(G_1)(W)$ can be identified with $V\mathbb{D}^*(G_1)(W)$, which grants that the isomorphism is also compatible with filtrations.

2. We now iteratively lift this construction. Assume, for $i \in [2, e]$, that we have an isomorphism

$$\mathbb{D}^*(G_{i-1})(R_{i-1}) \xrightarrow{\sim} M_{i-1} \tag{6.1}$$

   compatible with Frobenius and filtrations, i.e. an isomorphism in $\mathsf{C}_{R_{i-1}}$. We can notice that the kernel of $R_i \twoheadrightarrow O_K/(\pi^{i-1})$ is (p, u^{i-1}) which is still equipped with divided powers. In fact, following item 3 of example 4.4, we simply put $\gamma_1(u^{i-1}) = u^{i-1}$ and $\gamma_n(u^{i-1}) = 0$ for all $n \geq 2$, since $u^{2(i-1)} = 0$ in R_i. Then we are done invoking proposition 4.9. Again, this means that we can compute $\mathbb{D}^*(G_{i-1})(R_i)$. We have already seen that $M_i \in \mathsf{C}_{R_i}$. Moreover lemma 6.23, applied to the surjection $R_i \twoheadrightarrow O_k/(\pi^{i-1})$, implies that also $\mathbb{D}^*(G_{i-1})(R_i)$ is in C_{R_i}. Recalling remark 6.34 and that the isomorphism in equation (6.1) is a morphism in $\mathsf{C}_{R_{i-1}}$, we can apply lemma 6.29 to the surjection $R_i \twoheadrightarrow R_{i-1}$ and obtain a lift to an isomorphism

$$\mathbb{D}^*(G_{i-1})(R_i) \xrightarrow{\sim} M_i$$

compatible with Frobenius. Finally, since the kernel of $R_i \twoheadrightarrow R_{i-1}$ is nilpotent, we can invoke theorem 5.43 and obtain that there is a unique $G_i \in \mathsf{BT}/(O_K/\pi^i O_K)$ lifting G_{i-1} and such that $(\operatorname{Lie} G_i)^\vee \subset \mathbb{D}^*(G_{i-1})(O_K/\pi^i O_K)$ is equal to the image of $\operatorname{Fil}^i M_i$ under the composite

$$\operatorname{Fil}^1 M_i \subset M_i \xrightarrow{\sim} \mathbb{D}^*(G_{i-1})(R_i) \longrightarrow \mathbb{D}^*(G_{i-1})(O_K/\pi^i O_K).$$

Then, by construction, we obtain that the isomorphism $\mathbb{D}^*(G_i)(R_i) \simeq M_i$, where we recall the implicit use of remark 6.19, is compatible also with filtrations, i.e. is in C_{R_i}. This concludes the first step of induction.

3. Finally we need to reiterate the above argument to the surjection $S \twoheadrightarrow R_e$. At first we need to show that the kernel of this map is equipped with divided powers. Since it is the p-adic completion of the kernel of the map $\mathcal{D}_{W[u]}(E(u)) \twoheadrightarrow R_e$, induced by $W[u] \twoheadrightarrow R_e$, we can study this and then apply lemma 4.10. But this kernel is the P.D. ideal topologically generated by u^e and p hence it is equipped with divided powers, since $(E(u)) \lhd \mathcal{D}_{W[u]}(E(u))$ has a P.D. structure compatible with that of (p) (and it is an Eisenstein polynomial). Then we can apply lemma 6.23 and obtain that the evaluation $\mathbb{D}^*(G_e)(S)$ is in C_S. As before, thanks to lemma 6.29 we lift the isomorphism

$$M_e \xrightarrow{\sim} \mathbb{D}^*(G_e)(R_e)$$

in C_{R_e} to an isomorphism $M \simeq \mathbb{D}^*(G_e)(S)$ compatible with φ. Here notice that we need remark 6.34 to invoke lemma 6.29, and we can argue as in remark 6.34 since the kernel of the projection $S \twoheadrightarrow R_e$ is the P.D. ideal topologically generated by u^e and p, on which the Frobenius acts as the pth power map. Now we need to lift the group G_e to O_K for which we assume that $p > 2$. In order to do so we notice that, for all i, $O_K/(p^{i-1}) \twoheadrightarrow O_K/(p^i)$ and $S \twoheadrightarrow O_K/(p^i)$ have kernels equipped with divided powers, the first being nilpotent, the second existing by compatibility of divided powers on u^e with those on p. Moreover, since O_K is p-adically complete, thanks to [Jon95, Lemma 2.4.4] or to lemma 3.58, we see that the datum of a Barsotti-Tate group on O_K is equivalent to the datum of a compatible sequence of Barsotti-Tate groups G^i on $O_K/(p^i)$. Here compatible means that the restriction of G^i to $O_K/(p^{i-1})$ is isomorphic to G^{i-1}. Then, invoking again theorem 5.43, we can construct this sequence by induction, taking at each time the group G^i determined by $(\operatorname{Lie} G^i)^\vee \subset \mathbb{D}^*(G_e)(O_K/p^i O_K)$, given by the image of $\operatorname{Fil}^1 M$ under

$$M \xrightarrow{\sim} \mathbb{D}^*(G_e)(S) \longrightarrow \mathbb{D}^*(G_e)(O_K/p^i O_K).$$

By functoriality of $\mathbb{D}^*(G_e)$ this gives rise to a compatible family G^i, which in turn, by [Jon95, Lemma 2.4.4], defines $G(M) \in \mathsf{BT}/O_K$ such that $(\operatorname{Lie} G)^\vee \subset \mathbb{D}^*(G_e)(O_K)$ is equal to the image of $\operatorname{Fil}^i M$ under

$$M \xrightarrow{\sim} \mathbb{D}^*(G_e)(S) \longrightarrow \mathbb{D}^*(G_e)(O_K).$$

At last we are only left to prove that the above morphisms are quasi inverses to each other. It is clear, by construction, that $M \simeq M(G(M))$. For the other direction we see, by induction on $i = 1, \dots, e$, that uniqueness in lemma 4.10 grants that, given any $G \in \mathsf{BT}/O_K$, the group $G_i(M(G))$ is isomorphic to the base change of G to $O_K/(\pi^i)$. Analogously, for $i \in \mathbb{N}$, uniqueness in lemma 4.10 grants that $G^i(M(G))$ is isomorphic to the base change of G to $O_K/(p^i)$. Then, invoking again [Jon95, Lemma 2.4.4], we can conclude that $G(M(G)) \simeq G$ and the two functors are quasi-inverses to each other. ∎

Now that we have proved this theorem let's compute some simple examples. These will also play an important role in what follows.

Example 6.38. We want to compute $M(G) \coloneqq \mathbb{D}^*(G)(S)$ for $G = \mathbb{G}_m(p)$ and its dual $G^D = \underline{\mathbb{Q}_p/\mathbb{Z}_p}$, both seen in BT/O_K. Let's denote by $\widetilde{G}$ a lift of G to S. Then, via definition 6.20 and thanks to remark 6.19, we obtain that $M(G) \simeq \mathbb{D}^*(\widetilde{G})(S)$. Still by remark 6.19, we see that $M(G)$ sits in the following short exact sequence

$$0 \longrightarrow (\mathrm{Lie}\ \widetilde{G})^\vee \longrightarrow M(G) \longrightarrow \mathrm{Lie}(\widetilde{G}^D) \longrightarrow 0. \tag{6.2}$$

Moreover, recalling remark 4.38, we have $(\mathrm{Lie}\ \widetilde{G})^\vee = \omega_{\widetilde{G}}$ and $\mathrm{Lie}(\widetilde{G}^D) = \omega^\vee_{\widetilde{G}^D}$. Also, when determining the filtration, it is useful to keep in mind remark 6.24, where we stated that

$$\mathrm{Fil}^1 M(G) = (\mathrm{Lie}\,\widetilde{G})^\vee + \mathrm{Fil}^1 S \cdot M(G).$$

Then we need to compute the conormal sheaves ω_G for $\mathbb{G}_m(p)$ and $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$. Let's notice that, seeing $G = \varinjlim_{v\in\mathbb{N}} G_v$, we obtain $\omega_G = \varprojlim_{v\in\mathbb{N}} \omega_{G_v}$. We'll start by arguing over $\mathbb{Z}$, then we will base change to S.

1. Let's start with $G = \varinjlim \mu_{p^v}$ and denote $G_v \coloneqq \mu_{p^v}$. As seen in example 2.20 this is affine over $\mathbb{Z}$ and it is given by

   $$\mu_{p^v} = \mathrm{Spec}(\mathbb{Z}[T]/(T^{p^v} - 1)) = \mathrm{Spec}(A_v).$$

   Then we recall that the closed immersion of the pointed scheme G_v corresponds to the augmentation morphism

   $$\widetilde{\varepsilon}\colon \mathbb{Z}[T]/(T^{p^v} - 1) \longrightarrow \mathbb{Z}.$$

   Denoting by I the augmentation ideal of A_v, the sheaf ω_{G_v} is the $\mathcal{O}_{\mathrm{Spec}(\mathbb{Z})}$-module $\mathcal{I}/\mathcal{I}^2$ associated to I/I^2. We can reduce its computation to that of I/I^2. To this aim we recall [Liu06, §6.1, proposition 1.8(d) and example 1.10] which let us compute

   $$\Omega^1_{A_v/\mathbb{Z}} = \frac{A_v \mathrm{d}T}{A_v p^v T^{p^v-1} \mathrm{d}T} = A_v/(p^v)\frac{\mathrm{d}T}{T}.$$

   Now we can invoke [Stacks, Lemma 0474] (taking $S = Z = \mathrm{Spec}(\mathbb{Z})$ and $X = G_v$), since $i_v = \mathrm{Spec}(\widetilde{\varepsilon})$ admits the structure morphism as a left inverse. This grants that

   $$\omega_{G_v} = i_v^* \Omega^1_{A_v/\mathbb{Z}} = \mathbb{Z}/(p^v)\frac{\mathrm{d}T}{T}.$$

2. Let's now analyze $G^D = \varinjlim \underline{\mathbb{Z}/p^v\mathbb{Z}}$, where we will denote $G^D_v = \underline{\mathbb{Z}/p^v\mathbb{Z}}$. We can use lemma 2.32 (as we did in example 2.36) to obtain that this is an étale group scheme over $\mathbb{Z}$. In fact we need to consider fiber by fiber what happens, but we are just base changing a finite product of copies of $\mathbb{Z}$ to the residue field. Then [Stacks, Section 00U0] grants that $\Omega_{G^D_v/\mathbb{Z}} = 0$ and finally that $\omega_{G^D_v} = i_v^* \Omega_{G^D_v/\mathbb{Z}} = 0$ thanks, as before, to [Stacks, Lemma 0474] (again, taking $S = Z = \mathrm{Spec}(\mathbb{Z})$, $X = G^D_v$ and noticing that $i_v = \mathrm{Spec}(\widetilde{\varepsilon})$ admits the structure morphism as a left inverse).

