UNIVERSITÉ PARIS 13 – Institut Galilée
«U.F.R DE MATHÉMATIQUES »

THÈSE

pour obtenir

le grade de Docteur
de l'Université Paris 13
Spécialité : Mathématiques

présentée et soutenue publiquement par

Yichao TIAN
le 19 Novembre 2007

Sous-groupe canonique et monodromie p-adique des groupes de Barsotti-Tate

Directeur de Thèse

Ahmed ABBES

Jury

M.	Ahmed Abbes	directeur de thèse
M.	Fabrizio Andreatta	rapporteur
M.	Pierre Berthelot	rapporteur
M.	Lawrence Breen	
M.	Olivier Brinon	
M.	Jean-Marc Fontaine	
M.	Luc Illusie	

Remerciements

Je tiens à remercier, avant tout, mon directeur de thèse, Monsieur le Professeur Ahmed Abbes. C'est lui qui m'a proposé ce sujet de thèse, et m'a conduit à un domaine de recherche profond et riche en développement. Il a accompli sa tâche avec enthousiasme et abnégation. Pendant les 3 année qui viennent de passer, il a consacré beaucoup de temps et d'énergie à m'apprendre à faire des recherches mathématiques et la rédaction professionnelle. Ses remarques et ses critiques nombreuses et instructives sur les versions préliminaires de ce texte ont énormément amélioré la structure de l'exposition, la rigueur des démonstrations, ainsi que les expressions des langues. Pour moi, il est non seulement mon professeur de mathématiques, mais aussi un ami dans la vie. Dans les moments les plus difficiles, il m'a encouragé avec toutes ses amitiés et m'a poussé à donner le meilleur de moi. Je lui en suis profondément reconnaissant.

Je souhaite remercier les professeurs Fabrizio Andreatta et Pierre Berthelot pour leur travaux de rapporteur et leurs commentaires sur les versions préliminaires de cette thèse. Ils me font l'honneur d'avoir accepté de faire partie du jury de la soutenance.

Je garde une vive reconnaissance aux professeurs Jean-Marc Fontaine, Luc Illusie et Michel Raynaud. C'était leur collaboration avec l'Université Tsinghua qui m'a amené en France. Dans l'année 2003/2004, ils ont donné des cours d'arithmétique et de géométrie algébrique à l'Université Tsinghua en Chine, et j'ai eu la chance de les suivre. C'étaient mes premières introductions à la géométrie algébrique moderne. La complexité des outils utilisés et les vastes belles mathématiques qu'ils ont exposées m'ont beaucoup impressionné et ont aussi surgi toute mon envie d'explorer cette voie. Après ces cours magnifiques et grâce aux aides de ces professeurs honorables, j'ai pu venir en France pour continuer mon étude en mathématiques. Je les remercie infiniment pour toutes les mathématiques qu'ils m'ont apprises et aussi pour toute l'énergie qu'ils ont consacrée à la collaboration franco-chinoise. Ils me font l'honneur d'assister à la soutenance d'aujourd'hui.

Je remercie également les professeurs Lawrence Breen et Olivier Brinon pour d'avoir accepté de faire partie du jury.

Je voudrais remercier les professeurs Ouyang Yi, Wen Zhiying, Zhang Xianke et Zheng Zhiyong à l'Université Tsinghua pour leurs aides à m'envoyer en France et aussi pour toutes les sollicitudes qu'ils ont mises sur moi.

Je remercie aussi tous les collègues du LAGA à l'Institut Galilée, surtout ceux de l'équipe d'arithmétique et géométrie algébrique, ainsi que les secrétaires, le bibliothécaire et la technicienne, pour leur sympathie et gentillesse.

Enfin, un grand merci à mes amis aimables, proches ou lointains, mathématiciens ou non, pour leurs amitiés sincères et précieuses : Chen Ke, Chen Miaofen, Chen Zongbin, Hu Yong, Hu Yongquan, Jiang Zhi, Lei Lei, Liang Xiangyu, Liu Qian, Lü Xuemin, Qian Yingying, Shan Peng, Tan Fucheng, Tong Jilong, Xin Pei, Wang Shanwen, Wen Wen, Xiao Liang, Yuan Zhiye, Zheng Weizhe, Zhou Guodong, ...

Table des matières

Introduction

Cette thèse trouve sa source dans le célèbre papier de N. Katz *p-adic properties of modular schemes and modular forms* [14]. Pour développer la théorie des formes modulaires p-adiques pour GL_2, Katz utilise deux résultats géométriques profonds pour les courbes elliptiques, à savoir, la théorie du sous-groupe canonique et le théorème d'Igusa sur la monodromie p-adique d'une famille verselle de courbes elliptiques ordinaires. On se propose dans ce travail de généraliser ces deux résultats aux groupes de Barsotti-Tate.

0.1. Soit $\mathscr{O}_K$ un anneau de valuation discrète complet, de corps résiduel parfait de caractéristique $p > 0$ et de corps des fractions K de caractéristique 0. Notons $S = \mathrm{Spec}(\mathscr{O}_K)$ et s son point fermé. Soit G un groupe de Barsotti-Tate sur S. Dans la premiére partie de ce travail [I], intitulée *Canonical subgroups of Barsotti-Tate groups*, je m'intéresse au problème d'existence d'un relèvement canonique de l'homomorphisme de Frobenius de la fibre spéciale G_s. Si G_s est ordinaire, le noyau de l'homomorphisme de Frobenius est un groupe de type multiplicatif, qui se relève uniquement en un sous-schéma en groupes fermé de G, fini et plat sur S. Si on ne suppose plus G_s ordinaire mais seulement que "G est suffisamment proche d'un groupe de Barsotti-Tate ordinaire", ce qui se traduit de façon précise en terme de la valuation d'un certain déterminant, je montre que le noyau de l'homomorphisme de Frobenius de G_s se relève canoniquement en un sous-schéma en groupes de G, fini et plat sur S. C'est le *sous groupe canonique* de G. En d'autres termes, sous la même condition, l'homomorphisme de Frobenius de G_s se relève canoniquement en une isogénie de groupes de Barsotti-Tate sur S.

Ce problème a été posé pour la première fois par Lubin en 1967 et résolu par lui pour les groupes formels de dimension 1 [16]. Deux ans plus tard, Dwork a posé une question un peu plus faible pour les schémas abéliens et l'a résolue pour les courbes elliptiques, à savoir, est-ce qu'on peut étendre la construction du sous-groupe canonique dans le cas ordinaire à un "voisinage tubulaire" (sans exiger que le prolongement relève le noyau du Frobenius) ? En dimension supérieure, la conjecture de Dwork a été résolue par Abbes et Mokrane [1]. Ultérieurement, il y a eu d'autres approches, toujours pour les schémas abéliens, dues à Andreatta et Gasbarri [4], Kisin et Lai [15], et Conrad [6].

Soit G un groupe de Barsotti-Tate tronqué de niveau 1 sur S. Suivant [1, 2], on peut munir G d'une filtration canonique par des sous-schémas en groupes fermés, finis et plats sur S. Dans le résultat principal de la première partie, je donne une condition différentielle simple et explicite pour que G admette un sous-groupe canonique, et je montre que ce dernier est un cran de la filtration canonique. Par un théorème de Raynaud, G se plonge dans un S-schéma abélien. On se ramène alors pour une partie de l'énoncé au cas d'un schéma abélien [1]. Pour montrer que le sous-groupe canonique relève le noyau du Frobenius (ce qui est nouveau même pour les schémas abéliens), je décris la filtration canonique d'un S-schéma en groupes commutatif, annulé par p, fini et plat sur S, en terme de groupes de congruence. Cet énoncé, fortement intéressant en soi, fait le lien avec l'approche d'Andreatta-Gasbarri [4].

0.2. Dans la seconde partie de cette thèse [II], intitulée *p-adic monodromy of the universal deformation of an elementary Barsotti-Tate group*, je généralise un théorème d'Igusa qui dit que la monodromie p-adique d'une famille verselle de courbes elliptiques ordinaires est maximale. Soient k un corps algébriquement clos de caractéristique $p > 0$, S un k-schéma, G un groupe de Barsotti-Tate sur S de hauteur h et de dimension d, U le lieu ordinaire de G (*i.e.* l'ouvert de S formé des points audessus desquels les fibres de G sont ordinaires), $\overline{\xi}$ un point géométrique de U. Notons $G_U^{\text{ét}}$

le quotient étale maximal de $G_U = S \times_S U$ sur U, $G(n)$ le noyau de la multiplication par p^n dans G et

$$\mathrm{T}_p(G, \overline{\xi}) = \varprojlim_n G(n)(\overline{\xi}) = \varprojlim_n G_U^{\text{ét}}(n)(\overline{\xi})$$

le module de Tate de G en $\overline{\xi}$, qui est un $\mathbb{Z}_p$-module libre de rang $d^* = h - d$. Le groupe de Barsotti-Tate étale $G_U^{\text{ét}}$ donne naissance à une représentation du groupe fondamental de U

$$\rho_G \colon \pi_1(U, \overline{\xi}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G, \overline{\xi})) \simeq \mathrm{GL}_{d^*}(\mathbb{Z}_p). \tag{0.2.1}$$

On dit que ρ_G est l'homomorphisme de monodromie associé à G, et son image est la monodromie p-adique de G. Suivant Igusa [13, 14], il est raisonnable de conjecturer que si G est versel, sa monodromie est aussi large que possible ; on s'attend souvent à ce que ρ_G soit surjectif ou au moins à ce que son image contienne un sous-groupe ouvert de $\mathrm{GL}_{d^*}(\mathbb{Z}_p)$. Mon résultat principal dans cette partie est que *ρ_G est surjectif lorsque G est la déformation universelle de l'unique groupe de Barsotti-Tate connexe de hauteur* 3 *et dimension* 1.

Le théorème d'Igusa a été l'origine de beaucoup de travaux et de nombreuses généralisations. Citons en particulier la généralisation de Faltings et Chai [10] à l'espace de modules des variétés abéliennes principalement polarisées de dimension g en caractéristique p munies d'une structure symplectique de niveau n (premier à p), celles de Deligne-Ribet [7] et Hida [12] à certains espaces de modules de type PEL, celle de Gross aux groupes formels de Lubin-Tate, et enfin celle d'Ekedahl [9] à la jacobienne de la courbe stable universelle de genre g en caractéristique p, munie d'une structure symplectique de niveau n (premier à p). Mon approche est fortement inspirée par celle d'Ekedahl.

Pour un nombre rationnel $\lambda \in (0,1)$, je considère l'homomorphisme $\rho^\lambda = \rho_G$ lorsque G est la déformation universelle du groupe de Barsotti-Tate élémentaire de pente λ (*i.e.* dont le module de Dieudonné est monogène de pente λ). On notera qu'un groupe de Barsotti-Tate de hauteur h et dimension 1 est élémentaire de pente $\lambda = 1/h$. Je conjecture que ρ^λ est surjectif. Le théorème d'Igusa équivaut à dire que $\rho^{1/2}$ est surjectif. Pour l'instant, j'ai pu mener mon approche jusqu'au bout et montrer la conjecture seulement pour $\lambda = 1/3$. Mais j'ai aussi obtenu des résultats intéressants sur la réduction modulo p de ρ^λ, pour tout λ, qui peuvent être considérés comme des analogues en caractéristique p des résultats de Serre sur la représentation galoisienne modulo p associée à une courbe elliptique sur un corps de nombres [18].

Dans la suite de cette introduction, je présenterai un résumé en français des principaux résultats de chaque partie.

1 Sous-groupes canoniques des groupes de Barsotti-Tate

1.1. Soient $\mathscr{O}_K$ un anneau de valuation discrète complet de corps résiduel k parfait de caractéristique $p > 0$ et de corps des fractions K de caractéristique 0, $S = \mathrm{Spec}(\mathscr{O}_K)$. Soit G un groupe de Barsotti-Tate tronqué de niveau 1 sur S. Pour énoncer le résultat principal, j'aurais besoin de deux notions : la hauteur de Hodge de G, qui est un invariant numérique mesurant le défaut de l'ordinarité de G, et la filtration canonique de G.

1.2. Posons $S_1 = \mathrm{Spec}(\mathscr{O}_K/p\mathscr{O}_K)$. La valuation v_p de $\mathscr{O}_K$ normalisée par $v_p(p) = 1$ induit une valuation tronquée $\mathscr{O}_{S_1}\backslash\{0\} \to [0,1)$. Posons $G_1 = G \times_S S_1$ et $\mathrm{Lie}(G_1^\vee)$ l'algèbre de Lie de son dual de Cartier. Rappelons que l'on a la dualité de Grothendieck [5, 3.2.1.3]

$$\mathrm{Lie}(G_1^\vee) \simeq \mathscr{H}om_{(S_1)_{\mathrm{fppf}}}(G_1, \mathbb{G}_a), \tag{1.2.2}$$

où $\mathbb{G}_a$ est le schéma en groupes additif sur S_1. L'homomorphisme de Frobenius de $\mathbb{G}_a$ induit donc un endomorphisme semi-linéaire de $\mathrm{Lie}(G_1^\vee)$; on le note HW_{G_1} et l'appelle *morpshisme de Hasse-Witt de* G_1. Suivant [1], on définit la *hauteur de Hodge* de $\mathrm{Lie}(G_1^\vee)$ comme la valuation p-adique tronquée du déterminant d'une matrice de HW_{G_1}. Il est clair que la fibre spéciale G_s est ordinaire si et seulement si la hauteur de Hodge de $\mathrm{Lie}(G_1^\vee)$ est nulle.

1.3. Suivant [1, 2], on peut munir G d'une filtration canonique, exhaustive et décroissante $(G^a, a \in \mathbb{Q}_{\geq 0})$ par des sous-schémas en groupes fermés de G, finis et plats sur S, appelée *filtraion canonique*. Pour tout nombre réel $a \geq 0$, on pose $G^{a+} = \cup_{b>a} G^b$ où b parcourt les nombres rationnels supérieurs à a.

Théorème 1.4 ([I] Thm. 1.4)**.** *Soient e l'indice de ramification absolu de K, $j = e/(p-1)$, G un groupe de Barsotti-Tate tronqué de niveau 1 sur S, de hauteur h, d la dimension de l'algèbre de Lie de G_s sur k. Supposons $p \geq 3$ et la hauteur de Hodge de* $\mathrm{Lie}(G_1^\vee)$ *strictement inférieure à $1/p$. Alors :*
(i) *Le sous-schéma en groupes G^{j+} est localement libre de rang p^d sur S.*
(ii) *La fibre spéciale de G^{j+} est le noyau de l'homomorphisme de Frobenius de G_s.*

Lorsque G est le noyau de la multiplication par p d'un schéma abélien sur S, l'énoncé 1.4(i) a été prouvé par Abbes et Mokrane [1, 3.1.2] avec une borne moins optimale sur la hauteur de Hodge. En utilisant un théorème de Raynaud [5, 3.1], on peut plonger G dans un schéma abélien sur S, ce qui nous permet d'étendre leur résultat à G. L'énoncé 1.4(ii) est nouveau même pour les schémas abéliens. Pour le prouver, on donnera une nouvelle description élémentaire de la filtration canonique en terme des groupes de congruence. Cette approche est inspirée par celle d'Andreatta et Gasbarri [4].

1.5. Rappelons la définition des groupes de congruence suivant [17]. Soient $\overline{K}$ une clôture algébrique de K, $\mathscr{O}_{\overline{K}}$ la clôture intégrale de $\mathscr{O}_K$ dans $\overline{K}$, $\overline{S} = \mathrm{Spec}(\mathscr{O}_{\overline{K}})$, v la valuation de $\overline{K}$ normalisée par $v(p) = e$. Pour tout $\lambda \in \mathscr{O}_{\overline{K}}$, posons

$$P_\lambda(T) = \frac{(1+\lambda T)^p - 1}{\lambda^p} \in \overline{K}[T].$$

Si $0 \leq v(\lambda) \leq e/(p-1)$, le polynôme $P_\lambda(T)$ a des coefficients entiers, et on peut munir $G_\lambda = \mathrm{Spec}(\mathscr{O}_{\overline{K}}[T]/P_\lambda(T))$ d'une structure de schéma en groupes tel que la co-multiplication soit définie par $T \mapsto 1 \otimes T + T \otimes 1 + \lambda T \otimes T$ et le co-inverse par $T \mapsto -\frac{T}{1+\lambda T}$. On appelle G^λ le *groupe de congruence de niveau* λ (la terminologie est due à Raynaud). Si $v(\lambda) = 0$, G_λ est isomorphe au groupe multiplicatif μ_p sur $\overline{S}$. Si $v(\lambda) = e/(p-1)$, G_λ est isomorphe au groupe étale constant $\mathbb{Z}/p\mathbb{Z}$ sur $\overline{S}$.

Pour tout $\lambda \in \mathscr{O}_{\overline{K}}$ avec $0 \leq v(\lambda) \leq e/(p-1)$, on définit un homomorphisme

$$\theta_\lambda \colon G_\lambda \to \mu_p = \mathrm{Spec}(\mathscr{O}_{\overline{K}}[X]/(X^p - 1))$$

en posant $X \mapsto 1 + \lambda T$ au niveau des algèbres de Hopf. Observons que la restriction de θ_λ aux fibres spéciales est un isomorphisme et que θ_λ est un isomorphisme si $v(\lambda) = 0$. Pour tous $\lambda, \gamma \in \mathscr{O}_{\overline{K}}$ vérifiant $0 \leq v(\gamma) \leq v(\lambda) \leq e/(p-1)$, posons $\theta_{\lambda,\gamma} : G_\lambda \to G_\gamma$ l'homomorphisme défini par $T \mapsto (\lambda/\gamma)T$ au niveau des algèbres de Hopf. On a $\theta_\lambda = \theta_\gamma \circ \theta_{\lambda,\gamma}$.

1.6. Soient G un S-schéma en groupes commutatif, annulé par p, fini et plat sur S, $G^\vee$ son dual de Cartier. Pour tout $\lambda \in \mathscr{O}_{\overline{K}}$ tel que $0 \leq v(\lambda) \leq e/(p-1)$, θ_λ induit un homomorphisme injectif de groupes

$$\theta_\lambda(G)\colon \operatorname{Hom}_{\overline{S}}(G, G_\lambda) \to \operatorname{Hom}_{\overline{S}}(G, \mu_p) = G^\vee(\overline{K})$$

dont l'image ne dépend que de $a = v(\lambda)$ [I, Lemma 7.4]. On pose $G^\vee(\overline{K})^{[a]}$ l'image de $\theta_\lambda(G)$. On obtient ainsi une filtration exhaustive décroissante de $G^\vee(\overline{K})$, indexée par $\mathbb{Q} \cap [0, \frac{e}{p-1}]$, qu'on appelle *filtration par les groupes de congruence.*

Théorème 1.7 ([I] Thm. 1.6)**.** *Soient G un S-schéma en groupes commutatif, annulé par p, fini et plat sur S, $G^\vee$ son dual de Cartier. Alors, sous l'accouplement canonique*

$$G(\overline{K}) \times G^\vee(\overline{K}) \to \mu_p(\overline{K}),$$

on a, pour tout $a \in \mathbb{Q}_{\geq 0}$,

$$G^{a+}(\overline{K})^\perp = \begin{cases} G^\vee(\overline{K})^{[\frac{e}{p-1} - \frac{a}{p}]}, & si\ 0 \leq a \leq \frac{ep}{p-1}; \\ G^\vee(\overline{K}), & si\ a > \frac{ep}{p-1}. \end{cases}$$

Andreatta et Gasbarri [4] ont utilisé les groupes de congruence pour montrer l'existence du sous-groupe canonique pour les schémas abéliens. Le théorème 1.7 explique le lien entre l'approche de [1] et de cette thèse via la théorie de ramification et celle de [4].

1.8. Introduisons maintenant une troisième filtration, la filtration de Bloch-Kato, qui jouera un rôle clé dans les démonstrations de 1.4(i) et de 1.7. Soient X un schéma propre et lisse sur S, $\overline{X} = X \times_S \overline{S}$. Considérons le diagramme cartésien

$$\begin{tikzcd} X_{\overline{s}} \arrow[r, "\overline{i}"] \arrow[d] & \overline{X} \arrow[d] & X_{\overline{\eta}} \arrow[l, "\overline{j}"'] \arrow[d] \\ \overline{s} = \operatorname{Spec} \overline{k} \arrow[r] & \overline{S} & \overline{\eta} = \operatorname{Spec} \overline{K} \arrow[l] \end{tikzcd}$$

et les faisceaux des cycles évanescents sur $X_{\overline{s}}$

$$\Psi_X^q = \overline{i}^* R^q \overline{j}_*(\mathbb{Z}/p\mathbb{Z}(q)),$$

où $q \geq 0$ est un entier et $\mathbb{Z}/p\mathbb{Z}(q)$ désigne le q-ème tordu de Tate de $\mathbb{Z}/p\mathbb{Z}$. Il est clair que $\Psi_X^0 \simeq \mathbb{Z}/p\mathbb{Z}$. Par le théorème de changement de base propre, on a une suite spectrale

$$E_2^{p,q}(X) = \mathrm{H}^p(X_{\overline{s}}, \Psi_X^q)(-q) \Longrightarrow \mathrm{H}^{p+q}(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}),$$

qui induit une suite exacte

$$(1.8.1) \qquad 0 \to \mathrm{H}^1(X_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{u} \mathrm{H}^0(X_{\overline{s}}, \Psi_X^1)(-1) \to \mathrm{H}^2(X_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}).$$

La suite exacte de Kummer $0 \to \mu_p \to \mathbb{G}_m \to \mathbb{G}_m \to 0$ sur $X_{\overline{\eta}}$ induit le morphisme de symbole

$$h_{\overline{X}} : \overline{i}^* \overline{j}_* \mathscr{O}_{X_{\overline{\eta}}}^\times \to \Psi_X^1.$$

Posons $\mathrm{U}^0\Psi_X^1 = \Psi_X^1$ et pour tout $a \in \mathbb{Q}_{>0}$

$$\mathrm{U}^a\Psi_X^1 = h_{\overline{X}}(1 + \pi^a \overline{i}^* \mathscr{O}_{\overline{X}}),$$

où par abus de notation π^a désigne un élément de $\mathscr{O}_{\overline{K}}$ tel que $v(\pi^a) = a$. D'après [1, Lemme 3.1.1], on a $\mathrm{U}^a\Psi^1_X = 0$ si $a \geq \frac{ep}{p-1}$.

En prenant la cohomologie, on obtient une filtration de $\mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})$ définie par

$$\mathrm{U}^a\mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} \mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) & \text{si } a = 0 \\ u^{-1}(\mathrm{H}^0(X_{\overline{s}}, \mathrm{U}^a\Psi^1_X)(-1)) & \text{si } a \in \mathbb{Q}_{>0} \end{cases} \tag{1.8.2}$$

appelée *filtration de Bloch-Kato.*

1.9. Soit G un S-schéma en groupes commutatif, annulé par p, fini et plat sur S. On se propose de munir le groupe $G^\vee(\overline{K})$ d'une filtration en utilisant les cycles évanescents. Pour ce faire, on utilisera le théorème suivant de Raynaud [5, 3.1.1] : il existe une suite exacte de faisceaux fppf abéliens sur S

$$0 \to G \to A \to B \to 0, \tag{1.9.3}$$

où A et B sont des schémas abéliens sur S. On appelera une telle suite exacte une *résolution de G par des schémas abéliens.*

La suite exacte (1.8.1) étant fonctorielle, on a un diagramme commutatif

(1.9.4)
$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_1"] & \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_2"] & \mathrm{H}^0(B_{\overline{s}}, \Psi^1_B)(-1) \arrow[r, "d_2^{1,0}(B)"] \arrow[d, "\alpha_3"] & \mathrm{H}^2(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\alpha_4"] \\
0 \arrow[r] & \mathrm{H}^1(A_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^0(A_{\overline{s}}, \Psi^1_A)(-1) \arrow[r, "d_2^{1,0}(A)"] & \mathrm{H}^2(A_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}).
\end{tikzcd}$$

Rappelons que pour tout schéma abélien X sur un corps algébriquement clos L, on a un isomorphisme canonique [I, Cor. 4.6]

$$\mathrm{H}^1_{\text{ét}}(X, \mathbb{F}_p) \simeq \mathrm{Ext}^1(X, \mathbb{F}_p),$$

où Ext^1 est l'extension dans la catégorie de faisceaux fppf abéliens sur L. En particulier, l'homomorphisme α_1 dans (1.9.4) s'identifie à l'homomorphisme fonctoriel

$$\mathrm{Ext}^1(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}^1(A_{\overline{s}}, \mathbb{Z}/p\mathbb{Z})$$

induit par l'isogénie $A \to B$. Donc compte tenu de (1.9.3), on a

$$\mathrm{Ker}(\alpha_1) = \mathrm{Hom}(G_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) = (G^\vee)^{\text{ét}}(\overline{K})(-1),$$

où $(G^\vee)^{\text{ét}}$ désigne la partie étale du dual de Cartier de G. De même, on a

$$\mathrm{Ker}(\alpha_2) = \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) = G^\vee(\overline{K})(-1).$$

Posant $N = \mathrm{Ker}(\alpha_3)$, On obtient un diagramme commutatif

(1.9.5)
$$\begin{tikzcd}
0 \arrow[r] & (G^\vee)^{\text{ét}}(\overline{K})(-1) \arrow[r] \arrow[d, hook, "\gamma_1"] & G^\vee(\overline{K})(-1) \arrow[r, "u"] \arrow[d, hook, "\gamma_2"] & N \arrow[d, hook, "\gamma_3"] & \\
0 \arrow[r] & \mathrm{H}^1(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^0(B_{\overline{s}}, \Psi^1_B)(-1) \arrow[r, "d_2^{1,0}(B)"] & \mathrm{H}^2(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z})
\end{tikzcd}$$

Pour $a \in \mathbb{Q}_{\geq 0}$, on pose

$$\mathrm{U}^a G^\vee(\overline{K}) = \gamma_2^{-1}\big(\mathrm{U}^a \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})\big)(1).$$

On obtient ainsi une filtration exhaustive décroissante de $G^\vee(\overline{K})$, qu'on appelle *filtration de Bloch-Kato.*

Proposition 1.10 ([I] Prop. 5.5). *Soient G un S-schéma en groupes commutatif, annulé par p, fini et plat sur S, e l'indice de ramification absolu de K, $e' = \frac{ep}{p-1}$. Alors :*

(i) *Le morphisme u dans* (1.9.5) *est surjectif.*

(ii) *Sous l'accouplement parfait canonique*

$$G(\overline{K}) \times G^\vee(\overline{K}) \to \mu_p(\overline{K}),$$

on a, pour tout $a \in \mathbb{Q}_{\geq 0}$,

$$G^{a+}(\overline{K})^\perp = \begin{cases} \mathrm{U}^{e'-a} G^\vee(\overline{K}) & si\ 0 \leq a < e'; \\ G^\vee(\overline{K}) & si\ a \geq e'. \end{cases} \tag{1.10.1}$$

En particulier, la filtration $(\mathrm{U}^a G^\vee(\overline{K}), a \in \mathbb{Q}_{\geq 0})$ *ne dépend pas de la résolution de G par des schémas abéliens.*

La relation d'orthogonalité (1.10.1) entre la filtration canonique et la filtration de Bloch-Kato joue un rôle central dans la première partie de cette thèse. Elle nous permet, d'une part de réduire l'énoncé 1.4(i) à un calcul cohomologique des schémas abéliens, et d'autre part de déduire le théorème 1.7 de la proposition suivante.

Proposition 1.11 ([I] Prop. 7.8). *Sous les hypothèses de* (1.10), *on a $G^\vee(\overline{K})^{[a]} = \mathrm{U}^{pa} G^\vee(\overline{K})$ pour tout nombre rationnel a tel que $0 \leq a \leq e/(p-1)$, où $(G^\vee(\overline{K})^{[a]})$ est la filtration par les groupes de congruence de $G^\vee(\overline{K})$ définie dans* (1).

Pour un schéma abélien A sur S, Andreatta et Gasbarri [4, 6.8] ont défini une filtration sur $\mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})$ en utilisant les groupes de congruence, et l'ont comparée avec la filtration de Bloch-Kato (1.8.2). La proposition ci-dessus est une généralisation de *loc. cit.* aux schémas en groupes finis annulés par p.

2 Monodromie p-adique de la déformation universelle d'un groupe de Barsotti-Tate élémentaire

2.1. Soient k un corps algébriquement clos de caractéristique $p > 0$, s, r des entiers premiers entre eux tels que $0 \leq s < r$, $\lambda = \frac{s}{r}$. On désigne par G^λ le groupe de Barsotti-Tate sur k dont le module de Dieudonné est engendré par un élément e vérifiant la relation $(F^{r-s} - V^s) \cdot e = 0$; on l'appelle *groupe de Barsotti-Tate élémentaire de pente* λ. Il est de hauteur r et de dimension s. On notera que tout groupe de Barsotti-Tate de hauteur h et de dimension 1 est isomorphe à $G^{1/h}$.

2.2. D'après Grothendieck, le foncteur de déformations de G^λ en caractéristique p est pro-représentable par un schéma formel $\mathscr{S}^\lambda$, formellement lisse de dimension $(r-s)\cdot s$ sur k, *i.e.* on a un isomorphisme $\mathscr{S}^\lambda \simeq \mathrm{Spf}(R)$ où $R = k[[(t_{i,j})_{1\leq i\leq (r-s), 1\leq j\leq s}]]$. Posons $\mathfrak{m}_R$ l'idéal maximal de R et $S_n = \mathrm{Spec}(R/\mathfrak{m}_R^{n+1})$ pour $n \geq 0$. On note $\mathscr{G}^\lambda$ la déformation formelle universelle de G^λ au-dessus de $\mathscr{S}^\lambda$; c'est un système de groupes de Barsotti-Tate G_n sur S_n tels que $G_n = G_{n+1} \times_{S_{n+1}} S_n$. D'après de Jong, $\mathscr{G}^\lambda$ s'algébrise en un groupe de Barsotti-Tate $\mathbf{G}^\lambda$ sur $\mathbf{S}^\lambda = \mathrm{Spec}(R)$. On appelle $\mathbf{S}^\lambda$ *l'espace de modules local algébrique* de G^λ et $\mathbf{G}^\lambda$ la *déformation algébrique universelle* (en caractéristique p) de G^λ.

2.3. Soient $\mathbf{U}^\lambda$ le lieu ordinaire de $\mathbf{G}^\lambda$ sur $\mathbf{S}^\lambda$, $\overline{\xi}$ un point géométrique de $\mathbf{U}^\lambda$. On sait que $\mathbf{U}^\lambda$ est l'ouvert complémentaire d'un diviseur défini par un paramètre régulier de $\mathbf{S}^\lambda$ [II, Cor. 4.13]. Considérons la représentation de monodromie associée à $\mathbf{G}^\lambda$ (0.2.1)

$$\rho^\lambda \colon \pi_1(\mathbf{U}^\lambda, \overline{\xi}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G}^\lambda, \overline{\xi})) \simeq \mathrm{GL}_{r-s}(\mathbb{Z}_p) \tag{2.3.1}$$

Motivé par un célèbre théorème d'Igusa [14, thm. 4.3], on fait la conjecture suivante :

Conjecture 2.4. *L'homomorphisme ρ^λ est surjectif pour tout nombre rationnel $\lambda \in (0,1)$.*

2.5. Le théorème d'Igusa, mentionné ci-dessus, correspond au cas où $\lambda = 1/2$; on a alors $\mathbf{S}^{1/2} \simeq \mathrm{Spec}(k[[t]])$, $\mathbf{U}^{1/2} = \xi$ est le point générique de $\mathbf{S}^{1/2}$, et l'homomorphisme $\rho^{1/2}$ est une représentation galoisienne

$$\rho^{1/2} \colon \mathrm{Gal}(\overline{\xi}/\xi) \to \mathrm{GL}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G}^{1/2}, \overline{\eta})) \simeq \mathbb{Z}_p^\times .$$

2.6. Considérons le cas où $\lambda = 1/3$. On a $\mathbf{S}^{1/3} = \mathrm{Spec}(R)$ où $R = k[[t_1, t_2]]$, et $\mathbf{U}^{1/3} = \mathrm{Spec}(R[1/t_1])$. Le théorème suivant est le résultat principal de la seconde partie de cette thèse.

Théorème 2.7 ([II] Thm. 1.7). *La conjecture* 2.4 *est vraie pour* $\lambda = 1/3$, i.e. *l'homomorphisme*

$$\rho^{1/3} \colon \pi_1(\mathbf{U}^{1/3}, \overline{\xi}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G}^{1/3}, \overline{\xi})) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

est surjectif.

2.8. Pour tout nombre rationnel $\lambda \in (0,1)$, on désigne par

$$\overline{\rho}^\lambda \colon \pi_1(\mathbf{U}^\lambda, \overline{\xi}) \to \mathrm{Aut}_{\mathbb{F}_p}(\mathrm{T}_p(\mathbf{G}^\lambda, \overline{\xi})/p\mathrm{T}_p(\mathbf{G}^\lambda, \overline{\xi})) \simeq \mathrm{GL}_{r-s}(\mathbb{F}_p),$$

la réduction modulo p de l'homomorphisme ρ^λ. On a les résultats suivants :

Proposition 2.9. (i) *L'image de $\overline{\rho}^\lambda$ contient un sous-groupe H de $\mathrm{GL}_{r-s}(\mathbb{F}_p)$ tel que le sous-ensemble $H \cup \{0\}$ de l'algèbre des matrices $\mathrm{M}_{(r-s)\times(r-s)}(\mathbb{F}_p)$ soit un corps fini à p^{r-s} éléments.*

(ii) *L'ordre du groupe $\mathrm{Im}(\overline{\rho}^\lambda)$ est divisible par p^{r-s-1}.*

(iii) *Si $r - s = 1$ ou 2, l'homomorphisme $\overline{\rho}^\lambda$ est surjectif.*

Pour démontrer 2.7 et 2.9, mon approche, inspirée par celle d'Ekedahl [9], consiste, d'une part à étudier la monodromie d'une déformation de G^λ sur un trait de caractéristique p, et d'autre part à construire des traits sur l'espace de modules local algébrique $\mathbf{S}^\lambda$ au-dessus desquels $\mathbf{G}^\lambda$ a une large monodromie. Chemin faisant, on a obtenu des résultats intéressants qu'on se propose de résumer dans la suite.

2.10. Soient $A = k[[\pi]]$ l'anneau des séries formelles en une variable sur k, K son corps des fractions, $\overline{K}$ une clôture algébrique de K, K^{sep} la clôture séparable de K dans $\overline{K}$. Posons $S = \mathrm{Spec}(A)$, s (resp. η) le point fermé (resp. générique) de S, $\overline{\eta}$ le point géométrique de S

correspondant à $\overline{K}$, $I = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ le groupe de Galois de K^{sep} sur K et v la valuation de K normalisée par $\mathrm{v}(\pi) = 1$.

Soient G un groupe de Barsotti-Tate sur S, $G^\vee$ son dual de Serre. L'algèbre de Lie de $G^\vee$, notée $\mathrm{Lie}(G^\vee)$, est un module libre de rang fini sur A. L'homomorphisme de Frobenius de G induit alors un endomorphisme semi-linéaire de $\mathrm{Lie}(G^\vee)$ [II, 2.7.1]. On l'appelle *morphisme de Hasse-Witt* et on le note HW_G. *L'invariant de Hasse* de G, noté $hw(G)$, est la valuation du déterminant d'une matrice de HW_G [II, 5.4]. Cet invariant, analogue en caractéristique p de la hauteur de Hodge qu'on a introduit au début du chapitre §1, mesure l'ordinarité de G ; G est ordinaire si et seulement si $hw(G) = 0$, et G est génériquement ordinaire si et seulement si $hw(G) < \infty$. Le cas où $hw(G) = 1$ a un intérêt particulier. En effet, on peut reformuler le théorème d'Igusa comme suit.

Théorème 2.11 ([II] Théo. 5.14). *Soit G un groupe de Barsotti-Tate connexe de dimesion 1 et de hauteur 2 sur S tel que $hw(G) = 1$. Alors G est versel sur S et l'homomorphisme de monodromie associé à G*

$$\rho_G \colon I = \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G, \overline{\eta})) \simeq \mathbb{Z}_p^\times$$

est surjectif.

2.12. Pour un groupe de Barsotti-Tate général sur S, on peut décrire la réduction modulo p de l'homomorphisme de monodromie associé. Rappelons d'abord quelques propriétés sur le groupe d'inertie I. Soient $I_p \subset I$ le sous-groupe d'inertie sauvage, $I_t = I/I_p$ le groupe d'inertie modérée. On a un isomorphisme canonique

$$\theta \colon I_t \xrightarrow{\sim} \varprojlim_{(d,p)=1} \mu_d, \tag{2.12.1}$$

où d parcourt l'ensemble des entiers positifs premiers à p, μ_d est le groupe des racines d-ème de l'unité dans k, et le morphisme de transition $\mu_m \to \mu_d$ est donné par $\zeta \mapsto \zeta^{m/d}$ lorsque d divise m. Pour tout d, on note $\theta_d \colon I_t \to \mu_d$ la projection induite de (2.12.1). Soient q une puissance de p, $\mathbb{F}_q$ le sous-corps de k à q éléments. On a $\mathbb{F}_q^\times = \mu_{q-1}$; on peut donc écrire $\theta_{p^n-1} \colon I_t \to \mathbb{F}_{p^n}^\times$.

Soient G un groupe de Barsotti-Tate sur S de hauteur h et de dimension d, $G(1)$ le noyau de la multiplication par p sur G. On pose $d^* = h - d$ et

$$\overline{\rho}_G \colon I \to \mathrm{Aut}_{\mathbb{F}_p}(G(1)(\overline{K})) \simeq \mathrm{GL}_{d^*}(\mathbb{F}_p) \tag{2.12.2}$$

la réduction modulo p de l'homomorphisme de monodromie associé à G.

Proposition 2.13 ([II] Prop. 5.11). *Soient r, s des entiers premiers entre eux tels que $0 \leq s < r$, $\lambda = \frac{s}{r}$, $q = p^{r-s}$, G une déformation de G^λ au-dessus de S telle que $hw(G) = 1$. Alors la représentation $\overline{\rho}_G$ est modérée ; de plus, $G(1)(\overline{K})$ est un $\mathbb{F}_q$-espace vectoriel sur lequel l'action induite de I_t est donnée par le caractère $\theta_{q-1} \colon I_t \to \mathbb{F}_q^\times$.*

Cette proposition est un analogue en caractéristique p d'un résultat de Serre sur la monodromie modulo p associée aux groupes formels de dimension 1 en caractéristiques mixtes [18, Prop. 9]. Sa preuve, inspirée par *loc. cit.*, est basée sur l'étude du morphisme de Hasse-Witt de G.

