p-Adic Monodromy of the Universal Deformation of a HW-Cyclic Barsotti-Tate Group

Yichao Tian

Received: September 5, 2009

Communicated by Peter Schneider

Abstract. Let k be an algebraically closed field of characteristic $p>0$, and G be a Barsotti-Tate over k. We denote by $\mathbf{S}$ the "algebraic" local moduli in characteristic p of G, by $\mathbf{G}$ the universal deformation of G over $\mathbf{S}$, and by $\mathbf{U}\subset\mathbf{S}$ the ordinary locus of $\mathbf{G}$. The étale part of $\mathbf{G}$ over $\mathbf{U}$ gives rise to a monodromy representation $\rho_{\mathbf{G}}$ of the fundamental group of $\mathbf{U}$ on the Tate module of $\mathbf{G}$. Motivated by a famous theorem of Igusa, we prove in this article that $\rho_{\mathbf{G}}$ is surjective if G is connected and HW-cyclic. This latter condition is equivalent to saying that Oort's a-number of G equals 1, and it is satisfied by all connected one-dimensional Barsotti-Tate groups over k.

2000 Mathematics Subject Classification: 13D10, 14L05, 14H30, 14B12, 14D15, 14L15

Keywords and Phrases: Barsotti-Tate groups (p-divisible groups), p-adic monodromy representation, universal deformation, Hasse-Witt maps.

1. Introduction

1.1. A classical theorem of Igusa says that the monodromy representation associated with a versal family of ordinary elliptic curves in characteristic $p>0$ is surjective [Igu, Ka2]. This important result has deep consequences in the theory of p-adic modular forms, and inpsired various generalizations. Faltings and Chai [Ch2, FC] extended it to the universal family over the moduli space of higher dimensional principally polarized ordinary abelian varieties in characteristic p, and Ekedahl [Eke] generalized it to the jacobian of the universal n-pointed curve in characteristic p, equipped with a symplectic level structure. Recently, Chai and Oort [CO] proved the maximality of the p-adic monodromy over each "central leaf" in the moduli space of abelian varieties which is not contained in the supersingular locus. We refer to Deligne-Ribet [DR] and Hida [Hid] for other generalizations to some moduli spaces of PEL-type and their arithmetic applications. Though it has been formulated in a global setting, the proof of Igusa's theorem is purely local, and it has got also local generalizations. Gross [Gro] generalized it to one-dimensional formal $\mathscr{O}$-modules over a complete discrete valuation ring of characteristic p, where $\mathscr{O}$ is the integral closure of $\mathbb{Z}_p$ in a finite extension of $\mathbb{Q}_p$. We refer to Chai [Ch2] and Achter-Norman [AN] for more results on local monodromy of Barsotti-Tate groups. Motivated by these results, it has been longly expected/conjectured that the monodromy of a *versal* family of ordinary Barsotti-Tate groups in characteristic $p > 0$ is maximal. The aim of this paper is to prove the surjectivity of the monodromy representation associated with the universal deformation in characteristic p of a certain class of Barsotti-Tate groups.

1.2. To describe our main result, we introduce first the notion of HW-cyclic Barsotti-Tate groups. Let k be an algebraically closed field of characteristic $p > 0$, and G be a Barsotti-Tate group over k. We denote by $G^\vee$ the Serre dual of G, and by $\mathrm{Lie}(G^\vee)$ its Lie algebra. The Frobenius homomorphism of G (or dually the Verschiebung of $G^\vee$) induces a semi-linear endomorphism φ_G on $\mathrm{Lie}(G^\vee)$, called the Hasse-Witt map of G (2.6.1). We say that G is *HW-cyclic*, if $c = \dim(G^\vee) \geq 1$ and there is a $v \in \mathrm{Lie}(G^\vee)$ such that $v, \varphi_G(v), \cdots, \varphi_G^{c-1}(v)$ form a basis of $\mathrm{Lie}(G^\vee)$ over k (4.1). We prove in 4.7 that G is HW-cyclic and non-ordinary if and only if the a-number of G, defined previously by Oort, equals 1. Basic examples of HW-cyclic Barsotti-Tate groups are given as follows. Let r, s 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 whose (contravariant) Dieudonné module is generated by an element e over the non-commutative Dieudonné ring with the relation $(F^{r-s} - V^s) \cdot e = 0$ (4.10). It is easy to see that G^λ is HW-cyclic for any $0 < \lambda < 1$. Any connected Barsotti-Tate group over k of dimension 1 and height h is isomorphic to $G^{1/h}$ [Dem, Chap.IV §8].

Let G be a Barsotti-Tate group of dimension d and height $c+d$ over k; assume $c \geq 1$. We denote by $\mathbf{S}$ the "algebraic" local moduli of G in characteristic p, and by $\mathbf{G}$ be the universal deformation of G over $\mathbf{S}$ (cf. 3.8). The scheme $\mathbf{S}$ is affine of ring $R \simeq k[[(t_{i,j})_{1\leq i\leq c, 1\leq j\leq d}]]$, and the Barsotti-Tate group $\mathbf{G}$ is obtained by algebraizing the formal universal deformation of G over $\mathrm{Spf}(R)$ (3.7). Let $\mathbf{U}$ be the ordinary locus of $\mathbf{G}$ (*i.e.* the open subscheme of $\mathbf{S}$ parametrizing the ordinary fibers of $\mathbf{G}$), and $\overline{\eta}$ a geometric point over the generic point of $\mathbf{U}$. For any integer $n \geq 1$, we denote by $\mathbf{G}(n)$ the kernel of the multiplication by p^n on $\mathbf{G}$, and by

$$\mathrm{T}_p(\mathbf{G}, \overline{\eta}) = \varprojlim_n \mathbf{G}(n)(\overline{\eta})$$

the Tate module of $\mathbf{G}$ at $\overline{\eta}$. This is a free $\mathbb{Z}_p$-module of rank c. We consider the monodromy representation attached to the étale part of $\mathbf{G}$ over $\mathbf{U}$

$$\rho_{\mathbf{G}} : \pi_1(\mathbf{U}, \overline{\eta}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G}, \overline{\eta})) \simeq \mathrm{GL}_c(\mathbb{Z}_p). \tag{1.2.1}$$

The aim of this paper is to prove the following :

Theorem 1.3. *If G is connected and HW-cyclic, then the monodromy representation $\rho_{\mathbf{G}}$ is surjective.*

Igusa's theorem mentioned above corresponds to Theorem 1.3 for $G = G^{1/2}$ (cf. 5.7). My interest in the p-adic monodromy problem started with the second part of my PhD thesis [Ti1], where I guessed 1.3 for $G = G^{\lambda}$ with $0 < \lambda < 1$ and proved it for $G^{1/3}$. After I posted the manuscript on ArXiv [Ti2], Strauch proved the one-dimensional case of 1.3 by using Drinfeld's level structures [Str, Theorem 2.1]. Later on, Lau [Lau] proved 1.3 without the assumption that G is HW-cyclic. By using the Newton stratification of the universal deformation space of G due to Oort, Lau reduced the higher dimensional case to the one-dimensional case treated by Strauch. In fact, Strauch and Lau considered more generally the monodromy representation over each p-rank stratum of the universal deformation space. In this paper, we provide first a different proof of the one-dimensional case of 1.3. Our approach is purely characteristic p, while Strauch used Drinfeld's level structure in characteristic 0. Then by following Lau's strategy, we give a new (and easier) argument to reduce the general case of 1.3 to the one-dimensional case for HW-cyclic groups. The essential part of our argument is a versality criterion by Hasse-Witt maps of deformations of a connected one-dimensional Barsotti-Tate group (Prop. 4.11). This criterion can be considered as a generalization of another theorem of Igusa which claims that the Hasse invariant of a versal family of elliptic curves in characteristic p has simple zeros. Compared with Strauch's approach, our characteristic p approach has the advantage of giving also results on the monodromy of Barsotti-Tate groups over a discrete valuation ring of characteristic p.

1.4. Let $A = k[[\pi]]$ be the ring of formal power series over k in the variable π, K its fraction field, and $\mathtt{v}$ the valuation on K normalized by $\mathtt{v}(\pi) = 1$. We fix an algebraic closure $\overline{K}$ of K, and let 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, and $I_t = I/I_p$ the tame inertia group. 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 its Serre dual, $\mathrm{Lie}(G^{\vee})$ the Lie algebra of $G^{\vee}$, and φ_G the Hasse-Witt map of G, *i.e.* the semi-linear endomorphism of $\mathrm{Lie}(G^{\vee})$ induced by the Frobenius of G. We define $h(G)$ to be the valuation of the determinant of a matrix of φ_G, and call it the *Hasse invariant* of G (5.4). We see easily that $h(G) = 0$ if and only if G is ordinary over S, and $h(G) < \infty$ if and only if G is generically ordinary. If G is connected of height 2 and dimension 1, then $h(G) = 1$ is equivalent to that G is versal (5.7).

Proposition 1.5. *Let $S = \mathrm{Spec}(A)$ be as above, G be a connected HW-cyclic Barsotti-Tate group with Hasse invariant $h(G) = 1$, and $G(1)$ the kernel of the multiplication by p on G. Then the action of I on $G(1)(\overline{K})$ is tame; moverover,*

$G(1)(\overline{K})$ is an $\mathbb{F}_{p^c}$-vector space of dimension 1 on which the induced action of I_t is given by the surjective character $\theta_{p^c-1} : I_t \to \mathbb{F}_{p^c}^{\times}$.

This proposition is an analog in characteristic p of Serre's result [Se3, Prop. 9] on the tameness of the monodromy associated with one-dimensional formal groups over a trait of mixed characteristic. We refer to 5.8 for the proof of this proposition and more results on the p-adic monodromy of HW-cyclic Barsotti-Tate groups over a trait in characteristic p.

1.6. This 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 Dieudonné theory and the deformation theory of Barsotti-Tate groups. In Section 4, after establishing some basic properties of HW-cyclic groups, we give the fundamental relation between the versality of a Barsotti-Tate group and the coefficients of its Hasse-Witt matrix (Prop. 4.11). Section 5 is devoted to the study of the monodromy of a HW-cyclic Barsotti-Tate group over a complete trait of characteristic p. Section 6 is totally elementary, and contains a criterion (6.3) for the surjectivity of a homomorphism from a profinite group to $\mathrm{GL}_n(\mathbb{Z}_p)$. Section 7 is the heart of this work, and it contains a proof of Theorem 1.3 in the one-dimensional case. Finally in Section 8, we follow Lau's strategy and complete the proof of 1.3 by reducing the general case to the one-dimensional case treated in Section 7.
The proof in Section 7 of 1.3 in the one-dimensional case is based on an induction on the height $n+1 \geq 2$ of G. The case $n = 1$ is just the classical Igusa's theorem (5.7). For $n \geq 2$, by lemmas 6.3 and 6.5, it suffices to prove the following two statements: (a) the image of reduction modulo p of $\rho_{\mathbf{G}}$ contains a non-split Cartan subgroup; (b) under a suitable basis, the image of $\rho_{\mathbf{G}}$ contains all matrix of the form $\begin{pmatrix} B & b \\ 0 & 1 \end{pmatrix}$ with $B \in \mathrm{GL}_{n-1}(\mathbb{Z}_p)$ and $b \in \mathrm{M}_{(n-1)\times 1}(\mathbb{Z}_p)$. The first statement follows easily from 1.5 by considering a certain base change of $\mathbf{G}$ to a complete discrete valuation ring. To prove (b), we consider the formal completion $\mathrm{Spec}(R')$ of the localization of the local moduli $\mathbf{S} = \mathrm{Spec}(R)$ of G at the generic point of the locus where the universal deformation $\mathbf{G}$ has p-rank ≤ 1 (7.4). The ring R' is a complete regular ring of dimension $n-1$, and the Barsotti-Tate group $\mathscr{G}' = \mathbf{G} \otimes_R R'$ has a connected part of height n and an étale part of height 1. Let K_0 be the residue field of R', and $\overline{K}_0$ an algebraic closure of K_0. In order to apply the induction hypothesis, we consider the set of k-algebra homomorphisms $\sigma : R' \to \widetilde{R'} = \overline{K}_0[[t_1, \cdots, t_{n-1}]]$ lifting the natural inclusion $K_0 \to \overline{K}_0$. The key point is that, the natural map $\sigma \mapsto \mathscr{G}_{\widetilde{R'},\sigma} = \mathscr{G}' \otimes_{R',\sigma} \widetilde{R'}$ gives a bijection between the set of such σ's and the set of deformations of $\mathscr{G}_{\overline{K}_0} = \mathscr{G}' \otimes_{R'} \overline{K}_0$ to $\widetilde{R'}$; moreover, we can compute explicitly the Hasse-Witt map of the connected component $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}$ of $\mathscr{G}_{\widetilde{R'},\sigma}$ (Lemma 7.8). From the versality criterion for one-dimensional Barsotti-Tate groups in terms of the Hasse-Witt map established in Section 4 (Prop. 4.11), it follows immediately that there exists a σ such that the Barsotti-Tate group $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}$, which

is connected and one-dimensional of height n, is the universal deformation of its closed fiber. We fix such a σ. Then the set of all σ' with $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma'} \simeq \mathscr{G}^{\circ}_{\widetilde{R'},\sigma}$ as deformations of their common closed fiber is actually a group isomorphic to $\mathrm{Ext}^1_{\widetilde{R'}}(\mathbb{Q}_p/\mathbb{Z}_p, \mathscr{G}^{\circ}_{\widetilde{R'},\sigma})$ (Prop. 3.10). Let σ_1 be the element corresponding to neutral element in $\mathrm{Ext}^1_{\widetilde{R'}}(\mathbb{Q}_p/\mathbb{Z}_p, \mathscr{G}^{\circ}_{\widetilde{R'},\sigma})$. Applying the induction hypothesis to $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma_1}$, we see that the monodromy group of $\mathscr{G}_{\widetilde{R'},\sigma_1}$, hence that of $\mathbf{G}$, contains the subgroup $\begin{pmatrix} \mathrm{GL}_{n-1}(\mathbb{Z}_p) & 0 \\ 0 & 1 \end{pmatrix}$ under a suitable basis of the Tate module (7.5.3). In order to conclude the proof, we need another σ_2 such that $\mathscr{G}_{\widetilde{R'},\sigma_2}$ has the same connected component as $\mathscr{G}_{\widetilde{R'},\sigma_1}$, and that the induced extension between the Tate module of the étale part of $\mathscr{G}_{\widetilde{R'},\sigma_2}$ and that of $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma_2}$ is non-trivial after reduction modulo p (see 7.5 and 7.5.4). To verify the existence of such a σ_2, we reduce the problem to a similar situation over a complete trait of characteristic p (see 7.9), and we use a criterion of non-triviality of extensions by Hasse-Witt maps (5.12).

1.7. Acknowledgement. This paper is an expanded version of the second part of my Ph.D. thesis at University Paris 13. I would like to express my great gratitude to my thesis advisor Prof. A. Abbes for his encouragement during this work, and also for his various helpful comments on earlier versions of this paper. I also thank heartily E. Lau, F. Oort and M. Strauch for interesting discussions and valuable suggestions.

1.8. 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. If $S = \mathrm{Spec}(A)$ is affine and there is no risk of confusions, we also use ω_G and $\mathrm{Lie}(G)$ to denote the corresponding A-modules of global sections. 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. For an $\mathscr{O}_S$-module M, we denote by $M^{(p)} = \mathscr{O}_S \otimes_{F_S} M$ the scalar extension of M by the absolute Frobenius of $\mathscr{O}_S$. If $\varphi : M \to N$ be a semi-linear homomorphism of $\mathscr{O}_S$-modules, we denote by $\widetilde{\varphi} : M^{(p)} \to N$ the linearization of φ, *i.e.* we have $\widetilde{\varphi}(\lambda \otimes x) = \lambda \cdot \varphi(x)$, where λ (*resp.* x) is a local section of $\mathscr{O}_S$ (*resp.* of M).
Starting from Section 5, k will denote an algebraically closed field of characteristic $p > 0$.

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 [Ill, 2.1]

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

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. Since $\mathbb{G}_a^{(p)} \simeq \mathbb{G}_a$, the Frobenius homomorphism of $\mathbb{G}_a$ induces an endomorphism

$$\varphi_G : \mathrm{Lie}(G^\vee) \to \mathrm{Lie}(G^\vee), \tag{2.1.2}$$

semi-linear with respect to the absolute Frobenius map $F_S : \mathscr{O}_S \to \mathscr{O}_S$; we call it the *Hasse-Witt* map of G. By the functoriality of Frobenius, φ_G is also the canonical map induced by the Frobenius of G, or dually by the Verschiebung of $G^\vee$.

2.2. By a *commutative p-Lie algebra* over S, we mean a pair (L, φ), where L is an $\mathscr{O}_S$-module locally free of finite type, 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 confusions, 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-$\mathfrak{Lie}_S$. We denote by

$$\mathscr{U}(L) = \mathrm{Sym}(L) = \oplus_{n\geq 0} \mathrm{Sym}^n(L),$$

the symmetric algebra of L over $\mathscr{O}_S$. Let $\mathscr{I}_p(L)$ be the ideal sheaf of $\mathscr{U}(L)$ defined, for an open subset $V \subset S$, by

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

where $x^{\otimes p} = x \otimes x \otimes \cdots \otimes x \in \Gamma(V, \mathrm{Sym}^p(L))$. We put $\mathscr{U}_p(L) = \mathscr{U}(L)/\mathscr{I}_p(L)$, and call it the *p-enveloping algebra of* (L, φ). 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 $V_G : G^{(p)} \to G$ is the zero homomorphism. We denote by $\mathfrak{G}\mathrm{V}_S$ the category of such objects. For an object G of $\mathfrak{G}\mathrm{V}_S$, the Frobenius $F_{G^\vee}$ of $G^\vee$ is zero, so the Lie algebra $\mathrm{Lie}(G^\vee)$ is locally free of finite type over $\mathscr{O}_S$ ([DG] $\mathrm{VII_A}$ 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 ([DG] $\mathrm{VII_A}$, 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* $(L, \varphi) \mapsto \mathrm{Spec}(\mathscr{U}_p(L))$.

2.4. Assume $S = \mathrm{Spec}(A)$ affine. Let (L, φ) be an object of p-$\mathfrak{Lie}_S$ 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

$1 \le j \le n$. Then the group scheme attached to (L, φ) is explicitly given by

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

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 $(h_{ij})_{1 \le i,j \le n}$ is invertible. This condition is equivalent to that the linearization of φ is an isomorphism.

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 an isomorphism.*

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. $\square$

2.6. Let G be a BT-group over S of height $c + d$ and dimension d. The Lie algebra $\mathrm{Lie}(G^\vee)$ is an $\mathscr{O}_S$-module locally free of rank c, and canonically identified with $\mathrm{Lie}(G^\vee(1))$([BBM] 3.3.2). We define the *Hasse-Witt map* of G

$$\varphi_G : \mathrm{Lie}(G^\vee) \to \mathrm{Lie}(G^\vee) \tag{2.6.1}$$

to be that of $G(1)$ (2.1.2).

2.7. Let k be a field of characteristic $p > 0$, G be a BT-group over k. Recall that we have a canonical exact sequence of BT-groups over k

$$0 \to G^\circ \to G \to G^{\text{ét}} \to 0 \tag{2.7.1}$$

with G° connected and $G^{\text{ét}}$ étale ([Dem] Chap.II, §7). This induces an exact sequence of Lie algebras

$$0 \to \mathrm{Lie}(G^{\text{ét}\vee}) \to \mathrm{Lie}(G^\vee) \to \mathrm{Lie}(G^{\circ\vee}) \to 0, \tag{2.7.2}$$

compatible with Hasse-Witt maps.

