NORM MAPS FOR FORMAL GROUPS IV

Michiel Hazewinkel

1. INTRODUCTION

Let K be discretely valued complete field of characteristic zero with algebraically closed residue field k of characteristic $p > 0$. Let A be the ring of integers of K, and let F be a one-dimensional commutative formal group over A. Let K_∞/K be a $\mathbb{Z}_p$-extension (also called Γ-extension); *i.e.*, K_∞/K is Galois and $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, the p-adic integers. Let K_n be the invariant field of $p^n \mathrm{Gal}(K_\infty/K)$. There are natural norm maps $F - \mathrm{Norm}_{n/o}: F(K_n) \to F(K)$. Let v be the normalized exponential valuation on K; *i.e.*, $v(\pi) = 1$, where π is a uniformizing element of K. Let $F^s(K), s \in \mathbb{R}, s \geq 1$, denote the filtration subgroup of F (K) consisting of all elements x of A such that $v(x) \geq s$. Let h be the height of the formal group F and let e_K be the (absolute) ramification index of K; *i.e.*, $v(p) = e_K$. In [3] we proved:

THEOREM A. *There exist constants* c_1 *and* c_2 *such that for all* $n \in \mathbb{N}$, $F^{\beta_n}(K) \subset \mathrm{Im}(F - \mathrm{Norm}_{n/o}) \subset F^{\alpha_n}(K)$, *where*

$$\alpha_n = h^{-1}(h-1)ne_K - c_1, \; \beta_n = h^{-1}(h-1)ne_K + c_2.$$

The proof in [3] that there exists a constant c_1 such that the second inclusion holds is relatively easy, but the proof in [3] that there is a c_2 such that the first inclusion holds is very long and laborious. It is the purpose of the present note to give a much shorter and more conceptual proof of this part of the theorem by using some results on the logarithm of F. This proof is similar in spirit to the proof sketched in Section 12 of [3] for the main theorem of [2].

For more complete definitions of the notions mentioned above, see [2] and [3].

Here is some motivation for studying the images of norm maps for formal groups. Let $L - K - \mathbb{Q}_p$ be a tower of algebraic extensions of $\mathbb{Q}_p$ and let L/K be abelian galois. Then by local class field theory, $\mathrm{Gal}(L/K) \simeq K^*/N_{L/K}(L^*)$. The most interesting part (and the hardest to deal with) of this isomorphism is $\mathrm{Gal}(L/K)_1 = U^1(K)/N_{L/K}U^1(L)$, where $U^1(K)$ is the group of "Eins-Einheiten" of K; *i.e.*, $U^1(K) = 1 + \pi A$, and $\mathrm{Gal}(L/K)_1$ is the ramification subgroup of Gal (L/K) which corresponds to the wildly and totally ramified part of L/K of degree a power of p.

Now consider the multiplicative formal group $\hat{\mathbb{G}}_m(X,Y) = X + Y + XY$. Then $\hat{\mathbb{G}}_m(K) = U^1(K)$, $\hat{\mathbb{G}}_m(L) = U^1(L)$ and we see that the study of the norm maps $\hat{\mathbb{G}}_m - \mathrm{Norm}_{L/K}$ is what a not inconsiderable part of local class field theory is about.

Received June 4, 1976. Revisions received December 8, 1976 and July 18, 1977.

Michigan Math. J. 25 (1978).

The basic goal is now to look for a class field type theory for other algebraic groups than just $\mathbb{G}_m$, the multiplicative group. In [6, Section 4], such a theory is developed for an abelian variety A with nondegenerate reduction and invertible Hasse matrix, and the result obtained plays an important role in the remainder of [4]. The development of the theory goes via the formal group $\hat{A}$ obtained by completing A along the identity, and relies heavily (as does local class field theory) on the fact that $\hat{A}(L) \xrightarrow{\text{Norm}} \hat{A}(K)$ is surjective if L/K is a local field extension of a local field K with algebraically closed residue field. One consequence of Theorem A is that this fails if $h(\hat{E}) \geq 2$; that is, it fails in the case of supersingular elliptic curves (*cf.* also [6], Section 1, d1).

In local class field theory, in the theory developed in [6], and also in [10], the $\mathbb{Z}_p$-extensions play an especially distinguished role. This may be seen as motivation for paying particular attention to $\mathbb{Z}_p$-extensions.

Of course, from the point of a class field theory associated to an algebraic group in general, a weak consequence of Theorem A is an analogue of that well known theorem of class field theory which says that the subgroup of universal norms is trivial. We have: if height $(F(X, Y)) \geq 2$, then $\bigcap_{L/K} \text{F-Norm}(F(L)) = \{0\}$.

