Comparison theorems for p-divisible groups

Supervisor:
Prof. Olivier Brinon

Master thesis by:
Luming ZHAO

Università degli Studi
di Padova

Université Bordeaux 1

Academic year 2016/2017

Contents

1. Introduction

Let X be a smooth projective algebraic variety over $\mathbb{R}$. For $0 \leq n \leq 2\dim(X)$, there is a period pairing

$$\begin{aligned} H^n_{dR}(X(\mathbb{C})/\mathbb{R}) \times H_n(X(\mathbb{C}), \mathbb{Z}) &\to \mathbb{C} \\ (\omega, \gamma) &\mapsto \int_\gamma \omega \end{aligned}$$

relating de Rham cohomology and singular homology. It induces a comparison isomorphism:

$$H^n_{\mathrm{B}}(X(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} H^n_{\mathrm{dR}}(X(\mathbb{C})/\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C}$$

(where $H^n_{\mathrm{B}}(X(\mathbb{C}), \mathbb{Q}) = \mathrm{Hom}_{\mathrm{gr}}(H_n(X(\mathbb{C}), \mathbb{Z})), \mathbb{Q})$ is the Betti cohomology). This isomorphism is compatible with the $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ actions (trivial on the de Rham cohomology and induced by the complex conjugation on the singular cycles on the Betti cohomology) and filtrations (Hodge filtration on the de Rham cohomology). This provides a link between different cohomologies.

The simplest non trivial example is that of elliptic curves (or more generaly abelian varieties): in that case $X(\mathbb{C}) = \mathrm{Lie}(X(\mathbb{C}))/H_1(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{C}/\Lambda$ is a complex torus (*cf* [1, Chapter I], [2, Chapter IV]).

Let p be a prime integer. The aim of this report is to explain a p-adic analogue of this simple case. More generally, we will consider the case of Barsotti-Tate groups. Indeed, given an abelian variety A, the collection of groups of p^n torsion $A[p^n]$ gives rise to a Barsotti-Tate group $\varinjlim_n A[p^n]$, to which we can associate its Tate module

$\mathrm{T}_p\,A$. As we will see, the latter is the p-adic analogue of singular homology in the analytic case.

Barsotti-Tate groups are central objects in Arithmetic Geometry: they are useful to study finite group schemes (which are important in ramification theory for example), rational points in Diophantine Geometry, moduli spaces (*eg* Shimura varieties), *etc.*

This report is organized as follows. In section 2 we recall basic facts on group schemes, then we introduce Barsotti-Tate groups and their first properties. In section 3 we introduce divided powers. This allows us to define the crystalline site of a scheme of characteristic p and crystals, that are the natural context to develop Dieudonné theory. The latter aims at classifying Barsotti-Tate groups in terms of (semi-)linear algebra: we present its construction and main properties (following Messing, *cf* [3]) in section 4. A key result (Grothendieck-Messing theorem) describes deformation theory of Barsotti-Tate groups in terms of their Dieudonné crystal and filtrations: this will provide a complete classification (due to Breuil and Kisin) of Barsotti-Tate groups over the ring of integers of a complete discrete valuation field of characteristic 0 with perfect residue field of characteristic p (*cf* section 5). The Dieudonné module is an avatar of de Rham cohomology: in section 6 we use Breuil-Kisin funtor and arguments of Faltings to construct a crystalline comparison isomorphism for Barsotti-Tate groups, from which we derive the Hodge-Tate comparison theorem (which is due to Tate). Unlike the analytic setting, these comparison isomorphisms require to extend the scalars to sophisticated period rings (that were constucted by Fontaine), that we present as well.

Convention.
1. "p" is a fixed prime number.
2. Hopf algebras to appear are over a ring R that is noetherian and has a unity.
3. In our case, we can take as base scheme $S = \operatorname{Spec} R$ and focus on the category $(\mathbf{Sch}/\mathrm{S})$ in most cases.
4. "group over S, S-group, $\cdots$" will always mean a fppf sheaf of commutative groups on the site $(\mathbf{Sch}/\mathrm{S})_{\mathrm{fppf}}$.

Acknowledgement.
I'd like to give sincere thanks to my supervisor Prof. Olivier Brinon (Université de Bordeaux 1). Brinon spent countless time answering my questions, correcting my mistakes in the master thesis and giving me guidence and suggestions. I am impressed and influenced by his sincere attitude towards his career.
I thank Prof. Yichao Tian for his help during my last year Bachelor and afterwards. It's my great honor to have been a member of the Erasmus ALGANT program, which provides me excellent experience learning higher mathematics in Europe.
I give thanks to Prof. Qing Liu for his selfless help in all aspects, to Prof. Denis Benois for his helpful lecture on number theory and to Prof. Dajano Tossici for his helpful suggestions on my master thesis.
I thank professors of Padova University for their well-organized lectures: I give special thanks to Prof. Francesco Baldassarri and Prof. Bruno Chiarellotto for their helps and suggestions on my study, to Prof. Adrian Iovita for his interesting lecture on number theory and to Prof. Pietro Polesello and Prof. Andrea D'Agnolo for their tough but helpful lectures.
Finally, I thank my family and friends, for their endless patience and support.

2. Barsotti-Tate groups and formal Lie groups

2.1. **Group schemes.**

Let $\mathcal{C}$ be a category with finite products and hence in particular a terminal object (the empty product), denoted by $*$. If $G, T \in \mathcal{C}$, put $G(T) := h_G^\circ(T) = \mathrm{Hom}_{\mathcal{C}}(T, G)$.

Definition 2.2. A *group object* in $\mathcal{C}$, or a $\mathcal{C}$-group, is an object G in $\mathcal{C}$ such that $h_G^\circ \colon \mathcal{C} \to \mathbf{Set}$ factors through the forgetful functor $\mathbf{Gr} \to \mathbf{Set}$.

A $\mathcal{C}$-group G is *commutative* if the group $G(T)$ is commutative for every $T \in \mathcal{C}$.

A *morphism* of $\mathcal{C}$-groups $G \to G'$ is a morphism $\varphi \colon G \to G'$ in the category $\mathcal{C}$ such that, for every object T in $\mathcal{C}$, the induced map

$$\begin{aligned} G(T) &\to G'(T) \\ g &\mapsto \varphi \circ g \end{aligned}$$

is a group homomorphism.

Remark 2.3.
(1) The group structure on G is given by arrows

$$m : G \times G \to G$$

$$\epsilon : * \to G$$

$$\mathrm{inv} : G \to G$$

inducing the group law, the unit and the inverse on the groups $G(T)$ for $T \in G$. The group law $G(T) \times G(T) \to G(T)$ is got in an obvious way, noticing by definition of $G \times G$ we have $(G \times G)(T) = G(T) \times G(T)$. More explicitly, the induced law on $G(T)$ is just $(g_1, g_2) \mapsto m \circ (g_1, g_2)$ where $(g_1, g_2) : T \to G \times G$ represents the unique arrow given by the universal property of product, *i.e.* (g_1, g_2) satisfies $\mathrm{pr}_i \circ (g_1, g_2) = g_i$, for $i \in \{1, 2\}$.
(2) One checks that the group axioms are equivalent to the commutativity of the following diagrams:
(associativity)

$$\begin{tikzcd} G \times G \times G \arrow[r, "\mathrm{Id} \times m"] \arrow[d, "m \times \mathrm{Id}"'] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"] & G \end{tikzcd}$$

(neutral element)

$$\begin{tikzcd} G = * \times G = G \times * \arrow[r, "\mathrm{Id} \times \epsilon"] \arrow[d, "\epsilon \times \mathrm{Id}"'] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"] & G \end{tikzcd}$$

(inverse)

$$\begin{tikzcd} G \times G \arrow[r, "\mathrm{inv} \times \mathrm{Id}"] & G \times G \arrow[d, "m"] \\ G \arrow[u, "\Delta"] \arrow[r, "\epsilon_G := \epsilon \circ \pi_G"] & G \end{tikzcd}$$

where π_G is the unique morphism of G to $*$,
(commutativity)

$$\begin{tikzcd} G \times G \arrow[rr, "\tau=(\mathrm{pr}_2,\mathrm{pr}_1)"] \arrow[dr, "m"'] & & G \times G \arrow[dl, "m"] \\ & G & \end{tikzcd}$$

where τ is the automorphism interchanging the factors on the products.

Let S be a scheme, we now specialize to the category (**Sch**/S) of S-schemes.

Definition 2.4. A *S-group scheme*, or simply *S-group*, is a group object in (**Sch**/S).

In the cases to consider, we will only deal with affine group schemes.

Definition 2.5. An *affine group scheme* G over a noetherian ring R is a group scheme represented by an R-algebra A. Hence it is a representable group functor $G : \mathbf{Alg}_R \to \mathbf{Gr}$ from the category of R-algebras to the category of groups.
A *finite flat group scheme* G over R is an affine group scheme, represented by a finite flat R-algebra A. The *order* of G is the locally constant function with respect to the Zariski topology on $\mathrm{Spec}(R)$ = prime ideals of R given at $\mathfrak{p}$ by the rank of the free $R_{\mathfrak{p}}$-module $A_{\mathfrak{p}}$.

Let $G = h_A^\circ$ be a group functor on R-algebras. Note that

$$h_A^\circ \times h_B^\circ : T \to \mathrm{Hom}(A, T) \times \mathrm{Hom}(B, T)$$

is represented by $h_{A \otimes_R B}^\circ$. By this observation and the Yoneda Lemma we deduce that:
(1) the multiplication $G \times G \to G$ yields a comultiplication $\triangle$: $A \to A \otimes_R A$;
(2) the unit map ϵ yields a counit map $\varepsilon : A \to R$, necessarily surjective;
(3) the inverse $\mathrm{inv} : G \to G$, $g \mapsto g^{-1}$ yields the antipode $S : A \to A$.
All these maps are R-algebra maps. Similarily as when we define group scheme, the group axioms translates into certain commutative diagrams.

Definition 2.6. A *commutative Hopf algebra over R* is by definition an R-algebra A with comultiplication $\triangle$, augmentation ε and antipode S that make the diagrams mentioned above commutative.

Proposition 2.7. *The category of affine group schemes over R is contravariant equivalent to the category of commutative Hopf algebras, with a Hopf algebra A corresponding to the affine group scheme $G = \mathrm{Hom}_R(A, \bullet)$ that it represents.*

Proof. The proof is obvious from our definition of Hopf algebra above. □

Definition 2.8. Let H and G be two group schemes corresponding to Hopf algebras A and B respectively. Then a morphism $H \to G$ corresponds to a map $B \to A$ compatible with Hopf algebra structures. If $B \to A$ is surjective, we say that H is a *closed subgroup* of G.

Hence the study of affine group scheme is just the study of Hopf algebras. First examples are as follows.

Example 2.9. Let R be a noetherian ring.
(1) The *additive group* is the group scheme $\mathbb{G}_a$ given by $\mathbb{G}_a(A) = (A, +)$ for all R-algebra A. Its Hopf algebra is $R[X]$ with

$$\triangle\,(X) = 1 \otimes X + X \otimes 1,\ \varepsilon(X) = 0,\ S(X) = -X.$$

(2) The *multiplicative group* is the group scheme $\mathbb{G}_m$ given by $\mathbb{G}_m(A) = (A^\times, \cdot)$ for all R-algebra A. Its Hopf algera is $R[X, X^{-1}]$ with

$$\triangle (X) = X \otimes X,\, \varepsilon(X) = 1,\, S(X) = X^{-1}.$$

(3) The *group of n-th roots of unity.* $\mu_n = \mathrm{Spec}(R[X]/(X^n - 1))$ is the kernel of raising to the n-th power of $\mathbb{G}_m$, since

$$\mathrm{Hom}_{R-\mathrm{alg}}(R[X]/(X^n - 1), B) = \{b \in B, b^n = 1\}.$$

The Hopf algebra of μ_n is $R[X]/(X^n - 1)$ with

$$\triangle (X) = X \otimes X,\, \varepsilon(X) = 1,\, S(X) = X^{-1}.$$

Thus μ_n is finite flat of order n. In fact, the representing algebra is even a free R-module of rank n. Notice this is a closed subgroup of $\mathbb{G}_m$.
(4) Let Γ be an abstract commutative finite group. The group algebra $R[\Gamma] = \oplus_{\gamma\in\Gamma} R[\gamma]$ is a Hopf algera with

$$\triangle ([\gamma]) = [\gamma] \otimes [\gamma];\, \varepsilon([\gamma]) = 1,\, S([\gamma]) = [\gamma^{-1}]$$

Write $\Gamma = \oplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$, then $R[\Gamma] \simeq \otimes_{i=1}^r R[X]/(X^{n_i} - 1)$ and hence $\mathrm{Spec}\, R[\Gamma] \simeq \mu_{n_1} \times \cdots \times \mu_{n_r}$. Hence the associated group scheme is a finite product of copies of μ_n. Such a group scheme is called *diagonalizable.* The R-dual of $R[\Gamma]$ is $R^\Gamma = \mathrm{Maps}(\Gamma, R)$, which is a Hopf algebra with details described below in (5).
(5) If Γ is a finite abstract group, the *constant group scheme* $\underline{\Gamma}$ is represented by $\mathrm{Maps}(\Gamma, R) = \prod_{t\in\Gamma} R$, which is the R-dual of $R[\Gamma]$. Let $(f_\gamma)_{\gamma\in\Gamma}$ be the dual basis of $([\gamma])_{\gamma\in\Gamma}$ and so we have $f_\gamma^2 = f_\gamma$; $f_\gamma f_\tau = 0$; $\sum f_\gamma = 1$. Hence it is a canonical basis of $\prod_{\gamma\in\Gamma} R$ and we define the structure on $\prod_{\gamma\in\Gamma} R$ by:

$$\triangle (f_\gamma) = \textstyle\sum_{\tau\cdot\sigma=\gamma} f_\tau \otimes f_\gamma,\, \varepsilon(f_\gamma) = \delta_{\gamma,1},\, S(f_\gamma) = f_{\gamma^{-1}}$$

An important example of constant group scheme is $\underline{\mathbb{Z}/n\mathbb{Z}}$, whose Hopf algerba is $\prod_{t\in\mathbb{Z}/n\mathbb{Z}} R$ with structure as described above.
(6) If R has characteristic $p > 0$, then the affine group scheme α_p is defined by $\alpha_p(A) = \{a \in A | a^p = 0\}$ for all R-algebra A. Its Hopf algebra is $R[X]/(X^p)$ with

$$\triangle (X) = X \otimes 1 + 1 \otimes X,\, \varepsilon(X) = 0,\, S(X) = -X$$

Hence α_p is finite flat of order p and this is a closed subgroup of $\mathbb{G}_a$.

For later use we give the following definition that generalizes the notion of Hopf algebra.

Definition 2.10. A *co-commutative $\mathscr{O}_S$ co-algebra* $\mathcal{A}$ is the dual structure of a commutative $\mathscr{O}_S$-algebra. Precisely, we have two $\mathscr{O}_S$-linear maps $\triangle$: $\mathcal{A} \to \mathcal{A} \otimes_{\mathscr{O}_S} \mathcal{A}$ and $\eta : \mathcal{A} \to \mathscr{O}_S$ satisfying identities which are obtained by dualizing the arrows in the diagrams which define a commutative algebra, *i.e.* $(\mathrm{id}_\mathcal{A} \otimes \triangle)\circ \triangle = (\triangle \otimes \mathrm{id}_\mathcal{A})\circ \triangle$ and $(\mathrm{id}_\mathcal{A} \otimes \eta)\circ \triangle = (\eta \otimes \mathrm{id}_\mathcal{A})\circ \triangle = \mathrm{id}_\mathcal{A}$.
And $\mathcal{A}$ is called *augmented* if there is an $\mathscr{O}_S$-linear map $\sigma : \mathscr{O}_S \to \mathcal{A}$.

Proposition 2.11. [4, Theorem 6.3] *Let A be a finite k-algebra over the field k. Then the following are equivalent.*
(a) $A \otimes_k k^{sep} \simeq k^{sep} \times \cdots \times k^{sep}$*;*
(b) $A \otimes_k \overline{k} \simeq \overline{k} \times \cdots \times \overline{k}$*;*
(c) $A \otimes_k \overline{k}$ *is reduced (i.e. has no nilpotents);*
(d) $\Omega^1_{A/k} = 0$*;*
(e) $\Omega^1_{A\otimes\overline{k}/k} = 0$*;*

Definition 2.12. A k-algebra A satisfying the equivalence conditions above is called an *étale algebra.*

Definition 2.13. A *finite étale group scheme* over R is a finite flat group scheme G over R which is represented by an étale R-algebra. The multiplication map $\mu : G \times G \to G$, the inverse $\mathrm{inv} : G \to G$ and the unit $\mathrm{Spec}(R) \to G$ are maps between finite étale R-schemes.

Proposition 2.14. [5, Section 3.7] *Let R be a henselian local ring, e.g. $\mathfrak{m}_R$-adically complete, and let G be a finite flat group scheme over R.*
(1) Then there is an exact sequence of finite flat group schemes over R

$$1 \to G^0 \to G \to G^{ét} \to 1$$

with G^0 the connected component of the zero section of G and $G^{ét}$ finite étale over R;
(2) Any group homomorphism $\varphi : G \to H$ to a finite étale R-group scheme H factors uniquely through $G \to G^{ét}$;
(3) Any group homomorphism $\varphi : H \to G$ from a connected R-group H factors uniquely through $G^0 \to G$.

Corollary 2.15. *A flat affine algebraic group scheme G over R is finite étale (resp. connected) if and only if the connected component G^0 (resp. the maximal étale quotient $G^{ét}$) is trivial.*

Remark 2.16. It is often easier to describe the functor represented by the group scheme than to describe a group scheme itself. In the following, we will often see S-group schemes as group functors, more precisely as fppf-sheaves. *cf* [6, Chapter 2]

Definition 2.17. If $\mathcal{M}$ is a quasi coherent $\mathscr{O}_S$-module, we denote by $\underline{\mathcal{M}}$ the fppf sheaf given by $\underline{\mathcal{M}}(S') = \Gamma(S', \mathcal{M} \otimes_{\mathscr{O}_S} \mathscr{O}'_S)$ for any $S' \in (\mathbf{Sch}/\mathrm{S})_{\mathrm{fppf}}$.

Definition 2.18. The *Cartier dual* of a group scheme G is defined by $G^{\mathsf{D}} := \mathscr{H}om_{S-\mathrm{gr}}(G, \mathbb{G}_m)$, where the "sheaf hom" $\mathscr{H}om$ is defined by $\mathscr{H}om_S(A, B)(T) = \mathrm{Hom}_T(A \times_S T, B \times_S T)$, and the subscript S-gr denotes the subsheaf morphisms of group schemes.

Proposition 2.19. [4, Theorem 2.4]
(1) If G and H are group schemes over S, then $\mathrm{Hom}_{s-\mathrm{gr}}(G^{\mathsf{D}}, H^{\mathsf{D}}) \simeq \mathrm{Hom}_{s-\mathrm{gr}}(H, G)$
(2) Cartier duality is an involution, i.e. $G \simeq (G^{\mathsf{D}})^{\mathsf{D}}$.
(3) Cartier duality commutes with base change.
(4) If the Hopf algebra of G is A, then that of G^{D} is $A^\vee = \mathrm{Hom}_R(A, R)$.

Example 2.20. We compute the Cartier dual for the three typical examples of order p.
(1) The Cartier dual of the constant group scheme $G = \underline{\mathbb{Z}/n\mathbb{Z}}$ is μ_n because in $G^{\mathsf{D}} = \mathscr{H}om(\underline{\mathbb{Z}/n\mathbb{Z}}, \mathbb{G}_m)$ the image of $1 \in \underline{\mathbb{Z}/n\mathbb{Z}}$ is mapped to an n-th root of unity. In terms of Hopf algebras, we have that G^{D} is given by the group algebra $R[\mathbb{Z}/n\mathbb{Z}] = R[X]/(X^n - 1)$ as in Example 2.9 and comultiplication, counit and antipode are as follows:

$$\triangle(X) = X \otimes X,\ \varepsilon(X) = 1,\ S(X) = X^n - 1.$$

This Hopf algebra represents μ_n.
(2) It follows that the Cartier dual of μ_n is $\underline{\mathbb{Z}/n\mathbb{Z}}$.
(3) The Cartier dual of α_p is α_p.

2.21. **The Frobenius and Verschiebung maps.**

Fix S a scheme of characteristic $p > 0$. The Frobenius $F_S : S \to S$ is the morphism of schemes which is the identity topologically and sends a section s to s^p. Consider now an S-scheme X; clearly we have also a Frobenius $F_X : X \to X$.