Now we can base change to S. To do so it suffices to tensor product our $\mathbb{Z}$-algebras with S and obtain $\widetilde{G}_v$ and $\widetilde{G}_v^D$ for all v. Then, since the base change of an étale morphism is still étale (see for example [Stacks, Lemma 02GO]), $\widetilde{G}_v^D$ is étale over S. Then $\omega_{\widetilde{G}_v^D} = 0$ for all v, hence $\omega_{\widetilde{G}^D} = 0$. With regards to $\widetilde{G}_v$ the above computations carry faithfully to the base change to S, giving us

$$\omega_{\widetilde{G}} = \varprojlim_{v\in\mathbb{N}} \omega_{\widetilde{G}_v} = \varprojlim_{v\in\mathbb{N}} S/(p^n)\frac{\mathrm{d}T}{T} = S\frac{\mathrm{d}T}{T},$$

since S is p-adically complete. We now have everything we needed to finally compute $M(G)$, Frobenius and filtration.

1. Let $G = \mathbb{G}_m(p)$, then filling equation (6.2) with the terms we computed above, we obtain $M(G) \simeq S$. Moreover $\mathrm{Fil}^1 M(G) = S$, since it contains $(\mathrm{Lie}\ \widetilde{G})^\vee = \omega_{\widetilde{G}} = S$. Finally we also get that φ_1 has to coincide with φ, being φ-semilinear and defined on $S = M(G)$.
2. Let's now consider G^D. Again, looking at equation (6.2), we obtain $M(G^D) = S$. Though now $(\mathrm{Lie}\ \widetilde{G}^D)^\vee = 0$, hence $\mathrm{Fil}^1 M(G^D) = \mathrm{Fil}^1 S$. And this implies also that our φ-semilinear map φ_1 coincides with φ/p on $\mathrm{Fil}^1 S$.

7 Comparison morphisms

In this section we will finally put all the pieces together to construct the comparison morphisms we hinted at in the introduction. To reach this goal we will still need to construct the ring B_{cris} and give an introduction to the construction of period rings, carried out by Fontaine.

As of notation, we will fix the following. We will denote, for this section, by K a complete discrete valuation field, with perfect residue field k of characteristic p and uniformizer π, by $W := W(k)$ the ring of Witt vectors with coefficients in k and by $K_0 := W[1/p]$ its field of fractions. We will fix $e := [K : K_0]$ the absolute ramification index of K, we denote by $\overline{K}$ a fixed separable closure of K and by $\mathbb{C}_K$ its completion. Finally we will denote by $\mathscr{G}_K := \mathrm{Gal}\left(\overline{K}/K\right)$ the absolute Galois group of K and notice that its action on $\overline{K}$ extends to $\mathbb{C}_K$ by continuity.

7.1 Galois representations

Definition 7.1: p-adic representation.
A *p-adic representation* of a profinite group Γ is a representation $\rho\colon \Gamma \to \mathrm{Aut}_{\mathbb{Q}_p}(V)$ of Γ on a finite-dimensional $\mathbb{Q}_p$ vector space V, where ρ is continuous. Here the topology on $\mathrm{Aut}_{\mathbb{Q}_p}(V)$ is that of $\mathrm{GL}_n(\mathbb{Q}_p)$, which is well defined, independently of the chosen basis.

A *morphism of p-adic representations* V_1, V_2 of Γ is a Γ-equivariant linear map $f\colon V_1 \to V_2$, i.e. a linear map that commutes with the action of Γ. More explicitly, denoting $\rho_i(\gamma)$ simply by γ for an element $\gamma \in \Gamma$, a Γ-equivariant map satisfies $\gamma(f(v)) = f(\gamma(v))$ for all $v \in V_1$ and all $\gamma \in \Gamma$.

We denote the category of p-adic representations of Γ, whose objects and morphism have just been described, by $\mathsf{Rep}_{\mathbb{Q}_p}(\Gamma)$.

Remark 7.2. In general the above definition is used for representations of Galois groups. In particular $\mathscr{G}_K$ is profinite and one studies p-adic representations of $\Gamma = \mathscr{G}_K$.

Definition 7.3: (F,Γ)-regular algebra.
Let F be a field and Γ a group. Let B be an integral F-algebra equipped with an action of Γ via automorphisms of F-algebras. Denote by $C := \mathrm{Frac}(B)$ and by $E := B^\Gamma$. Notice that Γ acts on C in a natural way. We say that B is *(F,Γ)-regular* iff

1. $B^\Gamma = C^\Gamma$ and

2. if $b \in B$ generates a vector space $F \cdot b$ stable under the action of Γ, then $b \in B^\times$.

Remark 7.4. Notice that, for any (F, Γ)-regular algebra B, E/F is a field extension. Moreover if B is already a field, than it is clearly (F, Γ)-regular. Finally we will always be concerned with $\Gamma = \mathscr{G}_K$ and $F = \mathbb{Q}_p$, so we will fix them and assume that B is a $(\mathbb{Q}_p, \mathscr{G}_K)$-regular algebra. Moreover in the following we will simply write Γ-regular to mean $(\mathbb{Q}_p, \Gamma)$-regular.

Definition 7.5.
One can define the functor

$$\begin{aligned} \mathbf{D}_B \colon \mathsf{Rep}_{\mathbb{Q}_p}(\mathscr{G}_K) &\longrightarrow \mathsf{Vect}(E) \\ V &\longmapsto \mathbf{D}_B(V) \coloneqq \left(B \otimes_{\mathbb{Q}_p} V\right)^{\mathscr{G}_K}, \end{aligned}$$

where we denoted by $\mathsf{Vect}(E)$ the category of E-vector spaces. Moreover we can define a natural B-linear, $\mathscr{G}_K$-equivariant map

$$\begin{aligned} \alpha_B(V) \colon B \otimes_E \mathbf{D}_B(V) &\longrightarrow B \otimes_{\mathbb{Q}_p} V \\ b \otimes d &\longmapsto bd. \end{aligned}$$

Proposition 7.6 ([BC09, Theorem 5.2.1])**.** *Fix $V \in \mathsf{Rep}_{\mathbb{Q}_p}(\mathscr{G}_K)$. Then the map $\alpha_B(V)$ is always injective and $\dim_E \mathbf{D}_B(V) \leq \dim_E V$. Moreover there is equality of dimensions iff $\alpha_B(V)$ is an isomorphism.*

Definition 7.7: Admissible representations.
We say that $V \in \mathsf{Rep}_{\mathbb{Q}_p}(\mathscr{G}_K)$ is a *B-admissible representation* iff $\dim_E \mathbf{D}_B(V) = \dim_E V$. We denote by $\mathsf{Rep}^B_{\mathbb{Q}_p}(\mathscr{G}_K) \subset \mathsf{Rep}_{\mathbb{Q}_p}(\mathscr{G}_K)$ the full subcategory of B-admissible representations.

Proposition 7.8 ([BC09, Theorem 5.2.1])**.** *Let's denote by $\mathsf{Vect}_f(E)$ the category of finite dimensional E-vector spaces. Then, the functor*

$$\begin{aligned} \mathbf{D}_B \colon \mathsf{Rep}^B_{\mathbb{Q}_p}(\mathscr{G}_K) &\longrightarrow \mathsf{Vect}_f(E) \\ V &\longmapsto \mathbf{D}_B(V) \coloneqq \left(B \otimes_{\mathbb{Q}_p} V\right)^{\mathscr{G}_K}, \end{aligned}$$

is exact and faithful. Moreover any subrepresentation and quotient of a B-admissible representation is B-admissible.

7.2 Period rings

Definition 7.9.
Let A be an $\mathbb{F}_p$-algebra. We can associate it the perfect $\mathbb{F}_p$-algebra

$$R(A) \coloneqq \varprojlim_{x \mapsto x^p} A = \left\{ \mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \ldots) \in \prod_{n \in \mathbb{N}} A \;\middle|\; \mathbf{x}_{n+1}^p = \mathbf{x}_n \text{ for all } n \in \mathbb{N} \right\}$$

endowed with the product ring structure.

Remark 7.10.

1. The above $\mathbb{F}_p$-algebra is perfect since the pth power map is clearly surjective by definition. Moreover it is injective since any element $\mathbf{x} = (\mathbf{x}_n)$ satisfying $\mathbf{x}^p = 0$ has $\mathbf{x}_{n-1} = \mathbf{x}_n^p = 0$ for all $n \geq 1$.

2. We have a canonical morphism

$$\begin{aligned} R(A) &\longrightarrow A \\ (\mathbf{x}_n)_{n\in\mathbb{N}} &\longmapsto \mathbf{x}_0. \end{aligned}$$

   Moreover any morphism from a perfect $\mathbb{F}_p$-algebra to A factors through the above projection.