Proposition 2.8. *Let k be a field of characteristic $p > 0$, G be a BT-group over k. Then* $\mathrm{Lie}(G^{\text{ét}\vee})$ *is the unique maximal k-subspace V of* $\mathrm{Lie}(G^\vee)$ *with the following properties:*
(a) *V is stable under φ_G;*
(b) *the restriction of φ_G to V is injective.*

Proof. It is clear that $\mathrm{Lie}(G^{\text{ét}\vee})$ satisfies property (a). We note that the Verschiebung of $G^{\text{ét}}(1)$ vanishes; so $G^{\text{ét}}(1)$ is in the category $\mathfrak{G}\mathrm{V}_{\mathrm{Spec}(k)}$. Since k is a field, 2.5 implies that the restriction of φ_G to $\mathrm{Lie}(G^{\text{ét}\vee})$, which coincides with $\varphi_{G^{\text{ét}}}$, is injective. This proves that $\mathrm{Lie}(G^{\text{ét}\vee})$ verifies (b). Conversely, let V be an arbitrary k-subspace of $\mathrm{Lie}(G^\vee)$ with properties (a) and (b). We have to show that $V \subset \mathrm{Lie}(G^{\text{ét}\vee})$. Let σ be the Frobenius endomorphism of k. If M is a k-vector space, for each integer $n \ge 1$, we put $M^{(p^n)} = k \otimes_{\sigma^n} M$, *i.e.* we have $1 \otimes ax = \sigma^n(a) \otimes x$ in $k \otimes_{\sigma^n} M$ for $a \in k, x \in M$. Since $\varphi_G|_V : V \to V$ is injective by assumption, the linearization $\widetilde{\varphi_G^n}|_{V^{(p^n)}} : V^{(p^n)} \to V$ of $\varphi_G^n|_V$

is injective (hence bijective) for any $n \geq 1$. We have $V = \widetilde{\varphi^n_G}(V^{(p^n)})$. Since G° is connected, there is an integer $n \geq 1$ such that the n-th iterated Frobenius $F^n_{G^\circ(1)} : G^\circ(1) \to G^\circ(1)^{(p^n)}$ vanishes. Hence by definition, the linearized n-iterated Hasse-Witt map $\widetilde{\varphi^n_{G^\circ}} : \mathrm{Lie}(G^{\circ\vee})^{(p^n)} \to \mathrm{Lie}(G^{\circ\vee})$ is zero. By the compatibility of Hasse-Witt maps, we have $\widetilde{\varphi^n_G}(\mathrm{Lie}(G^\vee)^{(p^n)}) \subset \mathrm{Lie}(G^{\text{ét}\vee})$; in particular, we have $V = \widetilde{\varphi^n_G}(V^{(p^n)}) \subset \mathrm{Lie}(G^{\text{ét}\vee})$. This completes the proof. □

Corollary 2.9. *Let k be a field of characteristic $p > 0$, G be a BT-group over k. Then G is connected if and only if φ_G is nilpotent.*

Proof. In the proof of the proposition, we have seen that the Hasse-Witt map of the connected part of G is nilpotent. So the "only if" part is verified. Conversely, if φ_G is nilpotent, $\mathrm{Lie}(G^{\text{ét}\vee})$ is zero by the proposition. Therefore G is connected. □

Definition 2.10. Let S be a scheme of characteristic $p > 0$, G be a BT-group over S. We say that G is *ordinary* if there exists an exact sequence of BT-groups over S

$$0 \to G^{\text{mult}} \to G \to G^{\text{ét}} \to 0, \tag{2.10.1}$$

such that G^{mult} is multiplicative and $G^{\text{ét}}$ is étale.

We note that when it exists, the exact sequence (2.10.1) is unique up to a unique isomorphism, because there is no non-trivial homomorphisms between a multiplicative BT-group and an étale one in characteristic $p > 0$. The property of being ordinary is clearly stable under arbitrary base change and Serre duality. If S is the spectrum of a field of characteristic $p > 0$, G is ordinary if and only if its connected part G° is of multiplicative type.

Proposition 2.11. *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 φ_G is an isomorphism.*

First, we prove the following lemmas.

Lemma 2.12. *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 $H \otimes_T \kappa(x)$ is unramified over $\kappa(x)$ for every point $x \in T$. Hence the conclusion follows. □

Lemma 2.13. *Let G be a BT-group over S. Then* $\operatorname{Ker} V_G$ *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 zero. Moreover, we have a canonical isomorphism* $(\operatorname{Ker} V_G)^\vee \simeq \operatorname{Ker} F_{G^\vee}$*, which induces an isomorphism of Lie algebras* $\operatorname{Lie}\big((\operatorname{Ker} V_G)^\vee\big) \simeq \operatorname{Lie}(\operatorname{Ker} F_{G^\vee}) = \operatorname{Lie}(G^\vee)$*, and the Hasse-Witt map* (2.1.2) *of* $\operatorname{Ker} V_G$ *is identified with* φ_G (2.6.1).

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

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

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

By Cartier duality, we have $(\operatorname{Ker} V_G)^\vee = \operatorname{Coker}(F_{G^\vee(1)})$. 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

$$\operatorname{Coker}(F_{G^\vee(1)}) \xrightarrow{\sim} \operatorname{Im}(V_{G^\vee(1)}) = \operatorname{Ker} F_{G^\vee(1)} = \operatorname{Ker} F_{G^\vee}. \tag{2.13.1}$$

Hence, we deduce that

$$(\operatorname{Ker} V_G)^\vee \simeq \operatorname{Coker}(F_{G^\vee(1)}) \xrightarrow{\sim} \operatorname{Ker} F_{G^\vee} \hookrightarrow G^\vee(1). \tag{2.13.2}$$

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

$$\operatorname{Lie}\big((\operatorname{Ker} V_G)^\vee\big) \simeq \operatorname{Lie}(\operatorname{Ker} F_{G^\vee}) = \operatorname{Lie}(G^\vee(1)) = \operatorname{Lie}(G^\vee). \tag{2.13.3}$$

It remains to prove the compatibility of the Hasse-Witt maps with (2.13.3). We note that the dual of the morphism (2.13.2) is the canonical map $F : G(1) \to \operatorname{Ker} V_G = \operatorname{Im}(F_{G(1)})$ induced by $F_{G(1)}$. Hence by (2.1.1), the isomorphism (2.13.3) is identified with the functorial map

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

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

Proof of 2.11. (a)⇒(b). Indeed, the ordinarity of G is stable by base change. (b)⇒(c). By Lemma 2.12, it suffices to verify that for every point $x \in S$, the fiber $(\operatorname{Ker} V_G) \otimes_S \kappa(x) \simeq \operatorname{Ker} V_{G_x}$ 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 $\operatorname{Ker} V_{G_x}$ is canonically isomorphic to $\operatorname{Ker} V_{G_x^{\text{ét}}} \subset (G_x^{\text{ét}})^{(p)} \simeq (G_x^{(p)})^{\text{ét}}$, so our assertion follows.
$(c) \Leftrightarrow (d)$. It follows immediately from Lemma 2.13 and Corollary 2.5.
(c)⇔(c'). By 2.12, 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

$$0 \to \operatorname{Ker} F_G \to G(1) \xrightarrow{F} \operatorname{Ker} V_G \to 0, \tag{2.13.4}$$

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

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

where vertical arrows are the Verschiebung homomorphisms. We have seen that $V'' = 0$ (2.13). Therefore, by the snake lemma, we have a long exact sequence

$$\begin{aligned} 0 \to \operatorname{Ker} V' \to \operatorname{Ker} V_{G(1)} \xrightarrow{\alpha} (\operatorname{Ker} V_G)^{(p)} \to \\ \to \operatorname{Coker} V' \to \operatorname{Coker} V_{G(1)} \xrightarrow{\beta} \operatorname{Ker} V_G \to 0, \end{aligned} \tag{2.13.5}$$

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

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

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

$$0 \to \operatorname{Ker} F_G^n \to G(n) \xrightarrow{F^n} \operatorname{Ker} V_G^n \to 0, \tag{2.13.6}$$

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

$$\begin{tikzcd}[column sep=small] G^{(p^n)} \arrow[rr, "V^{n-j}_{G^{(p^j)}}"] \arrow[dr, "V^n_G"'] & & G^{(p^j)} \arrow[dl, "V^j_G"] \\ & G. & \end{tikzcd} \tag{2.13.7}$$

One notices that $\operatorname{Ker} V^{n-j}_{G^{(p^j)}} = (\operatorname{Ker} V^{n-j}_G)^{(p^j)}$ by the functoriality of Verschiebung . Since all maps in (2.13.7) are isogenies, we have an exact sequence

$$0 \to (\operatorname{Ker} V^{n-j}_G)^{(p^j)} \xrightarrow{i'_{n-j,n}} \operatorname{Ker} V^n_G \xrightarrow{p_{n,j}} \operatorname{Ker} V^j_G \to 0. \tag{2.13.8}$$

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

$$i_{n-j,n} : \operatorname{Ker} V^{n-j}_G \xrightarrow{\sim} (\operatorname{Ker} V^{n-j}_G)^{(p^j)} \xrightarrow{i'_{n-j,n}} \operatorname{Ker} V^n_G.$$

We claim that the kernel of the multiplication by p^{n-j} on $\operatorname{Ker} V^n_G$ is $\operatorname{Ker} V^{n-j}_G$. 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)

$$\begin{tikzcd} \operatorname{Ker} V^n_G \arrow[rr] \arrow[dd, "p^{n-j}"'] \arrow[dr, dashed, "p_{n,j}"] & & G^{(p^n)} \arrow[dd, "p^{n-j}"' near start] \arrow[dr, "V^{n-j}_{G^{(p^j)}}"] & \\ & \operatorname{Ker} V^j_G \arrow[rr, dashed] \arrow[dl, dashed, "i_{j,n}"] & & G^{(p^j)} \arrow[dl, "F^{n-j}_{G^{(p^j)}}"] \\ \operatorname{Ker} V^n_G \arrow[rr] & & G^{(p^n)}. & \end{tikzcd} \tag{2.13.9}$$

It follows from (2.13.8) that the subgroup $\operatorname{Ker} V^n_G$ of $G^{(p^n)}$ is sent by $V^{n-j}_{G^{(p^j)}}$ onto $\operatorname{Ker} V^j_G$. Therefore diagram (2.13.9) remains commutative when completed by the dotted arrows, hence our claim. It follows from the claim that $(\operatorname{Ker} V^n_G)_{n\geq 1}$ constitutes an étale BT-group over S, denoted by $G^{\text{ét}}$. By duality, we have an exact sequence

$$0 \to \operatorname{Ker} F^j_G \to \operatorname{Ker} F^n_G \to (\operatorname{Ker} F^{n-j}_G)^{(p^j)} \to 0. \tag{2.13.10}$$

Condition (c') implies by induction that $\operatorname{Ker} F^n_G$ is of multiplicative type. Hence the j-th iteration of Verschiebung $(\operatorname{Ker} F^{n-j}_G)^{(p^j)} \to \operatorname{Ker} F^{n-j}_G$ is an isomorphism. We deduce from (2.13.10) that $(\operatorname{Ker} F^n_G)_{n\geq 1}$ form a multiplicative BT-group over S that we denote by G^{mult}. Then the exact sequences (2.13.6) give a decomposition of G of the form (2.10.1). $\square$

Corollary 2.14. *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 inclusion $S^{\mathrm{ord}} \to S$ is affine.*

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

3. Preliminaries on Dieudonné Theory and Deformation Theory

3.1. We will use freely the conventions of 1.8. Let S be a scheme of characteristic $p > 0$, G be a Barsotti-Tate group over S, and $\mathbf{M}(G) = \mathbb{D}(G)_{(S,S)}$ be the coherent $\mathscr{O}_S$-module obtained by evaluating the (contravariant) Dieudonné crystal of G at the trivial divided power immersion $S \hookrightarrow S$ [BBM, 3.3.6]. Recall that $\mathbf{M}(G)$ is an $\mathscr{O}_S$-module locally free of finite type satisfying the following properties:
(i) Let $F_M : \mathbf{M}(G)^{(p)} \to \mathbf{M}(G)$ and $V_M : \mathbf{M}(G) \to \mathbf{M}(G)^{(p)}$ be the $\mathscr{O}_S$-linear maps induced respectively by the Frobenius and the Verschiebung of G. We have the following exact sequence:

$$\cdots \to \mathbf{M}(G)^{(p)} \xrightarrow{F_M} \mathbf{M}(G) \xrightarrow{V_M} \mathbf{M}(G)^{(p)} \to \cdots .$$

(ii) There is a connection $\nabla : \mathbf{M}(G) \to \mathbf{M}(G) \otimes_{\mathscr{O}_S} \Omega^1_{S/\mathbb{F}_p}$ for which F_M and V_M are horizontal morphisms.
(iii) We have two canonical filtrations on $\mathbf{M}(G)$ by $\mathscr{O}_S$-modules locally free of finite type:

$$0 \to \omega_G \to \mathbf{M}(G) \to \mathrm{Lie}(G^\vee) \to 0, \tag{3.1.1}$$

called the *Hodge filtration* on $\mathbf{M}(G)$ [BBM, 3.3.5], and the *conjugate filtration* on $\mathbf{M}(G)$

$$0 \to \mathrm{Lie}(G^\vee)^{(p)} \xrightarrow{\phi_G} \mathbf{M}(G) \to \omega_G^{(p)} \to 0, \tag{3.1.2}$$

which is obtained by applying the Dieudonné functor to the exact sequence of finite group schemes $0 \to \mathrm{Ker}\, F_G \to G(1) \to \mathrm{Ker}\, V_G \to 0$ [BBM, 4.3.1, 4.3.6, 4.3.11]. Moreover, we have the following commutative diagram (cf. [Ka1, 2.3.2

and 2.3.4])
(3.1.3)

$$
\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
& \omega_G^{(p)} \arrow[d] & \omega_G \arrow[r, "\psi_G"] \arrow[d] & \omega_G^{(p)} \arrow[d] & \\
{} \arrow[r] & \mathbf{M}(G)^{(p)} \arrow[r, "F_M"] \arrow[d] & \mathbf{M}(G) \arrow[r, "V_M"] \arrow[d] \arrow[ur] & \mathbf{M}(G)^{(p)} \arrow[r] \arrow[d] & {} \\
& \mathrm{Lie}(G^\vee)^{(p)} \arrow[r, "\widetilde{\varphi_G}"] \arrow[d] \arrow[ur, hook, "\phi_G"] & \mathrm{Lie}(G^\vee) \arrow[d] & \mathrm{Lie}(G^\vee)^{(p)} \arrow[d] & \\
& 0 & 0 & 0 &
\end{tikzcd},
$$

where the columns are the Hodge filtrations and the anti-diagonal is the conjugate filtration. By functoriality, we see easily that $\widetilde{\varphi_G}$ above is nothing but the linearization of the Hasse-Witt map φ_G (2.6.1), and the morphism $\psi_G^* : \mathrm{Lie}(G)^{(p)} \to \mathrm{Lie}(G)$, which is obtained by applying the functor $\mathscr{H}om_{\mathscr{O}_S}(\_, \mathscr{O}_S)$ to ψ_G, is identified with the linearization $\widetilde{\varphi_{G^\vee}}$ of $\varphi_{G^\vee}$.
The formation of these structures on $\mathbf{M}(G)$ commutes with arbitrary base changes of S. In the sequel, we will use $(\mathbf{M}(G), F_M, \nabla)$ to emphasize these structures on $\mathbf{M}(G)$.

3.2. In the reminder of this section, k will denote an algebraically closed field of characteristic $p > 0$. Let S be a scheme formally smooth over k such that $\Omega^1_{S/\mathbb{F}_p} = \Omega^1_{S/k}$ is an $\mathscr{O}_S$-module locally free of finite type, *e.g.* $S = \mathrm{Spec}(A)$ with A a formally smooth k-algebra with a finite p-basis over k. Let G be a BT-group over S. We put KS to be the composed morphism

(3.2.1) $$\mathrm{KS} : \omega_G \to \mathbf{M}(G) \xrightarrow{\nabla} \mathbf{M}(G) \otimes_{\mathscr{O}_S} \Omega^1_{S/k} \xrightarrow{pr} \mathrm{Lie}(G^\vee) \otimes_{\mathscr{O}_S} \Omega^1_{S/k}$$

which is $\mathscr{O}_S$-linear. We put $\mathscr{T}_{S/k} = \mathscr{H}om_{\mathscr{O}_S}(\Omega^1_{S/k}, \mathscr{O}_S)$, and define the *Kodaira-Spencer map* of G

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

to be the morphism induced by KS. We say that G is *versal* if Kod is surjective.

3.3. Let r be an integer ≥ 1, $R = k[[t_1, \cdots, t_r]]$, $\mathfrak{m}$ 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 of BT-groups $(G_n)_{n\geq 0}$ over $(S_n)_{n\geq 0}$ equipped with isomorphisms $G_{n+1} \times_{S_{n+1}} S_n \simeq G_n$.

According to [deJ, 2.4.4], *the functor* $G \mapsto (G\times_S S_n)_{n\geq 0}$ *induces 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 $\mathscr{G}$. We say that $\mathscr{G}$ is *versal* over $\mathscr{S}$, if its algebraization G is versal over S. Since S is local, by Nakayama's Lemma, $\mathscr{G}$ or G is versal if and only if the reduction of Kod modulo the maximal ideal

$$\mathrm{Kod}_0 : \mathscr{T}_{S/k}\otimes_{\mathscr{O}_S} k \longrightarrow \mathrm{Hom}_k(\omega_{G_0}, \mathrm{Lie}(G_0^\vee)) \tag{3.3.1}$$

is surjective.

3.4. We recall briefly the deformation theory of a BT-group. Let $\mathfrak{AL}_k$ be the category of local artinian k-algebras with residue field k. We notice that all morphisms of $\mathfrak{AL}_k$ are local. A morphism $A' \to A$ in $\mathfrak{AL}_k$ is called a *small extension*, if it is surjective and its kernel I satisfies $I\cdot\mathfrak{m}_{A'} = 0$, where $\mathfrak{m}_{A'}$ is the maximal ideal of A'.
Let G_0 be a BT-group over k, and A 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 $\phi : G\otimes_A k \xrightarrow{\sim} G_0$. When there is no risk of confusions, we will denote a deformation (G,ϕ) simply by G. Two deformations (G,ϕ) and (G',ϕ') over A are isomorphic if there exists an isomorphism of BT-groups $\psi : G \xrightarrow{\sim} G'$ over A such that $\phi = \phi'\circ(\psi\otimes_A k)$. Let's denote by $\mathcal{D}$ the functor which associates with each object A of $\mathfrak{AL}_k$ the set of isomorphsm classes of deformations of G_0 over A. If $f : A \to B$ is a morphism of $\mathfrak{AL}_k$, then the map $\mathcal{D}(f) : \mathcal{D}(A) \to \mathcal{D}(B)$ is given by extension of scalars. We call $\mathcal{D}$ the *deformation functor* of G_0 over $\mathfrak{AL}_k$.

