BA

Netherlands School of Economics

ECONOMETRIC INSTITUTE

Report 7206

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

by Michiel Hazewinkel

March 19, 1972

ON NORM MAPS FOR ONE DIMENSIONAL FORMAL GROUPS [1)]
I : THE CYCLOTOMIC Γ-EXTENSION.

by Michiel Hazewinkel

Contents

1. INTRODUCTION

Let K be a finite extension of 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 G_m be the multiplicative group. Then $G_m(A_L) = U(L)$, $G_m(A_K) = U(K)$ and the map $N_{L/K}$ is : $N_{L/K}(x) =$ sum of all the conjugates of x in $G_m(L)$.

The following generalization is now natural and also interesting for various reasons (cf. [7], §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 :

1) 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.

$G(A_L) \to G(A_K)$. As in the case of $\hat{G}_m$ 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: $F(A_{L_{ur}}) \to F(A_{K_{ur}})$ 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.

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 $K = Q_p$, the p-adic numbers. Let L be the extension of Q_p obtained by adjoining all p^r-th roots of unity. $Gal(L_\infty/Q_p) = U(Q_p) \simeq \Delta \times Z_p$ where Δ is the torsion subgroup of $U(Q_p)$. Let K be the invariant field of Δ. $Gal(K_\infty/Q_p) = Z_p$, i.e. K_∞/Q_p is a Γ-extension. Let K_n be the invariant field of $p^n Gal(K_\infty/Q_p)$. We determine $Im(F(K_n) \to F(Q_p))$, where F is any formal group over Z_p of height(F) ≥ 2.

The results (and proofs) turn out to be generalizable to some extent. (Cf. [3]). The motivation to study precisely Γ-extensions came from [7].

It remains for me to thank the reviewer who thoroughly criticised 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; π_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

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

which satisfies

$$(2.1.2) \qquad F(X,F(Y,Z)) = F(F(X,Y),Z)$$

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 m_L. In fact one simply sets

$$(2.2.1) \qquad x \underset{F}{+} y = F(x,y) , \quad x, y \in m_L$$

(The series $F(x,y)$ converges in m_L). This group is denoted F(L). If $x, y \in m_L^t = \pi_L^t A_L$, $t = 1, 2, \ldots$ then $x \underset{F}{+} y \in m_L^t$. 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

$$(2.2.2) \qquad F^t(L)/F^{t+1}(L) \xrightarrow{\sim} \ell^+$$

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 $G = Gal(L/K) = \{\sigma_1, \ldots, \sigma_r\}$. We define a norm map F-Norm : $F(L) \to F(K)$ by the formula

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

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

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

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

2.3. Height of a Formal Group.

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

$$(2.3.1) \qquad F_2(X_1,X_2) = F(X_1,X_2) \ , \ \dots \ , \ F_{n+1}(X_1, \dots, X_{n+1}) = = F(F_n(X_1, \dots, X_n), X_{n+1}), \dots$$

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

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

1° There exists a number $h \in N$ such that $[p]_F(X) \equiv g(X^{p^h})$ modπ_K where $g(Z) = b_1Z + h_2Z^2 + \dots$ is a power series over A_K with $b_1 \not\equiv 0$ modπ_K. The number $h = h(F)$ is called the height of F.

2° $[p]_F(X) \equiv 0$ modπ_K. In this case one defines $h = h(F)$, the height of F, as $h = \infty$.

2.4. Lemma on F-Norm.

Let F be a formal group over A_K. If M is a monomial in $X_1, \dots, X_n$, e.g. $M = X_1^{r_1} \dots X_n^{r_n}$, we define $Tr(M) = X_1^{r_1} \dots X_n^{r_n} + X_2^{r_1} \dots X_n^{r_{n-1}} X_1^{r_n} + \dots + X_n^{r_1} X_1^{r_2} \dots X_{n-1}^{r_n}$. We write $N^i(X)$ for $X_1^i \dots X_n^i$. Using these notations one has

2.4.1. Lemma

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

where a_i, $a_M \in A_K$, and M runs through a set of monomials of total degree ≥ 2 which are not of the form $N^i(X)$.
If moreover n = p, the residue characteristic of K, then $v_K(a_i) \geq 1$ unless $i = kp^{h-1}$, k = 1, 2, ..., and $v_K(a_i) = 0$ if $i = p^{h-1}$, where h is the height of F. (If $h = \infty, v(a_i) \geq 1$ 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 Tr(M) results in something $\equiv 0$ mod 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 $Tr_{L/K}$ and $N_{L/K}$ denote the trace and norm maps. We write $N^i_{L/K}(x)$ for $(N_{L/K}(x))^i$. From the definition of F-Norm and (2.4.1) one then immediately obtains the

2.4.2. Corollary.

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

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.

