RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

ELENA MANTOVAN

Additive extensions of a Barsotti-Tate group

Rendiconti del Seminario Matematico della Università di Padova, tome 99 (1998), p. 161-185

<http://www.numdam.org/item?id=RSMUP_1998__99__161_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 99 (1998)

Additive Extensions of a Barsotti-Tate Group.

ELENA MANTOVAN (*)

ABSTRACT - In this paper we classify up to isomorphism the additive extensions of a Barsotti-Tate group, in positive characteristic p over a perfect field k and in characteristic 0 over $W(k)$ the ring of Witt vectors with coefficients in k. The extensions arise as group functors associated to suitable submodules of the Dieudonné module. In particular we give an explicit description of the universal additive extension in both cases.

1. - Preliminary.

In this section we fix notations (for those we do not mention explicitly we refer to [3]), recall the main definitions and some known results.

1.1. Let p be a prime number and k a perfect field with characteristic p. Put $A = W(k)$ the ring of Witt vectors with coefficients in k, $K = \mathrm{frac}(A)$ its quotient field and denote by D_k the Dieudonné ring of k.

Let G be a Barsotti-Tate group over A and G_k its special fibre. Let R be the affine algebra of G, P the coproduct on R and ε the coidentity; put $R^+ = \ker \varepsilon$ and denote by R_K the ring $R \widehat{\otimes}_A K$, by $R_k = R \widehat{\otimes}_A k$ the affine algebra of G_k and by $\sigma \colon R \to R_k$ the natural projection.

DEFINITION 1. *An element $h \in R_K$ is an integral of G if dh is a one-form of R.*

An integral h of G is normalized if $(\varepsilon \widehat{\otimes}_A 1_K)(h) = 0$.

An integral of the first kind of G is an integral h such that

$$\mathrm{P}h - h \widehat{\otimes} 1 - 1 \widehat{\otimes} h = 0 .$$

(*) Indirizzo dell'A.: Dipartimento di Matematica, Università di Padova, Via Belzoni 7, 35131 Padova.

An integral of the second kind of G is a normalized integral h such that

$$\mathrm{P}h - h\widehat{\otimes}1 - 1\,\widehat{\otimes}h \in R\widehat{\otimes}_A R\,.$$

The integrals of the first and the second kind form two sub-A-modules of the A-module $I(G)$ of the integrals of G, which we denote by $I_1(G)$ and $I_2(G)$, respectively.

Let us define also the following sub-A-module of $I_2(G)$:

$$I_p(G) = \{h \in I_2(G)\,|\,\mathrm{P}h - h\widehat{\otimes}1 - 1\,\widehat{\otimes}h \in pR\widehat{\otimes}_A R\}\,.$$

We now recall the definition of the Dieudonné module of G_k and some results we need later on.

DEFINITION 2. *Let E be a formal group over k, the Dieudonné module of E is $M(E) = \mathrm{Hom}(E, CW_k)$, the group of homomorphisms of k-formal groups from E to CW_k, the covectors formal group over k* (see [3] ch. III, par. 1.2).

If we denote by B the affine algebra of E and by P_B its coproduct, then by the Yoneda's lemma we obtain:

$$M(E) = \{x \in CW_k(B)\,|\,CW_k(\mathrm{P}_B)\,x = x\widehat{\otimes}1 + 1\,\widehat{\otimes}x\}\,;$$

thus $M(E)$ is naturally a sub-D_k-module of $CW_k(B)$.

Moreover we have the following result.

THEOREM 3. *Let E be a formal p-group over k (i.e. a formal group over k such that $E = \varinjlim \ker p^n$) and denote by $M(E)$ its Dieudonné module. Then $E(S) = \mathrm{Hom}_{D_k}(M(E), CW_k(S))$, for each finite ring S over k* ([3] ch. III, Thm. 1).

For each A-module T and each homomorphism of A-modules $f\colon T \to P$, put $T^{(i)} = T \otimes_A A$ and $f^{(i)} = f \otimes_A 1_A$, where the A-structure on A is defined by the i-th power of the Frobenius map.

Let M be the Dieudonné module of G_k and denote by $V\colon M \to M^{(1)}$ its Verschiebung.

THEOREM 4. (1) *There exists an isomorphism of A-modules*

$$w\colon CW_k(R_k) \to I(G)/pR\,,$$

which is defined by $(a_{-n})_{n \in \mathrm{N}} \mapsto [\sum_{n=0}^{+\infty} p^{-n}\widehat{a}_{-n}^{p^n}] \bmod pR$, where $\widehat{a}_{-n} \in R$ is a lifting of a_{-n}, for each $n \in \mathbb{N}$.

(2) *There exists an isomorphism of A-modules*

$$\psi\colon CW_k(R_k)^{(1)} \to I(G)/R\,,$$

which is defined by $(a_{-n})_{n\in\mathbb{N}} \mapsto [\sum_{n=0}^{+\infty} p^{-(n+1)}\widehat{a}_{-n}^{p^{n+1}}] \bmod R$.

(3) *The restrictions* $w_0\colon M \to I_p(G)/pR^+$ *and* $\psi_0\colon M^{(1)} \to I_2(G)/R^+$ *of* w *and* ψ, *respectively, satisfy the relation*

$$c \circ w_0 = \psi_0 \circ V\,,$$

where $c\colon I_p(G)/pR^+ \to I_2(G)/R^+$ *is the homomorphism induced by the inclusion of* $I_p(G)$ *in* $I_2(G)$.

(4) *Let us assume* $p \neq 2$. *Put* $L = I_1(G)$ *and denote by* $j\colon L \to I_p(G)/pR^+$ *the homomorphism induced by the inclusion of* $I_1(G)$ *in* $I_p(G)$, *let* $\varrho\colon L \to M$ *be the composed map* $w_0^{-1} \circ j$; *then*:

– *the homomorphism* $\overline{\varrho}\colon L/pL \to M/FM$, *induced by* ϱ, *is an isomorphism*;

– *for each* p-*adic ring* S *over* A:

$$G(S) = \mathrm{Hom}_A\,(L, S_K) \times_{\mathrm{Hom}_A(L,\, S_K/pS)} \mathrm{Hom}_{D_k}(M, CW_k(S_k))\,,$$

i.e. we can identify each homomorphism of topological rings over A, $\varphi\colon R \to S$, *with the pair* (φ_1, φ_2), *where* $\varphi_1 = I_1(\varphi)$ *and* $\varphi_2 = CW_k(\varphi\,\widehat{\otimes}_A 1_k)_{|M}$, *which satisfies the relation* $t \circ \varphi_1 = w \circ \varphi_2 \circ \varrho$. ([3] ch. II, Prop. 5.5; ch. III, Prop. 6.5; ch. IV, Thm. 1; [4] ch. V, par. 5.5).

We introduce now the Barsotti algebra of G_k.

Let us denote by $[p]_k\colon R_k \to R_k$ the homomorphism of k-bialgebras which corresponds to the multiplication by p on G_k, and put $\mathfrak{R}^0 = \varinjlim (R_k, [p]_k)$, endowed with the direct limit topology.

For each $n \in \mathbb{N}$, let $\tau_n\colon R_k \to \mathfrak{R}^0$ be the natural homomorphism from the n-th element of the direct sistem into the direct limit (let us remark that, since $[p]_k$ is injective, τ_n is an injective homomorphism of topological k-rings, for each $n \in \mathbb{N}$); we define a coproduct over $\mathfrak{R}^0$ by

$$\mathrm{P}_{\mathfrak{R}^0}(x) = (\tau_n \widehat{\otimes} \tau_n) \circ \mathrm{P}_k \circ \tau_n^{-1}(x)\,,$$

for each $x \in \mathfrak{R}^0$ such that $x \in \tau_n(R_k)$.

Definition 5. *The Barsotti algebra of* G_k *is the pair* $(\mathfrak{R}, \tau)$, *where* $\mathfrak{R}$ *is the topological completion of* $\mathfrak{R}^0$ *and* $\tau\colon R_k \hookrightarrow \mathfrak{R}$ *is the injective homomorphism of* k-*bialgebras induced by* τ_0 (see [1] ch. IV, par. 33-37).

We consider now $W(\mathfrak{R})$ the ring of Witt vectors with coefficients in $\mathfrak{R}$ and denote by $\varsigma\colon W(\mathfrak{R}) \to \mathfrak{R}$ the projection on the 0-component; there is a naturally defined bialgebra structure on $W(\mathfrak{R})$ via $W(\mathrm{P}_{\mathfrak{R}})$.

Let $\mathrm{biv}(\mathfrak{R})$ be the module of bivectors with coefficients in $\mathfrak{R}$ (we recall that, for each ring S over k, the D_k-module of bivectors with coefficients in S is $\mathrm{biv}_k(S) = \varprojlim (CW_k(S)^{(-i)}, V^{(-i)})$—see [3] ch. V, par. 1.3); by the definition of bivectors, $W(\mathfrak{R})$ is naturally a sub-A-module of $\mathrm{biv}(\mathfrak{R})$.

THEOREM 6. (1) *There exists an unique injective homomorphism of A-algebras $j\colon R \to W(\mathfrak{R})$ such that $(j \widehat{\otimes} j) \circ \mathrm{P} = W(\mathrm{P}_{\mathfrak{R}}) \circ j$ and $\varsigma \circ j = \tau \circ \sigma$.*

(2) *The homomorphism j can be extended to an embedding of A-modules $j'\colon I(G) \to \mathrm{biv}(\mathfrak{R})$* ([2] Thm. 4.3.2; Prop. 4.3.1, part 3).