Thus the theorem we are going to prove in this paper is the more difficult half of Theorem A;

THEOREM B. *Let* K_∞/K *be a* $\mathbb{Z}_p$*-extension of a mixed characteristic local field* K *with algebraically closed residue field of characteristic* p. *Let* F *be a one-dimensional commutative formal group over* A *of height* h *over* A. *Then there exists a constant* c, *depending on* K_∞/K *and* F, *such that*

$$F^{\beta_n}(K) \subset \operatorname{Im}(\text{F-Norm}_{n/o}) \qquad \textit{for all } n,$$

where $\beta_n = h^{-1}(h-1)ne_K + c$. (*If* $h = \infty$, $h^{-1}(h-1)$ *is taken to be equal to* 1.)

All formal groups in this paper will be one-dimensional and commutative. The notation introduced above will remain in force throughout this paper. In addition we use A_n for the ring of integers of K_n; π_n for a uniformizing element of K_n; v_n for the normalized exponential valuation of K_n (*i.e.*, $v_n(\pi_n) = 1$); and $\text{Tr}_{n/o}$ is the trace map from K_n to K. The natural numbers are denoted by $\mathbb{N}$.

2. RECAPITULATION OF SOME RESULTS AND DEFINITIONS

2.1. Let L/K be a cyclic extension of degree p. There is a unique integer $m(L/K) \geq 1$ such that for all n, $\text{Tr}_{L/K}(\pi_L^n A_L) = \pi_K^r A_K$, where

$$r = [p^{-1}((m(L/K)+1)(p-1)+n)]$$

and [y] denotes the integral part of y. We shall use m_n to denote the number $m(K_n/K_{n-1})$.

2.2. LEMMA. (Tate [7]). *There is a constant* m_o *such that*

$$m_n = (1 + p + \dots + p^{n-1})\, e_K + m_o$$

for all sufficiently large n.

2.3. Let L/K be any totally ramified extension. We define the function $\lambda_{L/K}$ by $\lambda_{L/K}(n) = r$ if and only if $Tr_{L/K}(\pi_L^n A_L) = \pi_L^r A_K$. The function $\lambda_{L/K}$ can of course be described in terms of the various numbers, $m(L_i/L_{i-1})$, where $K = L_1 \subset L_2 \subset \dots \subset L_s = L$ is a tower of cyclic extensions of prime degree. As an immediate consequence we have:

2.4. LEMMA. $\lambda_{L/K}(t) = e_L^{-1} e_K t + e_t$, *where the numbers* e_t *are bounded independently of* t.

2.5. LEMMA. ([3], Lemma 3.4). *Let* L/K *be a totally ramified extension. Then there is a* $t_o \in \mathbb{N}$ *such that for all* $t \geq t_o$,

$$\text{F-Norm}_{L/K}(F^t(L)) = F^{\lambda_{L/K}(t)}(K)\,.$$

2.6. *Reduction of the Proof of Theorem B.*

If K_∞/K is a $\mathbb{Z}_p$-extension, then so is K_∞/K_r for all $r \in \mathbb{N}$. In view of 2.2 and 2.5, this reduces the proof of Theorem B to the case where K_∞/K is $\mathbb{Z}_p$-extension such that $m_n = (1 + \dots + p^{n-1})\, e_K + m_o$ for all $n \in \mathbb{N}$. Indeed, if K_∞/K is any $\mathbb{Z}_p$-extension, then by 2.2 there is an $r \in \mathbb{N}$ such that

$$\begin{aligned} m_n &= m(K_n/K_{n-1}) \\ &= (1 + \dots + p^{n-r-1})\, e_K p^r + m_o + (1 + p + \dots + p^{r-1})\, e_K \qquad \text{for all } n > r. \end{aligned}$$

Now apply Lemma 2.5 with $L = K_r$, using that

$$\text{F-Norm}_{n/o} = \text{F-Norm}_{r/o}(\text{F-Norm}_{n/r}).$$

2.7. LEMMA. *Let* F *be a formal group over* A *and* f(X) *its logarithm. Then for* t *large enough* f *is an isomorphism*

$$F^t(K) \xrightarrow{f} \hat{\mathbb{G}}_a^t(K),$$

where $\hat{\mathbb{G}}_a$ *is the additive formal group; i.e.,* $\hat{\mathbb{G}}_a(X, Y) = X + Y$.

Proof. We have $f(F(X, Y)) = f(X) + f(Y)$ and $nb_n \in A$ if $f(X) = \sum b_n X^n$. The lemma follows easily from this.

