ERASMUS UNIVERSITY ROTTERDAM

NETHERLANDS SCHOOL OF ECONOMICS

ECONOMETRIC INSTITUTE

# ON NORM MAPS FOR ONE DIMENSIONAL GROUPS I: THE CYCLOTOMIC Γ-EXTENSION

M. HAZEWINKEL

REPRINT SERIES no. 178

This article appeared in "Journal of Algebra", vol. 32 (1974) and is reprinted for private circulation by permission of the Editor.

Reprinted from JOURNAL OF ALGEBRA
Vol. 32, No. 1, October 1974
Printed in Belgium


# On Norm Maps for One Dimensional Formal Groups I: The Cyclotomic $\Gamma$-Extension*

MICHIEL HAZEWINKEL

*Mathematics Department, Econometric Institute, Erasmus University of Rotterdam, Burg Oudlaan 50, 3016 Rotterdam, The Netherlands*

*Communicated by A. Fröhlich*

Received March 31, 1970

## 1. INTRODUCTION

Let $K$ be a finite extension of $\mathbf{Q}_p$, the field of $p$-adic numbers. Let $L/K$ be a galois extension. Local class field theory studies the cokernel of the norm map $N_{L/K}: L^* \to K^*$. Let $A_L$, $A_K$ be the ring of integers of $L$, $K$ and let $U(L)$, $U(K)$ be the group of units of $A_L$, $A_K$. The most difficult part of the determination of $N_{L/K}(L^*)$ is the determination of the image (or cokernel) of $N_{L/K}$: $U(L) \to U(K)$. This map can also be viewed as follows. Let $\mathbf{G}_m$ be the multiplicative group. Then $\mathbf{G}_m(A_L) = U(L)$, $\mathbf{G}_m(A_K) = U(K)$ and the map $N_{L/K}$ is: $N_{L/K}(x) =$ sum of all the conjugates of $x$ in $\mathbf{G}_m(L)$.

The following generalization is now natural and also interesting for various reasons (cf., [7, Section 4]). Let $G$ be an arbitrary commutative group scheme over $A_K$. Define Norm$(x) =$ sum in $G(A_L)$ of all the conjugates of $x$, for $x \in G(A_L)$. Problem. Determine the cokernel of Norm: $G(A_L) \to G(A_K)$. As in the case of $\mathbf{G}_m$ an important step is to calculate the cokernel of the induced map $\hat{G}(A_L) \to \hat{G}(A_K)$ where $\hat{G}$ is the formal completion of $G$; $\hat{G}$ is a formal group over $A_K$.

In the following we study the cokernel of Norm: $F(A_L) \to F(A_K)$ where $F$ is a one-dimensional formal group over $A_K$. In case the height of $F$ is equal to 1 the answer is up to a twist given by local class field theory (cf., [7]). Important is the fact that Norm: $F(A_{\widehat{L_{ur}}}) \to F(A_{\widehat{K_{ur}}})$ is surjective if height $(F) = 1$, where $L_{ur}$, $K_{ur}$ is the maximal unramified extension of $L$, $K$. The picture changes drastically as soon as height $(F) > 1$. It is then not true in general that Norm $(F(L)) = F(K)$ if $L/K$ is a finite galois extension and the residue field of $K$ is algebraically closed.

* While the research for this paper was done the author stayed at the Steklov Institute of Mathematics in Moscow (1969/1970) and he was supported by Z.W.O., the Netherlands Organization for the advancement of Pure Research.

The main part of this paper is devoted to the precise determination of the cokernel of $F(L) \to F(K)$ for one special class of extensions $L/K$. We take $K = \mathbf{Q}_p$, the $p$-adic numbers. Let $L_\infty$ be the extension of $\mathbf{Q}_p$ obtained by adjoining all $p^r$-th roots of unity. $\text{Gal}(L_\infty/\mathbf{Q}_p) \simeq U(\mathbf{Q}_p) \simeq \Delta \times \mathbf{Z}_p$ where $\Delta$ is the torsion subroup of $U(\mathbf{Q}_p)$. Let $K_\infty$ be the invariant field of $\Delta$. $\text{Gal}(K_\infty/\mathbf{Q}_p) \simeq \mathbf{Z}_p$, i.e., $K_\infty/\mathbf{Q}_p$ is a $\Gamma$-extension. Let $K_n$ be the invariant field of $p^n \text{ Gal}(K_\infty/\mathbf{Q}_p)$. We determine $\text{Im}(F(K_n) \to F(\mathbf{Q}_p))$, where $F$ is any formal group over $\mathbf{Z}_p$ of height $(F) \geqslant 2$.

The results and proofs turn out to be generalizable to some extent (cf., [3]).

The motivation to study precisely $\Gamma$-extensions came from [7].

It remains for me to thank the reviewer who thoroughly criticized an earlier version of this note.

## 2. Generalities on Formal Groups

### 2.1. *Some Notations and Definitions*

$K$ will always denote a local field of characteristic 0 and residue characteristic $p > 0$; $A_K$ is its ring of integers; $\pi_K$ is a uniformizing element and $v_K$ is the normalized exponential valuation on $K$ (i.e., $v_K(\pi_K) = 1$); $\mathfrak{M}_K$ is the maximal ideal of $A_K$.

A one dimensional formal group over $A_K$ is a formal power series in two variables over $A_K$ of the form

$$F(X, Y) = X + Y + \sum_{i,j=1}^{\infty} a_{ij}X^iY^j, \qquad a_{ij} \in A_K, \tag{2.1.1}$$

which satisfies

$$F(X, F(Y, Z)) = F(F(X, Y), Z). \tag{2.1.2}$$

All formal groups considered in this paper will be one dimensional. A one dimensional formal group over $A_K$ is automatically commutative; i.e., it satisfies $F(X, Y) = F(Y, X)$ (cf. [4]).

### 2.2. *Points and Norm Maps*

Let $L$ be a finite extension of $K$. One can use a formal group over $A_K$ to define an abelian group structure on the set $\mathfrak{M}_L$. In fact one simply sets

$$x +_F y = F(x, y), \qquad x, y \in \mathfrak{M}_L. \tag{2.2.1}$$

(The series $F(x, y)$ converges in $\mathfrak{M}_L$.) This group is denoted $F(L)$. If

$x, y \in \mathfrak{M}_L{}^t = \pi_L{}^t A_L$, $t = 1, 2, \ldots$, then $x +_F y \in \mathfrak{M}_L{}^t$. The group $F(L)$ therefore has a natural filtration by subgroups $F^t(L)$ where the underlying set of $F^t(L)$ is $\pi_L{}^t A_L$.

Because $F(X, Y) \equiv X + Y \bmod(\text{degree } 2)$, cf. (2.1.1), we have

$$F^t(L)/F^{t+1}(L) \simeq l^+, \tag{2.2.2}$$

where $l^+$ is the underlying additive group of the residue field $l$ of $L$.

Now let $L/K$ be a galois extension with galois group $G = \mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_r\}$. We define a norm map $F$-Norm: $F(L) \to F(K)$ by the formula

$$F\text{-Norm}: F(L) \to F(K), \qquad x \mapsto \sigma_1 x +_F \sigma_2 x +_F \cdots +_F \sigma_r(x). \tag{2.2.3}$$

(The $F$-sum of the conjugates of $x$ is in $K$ because it is invariant under $G$.)

EXAMPLES. If $F = \hat{\mathbf{G}}_a$, the additive group, given by $\hat{\mathbf{G}}_a(X, Y) = X + Y$, then $F(L) = \mathfrak{M}_L$ (with its original additive group structure) and $F(K) = \mathfrak{M}_K$. The norm map, $\mathbf{G}_a$-Norm, is equal to $\mathrm{Tr}_{L/K}$, the trace map.

If $F = \hat{\mathbf{G}}_m$, the multiplicative group given by $\hat{\mathbf{G}}_m(X, Y) = X + Y + XY$, then $F(L) = U_L{}^1$, the group of units congruent to 1 mod $\pi_L$ of $A_L$. The norm map, $\hat{\mathbf{G}}_m$-Norm, becomes the ordinary norm map $U_L{}^1 \to U_K{}^1$ under the isomorphisms $F(L) \simeq U_L{}^1$ and $F(U) \simeq U_K{}^1$.