2.14. Soient G un groupe de Barsotti-Tate sur $S = \mathrm{Spec}(A)$, G_s sa fibre spéciale, d^* la dimension de son dual de Serre $G^\vee$. On dit que G est *HW-cyclique* [II, 5.6] s'il remplit les conditions équivalentes suivantes :

(i) Il existe un élément e de $\mathrm{Lie}(G_s^\vee)$ tel que

$$(e,\ \mathrm{HW}_{G_s}(e),\ \ldots\ ,(\mathrm{HW}_{G_s})^{d^*-1}(e))$$

forment une base de HW_{G_s}.

(ii) L'algèbre de Lie de $G^\vee$ admet une base sur A dans laquelle HW_G est représenté par une matrice à coefficients dans A de la forme

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d^*} \end{pmatrix} \tag{2.14.1}$$

L'équivalence de (i) et (ii) découle facilement du lemme de Nakayma.

2.15. On montre que pour tout nombre rationnel $\lambda \in (0,1)$, toute déformation de G^λ à S est HW-cyclique [II, 5.8]. Ce fait important est une conséquence immédiate d'un calcul du morphisme de Hasse-Witt de la déformation universelle de G^λ. D'autre part, tout groupe de Barsotti-Tate connexe sur S avec $hw(G) = 1$ est HW-cyclique. La proposition 2.13 se déduit alors de l'énoncé (i) de la proposition suivante.

Proposition 2.16 ([II] Prop. 5.11, 5.13). *Soient G un groupe de Barsotti-Tate HW-cyclique sur S de hauteur h et de dimension d,*

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d^*} \end{pmatrix}$$

une matrice de HW_G. Posons $d^* = h - d$ et $q = p^{d^*}$.

(i) *Supposons G connexe et $hw(G) = \mathrm{v}(a_1) = 1$. Alors la représentation $\overline{\rho}_G$* (2.12.2) *est modérée ; de plus, $G(1)(\overline{K})$ est un $\mathbb{F}_q$-espace vectoriel de dimension 1 sur lequel I_t agit par le caractère $\theta_{q-1}\colon I_t \to \mathbb{F}_q^\times$.*

(ii) *Supposons $d^* > 1$, $\mathrm{v}(a_i) \geq 2$ pour tout $1 \leq i \leq d^* - 1$ et $\mathrm{v}(a_{d^*}) = 1$. Alors l'ordre du groupe $\mathrm{Im}(\overline{\rho}_G)$ est divisible par p^{d^*-1}.*

(iii) *Posons $f(X) = X^{p^{d^*}} + a_{d^*}X^{p^{d^*-1}} + \cdots + a_1 X$, $a_{d^*+1} = 1$, et*

$$i_0 = \min_{1 \leq i \leq d^*} \{i ; \mathrm{v}(a_i) = 0\} - 1.$$

Supposons qu'il existe $\alpha \in k$ tel que $\mathrm{v}(f(\alpha)) = 1$. Alors on a $0 \leq i_0 \leq d^* - 1$, et l'ordre de $\mathrm{Im}(\overline{\rho}_G)$ est divisible par p^{i_0}.

La forme explicite de HW_G nous permet d'identifier $G(1)(\overline{K})$ au groupe additif formé par les racines de $f(X)$, et par suite de décrire explicitement l'action de I sur $G(1)(\overline{K})$.

Cette proposition est l'ingrédient principal dans les preuves de 2.7 et 2.9. En effet, les énoncés 2.16(i) et 2.16(ii) suffisent pour démontrer 2.9 [II, 7.3]. Pour prouver 2.7, on se ramène à vérifier la non-nullité d'une classe de cohomologie associée à un groupe de Barsotti-Tate sur un trait (cf. [II, 7.9]). L'énoncé 2.16(iii) nous permet de donner un critère explicite pour que cette classe soit non-nulle [II, 5.18].

Références

[I] Y. Tian, Canonical subgroups of Barsotti-Tate groups, Partie I de cette thèse.

[II] Y. Tian, p-adic monodromy of an elementary Barsotti-Tate group, Partie II de cette thèse.

[1] A. Abbes and A. Mokrane, Sous-groupes canoniques et cycles évanescents p-adiques pour les variétés abéliennes, *Publ. Math. Inst. Hautes Étud. Sci.* **99** (2004), 117-162.

[2] A. Abbes and T. Saito, Ramification of local fields with imperfect residue fields, *Am. J. Math.* **124** (2002), 879-920.

[3] J. Achter and P. Norman, Local monodromy of p-divisible groups, Preprint, (2006).

[4] F. Andreatta and C. Gasbarri, The canonical subgroup for families of abelian varieties, *Compos. Math.* **143** (2007), no. 3, 566-602.

[5] F. Berthelot, L. Breen and W. Messing, *Théorie de Dieudonné Cristalline II*, LNM **930**, Springer-Verlag, (1982).

[6] B. Conrad, Higher-level canonical subgroups in abelian varieties, Preprint (2005).

[7] P. Deligne and K. Ribet, Values of abelian L-functions at negative integers over totally real fields. *Inven. Math.* **59**, (1980), 227-286.

[8] B. Dwork, p-adic cycles, *Publ. Math. Inst. Hautes Étud. Sci.* **37** (1969), 27-115.

[9] T. Ekedahl, The action of monodromy on torsion points of Jacobians, *Arithmetic Algebraic Geometry*, G. van der Geer, F. Oort and J. Steenbrink, ed. Progress in Math. **89**, Birkhäuser, (1991), 41-49.

[10] G. Faltings and L. Chai, *Degeneration of Abelian Varieties*, Ergebnisse Bd **22**, Springer-Verlag,(1990).

[11] H. Gross, Ramification in p-adic Lie extensions, *Journée de Géométrie Algébrique de Rennes III, Astérisque* **65**, (1979), 81-102.

[12] H. Hida, p-adic automorphic forms on reductive groups, *Astérisque* **296** (2005), 147-254.

[13] J. Igusa, On the algebraic theory of elliptic modular functions. *J. Math. Soc. Japan* **20** (1968), 96-106.

[14] N. Katz, p-adic properties of modular schemes and modular forms, in *Modular functions of one variable III*, LNM **350**, Springer-Verlag, (1973).

[15] M. Kisin and K. F. Lai, Overconvergent Hilbert modular forms, *Amer. J. of Math.* **127** (2005), 735-783.

[16] J. Lubin, Finite subgroups and isogenies of one-parameter formal groups, *Ann. of Math.* **85**, 2nd series (1967), 296-302.

[17] T. Sekiguchi, F. Oort and N. Suwa, On the deformation of Artin-Schreier to Kummer, *Ann. Sci. de l'É.N.S.* 4^{e} série, tome 22, No.3 (1989), 345-375.

[18] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inven. Math.* **15** (1972), 259-331.

Canonical subgroups of Barsotti-Tate groups

1 Introduction

1.1. Let $\mathscr{O}_K$ be a complete discrete valuation ring with fraction field K of characteristic 0 and perfect residue field k of characteristic $p>0$. We put $S=\mathrm{Spec}(\mathscr{O}_K)$ and denote by s (resp. η) its closed (resp. generic) point. Let G be a truncated Barsotti-Tate group of level 1 over S. If G_s is ordinary, the kernel of its Frobenius endomorphism is a multiplicative group scheme and can be uniquely lifted to a closed subgroup scheme of G, finite and flat over S. If we do not assume G_s ordinary but only that "G is not too supersingular", a condition that will be explicitly expressed in terms of the valuation of a certain determinant, we will prove that we can still canonically lift the kernel of the Frobenius endomorphism of G_s to a subgroup scheme of G, finite and flat over S. We call it *the canonical subgroup* of G. Equivalently, under the same condition, we will prove that the Frobenius endomorphism of G_s can be canonically lifted to an isogeny of truncated Barsotti-Tate groups over S. This problem was first raised by Lubin in 1967 and solved by himself for 1-parameter formal groups [16]. A slightly weaker question was asked by Dwork in 1969 for abelian schemes and answered also by him for elliptic curves [9] : namely, could we extend the construction of the canonical subgroup in the ordinary case to a "tubular neighborhood" (without requiring that it lifts the kernel of the Frobenius) ? The dimension one case played a fundamental role in the pioneering work of Katz on p-adic modular forms [14]. For higher dimensional abelian schemes, Dwork's conjecture was first solved by Abbes and Mokrane [1] ; our approach is a generalization of their results. Later, there have been other proofs, always for abelian schemes, by Andreatta and Gasbarri [3], Kisin and Lai [15] and Conrad [7].

1.2. For an S-scheme X, we denote by X_1 its reduction modulo p. The valuation v_p of K, normalized by $v_p(p)=1$, induces a truncated valuation $\mathscr{O}_{S_1}\backslash\{0\}\to\mathbb{Q}\cap[0,1)$. Let G be a truncated Barsotti-Tate group of level 1 and height h over S, $G^\vee$ be its Cartier dual, and d be the dimension of the Lie algebra of G_s over k. The Lie algebra $\mathrm{Lie}(G_1^\vee)$ of $G_1^\vee$ is a free $\mathscr{O}_{S_1}$-module of rank $d^*=h-d$, canonically isomorphic to $\mathrm{Hom}_{(S_1)_{\mathrm{fppf}}}(G_1,\mathbb{G}_a)$ ([12] 2.1). The Frobenius homomorphism of $\mathbb{G}_a$ over S_1 induces an endomorphism F of $\mathrm{Lie}(G_1^\vee)$, which is semi-linear with respect to the Frobenius homomorphism of $\mathscr{O}_{S_1}$. We define the Hodge height (3) of $\mathrm{Lie}(G_1^\vee)$ to be the truncated valuation of the determinant of a matrix of F. This invariant measures the ordinarity of G.

1.3. Following [1], we construct the canonical subgroup of a truncated Barsotti-Tate group over S by the ramification theory of Abbes and Saito [2]. Let G be a commutative finite and flat group scheme over S. In [1], the authors defined a canonical exhaustive decreasing filtration $(G^a, a\in\mathbb{Q}_{\geq 0})$ by finite, flat and closed subgroup schemes of G. For a real number $a\geq 0$, we put $G^{a+}=\cup_{b>a}G^b$, where b runs over rational numbers.

Theorem 1.4. *Assume that $p\geq 3$, and let e be the absolute ramification index of K and $j=e/(p-1)$. Let G be a truncated Barsotti-Tate group of level 1 over S, d be the dimension of the Lie algebra of G_s over k. Assume that the Hodge height of $\mathrm{Lie}(G_1^\vee)$ is strictly smaller than $1/p$. Then,*

(i) *the subgroup scheme G^{j+} of G is locally free of rank p^d over S ;*

(ii) *the special fiber of G^{j+} is the kernel of the Frobenius endomorphism of G_s.*

1.5. Statement (i) was proved by Abbes and Mokrane [1] for the kernel of multiplication by p of an abelian scheme over S. We extend their result to truncated Barsotti-Tate groups by using a theorem of Raynaud to embed G into an abelian scheme over S. To prove statement (ii), which we call *"the lifting property of the canonical subgroup"*, we give a new description of the canonical filtration of a finite, flat and commutative group scheme over S killed by p in terms of *congruence groups*. Let $\overline{K}$ be an algebraic closure of the fraction field of S, $\mathscr{O}_{\overline{K}}$ be the integral closure of $\mathscr{O}_K$ in $\overline{K}$. Put $\overline{S} = \mathrm{Spec}(\mathscr{O}_{\overline{K}})$. For every $\lambda \in \mathscr{O}_{\overline{K}}$ with $0 \leq v_p(\lambda) \leq 1/(p-1)$, Sekiguchi, Oort and Suwa [20] introduced a finite and flat group scheme G_λ of order p over $\overline{S}$ (see (7)) ; following Raynaud, we call it the congruence group of level λ. If $v_p(\lambda) = 0$, G_λ is isomorphic to the multiplicative group scheme $\mu_p = \mathrm{Spec}(\mathscr{O}_{\overline{K}}[X]/(X^p - 1))$ over $\overline{S}$; and if $v_p(\lambda) = 1/(p-1)$, G_λ is isomorphic to the the constant étale group scheme $\mathbb{F}_p$. For general $\lambda \in \mathscr{O}_{\overline{K}}$ with $0 \leq \lambda \leq 1/(p-1)$, there is a canonical $\overline{S}$-homomorphism $\theta_\lambda : G_\lambda \to \mu_p$, such that $\theta \otimes \overline{K}$ is an isomorphism. For a finite, flat and commutative group scheme G over S killed by p, θ_λ induces a homomorphism

$$\theta_\lambda(G)\colon\ \mathrm{Hom}_{\overline{S}}(G, G_\lambda) \to G^\vee(\overline{K}) = \mathrm{Hom}_{\overline{S}}(G, \mu_p).$$

We prove that it is injective, and its image depends only on the valuation $a = v_p(\lambda)$; we denote it by $G^\vee(\overline{K})^{[ea]}$, where e is the absolute ramification index of K (the multiplication by e will be justified later). Moreover, we get a decreasing exhaustive filtration $(G^\vee(\overline{K})^{[a]}, a \in \mathbb{Q} \cap [0, \frac{e}{p-1}])$.

Theorem 1.6. *Let G be a finite, flat and commutative group scheme over S killed by p. Under the canonical perfect pairing*

$$G(\overline{K}) \times G^\vee(\overline{K}) \to \mu_p(\overline{K}),$$

we have for any rational number $a \in \mathbb{Q}_{\geq 0}$,

$$G^{a+}(\overline{K})^\perp = \begin{cases} G^\vee(\overline{K})^{[\frac{e}{p-1} - \frac{a}{p}]}, & \text{if } \ 0 \leq a \leq \frac{ep}{p-1}, \\ G^\vee(\overline{K}), & \text{if } \ a > \frac{ep}{p-1}. \end{cases}$$

Andreatta and Gasbarri [3] have used congruence groups to prove the existence of the canonical subgroup for abelian schemes. This theorem explains the relation between the approach via the ramification theory of [1] and this paper, and the approach of [3].

1.7. This article is organized as follows. For the convenience of the reader, we recall in section 2 the theory of ramification of group schemes over a complete discrete valuation ring, developed in [2] and [1]. Section 3 is a summary of the results in [1] on the canonical subgroup of an abelian scheme over S. Section 4 consists of some preliminary results on the fppf cohomology of abelian schemes. In section 5, we define the Bloch-Kato filtration for a finite, flat and commutative group scheme over S killed by p. Using this filtration, we prove Theorem 1.4(i) in section 6. Section 7 is dedicated to the proof of Theorem 1.6. Finally in section 8, we complete the proof of Theorem 1.4(ii).

1.8. This article is a part of the author's thesis at Université Paris 13. The author would like to express his great gratitude to his thesis advisor Professor A. Abbes for leading him to this problem and for his helpful comments on earlier versions of this work. The author thanks Professors W. Messing and M. Raynaud for their help. He is also grateful to the referee for his careful reading and very valuable comments.

1.9. Notation In this article, $\mathscr{O}_K$ denotes a complete discrete valuation ring with fraction field K of characteristic 0, and residue field k of characteristic $p > 0$. Except in Section **2**, we will assume that k is perfect. Let $\overline{K}$ be an algebraic closure of K, $\mathscr{G}_K = \mathrm{Gal}(\overline{K}/K)$ be the Galois group of $\overline{K}$ over K, $\mathscr{O}_{\overline{K}}$ be the integral closure of $\mathscr{O}_K$ in $\overline{K}$, $\mathfrak{m}_{\overline{K}}$ the maximal ideal of $\mathscr{O}_{\overline{K}}$, and $\bar{k}$ be the residue field of $\mathscr{O}_{\overline{K}}$.

We put $S = \mathrm{Spec}(\mathscr{O}_K)$, $\overline{S} = \mathrm{Spec}(\mathscr{O}_{\overline{K}})$, and denote by s and η (*resp.* $\bar{s}$ and $\bar{\eta}$) the closed and generic point of S (*resp.* of $\overline{S}$) respectively.

We fix a uniformizer π of $\mathscr{O}_K$. We will use two valuations v and v_p on $\mathscr{O}_K$, normalized respectively by $v(\pi) = 1$ and $v_p(p) = 1$; so we have $v = ev_p$, where e is the absolute ramification index of K. The valuations v and v_p extend uniquely to $\overline{K}$; we denote the extensions also by v and v_p. For a rational number $a \geq 0$, we put $\mathfrak{m}_a = \{x \in \overline{K}; v_p(x) \geq a\}$ and $\overline{S}_a = \mathrm{Spec}(\mathscr{O}_{\overline{K}}/\mathfrak{m}_a)$. If X is a scheme over S, we will denote respectively by $\overline{X}$, $X_{\bar{s}}$ and $\overline{X}_a$ the schemes obtained by base change of X to $\overline{S}$, $\bar{s}$ and $\overline{S}_a$.

If G is a commutative, finite and flat group scheme over S, we will denote by $G^\vee$ its Cartier dual. For an abelian scheme A over S, $A^\vee$ will denote the dual abelian scheme, and ${}_pA$ the kernel of multiplication by p, which is a finite and flat group scheme over S.

2 Ramification theory of finite flat group schemes over S

2.1. We begin by recalling the main construction of [2]. Let A be a finite and flat $\mathscr{O}_K$-algebra. We fix a finite presentation of A over $\mathscr{O}_K$

$$0 \to I \to \mathscr{O}_K[x_1, \cdots, x_n] \to A \to 0,$$

or equivalently, an S-closed immersion of $i\colon \mathrm{Spec}(A) \to \mathbb{A}^n_S$. For a rational number $a > 0$, let X^a be the tubular neighborhood of i of thickening a ([2] Section 3, [1] 2.1). It is an affinoid subdomain of the n-dimensional closed unit disc over K given by

$$X^a(\overline{K}) = \{(x_1, \cdots, x_n) \in \mathscr{O}^n_{\overline{K}} | \quad v(f(x_1, \cdots, x_n)) \geq a, \qquad \forall f \in I\}.$$

Let $\pi_0(X^a_{\overline{K}})$ be the set of geometric connected components of X^a. It is a finite $\mathscr{G}_K$-set that does not depend on the choice of the presentation ([2] Lemma 3.1). We put

$$\mathscr{F}^a(A) = \pi_0(X^a_{\overline{K}}). \tag{2.1.1}$$

For two rational numbers $b \geq a > 0$, X^b is an affinoid sub-domain of X^a. So there is a natural transition map $\mathscr{F}^b(A) \to \mathscr{F}^a(A)$.

2.2. We denote by $\mathrm{AFP}_{\mathscr{O}_K}$ the category of finite flat $\mathscr{O}_K$-algebras, and by $\mathscr{G}_K$-Ens the category of finite sets with a continuous action of $\mathscr{G}_K$. Let

$$\begin{array}{rcl} \mathscr{F}\colon \mathrm{AFP}^\circ_{\mathscr{O}_K} & \to & \mathscr{G}_K\text{-Ens} \\ A & \mapsto & \mathrm{Spec}(A)(\overline{K}) \end{array}$$

be the functor of geometric points. For $a \in \mathbb{Q}_{>0}$, (2.1.1) gives rise to a functor

$$\mathscr{F}^a : \mathrm{AFP}^\circ_{\mathscr{O}_K} \to \mathscr{G}_K\text{-Ens}.$$

For $b \geq a \geq 0$, we have morphisms of functors $\phi^a : \mathscr{F} \to \mathscr{F}^a$ and $\phi^a_b : \mathscr{F}^b \to \mathscr{F}^a$, satisfying the relations $\phi^a = \phi^b \circ \phi^a_b$ and $\phi^a_c = \phi^a_b \circ \phi^b_c$ for $c \geq b \geq a \geq 0$. To stress the dependence on K, we will denote $\mathscr{F}$ (*resp.* $\mathscr{F}^a$) by $\mathscr{F}_K$ (*resp.* $\mathscr{F}^a_K$). These functors behave well only for finite, flat and relative complete intersection algebras over $\mathscr{O}_K$ (EGA IV 19.3.6). We refer to [2] Propositions 6.2 and 6.4 for their main properties.

Lemma 2.3 ([1] Lemme 2.1.5). *Let K'/K be an extension (not necessarily finite) of complete discrete valuation fields with ramification index $e_{K'/K}$. Let A be a finite, flat and relative complete intersection algebra over $\mathscr{O}_K$. Then we have a canonical isomorphism $\mathscr{F}_{K'}^{ae_{K'/K}}(A') \simeq \mathscr{F}_K^a(A)$ for all $a \in \mathbb{Q}_{>0}$.*

2.4. Abbes and Saito show that the projective system of functors $(\mathscr{F}^a, \mathscr{F} \to \mathscr{F}^a)_{a\in\mathbb{Q}_{\geq 0}}$ gives rise to an exhaustive decreasing filtration $(\mathscr{G}_K^a, a \in \mathbb{Q}_{\geq 0})$ of the group $\mathscr{G}_K$, called the *ramification filtration* ([2] Proposition 3.3). Concretely, if L is a finite Galois extension of K contained in $\overline{K}$, $\mathrm{Gal}(L/K)$ is the Galois group of L/K, then the quotient filtration $(\mathrm{Gal}(L/K)^a)_{a\in\mathbb{Q}_{\geq 0}}$ induced by $(\mathscr{G}_K^a)_{a\in\mathbb{Q}_{\geq 0}}$ is determined by the following canonical isomorphisms

$$\mathscr{F}^a(L) \simeq \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/K)^a.$$

For a real number $a \geq 0$, we put $\mathscr{G}_K^{a+} = \overline{\cup_{b>a}\mathscr{G}_K^b}$, and if $a > 0$ $\mathscr{G}_K^{a-} = \cap_{b<a}\mathscr{G}_K^b$, where b runs over rational numbers. Then $\mathscr{G}_K^{0+}$ is the inertia subgroup of $\mathscr{G}_K$ ([2] Proposition 3.7).

2.5. We recall the definition of the canonical filtration of a finite and flat group schemes over S, following [1]. Let Gr_S be the category of finite, flat and commutative group schemes over S. Let G be an object of Gr_S and $a \in \mathbb{Q}_{\geq 0}$. Then there is a natural group structure on $\mathscr{F}^a(A)$ ([1] 2.3), and the canonical surjection $\mathscr{F}(A) \to \mathscr{F}^a(A)$ is a homomorphism of $\mathscr{G}_K$-groups. Hence, the kernel $G^a(\overline{K}) = \mathrm{Ker}(\mathscr{F}(A) \to \mathscr{F}^a(A))$ defines a subgroup scheme G_η^a of G_η over η, and the schematic closure G^a of G_η^a in G is a closed subgroup scheme of G, locally free of finite type over S. We put $G^0 = G$. The exhaustive decreasing filtration $(G^a, a \in \mathbb{Q}_{\geq 0})$ defined above is called *the canonical filtration of* G ([1] 2.3.1). Lemma 2.3 gives immediately the following.

Lemma 2.6. *Let K'/K be an extension (not necessarily finite) of complete discrete valuation fields with ramification index $e_{K'/K}$, $\mathscr{O}_{K'}$ be the ring of integers of K', and $\overline{K'}$ be an algebraic closure of K' containing $\overline{K}$. Let G be an object of Gr_S and $G' = G \times_S \mathrm{Spec}(\mathscr{O}_{K'})$. Then we have a canonical isomorphism $G^a(\overline{K}) \simeq G'^{ae_{K'/K}}(\overline{K'})$ for all $a \in \mathbb{Q}_{>0}$.*

2.7. For an object G of Gr_S and $a \in \mathbb{Q}_{\geq 0}$, we denote $G^{a+} = \cup_{b>a}G^b$ and if $a > 0$, $G^{a-} = \cap_{0<b<a}G^b$, where b runs over rational numbers. The construction of the canonical filtration is functorial : a morphism $u : G \to H$ of Gr_S induces canonical homomorphisms $u^a : G^a \to H^a$, $u^{a+} : G^{a+} \to H^{a+}$ and $u^{a-} : G^{a-} \to H^{a-}$.

Proposition 2.8 ([1] Lemmes 2.3.2 and 2.3.5). (i) *For any object G of Gr_S, G^{0+} is the neutral connected component of G.*

(ii) *Let $u : G \to H$ be a finite flat and surjective morphism in Gr_S and $a \in \mathbb{Q}_{>0}$. Then the homomorphism $u^a(\overline{K}) : G^a(\overline{K}) \to H^a(\overline{K})$ is surjective.*

2.9. Let A and B be two abelian schemes over S, $\phi : A \to B$ be an isogeny (*i.e.* a finite flat morphism of group schemes), and G be the kernel of ϕ. Let ν (*resp.* μ) be the generic point of the special fiber A_s (*resp.* B_s), and $\widehat{\mathscr{O}}_\nu$ (*resp.* $\widehat{\mathscr{O}}_\mu$) be the completion of the local ring of A at ν (*resp.* of B at μ). Let M and L be the fraction fields of $\widehat{\mathscr{O}}_\nu$ and $\widehat{\mathscr{O}}_\mu$ respectively. So we have the cartesian diagram

$$\begin{tikzcd}
\mathrm{Spec}\, M \arrow[r] \arrow[d] & \mathrm{Spec}\, \widehat{\mathscr{O}}_\nu \arrow[r] \arrow[d] & A \arrow[d] \\
\mathrm{Spec}\, L \arrow[r] & \mathrm{Spec}\, \widehat{\mathscr{O}}_\mu \arrow[r] & B
\end{tikzcd}$$

We fix a separable closure $\overline{L}$ of L containing $\overline{K}$, and an imbedding of M in $\overline{L}$. Since $\phi : A \to B$ is a G-torsor, M/L is a Galois extension, and we have a canonical isomorphism

$$G(\overline{K}) = \mathscr{F}_K(G) \xrightarrow{\sim} \mathscr{F}_L(\widehat{\mathscr{O}}_\nu) = \mathrm{Gal}(M/L). \tag{2.9.1}$$

Using the same arguments of ([1] 2.4.2), we prove the following

Proposition 2.10. *For all rational numbers $a \geq 0$, the isomorphism* (2.9.1) *induces an isomorphism $G^a(\overline{K}) \simeq \mathrm{Gal}(M/L)^a$.*

3 Review of the abelian scheme case following [1]

From this section on, we assume that the residue field k of $\mathscr{O}_K$ is perfect of characteristic $p > 0$.

3.1. Let X be a smooth and proper scheme over S, and $\overline{X} = X \times_S \overline{S}$. We consider the cartesian diagram

$$\begin{tikzcd}
X_{\bar{s}} \arrow[r, "\bar{i}"] \arrow[d] & \overline{X} \arrow[d] & X_{\bar{\eta}} \arrow[l, "\bar{j}"'] \arrow[d] \\
\bar{s} = \mathrm{Spec}\, \bar{k} \arrow[r] & \overline{S} & \bar{\eta} = \mathrm{Spec}\, \overline{K} \arrow[l]
\end{tikzcd}$$

and the sheaves of p-adic vanishing cycles on $X_{\bar{s}}$

$$\Psi^q_X = \bar{i}^* R^q \bar{j}_*(\mathbb{Z}/p\mathbb{Z}(q)), \tag{3.1.1}$$

where $q \geq 0$ is an integer and $\mathbb{Z}/p\mathbb{Z}(q)$ is the Tate twist of $\mathbb{Z}/p\mathbb{Z}$. It is clear that $\Psi^0_X \simeq \mathbb{Z}/p\mathbb{Z}$. By the base change theorem for proper morphisms, we have a spectral sequence

$$E_2^{p,q}(X) = \mathrm{H}^p(X_{\bar{s}}, \Psi^q_X)(-q) \Longrightarrow \mathrm{H}^{p+q}(X_{\bar{\eta}}, \mathbb{Z}/p\mathbb{Z}), \tag{3.1.2}$$

which induces an exact sequence

$$0 \to \mathrm{H}^1(X_{\bar{s}}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^1(X_{\bar{\eta}}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{u} \mathrm{H}^0(X_{\bar{s}}, \Psi^1_X)(-1) \to \mathrm{H}^2(X_{\bar{s}}, \mathbb{Z}/p\mathbb{Z}). \tag{3.1.3}$$

3.2. The Kummer's exact sequence $0 \to \mu_p \to \mathbb{G}_m \to \mathbb{G}_m \to 0$ on $X_{\bar{\eta}}$ induces the symbol map

$$h_{\overline{X}} : \bar{i}^* \bar{j}_* \mathscr{O}^\times_{X_{\bar{\eta}}} \to \Psi^1_X. \tag{3.2.4}$$

We put $\mathrm{U}^0\Psi^1_X = \Psi^1_X$, and for $a \in \mathbb{Q}_{>0}$,

$$\mathrm{U}^a\Psi^1_X = h_{\overline{X}}(1 + \pi^a \bar{i}^* \mathscr{O}_{\overline{X}}), \tag{3.2.5}$$

where by abuse of notation π^a is an element in $\mathscr{O}_{\overline{K}}$ with $v(\pi^a) = a$. We have $\mathrm{U}^a\Psi^1_X = 0$ if $a \geq \frac{ep}{p-1}$ ([1] Lemme 3.1.1).

Passing to the cohomology, we get a filtration on $\mathrm{H}^1(X_{\bar{\eta}}, \mathbb{Z}/p\mathbb{Z})$ defined by :

$$\begin{aligned}
&\mathrm{U}^0\mathrm{H}^1(X_{\bar{\eta}}, \mathbb{Z}/p\mathbb{Z}) = \mathrm{H}^1(X_{\bar{\eta}}, \mathbb{Z}/p\mathbb{Z}), \\
&\mathrm{U}^a\mathrm{H}^1(X_{\bar{\eta}}, \mathbb{Z}/p\mathbb{Z}) = u^{-1}(\mathrm{H}^0(X_{\bar{s}}, \mathrm{U}^a\Psi^1_X)(-1)), \quad \text{for } a \in \mathbb{Q}_{>0},
\end{aligned} \tag{3.2.6}$$

called the *Bloch-Kato filtration.*

Theorem 3.3 ([1] Théorème 3.1.2)**.** *Let A be an abelian scheme over S, ${}_pA$ its kernel of multiplication by p, and $e' = \frac{ep}{p-1}$. Then under the canonical perfect pairing*

$$(3.3.1) \qquad {}_pA(\overline{K}) \times \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z},$$

we have for all $a \in \mathbb{Q}_{\geq 0}$,

$${}_pA^{a+}(\overline{K})^{\perp} = \begin{cases} \mathrm{U}^{e'-a}\mathrm{H}^1(A_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) & \text{if } 0 \leq a \leq e'; \\ \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) & \text{if } a > e'. \end{cases}$$

3.4. Let X be a scheme over S, $\overline{X} = X \times_S \overline{S}$. For all $a \in \mathbb{Q}_{>0}$, we put $\overline{S}_a = \mathrm{Spec}(\mathscr{O}_{\overline{K}}/\mathfrak{m}_a)$ and $\overline{X}_a = X \times_S \overline{S}_a$ (1). We denote by $\mathbf{D}((\overline{X}_1)_{\text{ét}})$ the derived category of abelian étale sheaves over $\overline{X}_1$. A morphism of schemes is called *syntomic*, if it is flat and of complete intersection.

Let X be a syntomic and quasi-projective S-scheme, r and n be integers with $r \geq 0$ and $n \geq 1$. In [13], Kato constructed a canonical object $\mathscr{J}^{[r]}_{n,\overline{X}}$ in $\mathbf{D}((\overline{X}_1)_{\text{ét}})$, and if $0 \leq r \leq p-1$ a morphism $\varphi_r : \mathscr{J}^{[r]}_{n,\overline{X}} \to \mathscr{J}^{[0]}_{n,\overline{X}}$, which can be roughly seen as "$1/p^r$ times of the Frobenius map". We refer to [13] and ([1] 4.1.6) for details of these constructions. Let $\mathscr{S}_n(r)_{\overline{X}}$ be the fiber cone of the morphism $\varphi_r - 1$ for $0 \leq r \leq p-1$; so we have a distinguished triangle in $\mathbf{D}((\overline{X}_1)_{\text{ét}})$

$$(3.4.2) \qquad \mathscr{S}_n(r)_{\overline{X}} \to \mathscr{J}^{[r]}_{n,\overline{X}} \xrightarrow{\varphi_r - 1} \mathscr{J}^{[0]}_{n,\overline{X}} \xrightarrow{+1} .$$

The complexes $\mathscr{S}_n(r)_{\overline{X}}$ $(0 \leq r \leq p-1)$ are called the *syntomic complexes* of $\overline{X}$. For our purpose, we recall here some of their properties for $r = 1$.

3.5. According to ([13] section I.3), for any integer $n \geq 1$, there exists a surjective symbol map

$$\mathscr{O}^{\times}_{\overline{X}_{n+1}} \to \mathscr{H}^1(\mathscr{S}_n(1)_{\overline{X}}).$$

For a geometric point $\overline{x}$ of $X_{\overline{s}}$, we put

$$\mathfrak{S}^1_{\overline{x}} = \left(\mathscr{O}_{\overline{X},\overline{x}}[\frac{1}{p}]\right)^{\times} = (\overline{i}^* \overline{j}_* \mathscr{O}^{\times}_{X_{\overline{\eta}}})_{\overline{x}}.$$

By ([13] I.4.2), the above symbol map at $\overline{x}$ factorizes through the canonical surjection $\mathscr{O}^{\times}_{\overline{X},\overline{x}} \to \mathfrak{S}^1_{\overline{x}}/p^n\mathfrak{S}^1_{\overline{x}}$.

Theorem 3.6 ([13] I.4.3)**.** *Assume that $p \geq 3$. Let X be a smooth and quasi-projective scheme over S. Then there is a canonical isomorphism $\mathscr{H}^1(\mathscr{S}_1(1)_{\overline{X}}) \xrightarrow{\sim} \Psi^1_X$, which is compatible with the symbol maps $\mathfrak{S}^1_{\overline{x}} \to \mathscr{H}^1(\mathscr{S}_1(1)_{\overline{X}})_{\overline{x}}$ and $h_{\overline{X}} : \mathfrak{S}^1_{\overline{x}} \to \Psi^1_{X,\overline{x}}$ (3.2.4).*

3.7. Let X be a smooth and quasi-projective scheme over S. Let $\phi_{\overline{X}_1}$ and $\phi_{\overline{S}_1}$ be the absolute Frobenius morphisms of $\overline{X}_1$ and $\overline{S}_1$, and let $\overline{X}^{(p)}_1$ be the scheme defined by the cartesian diagram

$$\begin{tikzcd} \overline{X}^{(p)}_1 \arrow[r, "w"] \arrow[d] & \overline{X}_1 \arrow[d] \\ \overline{S}_1 \arrow[r, "\phi_{\overline{S}_1}"] & \overline{S}_1. \end{tikzcd}$$

For all integers $q \geq 0$, we denote by F the composed morphism

$$\Omega^q_{\overline{X}_1/\overline{S}_1} \xrightarrow{w^*} \Omega^q_{\overline{X}_1^{(p)}/\overline{S}_1} \to \Omega^q_{\overline{X}_1/\overline{S}_1}/d(\Omega^{q-1}_{\overline{X}_1/\overline{S}_1}),$$

where the second morphism is induced by the Cartier isomorphism

$$C^{-1}_{\overline{X}_1/\overline{S}_1} : \Omega^q_{\overline{X}_1^{(p)}/\overline{S}_1} \xrightarrow{\sim} \mathscr{H}^q(\Omega^\bullet_{\overline{X}_1/\overline{S}_1}).$$

Let c be the class in $\mathscr{O}_{\overline{S}_1}$ of a p-th root of $(-p)$. We set

$$\mathscr{P} = \mathrm{Coker}\Big(\mathscr{O}_{\overline{X}_1} \xrightarrow{\mathrm{F}-c} \mathscr{O}_{\overline{X}_1}\Big), \tag{3.7.1}$$

$$\mathscr{Q} = \mathrm{Ker}\Big(\Omega^1_{\overline{X}_1/\overline{S}_1} \xrightarrow{\mathrm{F}-1} \Omega^1_{\overline{X}_1/\overline{S}_1}/d(\mathscr{O}_{\overline{X}_1})\Big).$$

Proposition 3.8 ([1] 4.1.8)**.** *The notations are those as above, and we assume moreover that $p \geq 3$. Let $\overline{x}$ be a geometric point in $X_{\overline{s}}$.*

(i) *There exist canonical isomorphisms*

$$\mathscr{P} \xrightarrow{\sim} \mathrm{Coker}\Big(\mathscr{H}^0(\mathscr{J}^{[1]}_{1,\overline{X}}) \xrightarrow{\varphi_1-1} \mathscr{H}^0(\mathscr{J}^{[0]}_{1,\overline{X}})\Big), \quad \mathscr{Q} \xrightarrow{\sim} \mathrm{Ker}\Big(\mathscr{H}^1(\mathscr{J}^{[1]}_{1,\overline{X}}) \xrightarrow{\varphi_1-1} \mathscr{H}^1(\mathscr{J}^{[0]}_{1,\overline{X}})\Big),$$

so the distinguished triangle (3.4.2) *gives rise to an exact sequence*

$$0 \to \mathscr{P} \xrightarrow{\alpha} \mathscr{H}^1(\mathscr{S}_1(1)_{\overline{X}}) \xrightarrow{\beta} \mathscr{Q} \to 0. \tag{3.8.1}$$

(ii) *Let $e(T) = \sum_{i=0}^{p-1} T^i/i! \in \mathbb{Z}_p[T]$. Then the morphism $\alpha_{\overline{x}}$ in* (3.8.1) *is induced by the map $\mathscr{O}_{\overline{X}_1,\overline{x}} \to \mathfrak{S}^1_{\overline{x}}/p\mathfrak{S}^1_{\overline{x}}$ given by*

$$a \mapsto e(-\tilde{a}(\zeta-1)^{p-1}),$$

where $\tilde{a}$ is a lift of $a \in \mathscr{O}_{\overline{X}_1,\overline{x}}$ and $\zeta \in \overline{K}$ is a primitive p-th root of unity.

(iii) *The composed map*

$$\mathfrak{S}^1_{\overline{x}}/p\mathfrak{S}^1_{\overline{x}} \xrightarrow{\text{symbol}} \mathscr{H}^1(\mathscr{S}_1(1)_{\overline{X}})_{\overline{x}} \xrightarrow{\beta} \mathscr{Q}_{\overline{x}}$$

is the unique morphism sending $a \in \mathscr{O}^\times_{X,\overline{x}}$ to $a^{-1}da \in \mathscr{Q}_{\overline{x}}$.