2.8. *Idea of the Proof of Theorem B.*

We consider the diagram

$$\begin{array}{ccc} F(K_n) & \xrightarrow{\quad f \quad} & K_n \\ \Big\downarrow \text{F-Norm} & & \Big\downarrow Tr_{n/o} \\ F(K) & \xrightarrow{\quad f \quad} & K \end{array}$$

which is commutative. We claim that it now suffices to prove that there is a constant c such that

$$\pi^{\beta_n} A \subset \mathrm{Tr}_{n/o} f(\pi_n A_n) \tag{2.8.1}$$

Indeed, note first of all that it suffices to prove Theorem B for all $n \geq n_o$, where $n_o \in \mathbb{N}$ is some (yet to be determined) constant. This follows from Lemma 2.5. (*cf.* also Lemma 5.1 below.) Now choose a t_1 such that f: $F^t(K) \to \hat{\mathbb{G}}_a^t(K)$ is an isomorphism for $t \geq t_1$. By the easy half of Theorem A, there is an n_o such that $\mathrm{Im}(\text{F-Norm}_{n/o}) \subset F^{t_1}(K)$ for all $n \geq n_o$. By taking c or n_o sufficiently large we can also assume that $\beta_n \geq t_1$ for all $n \geq n_o$. Now let $n \geq n_o$, $x \in F^{\beta_n}(K)$. Let $y \in F(K_n)$ be such that $\mathrm{Tr}_{n/o} \circ f(y) \in \hat{\mathbb{G}}_a^{\beta_n}(K)$. Then $f \circ \text{F-Norm}_{n/o}(y) = f(x)$. But $\text{F-Norm}_{n/o}(y) \in F^{t_1}(K)$, $x \in F^{\beta_n}(K) \subset F^{t_1}(K)$, and f is injective on $F^{t_1}(K)$. Hence $\text{F-Norm}_{n/o}(y) = x$, proving our claim.

3. LEMMAS ON f (X)

3.1. Let h = height (F) $< \infty$. Let F^* be the reduction of the formal group F to a formal group over k, the residue field of K. Because k is algebraically closed, F^* is classified by its height h. Let F_T be the p-typically universal formal group of [4, Part I]. Substituting 1 for T_h and 0 for all T_i with $i \neq h$, we obtain a formal group G over A such that G^* is of height h. Hence G^* is isomorphic to F^*, by a theorem of Lazard, because k is algebraically closed; see for instance [1]. It now follows from [4, Part V, Section 3] and [5] that F is isomorphic to a formal group F_t obtained from F_T by substituting t_i for T_i, $i = 1, 2, \ldots$, where $t_i \in \pi A$, $i = 1, \ldots, h-1$, $t_h = 1$, $t_j = 0$, $j = h+1, h+2, \ldots$. We can therefore assume that F is equal to such an F_t. We can then write

$$F(X, Y) = f^{-1}(f(X) + f(Y)), \qquad f(X) = X + a_1 X^p + a_2 X^{p^2} + \ldots, \tag{3.1.1}$$

where, by [4, Part I], the coefficients of f (X) satisfy the relations

$$pa_n = a_{n-1} t_1^{p^{n-1}} + a_{n-2} t_2^{p^{n-2}} + \ldots + a_{n-h} t_h^{p^{n-h}}, \qquad n \geq h, \tag{3.1.2}$$
$$t_1, \ldots, t_{h-1} \in \pi A, \qquad t_h = 1.$$

3.2. LEMMA. *If* height (F) $< \infty$, *then there is no* $n_o \in \mathbb{N}$ *such that* $v(a_n) \geq 0$ *for all* $n \geq n_o$.

Proof. Suppose $v(a_n) \geq 0$ for all $n \geq n_o$. Then $v(a_n) \geq 0$ for all $n \geq n_o - 1$, by 3.1.2 (because $t_h = 1$). Thus, with induction, $v(a_n) \geq 0$ for all $n \geq 1$, which means that f (X) is an isomorphism of F with the additive group. And this, in turn, implies that height (F) $= \infty$.

3.3. LEMMA. *If* $h < \infty$, *then there is an* $n_o \in \mathbb{N}$ *such that* $v(a_{n_o}) < 0$ *and* $v(a_{n_o+rh}) = v(a_{n_o}) - re_K$, *for all* $r \in \mathbb{N}$.

Proof. Let $n_1 \in \mathbb{N}$ be such that $p^n \geq ne_K$ for $n \geq n_1$. Then for $n \geq n_1 + h$ we have that $v(a_{n-i} t_i^{p^{n-i}}) \geq 0$, $i = 1, \ldots, h-1$. Now let $n_o \geq n_1$ be such that $v(a_{n_o}) < 0$.