## 2.3. *Height of a Formal Group*

Let $F$ be a formal group over $A_K$. We define inductively

$$\begin{aligned} F_2(X_1, X_2) &= F(X_1, X_2), \ldots, F_{n+1}(X_1, \ldots, X_{n+1}) \\ &= F(F_n(X_1, \ldots, X_n), X_{n+1}), \ldots . \end{aligned} \tag{2.3.1}$$

Because $F$ is associative and commutative, one has that $F(X_1, \ldots, X_n) = F(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ for every permutation of $\{1, 2, \ldots, n\}$.

Let $p$ be the residue characteristic of $A_K$. One defines $[p]_F(X)$ as $[p]_F(X) = F_p(X, X, \ldots, X)$. We consider $[p]_F(X) \bmod \pi_K$. There are two possibilities (cf., [1, 4]).

(i) There exists a number $h \in \mathbf{N}$ such that $[p]_F(X) \equiv g(X^{p^h}) \bmod \pi_K$ where $g(Z) = b_1 Z + b_2 Z^2 + \cdots$ is a power series over $A_K$ with $b_1 \not\equiv 0 \bmod \pi_K$. The number $h = h(F)$ is called the *height* of $F$.

(ii) $[p]_F(X) \equiv 0 \bmod \pi_K$. In this case one defines $h = h(F)$, the height of $F$, as $h = \infty$.

2.4. *Lemma on* $F$-Norm

Let $F_r$ be a formal group over $A_K$. If $M$ is a monomial in $X_1, \ldots, X_n$, e.g., $M = X_1^{r_1} \cdots X_n^{r_n}$, we define

$$\mathrm{Tr}(M) = X_1^{r_1} \cdots X_n^{r_n} + X_2^{r_1} \cdots X_n^{r_{n-1}} X_1^{r_n} + \cdots + X_n^{r_1} X_1^{r_2} \cdots X_{n-1}^{r_n} .$$

We write $N^i(X)$ for $X_1{}^i \cdots X_n{}^i$. Using these notations one has the following.

Lemma 2.4.1.

$$F_n(X_1, \ldots, X_n) = \mathrm{Tr}(X_1) + \sum_{i=1}^{\infty} a_i N^i(X) + \sum_M a_M \mathrm{Tr}(M),$$

*where* $a_i$, $a_M \in A_K$, *and* $M$ *runs through a set of monomials of total degree* $\geqslant 2$ *which are not of the form* $N^i(X)$. *If moreover* $n = p$, *the residue characteristic of* $K$, *then* $v_K(a_i) \geqslant 1$ *unless* $i = kp^{h-1}$, $k = 1, 2, \ldots$, *and* $v_K(a_i) = 0$ *if* $i = p^{h-1}$, *where* $h$ *is the height of* $F$. (*If* $h = \infty$, $v(a_i) \geqslant 1$ *for all* $i$ *if* $p = n$.)

*Proof.* The first statement follows from the fact that $F(X, Y) \equiv X + Y$ mod (degree 2) and the fact that $F(X_1, \ldots, X_n)$ is invariant under permutations of the $X_1, \ldots, X_n$. The second part of the lemma follows from the first part and (2.3), because substituting $X$ for the $X_i$ in $\mathrm{Tr}(M)$ results in something $\equiv 0 \bmod p$ if $M$ is not of the form $N^i(X)$. Q.E.D.

Now let $L/K$ be a cyclic galois extension of degree $n$. Let $\mathrm{Tr}_{L/K}$ and $N_{L/K}$ denote the trace and norm maps. We write $N_{L/K}(x)$ for $(N_{L/K}(x))^i$. From the definition of $F$-Norm and (2.4.1) one then immediately obtains the following.

Corollary 2.4.2.

$$F\text{-Norm}_{L/K}(x) \equiv \mathrm{Tr}_{L/K}(x) + \sum_{i=1}^{\infty} a_i N^i_{L/K}(x) \bmod \mathrm{Tr}_{L/K}(x^2 A_L)$$

*for all* $x \in F(L)$. *If* $n = p$ *one has the same statements on the valuations of the* $a_i$ *as in* (2.4.1).

## 3. Unramified and Tamely Ramified Extensions

In the case of an unramified or tamely ramified extension $L/K$, the image of $F$-Norm: $F(L) \to F(K)$ is very easy to calculate.

Proposition 3.1. *Let* $L/K$ *be a tamely ramified galois extension, then* $F$-Norm: $F(L) \to F(K)$ *is surjective.*

*Proof.* First suppose that $L/K$ is unramified. $F$-Norm maps $F^s(L)$ into $F^s(K)$ and for every $y \in F(K)$ of valuation $v_K(y) = s$, there exists an $x \in F^s(L)$ such that

$$F\text{-Norm}(x) \equiv y \bmod(\pi_K^{2s}).$$

Indeed, according to (2.2.1) and (2.2.3) we have

$$F\text{-Norm}_{L/K}(x) \equiv \mathrm{Tr}_{L/K}(x) \bmod(\pi_K^{2s}),$$

and it thus suffices to select an $x \in F^s(L)$ such that $\mathrm{Tr}_{L/K}(x) = y$ which can be done because $L/K$ is unramified. It follows that the induced map $F^s(L) \to F^s(K)/F^{s+1}(K)$ is surjective and this proves the proposition in this case according to Lemma (3.2) below.

Now let $L/K$ be totally and tamely ramified. Because $\mathrm{Gal}(L/K)$ is cyclic of order prime to $p$ (cf. [8], Chapter IV, Section 2]), it suffices to treat tamely and totally ramified extensions of prime degree $l$, $(l, p) = 1$. For such extensions one has

$$\mathrm{Tr}_{L/K}(\pi_L{}^t A_L) = \pi_K{}^r A_K, \qquad r = [((l-1)+t)/l] \qquad (3.1.1)$$

where $[s/l]$ denotes the entier of $s/l$. (cf. [8, Chapter V, Section 3].) It follows that for every $s \in \mathbf{N}$ there exists a number $t_s$ such that

(i) $t_s > s$,

(ii) $v_K(\mathrm{Tr}_{L/K}(x)) > s$ if $v_L(x) > t_s$,

(iii) $v_K(\mathrm{Tr}_{L/K}(x)) = s$ if $v_L(x) = t_s$.

It follows from this and (2.4.2) that

$$F\text{-Norm}_{L/K}(zx) \equiv z\,\mathrm{Tr}_{L/K}(x) \bmod(\pi_K^{s+1}A_K)$$

if $v_L(x) = t_s$, $z \in A_K$. Using this, (2.2.2) and (iii) above we see that the induced map $F^{t_s}(L) \to F^s(K)/F^{s+1}(K)$ is surjective, which proves the proposition in this case.

Finally let $L/K$ be tamely ramified. The extension $L/K$ can be decomposed into a tower $K \subset L_{ur} \subset L$, where $L_{ur}/K$ is unramified and $L/L_{ur}$ is totally and tamely ramified. As $F\text{-Norm}_{L/K} = F\text{-Norm}_{L_{ur}/K} \cdot F\text{-Norm}_{L/L_{ur}}$ we are through. Q.E.D.

For completeness sake we state the lemma which was used twice in the proof above, and which we shall use a few more times in the sections below.

LEMMA 3.2. *Let $A$ and $B$ be abelian groups filtered by subgroups $A = A_1 \supset A_2 \supset B = B_1 \supset B_2 \supset \cdots$ such that $A = \varprojlim A/A_n$, and $\bigcap_n B_n = \{0\}$. Let $u\colon A \to B$ be a homomorphism and suppose that there exist indices $t_1 < t_2 < \cdots$*

*such that* $u(A_{t_i}) \subset B_i$ *and* $u\colon A_{t_i} \to B_i/B_{i+1}$ *is surjective for all* $i = 1, 2, \ldots$ . *Then* $u\colon A \to B$ *is surjective.*

*Proof.* Very easy, cf., e.g., [8, Chapter V, Section 1, Lemma 2].

## 4. The Cyclotomic $\Gamma$-Extension

A $\Gamma$-extension of a field $K$ is an (infinite) galois extension $K_\infty/K$ such that $\mathrm{Gal}(K_\infty/K) \simeq \mathbf{Z}_p$, the $p$-adic integers.