Proposition 3.5 ([Ill], 4.8). *Let* G_0 *be a BT-group over* k *of dimension* d *and height* $c+d$, $\mathcal{D}$ *be the deformation functor of* G_0 *over* $\mathfrak{AL}_k$.
(i) *Let* $A' \to A$ *be a small extension in* $\mathfrak{AL}_k$ *with ideal* I, $x = (G,\phi)$ *be an element in* $\mathcal{D}(A)$, $\mathcal{D}_x(A')$ *be the subset of* $\mathcal{D}(A')$ *with image* x *in* $\mathcal{D}(A)$. *Then the set* $\mathcal{D}_x(A')$ *is a nonempty homogenous space under the group* $\mathrm{Hom}_k(\omega_{G_0}, \mathrm{Lie}(G_0^\vee))\otimes_k I$.
(ii) *The functor* $\mathcal{D}$ *is pro-representable by a formally smooth formal scheme* $\mathscr{S}$ *over* k *of relative dimension* cd, i.e. $\mathscr{S} = \mathrm{Spf}(R)$ *with* $R \simeq k[[(t_{ij})_{1\leq i\leq c, 1\leq j\leq d}]]$, *and there exists a unique deformation* $(\mathscr{G},\psi)$ *of* G_0 *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* $(G,\phi) = \mathcal{D}(\varphi)(\mathscr{G},\psi)$.
(iii) *Let* $\mathscr{T}_{\mathscr{S}/k}(0) = \mathscr{T}_{\mathscr{S}/k}\otimes_{\mathscr{O}_\mathscr{S}} k$ *be the tangent space of* $\mathscr{S}$ *at its unique closed point,*

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

be the Kodaira-Spencer map 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 difference of deformations*

$$[\mathscr{G}\otimes_R (k[\epsilon]/\epsilon^2)] - [G_0\otimes_k (k[\epsilon]/\epsilon^2)],$$

which is a well-defined element in $\mathrm{Hom}_k(\omega_{G_0}, \mathrm{Lie}(G_0^\vee))$ *by* (i).

Remark 3.6. Let $(e_j)_{1\leq j\leq d}$ be a basis of ω_{G_0}, $(f_i)_{1\leq i\leq c}$ be a basis of $\mathrm{Lie}(G_0^\vee)$. In view of 3.5(iii), we can choose a system of parameters $(t_{ij})_{1\leq i\leq c, 1\leq j\leq d}$ 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 3.7 (Algebraization of the universal deformation). *The assumptions being those of* (3.5), *we put moreover* $\mathbf{S} = \mathrm{Spec}(R)$ *and* $\mathbf{G}$ *the algebraization of the universal formal deformation* $\mathscr{G}$. *Then the BT-group* $\mathbf{G}$ *is versal over* $\mathbf{S}$, *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. By the last remark of 3.3, $\mathbf{G}$ is clearly versal. It remains to prove that it satisfies the universal property in the corollary. 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 3.5(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 3.8. The notations are those of (3.7). 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.

If there is no confusions, we will omit "in characteristic p" for short.

3.9. Let G be a BT-group over k, G° be its connected part, and $G^{\text{ét}}$ be its étale part. Let r be the height of $G^{\text{ét}}$. Then we have $G^{\text{ét}} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r$, since k is algebraically closed. Let $\mathcal{D}_G$ (*resp.* $\mathcal{D}_{G^\circ}$) be the deformation functor of G (*resp.* G°) over $\mathfrak{AL}_k$. If A is an object in $\mathfrak{AL}_k$ and $\mathscr{G}$ is a deformation of G (*resp.* G°) over A, we denote by $[\mathscr{G}]$ its isomorphism class in $\mathcal{D}_G(A)$ (*resp.* in $\mathcal{D}_{G^\circ(A)}$).

Proposition 3.10. *The assumptions are as above, let $\Theta : \mathcal{D}_G \to \mathcal{D}_{G^\circ}$ be the morphism of functors that maps a deformation of G to its connected component.*
(i) *The morphism Θ is formally smooth of relative dimension r.*
(ii) *Let A be an object of $\mathfrak{AL}_k$, and $\mathscr{G}^\circ$ be a deformation of G° over A. Then the subset $\Theta_A^{-1}([\mathscr{G}^\circ])$ of $\mathcal{D}_G(A)$ is canonically identified with $\mathrm{Ext}^1_A(\mathbb{Q}_p/\mathbb{Z}_p, \mathscr{G}^\circ)^r$, where Ext^1_A means the group of extensions in the category of abelian* fppf*-sheaves on* $\mathrm{Spec}(A)$.

Proof. (i) Since $\mathcal{D}_G$ and $\mathcal{D}_{G^\circ}$ are both pro-representable by a noetherian local complete k-algebra and formally smooth over k (3.5), by a formal completion version of [EGA, IV 17.11.1(d)], we only need to check that the tangent map

$$\Theta_{k[\epsilon]/\epsilon^2} : \mathcal{D}_G(k[\epsilon]/\epsilon^2) \to \mathcal{D}_{G^\circ}(k[\epsilon]/\epsilon^2)$$

is surjective with kernel of dimension r over k. By 3.5(iii), $\mathcal{D}_G(k[\epsilon]/\epsilon^2)$ (*resp.* $\mathcal{D}_{G^\circ}(k[\epsilon]/\epsilon^2)$) is isomorphic to $\mathrm{Hom}_k(\omega_G, \mathrm{Lie}(G^\vee))$ (*resp.* $\mathrm{Hom}_k(\omega_{G^\circ}, \mathrm{Lie}(G^{\circ\vee}))$) by the Kodaira-Spencer morphism. In view of the canonical isomorphism $\omega_G \simeq \omega_{G^\circ}$, $\Theta_{k[\epsilon]/\epsilon^2}$ corresponds to the map

$$\Theta'_{k[\epsilon]/\epsilon^2} : \mathrm{Hom}_k(\omega_G, \mathrm{Lie}(G^\vee)) \to \mathrm{Hom}_k(\omega_G, \mathrm{Lie}(G^{\circ\vee}))$$

induced by the canonical surjection $\mathrm{Lie}(G^\vee) \to \mathrm{Lie}(G^{\circ\vee})$. It is clear that $\Theta'_{k[\epsilon]/\epsilon^2}$ is surjective of kernel $\mathrm{Hom}_k(\omega_G, \mathrm{Lie}(G^{\text{ét}\vee}))$, which has dimension r over k.
(ii) Since $G^{\text{ét}}$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$, every element in $\mathrm{Ext}^1_A(\mathbb{Q}_p/\mathbb{Z}_p, \mathscr{G}^\circ)^r$ defines clearly an element of $\mathcal{D}_G(A)$ with image $[\mathscr{G}^\circ]$ in $\mathcal{D}_{G^\circ}(A)$. Conversely, for any $\mathscr{G} \in \mathcal{D}_G(A)$ with connected component isomorphic to $\mathscr{G}^\circ$, the isomorphism $G^{\text{ét}} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r$ lifts uniquely to an isomorphism $\mathscr{G}^{\text{ét}} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r$ because A is henselian. The canonical exact sequence $0 \to \mathscr{G}^\circ \to \mathscr{G} \to \mathscr{G}^{\text{ét}} \to 0$ shows that $\mathscr{G}$ comes from an element of $\mathrm{Ext}^1_A(\mathbb{Q}_p/\mathbb{Z}_p, \mathscr{G}^\circ)^r$.

□

4. HW-cyclic Barsotti-Tate Groups

DEFINITION 4.1. Let S be a scheme of characteristic $p > 0$, G be a BT-group over S such that $c = \dim(G^\vee)$ is constant. We say that G is *HW-cyclic*, if $c \geq 1$ and there exists an element $v \in \Gamma(S, \mathrm{Lie}(G^\vee))$ such that

$$v, \varphi_G(v), \cdots, \varphi_G^{c-1}(v)$$

generate $\mathrm{Lie}(G^\vee)$ as an $\mathscr{O}_S$-module, where φ_G is the Hasse-Witt map (2.6.1) of G.

REMARK 4.2. It is clear that a BT-group G over S is HW-cyclic, if and only if $\mathrm{Lie}(G^\vee)$ is free over $\mathscr{O}_S$ and there exists a basis of $\mathrm{Lie}(G^\vee)$ over $\mathscr{O}_S$ under which φ_G is expressed by a matrix of the form

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_c \end{pmatrix}, \tag{4.2.1}$$

where $a_i \in \Gamma(S, \mathscr{O}_S)$ for $1 \leq i \leq c$.

LEMMA 4.3. *Let R be a local ring of characteristic $p > 0$, k be its residue field.*
(i) *A BT-group G over R is HW-cyclic if and only if so is $G \otimes k$.*
(ii) *Let $0 \to G' \to G \to G'' \to 0$ be an exact sequence of BT-groups over R. If G is HW-cyclic, then so is G'. In particular, if R is henselian, the connected part of a HW-cyclic BT-group over R is HW-cyclic.*

Proof. (i) The property of being HW-cyclic is clearly stable under arbitrary base changes, so the "only if" part is clear. Assume that $G_0 = G \otimes k$ is HW-cyclic. Let $\overline{v}$ be an element of $\mathrm{Lie}(G_0^\vee) = \mathrm{Lie}(G^\vee) \otimes k$ such that

$(\overline{v}, \varphi_{G_0}(\overline{v}), \cdots, \varphi_{G_0}^{c-1}(\overline{v}))$ is a basis of $\mathrm{Lie}(G_0^\vee)$. Let v be any lift of $\overline{v}$ in $\mathrm{Lie}(G^\vee)$. Then by Nakayama's lemma, $(v, \varphi_G(v), \cdots, \varphi_G^{c-1}(v))$ is a basis of $\mathrm{Lie}(G^\vee)$.
(ii) By statement (i), we may assume $R = k$. The exact sequence of BT-groups induces an exact sequence of Lie algebras

$$0 \to \mathrm{Lie}(G''^\vee) \to \mathrm{Lie}(G^\vee) \to \mathrm{Lie}(G'^\vee) \to 0, \tag{4.3.1}$$

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

$$u, \varphi_G(u), \cdots, \varphi_G^{c-1}(u)$$

form a basis of $\mathrm{Lie}(G^\vee)$ over k. We denote by u' the image of u in $\mathrm{Lie}(G'^\vee)$. Let $r \leq c$ be the maximal integer such that the vectors

$$u',\ \varphi_{G'}(u'),\ \cdots,\ \varphi_{G'}^{r-1}(u')$$

are linearly independent over k. It is easy to see that they form a basis of the k-vector space $\mathrm{Lie}(G'^\vee)$. Hence G' is HW-cyclic. □

Lemma 4.4. *Let $S = \mathrm{Spec}(R)$ be an affine scheme of characteristic $p > 0$, G be a HW-cyclic BT-group over R with $c = \dim(G^\vee)$ constant, and*

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_c \end{pmatrix} \in \mathrm{M}_{c\times c}(R),$$

be a matrix of φ_G. Put $a_{c+1} = 1$, and $P(X) = \sum_{i=0}^{c} a_{i+1} X^{p^i} \in R[X]$.
(i) *Let $V_G : G^{(p)} \to G$ be the Verschiebung homomorphism of G. Then* $\mathrm{Ker}\, V_G$ *is isomorphic to the group scheme* $\mathrm{Spec}(R[X]/P(X))$ *with comultiplication given by $X \mapsto 1 \otimes X + X \otimes 1$.*
(ii) *Let $x \in S$, and G_x be the fibre of G at x. Put*

$$i_0(x) = \min_{0\leq i\leq c} \{i; a_{i+1}(x) \neq 0\}, \tag{4.4.1}$$

where $a_i(x)$ denotes the image of a_i in the residue field of x. Then the étale part of G_x has height $c - i_0(x)$, and the connected part of G_x has height $d + i_0(x)$. In particular, G_x is connected if and only if $a_i(x) = 0$ for $1 \leq i \leq c$.

Proof. (i) By 2.3 and 2.13, $\mathrm{Ker}\, V_G$ is isomorphic to the group scheme

$$\mathrm{Spec}\Big(R[X_1, \ldots, X_c]/(X_1^p - X_2, \cdots, X_{c-1}^p - X_c, X_c^p + a_1X_1 + \cdots + a_cX_c)\Big)$$

with comultiplication $\Delta(X_i) = 1 \otimes X_i + X_i \otimes 1$ for $1 \leq i \leq c$. By sending $(X_1, X_2, \cdots, X_c) \mapsto (X, X^p, \cdots, X^{p^{c-1}})$, we see that the above group scheme is isomorphic to $\mathrm{Spec}(R[X]/P(X))$ with comultiplication $\Delta(X) = 1\otimes X + X\otimes 1$.

(ii) By base change, we may assume that $S = x = \mathrm{Spec}(k)$ and hence $G = G_x$. Let $G(1)$ be the kernel of the multiplication by p on G. Then we have an exact sequence

$$0 \to \mathrm{Ker}\, F_G \to G(1) \to \mathrm{Ker}\, V_G \to 0.$$

Since $\mathrm{Ker}\, F_G$ is an infinitesimal group scheme over k, we have $G(1)(\overline{k}) = (\mathrm{Ker}\, V_G)(\overline{k})$, where $\overline{k}$ is an algebraic closure of k. By the definition of $i_0(x)$, we have $P(X) = Q(X^{p^{i_0(x)}})$, where $Q(X)$ is an additive sepearable polynomial in $k[X]$ with $\deg(Q) = p^{c-i_0(x)}$. Hence the roots of $P(X)$ in $\overline{k}$ form an $\mathbb{F}_p$-vector space of dimension $c - i_0(x)$. By (i), $(\mathrm{Ker}\, V_G)(\overline{k})$ can be identified with the additive group consisting of the roots of $P(X)$ in $\overline{k}$. Therefore, the étale part of G has height $c - i_0(x)$, and the connected part of G has height $d + i_0(x)$. $\square$

4.5. Let k be a perfect field of characteristic $p > 0$, and $\alpha_p = \mathrm{Spec}(k[X]/X^p)$ be the finite group scheme over k with comultiplication map $\Delta(X) = 1 \otimes X + X \otimes 1$. Let G be a BT-group over k. Following Oort, we call

$$a(G) = \dim_k \mathrm{Hom}_{k_{\mathrm{fppf}}}(\alpha_p, G)$$

the a-number of G, where $\mathrm{Hom}_{k_{\mathrm{fppf}}}$ means the homomorphisms in the category of abelian fppf-sheaves over k. Since the Frobenius of α_p vanishes, any morphism of α_p in G factorize through $\mathrm{Ker}(F_G)$. Therefore we have

$$\begin{aligned}\mathrm{Hom}_{k_{\mathrm{fppf}}}(\alpha_p, G) &= \mathrm{Hom}_{k-gr}(\alpha_p, \mathrm{Ker}(F_G)) \\ &= \mathrm{Hom}_{k-gr}(\mathrm{Ker}(F_G)^\vee, \alpha_p) \\ &= \mathrm{Hom}_{p\text{-}\mathfrak{Lie}_k}(\mathrm{Lie}(\alpha_p), \mathrm{Lie}(\mathrm{Ker}(F_G))),\end{aligned}$$

where Hom_{k-gr} denotes the homomorphisms in the category of commutative group schemes over k, and the last equality uses Proposition 2.3. Since we have a canonical isomorphism $\mathrm{Lie}(\mathrm{Ker}(F_G)) \simeq \mathrm{Lie}(G)$ and $\mathrm{Lie}(\alpha_p)$ has dimension one over k with $\varphi_{\alpha_p} = 0$, we get

$$a(G) = \dim_k\{x \in \mathrm{Lie}(G) | \varphi_{G^\vee}(x) = 0\} = \dim_k \mathrm{Ker}(\varphi_{G^\vee}). \tag{4.5.1}$$

Due to the perfectness of k, we have also $a(G) = \dim_k \mathrm{Ker}(\widetilde{\varphi_{G^\vee}})$, where $\widetilde{\varphi_{G^\vee}}$ is the linearization of $\varphi_{G^\vee}$. By Proposition 2.11, we see that $a(G) = 0$ if and only if G is ordinary.

LEMMA 4.6. *Let G be a BT-group over k, and $G^\vee$ its Serre dual. Then we have $a(G) = a(G^\vee)$.*

Proof. Let $\psi_G : \omega_G \to \omega_G^{(p)}$ be the k-linear map induced by the Verschiebung of G. Then ψ_G^*, the morphism obtained by applying the functor $\mathrm{Hom}_k(\_, k)$ to ψ_G, is identified with $\widetilde{\varphi_{G^\vee}}$. By (4.5.1) and the exactitude of the functor $\mathrm{Hom}_k(\_, k)$, we have $a(G) = \dim_k \mathrm{Ker}(\psi_G^*) = \dim_k \mathrm{Coker}(\psi_G)$. Using the additivity of $\dim_k$, we get finally $a(G) = \dim_k \mathrm{Ker}(\psi_G)$. By considering the commutative diagram (3.1.3), we have

$$a(G) = \dim_k\Big(\omega_G \cap \phi_G(\mathrm{Lie}(G^\vee)^{(p)})\Big).$$

On the other hand, it follows also from (3.1.3) that

$$a(G^\vee) = \dim_k \mathrm{Ker}(\widetilde{\varphi_G}) = \dim_k\Big(\phi_G(\mathrm{Lie}(G^\vee)^{(p)}) \cap \omega_G\Big).$$

The lemma now follows immediately.

□

Proposition 4.7. *Let k be a perfect field of characteristic $p>0$, G a BT-group over k. Consider the following conditions:*
(i) *G is HW-cyclic and non-ordinary;*
(ii) *the connected part G° of G is HW-cyclic and not of multiplicative type;*
(iii) $a(G^\vee) = a(G) = 1$.
We have (i) $\Rightarrow$ (ii) $\Leftrightarrow$ (iii). *If k is algebraically closed, we have moreover* (ii) $\Rightarrow$ (i).

Remark 4.8. In [Oo1, Lemma 2.2], Oort proved the following assertion, which is a generalization of (iii) $\Rightarrow$ (ii): Let k be an algebraically closed field of characteristic $p>0$, and G be a connected BT-group with $a(G)=1$. Then there exists a basis of the Dieudonné module M of G over $W(k)$, such that the action of Frobenius on M is given by a display-matrix of "normal form" in the sense of [Oo1, 2.1].