3. If A is already perfect, then $R(A) \simeq A$. In particular the inverse map of the above projection is given by $a \mapsto \left(a^{1/p^n}\right)$. In particular, let's consider $\overline{k}$ a fixed separable closure of k. Since $\overline{k}$ is already perfect, we obtain $R(\overline{k}) \simeq \overline{k}$.

4. Given F a field of characteristic p, it can be shown that $R(F)$ is the largest perfect subfield of F.

Notation 7.11.
We introduce the following ring

$$R \coloneqq R(O_{\mathbb{C}_K}/pO_{\mathbb{C}_K}) = R(O_{\overline{K}}/pO_{\overline{K}}).$$

It is a perfect $\mathbb{F}_p$-algebra and also canonically an algebra over $\overline{k}$, since $O_{\mathbb{C}_K}$ is.

Proposition 7.12 ([BC09, Proposition 4.3.1])**.** *Let O be a p-adically separated and complete ring, and $\mathfrak{a} \triangleleft O$ an ideal of O containing p and such that $\mathfrak{a}^N \subset pO$ for some $N \in \mathbb{N}$ (i.e. the $\mathfrak{a}$-adic and p-adic topologies coincide). Then we have a map*

$$\begin{aligned} R(O/\mathfrak{a}) &\longrightarrow \varprojlim_{x\mapsto x^p} O \\ (\mathbf{x}_n)_{n\in\mathbb{N}} &\longmapsto \left(\mathbf{x}^{(n)}\right)_{n\in\mathbb{N}}, \end{aligned}$$

where we define $\mathbf{x}^{(n)} \coloneqq \lim_{m\to\infty} \widehat{\mathbf{x}_{n+m}}^{p^m}$, in which $\widehat{\mathbf{x}_m}$ is any lift of $\mathbf{x}_m$ to O. This map does not depend on the choice of lift, it is bijective and its inverse is given by

$$\begin{aligned} \varprojlim_{n\mapsto x^p} O &\longrightarrow R(O/\mathfrak{a}) \\ \left(\mathbf{x}^{(n)}\right)_{n\in\mathbb{N}} &\longmapsto \left(\mathbf{x}^{(n)} \bmod \mathfrak{a}\right)_{n\in\mathbb{N}}. \end{aligned}$$

Moreover $R(O/pO) \simeq R(O/\mathfrak{a})$ and this common ring is a domain as soon as O is.

Remark 7.13. If we endow $\varprojlim_{x\mapsto x^p} O$ with the ring structure given, for any $\mathbf{x} \coloneqq \left(\mathbf{x}^{(n)}\right)$ and $\mathbf{y} \coloneqq \left(\mathbf{y}^{(n)}\right)$, by

$$(\mathbf{xy})^{(n)} \coloneqq \mathbf{x}^{(n)}\mathbf{y}^{(n)} \qquad \text{and} \qquad (\mathbf{x}+\mathbf{y})^{(n)} \coloneqq \lim_{m\to\infty} \left(\mathbf{x}^{(n+m)} + \mathbf{y}^{(n+m)}\right)^{p^m},$$

then the above bijection is an isomorphism of rings.

Notation 7.14.
In view of the above isomorphism we might see an element $\mathbf{x} \in R$ either as an element $(\mathbf{x}_n) \in \varprojlim_{x \mapsto x^p} O_{\mathbb{C}_K}/(p)$ or as an element $\left(\mathbf{x}^{(n)}\right) \in \varprojlim_{x \mapsto x^p} O_{\mathbb{C}_K}$. We will use high and low indices accordingly.

Remark 7.15. Let's now notice that $\mathscr{G}_K \coloneqq \mathrm{Gal}\left(\overline{K}/K\right)$ acts naturally on $O_{\mathbb{C}_K}$, since it acts via isometries on $\overline{K}$. Moreover, since it acts via morphisms of rings, which commute with $x \mapsto x^p$, its action can be naturally extended to $R = \varprojlim_{x \mapsto x^p} O_{\mathbb{C}_K}$.

Lemma 7.16 ([BC09, Lemma 4.3.3])**.** *Denote by $|\cdot|_p$ the absolute value on $\mathbb{C}_K$ normalized by $|p|_p = 1/p$. The map*

$$\begin{aligned} |\cdot|_R : R &\longrightarrow p^{\mathbb{Q}} \cup \{0\} \\ \left(\mathbf{x}^{(n)}\right)_{n\in\mathbb{N}} &\longmapsto \left|\mathbf{x}^{(0)}\right|_p \end{aligned}$$

*is a $\mathscr{G}_K$-*equivariant absolute value *on R that makes R the valuation ring for the unique valuation ν_R on $\mathrm{Frac}\, R$ extending $-\log_p |\cdot|_R$ on R and having value group $\mathbb{Q}$. Moreover R is ν_R-adically separated and complete and the subfield $\overline{k}$ of R maps isomorphically onto the residue field of R.*

Example 7.17.

1. Fix $\left(p^{1/p^n}\right)_{n\in\mathbb{N}}$ a compatible family of p^nth roots of p in $O_{\mathbb{C}_K}$. Denote by $\mathbf{p}$ the element of R given by
$$\mathbf{p} \coloneqq \left(p^{(n)}\right)_{n\in\mathbb{N}} = \left(p, p^{1/p}, p^{1/p^2}, \dots\right) \in R.$$
Its valuation is easily computed by $\nu_R(\mathbf{p}) = \nu_p(p^{(0)}) = \nu_p(p) = 1$.

2. Fix a compatible family of primitive p^nth roots of unity $(\zeta_{p^n})_{n\in\mathbb{N}}$ in $O_{\mathbb{C}_K}$. We denote by $\boldsymbol{\varepsilon}$ the special element of R given by
$$\boldsymbol{\varepsilon} \coloneqq \left(\boldsymbol{\varepsilon}^{(n)}\right)_{n\in\mathbb{N}} = \left(1, \zeta_p, \zeta_{p^2}, \dots\right) \in R.$$
The element $\boldsymbol{\varepsilon}$ depends on the chosen compatible family and any two such $\boldsymbol{\varepsilon}$ are $\mathbb{Z}_p^\times$-powers of each other. Moreover we have $\nu_R\left(\boldsymbol{\varepsilon} - 1\right) = p/(p-1)$. Let's show this for $p > 2$: by definition we have $\nu_R(\boldsymbol{\varepsilon} - 1) = \nu_p\left((\boldsymbol{\varepsilon} - 1)^{(0)}\right)$. By remark 7.13 we have
$$(\boldsymbol{\varepsilon} - 1)^{(0)} = \lim_{n\to\infty} \left(\zeta_{p^n} + (-1)^{(n)}\right)^{p^n}.$$
Let's notice that $(-1)^{(n)} = -1$ for all n and that $\zeta_{p^n} - 1$ is a root of $\Phi_{p^n}(1+X)$, where Φ_m denotes the mth cyclotomic polynomial. In particular $\Phi_{p^n}(1+X)$ is Eisenstein of degree $p^{n-1}(p-1)$. Then
$$\nu_R(\boldsymbol{\varepsilon} - 1) = \lim_{n\to\infty} \frac{p^n}{p^{n-1}(p-1)} = \frac{p}{p-1}.$$
Finally we recall that $\mathscr{G}_K$ acts on ζ_{p^n} via the cyclotomic character, which is defined by $g(\zeta_{p^n}) = \zeta_{p^n}^{\chi(g)}$ for any $g \in \mathscr{G}_K$. As a consequence, since the induced action is componentwise, $\mathscr{G}_K$ acts also on $\boldsymbol{\varepsilon}$ via the cyclotomic character, i.e. $g(\boldsymbol{\varepsilon}) = \boldsymbol{\varepsilon}^{\chi(g)}$ for all $g \in \mathscr{G}_K$.

Theorem 7.18 ([BC09, Theorem 4.3.5])**.** *The field $\mathrm{Frac}\, R = R[1/\mathbf{p}]$ is algebraically closed.*

Remark 7.19. There is a natural family of ring homomorphisms

$$\begin{aligned} \theta_n \colon R &\longrightarrow O_{\mathbb{C}_K} \\ (\mathbf{x}_m)_{m\in\mathbb{N}} &\longmapsto \mathbf{x}_n. \end{aligned}$$

Let's give R a $\overline{k}$-algebra structure via the k-embedding

$$\begin{aligned} \overline{k} = R(\overline{k}) &\longrightarrow R(O_{\overline{K}}/pO_{\overline{K}}) = R \\ c &\longmapsto \left(j(c), j(c^{1/p}), j(c^{1/p^2}), \dots\right), \end{aligned}$$

where $j\colon \overline{k} \to O_{\overline{K}}/(p)$ is the canonical section to the reduction map $O_{\overline{K}}/(p) \twoheadrightarrow \overline{k}$. Then θ_0 is a morphism of $\overline{k}$-algebras. We wish to lift it to a ring map $W(R) \to O_{\mathbb{C}_K}$, but we cannot use universal property of the Witt vectors construction since $O_{\mathbb{C}_K}/(p)$ is not perfect (in particular the Frobenius is not injective).

Definition 7.20.
We define, set theoretically, the map

$$\begin{aligned} \theta\colon W(R) &\longrightarrow O_{\mathbb{C}_K} \\ \textstyle\sum_{n\in\mathbb{N}}[\mathbf{c}_n]p^n &\longmapsto \textstyle\sum_{n\in\mathbb{N}} \mathbf{c}_n^{(0)} p^n, \end{aligned}$$

where remark 6.14 allows us to write any element of $W(R)$ in a unique Teichmüller expansion and $\mathbf{c}_n^{(0)}$ is defined as in notation 7.14.