1.2. Let A be a pseudocompact commutative ring and G a smooth formal group over A.

Let us denote by $\mathbb{G}_a$ the additive formal group over A, *i. e.* $\mathbb{G}_a(S) = (S, +)$, for each finite ring S over A.

DEFINITION 7. *An additive extension of G is a pair (H, π) consisting of a formal group H over A together with a epimorphism of formal A-groups $\pi\colon H \to G$ such that* $\ker \pi$ *is isomorphic to $\mathbb{G}_a^n$, for some $n \in \mathbb{N}$, which is called the degree of the extension.*

A homomorphism $f\colon (H_1, \pi_1) \to (H_2, \pi_2)$ of additive extensions of G is a homomorphism $f\colon H_1 \to H_2$ of formal A-groups such that $\pi_2 \circ f = \pi_1$.

Since G is a smooth formal group, any additive extension (H, π) of G admits a section $\varrho\colon G \to H$ of π. It is then easy to check that the set of isomorphism classes of additive extensions of degree n can be identified with $\mathrm{Ext}(G, \mathbb{G}_a^n)$, the group of isomorphism classes of extensions of G by $\mathbb{G}_a^n$, with $\mathrm{Ext}^1(G, \mathbb{G}_a^n)$ and with $H^2(G, \mathbb{G}_a^n)_s$, the A-module of classes of symmetric factor sets modulo trivial ones.

DEFINITION 8. *An additive extension (H, π) of G is decomposable if there exists an additive extension (H', π') and an integer $n \geq 1$, such that (H, π) is isomorphic to $(H' \times \mathbb{G}_a^n, \pi' \times 0)$.*

DEFINITION 9. *An additive extension (H, π) of G is universal if, for each $n \in \mathbb{N}$, the homomorphism*

$$\mathrm{Hom}_A(\ker \pi, \mathbb{G}_a^n) \to \mathrm{Ext}(G, \mathbb{G}_a^n),$$

which arises from the exact sequence $0 \to \ker \pi \to H \xrightarrow{\pi} G \to 0$, *is an isomorphism* (see [5] ch. 1, par. 1, probl. B).

It follows from the definition that if $\mathrm{Ext}(G, \mathbb{G}_a)$ is not a free A-module of finite rank there are no universal additive extensions of G; moreover, if we suppose that $\mathrm{Hom}(G, \mathbb{G}_a) = 0$, then if an universal additive extension of G exists, it is unique up to a unique isomorphism.

DEFINITION 10. *A rigidified additive extension of G is a pair consisting of an additive extension (H, π) of G together with a A-linear section l of $t_\pi(A)$: $t_H(A) \to t_G(A)$, the corresponding tangent map over A.*

A homomorphism f: $((H, \pi), l) \to ((H', \pi'), l')$ of rigidified additive extensions of G is a homomorphism $f: (H, \pi) \to (H', \pi')$ of additive extensions of G such that $t_f(A) \circ l = l'$.

Since G is a smooth formal group, its tangent space over A is a free A-module, then any additive extension of G admits a rigidification, which is determinated up to an element of $\mathrm{Hom}_A(t_G(A), t_{\ker \pi}(A))$ (let us remark that $\mathrm{Hom}_A(t_G(A), t_{\ker \pi}(A)) \cong \underline{\omega}_G \otimes_A A^n$, if n is the degree of the extension).

As before the set of isomorphism classes of rigidified additive extensions of degree n can be identified with $\mathrm{Ext}^{\mathrm{rig}}(G, \mathbb{G}_a^n)$, the group of isomorphism classes of rigidified extensions of G by $\mathbb{G}_a^n$.

1.3. Let us maintain the notations of 1.1 and consider a Barsotti-Tate group G over $A = W(k)$.

REMARK 11. *To each set of integrals of the second kind of G, $\{h_1, \dots, h_n\}$, is associated a rigidified additive extension of G, of degree n.*

In fact let $\{h_1, \dots, h_n\} \subset I_2(G)$ and choose $\{U_1, \dots, U_n\}$ a set of indeterminates over R; then, for $i = 1, \dots, n$, $\gamma_i = \mathbb{P}h_i - h_i \widehat{\otimes} 1 - 1 \widehat{\otimes} h_i$ is a symmetric 2-cocycle of G and the homomorphism defined on $R[\widehat{U_1, \dots, U_n}]$ by $x \mapsto \mathbb{P}x$, for all $x \in R$, and $U_i \mapsto U_i \widehat{\otimes} 1 + 1 \widehat{\otimes} U_i + \gamma_i$, for $i = 1, \dots, n$, is a coproduct.

The rigidified additive extension of G associated to $\{h_1, \dots, h_n\}$ is $((H, \pi), l)$, where $H = \mathrm{Spf}_A R[\widehat{U_1, \dots, U_n}]$, π is the homomorphism of A-groups corresponding to the inclusion of A-bialgebras $R \hookrightarrow R[\widehat{U_1, \dots, U_n}]$ and l is the tangent map over A corresponding to the homomorphism of A-algebras $\varrho: R[\widehat{U_1, \dots, U_n}] \to R$ defined by $x \mapsto x$, for all $x \in R$, and $U_i \mapsto 0$, for $i = 1, \dots, n$.

Let us remark that from the construction it follows that

$$I_1(H) = I_1(G) \oplus \langle h_i - U_i \,|\, i = 1, \dots, n \rangle . \qquad \blacksquare$$

In particular, by means of the previous construction, we have defined a natural map, which we denote by $\tilde{\beta}$, from $I_2(G)$ to the set of rigidified additive extensions of G of degree 1.

We conclude this section by recalling the following result, which describes the relations existing among the A-modules of integrals of G and its additive extensions.

THEOREM 12. *Notations as before. Let us consider the following diagram:*

$$\begin{tikzcd}
0 \arrow[r] & \underline{\omega}_G \arrow[r, "\gamma"] & \mathrm{Ext}^{\mathrm{rig}}(G, \mathbb{G}_a) \arrow[r, "\delta"] & \mathrm{Ext}(G, \mathbb{G}_a) \arrow[r] & 0 \\
0 \arrow[r] & I_1(G) \arrow[r, "j"] \arrow[u, "\alpha"'] & I_2(G)/R^+ \arrow[r] \arrow[u, "\beta"'] & \mathrm{Ext}(G, \mathbb{G}_a) \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

where:

- *α is the restriction to $I_1(G)$ of the differential map*;
- *β is the homomorphism induced on the quotients by $\tilde{\beta}$*;
- *δ is the map that forgets the rigidifications*;
- *γ is the identification of $\underline{\omega}_G$ with* $\ker \delta$;
- *j is the homomorphism induced by the inclusion of $I_1(G)$ in $I_2(G)$.*

The diagram is commutative, with exact rows and vertical isomorphisms ([4] ch. 5, Thm. 5.2.1, par. 5.3).

Let us remark that, from the surjectivity of β asserted by the previous theorem, it follows that the map, which associates to each $h \in I_2(G)$ the 2-cocycle $\mathbb{P}h - h \widehat{\otimes} 1 - 1 \widehat{\otimes} h$, is surjective.

2. – Additive extensions of a Barsotti-Tate group over $W(k)$.

In this section we classify up to isomorphism the additive extensions of a Barsotti-Tate group G over $A = W(k)$.

2.1. Let us maintain the notations of 1.1 and assume $p \neq 2$ (the case $p = 2$ must be treated distinctly—see Thm. 4, part 4).

PROPOSITION 13. *To each additive extension (H, π) of G there is a canonically associated sub-A-module N_H of $M^{(1)}$, which contains $V\varrho L$.*

PROOF. Let (H, π) be an additive extension of G, of degree n.

Let us choose a symmetric factor set $\gamma: G \times G \to \mathbb{G}_a^n$, associated to (H, π) via an isomorphism of $\ker \pi$ with $\mathbb{G}_a^n$ and a section of π. Then, if we denote by $\gamma^*: A[\widehat{T_1, \dots, T_n}] \to R \widehat{\otimes}_A R$ the homomorphism of A-algebras corresponding to γ, the set of symmetric 2-cocycles associated to γ is $\{\gamma_1, \dots, \gamma_n\}$, where $\gamma_i = \gamma^*(T_i)$. For $i = 1, \dots, n$ let us choose $h_i \in I_2(G)$ such that $\mathbb{P}h_i - h_i \widehat{\otimes} 1 - 1 \widehat{\otimes} h_i = \gamma_i$ (see Thm. 12) and put

$$N_H = V\varrho L + \langle [h_i] \mid i = 1, \dots, n \rangle,$$

where we denote by $[h_i]$ the image of h_i in $M^{(1)}$ via the map $\psi_0^{-1} \circ pr: I_2(G) \to I_2(G)/R^+ \to M^{(1)}$.

Now it is straightforward to verify that the sub-A-module N_H is independent of the construction. ■

Let us remark that, since $V\varrho L$ is a direct summand of $M^{(1)}$ and $M^{(1)}$ is a free A-module of finite rank, for each sub-A-module N of $M^{(1)}$, containing $V\varrho L$, the quotient $N/V\varrho L$ is a free A-module of finite rank.

Thus the following definition makes sense.