Proof. (i) $\Rightarrow$ (ii) follows from 4.3(ii).
(ii) $\Rightarrow$ (iii). First, we note that $a(G)=a(G^\circ)$, so we may assume G connected. Since G is not of multiplicative type, we have $c=\dim(G^\vee)\geq 1$. By Lemma 4.4(ii), there exists a basis of $\mathrm{Lie}(G^\vee)$ over k under which φ_G is expressed by

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathrm{M}_{c\times c}(k).$$

According to (4.5.1), $a(G^\vee)$ equals to $\dim_k \mathrm{Ker}(\varphi_G)$, *i.e.* the k-dimension of the solutions of the equation system in $(x_1,\cdots,x_c)$

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1^p \\ x_2^p \\ \vdots \\ x_c^p \end{pmatrix} = 0$$

The solutions $(x_1,\cdots,x_c)$ form clearly a vector space over k of dimension 1, *i.e.* we have $a(G^\vee)=1$.
(iii) $\Rightarrow$ (ii). Let $G^{\text{ét}}$ be the étale part of G. Since k is perfect, the exact sequence (2.7.1) splits [Dem, Chap. II §7]; so we have $G \simeq G^\circ \times G^{\text{ét}}$. We put $M=\mathrm{Lie}(G^\vee)$, $M_1 = \mathrm{Lie}(G^{\circ\vee})$ and $M_2 = \mathrm{Lie}(G^{\text{ét}\vee})$ for short. By 2.8 and 2.9, we have a decomposition $M = M_1 \oplus M_2$, such that M_1, M_2 are stable under φ_G, and the action of φ_G is nilpotent on M_1 and bijective on M_2. We note

that $a(G^{\circ\vee}) = a(G^\circ) = a(G) = 1$. By the last remark of 4.5, G° is not of multiplicative type, hence $\dim_k M_1 = \dim(G^{\circ\vee}) \geq 1$. It remains to prove that G° is HW-cyclic. Let n be the minimal integer such that $\varphi_G^n(M_1) = 0$. We have a strictly increasing filtration

$$0 \subsetneq \operatorname{Ker}(\varphi_G) \subsetneq \cdots \subsetneq \operatorname{Ker}(\varphi_G^n) = M_1.$$

If $n = 1$, then M_1 is one-dimensional, hence G° is clearly HW-cyclic. Assume $n \geq 2$. For $2 \leq m \leq n$, φ_G^{m-1} induces an injective map

$$\overline{\varphi_G^{m-1}} : \operatorname{Ker}(\varphi_G^m)/\operatorname{Ker}(\varphi_G^{m-1}) \longrightarrow \operatorname{Ker}(\varphi_G).$$

Since $\dim_k \operatorname{Ker}(\varphi_G) = a(G^{\circ\vee}) = 1$, $\overline{\varphi_G^{m-1}}$ is necessarily bijective. So we have $\dim_k \operatorname{Ker}(\varphi_G^m) = m$ for $1 \leq m \leq n$. Let v be an element of M_1 but not in $\operatorname{Ker}(\varphi_G^{n-1})$. Then $v, \varphi_G(v), \cdots, \varphi_G^{n-1}(v)$ are linearly independant, hence they form a basis of M_1 over k. This proves that G° is HW-cyclic.
Assume k algebraically closed. We prove that (ii) $\Rightarrow$ (i). Noting that G is ordinary if and only if G° is of multiplicative type, we only need to check that G is HW-cyclic. We conserve the notations above. Since φ_G is bijective on M_2 and k algebraically closed, there exists a basis $(e_1, \cdots, e_m)$ of M_2 such that $\varphi_G(e_i) = e_i$ for $1 \leq i \leq m$. Let $v \in M_1$ but not in $\operatorname{Ker}(\varphi_G^{n-1})$ as above, and put $u = v + \lambda_1 e_1 + \cdots \lambda_m e_m$, where $\lambda_i (1 \leq i \leq m)$ are some elements in k to be determined later. Then we have

$$\begin{pmatrix} \varphi_G^n(u) \\ \vdots \\ \varphi_G^{n+m-1}(u) \end{pmatrix} = \begin{pmatrix} \lambda_1^{p^n} & \cdots & \lambda_m^{p^n} \\ \vdots & \ddots & \vdots \\ \lambda_1^{p^{n+m-1}} & \cdots & \lambda_m^{p^{n+m-1}} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix}.$$

Let $L(\lambda_1, \cdots, \lambda_m) \in k[\lambda_1, \cdots, \lambda_m]$ be the determinant polynomial of the matrix on the right side. An elementary computation shows that the polynomial $L(\lambda_1, \cdots, \lambda_m)$ is not null. We can choose $\lambda_1, \cdots, \lambda_m \in k$ such that $L(\lambda_1, \cdots, \lambda_m) \neq 0$ because k is algebraically closed. So $\varphi_G^n(u), \cdots, \varphi_G^{n+m-1}(u)$ form a basis of M_2 over k. Since

$$\varphi_G^i(u) \equiv \varphi_G^i(v) \mod M_2 \quad \text{for} \quad 0 \leq i \leq n,$$

by the choice of u, we see that $\{u, \varphi_G(u), \cdots, \varphi_G^{n+m-1}(u)\}$ form a basis of $M = \operatorname{Lie}(G^\vee)$ over k. □

By combining 4.6 and 4.7, we obtain the following

COROLLARY 4.9. *Let k be an algebraically closed field of characteristic $p > 0$. Then a BT-group over k is HW-cyclic if and only if so is its Serre dual.*

4.10. EXAMPLES. Let k be a perfect field, $W(k)$ be the ring of Witt vectors with coefficients in k, and σ be the Frobenius automorphism of $W(k)$. Let s, r be relatively prime integers such that $0 \leq s \leq r$ and $r \neq 0$; put $\lambda = \frac{s}{r}$. We consider the Dieudonné module $M^\lambda \simeq W(k)[F, V]/(F^{r-s} - V^s)$, where $W(k)[F, V]$ is the non-commutative ring with relations $FV = VF = p$, $Fa = \sigma(a)F$ and $V\sigma(a) = aV$ for all $a \in W(k)$. We note that M^λ is free of rank

r over $W(k)$ and $M^\lambda/VM^\lambda \simeq k[F]/F^{r-s}$. By the contravariant Dieudonné theory, M^λ corresponds to a BT-group G^λ over k of height r with $\mathrm{Lie}(G^{\lambda\vee}) = M^\lambda/VM^\lambda$. We see easily that G^λ is HW-cyclic, and we call it the *elementary BT-group of slope* λ. We note that $G^0 \simeq \mathbb{Q}_p/\mathbb{Z}_p$, $G^1 \simeq \mu_{p^\infty}$, and $(G^\lambda)^\vee \simeq G^{1-\lambda}$ for $0 \leq \lambda \leq 1$.
Assume k algebraically closed. Then by the Dieudonné-Manin's classification of isocrystals [Dem, Chap.IV §4], any BT-group over k is isogenous to a finite product of G^λ's; moreover, any connected one-dimensional BT-group over k of height r is necessarily isomorphic to $G^{1/r}$ [Dem, Chap.IV §8], hence in particular HW-cyclic.

Proposition 4.11. *Let k be an algebraically closed field of characteristic $p>0$, R be a noetherian complete regular local k-algebra with residue field k, and $S = \mathrm{Spec}(R)$. Let G be a connected HW-cyclic BT-group over R of dimension $d \geq 1$ and height $c+d$,*

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_c \end{pmatrix} \in \mathrm{M}_{c\times c}(R)$$

be a matrix of φ_G.
(i) *If G is versal over S, then $\{a_1, \cdots, a_c\}$ is a subset of a regular system of parameters of R.*
(ii) *Assume that $d=1$. The converse of* (i) *is also true,* i.e. *if $\{a_1, \cdots, a_c\}$ is a subset of a regular system of parameters of R then G is versal over S. Furthermore, G is the universal deformation of its special fiber if and only if $\{a_1, \cdots, a_c\}$ is a system of regular parameters of R.*

Proof. Let $(\mathbf{M}(G), F_M, \nabla)$ be the finite free $\mathscr{O}_S$-module equipped with a semi-linear endomorphism F_M and a connection $\nabla : \mathbf{M}(G) \to \mathbf{M}(G) \otimes_{\mathscr{O}_S} \Omega^1_{S/k}$, obtained by evaluating the Dieudonné crystal of G at the trivial immersion $S \hookrightarrow S$ (cf. 3.1). Recall that we have a commutative diagram

(4.11.1)
$$\begin{tikzcd} \mathbf{M}(G)^{(p)} \arrow[r, "F_M"] \arrow[d, "pr"'] & \mathbf{M}(G) \arrow[d, "pr"] \\ \mathrm{Lie}(G^\vee)^{(p)} \arrow[r, "\widetilde{\varphi_G}"] \arrow[ur, hook, "\phi_G"] & \mathrm{Lie}(G^\vee), \end{tikzcd}$$

where ϕ_G is universally injective (3.1.3). Let $\{v_1, \cdots, v_c\}$ be a basis of $\mathrm{Lie}(G^\vee)$ over $\mathscr{O}_S$ under which φ_G is expressed by $\mathfrak{h}$, *i.e.* we have $\varphi_G^{i-1}(v_1) = v_i$ for $1 \leq i \leq c$ and $\varphi_G^c(v_1) = \varphi_G(v_c) = -\sum_{i=1}^c a_i v_i$. Let f_1 be a lift of v_1 to $\Gamma(S, \mathbf{M}(G))$, and put $f_{i+1} = \phi_G(v_i^{(p)})$ for $1 \leq i \leq c-1$, where $v_i^{(p)} = 1 \otimes v_i \in \Gamma(S, \mathrm{Lie}(G^\vee)^{(p)})$. The image of f_i in $\Gamma(S, \mathrm{Lie}(G^\vee))$ is thus v_i for $1 \leq i \leq c$ by

(4.11.1). We put

$$e_1 = \phi_G(v_c^{(p)}) + a_1 f_1 + \cdots + a_c f_c \in \Gamma(S, \mathbf{M}(G)). \tag{4.11.2}$$

The image of e_1 in $\Gamma(S, \mathrm{Lie}(G^\vee))$ is $\varphi_G(v_c) + \sum_{i=1}^c a_i v_i = 0$; so we have $e_1 \in \Gamma(S, \omega_G)$. By 4.4(ii), we notice that $a_1, \cdots, a_c$ belong to the maximal ideal $\mathfrak{m}_R$ of R, as G is connected. Hence, we have $\overline{e_1} = \overline{\phi_G(v_c^{(p)})}$, where for a R-module M and $x \in M$, we denote by $\overline{x}$ the canonical image of x in $M \otimes k$. Since ϕ_G commutes with base change and is universally injective, we get $\overline{e_1} = \overline{\phi_G(v_c^{(p)})} = \phi_{G\otimes k}(\overline{v_c^{(p)}}) \neq 0$. Therefore, we can choose $e_2, \cdots, e_d \in \Gamma(S, \omega_G)$ such that $(e_1, \cdots, e_d)$ becomes a basis of ω_G over $\mathscr{O}_S$, so $(e_1, \cdots, e_d, f_1, \cdots, f_c)$ is a basis of $\mathbf{M}(G)$. Since F_M is horizontal for the connection ∇ (cf. 3.1(ii)), we have

$$\nabla(\phi_G(v_c^{(p)})) = \nabla(F_M(f_c^{(p)})) = 0.$$

In view of (4.11.2), we get

$$\begin{aligned} \nabla(e_1) &= \sum_{i=1}^c f_i \otimes da_i + \sum_{i=1}^c a_i \nabla(f_i) \\ &\equiv \sum_{i=1}^c f_i \otimes da_i \pmod{\mathfrak{m}_R}. \end{aligned} \tag{4.11.3}$$

Let KS_0 and Kod_0 be respectively the reductions modulo $\mathfrak{m}_R$ of (3.2.1) and (3.2.2). Since $(\overline{v_i})_{1\leq i\leq c}$ is a base of $\mathrm{Lie}(G^\vee) \otimes k$, we can write

$$\mathrm{KS}_0(e_j) = \sum_{i=1}^c \overline{v_i} \otimes \theta_{i,j} \qquad \text{for } 1 \leq j \leq d,$$

where $\theta_{i,j} \in \Omega_{S/k} \otimes k$. From (4.11.3), we deduce that $\theta_{i,1} = da_i$. By the definition of Kod_0, we have

$$\mathrm{Kod}_0(\partial) = \sum_{j=1}^d \sum_{i=1}^c < \partial, \theta_{i,j} > \overline{e_j}^* \otimes \overline{v_i} \tag{4.11.4}$$

where $\partial \in \mathscr{T}_{S/k} \otimes k$, $< \bullet, \bullet >$ is the canonical pairing between $\mathscr{T}_{S/k} \otimes k$ and $\Omega^1_{S/k} \otimes k$, and $(\overline{e_i}^*)_{1\leq i\leq d}$ denotes the dual basis of $(\overline{e_i})_{1\leq i\leq d}$. Now assume that G is versal over S, *i.e.* Kod_0 is surjective by definition (3.2). In particular, there are $\partial_1, \cdots, \partial_c \in \mathscr{T}_{S/k} \otimes k$ such that $\mathrm{Kod}_0(\partial_i) = \overline{e_1}^* \otimes v_i$ for $1 \leq i \leq c$, *i.e.* we have

$$< \partial_i, da_j >= \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \quad \text{for } 1 \leq i, j \leq c, \tag{4.11.5}$$

and

$$< \partial_i, \theta_{j,\ell} >= 0 \qquad \text{for } 1 \leq i, j \leq c, 2 \leq \ell \leq d.$$

From (4.11.5), we see easily that $da_1, \cdots, da_c$ are linearly independent in $\Omega_{S/k} \otimes k \simeq \mathfrak{m}_R/\mathfrak{m}_R^2$; therefore, $(a_1, \cdots, a_c)$ is a part of a regular system of parameters of R. Statement (i) is proved.

For statement (ii), we assume $d = 1$ and that $(a_1, \cdots, a_c)$ is a part of a regular system of parameters of R. Then the formula (4.11.4) is simplified as

$$\mathrm{Kod}_0(\partial) = \sum_{i=1}^{c} < \partial, da_i > \overline{e_1}^* \otimes \overline{v_i}.$$

Since $da_1, \cdots, da_c$ are linearly independent in $\Omega^1_{S/k} \otimes k$, there exist $\partial_1, \cdots, \partial_c \in \mathscr{T}_{S/k} \otimes k$ such that (4.11.5) holds, *i.e.* $(\overline{e_1}^* \otimes \overline{v_i})_{1 \leq i \leq c}$ are in the image of Kod_0. But the elements $(\overline{e_1}^* \otimes \overline{v_i})_{1 \leq i \leq c}$ form already a basis of $\mathscr{H}om_{\mathscr{O}_S}(\omega_G, \mathrm{Lie}(G^\vee)) \otimes k$. So Kod_0 is surjective, and hence G is versal over S by Nakayama's lemma. Let G_0 be the special fiber of G. It remains to prove that when $d = 1$, G is the universal deformation of G_0 if and only if $\dim(S) = c$ and G is versal over S. Let $\mathbf{S}$ be the local moduli in characteristic p of G_0. By the universal property of $\mathbf{G}$ (3.7), there exists a unique morphism $f : S \to \mathbf{S}$ such that $G \simeq \mathbf{G} \times_{\mathbf{S}} S$. Since S and $\mathbf{S}$ are local complete regular schemes over k with residue field k of the same dimension, f is an isomorphism if and only if the tangent map of f at the closed point of S, denoted by T_f, is an isomorphism. By the functoriality of Kodaira-Spencer maps (3.2.2), we have a commutative diagram

$$\begin{array}{ccc}
\mathscr{T}_{S/k} \otimes_{\mathscr{O}_S} k & \xrightarrow{\mathrm{Kod}_0^S} & \mathrm{Hom}_k(\omega_{G_0}, \mathrm{Lie}(G_0^\vee)) \\
\Big\downarrow{\scriptstyle T_f} & & \Big\| \\
\mathscr{T}_{\mathbf{S}/k} \otimes_{\mathscr{O}_{\mathbf{S}}} k & \xrightarrow{\mathrm{Kod}_0^{\mathbf{S}}} & \mathrm{Hom}_k(\omega_{G_0}, \mathrm{Lie}(G_0^\vee))
\end{array},$$

where horizontal arrows are the Kodaira-Spencer maps evaluated at the closed points (3.3.1). Since Kod_0^S and $\mathrm{Kod}_0^{\mathbf{S}}$ are isomorphisms according to the first part of this propostion, we deduce that so is T_f. This completes the proof. $\square$

5. Monodromy of a HW-cyclic 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. We put $S = \mathrm{Spec}(A)$, and denote by s its closed point, by η its generic point. Let $\overline{K}$ 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 [Se1, Chap. IV]. The subgroup I_p, called the *wild inertia subgroup*, is the unique maximal pro-p-group contained in I and hence 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

$$\theta : I_t \xrightarrow{\sim} \varprojlim_{(d,p)=1} \mu_d, \tag{5.2.1}$$

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 (5.2.1). 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 ([Se3] Prop.7). *Let a, d be relatively prime positive integers with d 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.*

5.4. Let G be a BT-group over S. We define $h(G)$ to be the valuation of the determinant of a matrix of φ_G if $\dim(G^\vee) \geq 1$, and $h(G) = 0$ if $\dim(G^\vee) = 0$. We call $h(G)$ the *Hasse invariant* of G.

(a) $h(G)$ does not depend on the choice of the matrix representing φ_G. Indeed, let c be the rank of $\mathrm{Lie}(G^\vee)$ over A, $\mathfrak{h} \in \mathrm{M}_{c\times c}(A)$ be a matrix of φ_G. Any other matrix representing φ_G can be written in the form $U^{-1} \cdot \mathfrak{h} \cdot U^{(p)}$, where $U \in \mathrm{GL}_c(A)$, 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 2.11, the generic fiber G_η is ordinary if and only if $h(G) < \infty$; G is ordinary over T if and only $h(G) = 0$.

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

Proposition 5.5. *Let G be a BT-group over S. Then we have $h(G) = h(G^\vee)$.*

Proof. The proof is very similar to that of Lemma 4.6. First, we have

$$h(G) = \mathrm{leng}\big(\mathrm{Lie}(G^\vee)/\widetilde{\varphi_G}(\mathrm{Lie}(G^\vee)^{(p)})\big),$$

where $\widetilde{\varphi_G}$ is the linearization of φ_G, and "leng" means the length of a finite A-module (note that this formulae holds even if $\dim(G^\vee) = 0$). By the commutative diagram (3.1.3), we have

$$h(G) = \mathrm{leng}\,\mathbf{M}(G)/(\phi_G(\mathrm{Lie}(G^\vee)^{(p)}) + \omega_G).$$

On the other hand, by applying the functor $\mathrm{Hom}_A(\_, A)$ to the A-linear map $\widetilde{\varphi_{G^\vee}} : \mathrm{Lie}(G)^{(p)} \to \mathrm{Lie}(G)$, we obtain a map $\psi_G : \omega_G \to \omega_G^{(p)}$. If U is a matrix of $\widetilde{\varphi_{G^\vee}}$, then the transpose of U, denoted by U^t, is a matrix of ψ_G. So we have

$$h(G^\vee) = \mathtt{v}(\det(U)) = \mathtt{v}(\det(U^t)) = \mathrm{leng}\big(\omega_G^{(p)}/\psi_G(\omega_G)\big).$$

By diagram 3.1.3, we get

$$h(G^\vee) = \mathrm{leng}\, \mathbf{M}(G)/(\phi_G(\mathrm{Lie}(G^\vee)^{(p)}) + \omega_G) = h(G).$$

□

5.6. Let G be a BT-group over S, $c = \dim(G^\vee)$. We put

$$\mathrm{T}_p(G) = \varprojlim_n G(n)(\overline{K}) \tag{5.6.1}$$

the Tate module of G, where $G(n)$ is the kernel of $p^n : G \to G$. It is a free $\mathbb{Z}_p$-module of rank $\leq c$, and 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

$$\rho : I = \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G)). \tag{5.6.2}$$

We denote by

$$\overline{\rho} : I = \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}_{\mathbb{F}_p}\big(G(1)(\overline{K})\big) \tag{5.6.3}$$

its reduction mod p.

Theorem 5.7 (Reformulation of Igusa's theorem). *Let G be a connected BT-group over S of height 2 and dimension 1. Then G is versal (3.2) if and only if $h(G) = 1$; moreover, if this condition is satisfied, the monodromy representation $\rho : I \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G)) \simeq \mathbb{Z}_p^\times$ is surjective.*

Proof. Since $\mathrm{Lie}(G^\vee)$ is an $\mathscr{O}_S$-module free of rank 1, the condition that $h(G) = 1$ is equivalent to that any matrix of φ_G is represented by a uniformizer of A. Hence the first part of this theorem follows from Proposition 4.11(ii).
We follow [Ka2, Thm 4.3] to prove the surjectivity of ρ under the assumption that $h(G) = 1$. For each integer $n \geq 1$, let

$$\rho_n : I \to \mathrm{Aut}_{\mathbb{Z}/p^n\mathbb{Z}}(G(n)(\overline{K})) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$$

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 $\mathrm{Gal}(K_n/K) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. By taking projective limits, we are reduced to proving 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 [Ka2, 3.6], there exists a parameter X of the formal group G normalized by the condition that $[\xi](X) = \xi(X)$ 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 $\mathtt{v}(a_1) = h(G) = 1$ by [Ka2, 3.6.1 and 3.6.5], and $\mathtt{v}(\alpha) = 0$, 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

$$\begin{cases} V(y_1) = a_1 y_1 + \alpha y_1^p + \cdots = 0; \\ V^{(p)}(y_2) = a_1^p y_2 + \alpha^p y_2^p + \cdots = y_1; \\ \vdots \\ V^{(p^{n-1})}(y_n) = a_1^{p^{n-1}} y_n + \alpha^{p^{n-1}} y_n^p + \cdots = y_{n-1}. \end{cases}$$

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

$$\mathtt{v}(y_i) = \frac{1}{p^{i-1}(p-1)} \qquad \text{for } 1 \leq i \leq n.$$

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 $[K_n : K] \geq [K(y_n) : K] \geq e(K(y_n)/K) \geq p^{n-1}(p-1)$. □

PROPOSITION 5.8. *Let G be a HW-cyclic BT-group over S of height $c+d$ and dimension d such that $G \otimes K$ is ordinary,*

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

be a matrix of φ_G. Put $q = p^c$, $a_{c+1} = 1$, and $P(X) = \sum_{i=0}^{c} a_{i+1} X^{p^i} \in A[X]$.
(i) *Assume that G is connected and the Hasse invariant $h(G) = 1$. Then the representation $\overline{\rho}$* (5.6.3) *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 $\theta_{q-1} : I_t \to \mathbb{F}_q^{\times}$.*
(ii) *Assume that $c > 1$, $\mathtt{v}(a_i) \geq 2$ for $1 \leq i \leq c-1$ and $\mathtt{v}(a_c) = 1$. Then the order of $\mathrm{Im}(\overline{\rho})$ is divisible by $p^{c-1}(p-1)$.*

(iii) *Put* $i_0 = \min_{0\leq i\leq c}\{i; \mathtt{v}(a_{i+1}) = 0\}$. *Assume that there exists* $\alpha \in k$ *such that* $\mathtt{v}(P(\alpha)) = 1$. *Then we have* $i_0 \leq c-1$ *and the order of* $\mathrm{Im}(\overline{\rho})$ *is divisible by* p^{i_0}.