Remark 3.9. *Statement (ii) of Proposition 3.8 implies that, via the canonical isomorphism $\mathscr{H}^1(\mathscr{S}_1(1)_{\overline{X}}) \simeq \Psi^1_X$ (3.6), $\mathscr{P}$ can be identified with the submodule $\mathrm{U}^e\Psi^1_X$ of Ψ^1_X defined in (3.2.5).*

Proposition 3.10 ([1] 4.1.9)**.** *Assume that $p \geq 3$. Let X be a smooth projective scheme over S, $t = (p-1)/p$.*

(i) *The morphism $\mathrm{F} - c : \mathscr{O}_{\overline{X}_1} \to \mathscr{O}_{\overline{X}_1}$ factorizes through the quotient morphism $\mathscr{O}_{\overline{X}_1} \to \mathscr{O}_{\overline{X}_t}$, and we have an exact sequence*

$$0 \to \mathbb{F}_p \to \mathscr{O}_{\overline{X}_t} \xrightarrow{\mathrm{F}-c} \mathscr{O}_{\overline{X}_1} \to \mathscr{P} \to 0. \tag{3.10.1}$$

(ii) *Let $\delta_E : \mathrm{H}^0(\overline{X}_1, \mathscr{P}) \to \mathrm{H}^2(\overline{X}_1, \mathbb{F}_p)$ be the cup-product with the class of* (3.10.1) *in* $\mathrm{Ext}^2(\mathscr{P}, \mathbb{F}_p)$*, and*

$$d_2^{0,1} : \mathrm{H}^0(\overline{X}_{\overline{s}}, \Psi^1_X)(-1) \to \mathrm{H}^2(\overline{X}_{\overline{s}}, \mathbb{F}_p)$$

be the connecting morphism in (3.1.3). *Then the composed morphism*

$$\mathrm{H}^0(\overline{X}_1, \mathscr{P}) \to \mathrm{H}^0(\overline{X}_{\overline{s}}, \mathscr{H}^1(\mathscr{S}_1(1)_{\overline{X}})) \xrightarrow{\sim} \mathrm{H}^0(\overline{X}_{\overline{s}}, \Psi^1_X) \xrightarrow{d_2^{0,1}(1)} \mathrm{H}^2(\overline{X}_{\overline{s}}, \mathbb{F}_p)(1)$$

coincides with $\zeta\delta_E$, where the middle isomorphism is given by Theorem 3.6, and ζ is a chosen p-th root of unity.

(iii) *Assume moreover that $\mathrm{H}^0(\overline{X}_r, \mathscr{O}_{\overline{X}_r}) = \mathscr{O}_{S_r}$ for $r = 1$ and t. Then we have an exact sequence*
(3.10.2)

$$0 \to \mathrm{H}^1(X_{\overline{s}}, \mathbb{F}_p) \to \mathrm{Ker}\Big(\mathrm{H}^1(\overline{X}_1, \mathscr{O}_{\overline{X}_t}) \xrightarrow{\mathrm{F}-c} \mathrm{H}^1(\overline{X}_1, \mathscr{O}_{\overline{X}_1})\Big) \to \mathrm{H}^0(\overline{X}_1, \mathscr{P}) \xrightarrow{\delta_E} \mathrm{H}^2(X_{\overline{s}}, \mathbb{F}_p)$$

3.11.

Let M be a free $\mathscr{O}_{\overline{S}_1}$-module of rank r and $\varphi : M \to M$ be a semi-linear endomorphism with respect to the absolute Frobenius of $\mathscr{O}_{\overline{S}_1}$. Following [1], we call M a *φ-$\mathscr{O}_{\overline{S}_1}$-module* of rank r. Then $\varphi(M)$ is an $\mathscr{O}_{\overline{S}_1}$-submodule of M, and there exist rational numbers $0 \leq a_1 \leq a_2 \leq \cdots \leq a_r \leq 1$, such that

$$M/\varphi(M) \simeq \oplus_{i=1}^r \mathscr{O}_{\overline{K}}/\mathfrak{m}_{a_i}.$$

We define the *Hodge height* of M to be $\sum_{i=1}^r a_i$. For any rational number $0 \leq t \leq 1$, we put $M_t = M \otimes_{\mathscr{O}_{\overline{S}_1}} \mathscr{O}_{\overline{S}_t}$.

Proposition 3.12 ([3] 9.1 and 9.7). *Assume that $p \geq 3$. Let λ be an element in $\mathscr{O}_{\overline{K}}$, and $r \geq 1$ an integer. We assume $v = v_p(\lambda) < \frac{1}{2}$ and let M be a φ-$\mathscr{O}_{\overline{S}_1}$-module of rank r such that its Hodge height is strictly smaller than v.*

(i) *The morphism $\varphi - \lambda : M \to M$ factorizes through the canonical map $M \to M_{1-v}$ and the kernel of $\varphi - \lambda : M_{1-v} \to M$ is an $\mathbb{F}_p$-vector space of dimension r.*

(ii) *Let N_0 be the kernel of the morphism $M_{1-v} \to M$ induced by $\varphi - \lambda$, and N be the $\mathscr{O}_{\overline{K}}$-submodule of M_{1-v} generated by N_0. Then we have $\dim_{\overline{k}}(N/\mathfrak{m}_{\overline{K}}N) = \dim_{\mathbb{F}_p} N_0 = r$.*

3.13. We can now summarize the strategy of [1] as follows. Let A be a projective abelian scheme of dimension g over S. By Proposition 3.10(iii), we have

$$\begin{aligned} \dim_{\mathbb{F}_p} \mathrm{H}^1(\overline{A}_1, \mathbb{F}_p) + \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{H}^0(\overline{A}_1, \mathscr{P}) \xrightarrow{\delta_E} \mathrm{H}^2(\overline{A}_1, \mathbb{F}_p)\Big) \\ = \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{H}^1(\overline{A}_1, \mathscr{O}_{\overline{A}_t}) \xrightarrow{\mathrm{F}-c} \mathrm{H}^1(\overline{A}_1, \mathscr{O}_{\overline{A}_1})\Big). \end{aligned} \tag{3.13.1}$$

By Remark 3.9 and Proposition 3.10(ii), the left hand side equals $\dim_{\mathbb{F}_p} \mathrm{U}^e\mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})$ (3.2.6). Taking account of Theorem 3.3, we get

$$2g - \dim_{\mathbb{F}_p}\big({}_pA^{j+}(\overline{K})\big) = \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{H}^1(\overline{A}_1, \mathscr{O}_{\overline{X}_t}) \xrightarrow{\mathrm{F}-c} \mathrm{H}^1(\overline{A}_1, \mathscr{O}_{\overline{X}_1})\Big), \tag{3.13.2}$$

where $j = \frac{e}{p-1}$. Applying 3.12(i) to $M = \mathrm{H}^1(\overline{A}_1, \mathscr{O}_{\overline{X}_1})$ and $\lambda = c$, we obtain immediately the first statement of Theorem 1.4 for projective abelian schemes. In fact, Abbes and Mokrane proved a less optimal bound on the Hodge height ([1] 5.1.1).

4 Cohomological preliminaries

4.1. Let $f : X \to T$ be a proper, flat and finitely presented morphism of schemes. We work with the fppf-topology on T, and denote by $\mathrm{Pic}_{X/T}$ the relative Picard functor $R^1_{\mathrm{fppf}}f_*(\mathbb{G}_m)$.

If T is the spectrum of a field, $\mathrm{Pic}_{X/T}$ is representable by a group scheme locally of finite type over k. We denote by $\mathrm{Pic}^0_{X/T}$ the neutral component, and put $\mathrm{Pic}^\tau_{X/T} = \bigcup_{n\geq 1} n^{-1}\,\mathrm{Pic}^0_{X/T}$, where $n : \mathrm{Pic}_{X/T} \to \mathrm{Pic}_{X/T}$ is the multiplication by n. Then $\mathrm{Pic}^0_{X/T}$ and $\mathrm{Pic}^\tau_{X/T}$ are open sub-group schemes of $\mathrm{Pic}_{X/T}$.

For a general base, $\mathrm{Pic}_{X/T}$ is representable by an algebraic space over T ([4] thm. 7.3). We denote by $\mathrm{Pic}^0_{X/T}$ (*resp.* $\mathrm{Pic}^\tau_{X/T}$) the subfunctor of $\mathrm{Pic}_{X/T}$ which consists of all elements whose restriction to all fibres X_t, $t \in T$, belong to $\mathrm{Pic}^0_{X_t/t}$ (*resp.* $\mathrm{Pic}^\tau_{X_t/t}$). By (SGA 6 XIII, thm 4.7), the canonical inclusion $\mathrm{Pic}^\tau_{X/T} \to \mathrm{Pic}_{X/T}$ is relatively representable by an open immersion.

4.2. Let $f : A \to T$ be an abelian scheme. If T is the spectrum of a field, the Néron-Séveri group $\mathrm{Pic}_{A/T} / \mathrm{Pic}^0_{A/T}$ is torsion free, *i.e.* we have $\mathrm{Pic}^0_{A/T} = \mathrm{Pic}^\tau_{A/T}$. This coincidence remains true for a general base T by the definitions of $\mathrm{Pic}^0_{A/T}$ and $\mathrm{Pic}^\tau_{A/T}$. Moreover, $\mathrm{Pic}^\tau_{A/T}$ is formally smooth (cf. [18] Prop. 6.7), and $\mathrm{Pic}^\tau_{A/T}$ is actually open and closed in $\mathrm{Pic}_{A/T}$, and is representable by a proper and smooth algebraic space over T, *i.e.* an abelian algebraic space over T. By a theorem of Raynaud ([10] Ch. 1, thm. 1.9), every abelian algebraic space over T is automatically an abelian scheme over T. So $\mathrm{Pic}^0_{A/T} = \mathrm{Pic}^\tau_{A/T}$ is an abelian scheme, called the *dual abelian scheme of* A, and denoted by $A^\vee$.

Let H be a commutative group scheme locally free of finite type over T. Recall the following isomorphism due to Raynaud ([19] 6.2.1) :

$$R^1_{\mathrm{fppf}}f_*(H_A) \xrightarrow{\sim} \mathscr{H}om(H^\vee, \mathrm{Pic}_{A/T}), \tag{4.2.3}$$

where $H_A = H \times_T A$, $H^\vee$ is the Cartier dual of H, and $\mathscr{H}om$ is taken for the fppf-topology on T.

Proposition 4.3. *Let A be an abelian scheme over a scheme T, and H a commutative group scheme locally free of finite type over T. Then we have canonical isomorphisms*

$$\mathscr{E}xt^1(A, H) \xrightarrow{\sim} \mathscr{H}om(H^\vee, A^\vee), \tag{4.3.1}$$

$$\mathrm{Ext}^1(A, H) \xrightarrow{\sim} \mathrm{H}^0_{\mathrm{fppf}}(T, \mathscr{E}xt^1(A, H)) \xrightarrow{\sim} \mathrm{Hom}(H^\vee, A^\vee). \tag{4.3.2}$$

Proof. For any fppf-sheaf E on T, we have

$$\mathscr{H}om(H^\vee, \mathscr{H}om(E, \mathbb{G}_m)) \simeq \mathscr{H}om(H^\vee \otimes_{\mathbb{Z}} E, \mathbb{G}_m) \simeq \mathscr{H}om(E, H).$$

Deriving this isomorphism of functors in E and putting $E = A$, we obtain a spectral sequence

$$E_2^{p,q} = \mathscr{E}xt^p(H^\vee, \mathscr{E}xt^q(A, \mathbb{G}_m)) \Longrightarrow \mathscr{E}xt^{p+q}(A, H).$$

Since $\mathscr{H}om(A, \mathbb{G}_m) = 0$, the exact sequence

$$0 \to E_2^{1,0} \to \mathscr{E}xt^1(A, H) \to E_2^{0,1} \to E_2^{2,0}$$

induces an isomorphism

$$\mathscr{E}xt^1(A, H) \simeq \mathscr{H}om(H^\vee, \mathscr{E}xt^1(A, \mathbb{G}_m)).$$

Then (4.3.1) follows from the canonical identification $\mathscr{E}xt^1(A, \mathbb{G}_m) \simeq A^\vee$ ([8] 2.4). For (4.3.2), the spectral sequence

$$E_2^{p,q} = \mathrm{H}^p_{\mathrm{fppf}}(T, \mathscr{E}xt^q(A, H)) \Longrightarrow \mathrm{Ext}^{p+q}(A, H)$$

induces a long exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{fppf}}(T, \mathscr{H}om(A, H)) \to \mathrm{Ext}^1(A, H) \xrightarrow{(1)} \mathrm{H}^0_{\mathrm{fppf}}(T, \mathscr{E}xt^1(A, H)) \to \mathrm{H}^2_{\mathrm{fppf}}(T, \mathscr{H}om(A, H)).$$

Since $\mathscr{H}om(A, H) = 0$, the arrow (1) is an isomorphism, and (4.3.2) follows by applying the functor $\mathrm{H}^0_{\mathrm{fppf}}(T, \_)$ to (4.3.1). □

4.4. The assumptions are those of (4.3). We define a canonical morphism

$$\mathrm{Ext}^1(A, H) \to \mathrm{H}^1_{\mathrm{fppf}}(A, H) \tag{4.4.3}$$

as follows. Let a be an element in $\mathrm{Ext}^1(A, H)$ represented by the extension $0 \to H \to E \to A \to 0$. Then the fppf-sheaf E is representable by a scheme over T, and is naturally a H-torsor over A. The image of a by the homomorphism (4.4.3) is defined to be the class of the torsor E. Since this construction is functorial in T, by passing to sheaves, we obtain a canonical morphism

$$\mathscr{E}xt^1(A, H) \to R^1_{\mathrm{fppf}} f_*(H_A). \tag{4.4.4}$$

Via the isomorphisms (4.2.3) and (4.3.1), we check that (4.4.4) is induced by the canonical map $A^\vee = \mathrm{Pic}^0_{A/T} \to \mathrm{Pic}_{A/T}$.

Since H is faithfully flat and finite over T, the inverse image of the fppf-sheaf H by f is representable by H_A, *i.e.* we have $f^*(H) = H_A$. Therefore, we deduce an adjunction morphism

$$H \to R^0_{\mathrm{fppf}} f_*(H_A). \tag{4.4.5}$$

Proposition 4.5. *Let $f : A \to T$ be an abelian scheme, and H be a commutative group scheme locally free of finite type over T. Then the canonical maps* (4.4.4) *and* (4.4.5) *are isomorphisms.*

Proof. First, we prove that (4.4.4) is an isomorphism. By (4.2.3) and (4.3.1), we have to verify that the canonical morphism

$$\mathscr{H}om(H^\vee, A^\vee) \to \mathscr{H}om(H^\vee, \mathrm{Pic}_{A/T})$$

is an isomorphism. Let $g : H^\vee \to \mathrm{Pic}_{A/T}$ be a homomorphism over T. For every $t \in T$, the induced morphism $g_t : H^\vee_t \to \mathrm{Pic}_{A_t/t}$ falls actually in $\mathrm{Pic}^\tau_{A_t/t}$, because $H^\vee$ is a finite group scheme. Hence, by the definition of $\mathrm{Pic}^\tau_{A/T}$, the homomorphism g factorizes through the canonical inclusion $A^\vee = \mathrm{Pic}^\tau_{A/T} \to \mathrm{Pic}_{A/T}$; so the canonical morphism $\mathrm{Hom}(H^\vee, A^\vee) \to \mathrm{Hom}(H^\vee, \mathrm{Pic}_{A/T})$ is an isomorphsim.

Secondly, we prove that (4.4.5) is an isomorphism. For T-schemes U and G, we denote $G_U = G \times_T U$. We must verify that for any T-scheme U, the adjunction morphism

$$\varphi(U) : H(U) \to R^0_{\mathrm{fppf}} f_*(H_A)(U) = H(A_U) \tag{4.5.1}$$

is an isomorphism. We note that $H(U) = H_U(U)$ and $H(A_U) = H_U(A_U)$; therefore, up to taking base changes, it suffices to prove that $\varphi(T)$ (4.5.1) is an isomorphism. We remark that f is surjective, hence $\varphi(T)$ is injective. To prove the surjectivity of $\varphi(T)$, we take an element $h \in H(A)$, *i.e.* a morphism of T-schemes $h : A \to H$; by rigidity lemma for abelian schemes (cf. [18] Prop. 6.1), there exists a section $s : T \to H$ of the structure morphism $H \to T$ such that $s \circ f = h$. Hence we have $\varphi(T)(s) = h$, and $\varphi(T)$ is an isomorphism. □

Corollary 4.6. *Let T be the spectrum of a stirctly henselian local ring, $f : A \to T$ an abelian scheme, and H a finite étale group scheme over T. Then we have canonical isomorphisms*

$$\mathrm{H}^1_{\text{ét}}(A, H) \simeq \mathrm{H}^1_{\text{fppf}}(A, H) \simeq \mathrm{Ext}^1(A, H).$$

Proof. The first isomorphism follows from the étaleness of H ([11], 11.7). For the second one, the "local-global" spectral sequence induces a long exact sequence

$$0 \to \mathrm{H}^1_{\text{fppf}}(T, R^0_{\text{fppf}}f_*(H_A)) \to \mathrm{H}^1_{\text{fppf}}(A, H) \to \mathrm{H}^0_{\text{fppf}}(T, R^1_{\text{fppf}}f_*(H_A)) \to \mathrm{H}^2_{\text{fppf}}(T, R^0_{\text{fppf}}f_*(H_A)).$$

By Prop. 4.5, we have $R^0_{\text{fppf}}f_*(H_A) = H$. Since T is strictly henselian and H étale, we have $\mathrm{H}^q_{\text{fppf}}(T, H) = \mathrm{H}^q_{\text{ét}}(T, H) = 0$ for all integers $q \geq 1$. Therefore, we obtain $\mathrm{H}^1_{\text{fppf}}(A, H) \xrightarrow{\sim} \mathrm{H}^0_{\text{fppf}}(T, R^1_{\text{fppf}}f_*(H_A))$, and the corollary follows from 4.5 and (4.3.2). □

4.7. Let T be a scheme, and G be a commutative group scheme locally free of finite type over T. We denote by $\mathbb{G}_a$ the additive group scheme, and by $\mathrm{Lie}(G^\vee)$ the Lie algebra of $G^\vee$. By Grothendieck's duality formula ([17] II §14), we have a canonical isomorphism

$$\mathrm{Lie}(G^\vee) \simeq \mathscr{H}om_T(G, \mathbb{G}_a), \tag{4.7.1}$$

where we have regarded G and $\mathbb{G}_a$ as abelian fppf-sheaves on T. If T is of characteristic p and G is a truncated Barsotti-Tate group over T, then $\mathrm{Lie}(G^\vee)$ is a locally free of finite type $\mathscr{O}_T$-module ([12] 2.2.1(c)).

Similarly, for an abelian scheme $f : A \to T$, we have a canonical isomorphism ([5] 2.5.8)

$$\mathrm{Lie}(A^\vee) \simeq \mathscr{E}xt^1_T(A, \mathbb{G}_a) \simeq R^1f_*(\mathbb{G}_a). \tag{4.7.2}$$

In the sequel, we will frequently use the identifications (4.7.1) and (4.7.2) without any indications.

The following Lemma is indicated by W. Messing.

Lemma 4.8. *Let L be an algebraically closed field of characteristic $p > 0$, R be an L-algebra integral over L, and M be a module of finite presentation over R, equipped with an endomorphism φ semi-linear with respect to the Frobenius of R. Then the map $\varphi - 1 : M \to M$ is surjective.*

Proof. First, we reduce the lemma to the case $R = L$. Consider R as a filtrant inductive limit of finite L-algebras $(R_i)_{i\in I}$. Since M is of finite presentation, there exists an $i \in I$, and an R_i-module M_i of finite presentation endowed with a Frobenius semi-linear endomorphism φ_i, such that $M = M_i \otimes_{R_i} R$ and $\varphi = \varphi_i \otimes \sigma$, where σ is the Frobenius on R. For $j \geq i$, we put $M_j = M_i \otimes_{R_i} R_j$ and $\varphi_j = \varphi_i \otimes_{R_i} \sigma_j$, where σ_j is the Frobenius of R_j. In order to prove $\varphi - 1$ is surjective on M, it is sufficient to prove the surjectivity of $\varphi_j - 1$ on each M_j for $j \geq i$. Therefore, we may assume that R is a finite dimensional L-algebra, and M is thus a finite dimensional vector space over L.

We put $M_1 = \bigcup_{n\geq 1} \mathrm{Ker}(\varphi^n)$ and $M_2 = \bigcap_{n\geq 1} \mathrm{Im}(\varphi^n)$. Then we have a decomposition $M = M_1 \oplus M_2$ as φ-modules, such that φ is nilpotent on M_1 and bijective on M_2 (Bourbaki, Algèbre VIII §2 n° 2 Lemme 2). Therefore, it is sufficient to prove the surjectivity of $\varphi - 1$ in the following two cases :

(i) φ is nilpotent. In this case, the endomorphism $1 - \varphi$ admits an inverse $1 + \sum_{n\geq 1} \varphi^n$. Hence it is surjective.

(ii) φ is invertible. We choose a basis of M over L, and let $U = (a_{i,j})_{1\leq i,j\leq n}$ be the matrix of φ in this basis. The problem reduces to prove that the equation system $\sum_{j=1}^n a_{i,j}x_j^p - x_i = b_i$

$(1 \leq i \leq n)$ in $X = (x_1, \cdots, x_n)$ has solutions for all $b = (b_1, \cdots, b_n) \in L^n$. Since U is invertible, let $V = (c_{i,j})_{1 \leq i,j \leq n}$ be its inverse. Then the equation system $\sum_{j=1}^{n} a_{i,j} x_j^p - x_i = b_i$ is equivalent to $x_i^p - \sum_{j=1}^{n} c_{i,j} x_j = b_i'$ for $1 \leq i \leq n$ with $b' = \sum_j c_{i,j} b_j$. But these n equations define a finite étale cover of $\operatorname{Spec} L$ of degree p^n. Hence they admit solutions in L, since L is separably closed. This completes the proof. □

Corollary 4.9. *Let H be a Barsotti-Tate group or an abelian scheme over $\overline{S}_1$ (1). Then* $\operatorname{Ext}^2(H, \mathbb{F}_p) = 0$ *for the* fppf *topology on $\overline{S}_1$.*

Proof. Let K_0 be the fraction field of the ring of Witt vectors with coefficients in k ; so K is a finite extension of degree e of K_0. Let $\mathscr{O}_{K_0}^{ur}$ be the ring of integers of the maximal unramified extension of K_0 in $\overline{K}$. Then $\mathscr{O}_{\overline{S}_1} = \mathscr{O}_{\overline{K}}/p\mathscr{O}_{\overline{K}}$ is integral over the algebraically closed field $\overline{k} = \mathscr{O}_{K_0}^{ur}/p\mathscr{O}_{K_0}^{ur}$. As $\operatorname{Ext}^2(H, \mathbb{G}_a) = 0$ ([5] Proposition 3.3.2), the Artin-Schreier's exact sequence $0 \to \mathbb{F}_p \to \mathbb{G}_a \xrightarrow{\mathrm{F}-1} \mathbb{G}_a \to 0$ induces an exact sequence

$$\operatorname{Ext}^1(H, \mathbb{G}_a) \xrightarrow{\varphi-1} \operatorname{Ext}^1(H, \mathbb{G}_a) \to \operatorname{Ext}^2(H, \mathbb{F}_p) \to 0.$$

Since $\operatorname{Ext}^1(H, \mathbb{G}_a)$ is a free $\mathscr{O}_{\overline{S}_1}$-module ([5] 3.3.2.1), the corollary follows immediately from Lemma 4.8. □

5 The Bloch-Kato filtration for finite flat group schemes killed by p

5.1. Recall the following theorem of Raynaud ([5] 3.1.1) : *Let T be a scheme, G be a commutative group scheme locally free of finite type over T. Then locally for the Zariski topology, there exists a projective abelian scheme A over T, such that G can be identified to a closed subgroup of A.*

In particular, if G is a commutative finite and flat group scheme over $S = \operatorname{Spec}(\mathscr{O}_K)$, we have an exact sequence of abelian fppf-sheaves over S

$$0 \to G \to A \to B \to 0, \tag{5.1.1}$$

where A and B are projective abelian schemes over S. In the sequel, such an exact sequence is called a *resolution of G by abelian schemes.*

5.2. Let $f : X \to Y$ be a morphism of proper and smooth S-schemes. For any integer $q \geq 0$, we have a base change morphism $f_{\overline{s}}^*(\Psi_Y^q) \to \Psi_X^q$ of p-adic vanishing cycles (3.1.1) (SGA 7 XIII 1.3.7.1). For $q = 1$, this morphism respects the Bloch-Kato filtrations (3.2.5), that is, it sends $f_{\overline{s}}^*(\mathrm{U}^a\Psi_Y^1)$ to $\mathrm{U}^a\Psi_X^1$ for all $a \in \mathbb{Q}_{\geq 0}$.

Passing to cohomology, we get a functorial map $\mathrm{H}^p(Y_{\overline{s}}, \Psi_Y^q)(-q) \to \mathrm{H}^p(X_{\overline{s}}, \Psi_X^q)(-q)$ for each pair of integers $p, q \geq 0$. These morphisms piece together to give a morphism of spectral sequences (3.1.2) $E_2^{(p,q)}(Y) \to E_2^{(p,q)}(X)$, which converges to the map $\mathrm{H}^{p+q}(Y_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^{p+q}(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})$ induced by $f_{\overline{\eta}}^*$. Therefore, we have the following commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{H}^1(Y_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_1"] & \mathrm{H}^1(Y_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_2"] & \mathrm{H}^0(Y_{\overline{s}}, \Psi_Y^1)(-1) \arrow[r, "d_2^{1,0}"] \arrow[d, "\alpha_3"] & \mathrm{H}^2(Y_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\alpha_4"] \\ 0 \arrow[r] & \mathrm{H}^1(X_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^0(X_{\overline{s}}, \Psi_X^1)(-1) \arrow[r, "d_2^{1,0}"] & \mathrm{H}^2(X_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}). \end{tikzcd} \tag{5.2.2}$$

It is clear that the Bloch-Kato filtration on $\mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})$ (3.2.6) is functorial in X. More precisely, the following diagram is commutative :

(5.2.3)
$$\begin{tikzcd}
\mathrm{U}^a\mathrm{H}^1(Y_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r, hook] \arrow[d] & \mathrm{H}^1(Y_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\alpha_2"] \\
\mathrm{U}^a\mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r, hook] & \mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})
\end{tikzcd}$$

5.3. Let G be a commutative finite and flat group scheme over S killed by p, and $0 \to G \to A \to B \to 0$ a resolution of G by abelian schemes (5.1.1). We apply the construction (5.2.2) to the morphism $A \to B$. Using Corollary 4.6, we obtain immediately that

$$\begin{aligned}
\mathrm{Ker}\,\alpha_2 &= \mathrm{Ker}\Big(\mathrm{Ext}^1(B_{\overline{\eta}}, \mathbb{F}_p) \to \mathrm{Ext}^1(A_{\overline{\eta}}, \mathbb{F}_p)\Big) \\
&= \mathrm{Hom}(G_{\overline{\eta}}, \mathbb{F}_p) = G^\vee(\overline{K})(-1), \\
\mathrm{Ker}\,\alpha_1 &= \mathrm{Ker}\Big(\mathrm{Ext}^1(B_{\overline{s}}, \mathbb{F}_p) \to \mathrm{Ext}^1(A_{\overline{s}}, \mathbb{F}_p)\Big) \\
&= \mathrm{Hom}(G_{\overline{s}}, \mathbb{F}_p) = (G_{\text{ét}})^\vee(\overline{K})(-1),
\end{aligned}$$

where $G_{\text{ét}} = G/G^{0+}$ is the étale part of G (cf. 2.8). Setting $N = \mathrm{Ker}\,\alpha_3$, we can complete (5.2.2) as follows :
(5.3.4)
$$\begin{tikzcd}
0 \arrow[r] & (G_{\text{ét}})^\vee(\overline{K})(-1) \arrow[r] \arrow[d, hook, "\gamma_1"] & G^\vee(\overline{K})(-1) \arrow[r, "u"] \arrow[d, hook, "\gamma_2"] & N \arrow[r, dashed] \arrow[d, hook, "\gamma_3"] & 0 \arrow[d, dashed] \\
0 \arrow[r] & \mathrm{H}^1(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_1"] & \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_2"] & \mathrm{H}^0(B_{\overline{s}}, \Psi^1_B)(-1) \arrow[r, "d_2^{1,0}(B)"] \arrow[d, "\alpha_3"] & \mathrm{H}^2(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\alpha_4"] \\
0 \arrow[r] & \mathrm{H}^1(A_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^0(A_{\overline{s}}, \Psi^1_A)(-1) \arrow[r, "d_2^{1,0}(A)"] & \mathrm{H}^2(A_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}).
\end{tikzcd}$$

We will show later that the morphism u is surjective.

Definition 5.4. *The assumptions are those of 5. We call the* Bloch-Kato filtration *on $G^\vee(\overline{K})$, and denote by $(\mathrm{U}^aG^\vee(\overline{K}), a \in \mathbb{Q}_{\geq 0})$, the decreasing and exhaustive filtration defined by $\mathrm{U}^0G^\vee(\overline{K}) = G^\vee(\overline{K})$, and for $a \in \mathbb{Q}_{>0}$,*

(5.4.1)
$$\mathrm{U}^aG^\vee(\overline{K}) = \gamma_2^{-1}(\mathrm{U}^a\mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}))(1).$$

Proposition 5.5. *Let $e' = \frac{ep}{p-1}$, G be a commutative finite and flat group scheme over S killed by p, and $0 \to G \to A \to B \to 0$ be a resolution of G by abelian schemes* (5.1.1).

(i) *For all $a \in \mathbb{Q}_{\geq 0}$, we have*

(5.5.1)
$$\begin{aligned}
\mathrm{U}^aG^\vee(\overline{K}) &\simeq \mathrm{Ker}\Big(\mathrm{U}^a\mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})(1) \xrightarrow{\alpha_2(1)} \mathrm{U}^a\mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})(1)\Big) \\
&\simeq u^{-1}\Big(N(1) \cap \mathrm{H}^0(B_{\overline{s}}, \mathrm{U}^a\Psi^1(B))\Big),
\end{aligned}$$

where $N(1)$ is identified to a subgroup of $\mathrm{H}^0(B_{\overline{s}}, \Psi^1(B))$ *by* $\gamma_3(1)$ *in* (5.3.4).

(ii) *The morphism* $u : G^\vee(\overline{K})(-1) \to N$ *in* (5.3.4) *is surjective. In particular, N is contained in the kernel of the morphism* $d_2^{1,0}(B)$ *in* (5.3.4).

(iii) *Under the canonical perfect pairing*

$$G(\overline{K}) \times G^\vee(\overline{K}) \to \mu_p(\overline{K}), \tag{5.5.2}$$

we have, for all $a \in \mathbb{Q}_{\geq 0}$,

$$G^{a+}(\overline{K})^\perp = \begin{cases} \mathrm{U}^{e'-a}G^\vee(\overline{K}) & \text{if } 0 \leq a \leq e' \text{ ;} \\ G^\vee(\overline{K}) & \text{if } a > e'. \end{cases}$$

In particular, the filtration $(\mathrm{U}^a G^\vee(\overline{K}), a \in \mathbb{Q}_{\geq 0})$ *does not depend on the resolution of G by abelian schemes.*

Proof. Statement (i) is obvious from definition 5.4 and diagrams (5.2.3) and (5.3.4).

For (ii) and (iii), thanks to Lemma 2.6, we need only to prove the proposition after a base change $\mathscr{O}_K \to \mathscr{O}_{K'}$, where K'/K is a finite extension. Therefore, up to such a base change, we may add the following assumptions.

(1) We may assume that k is algebraically closed, K contains a primitive p-th root of unity, and $G(\overline{K}) = G(K)$.

(2) For $X = A$ or B, we consider the cartesian diagram

$$\begin{tikzcd}
X_s \arrow[r, "i"] \arrow[d] & X \arrow[d] & X_\eta \arrow[l, "j"'] \arrow[d] \\
s = \overline{s} \arrow[r] & S & \eta \arrow[l]
\end{tikzcd}$$

and the étale sheaf $\Psi^1_{X,K} = i^*R^1j_*(\mathbb{Z}/p\mathbb{Z})$ over X_s. By an argument as in the proof of ([1] 3.1.1), we may assume that $\mathrm{H}^0(X_s, \Psi^1_X) = \mathrm{H}^0(X_s, \Psi^1_{X,K})$.

Since $\mathrm{U}^a\Psi^1_X = 0$ for $a \geq e'$ ([1] Lemme 3.1.1), we have $\mathrm{U}^{e'}G^\vee(\overline{K}) = \mathrm{Ker}(u)(1) = (G_{\text{ét}})^\vee(\overline{K})$. Statement (iii) for $a = 0$ follows immediately from Proposition 2.8(i). The pairing (5.5.2) induces a perfect pairing

$$G^{0+}(\overline{K}) \times \mathrm{Im}(u)(1) \longrightarrow \mu_p(\overline{K}). \tag{5.5.3}$$

In particular, we have $\dim_{\mathbb{F}_p}\big(\mathrm{Im}(u)(1)\big) = \dim_{\mathbb{F}_p}\big(G^{0+}(\overline{K})\big)$.

Let μ (*resp.* ν) be the generic point of $B_s = B_{\overline{s}}$ (*resp.* of $A_s = A_{\overline{s}}$), and $\overline{\nu}$ be a geometric point over ν. Then $\overline{\nu}$ induces by the morphism $\nu \to \mu$ a geometric point over μ, denoted by $\overline{\mu}$. Let $\mathscr{O}_\mu$ (*resp.* $\mathscr{O}_\nu$) be the local ring of B at μ (*resp.* of A at ν), $\mathscr{O}_{\overline{\mu}}$ (*resp.* $\mathscr{O}_{\overline{\nu}}$) be the henselization of $\mathscr{O}_\mu$ at $\overline{\mu}$ (*resp.* of $\mathscr{O}_\nu$ at $\overline{\nu}$). We denote by $\widehat{\mathscr{O}}_\mu$ and $\widehat{\mathscr{O}}_\nu$ the completions of $\mathscr{O}_\mu$ and $\mathscr{O}_\nu$, and by $(\widehat{\mathscr{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}}$ (*resp.* by $(\widehat{\mathscr{O}}_\nu)^{\mathrm{h}}_{\overline{\nu}}$) the henselization of $\widehat{\mathscr{O}}_\mu$ (*resp.* of $\widehat{\mathscr{O}}_\nu$) at $\overline{\mu}$ (*resp.* at $\overline{\nu}$). Let L_0 (*resp.* M_0) be the fraction field of $\mathscr{O}_\mu$ (*resp.* of $\mathscr{O}_\nu$), L_0^{ur} (*resp.* M_0^{ur}) be the fraction field of $\mathscr{O}_{\overline{\mu}}$ (*resp.* of $\mathscr{O}_{\overline{\nu}}$). We denote by L (*resp.* by M) the fraction field of $\widehat{\mathscr{O}}_\mu$ (*resp.* of $\widehat{\mathscr{O}}_\nu$), and by L^{ur} (*resp.* by M^{ur}) the fraction field of $(\widehat{\mathscr{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}}$ (*resp.* of $(\widehat{\mathscr{O}}_\nu)^{\mathrm{h}}_{\overline{\nu}}$). We notice that π is a uniformizing element in $\widehat{\mathscr{O}}_\mu$ and in $(\widehat{\mathscr{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}}$.

$$\begin{tikzcd}
\mathscr{O}_{\overline{\mu}} \arrow[r] & L_0^{ur} \arrow[r] & L^{ur} & (\widehat{\mathscr{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}} \arrow[l] \\
\mathscr{O}_\mu \arrow[r] \arrow[u] & L_0 \arrow[r] \arrow[u] & L \arrow[u] & \widehat{\mathscr{O}}_\mu \arrow[l] \arrow[u]
\end{tikzcd}$$

Since $G = \mathrm{Ker}(A \to B)$, we have an identification $\mathrm{Gal}(M/L) \simeq G(K) = G(\overline{K})$. We fix a separable closure $\overline{L}$ of L, and an imbedding of M in $\overline{L}$, which induces a surjection $\varphi : \mathrm{Gal}(\overline{L}/L) \to \mathrm{Gal}(M/L)$. By 2.10, we have $\varphi(\mathrm{Gal}(\overline{L}/L)^a) = \mathrm{Gal}(M/L)^a = G^a(\overline{K})$, for all $a \in \mathbb{Q}_{>0}$. In particular, we have

(5.5.4) $$\varphi(\mathrm{Gal}(\overline{L}/L^{ur})) = \mathrm{Gal}(M/M \cap L^{ur}) = \mathrm{Gal}(M^{ur}/L^{ur}) = G^{0+}(\overline{K}).$$

Since L^{ur}/L is unramified, we have, for all $a \in \mathbb{Q}_{>0}$,

(5.5.5) $$\mathrm{Gal}(M^{ur}/L^{ur})^a = \mathrm{Gal}(M/L)^a = G^a.$$

Let ρ_B be the composition of the canonical morphisms

$$\mathrm{H}^0(B_s, \Psi^1_B) = \mathrm{H}^0(B_s, \Psi^1_{B,K}) \to (\Psi^1_{B,K})_{\overline{\mu}} = \mathrm{H}^1(\mathrm{Spec}\, L_0^{ur}, \mu_p) \to \mathrm{H}^1(\mathrm{Spec}\, L^{ur}, \mu_p),$$

and we define ρ_A similarly. By functoriality and (5.5.4), we have a commutative diagram

(5.5.6) $$\begin{tikzcd}
0 \arrow[r] & N(1) \arrow[r] \arrow[d, hook] & \mathrm{H}^0(B_s, \Psi^1_B) \arrow[r] \arrow[d, hook, "\rho_B"] & \mathrm{H}^0(A_s, \Psi^1_A) \arrow[d, hook, "\rho_A"] \\
0 \arrow[r] & \mathrm{H}^1(G^{0+}(\overline{K}), \mu_p) \arrow[r, "inf"] & \mathrm{H}^1(\mathrm{Spec}\, L^{ur}, \mu_p) \arrow[r, "res"] & \mathrm{H}^1(\mathrm{Spec}\, M^{ur}, \mu_p),
\end{tikzcd}$$

where the lower horizontal row is the "inflation-restriction" exact sequence in Galois cohomology. By ([6] Prop. 6.1), ρ_B and ρ_A are injective. Hence $\mathrm{Im}(u)(1) \subset N(1)$ is identified with a subgroup of $\mathrm{H}^1(G^{0+}(\overline{K}), \mu_p)$. By assumption (1), we have $\mathrm{H}^1(G^{0+}(\overline{K}), \mu_p) = \mathrm{Hom}(G^{0+}(\overline{K}), \mu_p(\overline{K}))$, which has the same dimension over $\mathbb{F}_p$ as $G^{0+}(\overline{K})$. Hence by the remark below (5.5.3), we get

(5.5.7) $$\mathrm{Im}(u)(1) = N(1) \simeq \mathrm{H}^1(G^{0+}(\overline{K}), \mu_p) = \mathrm{Hom}(G^{0+}(\overline{K}), \mu_p(\overline{K})).$$

This proves statement (ii) of the proposition.