DEFINITION 14. *The rank of an additive extension (H, π) of G is the rank of the free A-module $N_H/V\varrho L$.*

An additive extension of G is non-degenerate if its degree is equal to its rank.

From the construction of the sub-A-module associated to an additive extension of G it follows that the degree of an additive extension (H, π) is always greater than or equal to its rank.

We now prove that each degenerate additive extension is decomposable.

PROPOSITION 15. *Let (H, π) be an additive extension of G, of degre n and rank r. Then (H, π) is isomorphic to $(H_{nd} \times \mathbb{G}_a^{n-r}, \pi_{nd} \times 0)$, where (H_{nd}, π_{nd}) is a non-degenerate additive extension of G, of degree r, which is called the non-degenerate component of (H, π).*

PROOF. Let us choose an isomorphism of $\ker\pi$ with $\mathbb{G}_a^n$ and a section of π, then we obtain an isomorphism (of formal schemes over A) of H with $G\times\mathbb{G}_a^n$, *i. e.* an isomorphism (of topological A-algebras) of $R\widehat{\otimes}A[\overline{T_1, \dots, T_n}]$ with E, the affine algebra of H.

Let $U_1, \dots, U_n$ be the images of $1\widehat{\otimes}T_1, \dots, 1\widehat{\otimes}T_n$ in E; then by construction $\{\gamma_i = \mathbb{P}U_i - U_i\widehat{\otimes}1 - 1\widehat{\otimes}U_i \mid i=1, \dots n\}$ is a set of symmetric 2-cocycles of (H, π) (actually this set is the same we introduced in the previous proposition). If we consider the set of integrals of the second kind of G, $\{h_1, \dots, h_n\}$, such that $\mathbb{P}h_i - h_i\widehat{\otimes}1 - 1\widehat{\otimes}h_i = \gamma_i$ (for $i = {}$ $= 1, \dots n$), then we deduce that $I_1(H) = I_1(G)\oplus\langle h_i - U_i \mid i=1, \dots, n\rangle$.

Thus the associated sub-A-module N_H in $M^{(1)}$ is $N_H = V\varrho L + N'$, where $N' = \langle [h_i] \mid i = 1, \dots, n\rangle$ (we denote by L the A-module $I_1(G)$).

Let us choose now $[f_1], \dots, [f_r]\in N'$ lifting an A-basis of $N_H/V\varrho L$, then $N_H = V\varrho L\oplus\langle [f_i] \mid i=1, \dots, r\rangle$. From this decomposition of N_H it follows that there exist $V_1, \dots, V_n\in E$ and $f_i\in I_2(G)$ lifting $[f_i]$ (for $i = 1, \dots, r$), such that $E = R[\overline{V_1, \dots, V_n}]$ and

$$I_1(H) = I_1(G)\oplus\langle f_i - V_i \mid i = 1, \dots, r\rangle\oplus\langle V_j \mid j = r+1, \dots, n\rangle .$$

In fact let $B\in M(A, r\times n)$ and $D\in M(A, n\times r)$ such that $\underline{[f]} = B\,\underline{[h]}$ and $\underline{[h]} \equiv D\,\underline{[f]}$ modulo $V\varrho L$. Then we deduce that $BD = \mathbf{1}_r$ and that $(\mathbf{1}_n - DB)\,\underline{h} = \underline{g} + \underline{a}$, for some suitable $g_1, \dots, g_n\in L$ and $a_1, \dots, a_n\in R$.

We obtain the previous relations by defining ${}^t(f_1, \dots, f_r) = {}$ $= B\ {}^t(h_1, \dots, h_n)$, ${}^t(V_1, \dots, V_r) = B\ {}^t(U_1, \dots, U_n)$ and choosing $\{V_{r+1}, \dots, V_n\}\subseteq\{Y_1, \dots, Y_n\}$ a maximal linearly indipendent sistem of rank r (we define ${}^t(Y_1, \dots, Y_n) = (\mathbf{1}_n - DB)\ {}^t(U_1, \dots, U_n) - {}$ $- {}^t(a_1, \dots, a_n)$).

From the construction, it follows that the coproduct on E is defined by

$$\mathbb{P}x = \mathbb{P}_R x \qquad \forall x\in R\,,$$

$$\mathbb{P}V_i - V_i\widehat{\otimes}1 - 1\widehat{\otimes}V_i = \mathbb{P}f_i - f_i\widehat{\otimes}1 - 1\widehat{\otimes}f_i \qquad \text{for } i = 1, \dots, r\,,$$

$$\mathbb{P}V_j - V_j\widehat{\otimes}1 - 1\widehat{\otimes}V_j = 0 \qquad \text{for } j = r+1, \dots, n\,.$$

Thus $E\cong R[\overline{V_1, \dots, V_r}]\widehat{\otimes}_A A[\overline{V_{r+1}, \dots, V_n}]$, where $R[\overline{V_1, \dots, V_r}]$ is the affine algebra of a non-degenerate additive extension of G and $A[\overline{V_{r+1}, \dots, V_n}]$ is isomorphic to the affine algebra of $\mathbb{G}_a^n$, and that describes the desired isomorphism. ■

2.2. In view of the previous proposition we can consider only non-degenerate additive extensions of G. Now we proceed by associating to each sub-A-module N of $M^{(1)}$, containing $V\varrho L$, a non-degenerate additive extension of G, which we denote by (H_N, π_N).

Let S be a p-adic ring over A, we denote by S_K its generic fibre, by S_k its special fibre and by $\sigma\colon S \to S_k$ the reduction modulo p. Let $t\colon S_K \to S_K/pS$ and $c\colon S_K/pS \to S_K/S$ be the natural projections of A-modules.

PROPOSITION 16. *Let N be a sub-A-module of $M^{(1)}$, containing $V\varrho L$, and denote by $\tau\colon L \to N$ the factorization of $V \circ \varrho\colon L \to M^{(1)}$ through N.*

Let H_N be the formal A-group defined by

$$H_N(S) = \mathrm{Hom}_A(N, S_K) \times_{\mathrm{Hom}_A(L,\, S_K/pS) \times \mathrm{Hom}_A(N,\, S_K/S)} \mathrm{Hom}_{D_k}(M, CW_k(S_k)),$$

for each p-adic ring S over A, and $\pi_N\colon H_N \to G$ the homomorphism of formal A-groups defined by $(\phi, \varphi) \mapsto (\phi \circ \tau, \varphi)$.

Then (H_N, π_N) is an additive extension of G, of degree $r = \mathrm{rk}_A N/\tau L$.

PROOF. Let S be a p-adic ring over A and consider the following diagram:

$$\begin{tikzcd}
M \arrow[rrr, "\varphi_2"] \arrow[dr, "V"] & & & CW_k(S_k) \arrow[dr, "V"] \arrow[dd, "w"] & \\
& M^{(1)} \arrow[rrr, "\varphi_2^{(1)}"] & & & CW_k(S_k)^{(1)} \arrow[d, "\psi"] \\
L \arrow[uu, "\varrho"] \arrow[r, "\tau"] & N \arrow[u, "j"] \arrow[r, "\varphi_1"] & S_K \arrow[r, "t"] & S_K/pS \arrow[r, "c"] & S_K/S
\end{tikzcd}$$

By definition a point of $H_N(S)$ is a pair of homomorphisms (φ_1, φ_2) such that the diagram commutes, *i.e.*

$$t \circ \varphi_1 \circ \tau = w \circ \varphi_2 \circ \varrho \quad \text{and} \quad c \circ t \circ \varphi_1 = \psi \circ \varphi_2^{(1)} \circ j\,.$$

Let us consider the formal A-group $\mathrm{Hom}_A(N/\tau L, \cdot)$; since $N/\tau L$ is a free A-module of finite rank r, it is isomorphic to $\mathbb{G}_a^r$.

Let us define a homorphism of formal A-groups

$$a_N(S)\colon \mathrm{Hom}_A(N/\tau L, S) \to \mathrm{Hom}_A(N, S_K) \times \mathrm{Hom}_{D_k}(M, CW_k(S_k))$$

by $\phi \mapsto (\phi \circ pr, 0)$, for each p-adic ring S over A, where we denote by pr the canonical projection from N to $N/\tau L$. It is easy to check that actually $\operatorname{Im} \alpha_N \subseteq H_N$, thus we obtain the following sequence of formal A-groups:

$$0 \to \operatorname{Hom}_A(N/\tau L, \cdot) \xrightarrow{\alpha_N} H_N \xrightarrow{\pi_N} G \to 0 .$$

Now we have to check that the sequence is exact. The surjectivity of π_N follows from the surjectivity of $c \circ t$ and the facts that N is a free A-module and τL a direct summand of N; the rest is straightforward. ■

THEOREM 17. *Let N be a sub-A-module of $M^{(1)}$ which contains $V\varrho L$.*

Each non-degenerate additive extension (H, π) of G such that $N_H = N$ is isomorphic to (H_N, π_N).

PROOF. Let (H, π) be a non-degenerate additive extension of G, of degree r, such that $N_H = N$, and let E be the affine algebra of H. With the notations of the previous proofs we have:

- $E = R\widehat{[U_1, \ldots, U_r]}$, where $U_1, \ldots, U_r$ are algebraically independent over R;
- $I_1(H) = I_1(G) \oplus \langle h_i - U_i \mid i = 1, \ldots, r\rangle$;
- $N = \tau L \oplus \langle [h_1], \ldots, [h_r]\rangle$, where $\{[h_1], \ldots, [h_r]\}$ is a set of linearly independent elements over A.