3.1. Proposition.

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

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

Indeed, according to (2.2.1) and (2. 2.3) we have

$$F\text{-Norm}_{L/K}(x) \equiv Tr_{L/K}(x) \quad \mod(\pi_K^{2s})$$

and it thus suffices to select an $x \in F^s(L)$ such that $Tr_{L/K}(x) = y$ 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 Gal(L/K) is cyclic of order prime to p (cf. [8], Ch.IV, §2), it suffices to treat tamely and totally ramified extensions of prime degree ℓ, $(\ell,p) = 1$. For such extensions one has

(3.1.1) $$Tr_{L/K}(\pi_L^t A_L) = \pi_K^r A_K \ , \ r = [\frac{(\ell-1)+t}{\ell}]$$

where $[\frac{s}{\ell}]$ denotes the entier of $\frac{s}{\ell}$. (Cf. [8], Ch. V, §3)
It follows that for every $s \in N$ there exists a number t_s such that

1° $t_s > s$

2° $v_K(Tr_{L/K}(x)) > s$ if $v_L(x) > t_s$

3° $v_K(Tr_{L/K}(x)) = s$ if $v_L(x) = t_s$

It follows from this and (2.4.2) that

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

if $v_L(x) = t_s$, $z \in A_K$. Using this, (2.2.2) and 3° 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 $\text{F-Norm}_{L/K} = \text{F-Norm}_{L_{ur}/K} \circ \text{F-Norm}_{L/L_{ur}}$ 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.

3.2. Lemma.

Let A and B be abelian groups filtered by subgroups $A = A_1 \supset A_2 \supset$ $B = B_1 \supset B_2 \supset \dots$ such that $A = \varprojlim A/A_n$, and $\bigcap_n B_n = \{0\}$.

Let $u : A \to B$ be a homomorphism and suppose that there exist indices $t_1 < t_2 < \dots$ such that $u(A_{t_i}) \subset B_i$ and $u : A_{t_i} \to B_i/B_{i+1}$ is surjective for all $i = 1, 2, \dots$. Then $u : A \to B$ is surjective.

Proof. Very easy, cf. e.g. [8], Ch. V, §1, lemma 2.

4. THE CYCLOTOMIC Γ-EXTENSION.

A Γ-extension of a field K is an (infinite) galois extension K_∞/K such that $\text{Gal}(K_\infty/K) \simeq Z_p$, the p-adic integers.

4.1. The Cyclotomic Γ-Extension of Q_p.

Let Q_p be the field of p-adic numbers. Adjoin to Q_p all p^r-th roots of unity, for all r. The result is a totally ramified abelian extension L_∞/Q_p of galois group isomorphic to $U(Q_p)$. Let Δ be the torsion subgroup of $U(Q_p)$. 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_∞ be the invariant field of Δ. Then K_∞/Q_p is a Γ-extension (associated to the prime p). We shall call this extension the cyclotomic Γ-extension of Q_p. Let K_n be the invariant field of the closed subgroup $p^n\text{Gal}(K_\infty/Q_p)$. We obtain a tower of totally ramified extensions of degree p

$$\ldots - K_{n+1} - K_n - \ldots - K_2 - K_1 - Q_p = K$$

Another way to construct this Γ-extension of $K = Q_p$ for $p > 2$ is as follows. Let $f(X) = X^p + p$; Let $f^{(m)}(X)$ be the m-th iterate of $f(X)$, i.e. $f^{(m)}(X) = f^{(m-1)}(f(X))$, $f^{(o)}(X) = X$. Let $(LT)_{n+1}$ (the (n+1)-st Lubin-Tate extension of K; cf [6] or [2]) be the extension generated by any root λ_{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 $U(Q_p)/U^{n+1}(Q_p)$. (Cf. [6] or [2]; $U(Q_p)$ = units of Z_p; $U^n(Q_p) = \{u \in U(Q_p) \mid u \equiv 1 \bmod p^n\}$). The action of $u \in U(Q_p)$ is given by $\lambda_{n+1} \mapsto [u]_f(\lambda_{n+1})$, where $[u]_f(X)$ is the unique power series such that $[u]_f(X) \equiv uX$ mod(degree 2) and $[u]_f \circ f = f \circ [u]_f$. Let ζ be a (p-1)-st root of unity, then $[\zeta]_f(X) = \zeta X$, because $(\zeta X)^p + p(\zeta X) = \zeta(X^p + p)$. The element $\mu_n = \lambda_{n+1}^{p-1}$ is therefore invariant under the action of Δ. The extension $\bigcup_n Q_p(\mu_n) / Q_p$ is the cyclotomic Γ-extension of Q_p. (If p=2 one obtains in this way the whole extension L_∞/Q_2).