### 4.1. *The Cyclotomic $\Gamma$-Extension of* $\mathbf{Q}_p$

Let $\mathbf{Q}_p$ be the field of $p$-adic numbers. Adjoin to $\mathbf{Q}_p$ all $p^r$-th roots of unity, for all $r$. The result is a totally ramified abelian extension $L_\infty/\mathbf{Q}_p$ of galois group isomorphic to $U(\mathbf{Q}_p)$. Let $\Delta$ be the torsion subgroup of $U(\mathbf{Q}_p)$. If $p > 2$, this is the subgroup of the $(p-1)$-st roots of unity; if $p = 2$ this is the subgroup $\{1, -1\}$. Let $K_\infty$ be the invariant field of $\Delta$. Then $K_\infty/\mathbf{Q}_p$ is a $\Gamma$-extension (associated to the prime $p$). We shall call this extension the cyclotomic $\Gamma$-extension of $\mathbf{Q}_p$. Let $K_n$ be the invariant field of the closed subgroup $p^n \, \mathrm{Gal}(K_\infty/\mathbf{Q}_p)$. We obtain a tower of totally ramified extensions of degree $p$ $\cdots - K_{n+1} - K_n - \cdots - K_2 - K_1 - \mathbf{Q}_p = K$.

Another way to construct this $\Gamma$-extension of $K = \mathbf{Q}_p$ for $p > 2$ is as follows. Let $f(X) = X^p + pX$; Let $f^{(m)}(X)$ be the $m$-th iterate of $f(X)$, i.e., $f^{(m)}(X) = f^{(m-1)}(f(X))$, $f^{(0)}(X) = X$. Let $(LT)_{n+1}$ (the $(n+1)$-st Lubin–Tate extension of $K$; cf. [6] or [2]) be the extension generated by any root $\lambda_{n+1}$ of $f^{(n+1)}(X)$, which is not a root of $f^{(n)}(X)$. The extension $(LT)_{n+1}/K$ is galois and totally ramified; the galois group is isomorphic to $U(\mathbf{Q}_p)/U^{n+1}(\mathbf{Q}_p)$. (Cf. [6] or [2]; $U(\mathbf{Q}_p) =$ units of $\mathbf{Z}_p$; $U^n(\mathbf{Q}_p) = \{u \in U(\mathbf{Q}_p) \mid u \equiv 1 \bmod p^n\}$). The action of $u \in U(\mathbf{Q}_p)$ is given by $\lambda_{n+1} \mapsto [u]_f(\lambda_{n+1})$, where $[u]_f(X)$ is the unique power series such that $[u]_f(X) \equiv uX \bmod (\text{degree } 2)$ and $[u]_f \circ f = f \circ [u]_f$. Let $\zeta$ be a $(p-1)$-st root of unity, then $[\zeta]_f(X) = \zeta X$, because $(\zeta X)^p + p(\zeta X) = \zeta(X^p + pX)$. The element $\mu_n = \lambda_{n+1}^{p-1}$ is therefore invariant under the action of $\Delta$. The extension $\bigcup_n \mathbf{Q}_p(\mu_n)/\mathbf{Q}_p$ is the cyclotomic $\Gamma$-extension of $\mathbf{Q}_p$. (If $p = 2$ one obtains in this way the whole extension $L_\infty/\mathbf{Q}_2$.)

### 4.2. *The Number* $m(L/K)$

Let $L/K$, be a totally ramified extension of degree $p$. Then there exists a certain number $m(L/K) \in \mathbf{N}$ such that

$$\mathrm{Tr}_{L/K}(\pi_L{}^t A_L) = \pi_K{}^r A_K \quad \text{where} \quad r = [\{(m(L/K) + 1)(p-1) + t\}/p] \tag{4.2.1}$$

(cf. [8, Chapter IV, Section 2]).

### 4.3. *Equations for* $\mu_n$

It is not difficult to find equations for the $\mu_n$ defined in (4.1). Indeed, we can choose $\lambda_1, \lambda_2, \ldots$ inductively such that $\lambda_{n+1}^p + p\lambda_{n+1} = \lambda_n$, $n \geqslant 1$, $\lambda_1^{p-1} = -p$. We have $\mu_n = \lambda_{n+1}^{p-1}$; it follows that $\mu_0 = -p$ and that

$$X(X + p)^{p-1} - \mu_{n-1} \tag{4.3.1}$$

is the minimal polynomial of $\mu_n$ over $K_{n-1}$. (Note that $\mu_n$ is a uniformizing element of $K_n$.)

### 4.4. *The Numbers* $m_n$

Let $m_n = m(K_n/K_{n-1})$, $n = 1, 2, \ldots$. One finds by explicit calculations from Eq. (4.3.1) above that

$$\begin{aligned} \mathrm{Tr}_{n/n-1}(\mu_n) &= -(p-1)p, \\ \mathrm{Tr}_{n/n-1}(\mu_n{}^2) &= (p-1)\,p^2, \\ \mathrm{Tr}_{n/n-1}(\mu_n^{p-1}) &= (-1)^{p-1}(p-1)\,p^{p-1}. \end{aligned} \tag{4.4.1}$$

(We have written $\mathrm{Tr}_{n/n-1}$ for $\mathrm{Tr}_{K_n/K_{n-1}}$). Comparing this with (4.2.1) one finds that

$$m_n = 1 + p + \cdots + p^{n-1}. \tag{4.4.2}$$

In the sections below we shall need to know something about $\mathrm{Tr}_{n/n-1}(\mu_n{}^k)$, especially in the case that $k$ is a multiple of $p$.

TRACE LEMMA 4.5.

$$\mathrm{Tr}_{n/n-1}(\mu_n^{kp+c}) \equiv 0 \bmod \mu_{n-1}^k p^c,\ c = 1, 2, \ldots, p-1;\ k = 0, 1, 2, \ldots,$$

$$\mathrm{Tr}_{n/n-1}(\mu_n^{kp}) \equiv p\mu_{n+1}^k \bmod \mu_{n-1}^{k-1} p^p,\ k = 1, 2, \ldots.$$

*Proof.* The formulas (4.4.1) above take care of the cases $k = 0$, $c = 1, 2, \ldots, p-1$. We have the relation

$$\mu_n{}^p + \binom{p-1}{1}\mu_n^{p-1}p + \cdots + \mu_n\binom{p-1}{p-1}p^{p-1} = \mu_{n-1}. \tag{4.5.1}$$

Applying $\mathrm{Tr}_{n/n-1}$ and using (4.4.1) we see that

$$\mathrm{Tr}_{n/n-1}(\mu_n{}^p) \equiv p\mu_{n-1} \quad \mathrm{mod}(\,p^p). \tag{4.5.2}$$

To prove the lemma for $kp + c > p$, multiply the relation (4.5.1) with $\mu_n^{(k-1)p+c}$ and use induction.

## 5. Some Preliminary Calculations

In this and the following Sections 6, 7, $K = K_0 = \mathbf{Q}_p$, and

$$\cdots - K_n - \cdots - K_1 - K$$

is the tower of extensions constructed in 4.1, $K_n = K_{n-1}(\mu_n)$. If $p > 2$, $\bigcup_n K_n$ is the cyclotomic $\Gamma$-extension: if $p = 2$, $\bigcup_n K_n/K$ has galois group isomorphic to $U(\mathbf{Q}_2) \simeq \mathbf{Z}_2 \times \{1, -1\}$. We write $F$-$\mathrm{Norm}_{n/k}$ or $\mathrm{Norm}_{n/k}$ for $F$-$\mathrm{Norm}_{K_n/K_k}$ and $N_{n/k}$ for $N_{K_n/K_k}$. Further $v_{K_n} = v_n$, $A_{K_n} = A_n$.

Lemma 5.1. *Let $x \in F^t(K_n)$. Then*

$$v_{n-1}(\mathrm{Norm}_{n/n-1}(x) \geqslant \min\{[p^{-1}((m_n+1)(p-1)+t)], p^{h-1}t\}.$$

*Proof.* It follows from (2.4.2) that

$$v_{n-1}(\mathrm{Norm}_{n/n-1}(x) \geqslant \min\{[p^{-1}((m_n+1)(p-1)+t)], v_{n-1}(a_i)+ti\}.$$

Because $v_{n-1}(a_{p^{h-1}}) = 0$, we can omit $v_{n-1}(a_i) + ti$ for $i > p^{h-1}$ without changing the minimum. If $1 \leqslant i < p^{h-1}$, then $p \mid a_i$, and $v_{n-1}(a_i) + ti \geqslant p^{n-1} + ti > p^{-1}((m_n+1)(p-1)+t)$, because $m_n = 1 + p + \cdots + p^{n-1}$ and $t \geqslant 1$, $i \geqslant 1$. Q.E.D.