Let us define $\varepsilon\colon I_1(H) \to N$ by $g \mapsto \tau(g)$, for all $g \in I_1(G) = L$, and $h_i - U_i \mapsto [h_i]$, for $i = 1, \ldots, n$; then ε is an isomorphism of A-modules, since (H, π) is non-degenerate.

For each p-adic ring S over A, a point of $H(S)$ is a homomorphism $\varphi\colon E \to S$ of topological rings over A and is determinated by $\varphi_{|R}$, its image in $G(S)$, together with the values $\varphi(U_i)$, for $i = 1, \ldots, r$.

Let us define a homomorphism

$$\zeta(S)\colon H(S) \to \operatorname{Hom}_A(N, S_K) \times \operatorname{Hom}_{D_k}(M, CW_k(S_k)),$$

by $\varphi \mapsto (I_1(\varphi) \circ \varepsilon^{-1}, CW_k(\varphi_{|R} \widehat{\otimes}_A 1_k)_{|M})$, for each p-adic ring S over A. Since $\varphi(U_i) \in S$, for $i = 1, \ldots, r$, we deduce that actually $\operatorname{Im} \zeta \subseteq H_N$; moreover, from Theorem 4 (part (2)), it follows that $\pi_N \circ \zeta = \pi$.

Now let S be a p-adic ring over A and (φ_1, φ_2) be a point of $H_N(S)$. Let us consider the pair $(\varphi_1 \circ \tau, \varphi_2) \in G(S)$, it identifies a homomorphism $f\colon R \to S$ of topological rings over A such that $\varphi_1 \circ \tau = I_1(f)$ and $\varphi_2 = CW_k(f \widehat{\otimes}_A 1_k)_{|M}$ (see Thm. 4, part 4).

Moreover, for $i = 1, \ldots, r$, $I_2(f)(h_i) - \varphi_1([h_i]) \in S$, thus we can define a homomorphism $\varphi\colon E \to S$ by $\varphi_{|R} = f$ and $\varphi(U_i) = I_2(f)(h_i) - \varphi_1([h_i])$, for $i = 1, \ldots, r$.

It is easy to check that the map $\varsigma\colon H_N \to H$, defined by $(\varphi_1, \varphi_2) \mapsto \varphi$, is the inverse homomorphism of ζ. ■

2.3. We conclude this section by studying the affine algebras of the non-degenerate additive extension H_N, for each sub-A-module N of $M^{(1)}$ which contains $V\varrho L$.

Let $j\colon R \to W(\mathfrak{N})$ and $j'\colon I(G) \to \operatorname{biv}(\mathfrak{N})$ be as in Theorem 6, so we can consider R as a sub-A-bialgebra of $W(\mathfrak{N})$ and $I(G)$ as a sub-A-module of $\operatorname{biv}(\mathfrak{N})$.

We recall that there exists a canonical embedding $\mathcal{C}\colon M \to \operatorname{biv}(\mathfrak{N})$, which is defined by mapping each $x \in M$ to the unique element $\mu \in \operatorname{biv}(\mathfrak{N})$ such that $\mu_i = x_i$, for all $i < 0$, and $\operatorname{biv}(\mathrm{P}_{\mathfrak{N}_k})\mu = \mu \hat{\otimes} 1 + 1 \hat{\otimes} \mu$ ([1], ch. IV, Thm. 4.31).

Since the Verschiebung map on $\operatorname{biv}(\mathfrak{N})$ is an isomorphism, we can extend $\mathcal{C}$ to an embedding $\mathcal{C}'\colon M^{(1)} \to \operatorname{biv}(\mathfrak{N})$ by putting $\mathcal{C}' h = V^{-1} \circ \mathcal{C}^{(1)} h$, for each $h \in M^{(1)}$. Thus $M^{(1)}$ can be canonically identified with a sub-A-module of $\operatorname{biv}(\mathfrak{N})$.

Let us remark that, by construction, $\mathcal{C}'[h^*] \equiv h^* \bmod W(\mathfrak{N})$, for each $h^* \in I_2(G)$.

THEOREM 18. *Let N be a sub-A-module of $M^{(1)}$, containing $V\varrho L$, and (H_N, π_N) the associated additive extension of G. There exists one and only one sub-A-bialgebra E_N of $W(\mathfrak{N})$, containing R, such that its module of integrals of the first kind is N.*

The bialgebra E_N represents H_N, i.e. $H_N(S) \cong \operatorname{Hom}_A^{\text{cont.}}(E_N, S)$, for each p-adic ring S over A; thus the affine algebra of H_N can be identified with the completion of E_N for the profinite topology.

PROOF. Let us choose $h_1, \ldots, h_r \in N$ which lift a basis of $N/V\varrho L$; for each $i \in \{1, \ldots, r\}$ we denote by μ_i the additive bivector $\mathcal{C}' h_i$ and by $h_i^* \in I_2(G)$ a lifting of h_i.

For each $i \in \{1, \ldots, r\}$ let us consider the 2-cocycles γ_i, associated to h_i^*, and put $\lambda_i = h_i^* - \mu_i$; thus $\lambda_i \in W(\mathfrak{N})$ and $\gamma_i = W(\mathrm{P}_{\mathfrak{N}_k})\lambda_i - \lambda_i \hat{\otimes} 1 - 1 \hat{\otimes} \lambda_i$, since μ_i is additive.

Moreover, since $W(\mathfrak{N})$ does not contain any additive elements, λ_i is the unique element of $W(\mathfrak{N})$ which satisfies the previous condition.

Let us define $E_N = R[\lambda_1, \ldots, \lambda_r]$. It is straightforward to verify that E_N is a sub-A-bialgebra of $W(\mathfrak{N})$ which depends only on N, not on the choice of $h_1, \ldots, h_r \in N$.

Now let us denote by $\widehat{E}_N$ the completion of E_N for the profinite topology, it follows from the construction that

$$I_1(\widehat{E}_N) = I_1(G) + \langle h_i^* - \lambda_i \,|\, i = 1, \dots, r\rangle = N\,.$$

Then the homomorphism

$$i\colon \mathcal{O}(H_N) = R[\overline{U_1, \dots, U_r}] \rightarrow \widehat{E}_N = R[\overline{\lambda_1, \dots, \lambda_r}],$$

which extends the identity on R by $i(U_i) = \lambda_i$ for $i = 1, \dots, r$, induces an isomorphism on the modules of integrals of the first kind; thus, in view of the Jacobian criterion, we conclude that i is an isomorphism. ∎

3. – The universal additive extension of a Barsotti-Tate group over $W(k)$.

In this section we deduce from the previous results the existence and an explicit description of the universal additive extension of a Barsotti-Tate group G over $A = W(k)$.

3.1. Let us maintain the notations of section 2.

THEOREM 19. *The additive extension $(H_{M^{(1)}}, \pi_{M^{(1)}})$ of G is universal.*

PROOF. By Definition 9 we must prove that, for each $n \in \mathbb{N}$, the map

$$[\mathcal{E}]\colon \mathrm{Hom}_A(\ker \pi_{M^{(1)}}, \mathbb{G}_a^n) \rightarrow \mathrm{Ext}(G, \mathbb{G}_a^n),$$

which associates to each $f \in \mathrm{Hom}_A(\ker \pi_{M^{(1)}}, \mathbb{G}_a^n)$ the isomorphism class of the amalgamated sum $\mathcal{E}(f) = (H_{M^{(1)}} \coprod_{\ker \pi_{M^{(1)}}} \mathbb{G}_a^n, \pi_{M^{(1)}} \coprod 0)$ whose structural homomorphisms are the embedding of $\ker \pi_{M^{(1)}}$ in $H_{M^{(1)}}$ and f, is an isomorphism. In view of Theorem 17, to prove the surjectivity it suffices to show that, for each sub-A-module N of $M^{(1)}$ containing $V_Q L$, there exists a homomorphism $\Theta_N\colon \ker \pi_{M^{(1)}} \rightarrow \ker \pi_N$ such that the additive extension (H_N, π_N) is isomorphic to $\mathcal{E}(\Theta_N)$.

Let S be a p-adic ring over A and consider the following commutative diagram:

$$\begin{tikzcd}
M \arrow[rrr, "\theta_2"] \arrow[dr, "V"] & & & CW_k(S_k) \arrow[dr, "V"] \arrow[dd, "w"] & \\
 & M^{(1)} \arrow[rrr, "\theta_2^{(1)}"] \arrow[dr, "\theta_1"] & & & CW_k(S_k)^{(1)} \arrow[d, "\psi"] \\
L \arrow[uu, "\varrho"] \arrow[r, "\tau"'] & N \arrow[u, "j"'] & S_K \arrow[r, "t"] & S_K/pS \arrow[r, "c"] & S_K/S
\end{tikzcd}$$

where $(\theta_1, \theta_2) \in H_{M^{(1)}}(S)$.

We define the homomorphism of formal A-groups

$$\Theta_N\colon \ker \pi_{M^{(1)}} = \mathrm{Hom}_A(M^{(1)}/V\varrho L, \cdot) \to \ker \pi_N = \mathrm{Hom}_A(N/V\varrho L, \cdot)$$

by $\phi' \mapsto \phi' \circ \bar{j}$, where $\bar{j}$ is the inclusion of $N/V\varrho L$ in $M^{(1)}/V\varrho L$.

