

Algebra & Number Theory

Volume 8

2014

No. 2

**On lower ramification subgroups and canonical
subgroups**

Shin Hattori



On lower ramification subgroups and canonical subgroups

Shin Hattori

Let p be a rational prime, k be a perfect field of characteristic p and K be a finite totally ramified extension of the fraction field of the Witt ring of k . Let \mathcal{G} be a finite flat commutative group scheme over \mathbb{O}_K killed by some p -power. In this paper, we prove a description of ramification subgroups of \mathcal{G} via the Breuil–Kisin classification, generalizing the author’s previous result on the case where \mathcal{G} is killed by $p \geq 3$. As an application, we also prove that the higher canonical subgroup of a level n truncated Barsotti–Tate group \mathcal{G} over \mathbb{O}_K coincides with lower ramification subgroups of \mathcal{G} if the Hodge height of \mathcal{G} is less than $(p-1)/p^n$, and the existence of a family of higher canonical subgroups improving a previous result of the author.

1. Introduction

Let p be a rational prime, k be a perfect field of characteristic p and $W = W(k)$ be the Witt ring of k . The natural Frobenius endomorphism of the ring W lifting the p -th power Frobenius of k is denoted by φ . Let K be a finite extension of $K_0 = \text{Frac}(W)$ with integer ring \mathbb{O}_K , uniformizer π and absolute ramification index e . We fix an algebraic closure \bar{K} of K and extend the valuation v_p of K satisfying $v_p(p) = 1$ to \bar{K} . Let $\hat{\mathbb{O}}_{\bar{K}}$ be the completion of the integer ring $\mathbb{O}_{\bar{K}}$. We also fix a system $\{\pi_n\}_{n \geq 0}$ of p -power roots of π in \bar{K} satisfying $\pi_0 = \pi$ and $\pi_{n+1}^p = \pi_n$ and put $K_\infty = \bigcup_n K(\pi_n)$. The absolute Galois groups of K and K_∞ are denoted by G_K and G_{K_∞} , respectively. For any positive rational number i , put $m_K^{\geq i} = \{x \in \mathbb{O}_K \mid v_p(x) \geq i\}$ and $\mathbb{O}_{K,i} = \mathbb{O}_K/m_K^{\geq i}$. For any valuation ring V of height one, we define $m_V^{\geq i}$ and V_i similarly. We also put $\mathcal{S}_i = \text{Spec}(\mathbb{O}_{K,i})$, $\mathcal{S}_{L,i} = \text{Spec}(\mathbb{O}_{L,i})$ for any finite extension L/K , and $\bar{\mathcal{S}}_i = \text{Spec}(\hat{\mathbb{O}}_{\bar{K},i})$.

Breuil conjectured a classification of finite flat (commutative) group schemes over \mathbb{O}_K killed by some p -power via φ -modules over the formal power series ring $\mathfrak{S} = W[[u]]$ and obtained such a classification for the case where groups are killed

MSC2010: primary 11S23; secondary 14L05, 14L15.

Keywords: finite flat group scheme, Breuil–Kisin module, canonical subgroup.

by $p \geq 3$ [Breuil 2002]. It is often referred to as the Breuil–Kisin classification, since Kisin showed the conjecture for $p \geq 3$ [Kisin 2006] and for the case where $p = 2$ and groups are connected [Kisin 2009]. The conjecture was proved for any p independently in [Kim 2012; Lau 2010; Liu 2013]. In particular, we have an exact category $\text{Mod}_{\mathfrak{S}_\infty}^{1,\varphi}$ of such φ -modules over \mathfrak{S} killed by some p -power (for the definition, see Section 2) and an anti-equivalence of exact categories $\mathfrak{M}^*(-)$ from the category of finite flat group schemes over \mathbb{O}_K killed by some p -power to the category $\text{Mod}_{\mathfrak{S}_\infty}^{1,\varphi}$. Moreover, we can recover the G_{K_∞} -module $\mathcal{G}(\mathbb{O}_{\bar{K}})$ via this classification: Let R be the valuation ring defined as the projective limit of p -th power maps

$$R = \varprojlim(\mathbb{O}_{\bar{K},1} \leftarrow \mathbb{O}_{\bar{K},1} \leftarrow \cdots)$$

and $\underline{\pi}$ be the element of the ring R defined by $\underline{\pi} = (\pi_0, \pi_1, \dots)$. We normalize the valuation v_R by $v_R(\underline{\pi}) = 1/e$ and define R_i similarly to $\mathbb{O}_{K,i}$, using v_R in place of v_p . For any positive integer n , let $W_n(R)$ be the Witt ring of length n of R , which is considered as an \mathfrak{S} -algebra by the map $u \mapsto [\underline{\pi}]$. The ring $W_n(R)$ admits a natural G_K -action. Then, by the Breuil–Kisin classification, we also have an isomorphism of G_{K_∞} -modules

$$\varepsilon_{\mathcal{G}} : \mathcal{G}(\mathbb{O}_{\bar{K}}) \rightarrow T_{\mathfrak{S}}^*(\mathfrak{M}^*(\mathcal{G})) = \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}^*(\mathcal{G}), W_n(R)).$$

On the other hand, for any positive rational number i , we have a finite flat closed subgroup scheme \mathcal{G}_i of \mathcal{G} over \mathbb{O}_K , the i -th lower ramification subgroup of \mathcal{G} , whose index is adapted to the valuation v_p . Namely, it is defined as the unique finite flat closed subgroup scheme of \mathcal{G} over \mathbb{O}_K satisfying

$$\mathcal{G}_i(\mathbb{O}_{\bar{K}}) = \text{Ker}(\mathcal{G}(\mathbb{O}_{\bar{K}}) \rightarrow \mathcal{G}(\mathbb{O}_{\bar{K},i})).$$

The lower ramification subgroups, which are named as such because of their similarity to the lower numbering ramification groups in algebraic number theory, have similar properties to the upper ramification subgroups [Abbes and Mokrane 2004, §2.3] such as the functoriality and the compatibility with base extension. While this upper variant is used to construct canonical subgroups of abelian varieties [Abbes and Mokrane 2004], the lower ramification subgroups have been also studied and used to construct canonical subgroups [Hattori 2013; 2014; Rabinoff 2012], as explained later.

If \mathcal{G} is killed by $p \geq 3$, then [Hattori 2012, Theorem 1.1] shows that the isomorphism $\varepsilon_{\mathcal{G}}$ induces an isomorphism

$$\mathcal{G}_i(\mathbb{O}_{\bar{K}}) \simeq \text{Ker}(T_{\mathfrak{S}}^*(\mathfrak{M}^*(\mathcal{G})) \rightarrow \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}^*(\mathcal{G}), R_i))$$

for any i . This description of the lower ramification subgroups of \mathcal{G} via the Breuil–Kisin classification is used in [Hattori 2013] to deduce various properties

of canonical subgroups. In this paper, we prove the following theorem, which generalizes this description.

Theorem 1.1. *Let i be a positive rational number satisfying $i \leq 1$ and $W_n^{\text{DP}}(R)_i$ be the divided power envelope of the natural surjection*

$$W_n(R) \rightarrow \mathbb{O}_{\bar{K},i}, \quad (r_0, \dots, r_{n-1}) \mapsto \text{pr}_0(r_0) \bmod m_{\bar{K}}^{\geq i}.$$

Let $I_{n,i}$ be the kernel of the map $W_n(R) \xrightarrow{\varphi} W_n^{\text{DP}}(R)_i$ induced by the Frobenius map

$$\varphi : (r_0, \dots, r_{n-1}) \mapsto (r_0^p, \dots, r_{n-1}^p).$$

Let \mathcal{G} be a finite flat group scheme over \mathbb{O}_K killed by p^n and $\mathfrak{M} = \mathfrak{M}^(\mathcal{G})$ be the corresponding object of the category $\text{Mod}_{\mathbb{O}_\infty}^{1,\varphi}$. Then the natural isomorphism*

$$\varepsilon_{\mathcal{G}} : \mathcal{G}(\mathbb{O}_{\bar{K}}) \rightarrow T_{\mathfrak{G}}^*(\mathfrak{M}) = \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R))$$

induces an isomorphism

$$\mathcal{G}_i(\mathbb{O}_{\bar{K}}) \simeq \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, I_{n,i}).$$

For the case of $n = 1$, Theorem 1.1 can be interpreted as a correspondence of both upper and lower ramification between \mathcal{G} and a finite flat group scheme $\mathcal{H}(\mathfrak{M}^*(\mathcal{G}))$ over $k[[u]]$ (Corollary 3.3), generalizing [Hattori 2012, Theorem 1.1]. Indeed, by a theorem of Tian and Fargues, Theorem 3.3 of [Hattori 2012], and the compatibility of the Breuil–Kisin classification with Cartier duality, Theorem 1.1 for $n = 1$ also implies the assertion of the corollary on upper ramification subgroups. However, the author does not know if a description of upper ramification subgroups via the Breuil–Kisin classification for $n > 1$ can be obtained from Theorem 1.1, since we do not have a comparison result between upper and lower ramification subgroups similar to the theorem of Tian and Fargues for $n > 1$.

In [Hattori 2012], the proof of Theorem 1.1 for the case where \mathcal{G} is killed by $p \geq 3$ is reduced to showing a congruence of the defining equations of \mathcal{G} and $\mathcal{H}(\mathfrak{M}^*(\mathcal{G}))$ with respect to the identification $k[[u]]/(u^e) \simeq \mathbb{O}_{K,1}$ sending u to π . This congruence is a consequence of an explicit description of the affine algebra of \mathcal{G} in terms of $\mathfrak{M}^*(\mathcal{G})$ due to Breuil [2000, Proposition 3.1.2], which is known only for the case where \mathcal{G} is killed by $p \geq 3$. Here, instead, we study a relationship between the groups

$$\mathcal{G}(\mathbb{O}_{\bar{K},i}) \text{ and } \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}^*(\mathcal{G}), W_n(R)/I_{n,i})$$

by using the faithfulness of the crystalline Dieudonné functor [de Jong and Messing 1999], from which Theorem 1.1 follows easily.

As an application of Theorem 1.1 and an explicit description of the ideal $I_{n,i}$ (Lemma 4.3), we also prove the coincidence with canonical subgroups with lower

ramification subgroups, and the existence of a family of canonical subgroups improving Corollary 1.2 of [Hattori 2014]. Before stating the results, we briefly explain a background of this application.

Let K/\mathbb{Q}_p be an extension of complete discrete valuation fields, \mathfrak{X} be an admissible formal scheme over $\mathrm{Spf}(\mathbb{O}_K)$ and \mathfrak{G} be a truncated Barsotti–Tate group of level n over \mathfrak{X} . Consider their Raynaud generic fibers X and G . For any point $x \in X$, the fiber \mathfrak{G}_x is a truncated Barsotti–Tate group of level n over the ring of integers of a finite extension of K . If \mathfrak{G}_x is ordinary, then the unit component \mathfrak{G}_x^0 satisfies $\mathfrak{G}_x^0(\mathbb{O}_{\bar{K}}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{\dim \mathfrak{G}_x}$ and its special fiber is equal to the Frobenius kernel of the special fiber of \mathfrak{G}_x . We refer to a finite flat closed subgroup scheme of \mathfrak{G}_x as a canonical subgroup if it has these properties. What we want to construct here is a family of canonical subgroups for G : namely, an admissible open subgroup C of G over a strict neighborhood U of the ordinary locus $X^{\mathrm{ord}} \subseteq X$ for \mathfrak{G} such that for any $x \in U$, the fiber C_x is the generic fiber of a canonical subgroup of \mathfrak{G}_x . The existence of a family of canonical subgroups is one of the key ingredients in the theory of p -adic Siegel modular forms, and for such arithmetic applications, we also need a precise understanding of C_x . This leads us to construct such a family by first constructing and studying a canonical subgroup of \mathfrak{G}_x fiberwise, and then patching them into a family.

For each fiber \mathfrak{G}_x , the method of lifting the conjugate Hodge filtration to the Breuil–Kisin module [Hattori 2013; 2014] gives a sharp result on the existence of a canonical subgroup of \mathfrak{G}_x , which is stronger than other methods such as the one using the Hodge–Tate map. Namely, it shows that a canonical subgroup \mathcal{C}_n of \mathfrak{G}_x exists if the Hodge height of \mathfrak{G}_x is less than $1/(p^{n-2}(p+1))$ and \mathcal{C}_n has various properties needed for arithmetic applications.

To obtain a family of canonical subgroups (from any of such fiberwise constructions), we typically need to show the coincidence of canonical subgroups with a specific series of subgroups of \mathfrak{G}_x which can be patched into a family when varying x , and this step often requires us to restrict to a smaller admissible open subset than the locus of x such that a canonical subgroup of \mathfrak{G}_x exists. We have at least three series of such subgroups: Harder–Narasimhan filtrations, upper ramification subgroups and lower ramification subgroups, where the former two were mainly used in preceding works; see [Abbes and Mokrane 2004, Fargues 2011, Hattori 2013; 2014, Tian 2010; 2012].

For $n = 1$, the canonical subgroup \mathcal{C}_1 constructed in [Hattori 2013; 2014] was shown to coincide with both upper and lower ramification subgroups, and this again gives a sharp result, namely the existence of a family of canonical subgroups over the locus of Hodge height less than $p/(p+1)$. For $n \geq 2$, it was also shown that \mathcal{C}_n coincides with upper ramification subgroups under a condition on the Hodge height, and this yields a family over the locus of Hodge height less than $1/(2p^{n-1})$ [Hattori

2013; 2014] A weaker result can be obtained also by the Harder–Narasimhan method [Fargues 2011].

In this paper, to obtain a stronger existence theorem of a family of canonical subgroups, we also prove the coincidence of the canonical subgroup constructed in [Hattori 2013; 2014] with lower ramification subgroups, as follows.