We define a scheme $X^{(p)}$ through the cartisian diagram:

$$\begin{tikzcd} X^{(p)} \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & X \arrow[d] \\ S \arrow[r, "F_S"] & S \end{tikzcd}$$

Note moreover that the absolute Frobenius morphism $F_S : S \to S$ and $F_X : X \to X$ commutes through the structure map $X \to S$. Therefore we deduce a map $F_{X/S} : X \to X^{(p)}$, called the *relative Frobenius*, making the following diagram commutative.

$$\begin{tikzcd} X \arrow[dr, dotted, "F_{X/S}"] \arrow[drr, bend left, "F_X"] \arrow[ddr, bend right] & & \\ & X^{(p)} \arrow[r] \arrow[d] & X \arrow[d] \\ & S \arrow[r, "F_S"] & S \end{tikzcd}$$

If X is a group scheme, then $F_{X/S} : X \to X^{(p)}$ is a morphism of group schemes. There exists a map $V_{X/S} : X^{(p)} \to X$ called the *Verschiebung*, which is also a morphism of group schemes when X is and makes the following diagrams commute:

$$\begin{tikzcd} X \arrow[d, "V_{X/S}"'] \arrow[dr, "\bullet p"] & \\ X^{(p)} \arrow[r, "F_{X/S}"'] & X \end{tikzcd}$$

$$\begin{tikzcd} & X^{(p)} \arrow[dl, "\bullet p"'] \arrow[d, "V_{X/S}"] \\ X^{(p)} & X \arrow[l, "F_{X/S}"] \end{tikzcd}$$

Remark 2.22. $V_{G/S} : G^{(p)} \to G$ is dual to $F_{G^{\mathsf{D}}/S} : G^{\mathsf{D}} \to (G^{\mathsf{D}})^{(p)} \simeq (G^{(p)})^{\mathsf{D}}$ when G is a finite commutative group scheme over S.

Example 2.23. We compute the Frobenius and Verschiebung for the three typical examples of groups of order p.
(1) The group α_p is connected and thus of finite Frobenius height. Hence the Frobenius $F : \alpha_p \to \alpha_p$ is the homomorphism 0, and by Cartier duality also the Verschiebung $V : \alpha_p \to \alpha_p$ vanishes.
(2) By the same argument the Frobenius $F : \mu_p \to \mu_p$ vanishes, and thus by Cartier duality also the Verschiebung $V : \underline{\mathbb{Z}/p\mathbb{Z}} \to \underline{\mathbb{Z}/p\mathbb{Z}}$ is the homomorphism 0.
(3) The Frobenius $F : \underline{\mathbb{Z}/p\mathbb{Z}} \to \underline{\mathbb{Z}/p\mathbb{Z}}$ is the identity map. Because on the Hopf algebra $R^{\mathbb{Z}/p\mathbb{Z}} = \oplus_{\gamma \in \mathbb{Z}/p\mathbb{Z}} R[f_\gamma]$ we have $F(f_\gamma) = f_\gamma$ for all $\gamma \in \mathbb{Z}/p\mathbb{Z}$, as given by below where the 1 in the tuple are both in the position of g.

$$\prod_{g \in \mathbb{Z}/p\mathbb{Z}} R = (\prod_{g \in \mathbb{Z}/p\mathbb{Z}} R) \otimes_{R,\varphi} R \to \prod_{g \in \mathbb{Z}/p\mathbb{Z}} R$$

$$(a_g)_{g \in G} \mapsto \sum_g (0, \dots, 1, \dots, 0) \otimes a_g \mapsto \sum_g a_g \cdot (0, \dots, 1, \dots, 0)^p = (a_g)_{g \in G}$$

Consequently, the Verschiebung $V : \mu_p \to \mu_p$ is the identity map by Cartier duality.

Proposition 2.24. [7, Section 6] *Let $R = k$ be a field and let G/k be a finite flat group.*
(1) G is étale if and only if its Frobenius $F : G \to G^{(p)}$ is an isomorphism.
(2) G is connected if and only if the Frobenius $F : G \to G^{(p)}$ is nilpotent.

Remark 2.25. We see $\underline{\mathbb{Z}/p\mathbb{Z}}$ is étale and μ_p is connected by example 2.23 and the proposition 2.24.

2.26. **Barsotti-Tate groups.**

Let p be a prime integer, S be a scheme and G be a commutative fppf sheaf of groups on S.

Lemma 2.27. [3, Chapter I, Lemma 1.1] *Assume $p^n G = 0$, then the following conditions are equivalent:*
(1) G is a flat $\mathbb{Z}/p^n\mathbb{Z}$-module;
(2) $\mathrm{Ker}(p^{n-i}) = \mathrm{Im}(p^i)$ for $i \in \{1, 2, \dots, n\}$

Definition 2.28.
If $n \geq 2$, a *truncted Barsotti-Tate group* of level n is an S-group G such that:
(1) G is a finite locally-free group scheme;
(2) G is killed by p^n and satisfies the equivalent conditions of the lemma above.

Denote by $G(n)$ the kernel of multiplication by p^n on G.

Lemma 2.29. [3, Chapter I, Lemma 1.5]
(a) If $G(n)$ is a flat $\mathbb{Z}/p^n\mathbb{Z}$-module then $G(n)$ is a finite locally free group scheme if and only if $G(1)$ is (and then all the $G(i)$ are)
(b) If $G(n)$ is finite and locally free then $p^i : G(n) \to G(n-i)$ is an epimorphism if and only if it is faithfully flat.

Definition 2.30. (Grothendieck) G is a Barsotti-Tate group if it satisfies the following three conditions:
(1) G is of p-torsion; *i.e.* $\varinjlim G(n) = G$;
(2) G is p-divisible; *i.e.* $p : G \to G$ is an epimorphism;
(3) $G(1)$ is a finite, locally-free group scheme.

Remark 2.31. Let G be a Barsotti-Tate group.
(1) $G(n) = G(n+1)(n)$
(2) for any i such that $0 \leq i \leq n$, the multiplication by p^{n-i} induces an epimorphism $G(n) \to G(i)$ (because multiplication by p^{n-i} is an epimorphism of G)
(3) from (1) and (2) and the fact that $G(1)$ is finite locally-free it follows from the lemma above that the $G(n)$ for $n \geq 2$ are truncated Barsotti-Tate groups and that we have exact sequences:

$$0 \longrightarrow G(n-i) \longrightarrow G(n) \xrightarrow{p^{n-i}} G(i) \longrightarrow 0$$

(4) it follows from theory of finite group schemes over a field that the rank of the fibre of $G(1)$ at a point $s \in S$ is of the form $p^{h(s)}$ where h is a locally constant function on S. It also follows from (3) that the rank of the fibre of $G(n)$ at s is $p^{nh(s)}$.

Definition 2.32. (Tate)[8, Section 2, (2.1)] A *p-divisible group of height h* over a commutative ring R is an inductive system $(G_n, i_n)_{i \geq 1}$ in which:

(1) G_n is a finite, commutative group scheme over R of order p^{nh};
(2) for each n, we have an exact sequence

$$0 \longrightarrow G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{p^n} G_{n+1}$$

(that is, i_n is a closed immersion and identifies G_n with the kernel of multiplication by p^n on G_{n+1}).

Starting from a Barsotti-Tate group G over $\operatorname{Spec} R$, we get a p-divisible group $(G(n), i_n)_{n\geq 1}$ over R as defined by Tate above.
Conversely, given a p-divisible group $(G_n, i_n)_{i\geq 1}$, we construct $G := \varinjlim_n G_n$, the following commutative diagram shows that G_n is the kernel of multiplication by p^n on G_{n+2} via the iterated injection $i_{n+1} \circ i_n$:

$$\begin{tikzcd}
 & & G_{n+2} \arrow[r, "p^n"] & G_{n+2} \arrow[r, "p"] & G_{n+2} \\
0 \arrow[r] & G_n \arrow[r, "i_n"] & G_{n+1} \arrow[r, "p^n"] \arrow[u, "i_{n+1}"] & G_{n+1} \arrow[u, "i_{n+1}"] &
\end{tikzcd}$$

More generally, G_n is the kernel of multiplication by p^n in G_m for all $m \geq n$, hence the kernel of multiplication by p^n in G. This implies that $G = \varinjlim_n G_n$ is p-torsion. The fact G is p-divisible and G_1 is finite and locally free can also be easily checked, *cf* [3, Chapter I, Remark 2.3].

Definition 2.33. Let $G = (G(n), i_n)_{n\geq 1}$ be a p-divisible group on S. Since $G(n)$ are finite locally free S-group schemes, the dual group schemes $G(n)^{\mathsf{D}} = \mathcal{H}om_{S-\mathrm{gr}}(G(n), \mathbb{G}_m)$ are also finite and locally free. The epimorphism $p : G(n+1) \to G(n)$ gives a monomorphism $p^{\mathsf{D}} : G(n)^{\mathsf{D}} \to G(n+1)^{\mathsf{D}}$. Then the inductive system $(G(n)^{\mathsf{D}})$ with respect to p^{D} gives p-divisible group G^{D} over S (in the Tate sense). We call G^{D} the *Cartier dual* of G.

Example 2.34.
(1) $\mu_{p^\infty} = \varinjlim_n \mu_{p^n}$, where μ_{p^n} denotes the group of p^n-th roots of unity as in example 2.9. μ_{p^∞} has height 1.
(2) $\mathbb{Q}_p/\mathbb{Z}_p = \varinjlim_n \underline{\mathbb{Z}/p^n\mathbb{Z}}$, and this is obviously the Cartier dual of μ_{p^∞} by the definition above and example 2.20. $\underline{\mathbb{Z}/p^n\mathbb{Z}}$ is the constant group scheme as in example 2.9 and hence $\mathbb{Q}_p/\mathbb{Z}_p$ also has height 1.
(3) Let A/S be an abelian scheme of dimension g. Then multiplication by p^n is an isogeny of A/S of degree p^{2gn}, hence the kernels $G_n = A[p^n]$ lead to a p-divisible group $G = A[p^\infty]$ of height $h = 2g$.

Let K be a field of characteristic 0, let $\overline{K}$ be an algebraic closure and denote $\mathscr{G}_K = \operatorname{Gal}(\overline{K}/K)$ the absolute Galois group.

Definition 2.35.
(1) Let X be a commutative group scheme, the *Tate module* of X, denoted $\mathrm{T}_p(X)$ is

$$\mathrm{T}_p(X) = \varprojlim_n (\operatorname{Ker}(X(\overline{K}) \xrightarrow{p^n} X(\overline{K})))$$

(2) If $G = \varinjlim_n G_n$ is a p-divisible group, then the *Tate module* of G, denoted $\mathrm{T}_p(G)$ is $\mathrm{T}_p(G) = \varprojlim_n G_n(\overline{K})$.

Remark 2.36.
(1) The inverse limit is taken over positive integers n with transitive morphisms given by multiplication by p: $X(\overline{K})[p^{n+1}] \to X(\overline{K})[p^n]$, where $X(\overline{K})[p^n]$ denotes

$\mathrm{Ker}(X(\overline{K}) \xrightarrow{p^n} X(\overline{K}))$.
(2) There is another way to see Tate module

$$\begin{aligned}
\mathrm{T}_p(G) &= \varprojlim_n G_n(\overline{K}) \\
&= \varprojlim_n \mathrm{Hom}_{\mathrm{gr}}(\mathbb{Z}/p^n\mathbb{Z}, G_n(\overline{K})) \\
&= \varprojlim_n \mathrm{Hom}_{\mathrm{gr}}(\mathbb{Z}/p^n\mathbb{Z}, G(\overline{K})) \\
&= \mathrm{Hom}_{\mathrm{gr}}(\mathbb{Q}_p/\mathbb{Z}_p, G(\overline{K}))
\end{aligned}$$

(3)Assume K is a discrete valuation field with ring of integer $\mathcal{O}_K$ and $G \in \mathbf{BT}(\mathcal{O}_K)$. If $n \in \mathbb{N}_{>0}$, and L/K is finite, then $G_n(L) = G_n(\mathcal{O}_L)$ by the valuative criterion of properness (recall that G_n is finite over $\mathcal{O}_K$). Taking inductive limit we get

$$G_n(\overline{K}) = G_n(\mathcal{O}_{\overline{K}}) = \mathrm{Hom}_{\mathcal{O}_{\overline{K}}-\mathrm{gr}}(\underline{\mathbb{Z}/p^n\mathbb{Z}}, G_n \otimes \mathcal{O}_{\overline{K}})$$

Taking inverse limit, we deduce

$$\begin{aligned}
\mathrm{T}_p(G) &= \varprojlim G_n(\overline{K}) \\
&= \varprojlim \mathrm{Hom}_{\mathcal{O}_{\overline{K}}-\mathrm{gr}}(\underline{\mathbb{Z}/p^n\mathbb{Z}}, G_n \otimes \mathcal{O}_{\overline{K}}) \\
&= \varprojlim \mathrm{Hom}_{\mathcal{O}_{\overline{K}}-\mathrm{gr}}(\underline{\mathbb{Z}/p^n\mathbb{Z}}, G \otimes \mathcal{O}_{\overline{K}}) \\
&\simeq \mathrm{Hom}_{\mathbf{BT}(\mathcal{O}_{\overline{K}})}(\mathbb{Q}_p/\mathbb{Z}_p, G \otimes \mathcal{O}_{\overline{K}})
\end{aligned}$$

2.37. **Formal Lie groups.**

We establish some relations between Barsotti-Tate groups and formal Lie group. Let X, Y be sheaves of groups over S such that Y is a subsheaf of X. We define for every $k \geq 0$ a subsheaf $\mathrm{Inf}^k_Y(X)$ of X.

Definition 2.38. For each integer $k \geqslant 0$, the k^{st} *infinitesimal neighborhood* of Y in X, denoted $\mathrm{Inf}^k_Y(X)$, is the subsheaf of X whose sections over an S-scheme T are given as follows: $\Gamma(T, \mathrm{Inf}^k_Y(X)) = \{t \in \Gamma(T, X)|$ there is a covering $T_i \to T$ and for each T_i a closed subscheme $T_i^{'}$ defined by an ideal whose $k+1^{st}$ power is (0) with the property that $t_{T_i^{'}} \in \Gamma(T_i^{'}, X)$ is actually an element of $\Gamma(T_i^{'}, Y)\}$

Definition 2.39. A pointed sheaf (X, e_X) over S is said to be a *formal Lie variety* if :
(1) $X = \varinjlim_k \mathrm{Inf}^k_S(X)$ and the $\mathrm{Inf}^k_S(X)$ are representable for every $k \geq 0$;
(2) $e_x^*\Omega^1_{X/S} = e_x^*\Omega^1_{\mathrm{Inf}^k_S(X)/S}$ is locally free of finite type;
(3) denoting by $\mathrm{gr}^{\mathrm{inf}}(X)$ the unique graded $\mathscr{O}_S$-algebra such that $\mathrm{gr}^{\mathrm{inf}}_i(X) = \mathrm{gr}_i(\mathrm{Inf}^i_S(X))$ holds for all $i \geq 0$, we have an isomorphism $\mathrm{Sym}(\omega_X) \to \mathrm{gr}^{\mathrm{inf}}(X)$ induced by the canonical mapping $\omega_X \to \mathrm{gr}^{\mathrm{inf}}_1(X)$.

Definition 2.40. A *formal Lie group* (G, e_G) over S is a group in the category of formal Lie varieties.

Now we give a characterization of formal Lie group in the case the base scheme S is of characteristic $p > 0$. Let G be a sheaf of groups over S. We have Frobenius and Verschiebung morphisms:

$$F_{G/S} : G \to G^{(p)}$$

and

$$V_{G/S} : G^{(p)} \to G$$

We denote by $G[n]$ the kernel of the n-th iterate $(F_{G/S})^n$.

Definition 2.41. We say that G is of $F_{G/S}$*-torsion* if $G = \varinjlim_n G[n]$. We say that G is $F_{G/S}$-divisible if $F_{G/S}$ is surjective.

Theorem 2.42. [3, chapter II, Theorem 2.1.7] *Notations as above, G is a formal Lie group if and only if:*
(1) G is of $F_{G/S}$-torsion;
(2) G is $F_{G/S}$-divisible;
(3) the $G[n]$ are finite and locally free S-group schemes.

Notation 2.43. $\bar{G} = \varinjlim_k \mathrm{Inf}_S^k(G)$

Theorem 2.44. [3, Chapter II, Theorem 3.3.18] *Suppose p is locally nilpotent on S and G is a Barsotti-Tate group, then $\bar{G}$ is a formal Lie group.*

There is another way to define a formal Lie group and one can check these two definitions are compatible.

Definition 2.45. Let R be a complete, noetherian, local ring with residue field k of characteristic $p > 0$. An *n-dimensional commutative formal Lie group over R*, denoted $\Gamma = \mathrm{Spf}(R[[x_1, \ldots, x_n]])$, is $F = (F_i \in R[[z_1, \ldots, z_n, y_1, \ldots, y_n]])_{i=1}^n$ satisfying:
(1) $X = F(X, 0) = F(0, X)$;
(2) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;
(3) $F(X, Y) = F(Y, X)$.

We write $X * Y = F(X, Y)$. It follows from the axiom that $X * Y = X + Y +$ trems in higher powers of the variables. Put $\psi(X) = X * \cdots * X$ (p times) and denote $[p]$ the corresponding map on Γ. We say Γ is *p-divisible* if $[p] : \Gamma \to \Gamma$ is an isogeny, *i.e.* $R[[x_1, ..., x_n]]$ is free of finite rank over itself with respect to ψ. If Γ is p-divisible, then for $v \in \mathbb{N}$, the scheme

$$G_v = \mathrm{Spec}(R[[x_1, ..., x_n]]/\psi^v(< x_1, \ldots, x_n >))$$

is a connected group scheme over R. We get a p-divisible group $\Gamma(p) = (G_v, i_v)_{v \geq 1}$.

Theorem 2.46. [8, Proposition 1] ($Tate$) *Given R as above, the map $\Gamma \to \Gamma(p)$ is an equivalence of categories between p-divisible commutative formal Lie groups over R and connected p-divisible groups over R.*

Definition 2.47. Given a p-divisible group G, the *dimension of G* is defined to be the dimension of the formal Lie group corresponding to the connected component G^0.

Remark 2.48. We can define the dimension in a more simple way in the next subsection, refering to Remark 2.66.

2.49. **The relation between Lie algebra and the sheaf of invariant differentials of a Barsotti-Tate group.**

Let X be an affine group over a complete noetherian local ring R, and let $R[\varepsilon]$ be the ring of *dual numbers*:

$$R[\varepsilon] := R[T]/(T^2)$$

Thus $R[\varepsilon] = R \oplus R\varepsilon$ and $\varepsilon^2 = 0$. There is a homomorphism

$$\pi : R[\varepsilon] \to R, \quad \pi(a + \varepsilon b) = a.$$

Definition 2.50. For any affine group scheme X over R,

$$\operatorname{Lie} X := \operatorname{Ker}(X(R[\varepsilon]) \xrightarrow{\pi} X(R))$$

Remark 2.51. Same notation as above, since we have exact sequence

$$1 \to X^0 \to X \to X^{\acute{e}t} \to 1$$

by Proposition 2.14. Taking Lie is like taking the derivative, hence kills $X^{\acute{e}t}$ by Proposition 2.11. We concludes that $\operatorname{Lie}(X^0) \simeq \operatorname{Lie} X$.
In particular, when R is a field we have the following computation: If $a \neq 0$, then $a + b\varepsilon = a(1 + \frac{b}{a}\varepsilon)$ has inverse $a^{-1}(1 - \frac{b}{a}\varepsilon)$ in $R[\varepsilon]$, and so

$$R[\varepsilon]^{\times} = \{a + b\varepsilon | a \neq 0\}$$

An element of $\operatorname{Lie}(X)$ is a R-algebra homomorphism $u : \mathscr{O}(X) \to R[\varepsilon]$ whose composite with $\varepsilon \to 0$ is ϵ. Therefore, elements of $\mathscr{O}(X)$ not in the kernel $\mathfrak{m}$ of ϵ map to units in $R[\varepsilon]$, and so u factors uniquely through the local ring $\mathscr{O}(X)_{\mathfrak{m}}$. This shows that $\operatorname{Lie} X$ depends only on $\mathscr{O}(X)_{\mathfrak{m}}$. In particular, $\operatorname{Lie}(X^0) \simeq \operatorname{Lie} X$.

Recall that $\mathscr{O}(X)$ has a co-algebra structure $(\triangle, \epsilon)$. By definition, the elements of $\operatorname{Lie}(X)$ are the R-algebra homomorphisms $\mathscr{O}(X) \to R[\varepsilon]$ such that the composite

$$\mathscr{O}(X) \xrightarrow{u} R[\varepsilon] \xrightarrow{\varepsilon \mapsto 0} R$$

is ϵ.