Lemma 5.1 shows that the numbers $[p^{-1}((m_n+1)(p-1)+t)]$, $p^{h-1}t$ are probably important in the determination of $\mathrm{Norm}_{n/0}(F(K_n))$.

### 5.2. *The Functions $\sigma_{n/k}(t)$ and $\iota_{n/k}(t)$*

We define inductively

$$\begin{aligned} \sigma_{n/n}(t) &= t,\ \sigma_{n/k}(t) = \sigma_{k+1/k}(\sigma_{n/k+1}(t)), \\ \sigma_{n/n-1}(t) &= \min\{[p^{-1}((m_n+1)(p-1)+t)], p^{h-1}t\}. \end{aligned} \tag{5.2.1}$$

It is also convenient to define

$$\begin{aligned} \sigma^0_{n/n-1}(t) &= [p^{-1}((m_n+1)(p-1)+t)], \\ \sigma^1_{n/n-1}(t) &= p^{h-1}t, \end{aligned} \tag{5.2.2}$$

and

$$\begin{aligned} \iota_{n/k}(t) &= -1 \text{ if } \sigma^0_{k/k-1}(\sigma_{n/k}(t)) \leqslant \sigma^1_{k/k-1}(\sigma_{n/k}(t)) \\ &= h-1 \text{ if } \sigma^0_{k/k-1}(\sigma_{n/k}(t)) > \sigma^1_{k/k-1}(\sigma_{n/k}(t)). \end{aligned} \tag{5.2.3}$$

It follows immediately from the definitions that if $k < n$

$$\sigma_{n/k}(t) = \min\{\sigma^0_{k+1/k}(\sigma_{n/k+1}(t)),\ \sigma^1_{k+1/k}(\sigma_{n/k+1}(t))\}. \qquad (5.2.4)$$

The function $\iota_{n/k}(t)$ indicates whether it is the value of $\sigma^0_{k/k-1}$ or $\sigma^1_{k/k-1}$ which determines $\sigma_{n/k-1}(t)$, or in other words whether in the step from $K_k$ to $K_{k-1}$ (having started in $K_n$ with an element of valuation $t$), it is $\mathrm{Tr}_{k/k-1}(\mathrm{Norm}_{n/k}(x))$ or $N^{p^{h-1}}_{k/k-1}(\mathrm{Norm}_{n/k}(x))$ for which the lower bound on the valuation is sharpest.

LEMMA 5.3.

$$\mathrm{Norm}_{n/0}(F^t(K_n)) \subset F^{\sigma_{n/0}(t)}(K).$$

This follows immediately from (5.2.1) and Lemma 5.1.

We now proceed to calculate the functions $\sigma_{n/0}(t)$. In case $h = 1$, the functions $\sigma_{n/0}(t)$ are determined by the Herbrand functions $\psi_{K_n/K}(s)$. Indeed $\psi_{K_n/K}(s) < t \leqslant \psi_{K_n/K}(s+1)$ is equivalent to $\sigma_{n/0}(t) = s + 1$.

LEMMA 5.4.

$$\iota_{n/n}(t) = -1 \leftrightarrow t \geqslant (p^n - 1)/(p^h - 1).$$

*Proof.* $\iota_{n/n}(t) = -1$ is equivalent to $\sigma^0_{n/n-1}(t) \leqslant \sigma^1_{n/n-1}(t)$; i.e., $\iota_{n/n}(t) = -1$ iff

$$\begin{aligned}
&[p^{-1}((1 + p + \cdots + p^{n-1} + 1)(p - 1) + t)] \leqslant p^{h-1}t \\
&\leftrightarrow p^{-1}((1 + p + \cdots + p^{n-1} + 1)(p - 1) + t) \leqslant p^{h-1}t + (p - 1)/p \\
&\qquad \leftrightarrow (p^n - 1) + (p - 1) + t \leqslant p^h t + (p - 1) \\
&\qquad\qquad \leftrightarrow t \geqslant (p^n - 1)/(p^h - 1).
\end{aligned}$$

LEMMA 5.5. *If $k \geqslant 2$ and $\iota_{n/k}(t) = -1$, then $\iota_{n/k-1}(t) = -1$.*

*Proof.* Let $s = \sigma_{n/k}(t)$. Then $\iota_{k/k}(s) = -1$. Let $s' = \sigma_{k/k-1}(s) = \sigma^0_{k/k-1}(s)$. We must show that $\iota_{k-1/k-1}(s') = -1$. We know that

$$s \geqslant (p^k - 1)/(p^h - 1).$$

Hence

$$\begin{aligned}
s' &= \left[\frac{(m_k + 1)(p - 1) + s}{p}\right] \geqslant \frac{m_k(p - 1)}{p} + \frac{p^k - 1}{(p^h - 1)p} \\
&= \frac{p^k - 1}{p} + \frac{p^k - 1}{(p^h - 1)p} \geqslant \frac{p^{k-1} - 1}{p^h - 1}.
\end{aligned}$$

Using (5.4), (5.5) and (4.2) it is not difficult to calculate $\sigma_{n/0}(t)$ for large enough $t$. We find the following.

LEMMA 5.6.

$$\frac{p^n-1}{p^k-1} \leqslant t \leqslant \frac{p^n-1}{p-1} \rightarrow \sigma_{n/0}(t) = n$$

$$\frac{p^n-1}{p-1} + kp^n < t \leqslant \frac{p^n-1}{p-1} + (k+1)\,p^n \rightarrow \sigma_{n/0}(t) = n+k+1.$$

Let $j_n(t)$ be the number of indices $k = n, n-1,..., 2, 1$ such that $\iota_{n/k}(t) = h-1$. In view of (5.5) we have $j_n(t) = s \geqslant 1 \leftrightarrow \iota_{n/n}(t) = h-1,..., \iota_{n/n-s+1}(t) = h-1$, $\iota_{n/n-s}(t) = -1,..., \iota_{n/1}(t) = -1$.

LEMMA 5.7.

$$j_n(t) = s \geqslant 1 \leftrightarrow \frac{p^{n-sh} - p^{s-sh}}{p^h-1} \leqslant t < \frac{p^{n-(s-1)h} - p^{(s-1)-(s-1)h}}{p^h-1},$$

$$j_n(t) = 0 \leftrightarrow \frac{p^n-1}{p^h-1} \leqslant t.$$

*Proof.* The second formula follows from (5.4) and (5.5). As to the first:

$$j_n(t) = s \geqslant 1 \leftrightarrow p^{s(h-1)}t < \left[\frac{(m_{n-s+1}+1)(p-1) + p^{(s-1)(h-1)}t}{p}\right]$$

$$\text{and } p^{(s+1)(h-1)}t \geqslant \left[\frac{(m_{n-s}+1)(p-1) + p^{s(h-1)}t}{p}\right].$$

(Use (5.5) and the fact that $\iota_{k/k}(t') = -1$ if $\iota_{k/k}(t'') = -1$ and $t' \geqslant t''$ (cf. (5.4)) and $p^{m(h-1)}t \geqslant \sigma_{n/n-m}(t)$.) The same calculations as in (5.4) now prove (5.7). Q.E.D.

PROPOSITION 5.8. *Write $n = lh + r$, with $1 \leqslant r \leqslant h$. Then we have*

$$1 \leqslant t \leqslant \frac{p^r-1}{p-1} \rightarrow \sigma_{n/0}(t) = n-l,$$

$$\frac{p^r-1}{p-1} < t \leqslant \frac{p^{r+h}-1}{p-1} \rightarrow \sigma_{n/0}(t) = n-l+1,$$

$$\frac{p^{r+kh}-1}{p-1} < t \leqslant \frac{p^{r+kh+h}-1}{p-1} \rightarrow \sigma_{n/0}(t) = n-l+k+1, \quad k = 0, 1,..., l-1,$$

$$\frac{p^n-1}{p-1} < t \leqslant \frac{p^h-1}{p-1} + p^n \rightarrow \sigma_{n/0}(t) = n+1,$$

$$\frac{p^n-1}{p-1} + kp^n < t \leqslant \frac{p^n-1}{p-1} + (k+1)\,p^n \rightarrow \sigma_{n/0}(t) = n+k+1, \quad k = 1, 2,... .$$

5.9. *Remark*

These formulas are also true if $h = \infty$; take $l = 0$, $r = n$.