Theorem 1.2. *Let K/\mathbb{Q}_p be an extension of complete discrete valuation fields. Let \mathcal{G} be a truncated Barsotti–Tate group of level n , height h and dimension d over \mathbb{C}_K with $0 < d < h$ and Hodge height $w < (p - 1)/p^n$. Then the level n canonical subgroup \mathcal{C}_n of \mathcal{G} [Hattori 2014, Theorem 1.1] satisfies $\mathcal{C}_n = \mathcal{G}_{i_n} = \mathcal{G}_{i'_n}$ for*

$$i_n = \frac{1}{p^{n-1}(p - 1)} - \frac{w}{p - 1}, \quad i'_n = \frac{1}{p^n(p - 1)}.$$

Note that by our assumption and [Hattori 2014, Theorem 1.1], we have an isomorphism of groups

$$\mathcal{C}_n(\mathbb{C}_{\bar{K}}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^d.$$

The fact that the lower ramification subgroup $\mathcal{G}_{i_n}(\mathbb{C}_{\bar{K}})$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^d$ for $w < (p - 1)/p^n$ was proved by Rabinoff [2012, Theorem 1.9] for the case where K/\mathbb{Q}_p is an extension of (not necessarily discrete) complete valuation fields of height one, by a different method. Theorem 1.2 reproves this result of Rabinoff for the case where the base field K is a complete discrete valuation field, and also shows that the subgroup considered by Rabinoff coincides with \mathcal{C}_n . In particular, we show that his subgroup has standard properties as a canonical subgroup as in [Hattori 2014, Theorem 1.1], such as the coincidence with a lift of the Frobenius kernel.

Using Theorem 1.2, we also prove the following theorem on a family construction of canonical subgroups, which is stronger than [Hattori 2014, Corollary 1.2] for $n \geq 2$.

Theorem 1.3. *Let K/\mathbb{Q}_p be an extension of complete discrete valuation fields. Let \mathfrak{X} be an admissible formal scheme over $\mathrm{Spf}(\mathbb{C}_K)$ and \mathfrak{G} be a truncated Barsotti–Tate group of level n over \mathfrak{X} of constant height h and dimension d with $0 < d < h$. We let X and G denote the Raynaud generic fibers of the formal schemes \mathfrak{X} and \mathfrak{G} , respectively. Put $r_n = (p - 1)/p^n$ and let $X(r_n)$ be the admissible open subset of X defined by*

$$X(r_n)(\bar{K}) = \{x \in X(\bar{K}) \mid \mathrm{Hdg}(\mathfrak{G}_x) < r_n\}.$$

Then there exists an admissible open subgroup C_n of $G|_{X(r_n)}$ over $X(r_n)$ such that, etale locally on $X(r_n)$, the rigid-analytic group C_n is isomorphic to the constant group $(\mathbb{Z}/p^n\mathbb{Z})^d$ and, for any finite extension L/K and $x \in X(L)$, the fiber $(C_n)_x$ coincides with the generic fiber of the level n canonical subgroup of \mathfrak{G}_x .

2. The Breuil–Kisin classification

In this section, we briefly recall the classification of finite flat group schemes and Barsotti–Tate groups over \mathbb{O}_K due to Kisin ([2006] for $p \geq 3$ and [2009] for $p = 2$ and connected group schemes) and to Kim [2012], Lau [2010] and Liu [2013] for $p = 2$. We basically follow the presentation of [Kim 2012].

We let the continuous φ -semilinear endomorphism of \mathfrak{S} defined by $u \mapsto u^p$ be denoted also by φ . Put $\mathfrak{S}_n = \mathfrak{S}/p^n\mathfrak{S}$. Let $E(u) \in W[u]$ be the (monic) Eisenstein polynomial of the uniformizer π . Then a Kisin module (of E -height ≤ 1) is an \mathfrak{S} -module endowed with a φ -semilinear map $\varphi_{\mathfrak{M}} : \mathfrak{M} \rightarrow \mathfrak{M}$, which we also write abusively as φ , such that the cokernel of the map

$$1 \otimes \varphi : \varphi^*\mathfrak{M} = \mathfrak{S} \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \rightarrow \mathfrak{M}$$

is killed by $E(u)$. The Kisin modules form an exact category in an obvious manner, and its full subcategory consisting of \mathfrak{M} such that \mathfrak{M} is free of finite rank over \mathfrak{S} (resp. free of finite rank over \mathfrak{S}_1 , resp. finitely generated, p -power torsion and u -torsion free) is denoted by $\text{Mod}_{/\mathfrak{S}}^{1, \varphi}$ (resp. $\text{Mod}_{/\mathfrak{S}_1}^{1, \varphi}$, resp. $\text{Mod}_{/\mathfrak{S}_\infty}^{1, \varphi}$).

We also have categories of Breuil modules $\text{Mod}_{/S}^{1, \varphi}$, $\text{Mod}_{/S_1}^{1, \varphi}$ and $\text{Mod}_{/S_\infty}^{1, \varphi}$ defined as follows (for more precise definitions, see for example [Hattori 2012, §2.1], where the definitions are valid also for $p = 2$). Let S be the p -adic completion of the divided power envelope of $W[u]$ with respect to the ideal $(E(u))$ and put $S_n = S/p^n S$. The ring S has a natural divided power ideal $\text{Fil}^1 S$, a continuous φ -semilinear endomorphism defined by $u \mapsto u^p$ which is also denoted by φ and a differential operator $N : S \rightarrow S$ defined by $N(u) = -u$. We can also define a φ -semilinear map $\varphi_1 = p^{-1}\varphi : \text{Fil}^1 S \rightarrow S$. Then a Breuil module (of Hodge–Tate weights in $[0, 1]$) is an S -module endowed with an S -submodule $\text{Fil}^1 \mathcal{M}$ containing $(\text{Fil}^1 S)\mathcal{M}$ and a φ -semilinear map $\varphi_{1, \mathcal{M}} : \text{Fil}^1 \mathcal{M} \rightarrow \mathcal{M}$ satisfying some conditions. We also define $\varphi_{\mathcal{M}} : \mathcal{M} \rightarrow \mathcal{M}$ by $\varphi_{\mathcal{M}}(x) = \varphi_1(E(u))^{-1}\varphi_{1, \mathcal{M}}(E(u)x)$. We drop the subscript \mathcal{M} if there is no risk of confusion. The Breuil modules also form an exact category. Its full subcategory $\text{Mod}_{/S}^{1, \varphi}$ (resp. $\text{Mod}_{/S_1}^{1, \varphi}$) is defined to be the one consisting of \mathcal{M} such that \mathcal{M} is free of finite rank over S and $\mathcal{M}/\text{Fil}^1 \mathcal{M}$ is p -torsion free (resp. \mathcal{M} is free of finite rank over S_1). The category $\text{Mod}_{/S_\infty}^{1, \varphi}$ is defined as the smallest full subcategory containing $\text{Mod}_{/S_1}^{1, \varphi}$ and closed under extensions. Then the functor $\mathfrak{M} \mapsto S \otimes_{\varphi, \mathfrak{S}} \mathfrak{M}$ induces exact functors

$$\text{Mod}_{/\mathfrak{S}}^{1, \varphi} \rightarrow \text{Mod}_{/S}^{1, \varphi}, \quad \text{Mod}_{/\mathfrak{S}_1}^{1, \varphi} \rightarrow \text{Mod}_{/S_1}^{1, \varphi}, \quad \text{Mod}_{/\mathfrak{S}_\infty}^{1, \varphi} \rightarrow \text{Mod}_{/S_\infty}^{1, \varphi}$$

which are all denoted by $\mathcal{M}_{\mathfrak{S}}(-)$, by putting

$$\text{Fil}^1 \mathcal{M}_{\mathfrak{S}}(\mathfrak{M}) = \text{Ker}(S \otimes_{\varphi, \mathfrak{S}} \mathfrak{M} \xrightarrow{1 \otimes \varphi} S/\text{Fil}^1 S \otimes_{\mathfrak{S}} \mathfrak{M}).$$

Put $\underline{\pi} = (\pi_0, \pi_1, \dots) \in R$ as before and consider the Witt ring $W(R)$ as an \mathfrak{S} -algebra by the map $u \mapsto [\underline{\pi}]$. The p -adic period ring A_{crys} is defined as the p -adic completion of the divided power envelope of $W(R)$ with respect to the ideal $E(u)W(R)$ and the ring $A_{\text{crys}}[1/p]$ is denoted by B_{crys}^+ . For any $r = (r_0, r_1, \dots) \in R$ with $r_l \in \mathbb{O}_{\bar{K},1}$, choose a lift \hat{r}_l of r_l in $\mathbb{O}_{\bar{K}}$ and put $r^{(m)} = \lim_{l \rightarrow \infty} \hat{r}_{l+m}^{p^l} \in \hat{\mathbb{O}}_{\bar{K}}$. Consider the surjection $\theta_n : W_n(R) \rightarrow \mathbb{O}_{\bar{K},n}$ sending $(r_0, r_1, \dots, r_{n-1})$ to $\sum_{l=0}^{n-1} p^l r_l^{(l)}$. Then the quotient $A_{\text{crys}}/p^n A_{\text{crys}}$ can be identified with the divided power envelope $W_n^{\text{DP}}(R)$ of the surjection θ_n compatible with the canonical divided power structure on the ideal $pW_n(R)$. For any objects $\mathfrak{M} \in \text{Mod}_{/\mathfrak{S}}^{1,\varphi}$ and $\mathcal{M} \in \text{Mod}_{/S}^{1,\varphi}$, we have the associated G_{K_∞} -modules

$$T_{\mathfrak{S}}^*(\mathfrak{M}) = \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W(R)), \quad T_{\text{crys}}^*(\mathcal{M}) = \text{Hom}_{S,\varphi,\text{Fil}^1}(\mathcal{M}, A_{\text{crys}}),$$

which are related by the injection

$$T_{\mathfrak{S}}^*(\mathfrak{M}) \rightarrow T_{\text{crys}}^*(\mathcal{M}_{\mathfrak{S}}(\mathfrak{M}))$$

defined by $f \mapsto 1 \otimes (\varphi \circ f)$. Similarly, for any object $\mathfrak{M} \in \text{Mod}_{/\mathfrak{S}_\infty}^{1,\varphi}$, we have the associated G_{K_∞} -module

$$T_{\mathfrak{S}}^*(\mathfrak{M}) = \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} W(R)).$$

Let D be an admissible filtered φ -module over K such that $\text{gr}^i D_K = 0$ unless $i = 0, 1$. Put $S_{K_0} = S \otimes_W K_0$ and $\mathfrak{D} = S_{K_0} \otimes_{K_0} D$. The S_{K_0} -module \mathfrak{D} is endowed with a natural Frobenius map $\varphi_{\mathfrak{D}} : \mathfrak{D} \rightarrow \mathfrak{D}$ induced by the Frobenius of D , a derivation $N_{\mathfrak{D}} = N \otimes 1 : \mathfrak{D} \rightarrow \mathfrak{D}$ and an S_{K_0} -submodule $\text{Fil}^1 \mathfrak{D}$ defined as the inverse image of $\text{Fil}^1 D_K$ by the map $\mathfrak{D} \rightarrow \mathfrak{D}/(\text{Fil}^1 S)\mathfrak{D} = D_K$. Then a strongly divisible lattice in \mathfrak{D} is an S -submodule \mathcal{M} of \mathfrak{D} which satisfies the following:

- \mathcal{M} is a free S -module of finite rank and $\mathfrak{D} = \mathcal{M}[1/p]$.
- \mathcal{M} is stable under $\varphi_{\mathfrak{D}}$ and $N_{\mathfrak{D}}$.
- $\varphi_{\mathfrak{D}}(\text{Fil}^1 \mathcal{M}) \subseteq p\mathcal{M}$, where $\text{Fil}^1 \mathcal{M} = \mathcal{M} \cap \text{Fil}^1 \mathfrak{D}$.

We put $V_{\text{crys}}^*(\mathfrak{D}) = \text{Hom}_{S_{K_0},\varphi,\text{Fil}^1}(\mathfrak{D}, B_{\text{crys}}^+)$. If \mathcal{M} is a strongly divisible lattice in \mathfrak{D} , then the natural G_{K_∞} -actions on $T_{\text{crys}}^*(\mathcal{M})$ and $V_{\text{crys}}^*(\mathfrak{D}) = T_{\text{crys}}^*(\mathcal{M})[1/p]$ extend to G_K -actions and we have a natural isomorphism of G_K -modules

$$V_{\text{crys}}^*(\mathfrak{D}) \rightarrow V_{\text{crys}}^*(D) = \text{Hom}_{K_0,\varphi,\text{Fil}^1}(D, B_{\text{crys}}^+)$$

[Breuil 2002, Proposition 2.2.5] and [Liu 2008, Lemma 5.2.1].

Let (BT/\mathbb{O}_K) (resp. $(p\text{-Gr}/\mathbb{O}_K)$) be the exact category of Barsotti–Tate groups (resp. finite flat group schemes killed by some p -power) over \mathbb{O}_K . For any Barsotti–Tate group Γ over \mathbb{O}_K , we let $T_p(\Gamma)$ denote its p -adic Tate module, $V_p(\Gamma) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(\Gamma)$ and $D^*(\Gamma)$ be the filtered φ -module over K associated to $V_p(\Gamma)$. We

also let $\mathbb{D}^*(-)$ denote the contravariant crystalline Dieudonné functor [Berthelot et al. 1982] and consider its module of sections

$$\mathbb{D}^*(\Gamma)(S \rightarrow \mathbb{O}_K) = \varprojlim_n \mathbb{D}^*(\Gamma)(S_n \rightarrow \mathbb{O}_{K,n})$$

on the divided power thickening $S \rightarrow \mathbb{O}_K$ defined by $u \mapsto \pi$. Note that the S -module $\mathbb{D}^*(\Gamma)(S \rightarrow \mathbb{O}_K)$ can be considered as an object of the category $\text{Mod}_{/S}^{1,\varphi}$ and also as a strongly divisible lattice in $\mathcal{D}^*(\Gamma) = S_{K_0} \otimes_{K_0} D^*(\Gamma)$ [Faltings 1999, §6]. For any finite flat group scheme \mathcal{G} over \mathbb{O}_K killed by some p -power, we define an object $\mathbb{D}^*(\mathcal{G})(S \rightarrow \mathbb{O}_K)$ of the category $\text{Mod}_{/S_\infty}^{1,\varphi}$ similarly. Then we have the following classification theorem, whose first assertion (which is Theorem 2.2.7 of [Kisin 2006] for $p \geq 3$, and Theorem 4.1 and Proposition 4.2 of [Kim 2012] for $p = 2$) implies the second one (Theorem 2.3.5 of [Kisin 2006] for $p \geq 3$, and Corollary 4.3 of [Kim 2012] for $p = 2$) by an argument of taking a resolution.