Remark 7.21. In remark 6.14 we explicitly computed the Teichmüller expansion of $(\mathbf{r}_n)_{n\in\mathbb{N}}$ to be $\sum_{n\in\mathbb{N}}[\mathbf{r}_n^{p^{-n}}]p^n$. Moreover, by compatibility of the elements in $\varprojlim_{x\mapsto x^p} O_{\mathbb{C}_K}$ and multiplicativity of $\mathbf{r} \mapsto \mathbf{r}^{(n)}$, we have that $\left(\mathbf{r}^{p^{-n}}\right)^{(0)} = \left((\mathbf{r}^{p^{-n}})^{(n)}\right)^{p^n} = \mathbf{r}^{(n)}$. Hence we can compute θ also via

$$\theta\colon (\mathbf{r}_0, \mathbf{r}_1, \dots) \longmapsto \textstyle\sum_{n\in\mathbb{N}} \mathbf{r}_n^{(n)} p^n.$$

Remark 7.22. Let's recall that in remark 7.15 we saw that the action of $\mathscr{G}_K$ extends naturally from $O_{\mathbb{C}_K}$ to R. Then, thanks to proposition 6.15, this naturally induces an action of $\mathscr{G}_K$ on $W(R)$. More explicitly the action of $\mathscr{G}_K$ is defined, for all $g \in \mathscr{G}_K$, by

$$g\left(\sum_{n\in\mathbb{N}}[\mathbf{c}_n]p^n\right) = \sum_{n\in\mathbb{N}}[g(\mathbf{c}_n)]p^n.$$

Moreover, recalling the explicit description of the Teichmüller expansion given in remark 6.14, we see that this action of $\mathscr{G}_K$ on $W(R)$ corresponds with the component-wise action (again, since it commutes with Frobenius on R).

Lemma 7.23 ([BC09, Lemma 4.4.1])**.** *The map $\theta\colon W(R) \to O_{\mathbb{C}_K}$ is a $\mathscr{G}_K$-equivariant surjective ring homomorphism.*

Remark 7.24. Notice that θ is clearly $\mathscr{G}_K$-equivariant, since $\mathscr{G}_K$ acts on $O_{\mathbb{C}_K}$ via isometries (hence via continuous maps). Moreover, inverting p, we obtain another $\mathscr{G}_K$-equivariant surjective ring homomorphism

$$\theta_{\mathbf{Q}}\colon W(R)[1/p] \longrightarrow O_{\mathbb{C}_K}[1/p] = \mathbb{C}_K.$$

It is important to notice, though, that the source ring is not a complete valuation ring.

Proposition 7.25 ([BC09, Proposition 4.4.3])**.** *Let* $\mathbf{p}$ *be as in example 7.17 and let*

$$\xi \coloneqq \xi_{\mathbf{p}} = [\mathbf{p}] - p \in W(R).$$

1. *The ideal* $\ker\theta \lhd W(R)$ *is principal and it is generated by* ξ*.*
2. *An element* $\mathbf{w} = (\mathbf{w}_0, \mathbf{w}_1, \ldots) \in \ker\theta$ *generates the ideal if and only if* $\mathbf{w}_1 \in R^\times$*.*

Corollary 7.26 ([BC09, Corollary 4.4.5])**.** *For all* $j \geq 1$ *we have* $W(R) \cap (\ker\theta_{\mathbf{Q}})^j = (\ker\theta)^j$*. Moreover* $\bigcap_{j\geq 1}(\ker\theta)^j = \bigcap_{j\geq 1}(\ker\theta_{\mathbf{Q}})^j = 0$*.*

Remark 7.27. As a consequence of the above we see that $W(R)[1/p]$ injects into its $\ker\theta_{\mathbf{Q}}$-completion

$$B^+_{\mathrm{dR}} \coloneqq \varprojlim_{j\geq 1} \frac{W(R)[1/p]}{(\ker\theta_{\mathbf{Q}})^j}.$$

Recall that $\mathscr{G}_K$ acts component-wise on the ring of Witt vectors, so $\ker\theta_{\mathbf{Q}}$ is stable under the action of $\mathscr{G}_K$ and the transition maps of the above projective limit are $\mathscr{G}_K$-equivariant. As a consequence B^+_{dR} inherits a natural action of $\mathscr{G}_K$ which is compatible with that on its subring $W(R)[1/p]$. Then B^+_{dR} projects $\mathscr{G}_K$-equivariantly on its quotients by $(\ker\theta_{\mathbf{Q}})^j$. In particular, for $j = 1$, we obtain a lift of θ to a $\mathscr{G}_K$-equivariant surjection

$$\theta^+_{\mathrm{dR}} \colon B^+_{\mathrm{dR}} \longrightarrow \mathbb{C}_K.$$

Finally we see that the action of the Frobenius on $W(R)[1/p]$ does not naturally extend to B^+_{dR}. In fact $\ker\theta_{\mathbf{Q}}$ is not stable under its action, since $\varphi(\xi) = [\mathbf{p}^p] - p \notin \ker\theta_{\mathbf{Q}}$.

By construction B^+_{dR} is a discrete valuation ring, so we want to find a uniformizer which behaves well under the action of $\mathscr{G}_K$

Definition 7.28.
Let $\boldsymbol{\varepsilon}$ be as in example 7.17. We define

$$t \coloneqq \log([\boldsymbol{\varepsilon}]) = \log(1 + ([\boldsymbol{\varepsilon}] - 1)) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{([\boldsymbol{\varepsilon}] - 1)^n}{n} \in B^+_{\mathrm{dR}}.$$

Remark 7.29 ([BC09, pp. 60–62])**.**

1. The element $[\boldsymbol{\varepsilon}] - 1$ lies in $\ker\theta$, hence the element $\log([\boldsymbol{\varepsilon}])$ is well defined in B^+_{dR}.
2. One can show, via careful topological arguments, that, since any two different choices of $\boldsymbol{\varepsilon}$ are related by $\boldsymbol{\varepsilon}' = \boldsymbol{\varepsilon}^a$ for $a \in \mathbb{Z}_p^\times$, then $t' = at$.
3. $\mathscr{G}_K$ acts multiplicatively on t via the cyclotomic character, i.e. for all $g \in \mathscr{G}_K$ we have

$$g(t) = \chi(g)t.$$

4. The element t is a uniformizer of B^+_{dR}.

Definition 7.30: Field of p-adic periods.
We define the *field of p-adic periods*, also called the *de Rham period ring*,

$$B_{\mathrm{dR}} \coloneqq \operatorname{Frac} B^+_{\mathrm{dR}} = B^+_{\mathrm{dR}}[1/t].$$

Remark 7.31. Notice that, just like B_{dR}^+, the field of p-adic periods B_{dR} is endowed with a natural action of $\mathscr{G}_K$. Moreover we can notice that, set theoretically, the construction of B_{dR} depends only on $\mathbb{C}_K$ and not on K, though the choice of K changes, functorially, the Galois group acting on it, up to restriction to a closed subgroup.

Proposition 7.32 ([BC09, Theorem 4.4.13 and example 5.1.3])**.** *B_{dR} is $\mathscr{G}_K$-regular (being a field) and $B_{\mathrm{dR}}^{\mathscr{G}_K} = K$.*

Definition 7.33.
We define A_{cris} to be the p-adic completion of the divided power envelope of $W(R)$ with respect to the ideal $\ker\theta$. More explicitly

$$A_{\mathrm{cris}} = \varprojlim_{n\in\mathbb{N}} \mathcal{D}_{W(R)}(\ker\theta)/p^n\mathcal{D}_{W(R)}(\ker\theta).$$

Remark 7.34 ([BC09, §9.1])**.** The ring A_{cris} is identified with a subring of B_{dR}^+, whose elements are given by

$$A_{\mathrm{cris}} = \left\{ \sum_{n\in\mathbb{N}} \mathbf{a}_n \frac{\xi^n}{n!} \;\middle|\; \mathbf{a}_n \in W(R) \text{ s.t. } \lim_{n\to\infty} \mathbf{a}_n = 0 \text{ for the } p\text{-adic topology} \right\}.$$

In particular this grants that A_{cris} is a domain. Moreover the composite $A_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}^+ \twoheadrightarrow \mathbb{C}_K$ lands in $O_{\mathbb{C}_K}$ and induces a surjective ring homomorphism $A_{\mathrm{cris}} \twoheadrightarrow O_{\mathbb{C}_K}$. Also, by [BC09, Proposition 9.1.3], we see that the important element $t = \log([\boldsymbol{\varepsilon}])$ is in A_{cris}.

Remark 7.35. As seen in remark 7.22, $\mathscr{G}_K$ acts on $W(R)$ sending $pW(R)$ to $pW(R)$ and, as seen in remark 7.27, $\ker\theta$ to $\ker\theta$. Then by universal property of divided powers envelope the action extends to $\mathcal{D}_{W(R)}(\ker\theta)$. More explicitly any $g \in \mathscr{G}_K$ induces the unique dashed arrow

$$\begin{array}{ccc} & & \mathcal{D}_{W(R)}(\ker\theta) \\ & \nearrow & \\ (W(R), \ker\theta) & \longrightarrow & W(R) \subset \mathcal{D}_{W(R)}(\ker\theta). \end{array} \tag{7.1}$$

This then extends to A_{cris}. By [BC09, Proposition 9.1.2] the action of $\mathscr{G}_K$ on A_{cris} is continuous for the p-adic topology. Also, following [BC09, Lemmas 9.1.7-9.1.8], we can extend the Frobenius morphism φ on $W(R)$ to A_{cris}. In fact one can check on the generator $\xi = [\mathbf{p}] - p$ of $\ker\theta$ that φ on $W(R)$ sends $\ker\theta + (p)$ to $\ker\theta + (p)$ and argue as in equation (7.1) that the Frobenius extends to $\mathcal{D}_{W(R)}(\ker\theta)$ and then to A_{cris}. In particular the above holds since

$$\varphi(\xi) = [\mathbf{p}^p] - p = [\mathbf{p}]^p - p = \underbrace{[\mathbf{p}]^p - p^p}_{\in\ker\theta} + \underbrace{p^p - p}_{\in(p)}.$$

Moreover one can check that $\varphi(t) = pt$.