Proposition 2.52. *There is a natural one-to-one correspondence between the elements of* $\operatorname{Lie}(X)$ *and the R-derivations $\mathscr{O}(X) \to R$ (where $\mathscr{O}(X)$ acts on R through ϵ), i.e.*

$$\operatorname{Lie}(X) \simeq \operatorname{Der}_{R,\epsilon}(\mathscr{O}(X), R)$$

The correspondence is $\epsilon + \varepsilon D \leftrightarrow D$, and the Leibniz condition is

$$\mathrm{D}(fg) = \epsilon(f) \cdot D(g) + \epsilon(g) \cdot D(f)$$

Example 2.53. Suppose R is a field of characteristic $p > 0$, and let $X = \alpha_p$, so that $\alpha_p(B) = \{b \in B | b^p = 0\}$. Then $\alpha_p(R) = \{0\}$ and $\alpha_p(R[\varepsilon]) = \{a\varepsilon | a \in R\}$. Therefore,

$$\operatorname{Lie}(\alpha_p) = \{a\varepsilon | a \in R\} \simeq R;$$

Similarly,

$$\operatorname{Lie}(\mu_p) = \{1 + a\varepsilon | a \in R\} \simeq R.$$

Let $\mathcal{A}$ be an augmented quasi-coherent co-algebra in $(\mathbf{Sch}/\mathrm{S})_{\mathrm{fppf}}$.

Definition 2.54. [3, Chapter III, (2.0)] $\operatorname{Cospec}(\mathcal{A})$ is the functor $(\mathbf{Sch}/\mathrm{S})^{\circ} \to \mathbf{Set}$ given by $S^{'} \mapsto \{y \in \Gamma(S^{'}, \mathcal{A}_{S'}) | \eta(y) = 1, \triangle\,(y) = y \otimes y\}$.

Definition 2.55. A section x of $\mathcal{A}$ is *primitive* if $\triangle\,(x) = 1 \otimes x + x \otimes 1$

Definition 2.56. We denote by $\underline{\operatorname{Lie}}(\mathcal{A})$ the fppf sheaf of $\mathscr{O}_S$-module whose sections over $S^{'}$ are the primitive elements in $\Gamma(S^{'}, \mathcal{A}_{S'})$ and where the operations are induced by those on $\mathcal{A}$. By abuse of notation, if $G = \operatorname{Cospec}(\mathcal{A})$, then $\underline{\operatorname{Lie}}(\mathcal{A})$ is also denoted $\underline{\operatorname{Lie}}(G)$.

Remark 2.57. Assume $\mathcal{A}$ is finite and locally-free, then $\operatorname{Cospec}(\mathcal{A}) = \operatorname{Spec}(\mathcal{A}^{\vee})$, where $\mathcal{A}^{\vee} = \operatorname{Hom}_{\mathscr{O}_S\text{-mod}}(\mathcal{A}, \mathscr{O}_S)$

The $\mathscr{O}_S$-algebra structure on $\mathcal{A}^\vee = \mathrm{Hom}_{\mathscr{O}_S\text{-mod}}(\mathcal{A}, \mathscr{O}_S)$ is given as follows. The unit is $\mathscr{O}_S \xrightarrow{\eta^\vee} \mathcal{A}^\vee$ and the multiplication is given by $(\mathcal{A} \otimes_{\mathscr{O}_S} \mathcal{A})^\vee \simeq \mathcal{A}^\vee \otimes_{\mathscr{O}_S} \mathcal{A}^\vee \xrightarrow{m=\Delta^\vee} \mathcal{A}^\vee$, where the first isomorphism comes from the fact that $\mathcal{A}$ is finite and locally free.
By [3, chapter3 2.1.3], any Barsotti-Tate group can be written as $\mathrm{Cospec}(\mathcal{A}) = \mathrm{Spec}(\mathcal{A}^\vee)$ for an appropriate co-algebra $\mathcal{A}$. Now given a Barsotti-Tate group, say $G = \mathrm{Cospec}(\mathcal{A}) = \mathrm{Spec}(\mathcal{A}^\vee)$ over S, then the unit section $S \to G$ is deduced from the augmentation map.

Definition 2.58. If (X, e) is a pointed S-scheme (*i.e.* $e : S \to X$ is a section of the structure map), then we define the *sheaf of invariant differentials*, denoted $\underline{\omega}_{X/S}$, to be the fppf sheaf associated to the Zariski sheaf below:

$$\omega_{X/S} = e^*(\Omega^1_{X/S})$$

When X is a group scheme, e is just the unit section $S \hookrightarrow X$.

Remark 2.59. We see that $\mathrm{Lie}\, X = \omega^\vee_{X/S}$. Since Proposition 2.52 tells us $\mathrm{Lie}\, X$ corresponds to the invariant derivation, *i.e.* the tanget space of the origin.

Proposition 2.60. [3, Chapter II, Remark 3.3.20] *Let G be a Barsotti-Tate group over S, then the sheaves $\underline{\omega}_{G(m)/S}$ are locally free of finite rank. If $p^N \cdot 1_S = 0$, then $\underline{\omega}_{G(m)/S} = \underline{\omega}_{G(N)/S}$ for all $m \geq N$.*

Definition 2.61. Let G be a Barsotti-Tate group on the base scheme S, then we define the *sheaf of invariant differentials* by

$$\underline{\omega}_{G/S} = \underline{\omega}_{G(m)/S}$$

for $m \gg 0$.

Remark 2.62.
(1) Under the same assumption as Proposition 2.59 above, Proposition 2.58 implies that we can define $\mathrm{Lie}\, G$ similarly. $\mathrm{Lie}\, G := \mathrm{Lie}\, G(m)$ for $m \gg 0$.
(2) Suppose that $G \in \mathbf{BT}(S)$, then one can check $(\underline{\mathrm{Lie}}\, G)(S) = \mathrm{Lie}\, G$. In fact, one can take this as the definition of $\mathrm{Lie}\, G$ at the beginning.

Remark 2.63. $\underline{\omega}_G = \underline{\omega}_{\overline{G}}$

Lemma 2.64. *Let $\mathcal{A}$ be a finite locally free co-algebra over S, $X = \mathrm{Cospec}\, \mathcal{A} = \mathrm{Spec}(\mathcal{A}^\vee)$. Then $\underline{\mathrm{Lie}}(X) = \underline{\omega}^\vee_{X/S}$*

Proof. Given any S-scheme S', we have $\underline{\omega}^\vee_{X/S}(S') = \Gamma(S', \omega^\vee_{X/S} \otimes_{\mathscr{O}_S} \mathscr{O}_{S'})$. Now we focus on the sheaf, which is easier to study since we can study it locally.

$$
\begin{aligned}
&\omega^{\vee}_{X/S} \otimes_{\mathscr{O}_S} \mathscr{O}_{S'} \\
&= \mathrm{Hom}_{\mathscr{O}_S}(\omega_{X/S}, \mathscr{O}_{S'}) \\
&= \mathrm{Hom}_{\mathscr{O}_{S'}}(\mathscr{O}_{S'} \otimes_{\mathscr{O}_S} \omega_{X/S}, \mathscr{O}_{S'}) \\
&= \mathrm{Hom}_{\mathscr{O}_{S'}}(\omega_{X'/S'}, \mathscr{O}_{S'}) \\
&= \mathrm{Hom}_{\mathscr{O}_{S'}}(\mathscr{O}_{S'} \otimes_{\mathscr{O}_{X_S}} \Omega_{X_S/S}, \mathscr{O}_{S'}) \\
&= \mathrm{Hom}_{\mathscr{O}_{S'}}(\Omega_{X_{S'}/S'}, \mathscr{O}_{S'}) \\
&= \mathrm{Der}_{\mathscr{O}_{S'}}(\mathscr{O}_{X_{S'}}, \mathscr{O}_{S'}) \\
&= \mathrm{Der}_{\mathscr{O}_{S'}}(\mathcal{A}^{\vee}_{S'}, \mathscr{O}_{S'}) \\
&= \{d \in \mathrm{Hom}_{\mathscr{O}_{S'}}(\mathcal{A}^{\vee}_{S'}, \mathscr{O}_{S'})(= \mathcal{A}_{S'}) | (\forall x, y \in \mathcal{A}^{\vee}_{S'}) d(xy) = xd(y) + yd(x)\} \\
&= \{a \in \mathcal{A}_{S'} | (\forall x, y \in \mathcal{A}^{\vee}_{S'})(x \otimes y)(\triangle\ (a)) = (x \otimes y)(1 \otimes a) + (x \otimes y)(a \otimes 1)\} \\
&= \{a \in \mathcal{A}_{S'} |\ \triangle\ (a) = 1 \otimes a + a \otimes 1.\}
\end{aligned}
$$

So

$$\underline{\omega}^{\vee}_{X/S}(S^{'}) = \underline{\mathrm{Lie}}(\mathcal{A})(S^{'}) = \underline{\mathrm{Lie}}(X)(S^{'})$$

□

Proposition 2.65. *If* $G = \mathrm{Cospec}(\mathcal{A})$ *is a Barsotti-Tate group over* S*, then* $\underline{\mathrm{Lie}}(G) = \underline{\omega}^{\vee}_{G/S}$.

Proof. By the lemma above, we know that $\underline{\mathrm{Lie}}(G(m)) = \underline{\omega}_{G(m)/S}$. By proposition 2.60 $\underline{\omega}_{G(m)/S}$ stablizes, hence we see $\varinjlim \underline{\omega}_{G(m)/S} = \underline{\omega}_{G/S}$. So together with $\underline{\mathrm{Lie}}(G) = \underline{\mathrm{Lie}}(\varinjlim G(m))$, we see it suffices to show $\varinjlim \underline{\mathrm{Lie}}(G(m)) = \underline{\mathrm{Lie}}(\varinjlim G(m))$, which follows directly by the definition of $\underline{\mathrm{Lie}}(\mathcal{A})$ above described by sections. □

Remark 2.66.
(1) By definition, $\underline{\mathrm{Lie}}(G)$ coincides with the fppf sheaf corresponds to the usual Lie algebra of a Lie group when G is a Lie group. Indeed, given a Lie group G, its Lie algebra is the tangent space at the origin, denoted t_eG. It consists of the derivations Der, hence corresponds to $\omega^{\vee}_G$. By the lemma above, $\underline{\mathrm{Lie}}(G) = \underline{\omega}^{\vee}_G$.
(2) By Proposition 2.11 and discussion above, we see that $\underline{\mathrm{Lie}}(G) = 0$ if G is an étale group scheme.
(3) We can replace Definition 2.47 by defining the dimension of a p-divisible group $G \in \mathbf{BT}(\mathcal{O}_K)$ as the rank of the free module ω_G. Moreover by the fully-faithfulness of the generic fiber, *cf* Theorem 6.48 to be proved later, the rank is the same as the rank of the vector space $G \otimes_{\mathcal{O}_K} K$, where $K = \mathrm{Frac}(\mathcal{O}_K)$.

3. Divided powers, exponentials and crystals

3.1. **Divided powers.**

The notion of divided power on a commutative ring A is defined to "make sense" of $\dfrac{x^n}{n!}$ for some element $x \in A$, even when $n!$ is not invertible in A. This will enable us to define exponential maps. The exponential will involve sheaves of Lie algebra and play an important role in the classification of Barsotti-Tate groups over some fixed base scheme.

Definition 3.2. Let A be a ring and I an ideal of A. A *divided power structure* on I is a family of mappings $\{\gamma_n : I \to I, n \geq 1\}$ which satisfies the following conditions for any $\lambda \in A$ and $x, y \in I$:
(1)$\gamma_n(\lambda x) = \lambda^n \gamma_n(x)$;
(2) $\gamma_n(x) \cdot \gamma_m(x) = \dfrac{(m+n)!}{m!n!}\gamma_{m+n}(x)$;
(3) $\gamma_n(x+y) = \gamma_n(x) + \sum_{i=1,n-1} \gamma_{n-i}(x)\gamma_i(y) + \gamma_n(y)$;
(4) $\gamma_m(\gamma_n(x)) = \dfrac{(mn!)}{(n!)^m m!}\gamma_{mn}(x)$.

Given such a system we define γ_0 by $\gamma_0(x) = 1$ for all $x \in I$ and refer to (I, γ) as an *ideal with divided powers.* If $x \in I$, the element $\gamma_n(x)$ is sometimes denoted $x^{[n]}$. The structure (A, I, γ) as above is called a *P.D. ring.*

Remark 3.3.
(1) If A is a $\mathbb{Q}$-algebra, then any ideal has a unique P.D. structure, namely $\gamma_n(x) = \dfrac{x^n}{n!}$, for all $x \in A$.
(2) When A has characteristic 0, if the P.D. structure exists then it is unique. Besides the above example, consider a DVR (A, π, k) of mixed characteristic $(0, p)$, $p = \pi^e u$, where $u \in A^\times$. Then (π) admits a P.D. structure if and only if $e \leq p - 1$. Hence the ring of Witt vectors of a perfect field of characteristic p admits a P.D. structure, since it is an unramified DVR of characteristic $(0, p)$.
(3) In the positive characteristic case P.D. structures may not be unique when it exists.

Definition 3.4. Let (A, I, γ) and (B, J, δ) be triples with P.D. structures. A *morphism of P.D. rings* or *P.D. morphism* $u : (A, I, \gamma) \to (B, J, \delta)$ is a ring homomorphism $u : A \to B$ such that $u(I) \subseteq J$ and $u(\gamma_n(x)) = \delta_n(u(x))$ holds for all $x \in I$ and $n \in \mathbb{N}$.

We globalize considerations above by defining *P.D. schemes* as follows. We replace A by a scheme S, I by a quasi-coherent ideal $\mathcal{I}$. Divided powers on $\mathcal{I}$ are given by assigning to each open set U a system of divided powers on $\Gamma(U, I)$ such that the restriction maps commute with the divided powers.
Given P.D. schemes $(S, \mathcal{I}, \gamma)$ and $(S^{'}, \mathcal{I}^{'}, \gamma^{'})$, a divided power morphism f between them is a morphism of schemes $f : S \to S^{'}$ such that $f^{-1}(\mathcal{I}^{'})$ maps into $\mathcal{I}$ under the map $f^{-1}(\mathscr{O}_{S'}) \to \mathscr{O}_S$ and such that the divided powers induced on the image of $f^{-1}(\mathcal{I}^{'})$ coincide with those defined on $\gamma^{'}$.

Definition 3.5. Let (A, I, γ) be a P.D. ring and $f\colon A \to B$ be an A-algebra. We say that γ *extends to* B if there is a P.D. structure $(B, IB, \overline{\gamma})$ such that $(A, I, \gamma) \to (B, IB, \overline{\gamma})$ is a P.D. morphism, that is $f(\gamma_n(x)) = \overline{\gamma}_n(f(x))$ for every $x \in I$, $n \in \mathbb{N}$

Remark 3.6. In fact the definition is equivalent to the following statement: there is a P.D. structure (J, δ) on B with a P.D. morphism $(A, I, \gamma) \to (B, J, \delta)$, indeed IB is a sub-P.D. ideal of J.

Definition 3.7. Let (A, I, γ) be a P.D. ring and B an A-algebra with a P.D. structure (J, δ). We say that γ and δ are *compatible* if the following equivalent conditions hold:
(1) γ extends to δ and $\overline{\gamma} = \delta$ on $IB \cap J$;
(2) the ideal $K = IB + J$ has a P.D. structure $\overline{\delta}$ such that $(A, I, \gamma) \to (B, K, \overline{\delta})$ and $(B, J, \delta) \to (B, K, \overline{\delta})$ are P.D. morphisms.

3.8. **P.D. envelopes.**

Theorem 3.9. [9, Theorem 3.19]
Let (A, I, γ) be a P.D. algebra, B is an A-algebra and J is an ideal of B. There exists a B-algebra $\mathcal{D}_{B,\gamma}(J)$ with a P.D. ideal $(\overline{J}, \theta)$ such that $J\mathcal{D}_{B,\gamma}(J) \subseteq \overline{J}$ and satisfies the following universal property: for any B-algebra C with a P.D. ideal (K, δ) such that K contains the image of J and δ is compatible with the γ there exists a unique P.D. morphism $(\mathcal{D}_{B,\gamma}(J), \overline{J}, \theta) \to (C, K, \delta)$ such that the following diagram commutes:

$$\begin{tikzcd}
& (\mathcal{D}_{B,\gamma}(J), \overline{J}, \theta) \arrow[dr, dotted] & \\
(B, J) \arrow[ur, "\psi"] \arrow[rr] & & (C, K, \delta) \\
& (A, I, \gamma) \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Definition 3.10. The B-algebra $\mathcal{D}_{B,\gamma}(J)$ in the above theorem is called the *P.D. envelope* of B relative to the ideal J.

3.11. **Exponentials.**

Definition 3.12.
Let (A, I, γ) be a P.D. ring. We say that the divided powers are *nilpotent* if there is an integer N such that the ideal generated by elements of the form $\gamma_{i_1}(x_1) \cdots \gamma_{i_k}(x_k)$ with $i_1 + \cdots + i_k \geq N$ is zero.

Remark 3.13. The definition implies, by taking $k = N$ and $i_1 = \cdots = i_k = 1$, that $I^N = (0)$. This enables us to define exponential.

Definition 3.14. If the divided powers (A, I, γ) are nilpotent we define two maps:

$$\exp : I \to (1 + I)^\times$$
$$\log : (1 + I)^\times \to I$$

by the formula $\exp(x) = \sum_{n \geq 0} \gamma_n(x)$ and $\log(1 + x) = \sum_{n \geq 1} (-1)^{n-1}(n-1)!\gamma_n(x)$

Remark 3.15. The two maps are well defined and inverse to each other.

Let $S = \mathrm{Spec}(A)$ be an affine scheme where p is nilpotent, I an ideal of A with nilpotent divided powers and $S_0 = \mathrm{Spec}(A/I)$. For any Barsotti-Tate group G over S and V a locally-free A-module of finite rank, there is a well-defined exponential map:

$$\exp : \mathrm{Hom}(V, I \cdot \underline{\mathrm{Lie}}(G)) \hookrightarrow \mathrm{Ker}[\mathrm{Hom}_{S-\mathrm{gr}}(V, G) \to \mathrm{Hom}_{S_0-\mathrm{gr}}(V_0, G_0)]$$

defined by $\exp(\theta)(x) = \exp(\theta(x))$.

We study extensions of homomorphisms and the relations between these and the exponential.
Assume $u_0 : V_0 \to G_0$ is a S_0-monomorphism with image $H_0 \subseteq G_0$, we want to examine the set of S-flat liftings of H_0 to subgroups H of G, together with structure of locally-free module on H, lifting that of H_0. Let H be a solution of this problem. Then H is given by V where V is a finite locally-free $\mathscr{O}_S$-module and any such V

is determined up to isomorphism by [S.G.A 1 III.7.1]. Let us fix once and for all a V lifting V_0. Then to give an H as above is equivalent to giving a monomorphism $V \to G$ lifting u_0, and two such u and $u^{'}$ are being identified if they differ by an $\mathscr{O}_S$-automorphism of V which restricts to the identity on S_0

Definition 3.16. Notations as above, the subtitle "0" of a group scheme over S denotes its base change over S_0. Two liftings $u^{'}, u^{''}$ of $u_0 : V_0 \to G_0$ are said *linearly compatible* if their difference is in the image of

$$\exp : \mathrm{Hom}(V, I \cdot \underline{\mathrm{Lie}}(G)) \hookrightarrow \mathrm{Ker}[\mathrm{Hom}(V, G) \to \mathrm{Hom}(V_0, G_0)]$$

Remark 3.17. This is obviously an equivalence relation on the set of liftings of u_0.

Definition 3.18. Two liftings $u^{'}, u^{''}$ of $u_0 : V_0 \to G_0$ are said to be *congruent* if they differ by an $\mathscr{O}_S$-linear automorphism of V reducing to the identity on V_0

Remark 3.19. u and $u^{'}$ are thus congruent if and only if they define the same solution of our lifting problem.

Lemma 3.20. [3, Chapter III, 2.7.6] *If u and $u^{'}$ are congruent then they are linearly compatible.*

Remark 3.21. Hence we see u and $u^{'}$ are congruent if and only if they are linearly compatible, since obviously linearly equivalence implies congruence. Hence the exponential map allows us to define an equivalence relation on the set of solutions of our problem.

Let $\underline{h} \subseteq \underline{\mathrm{Lie}}(G)$ be a locally free sub-module lifting $\underline{h}_0 = \underline{\mathrm{Lie}}(H_0)$, then we have the following result which is important for the Grothendieck-Messing theorem later.

Proposition 3.22. [3, Chapter III, 2.7.7] *In each linear equivalence class of solutions of our problem, there is exactly one H with $\underline{\mathrm{Lie}}(H) = \underline{h}$*

3.23. **Crystalline site and crystals.**

Let $S = (S, \mathcal{I}, \delta)$ be a P.D. scheme, X is a S-scheme to which δ extends. Recall this means that the $\mathscr{O}_S$-algebra $\mathscr{O}_X$ has a P.D. structure $\overline{\delta}$ such that

$$(\mathscr{O}_S, \mathcal{I}, \delta) \to (\mathscr{O}_X, \mathcal{I}\mathscr{O}_X, \overline{\delta})$$

is a P.D. morphism.