Theorem 2.1 (Kisin). (1) *There exists an anti-equivalence of exact categories*

$$\mathfrak{M}^*(-) : (\text{BT}/\mathbb{O}_K) \rightarrow \text{Mod}_{/S}^{1,\varphi}$$

with a natural isomorphism of G_{K_∞} -modules

$$\varepsilon_\Gamma : T_p(\Gamma) \rightarrow T_{S}^*(\mathfrak{M}^*(\Gamma)).$$

Moreover, the S -module $\mathcal{M}_S(\mathfrak{M}^(\Gamma))$ can be considered as a strongly divisible lattice in $\mathcal{D}^*(\Gamma)$ and we also have a natural isomorphism of strongly divisible lattices in $\mathcal{D}^*(\Gamma)$*

$$\mu_\Gamma : \mathcal{M}_S(\mathfrak{M}^*(\Gamma)) \rightarrow \mathbb{D}^*(\Gamma)(S \rightarrow \mathbb{O}_K).$$

(2) *There exists an anti-equivalence of exact categories*

$$\mathfrak{M}^*(-) : (p\text{-Gr}/\mathbb{O}_K) \rightarrow \text{Mod}_{/S_\infty}^{1,\varphi}$$

with a natural isomorphism of G_{K_∞} -modules

$$\varepsilon_{\mathcal{G}} : \mathcal{G}(\mathbb{O}_{\bar{K}}) \rightarrow T_{S_\infty}^*(\mathfrak{M}^*(\mathcal{G})).$$

Moreover, we also have a natural isomorphism of the category $\text{Mod}_{/S_\infty}^{1,\varphi}$

$$\mu_{\mathcal{G}} : \mathcal{M}_{S_\infty}(\mathfrak{M}^*(\mathcal{G})) \rightarrow \mathbb{D}^*(\mathcal{G})(S \rightarrow \mathbb{O}_K).$$

On the other hand, for any object \mathfrak{M} of the category $\text{Mod}_{/S}^{1,\varphi}$ or $\text{Mod}_{/S_\infty}^{1,\varphi}$, we can define a dual object \mathfrak{M}^\vee which is compatible with Cartier duality of Barsotti–Tate groups or finite flat group schemes. In particular, for any object \mathfrak{M} of the category

$\text{Mod}_{\mathbb{C}_\infty}^{1,\varphi}$ killed by p^n , we have a commutative diagram of G_{K_∞} -modules

$$\begin{array}{ccc} \mathcal{G}(\mathbb{C}_{\bar{K}}) \times \mathcal{G}^\vee(\mathbb{C}_{\bar{K}}) & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z}(1) \\ \varepsilon_{\mathcal{G}} \downarrow \wr & & \delta_{\mathcal{G}} \downarrow \wr \\ T_{\mathbb{C}}^*(\mathfrak{M}^*(\mathcal{G})) \times T_{\mathbb{C}}^*(\mathfrak{M}^*(\mathcal{G})^\vee) & \longrightarrow & W_n(R) \end{array}$$

where the upper horizontal arrow is the pairing of Cartier duality, the lower horizontal arrow is a natural perfect pairing, $\delta_{\mathcal{G}}$ is the composite

$$\mathcal{G}^\vee(\mathbb{C}_{\bar{K}}) \xrightarrow{\varepsilon_{\mathcal{G}^\vee}} T_{\mathbb{C}}^*(\mathfrak{M}^*(\mathcal{G}^\vee)) \simeq T_{\mathbb{C}}^*(\mathfrak{M}^*(\mathcal{G})^\vee)$$

and the right vertical arrow is an injection (see [Kim 2012, §5.1], and also [Hattori 2012, Proposition 4.4]).

Let Γ be a Barsotti–Tate group over \mathbb{C}_K . We consider any element g of $T_p(\Gamma)$ as a homomorphism $g : \mathbb{Q}_p/\mathbb{Z}_p \rightarrow \Gamma \times \text{Spec}(\hat{\mathbb{C}}_{\bar{K}})$. By evaluating the map

$$\mathbb{D}^*(g) : \mathbb{D}^*(\Gamma \times \text{Spec}(\hat{\mathbb{C}}_{\bar{K}})) \rightarrow \mathbb{D}^*(\mathbb{Q}_p/\mathbb{Z}_p)$$

on the natural divided power thickening $A_{\text{crys}} \rightarrow \hat{\mathbb{C}}_{\bar{K}}$, we obtain a homomorphism of G_{K_∞} -modules

$$\begin{aligned} T_p(\Gamma) &\rightarrow \text{Hom}_{S,\varphi,\text{Fil}}(\mathbb{D}^*(\Gamma)(A_{\text{crys}} \rightarrow \hat{\mathbb{C}}_{\bar{K}}), \mathbb{D}^*(\mathbb{Q}_p/\mathbb{Z}_p)(A_{\text{crys}} \rightarrow \hat{\mathbb{C}}_{\bar{K}})) \\ &= T_{\text{crys}}^*(\mathbb{D}^*(\Gamma)(S \rightarrow \mathbb{C}_K)). \end{aligned}$$

This map is an injection, and an isomorphism after inverting p [Faltings 1999, Theorem 7]. Then we have the following compatibility of this map with the Breuil–Kisin classification.

Lemma 2.2. *Let Γ be a Barsotti–Tate group over \mathbb{C}_K . Then the following diagram is commutative:*

$$\begin{array}{ccc} T_p(\Gamma) & \xrightarrow[\varepsilon_\Gamma]{\sim} & T_{\mathbb{C}}^*(\mathfrak{M}^*(\Gamma)) \\ \downarrow & & \downarrow \\ T_{\text{crys}}^*(\mathbb{D}^*(\Gamma)(S \rightarrow \mathbb{C}_K)) & \xrightarrow[T_{\text{crys}}^*(\mu_\Gamma)]{\sim} & T_{\text{crys}}^*(\mathcal{M}_{\mathbb{C}}(\mathfrak{M}^*(\Gamma))) \end{array}$$

Proof. Put $D = \mathbb{D}^*(\Gamma)$ and $\mathfrak{M} = \mathfrak{M}^*(\Gamma)$. Consider the diagram

$$\begin{array}{ccccc} T_p(\Gamma) & \longrightarrow & T_{\text{crys}}^*(\mathbb{D}^*(\Gamma)(S \rightarrow \mathbb{C}_K)) & \xrightarrow{\sim} & T_{\text{crys}}^*(\mathcal{M}_{\mathbb{C}}(\mathfrak{M})) \longleftarrow T_{\mathbb{C}}^*(\mathfrak{M}) \\ & \searrow & \downarrow & \swarrow & \\ & & V_{\text{crys}}^*(D) & & \end{array}$$

where the left and middle triangles are commutative by [Kim 2012, Theorem 5.6.2]

and Theorem 2.1 (1), respectively. The commutativity of the right one is remarked in [Kim 2012, footnote 11]. We briefly reproduce a proof of this remark for the convenience of the reader. We follow the notation of [Kisin 2006]. In particular, let $\mathbb{C} = \mathbb{C}_{[0,1]}$ be the ring of rigid-analytic functions on the open unit disc over K_0 and $M = \mathbb{C} \otimes_{\mathfrak{S}} \mathfrak{M}$ be the associated φ -module over the ring \mathbb{C} . We also put $\mathcal{D}_0 = (\mathbb{C}[l_u] \otimes_{K_0} D)^{N=0} = \mathbb{C} \otimes_{K_0} D$. Then the map $T_{\mathfrak{S}}^*(\mathfrak{M}) \rightarrow V_{\text{crys}}^*(D)$ is defined as the composite

$$\begin{aligned} \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W(R)) &\rightarrow \text{Hom}_{\mathbb{C},\varphi}(M, B_{\text{crys}}^+) \xrightarrow{(1 \otimes \varphi)^*} \text{Hom}_{\mathbb{C},\varphi}(\varphi^* M, B_{\text{crys}}^+) \\ &\xrightarrow{(1 \otimes \xi)^*} \text{Hom}_{\mathbb{C},\varphi, \text{Fil}}(\mathcal{D}_0, B_{\text{crys}}^+) \rightarrow \text{Hom}_{K_0, \varphi, \text{Fil}}(D, B_{\text{crys}}^+). \end{aligned}$$

Here the map $\xi : D \rightarrow M$ is the unique φ -compatible section and the map $1 \otimes \xi : \mathcal{D}_0 = \mathbb{C} \otimes_{K_0} D \rightarrow M$ factors through the injection

$$1 \otimes \varphi : \varphi^* M = \mathbb{C} \otimes_{\varphi, \mathbb{C}} M \rightarrow M$$

[Kisin 2006, Lemma 1.2.6]. Put $\mathcal{D}_{\mathfrak{S}}(\mathfrak{M}) = \mathcal{M}_{\mathfrak{S}}(\mathfrak{M})[1/p] = S_{K_0} \otimes_{\mathbb{C}} \varphi^* M$. Then we have $K_0 \otimes_{S_{K_0}} \mathcal{D}_{\mathfrak{S}}(\mathfrak{M}) = K_0 \otimes_{\varphi, K_0} D$ and the composite

$$s_0 : K_0 \otimes_{\varphi, K_0} D \xrightarrow{1 \otimes \varphi} D \xrightarrow{\xi} \varphi^* M \rightarrow \mathcal{D}_{\mathfrak{S}}(\mathfrak{M})$$

is the unique φ -compatible section. Using this, we can check that $K_0 \otimes_{\varphi, K_0} D \xrightarrow{1 \otimes \varphi} D$ is an isomorphism of filtered φ -modules, where we consider on the left-hand side the induced filtration by the isomorphism

$$\mathcal{D}_{\mathfrak{S}}(\mathfrak{M}) / (\text{Fil}^1 S) \mathcal{D}_{\mathfrak{S}}(\mathfrak{M}) \rightarrow K \otimes_{\varphi, K_0} D,$$

and hence we can also check the above remark easily. Since the map ε_{Γ} is defined by identifying the images of $T_p(\Gamma)$ and $T_{\mathfrak{S}}^*(\mathfrak{M})$ in $V_{\text{crys}}^*(D)$, the lemma follows. \square

3. Lower ramification subgroups

In this section, we prove Theorem 1.1. We begin with the following lemma, which gives upper bounds of the lower ramification of finite flat group schemes. For any valuation ring V of height one with valuation v and any N -tuple $\underline{x} = (x_1, \dots, x_N)$ in V , we put $v(\underline{x}) = \min_{l=1, \dots, N} v(x_l)$.

Lemma 3.1. (1) *Let \mathcal{H}/\mathbb{Q}_p be an extension of complete discrete valuation fields and \mathcal{G} be a finite flat group scheme over $\mathbb{C}_{\mathcal{H}}$ killed by some p -power. Then we have $\mathcal{G}_i = 0$ for any $i > 1/(p-1)$.*

(2) *Let \mathcal{H} be an extension of complete discrete valuation fields over \mathbb{Q}_p or $k((u))$ with valuation v and \mathcal{G} be a finite flat generically etale group scheme over $\mathbb{C}_{\mathcal{H}}$ killed by some p -power. Then we have the following.*

- (a) $\mathcal{G}_i = (\mathcal{G}^0)_i$ for any $i > 0$.
- (b) $\mathcal{G}_i = 0$ for any $i > \deg(\mathcal{G})/(p - 1)$.

Here \mathcal{G}_i and $\deg(\mathcal{G})$ are defined using v . Namely, we extend v to a separable closure \mathcal{K}^{sep} of \mathcal{K} , write as $\omega_{\mathcal{G}} \simeq \bigoplus_l \mathbb{O}_{\mathcal{K}^{\text{sep}}}/(a_l)$ and put

$$\mathcal{G}_i(\mathbb{O}_{\mathcal{K}^{\text{sep}}}) = \text{Ker}(\mathcal{G}(\mathbb{O}_{\mathcal{K}^{\text{sep}}}) \rightarrow \mathcal{G}(\mathbb{O}_{\mathcal{K}^{\text{sep}},i})), \quad \deg(\mathcal{G}) = \sum_l v(a_l).$$

Proof. For the assertion (1), we may replace \mathcal{K} by its finite extension and assume $\mathcal{G}^\vee(\mathbb{O}_{\bar{\mathcal{K}}}) = \mathcal{G}^\vee(\mathbb{O}_{\mathcal{K}})$ for an algebraic closure $\bar{\mathcal{K}}$ of \mathcal{K} . By Cartier duality, there exists a generic isomorphism $\mathcal{G} \rightarrow \mathcal{G}' = \bigoplus_l \mu_{p^{n_l}}$ for some n_l . Then $\mathcal{G}'_i = 0$ for any $i > 1/(p - 1)$ and the assertion follows from the commutative diagram

$$\begin{array}{ccc} \mathcal{G}(\mathbb{O}_{\bar{\mathcal{K}}}) & \xrightarrow{\sim} & \mathcal{G}'(\mathbb{O}_{\bar{\mathcal{K}}}) \\ \downarrow & & \downarrow \\ \mathcal{G}(\mathbb{O}_{\bar{\mathcal{K}},i}) & \longrightarrow & \mathcal{G}'(\mathbb{O}_{\bar{\mathcal{K}},i}) \end{array}$$

Let us consider the assertion (2). For any $i > 0$, we have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{G}^0(\mathbb{O}_{\mathcal{K}^{\text{sep}}}) & \longrightarrow & \mathcal{G}(\mathbb{O}_{\mathcal{K}^{\text{sep}}}) & \longrightarrow & \mathcal{G}^{\text{et}}(\mathbb{O}_{\mathcal{K}^{\text{sep}}}) \longrightarrow 0 \\ & & & & \downarrow & & \downarrow \\ & & & & \mathcal{G}(\mathbb{O}_{\mathcal{K}^{\text{sep}},i}) & \longrightarrow & \mathcal{G}^{\text{et}}(\mathbb{O}_{\mathcal{K}^{\text{sep}},i}) \end{array}$$

where the upper row is the connected-étale sequence. Then the right vertical arrow is an isomorphism and the part (a) follows.