Remark 7.36. We can give to A_{cris} the structure of W-algebra and then also of S-algebra. The construction goes as follows. We have the injections

$$W(R) \hookrightarrow \mathcal{D}_{W(R)}(\ker\theta) \hookrightarrow \varprojlim_{n\in\mathbb{N}} \mathcal{D}_{W(R)}(\ker\theta)/p^n\mathcal{D}_{W(R)}(\ker\theta) = A_{\mathrm{cris}}.$$

Since, moreover, $k \hookrightarrow R$ we obtain an injection $W \hookrightarrow W(R)$. Composed with the above it gives a canonical W-algebra structure to A_{cris}. We then use this structure to define the W-algebra morphism

$$\begin{aligned} \alpha\colon W[u] &\longrightarrow A_{\mathrm{cris}} \\ u &\longmapsto [\boldsymbol{\pi}], \end{aligned}$$

where $\boldsymbol{\pi}$ is defined, like $\mathbf{p}$, as $\boldsymbol{\pi} \coloneqq \left(\pi, \pi^{1/p}, \pi^{1/p^2}, \dots\right) \in \varprojlim O_{\mathbb{C}_K} = R$ for π a uniformizer of K. Notice, moreover, that by definition of Frobenius on both $W[u]$ and A_{cris}, the map α is compatible with Frobenius. In fact the image of α lies in $W(R) \subset A_{\text{cris}}$, hence we can check it here, since Frobenius of A_{cris} extends that of $W(R)$. Then, by definition we have the following square

$$\begin{array}{ccc} \sum_{n\in\mathbb{N}} a_n u^n & \xmapsto{\alpha} & \sum_{n\in\mathbb{N}} a_n \left[\boldsymbol{\pi}\right]^n \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} \\ \sum_{n\in\mathbb{N}} a_n^p u^{np} & \xmapsto[\alpha]{} & \sum_{n\in\mathbb{N}} a_n^p \left[\boldsymbol{\pi}\right]^{np}, \end{array}$$

which commutes since the Frobenius on $W(R)$ is a ring homomorphism. Now we notice that $\alpha(E(u)) \in \ker\theta$ by definition of θ. In fact $\alpha(E(u)) = E([\boldsymbol{\pi}])$ and $\theta([\boldsymbol{\pi}]) = \pi$ imply that $\theta(\alpha(E(u))) = E(\pi) = 0$. This implies that, by universal property of divided powers envelope, the morphism $W[u] \to W(R) \subset A_{\text{cris}}$ induces a morphism $\mathcal{D}_{W[u]}(E(u)) \to W(R)$. Now we can see $W(R) \subset \mathcal{D}_{W(R)}(\ker\theta)$ which, combined with the above comments, induces the diagram

$$\begin{array}{ccc} \mathcal{D}_{W[u]}(E(u)) & \longrightarrow & \mathcal{D}_{W(R)}(\ker\theta) \\ \downarrow & \searrow & \downarrow \\ S & \dashrightarrow & A_{\text{cris}}, \end{array}$$

where the dashed arrow exists by universal property of the completion of a ring with respect to the p-adic topology.

Definition 7.37.
We denote by B^+_{cris} the $\mathscr{G}_K$-stable $W(R)[1/p]$ subalgebra

$$B^+_{\text{cris}} \coloneqq A_{\text{cris}}[1/p] \subset B^+_{\text{dR}}.$$

We define the *crystalline period ring* for K to be the $\mathscr{G}_K$-stable $W(R)[1/p]$-subalgebra of B_{dR} given by $B_{\text{cris}} \coloneqq B^+_{\text{cris}}[1/t]$.

Remark 7.38.

1. With some computations (see [BC09, Proposition 9.1.3]) one can show that $t^{p-1} \in pA_{\text{cris}}$, hence that inverting t makes p a unit. Then $B_{\text{cris}} = B^+_{\text{cris}}[1/t] = A_{\text{cris}}[1/t]$.
2. As for B_{dR}, set theoretically the definition of B^+_{cris} and of B_{cris} only depends on $\mathbb{C}_K$. Again the choice of K changes, functorially, the Galois group $\mathscr{G}_K$ acting on the period rings.

Proposition 7.39 ([BC09, Proposition 9.1.6])**.** *B_{cris} is $\mathscr{G}_K$-regular and $B_{\text{cris}}^{\mathscr{G}_K} = K_0$.*

Finally we give a characterization of A_{cris} via a universal property.

Definition 7.40: Formal divided power thickening.
Let A be a ring, with a principal ideal $\mathfrak{p}$ equipped with divided powers and V be an A-algebra. A *$\mathfrak{p}$-adic divided power thickening of V* is a surjective homomorphism of A-algebras $\theta\colon D \to V$ such that $\ker\theta$ has a divided power structure compatible with those on $\mathfrak{p}$, similarly to definition 4.53. Morphisms between divided power thickening are divided power morphisms making the obvious diagram commute. If the category of $\mathfrak{p}$-adic divided power A-thickening of V, whose objects and morphisms have just been defined, admits an initial object we call it the *universal $\mathfrak{p}$-adic divided power A-thickening of V*.

If, moreover, V is separated and complete with respect to the $\mathfrak{p}$-adic topology we define *formal $\mathfrak{p}$-adic divided power A-thickenings of V* to be $\mathfrak{p}$-adic divided power A-thickenings of V which are separated and complete with respect to the $\mathfrak{p}$-adic topology. An initial object in the category of formal $\mathfrak{p}$-adic divided power A-thickening of V is called universal as before.

Proposition 7.41 ([Fon94, §2.3.2]). *A_{cris} is a universal formal p-adic divided power W-thickening of $O_{\mathbb{C}_K}$.*

Proof. It is clear that, by construction, A_{cris} is a formal p-adic divided power W-thickening of $O_{\mathbb{C}_K}$. In fact $\ker(A_{\mathrm{cris}} \to O_{\mathbb{C}_K})$ is the p-adic completion of the P.D. ideal generated by $\ker\theta$ in $\mathcal{D}_{W(R)}(\ker\theta)$. The latter is equipped with divided powers by construction, whereas the former is equipped with divided powers by lemma 4.10. We then need to show universality. Let (D, θ_D, γ) be another formal p-adic divided power W-thickening of $O_{\mathbb{C}_K}$. Giving a morphism of formal p-adic divided power W-thickening from A_{cris} to D is equivalent to giving a continuous morphism

$$\alpha\colon W(R) \longrightarrow D$$

between p-adic rings, such that $\theta_D \circ \alpha = \theta|_{W(R)}$. This is because universal property of divided powers envelope allows to extend α uniquely to $\mathcal{D}_{W(R)}(\ker\theta)$ and continuity to A_{cris}. Let's denote $J_D \coloneqq \ker\theta_D$. We now need to notice that, given $d_1 \equiv d_2 \mod J_D$ in D, then $d_1^p \equiv d_2^p \mod pJ_D$. In fact, given $d_1 \equiv d_2 \mod J_D$ there is $\lambda \in J_D$ such that $d_2 = d_1 + \lambda$. Then

$$d_2^p = d_1^p + \sum_{i=1}^{p-1} \binom{p}{i} d_1^i \lambda^{p-i} + \lambda^p.$$

Here we notice that $\binom{p}{i} d_1^i \lambda^{p-i} \in pJ_D$ for all $2 \leq i \leq p-1$ and that $\lambda^p = p!\gamma_p(\lambda)$, since J_D is equipped with divided powers. All in all we have $d_1^p - d_2^p \in pJ_D$ as we wished. Fix now $\mathbf{x} \in R$ and take, for any $m \in \mathbb{N}$, $\xi_m \in D$ a lift via θ_D of $\mathbf{x}^{(m)} \in O_{\mathbb{C}_K}$, defined as in notation 7.14. Then, from what we stated before, the sequence $\xi_m^{p^m}$ converges p-adically to an element $\rho(\mathbf{x}) \in D$ which does not depend on the chosen lift. To prove this let's notice that, since $(x^{(m+1)})^p = x^{(m)}$ in $O_{\mathbb{C}_K}$, we have $\xi_{m+1}^p \equiv \xi_m \mod J_D$. But, by what we just proved, this implies that $\xi_{m+1}^{p^{m+1}} \equiv \xi_m^{p^m} \mod p^m J_D$, hence that the sequence $\left\{\xi_m^{p^m}\right\}$ is p-adically Cauchy. Since D is p-adically complete this is enough to grant convergence. With regards to independence from the chosen lift, fix another family $\{\zeta_m\}$ of lifts of $x^{(m)}$ in D. Then, by construction, $\xi_m \equiv \zeta_m \mod J_D$ for all $m \in \mathbb{N}$, hence $\xi_m^{p^m} \equiv \zeta_m^{p^m} \mod p^m J_D$ by the above. This means that the sequence $\left\{\xi_m^{p^m} - \zeta_m^{p^m}\right\}$ is Cauchy, moreover it clearly converges to zero. Then, being D a topological ring (hence sum is continuous), we obtain that the two sequences $\left\{\zeta_m^{p^m}\right\}$ and $\left\{\xi_m^{p^m}\right\}$ converge to the same point, which is then independent from the choice of lifts. Let's now recall that

$$\theta([\mathbf{x}]) = \mathbf{x}^{(0)} = \lim_{n\to\infty} \widehat{\mathbf{x}_n}^{p^n}.$$