Definition 3.24. The *crystalline site of X relative to S*, denoted $\mathrm{Crys}(X/S)$, consists of the category whose objects are triples $(U \hookrightarrow T, \gamma)$ where:
(1) U is an open sub-scheme of X;
(2) $U \hookrightarrow T$ is a locally nilpotent closed immersion;
(3) $\gamma = (\gamma_n)_{n\in\mathbb{N}}$ is a (locally nilpotent) divided powers structure on the ideal $\mathcal{I}$ of U in T compatible with δ.
$U \hookrightarrow T$ as above is called a *P.D. thickening.*
Morphisms from $(U \hookrightarrow T)$ to $(U' \hookrightarrow T')$ are commutative diagrams:

$$\begin{tikzcd} U \arrow[r] \arrow[d, "f"'] & T \arrow[d, "\overline{f}"] \\ U' \arrow[r] & T' \end{tikzcd}$$

such that $U \to U'$ is an inclusion and $T \xrightarrow{\overline{f}} T'$ is a divided power morphism (*i.e.* the morphism of sheaf of rings $\overline{f}^{-1}(\mathscr{O}_{T'}) \to \mathscr{O}_T$ is a divided power morphism).
A covering family of an object $(U \hookrightarrow T, \gamma)$ of the crystalline site is a collection of morphisms $\{T_i \to T\}_i$ such that for all $i \in I$, $T_i \to T$ is an open immersion and $\cup T_i = T$. One may instead require $\cup U_i = U$, actually the working assumption implies that the ideal $\mathcal{I}$ is nilpotent and therefore $U \hookrightarrow T$ is a homeomorphism.

A sheaf of sets $\mathcal{F}$ on the crystalline site is equivalent to the following data: for every element $(U, T, \gamma) \in \mathrm{Crys}(X/S)$, a sheaf $\mathcal{F}_{(U,T,\gamma)}$ on T and for every morphism in the crystalline site

$$\begin{tikzcd} U \arrow[r] \arrow[d, "f"'] & T \arrow[d, "\overline{f}"] \\ U' \arrow[r] & T' \end{tikzcd}$$

a morphism of sheaves $\overline{f}^{-1}\mathcal{F}_{(U,T,\gamma)} \to \mathcal{F}_{(U',T',\gamma')}$, where $\overline{f}^{-1}$ is the pull-back of a sheaf of sets on T_{Zar}, together with the natural cocycle condition.

Example 3.25. The *structural sheaf* $\mathscr{O}_{X/S}$ on $\mathrm{Crys}(X/S)$ is defined by

$$(\mathscr{O}_{X/S})_{(U,T,\gamma)} = \mathscr{O}_T$$

for every (U, T, γ).

Definition 3.26. A *crystal* of $\mathscr{O}_{X/S}$-modules is a sheaf $\mathcal{F}$ of $\mathscr{O}_{X/S}$-modules such that for any morphism u: $(U \hookrightarrow T) \to (U^{'} \hookrightarrow T^{'})$ in $\mathrm{Crys}(X/S)$, the map $u^*\mathcal{F}_{(U',T',\delta')} \to \mathcal{F}_{(U,T,\delta)}$ is an isomorphism.

Example 3.27. The structural sheaf $\mathscr{O}_{X/S}$ on $\mathrm{Crys}(X/S)$ is a crystal.

Crystal is a sheaf that is "rigid" and "grows". The growing is true for any sheaf $\mathcal{F}$ on a crystalline site $\mathrm{Crys}(X/S)$, allowing us to associate a crystal to any lifting of a Barsotti-Tate group in our case. While the rigidity, precised by the isomorphism in the definition above, is not true for arbitrary sheaf.

4. Deformation theory

4.1. **The crystals associated to Barsotti-Tate groups.**

In this section we shall associate certain crystals to Barsotti-Tate groups on a scheme (on which p is locally nilpotent).

Let S be a scheme on which p^N is zero and G a Barsotti-Tate group on S. Recall that we have defined in the first section the sheaf of invariant differentials $\underline{\omega}_G$, namely the fppf sheaf associated to $\omega_G = e^*(\Omega^1_{G(m)/S})$ where $m \gg 0$ and e is the unit section $S \to G(m)$.

Definition 4.2. An extension of G by a vector group $\underline{V}(G)$ (*i.e.* an fppf sheaf associated to a quasi-coherent module)

$$\text{(E)}\ \ 0 \to \underline{V}(G) \to E(G) \to G \to 0$$

is said to be *universal* if given any extension of G by another vector group

$$0 \to M \to \bullet \to G \to 0$$

there is a unique linear map $\underline{V}(G) \xrightarrow{f} M$ such that $f_*((E))$ is the given extension.

Proposition 4.3. [3, Chapter IV, Proposition 1.10] *Notations as above, there is an universal extension of G by a vector group. In fact $\underline{V}(G) = \underline{\omega}_{(G(n)^{\mathrm{D}})}$ for n sufficiently large and the universal extension is*

$$0 \to \underline{\omega}_{(G(N)^{\mathrm{D}})} \to \underline{\omega}_{(G(N)^{\mathrm{D}})} \coprod_{G(N)} G \to G \to 0$$

up to isomorphism.

Proof. Consider the exact sequence

$$0 \to G(N) \to G \xrightarrow{p^N} G \to 0$$

Take M a quasi-coherent module and apply the left exact functor $\mathrm{Hom}(\bullet, M)$. We get the long exact sequence:

$$0 \to \mathrm{Hom}(G, M) \to \mathrm{Hom}(G, M) \to \mathrm{Hom}(G(N), M) \xrightarrow{\delta} \mathrm{Ext}^1(G, M) \to \mathrm{Ext}^1(G, M)$$

Since $p^N = 0$ on M, we get an isomorphism $\mathrm{Hom}(G(N), M) \xrightarrow{\delta} \mathrm{Ext}^1(G, M)$, which is functorial in M. *cf* [3, Chapter IV, Proposition 1.3], the left hand side functor is represented by $\underline{\omega}_{(G(N)^{\mathrm{D}})}$. Then again *cf* [3, Chapter IV, proposition 1.3] we have a homomorphism α inducing the universal extension.

$$\begin{tikzcd}
0 \arrow[r] & G(N) \arrow[r] \arrow[d, "\alpha"'] & G \arrow[r, "p^N"] \arrow[d] & G \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \underline{\omega}_{(G(N)^{\mathrm{D}})} \arrow[r] & \underline{\omega}_{(G(N)^{\mathrm{D}})} \coprod_{G(N)} G \arrow[r] & G \arrow[r] & 0
\end{tikzcd}$$

□

Corollary 4.4. [3, Chapter IV, Corollary 1.14] *Assume p is locally nilpotent on S and let G be a Barsotti-Tate group on S. Then there is an universal extension $0 \to \underline{V}(G) \to E(G) \to G \to 0$ of G by the vector group $V(G) = \underline{\omega}_{G^{\mathrm{D}}}$.*

From now on $E(G)$ will always represent the universal extension in the corollary above, which we know is a fppf sheaf of group.

Proposition 4.5. [3, Chapter IV, Proposition 1.19] *$\overline{E(G)}$ is a formal Lie group.*

Definition 4.6. $\underline{\mathrm{Lie}}(E(G)) := \underline{\mathrm{Lie}}(\overline{E(G)})$

If S_0 is a scheme on which p is locally nilpotent. Then $\mathbf{BT}(S_0)$ denotes the category of B.T groups over S_0 and $\mathbf{BT}'(S_0)$ denotes the full sub-category of $\mathbf{BT}(S_0)$, consisting of those G_0 with the following property: There is an open cover of S_0 (depending on G_0) formed of affine open sets $U_0 \subseteq S_0$ such that for any nilpotent immersion $U_0 \hookrightarrow U$ there is a B.T group G on U with $G|_{U_0} = G_0|_{U_0}$.

Theorem 4.7. [3, Chapter III, Theorem 2.2] *Let $S = \mathrm{Spec}(A)$ such that $p^N \cdot 1_S = 0$, $S_0 = \mathrm{Var}(I)$ where I is an ideal of A with nilpotent divided powers. Let G and H be two Barsotti-Tate groups on S and assume $u_0 : G_0 \to H_0$ is a homomorphism between their restrictions to S_0. u_0 defines a morphism $v_0 = E(u_0) : E(G_0) \to E(H_0)$ of extensions:*

$$\begin{tikzcd}
0 \arrow[r] & \underline{V}(G_0) \arrow[r] \arrow[d, "\underline{V}(u_0)"] & E(G_0) \arrow[r] \arrow[d, "v_0"] & G_0 \arrow[r] \arrow[d, "u_0"] & 0 \\
0 \arrow[r] & \underline{V}(H_0) \arrow[r] & E(H_0) \arrow[r] & H_0 \arrow[r] & 0
\end{tikzcd}$$

Then there is a unique morphism of groups $v = E_S(u_0)$: $E(G) \to E(H)$ (not necessarily respecting the structure of extensions) with the following properties:
1) v is a lifting of v_0;
2) given w: $\underline{V}(G) \to \underline{V}(H)$ a lifting of $\underline{V}(u_0)$, denote by i the inclusion $\underline{V}(H) \to E(H)$, so that $d = i \circ w - v|_{\underline{V}(G)} : \underline{V}(G) \to E(H)$ induces zero on S_0. Then, d is an exponential (this makes sense by [3, Chapter III.2.4]*).*

Corollary 4.8. [3, Chapter IV, Corollary 2.4.1] *Let K be a third Barsotti-Tate group on S, and $u_0' : H_0 \to K_0$ a homomorphism. Then $E_S(u_0' \circ u_0) = E_S(u_0') \circ E_S(u_0)$.*

Corollary 4.9. [3, Chapter IV, Corollary 2.4.3] *Let G, H, u_0 be as above and assume u_0 is an isomorphism, then $E_S(u_0)$ is an isomorphism.*

4.10. **Crystals associated to Barsotti-Tate group.**

The corollaries of above theorems permit the construction of crystals. Let S_0 be an arbitrary scheme (with p locally nilpotent on it) and let G_0 be in $\mathbf{BT}^{'}(S_0)$. By the reasoning recalled in [6], namely that fppf groups form a stack with respect to the Zariski topology, it suffices to give the value crystals to be constructed on objects $U_0 \hookrightarrow U$ of the crystalline site of S_0 with the property that $G_0|_{U_0}$ can be lifted to U, and U_0 is affine.
By corollaries above, the group $E(G)$ is independent up to canonical isomorphism of the lifting of $G_0|_{U_0}$ which has been chosen.
Let $V_0 \hookrightarrow V$ be a second object in the crystalline site and

$$\begin{tikzcd} U_0 \arrow[r, hook] & U \\ V_0 \arrow[u, "f"] \arrow[r, hook] & V \arrow[u, "\overline{f}"'] \end{tikzcd}$$

a morphism in Crys(X/S). Then for a lifting G_U of $G_0|_{U_0}$ to U and a lifting G_V of $G_0|_{V_0}$ to V the same corollaries give a canonical isomorphism $\overline{f}^*(E(G_U)) \xrightarrow{\sim} E(G_V)$, since both of them give an universal extension of a Barsotti-Tate group over V which lifts $G_0|_{V_0}$. This isomorphism is functorial in the sense of [3, Chapter III, Definition 3.6]

Now we know the following definition gives a well-defined crystal.

Definition 4.11. The rule that to any object $U_0 \hookrightarrow U$ in Crys(X/S) associates $E(G)$ where G is any lift of $G_0|_{U_0}$ to U gives a crystal that we denote $\mathbb{E}(G_0)$.

It is clear that for $u_0 : G_0 \to H_0$ a homomorphism between two liftable Barsotti-Tate groups, there is a morphism $\mathbb{E}(u_0)$ between the associated crystals which is defined on a "sufficiently small" open set $U_0 \hookrightarrow U$ via $E_U(u_0)$ in the notations introduced above.
Let $f : T_0 \to S_0$ be an arbitry morphism. The crystal $f^*(\mathbb{E}(G_0))$ is determined by its values on "sufficiently small" open sets in the crystalline site of T_0. Choose sufficiently small to mean that the object $V_0 \hookrightarrow V$ has to properties:
(1) $f(V_0) \subset U_0$ and $G_0|U_0$ can be lifted to infinitesimal neighborhoods;
(2) V_0 is affine.

Then we build the diagram

$$\begin{tikzcd} U_0 \arrow[r, hook] & U = U_0 \coprod_{V_0} V \\ V_0 \arrow[u, "f"] \arrow[r, hook] & V \arrow[u, "\overline{f}"'] \end{tikzcd}$$

It is immediate that, as we did above, for a lifting G_U of $G_0|U_0$ to U and a lifting G_V of $G_0|V_0$ to V

$$\overline{f}^*(E(G_U)) \xrightarrow{\sim} E(G_V) = \mathbb{E}(f^*(G_0))_{V_0 \hookrightarrow V}$$

Thus

$$\mathbb{E}(f^*(G_0)) = \mathbb{E}(f^*(G_0))$$

and we showed that taking crystal is stable under base change.
A more precise statement of the last equality would be that the following diagram is commutative up to a unique natural equivalence:

$$\begin{tikzcd} \mathbf{BT}^{'}(S_0) \arrow[r, "\mathbb{E}"] \arrow[d, "f^*"'] & \{\text{Crystals in fppf groups on } S_0\} \arrow[d, "f^*"'] \\ \mathbf{BT}^{'}(T_0) \arrow[r, "\mathbb{E}"] & \{\text{Crystals in fppf groups on } T_0\} \end{tikzcd}$$

From the construction of $\mathbb{E}(G_0)$ we can construct two other crystals as follows.

Definition 4.12. *cf* [3, Chapter IV, 2.5.4]. If $U_0 \hookrightarrow U$ is a nilpotent divided power immersion and G_0 can be lifted to a Barsotti-Tate group G on U, then we define crystals $\mathbb{E}(G_0)$, $\mathbb{D}(G_0)$ and $\mathbb{D}^*(G_0)$ as follows:

$$\begin{aligned} \mathbb{E}(G_0)_{U_0 \hookrightarrow U} &= E(G) \\ \mathbb{D}(G_0)_{U_0 \hookrightarrow U} &= \underline{\mathrm{Lie}}(E(G)) \\ \mathbb{D}^*(G_0)_{U_0 \hookrightarrow U} &= \underline{\mathrm{Lie}}(E(G^{\mathsf{D}})) \end{aligned}$$

Remark 4.13. By definition 4.12, we see that $\mathbb{E}(G_0)$ is a crystal in fppf groups on S_0 when $G_0 \in \mathbf{BT}(S_0)$. Hence $\mathbb{E}(G_0)_{U_0 \hookrightarrow U}$ is a sheaf of fppf groups on S_0, refering to our convention at the very beginning.

Proposition 4.14. *The sequence*

$$0 \to \underline{\omega}_{G^{\mathsf{D}}} \to \underline{\mathrm{Lie}}(E(G)) \to \underline{\mathrm{Lie}}(G) \to 0$$

is exact.

Proof. Recall we have

$$(*): \quad 0 \to \underline{\omega}_{G^{\mathsf{D}}} \to E(G) \to G \to 0$$

The sections of $\underline{\omega}_{G^{\mathsf{D}}}$ over $S^{'}$ are primitive elements, since it is a vector group and the commutativity gives the result. So $(*)$ tells us that $\underline{\omega}_{G^{\mathsf{D}}} \subset \underline{\mathrm{Lie}}(E(G))$ since $\underline{\mathrm{Lie}}(E(G))$ corresponds to the subsheaf of $E(G)$ whose sections over $S^{'}$ are primitive elements. $\underline{\omega}_{G^{\mathsf{D}}}$ is in the kernel of $\underline{\mathrm{Lie}}(E(G)) \to \underline{\mathrm{Lie}}(G)$, and conversely the kernel is obviously in the kernel of $\underline{\mathrm{Lie}}(E(G)) \to \underline{\mathrm{Lie}}(G)$, which is $\underline{\omega}_{G^{\mathsf{D}}}$ by $(*)$. Hence

$$\underline{\omega}_{G^{\mathsf{D}}} = \mathrm{Ker}(\underline{\mathrm{Lie}}(E(G)) \to \underline{\mathrm{Lie}}(G))$$

So it is left to prove $\underline{\mathrm{Lie}}(E(G)) \to \underline{\mathrm{Lie}}(G)$ is an epimorphism, which is proved by [3, Chapter IV, Proposition 1.22]. $\square$

Suppose now T_0 is a S-scheme with $p = 0$ on it, and G_0 is a p-divisible group over T_0. Let $T_0 \hookrightarrow T$ be an object of $\mathrm{Crys}(T_0/S)$ on which p is locally nilpotent, and G a lifting of G_0 to T. By construction of $\mathbb{D}$, we have an isomorphism $\mathbb{D}(G_0)(T) \xrightarrow{\sim} \mathbb{D}(G)(T)$.

Remark 4.15.
(1) Actually in the above isomorphism, $\mathbb{D}(G_0)(T) \xrightarrow{\sim} \mathbb{D}(G)(T)$, $\mathbb{D}(G_0)(T)$ is short for $\mathbb{D}(G_0)_{T_0 \hookrightarrow T}(T)$ and $\mathbb{D}(G)(T)$ is short for $\mathbb{D}(G)_{T \hookrightarrow T}(T)$. It suffices to show $\mathbb{D}(G_0)_{T_0 \hookrightarrow T} = \mathbb{D}(G)_{T \hookrightarrow T}$. In a more general case, suppose $U_0 \hookrightarrow U$ is a nilpotent closed immersion as usual, we have a morphism $\mathrm{Crys}(U/S) \to \mathrm{Crys}(U_0/S)$ by restricting an open scheme of U on U_0, hence we get an open scheme of U_0. Hence given $(W \hookrightarrow T) \in \mathrm{Crys}(U/S)$, it makes sense to envalute $\mathbb{D}(G_0)$ on $W|_{U_0} \hookrightarrow T$. And we have $\mathbb{D}(G_0)_{W|_{U_0} \hookrightarrow T} = \mathbb{D}(G)_{W \hookrightarrow T}$ since our construction of $\mathbb{D}(G)$ is compatible with arbitrary base change. We sometimes simply denote $\mathbb{D}(G_0)(T) = \mathbb{D}(G)(T)$.
(2) If $T = \operatorname{Spec} A$ is affine we will write $\mathbb{D}(G)(A)$ instead of $\mathbb{D}(G)(\operatorname{Spec} A)$.

Corollary 4.16. *The locally free sheaf on crystalline site* $\mathrm{Crys}(T_0/S)$*,* $\mathbb{D}^*(G)_{T_0 \hookrightarrow T}$*, sits in an exact sequence*

$$0 \to (\underline{\mathrm{Lie}}(G))^\vee \to \mathbb{D}^*(G)_{T_0 \hookrightarrow T} \to \underline{\mathrm{Lie}}(G^{\mathsf{D}}) \to 0$$

Proof. Let $\mathcal{A}$ be finite and locally-free and $G = \mathrm{Cospec}(\mathcal{A}) = \mathrm{Spec}(\mathcal{A}^\vee)$, where $\mathcal{A}^\vee = \mathrm{Hom}(\mathcal{A}, \mathscr{O}_S)$.

Then by Proposition 4.14 applied to G^{D} and by Proposition 2.65, $\underline{\omega}_G^\vee = \underline{\mathrm{Lie}}(G)$, we get the exact sequence:

$$0 \to (\underline{\mathrm{Lie}}(G))^\vee \to \mathbb{D}^*(G)_{T_0 \hookrightarrow T} \to \underline{\mathrm{Lie}}(G^{\mathsf{D}}) \to 0$$

□

Corollary 4.17. *If T is affine and $G \in \mathbf{BT}(T)$, then*

$$0 \to (\mathrm{Lie}(G))^\vee \to \mathbb{D}^*(G)(T) \to \mathrm{Lie}(G^{\mathsf{D}}) \to 0$$

is an exact sequence of $\Gamma(T, \mathscr{O}_T)$-modules.

Proof. Remark 2.62 indicates that one may envaluate the exact sequence in Corollary 4.16 on an affine scheme $T = \operatorname{Spec} A$. To do this, we define the fppf cohomology functor $H^i_{\mathrm{fppf}}(T, \bullet)$ to be the right derived functors of $\Gamma(T, \bullet)$. Hence to get the exact sequence we want, it suffices to show that $H^1_{\mathrm{fppf}}(T, (\underline{\mathrm{Lie}}(G))^\vee) = 0$. But we have

$$H^1_{\mathrm{fppf}}(T, (\underline{\mathrm{Lie}}(G))^\vee) = H^1_{Zar}(T, (\mathrm{Lie}(G))^\vee) = 0$$

Where the first equality is by [10, Tag 03OJ] and [10, Tag 03P2] and the second equality is by [EGA III, 1.3.1] since $(\underline{\mathrm{Lie}}(G))^\vee$ is locally free and hence quasi-coherent. One can also check [11, Theorem 3.7] for a reference. □

4.18. **Grothendieck-Messing theory.**

Notation 4.19.
(1)Let S be a scheme on which p is locally nilpotent, $\mathcal{I}$ a quasi-coherent ideal of $\mathscr{O}_S$ endowed with locally nilpotent divided powers. Let $S_0 = \mathrm{Var}(\mathcal{I})$ so that $S_0 \hookrightarrow S$ is an object of the crystalline site of S_0. Denote by $\mathbf{BT}'(S_0)$ the full sub-category of $\mathbf{BT}(S_0)$ consisting of those G_0 which can locally (for the Zariski topology) be

lifted to a $G \in \mathbf{BT}(S)$.
(2) Notice the definition of $\mathbf{BT}^{'}(S_0)$ here is different from above, because in this part we will only consider crystals with their values on particular object of the crystalline site, namely the object $S_0 \hookrightarrow S$.
(3) $\mathbb{E}(G_0)_S$ and $\mathbb{D}(G_0)_S$ will refer to the values of the corresponding crystals on the object $S_0 \hookrightarrow S$.