COROLLARY 5.10.

$$F\text{-Norm}_{n/0}(F(K_n)) \subset F^{\alpha_n}(K),$$

*where* $\alpha_n = n - [(n-1)/h]$.

5.11. *Proof of Proposition* 5.8

Let $j_n(t) = s \geqslant 1$. Then according to (5.7)

$$\frac{p^{n-sh} - p^{s-sh}}{p^h - 1} \leqslant t < \frac{p^{n-sh+h} - p^{s-1-sh+h}}{p^h - 1}.$$

Further

$$\frac{p^{n-s} - 1}{p^h - 1} \leqslant \sigma_{n/n-s}(t) = p^{s(h-1)}t < \frac{p^{n+h-s} - p^{h-1}}{p^h - 1}.$$

We have $\iota_{n-s/n-s}(\sigma_{n/n-s}(t)) = -1$ (because $j_n(t) = s$) and we can therefore now calculate $\sigma_{n-s/0}(\sigma_{n/n-s}(t)) = \sigma_{n/0}(t)$ by means of Lemma 5.6. The result is

$$\frac{p^{n-sh} - p^{s-sh}}{p^h - 1} \leqslant t \leqslant \frac{p^{n-sh} - p^{s-sh}}{p - 1} \rightarrow \sigma_{n/0}(t) = n - s \qquad (5.11.1)$$

and

$$\frac{p^{n-sh} - p^{s-sh}}{p - 1} < t < \frac{p^{n+h-sh} - p^{s-1-sh+h}}{p^h - 1} \rightarrow \sigma_{n/0}(t) = n - s + 1. \qquad (5.11.2)$$

Because $h \geqslant 1$, we have that $0 < p^{s-sh} \leqslant 1$ for all $s = 0, 1, 2, \ldots$. It follows that

$$t \geqslant \frac{p^{n-sh} - p^{s-sh}}{p - 1} \leftrightarrow \frac{p^{n-sh} - 1}{p - 1} \leqslant t. \qquad (5.11.3)$$

Now put the formulas (5.11.2) and (5.11.1) for $s = 1, 2, \ldots, l$ together (note that $s = l + 1$ gives nothing if $n = lh + h$); use (5.11.3) and combine this with the result of (5.6). The result is Proposition 5.8.

## 6. STATEMENT OF THE THEOREM AND OUTLINE OF THE PROOF

THEOREM 6.1. *Let $F$ be a formal group over $\mathbf{Z}_p$. Let*

$$\cdots - K_n - K_{n-1} - \cdots - K_1 - K = \mathbf{Q}_p$$

*be the tower of extensions constructed in Section* 4. *(If $p > 2$, $\bigcup_n K_n$ is the* *cyclotomic $\Gamma$-extension of $\mathbf{Q}_p$: if $p = 2$ it is a slightly larger abelian totally ramified extension). Let $h = h(F) \geqslant 2$. Then we have ($n \geqslant 1$)*

$$F\text{-Norm}_{n/0}(F(K_n)) = F^{\alpha_n}(K),$$

*where $\alpha_n$ is equal to $\alpha_n = n - [(n-1)/h]$.*

*Remark* 6.2. The theorem is also true for $h = \infty$; $(n-1)/h = 0$.

6.3. *Proof of Theorem* 6.1 *in case $h = \infty$.* For each $s \geqslant n$, let

$$t_s = (p^n - 1)/(p-1) + (s-n)p^n.$$

It is not difficult to calculate $\sigma_{n/k}(t_s)$ and $\sigma_{n/k}(t_s+1)$ for $k = n-1$, $n-2, \ldots, 2, 1, 0$. One finds

$$\sigma_{n/k}(t_s) = (p^k - 1)/(p-1) + (s-n)\,p^k + (n-k)\,p^k \quad \text{for } k \geqslant 1 \text{ and } \sigma_{n/0}(t_s) = s \tag{6.3.1}$$

$$\sigma_{n/k}(t_s+1) = (p^k - 1)/(p-1) + (s-n)\,p^k + (n-k)\,p^k + 1 \quad \text{for } k \geqslant 1 \text{ and } \sigma_{n/0}(t_s+1) = s+1.$$

It is now easy to check that

$$\sigma^0_{k/k-1}(\sigma_{n/k}(t_s)) < \sigma^1_{k/k-1}(\sigma_{n/k}(t_s)). \tag{6.3.2}$$

It follows from this, (2.4.2) and (6.3.1) that the induced map

$$\text{Norm}_{k/k-1} : F^{\sigma_{n/k}(t_s)}(K_k)/F^{\sigma_{n/k}(t_s)+1}(K_k) \to F^{\sigma_{n/k-1}(t_s)}(K_{k-1})/F^{\sigma_{n/k-1}(t_s)+1}(K_{k-1}) \tag{6.3.3}$$

is equal to the map

$$\text{Tr}_{k/k-1} : \pi_k^{\sigma_{n/k}(t_s)} A_k / \pi_k^{\sigma_{n/k}(t_s)+1} A_k \to \pi_{k-1}^{\sigma_{n/k-1}(t_s)} A_{k-1} / \pi_{k-1}^{\sigma_{n/k-1}(t_s)+1} A_{k-1}\,. \tag{6.3.4}$$

This last map is surjective because

$$\sigma^0_{k/k-1}(\sigma_{n/k}(t_s) + 1) = \sigma^0_{k/k-1}(\sigma_{n/k}(t_s)) + 1,$$

and $K_k/K_{k-1}$ is totally ramified (cf. 4.2.1). It follows from this and the fact that (6.3.3) and (6.3.4) are the same maps that the map

$$\text{Norm}_{n/0} : F^{t_s}(K_n) \to F^{\sigma_{n/0}(t_s)}(K)/F^{\sigma_{n/0}(t_s)+1}(K) \tag{6.3.5}$$

is surjective. In view of Lemma 3.2 and Corollary 5.10 this concludes the proof in case $h = \infty$ because $\sigma_{n/0}(t_n) = n = \alpha_n$ if $h = \infty$.

6.4. *Idea of the proof of Theorem* 6.1 *in case $h < \infty$*. A first step in the proof of Theorem 6.1 is to show that for every $s \geqslant n - [(n-1)/h]$ there exists a $t_s$, and an element $x_s \in \pi_n A_n$ such that $v_0(\mathrm{Norm}_{n/0}(x_s)) = s$. For $s \geqslant n$ one can take $t_s = (p^n - 1)/(p-1) + (s-n)p^n$ (cf. (6.3)). Let $l = [(n-1)/h]$. For $n - l \leqslant s < n$ a natural choice of $t_s$ is

$$t_s = \frac{p^{n-(n-s)h} - 1}{p - 1}. \tag{6.4.1}$$

Then $j_n(t_s) = n - s$ (cf. (5.7)). It is easy to calculate $\sigma_{n/k}(t_s)$ for $k = n-1, n-2, \ldots, 1, 0$. The result is

$$\begin{aligned}
\sigma_{n/m}(t_s) &= p^{(n-m)(h-1)}t_s \qquad \text{for} \quad n \geqslant m \geqslant s,\\
\sigma_{n/m}(t_s) &= p^{(n-s)(h-1)}p^{-(s-m)}t_s + (s-m)p^m, \quad s \geqslant m \geqslant n-(n-s)h,\\
\sigma_{n/n-(n-s)h}(t_s) &= t_s + (n-s)(h-1)p^{n-(n-s)h},\\
\sigma_{n/m}(t_s) &= (p^m - 1)/(p-1) + (s-m)p^m, \quad n-(n-s)h \geqslant m \geqslant 0,\\
\sigma_{n/0}(t_s) &= s.
\end{aligned} \tag{6.4.2}$$

As in (6.3) it is useful to calculate also $\sigma_{n/k}(t_s + 1)$. Because $h > 1$, also $j_n(t_s + 1) = n - s$. Let $\alpha_{n/k}(t_s)$ be defined by

$$\begin{aligned}
\alpha_{n/k}(t_s) &= (n-m)(h-1), && \text{for} \quad n \geqslant m \geqslant s,\\
\alpha_{n/k}(t_s) &= (n-s)(h-1) - (s-m), && \text{for} \quad s \geqslant m \geqslant n-(n-s)h,\\
\alpha_{n/k}(t_s) &= 0, && \text{for} \quad n-(n-s)h \geqslant m \geqslant 0.
\end{aligned} \tag{6.4.3}$$