Proof. Since G is generically ordinary, we have $a_1 \neq 0$ by 2.11(d). Hence $P(X) \in K[X]$ is a separable polynomial. By 4.4, $G(1)(\overline{K}) \simeq (\mathrm{Ker}\, V_G)(K^{\mathrm{sep}})$ is identified with the additive group consisting of the roots of $P(X)$ in K^{sep}.
(i) By definition of the Hasse invariant, we have $\mathtt{v}(a_1) = h(G) = 1$. By 4.4(ii), the assumption that G is connected is equivalent to saying $\mathtt{v}(a_i) \geq 1$ for $1 \leq i \leq c$. From the Newton polygon of $P(X)$, we deduce that all the non-zero roots of $P(X)$ 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 sends each root $x \in K^{\mathrm{sep}}$ of $P(X)$ to the class of x in $V_{1/(q-1)} = \mathfrak{m}_{1/(q-1)}/\mathfrak{m}^+_{1/(q-1)}$ (5.1.1). We remark that $G(1)(\overline{K})$ is an $\mathbb{F}_p$-vector space of dimension c. 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 4.4(i), ψ is obviously an I-equivariant homomorphism of groups. Let x_0 be a root of $P(X)$, and put $Q(y) = P(x_0 y)$. Then the polynomial $Q(y)$ has the form $Q(y) = x_0^q Q_1(y)$, where

$$Q_1(y) = y^q + b_c y^{p^{c-1}} + \cdots + b_2 y^p + b_1 y$$

with $b_i = a_i / x_0^{(q-p^{i-1})} \in K^{\mathrm{sep}}$. We have $\mathtt{v}(b_i) > 0$ for $2 \leq i \leq c$ 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 $P(X)$ in $V_{1/(q-1)}$ are $x_0 \overline{b}_1^{1/(q-1)} \zeta$, where ζ runs over the finite field $\mathbb{F}_q$. Therefore, ψ is injective.
(ii) By computing the slopes of the Newton polygon of $P(X)$, we see that $P(X)$ has $p^{c-1}(p-1)$ roots of valuation $1/(p^c - p^{c-1})$. Let L be the sub-extension of K^{sep} obtained by adding to K all the roots of $P(x)$. Then the ramification index $e(L/K)$ is divisible by $p^{c-1}(p-1)$. Let $\widetilde{L}$ be the sub-extension of K^{sep} fixed by the kernel of $\overline{\rho}$ (5.6.3). The Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/\widetilde{L})$ fixes the roots of $P(x)$ by definition. Hence we have $L \subset \widetilde{L}$, and $|\,\mathrm{Im}(\overline{\rho})| = [\widetilde{L} : K]$ is divisible by $[L : K]$; in particular, it is divisible by $p^{c-1}(p-1)$.
(iii) Note that the relation $i_0 \leq c-1$ is equivalent to saying that G is not connected by 4.4(ii). Assume conversely $i_0 = c$, *i.e.* G is connected. Then we would have

$$P(X) \equiv X^q \mod (\pi A[X]).$$

But $\mathtt{v}(P(\alpha)) = 1$ implies that $\alpha^{p^c} \in \pi A$, *i.e.* $\alpha = 0$; hence we would have $P(\alpha) = 0$, which contradicts the condition $\mathtt{v}(P(\alpha)) = 1$.
We put $Q(X) = P(X+\alpha) = P(X) + P(\alpha)$. As $\mathtt{v}(P(\alpha)) = 1$, then $(0,1)$ and $(p^{i_0}, 0)$ are the first two break points of the Newton polygon of $Q(X)$. Hence there exists p^{i_0} roots of $Q(X)$ of valuation $1/p^{i_0}$. Let L be the subextension of K in K^{sep} generated by the roots of $P(X)$. The ramification index $e(L/K)$ is divisible by p^{i_0}. As in the proof of (ii), if $\widetilde{L}$ is the subextension of K^{sep}

fixed by the kernel of $\overline{\rho}$, then it is an extension of L. Therefore, we have $|\operatorname{Im}(\overline{\rho})| = [\widetilde{L}:K]$ is divisible by $[L:K]$, and in particular, divisible by p^{i_0}. $\square$

5.9. Let G be a BT-group over S with connected part G°, and étale part $G^{\text{ét}}$ of height r. We have a canonical exact sequence of I-modules

$$0 \to G^\circ(1)(\overline{K}) \to G(1)(\overline{K}) \to G^{\text{ét}}(1)(\overline{K}) \to 0 \tag{5.9.1}$$

giving rise to a class $\overline{C} \in \operatorname{Ext}^1_{\mathbb{F}_p[I]}(G^{\text{ét}}(1)(\overline{K}), G^\circ(1)(\overline{K}))$, which vanishes if and only if (5.9.1) splits. Since I acts trivially on $G^{\text{ét}}(1)(\overline{K})$, we have an isomorphism of I-modules $G^{\text{ét}}(1)(\overline{K}) \simeq \mathbb{F}_p^r$. Recall that for any $\mathbb{F}_p[I]$-module M, we have a canonical isomorphism ([Se1] Chap.VII, §2)

$$\operatorname{Ext}^1_{\mathbb{F}_p[I]}(\mathbb{F}_p, M) \simeq H^1(I, M).$$

Hence we deduce that

$$\overline{C} \in \operatorname{Ext}^1_{\mathbb{F}_p[I]}(G^{\text{ét}}(1)(\overline{K}), G^\circ(1)(\overline{K})) \simeq H^1(I, G^\circ(1)(\overline{K}))^r. \tag{5.9.2}$$

PROPOSITION 5.10. *Let G be a HW-cyclic BT-group over S such that $h(G) = 1$, $\overline{\rho}$ (5.6.3) be the representation of I on $G(1)(\overline{K})$. Then the cohomology class $\overline{C}$ does not vanish if and only if the order of the group $\operatorname{Im}(\overline{\rho})$ is divisible by p.*

First, we prove the following result on cohomology of groups.

LEMMA 5.11. *Let F be a field, Γ be a commutative group, and $\chi : \Gamma \to F^\times$ be a non-trivial 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

$$C(gh) = C(g) + \chi(g)C(h),$$
$$C(hg) = C(h) + \chi(h)C(g).$$

Since Γ is commutative, it follows from the relation $C(gh) = C(hg)$ that

$$(\chi(g) - 1)C(h) = (\chi(h) - 1)C(g). \tag{5.11.1}$$

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 $x \in F(\overline{\chi})$ 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 (5.11.1). This shows that C is a 1-coboundary. $\square$

Proof of 5.10. By 4.3(ii) and 5.4(c), the connected part G° of G is HW-cyclic with $h(G^\circ) = h(G) = 1$. Assume that $\mathrm{T}_p(G^\circ)$ has rank ℓ over $\mathbb{Z}_p$, and $\mathrm{T}_p(G^{\text{ét}})$ has rank r. Then by 5.8(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 $G^\circ(1)(\overline{K}) = \mathbb{F}_q(\overline{\chi})$ for short. If the cohomology class $\overline{C}$ is zero, then the exact sequence (5.9.1) splits, *i.e.* we have an isomorphism

of Galois modules $G(1)(\overline{K}) \simeq \mathbb{F}_q(\chi) \oplus \mathbb{F}_p^r$. It is clear that the group $\mathrm{Im}(\overline{\rho})$ has 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 (5.9.1) such that the action of $g \in I$ is given by

$$\overline{\rho}(g) = \begin{pmatrix} \overline{\chi}(g) & \overline{C}(g) \\ 0 & \mathbf{1}_r \end{pmatrix}, \tag{5.11.2}$$

where $\mathbf{1}_r$ is the unit matrix of type (r,r) 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

$$0 \to H^1(\Gamma, \mathbb{F}_q(\overline{\chi}))^r \xrightarrow{\mathrm{Inf}} H^1(I, \mathbb{F}_q(\overline{\chi}))^r \xrightarrow{\mathrm{Res}} H^1(I_1, \mathbb{F}_q(\overline{\chi}))^r,$$

where "Inf" and "Res" are respectively the inflation and restriction homomorphisms in group cohomology. Since $H^1(\Gamma, \mathbb{F}_q(\overline{\chi}))^r = 0$ by 5.11, the restriction of the cohomology class $\overline{C}$ to $H^1(I_1, \mathbb{F}_q(\overline{\chi}))^r$ 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

$$\overline{\rho}(h)^p = \begin{pmatrix} \mathbf{1}_\ell & p\overline{C}(h) \\ 0 & \mathbf{1}_r \end{pmatrix} = \mathbf{1}_{\ell+r}.$$

Thus the order of $\overline{\rho}(h)$ is p. □

Corollary 5.12. *Let G be a HW-cyclic BT-group over S,*

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

be a matrix of φ_G, $P(X) = X^{p^c} + a_c X^{p^{c-1}} + \cdots + a_1 X \in A[X]$. If $h(G) = 1$ and if there exists $\alpha \in k \subset A$ such that $\mathtt{v}(P(\alpha)) = 1$, then the cohomology class (5.9.2) *is not zero,* i.e. *the extension of I-modules* (5.9.1) *does not split.*

Proof. Since $\mathtt{v}(a_1) = h(G) = 1$, the integer i_0 defined in 5.8(iii) is at least 1. Then the corollary follows from 5.8(iii) and 5.10. □

6. Lemmas in Group Theory

In this section, we fix a prime number $p \geq 2$ and an integer $n \geq 1$.

6.1. Recall that the general linear group $\mathrm{GL}_n(\mathbb{Z}_p)$ admits a natural exhaustive decreasing filtration by normal subgroups

$$\mathrm{GL}_n(\mathbb{Z}_p) \supset 1 + p\mathrm{M}_n(\mathbb{Z}_p) \supset \cdots \supset 1 + p^m\mathrm{M}_n(\mathbb{Z}_p) \supset \cdots,$$

where $\mathrm{M}_n(\mathbb{Z}_p)$ denotes the ring of matrix of type (n,n) with coefficients in $\mathbb{Z}_p$. We endow $\mathrm{GL}_n(\mathbb{Z}_p)$ with the topology for which $(1 + p^m\mathrm{M}_n(\mathbb{Z}_p))_{m\geq 1}$ form a fundamental system of neighborhoods of 1. Then $\mathrm{GL}_n(\mathbb{Z}_p)$ is a complete and separated topological group.

6.2. Let $\mathfrak{G}$ be a profinite group, $\rho : \mathfrak{G} \to \mathrm{GL}_n(\mathbb{Z}_p)$ be a continuous homomorphism of topological groups. By taking inverse images, we obtain a decreasing filtration $(F^m\mathfrak{G}, m \in \mathbb{Z}_{\geq 0})$ on $\mathfrak{G}$ by open normal subgroups:

$$F^0\mathfrak{G} = \mathfrak{G}, \quad \text{and} \quad F^m\mathfrak{G} = \rho^{-1}(1 + p^m\mathrm{M}_n(\mathbb{Z}_p)) \text{ for } m \geq 1.$$

Furthermore, the homomorphism ρ induces a sequence of injective homomorphisms of finite groups

$$\rho_0 \colon F^0\mathfrak{G}/F^1\mathfrak{G} \longrightarrow \mathrm{GL}_n(\mathbb{F}_p) \tag{6.2.1}$$

$$\rho_m \colon F^m\mathfrak{G}/F^{m+1}\mathfrak{G} \to \mathrm{M}_n(\mathbb{F}_p), \quad \text{for } m \geq 1. \tag{6.2.2}$$

LEMMA 6.3. *The homomorphism ρ is surjective if and only if the following conditions are satisfied:*
(i) *The homomorphism ρ_0 is surjective.*
(ii) *For every integer $m \geq 1$, the subgroup $\mathrm{Im}(\rho_m)$ of $\mathrm{M}_n(\mathbb{F}_p)$ contains an element of the form*

$$\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

with $x \neq 0$; or equivalently, there exists, for every $m \geq 1$, an element $g_m \in \mathfrak{G}$ such that $\rho(g_m)$ is of the form

$$\begin{pmatrix} 1+p^m a_{1,1} & p^{m+1}a_{1,2} & \cdots & p^{m+1}a_{1,n} \\ p^{m+1}a_{2,1} & 1+p^{m+1}a_{2,2} & \cdots & p^{m+1}a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p^{m+1}a_{n,1} & p^{m+1}a_{n,2} & \cdots & 1+p^{m+1}a_{n,n} \end{pmatrix},$$

where $a_{i,j} \in \mathbb{Z}_p$ for $1 \leq i, j \leq n$ and $a_{1,1}$ is not divisible by p.

Proof. We notice first that ρ is surjective if and only if ρ_m is surjective for every $m \geq 0$, because $\mathfrak{G}$ is complete and $\mathrm{GL}_n(\mathbb{Z}_p)$ is separated [Bou, Chap. III §2 n°8 Cor.2 au Théo. 1]. The surjectivity of ρ_0 is condition (i). Condition (ii) is clearly necessary. We prove that it implies the surjectivity of ρ_m for all $m \geq 1$, under the assumption of (i). First, we remark that under condition (i), if A lies in $\mathrm{Im}(\rho_m)$, then for any $U \in \mathrm{GL}_n(\mathbb{F}_p)$ the conjuagate matrix $U \cdot A \cdot U^{-1}$ lies also in $\mathrm{Im}(\rho_m)$. In fact, let $\widetilde{A}$ be a lift of A in $\mathrm{M}_n(\mathbb{Z}_p)$ and $\widetilde{U} \in \mathrm{GL}_n(\mathbb{Z}_p)$ a lift of U. By assumption, there exist $g, h \in \mathfrak{G}$ such that

$$\rho(g) \equiv 1+p^m\widetilde{A} \mod (1+p^{m+1}M_n(\mathbb{Z}_p)) \text{ and } \rho(h) \equiv \widetilde{U} \mod (1+p\mathrm{M}_n(\mathbb{Z}_p)).$$

Therefore, we have $\rho(hgh^{-1}) \equiv (1 + p^m\widetilde{U} \cdot \widetilde{A} \cdot \widetilde{U}^{-1}) \mod (1 + p^{m+1}\mathrm{M}_n(\mathbb{Z}_p))$. Hence $hgh^{-1} \in F^m\mathfrak{G}$ and $\rho_m(hgh^{-1}) = U \cdot A \cdot U^{-1}$.
For $1 \leq i, j \leq n$, let $E_{i,j} \in \mathrm{M}_n(\mathbb{F}_p)$ be the matrix whose (i, j)-th entry is 0 and the other entries are 0. The matrices $E_{i,j} (1 \leq i, j \leq n)$ form clearly

a basis of $\mathrm{M}_n(\mathbb{F}_p)$ over $\mathbb{F}_p$. To prove the surjectivity of ρ_m, we only need to verify that $E_{i,j} \in \mathrm{Im}(\rho_m)$ for $1 \le i, j \le n$, because $\mathrm{Im}(\rho_m)$ is an $\mathbb{F}_p$-subspace of $\mathrm{M}_n(\mathbb{F}_p)$. By assumption, we have $E_{1,1} \in \mathrm{Im}(\rho_m)$. For $2 \le i \le n$, we put $U_i = E_{1,i} - E_{i,1} + \sum_{j \ne 1,i} E_{j,j}$. Then we have $U_i \in \mathrm{GL}_n(\mathbb{Z}_p)$ and $U_i \cdot E_{1,1} \cdot U_i^{-1} = E_{i,i} \in \mathrm{Im}(\rho_m)$. For $1 \le i < j \le n$, we put $U_{i,j} = I + E_{i,j}$ where I is the unit matrix. Then we have $U_{i,j} \cdot E_{i,i} \cdot U_{i,j}^{-1} = E_{i,i} + E_{i,j} \in \mathrm{Im}(\rho_m)$, and hence $E_{i,j} \in \mathrm{Im}(\rho_m)$. This completes the proof.

□

Remark 6.4. By using the arguments in [Se2, Chap. IV 3.4 Lemma 3], we can prove the following stronger form of Lemma 6.3: *If $p = 2$, condition* (i) *and* (ii) *for $m = 1, 2$ are sufficient to guarantee the surjectivity of ρ; if $p \ge 3$, then* (i) *and* (ii) *just for $m = 1$ suffice already.*

A subgroup C of $\mathrm{GL}_n(\mathbb{F}_p)$ is called a *non-split Cartan subgroup*, if the subset $C \cup \{0\}$ of the matrix algebra $\mathrm{M}_n(\mathbb{F}_p)$ is a field isomorphic to $\mathbb{F}_{p^n}$; such a group is cyclic of order $p^n - 1$.

Lemma 6.5. *Assume that $n \ge 2$. We denote by H the subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ consisting of all the elements of the form $\begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix}$, where $A \in \mathrm{GL}_{n-1}(\mathbb{F}_p)$ and*

$b = \begin{pmatrix} b_1 \\ \vdots \\ b_{n-1} \end{pmatrix}$ with $b_i \in \mathbb{F}_p (1 \le i \le n-1)$. Let G be a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. Then $G = \mathrm{GL}_n(\mathbb{F}_p)$ if and only if G contains H and a non-split Cartan subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.

Proof. The "only if" part is clear. For the "if" part, let C be a non-split Cartan subgroup contained in G. For a finite group Λ, we denote by $|\Lambda|$ its order. An easy computation shows that $|\mathrm{GL}_n(\mathbb{F}_p)| = |H| \cdot |C|$. So we just need to prove that $U \cap C = \{1\}$; since then we will have $|\mathrm{GL}_n(\mathbb{F}_p)| = |G|$, hence $G = \mathrm{GL}_n(\mathbb{F}_p)$. Let $g \in H \cap C$, and $P(T) \in \mathbb{F}_p[T]$ be its characteristic polynomial. We fix an isomorphism $C \simeq \mathbb{F}_{p^n}^\times$, and let $\zeta \in \mathbb{F}_{p^n}^\times$ be the element corresponding to g. We have $P(T) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)} (T - \sigma(\zeta))$ in $\mathbb{F}_{p^n}[T]$. On the other hand, the fact that $g \in H$ implies that $(T-1)$ divises $P(T)$. Therefore, we get $\zeta = 1$, *i.e.* $g = 1$. □

Remark 6.6. E. Lau point out the following strengthened version of 6.5: *When $n \ge 3$, a subgroup $G \subset \mathrm{GL}_n(\mathbb{F}_p)$ coincides with $\mathrm{GL}_n(\mathbb{F}_p)$ if and only if G contains a non-split Cartan subgroup and the subgroup* $\begin{pmatrix} \mathrm{GL}_{n-1}(\mathbb{F}_p) & 0 \\ 0 & 1 \end{pmatrix}$. This can be used to simplify the induction process in the proof of Theorem 7.3 when $n \ge 3$.