Such an n_o exists by Lemma 3.2. Then by (3.1.2) we have that

$$v(a_{n_o+h}) = v(a_{n_o}) - e_K,$$

and, with induction, $v(a_{n_o+rh}) = v(a_{n_o}) - re_K$, $r \in \mathbb{N}$.

3.4. LEMMA. *Let* $h < \infty$. *There is a constant* c *such that*

$$v(a_n) \geq -h^{-1}ne_K - c \qquad \textit{for all } n \in \mathbb{N}.$$

Proof. We have that (*cf.* [4, Part I])

$$a_n = \sum_{(i_1,\dots,i_r)} p^{-r} t_{i_1} t_{i_2}^{p^{i_1}} \dots t_{i_r}^{p^{i_1+\dots+i_{r-1}}} \tag{3.4.1}$$

where the sum is over all sequences $(i_1, \dots, i_r)$ such that

$$i_1 + \dots + i_r = n, \qquad i_j \in \{1, \dots, h\}.$$

Let $s = s(i_1, \dots, i_r)$ be the number of indices j such $i_j = h$. Let $\ell_1, \dots, \ell_{r-s}$ be the indices in $(i_1, \dots, i_r)$ which are different from h. Then

$$\begin{aligned} v(a_n) &\geq \min_{(i_1,\dots,i_r)} \{1 + p^{\ell_1} + \dots + p^{\ell_1+\dots+\ell_{r-s}} - re_K\} \\ &\geq \min_{(i_1,\dots,i_r)} \{(1 + p + \dots + p^{r-s}) - re_K\}. \end{aligned} \tag{3.4.2}$$

Choose c' such that $1 + p + \dots + p^{c'+1} \geq e_K$, and let $c = e_K c'$. If $r \leq \frac{n}{h} + c'$, the term $p^{-r} t_{i_1} t_{i_2}^{p^{i_1}} \dots t_{i_r}^{p^{i_1+\dots+i_{r-1}}}$ has valuation greater than or equal to $-h^{-1}ne_K - e_K c'$. Suppose that

$$r = \frac{n}{h} + c' + d, \qquad d > 0.$$

Because $\ell_1 + \dots + \ell_{r-s} + hs = n$, we have that $r - s + hs \leq n$; hence

$$(h-1)s \leq n - r = (h-1)\left(\frac{n}{h}\right) - (c' + d).$$

Thus $s \leq \frac{n}{h} - \frac{c'+d}{h-1}$ and $r - s \geq c' + d$. Therefore,

$$1 + p + \dots + p^{r-s} - re_K \geq 1 + p + \dots + p^{c'+d} - \left(\frac{n}{h} + c' + d\right)e_K \tag{3.4.3}$$

$$\geq p^d(1 + p + \dots + p^{c'}) - \left(\frac{n}{h} + c'\right) e_K - de_K$$

$$\geq -\left(\frac{n}{h} + c'\right) e_K,$$

which proves the lemma.

3.5. *Remark.* The estimate of 3.4 is (up to a constant) the best possible. This follows from Lemma 3.3, which says that for n of the form $n_o + rh$ there is a constant d such that $v(a_n) = -h^{-1}ne_K + d$.

4. VARIOUS FUNCTIONS AND ESTIMATES

From now on K_∞/K is a $\mathbb{Z}_p$-extension such that

$$m_n = (1 + p + \dots + p^{n-1})e_K + m_o \qquad \text{for all } n \in \mathbb{N},$$

and F is a formal group over A of height $h < \infty$ of the form

$$F(X, Y) = f^{-1}(f(X) + f(Y)),$$

where f(X) is as in (3.1.1) and (3.1.2).

4.1. *The functions* $\mu_n, \sigma_n, j_n, \ell_n$: we define for all $n \in \mathbb{N}$, $t \in \mathbb{N}$, and $i \in \mathbb{N}$

(4.1.1) $\mu_n(p^i, t) = ie_K + \lambda_{n-i/o}(t)$ if $i \leq n$,

$\mu_n(p^i, t) = ne_K + p^{i-n}t$ if $i \geq n$,

(4.1.2) $\sigma_n(t) = \min_i \{v(a_i) + \mu_n(p^i, t)\}$,

(4.1.3) $j_n(t) =$ smallest integer i such that $\sigma_n(t) = v(a_i) + \mu_n(p^i, t)$,

(4.1.4) $\ell_n(t) = n - j_n(t)$.

4.2. LEMMA. *For every* n *and* t *there are only finitely many* i *such that* $\sigma_n(t) = v(a_i) + \mu_n(p^i, t)$.

Proof. This follows immediately from (4.1.1) and Lemma 3.4.