For the part (b), suppose $i > \deg(\mathcal{G})/(p - 1)$. By part (a), we may assume that \mathcal{G} is connected. By [Tian 2012, Proposition 1.5], we have a presentation of the affine algebra $\mathbb{O}_{\mathcal{G}}$ of \mathcal{G}

$$\begin{aligned} \mathbb{O}_{\mathcal{G}} &\simeq \mathbb{O}_{\mathcal{K}}\llbracket X_1, \dots, X_d \rrbracket / (f_1, \dots, f_d), \\ (f_1, \dots, f_d) &\equiv (X_1, \dots, X_d)U \text{ mod } \deg p \end{aligned}$$

with some $U \in M_d(\mathbb{O}_{\mathcal{K}})$ satisfying the equality $v(\det(U)) = \deg(\mathcal{G})$, where $X_1 = \dots = X_d = 0$ gives the zero section. Let \hat{U} be the matrix satisfying $U\hat{U} = \det(U)I_d$, where I_d is the identity matrix. For any element $\underline{x} = (x_1, \dots, x_d)$ of $\mathcal{G}(\mathbb{O}_{\mathcal{K}^{\text{sep}}})$, multiplying by \hat{U} implies the inequality

$$v(\underline{x}) + v(\det(U)) \geq pv(\underline{x}).$$

Thus we obtain the inequality $v(\underline{x}) \leq \deg(\mathcal{G})/(p - 1)$ unless $\underline{x} = 0$ and the assertion follows. □

For any positive rational number $i \leq 1$, we let $W_n^{\text{DP}}(R)_i$ denote the divided power envelope of the composite

$$\theta_{n,i} : W_n(R) \xrightarrow{\theta_n} \mathbb{O}_{\bar{K},n} \rightarrow \mathbb{O}_{\bar{K},i}, \quad (r_0, \dots, r_{n-1}) \mapsto \text{pr}_0(r_0) \bmod m_{\bar{K}}^{\geq i}$$

compatible with the canonical divided power structure on the ideal $pW_n(R)$. Note that, by fixing a generator \underline{p}^i of the principal ideal $m_{\bar{K}}^{\geq i}$, we have an isomorphism of R -algebras

$$W_n(R)[Y_1, Y_2, \dots]/([\underline{p}^i]^p - pY_1, Y_1^p - pY_2, Y_2^p - pY_3, \dots) \rightarrow W_n^{\text{DP}}(R)_i \quad (1)$$

sending Y_l to $\delta^l([\underline{p}^i])$, where we put $\delta(x) = (p-1)!\gamma_p(x)$ with the p -th divided power γ_p . The surjection $\theta_{n,i}$ defines a divided power thickening $W_n^{\text{DP}}(R)_i \rightarrow \mathbb{O}_{\bar{K},i}$ over the thickening $S \rightarrow \mathbb{O}_K$, which is denoted by $A_{n,i}$. Put

$$I_{n,i} = \text{Ker}(W_n(R) \xrightarrow{\varphi} W_n^{\text{DP}}(R)_i).$$

From the definition, we see the inclusion $I_{n,i} \subseteq I_{n,i'}$ for any $i > i'$.

We show Theorem 1.1 by relating both sides of the isomorphism in its statement via Breuil modules using the lemma below.

Lemma 3.2. *Let $i \leq 1$ be a positive rational number and \mathcal{G} be a finite flat group scheme over $\mathbb{O}_{K,i}$ killed by p^n . Then the map*

$$\begin{aligned} \mathcal{G}(\mathbb{O}_{\bar{K},i}) &= \text{Hom}_{\mathbb{O}_{\bar{K},i}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{G} \times \bar{\mathcal{F}}_i) \rightarrow \text{Hom}(\mathbb{D}^*(\mathcal{G})(A_{n,i}), \mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z})(A_{n,i})) \\ &= \text{Hom}(\mathbb{D}^*(\mathcal{G})(A_{n,i}), W_n^{\text{DP}}(R)_i) \end{aligned}$$

defined by $g \mapsto \mathbb{D}^*(g)(A_{n,i})$ is an injection.

Proof. Suppose that a homomorphism $g : \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathcal{G} \times \bar{\mathcal{F}}_i$ satisfies $\mathbb{D}^*(g)(A_{n,i}) = 0$. We can take a finite extension L/K such that the map g is defined over $\text{Spec}(\mathbb{O}_{L,i})$. Then we have the commutative diagram

$$\begin{array}{ccc} \text{Hom}_{\mathbb{O}_{L,i}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{G} \times \mathcal{F}_{L,i}) & \longrightarrow & \text{Hom}(\mathbb{D}^*(\mathcal{G} \times \mathcal{F}_{L,i})(A_{n,i}), \mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z})(A_{n,i})) \\ \downarrow & & \downarrow \wr \\ \text{Hom}_{\mathbb{O}_{\bar{K},i}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{G} \times \bar{\mathcal{F}}_i) & \longrightarrow & \text{Hom}(\mathbb{D}^*(\mathcal{G} \times \bar{\mathcal{F}}_i)(A_{n,i}), \mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z})(A_{n,i})) \end{array}$$

and thus we may assume $L = K$.

Put $\Sigma = \text{Spec}(\mathbb{Z}_p)$ and $\Sigma_n = \text{Spec}(\mathbb{Z}/p^n\mathbb{Z})$. Consider the big fppf crystalline site $\text{CRY}(\mathcal{F}_i/\Sigma)$ and its topos $(\mathcal{F}_i/\Sigma)_{\text{CRY}}$ [Berthelot et al. 1982]. Note that the local ring $\mathbb{O}_{K,i}$ is a Noetherian complete intersection ring and, for any finite extension L/K , the ring $\mathbb{O}_{L,i}$ is faithfully flat and of relative complete intersection over $\mathbb{O}_{K,i}$.

Thus, by [de Jong and Messing 1999, Proposition 1.2 and Lemma 4.1], we see that the composite

$$\begin{aligned} \mathrm{Hom}_{\mathbb{O}_{\bar{K},i}}(\mathbb{Z}/p^n\mathbb{Z}, \mathcal{G}) &\rightarrow \mathrm{Hom}_{(\mathcal{G}_i/\Sigma)_{\mathrm{CRYST}}}(\mathbb{D}^*(\mathcal{G}), \mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z})) \\ &\rightarrow \mathrm{Hom}_{(\tilde{\mathcal{G}}_i/\Sigma)_{\mathrm{CRYST}}}(\mathbb{D}^*(\mathcal{G}), \mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z})) \end{aligned}$$

is an injection.

Consider the natural morphism of topoi

$$i_{n\mathrm{CRYST}} : (\tilde{\mathcal{G}}_i/\Sigma_n)_{\mathrm{CRYST}} \rightarrow (\tilde{\mathcal{G}}_i/\Sigma)_{\mathrm{CRYST}}.$$

Since the crystal $\mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z})$ is isomorphic to the quotient $\mathbb{O}_{\tilde{\mathcal{G}}_i/\Sigma}/p^n\mathbb{O}_{\tilde{\mathcal{G}}_i/\Sigma}$ of the structure sheaf $\mathbb{O}_{\tilde{\mathcal{G}}_i/\Sigma}$ [Berthelot et al. 1982, Exemples 4.2.16] and this is equal to $i_{n\mathrm{CRYST}*}(\mathbb{O}_{\tilde{\mathcal{G}}_i/\Sigma_n})$ [Berthelot et al. 1982, (4.2.17.4)], the natural map

$$\begin{aligned} i_{n\mathrm{CRYST}}^* : \mathrm{Hom}_{(\tilde{\mathcal{G}}_i/\Sigma)_{\mathrm{CRYST}}}(\mathbb{D}^*(\mathcal{G}), \mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z})) \\ \rightarrow \mathrm{Hom}_{(\tilde{\mathcal{G}}_i/\Sigma_n)_{\mathrm{CRYST}}}(i_{n\mathrm{CRYST}}^*(\mathbb{D}^*(\mathcal{G})), i_{n\mathrm{CRYST}}^*(\mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z}))) \end{aligned}$$

is an isomorphism.

Finally, we claim that the thickening $A_{n,i}$ defines the final object of the big crystalline site $\mathrm{CRYST}(\tilde{\mathcal{G}}_i/\Sigma_n)$. This follows as the proof of [Fontaine 1994, Théorème 1.2.1]. Indeed, it suffices to show that for any $\mathbb{O}_{\bar{K},i}$ -algebra \mathbb{O}_U , any $\mathbb{Z}/p^n\mathbb{Z}$ -algebra \mathbb{O}_T and any surjection $\mathbb{O}_T \rightarrow \mathbb{O}_U$ defined by a divided power ideal J_T , the composite

$$W_n(R) \xrightarrow{\theta_{n,i}} \mathbb{O}_{\bar{K},i} \rightarrow \mathbb{O}_U$$

uniquely factors through \mathbb{O}_T . For this, we define the map $f : W_n(R) \rightarrow \mathbb{O}_T$ as follows: For any element $r = (r_0, \dots, r_{n-1})$ of the ring $W_n(R)$, choose a lift $\widehat{\mathrm{pr}_n(r_l)}$ in \mathbb{O}_T of the element $\mathrm{pr}_n(r_l)$ for any $l = 0, \dots, n-1$ and put

$$f(r) = \sum_{l=0}^{n-1} p^l \widehat{\mathrm{pr}_n(r_l)} p^{n-l}.$$

This is independent of the choice of lifts and gives a ring homomorphism satisfying the condition. Conversely, suppose that a homomorphism $f' : W_n(R) \rightarrow \mathbb{O}_T$ satisfies the condition. Then, for any element $r = (r_0, \dots, r_{n-1})$ of the ring $W_n(R)$, we have $f'(r) = \sum_{l=0}^{n-1} p^l f'([r_l]^{1/p^n}) p^{n-l}$ and $f'([r_l]^{1/p^n}) \bmod J_T = \mathrm{pr}_n(r_l)$. Thus the uniqueness follows. Hence the evaluation map on the thickening $A_{n,i}$

$$\begin{aligned} \mathrm{Hom}_{(\tilde{\mathcal{G}}_i/\Sigma_n)_{\mathrm{CRYST}}}(i_{n\mathrm{CRYST}}^*(\mathbb{D}^*(\mathcal{G})), i_{n\mathrm{CRYST}}^*(\mathbb{D}^*(\mathbb{Z}/p^n\mathbb{Z}))) \\ \rightarrow \mathrm{Hom}(\mathbb{D}^*(\mathcal{G})(A_{n,i}), W_n^{\mathrm{DP}}(R)_i) \end{aligned}$$

is an injection. This concludes the proof of the lemma. □

Proof of Theorem 1.1. Take a resolution of \mathcal{G} by Barsotti–Tate groups over \mathbb{O}_K

$$0 \rightarrow \mathcal{G} \rightarrow \Gamma_1 \rightarrow \Gamma_2 \rightarrow 0$$

and consider the associated exact sequence of Kisin modules

$$0 \rightarrow \mathfrak{N}_2 \rightarrow \mathfrak{N}_1 \rightarrow \mathfrak{M} \rightarrow 0.$$

Put $\mathcal{M} = \mathcal{M}_{\mathfrak{S}}(\mathfrak{M})$ and $\mathcal{N}_l = \mathcal{M}_{\mathfrak{S}}(\mathfrak{N}_l)$ for $l = 1, 2$. By Lemma 2.2 and the definition of the anti-equivalence $\mathfrak{M}^*(-)$, we have a diagram

$$\begin{array}{ccccc}
 T_p(\Gamma_1) & \xrightarrow{\quad \varepsilon_{\Gamma_1} \quad} & T_{\text{crys}}^*(\mathcal{N}_1) & \xleftarrow{\quad} & T_{\mathfrak{S}}^*(\mathfrak{N}_1) \\
 \downarrow & & \downarrow & & \downarrow \\
 T_p(\Gamma_2) & \xrightarrow{\quad \varepsilon_{\Gamma_2} \quad} & T_{\text{crys}}^*(\mathcal{N}_2) & \xleftarrow{\quad} & T_{\mathfrak{S}}^*(\mathfrak{N}_2) \\
 \downarrow \pi_{\mathcal{G}} & & \downarrow \pi_{\mathcal{M}} & & \downarrow \pi_{\mathfrak{M}} \\
 \mathcal{G}(\mathbb{O}_{\bar{K}}) & \xrightarrow{\quad \varepsilon_{\mathcal{G}} \quad} & \text{Hom}_{S,\varphi}(\mathcal{M}, W_n^{\text{DP}}(R)) & \xleftarrow{\quad} & T_{\mathfrak{S}}^*(\mathfrak{M}) \\
 \downarrow & & \downarrow & & \downarrow \\
 \mathcal{G}(\mathbb{O}_{\bar{K},i}) & \xrightarrow{\quad} & \text{Hom}_{S,\varphi}(\mathcal{M}, W_n^{\text{DP}}(R)_i) & \xleftarrow{\quad} & \text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R)/I_{n,i})
 \end{array}$$

where the left horizontal arrows are induced by $g \mapsto \mathbb{D}^*(g)$ and the right horizontal arrows are the maps sending f to $1 \otimes (\varphi \circ f)$. The middle left vertical arrow $\pi_{\mathcal{G}} : T_p(\Gamma_2) \rightarrow \mathcal{G}(\mathbb{O}_{\bar{K}})$ is defined as follows: For $g \in T_p(\Gamma_2)$, the element $p^n g$ is contained in the image of $T_p(\Gamma_1) = \varprojlim_l \Gamma_1[p^l](\mathbb{O}_{\bar{K}})$ and put $p^n g = h = (h_n)_{n>0}$. Then the element $h_n \in \Gamma_1[p^n](\mathbb{O}_{\bar{K}})$ is contained in the subgroup $\mathcal{G}(\mathbb{O}_{\bar{K}})$ and the map $\pi_{\mathcal{G}}$ is defined by $g \mapsto h_n$. We define the map $\pi_{\mathcal{M}} : T_{\text{crys}}^*(\mathcal{N}_2) \rightarrow \text{Hom}_{S,\varphi}(\mathcal{M}, W_n^{\text{DP}}(R))$ similarly: For any map $f : \mathcal{N}_2 \rightarrow A_{\text{crys}}$, the map $p^n f$ induces a map $\mathcal{N}_1 \rightarrow A_{\text{crys}}$. Its composite with the natural map $A_{\text{crys}} \rightarrow W_n^{\text{DP}}(R)$ factors through \mathcal{M} and defines the map $\pi_{\mathcal{M}}(f) : \mathcal{M} \rightarrow W_n^{\text{DP}}(R)$. The map $\pi_{\mathfrak{M}}$ is defined in the same way. From these definitions, we see that the diagram is commutative. Note that the bottom left horizontal arrow is an injection by Lemma 3.2, and that the bottom right horizontal arrow is also an injection by the definition of the ideal $I_{n,i}$.