One then has

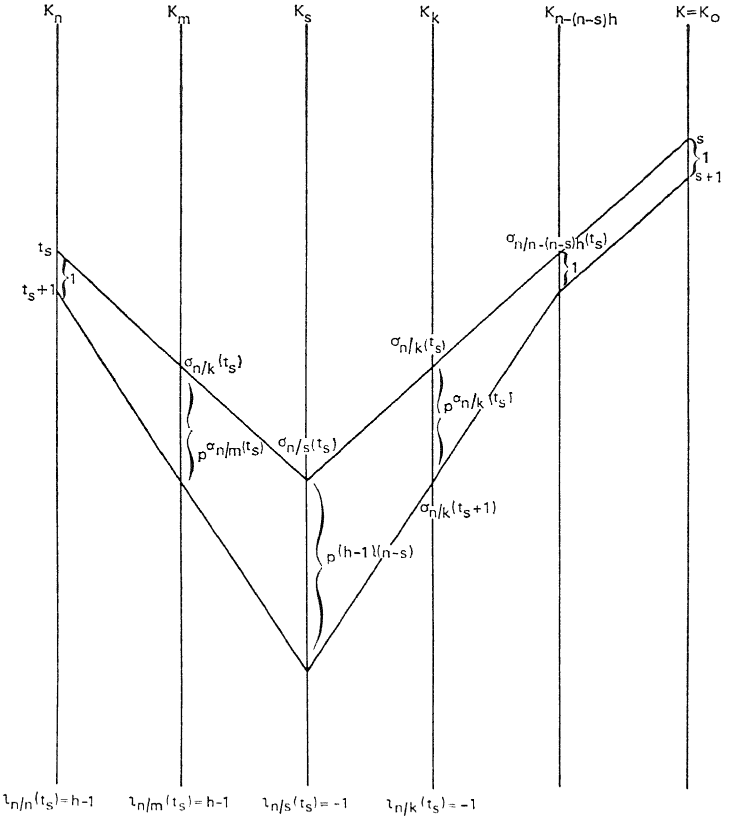
$$\sigma_{n/k}(t_s + 1) = \sigma_{n/k}(t_s) + p^{\alpha_{n/k}(t_s)}. \tag{6.4.4}$$

(In all these calculations the simple fact $\sigma^0_{k/k-1}(rp) = r + p^{k-1}$, $k \geqslant 2$ is very usefull. It follows immediately from $m_k = (1 + p + \cdots + p^{k-1})$).

A convenient picture of $\sigma_{n/k}(t_s)$ and $\sigma_{n/k}(t_s + 1)$ is sketched below.

According to Lemma 6.5, to calculate $\mathrm{Norm}_{n/k}(x) \bmod \pi_k^{\sigma_{n/k}(t_s+1)}$, where $x$ has valuation $v_n(x) = t_s$, we can disregard for all $m$, where $n \geqslant m \geqslant k$ all terms of $\mathrm{Norm}_{n/m}(x)$ of which the valuation falls below the lower line in the picture above. In Section 7 below we shall show that in fact for $x \in \pi_m A_m$

$$\mathrm{Norm}_{m/m-1}(x) \equiv N^{p^{h-1}}_{m/m-1}(x) \bmod \pi_{m-1}^{\sigma_{n/m-1}(t_s+1)}, \text{ if } v_m(x) = \sigma_{n/m}(t_s)$$
$$\text{and} \quad n \geqslant m > s \tag{6.4.5}$$




and for $x \in \pi_k A_k$

$$\mathrm{Norm}_{k/k-1}(x) \equiv \mathrm{Tr}_{k/k-1}(x) \bmod \pi_{k-1}^{\sigma_{n/k-1}(t_s+1)} \quad \text{if} \quad v_k(x) = \sigma_{n/k}(t_s)$$

$$\text{and} \quad s \geqslant k > 0. \qquad (6.4.6)$$

LEMMA 6.5. *Let* $t > t' \geqslant 1$, $\sigma_{m/k}(t) = s$, $\sigma_{m/k}(t') = s'$. *If* $x, y \in \pi_m A_m$, $v_m(x) = t$, $v_m(y) = t'$, *then*

$$\mathrm{Norm}_{m/k}(x + y) \equiv \mathrm{Norm}_{m/k}(x) \bmod \pi_k^{s'}.$$

*Proof.* Because $A_m$ is complete and (2.1.1), (2.2.1), there is an $y' \in \pi_m^{t'} A_m$ such that $x + y = x +_F y'$. Now

$$\mathrm{Norm}_{m/k}(x +_F y') = \mathrm{Norm}_{m/k}(x) +_F \mathrm{Norm}_{m/k}(y').$$

Because $\sigma_{m/k}(t') = s'$, $\mathrm{Norm}_{m/k}(y') \equiv 0 \bmod \pi_k^{s'}$. Another appeal to (2.1.1) concludes the proof.

## 7. Proof of Theorem 6.1

Proposition 7.1. *Let $F$, $K_n$, $h$, $\alpha_n$ be as in Theorem 6.1. In this section we take the uniformizing element $\pi_n$ of $K_n$ equal to $\mu_n$. Then for every $s \geqslant \alpha_n = n - [(n-1)/h]$, there is a $t_s$ such that*

(i) *$F$-$\mathrm{Norm}_{n/0}$ maps $F^{t_s}(K_n)$ into $F^s(K)$.*

(ii) *$F$-$\mathrm{Norm}_{k/0}$ maps $F^{\sigma_{n/k}(t_s+1)}(K_k)$ into $F^{s+1}(K)$ for all $0 < k \leqslant n$.*

(iii) *The induced map*

$$F^{t_s}(K_n) \to F^s(K)/F^{s+1}(K)$$

*is surjective.*

*Proof.* Let $n = lh + r$, $1 \leqslant r \leqslant h$. For $s \geqslant n$ take

$$t_s = (p^n - 1)/(p-1) + (s-n)p^n.$$

For $n - l \leqslant s < n$ take $t_s = (p^{n-(n-s)h} - 1)/(p-1)$. Parts (i) and (ii) of the proposition then follow from (6.4.2)–(6.4.4). For $s \geqslant n$ (iii) follows from (6.3) (the proof for $h = \infty$) and (6.5). Now let $n - l \leqslant s < n$. We shall first establish (6.4.5) and (6.4.6).

Let $n \geqslant j > s$. To prove (6.4.5) we must show that

$$\sigma^0_{j/j-1}(\sigma_{n/j}(t_s)) \geqslant \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)}, \tag{7.1.1}$$

$$v_{j-1}(a_i) + i\sigma_{n/j}(t_s) \geqslant \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)}, \quad i \in \mathbf{N}, \quad i \neq p^{h-1}, \tag{7.1.2}$$

where $a_i$, $i = 1, 2, \ldots$ are the coefficients appearing in formula (2.4.2) for $F$-Norm.

Now

$$\begin{aligned}\sigma^0_{j/j-1}(\sigma_{n/j}(t_s)) &= \left[\frac{(m_j+1)(p-1) + p^{(n-j)(h-1)}\,t_s}{p}\right] \\ &\geqslant p^{j-1} + p^{-1}p^{(n-j)(h-1)}\,\frac{p^{n-(n-s)h} - 1}{p-1} - \frac{1}{p},\end{aligned}$$

and

$$\begin{aligned}\sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)} &= p^{(n-j+1)(h-1)} \cdot \frac{p^{n-(n-s)h} - 1}{p-1} + p^{(n-j+1)(h-1)} \\ &= p^{h+sh-jh+j-2} + \cdots + p^{(n-j+1)(h-1)+1} + 2p^{(n-j+1)(h-1)} \\ &\leqslant p^{j-1}\end{aligned}$$

because $j-1 \geqslant (h+sh-jh+j-2)+1$ (as $j \geqslant s+1$). This proves (7.1.1). If $i$ is not a multiple of $p^{h-1}$, $v_{j-1}(a_i)+i.\ t \geqslant \sigma^0_{j/j-1}(t)$ for all $t \in \mathbf{N}$, this proves (7.1.2) for those $i \neq p^{h-1}$, which are not a multiple of $p^{h-1}$. Finally if $i \geqslant 2p^{h-1}$, then

$$\begin{aligned} v_{j-1}(a_i) + i\sigma_{n/j}(t_s) &\geqslant p^{2(h-1)}\sigma_{n/j}(t_s) \\ &\geqslant 2p^{h-1}\sigma_{n/j}(t_s) \geqslant p^{h-1}\sigma_{n/j}(t_s) + p^{h-1}\cdot p^{\alpha_{n/j}(t_s)} \\ &= p^{h-1}\sigma_{n/j}(t_s) + p^{\alpha_{n/j-1}(t_s)} \end{aligned}$$

because $\sigma_{n/j}(t_s) \geqslant p^{\alpha_{n/j}(t_s)}$. This proves (7.1.2).