4.2. <u>The Number m(L/K)</u>.

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

(4.2.1) $$Tr_{L/K}(\pi_L^t A_L) = \pi_K^r A_K \text{ where } r = \left[\frac{(m(L/K) + 1)(p-1)+t}{p} \right]$$

Cf [8], Ch. IV, §2.

4.3. <u>Equations for</u> μ_n.

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

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

is the minimal polynomial of μ_n over K_{n-1}

4.4. The Numbers m_n

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

$$Tr_{n/n-1}(\mu_n) = -(p-1)p$$

(4.4.1) $$Tr_{n/n-1}(\mu_n^2) = (p-1)p^2$$

$$Tr_{n/n-1}(\mu_n^{p-1}) = (-1)^{p-1}(p-1)p^{p-1}$$

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

(4.4.2) $$m_n = 1 + p + \ldots + p^{n-1}$$

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

4.5. Trace Lemma.

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

$$Tr_{n/n-1}(\mu_n^{kp}) \equiv p\mu_{n-1}^k \mod \mu_{n-1}^{k-1}p^p, \ k = 1, 2, \ldots$$

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

(4.5.1) $$\mu_n^p + \binom{p-1}{1}\mu_n^{p-1}p + \ldots + \mu_n\binom{p-1}{p-1}p^{p-1} = \mu_{n-1}$$

Applying $Tr_{n/n-1}$ and using (4.4.1) we see that

(4.5.2) $$Tr_{n/n-1}(\mu_n^p) \equiv p\mu_{n-1} \quad \mod (p^p)$$

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 PRELIMANARY CALCULATIONS.

In this and the following sections 6, 7, $K = K_o = \mathbb{Q}_p$, and

$$\ldots - K_n - \ldots - K_1 - K$$

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 Γ-extension: if $p = 2$, $\bigcup_n K_n/K$ has galois group isomorphic to $U(\mathbb{Q}_2) \simeq \mathbb{Z}_2 \times \{1,-1\}$. We write F-$\mathrm{Norm}_{n/k}$ or $\mathrm{Norm}_{n/k}$ for F-Norm_{K_n/K_k} and $N_{n/k}$ for N_{K_n/K_k}.

Further $v_{K_n} = v_n$, $A_{K_n} = A_n$.

5.1. Lemma.

Let $x \in F^k(K_n)$. Then $v_{n-1}(\mathrm{Norm}_{n/n-1}(x) \geq \min\{[\frac{(m_n+1)(p-1)+t}{p}], p^{h-1}t\}$

Proof. It follows from (2.4.2) that

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

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 $1 \leq i < p^{h-1}$, then $p|a_i$, and $v_{n-1}(a_i) + ti \geq p^{n-1} + ti > p^{-1}(m_n+1)(p-1) + t)$, because $m_n = 1 + p + \ldots + p^{n-1}$ and $t \geq 1$, $i \geq 1$. q.e.d.

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

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

We define inductively

$$(5.2.1) \qquad \sigma_{n/n}(t) = t,\ \sigma_{n/k}(t) = \sigma_{k+1/k}(\sigma_{n/k+1}(t))$$

$$\sigma_{n/n-1}(t) = \min\{[\frac{(m_n+1)(p-1)+t}{p}], p^{h-1}t\}$$

It is also convenient to define

$$(5.2.2)\qquad \sigma^{o}_{n/n-1}(t) = \left[\frac{(m_n+1)(p-1)+t}{p}\right]$$

$$\sigma^{1}_{n/n-1}(t) = p^{h-1}t$$

and

$$(5.2.3)\qquad \iota_{n/k}(t) = -1 \text{ if } \sigma^{o}_{k/k-1}(\sigma_{n/k}(t)) \leqslant \sigma^{1}_{k/k-1}(\sigma_{n/k}(t))$$

$$= h-1 \text{ if } \sigma^{o}_{k/k-1}(\sigma_{n/k}(t)) > \sigma^{1}_{k/k-1}(\sigma_{n/k}(t))$$

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

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

The function $\iota_{n/k}(t)$ indicates whether it is the value of $\sigma^{o}_{k/k-1}$ 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 $Tr_{k/k-1}(Norm_{n/k}(x))$ or $N^{p^{h-1}}_{k/k-1}(Norm_{n/k}(x))$ for which the lower bound on the valuation is sharpest.