We want to construct a family of lifts ξ_n such that $\xi_n \to \alpha([\mathbf{x}])$, in order to show that $\alpha([\mathbf{x}]) = \rho(\mathbf{x})$. We denote by $y_n \coloneqq \widehat{\mathbf{x}_n}^{p^n} \in O_{\mathbb{C}_K}$ and by

$$\mathbf{y}_n \coloneqq \left(y_n, y_n^{1/p}, y_n^{1/p^2}, \dots\right) \in \varprojlim_{x\mapsto x^p} O_{\mathbb{C}_K} \simeq R.$$

Then $\theta([\mathbf{y}_n]) = \widehat{\mathbf{x}_n}^{p^n}$ by definition of θ. Moreover it is clear that $\mathbf{y}_n \to \mathbf{x}$ in R, hence that $[\mathbf{y}_n] \to [\mathbf{x}]$, if we endow $W(R)$ with the weak topology. The first statement is true since, by definition of the element $\mathbf{x}^{(0)}$ (and independence of the chosen lift in its definition), we have $y_n \to \mathbf{x}^{(0)}$. Then an easy induction argument shows that $y_n^{1/p^m} \to \mathbf{x}^{(m)}$, hence that we have convergence in $R \simeq \varprojlim_{x\mapsto x^p} O_{\mathbb{C}_K}$ (notice that we can uniformly bound the distance of each component from its limit). By continuity of α, then, we get that

$$\alpha([\mathbf{x}]) = \alpha\left(\lim_{n\to\infty} [\mathbf{y}_n]\right) = \lim_{n\to\infty} \alpha([\mathbf{y}_n]) = \rho(\mathbf{x}),$$

where the last equality holds by compatibility of α with θ, which implies that $\alpha([\mathbf{y}_n])$ is a lift of $\widehat{\mathbf{x}_n}^{p^n}$. Then, since α is a continuous morphism of p-adic rings, it acts on the general element of $W(R)$ by

$$\alpha\colon (\mathbf{x}_1, \mathbf{x}_2, \ldots) = \textstyle\sum_{n\in\mathbb{N}} [\mathbf{x}_n^{p^{-n}}]p^n \longmapsto \sum_n \rho(\mathbf{x}_n^{p^{-n}})p^n.$$

This proves uniqueness, but it is also an explicit description of α. As a consequence also existence is clear, since the above α is a continuous homomorphism which commutes with the morphisms θ. ∎

7.3 Comparison morphisms

This last section will be dedicated to constructing and studying a few properties of our desired comparison morphism and related ones.

Remark 7.42. Consider $G \in \mathsf{BT}/O_K$, seen as the inductive limit of G_v, as in definition 3.41. Let's notice that, in proposition 3.72 we could have carried out the proof in $O_{\mathbb{C}_K}$ instead of $O_{\overline{K}}$. This follows from remark 3.69, in which we saw that $G_v(\overline{K}) = G_v(O_{\mathbb{C}_K})$. Then we have

$$T_p(G) \simeq \mathrm{Hom}_{\mathsf{BT}/O_{\mathbb{C}_K}}\left(\underline{\mathbb{Q}_p/\mathbb{Z}_p}, G_{O_{\mathbb{C}_K}}\right).$$

Remark 7.43. Among other things, lemma 4.10 states that $A_{\mathrm{cris}} \twoheadrightarrow O_{\mathbb{C}_K}$ is a divided power thickening. Since we will need to compute $\mathbb{D}^*(G_{O_{\mathbb{C}_K}})(A_{\mathrm{cris}})$ for certain $G \in \mathsf{BT}/O_K$, we wish to reduce its computation to that of $\mathbb{D}^*(G)(S)$. In order to do so, let's recall remark 5.34, where we explicitly defined the pullback of our crystals. In particular consider the cartesian diagram

$$\begin{array}{ccc} V := \mathrm{Spec}(A_{\mathrm{cris}}) & \longrightarrow & U \\ \uparrow & & \uparrow \\ V_0 := \mathrm{Spec}(O_{\mathbb{C}_K}) & \xrightarrow{f} & \mathrm{Spec}(O_K) =: U_0. \end{array}$$

In this context we have $f^*G = G_{O_{\mathbb{C}_K}}$. Then stability under base change means

$$f^*\mathbb{D}^*(G)_{U_0\hookrightarrow U} \simeq \mathbb{D}^*(G_{O_{\mathbb{C}_K}})_{V_0\hookrightarrow V}$$

as Zariski sheaves. Moreover, since both A_{cris} and O_K are endowed with a morphism from S (hence with an S-module structure), from the universal property of pushouts, we obtain a morphism in $\mathsf{Crys}(O_K)$

$$\begin{array}{ccc} U & \xrightarrow{\overline{\alpha}} & \mathrm{Spec}(S) \\ \uparrow & & \uparrow \\ \mathrm{Spec}(O_K) & = & \mathrm{Spec}(O_K) \end{array}$$

which we will denote by α. Since crystals are special sheaves on $\mathsf{Crys}(O_K)$, as of definition 4.62, we finally have $\alpha^*\mathbb{D}^*(G)_{S\twoheadrightarrow O_K} = \mathbb{D}^*(G)_{U_0\hookrightarrow U}$. Now we can conclude since, taking evaluations, we have

$$\mathbb{D}^*(G_{O_{\mathbb{C}_K}})(A_{\mathrm{cris}}) \simeq f^*\mathbb{D}^*(G)(S) = A_{\mathrm{cris}} \otimes_S \mathbb{D}^*(G)(S).$$

Remark 7.44. From remark 7.42 we see that any $f \in T_p(G)$ can be interpreted as a morphism of Barsotti-Tate groups on $O_{\mathbb{C}_K}$ between $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$ (base changed to $O_{\mathbb{C}_K}$) and $G_{O_{\mathbb{C}_K}}$. Since $\mathbb{D}^*$ acts contravariantly on Barsotti-Tate groups and covariantly on rings, it associates to f the map

$$\mathbb{D}^*(f)(A_{\mathrm{cris}})\colon \mathbb{D}^*(G_{O_{\mathbb{C}_K}})(A_{\mathrm{cris}}) \longrightarrow \mathbb{D}^*(\underline{\mathbb{Q}_p/\mathbb{Z}_p})(A_{\mathrm{cris}}).$$

We use remark 7.43 to compute those crystals in terms of the modules $M(G) = \mathbb{D}^*(G)(S)$ of proposition 6.37. In particular, from example 6.38, we get $\mathbb{D}^*(\underline{\mathbb{Q}_p/\mathbb{Z}_p})(S) = S$. Then we have

$$\mathbb{D}^*(\underline{\mathbb{Q}_p/\mathbb{Z}_p})(A_{\text{cris}}) \simeq A_{\text{cris}} \qquad \text{and} \qquad \mathbb{D}^*(G_{O_{\mathbb{C}_K}})(A_{\text{cris}}) \simeq A_{\text{cris}} \otimes_S \mathbb{D}^*(G)(S).$$

Recalling that A_{cris} has an S-algebra structure, defined in remark 7.36, we obtain a pairing

$$\begin{aligned} T_p(G) \times \mathbb{D}^*(G_{O_{\mathbb{C}_K}})(A_{\text{cris}}) &\longrightarrow A_{\text{cris}} \\ (f, a) &\longmapsto \mathbb{D}^*(f)(A_{\text{cris}})(a). \end{aligned}$$

But this allows to associate to each $a \in \mathbb{D}^*(G_{O_{\mathbb{C}_K}})(A_{\text{cris}})$ the evaluation morphism

$$\begin{aligned} \rho_a \colon T_p(G) &\longrightarrow A_{\text{cris}} \\ f &\longmapsto \mathbb{D}^*(f)(A_{\text{cris}})(a). \end{aligned}$$

Since $\mathbb{D}^*$ is an additive functor this morphism is $\mathbb{Z}$-linear, moreover it can be shown to be $\mathbb{Z}_p$-linear too. As stated in remark 3.71, $T_p(G)$ is a free $\mathbb{Z}_p$-module of finite rank. As a consequence we have a canonical isomorphism

$$\text{Hom}_{\mathbb{Z}_p\text{-Mod}}\left(T_p(G), \mathbb{Z}_p\right) \otimes_{\mathbb{Z}_p} A_{\text{cris}} \xrightarrow{\sim} \text{Hom}_{\mathbb{Z}_p\text{-Mod}}\left(T_p(G), A_{\text{cris}}\right).$$

All in all, the above allows us to define the following homomorphism

$$\rho_G \colon A_{\text{cris}} \otimes_S \mathbb{D}^*(G)(S) \longrightarrow A_{\text{cris}} \otimes_{\mathbb{Z}_p} T_p(G)^\vee.$$

Definition 7.45.
Fix $\left\{\pi^{1/p^n}\right\}$, a compatible family of roots of the uniformizer π of K. By compatible we mean that $(\pi^{1/p^n})^p = \pi^{1/p^{n-1}}$ for all $n \in \mathbb{N}$. We define the algebraic extension K_∞/K as the extension given by $K_\infty \coloneqq \bigcup_{n\in\mathbb{N}} K(\pi^{1/p^n})$. As usual we will denote by $\mathscr{G}_{K_\infty} \coloneqq \text{Gal}\left(\overline{K}/K_\infty\right)$ the absolute Galois group of K_∞.

Theorem 7.46 ([Fal99, §6, theorem 7])**.** *The morphism constructed in remark 7.44*

$$\rho_G \colon A_{\text{cris}} \otimes_S \mathbb{D}^*(G)(S) \longrightarrow A_{\text{cris}} \otimes_{\mathbb{Z}_p} T_p(G)^\vee$$

is a functorial $\mathscr{G}_{K_\infty}$-equivariant injection which respects Frobenius and filtrations. Moreover the cokernel of ρ_G is annihilated by t.

Proof. The idea of the proof, as carried out in [Fal99, §6], is to first concentrate on the particular case of $G = \mathbb{G}_m(p)$ and then reduce, using functoriality of ρ_G, the general case to this one. Here, though, we will not be concerned with filtrations nor with Frobenius.