Definition 4.20. A filtration $\mathrm{Fil}^1 \subset \mathbb{D}(G_0)_S$ is said to be *admissible* if Fil^1 is a locally-free vector sub-group with locally free quotient, which reduces to $\underline{V}(G_0) \hookrightarrow \underline{\mathrm{Lie}}(E(G_0))$ on S_0.

We define an obvious category, denoted by $\mathcal{C}_{S_0 \hookrightarrow S}$, whose objects are pairs (G_0, Fil^1) with G_0 in $\mathbf{BT}'(S_0)$ and Fil^1 an admissible filtration on $\mathbb{D}(G_0)_S$. Morphisms are defined as pairs (u_0, ξ) where $u_0 : H_0 \to G_0$ is a morphism in $\mathbf{BT}(S_0)$ and ξ is a morphism of filtered objects, *i.e.* , a commutative diagram

$$\begin{tikzcd}
\mathrm{Fil}^1 \arrow[r, hook] \arrow[d, "\xi"'] & \mathbb{D}(G_0)_S \arrow[d, "\mathbb{D}(u_0)_S"] \\
\mathrm{Fil}^{1'} \arrow[r, hook] & \mathbb{D}(H_0)_S
\end{tikzcd}$$

which reduces on S_0 to

$$\begin{tikzcd}
\underline{V}(G_0) \arrow[r, hook] \arrow[d, "\underline{V}(u_0)"'] & \underline{\mathrm{Lie}}(E(G_0)) \arrow[d, "\underline{\mathrm{Lie}}(E(u_0))"] \\
\underline{V}(H_0) \arrow[r, hook] & \underline{\mathrm{Lie}}(E(H_0))
\end{tikzcd}$$

Theorem 4.21. [3, Chapter V, Theorem 1.6] *The functor $G \to (G_0, \underline{V}(G) \hookrightarrow \mathbb{D}(G_0)_S)$ establishes an equivalence of categories:*

$$\mathbf{BT}(S) \to \mathcal{C}_{S_0 \hookrightarrow S}$$

Remark 4.22. (1) Let G_0 be in $\mathbf{BT}^{'}(S_0)$. We have a sheaf $\mathcal{L}$ on S defined by $\Gamma(U, \mathcal{L})$ = set of linear equivalence classes of lifts of $\underline{V}(G_0) \hookrightarrow E(G_0)|_{U_0}$ to a vector subgroup $V \hookrightarrow \mathbb{E}(G_0)_S|_{U_0}$, for any affine open $U \subset S$. By our construction of $\mathbb{E}(G_0)_S$, $\mathcal{L}$ has a canonical section $\Theta \in \Gamma(S, \mathcal{L})$ which is determined on any sufficiently small affine open U by the equivalence class of $\underline{V}(G)$ where G is any lifting of $G_0|_{U_0}$ to U. Choose two different liftings of G_0, say G_1 and G_2, and hence different liftings of $\underline{V}|_{U_0} \hookrightarrow E(G_0)|_{U_0}$, say $\underline{V}(G_1) \hookrightarrow E(G_1)$ and $\underline{V}(G_2) \hookrightarrow E(G_2)$. Then by [3, Chapter IV, Theorem 2.2] we have a diagram

$$\begin{tikzcd}
\underline{V}(G_1) \arrow[r, hook] \arrow[d, "\omega"'] & E(G_1) \arrow[d, "v", "\sim"'] \\
\underline{V}(G_2) \arrow[r, "i"] & E(G_2)
\end{tikzcd}$$

with $i \circ w - v|_{\underline{V}(G_1)}$ an exponential. Hence the two liftings are equivalent and thus by [3, Chapter III, Proposition 2.7.7] they corresponds to a same section in $\Gamma(S, \mathcal{L})$.
(2) Hence we see that giving a $V \subset \mathbb{E}(G_0)_S$ which belongs to Θ is equivalent to giving an admissssible filtration $\mathrm{Fil}^1 \hookrightarrow \mathbb{D}(G_0)_S$ *cf* [3, Chapter III, Proposition 2.7.7]. In particular to know $\underline{V}(G) \subset \mathbb{E}(G_0)_S$ is the same as knowing $\underline{V}(G) \subset \mathbb{D}(G_0)_S$. Knowing $\underline{V}(G) \subset \mathbb{E}(G_0)_S$ gives $G \simeq \mathbb{E}(G_0)_S / \underline{V}(G)$.
(3) By the observations in (1) and (2), we can construct another category that

is equivalent with $\mathbf{BT}(S)$, with objects simply $(G_0, V \subset \mathbb{E}(G_0)_S)$ but more complicated morphisms relating liftings. $\mathcal{C}_{S_0 \hookrightarrow S}$ is better since it is just described by algera structure, avoiding the mess with liftings.

5. A classification of p-divisible groups over $\mathcal{O}_K$

Let k be a perfect field of characteristic $p > 0$ and let $W := W(k)$ be its ring of Witt vectors. We consider a totally ramied extension K of degree e of the field of fractions $W[1/p]$. Fix a uniformizer $\pi \in K$ and denote by $\mathrm{E}(u)$ its minimal polynomial.

Lemma 5.1. [12, Lemma A.2]
Let $A \to A_0$ be a surjection of p-adically complete and separated local $\mathbb{Z}_p$-algebras with residue field k, whose kernel $\mathrm{Fil}^1 A$ is equipped with divided powers. Suppose that
(1) A is p-torsion-free, and equipped with an endomorphism $\varphi : A \to A$ lifting the Frobenius on A/pA.
(2) The induced map $\varphi^*(\mathrm{Fil}^1 A) \xrightarrow{1 \otimes \varphi/p} A$ is surjective.
If G_0 is a p-divisible group over A_0, write $\mathrm{Fil}^1 \mathbb{D}^*(G_0)(A) \subseteq \mathbb{D}^*(G_0)(A)$ for the preimage of $(\mathrm{Lie}\, G_0)^\vee \subset \mathbb{D}^*(G_0)(A_0)$. Then the restriction of $\varphi : \mathbb{D}^*(G_0)(A) \to \mathbb{D}^*(G_0)(A)$ to $\mathrm{Fil}^1 \mathbb{D}^*(G_0)(A)$ is divisible by p and the induced map

$$\varphi^* \mathrm{Fil}^1 \mathbb{D}^*(G_0)(A) \xrightarrow{1 \otimes \varphi/p} \mathbb{D}^*(G_0)(A)$$

is surjective.

Remark 5.2. The $\mathrm{Fil}^1 \mathbb{D}^*(G_0)(A) \subseteq \mathbb{D}^*(G)(A)$ is got by the following way:

$$\begin{tikzcd}
\mathrm{Fil}^1 \mathbb{D}^*(G_0)(A) \arrow[r, hook] \arrow[d] & \mathbb{D}^*(G_0)(A) \arrow[d] \\
(\mathrm{Lie}\, G_0)^\vee \arrow[r, hook] & \mathbb{D}^*(G_0)(A_0)
\end{tikzcd}$$

Moreover, we have $\mathbb{D}^*(G_0)(A)/\mathrm{Fil}^1 \mathbb{D}^*(G_0)(A) \simeq \mathrm{Lie}(G_0^{\mathsf{D}})$. Indeed choose G, a lift of G_0, consider the following morphism of extensions:

$$\begin{tikzcd}
0 \arrow[r] & (\mathrm{Lie}\, G)^\vee \arrow[r] \arrow[d, "\alpha"'] & \mathbb{D}^*(G_0)(A) \arrow[r] \arrow[d, "\beta"] & \mathrm{Lie}(G^{\mathsf{D}}) \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & (\mathrm{Lie}\, G_0)^\vee \arrow[r] & \mathbb{D}^*(G_0)(A_0) \arrow[r] & \mathrm{Lie}(G_0^{\mathsf{D}}) \arrow[r] & 0
\end{tikzcd}$$

A maps surjectively onto A_0 so β and hence γ is surjective. Moreover, the first column corresponds to nothing but $M \to M \otimes_A A_0$ where M is an A-module $(\mathrm{Lie}\, G)^\vee$ associates to. Hence we see the first column is also a surjective map.

Applying Snake Lemma we get the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}\alpha \arrow[r] \arrow[d] & \operatorname{Ker}\beta \arrow[r] \arrow[d] & \operatorname{Ker}\gamma \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & (\operatorname{Lie} G)^{\vee} \arrow[r] \arrow[d, "\alpha"'] & \mathbb{D}^*(G_0)(A) \arrow[r] \arrow[d, "\beta"] \arrow[dr, "h"] & \operatorname{Lie}(G^{\mathsf{D}}) \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & (\operatorname{Lie} G_0)^{\vee} \arrow[r] \arrow[d] & \mathbb{D}^*(G_0)(A_0) \arrow[r] \arrow[d] & \operatorname{Lie}(G_0^{\mathsf{D}}) \arrow[r] \arrow[d] & 0 \\
& 0 & 0 & 0 &
\end{tikzcd}$$

and hence one has $\operatorname{Ker} h = \operatorname{Ker}\beta + (\operatorname{Lie} G)^{\vee} = \operatorname{Fil}^1 A \cdot \mathbb{D}^*(G_0)(A) + (\operatorname{Lie} G)^{\vee}$. This is exactly the preimage of $(\operatorname{Lie} G_0)^{\vee}$ under map β, *i.e.* $\operatorname{Fil}^1 \mathbb{D}^*(G_0)(A)$. Hence $\operatorname{Ker} h = \operatorname{Fil}^1 \mathbb{D}^*(G_0)(A)$ and we get the desired isomorphism.

Definition 5.3. A *special ring* is a p-adically complete, separated, p-torsion free, local $\mathbb{Z}_p$-algebra A with residue field k, equipped with an endormorphism φ lifting the Frobenius on A/pA.

For a special ring A, we denote by $\mathcal{C}_A$ the category of finite free A-modules $\mathcal{M}$, equipped with a Frobenius semilinear map $\varphi : \mathcal{M} \to \mathcal{M}$ and an A-submodule $\mathcal{M}_1 \subseteq \mathcal{M}$ such that $\varphi(\mathcal{M}_1) \subseteq p\mathcal{M}$ and the map $1 \otimes \varphi/p : \varphi^*(\mathcal{M}_1) \to \mathcal{M}$ is surjective.

Given a map of special rings $A \to B$, (that is a map of $\mathbb{Z}_p$-algebra compatible with φ) and $\mathcal{M}$ in $\mathcal{C}_A$, we give $\mathcal{M} \otimes_A B$ the structure of an object in $\mathcal{C}_B$, by giving it the induced Frobenius, and setting $(\mathcal{M} \otimes_A B)_1$ equal to the image of $\mathcal{M} \otimes_A B$ in $\mathcal{M}_1 \otimes_A B$.

Lemma 5.4. [12, Lemma A.4]
Let $h : A \to B$ be a surjection of special rings with kernel J. Suppose that for $i \geq 1$, $\varphi^i(J) \subseteq p^{i+j_i} J$, where $\{j_i\}_{i\geq 1}$ is a sequence of integers such that $\varinjlim_{i\to\infty} j_i = \infty$ Let $\mathcal{M}$ and $\mathcal{M}'$ be in $\mathcal{C}_A$, and $\theta_B : \mathcal{M} \otimes_A B \xrightarrow{\sim} \mathcal{M}' \otimes_A B$ an isomorphism in $\mathcal{C}_B$. Then there exists an unique isomorphism of A-modules $\theta_A : \mathcal{M} \to \mathcal{M}'$ lifting θ_B, and compatible with φ.

We will apply lemma above in the following situation: J is equipped with divided powers, and there exist a finite set of elements $x_1, \ldots x_n \in J$ such that J is topologically (for the p-adic topology) generated by the x_i and their divided powers, and $\varphi(x_i) = x_i^p$. The integers j_i may then be taken to be $v_p((p^i - 1)!) - i$.

Remark 5.5.
(1) Since J is equipped with divided powers, so $\gamma_{p^i-1}(x_k) \in J$ for $k \in \{1, \ldots, n\}$. Notice $\varphi^i(x_k) = x_k^{p^i} = (p^i - 1)!\gamma_{p^i-1}(x_k)x_k$, so take j_i to be $v_p((p^i - 1)!) - i$ guarantees $\varphi^i(J) \subseteq p^{i+j_i} J$.
(2) Suppose A is a special ring with a P.D. ring (J, γ). For any $a \in A$, $\varphi(a) \equiv a^p \equiv \gamma_p(a)p! \pmod{pA}$, hence $\varphi(J) \subset pJ$ and we can put $\varphi_1 = \varphi/p$ on J as A has no p-torsion.

Denote by $W[u][\mathrm{E}(u)^{[i]}]_{i\geq 1}$ the divided power envelope of $W[u]$ generated by the ideal $\mathrm{E}(u)$. There is a surjective map

$$W[u][\mathrm{E}(u)^{[i]}]_{i\geq 1} \twoheadrightarrow \mathcal{O}_K$$
$$u \mapsto \pi$$

Denote by S the p-adic completion of the divided power envelope of $W[u]$ with respect to the ideal $\mathrm{E}(u)$, *i.e.*

$$\mathsf{S} := \widehat{W[u][\mathrm{E}(u)^{[i]}]}$$

The ring S is equipped with an endomorphism φ, by extending the Frobenius on W to S : $\varphi(u) = u^p$. We denote by $\mathrm{Fil}^1 \mathsf{S} \subseteq \mathsf{S}$ the closure of the ideal generated by $\mathrm{E}(u)$ and its divided powers. Then we have an isomorphism:

$$\mathsf{S}/\operatorname{Fil}^1 \mathsf{S} \xrightarrow{\simeq} \mathcal{O}_K$$

By Remark 5.5 (2), $\varphi(\mathrm{Fil}^1 \mathsf{S}) \subseteq p\mathsf{S}$ and we set $\varphi_1 = \varphi/p : \mathrm{Fil}^1 \mathsf{S} \to \mathsf{S}$.

Definition 5.6. We will denote by $\mathbf{BT}^{\varphi}_{/\mathsf{S}}$ the category of finite free S-modules $\mathcal{M}$ equipped with an S-submodule $\mathrm{Fil}^1 \mathcal{M}$ and a φ-semilinear map $\varphi_1 : \mathrm{Fil}^1 \mathcal{M} \to \mathcal{M}$ such that
(1) $\mathrm{Fil}^1 \mathsf{S} \cdot \mathcal{M} \subseteq \mathrm{Fil}^1 \mathcal{M}$, and the quotient $\mathcal{M}/\operatorname{Fil}^1 \mathcal{M}$ is a free $\mathcal{O}_K$-module.
(2) The map $\varphi^*(\mathrm{Fil}^1 \mathcal{M}) \xrightarrow{1\otimes\varphi_1} \mathcal{M}$ is surjective.

Any $\mathcal{M}$ in $\mathbf{BT}^{\varphi}_{/\mathsf{S}}$ is equipped with a Frobenius semilinear map $\varphi : \mathcal{M} \to \mathcal{M}$ defined by $\varphi(x) := \varphi_1(E(u))^{-1}\varphi_1(E(u)x)$.

Remark 5.7. By [13], we know that the data of a p-divisible group over $\mathcal{O}_K$ is equivalent to the data of a compatible collection of p-divisible groups over $\mathcal{O}_K/(p^i)$ for $i \in \{1, 2, \dots\}$. One direction is simply by base changing the original p-divisible group G to group G_i over $\mathcal{O}_K/(p^i)$.

Given a p-divisible group G over $\mathcal{O}_K$. Write $\mathsf{S} = \varprojlim_n \mathsf{S}/(p^n)$. Hence $\mathbb{D}^*(G_i)(\mathsf{S}/p^m)$ makes sense for $m \geq i$. Since $\mathsf{S} \twoheadrightarrow \mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/(p^i)$, we have $\mathsf{S}/(p^i) \twoheadrightarrow \mathcal{O}_K/(p^i)$. By Remark 4.15 (1), we have $\mathbb{D}^*(G_i)(\mathsf{S}/(p^{i+1})) = \mathbb{D}^*(G_{i+1})(\mathsf{S}/(p^{i+1}))$. Hence we can define

$$\mathbb{D}^*(G)(\mathsf{S}) := \varprojlim_{m\geq i} \mathbb{D}^*(G_i)(\mathsf{S}/(p^m))$$

which is independent of the i. Using Remark 5.2, $\mathbb{D}^*(G)(\mathsf{S})$ is endowed with a sub S-module $\mathrm{Fil}^1 \mathbb{D}^*(G)(\mathsf{S})$ that contains $\mathrm{Fil}^1 \mathsf{S} \cdot \mathbb{D}^*(G)(\mathsf{S})$.

Remark 5.8. We know how to evaluate a crystal on a P.D. thickening, whose kernel $\mathcal{I}$ is nilpotent with divided power structure. However, in the proof of the proposition below we will face the case when the ideal $\mathcal{I} = (p) \subset W$ has divided power but is not nilpotent. In this case, we can use similar method as in (1) above, to deal with $W/p^iW,\ i \geq 1$ and then take limit to get the desired evalution.

Proposition 5.9. *There is an exact contravariant functor $G \mapsto \mathbb{D}^*(G)(\mathsf{S})$ from the category of p-divisible groups over $\mathcal{O}_K$ to $\mathbf{BT}^{\varphi}_{/\mathsf{S}}$. If $p > 2$ this functor is an antiequivalence.*

Proof. Given a p-dividible group G over $\mathcal{O}_K$, the S-module $\mathcal{M}(G) := \mathbb{D}^*(G)(\mathsf{S})$ is well defined by Remark 5.7. One checks that it has a natural structure of an object of $\mathbf{BT}^{\varphi}_{/\mathsf{S}}$, hence this gives a functor from the category of p-divisible groups over $\mathcal{O}_K$ to $\mathbf{BT}^{\varphi}_{/\mathsf{S}}$.
Indeed, by Remark 5.2 applying to the case $\mathsf{S} \twoheadrightarrow \mathcal{O}_K$ we have an isomorphism:

$$\mathbb{D}^*(G)(\mathsf{S})/\operatorname{Fil}^1 \mathbb{D}^*(G)(\mathsf{S}) \xrightarrow{\sim} \operatorname{Lie}(G^{\mathsf{D}})$$

So $\mathbb{D}^*(G)(\mathsf{S})/\operatorname{Fil}^1 \mathbb{D}^*(G)(\mathsf{S})$ is a free $\mathcal{O}_K$-module.

Recall that $\varphi^* \operatorname{Fil}^1 \mathsf{S}$ is the tensor product of two S-modules S and $\operatorname{Fil}^1 \mathsf{S}$, and the map is given by

$$\varphi^* \operatorname{Fil}^1 \mathsf{S} \xrightarrow{1\otimes\varphi/p} \mathsf{S}$$

$$s \otimes a \mapsto s\frac{\varphi}{p}(a)$$

To shows $\varphi^* \operatorname{Fil}^1 \mathsf{S} \xrightarrow{1\otimes\varphi/p} \mathsf{S}$ is surjective, it is equivalent to prove $\varphi_1(\operatorname{Fil}^1 \mathsf{S})$ generates S. Recall that $\mathrm{E}(u) = u^e + pa_{e-1}u^{e-1} + \cdots + pa_0 \in \operatorname{Fil}^1 \mathsf{S}$ and by the definition of φ_1 we have $\varphi_1(\mathrm{E}(u)) = \frac{1}{p}(u^{ep} + p\varphi(a_{e-1})u^{(e-1)p} + \cdots + p\varphi(a_0)) = \varphi(a_0) + \varphi(a_1)u^p + \cdots + \frac{u^{ep}}{p}$. $\varphi_1(\mathrm{E}(u))$ is mapped to $\varphi(a_0) + \varphi(a_1)\pi^p + \cdots + \frac{\pi^{ep}}{p}$ under the map $\mathsf{S} \to \mathcal{O}_K$ and we have $v_p(\frac{u^{ep}}{p}) = p - 1 > 0$. One checks that this element is not in the maximal ideal of $\mathcal{O}_K$, hence in $\mathcal{O}_K^\times$. So $\varphi_1(\mathrm{E}(u))$ is invertible in S and hence $\varphi_1(\operatorname{Fil}^1 \mathsf{S})$ generates S. Now by applying Lemma 5.1, $\varphi^* \operatorname{Fil}^1 \mathbb{D}^*(G)(\mathsf{S}) \xrightarrow{1\otimes\varphi/p} \mathbb{D}^*(G)(\mathsf{S})$ is surjective. These results together show that $\mathcal{M}(G) := \mathbb{D}^*(G)(\mathsf{S})$ is indeed an object of the category $\mathbf{BT}^{\varphi}_{/\mathsf{S}}$.