Then the desired isomorphism of $\mathcal{E}(\Theta_N)$ with (H_N, π_N) is the map induced on the amalgamated sum by the homomorphism from $H_{M^{(1)}} \oplus \oplus \mathrm{Hom}_A(N/V\varrho L, \cdot)$ to H_N which maps $((\theta_1, \theta_2), \phi)$ to $(\theta_1 \circ j + \phi \circ pr, \theta_2)$ (we denote by j the inclusion of N in $M^{(1)}$ and by $pr\colon N \to N/V\varrho L$ the projection onto the quotient).

Finally from the theorem of elementary divisors, since $[\mathcal{E}]$ is a surjective homomorphism between free A-modules of the same rank, it follows that $[\mathcal{E}]$ is an isomorphism. ■

Actually it is possible to give a more transparent description of the universal additive extension of G, namely that stated without proof by Fontaine in [3] (ch. V, par. 3.7). This is done in Theorem 23, but we first need to prove some lemmas.

Let us maintain the notations of the previous theorem, moreover put $q = CW(\sigma)\colon CW_A(S) \to CW_k(S_k)$ and define

$$\widehat{w}\colon CW_A(S) \to S_K$$

by $(a_{-n})_{n \in \mathbb{N}} \mapsto [\sum_{n=0}^{+\infty} p^{-n} a_{-n}^{p^n}]$ (see [3] ch. II, prop. 5.1), then $\widehat{w}$ is a homomorphism of A-modules and it is easy to check that $t \circ \widehat{w} = w \circ q$.

Let us remark that, from the definitions of $CW_A(S)$ and $CW_k(S_k)$

([3] ch. IV, par. 1.3), it follows that the two homomorphisms

$$\hat{\zeta} = (\hat{w} \circ V^n)_{n \in \mathbb{N}} \colon CW_A(S) \to \bigoplus_{n=0}^{\infty} S_K^{(n)} \quad \text{and}$$

$$\zeta = (w \circ V^n)_{n \in \mathbb{N}} \colon CW_k(S_k) \to \bigoplus_{n=0}^{\infty} (S_K/pS)^{(n)}$$

are injective. Moreover, if we denote by Π the homomorphism $\bigoplus_{n=0}^{\infty} p^{(n)} \colon \bigoplus_{n=0}^{\infty} S_K^{(n)} \to \bigoplus_{n=0}^{\infty} (S_K/pS)^{(n)}$, they satisfy the condition $\Pi \circ \hat{\zeta} = \zeta \circ q$ and $\ker \Pi \subseteq \mathrm{Im}\ \hat{\zeta}$ (see [1] ch. I, Prop. 1.9, Prop. 1.10).

LEMMA 20. *Let D be a $A[V]$-module, S a p-adic ring over A and S_k the special fibre of S. Then the homomorphisms*

$$\hat{\varepsilon} \colon \mathrm{Hom}_{A[V]}(D, CW_A(S)) \to \mathrm{Hom}_A(D, S_K),$$

defined by $\psi \mapsto \hat{w} \circ \psi$, and

$$\varepsilon \colon \mathrm{Hom}_{A[V]}(D, CW_k(S_k)) \to \mathrm{Hom}_A(D, S_K/pS),$$

defined by $\varphi \mapsto w \circ \varphi$, are injective.

PROOF. Let $\psi \colon D \to CW_A(S)$ be a homomorphism of $A[V]$-modules and assume that $\hat{w} \circ \psi = 0$. Recalling that $\psi \circ V = V \circ \psi$, we deduce that $0 = (\hat{w} \circ \psi) \circ V^n = (\hat{w} \circ V^n) \circ \psi$, for each $n \in \mathbb{N}$; then $\hat{\zeta} \circ \psi = 0$ and so, from the injectivity of $\hat{\zeta}$, it follows that $\psi = 0$.

In the same way one can also prove that ε is injective. ■

LEMMA 21. *Let D be a $A[V]$-module, S a p-adic ring over A and S_k the special fibre of S. Then*

$$\mathrm{Hom}_{A[V]}(D, CW_A(S)) \cong$$

$$\cong \mathrm{Hom}_A(D, S_K) \times_{\mathrm{Hom}_A(D,\, S_K/pS)} \mathrm{Hom}_{A[V]}(D, CW_k(S_k)) .$$

PROOF. Let us consider the following commutative diagram

$$\begin{tikzcd}
D \arrow[dr, "\psi"] \arrow[drr, "\psi_2"] \arrow[ddr, "\psi_1"'] & & \\
& CW_A(S) \arrow[r, "q"] \arrow[d, "\widehat{w}"] & CW_k(S_k) \arrow[d, "w"] \\
& S_K \arrow[r, "t"] & S_K/pS
\end{tikzcd}$$

and define the homomorphism

$$\mu\colon \mathrm{Hom}_{A[V]}(D, CW_A(S)) \to \mathrm{Hom}_A(D, S_K) \times \mathrm{Hom}_{A[V]}(D, CW_k(S_k))\,,$$

by $\psi \mapsto (\widehat{w} \circ \psi, q \circ \psi)$. It is easy to check that actually

$$\mathrm{Im}\,\mu \subseteq \mathrm{Hom}_A(D, S_K) \times_{\mathrm{Hom}_A(D, S_K/pS)} \mathrm{Hom}_{A[V]}(D, CW_k(S_k))\,;$$

moreover, from Lemma 20, it follows that μ is injective.

We prove now that μ is also surjective onto the fibre product.

Let $(\psi_1, \psi_2) \in \mathrm{Hom}_A(D, S_K) \times_{\mathrm{Hom}_A(D, S_K/pS)} \mathrm{Hom}_{A[V]}(D, CW_k(S_k))$ and consider the homomorphism $\widetilde{\Psi} = (\psi_1 \circ V^n)_{n \in \mathbb{N}}\colon D \to \bigoplus_{n=0}^{\infty} S_K^{(n)}$. From $t \circ \psi_1 = w \circ \psi_2$ we deduce that $\Pi(\mathrm{Im}\,\widetilde{\Psi}) \subseteq \mathrm{Im}\,\zeta$ and then $\mathrm{Im}\,\widetilde{\Psi} \subseteq \mathrm{Im}\,\widehat{\zeta}$, since $\ker \Pi \subseteq \mathrm{Im}\,\widehat{\zeta}$.

Put $\Psi = (\widehat{\zeta}_{|\mathrm{Im}\,\widehat{\zeta}})^{-1} \circ \widetilde{\Psi}\colon D \to CW_A(S)$, it follows from the construction that Ψ is a homomorphism of $A[V]$-modules and $\widehat{w} \circ \Psi = \psi_1$, moreover $w \circ q \circ \Psi = t \circ \widehat{w} \circ \Psi = w \circ \psi_2$; then, thanks to Lemma 20, we conclude that $q \circ \Psi = \psi_2$. ■

LEMMA 22. *Let M be the Dieudonné module of G_k. Then the homomorphism of formal k-groups*

$$\Delta\colon \mathrm{Hom}_{A[V]}(M^{(1)}, CW_k(\cdot)) \to \mathrm{Hom}_{D_k}(M, CW_k(\cdot))\,,$$

defined by $\psi \mapsto \psi \circ V$, is surjective.

PROOF. Let S be a finite ring over k and $\psi\colon M^{(1)} \to CW_k(S)$ a homomorphism of $A[V]$-modules. Since $(\psi \circ V) \circ F = F \circ (\psi \circ V)$, $\Delta(S)(\psi)$ is an element of $\mathrm{Hom}_{D_k}(M, CW_k(S))$.

Let us recall that M is a free A-module and its Verschiebung $V\colon M \to M^{(1)}$ is injective; then from the inclusion of $pM^{(1)}$ in VM, by the theorem of elementary divisors, there exist two A-bases η e ξ of M and $M^{(1)}$, respectively, such that the corresponding matrix of V is $\begin{pmatrix} \mathbf{1}_d & 0 \\ 0 & p\mathbf{1}_{h-d} \end{pmatrix}$, where $h = \mathrm{rk}_A M$ and $d = \dim_k M/FM$.

Now let $\varphi \in \mathrm{Hom}_{D_k}(M, CW_k(S))$ and define an A-linear homomorphism $\psi\colon M^{(1)} \to CW_k(S)$ on the A-basis ξ in the following way:

$$\psi(\xi_i) = \varphi(\eta_i) \quad \text{for } i = 1, \dots, d \quad \text{and}$$

$$\psi(\xi_j) \text{ is such that } V\psi(\xi_j) = \varphi(\xi_j) \text{ for } j = d+1, \dots, h$$

(let us recall that the Verschiebung map on $CW_k(S)$ is surjective). Then from our construction, it follows that $\eta_j = F\xi_j$, for $j = d+1, \dots, h$, thus ψ is $A[V]$-linear and $\varphi = \psi \circ V$. ■

Theorem 23. *Let $U(G)$ be the formal A-group defined by*

$$U(G)(S) = \mathrm{Hom}_{A[V]}(M^{(1)}, CW_A(S)),$$

for each p-adic ring S over A, and denote by $\beta\colon U(G) \to G$ the homomorphism of formal A-groups which maps Θ to $(\widehat{w} \circ \Theta \circ V \circ \varrho, q \circ \Theta \circ V)$. Then $(U(G), \beta)$ is the universal additive extension of G.