To prove (6.4.6) we must show that (cf., (2.4.2)) for $s \geqslant j > 0$

$$\sigma^1_{j/j-1}(\sigma_{n/j}(t_s)) \geqslant \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)}, \tag{7.1.3}$$

$$v_{j-1}(a_i) + i\cdot t_s \geqslant \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)},\ i = 1, 2, 3, \ldots, \tag{7.1.4}$$

$$\sigma^0_{j/j-1}(2\sigma_{n/j}(t_s)) \geqslant \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)}. \tag{7.1.5}$$

First let $s \geqslant j > n-(n-s)h$. Then $\alpha_{n/j}(t_s) > 0$ and $p$ divides $\sigma_{n/j}(t_s)$ (cf. (6.4.2)). It follows that

$$\sigma^0_{j/j-1}(2\sigma_{n/j}(t_s)) = \sigma_{n/j-1}(t_s) + p^{-1}\sigma_{n/j}(t_s).$$

As $\sigma_{n/j}(t_s) \geqslant p^{\alpha_{n/j}}(t_s)$, and $\alpha_{n/j-1}(t_s) = \alpha_{n/j}(t_s) - 1$, this proves (7.1.5) for $s \geqslant j > n-(n-s)h$. If $n-(n-s)h \geqslant j > 0$, then $\sigma_{n/j}(t_s) \geqslant p$ and hence

$$\begin{aligned} \sigma_{j/j-1}(2\sigma_{n/j}(t_s)) &\geqslant \sigma_{j/j-1}(\sigma_{n/j}(t_s)) + 1 \\ &= \sigma_{n/j-1}(t_s) + 1 = \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)}. \end{aligned}$$

This proves (7.1.5). As to (7.1.4), let $i$ be not divisible by $p^{h-1}$. Then $v_{j-1}(a_i) \geqslant p^{j-1}$ and we have

$$\begin{aligned} \left[\frac{(m_j+1)(p-1)+2t}{p}\right] &\leqslant \frac{(m_j+1)(p-1)+2t}{p} \\ &= p^{j-1} + \frac{p-1}{p} + \frac{2t}{p} \leqslant p^{j-1} + it \leqslant v_{j-1}(a_i) + it \end{aligned}$$

provided $p > 2$ and $t \geqslant p$. If $p = 2$ then

$$\left[\frac{(m_j+1)(p-1)+2t}{p}\right] = 2^{j-1} + t \leqslant v_{j-1}(a_i) + it$$

for all $t \geqslant 1$. As $\sigma_{n/j}(t_s) \geqslant p$ for all $s \geqslant j > 0$ this shows that (7.1.5) implies (7.1.4) for those $i$ which are not divisible by $p^{h-1}$. If $i$ is divisible by $p^{h-1}$ (7.1.4) follows from (7.1.3) (which is the case $i = p^{h-1}$ of (7.1.4)). It therefore remains to prove (7.1.3). We have

$$\sigma^1_{j/j-1}(\sigma_{n/j}(t_s)) = p^{h-1} \cdot p^{(n-s)(h-1)} \cdot p^{-(s-j)} t_s + (s-j) p^j \cdot p^{h-1}$$

and

$$\begin{aligned}\sigma_{n/j-1}(t_s) &+ p^{\alpha_{n/j-1}(t_s)} \\ &= p^{(n-s)(h-1)} \cdot p^{-(s-j+1)} \cdot t_s + (s-j+1) p^{j-1} + p^{(n-s)(h-1)} p^{-(s-j+1)}.\end{aligned}$$

If $s > j > n-(n-s)h$, we have $(s-j)p^j p^{h-1} - (s-j+1)p^{j-1} \geqslant 3p^{j-1}$ and $(n-s)(h-1) - (s-j+1) \leqslant j-1$ because $s \geqslant n-l > n-(n/h)$. This proves (7.1.3) in this case. If $s > n-(n-s)h \geqslant j > 0$, then $\alpha_{n/j-1}(t_s) = 0$ and $(s-j)p^j p^{h-1} \geqslant (s-j+1)p^{j-1} + 1$. It remains to prove (7.1.3) in the case $s = j$. We have to prove that

$$p^{h-1} \cdot p^{(n-s)(h-1)} \cdot t_s \geqslant p^{-1} \cdot p^{(n-s)(h-1)} \cdot t_s + p^{s-1} + p^{-1} \cdot p^{(n-s)(h-1)}$$

or equivalently

$$t_s \geqslant (p^{n-(n-s)h} + 1)/(p^h - 1)$$

as $t_s = (p-1)^{-1}(p^{n-(n-s)h} - 1)$, this follows from the fact that

$$(p-1)^{-1}(p^f - 1) \geqslant (p^h - 1)^{-1}(p^f + 1)$$

if $f \geqslant 1$, and $h \geqslant 2$ and the fact that $n-(n-s)h = n - nh + sh \geqslant n - nh + (n-l)h = n - lh = r \geqslant 1$ because $s \geqslant n-l$ and $n = lh + r$, $1 \leqslant r \leqslant h$. This concludes the proof of (6.4.6).

Let $a = a_{p^{h-1}}$, the coefficient of $N^{p^{h-1}}$ in (2.4.2). Let $z \in A_0 = A_K = \mathbf{Z}_p$. According to (6.4.5) and (5.5) we have

$$\mathrm{Norm}_{n/s}(z\mu_n^{t_s}) \equiv \pm z^{p^{(n-s)h}} a^{n-s} \cdot \mu_{n-s}^{\sigma_{n/s}(t_s)} \bmod \mu_{n-s}^{\sigma_{n/s}(t_s+1)} \qquad (7.1.6)$$

(the sign is $+$ if $p > 2$, and $(-1)^{n-s}$ if $p = 2$).

For $k \leqslant s$, it is $\mathrm{Tr}_{k/k-1}$ which is the most important part of $F$-$\mathrm{Norm}_{k/k-1}$ according to (6.4.6). We wish to apply (4.5) and shall therefore need to show that for $s \geqslant k > n-(n-s)h$

$$\mathrm{Tr}_{k/k-1}(p^{s-k}\mu_k^{p^{-(s-k)}\sigma_{n/s}(t_s)}) \equiv p^{s-k+1}\mu_{k-1}^{p^{-(s-k+1)}\sigma_{n/s}(t_s)} \bmod \mu_{k-1}^{\sigma_{n/k-1}(t_s+1)}. \qquad (1.1.7)$$

(Note that $v_k(p^{s-k}) + p^{-(s-k)}\sigma_{n/s}(t_s) = \sigma_{n/k}(t_s)$ for $s \geqslant k \geqslant n-(n-s)h$; furthermore, $n-(n-s)h \geqslant r \geqslant 1$, and for $k \leqslant n-(n-s)h$, $\sigma_{n/k}(t_s)$

contains no factors $p$ so that we cannot apply (the second formula of) Lemma 4.5 for $k \leqslant n - (n-s)h$).