4.3. We define

$$r_n = p^{-1}[(1 + m_n)(p - 1) + 1] \tag{4.3.1}$$

LEMMA. *Suppose that* $m_o \geq 2$ *and* $e_K \geq p$. *Then for all* $n \geq r \geq 0$,

$$\lambda_{n/n-r}(2r_{n+1} - 1) \geq (r + 1)e_K p^{n-r} + p^{n-r}.$$

Proof. One easily sees that

$$\lambda_{n/n-r}(m_n) = m_{n-r} + re_K p^{n-r} = (1 + p + \dots + p^{n-r-1})e_K + m_o + re_K p^{n-r}.$$

Hence it suffices to prove that

$$2r_{n+1} - 1 \geq e_K p^n + p^n + (1 + p + \dots + p^{r-1}) e_K + m_o - m_o p^r.$$

If $r = n$, then $m_o p^r \geq p^n$, because $m_o \geq 2$. We also have $p^n \leq p^{n-1} e_K$ because $e_K \geq p$. It follows that to prove the lemma for all r, it suffices to show that $2r_{n+1} - 1 \geq e_K p^n + (1 + p + \dots + p^{n-1})\, e_K + m_o$. We have

$$2r_{n+1} - 1 \geq 2p^{-1}(p^{n+1} - 1) e_K + 2p^{-1}(p - 1)\, m_o + 2p^{-1} - 1.$$

Now if $p > 2$, then $2p^{-1}(p - 1)\, m_o \geq m_o + 1$, because $m_o \geq 2$; and if $p = 2$, then $2p^{-1} = 1$. Hence

$$2r_{n+1} - 1 \geq 2p^n e_K - 2p^{-1} e_K + m_o \geq (1 + \dots + p^{n-1})\, e_K + m_o + p^n e_K.$$

4.4. TRACE LEMMA [3, Proposition 4.1]. *Let* $\pi_{n-1} = (-1)^{p-1} N_{n/n-1}(\pi_n)$, *where* $N_{n/n-1}$ *is the norm map* $K_n \to K_{n-1}$. *Then we have*

(4.4.1) $$\mathrm{Tr}_{n/n-1}(\pi_n^{pt}) \equiv p\pi_{n-1}^t \mod \pi_{n-1}^{2r_n + t - 1}.$$

4.5. LEMMA. *If* $m_o \geq 2$ *and* $e_K \geq p$, *then* $v(\mathrm{Tr}_{n/o}(\pi_n^{p^r t})) \geq \mu_n(p^r, t)$.

Proof. First let $r \leq n$. Then the trace lemma gives us that

$$\begin{aligned}
&\mathrm{Tr}_{n/n-1}(\pi_n^{p^r t}) \equiv p\pi_{n-1}^{p^{r-1}t} \mod \pi_{n-1}^{s_{n-1}} \\
&\mathrm{Tr}_{n-1/n-2}(p\pi_{n-1}^{p^{r-1}t}) \equiv p^2\pi_{n-2}^{p^{r-2}t} \mod \pi_{n-2}^{s_{n-2}} \\
&\dots \\
&\dots \\
&\dots \\
&\mathrm{Tr}_{n-r+1/n-r}(p^{r-1}\pi p_{n-r+1}^{pt}) \equiv p^r \pi_{n-r}^t \mod \pi_{n-r}^{s_{n-r}},
\end{aligned}$$

where $s_{n-1} = 2r_n + tp^{r-1} - 1$, $s_{n-2} = 2r_{n-1} + tp^{r-2} - 1 + p^{n-2} e_K, \dots,$ and

$$s_{n-r} = 2r_{n-r+1} + t - 1 + (r - 1)\, p^{n-r}.$$

Now, by Lemma 4.3,

$$\begin{aligned}
\lambda_{n-i/n-r}&(2r_{n-i+1} + p^{r-i}t - 1 + p^{n-i}(i - 1)\, e_K) \\
&= t + p^{n-r}(i - 1)\, e_K + \lambda_{n-i/n-r}(2r_{n-i+1} - 1) \geq t + re_K p^{n-r} + p^{n-r}.
\end{aligned}$$

It follows that

(4.5.1) $$\mathrm{Tr}_{n/n-r}(\pi_n^{p^r t}) \equiv p^r \pi_{n-r}^t \mod (v_{n-r} - \text{valuation } t + re_K p^{n-r} + p^{n-r}).$$

Now $v_{n-r}(p^r \pi_{n-r}^t) = re_K p^{n-r} + t$. Hence

(4.5.2) $$v(\mathrm{Tr}_{n/o}(\pi_n^{p^r t})) \geq re_K + \lambda_{n-r/o}(t) = \mu_n(p^r, t).$$

Now suppose that $r > n$; then replacing t with $p^{r-n}t$ and r with n, we obtain from (4.5.1)

$$\text{(4.5.3)} \qquad \mathrm{Tr}_{n/o}(\pi_n^{p^r t}) \equiv p^n \pi^{p^{r-n}t} \mod (v - \text{valuation } p^{r-n}t + ne_K + 1),$$

which proves the lemma also in this case.