Now we construct a quasi-inverse. Let $\mathcal{M}$ be in $\mathbf{BT}^{\varphi}_{/\mathsf{S}}$ and for any such i

$$R_i := W[u]/(u^i)$$

It is equipped with a Frobenius endomorphism φ given by the Frobenius on W and $u \mapsto u^p$. We regard $\mathcal{O}_K/(\pi^i)$ as an R_i-algebra via

$$W[u]/(u^i) \to \mathcal{O}_K/(\pi^i)$$

$$u \mapsto \pi$$

This is a surjection with kernel pR_i (since u^e is killed, $E(u)$ become pt, where t is an unit), so R_i is a divided power thickening of $\mathcal{O}_K/(\pi^i)$, *i.e.* we have

$$\operatorname{Spec}(\mathcal{O}_K/(\pi^i)) \hookrightarrow \operatorname{Spec}(W[u]/(u^i)) \in \operatorname{Crys}(\operatorname{Spec}(\mathcal{O}_K/(\pi^i))/W)$$

and given any p-divisible group G_i over $\mathcal{O}_K/(\pi^i)$ we may form $\mathbb{D}^*(G_i)(R_i)$ (as explained below Remark 5.7). As in Lemma 5.2 we denote by $\operatorname{Fil}^1 \mathbb{D}^*(G_i)(R_i)$ the preimage of $(\operatorname{Lie} G_i)^\vee \subset \mathbb{D}^*(G_i)(\mathcal{O}_K/(\pi^i))$ in $\mathbb{D}^*(G_i)(R_i)$.

$$\begin{tikzcd}
\operatorname{Fil}^1 \mathbb{D}^*(G_i)(R_i) \arrow[r, hook] \arrow[d] & \mathbb{D}^*(G_i)(R_i) \arrow[d] \\
(\operatorname{Lie} G_i)^\vee \arrow[r, hook] & \mathbb{D}^*(G_i)(\mathcal{O}_K/(\pi^i))
\end{tikzcd}$$

On the other hand, by the universal property of P.D. envelope we have a φ-compatible (by unicity) map $f_i : \mathsf{S} \to R_i$,

$$\begin{tikzcd}
& \mathsf{S} \arrow[dr, "f_i"] & \\
W[u] \arrow[ur] \arrow[rr] & & W[u]/(u^i) = R_i
\end{tikzcd}$$

sending u to u, and $u^{ej}/j!$ to 0 for $j \geq 1$. Write I_i for the kernel of this map. We equip $\mathcal{M}_i = R_i \otimes_{\mathsf{S}} \mathcal{M}$ with the induced Frobenius φ, and we let $\operatorname{Fil}^1 \mathcal{M}_i \subset \mathcal{M}_i$ be equal to the image of $\operatorname{Fil}^1 \mathcal{M}$ in $\mathcal{M}_i$

$$\begin{tikzcd}
\operatorname{Fil}^1 \mathcal{M}_i \arrow[r, hook] & \mathcal{M}_i \\
\operatorname{Fil}^1 \mathcal{M} \arrow[r, hook] \arrow[u] & \mathcal{M} \arrow[u]
\end{tikzcd}$$

Note that $1 \otimes \varphi_1 : \varphi^*(\operatorname{Fil}^1 \mathcal{M}) \to \mathcal{M}$ induces a surjective map $\varphi^*(\operatorname{Fil}^1 \mathcal{M}_i) \to \mathcal{M}_i$.

We proceed by steps. In *step 1* and *step 2* we will construct a p-divisible group G_i together with a canonical isomorphism $\mathbb{D}^*(G_i)(R_i) \xrightarrow{\sim} \mathcal{M}_i$, $(i \in 1, 2, \ldots, e)$ compatible with φ and filtrations. In *step 3*, we get the p-divisible group G_e over $\mathcal{O}_K/(p)$ such that $\mathcal{M} \xrightarrow{\sim} \mathbb{D}^*(G_e)(\mathsf{S})$. In *step 4*, we then get p-divisible groups over $\mathcal{O}_K/(p^i)$ for $i \in \{1, 2, \ldots\}$, which corresponds to a unique p-divisible group G over $\mathcal{O}_K$.

Step 1:
Denote by $F : \mathcal{M}_i \to \mathcal{M}_i$ the map induced by $\varphi : \mathcal{M} \to \mathcal{M}$. A simple computation shows that both sides of the surjective map $\varphi^*(\operatorname{Fil}^1 \mathcal{M}_1) \to \mathcal{M}_1$, are free W-modules of the same rank, hence the map

$$1 \otimes \varphi_1 : \varphi^*(\operatorname{Fil}^1 \mathcal{M}_1) \xrightarrow{\sim} \mathcal{M}_1$$

is an isomorphism. Composing the inverse of this isomorphism with the composite,

$$\varphi^*(\operatorname{Fil}^1 \mathcal{M}_1) \to \varphi^*(\mathcal{M}_1) \xrightarrow{\sim} \mathcal{M}_1$$

where the first map is induced by the inclusion $\operatorname{Fil}^1 \mathcal{M} \subset \mathcal{M}$, while the second is given by $a \otimes m \mapsto \varphi^{-1}(a)m$, gives a φ^{-1} semilinear Vershiebung map $V : \mathcal{M}_1 \to \mathcal{M}_1$, such that $\varphi V = V \varphi = p$. Denote by G_1 to be the p-divisible group associated to this Dieudonné module by classical contravariant Dieudonné theory.
The tautological isomorphism $\mathbb{D}^*(G_1)(W) \xrightarrow{\sim} \mathcal{M}_1$ is compatible with Frobenius, and it is compatible with filtrations because $\operatorname{Fil}^1 \mathbb{D}^*(G_1)$ may be identified with $V\mathbb{D}^*(G_1)$, as explained [12, A.2]

Step 2:
Now we suppose that $i \in [2, e]$ is an integer and that we have constructed G_{i-1} such that $\mathbb{D}^*(G_{i-1})(R_{i-1}) \xrightarrow{\sim} \mathcal{M}_{i-1}$ is compatible with Frobenius and filtrations. Note that the kernel of $R_i \to \mathcal{O}_K/(\pi^{i-1})$ is equal to (u^{i-1}, p) which admits divided powers.
Indeed, we know (p) admits divided powers by Remark 3.3(2); and if the divide power structure exists, then we have $n!\gamma_n(u^{i-1}) = u^{n(i-1)}$. Hence $\gamma_n(u^{i-1})$ is u^{i-1} when $n = 1$, and is 0 when $i \geq 2$. So we are left to prove the existence of this divided power structure, but this follows from $W[u]/(u^i) \subset K_0[u]/(u^i)$, where $K_0 = W[1/p]$ is a $\mathbb{Q}$-algebra hence has divided power structure.

So we may evaluate $\mathbb{D}^*(G_{i-1})$ on R_i as explained below Remark 5.7. By Lemma 5.2 and what we have already seen, $\mathbb{D}^*(G_{i-1})(R_i)$ and $\mathcal{M}_i$ both have the structure of objects of $\mathcal{C}_{R_i}$ and the above isomorphism $\mathbb{D}^*(G_{i-1})(R_{i-1}) \xrightarrow{\sim} \mathcal{M}_{i-1}$ is an isomorphism in $\mathcal{C}_{R_{i-1}}$. Hence by Lemma 5.5 applied to the surjection $R_i \twoheadrightarrow R_{i-1}$, it lifts to a unique φ-compatible isomorphism

$$\mathbb{D}^*(G_{i-1})(R_i) \xrightarrow{\sim} \mathcal{M}_i$$

By the deformation theory we presented in Section 4, there is a unique p-divisible group G_i over $\mathcal{O}_K/(\pi^i)$ which lifts G_{i-1}, and such that $(\operatorname{Lie} G_i)^\vee \subset \mathbb{D}^*(G_{i-1})(\mathcal{O}_K/(\pi^i))$ is equal to the image of $\operatorname{Fil}^1 \mathcal{M}_i$ under the composition:

$$\operatorname{Fil}^1 \mathcal{M}_i \subset \mathcal{M}_i \xrightarrow{\sim} \mathbb{D}^*(G_{i-1})(R_i) \to \mathbb{D}^*(\mathcal{O}_K/(\pi^i))$$

By construction we have $\mathbb{D}^*(G_i)(R_i) \xrightarrow{\sim} \mathcal{M}_i$ compatible with φ and filtrations, which completes the induction.

Step 3:
We now apply Lemma 5.5 to the surjection $\mathsf{S} \to R_e$, and the module $\mathcal{M}$ and $\mathbb{D}^*(G_e)(\mathsf{S})$ in $\mathcal{C}_{\mathsf{S}}$. Note that the kernel of $\mathsf{S} \to \mathcal{O}_K/(\pi^e) = \mathcal{O}_K/(p)$ admits divided powers, so we may evaluate $\mathbb{D}^*(G_e)$ on S as explained below Remark 5.7, and the result is in $\mathcal{C}_{\mathsf{S}}$ by Lemma 5.2. Since $\mathcal{M}_e \xrightarrow{\sim} \mathbb{D}^*(G_e)(R_e)$ in $\mathcal{C}_{R_e}$, we have a canonical φ-compatible isomorphism by Lemma A.4:

$$\mathcal{M} \xrightarrow{\sim} \mathbb{D}^*(G_e)(\mathsf{S})$$

Step 4:
Suppose that $p > 2$, then the divided powers on the kernel of $\mathcal{O}_K \to \mathcal{O}_K/(p)$ are nilpotent, and we can take $G = G(\mathcal{M})$ to be the unique lift of G_e to $\mathcal{O}_K$ such that $(\operatorname{Lie} G)^\vee \subseteq \mathbb{D}^*(G_e)(\mathcal{O}_K)$ is equal to the image of $\operatorname{Fil}^1 \mathcal{M}$ under the composition of the above isomorphism and the projection $\mathbb{D}^*(G_e)(\mathsf{S}) \to \mathbb{D}^*(G_e)(\mathcal{O}_K)$. Strictly speaking what Grothendieck-Messing theory produces is a sequence of p-divisible groups over $\mathcal{O}_K/(p^i)$ for $i = 1, 2, \ldots$ which are compatible under the maps $\mathcal{O}_K/(p^i) \to \mathcal{O}_K/(p^{i-1})$. However, this data corresponds to a unique p-divisible group over $\mathcal{O}_K$ as expalined in Remark 5.7.
From the construction we have $\mathcal{M} \xrightarrow{\sim} \mathcal{M}(G(\mathcal{M}))$. And on the other hand using the uniquness at every stage of the construction, one sees by induction on i that that for $i = 1, 2, \ldots, e$ and any p-divisible group G over $\mathcal{O}_K$, $G_i(\mathcal{M}(G))$ is isomorphic to $G \otimes_{\mathcal{O}_K} \mathcal{O}_K/(\pi^i)$, (hence we have $G \xrightarrow{\sim} G_i(\mathcal{M}(G))$ modulo π^i) and then that $G \xrightarrow{\sim} G(\mathcal{M}(G))$. $\square$

Example 5.10. Let's see some basic examples of the functor constructed in this section

$$\mathbf{BT}(\mathcal{O}_K) \xrightarrow{\mathcal{M}} \mathbf{BT}^{\varphi}_{/\mathsf{S}}$$

$$G \mapsto \mathbb{D}^*(G)(\mathsf{S})$$

Let $G^{'}$ be a lifting of G over S, the universal extension of G gives us a sequence

$$0 \to (\operatorname{Lie}(G^{'}))^\vee \to \mathbb{D}^*(G)(\mathsf{S}) \to \operatorname{Lie}(G^{'\mathsf{D}}) \to 0$$

Recall in Lemma 2.21 we proved that $\omega_G^\vee = \operatorname{Lie}(G)$. Hence

$$0 \to \omega_{G'} \to \mathbb{D}^*(G)(\mathsf{S}) \to \omega^\vee_{G'^{\mathsf{D}}} \to 0$$

(1) Consider $G = \mu_{p^\infty/\mathcal{O}_K} = \varinjlim \mu_{p^n/\mathcal{O}_K}$. We have results:

$$\mathcal{M}(\mu_{p^\infty/\mathcal{O}_K}) = \mathsf{S} \quad ; \quad \operatorname{Fil}^1 \mathcal{M}(\mu_{p^\infty/\mathcal{O}_K}) = \mathsf{S}$$

Choose $G^{'} = \mu_{p^\infty/\mathsf{S}}$ as a special lift of $\mu_{p^\infty/\mathcal{O}_K}$ over S. We do precise computations to prove above results:

$$\begin{aligned}\Omega^1_{\mu_{p^n}/\mathsf{S}} &= \frac{\mathsf{S}[T]}{(T^{p^n}-1)}dT/(p^nT^{p^n-1}dT)\\ &= \frac{\mathsf{S}[T]}{(T^{p^n}-1)}dT/(p^n)\frac{dT}{T}\\ &= \mathsf{S}[T]/(p^n, T^{p^n-1})\frac{dT}{T}\end{aligned}$$

Hence

$$\omega_{\mu_{p^n}/\mathsf{S}} = e^*(\Omega^1_{\mu_{p^n}/\mathsf{S}}) \simeq \mathsf{S}/(p^n)\frac{dT}{T}$$
$$\omega_{G'} = \omega_{\mu_{p^\infty}/\mathsf{S}} \simeq \mathsf{S}\frac{dT}{T} \simeq \mathsf{S}$$

$G^{'\mathsf{D}} = \mathbb{Q}_p/\mathbb{Z}_{p/\mathsf{S}}$ is étale implies $\omega_{G'^{\mathsf{D}}} = 0$, hence $\mathbb{D}^*(G)(\mathsf{S})$ equals $\omega_{G'}$ by the beginning exact sequence. Apply the above computation we have $\mathbb{D}^*(G)(\mathsf{S}) = \mathsf{S}$. By Remark 5.2 we have $\mathbb{D}^*(G)(\mathsf{S})/\operatorname{Fil}^1\mathbb{D}^*(G)(\mathsf{S}) \simeq \operatorname{Lie}(G^{\mathsf{D}})$, the right hand is $\operatorname{Lie}(\mathbb{Q}_p/\mathbb{Z}_p)$ hence equals 0. So $\operatorname{Fil}^1\mathcal{M}(G) \simeq \mathcal{M}(G) = \mathsf{S}$.
(2) For the dual $\mathbb{Q}_p/\mathbb{Z}_p$, similarly we have $\mathcal{M}(\mathbb{Q}_p/\mathbb{Z}_p) = \mathsf{S}$, $\operatorname{Fil}^1\mathcal{M}(\mathbb{Q}_p/\mathbb{Z}_p) = \operatorname{Fil}^1\mathsf{S}$. Indeed, in this case $\mathbb{D}^*(G)(\mathsf{S})/\operatorname{Fil}^1\mathbb{D}^*(G)(\mathsf{S}) \simeq \mathcal{O}_K\frac{dT}{T}$ and hence $\operatorname{Fil}^1\mathcal{M}(G) \simeq \operatorname{Fil}^1\mathsf{S}$, since $\mathcal{O}_K \simeq \mathsf{S}/\operatorname{Fil}^1\mathsf{S}$.

6. Comparison theorems

6.1. **Period rings.**

Notation 6.2. From now on, K will always denote a complete discrete valuation field of characteristic 0, whose residue field k is perfect of characteristic p. For example when k is finite, K is a finite extension of $\mathbb{Q}_p$.
Let $v : K \to \mathbb{Q}\cup\{+\infty\}$ be the valuation normalized by $v(p) = 1$. Fix $\overline{K}$ an algebraic closure of K and let $\mathscr{G}_K = \operatorname{Gal}(\overline{K}/K)$ be the absolute Galois group. The valuation extends uniquely to a (non-discrete) valuation $v : \overline{K} \to \mathbb{Q}\cup\{+\infty\}$, which is $\mathscr{G}_K$*-equivariant, i.e.* $(\forall x \in \overline{K})(\forall g \in \mathscr{G}_K)\ v(g(x)) = v(x)$.
Let C be the completion of $\overline{K}$ for the valuation. The action of $\mathscr{G}_K$ extends to C by continuity. For any subfield $L \subset C$, we will write $\mathcal{O}_L$ (resp. $\mathfrak{m}_L$) for the ring of integers (resp. the maximal ideal) of L.
Finally, we put $W = W(k)$ and denote σ the Witt vectors Frobenius. It extends to $F := \operatorname{Frac}(W)$. One has $F \hookrightarrow K$, and the extension K/F is totally ramified of degree e_K(we have $v(K) = \dfrac{1}{e_K}\mathbb{Z}\cup\{\infty\}$). We denote by $|\cdot|$ the absolute value on C defined by $|x| = p^{-v(x)}$ for $x \in C$.

Definition 6.3. Let G be a profinite group. Let B be a topological ring with unity endowed with a continuous action of G, preserving the unity. Then a B-*representation* of G is a free B-module M of finite rank endowed with a continuous and semi-linear action of G, *i.e.*

$$(\forall g \in G)(\forall b \in B)(\forall m_1, m_2 \in M) \;\; g(bm_1 + m_2) = g(b)g(m_1) + g(m_2)$$

With B-linear G-equivalent maps, they form a category denoted by $\mathrm{Rep}_B(G)$.
We say that a B-representation M is *trivial* if $M \xrightarrow{\sim} B^d$ for some d, with the natural action of G.

Definition 6.4. Let ℓ be a prime number. A *ℓ-adic representation* of G is a $\mathbb{Q}_\ell$-representation (where the action of G on $\mathbb{Q}_\ell$ is trivial). An *integral ℓ-adic representation* of G is a $\mathbb{Z}_\ell$-representation of G.

In particular, $\mathrm{Rep}_{\mathbb{Q}_\ell}(\mathscr{G}_K)$ is the category of ℓ-adic representation of $\mathscr{G}_K$, and $\mathrm{Rep}_{\mathbb{Z}_\ell}(\mathscr{G}_K)$ is the category of $\mathbb{Z}_\ell$-representations of $\mathscr{G}_K$.

Definition 6.5. We say that V is *B-admissible* if $B \otimes_F V$ is a trivial B-representation of $\mathscr{G}_K$. The category of B-admissible representations is denoted by $\mathrm{Rep}^B(\mathscr{G}_K)$

Given the $B^{\mathscr{G}_K}$-vector space

$$D_B(V) := (B \otimes_F V)^{\mathscr{G}_K}$$

we have a linear map

$$\alpha_V : B \otimes_{B^{\mathscr{G}_K}} D_B(V) \to B \otimes_F V$$
$$\lambda \otimes x \mapsto \lambda x$$

Notice that $\mathscr{G}_K$ acts on $B \otimes_{B^{\mathscr{G}_K}} D_B(V)$ through $g(\lambda \otimes x) = g(\lambda) \otimes x$, for $\lambda \in B$, $x \in D_B(V)$, $g \in G$.

Definition 6.6. We say that B is *(F, G)-regular* if the following conditions holds:
(1) B is a domain;
(2) $B^{\mathscr{G}_K} = (\mathrm{Frac}\, B)^{\mathscr{G}_K}$;
(3) If a non-zero $b \in B$ satisfies that $\forall g \in \mathscr{G}_K$ there exists $\lambda \in F$ such that $g(b) = \lambda b$, then b is invertible.

For example, a field always satisfies the above conditions.

Proposition 6.7. [14, Theorem 2.13] *Suppose B is (F, G)-regular. Then for any F-representation V the map α_V is injective, and it is an isomorphism if and only if V is B-admissible.*

Put

$$\mathcal{R} = \varprojlim_{x \mapsto x^p} \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}} = \{(x_n)_{n\in\mathbb{N}} \in (\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})^{\mathbb{N}} | (\forall n \in \mathbb{N}) \;\; x_{n+1}^p = x_n\}$$

It is a perfect ring of characteristic p with an action of $\mathscr{G}_K$ (componentwise). It is a $\overline{k}$-algerba via the map

$$\overline{k} \to \mathcal{R}$$
$$x \mapsto (x, x^{1/p}, x^{1/p^2}, \ldots)$$

For $n \in \mathbb{N}$, we will denote by $\mathrm{pr}_n : \mathcal{R} \to \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ the projection on the n-th factor. This is a ring homomorphism. If $n \leq m$, and $x \in \mathcal{R}$, one has $\mathrm{pr}_m(x)^{m-n} = \mathrm{pr}_n(x)$. As $\overline{K}$ is algebraically closed, p^n-th roots always exists in $\mathcal{O}_{\overline{K}}$, so the maps pr_n are surjective.
The componentwise reduction modulo p provides a (multiplicative and $\mathscr{G}_K$-equivariant) map

$$\varprojlim_{x \mapsto x^p} \mathcal{O}_C = \{(x^{(n)})_{n\in\mathbb{N}} \in \mathcal{O}_C^{\mathbb{N}} | (\forall n \in \mathbb{N}) \;\; (x^{(n+1)})^p = x^{(n)}\} \to \mathcal{R}$$

Proposition 6.8. [15, Proposition 4.3.] *The map above is a bijection.*

Thanks to the proposition, we will identify $\mathcal{R}$ with $\varprojlim_{x\mapsto x^p} \mathcal{O}_C$. As C is algebraically closed, the maps

$$\begin{aligned} \mathcal{R} &\to \mathcal{O}_C \\ x &\mapsto x^{(n)} \end{aligned}$$

are surjective for all $n \in \mathbb{N}$.