Statement (iii) for $a = 0$ has been proved above. Since the filtration G^a is decreasing and $\mathrm{U}^0 G^\vee(\overline{K}) = G^\vee(\overline{K})$, we may assume, for the proof of (iii), that $0 < a \leq e'$. It suffices to prove that, under the pairing (5.5.3), we have

$$G^{a+}(\overline{K})^\perp = \mathrm{Im}(u)(1) \cap \mathrm{H}^0(B_s, \mathrm{U}^{e'-a}\Psi^1_B).$$

From (5.5.6) and (5.5.7), we check easily that (5.5.3) is identified with the canonical pairing

$$G^{0+}(\overline{K}) \times \mathrm{H}^1(G^{0+}(\overline{K}), \mu_p) \to \mu_p(\overline{K}).$$

Hence we are reduced to prove that, under this pairing, we have

(5.5.8) $$G^{a+}(\overline{K})^\perp = \mathrm{H}^1(G^{0+}(\overline{K}), \mu_p) \cap \mathrm{H}^0(B_s, \mathrm{U}^{e'-a}\Psi^1_B),$$

where the "$\cap$" is taken in $\mathrm{H}^1(\operatorname{Spec} L^{ur}, \mu_p)$ (5.5.6).

Let $h : (L^{ur})^\times \to H^1(\operatorname{Spec} L^{ur}, \mu_p)$ be the symbol morphism. We define a decreasing filtration on $\mathrm{H}^1(\operatorname{Spec} L^{ur}, \mu_p)$ in a similar way as (3.2.5) by

$$\mathrm{U}^0\mathrm{H}^1 = \mathrm{H}^1, \quad \text{and} \quad \mathrm{U}^b\mathrm{H}^1 = h(1 + \pi^b(\widehat{\mathscr{O}}_\mu)_{\overline{\mu}}^{\mathrm{h}}) \text{ for all integers } b > 0.$$

We extend this definition to all $b \in \mathbb{Q}_{\geq 0}$ by setting $\mathrm{U}^b\mathrm{H}^1 = \mathrm{U}^{[b]}\mathrm{H}^1$, where $[b]$ denotes the integer part of b. By ([1] Lemme 3.1.3), for all $b \in \mathbb{Q}_{>0}$, we have $\mathrm{H}^0(B_s, \mathrm{U}^b\Psi_B^1) = \rho_B^{-1}\Big(\mathrm{U}^b\mathrm{H}^1(\operatorname{Spec} L^{ur}, \mu_p)\Big)$. Therefore, the right hand side of (5.5.8) is

$$\mathrm{H}^1(G^{0+}(\overline{K}), \mu_p) \cap \mathrm{U}^{(e'-a)}\mathrm{H}^1(\operatorname{Spec} L^{ur}, \mu_p). \tag{5.5.9}$$

We identify $\mathrm{H}^1(G^{0+}(\overline{K}), \mu_p)$ with the character group $\operatorname{Hom}(\operatorname{Gal}(M^{ur}/L^{ur}), \mu_p(\overline{K}))$; then by ([1] Prop. 2.2.1), the subgroup (5.5.9) consists of the characters χ such that $\chi(\operatorname{Gal}(M^{ur}/L^{ur})^{(e'-a)+}) = 0$. In view of (5.5.5), we obtain immediately (5.5.8), which completes the proof.

□

Remark 5.6. *The proof of 5.5(iii) follows the same strategy as the proof of ([1] Théorem 3.1.2). The referee point out that we can also reduce 5.5(iii) to 3.3. Indeed, the commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] & G \arrow[r] \arrow[d, "\times p"] & A \arrow[r] \arrow[d, "\times p"] & B \arrow[r] \arrow[d, "\times p"] & 0 \\
0 \arrow[r] & G \arrow[r] & A \arrow[r] & B \arrow[r] & 0
\end{tikzcd}$$

induces, by snake lemma, an exact sequence of finite group schemes $0 \to G \to {}_pA \xrightarrow{\phi} {}_pB \xrightarrow{\psi} G \to 0$. We consider the following perfect pairing

$$\begin{tikzcd}
 & {}_pA(\overline{K}) \arrow[d, "\phi"'] & {}_pA(\overline{K}) \times \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{F}_p) \arrow[r, "(\bullet{,}\bullet)_A"] & \mathbb{F}_p \arrow[d, equal] & \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{F}_p) \\
{}_pB^{a+}(\overline{K}) \arrow[r, hook] \arrow[d, two heads] & {}_pB(\overline{K}) \arrow[d, two heads, "\psi"'] & {}_pB(\overline{K}) \times \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{F}_p) \arrow[r, "(\bullet{,}\bullet)_B"] & \mathbb{F}_p \arrow[d, equal] & \mathrm{H}^1(B_\eta, \mathbb{F}_p) \arrow[u, "\alpha_2"'] \\
G^{a+}(\overline{K}) \arrow[r, hook] & G(\overline{K}) & G(\overline{K}) \times G^\vee(\overline{K})(-1) \arrow[r, "(\bullet{,}\bullet)_G"] & \mathbb{F}_p & G^\vee(\overline{K}). \arrow[u, hook, "\gamma_2"']
\end{tikzcd}$$

By functoriality, the homomorphism ϕ is adjoint to α_2 and ψ is adjoint to γ_2, i.e. *we have $(\phi(x), f)_B = (x, \alpha_2(f))_A$ and $(\psi(y), g)_B = (y, \gamma_2(g))_G$, for all $x \in {}_pA(\overline{K})$, $y \in {}_pB(\overline{K})$, $f \in \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{F}_p)$ and $g \in G^\vee(\overline{K})$. By 2.8(ii), ψ induces a surjective homomorphism ${}_pB^{a+}(\overline{K}) \to G^{a+}(\overline{K})$ for all $a \in \mathbb{Q}_{\geq 0}$. Now statement 5.5(iii) follows from* (5.4.1) *and Theorem 3.3 applied to B.*

6 Proof of Theorem 1.4(i)

6.1. For $r \in \mathbb{Q}_{>0}$, we denote by $\mathbb{G}_{a,r}$ the additive group scheme over $\overline{S}_r$ (1). Putting $t = 1 - 1/p$, we identify $\mathbb{G}_{a,t}$ with an abelian fppf-sheaf over $\overline{S}_1$ by the canonical immersion $i : \overline{S}_t \to \overline{S}_1$. Let

$\mathrm{F}:\mathbb{G}_{a,1}\to\mathbb{G}_{a,1}$ be the Frobenius homomorphism, and c a p-th root of $(-p)$. It is easy to check that the morphism $\mathrm{F}-c:\mathbb{G}_{a,1}\to\mathbb{G}_{a,1}$, whose cokernel is denoted by $\mathbb{P}$, factorizes through the canonical reduction morphism $\mathbb{G}_{a,1}\to\mathbb{G}_{a,t}$, and we have an exact sequence of abelian fppf-sheaves on $\overline{S}_1$.

$$0\to\mathbb{F}_p\to\mathbb{G}_{a,t}\xrightarrow{\mathrm{F}-c}\mathbb{G}_{a,1}\to\mathbb{P}\to 0. \tag{6.1.1}$$

This exact sequence gives (3.10.1) after restriction to the small étale topos $(\overline{X}_1)_{\text{ét}}$ for a smooth S-scheme X.

Proposition 6.2. *Assume $p\geq 3$. Let G be a truncated Barsotti-Tate group of level* 1 *over S, and $t=1-1/p$. Then we have the equality*

$$\dim_{\mathbb{F}_p}\mathrm{U}^eG^{\vee}(\overline{K})=\dim_{\mathbb{F}_p}\mathrm{Ker}\bigg(\mathrm{Lie}(\overline{G}_t^{\vee})\xrightarrow{\mathrm{F}-c}\mathrm{Lie}(\overline{G}_1^{\vee})\bigg),$$

where $\mathrm{U}^eG^{\vee}(\overline{K})$ is the Bloch-Kato filtration (5.4)*, and the morphism in the right hand side is obtained by applying the functor $\mathrm{Hom}_{\overline{S}_1}(\overline{G}_1,\_)$ to the map $\mathrm{F}-c:\mathbb{G}_{a,t}\to\mathbb{G}_{a,1}$.*

6.3. Before proving this proposition, we deduce first Theorem 1.4(i). Let G be a truncated Barsotti-Tate group of level 1 and height h over S satisfying the assumptions of 1.4, d be the dimension of $\mathrm{Lie}(G_s^{\vee})$ over k, and $d^*=h-d$. It follows from 5.5(iii) and 6.2 that

$$\dim_{\mathbb{F}_p}G^{\frac{e}{p-1}+}(\overline{K})=h-\dim_{\mathbb{F}_p}\mathrm{Ker}\bigg(\mathrm{Lie}(\overline{G}_t^{\vee})\xrightarrow{\mathrm{F}-c}\mathrm{Lie}(\overline{G}_1^{\vee})\bigg).$$

Since $\mathrm{Lie}(\overline{G}_1^{\vee})$ is a free $\mathscr{O}_{\overline{S}_1}$-module of rank d^*, we obtain immediately Theorem 1.4(i) by applying Proposition 3.12 to $\lambda=c$ and $M=\mathrm{Lie}(\overline{G}_1^{\vee})$.

The rest of this section is dedicated to the proof of Proposition 6.2.

Lemma 6.4. *Let G be a Barsotti-Tate group of level 1 over S, $t=1-\frac{1}{p}$. Then the morphism $\phi:\mathrm{Ext}^1(\overline{G}_1,\mathbb{F}_p)\to\mathrm{Ext}^1(\overline{G}_1,\mathbb{G}_{a,t})$ induced by the morphism $\mathbb{F}_p\to\mathbb{G}_{a,t}$ in* (6.1.1) *is injective.*

Proof. By ([12] Théorème 4.4(e)), there exists a Barsotti-Tate group H over S such that we have an exact sequence $0\to G\to H\xrightarrow{\times p}H\to 0$, which induces a long exact sequence

$$\mathrm{Ext}^1(\overline{H}_1,\mathbb{F}_p)\xrightarrow{\times p}\mathrm{Ext}^1(\overline{H}_1,\mathbb{F}_p)\to\mathrm{Ext}^1(\overline{G}_1,\mathbb{F}_p)\to\mathrm{Ext}^2(\overline{H}_1,\mathbb{F}_p).$$

It is clear that the multiplication by p on $\mathrm{Ext}^1(\overline{H}_1,\mathbb{F}_p)$ is 0, and $\mathrm{Ext}^2(\overline{H}_1,\mathbb{F}_p)=0$ by Corollary 4.9; hence the middle morphism in the exact sequence above is an isomorphism. Similarly, using $\mathrm{Ext}^2(\overline{H}_1,\mathbb{G}_{a,t})=0$ ([5] 3.3.2), we prove that the natural map $\mathrm{Ext}^1(\overline{H}_1,\mathbb{G}_{a,t})\to\mathrm{Ext}^1(\overline{G}_1,\mathbb{G}_{a,t})$ is an isomorphism. So we get a commutative diagram

$$\begin{tikzcd}
\mathrm{Ext}^1(\overline{H}_1,\mathbb{F}_p) \arrow[r] \arrow[d, "\phi_H"] & \mathrm{Ext}^1(\overline{G}_1,\mathbb{F}_p) \arrow[d, "\phi"] \\
\mathrm{Ext}^1(\overline{H}_1,\mathbb{G}_{a,t}) \arrow[r] & \mathrm{Ext}^1(\overline{G}_1,\mathbb{G}_{a,t}),
\end{tikzcd}$$

where the horizontal maps are isomorphisms. Now it suffices to prove that ϕ_H is injective.

Let $\mathbb{K}$ be the fppf-sheaf on $\overline{S}_1$ determined by the following exact sequences :

$$0 \to \mathbb{F}_p \to \mathbb{G}_{a,t} \to \mathbb{K} \to 0; \quad 0 \to \mathbb{K} \to \mathbb{G}_{a,1} \to \mathbb{P} \to 0.$$

Applying the functors $\mathrm{Ext}^q(\overline{H}_1, \_)$, we get

$$\mathrm{Hom}(\overline{H}_1, \mathbb{K}) \to \mathrm{Ext}^1(\overline{H}_1, \mathbb{F}_p) \xrightarrow{\phi_H} \mathrm{Ext}^1(\overline{H}_1, \mathbb{G}_{a,t});$$
$$0 \to \mathrm{Hom}(\overline{H}_1, \mathbb{K}) \to \mathrm{Hom}(\overline{H}_1, \mathbb{G}_{a,1}) \to \mathrm{Hom}(\overline{H}_1, \mathbb{P}).$$

Since $\mathrm{Hom}(\overline{H}_1, \mathbb{G}_{a,1}) = 0$ ([5] 3.3.2), the injectivity of ϕ_H follows immediately. □

6.5. Assume that $p \geq 3$. Let G be a commutative finite and flat group scheme killed by p over S, and $0 \to G \to A \to B \to 0$ be a resolution of G by abelian schemes (5.1.1). We denote $\mathscr{P}(B) = \mathrm{Coker}(\mathscr{O}_{\overline{B}_1} \xrightarrow{\mathrm{F}-c} \mathscr{O}_{\overline{B}_1})$ (3.7.1), and similarly for $\mathscr{P}(A)$. According to Remark 3.9, we have an identification

$$\mathrm{H}^0(B_{\overline{s}}, \mathrm{U}^e\Psi^1_B) \simeq \mathrm{H}^0(B_{\overline{s}}, \mathscr{P}(B)) = \mathrm{H}^0(\overline{B}_1, \mathscr{P}(B)) \tag{6.5.1}$$

as submodules of $\mathrm{H}^0(B_{\overline{s}}, \Psi^1_B)$; in the last equality, we have identified the topos $(B_{\overline{s}})_{\text{ét}}$ with $(\overline{B}_1)_{\text{ét}}$. We denote

$$\begin{aligned}\mathrm{Ker}(B, \mathrm{F}-c) &= \mathrm{Ker}\Big(\mathrm{H}^1(\overline{B}_1, \mathbb{G}_{a,t}) \xrightarrow{\mathrm{F}-c} \mathrm{H}^1(\overline{B}_1, \mathbb{G}_{a,1})\Big)\\ &= \mathrm{Ker}\Big(\mathrm{Lie}(\overline{B}^\vee_t) \xrightarrow{\mathrm{F}-c} \mathrm{Lie}(\overline{B}^\vee_1)\Big),\\ \mathrm{Ker}(B, \delta_E) &= \mathrm{Ker}\Big(\mathrm{H}^0(\overline{B}_1, \mathscr{P}(B)) \xrightarrow{\delta_E} \mathrm{H}^2(B_{\overline{s}}, \mathbb{F}_p)\Big),\end{aligned}$$

where δ_E is the morphism defined in Proposition 3.10(2); we have also similar notations for A. Since the exact sequence (3.10.2) is functorial in X, we have a commutative diagram

(6.5.2)
$$\begin{tikzcd} 0 \arrow[r] & \mathrm{H}^1(B_{\overline{s}}, \mathbb{F}_p) \arrow[r] \arrow[d, "\beta_1"] & \mathrm{Ker}(B, \mathrm{F}-c) \arrow[r] \arrow[d, "\beta_2"] & \mathrm{Ker}(B, \delta_E) \arrow[r] \arrow[d, "\beta_3"] & 0 \\ 0 \arrow[r] & \mathrm{H}^1(A_{\overline{s}}, \mathbb{F}_p) \arrow[r] & \mathrm{Ker}(A, \mathrm{F}-c) \arrow[r] & \mathrm{Ker}(A, \delta_E) \arrow[r] & 0. \end{tikzcd}$$

Lemma 6.6. *The assumptions are those of* (6).

(i) *In diagram* (6.5.2), *we have*

$$\mathrm{Ker}\,\beta_1 = \mathrm{Ker}\Big(\mathrm{Ext}^1(B_{\overline{s}}, \mathbb{F}_p) \to \mathrm{Ext}^1(A_{\overline{s}}, \mathbb{F}_p)\Big) = (G_{\text{ét}})^\vee(\overline{K})(-1); \tag{6.6.1}$$

$$\mathrm{Ker}\,\beta_2 = \mathrm{Ker}\Big(\mathrm{Lie}(\overline{G}^\vee_t) \xrightarrow{\mathrm{F}-c} \mathrm{Lie}(\overline{G}^\vee_1)\Big); \tag{6.6.2}$$

$$\mathrm{Ker}\,\beta_3 = \mathrm{H}^0(B_{\overline{s}}, \mathscr{P}(B)) \cap N(1) \subset \mathrm{H}^0(B_{\overline{s}}, \Psi^1_B), \tag{6.6.3}$$

where $N(1)$ *is defined in* (5.3.4).

(ii) *We have the equality*

$$\dim_{\mathbb{F}_p} \mathrm{U}^e G^\vee(\overline{K}) = \dim_{\mathbb{F}_p} \operatorname{Ker}\beta_1 + \dim_{\mathbb{F}_p} \operatorname{Ker}\beta_3. \tag{6.6.4}$$

In particular, we have

$$\dim_{\mathbb{F}_p} \mathrm{U}^e G^\vee(\overline{K}) \geq \dim_{\mathbb{F}_p} \operatorname{Ker}\Big(\mathrm{Lie}(\overline{G}_t^\vee) \xrightarrow{\mathrm{F}-c} \mathrm{Lie}(\overline{G}_1^\vee)\Big), \tag{6.6.5}$$

Moreover, the equality holds in (6.6.5) *if and only if the morphism* $\operatorname{Coker}\beta_1 \to \operatorname{Coker}\beta_2$ *induced by diagram* (6.5.2) *is injective.*

Proof. (i) By Corollary 4.6, we have a canonical isomorphism $\mathrm{Ext}^1(X_{\overline{s}}, \mathbb{F}_p) \simeq \mathrm{H}^1(X_{\overline{s}}, \mathbb{F}_p)$ for $X = A$ or B. Hence formula (6.6.1) follows easily by applying the functors $\mathrm{Ext}^q(\_, \mathbb{F}_p)$ to the exact sequence $0 \to G_{\overline{s}} \to A_{\overline{s}} \to B_{\overline{s}} \to 0$. Applying the morphism of functors $\mathrm{F} - c : \mathrm{Ext}^i(\_, \mathbb{G}_{a,t}) \to \mathrm{Ext}^i(\_, \mathbb{G}_{a,1})$ to the exact sequence $0 \to G \to A \to B \to 0$, we obtain the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Lie}(\overline{G}_t^\vee) \arrow[r] \arrow[d, "\mathrm{F}-c"] & \mathrm{Lie}(\overline{B}_t^\vee) \arrow[r] \arrow[d, "\mathrm{F}-c"] & \mathrm{Lie}(\overline{A}_t^\vee) \arrow[d, "\mathrm{F}-c"] \ , \\
0 \arrow[r] & \mathrm{Lie}(\overline{G}_1^\vee) \arrow[r] & \mathrm{Lie}(\overline{B}_1^\vee) \arrow[r] & \mathrm{Lie}(\overline{A}_1^\vee)
\end{tikzcd}$$

where we have used (4.7.1) and (4.7.2). Formula (6.6.2) follows immediately from this diagram. For (6.6.3), using (6.5.1), we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Ker}(B, \delta_E) \arrow[r, "(1)"] \arrow[d, "\beta_3"'] & \mathrm{H}^0(B_{\overline{s}}, \Psi_B^1) \arrow[d] \\
\mathrm{Ker}(A, \delta_E) \arrow[r, "(2)"] & \mathrm{H}^0(A_{\overline{s}}, \Psi_A^1),
\end{tikzcd}$$

where the maps (1) and (2) are injective. Hence we obtain

$$\begin{aligned}
\operatorname{Ker}\beta_3 &= \mathrm{Ker}(B, \delta_E) \cap \operatorname{Ker}\Big(\mathrm{H}^0(B_{\overline{s}}, \Psi^1(B)) \to \mathrm{H}^0(A_{\overline{s}}, \Psi^1(A))\Big) \\
&= \mathrm{Ker}(B, \delta_E) \cap N(1).
\end{aligned}$$

The morphisms δ_E and $d_2^{1,0}$ are compatible in the sense of Proposition 3.10, and Proposition 5.5 implies that $\mathrm{Ker}(B, \delta_E) \cap N(1) = \mathrm{H}^0(B_{\overline{s}}, \mathscr{P}(B)) \cap N(1)$, which proves (6.6.3).

(ii) By the isomorphism (5.5.1) and the surjectivity of the morphism u in (5.3.4), we have

$$\begin{aligned}
\dim_{\mathbb{F}_p} \mathrm{U}^e G^\vee(\overline{K}) &= \dim_{\mathbb{F}_p}\Big(G^\vee(\overline{K})(-1) \cap \mathrm{U}^e\mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})\Big) \\
&= \dim_{\mathbb{F}_p}\Big((G_{\text{ét}})^\vee(\overline{K})(-1)\Big) + \dim_{\mathbb{F}_p}\Big(N \cap \mathrm{H}^0(B_{\overline{s}}, \mathrm{U}^e\Psi^1(B))(-1)\Big). \qquad (6.6.6)
\end{aligned}$$

Then the equality (6.6.4) follows from (i) of this lemma and (6.5.1). The rest part of (ii) follows immediately from diagram (6.5.2). □

6.7. ***Proof of Proposition 6.2*** We choose a resolution $0 \to G \to A \to B \to 0$ of G by abelian schemes (5.1.1). By Lemma 6.6, we have to prove that if G is a truncated Barsotti-Tate group of level 1 over S, the morphism $\phi_{12} : \operatorname{Coker}\beta_1 \to \operatorname{Coker}\beta_2$ induced by diagram (6.5.2) is injective.

By 4.6, we have $\mathrm{H}^1_{\text{ét}}(X_{\overline{s}}, \mathbb{F}_p) = \mathrm{H}^1_{\text{ét}}(\overline{X}_1, \mathbb{F}_p) = \operatorname{Ext}^1(\overline{X}_1, \mathbb{F}_p)$ for $X = A$ or B. Thus the morphism β_1 is canonically identified to the morphism $\operatorname{Ext}^1(\overline{B}_1, \mathbb{F}_p) \to \operatorname{Ext}^1(\overline{A}_1, \mathbb{F}_p)$ induced by the map $A \to B$. Applying the functors $\operatorname{Ext}^i(\_, \mathbb{F}_p)$ to $0 \to \overline{G}_1 \to \overline{A}_1 \to \overline{B}_1 \to 0$, we obtain a long exact sequence

$$\operatorname{Ext}^1(\overline{B}_1, \mathbb{F}_p) \to \operatorname{Ext}^1(\overline{A}_1, \mathbb{F}_p) \to \operatorname{Ext}^1(\overline{G}_1, \mathbb{F}_p) \to \operatorname{Ext}^2(\overline{B}_1, \mathbb{F}_p).$$

Since $\operatorname{Ext}^2(\overline{B}_1, \mathbb{F}_p) = 0$ by 4.9, we have $\operatorname{Coker}\beta_1 = \operatorname{Ext}^1(\overline{G}_1, \mathbb{F}_p)$. The commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}(B, \mathrm{F} - c) \arrow[r] \arrow[d, "\beta_2"'] & \operatorname{Lie}(B_t^\vee) \arrow[r, "\mathrm{F}-c"] \arrow[d, "\gamma"'] & \operatorname{Lie}(B_1^\vee) \arrow[d] \\
0 \arrow[r] & \operatorname{Ker}(A, \mathrm{F} - c) \arrow[r] & \operatorname{Lie}(A_t^\vee) \arrow[r, "\mathrm{F}-c"] & \operatorname{Lie}(A_1^\vee),
\end{tikzcd}$$

induces a canonical morphism $\psi : \operatorname{Coker}\beta_2 \to \operatorname{Coker}\gamma = \operatorname{Ext}^1(\overline{G}_1, \mathbb{G}_{a,t})$. Let $\phi : \operatorname{Ext}^1(\overline{G}_1, \mathbb{F}_p) \to \operatorname{Ext}^1(\overline{G}_1, \mathbb{G}_{a,t})$ be the morphism induced by the map $\mathbb{F}_p \to \mathbb{G}_{a,t}$ in (6.1.1). Then we have the following commutative diagram

$$\begin{tikzcd}
\operatorname{Ext}^1(\overline{G}_1, \mathbb{F}_p) = \operatorname{Coker}\beta_1 \arrow[r, "\phi_{12}"] \arrow[dr, "\phi"'] & \operatorname{Coker}\beta_2 \arrow[d, "\psi"] \\
 & \operatorname{Ext}^1(\overline{G}_1, \mathbb{G}_{a,t}).
\end{tikzcd}$$

Now Lemma 6.4 implies that ϕ is injective, hence so is ϕ_{12}. This completes the proof.

7 The canonical filtration in terms of congruence groups

7.1. Recall the following definitions in [20]. For any $\lambda \in \mathscr{O}_{\overline{K}}$, let $\mathscr{G}^{(\lambda)}$ be the group scheme $\operatorname{Spec}(\mathscr{O}_{\overline{K}}[T, \frac{1}{1+\lambda T}])$ with the comultiplication given by $T \mapsto T \otimes 1 + 1 \otimes T + \lambda T \otimes T$, the counit by $T = 0$ and the coinverse by $T \mapsto -\frac{T}{1+\lambda T}$. If $v(\lambda) \leq e/(p-1)$, we put

$$P_\lambda(T) = \frac{(1 + \lambda T)^p - 1}{\lambda^p} \in \mathscr{O}_{\overline{K}}[T]$$

and let $\phi_\lambda : \mathscr{G}^{(\lambda)} \to \mathscr{G}^{(\lambda^p)}$ be the morphism of $\mathscr{O}_{\overline{K}}$-group schemes defined on the level of Hopf algebras by $T \mapsto P_\lambda(T)$. We denote by G_λ the kernel of ϕ_λ, so we have $G_\lambda = \operatorname{Spec}\big(\mathscr{O}_{\overline{K}}[T]/P_\lambda(T)\big)$. We call it, following Raynaud, the *congruence group of level* λ. It is a finite flat group scheme over $\overline{S} = \operatorname{Spec}(\mathscr{O}_{\overline{K}})$ of rank p.

7.2. For all $\lambda \in \mathscr{O}_{\overline{K}}$ with $v(\lambda) \leq e/(p-1)$, let $\theta_\lambda : G_\lambda \to \mu_p = \operatorname{Spec}(\mathscr{O}_{\overline{K}}[X]/(X^p - 1))$ be the homomorphism given on the level of Hopf algebras by $X \mapsto 1 + \lambda T$. Then $\theta_\lambda \otimes \overline{K}$ is an isomorphism, and if $v(\lambda) = 0$, θ_λ is an isomorphism. For all $\lambda, \gamma \in \mathscr{O}_{\overline{K}}$ with $v(\gamma) \leq v(\lambda) \leq e/(p-1)$, let $\theta_{\lambda,\gamma} : G_\lambda \to G_\gamma$ be the map defined by the homomorphism of Hopf algebras $T \mapsto (\lambda/\gamma)T$. We have $\theta_\lambda = \theta_\gamma \circ \theta_{\lambda,\gamma}$.

7.3. Let $\lambda \in \mathscr{O}_{\overline{K}}$ with $v(\lambda) \leq e/(p-1)$, A be an abelian scheme over S. We define

$$\theta_\lambda(A) : \mathrm{Ext}^1_{\overline{S}}(A, G_\lambda) \to \mathrm{Ext}^1_{\overline{S}}(A, \mu_p) \tag{7.3.7}$$

to be the homomorphism induced by the canonical morphism $\theta_\lambda : G_\lambda \to \mu_p$, where, by abuse of notations, A denotes also the inverse image of A over $\overline{S}$, and $\mathrm{Ext}^1_{\overline{S}}$ means the extension in the category of abelian fppf-sheaves over $\overline{S}$. Similarly, let G be a commutative finite and flat group scheme killed by p over S; we define

$$\theta_\lambda(G) : \mathrm{Hom}_{\overline{S}}(G, G_\lambda) \to \mathrm{Hom}_{\overline{S}}(G, \mu_p) = G^\vee(\overline{K}) \tag{7.3.8}$$

to be the homomorphism induced by θ_λ. If $G = {}_pA$, where A is an S-abelian scheme, the natural exact sequence $0 \to {}_pA \to A \xrightarrow{\times p} A \to 0$ induces a commutative diagram

(7.3.9)
$$\begin{tikzcd}
\mathrm{Hom}_{\overline{S}}({}_pA, G_\lambda) \arrow[r] \arrow[d, "\theta_\lambda({}_pA)"'] & \mathrm{Ext}^1_{\overline{S}}(A, G_\lambda) \arrow[d, "\theta_\lambda(A)"] \\
{}_pA^\vee(\overline{K}) \arrow[r] & \mathrm{Ext}^1_{\overline{S}}(A, \mu_p),
\end{tikzcd}$$

where horizontal maps are isomorphisms (4.3.2). Hence, $\theta_\lambda(A)$ is canonically identified to $\theta_\lambda({}_pA)$.

Lemma 7.4. *Let $\lambda, \gamma \in \mathscr{O}_{\overline{K}}$ with $v(\gamma) \leq v(\lambda) \leq e/(p-1)$, G be a commutative finite and flat group scheme killed by p over S.*

(i) *$\theta_\lambda(G)$ is injective.*

(ii) *The image of $\theta_\lambda(G)$ is contained in that of $\theta_\gamma(G)$.*

(iii) *The image of $\theta_\lambda(G)$ depends only on $v(\lambda)$, and it is invariant under the action of the Galois group* $\mathrm{Gal}(\overline{K}/K)$.

Proof. We have a commutative diagram

(7.4.1)
$$\begin{tikzcd}
\mathrm{Hom}_{\overline{S}}(G_\lambda^\vee, G^\vee) \arrow[r, "\theta_\lambda(G)"] \arrow[d, "(1)"'] & \mathrm{Hom}_{\overline{S}}(\mathbb{Z}/p\mathbb{Z}, G^\vee) \arrow[d, equal] \\
\mathrm{Hom}_{\overline{\eta}}(G_\lambda^\vee, G^\vee) \arrow[r, "(2)"] & \mathrm{Hom}_{\overline{\eta}}(\mathbb{Z}/p\mathbb{Z}, G^\vee),
\end{tikzcd}$$

where the horizontal maps are induced by $\theta_\lambda^\vee : \mathbb{Z}/p\mathbb{Z} \to G_\lambda^\vee$, and the vertical maps are induced by the base change $\overline{\eta} \to \overline{S}$. Since θ_λ is an isomorphism over the generic point (7), the map (2) is an isomorphism. Hence statement (i) follows from the fact that (1) is injective by the flatness of G and G_λ.

Statement (ii) follows easily from the existence of the morphism $\theta_{\lambda,\gamma} : G_\lambda \to G_\gamma$ with $\theta_\lambda = \theta_\gamma \circ \theta_{\lambda,\gamma}$. The first part of (iii) follows immediately from (ii). Any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ sends the image of $\theta_\lambda(G)$ isomorphically to the image of $\theta_{\sigma(\lambda)}(G)$, which coincides with the former by the first assertion of (iii). □

7.5. Filtration by congruence groups Let a be a rational number with $0 \leq a \leq e/(p-1)$, and G be a commutative finite and flat group scheme over S killed by p. We choose $\lambda \in \mathscr{O}_{\overline{K}}$ with $v(\lambda) = a$, and denote by $G^\vee(\overline{K})^{[a]}$ the image of $\theta_\lambda(G)$. By Lemma 7.4, $G^\vee(\overline{K})^{[a]}$ depends only on

a, and not on the choice of λ. Then $\big(G^\vee(\overline{K})^{[a]}, a \in \mathbb{Q} \cap [0, e/(p-1)]\big)$ is an exhaustive decreasing filtration of $G^\vee(\overline{K})$ by $\mathrm{Gal}(\overline{K}/K)$-groups.

7.6. Let $\lambda \in \mathscr{O}_{\overline{K}}$ with $0 \leq v(\lambda) \leq e/(p-1)$, $f : A \to S$ be an abelian scheme, and $\overline{f} : \overline{A} \to \overline{S}$ its base change by $\overline{S} \to S$. In ([3] §6), Andreatta and Gasbarri consider the homomorphism $\theta'_\lambda(A) : \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, G_\lambda) \to \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, \mu_p)$ induced by θ_λ, where by abuse of notation, G_λ denotes also the fppf-sheaf G_λ restricted to $\overline{A}$. We have a commutative diagram

(7.6.2)
$$\begin{tikzcd}
\mathrm{Ext}^1_{\overline{S}}(A, G_\lambda) \arrow[r, "\varphi(G_\lambda)"] \arrow[d, "\theta_\lambda(A)"'] & \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, G_\lambda) \arrow[d, "\theta'_\lambda(A)"] \\
\mathrm{Ext}^1_{\overline{S}}(A, \mu_p) \arrow[r, "\varphi(\mu_p)"] & \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, \mu_p),
\end{tikzcd}$$

where the horizontal arrows are the homomorphisms (4.4.3).

Lemma 7.7. (i) *The homomorphisms $\varphi(G_\lambda)$ and $\varphi(\mu_p)$ in (7.6.2) are isomorphisms. In particular, the homomorphism $\theta'_\lambda(A)$ is canonically isomorphic to $\theta_\lambda(A)$ (7.3.7).*

(ii) *The canonical morphism $\mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, \mu_p) \to \mathrm{H}^1(A_{\overline{\eta}}, \mu_p)$ is an isomorphism. Let $\mathrm{H}^1(A_{\overline{\eta}}, \mu_p)^{[v(\lambda)]}$ be the image of $\theta'_\lambda(A)$ composed with this isomorphism. Then via the canonical isomorphism $\mathrm{H}^1(A_{\overline{\eta}}, \mu_p) \simeq {}_pA^\vee(\overline{K})$, the subgroup $\mathrm{H}^1(A_{\overline{\eta}}, \mu_p)^{[v(\lambda)]}$ is identified to ${}_pA^\vee(\overline{K})^{[v(\lambda)]}$.*

Proof. (i) For $H = G_\lambda$ or μ_p, the "local-global" spectral sequence induces an exact sequence

(7.7.1)
$$0 \to \mathrm{H}^1_{\mathrm{fppf}}(\overline{S}, R^0_{\mathrm{fppf}}\overline{f}_*(H_{\overline{A}})) \to \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, H_{\overline{A}}) \xrightarrow{\psi(H)} \mathrm{H}^0_{\mathrm{fppf}}(\overline{S}, R^1_{\mathrm{fppf}}\overline{f}_*(H_{\overline{A}})).$$

By Prop. 4.5 and (4.3.2), we have isomorphisms

$$\mathrm{H}^0_{\mathrm{fppf}}(\overline{S}, R^1_{\mathrm{fppf}}\overline{f}_*(H_{\overline{A}})) \simeq \mathrm{H}^0_{\mathrm{fppf}}(\overline{S}, \mathscr{E}xt^1_{\overline{S}}(A, H)) \simeq \mathrm{Ext}^1_{\overline{S}}(A, H).$$

Therefore, we obtain a homomorphism $\psi(H) : \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, H_{\overline{A}}) \to \mathrm{Ext}^1_{\overline{S}}(A, H)$. We check that the composed map $\psi(H) \circ \varphi(H)$ is the identity morphism on $\mathrm{Ext}^1_{\overline{S}}(A, H)$; in particular, $\psi(H)$ is surjective. By Prop. 4.5, we have also $R^0_{\mathrm{fppf}}\overline{f}_*(H_{\overline{A}}) = H_{\overline{S}}$; on the other hand, it follows from ([3] Lemma 6.2) that $\mathrm{H}^1_{\mathrm{fppf}}(\overline{S}, H_{\overline{S}}) = 0$. Hence $\psi(H)$ is injective by the exact sequence (7.7.1), and $\varphi(H)$ and $\psi(H)$ are both isomorphisms.

(ii) We have a commutative diagram

$$\begin{tikzcd}
\mathrm{Ext}^1_{\overline{S}}(A, \mu_p) \arrow[r, "\varphi(\mu_p)"] \arrow[d, "(1)"'] & \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, \mu_p) \arrow[d, "(2)"] \\
\mathrm{Ext}^1_{\overline{\eta}}(A_{\overline{\eta}}, \mu_p) \arrow[r] & \mathrm{H}^1(A_{\overline{\eta}}, \mu_p),
\end{tikzcd}$$

where the vertical maps are base changes to the generic fibres, and the horizontal morphisms are (4.4.3), which are isomorphisms in our case by (4.6) and statement (i). The morphism (1) is easily checked to be an isomorphism using (4.3.2), hence so is the morphism (2). The second part of statement (ii) is a consequence of (i). □

The following proposition, together with Proposition 5.5, implies Theorem 1.6.

Proposition 7.8. *Let G be a commutative finite and flat group scheme over S killed by p. Then, for all rational numbers $0 \leq a \leq e/(p-1)$, we have $G^\vee(\overline{K})^{[a]} = \mathrm{U}^{pa}G^\vee(\overline{K})$, where $\mathrm{U}^\bullet G^\vee(\overline{K})$ is the Bloch-Kato filtration* (5.4).

Proof. Let $0 \to G \to A \to B \to 0$ be a resolution of G by abelian schemes (5.1.1). We have, for all $\lambda \in \mathscr{O}_{\overline{K}}$ with $0 \leq v(\lambda) \leq e/(p-1)$, a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{\overline{S}}(G, G_\lambda) \arrow[r] \arrow[d, hook, "\theta_\lambda(G)"] & \mathrm{Ext}^1_{\overline{S}}(B, G_\lambda) \arrow[r] \arrow[d, hook, "\theta_\lambda(B)"] & \mathrm{Ext}^1_{\overline{S}}(A, G_\lambda) \arrow[d, hook, "\theta_\lambda(A)"] \\
0 \arrow[r] & G^\vee(\overline{K}) \arrow[r] & {}_pB^\vee(\overline{K}) \arrow[r] & {}_pA^\vee(\overline{K}).
\end{tikzcd}$$

Hence, for all rational numbers a satisfying $0 \leq a \leq e/(p-1)$, we have by 7.7(ii)

$$G^\vee(\overline{K})^{[a]} = G^\vee(\overline{K}) \cap {}_pB^\vee(\overline{K})^{[a]} = G^\vee(\overline{K}) \cap \mathrm{H}^1(B_{\overline{\eta}}, \mu_p)^{[a]}. \tag{7.8.1}$$

According to ([3] Theorem 6.8), the filtration $(\mathrm{H}^1(B_{\overline{\eta}}, \mu_p)^{[a]}, 0 \leq a \leq e/(p-1))$ coincides with the filtration $(\mathrm{U}^{pa}\mathrm{H}^1(B_{\overline{\eta}}, \mu_p), 0 \leq a \leq \frac{e}{p-1})$ (3.2.6). Hence by (7.8.1) and (5.4.1), the two filtrations $\big(G^\vee(\overline{K})^{[a]}\big)$ and $\big(\mathrm{U}^{pa}G^\vee(\overline{K})\big)$ on $G^\vee(\overline{K})$ coincide. This completes the proof.