4.6. LEMMA. *Suppose that* $m_o \geq 2$, $e_K \geq p$, *and let* t *be such that*

$$\lambda_{n-r/o}(t+1) = \lambda_{n-r/o}(t) + 1$$

for a certain $r \in \mathbb{N}$. *Then if* $r \leq n$, *we have* $v(\mathrm{Tr}_{n/o}(\pi_n^{p^r t})) = \mu_n(p^r, t)$; *and if* $r > n$, *then* $v(\mathrm{Tr}_{n/o}(\pi_n^{p^r t})) = \mu_n(p^r, t)$ for all t.

Proof. If $x \in A_{n-r}$ and $v_{n-r}(x) = s$ and $\lambda_{n-r/o}(s+1) = \lambda_{n-r/o}(s) + 1$, then always $v(\mathrm{Tr}_{n-r/o}(x)) = \lambda_{n-r/o}(s)$. Lemma 4.6 now follows immediately from (4.5.1). The second statement of the lemma follows from (4.5.3).

4.7. LEMMA. *For every* $t \in \mathbb{N}$ *there is a constant* c *such that*

$$\sigma_n(t) \leq h^{-1}(h-1)ne_K + c.$$

Proof. Let i_o be such that $v(a_{i_o}) < 0$,

$$v(a_{i_o+rh}) = v(a_{i_o}) - re_K \qquad \text{for } r \in \mathbb{Z},\ r \geq -1.$$

For $n \leq i_o$ take $i = i_o$. Then we have

$$\sigma_n(t) \leq v(a_{i_o}) + \mu_n(p^{i_o}, t) \leq p^{i_o - n} = t + i_o e_K \leq p^{i_o}t + i_o e_K$$

If $n > i_o$, let i be the largest number of the form $i = i_o + rh$ which is smaller than n. Then $n - i \leq h$, and we have

$$\begin{aligned}\sigma_n(t) &\leq v(a_i) + \mu_n(p^i, t) = v(a_{i_o}) - re_K + \lambda_{n-i/o}(t) + ie_K \\ &\leq ne_K - re_K + \lambda_{n-i/o}(t).\end{aligned}$$

Now $\lambda_{n-i/o}(t)$ is bounded because $n - i \leq h$. Let $d = \max\{\lambda_{1/o}(t), \ldots, \lambda_{h/o}(t)\}$. As $i_o + rh + h \geq n$, we have that $r \geq h^{-1}n - 1 - h^{-1}i_o$, so that indeed, for all $n \in \mathbb{N}$, $\sigma_n(t) \leq h^{-1}(h-1)ne_K + c$, with $c = \max(p^{i_o}t + i_o e_K, (1 + h^{-1}i_o)e_K + d)$.

5. PROOF OF THEOREM B

By Lemma 2.2 and 2.6 we can assume that the $\mathbb{Z}_p$-extension K_∞/K is such that $m_n = (1 + p + \ldots + p^{n-1})e_K + m_o$ for all $n \in \mathbb{N}$ and that moreover, $e_K \geq p$ and $m_o \geq 2$.

5.1. LEMMA. *Let* L/K *be an extension. Then there is a* $t \in \mathbb{N}$ *such that* $\text{F-Norm}_{L/K}(F(L)) \supset F^t(K)$.

Proof. Let $F(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^i$. Let s be such that

$$\lambda_{L/K}(s) < [L: K]^{-1} 2s,$$

and let $v_L(x) = s$. It follows that

$$\text{F-Norm}(x) \equiv Tr_{L/K}(x) \mod (v - \text{valuation } \lambda_{L/K}(s) + 1).$$

Up to a constant we have $\lambda_{L/K}(s) = [L: K]^{-1} s$, proving the lemma.

5.2. *Proof of Theorem B in the case* $h = \infty$. This case follows from Lemma 5.1; *cf.* also [3].

5.3. In view of 5.2, we can assume that $h < \infty$. Hence we can assume that $F(X, Y)$ is a formal group with logarithm $f(X)$ such that (3.1.1) and (3.1.2) hold. Given all this, we have available the various functions defined in Sections 3 and 4 and the various lemmas of Sections 3 and 4.