5.3. <u>Lemma</u>

$$Norm_{n/o}(F^{t}(K_n)) \subset F^{\sigma_{n/o}(t)}(K)$$

This follows immediately from (5.2.1) and lemma (5.1).

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

5.4. <u>Lemma</u>.

$$\iota_{n/n}(t) = -1 \iff t \geq \frac{p^n-1}{p^h-1}$$

<u>Proof</u>. $\iota_{n/n}(t) = -1$ is equivalent to $\sigma^{o}_{n/n-1}(t) \leq \sigma^{1}_{n/n-1}(t)$. I.e.

$\iota_{n/n}\ (t) = -1$ iff

$$[\frac{(1+p+\ldots+p^{n-1}+1)(p-1)+t}{p}] \leq p^{h-1}t$$

$$\Leftrightarrow \frac{(1+p+\ldots+p^{n-1}+1)(p-1)+t}{p} \leq p^{h-1}t + \frac{p-1}{p}$$

$$\Leftrightarrow (p^n-1)+(p-1)+t \leq p^h t + (p-1)$$

$$\Leftrightarrow t \geq \frac{p^n-1}{p^h-1}$$

5.5. Lemma.

If $k \geq 2$ 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 $s' = \sigma_{k/k-1}(s) = \sigma^o_{k/k-1}(s)$

We must show that $\iota_{k-1/k-1}(s') = -1$. We know that

$$s \geq \frac{p^k-1}{p^h-1}$$

Hence

$$s' = [\frac{(m_k+1)(p-1)+s}{p}] \geq \frac{m_k(p-1)}{p} + \frac{p^k-1}{(p^h-1)p} = \frac{p^k-1}{p} + \frac{p^k-1}{(p^h-1)p} \geq \frac{p^{k-1}-1}{p^h-1}$$

q.e.d.

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

We find

5.6. Lemma.

$$\frac{p^n-1}{p^k-1} \leq t \leq \frac{p^n-1}{p-1} \Rightarrow \sigma_{n/o}(t) = n$$

$$\frac{p^n-1}{p-1} + kp^n < t \leq \frac{p^n-1}{p-1} + (k+1)p^n \Rightarrow \sigma_{n/o}(t) = n + k + 1.$$

Let $j_n(t)$ be the number of indices $k = n, n-1, \ldots, 2, 1$ such that

$\iota_{n/k}(t) = h-1$. In view of (5.5) we have $j_n(t) = s \geq 1 \Leftrightarrow \iota_{n/n}(t) = h-1, \ldots, \iota_{n/n-s+1}(t) = h-1, \iota_{n/n-s}(t) = -1, \ldots, \iota_{n/1}(t) = -1$.

5.7 Lemma.

$$j_n(t) = s \geq 1 \Leftrightarrow \frac{p^{n-sh}-p^{s-sh}}{p^h-1} \leq t < \frac{p^{n-(s-1)h}-p^{(s-1)-(s-1)h}}{p^h-1}$$

$$j_n(t) = 0 \Leftrightarrow \frac{p^n-1}{p^h-1} \leq t$$

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

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

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

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

q.e.d.

5.8. Proposition.

Write $n = \ell h + r$, with $1 \leq r \leq h$. Then we have

$$1 \leq t \leq \frac{p^r-1}{p-1} \Rightarrow \sigma_{n/o}(t) = n - \ell$$

$$\frac{p^r{}_n-1}{p-1} < t \leq \frac{p^{r+h}-1}{p-1} \Rightarrow \sigma_{n/o}(t) = n - \ell + 1$$

$$\frac{p^{r+kh}}{p-1} < t \leq \frac{p^{r+kh+h}-1}{p-1} \Rightarrow \sigma_{n/o}(t) = n - \ell + k + 1,\ k = 0,1,\ldots,\ell-1$$

$$\frac{p^n-1}{p-1} < t \leq \frac{p^n-1}{p-1} + p^n \Rightarrow \sigma_{n/o}(t) = n + 1$$

$$\frac{p^n-1}{p-1} + kp^n < t \leq \frac{p^n-1}{p-1} + (k+1)p^n \Rightarrow \sigma_{n/o}(t) = n + k + 1,\ k = 1, 2, \ldots$$