Example 6.9. We will consider elements $\varepsilon := (\zeta_{p^n})_{n\geq 0}$ (resp. $\tilde{p} := (p^{(n)})_{n\geq 0}$ and $\tilde{\pi} := (\pi^{(n)})_{n\geq 0}$) in $\mathcal{R}$ (such that $p^{(0)} = p$ and $\pi^{(0)} = \pi$). Note that these elements are not canonical, since extration of p^n-th roots requires choices.

Notation 6.10. Fix a $\tilde{\pi} := (\pi^{(n)})_{n\geq 0} \in \mathcal{M}$, $\pi^{(0)} = \pi$. We define $K_\infty := K(\pi^{(n)})_{n\in\mathbb{N}}$. Notice our definition of K_∞ depends on the $\tilde{\pi}$ we fix.

Remark 6.11.
(1) Let $x = (x_n)_{n\in\mathbb{N}}$ and $y = (y_n)_{n\in\mathbb{N}}$ be elements in $\mathcal{R}$ corresponding to $(x^{(n)})_{n\in\mathbb{N}}$ and $(y^{(n)})_{n\in\mathbb{N}}$ in $\varprojlim_{x\mapsto x^p} \mathcal{O}_C$. As $x^{(n)}y^{(n)}$ lifts $x_n y_n$ and $(x^{(n+1)}y^{(n+1)})^p = x^{(n)}y^{(n)}$ for all $n \in \mathbb{N}$, one has $(xy)^{(n)} = x^{(n)}y^{(n)}$ for all $n \in \mathbb{N}$, *i.e.* $x \mapsto x^{(n)}$ is a multiplicative map. It is not additive, one has the formula

$$(x+y)^{(n)} = \lim_{m\to\infty} (x^{(n+m)} + y^{(n+m)})^{p^m}$$

(2) If $g \in G_K$, one has $g(\zeta_{p^n}) = \zeta_{p^n}^{\chi(g)}$ whence $g(\varepsilon) = \varepsilon^{\chi(g)}$.

If $x = (x^{(n)})_{n\in\mathbb{N}} \in \mathcal{R}$, we put

$$v_{\mathcal{R}}(x) := v(x^{(0)}) \in \mathbb{R}_{\geq 0} \cup \{\infty\}$$

For example, $v_{\mathcal{R}}(\tilde{p}) = 1$, $v_{\mathcal{R}}(\tilde{\pi}) = v(\pi)$. and $v_{\mathcal{R}}(\varepsilon - 1) = \lim_{m\to\infty} v(\zeta_{p^m} - 1)^{p^m} = \frac{p}{p-1}$, where $v_{\mathcal{R}}(\varepsilon - 1) = \lim_{m\to\infty} v(\zeta_{p^m} - 1)^{p^m}$ is by the concrete construction of the bijection between $\mathcal{R}$ and $\varprojlim_{x\mapsto x^p} \mathcal{O}_C$.

Proposition 6.12. *The map $v_{\mathcal{R}}$ is a valuation, for which $\mathcal{R}$ is complete. Moreover, the action of $\mathscr{G}_K$ on $\mathcal{R}$ is continuous for $v_{\mathcal{R}}$.*

Remark 6.13. Define a map as following

$$\begin{aligned} \theta : W(\mathcal{R}) &\to \mathcal{O}_C \\ (x_0, x_1, \ldots) &\mapsto \sum_{i=0}^{\infty} p^i x_i^{(i)} \end{aligned}$$

This is a $\mathscr{G}_K$-equivariant map.

Proposition 6.14. [15, Lemma 4.4.1] *θ is a surjective ring homomorphism.*

Proposition 6.15. [15, proposition 4.4.3] *The ideal* $\mathrm{Ker}(\theta)$ *is principal, generated by any element $x \in \mathrm{W}(\mathcal{R})$ whose reduction $\overline{x} \in \mathcal{R}$ satisfies $v_{\mathcal{R}}(\overline{x}) = 1$. For instance, $\xi := [\tilde{p}] - p$ is such an element.*

Example 6.16. Let $\varpi = \frac{[\varepsilon]-1}{[\varepsilon^{1/p}]-1} = 1 + [\varepsilon^{1/p}] + [\varepsilon^{1/p}]^2 + \cdots + [\varepsilon^{1/p}]^{p-1} \in \mathrm{W}(\mathcal{R})$. One has $\overline{\varpi} = \frac{\varepsilon - 1}{\varepsilon^{1/p} - 1} = (\varepsilon^{1/p} - 1)^{p-1}$, so $v_{\mathcal{R}}(\overline{\varpi}) = (p-1)v_{\mathcal{R}}(\varepsilon^{1/p} - 1) = \frac{p-1}{p} v_{\mathcal{R}}(\varepsilon - 1) = 1$, so $\mathrm{Ker}(\theta) = \varpi\, \mathrm{W}(\mathcal{R})$.

Remark 6.17. By proposition and example above we see ϖ is a generator of $\mathrm{Ker}(\theta)$.

Definition 6.18. Let $\mathrm{A}_{\mathrm{cris}}$ be the p-adic completion of the P.D. envelope of $\mathrm{W}(\mathcal{R})$ with respect to the ideal $\mathrm{Ker}(\theta)$

Hence we see that

$$\mathrm{A}_{\mathrm{cris}} = \widehat{\mathcal{D}_{\mathrm{W}(\mathcal{R})}(\mathrm{Ker}(\theta))} = \widehat{\mathrm{W}(\mathcal{R})[\xi^{[i]}]}$$

Proposition 6.19. *The action of $\mathscr{G}_K$ and of the Witt vectors Frobenius on* $\mathrm{W}(\mathcal{R})$ *extends to an action of $\mathscr{G}_K$ and a Frobenius operator φ on A_{cris}.*

Recall that

$$\mathsf{S} = \widehat{W[u][\mathrm{E}(u)^{[i]}]}$$

Then we have the following map

$$W[u] \to \mathrm{A}_{\mathrm{cris}}$$
$$u \mapsto [\tilde{\pi}]$$

Since

$$\mathrm{E}(u) \mapsto \mathrm{E}([\tilde{\pi}]) \xrightarrow{\theta} \mathrm{E}(\pi) = 0$$

so the image of the P.D. ideal $(\mathrm{E}(u))$ is inside $\mathrm{Ker}(\theta)$, a P.D. ideal of $\mathrm{A}_{\mathrm{cris}}$. Hence the previous map extends into

$$W[u][\mathrm{E}(u)^{[i]}] \to \mathrm{A}_{\mathrm{cris}}$$

cf Theorem 3.9.

As $\mathrm{A}_{\mathrm{cris}}$ is p-adically separated and complete, it extends into a map $\mathsf{S} \to \mathrm{A}_{\mathrm{cris}}$. This endows $\mathrm{A}_{\mathrm{cris}}$ with a S-algebra structure.

Remark 6.20. $\mathsf{S} \subset \mathrm{A}_{\mathrm{cris}}^{\mathscr{G}_{K_\infty}}$ but S is not stable under the action of $\mathscr{G}_K$ in $\mathrm{A}_{\mathrm{cris}}$.

Put

$$t = \log([\varepsilon]) := \sum_{n=1}^{\infty} (-1)^{n-1} \frac{([\varepsilon]-1)^n}{n}$$

notice

$$t = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{([\varepsilon]-1)^n}{n} = \sum_{n=1}^{\infty} (-1)^{n-1} (n-1)! ([\varepsilon]-1)^{[n]}$$

Hence $\mathbb{Z}_p\, t \subset \mathrm{A}_{\mathrm{cris}}$.

Proposition 6.21. *$g(t) = \chi(g)t$ and $\varphi(t) = pt$.*

Theorem 6.22.
(1) (Universal property of $\mathrm{A}_{\mathrm{cris}}$*). The map $\theta : \mathrm{A}_{\mathrm{cris}} \to \mathcal{O}_C$ is a universal p-adically complete divided powers thickening of $\mathcal{O}_C$, i.e. for any p-adically separated and complete ring A, and any continuous and surjective ring homomorphism $\lambda : A \to \mathcal{O}_C$ whose kernel has divided powers (compatible with the canonical divided powers on pA), there exists a unique homomorphism $\alpha : \mathrm{A}_{\mathrm{cris}} \to A$ such that the diagram*

$$\begin{tikzcd}
\mathrm{A}_{\mathrm{cris}} \arrow[rr, dotted, "\alpha"] \arrow[dr, "\theta"'] & & A \arrow[dl] \\
& \mathcal{O}_C &
\end{tikzcd}$$

commutes.
(2) Crystalline interpretation of $\mathrm{A}_{\mathrm{cris}}$*. We have:*

$$\mathrm{A}_{\mathrm{cris}} = \varprojlim_n H^0(\mathrm{Spec}(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})/W_n)_{cris}, \mathcal{O}_{\mathrm{Spec}(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})/W_n})$$

Definition 6.23. $\mathrm{B}_{\mathrm{cris}} := \mathrm{A}_{\mathrm{cris}}[\frac{1}{t}]$.

Remark 6.24.
(1) $p \in \mathrm{B}_{\mathrm{cris}}^{\times}$, hence $\mathrm{B}_{\mathrm{cris}}$ is a K_0-module, where $K_0 = W[\frac{1}{p}]$.
(2) In fact, $\mathrm{B}_{\mathrm{cris}}^{\mathscr{G}_K} = K_0$.

Definition 6.25. We say that a p-adic representation V of $\mathscr{G}_K$ is *crystalline* if it is $\mathrm{B}_{\mathrm{cris}}$-admissible. We denote by $\mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{cris}}(\mathscr{G}_K)$ the corresponding subcategory of $\mathrm{Rep}_{\mathbb{Q}_p}(\mathscr{G}_K)$.

In particular we have a functor

$$\mathrm{D}_{\mathrm{cris}} := \mathrm{D}_{\mathrm{B}_{\mathrm{cris}}} : \mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{cris}}(\mathscr{G}_K) \to \mathbf{Mod}_{K_0}(\varphi)$$

where $\mathbf{Mod}_{K_0}(\varphi)$ is the category of finite dimensional K_0-vector spaces D endowed with a semi-linear Frobenius operator:

$$\varphi : D \to D$$

(*i.e.* $\varphi(\sigma\alpha) = \varphi(\sigma)\varphi(\alpha)$ for all $\sigma \in K_0$ and $\alpha \in D$.)

Notation 6.26. Let $\mathrm{T}_p(\mathbb{G}_m) = \varprojlim_n \mu_{p^n}(\overline{K}) = \mathbb{Z}_p(1)$ denote the Tate module of the multiplicative group, which is isomorphic to $\mathbb{Z}_p$ as a group but also possesses a Galois action given by the p-adic cyclotomic character $\chi : \mathscr{G}_K \to \mathbb{Z}_p^{\times}$:

$$g \cdot x = \chi(g)x \text{ for all } g \in \mathscr{G}_K.$$

More generally, if $i \in \mathbb{Z}$ and M is an $\mathbb{Z}_p$-module with an action by $\mathscr{G}_K$, denoted $(g, m) \mapsto g(m)$, then we may form a $\mathscr{G}_K$-module $M(i)$ which is M as a group, but whose Galois action is twisted by the i-th power of the cyclotomic character:
for all $m \in M(i)$,

$$g \cdot m = \chi(g)^i g(m) \text{ for all } g \in \mathscr{G}_K$$

Definition 6.27. The module $M(i)$ is called the *i-th Tate twist* of M.

Consequently, $M(i)$ may be realized as

$$M(i) = M \otimes_{\mathbb{Z}_p} \mathrm{T}_p(\mathbb{G}_m)^{\otimes i}$$

Example 6.28. Given $i \in \mathbb{Z}$, $\mathrm{D}_{\mathrm{cris}}(\mathbb{Q}_p(i)) \simeq \{b \in \mathrm{B}_{\mathrm{cris}} \,|(\forall g \in \mathscr{G}_K)\ \ g(b)\chi^i(g) = b\}$

$$g(b)\chi^i(g) = b \Leftrightarrow g(b)\chi^i(g)t^i = bt^i \Leftrightarrow g(bt^i) = bt^i$$

$$\mathrm{D}_{\mathrm{cris}}(V) \cong \{b \in \mathrm{B}_{\mathrm{cris}} \,|bt^i \in \mathrm{B}_{\mathrm{cris}}^{\mathscr{G}_K}\} = \{b \in \mathrm{B}_{\mathrm{cris}} \,|bt^i \in K_0\} = t^{-i}K_0$$

Recall that

$$\mathrm{T}_p(G) = \mathrm{Hom}_{\mathbf{BT}(\mathcal{O}_{\overline{K}})}(\mathbb{Q}_p/\mathbb{Z}_p, G_{\mathcal{O}_{\overline{K}}})$$

Given

$$f : \mathbb{Q}_p/\mathbb{Z}_p \to G_{\mathcal{O}_{\overline{K}}}$$

a map in $\mathbf{BT}(\mathcal{O}_{\overline{K}})$ and we still denote by f its base change to $\mathcal{O}_C$. Since $\mathbb{D}^*$ is a contravariant functor, we induce a map

$$\mathbb{D}^*(f) : \mathbb{D}^*(G_{\mathcal{O}_C}) \to \mathbb{D}^*(\mathbb{Q}_p/\mathbb{Z}_p)$$

Its envaluation at the P.D. thickening $\operatorname{Spec} \mathcal{O}_C \to \operatorname{Spec} \mathrm{A}_{\mathrm{cris}}$ provides a map

$$\mathbb{D}^*(f)_{\mathrm{A}_{\mathrm{cris}}} : \mathbb{D}^*(G_{\mathcal{O}_C})_{\mathrm{A}_{\mathrm{cris}}} \to \mathbb{D}^*(\mathbb{Q}_p/\mathbb{Z}_p)_{\mathrm{A}_{\mathrm{cris}}} \simeq \mathrm{A}_{\mathrm{cris}}$$

We already saw that $\mathrm{A}_{\mathrm{cris}}$ is an S-module before Remark 6.16, hence given any element $a \in \mathbb{D}^*(G)(\mathsf{S})$ we map it to an element $a_{\mathrm{A}_{\mathrm{cris}}} \in \mathbb{D}^*(G)_{\mathrm{A}_{\mathrm{cris}}}$. Hence the following pairing is well-defined.

$$\begin{aligned} \mathrm{T}_p(G) \times \mathbb{D}^*(G)(\mathsf{S}) &\to \mathrm{A}_{\mathrm{cris}} \\ (f,a) &\mapsto (\mathbb{D}^*(f)_{\mathrm{A}_{\mathrm{cris}}})(a_{\mathrm{A}_{\mathrm{cris}}}) \end{aligned}$$

It induces an S-linear map

$$\mathbb{D}^*(G)(\mathsf{S}) \to \mathrm{A}_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee$$

By $\mathrm{A}_{\mathrm{cris}}$-linearity we have

$$\rho_G : \mathrm{A}_{\mathrm{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(G)(\mathsf{S}) \to \mathrm{A}_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee$$

Lemma 6.29.

$$\mathrm{T}_p(G^{\mathsf{D}}) \simeq (\mathrm{T}_p\, G)^\vee(1)$$

Proof. By definition we have

$$G_n^{\mathsf{D}}(\overline{K}) = \mathrm{Hom}_{\mathrm{gr}}(G_n(\overline{K}), \overline{K}^\times) = \mathrm{Hom}_{\mathrm{gr}}(G_n(\overline{K}), \mu_{p^\infty}(\overline{K}))$$

For any $n \in \mathbb{N}$, the map $j_n : G_{n+1}^{\mathsf{D}} \to G_n^{\mathsf{D}}$ is i_n^{D} where $i_n : G_n \to G_{n+1}$ is the closed immersion that identifies G_n with the p^n-torsion of G_{n+1}. Then

$$\begin{aligned} \mathrm{T}_p(G^{\mathsf{D}}) &= \varprojlim_{j_n} G_n^{\mathsf{D}}(\overline{K}) \\ &= \varprojlim_{j_n} \mathrm{Hom}_{\mathrm{gr}}(G_n(\overline{K}), \mu_{p^\infty}(\overline{K})) \\ &= \mathrm{Hom}_{\mathrm{gr}}(\varinjlim_{i_n} G_n(\overline{K}), \mu_{p^\infty}(\overline{K})) \\ &= \mathrm{Hom}_{\mathrm{gr}}(G(\overline{K}), (\mathbb{Q}_p/\mathbb{Z}_p)(1)) \end{aligned}$$

Since $\mathrm{T}_p(G) = \mathrm{Hom}_{\mathrm{gr}}(\mathbb{Q}_p/\mathbb{Z}_p, G(\overline{K}))$ implies $G(\overline{K}) \simeq \mathrm{T}_p\, G \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p)$ and so we have

$$\begin{aligned} \mathrm{T}_p(G^{\mathsf{D}}) &\simeq \mathrm{Hom}_{\mathrm{gr}}(\mathrm{T}_p(G) \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p), (\mathbb{Q}_p/\mathbb{Z}_p)(1)) \\ &\simeq \mathrm{Hom}_{\mathrm{gr}}(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee(1) \\ &= \mathbb{Z}_p \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee(1) \\ &= (\mathrm{T}_p\, G)^\vee(1) \end{aligned}$$

□

Remark 6.30. By Cartier duality there is a pairing

$$G_m(\overline{K}) \times G_n^{\mathsf{D}}(\overline{K}) \to \mu_{p^n}(\overline{K})$$

for all $m \leq n$. Taking projective limit on m we have

$$\mathrm{T}_p\, G \times G_n^{\mathsf{D}}(\overline{K}) \to \mu_{p^n}(\overline{K})$$

Taking projective limit on n we have

$$\mathrm{T}_p\, G \times \mathrm{T}_p(G^{\mathsf{D}}) \to \mathrm{T}_p(\mu_{p^\infty}) = \mathbb{Z}_p(1)$$

hence the map

$$\mathrm{T}_p(G^{\mathsf{D}}) \to (\mathrm{T}_p\, G)^\vee(1)$$

of Lemma 6.29.

Theorem 6.31. [16, Section 6] *ρ_G is a functorial injection, respecting Frobenius and $\mathscr{G}_{K_\infty}$ action. Its cokernel is killed by t.*

Proof. We use same notation as in the above lemma. To study ρ_G, we first consider the special case of $G = \mu_{p^\infty}$, where $\mathrm{T}_p(\mu_{p^\infty}) = \mathbb{Z}_p(1)$.

$$\begin{tikzcd}
\mathrm{A_{cris}} \otimes_{\mathsf{S}} \mathsf{S}\frac{dT}{T} \arrow[r, "\rho_{\mu_{p^\infty}}"] \arrow[d, "\simeq"'] & \mathrm{A_{cris}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-1) \arrow[d, "\simeq"] \\
\mathrm{A_{cris}} \arrow[r, hook] & \mathrm{A_{cris}}(-1) = t^{-1}\,\mathrm{A_{cris}}
\end{tikzcd}$$

Then we reduce the general case to this one. Consider

$$\rho_G : \mathrm{A_{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(G)(\mathsf{S}) \to \mathrm{A_{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee$$

Let $y \in (\mathrm{T}_p(G))^\vee \simeq (\mathrm{T}_p(G^{\mathsf{D}}))(-1)$, hence ty defines an element in

$$\mathrm{T}_p(G^{\mathsf{D}}) = \mathrm{Hom}_{\mathbf{BT}(\mathcal{O}_{\overline{K}})}(\mathbb{Q}_p/\mathbb{Z}_p, G^{\mathsf{D}} \otimes \mathcal{O}_{\overline{K}})$$

Hence $(ty)^{\mathsf{D}} \in \mathrm{Hom}_{\mathbf{BT}(\mathcal{O}_{\overline{K}})}(G \otimes \mathcal{O}_{\overline{K}}, \mu_{p^\infty})$ and this induces a morphism:

$$\mathbb{D}^*((ty)^{\mathsf{D}})_{\mathrm{A_{cris}}} : \mathrm{A_{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(\mu_{p^\infty})(\mathsf{S}) \to \mathrm{A_{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(G)(\mathsf{S})$$

Also

$$\begin{aligned}(\mathrm{T}_p(ty)^{\mathsf{D}})^\vee(1) \simeq \mathrm{T}_p(ty) : \mathbb{Z}_p &\to \mathrm{T}_p(G^{\mathsf{D}}) = (\mathrm{T}_p\, G)^\vee(1)\\ 1 &\mapsto ty\end{aligned}$$

gives a map

$$\begin{aligned}(\mathrm{T}_p(ty)^{\mathsf{D}})^\vee : \mathbb{Z}_p(-1) &\to (\mathrm{T}_p\, G)^\vee\\ t^{-1} &\mapsto y\end{aligned}$$

We have the following commutative diagram:

$$\begin{tikzcd}
\mathrm{A_{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(G)(\mathsf{S}) \arrow[r, "\rho_G"] & \mathrm{A_{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee \\
\mathrm{A_{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(\mu_{p^\infty})(\mathsf{S}) \arrow[u, "\mathbb{D}^*((ty)^{\mathsf{D}})_{\mathrm{A_{cris}}}"] \arrow[r, hook, "\rho_{\mu_{p^\infty}}"] & \mathrm{A_{cris}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-1) \arrow[u, "1\otimes(\mathrm{T}_p(ty)^{\mathsf{D}})^\vee"']
\end{tikzcd}$$

where

$$\begin{array}{ccccc}
\mathrm{A_{cris}} \simeq \mathrm{A_{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(\mu_{p^\infty})(\mathsf{S}) & \xrightarrow{\rho_{\mu_{p^\infty}}} & \mathrm{A_{cris}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-1) & \xrightarrow{1\otimes \mathrm{T}_p((ty)^{\mathsf{D}})^\vee} & \mathrm{A_{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee \\
1 \otimes 1 & \longmapsto & -t \otimes t^{-1} & \longmapsto & -t\otimes y
\end{array}$$

Hence $-t \otimes y = \rho_G((\mathbb{D}^*((ty)^{\mathsf{D}})_{\mathrm{A_{cris}}}(1 \otimes 1)) \in \mathrm{Im}\,\rho_G$ and so we proved $\mathrm{Coker}\,\rho_G$ is killed by t.