Proof. Let S be a p-adic ring over A and consider the following commutative diagram, where $\Theta \in \mathrm{Hom}_{A[V]}(M^{(1)}, CW_A(S))$.

$$\begin{tikzcd}
M \arrow[rrr, "\varphi_2"] \arrow[dr, "V"] & & & CW_k(S_k) \arrow[r, "V"] \arrow[dd, "w"] & CW_k(S_k)^{(1)} \arrow[dd, "\psi"] \\
& M^{(1)} \arrow[r, "\Theta"] \arrow[d, equal] & CW_A(S) \arrow[ur, "q"] \arrow[d, "\widehat{w}"] & & \\
L \arrow[uu, "\varrho"] \arrow[r, "\tau"] & M^{(1)} \arrow[r, "\varphi_1"] & S_K \arrow[r, "t"] & S_K/pS \arrow[r, "c"] & S_K/S
\end{tikzcd}$$

Let us remark that, for each $\Theta \in U(G)(S)$, the pair $(\widehat{w} \circ \Theta \circ V \circ \varrho$, $q \circ \Theta \circ V)$ satisfies the condition $t \circ (\widehat{w} \circ \Theta \circ V \circ \varrho) = w \circ (q \circ \Theta \circ V) \circ \varrho$ and the homomorphism $q \circ \Theta \circ V$ is D_k-linear; therefore $\beta(S)(\Theta)$ is actually an element of $G(S)$.

Let us define a homomorphism of formal A-groups:

$$\eta(S)\colon \operatorname{Hom}_{A[V]}(M^{(1)}, CW_A(S)) \to$$

$$\to \operatorname{Hom}_A(M^{(1)}, S_K) \times \operatorname{Hom}_{A[V]}(M, CW_k(S_k)),$$

by $\Theta \mapsto (\widehat{w} \circ \Theta, q \circ \Theta \circ V)$.

Since $q \circ \Theta \circ V$ is a homomorphism of D_k-modules and $(\widehat{w} \circ \Theta, q \circ \Theta \circ V)$ satisfies the two conditions:

$$t \circ (\widehat{w} \circ \Theta) \circ V\varrho = w \circ (q \circ \Theta \circ V) \circ \varrho \quad \text{and} \quad c \circ t \circ (w \circ \Theta) = \psi \circ (q \circ \Theta \circ V)^{(1)},$$

η induces a homomorphism from $U(G)$ to $H_{M^{(1)}}$ (see Prop. 16), which we denote by $\overline{\eta}$. Since it is easy to check that $\overline{\eta}$ satisfies the condition $\pi_{M^{(1)}} \circ \overline{\eta} = \beta$, we limit ourselves to proving that $\overline{\eta}$ is an isomorphism. In view of Lemma 20, it follows from the definition that $\overline{\eta}$ is injective, so we need only prove that it is surjective.

Let $(\varphi_1, \varphi_2) \in H_{M^{(1)}}(S)$ and choose an $A[V]$-linear homomorphism $\theta\colon M^{(1)} \to CW_k(S_k)$ such that $\theta \circ V = \varphi_2$ (see Lemma 22). Then the homomorphism $\phi = t \circ \varphi_1 - w \circ \theta$ is an element of $\operatorname{Hom}_A(M^{(1)}, S_K/pS)$, such that $\phi \circ V \circ \varrho = 0$ and $c \circ \phi = 0$, or equivalently such that $\phi(M^{(1)}) \subseteq S_k$ and $\phi(VM) = 0$ (let us recall that $VM = V\varrho L + pM^{(1)}$). It follows that the map $\tilde{\phi}\colon M^{(1)} \to CW_k(S_k)$, defined by $x \mapsto (\dots 0, \underset{\sim}{\dots}, \underset{\sim}{0}, \phi x)$, is a homomorphism of $A[V]$-modules, in particular $V \circ \tilde{\phi} = \tilde{\phi} \circ V = 0$. Then the pair $(\varphi_1, \theta + \tilde{\phi})$, is an element of $\operatorname{Hom}_A(M^{(1)}, S_K) \times {\times_{\operatorname{Hom}_A(M^{(1)}, S_K/pS)}} \operatorname{Hom}_{A[V]}(M^{(1)}, CW_k(S_k))$ and so, thanks to Lemma 21, there exists a homomorphism of $A[V]$-modules $\Theta\colon M^{(1)} \to CW_A(S)$ such that $w \circ \Theta = \varphi_1$ and $q \circ \Theta = \theta + \tilde{\phi}$, which is the same as $w \circ \Theta = \varphi_1$ and $q \circ \Theta \circ V = \varphi_2$; so that $\eta(\Theta) = (\varphi_1, \varphi_2)$. ■

Let us remark that from the previous theorem it follows that the universal additive extension of a Barsotti-Tate group G over A depends only on its special fibre G_k.

3.2. From the knowledge of the universal additive extension of G we can deduce the following result which completes what is asserted in Proposition 15.

PROPOSITION 24. *An additive extension of G is decomposable if and only if it is degenerate.*

PROOF. In view of Proposition 15 and Theorem 17 we need just to prove that $(H_N; \pi_N)$ is non-decomposable, for each sub-A-module N of $M^{(1)}$ which contains $V\varrho L$.

We recall that, in the proof of Theorem 19, we have shown that $H_N \cong \cong U(G) \coprod_{\ker\beta} \ker\pi_N$, where the structural homomorphisms of the amalgamated sum are the embedding of $\ker\beta$ in $U(G)$ and $\Theta_N: \ker\beta \to \to \ker\pi_N$ (we denote by $(U(G), \beta)$ the universal additive extension of G).

Let us assume that (H_N, π_N) is decomposable, for any N as before; then there exists an isomorphism $\Psi: (H_N, \pi_N) \to (H \times \mathbb{G}_a, \pi \times 0)$, for a suitable additive extension (H, π) of G. By the universal property of $(U(G), \beta)$, there exists a map $\varepsilon: \ker\beta \to \ker\pi$ such that $\Psi_{|\ker\pi_N} \circ \Theta_N = = \iota \circ \varepsilon$ ($\iota: \ker\pi \to \mathbb{G}_a \times \ker\pi$ denotes the natural embedding); then the map $\Psi_{|\ker\pi_N}: \ker\pi_N \to \mathbb{G}_a \times \ker\pi$ induces a homomorphism $\delta: \operatorname{coker}\Theta_N \to \mathbb{G}_a$ on the quotients. Since $\Psi_{|\ker\pi_N}$ is surjective so is δ, but this is impossible because $\operatorname{coker}\Theta_N$ is a p-torsion group (this fact follows from the theorem of elementary divisors); thus our assumption is false. ■

4. – Additive extensions of a Barsotti-Tate group over k.

In this section we classify up to isomorphism the additive extensions of a Barsotti-Tate group G over k, a perfect field with characteristic p. In particular we consider the special fibres of the additive extensions of any lifting of G over $W(k)$, noting that the universal additive extension of G is the special fibre of the universal additive extension of its liftings.

4.1. Let G_L be the lifting of G over $A = W(k)$ associated to (L, ϱ) (see Thm. 4, part (4)).

The following proposition describes the relation between the additive extensions of G_L and the additive extensions of G.

PROPOSITION 25. *The map that to each additive extension (H, π) of G_L associates its special fibre (H_k, π_k) induces an epimorphism*

$$\gamma: \operatorname{Ext}(G_L, \mathbb{G}_{a,A}) \to \operatorname{Ext}(G, \mathbb{G}_{a,k}).$$

PROOF. Via the isomorphisms $\operatorname{Ext}(G_L, \mathbb{G}_{a,A}) \cong M^{(1)}/V\varrho L$ (see Thm. 4, part (3) and Thm. 12) and $\operatorname{Ext}(G, \mathbb{G}_{a,k}) \cong t_{G^\vee}(k) \cong M^{(1)}/VM$ ([6] ch. IV, par. 1), γ corresponds to the natural projection $g: M^{(1)}/V\varrho L \to \to M^{(1)}/VM$. Since $VM = V\varrho L + pM^{(1)}$, g is the map of the reduction modulo p, thus γ is surjective. ■

The previous proposition tells us that each additive extension of G is isomorphic to the special fibre of an additive extension of G_L.

Now we give an explicit description of the special fibre of the additive extension of G_L associated to a sub-A-modules N of $M^{(1)}$ containing $V\varrho L$, which we denote by $(H_{N,L}, \pi_{N,L})$.

PROPOSITION 26. *Let N be a sub-A-module of $M^{(1)}$ containing $V\varrho L$, and let $(H_{N,L}, \pi_{N,L})$ be the associated additive extension of G_L.*

Then, for each finite ring S over k:

$$(H_{N,L})_k(S) =$$

$$= \mathrm{Hom}_{A[V]}(M^{(1)}, CW_k(S)) \coprod_{\mathrm{Hom}_k(M^{(1)}/VM,\, S)} \mathrm{Hom}_k\left(\frac{N}{V\varrho L + pN}, S\right),$$

and $(\pi_{N,L})_k(S)\colon (H_{N,L})_k(S) \to \mathrm{Hom}_{D_k}(M, CW_k(S)) = G(S)$ maps (ψ, ϕ) to $\psi \circ V$.