Let's start by tackling functoriality and $\mathscr{G}_{K_\infty}$-equivariance. Both of them can be explicitly checked in the construction of remark 7.44. In fact each step is clearly functorial and, upon inspecting the various action at each step, it turns out that each is also $\mathscr{G}_{K_\infty}$-equivariant.

Let's now concentrate on the particular case, so let's fix $G = \mathbb{G}_m(p)$ for now. We need to explicitly compute the morphism ρ_G, using Messing's theory, in order to prove that t kills $\text{coker}\,\rho_G$. Recall that $T_p(G) = \mathbb{Z}_p(1)$, hence that $T_p(G)^\vee = \mathbb{Z}_p(-1)$. Now, since $\mathscr{G}_K$ acts on $t \in A_{\text{cris}}$ via the cyclotomic character, we have an isomorphism of $\mathscr{G}_K$-modules $\mathbb{Z}_p(-1) \simeq \mathbb{Z}_p t^{-1}$. Let's recall that we denoted $t = \log([\varepsilon]) \in A_{\text{cris}}$. Moreover, as defined in example 7.17, we will use the notation $\varepsilon^{(n)}$ to denote our fixed p^nth root of unity $\zeta_{p^n} \in O_{\mathbb{C}_K}$, Then $t \in T_p(G)$

corresponds, as shown in proposition 3.72, to a morphism of Barsotti-Tate groups $\underline{\mathbb{Q}_p/\mathbb{Z}_p} \to \mathbb{G}_m(p)$. In particular, when evaluated at $O_{\mathbb{C}_K}$, it gives rise to

$$\begin{aligned} u_0 \colon \mathbb{Q}_p/\mathbb{Z}_p &\longrightarrow \mu_{p^\infty}(O_{\mathbb{C}_K}) \\ \tfrac{1}{p^n} &\longmapsto \boldsymbol{\varepsilon}^{(n)}, \end{aligned}$$

where by $\mu_{p^\infty}(O_{\mathbb{C}_K})$ we mean the multiplicative group of all p^∞ roots of unity in $O_{\mathbb{C}_K}$. Starting from the construction of proposition 5.13 one can compute the universal extension of G and G^D. In particular they are

$$0 \longrightarrow \mathbb{G}_a \longrightarrow (\mathbb{G}_a \oplus \underline{\mathbb{Q}_p})/\underline{\mathbb{Z}_p} \longrightarrow \underline{\mathbb{Q}_p/\mathbb{Z}_p} \longrightarrow 0$$

for $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$, where the quotient is given by the pushout of $\mathbb{G}_a$ and $\underline{\mathbb{Q}_p}$ over their common subgroup $\underline{\mathbb{Z}_p}$, and

$$1 \longrightarrow 1 \longrightarrow \mathbb{G}_m(p) \longrightarrow \mathbb{G}_m(p) \longrightarrow 1$$

for $\mathbb{G}_m(p)$. For this last notice that dual of $\mathbb{G}_m(p)$ is étale, hence $\omega_{G^D} = 0$. Considering t as a morphism of Barsotti-Tate groups, proposition 5.18 grants the existence of a morphism of extensions which, when evaluated at $O_{\mathbb{C}_K}$, gives rise to the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & O_{\mathbb{C}_K} & \longrightarrow & \frac{O_{\mathbb{C}_K} \oplus \mathbb{Q}_p}{\mathbb{Z}_p} & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle v_0} & & \downarrow{\scriptstyle u_0} & & \\ 1 & \longrightarrow & 1 & \longrightarrow & \mu_{p^\infty}(O_{\mathbb{C}_K}) & \longrightarrow & \mu_{p^\infty}(O_{\mathbb{C}_K}) & \longrightarrow & 1. \end{array}$$

Here it is clear that the map v_0, making the diagram commute, is defined by

$$v_0 \colon (\lambda, x) \longmapsto u_0(x).$$

Henceforth we will denote by $\boldsymbol{\varepsilon}^x := u_0(x)$, for $x \in \mathbb{Q}_p/\mathbb{Z}_p$. In particular, if we write $x = a/p^m$, for $a \in \mathbb{Z}_p$ and $-m = \nu_p(x)$, we can explicitly compute $\boldsymbol{\varepsilon}^x := \left(\boldsymbol{\varepsilon}^{(m)}\right)^a$. Theorem 5.26, recalling remark 6.21 and that A_{cris} is p-adically complete, grants that v_0 can be uniquely lifted to a morphism

$$v \colon (A_{\text{cris}} \oplus \mathbb{Q}_p)/\mathbb{Z}_p \longrightarrow A_{\text{cris}}^\times$$

such that $-v|_{\underline{\mathcal{V}}(\mathbb{G}_m(p)_{A_{\text{cris}}})}$ is an exponential (notice that, following the notation of theorem 5.26, $j = 0$ in our case). Moreover we can define a morphism

$$\begin{aligned} \widetilde{v} \colon (A_{\text{cris}} \oplus \mathbb{Q}_p)/\mathbb{Z}_p &\longrightarrow A_{\text{cris}}^\times \\ (a, x) &\longmapsto \exp(-at)\,[\alpha(x)]\,, \end{aligned}$$

where, writing as before $x = a/p^m$ with $-m = \nu_p(x)$,

$$\alpha(x) := \left((\boldsymbol{\varepsilon}^{(m+n)})^a\right)_{n \in \mathbb{N}} \in R = \varprojlim O_{\mathbb{C}_K}.$$

Here it is important to notice that A_{cris} is complete with respect to the p-adic topology and that $\ker\theta$ is equipped with divided powers, hence that the above map is well defined. Then, since $t \in \ker\theta$, ideal with divided powers, we also obtain that $\exp(-at) \in \ker\theta$. As a consequence

we obtain that $\theta(\widetilde{v}(x)) = \boldsymbol{\varepsilon}^x$, i.e. that $\widetilde{v}$ lifts v_0. Moreover, restricting v to $\underline{\mathcal{V}(\underline{\mathbb{Q}_p/\mathbb{Z}_p}_{A_{\mathrm{cris}}})}$ is the same as computing it at $x = 0$, which is an exponential. By uniqueness this grants that $v = \widetilde{v}$. Then we have explicitly computed $\mathbb{E}(u_0) \coloneqq \mathbb{E}(t) = \widetilde{v}$. Now, taking Lie of all that, we get (what else could it be)

$$\mathbb{D}^*(t)(A_{\mathrm{cris}})(a) = \log\left(\exp(-at)\right) = -at$$

for all $a \in A_{\mathrm{cris}}$. And this is exactly the required explicit construction of ρ_G, which then acts by

$$\begin{aligned} \rho_G \colon A_{\mathrm{cris}} \otimes_S \mathbb{D}^*(\mathbb{G}_m(p))(S) &\longrightarrow A_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p t^{-1} \\ 1 \otimes 1 &\longmapsto -t \otimes t^{-1}. \end{aligned}$$

Here we clearly see that t kills $\operatorname{coker} \rho_G$, since $\operatorname{im} \rho_G = t \cdot (A_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p t^{-1})$.

Let's now switch to the general case, in which $G \in \mathsf{BT}/O_K$ is arbitrary. We want to explicitly construct a morphism $G_{O_{\overline{K}}} \to \mathbb{G}_m(p)$ which will allow us to reduce the study of ρ_G to the one we have just defined. To achieve this goal we recall that $T_p(G)^\vee = T_p(G^D)(-1) = t^{-1}T_p(G^D)$. Hence, given any $y \in T_p(G)^\vee$, we obtain $ty \in T_p(G^D)$, which can be interpreted as a map in $\mathrm{Hom}_{\mathsf{BT}/O_{\overline{K}}}\left(\underline{\mathbb{Q}_p/\mathbb{Z}_p}, G^D_{O_{\overline{K}}}\right)$. By theorem 2.42 this gives a morphism

$$(ty)^D : G_{O_{\overline{K}}} \longrightarrow \mathbb{G}_m(p)_{O_{\overline{K}}}$$

Now, by functoriality of the comparison morphism ρ_G, we obtain the commutative diagram

$$\begin{array}{ccc} A_{\mathrm{cris}} \otimes_S \mathbb{D}^*(G)(S) & \xrightarrow{\rho_G} & A_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} (T_p(G))^\vee \\ {\scriptstyle \mathrm{id}_{A_{\mathrm{cris}}} \otimes \mathbb{D}^*((ty)^D)(A_{\mathrm{cris}})}\uparrow & & \uparrow{\scriptstyle \mathrm{id}_{A_{\mathrm{cris}}} \otimes T_p((ty)^D)^\vee} \\ A_{\mathrm{cris}} \otimes_S \mathbb{D}^*(\mathbb{G}_m(p))(S) & \xrightarrow{\rho_{\mathbb{G}_m(p)}} & A_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p t^{-1}, \end{array}$$

where we recall that both $\mathbb{D}^*$ and $T_p(G)^\vee$ act contravariantly on morphisms. Now we need to determine the morphism $T_p((ty)^D)^\vee$. To do so let's notice that

$$\begin{aligned} T_p((ty)^D)^\vee(1) = T_p(ty) \colon T_p\big(\underline{\mathbb{Q}_p/\mathbb{Z}_p}\big) &\longrightarrow T_p(G^D) \\ 1 = (1/p^v)_{v\in\mathbb{N}} &\longmapsto ty. \end{aligned}$$

Here, as computed before, we have $T_p(\underline{\mathbb{Q}_p/\mathbb{Z}_p}) = \mathbb{Z}_p$ and $T_p(G^D) = T_p(G)^\vee(1)$. Combined with the above this determines the morphism

$$T_p((ty)^D)^\vee \colon t^{-1} \longmapsto y.$$

Then, in the above square, we see that

$$\begin{array}{ccc} 1 \otimes \mathbb{D}^*((ty)^D)(A_{\mathrm{cris}})(1) & \xmapsto{\rho_G} & -t \otimes y \\ {\scriptstyle \mathrm{id}_{A_{\mathrm{cris}}} \otimes \mathbb{D}^*((ty)^D)(A_{\mathrm{cris}})}\uparrow & & \uparrow{\scriptstyle \mathrm{id}_{A_{\mathrm{cris}}} \otimes T_p((ty)^D)^\vee} \\ 1 \otimes 1 & \xmapsto{\rho_{\mathbb{G}_m(p)}} & -t \otimes t^{-1}. \end{array}$$

Now, since we imposed no restriction to the choice of $y \in T_p(G)^\vee$, commutativity of the square tells us that t kills $\operatorname{coker} \rho_G$.