Choose n_o such that $v(a_{n_o}) < 0$ and $v(a_{n_o+rh}) = v(a_{n_o}) - re_K$, $r \geq 0$, and such that $p^n \geq ne_K$ for $n \geq n_o$. Note that if $n \geq n_o + h$, and $v(a_n) < -1$, then

$$v(a_{n-h}) = v(a_n) + 1$$

by (3.1.2). Let $t_o \in \mathbb{N}$ be such that $t_o \geq (1 + p + \dots + p^{h-1}) e_K + m_o$, and choose a constant c_o as in Lemma 4.7. Now let $n_1 \in \mathbb{N}$ be such that $n_1 \geq n_o + h$, and such that $\sigma_n(t_o) < ne_K$ for $n \geq n_1$. We then have:

5.4. LEMMA. *If* $n \geq n_1$, *then* $j_n(t_o) \leq n$.

Proof. Suppose $n' = j_n(t_o) > n$. Then $v(a_{n'}) + \mu_n(p^{n'}, t_o) = \sigma_n(t_o) < ne_K$. But $\mu_n(p^{n'}, t_o) = ne_K + p^{n'-n} t$. Hence $v(a_{n'}) < -1$ and $v(a_{n'-h}) = v(a_{n'}) + 1$. Then, if $n' \geq n + h$, we have

$$v(a_{n'-h}) + \mu_n(p^{n'-h}, t_o) = v(a_{n'}) + 1 + ne_K + p^{n'-h-n} t_o \leq v(a_{n'}) + \mu_n(p^{n'}, t_o),$$

which is a contradiction. And if $n' - h < n$, we have

$$v(a_{n'-h}) + \mu_n(p^{n'-h}, t_o) = v(a_{n'}) + 1 + (n' - h) e_K + \lambda_{n-n'+h/o}(t_o).$$

This last expression is also less than or equal to $v(a_{n'}) + \mu_n(p^{n'}, t_o)$, because $\lambda_{i/o}(t_o) \leq t_o$ for $i = 1, \dots, h$ if $t_o \geq (1 + p + \dots + p^{h-1}) e_K + m_o$.

5.5. *Proof of Theorem* B. We assume all the conditions mentioned above. Let n_1 be as in 5.3 above. By Lemma 5.1, it suffices to prove Theorem B for $n \geq n_1$. According to 2.8, it hence suffices to prove that

$$Tr_{n/o} f(\pi_n A_n) \supset \pi^{\beta_n} A \qquad \text{for } n \geq n_1 .$$

We note that, because $f(F(X, Y)) = f(X) + f(Y)$, we have

$$x, y \in Tr_{n/o} f(\pi_n A_n) \Rightarrow x + y \in Tr_{n/o} f(\pi_n A_n) . \tag{5.5.1}$$

Now let $t_o \in \mathbb{N}$ be larger than $(1 + p + \ldots + p^{h-1}) e_K + m_o$, and let $j = j_n(t_o)$. Then $j \leq n$ by Lemma 5.4. Let $\ell = \ell_n(t_o) = n - j_n(t_o) = n - j$, and let t be the largest integer such that $t \geq t_o$ and $\lambda_{\ell/o}(t) = \lambda_{\ell/o}(t_o)$. Then we have (*cf.* 4.1)

$$\begin{aligned} &\mu_n(p^i, t) \geq \mu_n(p^i, t_o) \qquad \text{for all } i = 1, 2, \ldots, \\ &\mu_n(p^j, t) = \mu_n(p^j, t_o) . \end{aligned} \tag{5.5.2}$$

If follows that (*cf.* 4.1)

$$\sigma_n(t) = \sigma_n(t_o), \quad j_n(t) = j_n(t_o) = j . \tag{5.5.3}$$

Now we also know by Lemmas 4.6 and 4.5 that

$$\begin{aligned} &v(\mathrm{Tr}_{n/o}(a_j \pi_n^{p^j t})) = v(a_j) + \mu_n(p^j, t) , \\ &v(\mathrm{Tr}_{n/o}(a_i \pi_n^{p^i t})) \geq v(a_i) + \mu_n(p^i, t) , \quad i \neq j . \end{aligned} \tag{5.5.4}$$