Thus, for any element $g \in \mathcal{G}(\mathbb{O}_{\bar{K}})$, its image in $\mathcal{G}(\mathbb{O}_{\bar{K},i})$ is zero if and only if the image of $\varepsilon_{\mathcal{G}}(g) \in T_{\mathfrak{S}}^*(\mathfrak{M})$ in $\text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R)/I_{n,i})$ is zero. Hence the theorem follows. \square

The special case of $n = 1$ of Theorem 1.1 can be interpreted as a correspondence of ramification for finite flat group schemes over \mathbb{O}_K and $k[[u]]$ generalizing [Hattori 2012, Theorem 1.1], as follows. Recall that we have an anti-equivalence $\mathcal{H}(-)$ from the category $\text{Mod}_{/\mathfrak{S}_1}^{1,\varphi}$ to an exact category of finite flat generically etale group

schemes over $k[[u]]$ whose Verschiebung is zero [Gabriel 1965, Théorème 7.4]. This gives the equality $T_{\mathbb{G}}^*(\mathfrak{M}) = \mathcal{H}(\mathfrak{M})(R)$ for any object \mathfrak{M} of the category $\text{Mod}_{\mathbb{G}_1}^{1,\varphi}$. We normalize the indices of the upper and the lower ramification subgroups of finite flat generically etale group schemes \mathcal{G} over \mathbb{C}_K and \mathcal{H} over $k[[u]]$ to be adapted to v_p and v_R , respectively. In particular, we define the i -th lower ramification subgroup of \mathcal{H} by

$$\mathcal{H}_i(R) = \text{Ker}(\mathcal{H}(R) \rightarrow \mathcal{H}(R_i)).$$

Note that the field $\text{Frac}(R)$ can be identified with the completion of an algebraic closure of $k((u))$.

Corollary 3.3. *Let p be a rational prime and K/\mathbb{Q}_p be an extension of complete discrete valuation fields with perfect residue field k . Let \mathcal{G} be a finite flat group scheme over \mathbb{C}_K killed by p and consider the associated object $\mathfrak{M}^*(\mathcal{G})$ of the category $\text{Mod}_{\mathbb{G}_1}^{1,\varphi}$. Then the map $\varepsilon_{\mathcal{G}}: \mathcal{G}(\mathbb{C}_{\bar{K}}) \simeq \mathcal{H}(\mathfrak{M}^*(\mathcal{G}))(R)$ induces the isomorphisms of G_{K_∞} -modules*

$$\mathcal{G}_i(\mathbb{C}_{\bar{K}}) \simeq \mathcal{H}(\mathfrak{M}^*(\mathcal{G}))_i(R), \quad \mathcal{G}^j(\mathbb{C}_{\bar{K}}) \simeq \mathcal{H}(\mathfrak{M}^*(\mathcal{G}))^j(R)$$

for any positive rational numbers i and j .

Proof. By Cartier duality, a theorem of Tian and Fargues [Tian 2010, Theorem 1.6; Fargues 2011, Proposition 6] and Theorem 3.3 of [Hattori 2012], it is enough to show the assertion of Corollary 3.3 on lower ramification subgroups. Moreover, since the i -th lower ramification subgroups of \mathcal{G} and $\mathcal{H}(\mathfrak{M}^*(\mathcal{G}))$ vanish for any $i > 1/(p-1)$ [Hattori 2012, Corollary 3.5 and Remark 3.6], we may assume $i \leq 1$. Then the equality $I_{1,i} = m_R^{\geq i}$ and Theorem 1.1 imply Corollary 3.3. \square

4. Description of the ideal $I_{n,i}$

In this section, we give an explicit description of the ideal $I_{n,i}$. We identify the rings of both sides of the isomorphism (1).

Proposition 4.1. *Let n_1, \dots, n_l be integers satisfying $0 \leq n_j \leq p-1$ for any j and r be an element of $W_n(R)$. If the element $rY_1^{n_1} \dots Y_l^{n_l}$ is zero in the ring $W_n^{\text{DP}}(R)_i$, then $[\underline{p}^i]^p \mid r$ in the ring $W_n(R)$. In particular, we have the inclusion $I_{n,i} \subseteq ([\underline{p}^i])$.*

Proof. By substituting $Y_j = 0$ for $j > l$, we reduce ourselves to showing that the equality in the ring $W_n(R)[Y_1, \dots, Y_l]$

$$rY_1^{n_1} \dots Y_l^{n_l} = ([\underline{p}^i]^p - pY_1)f_0 + (Y_1^p - pY_2)f_1 + \dots + (Y_{l-1}^p - pY_l)f_{l-1} + Y_l^p f_l \quad (2)$$

with f_0, \dots, f_l in this ring implies $[\underline{p}^i]^p \mid r$. By replacing f_j 's, we may assume the inequality

$$\deg_{j'}(f_j) < p \quad (j' = j + 1, \dots, l), \quad (3)$$

where $\deg_{j'}$ means the degree with respect to $Y_{j'}$.

For any l -tuple $\underline{m} = (m_1, \dots, m_l)$, write $\underline{Y}^{\underline{m}} = Y_1^{m_1} \cdots Y_l^{m_l}$ and let $c_{j, \underline{m}}$ be the coefficient of $\underline{Y}^{\underline{m}}$ in f_j . Put $\underline{n} = (n_1, \dots, n_l)$ and $e_j = (0, \dots, 0, 1, 0, \dots, 0)$ with 1 on the j -th entry. We consider a lexicographic order on the module \mathbb{Z}^l : we say $\underline{m} < \underline{m}'$ if there exists j with $1 \leq j \leq l$ such that $m_j < m'_j$ and $m_{j'} = m'_{j'}$ for any $j < j' \leq l$. Taking the terms of scalar multiples of the monomial $\underline{Y}^{\underline{n}}$ in (2), we have the equality

$$r \underline{Y}^{\underline{n}} = [\underline{p}^i]^p c_{0, \underline{n}} \underline{Y}^{\underline{n}} + \sum_{j=0}^{l-1} (-p Y_{j+1}) c_{j, \underline{n} - e_{j+1}} \underline{Y}^{\underline{n} - e_{j+1}}.$$

Now we claim that

$$c_{j, \underline{n} - e_{j+1}} = 0 \quad (j = 0, \dots, l-1). \quad (4)$$

Suppose the contrary. Choose j such that $0 \leq j \leq l-1$ and $c_{j, \underline{n} - e_{j+1}} \neq 0$. Consider the term $c_{j, \underline{n} - e_{j+1}} \underline{Y}^{\underline{n} - e_{j+1}}$ in f_j . The right-hand side of the equality (2) contains the term $c_{j, \underline{n} - e_{j+1}} \underline{Y}^{\underline{n} + pe_j - e_{j+1}}$ for $j \geq 1$ and $[\underline{p}^i]^p c_{0, \underline{n} - e_1} \underline{Y}^{\underline{n} - e_1}$ for $j = 0$. Note that, for $j' \leq j-2$, the j -th entry of the l -tuple $\underline{n} + pe_j - e_{j+1} - e_{j'+1}$ is equal to $n_j + p$ and thus $f_{j'}$ does not contain any scalar multiple of $\underline{Y}^{\underline{n} + pe_j - e_{j+1} - e_{j'+1}}$ by assumption (3). Since $\underline{n} + pe_j - e_{j+1} < \underline{n}$ and $\underline{n} - e_1 < \underline{n}$, it follows from (2) that

$$c_{j, \underline{n} - e_{j+1}} \underline{Y}^{\underline{n} + pe_j - e_{j+1}} = - \sum_{j'=j-1}^{l-1} (-p Y_{j'+1}) c_{j', \underline{n} + pe_j - e_{j+1} - e_{j'+1}} \underline{Y}^{\underline{n} + pe_j - e_{j+1} - e_{j'+1}}$$

for $j \geq 1$ and

$$[\underline{p}^i]^p c_{0, \underline{n} - e_1} \underline{Y}^{\underline{n} - e_1} = - \sum_{j'=0}^{l-1} (-p Y_{j'+1}) c_{j', \underline{n} - e_1 - e_{j'+1}} \underline{Y}^{\underline{n} - e_1 - e_{j'+1}}$$

for $j = 0$.

We let Eq(1) denote this equation. Put $\underline{m}(1) = \underline{n} + pe_j - e_{j+1}$ for $j \geq 1$ and $\underline{m}(1) = \underline{n} - e_1$ for $j = 0$. Repeating this by arbitrarily choosing a term with nonzero coefficient $c_{j', \underline{m}'}$ on the right-hand side of the equation Eq(s), we obtain a series of equations Eq(1), Eq(2), \dots and a sequence of l -tuples of non-negative integers $\underline{m}(1), \underline{m}(2), \dots$ such that Eq(s) is an equation of monomials of degree $\underline{m}(s)$ for any $s \geq 1$. Note that if there is no such term on the right-hand side of the equation Eq(s), the procedure stops. On the other hand, if the equation Eq(s) is either of the types

$$c \underline{Y}^{\underline{m}(s)} = \begin{cases} - \cdots - (Y_j^p) c_{j, \underline{m}(s) - pe_j} \underline{Y}^{\underline{m}(s) - pe_j} - \cdots & (1 \leq j \leq l-1), \\ - [\underline{p}^i]^p c_{0, \underline{m}(s)} \underline{Y}^{\underline{m}(s)} - \cdots & (j = 0), \end{cases}$$

with some $c \in W_n(R)$ such that the indicated term is chosen and that $c_{j, \underline{m}(s) - pe_j}$ (resp. $c_{0, \underline{m}(s)}$) is contained in the ideal $p^{n-1}W_n(R)$, then the equation $\text{Eq}(s+1)$ is empty and the procedure also stops. In the latter case, we put $\underline{m}(s+1) = \underline{m}(s) - pe_j + e_{j+1}$ for $1 \leq j \leq l-1$ and $\underline{m}(s+1) = \underline{m}(s) + e_1$ for $j = 0$.

Lemma 4.2. *The sequence $\underline{m}(s)$ is strictly decreasing with respect to the lexicographic order on \mathbb{Z}^l defined as above.*

Proof. Note the inequalities $n > \underline{m}(1) > \underline{m}(2)$. Suppose that we have $\underline{m}(1) > \underline{m}(2) > \dots > \underline{m}(t) \leq \underline{m}(t+1)$ for some $t \geq 2$. Then the term $Y_l^p f_l$ in (2) does not affect $\text{Eq}(s)$ for $1 \leq s \leq t$. Thus, by the construction, one of the following four cases holds for each $1 \leq s \leq t$:

- (C_j) $\quad \underline{m}(s+1) = \underline{m}(s) + pe_j - e_{j+1}$ for some $1 \leq j \leq l-1$,
- (C'_j) $\quad \underline{m}(s+1) = \underline{m}(s) - pe_j + e_{j+1}$ for some $1 \leq j \leq l-1$,
- (C_0) $\quad \underline{m}(s+1) = \underline{m}(s) - e_1$,
- (C'_0) $\quad \underline{m}(s+1) = \underline{m}(s) + e_1$.

Moreover, (C_j) and (C'_j) do not occur consecutively for any j satisfying $0 \leq j \leq l-1$. Note that $\underline{m}(s) > \underline{m}(s+1)$ for (C_j) and $\underline{m}(s) < \underline{m}(s+1)$ for (C'_j).

First we claim that (C'_0) does not hold for $s = t$. Suppose the contrary. Then (C_j) holds for $s = t-1$ with some j satisfying $1 \leq j \leq l-1$. Hence the j -th entry $m(t)_j$ of the l -tuple $\underline{m}(t)$ is no less than p . The equation $\text{Eq}(t)$

$$c_{j, \underline{m}(t-1) - e_{j+1}} \underline{Y}^{\underline{m}(t)} = -[p^i]^p c_{0, \underline{m}(t)} \underline{Y}^{\underline{m}(t)} - \dots$$

implies $\deg_j(f_0) \geq p$. This contradicts (3).

Hence (C'_j) holds for $s = t$ with some $1 \leq j \leq l-1$. From this we see that $m(t)_j \geq p$. Since $n_j < p$, there exists an integer t' with $1 \leq t' \leq t-2$ such that (C_j) holds for $s = t'$ and that it does not hold for any s satisfying $t' < s \leq t$.

Next we claim that $m(s)_j = m(t')_j + p$ for any s satisfying $t' < s \leq t$. Suppose the contrary and take the smallest integer t'' with $t' < t'' < t$ such that (C_{j-1}) holds for $s = t''$. Then $m(s)_j = m(t')_j + p$ for $t' < s \leq t''$ and $m(t''+1)_j = m(t')_j + p - 1$. By assumption, we also have $m(t''+1)_j \geq m(t)_j \geq p$. On the other hand, the equation $\text{Eq}(t'')$ is

$$c \underline{Y}^{\underline{m}(t'')} = \dots - (-pY_j) c_{j-1, \underline{m}(t'') - e_j} \underline{Y}^{\underline{m}(t'') - e_j} - \dots$$

with some $c \in W_n(R)$. Hence we obtain

$$\deg_j(f_{j-1}) \geq m(t'')_j - 1 = m(t')_j + p - 1 \geq p,$$

which contradicts (3).