□

8 The lifting property of the canonical subgroup

In this section, by abuse of notations, $\mathbb{G}_a$ will denote the additive group both over S and over $\overline{S}$. For a rational number $r > 0$, we denote by $\mathbb{G}_{a,r}$, $\mathscr{G}_r^{(\lambda)}$ and $G_{\lambda,r}$ the base changes to $\overline{S}_r$ of the respective group schemes.

8.1. Following [21], for $a, c \in \mathscr{O}_{\overline{K}}$ with $ac = p$, we denote by $G_{a,c}$ the group scheme $\mathrm{Spec}\big(\mathscr{O}_{\overline{K}}[y]/(y^p - ay)\big)$ over $\mathscr{O}_{\overline{K}}$ with comultiplication

$$y \mapsto y \otimes 1 + 1 \otimes y + \frac{cw_{p-1}}{1-p} \sum_{i=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$$

and the counit given by $y = 0$, where w_i $(1 \leq i \leq p-1)$ are universal constants in $\mathscr{O}_{\overline{K}}$ with $v(w_i) = 0$ (see [21] p.9). Tate and Oort proved that $(a, c) \mapsto G_{a,c}$ gives a bijection between equivalence classes of factorizations of $p = ac$ in $\mathscr{O}_{\overline{K}}$ and isomorphism classes of $\mathscr{O}_{\overline{K}}$-group schemes of order p, where two factorizations $p = a_1c_1$ and $p = a_2c_2$ are called equivalent if there exists $u \in \mathscr{O}_{\overline{K}}$ such that $a_2 = u^{p-1}a_1$ and $c_2 = u^{1-p}c_1$.

Let $\lambda \in \mathscr{O}_{\overline{K}}$ with $0 \leq v_p(\lambda) \leq 1/(p-1)$. There exists a factorization $p = a(\lambda)c(\lambda)$ such that $G_\lambda \simeq G_{a(\lambda),c(\lambda)}$. More explicitly, we may take $c(\lambda) = \frac{(\lambda(1-p))^{p-1}}{w_{p-1}}$ and $a(\lambda) = \frac{p}{c(\lambda)}$, and we notice that $v_p(a(\lambda)) = 1 - (p-1)v_p(\lambda)$ is well defined independently of the factorization $p = a(\lambda)c(\lambda)$.

Lemma 8.2 ([3] Lemma 8.2 and 8.10)**.** *Let $0 < r \leq 1$ be a rational number and $\lambda \in \mathscr{O}_{\overline{K}}$ with $v_p(\lambda) \leq 1 - 1/p$ and $v_p(\lambda^{p-1}) \geq r$.*

(i) *Let ρ_r^λ be the morphism of groups schemes $\mathscr{G}_r^{(\lambda)} = \mathrm{Spec}\big(\mathscr{O}_{\overline{S}_t}[T]\big) \to \mathbb{G}_{a,r} = \mathrm{Spec}\big(\mathscr{O}_{\overline{S}_r}[X]\big)$ defined on the level of Hopf algebras by $X \mapsto \sum_{i=1}^{p-1}(-\lambda)^{i-1}\frac{T^i}{i}$. Then ρ_r^λ is an isomorphism. Moreover, the following diagram is commutative*

$$\begin{tikzcd}
\mathscr{G}_r^{(\lambda)} \arrow[r, "\phi_{\lambda,r}"] \arrow[d, "\rho_r^\lambda"'] & \mathscr{G}_r^{(\lambda^p)} \arrow[d, "\rho_r^{\lambda^p}"] \\
\mathbb{G}_{a,r} \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathbb{G}_{a,r},
\end{tikzcd}$$

where F *is the Frobenius homomorphism and $a(\lambda) \in \mathscr{O}_{\overline{K}}$ is introduced in* (8).

(ii) *Let $\delta_{\lambda,r}$ be the composed morphism $G_{\lambda,r} \xrightarrow{i} \mathscr{G}_r^{(\lambda)} \xrightarrow{\rho_r^\lambda} \mathbb{G}_{a,r}$. Then $\delta_{\lambda,r}$ generates* $\mathrm{Lie}(G_{\lambda,r}^\vee) \simeq \mathrm{Hom}_{\overline{S}_r}(G_{\lambda,r}, \mathbb{G}_{a,r})$ *as an $\mathscr{O}_{\overline{S}_r}$-module.*

Lemma 8.3 ([3] Lemma 8.3)**.** *Let $\lambda \in \mathscr{O}_{\overline{K}}$ with $\frac{1}{p(p-1)} \le v_p(\lambda) \le \frac{1}{p-1}$, and $r = (p-1)v_p(\lambda)$. Then the following diagram is commutative*

$$\begin{tikzcd}
\mathscr{G}_1^{(\lambda)} \arrow[rr, "\phi_{\lambda,1}"] \arrow[d, "\iota_{1,r}"'] & & \mathscr{G}_1^{(\lambda^p)} \arrow[d, "\rho_r^{\lambda^p}"] \\
\mathscr{G}_r^{(\lambda)} \arrow[r, "\rho_r^\lambda"] & \mathbb{G}_{a,r} \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathbb{G}_{a,1},
\end{tikzcd}$$

where $\iota_{1,r}$ is the reduction map.

8.4. Let $\lambda \in \mathscr{O}_{\overline{K}}$ with $v_p(\lambda) = \frac{1}{p}$, $t = 1 - 1/p$, and G be a commutative finite and flat group scheme killed by p over S. We define Φ_G to be

$$\Phi_G : \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \xrightarrow{\iota_t} \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, G_{\lambda,t}) \xrightarrow{\delta} \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) = \mathrm{Lie}(\overline{G}_t^\vee), \tag{8.4.1}$$

where ι_t is the canonical reduction map, and δ is the morphism induced by the element $\delta_{\lambda,t} \in \mathrm{Hom}_{\overline{S}_t}(G_{\lambda,t}, \mathbb{G}_{a,t})$ (8.2(ii)).

Proposition 8.5. *Let $\lambda \in \mathscr{O}_{\overline{K}}$ with $v_p(\lambda) = \frac{1}{p}$, $t = 1 - 1/p$, and G be a a Barsotti-Tate group of level 1 over S, satisfying the hypothesis of Theorem* 1.4*. Then we have an exact sequence*

$$0 \to \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \xrightarrow{\Phi_G} \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) \xrightarrow{\mathrm{F}-a(\lambda)} \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathbb{G}_{a,1}), \tag{8.5.1}$$

where $a(\lambda)$ is defined in 8.

Proof. From Lemma 8.3, we deduce a commutative diagram
(8.5.2)

$$\begin{tikzcd}
\mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, G_{\lambda,1}) \arrow[r] \arrow[d, "\iota_{1,t}"'] & \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathscr{G}_1^{(\lambda)}) \arrow[rr, "\phi_{\lambda,1}"] \arrow[d, "\iota'_{1,t}"'] & & \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathscr{G}_1^{(\lambda^p)}) \arrow[d, "\rho_1^{\lambda^p}"] \\
\mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, G_{\lambda,t}) \arrow[r] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathscr{G}_t^{(\lambda)}) \arrow[r, "\rho_t^\lambda"] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathbb{G}_{a,1}),
\end{tikzcd}$$

where the upper row is exact and $\iota_{1,t}$ and $\iota'_{1,t}$ are reduction maps. Therefore, the composition of Φ_G with the morphism $\mathrm{F}-a(\lambda)$ in (8.5.1) factorizes through the upper row of (8.5.2), and equals thus 0. Let L be the kernel of the map $\mathrm{F}-a(\lambda)$ in (8.5.1). Then Φ_G induces a map $\Phi' : \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \to L$. We have to prove that Φ' is an isomorphism.

Let d^* be the rank of $\mathrm{Lie}(\overline{G}_1^\vee) = \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathbb{G}_{a,1})$ over $\mathscr{O}_{\overline{S}_1}$, and recall that $v_p(a(\lambda)) = 1/p$. Since G satisfies the assumptions of Theorem 1.4, applying Prop. 3.12 to $\mathrm{Lie}(\overline{G}_1^\vee)$ and the operator $\mathrm{F} - a(\lambda)$, we see that the group L is an $\mathbb{F}_p$-vector space of dimension d^*. On the other hand, $\mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda)$ is identified with $G^{\frac{e}{p-1}+}(\overline{K})^\perp$ by Theorem 1.6. Thus it is also an $\mathbb{F}_p$-vector space of dimension d^* by Theorem 1.4(i). Therefore, to finish the proof, it suffices to prove that Φ' is surjective.

By Lemma 8.2(i), we have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "\alpha"'] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) \arrow[r, "\mathrm{F}-a(\lambda)"] \arrow[d, equal] & \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathbb{G}_{a,1}) \arrow[d, "\iota_{1,t}"] \\
0 \arrow[r] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, G_{\lambda,t}) \arrow[r] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}),
\end{tikzcd}$$

where $\iota_{1,t}$ is the reduction map. The composed morphism $\alpha \circ \Phi'$ is the canonical reduction map, whose injectivity will implies the injectivity of Φ'. Thus the following lemma will conclude the proof of the proposition. □

Lemma 8.6. *Assume that $p \geq 3$. Let $t = 1 - 1/p$, $\lambda \in \mathscr{O}_{\overline{K}}$ with $v_p(\lambda) = 1/p$, and G be a commutative finite flat group scheme killed by p over S. Then the reduction map*

$$\iota_t : \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \to \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, G_{\lambda,t})$$

is injective.

Proof. We put $G \times_S \overline{S} = \mathrm{Spec}(A)$, where A is a Hopf algebra over $\mathscr{O}_{\overline{K}}$ with the comultiplication Δ. An element $f \in \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda)$ is determined by an element $x \in A$ satisfying

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \lambda x \otimes x$$

$$P_\lambda(x) = \frac{(1+\lambda x)^p - 1}{\lambda^p} = 0. \tag{8.6.1}$$

Suppose that $\iota_t(f) = 0$, which means $x \in \mathfrak{m}_t A$. We want to prove that in fact $x = 0$. Let us write $x = \lambda^a y$ where $a \geq p - 1 \geq 2$ is an integer, and $y \in A$. Substituting x in (8.6.1), we obtain

$$(\lambda^a y)^p + \sum_{i=1}^{p-1} \frac{1}{\lambda^p} \binom{p}{i} \lambda^{i(a+1)} y^i = 0.$$

Since $v_p(\frac{1}{\lambda^p}\binom{p}{i}) = 0$ for $1 \leq i \leq p-1$ and A is flat over $\mathscr{O}_K$, we see easily that $y = \lambda^{a+1} y_1$ for some $y_1 \in A$. Continuing this process, we find that $x \in \cap_{a \in \mathbb{Q}_{>0}} \mathfrak{m}_a A = 0$ (1). □

Lemma 8.7. *Let G be a Barsotti-Tate group of level 1 and height h over S, and H be a flat closed subgroup scheme of G. We denote by d the dimension of $\mathrm{Lie}(G_s)$ over k, and $d^* = h - d$. Then the following conditions are equivalent :*

(i) *The special fiber H_s of H coincides with the kernel of the Frobenius of G_s.*
(i') *The special fiber $H_s^\perp$ of $H^\perp = (G/H)^\vee$ coincides with the kernel of the Frobenius of $G_s^\vee$.*
(ii) *H has rank p^d over S and* $\dim_k \mathrm{Lie}(H_s) \geq d$.
(ii') *$H^\perp$ has rank p^{d^*} over S and* $\dim_k \mathrm{Lie}(H_s^\perp) \geq d^*$.

Proof. We have two exact sequences

$$0 \to H \to G \to G/H \to 0$$
$$0 \to H^\perp \to G^\vee \to H^\vee \to 0.$$

Denote by $\mathfrak{F}_{G_s}$ (*resp.* by $\mathfrak{V}_{G_s}$) the Frobenius (*resp.* the Verschiebung) of G_s. Assume that (i) is satisfied, then we have $H_s^\vee = \mathrm{Coker}(\mathfrak{V}_{G_s^\vee})$ by duality. Since G is a Barsotti-Tate group of level 1, $H_s^\perp$ coincides with $\mathrm{Im}(\mathfrak{V}_{G_s^\vee}) = \mathrm{Ker}(\mathfrak{F}_{G_s^\vee})$. Conversely, if $H_s^\perp = \mathrm{Ker}(\mathfrak{F}_{G_s^\vee})$, we have also $H_s = \mathrm{Ker}(\mathfrak{F}_{G_s})$. This proves the equivalence of (i) and (i').

If (i) or (i') is satisfied, then (ii) and (ii') are also satisfied (SGA 3_1 $\mathrm{VII}_{\mathrm{A}}$ 7.4). Assume (ii) satisfied. Since $\mathrm{Ker}(\mathfrak{F}_{H_s})$ has rank $p^{\dim_k \mathrm{Lie}(H_s)}$ (*loc. cit.*) and is contained in both $\mathrm{Ker}(\mathfrak{F}_{G_s})$ and H_s, condition (ii) implies that these three groups have the same rank; hence they coincide. This proves that (ii) implies (i). The equivalence of (i') and (ii') is proved in the same way. □

8.8. *Proof of Theorem* 1.4(*ii*). By Lemma 8.7, the following lemma will complete the proof of 1.4(ii).

Lemma 8.9. *Let G be a Barsotti-Tate group of level 1 and height h over S, satisfying the hypothesis of Theorem* 1.4, *d be the dimension of* $\mathrm{Lie}(G_s^\vee)$ *over k, and $d^* = h - d$. Let H be the flat closed subgroup scheme $G^{\frac{e}{p-1}+}$, and $H^\perp = (G/H)^\vee$. Then $H^\perp$ has rank p^{d^*} over S and* $\dim_k \mathrm{Lie}(H_s^\perp) \geq d^*$.

Proof. Since H has rank p^d over S by 1.4(i), $H^\perp$ has rank p^{d^*} over S and $\dim_{\mathbb{F}_p}(G/H)(\overline{K}) = d^*$. Let $\lambda \in \mathscr{O}_{\overline{K}}$ with $v_p(\lambda) = 1/p$, and $t = 1 - 1/p$. The canonical projection $G \to G/H$ induces an injective homomorphism

$$\mathrm{Hom}_{\overline{S}}(\overline{G}/\overline{H}, G_\lambda) \to \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda). \tag{8.9.1}$$

By Theorem 1.6, $H^\perp(\overline{K})^{[\frac{e}{p}]} = \mathrm{Hom}_{\overline{S}}(\overline{G}/\overline{H}, G_\lambda)$ is orthogonal to $(G/H)^{\frac{e}{p-1}+}(\overline{K})$ under the perfect pairing $(G/H)(\overline{K}) \times H^\perp(\overline{K}) \to \mu_p(\overline{K})$. As $H = G^{\frac{e}{p-1}+}$, Prop. 2.8(ii) implies that the group scheme $(G/H)^{\frac{e}{p-1}+}$ is trivial. Hence we have

$$\dim_{\mathbb{F}_p} \mathrm{Hom}_{\overline{S}}(\overline{G}/\overline{H}, G_\lambda) = \dim_{\mathbb{F}_p} H^\perp(\overline{K}) = d^* = \dim_{\mathbb{F}_p} \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda),$$

and the canonical map (8.9.1) is an isomorphism. By the functoriality of Φ_G (8.4.1), we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\overline{S}}(\overline{G}/\overline{H}, G_\lambda) \arrow[r, equal] \arrow[d, "\Phi_{G/H}"] & \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \arrow[d, "\Phi_G"] \\
\mathrm{Lie}(\overline{H}_t^\perp) \arrow[r] & \mathrm{Lie}(\overline{G}_t^\vee)
\end{tikzcd} \tag{8.9.2}$$

where the lower row is an injective homomorphism of $\mathscr{O}_{\overline{S}_t}$-modules. Put $N_0 = \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda)$, $M = \mathrm{Lie}(\overline{G}_1^\vee)$ and $M_t = \mathrm{Lie}(\overline{G}_1^\vee) \otimes_{\mathscr{O}_{\overline{S}_1}} \mathscr{O}_{\overline{S}_t} = \mathrm{Lie}(\overline{G}_t^\vee)$. By 8.5(ii), N_0 is identified with the kernel of $\mathrm{F}-a(\lambda): M_t \to M$. Let N be the $\mathscr{O}_{\overline{K}}$-submodule of M_t generated by N_0. Applying 3.12(ii) to the morphism $\mathrm{F}-a(\lambda)$, we get

$$\dim_{\overline{k}}(N/\mathfrak{m}_{\overline{K}}N) = \dim_{\mathbb{F}_p} N_0 = d^*.$$

By (8.9.2), N is contained in $M' = \mathrm{Lie}(\overline{H}_t^{\perp}) \subset M$. By applying Lemma 8.10 (ii) below to $N \subset M'$, we obtain

$$d^* = \dim_{\overline{k}}(N/\mathfrak{m}_{\overline{K}}N) \leq \dim_{\overline{k}}(M'/\mathfrak{m}_{\overline{K}}M'). \tag{8.9.3}$$

Let $\omega_{\overline{H}_t^{\perp}}$ be the module of invariant differentials of $\overline{H}_t^{\perp}$ over $\mathscr{O}_{\overline{S}_t}$. Then we have $\omega_{H_{\overline{s}}^{\perp}} = \omega_{\overline{H}_t^{\perp}} \otimes_{\mathscr{O}_{\overline{S}_t}} \overline{k}$ and

$$M' = \mathrm{Lie}(\overline{H}_t^{\perp}) = \mathrm{Hom}_{\mathscr{O}_{\overline{S}_t}}(\omega_{\overline{H}_t^{\perp}}, \mathscr{O}_{\overline{S}_t}).$$

Applying Lemma 8.10 (i) to $\omega_{\overline{H}_t^{\perp}}$, we obtain

$$\dim_{\overline{k}}(M'/\mathfrak{m}_{\overline{K}}M') = \dim_{\overline{k}} \omega_{H_{\overline{s}}^{\perp}}. \tag{8.9.4}$$

From the relations $\mathrm{Lie}(H_s^{\perp}) \otimes_k \overline{k} = \mathrm{Lie}(H_{\overline{s}}^{\perp}) = \mathrm{Hom}_{\overline{k}}(\omega_{H_{\overline{s}}^{\perp}}, \overline{k})$, we deduce

$$\dim_{\overline{k}} \omega_{H_{\overline{s}}^{\perp}} = \dim_k \mathrm{Lie}(H_s^{\perp}). \tag{8.9.5}$$

The desired inequality $\dim_k \mathrm{Lie}(H_s^{\perp}) \geq d^*$ then follows from (8.9.3), (8.9.4) and (8.9.5).

□

Lemma 8.10. *Let t be a positive rational number, M be an $\mathscr{O}_{\overline{S}_t}$-module of finite presentation.*

(i) *Put $M^* = \mathrm{Hom}_{\mathscr{O}_{\overline{S}_t}}(M, \mathscr{O}_{\overline{S}_t})$. Then we have $\dim_{\overline{k}}(M^*/\mathfrak{m}_{\overline{K}}M^*) = \dim_{\overline{k}}(M/\mathfrak{m}_{\overline{K}}M)$.*

(ii) *If N is a finitely presented $\mathscr{O}_{\overline{S}_t}$-submodule of M, then $\dim_{\overline{k}}(N/\mathfrak{m}_{\overline{K}}N) \leq \dim_{\overline{k}}(M/\mathfrak{m}_{\overline{K}}M)$.*

Proof. Since M is of finite presentation, up to replacing K by a finite extension, we may assume that there exists a positive integer n and a finitely generated $\mathscr{O}_K/\pi^n\mathscr{O}_K$-module M_0, where π is a uniformizer of $\mathscr{O}_K$, such that $\mathscr{O}_{\overline{S}_t} = \mathscr{O}_{\overline{K}}/\pi^n\mathscr{O}_{\overline{K}}$ and $M = M_0 \otimes_{\mathscr{O}_K} \mathscr{O}_{\overline{K}}$. Note that there exist integers $0 < a_1 \leq \cdots a_r \leq n$ such that we have an exact sequence of $\mathscr{O}_K$-modules

$$0 \to \mathscr{O}_K^r \xrightarrow{\varphi} \mathscr{O}_K^r \to M_0 \to 0, \tag{8.10.1}$$

where φ is given by $(x_i)_{1\leq i\leq r} \mapsto (\pi^{a_i}x_i)_{1\leq i\leq r}$. In order to prove (i), it suffices to verify that $\dim_k(M_0^*/\pi M_0^*) = \dim_k(M_0/\pi M_0)$, where $M_0^* = \mathrm{Hom}_{\mathscr{O}_K}(M_0, \mathscr{O}_K/\pi^n\mathscr{O}_K)$. Let

$$(\mathscr{O}_K/\pi^n\mathscr{O}_K)^r \xrightarrow{\varphi_n} (\mathscr{O}_K/\pi^n\mathscr{O}_K)^r \to M_0 \to 0$$

be the reduction of (8.10.1) modulo π^n. Applying the functor $\mathrm{Hom}_{\mathscr{O}_K}(\_, \mathscr{O}_K/\pi^n\mathscr{O}_K)$ to the above exact sequence, we get

$$0 \to M_0 \to (\mathscr{O}_K/\pi^n\mathscr{O}_K)^r \xrightarrow{\varphi_n^*} (\mathscr{O}_K/\pi^n\mathscr{O}_K)^r$$

with $\varphi_n^* = \varphi_n$. Hence M_0^* is isomorphic to the submodule $\oplus_{i=1}^r(\pi^{n-a_i}\mathscr{O}_K/\pi^n\mathscr{O}_K)$ of $(\mathscr{O}_K/\pi^n\mathscr{O}_K)^r$, and we have

$$\dim_k(M_0^*/\pi M_0^*) = r = \dim_k(M_0/\pi M_0).$$

For statement (ii), by the same reasoning, we may assume that there exists a finite $\mathscr{O}_K$-submodule N_0 of M_0 such that $N = N_0 \otimes_{\mathscr{O}_K} \mathscr{O}_{\overline{K}}$.We need to prove that $\dim_k(N_0/\pi N_0) \leq \dim_k(M_0/\pi M_0)$. Let ${}_\pi M_0$ be the kernel of M_0 of the multiplication by π. We have an exact sequence of Artinian modules

$$0 \to {}_\pi M_0 \to M_0 \xrightarrow{\times\pi} M_0 \to M_0/\pi M_0 \to 0.$$

By the additivity of length of Artinian modules, we obtain $\dim_k({}_\pi M_0) = \dim_k(M_0/\pi M_0)$. Similarly, we have $\dim_k({}_\pi N_0) = \dim_k(N_0/\pi N_0)$. The assertion follows from the fact that ${}_\pi N_0$ is a submodule of ${}_\pi M_0$. □

Remark 8.11. *If we could prove the exact sequence (8.5.1) without knowing* a priori *the rank of* $\mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda)$ *for* $v_p(\lambda) = 1/p$, *then we would get another proof of the existence of the canonical subgroup of G. Since then, by Proposition 3.12 and (8.5.1),* $\mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda)$ *has* $\mathbb{F}_p$*-rank* d^* *under the assumptions of 1.4. Then we identify it to be a subgroup of* $G^\vee(\overline{K})$ *by* $\theta_\lambda(G)$ *(7.3.8), and define H to be the subgroup scheme of G determined by* $H(\overline{K})^\perp = \mathrm{Hom}_{\overline{S}}(G, G_\lambda)$. *The arguments in this section imply that H is the canonical subgroup of G. For abelian schemes, this approach is due to Andreatta-Gasbarri [3].*

References

[1] A. Abbes and A. Mokrane, Sous-groupes canoniques et cycles évanescents p-adiques pour les variétés abéliennes, *Publ. Math. Inst. Hautes Étud. Sci.* **99** (2004), 117-162.

[2] A. Abbes and T. Saito, Ramification of local fields with imperfect residue fields, *Am. J. Math.* **124** (2002), 879-920.

[3] F. Andreatta and C. Gasbarri, The canonical subgroup for families of abelian varieties, Preprint (2004).

[4] M. Artin, Algebraization of formal moduli, *Global analysis*, Univ. Tokyo Press (1969), 21-71.

[5] F. Berthelot, L. Breen and W. Messing, *Théorie de Dieudonné Cristalline II*, LNM **930**, Springer-Verlag, (1982).

[6] S. Bloch and K. Kato, p-adic étale cohomology, *Publ. Math. Inst. Hautes Étud. Sci.* **63** (1986), 107-152.

[7] B. Conrad, Higher-level canonical subgroups in abelian varieties, Preprint (2005).

[8] M. Demazure, Bidualité des schémas abéliens, in *Séminaire de géométrie algébrique*, Orsay, (1967-1968).

[9] B. Dwork, p-adic cycles, *Publ. Math. Inst. Hautes Étud. Sci.* **37** (1969), 27-115.

[10] G. Faltings and L. Chai, *Degeneration of abelian varieties*, Springer-Verlag (1990).

[11] A. Grothendieck, Le groupe de Brauer III, in *Dix exposés sur la cohomologie des schémas*, North-Holland (1968).

[12] L. Illusie, Déformations de groupes de Barsotti-Tate (d'après A. Grothendieck), *Astérisque* **127** (1985), 151-198.

[13] K. Kato, On p-adic vanishing cycles (Applications of ideas of Fontaine-Messing), *Adv. Stud. Pure Math.*, **10** (1987), 207-251.

[14] N. Katz, p-adic properties of modular schemes and modular forms, in *Modular functions of one variable III*, LNM **350**, Springer-Verlag, (1973).

[15] M. Kisin and K. F. Lai, Overconvergent Hilbert modular forms, *Amer. J. of Math.* **127** (2005), 735-783.

[16] J. Lubin, Finite subgroups and isogenies of one-parameter formal groups, *Ann. of Math.* **85**, 2nd series (1967), 296-302.

[17] B. Mazur and W. Messing, *Universal extensions and one dimensional crystalline cohomology*, LNM **370**, Springer-Verlag, (1974).

[18] D. Mumford, *Geometric invariant theory*, Springer-Verlag, (1965).

[19] M. Raynaud, Spécilisation du foncteur de Picard, *Publ. Math. Inst. Hautes Étud. Sci.* **38** (1970), 27-76.

[20] T. Sekiguchi, F. Oort and N. Suwa, On the deformation of Artin-Schreier to Kummer, *Ann. Sci. de l'É.N.S.* 4^e série, tome 22, No.3 (1989), 345-375.

[21] J. Tate and F. Oort, Group schemes of prime order, *Ann. Sci. de l'É.N.S.* 4^e série, tome 3, No. 1 (1970), 1-21.

p-ADIC MONODROMY OF THE UNIVERSAL DEFORMATION OF AN ELEMENTARY BARSOTTI-TATE GROUP

1 Introduction

1.1. Let k be an algebraically closed field of characteristic $p > 0$, S be a scheme over k, G be a Barsotti-Tate group over S of height h and dimension d. Let U be the ordinary locus of G (*i.e.* the open subscheme of S parametrizing the ordinary fibers of G), and assume that U is not empty. Let $\overline{\xi}$ be a geometric point of U, $G_U^{\text{ét}}$ be the maximal étale quotient of $G_U = G \times_S U$ over U. We denote by $G(n)$ (resp. $G_U^{\text{ét}}(n)$) the kernel of the multiplication by p^n on G (resp. $G_U^{\text{ét}}$) and by

$$\mathrm{T}_p(G, \overline{\xi}) = \varprojlim_n G(n)(\overline{\xi}) = \varprojlim_n G_U^{\text{ét}}(n)(\overline{\xi})$$

the Tate module of G at $\overline{\xi}$, which is a free $\mathbb{Z}_p$-module of rank $d^* = h - d$. The étale Barsotti-Tate group $G_U^{\text{ét}}$ over U gives rise to a continuous homomorphism

$$\rho_G : \pi_1(U, \overline{\xi}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G, \overline{\xi})) \simeq \mathrm{GL}_{d^*}(\mathbb{Z}_p). \tag{1.1.1}$$

We are interested in the monodromy of G, that is, the image of ρ_G. Motivated by a well known result of Igusa, it has been longly thought that when G is *versal*, its monodromy is as large as possible (and often that ρ_G is surjective), or at least that $\mathrm{Im}(\rho_G)$ contains an open subgroup of $\mathrm{GL}_{d^*}(\mathbb{Z}_p)$. In this paper, we prove that ρ_G is surjective when G is the universal deformation of the unique connected Barsotti-Tate group of height 3 and dimension 1.

1.2. This problem has been extensively studied in various settings. The first pioneering result is due to Igusa [15, 17] who proved that the monodromy homomorphism attached to a versal family of ordinary elliptic curves in characteristic p is surjective. Faltings and Chai [10] generalized this theorem to the moduli space of principally polarized abelian varieties of dimension g in characteristic p with a symplectic level n structure (n prime to p). We refer to [5] for other proofs of this result, and to Deligne-Ribet [6] and Hida [13] for other generalizations to some moduli spaces of PEL-type.

Though it is has been first formulated in a global setting, Igusa's theorem is purely local, and has got some local generalizations. Gross [11] extended it to one-dimensional formal A-modules over a complete discrete valuation ring of characteristic p, where A is the integral closure of $\mathbb{Z}_p$ in a finite extension of $\mathbb{Q}_p$. More recently, Achter and Norman [1] proved that for certain deformations of Barsotti-Tate groups, the p-adic monodromy representation has large image.

We should mention also the generalization of Ekedahl [9] to the jacobian of the universal n-pointed curve in characteristic p, equipped with a symplectic structure. His approach is inspired by Igusa's local proof, and has strongly inspired our work.

Finally, we would like to see our problem as an analogue in characteristic p of a famous result of Serre over number fields [18], namely, if an elliptic curve E over a number field has no complex multiplication, the Galois representation attached to its ℓ-adic Tate modules has an open image in $\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$, where ℓ runs over all prime numbers. Some ideas of this paper are inspired by Serre's method for studying Galois representations modulo p.

1.3. Let s, r be relatively prime integers such that $0 \leq s \leq r$ and $r \neq 0$, $\lambda = s/r$, G^{λ} be the Barsotti-Tate group over k with a monogenic Dieudonné module generated by an element e satisfying the relation $(F^{r-s} - V^{s}) \cdot e = 0$ (3.3). We call G^{λ} the *elementary Barsotti-Tate group of slope* λ over k; it has height r and dimension s. The terminology is justified by the fact that any Barsotti-Tate group over k is isogenous to a product of some G^{λ}'s. We notice that a connected Barsotti-Tate group over k of height h and dimension 1 is necessarily isomorphic to $G^{1/h}$ (3.5).

Let $\mathbf{S}^{\lambda}$ be the "algebraic" local moduli in characteristic p of G^{λ}, $\mathbf{G}^{\lambda}$ be the "algebraic" universal deformation of G^{λ} over $\mathbf{S}^{\lambda}$. The scheme $\mathbf{S}^{\lambda}$ is affine of ring $R \simeq k[[(t_{i,j})_{1 \leq i \leq r-s, 1 \leq j \leq s}]]$, and the Barsotti-Tate group $\mathbf{G}^{\lambda}$ is obtained by algebraizing the "formal" universal deformation of G^{λ} over $\mathrm{Spf}(R)$ (cf. 4.5 and 4.7). Let $\mathbf{U}^{\lambda}$ be the ordinary locus of $\mathbf{G}^{\lambda}$ (*i.e.* the open subscheme of $\mathbf{S}^{\lambda}$ parametrizing the ordinary fibers of $\mathbf{G}^{\lambda}$); it is the complement in $\mathbf{S}^{\lambda}$ of a divisor defined by a regular parameter of R (4.13). Let $\overline{\xi}$ be a geometric point over the generic point ξ of $\mathbf{U}^{\lambda}$. We consider the monodromy representation

$$(1.3.2) \qquad \rho^{\lambda} : \pi_1(\mathbf{U}^{\lambda}, \overline{\xi}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G}^{\lambda}, \overline{\xi})) \simeq \mathrm{GL}_{r-s}(\mathbb{Z}_p)$$

associated to $\mathbf{G}^{\lambda}$ (1.1.1). Inspired by a well known result of Igusa [15, 17], we conjecture the following :

Conjecture 1.4. *For any rational number $\lambda \in (0,1)$, the homomorphism ρ^{λ} is surjective.*

Though it has been formulated in a global setting, Igusa's theorem mentioned above corresponds to the case $\lambda = 1/2$; then $\mathbf{S}^{1/2} = \mathrm{Spec}(k[[t]])$ and the ordinary locus $\mathbf{U}^{1/2}$ is reduced to the generic point ξ of $\mathbf{S}^{1/2}$. Let K be the fraction field of $R = k[[t]]$, K^{sep} be a separable closure of K, $\overline{\xi}$ be the associated geometric generic point of $\mathbf{S}^{1/2}$. The monodromy homomorphism (1.3.2) is reduced to a Galois representation

$$\rho^{1/2} : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G}^{1/2}, \overline{\xi})) \simeq \mathbb{Z}_p^{\times}.$$

Theorem 1.5 (Igusa, [17] Thm. 4.3). *Conjecture* 1.4 *is true for* $\lambda = 1/2$.

In section 5, we will reformulate this theorem in a slightly more general form (5.14), and reprove it following [17].

1.6. In this paper, we consider the case $\lambda = 1/3$; then $\mathbf{S}^{1/3} = \mathrm{Spec}(R)$ with $R = k[[t_1, t_2]]$, and $\mathbf{U}^{1/3} = \mathrm{Spec}(R[1/t_1])$. The following theorem is our main result, and will be ultimately proved in section 7.

Theorem 1.7. *Conjecture* 1.4 *is true for* $\lambda = 1/3$, *i.e. the homomorphism*

$$\rho^{1/3} : \pi_1(\mathbf{U}^{1/3}, \overline{\xi}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G}^{1/3}, \overline{\xi})) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

is surjective.

1.8. For a general slope λ, we denote by

$$(1.8.1) \qquad \overline{\rho}^{\lambda} : \pi_1(\mathbf{U}^{\lambda}, \overline{\xi}) \to \mathrm{Aut}_{\mathbb{F}_p}\big(\mathrm{T}_p(\mathbf{G}^{\lambda}, \overline{\xi})/p\mathrm{T}_p(\mathbf{G}^{\lambda}, \overline{\xi})\big) \simeq \mathrm{GL}_{r-s}(\mathbb{F}_p)$$

the canonical reduction modulo p of ρ^{λ}. Then we have the following partial results on $\overline{\rho}^{\lambda}$.

Proposition 1.9. (a) *The group* $\mathrm{Im}(\overline{\rho}^\lambda)$ *contains a subgroup* H *of* $\mathrm{GL}_{r-s}(\mathbb{F}_p)$ *such that the subset* $H \cup \{0\}$ *of the matrix algebra* $\mathrm{M}_{(r-s)\times(r-s)}(\mathbb{F}_p)$ *is a finite field with* p^{r-s} *elements.*

(b) *The order of* $\mathrm{Im}(\overline{\rho}^\lambda)$ *is divisible by* p^{r-s-1}*.*

(c) *If* $r - s = 2$*, the homomorphism* $\overline{\rho}^\lambda$ *is surjective.*

This proposition will be proved in section 7.

1.10. Let $A = k[[\pi]]$ be the ring of formal power series over k in one variable π, K be the fraction field of A, v be the valuation on K normalized by $\mathrm{v}(\pi) = 1$. Let $\overline{K}$ be an algebraical closure of K, K^{sep} be the separable closure of K contained in $\overline{K}$, I be the Galois group of K^{sep} over K, $I_p \subset I$ be the wild inertia subgroup, $I_t = I/I_p$ be the tame inertia group. Recall that for every integer $n \geq 1$, there is a canonical surjective character $\theta_{p^n-1} : I_t \to \mathbb{F}_{p^n}^\times$ (5.2), where $\mathbb{F}_{p^n}$ is the finite subfield of k with p^n elements.

We put $S = \mathrm{Spec}(A)$. Let G be a Barsotti-Tate group over S, $G^\vee$ be the Serre dual of G, $\mathrm{Lie}(G^\vee)$ be its sheaf of Lie algebras. The Hasse-Witt map of G, denoted by HW_G, is the semi-linear endomorphism on $\mathrm{Lie}(G^\vee)$ induced by the Frobenius homomorphism of G (2.7.2). We define $hw(G)$ to be the π-adic valuation of the determinant of a matrix of HW_G, and call it the *Hasse invariant* of G (5.4).

Proposition 1.11. *Let* r, s *be relatively prime integers with* $0 < s < r$*,* $\lambda = s/r$*, and* G^λ *the elementary Barsotti-Tate group over* k *of slope* λ*. Let* G *be a deformation of* G^λ *over* S *with* $hw(G) = 1$*, and* $G(1)$ *be the kernel of the multiplication by* p *on* G*. Then the action of* I *on* $G(1)(\overline{K})$ *is tame;* $G(1)(\overline{K})$ *is an* $\mathbb{F}_{p^{r-s}}$*-vector space of dimension* 1 *on which the induced action of* I_t *is given by the surjective character* $\theta_{p^{r-s}-1} : I_t \to \mathbb{F}_{p^{r-s}}^\times$*.*

This proposition is an analogue of ([18] Prop. 9) in characteristic p, and will be proved in (5.12).

1.12. The paper is organized as follows. In section 2, we review some well known facts on ordinary Barsotti-Tate groups. Section 3 contains some preliminaries on the classical Dieudonné theory. In section 4, after recalling the general deformation theory of a Barsotti-Tate group over k, we compute the Hasse-Witt map of the universal deformation of G^λ (4.12). Section 5, which is the heart of the paper, is dedicated to the study of the monodromy of a Barsotti-Tate group over a complete trait. Section 6 is elementary, and contains a criterion (6.3) for the surjectivity of a homomorphism from a profinite group to $\mathrm{GL}_2(\mathbb{Z}_p)$. In section 7, we gather the results of previous sections to complete the proof of 1.7 and 1.9.

1.13. This paper is a part of the author's thesis at University Paris 13. The author would like to express his great gratitude to his thesis advisor Prof. A. Abbes for his encouragement during this work, and also for his various helpful instructions and comments on earlier versions of this paper.

1.14. Notations Let S be a scheme of characteristic $p > 0$. A *BT-group* over S stands for a Barsotti-Tate group over S. Let G be a commutative finite group scheme (*resp.* a BT-group) over S. We denote by $G^\vee$ its Cartier dual (*resp.* its Serre dual), by ω_G the sheaf of invariant differentials of G over S, and by $\mathrm{Lie}(G)$ the sheaf of Lie algebras of G. We put $G^{(p)}$ the pull-back of G by the absolute Frobenius of S, $F_G \colon G \to G^{(p)}$ the Frobenius homomorphism and $V_G \colon G^{(p)} \to G$ the Verschiebung homomorphism. If G is a BT-group and n an integer ≥ 1, we denote by $G(n)$ the kernel of the multiplication by p^n on G; we have $G^\vee(n) = (G^\vee)(n)$ by definition.