If $s \geqslant k > n - (n-s)k$, there is a factor $p$ in $p^{-(s-k)}\sigma_{n/s}(t_s)$ so that we can apply the second formula of Lemma 4.5. The result is that formula (7.1.7) holds modulo

$$p^{s-k} \cdot p^p \cdot \mu_{k-1}^{p^{-(s-k+1)}\sigma_{n/s}(t_s)} \cdot \mu_{k-1}^{-1} .$$

We must show that the valuation of this is larger than or equal to $\sigma_{n/k-1}(t_s)$. But $v_{k-1}(p^{s-k+1}) + p^{-(s-k+1)}\sigma_{n/s}(t_s) = \sigma_{n/k-1}(t_s)$ so that it suffices to show that

$$v_{k-1}(p^{p-1}\mu_{k-1}^{-1}) \geqslant p^{\alpha_{n/k-1}(t_s)}. \tag{7.1.8}$$

We have

$$v_{k-1}(p^{p-1}\mu_{k-1}^{-1}) \geqslant p^{k-1} - 1; \quad \alpha_{n/k-1}(t_s) = (n-s)(h-1) - (s-k+1).$$

(7.1.8) follows from this because $(k-1) - \{(n-s)(h-1) - (s-k+1) = -nh + sh + n \geqslant -nh + (n-l)h + n = n - lh = r \geqslant 1$. This proves (7.1.7).

Using (6.4.6), (7.1.6), (7.1.7), and (6.5) we now obtain, writing $l(s)$ for $n-(n-s)h$,

$$\mathrm{Norm}_{n/l(s)}(z\mu_n^{t_s}) \equiv \pm z^{p^{(n-s)h}} \cdot a^{n-s} \cdot p^{s-l(s)} \cdot \mu_{l(s)}^{t_s} \bmod \mu_{l(s)}^{\sigma_{n/l(s)}(t_s+1)} \tag{7.1.9}$$

(because $p^{-(s-l(s))}\sigma_{n/s}(t_s) = p^{-s-n+nh-sh} \cdot p^{(n-s)(h-1)}t_s = t_s$). Now

$$t_s = \frac{p^{n-(n-s)h} - 1}{p-1} = \frac{p^{l(s)} - 1}{p-1} .$$

It follows from (4.2.1) that

$$v_{l(s)-1}(\mathrm{Tr}_{l(s)/l(s)-1}(\mu_{l(s)}^{t_s})) = (p^{l(s)-1} - 1)/(p-1) + p^{l(s)-1}$$

and (using induction) one finds

$$v_0(\mathrm{Tr}_{l(s)/0}(\mu_{l(s)}^{t_s})) = l(s). \tag{7.1.10}$$

Combining this with (7.1.9) and (6.4.6) we find

$$\mathrm{Norm}_{n/0}(z\mu_n^{t_s}) \equiv \pm z^{p^{(n-s)h}} a^{n-s} p^s b \bmod p^{s+1}, \tag{7.1.11}$$

where $b$ is some elemnt of $\mathbf{Z}_p$ of valuation $v(b) = l(s)$. Part (iii) of Proposition 7.1 follows because $v(a) = 0$ and we can extract $p$-th roots in $\mathbf{Z}/(p)$.

Q.E.D.

7.2. *Proof of Theorem* (6.1). Combine (7.1) and (5.10) and use the Lemma 3.2 on filtered abelian groups.

COROLLARY 7.3 (of the proof of Theorem 6.1). *Let $L$ be an unramified algebraic extension of $\mathbf{Q}_p$; let $L_n = K_n \cdot L$ where $K_n$ is as in Theorem* 6.1. *Then Theorem* 6.1 *also holds with $K_n$ replaced by $L_n$.*

COROLLARY 7.4. *Let $L$ be an unramified algebraic extension of $\mathbf{Q}_p$, and let $\cdots - L_n - \cdots - L_1 - L$ be an extension such that there exists a finite unramified extension $K'$ of $L$ such that $L_n \cdot K' = K' \cdot K_n$. Then Theorem* 6.1 *also holds with $K_n$ replaced by $L_n$.*

*Proof.* Consider the commutative diagram

$$\begin{array}{ccc} F(L_n) & \xleftarrow{\operatorname{Norm}_{K_n'/L_n}} & F(K' \cdot L_n) = F(K_n') \\ \Big\downarrow \operatorname{Norm}_{L_n/L} & & \Big\downarrow \operatorname{Norm}_{K_n'/K'} \\ F(L) & \xleftarrow{\operatorname{Norm}_{K'/L}} & F(K') \end{array}.$$

The map $\operatorname{Norm}_{K_n'/L_n}$ is surjective according to Proposition 3.1. The image of $\operatorname{Norm}_{K_n'/K'}$ is $F^{\alpha_n}(K')$ according to (7.3). The same arguments as used to prove (3.1) in the unramified case show that $\operatorname{Norm}_{K'/L}(F^{\alpha_n}(K')) = F^{\alpha_n}(L)$.

Q.E.D.

## 8. CONCLUDING REMARKS

### 8.1. *A Counter Example*

Let $K_n$ be as in Theorem 6.1. Fix an index $i$ and consider the $\Gamma$-extension $\cdots - K_n - \cdots - K_{i+1} - K_i$ of $K_i$. It is not difficult to check that Theorem 6.1 is not true for this $\Gamma$-extension if $i$ is large enough, even if $F$ is defined over $\mathbf{Z}_p$.

### 8.2. *More General $\Gamma$-Extensions*

Let $K$ be a local field of characteristic 0 and residue characteristic $p$, and let $K_\infty/K$ be a totally ramified extension of galois group $\operatorname{Gal}(K_\infty/K) \simeq Z_p$. Let $K_n$ be the invariant field of $p^n \operatorname{Gal}(K_\infty/K)$. Let $F$ be a formal group of height $h \geqslant 2$ over $K$. For each $n$ we define

$\gamma_n$ is the smallest natural number such that $\operatorname{Norm}_{n/0}(F(K_n)) \subset F^{\gamma_n}(K)$,

$\delta_n$ is the largest natural number such that $F^{\delta_n}(K) \subset \operatorname{Norm}_{n/0}(F(K_n))$.

Then one can prove the following.

If the residue field of $K$ is algebraically closed then the differences

$$\delta_n - \frac{(h-1)}{h} ne_K \quad \text{and} \quad \gamma_n - \frac{(h-1)}{h} ne_K$$

are bounded independently of $n$ (cf. [3]).

*Remark* 8.3. In the case considered in this paper, i.e., the situation $F$-Norm: $F(K_n) \to F(K)$, where $K = \mathbf{Q}_p$, $K_n$ is the $n$-th level of the cyclotomic $\Gamma$-extension of $\mathbf{Q}_p$ and $F$ is a formal group defined over $\mathbf{Z}_p$, the cokernel of $F$-Norm depends only on the height $h$ of $F$ and the extension $K_n/K$.

Now consider the following situation

$$F\text{-Norm}: F(L) \to F(K),$$

where $K$ is the quotient field of the ring of Witt-vectors, $W(\mathbf{F}_q)$, over the finite field of $q$ elements, $\mathbf{F}_q$; where $F$ is defined over $W(\mathbf{F}_q)$ and $L/K$ is a finite (galois) extension. In this situation one can conjecture that the cokernel of $F$-Norm depends only on the reduction $F^*$ over $\mathbf{F}_q$ of $F$ and the extension $L/K$. This is certainly the case if $K = \mathbf{Z}_p$ because two formal groups over $\mathbf{Z}_p$ with isomorphic reductions are isomorphic. Moreover, in the situation described above, one can show that the image of $F$-Norm is necessarily of the form $F^i(K)$, i.e., a filtration subgroup of $F(K)$.

## References


1. A. Fröhlich, "Formal Groups," Lecture notes in mathematics 74, Springer, Berlin/New York, 1968.
2. M. Hazewinkel, Abelian extensions of local fields, Thesis, Amsterdam.
3. M. Hazewinkel, On norm maps for one dimensional formal groups. II: $\Gamma$-extensions of local fields with algebraically closed residue field, Report 7210, Econometric Institute, Rotterdam, *J. Reine Angew. Math.* (1974), to appear.
4. M. Lazard, Sur les groupes de Lie formels à un paramètre, *Bull. Soc. Math. France* **94** (1955), 251–274.
5. J. Lubin, One parameter formal lie groups over p-adic integer rings, *Ann. of Math.* **80** (1964), 464–484.
6. J. Lubin and J. Tate, Formal complex multiplication in local fields, *Ann. of Math.* **81** (1965), 380–387.
7. B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* 18 (1972), 183–266.
8. J. P. Serre, "Corps Locaux," Hermann, Paris, 1962.
9. J. Tate, "$p$-divisible Groups," Proceedings of a Conference on Local Fields held at Driebergen, ed. by T. A. Springer, Springer, Berlin–New York, 1967, 158–183.


Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.