7. Proof of Theorem 1.3 in the One-dimensional Case

7.1. We start with a general remark on the monodromy of BT-groups. Let X be a scheme, G be an ordinary BT-group over a scheme X, $G^{\text{ét}}$ be its étale part (2.10.1). 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 the functoriality, we have a commutative diagram

$$\begin{tikzcd} \pi_1(Y,\xi) \arrow[r, "\pi_1(f)"] \arrow[d, "\rho(G_Y)"'] & \pi_1(X, f(\overline{\xi})) \arrow[d, "\rho(G)"] \\ \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G_Y,\overline{\xi})) \arrow[r, equal] & \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(G, f(\overline{\xi}))) \end{tikzcd} \tag{7.1.1}$$

In particular, the monodromy of G_Y is a subgroup of the monodromy of G. In the sequel, diagram (7.1.1) will be refereed as the *functoriality of monodromy* for the BT-group G and the morphism f.

7.2. Let k be an algebraically closed field of characteristic $p>0$, G be the unique connected BT-group over k of dimension 1 and height $n+1\geq 2$ (4.10). We denote by $\mathbf{S}$ the algebraic local moduli of G in characteristic p, by $\mathbf{G}$ the universal deformation of G over $\mathbf{S}$, and by $\mathbf{U}$ the ordinary locus of $\mathbf{G}$ over $\mathbf{S}$ (3.8). Recall that $\mathbf{S}$ is affine of ring $R\simeq k[[t_1,\cdots,t_n]]$ (3.7), and that G and $\mathbf{G}$ are HW-cyclic (cf. 4.3(i) and 4.10). Let $\overline{\eta}$ be a geometric point of $\mathbf{U}$ over its generic point. We put

$$\mathrm{T}_p(\mathbf{G},\overline{\eta}) = \varprojlim_{m\in\mathbb{Z}_{\geq 1}} \mathbf{G}(m)(\overline{\eta})$$

to be the Tate module of $\mathbf{G}$ at the point $\overline{\eta}$. This is a free $\mathbb{Z}_p$-module of rank n. We have the monodromy representation

$$\rho_n : \pi_1(\mathbf{U},\overline{\eta}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathbf{G},\overline{\eta})) \simeq \mathrm{GL}_n(\mathbb{Z}_p).$$

The following is the one-dimensional case of Theorem 1.3.

Theorem 7.3. *Under the above assumptions, the homomorphism ρ_n is surjective for $n\geq 1$.*

7.4. First, we assume $n\geq 2$. By Proposition 4.11(ii), we may assume that

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -t_1 \\ 1 & 0 & \cdots & 0 & -t_2 \\ 0 & 1 & \cdots & 0 & -t_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -t_n \end{pmatrix} \tag{7.4.1}$$

is a matrix of the Hasse-Witt map $\varphi_{\mathbf{G}}$. Let $\mathfrak{p}$ be the prime ideal of R generated by $t_1, \cdots, t_{n-1}$. Then the closed subscheme of $\mathbf{S}$ defined by $\mathfrak{p}$ is just the locus where the p-rank of $\mathbf{G}$ is ≤ 1 by 4.4(ii). Let $K_0 \simeq k((t_n))$ be the fraction field of $R/\mathfrak{p}$, $R' = \widehat{R}_{\mathfrak{p}}$ be the completion of the localization of R at $\mathfrak{p}$, and $\mathscr{G}_{R'} = \mathbf{G} \otimes_R R'$. Since the natural map $R \to R'$ is injective, for any $a \in R$, we will denote also by a its image in R'. Since the Hasse-Witt map commutes with base change, the image of $\mathfrak{h}$ in $\mathrm{M}_{n\times n}(R')$, denoted also by $\mathfrak{h}$, is a matrix of $\varphi_{\mathscr{G}_{R'}}$. We see easily that the étale part of $\mathscr{G}_{R'}$ has height 1 and its connected part $\mathscr{G}^{\circ}_{R'}$ has height n. We have an exact sequence of BT-groups over R'

$$0 \to \mathscr{G}^{\circ}_{R'} \to \mathscr{G}_{R'} \to \mathscr{G}^{\text{ét}}_{R'} \to 0. \tag{7.4.2}$$

We fix an imbedding $i : K_0 \to \overline{K}_0$ of K_0 into an algebraically closed field. Put $\mathscr{G}^{*}_{\overline{K}_0} = \mathscr{G}^{*}_{R'} \otimes \overline{K}_0$ for $* = \emptyset, \text{ét}, \circ$. We have $\mathscr{G}^{\text{ét}}_{\overline{K}_0} \simeq \mathbb{Q}_p/\mathbb{Z}_p$, and $\mathscr{G}^{\circ}_{\overline{K}_0}$ is the unique connected one-dimensional BT-group over $\overline{K}_0$ of height n (cf. 4.10). We put $\widetilde{R'} = \overline{K}_0[[x_1, \cdots, x_{n-1}]]$, and

$$\Sigma = \{\text{ring homomorphisms } \sigma : R' \to \widetilde{R'} \text{ lifting } R' \to K_0 \xrightarrow{i} \overline{K}_0\} \tag{7.4.3}$$

Let $\sigma \in \Sigma$. We deduce from (7.4.2) by base change an exact sequence of BT-groups over $\widetilde{R'}$

$$0 \to \mathscr{G}^{\circ}_{\widetilde{R'},\sigma} \to \mathscr{G}_{\widetilde{R'},\sigma} \to \mathscr{G}^{\text{ét}}_{\widetilde{R'},\sigma} \to 0, \tag{7.4.4}$$

where we have put $\mathscr{G}^{*}_{\widetilde{R'},\sigma} = \mathscr{G}^{*}_{R'} \otimes_{\sigma} \widetilde{R'}$ for $* = \circ, \emptyset, \text{ét}$. Due to the henselian property of $\widetilde{R'}$, the isomorphism $\mathscr{G}^{\text{ét}}_{\overline{K}_0} \simeq \mathbb{Q}_p/\mathbb{Z}_p$ lifts uniquely to an isomorphism $\mathscr{G}^{\text{ét}}_{\widetilde{R'},\sigma} \simeq \mathbb{Q}_p/\mathbb{Z}_p$. Assume that $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}$ is generically ordinary over $\widetilde{S}' = \mathrm{Spec}(\widetilde{R'})$. Let $\widetilde{U}'_{\sigma} \subset \widetilde{S}'$ be its ordinary locus, and $\overline{x}$ be a geometric point over the generic point of $\widetilde{U}'_{\sigma}$. The exact sequence (7.4.4) induces an exact sequence of Tate modules

$$0 \to \mathrm{T}_p(\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}, \overline{x}) \to \mathrm{T}_p(\mathscr{G}_{\widetilde{R'},\sigma}, \overline{x}) \to \mathrm{T}_p(\mathscr{G}^{\text{ét}}_{\widetilde{R'},\sigma}, \overline{x}) \to 0 \tag{7.4.5}$$

compatible with the actions of $\pi_1(\widetilde{U}'_{\sigma}, \overline{x})$. Since we have $\mathrm{T}_p(\mathscr{G}^{\text{ét}}_{\widetilde{R'},\sigma}, \overline{x}) \simeq \mathrm{T}_p(\mathbb{Q}_p/\mathbb{Z}_p, \overline{x}) = \mathbb{Z}_p$, this determines a cohomology class

$$C_{\sigma} \in \mathrm{Ext}^1_{\mathbb{Z}_p[\pi_1(\widetilde{U}'_{\sigma},\overline{x})]}(\mathbb{Z}_p, \mathrm{T}_p(\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}, \overline{x})) \simeq H^1(\pi_1(\widetilde{U}'_{\sigma}, \overline{x}), \mathrm{T}_p(\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}, \overline{x})). \tag{7.4.6}$$

We consider also the "mod-p version" of (7.4.5)

$$0 \to \mathscr{G}^{\circ}_{\widetilde{R'},\sigma}(1)(\overline{x}) \to \mathscr{G}_{\widetilde{R'},\sigma}(1)(\overline{x}) \to \mathbb{F}_p \to 0,$$

which determines a cohomology class

$$\overline{C}_{\sigma} \in \mathrm{Ext}^1_{\mathbb{F}_p[\pi_1(\widetilde{U}'_{\sigma},\overline{x})]}(\mathbb{F}_p, \mathscr{G}^{\circ}_{\widetilde{R'},\sigma}(1)(\overline{x})) \simeq H^1(\pi_1(\widetilde{U}'_{\sigma}, \overline{x}), \mathscr{G}^{\circ}_{\widetilde{R'},\sigma}(1)(\overline{x})). \tag{7.4.7}$$

It is clear that $\overline{C}_{\sigma}$ is the image of C_{σ} by the canonical reduction map

$$H^1(\pi_1(\widetilde{U}'_{\sigma}, \overline{x}), \mathrm{T}_p(\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}, \overline{x})) \to H^1(\pi_1(\widetilde{U}'_{\sigma}, \overline{x}), \mathscr{G}^{\circ}_{\widetilde{R'},\sigma}(1)(\overline{x})).$$

Lemma 7.5. *Under the above assumptions, there exist $\sigma_1, \sigma_2 \in \Sigma$ satisfying the following properties:*
(i) *We have $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma_1} = \mathscr{G}^{\circ}_{\widetilde{R'},\sigma_2}$, and it is the universal deformation of $\mathscr{G}^{\circ}_{\overline{K}_0}$.*
(ii) *We have $C_{\sigma_1} = 0$ and $\overline{C}_{\sigma_2} \neq 0$.*

Before proving this lemma, we prove first Theorem 7.3.

Proof of 7.3. First, we notice that the monodromy of a BT-group is independent of the base point. So we can change $\overline{\eta}$ to any geometric point of $\mathbf{U}$ when discussing the monodromy of $\mathbf{G}$. We make an induction on the codimension $n = \dim(G^{\vee})$. The case of $n = 1$ is proved in Theorem 5.7. Assume that $n \geq 2$ and the theorem is proved for $n-1$. We denote by

$$\overline{\rho}_n : \pi_1(\mathbf{U}, \overline{\eta}) \to \mathrm{Aut}_{\mathbb{F}_p}(\mathbf{G}(1)(\overline{\eta})) \simeq \mathrm{GL}_n(\mathbb{F}_p)$$

the reduction of ρ_n modulo by p. By Lemma 6.3 and 6.5, to prove the surjectivity of ρ_n, we only need to verify the following conditions:
(a) $\mathrm{Im}(\overline{\rho}_n)$ contains a non-split Cartan subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$;
(b) $\mathrm{Im}(\rho_n)$ contains the subgroup $H \subset \mathrm{GL}_n(\mathbb{Z}_p)$ consisting of all the elements of the form $\begin{pmatrix} B & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}_p)$, with $B \in \mathrm{GL}_{n-1}(\mathbb{Z}_p)$ and $b \in \mathrm{M}_{(n-1)\times 1}(\mathbb{Z}_p)$;
For condition (a), let $A = k[[\pi]]$, $T = \mathrm{Spec}(A)$, ξ be its generic point, $\overline{\xi}$ be a geometric point over ξ, and $I = \mathrm{Gal}(\overline{\xi}/\xi)$ be the absolute Galois group over ξ. We keep the notations of 7.4. Let $f^* : R \to A$ be the homomorphism of k-algebras such that $f^*(t_1) = \pi$ and $f^*(t_i) = 0$ for $2 \leq i \leq n$. We denote by $f : T \to \mathbf{S}$ the corresponding morphism of schemes, and put $G_T = \mathbf{G} \times_{\mathbf{S}} T$. By the functoriality of Hasse-Witt maps,

$$\mathfrak{h}_T = \begin{pmatrix} 0 & 0 & \cdots & 0 & -\pi \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

is a matrix of φ_{G_T}. By definition 5.4, the Hasse invariant of G_T is $h(G) = 1$. Hence G_T is generically ordinary; so $f(\xi) \in \mathbf{U}$. Let

$$\overline{\rho}_T : I = \mathrm{Gal}(\overline{\xi}/\xi) \to \mathrm{Aut}_{\mathbb{F}_p}(G_T(1)(\overline{\xi}))$$

be the mod-p monodromy representation attached to G_T. Proposition 5.8(i) implies that $\mathrm{Im}(\overline{\rho}_T)$ is a non-split Cartan subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. On the other hand, by the functoriality of monodromy, we get $\mathrm{Im}(\overline{\rho}_T) \subset \mathrm{Im}(\overline{\rho}_n)$. This verifies condition (a).
To check condition (b), we consider the constructions in 7.4. Let $S' = \mathrm{Spec}(R')$, $f : S' \to \mathbf{S}$ be the morphism of schemes corresponding to the natural ring homomorphism $R \to R'$, U' be the ordinary locus of $\mathscr{G}_{R'}$, and $\overline{\xi}$ be a geometric point of U'. From (7.4.2), we deduce an exact sequence of Tate modules

$$0 \to \mathrm{T}_p(\mathscr{G}^{\circ}_{R'}, \overline{\xi}) \to \mathrm{T}_p(\mathscr{G}_{R'}, \overline{\xi}) \to \mathrm{T}_p(\mathscr{G}^{\text{ét}}_{R'}, \overline{\xi}) \to 0. \tag{7.5.1}$$

Let $\rho_{\mathscr{G}'}:\pi_1(U',\overline{\xi})\to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathscr{G}_{R'},\overline{\xi}))\simeq \mathrm{GL}_n(\mathbb{Z}_p)$ be the monodromy representation of $\mathscr{G}_{R'}$. Under any basis of $\mathrm{T}_p(\mathscr{G}_{R'},\overline{\xi})$ adapted to (7.5.1), the action of $\pi_1(U',\overline{\xi})$ on $\mathrm{T}_p(\mathscr{G}_{R'},\overline{\xi})$ is given by

$$\rho_{\mathscr{G}_{R'}}: g\in \pi_1(U',\overline{\xi})\mapsto \begin{pmatrix}\rho_{\mathscr{G}^{\circ}_{R'}}(g) & * \\ 0 & \rho_{\mathscr{G}^{\text{ét}}_{R'}}(g),\end{pmatrix}$$

where $g\mapsto \rho_{\mathscr{G}^{\circ}_{R'}}(g)\in \mathrm{GL}_{n-1}(\mathbb{Z}_p)$ (*resp.* $g\mapsto \rho_{\mathscr{G}^{\text{ét}}_{R'}}(g)\in \mathbb{Z}_p^{\times}$) gives the action of $\pi_1(U',\overline{\xi})$ on $\mathrm{T}_p(\mathscr{G}^{\circ}_{R'},\overline{\xi})$ (*resp.* on $\mathrm{T}_p(\mathscr{G}^{\text{ét}}_{R'},\overline{\xi})$). Note that $f(U')\subset \mathbf{U}$. So by the functoriality of monodromy, we get $\mathrm{Im}(\rho_{\mathscr{G}'})\subset \mathrm{Im}(\rho_n)$. To complete the proof of Theorem 7.3, it suffices to check condition (b) with ρ_n replaced by $\rho_{\mathscr{G}_{R'}}$ under the induction hypothesis that 7.3 is valide for $n-1$. Let $\sigma_1,\sigma_2: R'\to\widetilde{R'}$ be the homomorphisms given by 7.5. For $i=1,2$, we denote by $f_i:\widetilde{S}'=\mathrm{Spec}(\widetilde{R'})\to S'=\mathrm{Spec}(R')$ the morphism of schemes corresponding to σ_i, and put $\mathscr{G}_i=\mathscr{G}_{\widetilde{R'},\sigma_i}=\mathscr{G}_{R'}\otimes_{\sigma_i}\widetilde{R'}$ to simply the notations. By condition 7.5(i), we can denote by $\mathscr{G}^{\circ}$ the common connected component of $\mathscr{G}_1$ and $\mathscr{G}_2$. Let $\widetilde{U'}\subset\widetilde{S}'$ be the ordinary locus of $\mathscr{G}^{\circ}$. Then we have $f_i(\widetilde{U'})\subset U'$ for $i=1,2$. Let $\overline{x}$ be a geometric point over the generic point of $\widetilde{U'}$. We have an exact sequence of Tate modules

$$0\to \mathrm{T}_p(\mathscr{G}^{\circ},\overline{x})\to \mathrm{T}_p(\mathscr{G}_i,\overline{x})\to \mathrm{T}_p(\mathbb{Q}_p/\mathbb{Z}_p,\overline{x})\to 0 \tag{7.5.2}$$

compatible with the actions of $\pi_1(\widetilde{U'},\overline{x})$. We denote by

$$\rho_{\mathscr{G}_i}:\pi_1(\widetilde{U'},\overline{x})\to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathscr{G}_i,\overline{x}))\simeq \mathrm{GL}_n(\mathbb{Z}_p)$$

the monodromy representation of $\mathscr{G}_i$. In a basis adapted to (7.5.2), the action of $\pi_1(\widetilde{U'},\overline{x})$ on $\mathrm{T}_p(\mathscr{G}_i,\overline{x})$ is given by

$$\rho_{\mathscr{G}_i}: g\mapsto \begin{pmatrix}\rho_{\mathscr{G}^{\circ}}(g) & C_{\sigma_i}(g)\\ 0 & 1\end{pmatrix},$$

where $\rho_{\mathscr{G}^{\circ}}:\pi_1(\widetilde{U'},\overline{x})\to \mathrm{GL}_{n-1}(\mathbb{Z}_p)$ is the monodromy representation of $\mathscr{G}^{\circ}$, and the cohomology class in $H^1(\pi_1(\widetilde{U'},\overline{x}),\mathrm{T}_p(\mathscr{G}^{\circ}))$ given by $g\mapsto C_{\sigma_i}(g)$ is nothing but the class defined in (7.4.6). By 7.5(i) and the induction hypothesis, $\rho_{\mathscr{G}^{\circ}}$ is surjective. Since the cohomology class $C_{\sigma_1}=0$ by 7.5(ii), we may assume $C_{\sigma_1}(g)=0$ for all $g\in\pi_1(U',\overline{x})$. Therefore $\mathrm{Im}(\rho_{\mathscr{G}_1})$ contains all the matrix of the form $\begin{pmatrix}B & 0\\ 0 & 1\end{pmatrix}$ with $B\in \mathrm{GL}_{n-1}(\mathbb{Z}_p)$. By the functoriality of monodromy, $\mathrm{Im}(\rho_{\mathscr{G}_{R'}})$ contains $\mathrm{Im}(\rho_{\mathscr{G}_1})$. Hence we have

$$\begin{pmatrix}\mathrm{GL}_{n-1}(\mathbb{Z}_p) & 0\\ 0 & 1\end{pmatrix}\subset \mathrm{Im}(\rho_{\mathscr{G}_1})\subset \mathrm{Im}(\rho_{\mathscr{G}_{R'}}). \tag{7.5.3}$$

On the other hand, since the cohomology class $\overline{C}_{\sigma_2}\neq 0$, there exists a $g\in\pi_1(\widetilde{U'},\overline{x})$ such that $b_2=\overline{C}_{\sigma_2}(g)\neq 0$. Hence the matrix $\rho_{\mathscr{G}_2}(g)$ has the form $\begin{pmatrix}B_2 & b_2\\ 0 & 1\end{pmatrix}$ such that $B_2\in \mathrm{GL}_{n-1}(\mathbb{Z}_p)$ and the image of $b_2\in \mathrm{M}_{1\times n-1}(\mathbb{Z}_p)$

in $\mathrm{M}_{1\times n-1}(\mathbb{F}_p)$ is non-zero. By the functoriality of monodromy, we have $\mathrm{Im}(\rho_{\mathscr{G}_2}) \subset \mathrm{Im}(\rho_{\mathscr{G}_{R'}})$; in particular, we have $\begin{pmatrix} B_2 & b_2 \\ 0 & 1 \end{pmatrix} \in \mathrm{Im}(\rho_{\mathscr{G}_{R'}})$. In view of (7.5.3), we get

$$\begin{pmatrix} \mathrm{GL}_{n-1}(\mathbb{Z}_p) & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} B_2 & b_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mathrm{GL}_{n-1}(\mathbb{Z}_p) & 0 \\ 0 & 1 \end{pmatrix} \subset \mathrm{Im}(\rho_{\mathscr{G}_{R'}}). \tag{7.5.4}$$

But the subset of $\mathrm{GL}_n(\mathbb{Z}_p)$ on the left hand side is just the subgroup H described in condition (b). Therefore, condition (b) is verified for $\rho_{\mathscr{G}_{R'}}$, and the proof of 7.3 is complete.