Starting from section 3, k will denote an algebraically closed field of characteristic $p > 0$, $W(k)$ the ring of Witt vectors with coefficients in k, and K_0 the fraction field of $W(k)$. We denote abusively by the same letter σ the Frobenius homomorphisms of k, $W(k)$ and K_0. Let A be one of the following rings k, $W(k)$ or K_0, and let M be a A-module. We denote by $M^{(p)}$ or M^σ the module $A\otimes_\sigma M$, *i.e.* we have $1\otimes(\lambda m)=\sigma(\lambda)\otimes m$ in $A\otimes_\sigma M$ for all $\lambda\in A$ and $m\in M$. We notice that, since k is algebraically closed, the natural inclusion $M\to M^\sigma$ given by $x\mapsto 1\otimes x$ is bijective.

2 Review of ordinary Barsotti-Tate groups

In this section, S denotes a scheme of characteristic $p>0$.

2.1. Let G be a commutative group scheme, locally free of finite type over S. We have a canonical isomorphism of coherent $\mathscr{O}_S$-modules ([14] 2.1)

$$\text{(2.1.1)}\qquad \mathrm{Lie}(G^\vee)\simeq \mathscr{H}om_{S_{\mathrm{fppf}}}(G,\mathbb{G}_a),$$

where $\mathscr{H}om_{S_{\mathrm{fppf}}}$ is the sheaf of homomorphisms in the category of abelian fppf-sheaves over S, and $\mathbb{G}_a$ is the additive group scheme. The Frobenius homomorphism of $\mathbb{G}_a$ induces an endomorphism

$$\text{(2.1.2)}\qquad \mathrm{HW}_G:\mathrm{Lie}(G^\vee)\to\mathrm{Lie}(G^\vee),$$

semi-linear with respect to the absolute Frobenius map $F_S:\mathscr{O}_S\to\mathscr{O}_S$, called the ***Hasse-Witt*** map of G. More precisely, if $f:G\to\mathbb{G}_a$ be an element of $\mathrm{Lie}(G^\vee)$, then $\mathrm{HW}_G(f)$ is the composed homomorphism $F_{\mathbb{G}_a}\circ f:G\to\mathbb{G}_a^{(p)}=\mathbb{G}_a$. By the functoriality of the Frobenius, we have also $\mathrm{HW}_G(f)=f^{(p)}\circ F_G$, where $f^{(p)}:G^{(p)}\to\mathbb{G}_a^{(p)}$ is the base change of f by the absolute Frobenius of S, *i.e.* the following diagram is commutative :

$$\begin{tikzcd} G \arrow[r, "F_G"] \arrow[d, "f"'] & G^{(p)} \arrow[d, "f^{(p)}"] \\ \mathbb{G}_a \arrow[r, "F_{\mathbb{G}_a}"] & \mathbb{G}_a^{(p)}. \end{tikzcd}$$

2.2. By a *commutative p-Lie algebra* over S, we mean a pair (L,φ), where L is a locally free sheaf of finite type over S, and $\varphi:L\to L$ is a semi-linear endomorphism with respect to the absolute Frobenius $F_S:\mathscr{O}_S\to\mathscr{O}_S$. When there is no risk of confusion, we omit φ from the notation. We denote by p-$\mathfrak{Lie}_S$ the category of commutative p-Lie algebras over S.

Let (L,φ) be an object of p-$\mathfrak{Lie}_S$, and $L^{(p)}=\mathscr{O}_S\otimes_{\{\mathscr{O}_S,F_S\}}L$ be the twist of L by the absolute Frobenius of $\mathscr{O}_S$, *i.e.* if λ and x are local sections of $\mathscr{O}_S$ and L respectively, we have $1\otimes(\lambda\cdot x)=\lambda^p\otimes x$. We define the *linearization of* φ to be the $\mathscr{O}_S$-linear homomorphism

$$\text{(2.2.3)}\qquad \Phi:L^{(p)}\to L$$

given by $\lambda\otimes x\mapsto\lambda\varphi(x)$. We notice that, in general, the canonical map $L\to L^{(p)}$ given by $x\mapsto 1\otimes x$ is neither injective nor surjective.

For an object L of p-$\mathfrak{Lie}_S$, we put

$$\mathscr{U}(L)=\mathrm{Sym}(L)=\oplus_{n\in\mathbb{N}}\,L^{\otimes n},$$

where $L^{\otimes 0} = \mathscr{O}_S$. Let $\mathscr{I}_p(L)$ be the ideal sheaf of $\mathscr{U}(L)$ defined, for an open subset $V \subset S$, by

$$\Gamma(V, \mathscr{I}_p(L)) = \{x^{\otimes p} - \varphi(x) \ ; \ x \in \Gamma(V, \mathscr{U}(L))\}.$$

We put $\mathscr{U}_p(L) = \mathscr{U}(L)/\mathscr{I}_p(L)$, and call it the *p-enveloping algebra of L*. We endow $\mathscr{U}_p(L)$ with the structure of a Hopf-algebra with the comultiplication given by $\Delta(x) = 1 \otimes x + x \otimes 1$ and the coinverse given by $i(x) = -x$.

Let G be a commutative group scheme, locally free of finite type over S. We say that G is *of coheight one* if the Verschiebung $V : G^{(p)} \to G$ is the zero homomorphism. We denote the category of such objects by $\mathfrak{G}\mathrm{V}_S$. For an object G of $\mathfrak{G}\mathrm{V}_S$, the Frobenius $F_{G^\vee}$ of the Cartier dual $G^\vee$ of G is the zero homomorphism; so the Lie algebra $\mathrm{Lie}(G^\vee)$ is locally free of finite type over S ([8] $\mathrm{VII_A}$ Théo. 7.4(iii)). The Hasse-Witt map of G (2.1.2) endows $\mathrm{Lie}(G^\vee)$ with a commutative p-Lie algebra structure over S.

Proposition 2.3 ([8] $\mathrm{VII_A}$, Théo. 7.2 et 7.4). *The functor $\mathfrak{G}\mathrm{V}_S \to p\text{-}\mathfrak{Lie}_S$ defined by $G \mapsto \mathrm{Lie}(G^\vee)$ is an anti-equivalence of categories; a quasi-inverse is given by the functor $p\text{-}\mathfrak{Lie}_S \to \mathfrak{G}\mathrm{V}_S$ defined by $(L, \varphi) \mapsto \mathrm{Spec}(\mathscr{U}_p(L))$.*

2.4. Assume $S = \mathrm{Spec}(A)$ affine. Let (L, φ) be an object of $p\text{-}\mathfrak{Lie}_S$ such that L is free of rank n over $\mathscr{O}_S$, $(e_1, \cdots, e_n)$ be a basis of L over $\mathscr{O}_S$, $(h_{ij})_{1\leq i,j\leq n}$ be the matrix of φ under the basis $(e_1, \cdots, e_n)$, *i.e.* $\varphi(e_j) = \sum_{i=1}^n h_{ij}e_i$ for $1 \leq j \leq n$. Then the group scheme associated to (L, φ) is explicitly given by

$$\mathrm{Spec}(\mathscr{U}_p(L)) = \mathrm{Spec}\Big(A[X_1, \cdots, X_n]/(X_j^p - \sum_{i=1}^n h_{ij}X_i)_{1\leq j\leq n}\Big),$$

with the comultiplication $\Delta(X_j) = 1 \otimes X_j + X_j \otimes 1$. By the Jacobian criterion of étaleness [EGA IV_0 22.6.7], the finite group scheme $\mathrm{Spec}(\mathscr{U}_p(L))$ is étale over S if and only if the matrix $(h_{ij})_{1\leq i,j\leq n}$ is invertible. This condition is equivalent to requiring that the linearization of φ (2.2.3) is universally injective.

Corollary 2.5. *An object G of $\mathfrak{G}\mathrm{V}_S$ is étale over S, if and only if the linearization of its Hasse-Witt map* (2.1.2) *is universally injective.*

Proof. The problem being local over S, we may assume S affine and $L = \mathrm{Lie}(G^\vee)$ free over $\mathscr{O}_S$. By Theorem 2.3, G is isomorphic to $\mathrm{Spec}(\mathscr{U}_p(L))$, and we conclude by the last remark of 2.4. □

Definition 2.6. *Let G be a BT-group over S. We say that G is* ordinary *if there exists an exact sequence of BT-groups over S*

$$0 \to G^{\mathrm{mult}} \to G \to G^{\mathrm{\acute{e}t}} \to 0, \tag{2.6.1}$$

such that G^{mult} is multiplicative and $G^{\mathrm{\acute{e}t}}$ is étale BT-group.

We note that when it exists, the exact sequence (2.6.1) is unique up to a unique isomorphism, since there is no non-trivial homomorphisms from a multiplicative BT-group to an étale one. The property of being ordinary is clearly stable by base change.

If S is the spectrum of a field, we have *a priori* an exact sequence of the form $0 \to G^\circ \to G \to G^{\mathrm{\acute{e}t}} \to 0$, where G° is merely a connected BT-group and $G^{\mathrm{\acute{e}t}}$ is an étale BT-group ([7] Chap.II, §7). Therefore, G is ordinary if and only if its connected part G° is of multiplicative type.

2.7. Let G be a BT-group over S of height h and dimension d. The Lie algebra $\mathrm{Lie}(G^\vee)$ is locally free of rank $(h-d)$ over S, and canonically identified with $\mathrm{Lie}(G^\vee(1))$([3] 3.3.2). We define the *Hasse-Witt map* of G

$$\mathrm{HW}_G : \mathrm{Lie}(G^\vee) \to \mathrm{Lie}(G^\vee) \tag{2.7.2}$$

to be the Hasse-Witt map of $G(1)$ (2.1.2).

Proposition 2.8. *Let G be a BT-group over S. The following conditions are equivalent :*
(a) *G is ordinary over S.*
(b) *For every $x \in S$, the fiber $G_x = G \otimes_S \kappa(x)$ is ordinary over $\kappa(x)$, .*
(c) *The finite group scheme $\mathrm{Ker}\, V_G$ is étale over S.*
(c') *The finite group scheme $\mathrm{Ker}\, F_G$ is of multiplicative type over S.*
(d) *The linearization of the Hasse-Witt map HW_G of G is universally injective.*

First, we prove the following lemmas.

Lemma 2.9. *Let T be a scheme, H be a commutative group scheme locally free of finite type over T. Then H is étale (*resp. *of multiplicative type) over T if and only if, for every $x \in T$, the fiber $H \otimes_T \kappa(x)$ is étale (*resp. *of multiplicative type) over $\kappa(x)$.*

Proof. We will consider only the étale case; the multiplicative case follows by duality. Since H is T-flat, it is étale over T if and only if it is unramified over T. By [EGA IV 17.4.2], this condition is equivalent to that for every point $x \in T$, the fiber $H \otimes_T \kappa(x)$ is unramified over $\kappa(x)$, hence the conclusion. □

Lemma 2.10. *Let G be a BT-group over S. Then $\mathrm{Ker}\, V_G$ is an object of the category $\mathfrak{G}\mathrm{V}_S$,* i.e. *it is locally free of finite type over S, and its Verschiebung is the zero homomorphism. Moreover, we have a canonical isomorphism $(\mathrm{Ker}\, V_G)^\vee \simeq \mathrm{Ker}\, F_{G^\vee}$, which induces an isomorphism of Lie algebras $\mathrm{Lie}\big((\mathrm{Ker}\, V_G)^\vee\big) \simeq \mathrm{Lie}(\mathrm{Ker}\, F_{G^\vee}) = \mathrm{Lie}(G^\vee)$, and the Hasse-Witt map* (2.1.2) *of $\mathrm{Ker}\, V_G$ is identified with HW_G* (2.7.2)*.*

Proof. The group scheme $\mathrm{Ker}\, V_G$ is locally free of finite type over S ([14] 1.3(b)), and we have a commutative diagram

$$\begin{tikzcd}
(\mathrm{Ker}\, V_G)^{(p)} \arrow[r, "V_{\mathrm{Ker}\, V_G}"] \arrow[d, hook] & \mathrm{Ker}\, V_G \arrow[d, hook] \\
(G^{(p)})^{(p)} \arrow[r, "V_{G^{(p)}}"] & G^{(p)}.
\end{tikzcd}$$

By the functoriality of Verschiebung, we have $V_{G^{(p)}} = (V_G)^{(p)}$ and $\mathrm{Ker}\, V_{G^{(p)}} = (\mathrm{Ker}\, V_G)^{(p)}$. Hence the composition of the left vertical arrow with $V_{G^{(p)}}$ vanishes, and the Verschiebung of $\mathrm{Ker}\, V_G$ is zero.

By Cartier duality, we have $(\mathrm{Ker}\, V_G)^\vee = \mathrm{Coker}(F_{G^\vee(1)})$. Moreover, the exact sequence

$$\cdots \to G^\vee(1) \xrightarrow{F_{G^\vee(1)}} \big(G^\vee(1)\big)^{(p)} \xrightarrow{V_{G^\vee(1)}} G^\vee(1) \to \cdots,$$

induces a canonical isomorphism

$$\mathrm{Coker}(F_{G^\vee(1)}) \xrightarrow{\sim} \mathrm{Im}(V_{G^\vee(1)}) = \mathrm{Ker}\, F_{G^\vee(1)} = \mathrm{Ker}\, F_{G^\vee}. \tag{2.10.1}$$

Hence, we deduce that

$$(\mathrm{Ker}\, V_G)^\vee \simeq \mathrm{Coker}(F_{G^\vee(1)}) \xrightarrow{\sim} \mathrm{Ker}\, F_{G^\vee} \hookrightarrow G^\vee(1). \tag{2.10.2}$$

Since the natural injection $\mathrm{Ker}\, F_{G^\vee} \to G^\vee(1)$ induces an isomorphism of Lie algebras, we get

$$\mathrm{Lie}\big((\mathrm{Ker}\, V_G)^\vee\big) \simeq \mathrm{Lie}(\mathrm{Ker}\, F_{G^\vee}) = \mathrm{Lie}(G^\vee(1)) = \mathrm{Lie}(G^\vee). \tag{2.10.3}$$

It remains to prove the compatibility of the Hasse-Witt maps with (2.10.3). We note that the dual of the morphism (2.10.2) is the canonical map $F : G(1) \to \mathrm{Ker}\, V_G = \mathrm{Im}(F_{G(1)})$ induced by $F_{G(1)}$. Hence by (2.1.1), the isomorphism (2.10.3) is identified with the functorial map

$$\mathscr{H}om_{S_{\mathrm{fppf}}}(\mathrm{Ker}\, V_G, \mathbb{G}_a) \to \mathscr{H}om_{S_{\mathrm{fppf}}}(G(1), \mathbb{G}_a)$$

induced by F, and its compatibility with the Hasse-Witt maps follows easily from the definition (2.1.2). □

Proof of 2.8. (a)⇒(b). Indeed, the ordinarity of G is stable by base change.

(b)⇒(c). By Lemma 2.9, it suffices to verify that for every point $x \in S$, the fiber $(\mathrm{Ker}\, V_G) \otimes_S \kappa(x) \simeq \mathrm{Ker}\, V_{G_x}$ is étale over $\kappa(x)$. Since G_x is assumed to be ordinary, its connected part $(G_x)^\circ$ is multiplicative. Hence, the Verschiebung of $(G_x)^\circ$ is an isomorphism, and $\mathrm{Ker}\, V_{G_x}$ is canonically isomorphic to $\mathrm{Ker}\, V_{(G_x)^{\text{ét}}} \subset (G_x)^{\text{ét}}$, so our assertion follows.

(*c*) ⇔ (*d*). It follows immediately from Lemma 2.10 and Corollary 2.5.

(c)⇔(c'). By 2.9, we may assume that S is the spectrum of a field. So the category of commutative finite group schemes over S is abelian. We will just prove (c)⇒(c'); the converse can be proved by duality. We have a fundamental short exact sequence of finite group schemes

$$0 \to \mathrm{Ker}\, F_G \to G(1) \xrightarrow{F} \mathrm{Ker}\, V_G \to 0, \tag{2.10.4}$$

where F is induced by $F_{G(1)}$. This induces a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \big(\mathrm{Ker}\, F_G\big)^{(p)} \arrow[r] \arrow[d, "V'"] & \big(G(1)\big)^{(p)} \arrow[r, "F^{(p)}"] \arrow[d, "V_{G(1)}"] & \big(\mathrm{Ker}\, V_G\big)^{(p)} \arrow[r] \arrow[d, "V''"] & 0 \\
0 \arrow[r] & \mathrm{Ker}\, F_G \arrow[r] & G(1) \arrow[r, "F"] & \mathrm{Ker}\, V_G \arrow[r] & 0
\end{tikzcd}$$

where vertical arrows are the Verschiebung homomorphisms. We have seen that $V'' = 0$ (2.10). Therefore, by the snake lemma, we have a long exact sequence

$$0 \to \mathrm{Ker}\, V' \to \mathrm{Ker}\, V_{G(1)} \xrightarrow{\alpha} \big(\mathrm{Ker}\, V_G\big)^{(p)} \to \mathrm{Coker}\, V' \to \mathrm{Coker}\, V_{G(1)} \xrightarrow{\beta} \mathrm{Ker}\, V_G \to 0, \tag{2.10.5}$$

where the map α is the Frobenius of $\mathrm{Ker}\, V_G$ and β is the composed isomorphism

$$\mathrm{Coker}(V_{G(1)}) \simeq G(1)/\,\mathrm{Ker}\, F_{G(1)} \xrightarrow{\sim} \mathrm{Im}(F_{G(1)}) \simeq \mathrm{Ker}\, V_G.$$

Then condition (c) is equivalent to that α is an isomorphism ; it implies that $\mathrm{Ker}\, V' = \mathrm{Coker}\, V' = 0$, *i.e.* the Verschiebung of $\mathrm{Ker}\, F_G$ is an isomorphism, and hence (c').

(c)⇒(a). For every integer $n > 0$, we denote by F_G^n the composed homomorphism

$$G \xrightarrow{F_G} G^{(p)} \xrightarrow{F_{G^{(p)}}} \cdots \xrightarrow{F_{G^{p^{n-1}}}} G^{(p^n)},$$

and by V_G^n the composed homomorphism

$$G^{(p^n)} \xrightarrow{V_{G^{p^{n-1}}}} G^{(p^{n-1})} \xrightarrow{V_{G^{(p^{n-2})}}} \cdots \xrightarrow{V_G} G;$$

F_G^n and V_G^n are isogenies of BT-groups. From the relation $V_G^n \circ F_G^n = p^n$, we deduce an exact sequence

$$0 \to \mathrm{Ker}\, F_G^n \to G(n) \xrightarrow{F^n} \mathrm{Ker}\, V_G^n \to 0, \tag{2.10.6}$$

where F^n is induced by F_G^n. For $1 \leq j < n$, we have a commutative diagram

$$\begin{tikzcd} G^{(p^n)} \arrow[rr, "V^{n-j}_{G^{(p^j)}}"] \arrow[dr, "V_G^n"'] & & G^{(p^j)} \arrow[dl, "V_G^j"] \\ & G. & \end{tikzcd} \tag{2.10.7}$$

One notices by the functoriality of Verschiebung that $\mathrm{Ker}\, V^{n-j}_{G^{(p^j)}} = (\mathrm{Ker}\, V_G^{n-j})^{(p^j)}$. Since all maps in (2.10.7) are isogenies, we have an exact sequence

$$0 \to (\mathrm{Ker}\, V_G^{n-j})^{(p^j)} \xrightarrow{i'_{n-j,n}} \mathrm{Ker}\, V_G^n \xrightarrow{p_{n,j}} \mathrm{Ker}\, V_G^j \to 0. \tag{2.10.8}$$

Therefore, condition (c) implies by induction that $\mathrm{Ker}\, V_G^n$ is an étale group scheme over S. The j-th iteration of the Frobenius $\mathrm{Ker}\, V_G^{n-j} \to (\mathrm{Ker}\, V_G^{n-j})^{(p^j)}$ is therefore an isomorphism, and $\mathrm{Ker}\, V_G^{n-j}$ is identified with a subgroup scheme of $\mathrm{Ker}\, V_G^n$ by the composed map

$$i_{n-j,n}: \ \mathrm{Ker}\, V_G^{n-j} \xrightarrow{\sim} (\mathrm{Ker}\, V_G^{n-j})^{(p^j)} \xrightarrow{i'_{n-j,n}} \mathrm{Ker}\, V_G^n.$$

We claim that the kernel of the multiplication by p^{n-j} on $\mathrm{Ker}\, V_G^n$ is $\mathrm{Ker}\, V_G^{n-j}$. Indeed, from the relation $p^{n-j} \cdot \mathrm{Id}_{G^{(p^n)}} = F^{n-j}_{G^{(p^j)}} \circ V^{n-j}_{G^{(p^j)}}$, we deduce a commutative diagram (without dotted arrows)

$$\begin{tikzcd} \mathrm{Ker}\, V_G^n \arrow[rr] \arrow[dr, dashed, "p_{n,j}"] \arrow[dd, "p^{n-j}"'] & & G^{(p^n)} \arrow[dr, "V^{n-j}_{G^{(p^j)}}"] \arrow[dd, "p^{n-j}"'] & \\ & \mathrm{Ker}\, V_G^j \arrow[rr, dashed] \arrow[dl, dashed, "i_{j,n}"] & & G^{(p^j)} \arrow[dl, "F^{n-j}_{G^{(p^j)}}"] \\ \mathrm{Ker}\, V_G^n \arrow[rr] & & G^{(p^n)}. & \end{tikzcd} \tag{2.10.9}$$

It follows from (2.10.8) that the subgroup $\mathrm{Ker}\, V_G^n$ of $G^{(p^n)}$ is sent by $V^{n-j}_{G^{(p^j)}}$ onto $\mathrm{Ker}\, V_G^j$. Therefore diagram (2.10.9) remains commutative when completed by the dotted arrows, hence our claim. It follows from the claim that $(\mathrm{Ker}\, V_G^n)_{n \geq 1}$ constitutes an étale BT-group over S, denoted by $G^{\text{ét}}$. By duality, we have an exact sequence

$$0 \to \mathrm{Ker}\, F_G^j \to \mathrm{Ker}\, F_G^n \to (\mathrm{Ker}\, F_G^{n-j})^{(p^j)} \to 0. \tag{2.10.10}$$

Condition (c') implies by induction that $\operatorname{Ker} F_G^n$ is of multiplicative type. Hence the j-th iteration of Verschiebung $(\operatorname{Ker} F_G^{n-j})^{(p^j)} \to \operatorname{Ker} F_G^{n-j}$ is an isomorphism. We deduce from (2.10.10) that $(\operatorname{Ker} F_G^n)_{n\geq 1}$ form a multiplicative BT-group over S that we denote by G^{mult}. Then the exact sequences (2.10.6) give a decomposition of G of the form (2.6.1). □

Corollary 2.11. *Let G be a BT-group over S, and S^{ord} be the locus in S of the points $x \in S$ such that $G_x = G \otimes_S \kappa(x)$ is ordinary over $\kappa(x)$. Then S^{ord} is open in S, and the canonical injection $S^{\mathrm{ord}} \to S$ is affine.*

The open subscheme S^{ord} of S is called the *ordinary locus* of G.

3 Review of classical Dieudonné theory

3.1. Let k be an algebraically closed field of characteristic $p > 0$, $W(k)$ be the ring of Witt vectors with coefficients in k, $\mathcal{D}$ be the *Dieudonné ring $\mathcal{D}$ over k*, *i.e.* the noncommutative ring $W(k)\{F, V\}$ over $W(k)$, generated by two variables F and V satisfying the following relations

$$F \cdot \lambda = \sigma(\lambda) \cdot F, \qquad V \cdot \lambda = \sigma^{-1}(\lambda) \cdot V, \quad F \cdot V = V \cdot F = p,$$

where $\lambda \in W(k)$ and σ is the Frobenius endomorphism of $W(k)$.

By a *Dieudonné module over k*, we mean a left $\mathcal{D}$-module M which is finitely generated as a $W(k)$-module. Equivalently, a Dieudonné module M over k is a $W(k)$-module of finite type endowed with two morphisms of $W(k)$-modules $F_M : M^\sigma \to M$ and $V_M : M \to M^\sigma$ such that

$$F_M V_M = p \cdot \mathrm{Id}_M \quad \text{and} \quad V_M F_M = p \cdot \mathrm{Id}_{M^\sigma}. \tag{3.1.1}$$

3.2. We say that a Dieudonné module is *of finite length* if so is its underlying $W(k)$-module. Let $\mathfrak{Mod}_{\mathcal{D};f.l.}(k)$ be the category of Dieudonné modules of finite length, p-$\mathfrak{GF}_k$ be the category of commutative finite group schemes over k killed by a power of p. After Dieudonné, *there exists an anti-equivalence of categories $\mathbf{M} : p\text{-}\mathfrak{GF}_k \to \mathfrak{Mod}_{\mathcal{D};f.l.}(k)$* ([12] Chap II 4.2).

By passing to projective limits, we can extend the functor $\mathbf{M}$ to BT-groups over k. More precisely, to a BT-group G over k, we associate a Dieudonné module $\mathbf{M}(G)$ which is free of finite type over $W(k)$; *the functor $G \mapsto \mathbf{M}(G)$ is an anti-equivalence of categories between the category of BT-groups over k and the category of Dieudonné modules over k, free of finite type over $W(k)$* ([12] Chap. III 5.6). Let G be a BT-group over k, then basic properties of the functor $\mathbf{M}$ are listed below :

(a) We have a canonical isomorphism $\mathbf{M}(G^{(p)}) = \mathbf{M}(G)^\sigma$, and the morphisms F and V on $\mathbf{M}(G)$ are induced respectively by the Frobenius $F_G : G \to G^{(p)}$ and the Verschiebung $V_G : G^{(p)} \to G$. For every integer $n \geq 1$, we have $\mathbf{M}(G(n)) = \mathbf{M}(G)/p^n\mathbf{M}(G)$, and the morphisms F and V on $\mathbf{M}(G)$ induce respectively the structural morphisms $F_n : \mathbf{M}(G(n))^\sigma \to \mathbf{M}(G(n))$ and $V_n : \mathbf{M}(G(n)) \to \mathbf{M}(G(n))^\sigma$ of the Dieudonné module $\mathbf{M}(G(n))$.

(b) We have a canonical exact sequence, called the Hodge filtration ([3] 3.3.5)

$$0 \to \omega_G \to \mathbf{M}(G(1)) \to \mathrm{Lie}(G^\vee) \to 0. \tag{3.2.2}$$

The k-vector space $(\omega_G)^{(p)} \subset \mathbf{M}(G(1))^{(p)}$ is identified with the image of $V_1 : \mathbf{M}(G(1)) \to \mathbf{M}(G(1))^{(p)}$ ([16] 2.5.2). Hence, we get an isomorphism of k-vector spaces

$$\big(\mathrm{Lie}(G^\vee)\big)^{(p)} \simeq \mathbf{M}(G(1))^{(p)} / \operatorname{Im}(V_1) = \mathbf{M}(G)^{(p)} / \operatorname{Im}(V). \tag{3.2.3}$$

On the other hand, the exact sequence

$$\cdots \xrightarrow{V_{G(1)}} G(1) \xrightarrow{F_{G(1)}} G(1)^{(p)} \xrightarrow{V_{G(1)}} G(1) \to \cdots$$

induces an exact sequence of Dieudonné modules

$$\cdots \to \mathbf{M}(G(1)) \xrightarrow{V_1} \mathbf{M}(G(1))^{(p)} \xrightarrow{F_1} \mathbf{M}(G(1)) \xrightarrow{V_1} \cdots . \tag{3.2.4}$$

In view of (3.2.3), the latter induces a commutative diagram

$$\begin{tikzcd}
\mathbf{M}(G(1))^{(p)} \arrow[r, "F_1"] \arrow[d] & \mathbf{M}(G(1)) \arrow[d] \\
\big(\mathrm{Lie}(G^\vee)\big)^{(p)} \arrow[r, "\varphi_G"] \arrow[ur, "\phi"] & \mathrm{Lie}(G^\vee),
\end{tikzcd} \tag{3.2.5}$$

where the vertical arrows are the natural projections (3.2.2), ϕ is injective, and φ_G is induced by F_1. Since F_1 is induced by the Frobenius of G, hence by functoriality, φ_G is the linearization (2.2.3) of the Hasse-Witt map of G (2.7.2).

(c) Assume that G has height h and dimension d; put $d^* = h - d$. Then we have $\dim_k \omega_G = d$, $\dim_k \mathrm{Lie}(G^\vee) = d^*$ and $\mathbf{M}(G)$ is free of rank h over $W(k)$ by (3.2.2).

3.3. Elementary BT-groups Let s, r be relatively prime integers such that $0 \leq s \leq r$ and $r \neq 0$; put $\lambda = \frac{s}{r}$. We define a Dieudonné module M^λ over k by

$$M^\lambda = \mathcal{D}/(F^{r-s} - V^s), \tag{3.3.6}$$

where $\mathcal{D}$ is the Dieudonné ring over k (3.1). We note that M^λ is free of rank r over $W(k)$ and $M^\lambda/V \cdot M^\lambda \simeq k[F]/F^{r-s}$. We denote by G^λ the BT-group over k such that $\mathbf{M}(G^\lambda) = M^\lambda$. By 3(c) and (3.2.3), the height of G^λ is r and its dimension is s. We call G^λ the *elementary BT-group of slope λ over k*. Note that $G^\lambda \simeq \mathbb{Q}_p/\mathbb{Z}_p$ if $\lambda = 1$, and G^λ is connected if $\lambda < 1$.

3.4. Isocrystals By an *isocrystal over k*, we mean a finite dimensional K_0-vector space E equipped with a bijective σ-linear endomorphism $F : E \to E$. Given a Dieudonné module (M, F_M, V_M) over k, we can associate to it an isocrystal $E = K_0 \otimes_{W(k)} M$ with the σ-linear endomorphism given by $\sigma \otimes_{W(k)} F_M$. For a BT-group G over k, we denote by $\mathbf{E}(G)$ the isocrystal $K_0 \otimes \mathbf{M}(G)$. By Dieudonné-Manin's classification of isocrystals over k ([7] Chap.IV §4), *the category of isocrystals over k is semi-simple, and each $\mathbf{E}(G^\lambda)$ is a simple object. Moreover, any isocrystal coming from a BT-group over k is a direct sum of $\mathbf{E}(G^\lambda)$'s.* Consequently, any BT-group over k is isogenous to a finite product of G^λ's. Moreover, in the dimension one case, we have the following :

Lemma 3.5 ([7] Chap. IV, §8). *If a BT-group G over k is isogenous to $G^{\frac{1}{r}}$* (resp. $G^{\frac{r-1}{r}}$ *), then G is isomorphic to it. In particular, the BT-group associated to a one-dimensional formal group over k of finite height r is necessarily isomorphic to $G^{1/r}$.*

4 The local moduli of an elementary BT-group

4.1. Let k be an algebraically closed field of characteristic $p > 0$, r be a positive integer, $R = k[[t_1, \cdots, t_r]]$, $\mathfrak{m}$ be the maximal ideal of R. We put $\mathscr{S} = \mathrm{Spf}(R)$, $S = \mathrm{Spec}(R)$ and for each integer $n \geq 0$, $S_n = \mathrm{Spec}(R/\mathfrak{m}^{n+1})$. By a BT-group $\mathscr{G}$ over the formal scheme $\mathscr{S}$, we mean a sequence $(G_n)_{n\geq 0}$ of BT-groups over $(S_n)_{n\geq 0}$ equipped with isomorphisms $G_{n+1} \times_{S_{n+1}} S_n \simeq G_n$.

According to ([16] 2.4.4), *the functor* $G \mapsto (G \times_S S_n)_{n\geq 0}$ *defines an equivalence of categories between the category of BT-groups over* S *and the category of BT-groups over* $\mathscr{S}$. For a BT-group $\mathscr{G}$ over $\mathscr{S}$, the corresponding BT-group G over S is called the *algebraization* of $\mathscr{G}$.

4.2. Let $S = \mathrm{Spec}(R)$ and $\mathscr{S} = \mathrm{Spf}(R)$ be as in (4.1). We denote by $\Omega^1_{\mathscr{S}/k} = \varprojlim_n \Omega^1_{S_n/k}$ the sheaf of 1-differential forms of $\mathscr{S}$ over k. The module of global sections of $\Omega^1_{\mathscr{S}/k}$ over $\mathscr{S}$ is $\widehat{\Omega}^1_{R/k}$, the module of continuous differentials of R over k with respect to $\mathfrak{m}$-adic topology ; hence $\Omega^1_{\mathscr{S}/k}$ is a free $\mathscr{O}_{\mathscr{S}}$-module of rank r (EGA 0_{IV} 21.9.3).

Let $\mathscr{G} = (G_n)_{n\geq 0}$ be a BT-group over $\mathscr{S}$. We put $\omega_{\mathscr{G}} = \varprojlim_n \omega_{G_n}$ the sheaf of invariant differential forms of $\mathscr{G}$ over $\mathscr{S}$, and $\mathrm{Lie}(\mathscr{G}^\vee) = \varprojlim_n \mathrm{Lie}(G_n^\vee)$. Then $\omega_{\mathscr{G}}$ and $\mathrm{Lie}(\mathscr{G}^\vee)$ are finite free $\mathscr{O}_{\mathscr{S}}$-modules. We recall that there exists a canonical homomorphism of $\mathscr{O}_{\mathscr{S}}$-modules ([16] 2.5.3)

(4.2.1) $$\mathrm{KS} : \omega_{\mathscr{G}} \to \Omega^1_{\mathscr{S}/k} \otimes_{\mathscr{O}_{\mathscr{S}}} \mathrm{Lie}(\mathscr{G}^\vee).$$

Let $\mathscr{T}_{\mathscr{S}/k} = \mathscr{H}om_{\mathscr{O}_{\mathscr{S}}}(\Omega^1_{\mathscr{S}/k}, \mathscr{O}_{\mathscr{S}/k})$ be the tangent sheaf of $\mathscr{S}$. The *Kodaira-Spencer* map of $\mathscr{G}$ is the homomorphism

(4.2.2) $$\mathrm{Kod} : \mathscr{T}_{\mathscr{S}/k} \longrightarrow \mathscr{H}om_{\mathscr{O}_{\mathscr{S}}}\big(\omega_{\mathscr{G}}, \mathrm{Lie}(\mathscr{G}^\vee)\big)$$

induced by (4.2.1). We say that $\mathscr{G}$ is a *versal* over $\mathscr{S}$ if its Kodaira-Spencer map is surjective.

4.3. Let G be the algebraization of a BT-group $\mathscr{G}$ over $\mathscr{S}$. By (EGA 0_{IV} 21.9.4), the module of global sections of $\Omega^1_{S/k}$, the sheaf of differential 1-forms of S, coincides with $\widehat{\Omega}^1_{R/k}$; hence $\Omega^1_{S/k}$ is free of rank r over $\mathscr{O}_S$, and its completion along the closed point of S is equal to $\Omega^1_{\mathscr{S}/k}$. We have also a canonical homomorphism

(4.3.3) $$\mathrm{KS} : \omega_G \to \Omega^1_{S/k} \otimes_{\mathscr{O}_S} \mathrm{Lie}(G^\vee),$$

and the induce Kodaira-Spencer map

(4.3.4) $$\mathrm{Kod} : \mathscr{T}_{S/k} \longrightarrow \mathscr{H}om_{\mathscr{O}_S}\big(\omega_G, \mathrm{Lie}(G^\vee)\big),$$

where $\mathscr{T}_{S/k} = \mathscr{H}om_{\mathscr{O}_S}(\Omega^1_{S/k}, \mathscr{O}_S)$. But $\omega_{\mathscr{G}}$ and $\mathrm{Lie}(\mathscr{G})$ coincide respectively with the completion of ω_G and $\mathrm{Lie}(G^\vee)$ along with the closed point of S (EGA I 10.8.4). Therefore, the morphisms KS (4.2.1) and Kod (4.2.2) for $\mathscr{G}$ are obtained respectively by applying the completion functor to (4.3.3) and (4.3.4). We say that G is *versal* over S if (4.3.4) is surjective. Note that G is versal if and only if $\mathscr{G}$ is versal.

4.4. We recall briefly the theory of deformations of a BT-group. Let $\mathfrak{AL}_k$ be the category of local artinian k-algebras with residue field k. For an object A of $\mathfrak{AL}_k$, we denote by $s_A : \mathrm{Spec}(k) \to \mathrm{Spec}(A)$ the closed point of A. We notice that all morphisms of $\mathfrak{AL}_k$ are local.

Let G_0 be a BT-group over k, A be an object of $\mathfrak{AL}_k$. A deformation of G_0 over A is a pair (G, ϕ), where G is a BT-group over $\mathrm{Spec}(A)$ and ϕ is an isomorphism $\phi : s_A^* G = G \otimes_A k \xrightarrow{\sim} G_0$. Two deformations (G, ϕ) and (G', ϕ') over A are isomorphic if there exists an isomorphism of BT-groups $\psi : G \xrightarrow{\sim} G'$ such that $\phi = \phi' \circ s_A^*(\psi)$. Let's denote by $\mathscr{D}$ the functor which associates to each object A of $\mathfrak{AL}_k$ the set of isomorphism classes of deformations of G_0 over A; if $f : A \to B$ is a morphism of $\mathfrak{AL}_k$, then the map $\mathscr{D}(f) : \mathscr{D}(A) \to \mathscr{D}(B)$ is given by extension of scalars. We call $\mathscr{D}$ the *deformation functor* of G_0 over $\mathfrak{AL}_k$.

Proposition 4.5 ([14] 4.8)**.** *Let G_0 be a BT-group over k of height h and dimension d, $\mathscr{D}$ be the deformation functor of G_0 over $\mathfrak{AL}_k$; put $d^* = h - d$.*

(a) *The set $\mathscr{D}(k[\epsilon]/\epsilon^2)$ is a k-vector space isomorphic to $\mathrm{Hom}_k(\omega_{G_0}, \mathrm{Lie}(G_0^\vee))$ such that the class of the trivial deformation $[G_0 \otimes_k k[\epsilon]/\epsilon^2]$ corresponds to* 0.