Now let j_0 be the non-negative integer such that (C_{j_0}) holds for $s = t - 1$. Then $j_0 \neq j, j - 1$ by the constancy of $m(s)_j$ which we have just proved. The equation $\text{Eq}(t - 1)$ is

$$c \underline{Y}^{m(t-1)} = - \dots - (-pY_{j_0+1})c_{j_0, \underline{m}(t-1) - e_{j_0+1}} \underline{Y}^{m(t-1) - e_{j_0+1}} - \dots$$

with some $c \in W_n(R)$ and thus $\deg_j(f_{j_0}) \geq m(t - 1)_j = m(t')_j + p \geq p$. By assumption (3), we obtain $j_0 > j$. In particular, we have $j_0 \geq 1$ and $\underline{m}(t) = \underline{m}(t - 1) + pe_{j_0} - e_{j_0+1}$. Therefore the equation $\text{Eq}(t)$ is

$$c' \underline{Y}^{m(t)} = - \dots - (Y_j^p)c_{j, \underline{m}(t) - pe_j} \underline{Y}^{m(t) - pe_j} - \dots$$

with some $c' \in W_n(R)$ and $\deg_{j_0}(f_j) \geq m(t)_{j_0} \geq p$. This contradicts (3), and the lemma follows. □

By Lemma 4.2, the case (C'_j) does not occur in the procedure for any non-negative integer j . In particular, if there is no term with non-zero $c_{j', \underline{m}'}$ on the right-hand side of $\text{Eq}(s)$ for some s , then the equation is

$$[\underline{p}^i]^{p\epsilon} c_{j'', \underline{m}''} \underline{Y}^{m(s)} = 0,$$

where $c_{j'', \underline{m}''} \underline{Y}^{m(s)}$ is the chosen term on the right-hand side of $\text{Eq}(s - 1)$ and $\epsilon \in \{0, 1\}$. Note that this occurs for s satisfying $\underline{m}(s) = (0, \dots, 0)$, since in this case (C_0) holds for $s - 1$. Therefore, Lemma 4.2 implies that, for any choice of terms as above, we end up with an equation of this type for a sufficiently large s . Since the element $[\underline{p}^i]^p$ is a non-zero divisor in the ring $W_n(R)$, we see that $c_{j'', \underline{m}''} = 0$. This contradicts the choice of terms, and (4) follows.

Hence we obtain the equality

$$r \underline{Y}^n = [\underline{p}^i]^p c_{0, n} \underline{Y}^n$$

and thus $[\underline{p}^i]^p \mid r$. This concludes the proof of Proposition 4.1. □

Lemma 4.3. *Put $\mathbf{n}(s) = v_p((ps)!)$ for any non-negative integer s . Then an element $r = (r_0, \dots, r_{n-1})$ of the ring $W_n(R)$ is contained in the ideal $I_{n, i}$ if and only if the condition*

$$[\underline{p}^i]^s \mid (r_0, \dots, r_{n-1-\mathbf{n}(s-1)}, 0, \dots, 0) \tag{5}$$

holds for any $s \geq 1$.

Proof. Let r be an element of the ideal $I_{n, i}$ and show the condition (5) for r by induction on s . The case of $s = 1$ follows from Proposition 4.1. Suppose that the condition (5) holds for some $s \geq 1$. Let $r' = (r'_0, \dots, r'_{n-1-\mathbf{n}(s-1)}, 0, \dots, 0)$ be the element of $W_n(R)$ such that

$$(r_0, \dots, r_{n-1-\mathbf{n}(s-1)}, 0, \dots, 0) = [\underline{p}^i]^s r'.$$

We write the p -adic expansion of the integer s as

$$s = n_1 + pn_2 + \dots + p^{l-1}n_l$$

with $0 \leq n_j \leq p - 1$. Then in the ring $W_n^{\text{DP}}(R)_i$ we have

$$\varphi(r) = p^{\mathbf{n}(s)}\varphi(r')Y_1^{n_1} \dots Y_l^{n_l},$$

and Proposition 4.1 implies that $[\underline{p}^i]$ divides $p^{\mathbf{n}(s)}r'$. Hence the element $[\underline{p}^i]$ divides $(r'_0, \dots, r'_{n-1-\mathbf{n}(s)}, 0, \dots, 0)$ and thus

$$[\underline{p}^i]^{s+1} \mid (r_0, \dots, r_{n-1-\mathbf{n}(s)}, 0, \dots, 0).$$

Conversely, suppose that an element r of the ring $W_n(R)$ satisfies the condition (5) for any $s \geq 1$. Since we have $\mathbf{n}(s) \geq n$ for some s , a similar argument as above shows that $\varphi(r) = 0$ in the ring $W_n^{\text{DP}}(R)_i$. This concludes the proof of the lemma. \square

Remark 4.4. Lemma 4.3 enables us to compute the ideal $I_{n,i}$. For example, $I_{2,i} = (m_R^{\geq 2i}, m_R^{\geq pi}) \subseteq W_2(R)$ and

$$I_{3,i} = \begin{cases} (m_R^{\geq 2i}, m_R^{\geq 4i}, m_R^{\geq 4i}) & (p = 2), \\ (m_R^{\geq 3i}, m_R^{\geq 2pi}, m_R^{\geq p^2i}) & (p \geq 3). \end{cases}$$

Finally we prove a relationship between the ideals $I_{n-1,pi}$ and $I_{n,i}$, which will be used in Section 5.

Lemma 4.5. *For any $r = (r_0, \dots, r_{n-2}) \in I_{n-1,pi}$ and $r_{n-1} \in R$, we have*

$$\hat{r} = (r_0, \dots, r_{n-2}, \underline{p}^{ip^{n-1}}r_{n-1}) \in I_{n,i}.$$

Proof. By Lemma 4.3, we have

$$[\underline{p}^{pi}]^s \mid (r_0, \dots, r_{n-2-\mathbf{n}(s-1)}, 0, \dots, 0)$$

in the ring $W_{n-1}(R)$ for any $s \geq 1$ satisfying $\mathbf{n}(s-1) < n-1$. Let us show that the element $\hat{r} = (\hat{r}_0, \dots, \hat{r}_{n-1})$ satisfies the condition

$$[\underline{p}^i]^s \mid (\hat{r}_0, \dots, \hat{r}_{n-1-\mathbf{n}(s-1)}, 0, \dots, 0)$$

in the ring $W_n(R)$ for any $s \geq 1$ satisfying $\mathbf{n}(s-1) < n$. The case of $s = 1$ follows from the definition of \hat{r} . Suppose $s \geq 2$. Since $\mathbf{n}(s-2) + 1 \leq \mathbf{n}(s-1)$, we have $n-1-\mathbf{n}(s-1) \leq n-2-\mathbf{n}(s-2)$ and $[\underline{p}^{pi}]^{s-1}$ divides $(\hat{r}_0, \dots, \hat{r}_{n-1-\mathbf{n}(s-1)})$. Then the inequality $p(s-1) \geq s$ implies the condition. This concludes the proof of the lemma. \square

5. Application to canonical subgroups

In this section, we prove Theorem 1.2 and Theorem 1.3. First we consider Theorem 1.2. Let K/\mathbb{Q}_p be an extension of complete discrete valuation fields. Let \mathcal{G} be a truncated Barsotti–Tate group of level n , height h and dimension d over \mathbb{O}_K with $0 < d < h$ and Hodge height $w < (p - 1)/p^n$. Let \mathcal{C}_n be the level n canonical subgroup of \mathcal{G} as in Theorem 1.1 of [Hattori 2014]. By a base change argument and the uniqueness of \mathcal{C}_n (see Proposition 3.8 of the same reference), we may assume that the residue field k is perfect. Recall that we normalized the valuation v_R on the ring R as $v_R(\pi) = 1/e$ in Section 1.

Let $\mathfrak{M} = \mathfrak{M}^*(\mathcal{G})$ be the corresponding object of the category $\text{Mod}_{\mathfrak{S}_\infty}^{1,\varphi}$. Then, by Remark 3.4 of [Hattori 2014], we can show as in the proof of [Hattori 2013, Lemma 3.3] that the object $\mathfrak{M}/p\mathfrak{M}$ has a basis $\bar{e}_1, \dots, \bar{e}_h$ such that

$$\varphi(\bar{e}_1, \dots, \bar{e}_h) = (\bar{e}_1, \dots, \bar{e}_h) \begin{pmatrix} P_1 & P_2 \\ u^e P_3 & u^e P_4 \end{pmatrix},$$

where the matrices P_i have entries in the ring $k[[u]]$ with

$$P_1 \in M_{h-d}(k[[u]]), \quad v_R(\det(P_1)) = w, \quad \begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix} \in \text{GL}_h(k[[u]]).$$

Let \hat{P}_1 be the element of $M_{h-d}(k[[u]])$ such that $P_1 \hat{P}_1 = u^{ew} I_{h-d}$. Let B be the unique solution in $M_{d,h-d}(k[[u]])$ of the equation

$$B = P_3 \hat{P}_1 - u^{ep(1-w)-ew} B P_2 \varphi(B) \hat{P}_1 + u^{ep(1-w)} P_4 \varphi(B) \hat{P}_1$$

and put $D = P_1 + u^{ep(1-w)} P_2 \varphi(B)$, which also satisfies $v_R(\det(D)) = w$ (see the proof just cited). Moreover, put

$$(\bar{e}'_1, \dots, \bar{e}'_{h-d}) = (\bar{e}_1, \dots, \bar{e}_h) \begin{pmatrix} I_{h-d} \\ u^{e(1-w)} B \end{pmatrix}.$$

The elements $\bar{e}'_1, \dots, \bar{e}'_{h-d}, \bar{e}_{h-d+1}, \dots, \bar{e}_h$ form a basis of the \mathfrak{S}_1 -module $\mathfrak{M}/p\mathfrak{M}$ satisfying

$$\varphi(\bar{e}'_1, \dots, \bar{e}'_{h-d}, \bar{e}_{h-d+1}, \dots, \bar{e}_h) = (\bar{e}'_1, \dots, \bar{e}'_{h-d}, \bar{e}_{h-d+1}, \dots, \bar{e}_h) \begin{pmatrix} D & P_2 \\ 0 & u^{e(1-w)} P'_4 \end{pmatrix}$$

for some matrix $P'_4 \in M_d(k[[u]])$. Then we have the following description of the level one canonical subgroup \mathcal{C}_1 of $\mathcal{G}[p]$.

Lemma 5.1. *Let f be an element of the module $\text{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}/p\mathfrak{M}, R)$ defined by*

$$(\bar{e}_1, \dots, \bar{e}_h) \mapsto (\underline{x}, \underline{y})$$

with an $(h - d)$ -tuple \underline{x} and a d -tuple \underline{y} in R . Then f corresponds to an element of $\mathcal{C}_1(\mathbb{C}_{\bar{K}})$ by the isomorphism

$$\varepsilon_{\mathcal{G}[p]} : \mathcal{G}[p](\mathbb{C}_{\bar{K}}) \simeq \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{M}/p\mathfrak{M}, R)$$

if and only if $v_R(\underline{x} + u^{e(1-w)}\underline{y}B) > w/(p - 1)$.

Proof. Let \mathfrak{L} be the \mathfrak{S}_1 -submodule of $\mathfrak{M}/p\mathfrak{M}$ generated by $\bar{e}'_1, \dots, \bar{e}'_{h-d}$. Then \mathfrak{L} defines a subobject of $\mathfrak{M}/p\mathfrak{M}$ in the category $\text{Mod}_{\mathfrak{S}_1}^{1, \varphi}$. Put $\mathfrak{N} = (\mathfrak{M}/p\mathfrak{M})/\mathfrak{L}$. Lemma 3.2 of [Hattori 2014] also holds for our $\mathcal{G}[p]$ and its subgroup scheme corresponding to \mathfrak{N} , by Remark 3.4 of the same reference. By Lemma 3.2 and Theorem 3.5(1) of that reference, the level one canonical subgroup \mathcal{C}_1 is the closed subgroup scheme of $\mathcal{G}[p]$ corresponding to the object \mathfrak{N} . We have the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{C}_1(\mathbb{C}_{\bar{K}}) & \longrightarrow & \mathcal{G}[p](\mathbb{C}_{\bar{K}}) & \longrightarrow & (\mathcal{G}[p]/\mathcal{C}_1)(\mathbb{C}_{\bar{K}}) \longrightarrow 0 \\ & & \downarrow \wr \varepsilon_{\mathcal{C}_1} & & \downarrow \wr \varepsilon_{\mathcal{G}[p]} & & \downarrow \wr \varepsilon_{\mathcal{G}[p]/\mathcal{C}_1} \\ 0 & \longrightarrow & \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{N}, R) & \longrightarrow & \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{M}/p\mathfrak{M}, R) & \xrightarrow{\iota^*} & \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{L}, R) \longrightarrow 0 \end{array}$$

where the rows are exact and the vertical arrows are isomorphisms. The element f corresponds to an element of $\mathcal{C}_1(\mathbb{C}_{\bar{K}})$ if and only if $\iota^*(f) = 0$. The map $\iota^*(f) : \mathfrak{L} \rightarrow R$ is defined by

$$(\bar{e}'_1, \dots, \bar{e}'_{h-d}) \mapsto \underline{x} + u^{e(1-w)}\underline{y}B,$$

which we consider as an element of $\mathcal{H}(\mathfrak{L})(R)$. Since $\text{deg}(\mathcal{H}(\mathfrak{L})) = w$, the lemma follows from [Hattori 2013, Lemma 2.4]. \square

Recall that we put

$$i_n = 1/(p^{n-1}(p - 1)) - w/(p - 1), \quad i'_n = 1/(p^n(p - 1)).$$

Lemma 5.2. *If $w < (p - 1)/p^n$, then we have $\mathcal{C}_1 = \mathcal{G}[p]_{i_m} = \mathcal{G}[p]_{i'_m}$ for any integer m satisfying $1 \leq m \leq n$.*

Proof. By [Hattori 2014, Theorem 1.1(c)], the equality $\mathcal{C}_1 = \mathcal{G}[p]_{i_1}$ holds. From the inequalities

$$i'_n < i_n \leq i'_{n-1} < \dots < i_2 \leq i'_1 < i_1,$$

we have the inclusions

$$\mathcal{C}_1 \subseteq \mathcal{G}[p]_{i'_1} \subseteq \mathcal{G}[p]_{i_2} \subseteq \dots \subseteq \mathcal{G}[p]_{i_n} \subseteq \mathcal{G}[p]_{i'_n}.$$