We are finally left to prove injectivity. Notice that, thanks to classical Dieudonné theory, $\mathbb{D}^*(G)(S)$ is a free S-module of rank h. Then, inverting t in A_{cris}, i.e. extending scalars to B_{cris}, we obtain a surjective map

$$B_{\mathrm{cris}} \otimes_S \mathbb{D}^*(G)(S) \longrightarrow B_{\mathrm{cris}} \otimes_S T_p(G)^\vee$$

between finitely generated free B_{cris}-modules. But then, applying Cayley-Hamilton, we see that this is an isomorphism, so in particular it is injective. Now, since $\mathbb{D}^*(G)(S)$ and $T_p(G)^\vee$ are free modules, they are also flat, hence the inclusion $A_{\mathrm{cris}} \hookrightarrow B_{\mathrm{cris}}$ induces the inclusions

$$A_{\mathrm{cris}} \otimes_S \mathbb{D}^*(G)(S) \hookrightarrow B_{\mathrm{cris}} \otimes_S \mathbb{D}^*(G)(S)$$

and

$$A_{\mathrm{cris}} \otimes_S T_p(G)^\vee \hookrightarrow B_{\mathrm{cris}} \otimes_S T_p(G)^\vee.$$

This allows us to see ρ_G as the restriction of an isomorphism to a subspace, which grants its injectivity. And we win. ■

Remark 7.47. Notice that it is important to consider only the action of $\mathscr{G}_{K_\infty}$. In fact, the S-module structure of A_{cris} is induced from the map $u \mapsto [\boldsymbol{\pi}]$ from $W[u]$ to $W(R)$. Then an action on the tensor product $A_{\mathrm{cris}} \otimes_S \mathbb{D}^*(G)(S)$ has to be compatible with this S-module structure. In particular, since $W \subset K$, it has to fix the element $[\boldsymbol{\pi}]$, which is not the case for $\mathscr{G}_K$.

We remark that, base changing to B_{cris}, the above result can actually be improved upon.

Theorem 7.48. *The base change to B_{cris} of the morphism constructed in remark 7.44*

$$B_{\mathrm{cris}} \otimes_S \mathbb{D}^*(G)(S) \xrightarrow{\sim} B_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} T_p(G)^\vee$$

is a $\mathscr{G}_{K_\infty}$-equivariant isomorphism compatible with filtrations and Frobenius.

Remark 7.49. This result actually extends previously known results in the context of classical Dieudonné theory. In fact, given $G \in \mathsf{BT}/O_K$, let's denote by G_k its base change to $k = O_K/\mathfrak{m}$ the residue field of O_K. Then, denoted by $\mathbb{D}^*(G_k)$ the Dieduonné module associated to G_k, we have the isomorphism of modules

$$\mathbb{D}^*(G)(S) \simeq S \otimes_W \mathbb{D}^*(G_k).$$

Though here we have not defined a natural filtration. As a consequence it will not be of concern when looking at the classical comparison morphism.

Theorem 7.50. *Let $G \in \mathsf{BT}/O_K$ and G_k be as above. Then we have a functorial $\mathscr{G}_K$-equivariant injection*

$$\rho_G \colon A_{\mathrm{cris}} \otimes_W \mathbb{D}^*(G_k) \longrightarrow A_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} \left(T_p(G)\right)^\vee$$

which is also compatible with Frobenius. Inverting t we obtain a functorial $\mathscr{G}_K$-equivariant isomorphism

$$\rho \colon B_{\mathrm{cris}} \otimes_W \mathbb{D}^*(G_k) \longrightarrow B_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} \left(T_p(G)\right)^\vee$$

which again is compatible with Frobenius.

Remark 7.51. Classically, in fact, in order to recover a natural filtration on $\mathbb{D}^*(G_k)$, one needs to base change to B_{dR}. In fact one can define $D_K \coloneqq O_K \otimes_W \mathbb{D}^*(G_k)$. Then

$$D_K = \mathbb{D}^*(G)(S)/\left(\mathrm{Fil}^1 S \otimes_W \mathbb{D}^*(G_k)\right),$$

hence it inherits a filtration from that on $\mathbb{D}^*(G)(S)$, via

$$\mathrm{Fil}^1 D_K \coloneqq \mathrm{Fil}^1 / \left(\mathrm{Fil}^1 S \otimes_W \mathbb{D}^*(G_k)\right).$$

And now this induces the usual filtration on the scalar extension $B_{\mathrm{dR}} \otimes_W D_K$, via

$$\begin{aligned}\mathrm{Fil}^i \left(B_{\mathrm{dR}} \otimes_W D_K\right) &= \sum_{j\in\mathbb{Z}} \mathrm{im}\left(\mathrm{Fil}^j B_{\mathrm{dR}} \otimes_W \mathrm{Fil}^{i-j} D_K\right) \\ &= \mathrm{Fil}^{i-1} B_{\mathrm{dR}} \otimes_W \mathrm{Fil}^1 D_K + \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_W D_K,\end{aligned}$$

since the (decreasing) filtration on D_K satisfies $\mathrm{Fil}^0 D_K = D_K$ and $\mathrm{Fil}^2 D_K = 0$. Moreover one defines

$$\mathrm{Fil}^i \left(B_{\mathrm{dR}} \otimes_{\mathbb{Z}_p} T_p(G)\right) \coloneqq \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_{\mathbb{Z}_p} T_p(G).$$

With all this in mind one can prove that the base change of the above isomorphism ρ to B_{dR}, i.e.

$$\mathrm{id}_{B_{\mathrm{dR}}} \otimes \rho \colon B_{\mathrm{dR}} \otimes_W D \longrightarrow B_{\mathrm{dR}} \otimes_{\mathbb{Z}_p} T_p(G)$$

is an isomorphism compatible with the filtrations we have just defined.

References

[BC09] Olivier Brinon and Brian Conrad. *CMI Summer School Notes on p-Adic Hodge Theory*. 2009.

[BO78] Pierre Berthelot and Arthur Ogus. *Notes on crystalline cohomology*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1978, pp. vi+243.

[EGA] Jean Dieudonné and Alexander Grothendieck. 'Éléments de géométrie algébrique : I. Le langage des schémas'. In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 4 (1960), pp. 5–228.

[Fal99] Gerd Faltings. 'Integral crystalline cohomology over very ramified valuation rings'. In: *Journal of the American Mathematical Society* 12 (1999), pp. 117–144.

[Fon94] Jean-Marc Fontaine. *Périodes p-adiques - Séminaire de Bures, 1988*. Ed. by Jean-Marc Fontaine. Astérisque 223. Société mathématique de France, 1994, pp. 59–103.

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics 52. Springer, 1977.

[Jon95] A. J. de Jong. 'Crystalline Dieudonné module theory via formal and rigid geometry'. In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 82 (1995), pp. 5–96.

[Kis07] Mark Kisin. 'Crystalline representations and F-crystals'. In: *Algebraic Geometry and Number Theory: In Honor of Vladimir Drinfeld's 50th Birthday*. Ed. by victor ginzburg victor. Progress in Mathematics. Birkhäuser Boston, 2007, pp. 459–496.

[Liu06] Qing Liu. *Algebraic geometry and arithmetic curves*. Oxford graduate texts in mathematics 6. Oxford University Press, 2006.

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

[Mil17] J. S. Milne. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*. Cambridge Studies in Advanced Mathematics 170. Cambridge University Press, 2017.

[SG80] Jean-Pierre Serre and Marvin J. Greenberg. *Local Fields*. 2nd edition. Graduate Texts in Mathematics 67. Springer, 1980.

[SGA3-1] Michel Demazure and Alexander Grothendieck. *Schémas en Groupes. Séminaire de Géométrie Algébrique du Bois Marie – 1962-64 – (SGA 3)*. Vol. 1: Propriétés Générales des Schémas en Groupes. Lecture Notes in Mathematics 151. Springer, 1970.

[Sha86] Stephen S. Shatz. 'Group Schemes, Formal Groups, and p-Divisible Groups'. In: *Arithmetic geoemtry*. Ed. by Gary Cornell and Joseph H. Silverman. Springer, 1986, pp. 29–78.

[Stacks] The Stacks project authors. *The Stacks project*. 2021. URL: `https://stacks.math.columbia.edu`.

[Tat67] John Tate. 'p-Divisible Groups'. In: *Proceedings of a Conference on Local Fields: NUFFIC Summer School*. Ed. by T. A. Springer. Springer, 1967, pp. 151–183.

[Tat98] John Tate. 'Finite Flat Group Schemes'. In: *Modular Forms and Fermat's Last Theorem*. Ed. by Gary Cornell and Joseph H. Silverman. Springer, 1998, pp. 121–154.

[Vis04] Angelo Vistoli. 'Notes on Grothendieck topologies, fibered categories and descent theory'. In: *arXiv preprint math/0412512* (2004).

[Wat79] William C. Waterhouse. *Introduction to Affine Group Schemes*. Graduate Texts in Mathematics 66. Springer, 1979.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*. Cambridge studies in advanced mathematics 38. Cambridge University Press, 1994.