(b) *The functor $\mathscr{D}$ is pro-representable by a formally smooth formal scheme $\mathscr{S}$ over k of relative dimension dd^*,* i.e. *$\mathscr{S} = \mathrm{Spf}(R)$ with $R \simeq k[[(t_{ij})_{1\leq i\leq d^*, 1\leq j\leq d}]]$, and there exists a BT-group $\mathscr{G}$ over $\mathscr{S}$ such that, for any object A of $\mathfrak{AL}_k$ and any deformation (G, ϕ) of G_0 over A, there is a unique homomorphism of local k-algebras $\varphi : R \to A$ with $G \simeq \mathscr{G} \otimes_R A$.*

(c) *Let $\mathscr{T}_{\mathscr{S}/k}(0) = \mathscr{T}_{\mathscr{S}/k} \otimes_R k$ be the tangent space of $\mathscr{S}$ at its unique closed point,*

$$\mathrm{Kod}_0 : \mathscr{T}_{\mathscr{S}/k}(0) \longrightarrow \mathrm{Hom}_k(\omega_{G_0}, \mathrm{Lie}(G_0^\vee)) \tag{4.5.1}$$

be the Kodaira-Spencer map (4.2.2) *of $\mathscr{G}$ evaluated at the closed point of $\mathscr{S}$. Then Kod_0 is bijective, and it can be described as follows. For an element $f \in \mathscr{T}_{\mathscr{S}/k}(0)$,* i.e. *a homomorphism of local k-algebras $f : R \to k[\epsilon]/\epsilon^2$, $\mathrm{Kod}_0(f)$ is the element in $\mathrm{Hom}_k(\omega_{G_0}, \mathrm{Lie}(G_0^\vee))$ corresponding to the class of deformation $[\mathscr{G} \otimes_R (k[\epsilon]/\epsilon^2)]$ by (a).*

Remark 4.6. *Let $(e_j)_{1\leq j\leq d}$ be a basis of ω_{G_0}, $(f_i)_{1\leq i\leq d^*}$ be a basis of $\mathrm{Lie}(G_0^\vee)$. In view of 4.5(c), we can choose a system of parameters $(t_{ij})_{1\leq i\leq d^*, 1\leq j\leq d}$ of $\mathscr{S}$ such that*

$$\mathrm{Kod}_0(\frac{\partial}{\partial t_{ij}}) = e_j^* \otimes f_i,$$

where $(e_j^*)_{1\leq j\leq d}$ is the dual basis of $(e_j)_{1\leq j\leq d}$. Moreover, if $\mathfrak{m}$ is the maximal ideal of R, the parameters t_{ij} are determined uniquely modulo $\mathfrak{m}^2$.

Corollary 4.7 (**Algebraization of the universal deformation**)**.** *The assumptions being those of* (4.5)*, we put moreover $\mathbf{S} = \mathrm{Spec}(R)$ and $\mathbf{G}$ the algebraization of the universal formal deformation $\mathscr{G}$* (4.1)*. Then the BT-group $\mathbf{G}$ is versal over $\mathbf{S}$* (4)*, and satisfies the following universal property. Let A be a noetherian complete local k-algebra with residue field k, G be a BT-group over A endowed with an isomorphism $G \otimes_A k \simeq G_0$; then there exists a unique continuous homomorphism of local k-algebras $\varphi : R \to A$ such that $G \simeq \mathbf{G} \otimes_R A$.*

Proof. For the versality of $\mathbf{G}$ (or of $\mathscr{G}$), we note that each side of the Kodaira-Spencer map Kod (4.2.2) is a free $\mathscr{O}_{\mathscr{S}}$-module of rank dd^*, and its reduction mod the maximal ideal of $\mathscr{O}_{\mathscr{S}}$ is an isomorphism by 4.5(c). It follows that Kod is an isomorphism, hence the conclusion.

Let G be a deformation of G_0 over a noetherian complete local k-algebra A with residue field k. We denote by $\mathfrak{m}_A$ the maximal ideal of A, and put $A_n = A/\mathfrak{m}_A^{n+1}$ for each integer $n \geq 0$. Then by 4.5(b), there exists a unique local homomorphism $\varphi_n : R \to A_n$ such that $G \otimes A_n \simeq \mathbf{G} \otimes_R A_n$. The φ_n's form a projective system $(\varphi_n)_{n\geq 0}$, whose projective limit $\varphi : R \to A$ answers the question. □

Definition 4.8. *The notations are those of* (4.7)*. We call* $\mathbf{S}$ *the* local moduli in characteristic p *of G_0, and* $\mathbf{G}$ *the* universal deformation of G_0 in characteristic p. *We will omit "in characteristic p" for short.*

4.9. Let r be a positive integer, $R = k[[t_1, \cdots, t_r]]$, $\mathfrak{m}$ be the maximal ideal of R. We put $S = \mathrm{Spec}(R)$, and for each integer $n \geq 0$, $R_n = R/\mathfrak{m}^{n+1}$ and $S_n = \mathrm{Spec}(R_n)$. Let G be a BT-group over S. In general, we denote by an index n the objects (e.g. schemes, modules, homomorphisms, $\cdots$) obtained by extension of scalars from R to R_n ; for example, $S_n = \mathrm{Spec}(R_n)$, $G_n = G \times_S S_n$, $\mathrm{Lie}(G_n^\vee) \simeq \mathrm{Lie}(G^\vee)_n, \cdots$.

We have the Hasse-Witt map $\mathrm{HW}_G : \mathrm{Lie}(G^\vee) \to \mathrm{Lie}(G^\vee)$ (2.7.2) and the Kodaira-Spencer map KS (4.2.1 and 4). Following [14], we will compute the map HW_{G_1} in terms of HW_{G_0} and KS_0.

Let $(e_j^0)_{1\leq j\leq d}$ be a basis of ω_{G_0}, $(f_i^0)_{1\leq i\leq d^*}$ be a basis of $\mathrm{Lie}(G_0^\vee)$. Under these basis, the Hasse-Witt map HW_{G_0} is expressed by a matrix $\mathfrak{h}_0$ of type (d^*, d^*) with coefficients in k, while KS_0 is expressed by a matrix κ_0 of type (d^*, d) with coefficients in $\mathfrak{m}/\mathfrak{m}^2$. Let $\mathbf{M}(G_0)$ be the Dieudonné module of G_0. Recall that the k-vector space $\mathbf{M}(G_0(1))$ is an extension of $\mathrm{Lie}(G_0^\vee)$ by ω_{G_0} (3.2.2), and the map HW_{G_0} factors through an injective map (3.2.5)

$$\psi : \mathrm{Lie}(G_0^\vee) \xrightarrow{\iota} \mathrm{Lie}(G_0^\vee)^{(p)} \xrightarrow{\phi} \mathbf{M}(G_0(1)), \tag{4.9.1}$$

where ι is the canonical injection $a \mapsto 1 \otimes a$. We choose a lift $(\tilde{f_i^0})$ of the basis $(f_i^0)_{1\leq i\leq d^*}$ to $\mathbf{M}(G_0(1))$. Under the basis (f_i^0) and $(e_j^0, \tilde{f_i^0})$, the morphism ψ is expressed by a matrix of the form $\begin{pmatrix} b_0 \\ \mathfrak{h}_0 \end{pmatrix}$, where b_0 is a matrix of type (d, d^*) with coefficients in k. Note that b_0 depends on the choice of the lifting $(\tilde{f_i^0})$.

Proposition 4.10 ([14] A 2.1.8)**.** *Under the assumptions above, there exists a basis $(f_i^1)_{1\leq i\leq d^*}$ of $\mathrm{Lie}(G_1^\vee)$ over R_1 lifting $(f_i^0)_{1\leq i\leq d^*}$, such that the Hasse-Witt map HW_{G_1} is expressed under (f_i^1) by the matrix*

$$\mathfrak{h}_1 = \mathfrak{h}_0 - \kappa_0 \cdot b_0$$

with coefficients in $R_1 = k \oplus \mathfrak{m}/\mathfrak{m}^2$.

Remark 4.11. *Let G_0 be a BT-group over k, $\mathbf{S}$ be the local moduli of G_0, $\mathbf{G}$ be the universal deformation of G_0. We apply the computation above to $S = \mathbf{S}$ and $G = \mathbf{G}$. If $(t_{ij})_{1\leq i\leq d^*, 1\leq j\leq d}$ is a system of parameters of $\mathbf{S}$ adapted to the bases $(e_j^0)_{1\leq j\leq d}$ and $(f_i^0)_{1\leq i\leq d^*}$ in the sense that*

$$\mathrm{Kod}_0(\frac{\partial}{\partial t_{ij}}) = e_j^{0*} \otimes f_i^0,$$

where (e_j^{0*}) is the basis dual to (e_j^0). Then κ_0 is just the matrix $(t_{ij}) \bmod \mathfrak{m}^2$.

We will apply the general theory above to elementary BT-groups over k.

Proposition 4.12. *Let r, s be relatively prime integers with $0 < s < r$, $\lambda = \frac{s}{r}$, G^λ be the elementary BT-group over k with slope λ (3.3), $\mathbf{S} = \mathrm{Spec}(R)$ be its local muduli, $\mathbf{G}$ be the universal deformation of G^λ. Then, there exists a system of parameters $(t_{ij})_{1\leq i\leq r-s, 1\leq j\leq s}$ of R and a basis of $\mathrm{Lie}(\mathbf{G}^\vee)$ over R, such that the Hasse-Witt map of $\mathbf{G}$ is expressed by the matrix*

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -t_{1,s} \\ 1 & 0 & \cdots & 0 & -t_{2,s} \\ 0 & 1 & \cdots & 0 & -t_{3,s} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -t_{r-s,s} \end{pmatrix} \tag{4.12.1}$$

Proof. We begin by computing the Hasse-Witt map of G^λ. Since $\mathbf{M}(G^\lambda) = M^\lambda$ (3.3.6) by definition, we have

$$M^\lambda/pM^\lambda = k\{F,V\}/(FV, VF, F^{r-s} - V^s),$$

where $k\{F,V\}$ is the noncommutative polynomial ring over k generated by F, V satisfying the relations $F\cdot a = a^p \cdot F$ and $V \cdot a = a^{1/p}\cdot V$ for all $a \in k$. As k is perfect, the relation (3.2.3) implies that

$$\mathrm{Lie}((G^\lambda)^\vee) \simeq M^\lambda/V\cdot M^\lambda = k[F]/(F^{r-s}),$$

and the Hasse-Witt map of G^λ is given by the multiplication by F. We denote by e the class of 1 in M^λ/pM^λ. Then the vectors

$$V\cdot e,\ V^2\cdot e,\ \cdots,\ V^s\cdot e,\ e,\ F\cdot e,\ \cdots,\ F^{r-s-1}\cdot e \tag{4.12.2}$$

form a basis of M^λ/pM^λ over k adapted to the Hodge filtration of M^λ/pM^λ (3.2.2), *i.e.* $(V\cdot e, V^2\cdot e, \cdots, V^s\cdot e)$ is a basis of ω_{G^λ}, and the images of $(e, F\cdot e, \cdots, F^{r-s-1}\cdot e)$ is a basis of $\mathrm{Lie}((G^\lambda)^\vee)$. Under these basis, the injective morphism $\psi : \mathrm{Lie}((G^\lambda)^\vee) \to M^\lambda/pM^\lambda$ (4.9.1) is expressed by the matrix $\begin{pmatrix} b_0 \\ \mathfrak{h}_0\end{pmatrix}$, where

$$b_0 = \begin{pmatrix} 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in \mathrm{M}_{s\times r-s}(k) \quad \text{and} \quad \mathfrak{h}_0 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathrm{M}_{r-s\times r-s}(k).$$

On the other hand, we choose a system of parameters $(t'_{i,j})_{1\leq i\leq r-s, 1\leq j\leq s}$ adapted to the basis (4.12.2). So the reduction KS_0 of the Kodaira-Spencer map (4.2.1) of $\mathbf{G}$ is expressed by the matrix $\kappa_0 = (t'_{i,j}) \in \mathrm{M}_{(r-s)\times s}(\mathfrak{m}/\mathfrak{m}^2)$ (cf. 4.11). Applying 4.10, we get a basis $(f^1_i)_{1\leq i\leq r-s}$ of $\mathrm{Lie}(\mathbf{G}_1^\vee)$ such that the Hasse-Witt map of $\mathbf{G}_1$ is represented by the matrix

$$\mathfrak{h}_1 = \mathfrak{h}_0 - \kappa_0\cdot b_0 = \begin{pmatrix} 0 & 0 & \cdots & 0 & -t'_{1,s} \\ 1 & 0 & \cdots & 0 & -t'_{2,s} \\ 0 & 1 & \cdots & 0 & -t'_{3,s} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -t'_{r-s,s} \end{pmatrix}.$$

Let v be a section of $\mathrm{Lie}(\mathbf{G}^\vee)$ over $\mathbf{S}$ lifting the vector $f^1_1 \in \mathrm{Lie}(\mathbf{G}_1^\vee)$, and denote by φ the Hasse-Witt map of $\mathbf{G}$ for short. Then the vectors $(v, \varphi(v), \cdots, \varphi^{r-s-1}(v))$ form a basis of $\mathrm{Lie}(\mathbf{G}^\vee)$ over $\mathscr{O}_{\mathbf{S}}$ lifting the basis $(f^1_i)_{1\leq i\leq r-s}$. If

$$\varphi(\varphi^{r-s-1}(v)) = a_1\cdot v + a_2\cdot\varphi(v) + \cdots + a_{r-s}\cdot\varphi^{r-s-1}(v)$$

with $a_i \in R$, then we have $a_i \equiv -t'_{i,s} \mod \mathfrak{m}^2$ for $1 \leq i \leq r-s$. Let $(t_{i,j})_{1\leq i\leq r-s, 1\leq j\leq s}$ be the system of parameters of R with $t_{i,j} = t'_{i,j}$ if $1 \leq j \leq s-1$, and $t_{i,s} = -a_i$. Then the Hasse-Witt map of $\mathbf{G}$ is expressed by the desired formula under the basis $(v, \varphi(v), \cdots, \varphi^{r-s-1}(v))$. □

The following corollary follows immediately from 4.12 and 2.8.

Corollary 4.13. *Under the assumptions of* (4.10), *the ordinary locus of* $\mathbf{G}$ *over* $\mathbf{S}$ *is the open subscheme* $\mathbf{U} = \mathrm{Spec}(R[1/t_{1,s}])$.

5 Monodromy of a BT-group over a complete trait of characteristic $p > 0$

5.1. Let k be an algebraically closed field of characteristic $p > 0$, A be a complete discrete valuation ring of characteristic p, with residue field k and fraction field K, $\overline{K}$ be an algebraic closure of K, K^{sep} be the maximal separable extension of K contained in $\overline{K}$, K^{t} be the maximal tamely ramified extension of K contained in K^{sep}. We put $I = \mathrm{Gal}(K^{\mathrm{sep}}/K)$, $I_p = \mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{t}})$ and $I_t = I/I_p = \mathrm{Gal}(K^{\mathrm{t}}/K)$.

Let π be a uniformizer of A; so we have $A \simeq k[[\pi]]$. Let $\mathtt{v}$ be the valuation on K normalized by $\mathtt{v}(\pi) = 1$; we denote also by $\mathtt{v}$ the unique extension of $\mathtt{v}$ to $\overline{K}$. For every $\alpha \in \mathbb{Q}$, we denote by $\mathfrak{m}_\alpha$ (*resp.* by $\mathfrak{m}_\alpha^+$) the set of elements $x \in K^{\mathrm{sep}}$ such that $\mathtt{v}(x) \geq \alpha$ (*resp.* $\mathtt{v}(x) > \alpha$). We put

$$V_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^+, \tag{5.1.1}$$

which is a k-vector space of dimension 1 equipped with a continuous action of the Galois group I.

5.2. First, we recall some properties of the inertia groups I_p and I_t (see [19] Chap. IV). The subgroup I_p, called the *wild inertia subgroup*, is the maximal pro-p-group contained in I and is normal in I. The quotient $I_t = I/I_p$ is a commutative profinite group, called the *tame inertia group.* We have a canonical isomorphism

$$\theta : I_t \xrightarrow{\sim} \varprojlim_{(d,p)=1} \mu_d, \tag{5.2.2}$$

where the projective system is taken over positive integers prime to p, μ_d is the group of d-th roots of unity in k, and the transition maps $\mu_m \to \mu_d$ are given by $\zeta \mapsto \zeta^{m/d}$, whenever d divides m. We denote by $\theta_d : I_t \to \mu_d$ the projection induced by (5.2.2). Let q be a power of p, $\mathbb{F}_q$ be the finite subfield of k with q elements. Then $\mu_{q-1} = \mathbb{F}_q^\times$, and we can write $\theta_{q-1} : I_t \to \mathbb{F}_q^\times$. The character θ_d is characterized by the following property.

Proposition 5.3 ([18] Prop.7)**.** *Let a, d be relatively prime positive integers, such that d is prime to p. Then the natural action of I_p on the k-vector space $V_{a/d}$ (5.1.1) is trivial, and the induced action of I_t on $V_{a/d}$ is given by the character $(\theta_d)^a : I_t \to \mu_d$. In particular, if q is a power of p, the action of I_t on $V_{1/(q-1)}$ is given by the character $\theta_{q-1} : I_t \to \mathbb{F}_q^\times$ and any I-equivariant $\mathbb{F}_p$-subspace of $V_{1/(q-1)}$ is an $\mathbb{F}_q$-vector space.*

In the sequel, we put $S = \mathrm{Spec}(A)$, and denote by s its closed point, and by η its generic point.

5.4. Let G be a BT-group over S. We define $hw(G)$ to be the valuation of the determinant of a matrix of HW_G, and call it the *Hasse invariant* of G.

(a) $hw(G)$ does not depend on the choice of the matrix representing HW_G. Indeed, let d^* be the rank of $\mathrm{Lie}(G^\vee)$ over A, $\mathfrak{h}$ be a matrix of type (d^*, d^*) with coefficients in A which represents HW_G. Any other matrix representing HW_G can be written in the form $U^{-1} \cdot \mathfrak{h} \cdot U^{(p)}$, where $U \in \mathrm{GL}_{d^*}(A)$, U^{-1} is the inverse of U, and $U^{(p)}$ is the matrix obtained by applying the Frobenius map of A to the coefficients of U.

(b) By 2.8, the generic fiber G_η is ordinary if and only if $hw(G) < \infty$; G is ordinary over T if and only $hw(G) = 0$.

(c) Let $0 \to G' \to G \to G'' \to 0$ be a short exact sequence of BT-groups over T, then we have $hw(G) = hw(G') + hw(G'')$. Indeed, the exact sequence of BT-groups induces a short exact sequence of Lie algebras (cf. [3] 3.3.2)

$$0 \to \mathrm{Lie}(G''^{\vee}) \to \mathrm{Lie}(G^{\vee}) \to \mathrm{Lie}(G'^{\vee}) \to 0,$$

from which our assertion then follows easily.

5.5. Let G be a BT-group over S. Recall that there exists a unique exact sequence of BT-groups over S :

$$0 \to G^{\circ} \to G \to G^{\text{ét}} \to 0, \tag{5.5.1}$$

such that G° is connected, called the *connected part of* G, and $G^{\text{ét}}$ is étale, called the *étale part of* G. Indeed, a unique decomposition of the form (5.5.1) exists over the closed point s of S by ([7] Chap. II §7); it lifts uniquely to S by the henselian property of S. It follows from 5(c) that $hw(G) = hw(G^{\circ})$.

5.6. Let G be a BT-group over S of height h and dimension d, $d^* = h - d$. We say that G is *HW-cyclic*, if $d^* \geq 1$ and there exists an element $\overline{u}$ of $\mathrm{Lie}(G_s^{\vee}) = \mathrm{Lie}(G^{\vee}) \otimes_A k$ such that $(\overline{u}, \mathrm{HW}_{G_s}(\overline{u}), \cdots, (\mathrm{HW}_{G_s})^{d^*-1}(\overline{u}))$ is a basis of $\mathrm{Lie}(G_s^{\vee})$ over k. By Nakayama lemma, G is HW-cyclic if and only if $d^* \geq 1$ and there exists an element $u \in \mathrm{Lie}(G^{\vee})$ such that $(u, \mathrm{HW}_G(u), \cdots, (\mathrm{HW}_G)^{d^*-1}(u))$ is a basis of the free A-module $\mathrm{Lie}(G^{\vee})$, or equivalently, the Hasse-Witt map HW_G can be expressed by a matrix of the form

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d^*} \end{pmatrix}, \tag{5.6.2}$$

where $a_i \in A$ for $1 \leq i \leq d^*$. Note that any BT-group over S with $d^* = 1$ is HW-cyclic.

Lemma 5.7. *Let $0 \to G' \to G \to G'' \to 0$ be an exact sequence of BT-groups over S. If G is HW-cyclic, then so is G'. In particular, the connected part of a HW-cyclic BT-group is HW-cyclic.*

Proof. The exact sequence of BT-groups induces an exact sequence of Lie algebras

$$0 \to \mathrm{Lie}(G''^{\vee}) \to \mathrm{Lie}(G^{\vee}) \to \mathrm{Lie}(G'^{\vee}) \to 0, \tag{5.7.1}$$

and the Hasse-Witt map $\mathrm{HW}_{G'}$ is induced by HW_G by functoriality. Assume that G is HW-cyclic and $G^{\vee}$ has of dimension d^*. Let $\overline{u}$ be an element of $\mathrm{Lie}(G_s^{\vee})$ such that

$$(\overline{u}, \mathrm{HW}_{G_s}(\overline{u}), \cdots, (\mathrm{HW}_{G_s})^{d^*-1}(\overline{u}))$$

is a basis of $\mathrm{Lie}(G_s^{\vee})$ over k. We denote by φ the canonical projection $\mathrm{Lie}(G_s^{\vee}) \to \mathrm{Lie}(G_s'^{\vee})$. Let r be the maximal integer $\leq d^*$ such that the vectors

$$\varphi(\overline{u}),\ \mathrm{HW}_{G'_t}(\varphi(\overline{u})),\ \cdots,\ (\mathrm{HW}_{G'_t})^{r-1}(\varphi(\overline{u}))$$

are linearly independent over k. Then they form a basis of the k-vector space $\mathrm{Lie}(G_s'^{\vee})$, hence G' is HW-cyclic. □

Lemma 5.8. *Let λ be a rational number in the interval $(0,1)$, G^{λ} be the elementary BT-group over k of slope λ (3.3), G be a deformation of G^{λ} over S. Then G is a connected HW-cyclic BT-group over S. In particular, all connected BT-groups of dimension 1 over S are HW-cyclic.*

Proof. Notice first that G is obviously connected. We denote by $\mathbf{S}^{\lambda} = \mathrm{Spec}(R)$ the local moduli of G^{λ}, and by $\mathbf{G}^{\lambda}$ the universal deformation of G^{λ}. By 4.7, there exists a unique continuous homomorphism of local rings $\varphi : R \to A$ such that $G \simeq \mathbf{G}^{\lambda} \otimes_R A$. If $\mathfrak{h}_{\mathbf{G}^{\lambda}}$ is a matrix of $\mathrm{HW}_{\mathbf{G}^{\lambda}}$, then $\varphi(\mathfrak{h}_{\mathbf{G}^{\lambda}})$ is a matrix of HW_G by the functoriality of Hasse-Witt maps. So it follows from (4.12.1) that G is HW-cyclic. If G is a connected BT-group of dimension 1 and height h, then by 3.5, the closed fiber of G is isomorphic to $G^{1/h}$ *i.e.* G is a deformation of $G^{1/h}$ over S, and the conclusion follows. □

Lemma 5.9. *Let G be BT-group over S generically ordinary of height h and dimension d; put $d^* = h - d$. Then we have a canonical isomorphism $G(1)(\overline{K}) \simeq (\mathrm{Ker}\, V_G)(K^{\mathrm{sep}})$. Assume moreover that G is HW-cyclic, and let*

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d^*} \end{pmatrix}$$

be a matrix of HW_G. *Then,*

(a) *$hw(G) = \mathrm{v}(a_1) < \infty$.*

(b) *Let $\mathbb{G}_a = \mathrm{Spec}(A[X])$ be the additive group scheme over S and $\varphi : \mathbb{G}_a \to \mathbb{G}_a$ be the homomorphism given by $X \mapsto f(X)$ at the level of Hopf-algebras, where*

$$f(X) = X^{p^{d^*}} + a_{d^*} X^{p^{d^*-1}} + \cdots + a_1 X \in A[X]. \tag{5.9.1}$$

Then we have an exact sequence of abelian fppf*-sheaves over S :*

$$0 \to \mathrm{Ker}\, V_G \to \mathbb{G}_a \xrightarrow{\varphi} \mathbb{G}_a \to 0. \tag{5.9.2}$$

In particular, the finite group scheme $\mathrm{Ker}\, V_G$ *is isomorphic to* $\mathrm{Spec}\big(A[X]/f(X)\big)$ *with the comultiplication given by $\Delta(X) = 1 \otimes X + X \otimes 1$.*

(c) *We put $a_{d^*+1} = 1$ and*

$$i_0 = \min_{1 \le j \le d^*+1} \{j; \mathrm{v}(a_j) = 0\} - 1. \tag{5.9.3}$$

Then the étale part $G^{\text{ét}}$ of G is of height $d^* - i_0$, and the connected part G° of G is of height $d + i_0$ and dimension d. In particular, i_0 is independent of the choice of matrix of the form (5.6.2)*; G is connected if and only if any matrix of* HW_G *of the form* (5.6.2) *satisfies $\mathrm{v}(a_j) \ge 1$ for $1 \le j \le d^*$.*

Proof. We have an exact sequence of commutative finite flat group schemes over S :

$$0 \to \mathrm{Ker}\, F_G \to G(1) \to \mathrm{Ker}\, V_G \to 0. \tag{5.9.4}$$

Since the generic fiber of $\mathrm{Ker}\, F_G$ is an infinitesimal group scheme, we get $G(1)(\overline{K}) \simeq (\mathrm{Ker}\, V_G)(\overline{K})$. Since by 2.8, $\mathrm{Ker}\, V_G$ is generically étale, every $\overline{K}$-point of $\mathrm{Ker}\, V_G$ is actually a K^{sep}-point; hence we have $G(1)(\overline{K}) \simeq (\mathrm{Ker}\, V_G)(K^{\mathrm{sep}})$. Assume in the sequel that G is HW-cyclic. Then

(a) It is immediate from definition.

(b) Since $A[X]$ is a free module of rank p^{d^*} over its subring $A[f(X)]$, φ is a finite and faithfully flat morphism of group schemes. Hence it is surjective as a morphism of abelian fppf-sheaves over S. On the other hand, by 2.10 and 2.3, $\operatorname{Ker} V_G$ is canonically isomorphic to the group scheme

$$\operatorname{Spec}\Big(A[X_1, \cdots, X_{d^*}]/(X_1^p - X_2, \cdots, X_{d^*-1}^p - X_{d^*}, X_{d^*}^p + a_1X_1 + \cdots a_{d^*}X_{d^*})\Big), \tag{5.9.5}$$

with comultiplication $\Delta(X_i) = 1\otimes X_i + X_i \otimes 1$ for $1 \leq i \leq d^*$. Let $\phi : \operatorname{Ker}(\varphi) = \operatorname{Spec}(A[X]/f(X)) \to \operatorname{Ker} V_G$ be the morphism of T-group schemes defined by the homomorphism of Hopf-algebras $(X_1, X_2, \cdots, X_{d^*}) \mapsto (X, X^p, \cdots, X^{p^{d^*-1}})$. It is clear that ϕ is an isomorphism of group schemes, hence the exact sequence (5.9.2) follows.

(c) From (5.5.1) and (5.9.4), we deduce canonical isomorphisms of groups

$$G(1)(k) \simeq G^{\text{ét}}(1)(k) \simeq (\operatorname{Ker} V_G)(k),$$

since the closed fibers of $G^\circ(1)$ and $\operatorname{Ker} F_G$ are infinitesimal group schemes. Let $\overline{f}(X) \in k[X]$ be the reduction of $f(X) \in A[X]$ (5.9.1). By the definition of i_0, one can write $\overline{f}(X) = g(X^{p^{i_0}})$, where $g(X)$ is an additive separable polynomial in $k[X]$ with $\deg(g) = p^{d^*-i_0}$. Hence the roots of $\overline{f}(X)$ form an $\mathbb{F}_p$-vector space of dimension $d^* - i_0$. By (b), $(\operatorname{Ker} V_G)(k)$ is identified with the set of roots of $\overline{f}(X)$ in k. Therefore, the height of $G^{\text{ét}}$ is $d^* - i_0$, and G° is a BT-group of height $d + i_0$ and dimension d. □

5.10. Let G be a BT-group over S, d^* be the dimension of $G^\vee$. We put

$$\mathrm{T}_p(G) = \varprojlim_n G(n)(\overline{K}) \tag{5.10.6}$$

the Tate module of G. It is a free $\mathbb{Z}_p$-module of rank $\leq d^*$; the equality holds if and only if the generic fiber G_η is ordinary. The Galois group I acts continuously on $\mathrm{T}_p(G)$. We are interested in the image of the monodromy representation

$$\rho : I = \operatorname{Gal}(K^{\text{sep}}/K) \to \operatorname{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G)). \tag{5.10.7}$$

We denote by

$$\overline{\rho} : I = \operatorname{Gal}(K^{\text{sep}}/K) \to \operatorname{Aut}_{\mathbb{F}_p}\big(G(1)(\overline{K})\big) \tag{5.10.8}$$

its reduction mod p.

Proposition 5.11. *Let G be a generically ordinary HW-cyclic BT-group over S of height h and dimension d,*

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d^*} \end{pmatrix}$$

be a matrix of HW_G *; put $d^* = h - d$ and $q = p^{d^*}$.*

(a) *Assume that G is connected and the Hasse invariant $hw(G) = 1$. Then the representation $\overline{\rho}$ (5.10.8) is tame, $G(1)(\overline{K})$ is endowed with the structure of an $\mathbb{F}_q$-vector space of dimension 1, and the induced action of I_t is given by the character $\theta_{q-1} : I_t \to \mathbb{F}_q^\times$.*

(b) *Assume that $d^* > 1$, $\mathtt{v}(a_i) \geq 2$ for $1 \leq i \leq d^* - 1$ and $\mathtt{v}(a_{d^*}) = 1$. Then the order of $\operatorname{Im}(\overline{\rho})$ is divisible by p^{d^*-1}.*

Proof. Let $f(X) \in A[X]$ be the polynomial (5.9.1) associated to $\mathfrak{h}$. By 5.9, $G(1)(\overline{K}) \simeq (\operatorname{Ker} V_G)(K^{\mathrm{sep}})$ is identified with the additive group of the roots of $f(X)$ (5.9.1) in K^{sep}.

(a) By 5.9(a) (c), the condition imposed on G is equivalent to $\mathtt{v}(a_1) = 1$ and $\mathtt{v}(a_i) \geq 1$ for $1 \leq i \leq d^*$. From the Newton polygon of $f(X)$, we deduce that all the non-zero roots of $f(X)$ in K^{sep} have the same valuation $1/(q-1)$. We denote by

$$\psi : G(1)(\overline{K}) \to V_{1/(q-1)}$$

the map which associates to each root $x \in K^{\mathrm{sep}}$ of $f(X)$ the class of x in $V_{1/(q-1)}$. We remark that $G(1)(\overline{K})$ is an $\mathbb{F}_p$-vector space of dimension d^*; hence $G(1)(\overline{K})$ is automatically of dimension 1 over $\mathbb{F}_q$ once we know it is an $\mathbb{F}_q$-vector space. By 5.3, it suffices to show that ψ is an injective I-equivariant homomorphism of groups. By 5.9(b), ψ is obviously an I-equivariant homomorphism of groups. Let x_0 be a root of $f(X)$, and put $g(y) = f(x_0 y)$. Then the polynomial $g(y)$ can be written as $g(y) = x_0^q g_1(y)$, where

$$g_1(y) = y^q + b_{r-s} y^{p^{d^*-1}} + \cdots + b_2 y^p + b_1 y$$

with $b_i = a_i / x_0^{(q-p^{i-1})} \in K^{\mathrm{sep}}$. We have $\mathtt{v}(b_i) > 0$ for $2 \leq i \leq d^*$ and $\mathtt{v}(b_1) = 0$. Let $\overline{b}_1$ be the class of b_1 in the residue field $k = \mathfrak{m}_0/\mathfrak{m}_0^+$. Then the images of the roots of $f(X)$ in $V_{1/(q-1)}$ are $x_0 \overline{b}_1^{-1/(q-1)} \zeta$, where ζ runs over the finite field $\mathbb{F}_q$; hence ψ is injective.

(b) By computing the slopes of the Newton polygon of $f(X)$, we see that there are $p^{d^*-1}(p-1)$ roots of valuation $1/(p^{d^*} - p^{d^*-1})$. Let L be the sub-extension of K^{sep} obtained by adding to K all the roots of $f(x)$. Then the ramification index $e(L/K)$ is divisible by $p^{d^*} - p^{d^*-1} = p^{d^*-1}(p-1)$. Let $\widetilde{L}$ be the sub-extension of K^{sep} fixed by the kernel of $\overline{\rho}$ (5.10.8). The Galois group $\operatorname{Gal}(K^{\mathrm{sep}}/\widetilde{L})$ fixes the roots of $f(x)$ by definition. Hence we have $L \subset \widetilde{L}$, and $|\operatorname{Im}(\overline{\rho})| = [\widetilde{L} : K]$ is divisible by $[L : K]$; in particular, it is divisible by p^{d^*-1}. □

Remark 5.12. *(i) We notice that Proposition 1.11 follows immediately from 5.8 and 5.11(a).*

(ii) The author conjectures that statement (a) holds without the assumption that G is HW-cyclic.

By the same method as 5.11(b), we can prove the following

Proposition 5.13. *Let G be a HW-cyclic BT-group over S,*

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d^*} \end{pmatrix}$$

be a matrix of HW_G, $f(X) = X^{p^{d^*}} + a_{d^*} X^{p^{d^*-1}} + \cdots + a_1 X \in A[X]$, i_0 be the integer (5.9.3). Assume that there exists $\alpha \in k$ such that $\mathtt{v}(f(\alpha)) = 1$. Then we have $0 \leq i_0 \leq d^* - 1$ and the order of $\operatorname{Im}(\overline{\rho})$ is divisible by p^{i_0}.

Proof. The relation $i_0 \leq d^* - 1$ is equivalent to that G is not connected by 5.9(c). Assume that $i_0 = d^*$, *i.e.* G is connected. Then we would have

$$f(X) \equiv X^{p^{d^*}} \mod (\pi A[X]).$$

But $\mathrm{v}(f(\alpha)) = 1$ implies that $\alpha^{p^{d^*}} \in \pi A$, *i.e.* $\alpha = 0$; hence we would have $f(\alpha) = 0$, which contradicts the condition $\mathrm{v}(f(\alpha)) = 1$.

We put $g(X) = f(X + \alpha) = f(X) + f(\alpha)$. As $\mathrm{v}(f(\alpha)) = 1$, then $(0,1)$ and $(p^{i_0}, 0)$ are the first two break points of the Newton polygon of $g(X)$. Hence there exists p^{i_0} roots of $g(X)$ of valuation $1/p^{i_0}$. Let L be the subextension of K in K^{sep} generated by the roots of $f(X)$. The ramification index $e(L/K)$ is divisible by p^{i_0}. If $\widetilde{L}$ is the subextension of K^{sep} fixed by the kernel of $\overline{\rho}$, then it is an extension of L as we saw in the proof of 5.11(b). Hence we have $|\operatorname{Im}(\overline{\rho})| = [\widetilde{L} : K]$ is divisible by $[L : K]$, and in particular, divisible by p^{i_0}. □

Theorem 5.14 (Reformulation of Igusa's theorem)**.** *Let G be a connected BT-group over S of height 2, dimension 1, and $hw(G) = 1$. Then G is versal (4.3), and the monodromy representation*

$$\rho : I \to \operatorname{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G)) \simeq \mathbb{Z}_p^\times \tag{5.14.1}$$

is surjective.

Proof. By 3.5, the closed fiber G_s of G is isomorphic to $G^{1/2}$; we choose an isomorphism $G_s \simeq G^{1/2}$. Let $\mathbf{S}^{1/2} = \operatorname{Spec}(R)$ be the local moduli of $G^{1/2}$, $\mathbf{G}^{1/2}$ be the universal deformation of $G^{1/2}$. Then there exists a unique local homomorphism of local rings $\varphi : R \to A$ such that $G \simeq \mathbf{G}^{1/2} \otimes_R A$. By functoriality, the image of a matrix of $\mathrm{HW}_{\mathbf{G}^{1/2}}$ by φ is a matrix of HW_G. We note that R is a complete discrete valuation ring, and $\mathrm{HW}_{\mathbf{G}^{1/2}}$ can be represented by a uniformizer π_R of R (4.12). Then $\varphi(\pi_R)$ is a matrix of HW_G. Since $hw(G) = 1$, $\varphi(\pi_R)$ must be a uniformizer of A. Hence the homomorphism φ is an isomorphism, and G is isomorphic to $\mathbf{G}$. The versality of G follows from 4.7.

We follow ([17] Thm. 4.3) to prove the surjectivity of ρ. For each integer $n \geq 1$, let

$$\rho_n : I \to \operatorname{Aut}_{\mathbb{Z}/p^n\mathbb{Z}}(G(n)(\overline{K})) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$$

be the reduction mod p^n of ρ, K_n be the subfield of K^{sep} fixed by the kernel of ρ_n. Then ρ_n induces an injective homomorphism $\operatorname{Gal}(K_n/K) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. By taking projective limits, we are reduced to prove the surjectivity of ρ_n for every $n \geq 1$. It suffices to verify that

$$|\operatorname{Im}(\rho_n)| = [K_n : K] \geq p^{n-1}(p-1)$$

(then the equality holds automatically).