Let us show the reverse inclusion. Let \mathfrak{N} be the quotient of $\mathfrak{M}/p\mathfrak{M}$ in the category $\text{Mod}_{\mathfrak{S}_1}^{1, \varphi}$ corresponding to the closed subgroup scheme $\mathcal{C}_1 \subseteq \mathcal{G}$. By Corollary 3.3, it is enough to show that

$$\text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{M}/p\mathfrak{M}, m_R^{\geq i'_n}) \subseteq \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{N}, R).$$

Consider a φ -compatible homomorphism of \mathfrak{S} -modules $\mathfrak{M}/p\mathfrak{M} \rightarrow R$ defined by

$$(\bar{e}_1, \dots, \bar{e}_h) \mapsto (\underline{x}, \underline{y}) = \underline{p}^{i'_n}(\underline{a}, \underline{b})$$

with an $(h - d)$ -tuple \underline{a} and a d -tuple \underline{b} in R . Then we have

$$\underline{p}^{pi'_n}(\underline{a}^p, \underline{b}^p) = \underline{p}^{i'_n}(\underline{a}, \underline{b}) \begin{pmatrix} I_{h-d} & 0 \\ 0 & u^e I_d \end{pmatrix} \begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix},$$

where $\underline{a}^p = (a_1^p, \dots, a_{h-d}^p)$ and similarly for \underline{b}^p . Multiplying this by $\begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix}^{-1} \in \text{GL}_h(k[[u]])$, we obtain the equality

$$(\underline{a}, u^e \underline{b}) = \underline{p}^{1/p^n}(\underline{a}^p, \underline{b}^p) \begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix}^{-1},$$

and we can write $\underline{a} = \underline{p}^{1/p^n} \underline{a}'$. The $(h - d)$ -tuple \underline{a}' satisfies

$$\underline{a}' = \underline{p}^{1/p^{n-1}-w}(\underline{a}')^p \hat{P}_1 - \underline{p}^{(p^n-1)/p^n-w} \underline{b} P_3 \hat{P}_1.$$

Hence $v_R(\underline{a}') \geq \min\{1/p^{n-1}, (p^n - 1)/p^n\} - w$ and

$$v_R(\underline{x}) \geq \min\{1/(p^{n-2}(p - 1)) - w, 1 + 1/(p^n(p - 1)) - w\} > w/(p - 1).$$

Since $1 - w > w/(p - 1)$, we obtain

$$v_R(\underline{x} + u^{e(1-w)} \underline{y} B) > w/(p - 1).$$

Then Lemma 5.1 implies the reverse inclusion, and the lemma follows. □

To show Theorem 1.2, we proceed by induction on n . The case of $n = 1$ follows from Lemma 5.2. Put $n \geq 2$ and suppose that the theorem holds for any truncated Barsotti–Tate groups of level $n - 1$ over \mathbb{O}_K . Consider a truncated Barsotti–Tate group \mathcal{G} of level n over \mathbb{O}_K with Hodge height $w < (p - 1)/p^n$, as in Theorem 1.2. In particular, we have $\mathcal{C}_{n-1} = \mathcal{G}[p^{n-1}]_{i_{n-1}} = \mathcal{G}[p^{n-1}]_{i'_{n-1}}$, and thus the inclusions $\mathcal{C}_{n-1} \subseteq \mathcal{G}_{i_n} \subseteq \mathcal{G}_{i'_n}$ also hold.

Lemma 5.3. *For any positive rational number i satisfying $i \leq 1/(p - 1)$, multiplication by p induces the map $\mathcal{G}_i(\mathbb{O}_{\bar{K}}) \rightarrow \mathcal{G}[p^{n-1}]_{pi}(\mathbb{O}_{\bar{K}})$.*

Proof. By Lemma 3.1(2), we may assume that \mathcal{G} is connected. By [Illusie 1985, Théorème 4.4(e)], there exists a p -divisible formal Lie group Γ over \mathbb{O}_K such that \mathcal{G} is isomorphic to $\Gamma[p^n]$. By [Rabinoff 2012, Lemma 11.3], we can choose formal parameters X_1, \dots, X_d of the formal Lie group Γ such that the multiplication-by- p map of Γ is written as

$$[p](\mathbb{X}) \equiv p\mathbb{X} + (X_1^p, \dots, X_d^p)U + pf(\mathbb{X}) \pmod{\deg p^2},$$

where $\mathbb{X} = (X_1, \dots, X_d)$, $f(\mathbb{X}) = (f_1(\mathbb{X}), \dots, f_d(\mathbb{X}))$ such that every f_i contains no monomial of degree less than p and $U \in M_d(\mathbb{O}_K)$. Let $\underline{x} = (x_1, \dots, x_d)$ be a d -tuple in $\mathbb{O}_{\bar{K}}$ satisfying $[p^n](\underline{x}) = 0$ and $v_p(\underline{x}) \geq i$. Since $1 + i \geq pi$, we have $1 + v_p(\underline{x}) \geq pi$ and $pv_p(\underline{x}) \geq pi$. Hence $v_p([p](\underline{x})) \geq pi$ and the lemma follows. \square

Lemma 5.4. *We have the inclusion $\mathcal{G}_{i'_n} \subseteq \mathcal{C}_n$.*

Proof. By Lemma 5.2 and Lemma 5.3, multiplication by p^{n-1} induces a homomorphism $\mathcal{G}_{i'_n}(\mathbb{O}_{\bar{K}}) \rightarrow \mathcal{G}[p]_{i'_n}(\mathbb{O}_{\bar{K}}) = \mathcal{C}_1(\mathbb{O}_{\bar{K}})$. Hence we have the inclusion

$$\mathcal{G}_{i'_n} \subseteq p^{-(n-1)}\mathcal{C}_1.$$

Consider the natural map $\mathcal{G} \rightarrow \mathcal{G}/\mathcal{C}_1$. By [Hattori 2014, Theorem 1.1], the subgroup scheme $\mathcal{C}_1 \times \mathcal{S}_{1-w}$ coincides with the kernel of the Frobenius of $\mathcal{G} \times \mathcal{S}_{1-w}$. Put $\bar{\mathcal{G}} = \mathcal{G} \times \mathcal{S}_{1-w}$ and similarly for $\overline{\mathcal{G}/\mathcal{C}_1}$. Note that $pi'_n = i'_{n-1} < 1 - w$. Then we have a commutative diagram

$$\begin{array}{ccc} \mathcal{G}(\mathbb{O}_{\bar{K}}) & \longrightarrow & (\mathcal{G}/\mathcal{C}_1)(\mathbb{O}_{\bar{K}}) \\ \downarrow & & \downarrow \\ \bar{\mathcal{G}}(\mathbb{O}_{\bar{K}, 1-w}) & \longrightarrow & \overline{\mathcal{G}/\mathcal{C}_1}(\mathbb{O}_{\bar{K}, 1-w}) \hookrightarrow \bar{\mathcal{G}}^{(p)}(\mathbb{O}_{\bar{K}, 1-w}) \\ & & \downarrow \qquad \qquad \downarrow \\ & & \overline{\mathcal{G}/\mathcal{C}_1}(\mathbb{O}_{\bar{K}, pi'_n}) \hookrightarrow \bar{\mathcal{G}}^{(p)}(\mathbb{O}_{\bar{K}, pi'_n}) \end{array}$$

where the composite of the middle row is the Frobenius map and the right horizontal arrows are injections. From this diagram, we see that the map $\mathcal{G} \rightarrow \mathcal{G}/\mathcal{C}_1$ induces a map

$$\mathcal{G}_{i'_n}(\mathbb{O}_{\bar{K}}) \rightarrow (\mathcal{G}/\mathcal{C}_1)_{i'_{n-1}}(\mathbb{O}_{\bar{K}}).$$

This implies the inclusion $\mathcal{G}_{i'_n}/\mathcal{C}_1 \subseteq (p^{-(n-1)}\mathcal{C}_1/\mathcal{C}_1)_{i'_{n-1}}$. Note that the group scheme $p^{-(n-1)}\mathcal{C}_1/\mathcal{C}_1$ is a truncated Barsotti–Tate group of level $n - 1$, height h and dimension d with Hodge height pw and that the subgroup scheme $\mathcal{C}_n/\mathcal{C}_1$ is its level $n - 1$ canonical subgroup (see the proof of [Hattori 2013, Theorem 1.1] and [Hattori 2014, Theorem 1.1]). From the induction hypothesis, we see that

$$(p^{-(n-1)}\mathcal{C}_1/\mathcal{C}_1)_{i'_{n-1}} = \mathcal{C}_n/\mathcal{C}_1.$$

This implies the inclusion $\mathcal{G}_{i'_n} \subseteq \mathcal{C}_n$, and the lemma follows. \square

Proposition 5.5. *The image of the map $\mathcal{G}_{i'_n}(\mathbb{O}_{\bar{K}}) \rightarrow \mathcal{G}[p^{n-1}]_{pi'_n}(\mathbb{O}_{\bar{K}})$ induced by the multiplication by p contains the subgroup $\mathcal{G}[p^{n-1}]_{i_{n-1}}(\mathbb{O}_{\bar{K}})$.*

Proof. By Theorem 1.1 and Lemma 5.3, we have a commutative diagram

$$\begin{array}{ccc}
 \mathcal{G}_{i_n}(\mathbb{O}_{\bar{K}}) & \xrightarrow{\sim} & \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{M}, I_{n, i_n}) \\
 \times p \downarrow & & \text{pr} \downarrow \\
 \mathcal{G}[p^{n-1}]_{p i_n}(\mathbb{O}_{\bar{K}}) & \xrightarrow{\sim} & \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{M}, I_{n-1, p i_n}) \\
 \uparrow & & \uparrow \\
 \mathcal{G}[p^{n-1}]_{i_{n-1}}(\mathbb{O}_{\bar{K}}) & \xrightarrow{\sim} & \text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{M}, I_{n-1, i_{n-1}}),
 \end{array}$$

where the horizontal arrows are isomorphisms and the map pr is induced by the natural projection $W_n(R) \rightarrow W_{n-1}(R)$. It suffices to show that the image of the map pr contains the subgroup $\text{Hom}_{\mathfrak{S}, \varphi}(\mathfrak{M}, I_{n-1, i_{n-1}})$.

Let e_1, \dots, e_h be a basis of the \mathfrak{S}_n -module \mathfrak{M} lifting $\bar{e}_1, \dots, \bar{e}_h$ and e'_1, \dots, e'_{h-d} be lifts of $\bar{e}'_1, \dots, \bar{e}'_{h-d}$ in \mathfrak{M} , respectively. Then $e'_1, \dots, e'_{h-d}, e_{h-d+1}, \dots, e_h$ also form a basis of the \mathfrak{S}_n -module \mathfrak{M} . Take a φ -compatible homomorphism of \mathfrak{S} -modules $\mathfrak{M} \rightarrow I_{n-1, i_{n-1}}$ defined by

$$(e'_1, \dots, e'_{h-d}, e_{h-d+1}, \dots, e_h) \mapsto (\underline{x}, \underline{y}),$$

where $\underline{x} = (x_1, \dots, x_{h-d})$ and \underline{y} are an $(h-d)$ -tuple and a d -tuple in the ideal $I_{n-1, i_{n-1}}$, respectively. Put $\hat{x}_l = (x_l, 0) \in W_n(R)$, $\hat{\underline{x}} = (\hat{x}_1, \dots, \hat{x}_{h-d})$ and similarly for $\hat{\underline{y}}$. Let A be the matrix in $M_h(\mathfrak{S}_n)$ satisfying

$$\varphi(e'_1, \dots, e'_{h-d}, e_{h-d+1}, \dots, e_h) = (e'_1, \dots, e'_{h-d}, e_{h-d+1}, \dots, e_h)A.$$

Define an $(h-d)$ -tuple $\underline{\xi} = (\xi_1, \dots, \xi_{h-d})$ and a d -tuple $\underline{\eta}$ in R by

$$p^{n-1}([\underline{\xi}], [\underline{\eta}]) = \varphi(\hat{\underline{x}}, \hat{\underline{y}}) - (\hat{\underline{x}}, \hat{\underline{y}})A,$$

where we put $[\underline{\xi}] = ([\xi_1], \dots, [\xi_{h-d}])$ and similarly for $[\underline{\eta}]$. By Proposition 4.1, the elements \hat{x} and \hat{y} are divisible by $[p^{i_{n-1}}]$ and thus we can write

$$(\underline{\xi}, \underline{\eta}) = \underline{p}^{i_{n-1}}(\underline{\xi}', \underline{\eta}').$$

Since $i_{n-1} = p i_n + w \geq p i_n$, Lemma 4.5 implies that, for any h -tuple \underline{z} in R , the element $(\hat{\underline{x}}, \hat{\underline{y}}) + p^{n-1}[\underline{p}^{i_n} \underline{z}]$ is contained in the ideal I_{n, i_n} . It is enough to show that there exists an h -tuple \underline{z} in R satisfying

$$\varphi((\hat{\underline{x}}, \hat{\underline{y}}) + p^{n-1}[\underline{p}^{i_n} \underline{z}]) = ((\hat{\underline{x}}, \hat{\underline{y}}) + p^{n-1}[\underline{p}^{i_n} \underline{z}])A.$$

Put $\underline{z} = (\underline{\zeta}, \underline{\omega})$ with an $(h-d)$ -tuple $\underline{\zeta}$ and a d -tuple $\underline{\omega}$. Then this is equivalent to the equation

$$(\underline{\xi}, \underline{\eta}) + \underline{p}^{p i_n}(\underline{\zeta}^p, \underline{\omega}^p) = \underline{p}^{i_n}(\underline{\zeta}, \underline{\omega}) \begin{pmatrix} D & P_2 \\ 0 & u^{e(1-w)} P'_4 \end{pmatrix}.$$

We claim that the equation

$$\underline{\xi} + \underline{p}^{p i_n} \underline{\zeta}^p = \underline{p}^{i_n} \underline{\zeta} D$$

for the first entry has a solution $\underline{\zeta} = \underline{p}^{(p-1)i_n} \underline{\zeta}'$ with an $(h-d)$ -tuple $\underline{\zeta}'$ in R . Indeed, let $\hat{D} \in M_{h-d}(k[[u]])$ be the matrix satisfying $D\hat{D} = u^{ew} I_{h-d}$. Then this is equivalent to the equation

$$\underline{\zeta}' = \underline{\xi}' \hat{D} + \underline{p}^{p(p-1)i_n-w} (\underline{\zeta}')^p \hat{D}.$$

Since $p(p-1)i_n > w$, we can find a solution $\underline{\zeta}'$ of the equation by recursion.