The rest of this section is dedicated to the proof of Lemma 7.5.

Lemma 7.6. *Let k be an algebraically closed field of characteristic $p > 0$, A be a noetherian henselian local k-algebra with residue field k, G be a BT-group over A, and $G^{\text{ét}}$ be its étale part. Put*

$$\mathrm{Lie}(G^\vee)^{\varphi=1} = \{x \in \mathrm{Lie}(G^\vee) \text{ such that } \varphi_G(x) = x\}.$$

Then $\mathrm{Lie}(G^\vee)^{\varphi=1}$ is an $\mathbb{F}_p$-vector space of dimension equal to the rank of $\mathrm{Lie}(G^{\text{ét}\vee})$, and the A-submodule $\mathrm{Lie}(G^{\text{ét}\vee})$ of $\mathrm{Lie}(G^\vee)$ is generated by $\mathrm{Lie}(G^\vee)^{\varphi=1}$.

Proof. Let r be the rank of $\mathrm{Lie}(G^{\text{ét}\vee})$, G° be the connected part of G, and s be the height of $\mathrm{Lie}(G^{\circ\vee})$. We have an exact sequence of A-modules

$$0 \to \mathrm{Lie}(G^{\text{ét}\vee}) \to \mathrm{Lie}(G^\vee) \to \mathrm{Lie}(G^{\circ\vee}) \to 0,$$

compatible with Hasse-Witt maps. We choose a basis of $\mathrm{Lie}(G^\vee)$ adapted to this exact sequence, so that φ_G is expressed by a matrix of the form $\begin{pmatrix} U & W \\ 0 & V \end{pmatrix}$ with $U \in \mathrm{M}_{r\times r}(A)$, $V \in \mathrm{M}_{s\times s}(A)$, and $W \in \mathrm{M}_{r\times s}(A)$. An element of $\mathrm{Lie}(G^\vee)^{\varphi=1}$ is given by a vector $\begin{pmatrix} x \\ y \end{pmatrix}$, where $x = \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}$ and $y = \begin{pmatrix} y_1 \\ \vdots \\ y_s \end{pmatrix}$ with $x_i, y_j \in A$, satisfying

$$\begin{pmatrix} U & W \\ 0 & V \end{pmatrix} \cdot \begin{pmatrix} x^{(p)} \\ y^{(p)} \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \quad \Leftrightarrow \quad \begin{cases} U \cdot x^{(p)} + W \cdot y^{(p)} = x \\ V \cdot y^{(p)} = y. \end{cases} \tag{7.6.1}$$

where $x^{(p)}$ (*resp.* $y^{(p)}$) is the vector obtained by applying $a \mapsto a^p$ to each $x_i (1 \leq i \leq r)$ (*resp.* $y_j (1 \leq j \leq s)$). By 2.9, the Hasse-Witt map of the special fiber of G° is nilpotent. So there exists an integer $N \geq 1$ such that $\varphi^N_{G^\circ}(\mathrm{Lie}(G^{\circ\vee})) \subset \mathfrak{m}_A \cdot \mathrm{Lie}(G^{\circ\vee})$, *i.e.* we have $V \cdot V^{(p)} \cdots V^{(p^{N-1})} \equiv 0 \pmod{\mathfrak{m}_A}$. From the equation $V \cdot y^{(p)} = y$, we deduce that

$$y = V \cdot V^{(p)} \cdots V^{(p^{N-1})} \cdot y^{(p^N)} \equiv 0 \pmod{\mathfrak{m}_A}.$$

But this implies that $y^{(p^N)} \equiv 0 \pmod{\mathfrak{m}_A^{p^N}}$. Hence we get $y = V \cdot y^{(p)} \equiv 0 \pmod{\mathfrak{m}_A^{p^N+1}}$. Repeting this argument, we get finally $y \equiv 0 \pmod{\mathfrak{m}_A^{\ell}}$ for all integers $\ell \geq 1$, so $y = 0$. This implies that $\mathrm{Lie}(G^\vee)^{\varphi=1} \subset \mathrm{Lie}(G^{\text{ét}\vee})$, and the equation (7.6.1) is simplified as $U \cdot x^{(p)} = x$. Since the linearization of $\varphi_{G^{\text{ét}}}$ is bijective by 2.11, we have $U \in \mathrm{GL}_r(A)$. Let $\overline{U}$ be the image of U in $\mathrm{GL}_r(k)$, and Sol be the solutions of the equation $\overline{U} \cdot x^{(p)} = x$. As k is algebraically closed, Sol is an $\mathbb{F}_p$-space of dimension r, and $\mathrm{Lie}(G^{\text{ét}\vee}) \otimes k$ is generated by Sol (cf. [Ka2, Prop. 4.1]). By the henselian property of A, every elements in Sol lifts uniquely to a solution of $U \cdot x^{(p)} = x$, *i.e.* the reduction map $\mathrm{Lie}(G^\vee)^{\varphi=1} \xrightarrow{\sim} \mathrm{Sol}$ is bijective. By Nakayama's lemma, $\mathrm{Lie}(G^\vee)^{\varphi=1}$ generates the A-module $\mathrm{Lie}(G^{\text{ét}\vee})$. □

7.7. We keep the notations of 7.4. Let $\mathbf{Comp}_{\overline{K}_0}$ be the category of noetherian complete local $\overline{K}_0$-algebras with residue field $\overline{K}_0$, $\mathcal{D}_{\mathscr{G}_{\overline{K}_0}}$ (*resp.* $\mathcal{D}_{\mathscr{G}^\circ_{\overline{K}_0}}$) be the functor which associates to every object A of $\mathbf{Comp}_{\overline{K}_0}$ the set of isomorphsm classes of deformations of $\mathscr{G}_{\overline{K}_0}$ (*resp.* $\mathscr{G}^\circ_{\overline{K}_0}$) . If A is an object in $\mathbf{Comp}_{\overline{K}_0}$ and G is a deformation of $\mathscr{G}_{\overline{K}_0}$ (*resp.* $\mathscr{G}^\circ_{\overline{K}_0}$) over A, we denote by $[G]$ its isomorphic class in $\mathcal{D}_{\mathscr{G}_{\overline{K}_0}}(A)$ (*resp.* in $\mathcal{D}_{\mathscr{G}^\circ_{\overline{K}_0}}$).

Lemma 7.8. *Let Σ be the set defined in* (7.4.3).
(i) *The morphism of sets $\Phi : \Sigma \to \mathcal{D}_{\mathscr{G}_{\overline{K}_0}}(\widetilde{R'})$ given by $\sigma \mapsto [\mathscr{G}_{\widetilde{R'},\sigma}]$ is bijective.*
(ii) *Let $\sigma \in \Sigma$. Then there exists a basis of $\mathrm{Lie}(\mathscr{G}^{\circ\vee}_{\widetilde{R'},\sigma})$ such that $\varphi_{\mathscr{G}^\circ_{\widetilde{R'},\sigma}}$ is represented by a matrix of the form*

$$\mathfrak{h}^\circ_\sigma = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_1 \\ 1 & 0 & \cdots & 0 & a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix} \tag{7.8.1}$$

with $a_i \equiv \alpha \cdot \sigma(t_i) \pmod{\mathfrak{m}^2_{\widetilde{R'}}}$ for $1 \leq i \leq n-1$, where $\alpha \in \widetilde{R'}^\times$ and $\mathfrak{m}_{\widetilde{R'}}$ is the maximal ideal of $\widetilde{R'}$. In particular, $\mathscr{G}^\circ_{\widetilde{R'},\sigma}$ is the universal deformation of $\mathscr{G}^\circ_{\overline{K}_0}$ if and only if $\{\sigma(t_1), \cdots, \sigma(t_{n-1})\}$ is a system of regular parameters of $\widetilde{R'}$.

Proof. (i) We begin with a remark on the Kodaira-Spencer map of $\mathscr{G}_{R'}$. Let $\mathscr{T}_{\mathbf{S}/k} = \mathscr{H}om_{\mathscr{O}_\mathbf{S}}(\Omega^1_{\mathbf{S}/k}, \mathscr{O}_\mathbf{S})$ be the tangent sheaf of $\mathbf{S}$. Since $\mathbf{G}$ is universal, the Kodaira-Spencer map (3.2.2)

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

is an isomorphism. By functoriality, this induces an isomorphism of R'-modules

$$\mathrm{Kod}_{R'} : T_{R'/k} \xrightarrow{\sim} \mathrm{Hom}_{R'}(\omega_{\mathscr{G}_{R'}}, \mathrm{Lie}(\mathscr{G}^\vee_{R'})), \tag{7.8.2}$$

where $T_{R'/k} = \mathrm{Hom}_{R'}(\Omega^1_{R'/k}, R') = \Gamma(\mathbf{S}, \mathscr{T}_{\mathbf{S}/k}) \otimes_R R'$.

For each integer $\nu \geq 0$, we put $\widetilde{R'}_\nu = \widetilde{R'}/\mathfrak{m}^{\nu+1}_{\widetilde{R'}}$, Σ_ν to be the set of liftings of $R \to K_0 \to \overline{K}_0$ to $R \to \widetilde{R'}_\nu$, and $\Phi_\nu : \Sigma_\nu \to \mathcal{D}_{\mathscr{G}_{\overline{K}_0}}(\widetilde{R'}_\nu)$ to be the morphism of sets $\sigma_\nu \mapsto [\mathscr{G}_{R'} \otimes_{\sigma_\nu} \widetilde{R'}_\nu]$. We prove by induction on ν that Φ_ν is bijective for all $\nu \geq 0$. This will complete the proof of (i). For $\nu = 0$, the claim holds trivially. Assume that it holds for $\nu - 1$ with $\nu \geq 1$. We have a commutative diagram

$$\begin{tikzcd}
\Sigma_\nu \arrow[r, "\Phi_\nu"] \arrow[d] & \mathcal{D}_{\mathscr{G}_{\overline{K}_0}}(\widetilde{R'}_\nu) \arrow[d] \\
\Sigma_{\nu-1} \arrow[r, "\Phi_{\nu-1}"] & \mathcal{D}_{\mathscr{G}_{\overline{K}_0}}(\widetilde{R'}_{\nu-1}),
\end{tikzcd}$$

where the vertical arrows are the canonical reductions, and the lower arrow is an isomorphism by induction hypothesis. Let τ be an arbitrary element of $\Sigma_{\nu-1}$. We denote by $\Sigma_{\nu,\tau} \subset \Sigma_\nu$ the preimage of τ, and by $\mathcal{D}_{\Phi_{\nu-1}(\tau)}(\widetilde{R'}_\nu) \subset \mathcal{D}_{\mathscr{G}_{\overline{K}_0}}(\widetilde{R'}_\nu)$ the preimage of $\Phi_{\nu-1}(\tau)$. It suffices to prove that Φ_ν induces a bijection between $\Sigma_{\nu,\tau}$ and $\mathcal{D}_{\Phi_{\nu-1}(\tau)}(\widetilde{R'}_\nu)$. Let $I_\nu = \mathfrak{m}^\nu_{\widetilde{R'}}/\mathfrak{m}^{\nu+1}_{\widetilde{R'}}$ be the ideal of the reduction map $\widetilde{R'}_\nu \to \widetilde{R'}_{\nu-1}$. By [EGA, 0_{IV} 21.2.5 and 21.9.4], we have $\Omega^1_{R'/k} \simeq \widehat{\Omega}^1_{R'/k}$, and they are free over A of rank n. By [EGA, 0_{IV} 20.1.3], $\Sigma_{\nu,\tau}$ is a (nonempty) homogenous space under the group

$$\mathrm{Hom}_{K_0}(\Omega^1_{R'/k} \otimes_{R'} K_0, I_\nu) = T_{R'/k} \otimes_{R'} I_\nu.$$

On the other hand, according to 3.5(i), $\mathcal{D}_{\Phi_{\nu-1}(\tau)}(\widetilde{R'}_\nu)$ is a homogenous space under the group

$$\mathrm{Hom}_{\overline{K}_0}(\omega_{\mathscr{G}_{\overline{K}_0}}, \mathrm{Lie}(\mathscr{G}^\vee_{\overline{K}_0})) \otimes_{\overline{K}_0} I_\nu = \mathrm{Hom}_{R'}(\omega_{\mathscr{G}_{R'}}, \mathrm{Lie}(\mathscr{G}^\vee_{R'})) \otimes_{R'} I_\nu.$$

Moreover, it is easy to check that the morphism of sets $\Phi_\nu : \Sigma_{\nu,\tau} \to \mathcal{D}_{\Phi_{\nu-1}(\tau)}(\widetilde{R'}_\nu)$ is compatible with the homomorphism of groups

$$\mathrm{Kod}_{R'} \otimes_{R'} \mathrm{Id} : T_{R'/k} \otimes_{R'} I_\nu \to \mathrm{Hom}_{R'}(\omega_{\mathscr{G}_{R'}}, \mathrm{Lie}(\mathscr{G}^\vee_{R'})) \otimes_{R'} I_\nu,$$

where $\mathrm{Kod}_{R'}$ is the Kodaira-Spencer map (7.8.2) associated to $\mathscr{G}_{R'}$. The bijectivity of Φ_ν now follows from the fact that $\mathrm{Kod}_{R'}$ is an isomorphism.

(ii) The second part of the statement follows immediately from 4.11. It remains to compute the Hasse-Witt map of $\mathscr{G}^\circ_{\widetilde{R'},\sigma}$. We determine first the submodule $\mathrm{Lie}(\mathscr{G}^{\text{ét}\vee}_{\widetilde{R'},\sigma})$ of $\mathrm{Lie}(\mathscr{G}^\vee_{\widetilde{R'},\sigma})$. We choose a basis of $\mathrm{Lie}(\mathbf{G}^\vee)$ over $\mathscr{O}_{\mathbf{S}}$ such that $\varphi_{\mathbf{G}}$ is expressed by the matrix $\mathfrak{h}$ (7.4.1). As $\mathscr{G}_{\widetilde{R'},\sigma}$ derives from $\mathbf{G}$ by base change $R \to R' \xrightarrow{\sigma} \widetilde{R'}$, there exists a basis $(e_1, \cdots, e_n)$ of $\mathrm{Lie}(\mathscr{G}^\vee_{\widetilde{R'},\sigma})$ such that $\varphi_{\mathscr{G}_{\widetilde{R'},\sigma}}$ is expressed by

$$\mathfrak{h}^\sigma = \begin{pmatrix} 0 & 0 & \cdots & 0 & -\sigma(t_1) \\ 1 & 0 & \cdots & 0 & -\sigma(t_2) \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -\sigma(t_n) \end{pmatrix}.$$

By Lemma 7.6, $\mathrm{Lie}(\mathscr{G}^{\text{ét}\vee}_{\widetilde{R'},\sigma})$ is generated by $\mathrm{Lie}(\mathscr{G}^\vee_{\widetilde{R'},\sigma})^{\varphi=1}$. If $\sum_{i=1}^n x_n e_n \in \mathrm{Lie}(\mathscr{G}^\vee_{\widetilde{R'},\sigma})^{\varphi=1}$ with $x_i \in \widetilde{R'}$ for $1 \leq i \leq n$, then $(x_i)_{1\leq i\leq n}$ must satisfy the equation $\mathfrak{h}^{\sigma}\cdot\begin{pmatrix}x_1^p\\ \vdots\\ x_n^p\end{pmatrix}=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$; or equivalently,

$$\begin{cases}x_1=-\sigma(t_1)x_n^p\\ x_2=-\sigma(t_2)x_n^p-\sigma(t_1)^p x_n^{p^2}\\ \cdots\\ x_{n-1}=-\sigma(t_{n-1})x_n^p-\cdots-\sigma(t_1)^{p^{n-2}}x_n^{p^{n-1}}\\ \sigma(t_1)^{p^{n-1}}x_n^{p^n}+\sigma(t_2)^{p^{n-2}}x_n^{p^{n-1}}+\cdots+\sigma(t_n)x_n^p+x_n=0.\end{cases}\tag{7.8.3}$$

We note that $\sigma(t_i)\in\mathfrak{m}_{\widetilde{R'}}$ for $1\le i\le n-1$ and $\sigma(t_n)\in\widetilde{R'}^{\times}$ with image $i(t_n)\in\overline{K}_0$, where $i:K_0\to\overline{K}_0$ is the fixed immbedding. By Hensel's lemma, every solution in $\overline{K}_0$ of the equation $i(t_n)x_n^p+x_n=0$ lifts uniquely to a solution of (7.8.3). As $\mathrm{Lie}(\mathscr{G}^{\text{ét}\vee}_{\widetilde{R'},\sigma})$ has rank 1, by Lemma 7.6, these are all the solutions of (7.8.3). Let $(\lambda_1,\cdots,\lambda_n)$ be a non-zero solution of (7.8.3). We have

$$\lambda_n\in\widetilde{R'}^{\times}\quad\text{and}\quad\lambda_i\equiv-\lambda_n^p\sigma(t_i)\pmod{\mathfrak{m}^2_{\widetilde{R'}}}.\tag{7.8.4}$$

We put $v=\lambda_1e_1+\cdots+\lambda_ne_n$; so v is a basis of $\mathrm{Lie}(\mathscr{G}^{\text{ét}\vee}_{\widetilde{R'},\sigma})$ by 7.6. For $1\le i\le n$, let f_i be the image of e_i in $\mathrm{Lie}(\mathscr{G}^{\circ\vee}_{\widetilde{R'},\sigma})$. Then $f_1,\cdots,f_n$ clearly generate $\mathrm{Lie}(\mathscr{G}^{\circ\vee}_{\widetilde{R'},\sigma})$. By the explicit description above of $\mathrm{Lie}(\mathscr{G}^{\text{ét}\vee}_{\widetilde{R'},\sigma})$, we have $f_n=-\lambda_n^{-1}(\lambda_1f_1\cdots+\lambda_{n-1}f_{n-1})$. Hence $f_1,\cdots,f_{n-1}$ form a basis of $\mathrm{Lie}(\mathscr{G}^{\circ\vee}_{\widetilde{R'},\sigma})$. By the functoriality of Hasse-Witt maps, we have $\varphi_{\mathscr{G}^{\circ}_{\widetilde{R'}}}(f_i)=f_{i+1}$ for $1\le i\le n-1$, or equivalently,

$$\varphi_{\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}}(f_1,\cdots,f_{n-1})=(f_1,\cdots,f_{n-1})\cdot\begin{pmatrix}0&0&\cdots&0&-\lambda_n^{-1}\lambda_1\\ 1&0&\cdots&0&-\lambda_n^{-1}\lambda_2\\ \vdots&&\ddots&&\vdots\\ 0&0&\cdots&1&-\lambda_n^{-1}\lambda_{n-1}\end{pmatrix}.$$

In view of (7.8.4), we see that the above matrix has the form of (7.8.1) by setting $\alpha=\lambda_n^{p-1}\in\widetilde{R'}^{\times}$. The second part of statement (ii) follows immediately from Proposition 4.11(ii) and the description above of $\varphi_{\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}}$. □

Now we can turn to the proof of 7.5.