We regard G as a formal group over S. Then by ([17] 3.6), there exists a parameter X of the formal group G normalized by the condition $[\xi](X) = \xi(X)$ for all $(p-1)$-th root of unity $\xi \in \mathbb{Z}_p$. For such a parameter, we have

$$[p](X) = a_1 X^p + \alpha X^{p^2} + \sum_{m \geq 2} c_m X^{p(1+m(p-1))} \in A[[X]],$$

where we have $\mathrm{v}(a_1) = hw(G) = 1$ by ([17] 3.6.1 and 3.6.5), and $\mathrm{v}(\alpha) = 0$, as G is of height 2. For each integer $i \geq 0$, we put

$$V^{(p^i)}(X) = a_1^{p^i} X + \alpha^{p^i} X^p + \sum_{m \geq 2} c_m^{p^i} X^{1+m(p-1)} \in A[[X]];$$

then we have $[p^n](X) = V^{(p^{n-1})} \circ V^{(p^{n-2})} \circ \cdots \circ V(X^{p^n})$. Hence each point of $G(n)(\overline{K})$ is given by a sequence $y_1, \cdots, y_n \in K^{\mathrm{sep}}$ (or simply an element $y_n \in K^{\mathrm{sep}}$) satisfying the equations

$$\begin{cases} V(y_1) = a_1 y_1 + \alpha y_1^p + \cdots = 0; \\ V^{(p)}(y_2) = a_1^p y_2 + \alpha^p y_2^p + \cdots = y_1; \\ \vdots \\ V^{(p^{n-1})}(y_n) = a_1^{p^{n-1}} y_{n-1} + \alpha^{p^{n-1}} y_{n-1}^p + \cdots = y_{n-1}. \end{cases}$$

Let $y_n \in K^{\mathrm{sep}}$ be such that $y_1 \neq 0$. By considering the Newton polygons of the equations above, we verify that $\mathrm{v}(y_i) = p^{i-1}(p-1)$ for $1 \leq i \leq n$; in particular, the ramification index $e(K_n/K)$ is at least $p^{n-1}(p-1)$. By the definition of K_n, the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K_n)$ must fix $y_n \in K^{\mathrm{sep}}$, *i.e.* K_n is an extension of $K(y_n)$. Therefore, we have $[K_n : K] \geq [K(y_n) : K] \geq e(K(y_n)/K) \geq p^{n-1}(p-1)$. □

5.15. Let G be a BT-group over S with connected part G°, and étale part $G^{\text{ét}}$ of height m. From (5.5.1), we deduce a canonical exact sequence of I-modules

$$0 \to G^\circ(1)(\overline{K}) \to G(1)(\overline{K}) \to G^{\text{ét}}(1)(\overline{K}) \to 0 \tag{5.15.2}$$

giving rise to a class $\overline{c} \in \mathrm{Ext}^1_{\mathbb{F}_p[I]}(G^{\text{ét}}(1)(\overline{K}), G^\circ(1)(\overline{K}))$, which vanishes if and only if (5.15.2) splits. Since I acts trivially on $G^{\text{ét}}(1)(\overline{K})$, we have an isomorphism of I-modules $G^{\text{ét}}(1)(\overline{K}) \simeq \mathbb{F}_p^m$. Recall that for any $\mathbb{F}_p[I]$-module M, we have a canonical isomorphism ([19] Chap.VII, §2)

$$\mathrm{Ext}^1_{\mathbb{F}_p[I]}(\mathbb{F}_p, M) \simeq H^1(I, M).$$

Hence we deduce that

$$\overline{c} \in \mathrm{Ext}^1_{\mathbb{F}_p[I]}(G^{\text{ét}}(1)(\overline{K}), G^\circ(1)(\overline{K})) \simeq H^1(I, G^\circ(1)(\overline{K}))^m. \tag{5.15.3}$$

Proposition 5.16. *Let G be a HW-cyclic BT-group over S such that $hw(G) = 1$, $\overline{\rho}$ (5.10.8) be the representation of I on $G(1)(\overline{K})$. Then the cohomology class $\overline{c}$ (5.15.3) does not vanish if and only if the order of the group $\mathrm{Im}(\overline{\rho})$ is divisible by p.*

First, we prove the following result on cohomology of groups.

Lemma 5.17. *Let F be a field, Γ be a commutative group, and $\chi : \Gamma \to F^\times$ be a character of Γ. We denote by $F(\chi)$ an F-vector space of dimension 1 endowed with an action of Γ given by χ. Then we have $H^1(\Gamma, F(\chi)) = 0$.*

Proof. Let c be a 1-cocycle of Γ with values in $F(\chi)$. We prove that c is a 1-coboundary. For any $g, h \in \Gamma$, we have

$$\begin{aligned} c(gh) &= c(g) + \chi(g)c(h), \\ c(hg) &= c(h) + \chi(h)c(g). \end{aligned}$$

Since Γ is commutative, it follows from the relation $c(gh) = c(hg)$ that

$$(\chi(g) - 1)c(h) = (\chi(h) - 1)c(g). \tag{5.17.1}$$

If $\chi(g) \neq 1$ and $\chi(h) \neq 1$, then

$$\frac{1}{\chi(g)-1}c(g) = \frac{1}{\chi(h)-1}c(h).$$

Therefore, there exists $x \in \mathbb{F}_q(\overline{\chi})$ such that $c(g) = (\chi(g)-1)x$ for all $g \in \Gamma$ with $\chi(g) \neq 1$. If $\chi(g) = 1$, we have also $c(g) = 0 = (\chi(g)-1)x$ by (5.17.1). This shows that c is a 1-coboundary. □

Proof of 5.16. By 5.7 and 5(c), the connected part G° of G is HW-cyclic with $hw(G^\circ) = hw(G) = 1$. Assume that $\mathrm{T}_p(G^\circ)$ has rank ℓ over $\mathbb{Z}_p$, and $\mathrm{T}_p(G^{\text{ét}})$ has rank m. Then by 5.11(a), $G^\circ(1)(\overline{K})$ is an $\mathbb{F}_q$-vector space of dimension 1 (with $q = p^\ell$), and the action of I on $G^\circ(1)(\overline{K})$ factors through the character $\overline{\chi} : I \to I_t \xrightarrow{\theta_{q-1}} \mathbb{F}_q^\times$. We write $G(1)(\overline{K}) = \mathbb{F}_q(\overline{\chi})$ for short. If the cohomology class $\overline{c}$ is zero, then the exact sequence (5.15.2) splits, *i.e.* we have an isomorphism of Galois modules $G(1)(\overline{K}) \simeq \mathbb{F}_q(\overline{\chi}) \oplus \mathbb{F}_p^m$. It is clear that the group $\mathrm{Im}(\overline{\rho})$ is of order $q-1$.

Conversely, if the cohomology class $\overline{c}$ is not zero, we will show that there exists an element in $\mathrm{Im}(\overline{\rho})$ of order p. We choose a basis adapted to the exact sequence (5.15.2) such that the action of $g \in I$ is given by

$$\overline{\rho}(g) = \begin{pmatrix} \overline{\chi}(g) & \overline{c}(g) \\ 0 & \mathbf{1}_m \end{pmatrix}, \tag{5.17.2}$$

where $\mathbf{1}_m$ is the unit matrix of type (m,m) with coefficients in $\mathbb{F}_p$, and the map $g \mapsto \overline{c}(g)$ gives rise to a 1-cocycle representing the cohomology class $\overline{c}$. Let I_1 be the kernel of $\overline{\chi} : I \to \mathbb{F}_q^\times$, Γ be the quotient I/I_1, so $\overline{\chi}$ induces an isomorphism $\overline{\chi} : \Gamma \xrightarrow{\sim} \mathbb{F}_q^\times$. We have an exact sequence

$$0 \to H^1(\Gamma, \mathbb{F}_q(\overline{\chi}))^r \xrightarrow{\text{Inf}} H^1(I, \mathbb{F}_q(\overline{\chi}))^m \xrightarrow{\text{Res}} H^1(I_1, \mathbb{F}_q(\overline{\chi}))^m,$$

where “Inf” and “Res” are respectively the inflation and restriction homomorphisms in group cohomology. Since $H^1(\Gamma, \mathbb{F}_q(\overline{\chi}))^m = 0$ by 5.17, the restriction of the cohomology class $\overline{c}$ to $H^1(I_1, \mathbb{F}_q(\overline{\chi}))^m$ is non-zero. Hence there exists $h \in I_1$ such that $\overline{c}(h) \neq 0$. As we have $\overline{\chi}(h) = 1$, then

$$\overline{\rho}(h)^p = \begin{pmatrix} \mathbf{1}_\ell & p\overline{c}(h) \\ 0 & \mathbf{1}_m \end{pmatrix} = \mathbf{1}_{\ell+m}.$$

Thus the order of $\overline{\rho}(h)$ is p. □

Corollary 5.18. *Let G be a HW-cyclic BT-group over S,*

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d^*} \end{pmatrix}$$

be a matrix of HW_G, $f(X) = X^{p^{d^*}} + a_{d^*}X^{p^{d^*-1}} + \cdots + a_1X \in A[X]$. *If $hw(G) = 1$ and if there exists $\alpha \in k \subset A$ such that $\mathrm{v}(f(\alpha)) = 1$, then the cohomology class* (5.15.3) *is not zero,* i.e. *the extension of I-modules* (5.15.2) *does not split.*

Indeed, this is an immediate consequence of 5.13 and 5.16.

6 Lemmas in group theory

6.1. Recall that the general linear group $\mathrm{GL}_2(\mathbb{Z}_p)$ admits a natural exhaustive decreasing filtration by open normal subgroups

$$\mathrm{GL}_2(\mathbb{Z}_p) \supset 1 + p\mathrm{M}_2(\mathbb{Z}_p) \supset \cdots \supset 1 + p^n\mathrm{M}_2(\mathbb{Z}_p) \supset \cdots,$$

where $\mathrm{M}_2(\mathbb{Z}_p)$ denotes the ring of matrix of type $(2,2)$ with coefficients in $\mathbb{Z}_p$. We endow $\mathrm{GL}_2(\mathbb{Z}_p)$ with the topology for which $(1 + p^n\mathrm{M}_2(\mathbb{Z}_p))_{n\geq 1}$ form a fundamental system of neighborhoods of 1; then $\mathrm{GL}_2(\mathbb{Z}_p)$ is a complete and separated topological group.

6.2. Let $\mathfrak{G}$ be a profinite group, $\phi : \mathfrak{G} \to \mathrm{GL}_2(\mathbb{Z}_p)$ be a continuous homomorphism of topological groups. By taking inverse images, we obtain a decreasing filtration $(F^n\mathfrak{G}, n \in \mathbb{Z}_{\geq 0})$ on $\mathfrak{G}$ by open normal subgroups :

$$F^0\mathfrak{G} = \mathfrak{G}, \quad \text{and} \quad F^n\mathfrak{G} = \phi^{-1}(1 + p^n\mathrm{M}_2(\mathbb{Z}_p)) \text{ for } n \geq 1.$$

Furthermore, the homomorphism ϕ induces a sequence of injective homomorphisms of finite groups

$$\phi_0 \colon F^0\mathfrak{G}/F^1\mathfrak{G} \longrightarrow \mathrm{GL}_2(\mathbb{F}_p) \tag{6.2.1}$$

$$\phi_n \colon F^n\mathfrak{G}/F^{n+1}\mathfrak{G} \to \mathrm{M}_2(\mathbb{F}_p), \quad \text{for } n \geq 1. \tag{6.2.2}$$

Lemma 6.3. *The homomorphism ϕ is surjective if and only if the following conditions are satisfied :*

(i) *The homomorphism ϕ_0 is surjective.*

(ii) *For every integer $n \geq 1$, the subgroup* $\mathrm{Im}(\phi_n)$ *of* $\mathrm{M}_2(\mathbb{F}_p)$ *contains an element of the form* $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ *with $x \neq 0$; or equivalently, there exists, for every $n \geq 1$, an element $g_n \in \mathfrak{G}$ such that $\phi(g_n)$ is of the form* $\begin{pmatrix} 1+p^n a & p^{n+1}b \\ p^{n+1}c & 1+p^{n+1}d \end{pmatrix}$, *where $a, b, c, d \in \mathbb{Z}_p$ and a is not divisible by p.*

Proof. We notice first that ϕ is surjective if and only if ϕ_n is surjective for every $n \geq 0$, because $\mathfrak{G}$ is complete and $\mathrm{GL}_2(\mathbb{Z}_p)$ is separated ([4] Chap. III §2 n°8 Cor. 2 au Théo. 1). The surjectivity of ϕ_0 is condition (i). Condition (ii) is clearly necessary. We prove that it implies that ϕ_n is surjective for $n \geq 1$, under the assumption of condition (i). First, we notice that under condition (i) if $A \in \mathrm{M}_2(\mathbb{F}_p)$ lies in $\mathrm{Im}(\phi_n)$, then for any $U \in \mathrm{GL}_2(\mathbb{F}_p)$ the conjugate matrix $U \cdot A \cdot U^{-1}$ lies also in $\mathrm{Im}(\phi_n)$. In fact, let $\tilde{A}$ be a lift of A to $\mathrm{M}_2(\mathbb{Z}_p)$ and $\tilde{U} \in \mathrm{GL}_2(\mathbb{Z}_p)$ a lift of U. By assumptions, there exist $g, h \in \mathfrak{G}$ such that

$$\phi(g) \equiv 1 + p^n\tilde{A} \bmod (1 + p^{n+1}\mathrm{M}_2(\mathbb{Z}_p)) \quad \text{and } \phi(h) \equiv \tilde{U} \bmod (1 + p\mathrm{M}_2(\mathbb{Z}_p)).$$

Therefore we have $\phi(hgh^{-1}) \equiv (1 + p^n\tilde{U} \cdot \tilde{A} \cdot \tilde{U}^{-1}) \bmod (1 + p^{n+1}\mathrm{M}_2(\mathbb{Z}_p))$, hence $hgh^{-1} \in F^n\mathfrak{G}$ and $\phi_n(hgh^{-1}) = U \cdot A \cdot U^{-1}$.

Let $A_1 = A = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in \mathrm{Im}(\phi_n)$, with $x \neq 0$, $U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $A_2 = U \cdot A \cdot U^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} \in \mathrm{Im}(\phi_n)$. For $V = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, we have $A_3 = V \cdot A \cdot V^{-1} = \begin{pmatrix} x & 0 \\ x & 0 \end{pmatrix} \in \mathrm{Im}(\phi_n)$. Finally for $W = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, we deduce that $A_4 = W \cdot A \cdot W^{-1} = \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} \in \mathrm{Im}(\phi_n)$. But $(A_i)_{1\leq i\leq 4}$ generate the additive group $\mathrm{M}_2(\mathbb{F}_p)$. Hence we get $\mathrm{Im}(\phi_n) = \mathrm{M}_2(\mathbb{F}_p)$, and this proves the surjectivity of ϕ_n. □

6.4. We recall that a subgroup H of $\mathrm{GL}_2(\mathbb{F}_p)$ is called

(i) a *split Cartan subgroup*, if it is conjugate to the diagonal subgroup.

(ii) a *Borel subgroup*, if it is conjugate to the upper triangle subgroup ; such a group H is of order $p(p-1)^2$.

(iii) a *non-split Cartan subgroup*, if the subset $H \cup \{0\}$ of the matrices algebra $\mathrm{M}_2(\mathbb{F}_p)$ is a field isomorphic to $\mathbb{F}_{p^2}$; such a group is cyclic of order p^2-1.

We notice that a Borel subgroup can never contain a non-split Cartan subgroup.

Lemma 6.5. *Let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Then $H = \mathrm{GL}_2(\mathbb{F}_p)$ if and only if the following two conditions are satisfied :*

(i) *H contains a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.*

(ii) *The order of H is divisible by p.*

Proof. According to ([18] Prop. 15), if a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ has an order divisible by p, then either it contains $\mathrm{SL}_2(\mathbb{F}_p)$, or it is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. In our case, H can not be contained in a Borel subgroup, because a Borel subgroup can never contain a non-split Cartan subgroup. Hence H contains $\mathrm{SL}_2(\mathbb{F}_p)$. Since the restriction of the determinant homomorphism to a non-split Cartan subgroup is surjective, we have $H = \mathrm{GL}_2(\mathbb{F}_p)$. □

7 Proofs of 1.9 and 1.7

7.1. We start by a tautological remark on the functoriality of the monodromy representation. Let n be an integer ≥ 1, $\Lambda = \mathbb{Z}/p^n\mathbb{Z}$, X be a scheme, $\mathscr{F}$ be a locally constant and constructible étale sheaf of free Λ-modules on X. If $\overline{\eta}$ is a geometric point of X, we denote by

$$\rho(\mathscr{F}) : \pi_1(X, \overline{\eta}) \to \mathrm{Aut}_\Lambda(\mathscr{F}_{\overline{\eta}})$$

the monodromy representation corresponding to $\mathscr{F}$, where $\pi_1(X, \overline{\eta})$ is the algebraic fundamental group of X with base point $\overline{\eta}$. Let $f : Y \to X$ be a morphism of schemes, and $\overline{\xi}$ a geometric point of Y. We have a functorial homomorphism of fundamental groups

$$\pi_1(f) : \pi_1(Y, \overline{\xi}) \to \pi_1(X, f(\overline{\xi})).$$

The fiber $\mathscr{F}_{f(\overline{\xi})}$ is canonically isomorphic to $f^*(\mathscr{F})_{\overline{\xi}}$, and the étale sheaf $f^*(\mathscr{F})$ on Y corresponds to the induced representation $\rho(\mathscr{F}) \circ \pi_1(f)$ of $\pi_1(Y, \overline{\xi})$. Therefore, we have a commutative diagram

(7.1.1)
$$\begin{tikzcd}
\pi_1(Y, \xi) \arrow[r, "\pi_1(f)"] \arrow[d, "\rho(f^*(\mathscr{F}))"'] & \pi_1(X, f(\overline{\xi})) \arrow[d, "\rho(\mathscr{F})"] \\
\mathrm{Aut}_\Lambda(f^*(\mathscr{F})_{\overline{\xi}}) \arrow[r, equal] & \mathrm{Aut}_\Lambda(\mathscr{F}_{f(\overline{\xi})}).
\end{tikzcd}$$

In particular, $\mathrm{Im}(\rho(f^*(\mathscr{F})))$ is canonically identified with a subgroup of $\mathrm{Im}(\rho(\mathscr{F}))$.

7.2. Let X be a scheme, G be an ordinary BT-group over a scheme X, $G^{\text{ét}}$ be its étale part (2.6.1). If $\overline{\eta}$ is a geometric point of X, we denote by

$$\mathrm{T}_p(G, \overline{\eta}) = \varprojlim_n G(n)(\overline{\eta}) = \varprojlim_n G^{\text{ét}}(n)(\overline{\eta})$$

the Tate module of G at $\overline{\eta}$, and by $\rho(G)$ the monodromy representation of $\pi_1(X,\overline{\eta})$ on $\mathrm{T}_p(G,\overline{\eta})$. Let $f : Y \to X$ be a morphism of schemes, $\overline{\xi}$ be a geometric point of Y, $G_Y = G \times_X Y$. Then by applying (7.1.1) to $G^{\text{ét}}(n)$ and passing to projective limits, we obtain a commutative diagram

$$\begin{tikzcd} \pi_1(Y,\xi) \arrow[r, "\pi_1(f)"] \arrow[d, "\rho(G_Y)"'] & \pi_1(X, f(\overline{\xi})) \arrow[d, "\rho(G)"] \\ \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G_Y,\overline{\xi})) \arrow[r, equal] & \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G, f(\overline{\xi}))) \end{tikzcd} \tag{7.2.2}$$

In particular, the monodromy of G_Y is a subgroup of the monodromy of G. In the sequel, diagram (7.2.2) will referred as the *functoriality of monodromy* for the BT-group G and the morphism f.

7.3. Proof of Proposition 1.9 : We note first that 1.9(c) follows immediately from 1.9(a), (b) and Lemma 6.5. Since the monodromy of a BT-group is independent of the base point, for each statement of (a) and (b), we only need to prove it with respect to any geometric point of $\mathbf{S}^\lambda$.

Let $(t_{i,j})_{1\leq i\leq r-s, 1\leq j\leq s}$ be a regular system of parameters of $\mathbf{S}^\lambda = \mathrm{Spec}(R)$ such that $\mathrm{HW}_{\mathbf{G}^\lambda}$ can be represented by a matrix $\mathfrak{h}$ of the form (5.6.2) (cf. 4.12). Let $S = \mathrm{Spec}(A)$ with $A = k[[\pi]]$, η be its generic point. Then any sequence of $(r-s)\cdot s$ elements $(a_{i,j})_{1\leq i\leq r-s,1\leq j\leq s} \in \pi A$ determines a continuous homomorphism $\varphi : R \to A$ by the condition that $\varphi(t_{i,j}) = a_{i,j}$ for $1 \leq i \leq r-s, 1 \leq j \leq s$. Let $f : S \to \mathbf{S}^\lambda$ be the morphism of schemes corresponding to φ, $G = \mathbf{G}^\lambda \times_{\mathbf{S}^\lambda} S$. By functoriality,

$$\varphi(\mathfrak{h}) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_{1,s} \\ 1 & 0 & \cdots & 0 & -a_{2,s} \\ 0 & 1 & \cdots & 0 & -a_{3,s} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{r-s,s} \end{pmatrix}$$

is a matrix of HW_G. Assume that G is generically étale, *i.e.* $a_{1,s} \neq 0$. Then we have $f(\eta) \in \mathbf{U}^\lambda$, and denote by $f|_\eta : \eta \to \mathbf{U}^\lambda$ the restriction of f. Let $\mathbf{G}^{\text{ét}}_{\mathbf{U}^\lambda}$ be the étale part of the $\mathbf{G}^\lambda_{\mathbf{U}^\lambda} = \mathbf{G}^\lambda \times_{\mathbf{S}^\lambda} \mathbf{U}^\lambda$. The étale sheaf $\mathbf{G}^{\text{ét}}_{\mathbf{U}^\lambda}(1)$ over $\mathbf{U}^\lambda$ corresponds to the monodromy representation $\overline{\rho}^\lambda$ (1.8.1), and its inverse image by $f|_\eta$ corresponds to the Galois representation $\overline{\rho}$ (5.10.8). Applying the commutative diagram (7.1.1) to $\mathscr{F} = \mathbf{G}^{\text{ét}}_{\mathbf{U}^\lambda}(1)$ and the morphism $f|_\eta$, we see that $\mathrm{Im}(\overline{\rho})$ is a subgroup of $\mathrm{Im}(\overline{\rho}^\lambda)$. We choose the morphism f such that the condition of 5.11(a) is satisfied for the BT-group $\mathbf{G}^\lambda \times_{\mathbf{S}^\lambda} S$ over S, then 1.9(a) follows from 5.11(a). Statement 1.9(b) can be proved in the same way.

7.4. Proof of Theorem 1.7 From now on, we let $\lambda = 1/3$, and $\mathbf{S}^{1/3} = \mathrm{Spec}(R)$ be the local moduli of the elementary BT-group $G^{1/3}$ with $R = k[[t_1, t_2]]$, $\mathbf{G}^{1/3}$ be the universal deformation of $G^{1/3}$ over $\mathbf{S}^{1/3}$. We denote by ξ the generic point of $\mathbf{S}^{1/3}$. We choose a system of parameters t_1, t_2 of R such that the Hasse-Witt map of $\mathbf{G}^{1/3}$ is represented by the matrix (cf. 4.12)

$$\mathfrak{h} = \begin{pmatrix} 0 & -t_1 \\ 1 & -t_2 \end{pmatrix}. \tag{7.4.3}$$

Let $X \subset \mathbf{S}^{1/3}$ be the divisor defined by $t_1 = 0$, $x \in \mathbf{S}^{1/3}$ be the generic point of X. Then the local ring $\mathscr{O}_{\mathbf{S}^{1/3},x}$ is a discrete valuation ring with residue field $k((t_2))$, and t_1 is a uniformizer of $\mathscr{O}_{\mathbf{S}^{1/3},x}$.

Lemma 7.5. *There exists a complete discrete valuation ring A over k and an injective homomorphism of local k-algebras $\varphi : \mathscr{O}_{\mathbf{S}^{1/3},x} \to A$, such that the following holds :*

(i) *the residue field of A is algebraically closed;*

(ii) *$\varphi(t_1)$ is a uniformizer of A.*

Proof. We give an explicit construction of (A, φ). Let $\overline{x}$ be a geometric point of $\mathbf{S}^{1/3}$ over x, $\mathbf{S}^{1/3}_{(\overline{x})} = \mathrm{Spec}(A_0)$ be the strict henselisation of $\mathbf{S}^{1/3}$ at $\overline{x}$. We denote by E_0 the residue field of A_0, by K_0 its fraction field. Then E_0 is a separable closure of $\kappa(x) = k((t_2))$, and t_1 is a uniformizer of A_0. Since the canonical homomorphism $R \to A_0$ is injective, we can identify R with a subring of A_0. For every integer $n \geq 1$, let $t_2^{(n)}$ be a p^n-th root of t_2 in an algebraic closure of K_0, $K_n = K_0(t_2^{(n)})$, A_n be the integral closure of A_0 in K_n. By ([4] Ch. VI §8 n°5 Cor. 2 au Théo. 2), A_n is a henselian discrete valuation ring, free of finite type as an A-module, and

$$e(K_n/K_0)f(K_n/K_0) = p^n,$$

where $e(K_n/K_0)$ is the ramification index of K_n/K_0, and $f(K_n/K_0)$ is the degree of corresponding residue extension. It is clear that the residue field of K_n is $E_n = E_0(t_2^{(n)})$. Hence $f(K_n/K_0) = p^n$, $e(K_n/K_0) = 1$, and t_1 is a uniformizer of A_n. Let A be the completion of $\cup_{n \geq 1} A_n$ with respect to its maximal ideal. Then the ring A, together with the canonical injective homomorphism $\varphi : \mathscr{O}_{\mathbf{S}^{1/3},x} \to A$, satisfies conditions (i) and (ii). □

7.6. In the sequel, we fix such a pair (A, φ) as in Lemma 7.5. Let E be the residue field of A, K be its fraction field. We identify $R = k[[t_1, t_2]]$ with its image in A. So t_1 is a uniformizer of A, and we have an isomorphism $A \simeq E[[t_1]]$. We fix an algebraically closure $\overline{K}$ of K. Let K^{sep} be the separable closure of K contained in $\overline{K}$, and put $I = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Let v be the valuation on K normalized by $\mathrm{v}(t_1) = 1$. We denote also by v the unique extension of v to $\overline{K}$.

Let $S = \mathrm{Spec}(A)$, $\overline{x}$ be the closed point of S, and η be its generic point. We denote by

(7.6.1) $$f : S \to \mathbf{S}^{1/3}$$

the morphism of schemes induced by φ. We have $f(\overline{x}) = x$ and $f(\eta) = \xi$. Let G be the BT-group $\mathbf{G}^{1/3} \times_{\mathbf{S}^{1/3}} S$ over S.

Lemma 7.7. (a) *G is a HW-cyclic BT-group over S* (5.6) *with Hasse invariant* (5.4) *$hw(G) = 1$.*

(b) *The étale part $G^{\text{ét}}$ of G has height* 1*; the connected part G° of G has height* 2*, dimension* 1*, and Hasse invariant $hw(G^{\circ}) = 1$.*

Proof. The Hasse-Witt map of G can be expressed by the matrix (7.4.3) with the coefficients viewed in A. Hence G is HW-cyclic by definition, and $hw(G) = 1$, since t_1 is a uniformizer of A. Statement (b) follows immediately from 5.9(c). □

7.8. We will study the monodromy representation (5.10.7)

(7.8.1) $$\rho : I = \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G)) \simeq \mathrm{GL}_2(\mathbb{Z}_p).$$

associated to G. The exact sequence $0 \to G^{\circ} \to G \to G^{\text{ét}} \to 0$ (5.5.1) induces an exact sequence of I-modules

(7.8.2) $$0 \to \mathrm{T}_p(G^{\circ}) \to \mathrm{T}_p(G) \to \mathrm{T}_p(G^{\text{ét}}) \to 0,$$

where $\mathrm{T}_p(G^\circ)$ and $\mathrm{T}_p(G^{\text{ét}})$ are free $\mathbb{Z}_p$-modules of rank 1. Note that I acts trivially on $\mathrm{T}_p(G^{\text{ét}})$, *i.e.* we have an isomorphism $\mathrm{T}_p(G^{\text{ét}}) \simeq \mathbb{Z}_p$ as I-modules. Under a basis adapted to the filtration (7.8.2), the action of $g \in I$ on $\mathrm{T}_p(G)$ is given by

$$\rho(g) = \begin{pmatrix} \chi(g) & c(g) \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p).$$

The map $g \mapsto \chi(g)$ defines a character $\chi : I \to \mathbb{Z}_p^\times$, which gives the action of I on $\mathrm{T}_p(G^\circ)$; we write $\mathrm{T}_p(G^\circ) = \mathbb{Z}_p(\chi)$. The map $g \mapsto c(g)$ is a continuous 1-cocycle of I with values in $\mathbb{Z}_p(\chi)$, which defines a cohomology class

$$c \in \mathrm{H}^1(I, \mathbb{Z}_p(\chi)). \tag{7.8.3}$$

Proposition 7.9. (a) *The homomorphism $\chi : I \to \mathbb{Z}_p^\times$ is surjective.*

(b) *Let J be the kernel of χ, Γ be the quotient group I/J. Then the image of the cohomologoy class c by the canonical homomorphism*

$$\mathrm{H}^1(I, \mathbb{Z}_p(\chi)) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(J, \mathbb{Z}_p(\chi)) \xrightarrow{\iota} \mathrm{H}^1(J, \mathbb{F}_p(\overline{\chi}))$$

is not zero, where $\overline{\chi} : I \to \mathbb{F}_p^\times$ is induced by χ, and ι is the canonical reduction map.

Proof. Statement (a) is an immediate consequence of Lemma 7.7 and Igusa's theorem 5.14 applied to G°. For statement (b), we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(\Gamma, \mathbb{Z}_p(\chi)) \arrow[r, "\mathrm{Inf}"] \arrow[d] & \mathrm{H}^1(I, \mathbb{Z}_p(\chi)) \arrow[r, "\mathrm{Res}"] \arrow[d] & \mathrm{H}^1(J, \mathbb{Z}_p(\chi)) \arrow[d] \\
0 \arrow[r] & \mathrm{H}^1(\Gamma, \mathbb{F}_p(\overline{\chi})) \arrow[r, "\mathrm{Inf}"] & \mathrm{H}^1(I, \mathbb{F}_p(\overline{\chi})) \arrow[r, "\mathrm{Res}"] & \mathrm{H}^1(J, \mathbb{F}_p(\overline{\chi})),
\end{tikzcd}$$

where vertical arrows are the canonical reductions mod p, and "Inf" (*resp.* "Res") means inflation (*resp.* restriction) maps in Galois cohomology. By Lemma 5.17, we have $\mathrm{H}^1(\Gamma, \mathbb{F}_p(\overline{\chi})) = 0$. To prove (b), it suffices to show that the canonical image of c in $\mathrm{H}^1(I, \mathbb{F}_p(\overline{\chi}))$, denoted by $\overline{c}$, is not zero. But $\overline{c}$ is nothing than the cohomology class (5.15.3). Hence by 5.18 and 7.7(a), we only need to find an $\alpha \in E$ such that $\mathtt{v}(f(\alpha)) = 1$, where $f(X) = X^{p^2} + t_2 X^p + t_1 X \in A[X]$. Let $\zeta \in E$ be such that $\zeta^{p-1} = -1$, and $t_2' \in E$ be a $p(p-1)$-th root of t_2 ; put $\alpha = \zeta t_2'$. Then we have $f(\alpha) = t_1 \alpha$, and hence $\mathtt{v}(f(\alpha)) = 1$. □

Corollary 7.10. *Let (δ_1, δ_2) be a basis of $\mathrm{T}_p(G)$ adapted to the filtration (7.8.2). Then for every integer $n \geq 1$, there exists $g_n \in I$ such that under the basis (δ_1, δ_2), the action of g_n on $\mathrm{T}_p(G)$ is given by a matrix of the form $\rho(g_n) = \begin{pmatrix} 1 + p^n a & p^{n+1} b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{Z}_p$ and a is not divisible by p.*

Proof. Since the image of the cohomology class c in $\mathrm{H}^1(J, \mathbb{F}_p(\overline{\chi}))$ is nontrivial by 7.9(b), there exists a $h \in J$ such that $c(h) = c_0 \cdot \delta_1$ with $c_0 \in \mathbb{Z}_p^\times$. The action of h on $\mathrm{T}_p(G)$ is represented under the basis (δ_1, δ_2) by the matrix $\rho(h) = \begin{pmatrix} 1 & c_0 \\ 0 & 1 \end{pmatrix}$. We fix an integer $n \geq 1$. The surjectivity of χ

(7.9(a)) implies that there exists a $g'_n \in I$ such that $\rho(g'_n) = \begin{pmatrix} 1+p^n a & b' \\ 0 & 1 \end{pmatrix}$, where $a, b' \in \mathbb{Z}_p$ and a is not divisible by p. Then for any $m \in \mathbb{Z}$, we have

$$\rho(g'_n h^m) = \begin{pmatrix} 1+p^n a & b' + (1+p^n a) m c_0 \\ 0 & 1 \end{pmatrix}.$$

As c_0 is invertible in $\mathbb{Z}_p$, there exists an integer m_0 such that $b' + (1+p^n a) m_0 c_0$ is divisible by p^{n+1}. Then the element $g_n = g'_n h^{m_0} \in I$ answers the question. □

7.11. End of the Proof of 1.7. It suffices to verify the two conditions of Lemma 6.3 for the homomorphism

$$\rho^{1/3} : \pi_1(\mathbf{U}^{1/3}, \overline{\eta}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G}^{1/3})) \simeq \mathrm{GL}_2(\mathbb{Z}_p).$$

The first condition of 6.3 is implied by Prop. 1.9(c). Let $f|_\eta : \eta \to \mathbf{U}^{1/3}$ be the restriction of the morphism f (7.6.1) to the generic point of S. We apply the functoriality of monodromy (7.2.2) to $f|_\eta$ and the ordinary BT-group $\mathbf{G}^{1/3}_{\mathbf{U}^{1/3}} = \mathbf{G}^{1/3} \times_{\mathbf{S}^{1/3}} \mathbf{U}^{1/3}$ over $\mathbf{U}^{1/3}$. Then the image $\mathrm{Im}(\rho)$ (7.8.1) is a subgroup of $\mathrm{Im}(\rho^{1/3})$. Therefore, Lemma 7.10 implies that condition (ii) of 6.3 is satisfied. This finishes the proof of 1.7.

References

[1] J. Achter and P. Norman, Local monodromy of p-divisible groups, Preprint, (2006).

[2] P. Berthelot, Théorie de Dieudonné sur un anneau de valuation parfait, *Ann. Scient. E.N.S*, 4ème série, **13**, (1980), 225-268.

[3] P. Berthelot, L. Breen and W. Messing, *Théorie de Dieudonné Cristalline II*, Lect. notes in Math. **930**, Springer-Verlag, (1982).

[4] N. Bourbaki, *Algèbre Commutative*, Masson, Paris (1985).

[5] L. Chai, Methods for p-adic monodromy, Preprint, (2006).

[6] P. Deligne and K. Ribet, Values of abelian L-functions at negative integers over totally real fields. *Inven. Math.* **59**, (1980), 227-286.

[7] M. Demazure, *Lectures on p-Divisible Groups*, Lect. notes in Math. **302**, Springer-Verlag, (1972).

[8] M. Demazure and A. Grothendieck, *Schéma en Groupes* I (SGA 3_I) , Lect. notes in Math. **151**, Springer-Verlag, (1970).

[9] T. Ekedahl, The action of monodromy on torsion points of Jacobians, *Arithmetic Algebraic Geometry*, G. van der Geer, F. Oort and J. Steenbrink, ed. Progress in Math. **89**, Birkhäuser, (1991), 41-49.

[10] G. Faltings and L. Chai, *Degeneration of Abelian Varieties*, Ergebnisse Bd **22**, Springer-Verlag,(1990).

[11] H. Gross, Ramification in p-adic Lie extensions, *Journée de Géométrie Algébrique de Rennes III, Astérisque* **65**, (1979), 81-102.

[12] A. Grothendieck, *Groupes de Barsotti-Tate et Cristaux de Dieudonné*, les Presses de l'Université de Montréal, (1974).

[13] H. Hida p-adic automorphic forms on reductive groups, *Astérisque* **296** (2005), 147-254.

[14] L. Illusie, Déformations de groupes de Barsotti-Tate (d'après A. Grothendieck), *Astérisque* **127** (1985), 151-198.

[15] J. Igusa, On the algebraic theory of elliptic modular functions. *J. Math. Soc. Japan* **20** (1968), 96-106.

[16] A. J. de Jong, Crystalline Diedonné module theory via formal and rigid geometry, *Publ. Math. Inst. Hautes Étud. Sci.* **82** (1995), 5-96.

[17] N. Katz, p-adic properties of modular schemes and modular forms, in *Modular Functions of One Variable III*, Lect. notes in Math. **350**, Springer-Verlag, (1973).

[18] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inven. Math.* **15** (1972), 259-331.

[19] J. P. Serre, *Corps Locaux*, Hermann, Paris, (1968).

Sous-groupe canonique et monodromie p-adique des groupes de Barsotti-Tate

RÉSUMÉ. Cette thèse est consacrée à deux problèmes indépendants sur les groupes de Barsotti-Tate. Dans la première partie, on considère un groupe de Barsotti-Tate tronqué d'échelon 1, noté G, sur un trait complet de caractéristiques mixtes, à corps résiduel parfait. On s'intéresse à une conjecture de Lubin sur l'existence d'un sous-groupe canonique de G qui relève le noyau du Frobenius de sa fibre spéciale. Si G est "proche d'un Barsotti-Tate ordinaire", une condition qu'on peut exprimer explicitement en terme de la valuation d'un certain déterminant, on montre qu'un cran précis de la filtration canonique de G, introduite par Abbes-Saito, répond à la question. Dans la seconde partie, on se donne k un corps algébriquement clos de caractéristique $p > 0$, et pour tout nombre rationnel $\lambda \in (0, 1)$, on considère G^λ le groupe de Barsotti-Tate connexe sur k dont le module de Dieudonné est monogène et isocline de pente λ. On note ρ^λ la représentation de monodromie associée à la déformation universelle en caractéristique $p > 0$ de G^λ, au-dessus du lieu ordinaire. Inspiré par un célèbre théorème d'Igusa, on conjecture que ρ^λ est surjective. On démontre la conjecture pour $\lambda = 1/3$, et on donne des résultats partiels sur la réduction modulo p de ρ^λ pour tout λ. Le théorème d'Igusa correspond à $\lambda = 1/2$.

Canonical subgroup and p-adic monodromy of Barsotti-Tate groups

ABSTRACT. In this thesis, we study two independant problems on Barsotti-Tate groups. In the first part, we consider a truncated Barsotti-Tate group G of level 1, over a complete discrete valuation ring of mixed characteristic, with perfect residue field. We are interested in a conjecture of Lubin on the existence of a canonical subgroup of G lifting the kernel of the Frobenius of its special fibre. If we assume that G is "not far from being ordinary", a condition that can be expressed in terms of the valuation of a certain determinant, we prove that a precise level of the Abbes-Saito canonical filtration of G answer the question. In the second part, we fix an algebraically closed field k of characteristic $p > 0$, and for each rational number $\lambda \in (0, 1)$, we consider the Barsotti-Tate group G^λ over k whose Dieudonné module is monogenic and isoclinic of slope λ. Let ρ^λ be the monodromy representation associated to the universal deformation of G^λ over the ordinary locus. Inspired by a famous theorem of Igusa, we conjecture that ρ^λ is surjective for all $\lambda \in (0, 1)$. We prove the conjecture for $\lambda = 1/3$, and we give some partial results on the reducton modulo p of ρ^λ for a general slope λ. Igusa's theorem corresponds to $\lambda = 1/2$.

DISCIPLINE : Mathématiques

MOTS-CLÉS : groupes de Barsotti-Tate, sous-groupe canonique, filtration canonique, monodromie p-adique, déformation universelle, morphisme de Hasse-Witt.

KEYWORDS : Barsotti-Tate groups, canonical subgroup, canonical filtration, p-adic monodromy, universal deformation, Hasse-Witt map.

Laboratoire Analyse, Géométrie et Applications, UMR 7539,
Institut Galilée, Université PARIS 13,
99 avenue Jean-Baptiste Clément
93430 Villetaneuse (France)