For the second entry, we have the equation

$$\underline{p}^{p i_n+w} \underline{\eta}' + \underline{p}^{p i_n} \underline{\omega}^p = \underline{p}^{i_n} (\underline{\zeta} P_2 + \underline{p}^{1-w} \underline{\omega} P_4').$$

This is equivalent to the equation

$$\underline{\omega}^p = \underline{p}^{1-w-(p-1)i_n} \underline{\omega} P_4' + \underline{\zeta}' P_2 - \underline{p}^w \underline{\eta}'.$$

Note that $1-w \geq (p-1)i_n$. Write this equation as

$$(\omega_1^p, \dots, \omega_d^p) + (\omega_1, \dots, \omega_d)C + (c'_1, \dots, c'_d) = 0$$

with some $C = (c_{i,j}) \in M_d(R)$ and $c'_i \in R$. Then the R -algebra

$$R[\omega_1, \dots, \omega_d] / \left(\omega_1^p + \sum_{j=1}^d c_{j,1} \omega_j + c'_1, \dots, \omega_d^p + \sum_{j=1}^d c_{j,d} \omega_j + c'_d \right)$$

is free of rank p^d over R . Since $\text{Frac}(R)$ is algebraically closed and R is integrally closed, this R -algebra admits at least one R -valued point. Hence we can find at least one solution $\underline{\omega}$ of the equation. This concludes the proof of the proposition. \square

Consider the exact sequence

$$0 \rightarrow \mathcal{G}[p]_{i_n}(\mathbb{O}_{\bar{K}}) \rightarrow \mathcal{G}_{i_n}(\mathbb{O}_{\bar{K}}) \xrightarrow{\times p} \mathcal{G}[p^{n-1}]_{p i_n}(\mathbb{O}_{\bar{K}}).$$

Proposition 5.5 implies that the image of the rightmost arrow contains the subgroup

$$\mathcal{G}[p^{n-1}]_{i_{n-1}}(\mathbb{O}_{\bar{K}}) \subseteq \mathcal{G}[p^{n-1}]_{p i_n}(\mathbb{O}_{\bar{K}}),$$

which coincides with $\mathcal{C}_{n-1}(\mathbb{O}_{\bar{K}})$ by induction hypothesis and thus is of order $p^{(n-1)d}$. By Lemma 5.2, the subgroup $\mathcal{G}[p]_{i_n}(\mathbb{O}_{\bar{K}})$ also coincides with $\mathcal{C}_1(\mathbb{O}_{\bar{K}})$ and this is of order p^d . Hence the group $\mathcal{G}_{i_n}(\mathbb{O}_{\bar{K}})$ is of order no less than p^{nd} . Since Lemma 5.4 implies the inclusions

$$\mathcal{G}_{i_n}(\mathbb{O}_{\bar{K}}) \subseteq \mathcal{G}'_{i_n}(\mathbb{O}_{\bar{K}}) \subseteq \mathcal{C}_n(\mathbb{O}_{\bar{K}}),$$

Theorem 1.2 follows by comparing orders. \square

To prove Theorem 1.3, we need the following lemma, which is a “lower” variant of [Hattori 2013, Lemma 4.5].

Lemma 5.6. *Let K/\mathbb{Q}_p be an extension of complete discrete valuation fields and i be a positive rational number. Let \mathfrak{X} be an admissible formal scheme over $\mathrm{Spf}(\mathbb{O}_K)$ and X be its Raynaud generic fiber. Let \mathfrak{G} be a finite locally free formal group scheme over \mathfrak{X} with Raynaud generic fiber G . Then there exists an admissible open subgroup G_i of G over X such that the open immersion $G_i \rightarrow G$ is quasicompact and that for any finite extension L/K and $x \in X(L)$, the fiber $(G_i)_x$ coincides with the lower ramification subgroup $(\mathfrak{G}_x)_i \times \mathrm{Spec}(L)$ of the finite flat group scheme $\mathfrak{G}_x = \mathfrak{G} \times_{\mathfrak{X}, x} \mathrm{Spf}(\mathbb{O}_L)$ over \mathbb{O}_L .*

Proof. Let \mathcal{I} be the augmentation ideal sheaf of the formal group scheme \mathfrak{G} . Write $i = m/n$ with positive integers m, n and put $\mathcal{J} = p^m \mathbb{O}_{\mathfrak{G}} + \mathcal{I}^n$. Let \mathfrak{B} be the admissible blow-up of \mathfrak{G} along the ideal \mathcal{J} and $\mathfrak{G}_{m,n}$ be the formal open subscheme of \mathfrak{B} where p^m generates the ideal $\mathcal{J}_{\mathfrak{G}_{m,n}}$. Since the Raynaud generic fiber of $\mathfrak{G}_{m,n}$ is the admissible open subset of G whose set of \bar{K} -valued points is given by

$$\{x \in G(\bar{K}) \mid v_p(\mathcal{I}(x)) \geq i\},$$

it is independent of the choice of m, n , and we write it as G_i . Using the universality of dilatations as in the proof of [Abbes and Mokrane 2004, Proposition 8.2.2], we can show that G_i is an admissible open subgroup of the rigid-analytic group G . For any affinoid open subset $U = \mathrm{Sp}(A)$ of G , put $I = \Gamma(U, \mathcal{I})$. Then the intersection $U \cap G_i$ is the affinoid $\mathrm{Sp}(A\langle I^n/p^m \rangle)$ and thus the open immersion $G_i \rightarrow G$ is quasicompact. This concludes the proof of the lemma. \square

Proof of Theorem 1.3. Set C_n to be the admissible open subgroup $G_{i'_n}$ of G as in Lemma 5.6 with $i'_n = 1/(p^n(p-1))$. Then, by this lemma and Theorem 1.2, each fiber $(C_n)_x$ coincides with the generic fiber of the level n canonical subgroup of \mathfrak{G}_x , and its group of \bar{K} -valued points is isomorphic to the group $(\mathbb{Z}/p^n\mathbb{Z})^d$. Moreover, C_n is étale, quasicompact and separated over $X(r_n)$. Thus [Conrad 2006, Theorem A.1.2] implies that C_n is finite over $X(r_n)$, and the theorem follows by a similar argument to the proof of [Hattori 2013, Corollary 1.2]. \square

Acknowledgments

This work was supported by JSPS KAKENHI grant no. 23740025.

References

- [Abbes and Mokrane 2004] A. Abbes and A. Mokrane, “Sous-groupes canoniques et cycles évanescents p -adiques pour les variétés abéliennes”, *Publ. Math. Inst. Hautes Études Sci.* 99 (2004), 117–162. MR 2005f:14090 Zbl 1062.14057

- [Berthelot et al. 1982] P. Berthelot, L. Breen, and W. Messing, *Théorie de Dieudonné cristalline, II*, Lecture Notes in Mathematics **930**, Springer, Berlin, 1982. MR 85k:14023 Zbl 0516.14015
- [Breuil 2000] C. Breuil, “Groupes p -divisibles, groupes finis et modules filtrés”, *Ann. of Math. (2)* **152**:2 (2000), 489–549. MR 2001k:14087 Zbl 1042.14018
- [Breuil 2002] C. Breuil, “Integral p -adic Hodge theory”, pp. 51–80 in *Algebraic geometry 2000, Azumino* (Hotaka, 2000), edited by S. Usui et al., Adv. Stud. Pure Math. **36**, Math. Soc. Japan, Tokyo, 2002. MR 2004e:11135 Zbl 1046.11085
- [Conrad 2006] B. Conrad, “Modular curves and rigid-analytic spaces”, *Pure Appl. Math. Q.* **2**:1 (2006), 29–110. MR 2007a:14026 Zbl 1156.14312
- [Faltings 1999] G. Faltings, “Integral crystalline cohomology over very ramified valuation rings”, *J. Amer. Math. Soc.* **12**:1 (1999), 117–144. MR 99e:14022 Zbl 0914.14009
- [Fargues 2011] L. Fargues, “La filtration canonique des points de torsion des groupes p -divisibles”, *Ann. Sci. Éc. Norm. Supér. (4)* **44**:6 (2011), 905–961. MR 2919687 Zbl 06026211
- [Fontaine 1994] J.-M. Fontaine, “Le corps des périodes p -adiques”, pp. 59–111 *Astérisque* **223**, Société Mathématique de France, Paris, 1994. MR 95k:11086 Zbl 0940.14012
- [Gabriel 1965] P. Gabriel, “Étude infinitésimale des schémas en groupe et groupes formels”, pp. 1–65+4 in *Schémas en Groupes (Sém. Géométrie Algébrique, Inst. Hautes Études Sci., 1963/64), Fasc. 2b, Exposé 7a*, Inst. Hautes Études Sci., Paris, 1965. MR 35 #4221
- [Hattori 2012] S. Hattori, “Ramification correspondence of finite flat group schemes over equal and mixed characteristic local fields”, *J. Number Theory* **132**:10 (2012), 2084–2102. MR 2944746 Zbl 1270.14021
- [Hattori 2013] S. Hattori, “Canonical subgroups via Breuil–Kisin modules”, *Math. Z.* **274**:3-4 (2013), 933–953. MR 3078253 Zbl 06197119
- [Hattori 2014] S. Hattori, “Canonical subgroups via Breuil–Kisin modules for $p = 2$ ”, *J. Number Theory* **137** (2014), 142–159. MR 3157783 Zbl 06256935
- [Illusie 1985] L. Illusie, “Déformations de groupes de Barsotti–Tate (d’après A. Grothendieck)”, pp. 151–198 in *Seminar on arithmetic bundles: The Mordell conjecture* (Paris, 1983/84), *Astérisque* **127**, Société Mathématique de France, Paris, 1985. MR 801922 Zbl 1182.14050
- [de Jong and Messing 1999] A. J. de Jong and W. Messing, “Crystalline Dieudonné theory over excellent schemes”, *Bull. Soc. Math. France* **127**:2 (1999), 333–348. MR 2001b:14075 Zbl 0963.14008
- [Kim 2012] W. Kim, “The classification of p -divisible groups over 2-adic discrete valuation rings”, *Math. Res. Lett.* **19**:1 (2012), 121–141. MR 2923180 Zbl 06194639
- [Kisin 2006] M. Kisin, “Crystalline representations and F -crystals”, pp. 459–496 in *Algebraic geometry and number theory*, edited by V. Ginzburg, Progr. Math. **253**, Birkhäuser, Boston, MA, 2006. MR 2007j:11163 Zbl 1184.11052
- [Kisin 2009] M. Kisin, “Modularity of 2-adic Barsotti–Tate representations”, *Invent. Math.* **178**:3 (2009), 587–634. MR 2010k:11089 Zbl 05636297
- [Lau 2010] E. Lau, “A relation between Dieudonné displays and crystalline Dieudonné theory”, preprint, 2010. arXiv 1006.2720v2
- [Liu 2008] T. Liu, “On lattices in semi-stable representations: A proof of a conjecture of Breuil”, *Compos. Math.* **144**:1 (2008), 61–88. MR 2009c:14087 Zbl 1133.14020
- [Liu 2013] T. Liu, “The correspondence between Barsotti–Tate groups and Kisin modules when $p = 2$ ”, *J. Théor. Nombres Bordeaux* **25**:3 (2013), 661–676.
- [Rabinoff 2012] J. Rabinoff, “Higher-level canonical subgroups for p -divisible groups”, *J. Inst. Math. Jussieu* **11**:2 (2012), 363–419. MR 2905309 Zbl 06028609

[Tian 2010] Y. Tian, “Canonical subgroups of Barsotti–Tate groups”, *Ann. of Math. (2)* **172**:2 (2010), 955–988. MR 2012a:14105 Zbl 1203.14026

[Tian 2012] Y. Tian, “An upper bound on the Abbes–Saito filtration for finite flat group schemes and applications”, *Algebra Number Theory* **6**:2 (2012), 231–242. MR 2950153 Zbl 1260.14055

Communicated by Brian Conrad

Received 2012-10-12 Revised 2013-11-18 Accepted 2013-11-19

shin-h@math.kyushu-u.ac.jp *Faculty of Mathematics, Kyushu University,
744 Motoooka, Nishi-ku, Fukuoka 819-0395, Japan*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Roger Heath-Brown	Oxford University, UK	Bernd Sturmfels	University of California, Berkeley, USA
Ehud Hrushovski	Hebrew University, Israel	Richard Taylor	Harvard University, USA
Craig Huneke	University of Virginia, USA	Ravi Vakil	Stanford University, USA
Mikhail Kapranov	Yale University, USA	Michel van den Bergh	Hasselt University, Belgium
Yujiro Kawamata	University of Tokyo, Japan	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Efim Zelmanov	University of California, San Diego, USA
Barry Mazur	Harvard University, USA	Shou-Wu Zhang	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2014 is US \$225/year for the electronic version, and \$400/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFlow[®] from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2014 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 8 No. 2 2014

Large self-injective rings and the generating hypothesis LEIGH SHEPPERSON and NEIL STRICKLAND	257
On lower ramification subgroups and canonical subgroups SHIN HATTORI	303
Wild models of curves DINO LORENZINI	331
Geometry of Wachspress surfaces COREY IRVING and HAL SCHENCK	369
Groups with exactly one irreducible character of degree divisible by p DANIEL GOLDSTEIN, ROBERT M. GURALNICK, MARK L. LEWIS, ALEXANDER MORETÓ, GABRIEL NAVARRO and PHAM HUU TIEP	397
The homotopy category of injectives AMNON NEEMAN	429
Essential dimension of spinor and Clifford groups VLADIMIR CHERNOUSOV and ALEXANDER MERKURJEV	457
On Deligne's category $\underline{\text{Rep}}^{ab}(S_d)$ JONATHAN COMES and VICTOR OSTRIK	473
Algebraicity of the zeta function associated to a matrix over a free group algebra CHRISTIAN KASSEL and CHRISTOPHE REUTENAUER	497



1937-0652(2014)8:2;1-9