7.9. Proof of Lemma 7.5. First, suppose that we have found a $\sigma_2\in\Sigma$ such that $\overline{C}_{\sigma_2}\neq0$ and $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma_2}$ is the universal deformation of $\mathscr{G}^{\circ}_{\overline{K}_0}$. Since $\Phi:\Sigma\xrightarrow{\sim}\mathcal{D}_{\mathscr{G}_{\overline{K}_0}}(\widetilde{R'})$ is bijective by 7.8(i), there exists a $\sigma_1\in\Sigma$ corresponding to the deformation $[\mathscr{G}^{\circ}_{\widetilde{R'},\sigma_2}\oplus\mathbb{Q}_p/\mathbb{Z}_p]\in\mathcal{D}_{\mathscr{G}_{\overline{K}_0}}(\widetilde{R'})$. It is clear that $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma_1}\simeq\mathscr{G}^{\circ}_{\widetilde{R'},\sigma_2}$. Besides, the exact sequence (7.4.5) for σ_1 splits; so we have $C_{\sigma_1}=0$. It remains to prove the existence of σ_2. We note first that $\overline{K}_0$ can be canonically imbedded into $\widetilde{R'}$, since it is perfect. Since R' is formally smooth over k and

$(t_1, \cdots, t_n)$ is a p-basis of R' over k, by [EGA, 0_{IV} 21.2.7], there is a $\sigma \in \Sigma$ such that $\sigma(t_i)$ $(1 \leq i \leq n-1)$ form a system of regular parameters of $\widetilde{R'}$ and $\sigma(t_n) \in \overline{K}_0 \subset \widetilde{R'}$. We claim that $\sigma_2 = \sigma$ answers the question. In fact, Lemma 7.8(ii) implies that $\mathscr{G}^{\circ}_{\widetilde{R'},\sigma}$ is the universal deformation of $\mathscr{G}^{\circ}_{\overline{K}_0}$. It remains to verify that $\overline{C}_\sigma \neq 0$.

Let $A = \overline{K}_0[[\pi]]$ be a complete discrete valuation ring of characteristic p with residue field $\overline{K}_0$, $T = \mathrm{Spec}(A)$, ξ be the generic point of T, $\bar{\xi}$ be a geometric over ξ, and $I = \mathrm{Gal}(\bar{\xi}/\xi)$ the Galois group. We define a homomorphism of $\overline{K}_0$-algebras $f^* : \widetilde{R'} \to A$ by putting $f^*(\sigma(t_1)) = \pi$ and $f^*(\sigma(t_i)) = 0$ for $2 \leq i \leq n-1$. This is possible, since $(\sigma(t_1), \cdots, \sigma(t_{n-1}))$ is a system of regular parameters of $\widetilde{R'}$. Let $f : T \to \widetilde{S}'$ be the homomorphism of schemes corresponding to f^*, and $\mathscr{G}_T = \mathscr{G}_{\widetilde{R'},\sigma} \times_{\widetilde{S'}} T$. By the functoriality of Hasse-Witt maps,

$$\mathfrak{h}_T = \begin{pmatrix} 0 & 0 & \cdots & 0 & -\pi \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -f^*(\sigma(t_n)) \end{pmatrix} \in \mathrm{M}_{n\times n}(\widetilde{R'})$$

is a matrix of $\varphi_{\mathscr{G}_T}$. By definition (5.4), the Hasse invariant of $\mathscr{G}_T$ is $h(\mathscr{G}_T) = 1$. In particular, $\mathscr{G}_T$ is generically ordinary. Let $\widetilde{U}'_\sigma \subset \widetilde{S}'$ be the ordinary locus of $\mathscr{G}_{\widetilde{R'},\sigma}$. We have $f(\xi) \in \widetilde{U}'_\sigma$. By the functoriality of fundamental groups, f induces a homomorphism of groups

$$\pi_1(f) : I = \mathrm{Gal}(\bar{\xi}/\xi) \to \pi_1(\widetilde{U}'_\sigma, f(\bar{\xi})) \simeq \pi_1(\widetilde{U}'_\sigma, \overline{x}).$$

Let $\mathscr{G}_T^\circ$ be the connected part of $\mathscr{G}_T$, and $\mathscr{G}_T^{\text{ét}}$ be the étale part of $\mathscr{G}_T$. Then $\mathscr{G}_T^{\text{ét}} \simeq \mathbb{Q}_p/\mathbb{Z}_p$. We have an exact sequence of $\mathbb{F}_p[I]$-modules

$$0 \to \mathscr{G}_T^\circ(1)(\bar{\xi}) \to \mathscr{G}_T(1)(\bar{\xi}) \to \mathscr{G}_T^{\text{ét}}(1)(\bar{\xi}) \to 0,$$

which determines a cohomology class $\overline{C}_T \in H^1(I, \mathscr{G}_T^\circ(1)(\bar{\xi}))$. We notice that $\mathscr{G}_T(1)(\bar{\xi})$ is isomorphic to $\mathscr{G}_{\widetilde{R'},\sigma}(1)(\overline{x})$ as an abelian group, and the action of I on $\mathscr{G}_T(1)(\bar{\xi})$ is induced by the action of $\pi_1(\widetilde{U}'_\sigma, \overline{x})$ on $\mathscr{G}_{\widetilde{R'},\sigma}(1)(\overline{x})$. Therefore, $\overline{C}_T$ is the image of $\overline{C}_\sigma$ by the functorial map

$$H^1\big(\pi_1(\widetilde{U}'_\sigma, \overline{x}), \mathscr{G}^\circ_{\widetilde{R'},\sigma}(1)(\overline{x})\big) \to H^1\big(I, \mathscr{G}_T^\circ(1)(\bar{\xi})\big).$$

To verify that $\overline{C}_\sigma \neq 0$, it suffices to check that $\overline{C}_T \neq 0$. We consider the polynomial $P(X) = X^{p^n} + f^*(\sigma(t_n))X^{p^{n-1}} + \pi X \in A[X]$. According to 5.12, it suffices to find a $\alpha \in \overline{K}_0 \subset A$ such that $P(\alpha)$ is a uniformizer of A. But by the choice of σ, we have $\sigma(t_n) \in \overline{K}_0$ and $\sigma(t_n) \neq 0$; so $f^*(\sigma(t_n)) \neq 0$ lies in $\overline{K}_0$. Let α be a $p^{n-1}(p-1)$-th root of $-f^*(\sigma(t_n))$ in $\overline{K}_0$. Then we have $\alpha \in \overline{K}_0^\times$, and $P(\alpha) = \alpha\pi$ is a uniformizer of A. This completes the proof of 7.5.

8. End of the Proof of Theorem 1.3

In this section, k denotes an algebraically closed field of characteristic $p > 0$.

8.1. First, we recall some preliminaries on Newton stratification due to F. Oort. Let G be an arbitrary BT-group over k, $\mathbf{S}$ be the local moduli of G in characteristic p, and $\mathbf{G}$ be the universal deformation of G over $\mathbf{S}$ (3.8). Put $d = \dim(G)$ and $c = \dim(G^\vee)$. We denote by $\mathcal{N}(G)$ the Newton polygon of G which has endpoints $(0, 0)$ and $(c + d, d)$. Here we use the normalization of Newton polygons such that slope 0 corresponds to étale BT- groups and slope 1 corresponds to groups of multiplicative type.
Let $\mathcal{NP}(c + d, d)$ be the set of Newton polygons with endpoints $(0, 0)$ and $(c + d, d)$ and slopes in $(0, 1)$. For $\alpha, \beta \in \mathcal{NP}(c + d, d)$, we say that $\alpha \preceq \beta$ if no point of α lies below β; then "$\preceq$" is a partial order on $\mathcal{NP}(c + d, d)$. For each $\beta \in \mathcal{NP}(c + d, d)$, we denote by V_β the subset of $\mathbf{S}$ consisting of points x with $\mathcal{N}(\mathbf{G}_x) \preceq \beta$, and by V_β° the subset of $\mathbf{S}$ consisting of points x with $\mathcal{N}(\mathbf{G}_x) = \beta$. By Grothendieck-Katz's specialization theorem of Newton polygons, V_β is closed in $\mathbf{S}$, and V_β° is open (maybe empty) in V_β. We put

$\Diamond(\beta) =$

$\{(x, y) \in \mathbb{Z}\times\mathbb{Z} \mid 0 \leq y < d, y < x < c+d, (x, y) \text{lies on or above the polygon } \beta\}$,

and $\dim(\beta) = \#(\Diamond(\beta))$.

Theorem 8.2 ([Oo2] Theorem 2.11). *Under the above assumptions, for each $\beta \in \mathcal{NP}(c + d, d)$, the subset V_β° is non-empty if and only if $\mathcal{N}(G) \preceq \beta$. In that case, V_β is the closure of V_β° and all irreducible components of V_β have dimension* $\dim(\beta)$*.*

8.3. Let G be a connected and HW-cyclic BT-group over k of dimension $d = \dim(G) \geq 2$. Let $\beta \in \mathcal{NP}(c + d, d)$ be the Newton polygon given by the following slope sequence:

$$\beta = (\underbrace{1/(c+1), \cdots, 1/(c+1)}_{c+1}, \underbrace{1, \cdots, 1}_{d-1}).$$

We have $\mathcal{N}(G) \preceq \beta$ since G is supposed to be connected. By Oort's Theorem 8.2, V_β is a equal dimensional closed subset of the local moduli $\mathbf{S}$ of dimension $c(d-1)$. We endow V_β with the structure of a reduced closed subscheme of $\mathbf{S}$.

Lemma 8.4. *Under the above assumptions, let R be the ring of* $\mathbf{S}$*, and*

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_1 \\ 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -a_c \end{pmatrix} \in \mathrm{M}_{c\times c}(R)$$

be a matrix of the Hasse-Witt map φ_G. Then the closed reduced subscheme V_β of $\mathbf{S}$ *is defined by the prime ideal $(a_1, \cdots, a_c)$. In particular, V_β is irreducible.*

Proof. Note first that $\{a_1, \cdots, a_c\}$ is a subset of a system of regular parameters of R by 4.11(i). Let I be the ideal of R defining V_β. Let x be an arbitrary point of V_β, we denote by $\mathfrak{p}_x$ the prime ideal of R corresponding to x. Since the Newton polygon of the fibre $\mathbf{G}_x$ lies above β, $\mathbf{G}_x$ is connected. By Lemma 4.4, we have $a_i \in \mathfrak{p}_x$ for $1 \leq i \leq c$. Since V_β is reduced, we have $a_i \in I$. Let $\mathfrak{P} = (a_1, \cdots, a_c)$, and $V(\mathfrak{P})$ the closed subscheme of $\mathbf{S}$ defined by $\mathfrak{P}$. Then $V(\mathfrak{P})$ is an integral scheme of dimension $c(d-1)$ and $V_\beta \subset V(\mathfrak{P})$. Since Theorem 8.2 implies that $\dim V_\beta = c(d-1)$, we have necessarily $V_\beta = V(\mathfrak{P})$. $\square$

We keep the assumptions above. Let $(t_{i,j})_{1\leq i\leq c, 1\leq j\leq d}$ be a regular system of parameters of R such that $t_{i,d} = a_i$ for all $1 \leq i \leq c$. Let x be the generic point of the Newton strata V_β, $k' = \kappa(x)$, and $R' = \widehat{\mathscr{O}}_{\mathbf{S},x}$. Since R is noetherian and integral, the canonical ring homomorphism $R \to \mathscr{O}_{\mathbf{S},x} \to R'$ is injective. The image in R' of an element $a \in R$ will be denoted also by a. By choosing a k-section $k' \to R'$ of the canonical projection $R' \to k'$, we get a (non-canonical) isomorphism of k-algebras $R' \simeq k'[[t_{1,d}, \cdots, t_{c,d}]]$. Let k'' be an algebraic closure of k', and $R'' = k''[[t_{1,d}, \cdots, t_{c,d}]]$. Then we have a natural injective homomorphism of k-algebras $R' \to R''$ mapping $t_{i,d}$ to $t_{i,d}$ for $1 \leq i \leq c$.
Let $S'' = \mathrm{Spec}(R'')$, $\overline{x}$ be its closed point. By the construction of S'', we have a morphism of k-schemes

$$f : S'' \to \mathbf{S} \tag{8.4.1}$$

sending $\overline{x}$ to x. We put $\mathscr{G} = \mathbf{G} \times_{\mathbf{S}} S''$. By the choice of the Newton polygon β, the closed fibre $\mathscr{G}_{\overline{x}}$ has a BT-subgroup $\mathscr{H}_{\overline{x}}$ of multiplicative type of height $d-1$. Since S'' is henselian, $\mathscr{H}_{\overline{x}}$ lifts uniquely to a BT-subgroup $\mathscr{H}$ of $\mathscr{G}$. We put $\mathscr{G}'' = \mathscr{G}/\mathscr{H}$. It is a connected BT-group over S'' of dimension 1 and height $c+1$.

Lemma 8.5. *Under the above assumptions, $\mathscr{G}''$ is the universal deformation in equal characteristic of its special fiber.*

This lemma is a particular case of [Lau, Lemma 3.1]. Here, we use 4.11(ii) to give a simpler proof.

Proof. We have an exact sequence of BT-groups over S''

$$0 \to \mathscr{H} \to \mathscr{G} \to \mathscr{G}'' \to 0,$$

which induces an exact sequence of Lie algebras $0 \to \mathrm{Lie}(\mathscr{G}''^\vee) \to \mathrm{Lie}(\mathscr{G}^\vee) \to \mathrm{Lie}(\mathscr{H}^\vee) \to 0$ compatible with Hasse-Witt maps. Since $\mathscr{H}$ is of multiplicative type, we get $\mathrm{Lie}(\mathscr{H}^\vee) = 0$ and an isomorphism of Lie algebras $\mathrm{Lie}(\mathscr{G}''^\vee) \simeq \mathrm{Lie}(\mathscr{G}^\vee)$. By the choice of the regular system $(t_{i,j})_{1\leq i\leq c, 1\leq j\leq d}$, there is a basis $(v_1, \cdots, v_c)$ of $\mathrm{Lie}(\mathscr{G}''^\vee)$ over $\mathscr{O}_{S''}$ such that $\varphi_{\mathscr{G}''}$ is given by the matrix

$$\mathfrak{h} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -t_{1,d} \\ 1 & 0 & \cdots & 0 & -t_{2,d} \\ 0 & 1 & \cdots & 0 & -t_{3,d} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -t_{c,d} \end{pmatrix}.$$

Now the lemma results from Proposition 4.11(ii). □

8.6. Proof of Theorem 1.3. The one-dimensional case is treated in 7.3. If $\dim(G) \geq 2$, we apply the preceding discussion to obtain the morphism $f\colon S'' \to \mathbf{S}$ and the BT-groups $\mathscr{G} = \mathbf{G} \times_{\mathbf{S}} S''$ and $\mathscr{G}''$, which is the quotient of $\mathscr{G}$ by the maximal subgroup of $\mathscr{G}$ of multiplicative type. Let U'' be the common ordinary locus of $\mathscr{G}$ and $\mathscr{G}''$ over S'', and $\overline{\xi}$ be a geometric point of U''. Then f maps U'' into the ordinary locus $\mathbf{U}$ of $\mathbf{G}$. We denote by

$$\rho_{\mathscr{G}} : \pi_1(U'', \overline{\xi}) \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\mathscr{G}, \overline{\xi}))$$

the monodromy representation associated to $\mathscr{G}$, and the same notation for $\rho_{\mathscr{G}''}$. By the functoriality of monodromy, we have $\mathrm{Im}(\rho_{\mathscr{G}}) \subset \mathrm{Im}(\rho_{\mathbf{G}})$. On the other hand, the canonical map $\mathscr{G} \to \mathscr{G}''$ induces an isomorphism of Tate modules $\mathrm{T}_p(\mathscr{G}, \overline{\eta}) \xrightarrow{\sim} \mathrm{T}_p(\mathscr{G}'', \overline{\eta})$ compatible with the action of $\pi_1(U'', \overline{\eta})$. Therefore, the group $\mathrm{Im}(\rho_{\mathscr{G}})$ is identified with $\mathrm{Im}(\rho_{\mathscr{G}''})$. Since $\mathscr{G}''$ is one-dimensional, we conclude the proof by Lemma 8.5 and Theorem 7.3.

References

[AN] J. Achter and P. Norman, Local monodromy of p-divisible groups, to appear in *Transactions of A.M.S.*, (2006).

[BBM] P. Berthelot, L. Breen and W. Messing, *Théorie de Dieudonné Cristalline II*, Lect. notes in Math. 930, Springer-Verlag, (1982).

[Bou] N. Bourbaki, *Algèbre Commutative*, Masson, Paris (1985).

[Ch1] L. Chai, Local monodromy for deformations of one dimensional formal groups, *J. reine angew. Math.* 524, (2000), 227-238.

[Ch2] L. Chai, Methods for p-adic monodromy, to appear in *Jussieu J. Math.*, (2006).

[CO] L. Chai and F. Oort, Monodromy and irreducibility of leaves, available at the webpage of F. Oort, (2008).

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

[Dem] M. Demazure, *Lectures on p-Divisible Groups*, Lect. notes in Math. 302, Springer-Verlag, (1972).

[DG] M. Demazure and A. Grothendieck, *Schéma en Groupes* I (SGA 3_{I}) , Lect. notes in Math. 151, Springer-Verlag, (1970).

[Eke] 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.

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

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

[EGA] A. Grothendieck, Éléments de Géométrie algébrique IV, Étude locale des schémas et des morphismes de schémas, *Publ. Math. Inst. Hautes Étud. Sci.* 20, 24, 28, 32 (1964-1967).

[Gr] A. Grothendieck, *Groupes de Barsotti-Tate et Cristaux de Dieudonné*, les Presses de l'Université de Montréal, (1974).

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

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

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

[deJ] A. J. de Jong, Crystalline Dieudonné module theory via formal and rigide geometry, *Publ. Math. Inst. Hautes Étud. Sci.* 82 (1995), 5-96.

[Ka1] N. Katz, Algebraic solutions of differential equations (p-curvature and the Hodge filtration), *Inven. Math.* 18 (1972), 1-118.

[Ka2] 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).

[Lau] E. Lau, Tate modules and universal p-divisible groups, arXiv:0803.1390v1, (2008).

[Oo1] F. Oort, Newton polygons and formal groups: conjectures by Manin and Grothendieck, *Ann. of Math.* 152 (2000), 183-206.

[Oo2] F. Oort, Newton polygon strata in the moduli space of abelian varieties, in *Moduli space of Abelian Varieties* (Progress in Mathematics 195), Birkhäuser-Verlag, (2001), 417-440.

[Se1] J. P. Serre, *Corps Locaux*, Hermann, Paris, (1968).

[Se2] J. P. Serre, *Abelian ℓ-adic representations and elliptic curves*, A K Peters, Wellesley, MA, (1998). Originally published in 1968 by W. A. Benjamin.

[Se3] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inven. Math.* 15 (1972), 259-331.

[Str] M. Strauch, Galois actions on torsion points of universal one-dimensional formal modules, arXiv: 0709.3542, (2007).

[Ti1] Y. Tian, Thesis at University Paris 13, defensed in November 2007.

[Ti2] Y. Tian, p-adic monodromy of the universal deformation of an elementary Barsotti-Tate group, arXiv: 0708.2022, (2007).

Yichao Tian
Department of Mathematics
Princeton University
Princeton
New Jersey
08544
USA
yichaot@princeton.edu