Let $x \in A$. Then it follows from (5.5.4) and Lemma 4.2 that

$$\mathrm{Tr}_{n/o} f(x\pi_n^t) \equiv b_o x^{p^j} + b_1 x^{p^{j+1}} + \ldots + b_r x^{p^{j+r}} \quad \mathrm{mod}\, \pi^{\sigma_n(t)+1} , \tag{5.5.5}$$

where r is such that $v(a_i) + \mu_n(p^i, t) \geq \sigma_n(t) + 1$ for all $i \geq j + r$, and where

$$v(b_o) = \sigma_n(t) = \sigma_n(t_o), \quad v(b_i) \geq \sigma_n(t), \qquad i = 1, \ldots, r . \tag{5.5.6}$$

Because k is algebraically closed, this implies that

$$\mathrm{Tr}_{n/o} f(\pi_n A_n)/\pi^{\sigma_n(t_o)+1} A \supset \pi^{\sigma_n(t_o)} A/\pi^{\sigma_n(t_o)+1} A . \tag{5.5.7}$$

We obtain an inclusion (5.5.7) for every $t_o \in \mathbb{N}$, $t_o \geq (1 + p + \ldots + p^{h-1}) e_K + m_o$.

Now we also have that $\sigma_n((1 + p + \ldots + p^{h-1}) e_K + m_o)) = h^{-1} n e_K + c$ for a certain constant c. Hence, in view of (5.5.1) and the completeness of the discrete valuation ring A, Theorem B will be proved if we can show that for every $n \geq n_1$, all $s \in \mathbb{N}$ with $s \geq s_o = \sigma_n((1 + p + \ldots + p^{h-1}) e_K + m_o))$ occur as a $\sigma_n(t)$ for some t.

This is done by induction on $s - s_o$. The induction hypothesis is: there is a $t_o \geq \sigma_n((1 + p + \ldots + p^{h-1}) e_K + m_o))$ such that $\sigma_n(t_o) = s \geq 0$. Let $j_o = j_n(t_o)$; then $j_o \leq n$. Let $\ell_o = n - j_o$ and let $t_1 = t_o + p^{\ell_o}$; then

$$\begin{aligned} &v(a_i) + \mu_n(p^i, t_1) \geq v(a_i) + \mu_n(p^i, t_o) + 1 \qquad \text{if } i > j_o, \\ &v(a_{j_o}) + \mu_n(p^{j_o}, t_1) = v(a_{j_o}) + \mu_n(p^{j_o}, t_o) + 1, \\ &v(a_i) + \mu_n(p^i, t_1) \geq v(a_i) + \mu_n(p^i, t_o) \qquad \text{if } i < j_o . \end{aligned} \tag{5.5.8}$$

It follows that

$$\sigma_n(t_1) \leq \sigma_n(t_o) + 1 . \tag{5.5.9}$$

If $\sigma_n(t_1) = \sigma_n(t_o) + 1$, we are finished. If $\sigma_n(t_1) = \sigma_n(t_o)$, then, because of (5.5.8), we must have $j_n(t_1) = j_1 < j_o$. Let $\ell_1 = n - j_1$ and $t_2 = t_1 + p^{\ell_1}$; then

$$\sigma_n(t_2) \leq \sigma_n(t_1) + 1.$$

If .... Because $j_o > j_1 > \ldots \geq 0$, this process must stop and finally yield a t such that $\sigma_n(t) = s + 1$. This concludes the proof of the theorem.

REFERENCES

1. A. Fröhlich, *Formal Groups.* Lecture Notes in Mathematics, Vol. 74, Springer, Berlin-Heidelberg-New York, 1968.
2. M. Hazewinkel, *Norm Maps for Formal Groups I: The Cyclotomic Γ-extension.* J. Algebra 32 (1974), 89–108.
3. ———, *Norm Maps for Formal Groups II: Γ-extensions of Local Fields with Algebraically Closed Residue Field.* J. Reine Angew. Math. 268/269 (1974), 222–250.
4. ———, *Constructing Formal Groups.* I–VIII; I: J. Pure Appl. Algebra 9 (1977), 131–149; II: ibid 9 (1977), 151–161; III: ibid 10 (1977), 1–18; IV–VII, Adv. Math, to appear; VIII Compositio Math, submitted.
5. J. Lubin and J. Tate, *Formal moduli for one-parameter formal Lie groups.* Bull. Soc. Math. France 94 (1966), 49–59.
6. B. Mazur, *Rational Points of Abelian Varieties with Values in Towers of Number Fields.* Invent. Math. 18 (1972), 183–266.
7. J. Tate, *p-divisible Groups.* Proc. Conf. Local Fields (Driebergen, 1966), pp. 158–183, Springer, Berlin, 1967.

Dept. Math., Econometric Inst.
Erasmus Universiteit Rotterdam
50, Burg. Oudlaan,
Rotterdam, The Netherlands