In particular the special fibre of the universal additive extension $(U(G_L), \beta)$ of G_L is

$$U(G_L)_k = \mathrm{Hom}_{A[V]}(M^{(1)}, CW_k(S))$$

and $(\beta_L)_k\colon U(G_L)_k \to G$ is defined by $(\psi, \phi) \mapsto \psi \circ V$.

PROOF. In view of Theorem 19 we know that

$$H_{N,L} = H_{M^{(1)},L} \coprod_{\mathrm{Hom}_A(M^{(1)}/V\varrho L,\, \cdot)} \mathrm{Hom}_A(N/V\varrho L, \cdot);$$

then for each finite ring S over k, if by $S_{[A]}$ we denote S with the structure of A-ring induced by the reduction map $\varepsilon\colon A \to k$, we obtain:

$$(H_{N,L})_k(S) = (H_{M^{(1)},L})_k(S) \coprod_{\mathrm{Hom}_A(M^{(1)}/V\varrho L,\, S_{[A]})} \mathrm{Hom}_A(N/V\varrho L, S_{[A]}).$$

It follows from the definitions that $CW_A(S_{[A]}) = CW_k(S)$ as $A[V]$-modules.

Thus in view of Theorem 23

$$(H_{M^{(1)},L})_k(S) = \mathrm{Hom}_{A[V]}(M^{(1)}, CW_A(S_{[A]})) = \mathrm{Hom}_{A[V]}(M^{(1)}, CW_k(S)).$$

Moreover

$$\mathrm{Hom}_A\left(\frac{N}{V\varrho L}, S_{[A]}\right) = \mathrm{Hom}_k\left(\frac{N}{V\varrho L + pN}, S\right)$$

and

$$\mathrm{Hom}_A\left(\frac{M^{(1)}}{V\varrho L}, S_{[A]}\right) = \mathrm{Hom}_k\left(\frac{M^{(1)}}{VM}, S\right), \quad \text{since } VM = V\varrho L + pM^{(1)}.$$

Finally it is straightforward to check the assertion regarding the homomorphism $(\beta_{N,L})_k$. ■

4.2. In view of the results obtained in the previous sections we can now easily prove that the universal additive extension of G is the special fibre of the universal additive extension of any lifting of G over A.

THEOREM 27. *With the previous notations, $(U(G_L)_k, (\beta_L)_k)$ is the universal additive extension of G.*

PROOF. Let (H, π) be an additive extension of G, then there exists an additive extension $(\tilde{H}, \tilde{\pi})$ of G_L such that $(\tilde{H}_k, \tilde{\pi}_k) \cong (H, \pi)$. From the universal property of $(U(G_L), \beta_L)$ it follows that $(\tilde{H}, \tilde{\pi})$ is isomorphic to $(U(G_L) \coprod_{\ker\beta_L} \ker\tilde{\pi}, \beta_L \coprod 0)$, for a suitable and unique homomorphism f: $\ker\beta_L \to \ker\tilde{\pi}$. Then, if we consider the special fibres, we obtain that (H, π) is isomorphic to $(U(G_L)_k \coprod_{\ker(\beta_L)_k} \ker\pi, (\beta_L)_k \coprod 0)$, where the structural homomorphism is f_k which is unique because f is unique. ■

4.3. Let us introduce the following additive extensions of G.

Let N be a sub-A-module of $M^{(1)}$, which contains VM, and denote by $(U(G), \beta)$ the universal additive extension of G.

We define the following formal group over k:

$$F_N = U(G) \coprod_{\ker\beta} \mathrm{Hom}_k\left(\frac{N}{VM}, \cdot\right),$$

where the amalgamated sum is defined by the embedding of $\ker\beta$ in $U(G)$ and the homomorphism

$$\Phi_N \colon \ker\beta = \mathrm{Hom}_k\left(\frac{M^{(1)}}{VM}, \cdot\right) \to \mathrm{Hom}_k\left(\frac{N}{VM}, \cdot\right)$$

which corresponds to the inclusion of N/VM in $M^{(1)}/VM$.

Let $\tau_N \colon F_N \to G$ be the homomorphism of formal k-groups $\beta \coprod_{\ker\beta} 0$.

PROPOSITION 28. *With the previous notations, for each sub-A-*

module N of $M^{(1)}$ containing VM, (F_N, τ_N) is an additive extension of G, of degree $\dim_k N/VM$.

PROOF. It follows from the definition that the sequence of formal k-groups

$$0 \to \mathrm{Hom}_k\left(\frac{N}{VM}, \cdot\right) \to F_N \xrightarrow{\tau_N} G \to 0$$

is exact. We conclude by observing that $\mathrm{Hom}_k(N/VM, \cdot) \cong \mathbb{G}_a^s$, where $s = \dim_k N/VM$. ■

Let us recall the notations of 4.1; let G_L be the lifting of G over A associated to (L, ϱ) and $(H_{N,L}, \pi_{N,L})$ the additive extension of G_L associated to a sub-A-module N of $M^{(1)}$ which contains $V\varrho L$.

THEOREM 29. *For each a sub-A-module N of $M^{(1)}$ containing $V\varrho L$,*

$$(H_{N,L}, \pi_{N,L})_k \cong (F_{N+VM} \times \mathbb{G}_a^{r-s}, \tau_{N+VM} \times 0),$$

where r and s are the degrees of $(H_{N,L}, \pi_{N,L})$ and (F_{N+VM}, τ_{N+VM}), respectively.

PROOF. From the definition of (F_N, τ_N) and the characterization of $(H_{N,L}, \pi_{N,L})_k$ in Proposition 26, it follows that

$$(H_{N,L}, \pi_{N,L})_k \cong$$

$$\cong \left(F_{N+VM} \coprod_{\mathrm{Hom}_k(N+VM/VM,\,\cdot)} \mathrm{Hom}_k\left(\frac{N}{V\varrho L + pN}, \cdot\right), \tau_{N+VM} \coprod 0\right),$$

where the amalgamated sum is defined by the embedding of $\ker \tau_{N+VM} = \mathrm{Hom}_k((N+VM)/VM, \cdot)$ in F_{N+VM} and the homomorphism ϕ_N from $\mathrm{Hom}_k((N+VM)/VM, \cdot)$ to $\mathrm{Hom}_k(N/(V\varrho L + pN), \cdot)$, which corresponds to the map induced on the quotients by the inclusion of N in $N + VM$.

By considering the canonical isomorphism (of k-spaces) of $N/(V\varrho L + pN)$ with $(N \cap VM)/(V\varrho L + pN) \oplus (N + VM)/VM$, we obtain an isomorphism of $\mathrm{Hom}_k(N/(V\varrho L + pN), \cdot)$ with $\mathrm{Hom}_k((N \cap VM)/(V\varrho L + pN), \cdot) \times \mathrm{Hom}_k((N + VM)/VM, \cdot)$ such that ϕ_N corresponds to the natural embedding into the product. Then we deduce that

$$(H_{N,L}, \pi_{N,L})_k \cong \left(F_{N+VM} \times \mathrm{Hom}_k \left(\frac{N \cap VM}{V\varrho L + pN}, \cdot \right), \tau_{N+VM} \times 0 \right),$$

where

$$\dim_k \frac{N \cap VM}{V\varrho L + pN} = \dim_k \frac{N}{V\varrho L + pN} - \dim_k \frac{N + VM}{VM} = r - s . \qquad \blacksquare$$

Finally we can recognize the decomposable additive extensions of G.

PROPOSITION 30. *Let N be a sub-A-module of $M^{(1)}$. If $N \supseteq VM$, then the additive extension (F_N, τ_N) is non-decomposable.*

Let L be the A-module associated to a lifting of G over A; if $N \supseteq V\varrho L$, then the special fibre of $(H_{N,L}, \pi_{N,L})$ is non-decomposable if and only if $N \cap pM^{(1)} = pN$.

PROOF. Let N be a sub-A-module of $M^{(1)}$, containing VM, then

$$(F_N, \tau_N) = (U(G) \textstyle\coprod_{\ker\beta} \mathrm{Hom}_k(N/VM, \cdot), \beta \coprod 0)$$

where the amalgamated sum is defined by the homomorphism

$$\varepsilon_N \colon \ker\beta = \mathrm{Hom}_k(M^{(1)}/VM, \cdot) \rightarrow \ker\tau_N = \mathrm{Hom}_k(N/VM, \cdot)$$

which corresponds to the inclusion of N/VM in $M^{(1)}/VM$.

Let us assume that (F_N, τ_N) is decomposable, then there exists an additive extension (H, π) of G and an isomorphism $\Theta_N \colon (F_N, \tau_N) \rightarrow \rightarrow (\mathbb{G}_a \times H, 0 \times \pi)$.

From the universal property of $(U(G), \beta)$ we know that there exists a homomorphism $\alpha \colon \ker\beta \rightarrow \ker\pi$ such that $\iota \circ \alpha = \theta_N \circ \varepsilon_N$, where we denote by $\theta_N \colon \ker\tau_N \rightarrow \mathbb{G}_a \times \ker\pi$ the restriction of Θ_N on the kernels and by ι the natural inclusion of $\ker\pi$ in $\mathbb{G}_a \times \ker\pi$.

Note that $\theta_N \circ \varepsilon$ is surjective because θ_N and ε_N are, while $\iota \circ \alpha$ is not, which is impossible.