It is left to prove ρ_G is injective. $\mathrm{A_{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(G)(\mathsf{S})$ and $A_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee$ are two free $\mathrm{A_{cris}}$-module of the same rank h, hence ρ_G is given by a matrix $\mathrm{M} \in \mathrm{M_h}(\mathrm{A_{cris}})$. $\mathrm{Coker}\,\rho_G$ is killed by t implies $\det(\mathrm{M}) \in (\mathrm{A_{cris}}[1/t])^\times$ and hence $\det(\mathrm{M})$ is a nonzero divisor (in fact $\mathrm{A_{cris}}$ is integral). So we proved ρ_G is injective. □

Remark 6.32. We give a precise computation of the map $\rho_{\mu_{p^\infty}}$ we used in the proof above. $t \in \mathrm{T}_p(\mu_{p^\infty}) = \mathbb{Z}(1)$ corresponds to the map of $\mathbf{BT}(\mathcal{O}_{\overline{K}})$

$$\begin{aligned}u_0 : \mathbb{Q}_p/\mathbb{Z}_p &\to \mu_{p^\infty}\\ \frac{1}{p^n} &\mapsto \zeta_{p^n}\end{aligned}$$

i.e. to the action of $\varepsilon = (\zeta_{p^n})_n \in \mathcal{R}$. The universal extension of $\mathbb{Q}_p/\mathbb{Z}_p$ is

$$0 \to \mathbb{G}_a \to \frac{\mathbb{G}_a \oplus \mathbb{Q}_p}{\mathbb{Z}_p} \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

that of μ_{p^∞} is

$$0 \to 0 \to \mu_{p^\infty} \to \mu_{p^\infty} \to 0$$

On $\mathcal{O}_C$ we have the morphism of extensions

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_C \arrow[r] \arrow[d, "\underline{V}(u_0)=0"] & \frac{\mathcal{O}_C \oplus \mathbb{Q}_p}{\mathbb{Z}_p} \arrow[r] \arrow[d, "v_0"] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] \arrow[d, "u_0"] & 0 \\
0 \arrow[r] & 0 \arrow[r] & \mu_{p^\infty}(\mathcal{O}_C) \arrow[r] & \mu_{p^\infty}(\mathcal{O}_C) \arrow[r] & 0
\end{tikzcd}$$

where $u_0(\lambda, z) = (\varepsilon^z)^{(0)}$ for $\lambda \in \mathcal{O}_C$ and $z \in \mathbb{Q}_p$ (for example, $u_0(0, \frac{1}{p^n}) = \zeta_{p^n}$ and $u_0(\lambda, 0) = 0$ for $\lambda \in \mathcal{O}_C$). By Theorem 4.7, there exist an unique morphism

$$v : \frac{\mathrm{A}_{\mathrm{cris}} \oplus \mathbb{Q}_p}{\mathbb{Z}_p} \to \mathrm{A}_{cris}^{\times}$$

such that (1) v is a lifting of v_0; (2) $d = -v|_{\underline{V}(\mathbb{Q}_p/\mathbb{Z}_p)_{\mathrm{A}_{\mathrm{cris}}}}$ is an exponential. Put

$$\begin{aligned}\tilde{v} : \mathrm{A}_{\mathrm{cris}} \oplus \mathbb{Q}_p &\to \mathrm{A}_{\mathrm{cris}} \\ (a, z) &\mapsto \exp(-ta)[\varepsilon^z]\end{aligned}$$

then $\theta(\tilde{v}(a, z)) = \theta([\varepsilon^z]) = (\varepsilon^z)^{(0)}$ so (1) holds and $\tilde{v}(a, 0) = \exp(-ta)$ so (2) holds (note that (2) is in addition notation while $\tilde{v}$ is multiplicative). By unicity we must have $\tilde{v} = v$ and hence we get:

$$\mathbb{D}^*(t)_{\mathrm{A}_{\mathrm{cris}}}(a) = \log((\exp(-at)) = -at$$

Hence we have

$$\begin{aligned}\mathrm{A}_{\mathrm{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(\mu_{p^\infty})(\mathsf{S}) &\to \mathrm{A}_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(-1) \\ 1 \otimes 1 &\mapsto -t \otimes t^{-1}\end{aligned}$$

and so $\rho_{\mu_{p^\infty}}$ identifies with the inclusion $\mathrm{A}_{\mathrm{cris}} \subset \frac{1}{t}\,\mathrm{A}_{\mathrm{cris}}$.

Corollary 6.33. *ρ_G induces a $\mathscr{G}_{K_\infty}$-equivariant, Frobenius compatible isomorphism*

$$\tilde{\rho_G} : \mathrm{B}_{\mathrm{cris}} \otimes_W D(G_0) = \mathrm{B}_{\mathrm{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(G)(\mathsf{S}) \xrightarrow{\sim} \mathrm{B}_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee$$

Where G_0 is the special fiber $G \times_{\mathrm{Spec}\, \mathcal{O}_K} \mathrm{Spec}\, k$ and $D(G_0)$ is the classical contravariant Dieudonné module of G_0.

Proof. The first equality holds because the Dieudonné module is stable with base change. □

Theorem 6.34. *ρ_G is $\mathscr{G}_K$-equivariant.*

Proof. Recall that

$$\mathrm{T}_p\, G \to \mathrm{Hom}_{\mathbf{BT}(\mathcal{O}_C)}(\mathbb{Q}_p/\mathbb{Z}_p, G_{\mathcal{O}_C}) \xrightarrow{\mathbb{D}^*_{\mathrm{A}_{\mathrm{cris}}}} \mathrm{Hom}_{\mathrm{A}_{\mathrm{cris}}}(\mathbb{D}^*(G_{\mathcal{O}_C})_{\mathrm{A}_{\mathrm{cris}}}, \mathbb{D}^*(\mathbb{Q}_p/\mathbb{Z}_p)_{\mathrm{A}_{\mathrm{cris}}})$$

Both maps are $\mathscr{G}_K$-equivariant (where the action of $\mathscr{G}_K$ on $\mathbb{D}^*(G_{\mathcal{O}_C})_{\mathrm{A}_{\mathrm{cris}}}$ is induced by the natural action on $\mathrm{A}_{\mathrm{cris}}$).
As $\mathbb{D}^*(\mathbb{Q}_p/\mathbb{Z}_p)_{\mathrm{A}_{\mathrm{cris}}} \simeq \mathrm{A}_{\mathrm{cris}}$, we get an $\mathrm{A}_{\mathrm{cris}}$-linear, $\mathscr{G}_K$-equivariant and φ-compatible map:

$$\mathrm{A}_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} \mathrm{T}_p\, G \to \mathrm{Hom}_{\mathrm{A}_{\mathrm{cris}}}(\mathbb{D}^*(G_{\mathcal{O}_C})_{\mathrm{A}_{\mathrm{cris}}}, \mathrm{A}_{\mathrm{cris}})$$

hence a map

$$\rho_G : \mathrm{A}_{\mathrm{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(G)(\mathsf{S}) \simeq \mathbb{D}^*(G_{\mathcal{O}_C})_{\mathrm{A}_{\mathrm{cris}}} \to \mathrm{A}_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee$$

□

Remark 6.35. ρ_G is $\mathscr{G}_K$-equivariant, but the composition

$$\mathbb{D}^*(G)(\mathsf{S}) \to \mathrm{A}_{\mathrm{cris}} \otimes_{\mathsf{S}} \mathbb{D}^*(G)(\mathsf{S}) \xrightarrow{\rho_G} \mathrm{A}_{\mathrm{cris}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee$$

is only $\mathscr{G}_{K_\infty}$-equivariant.

Corollary 6.36. *The p-adic representation* $\mathrm{V}_p\, G := \mathrm{T}_p\, G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ *is crystalline and*

$$\mathrm{D}_{\mathrm{cris}}(\mathrm{V}_p\, G) \simeq (D(G_0))^\vee \otimes_W W[\frac{1}{p}]$$

6.37. **The de Rham and Hodge-Tate comparison isomorphisms.**

Recall there is a surjective ring homomorphism $\mathrm{W}(\mathcal{R}) \to \mathcal{O}_C$, inverting p we get a map $\theta : \mathrm{W}(\mathcal{R})[1/p] \to C$ with kernel principal and generated by ξ.

Definition 6.38. $\mathrm{B}_{\mathrm{dR}}^+ = \varprojlim_n \mathrm{W}(\mathcal{R})[1/p]/(\xi^n)$ is the $\operatorname{Ker}\theta$-adic completion of $\mathrm{W}(\mathcal{R})[1/p]$.

Proposition 6.39.
(1) The map θ extends into a surjective ring homomorphism:

$$\mathrm{B}_{\mathrm{dR}}^+ \to C$$

(2) $\mathrm{B}_{\mathrm{dR}}^+$ *is a complete DVR with maximal ideal* $\operatorname{Ker}\theta$ *and residue field* C*;*
(3) $\mathrm{B}_{\mathrm{dR}}^+$ *carries an action of* $\mathscr{G}_K$ *for which* θ *is equivariant;*
(4) $t = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}([\varepsilon]-1)^n$ *converges in* $\mathrm{B}_{\mathrm{dR}}^+$ *and is an uniformizer of* $\mathrm{B}_{\mathrm{dR}}^+$.

Definition 6.40. $\mathrm{B}_{\mathrm{dR}} := \mathrm{B}_{\mathrm{dR}}^+[1/t] = \mathrm{Frac}(\mathrm{B}_{\mathrm{dR}}^+)$.

We endow B_{dR} with the valuation filtration: $\mathrm{Fil}^i\, \mathrm{B}_{\mathrm{dR}} := t^i\, \mathrm{B}_{\mathrm{dR}}^+$ for all $i \in \mathbb{Z}$.

Remark 6.41. $\mathrm{gr}\, \mathrm{B}_{\mathrm{dR}} = C[t, t^{-1}]$. Indeed, $\mathrm{gr}^i\, \mathrm{B}_{\mathrm{dR}} = t^i\, \mathrm{B}_{\mathrm{dR}}^+ / t^{i+1}\, \mathrm{B}_{\mathrm{dR}}^+ = t^i(\mathrm{B}_{\mathrm{dR}}^+/(t)) = Ct^i$ and so $\mathrm{gr}\, \mathrm{B}_{\mathrm{dR}} = \oplus_{i\in\mathbb{Z}} \mathrm{gr}^i\, \mathrm{B}_{\mathrm{dR}} = \oplus_{i\in\mathbb{Z}} Ct^i = C[t, t^{-1}]$.

Theorem 6.42. $(Tate)$ [8, Section 3, Proposition 8]

$$H^0(\mathscr{G}_K, C(i)) = \begin{cases} K & \text{if } i{=}0 \\ 0 & \text{if } i{\neq}0 \end{cases} \tag{1}$$

$$H^1(\mathscr{G}_K, C(i)) = \begin{cases} K \log \chi & \text{if } i{=}0 \\ 0 & \text{if } i{\neq}0 \end{cases} \tag{2}$$

Corollary 6.43. [14, 1.5.7] $H^0(\mathscr{G}_K, \mathrm{B}_{\mathrm{dR}}) = K$.

Proposition 6.44. [14, 4.2.3] $\mathrm{B}_{\mathrm{cris}} \subset K \otimes_{K_0} \mathrm{B}_{\mathrm{cris}} \subset \mathrm{B}_{\mathrm{dR}}$.

We endow $D(G_0)_K := D(G_0) \otimes_{K_0} K$ with its Hodge filtration, given by

$$\begin{aligned} &\mathrm{Fil}^i\, D(G_0)_K = D(G_0)_K, && \text{if } \leq 0 \\ &\mathrm{Fil}^1\, D(G_0)_K = \omega_G \otimes_{\mathcal{O}_K} K, && \text{if } i = 1 \\ &\mathrm{Fil}^i\, D(G_0)_K = 0, && \text{if } i \geq 2 \end{aligned}$$

Extending the scalars, $\tilde{\rho}_G$ induces an isomorphism, which is compatible with filtrations:

Theorem 6.45. (*de Rham comparison theorem*)

$$\tilde{\rho}_G : \mathrm{B}_{\mathrm{dR}} \otimes_K D(G_0)_K \xrightarrow{\sim} \mathrm{B}_{\mathrm{dR}} \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee$$

Proof. By what we discussed above. □

Theorem 6.46. (*Hodge-Tate comparison theorem*) [8, Section 4, Corollary 2]

$$C \otimes_{\mathbb{Z}_p} (\mathrm{T}_p\, G)^\vee \simeq C \otimes_{\mathcal{O}_K} \mathrm{Lie}(G^{\mathsf{D}}) \oplus C(-1) \otimes_{\mathcal{O}_K} (\mathrm{Lie}\, G)^\vee$$

Proof. This follows directly by taking the gr^0 on both sides of the de Rham comparison theorem. □

Corollary 6.47. *The height and dimension of $G \in \mathbf{BT}(\mathcal{O}_K)$ only depends on the generic fiber $G_K = G \otimes_{\mathcal{O}_K} K \in \mathbf{BT}(K)$.*

Proof.

$$\begin{aligned} d &= \mathrm{rank}(\mathrm{Lie}\, G) = \dim_K (C(1) \otimes_{\mathbb{Z}_p} \mathrm{T}_p\, G)^{\mathscr{G}_K} \\ h &= \mathrm{rank}(\mathrm{T}_p\, G) \end{aligned}$$

By Remark 2.36, $\mathrm{T}_p(G) = \mathrm{Hom}_{\mathbf{BT}(\mathcal{O}_{\overline{K}})}(\mathbb{Q}_p/\mathbb{Z}_p, G \otimes \mathcal{O}_{\overline{K}})$, and hence $\mathrm{T}_p(G)$ depends only on the generic fibre. □

Proposition 6.48. [8, Proposition 2] *Suppose (G_v, i_v) is a p-divisible group with $G_v = \mathrm{Spec}\, A_v$. Then the discriminant ideal of A_v over R is generated by $p^{nvp^{hv}}$, where $h = \mathrm{ht}(G)$ and $n = \dim(G)$.*

Theorem 6.49. *Let R be an integrally closed, noetherian, integral domain, whose field of fractions K is of characteristic 0. Let G and H be p-divisible groups over R. A homomorphism $f : G \otimes_R K \to H \otimes_R K$ of the general fibers extends uniquely to a homomorphism $G \to H$, i.e. the restriction functor*

$$\mathbf{BT}(\mathrm{Spec}\, R) \to \mathbf{BT}(\mathrm{Spec}\, K)$$

is fully faithful.

Corollary 6.50. *The map $\mathrm{Hom}(G, H) \to \mathrm{Hom}_{\mathscr{G}_K}(\mathrm{T}_p(G), \mathrm{T}_p(H))$ is bijective.*

Corollary 6.51. *If $g : G \to H$ is a homomorphism such that its restration $G \otimes_R K \to H \otimes_R K$ is an isomorphism, then g is an isomorphism.*

Since $R = \cap_p R_p$, where p runs over the minimal non-zero primes of R, and since each R_p is a discrete valuation ring, we are immediately reduced to the case R is a discrete valuation ring. There exists an extension $R^{'}$ of R which is a complete discrete valuation ring with algebraically closed residue field and such that $R = R^{'} \cap K$; hence we may assume R is complete with algebraically closed residue field. If $chark \neq p$, then G is étale and the theorem is obvious. Thus we are reduced to the case of mixed characteristic, which we assume from now on.

Proof of Corollary 6.51. Let $G = (G_v)$ and $H = (H_v)$, and let A_v (resp. B_v) denote the affine algebra of G_v (resp. H_v), We are given a coherent system of homomorphisms $u_v : B_v \to A_v$, of which we know that their extensions $u_v \otimes 1 : B_v \otimes_R K \to A_v \otimes_R K$ are isomorphisms. Since B_v is free over R, it follows that u_v is injective for all v. To prove surjectivity, we look at the discriminants of the R-algebras A_v and B_v. By Proposition 6.48 these discriminants are non-zero, and are determined by the heights of G and H and their dimensions. But the height and dimension of a p-divisible group over R are determined by its general fiber by Corollary 6.47. Hence the discriminants of A_v and B_v are equal and non-zero, and it follows that u_v is bijective. This proves Corollary 6.51. □

Proposition 6.52. [8, Proposition 12] *Suppose F is a p-divisible group over R, and M a $\mathscr{G}_K$-submodule of $\mathrm{T}_p(F)$ such that M is a $\mathbb{Z}_p$-direct summand. Then there exists a p-divisible group Γ over R and a homomorphism $\varphi : \Gamma \to F$ such that φ induces an isomorphism $\mathrm{T}_p(\Gamma) \xrightarrow{\sim} M$.*

Proof of Theorem 6.49. Granting this Proposition we prove the theorem, letting $F = G \times H$, and letting M be the graph of the homomorphism $\mathrm{T}_p(G) \to \mathrm{T}_p(H)$ which corresponds to the given homomorphism $f : G \otimes_R K \to H \otimes_R K$. By Proposition 6.52 we get a p-divisible group Γ over R and a homomorphism $\varphi : \Gamma \to G \times H$ such that the composition $\mathrm{pr}_1 \circ \varphi : \Gamma \to G$ induces an isomorphism $\mathrm{T}_p(\Gamma) \to \mathrm{T}_p(G)$, hence an isomorphism on the general fibers. By Corollary 6.51, it follows that $\mathrm{pr}_1 \circ \varphi$ is an isomorphism. Thus $\mathrm{pr}_2 \circ \varphi \circ (\mathrm{pr}_1 \circ \varphi)^{-1} : G \to H$ is a homomorphism extending f. The unicity of such an extension is obvious, and this concludes the proof of Theorem 6.49.

□

References

[1] D. Mumford, *Abelian varieties*, vol. 5. Oxford University Press, USA, 1974.
[2] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106. Springer Science & Business Media, 2009.
[3] W. Messing, "The crystals associated to barsotti-tate groups," *The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes*, pp. 112–149, 1972.
[4] W. C. Waterhouse, *Introduction to affine group schemes*, vol. 66. Springer Science & Business Media, 2012.
[5] J. Tate, "Finite flat group schemes," in *Modular forms and Fermats last theorem*, pp. 121–154, Springer, 1997.
[6] A. Vistoli, "Notes on grothendieck topologies, fibered categories and descent theory," *arXiv preprint math/0412512*, 2004.
[7] S. S. Shatz, "Group schemes, formal groups, and p-divisible groups," in *Arithmetic geometry*, pp. 29–78, Springer, 1986.
[8] J. T. Tate, "p-divisible groups," in *Proceedings of a conference on local fields*, pp. 158–183, Springer, 1967.
[9] P. Berthelot and A. Ogus, *Notes on Crystalline Cohomology.(MN-21)*. Princeton University Press, 2015.
[10] T. Stacks Project Authors, "*stacks project." `http://stacks.math.columbia.edu`, 2017.*
[11] R. Hartshorne, Algebraic geometry*, vol. 52. Springer Science & Business Media, 2013.*
[12] M. Kisin, "Crystalline representations and f-crystals," in Algebraic geometry and number theory*, pp. 459–496, Springer, 2006.*
[13] A. J. de Jong, "Crystalline dieudonné module theory via formal and rigid geometry," Publications mathématiques de l'IHÉS*, vol. 82, no. 1, pp. 5–96, 1995.*
[14] J.-M. Fontaine, "Représentations p-adiques des corps locaux (1ere partie)," in The Grothendieck Festschrift*, pp. 249–309, Springer, 2007.*
[15] O. Brinon and B. Conrad, "Cmi summer school notes on p-adic hodge theory," 2009.
[16] G. Faltings, "Integral crystalline cohomology over very ramified valuation rings," Journal of the American Mathematical Society*, vol. 12, no. 1, pp. 117–144, 1999.*