Now let us assume that $N \supseteq V\varrho L$, then

$$(H_{N,L}, \pi_{N,L})_k = (F_{N+VM} \times \mathbb{G}_a^q, \tau_{N+VM} \times 0)$$

where $q = \dim_k(N \cap VM)/(V\varrho L + pN)$ (see Thm. 29). Since (F_{N+VM}, τ_{N+VM}) is non-decomposable, $(H_{N,L}, \pi_{N,L})_k$ is non-decomposable if and only if $(N \cap VM)/(V\varrho L + pN) = 0$.

It is easy to check that the last condition is equivalent to $N \cap pM^{(1)} = = pN$.

Infact, if we assume that $N \cap VM = V\varrho L + pN$, recalling that $pM^{(1)} \subseteq VM$ and $pM^{(1)} \cap V\varrho L = p(V\varrho L)$ (see Thm. 4, part 4), we obtain:

$$pN \subseteq N \cap pM^{(1)} =$$

$$= N \cap VM \cap pM^{(1)} = V\varrho L \cap pM^{(1)} + pN = p(V\varrho L) + pN = pN\,.$$

On the other hand, recalling that $VM = V\varrho L + pM^{(1)}$, from $pN = N \cap \cap\, pM^{(1)}$ we deduce:

$$V\varrho L + pN \subseteq N \cap VM = N \cap (V\varrho L + pM^{(1)}) = V\varrho L + pN\,. \qquad \blacksquare$$

4.4. We conclude by proving that each non-decomposable additive extension of G is represented by a sub-k-bialgebra of the Barsotti algebra $\mathfrak{R}$ of G, which contains R.

THEOREM 31. *Let N be a sub-A-module of $M^{(1)}$, containing VM, and (F_N, τ_N) be the associated additive extension of G.*

Then there exists one and only one sub-k-bialgebra D_N of $\mathfrak{R}$, containing R, such that its module of invariant one-forms can be identified with $N/pM^{(1)}$.

The bialgebra D_N represents F_N, i.e. $F_N(S) \cong \mathrm{Hom}_k^{\mathrm{cont.}}(D_N, S)$, for each finite ring S over k; thus the affine algebra of F_N can be identified with the completion of D_N for the profinite topology.

PROOF. Let N be a sub-A-module of $M^{(1)}$, which contains VM. We organize the proof in 3 steps.

1) *Definition of D_N.*

Let G_L be a lifting of G over A and fix an embedding of its affine algebra R_L in $W(\mathfrak{R})$, as in Theorem 6. In view of Proposition 25, there exists a sub-A-module T of $M^{(1)}$, containing $V\varrho L$, such that $(F_N, \tau_N) = (H_{T,L}, \pi_{T,L})_k$, *i.e.* T satisfies the two conditions: $N = T + VM$ and $pT = T \cap pM^{(1)}$ (see Prop. 30). Moreover, by Theorem 18, we know that there exists a sub-A-algebra E_T of $W(\mathfrak{R})$, which contains R_L, such that its module of invariant one-forms can be identified with T.

Let us denote by $\varsigma\colon W(\mathfrak{R}) \to \mathfrak{R}$ the projection on the 0-component and put $D_N = \varsigma(E_T)$. Then D_N is a sub-k-bialgebra of $\mathfrak{R}$, which contains R, and it is not difficult to check that it depends only on N, not on the choice of T and L.

2) *The module of invariant one-forms of D_N can be identified with $N/pM^{(1)}$.*

Let us choose L and T as before. The map $\varsigma_{|E_T}: E_T \to D_N$ induces a homomorphism $\underline{\omega}(\varsigma_{|E_T}): \underline{\omega}_A(E_T) \to \underline{\omega}_k(D_N)$ and, since $\varsigma_{|E_T}$ is surjective, so is $\underline{\omega}(\varsigma_{|E_T})$. Composing $\underline{\omega}(\varsigma_{|E_T})$ with the canonical isomorphism between T and $\underline{\omega}_A(E_T)$ and reducing to the quotient, we obtain a homomorphism $\eta_T: T/pT \to \underline{\omega}_k(\mathfrak{R})$, whose image is $\underline{\omega}_k(D_N)$. Since $T/pT \cong \cong N/pM^{(1)}$, it suffices to prove that η_T is injective.

We note that we can limit ourselves to considering the case $N = M^{(1)}$ and $T = M^{(1)}$. In fact, for any T, if we denote by $j: T/pT \to M^{(1)}/pM^{(1)}$ the map induced by the inclusion of T in $M^{(1)}$, we obtain that $\eta_T = \eta_{M^{(1)}} \circ j$.

Let us denote by $d: M^{(1)} \to \underline{\omega}_A(W(\mathfrak{R}))$ the composition of the differential map of $E_{M^{(1)}}$ with the inclusion of $\underline{\omega}_A(E_{M^{(1)}})$ in $\underline{\omega}_A(W(\mathfrak{R}))$ and by $t: M^{(1)} \to M^{(1)}/pM^{(1)}$ the reduction modulo p, then it follows from the definition of $\eta_{M^{(1)}}$ that $\eta_{M^{(1)}} \circ t = \underline{\omega}(\varsigma) \circ d$. Thus to prove that $\eta_{M^{(1)}}$ is injective is the same as proving that $\ker(\underline{\omega}(\varsigma) \circ d) = pM^{(1)}$.

Let us choose a set of parameters on R, $\{x_1, \ldots, x_d\}$, and one of its liftings on R_L, $\{X_1, \ldots, X_d\}$, (*i.e.* $R = R^{et}[[x_1, \ldots, x_d]]$, $R_L = = W(R^{et})[[X_1, \ldots, X_d]]$ and $\varsigma(X_i) = x_i$ for $i = 1, \ldots, d$). Let $h = (h_n)_{n \in \mathbb{Z}} \in \in M^{(1)} \subseteq \mathrm{biv}(\mathfrak{R})$; since h is an integral we may write

$$h = \sum_{|\nu| \geq 0} p^{-h(\nu)} a_\nu X^\nu + ph',$$

where $h(\nu) = \min\{v_p(\nu_i) \mid i = 1, \ldots, d\}$, $a_\nu \in W(R^{et})$ for all $\nu \in \mathbb{N}^d$ and h' is an element of $W(\mathfrak{R})$. Thus the image of h in $\underline{\omega}_A(W(\mathfrak{R}))$ is

$$dh = \sum_{i=1}^{d} \sum_{|\nu| \geq 0} p^{-h(\nu)} \nu_i a_\nu X^{\nu - e_i} dX_i + pdh',$$

where the exponents e_i are such that $X^{e_i} = X_i$, and in $\underline{\omega}_k(\mathfrak{R})$

$$\underline{\omega}(\varsigma)(dh) = \sum_{i=1}^{d} \sum_{|\nu| \geq 0} p^{-h(\nu)} \nu_i a_{\nu,0} x^{\nu - e_i} dx_i .$$

Now let us assume that $\underline{\omega}(\varsigma)(dh) = 0$. Then, for each $i \in \{1, \ldots, d\}$ and $\nu \in \mathbb{N}^d$, $p^{-h(\nu)} \nu_i a_{\nu,0} = 0$; if we choose $i_0 \in \{1, \ldots, d\}$ such that $h(\nu) = = v_p(\nu_{i_0})$, from $p^{-h(\nu)} \nu_{i_0} a_{\nu,0} = 0$ we deduce $a_{\nu,0} = 0$, for each $\nu \in \mathbb{N}^d$. This means that $a_\nu \in pW(R^{et})$ and then the element of $I_2(R_L)$ which corresponds to h belongs to $pI_2(R_L)$; thus $h \in pM^{(1)}$.

Since the inclusion of $pM^{(1)}$ in $\ker(\underline{\omega}(\varsigma) \circ d)$ is obvious, we conclude.

3) *D_N represents F_N.*

Let us denote by $\sigma: E_T/pE_T \to D_N$ the homomorphism induced by

$\varsigma_{|E_T}: E_T \to D_N$; what we have proved at step 2 is equivalent to asserting that $\underline{\omega}_k(\sigma)$: $\underline{\omega}_k(E_T/pE_T) \to \underline{\omega}_k(D_N)$ is an isomorphism. Then, by the Jacobian criterion, we deduce that σ is an isomorphism and thus

$$F_N = (H_{T,L})_k \cong \mathrm{Hom}_k^{\mathrm{cont.}}(E_T/pE_T, \cdot) \cong \mathrm{Hom}_k^{\mathrm{cont.}}(D_N, \cdot).$$

REFERENCES

[1] I. Barsotti, *Metodi analitici per varietà abeliane in caratteristica p*, Ann. Sc. Norm. Sup. Pisa, **18** (1964), **19** (1965).

[2] M. Candilera - V. Cristante, *Witt Realization of p-adic Barsotti-Tate groups, Proceedings of Barsotti Memorial Symposium*, Academic Press (1994).

[3] J. M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Asterisque, **47-48** (1977).

[4] N. M. Katz, *Crystalline cohomology, Dieudonné modules, and Jacobi sums*, Collection: Automorphic forms, representation theory and arithmetic, Tata Inst. Fundamental Res., Bombay (1981).

[5] B. Mazur - W. Messing, *Universal Extention and One Dimensional Crystalline Cohomology*, Lecture Notes in Mathematics, n. 370, Springer, Berlin (1974).

[6] W. Messing, *The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes*, Lecture Notes in Mathematics, n. 264, Springer, Berlin (1972).

Manoscritto pervenuto in redazione il 12 luglio 1996.