5.9. Remark.

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

5.10. Corollary.

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

where $\alpha_n = n - [\frac{n-1}{h}]$

5.11. Proof of Proposition (5.8).

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

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

Further

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

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

(5.11.1) $$\frac{p^{n-sh}-p^{s-sh}}{p^h-1} \leq t \leq \frac{p^{n-sh}-p^{s-sh}}{p-1} \Rightarrow \sigma_{n/o}(t) = n - s$$

and

(5.11.2) $$\frac{p^{n-sh}-p^{s-sh}}{p-1} < t < \frac{p^{n+h-sh}-p^{s-1-sh+h}}{p^h-1} \Rightarrow \sigma_{n/o}(t) = n - s + 1$$

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

(5.11.3) $$t \geq \frac{p^{n-sh}-p^{s-sh}}{p-1} \Leftrightarrow \frac{p^{n-sh}-1}{p-1} \leqslant t$$

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

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

6.1. Theorem.

Let F be a formal group over Z_p. Let $\ldots - K_n - K_{n-1} - \ldots - K_1 - K = Q_p$ be the tower of extensions constructed in §4. (If $p > 2$, $\bigcup_n K_n$ is the cyclotomic Γ-extension of Q_p: if $p = 2$ it is a slightly larger abelian totally ramified extension). Let $h = h(F) \geq 2$. Then we have ($n \geq 1$)

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

where α_n is equal to $\alpha_n = n - [\frac{n-1}{h}]$.

6.2. Remark.

The theorem is also true for $h = \infty$; $[\frac{n-1}{h}] = 0$.

6.3. Proof of Theorem (6.1) in case $h = \infty$.

For each $s \geq n$, let $t_s = \frac{p^n-1}{p-1} + (s-n)p^n$. It is not difficult to calculate $\sigma_{n/k}(t_s)$ and $\sigma_{n/k}(t_s+1)$ for $k = n-1, n-2, \ldots, 2, 1$. One finds

$$(6.3.1)\quad \sigma_{n/k}(t_s) = \frac{p^k-1}{p-1} + (s-n)p^k + (n-k)p^k$$

$$\sigma_{n/k}(t_s+1) = \frac{p^k-1}{p-1} + (s-n)p^k + (n-k)p^k + 1$$

It is now easy to check that

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

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

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

$$\longrightarrow F^{\sigma_{n/k-1}(t_s)}(K_{k-1})/F^{\sigma_{n/k-1}(t_s)+1}(K_{k-1})$$

is equal to the map

$$(6.3.4)\quad Tr_{k/k-1} : \pi_k^{\sigma_{n/k}(t_s)} A_k / \pi_k^{\sigma_{n/k}(t_s)+1} A_k \to$$

$$\to \pi_{k-1}^{\sigma_{n/k-1}(t_s)} A_{k-1} / \pi_{k-1}^{\sigma_{n/k-1}(t_s)+1} A_{k-1}$$

This last map is surjective because $\sigma^{o}_{k/k-1}(\sigma_{n/k}(t_s) + 1) =$

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

$$(6.3.5)\qquad Norm_{n/o}: F^{t_s}(K_n) \to F^{\sigma_{n/o}(t_s)}(K)/F^{\sigma_{n/o}(t_s)+1}(K)$$

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

6.4. <u>Idea of the proof of theorem (6.1) in case $h < \infty$.</u>

A first step in the proof of theorem (6.1) is to show that for every $s \geq n - [\frac{n-1}{n}]$ there exists a t_s, and an element $x_s \in \pi_n K_n$ such that $v_o(Norm_{n/o}(x_s)) = s$. For $s \geq n$ one can take $t_s = \frac{p^n-1}{p-1} + (s-n)p^n$ (cf. (6.3)). Let $\ell = [\frac{n-1}{n}]$. For $n - \ell \leq s < n$ a natural choice of t_s is

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

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

$$\sigma_{n/m}(t_s) = p^{(n-m)(h-1)}t_s \quad \text{for} \quad n \geq m \geq s$$

$$(6.4.2)\ \sigma_{n/m}(t_s) = p^{(n-s)(h-1)}p^{-(s-m)}t_s + (s-m)p^m \quad s \geq m \geq n-(n-s)h$$

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

$$\sigma_{n/m}(t_s) = \frac{p^m-1}{p-1} + (s - m)p^m \qquad n - (n-s)h \geq m \geq 0$$

(6.4.2)

$$\sigma_{n/o}(t_s) = s$$

As in (6.3) it is usefull 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

$$\alpha_{n/k}(t_s) = (n-m)(h-1) \qquad \text{for } n \geq m \geq s$$

(6.4.3) $$\alpha_{n/k}(t_s) = (n-s)(h-1) - (s-m) \qquad \text{for } s \geq m \geq n-(n-s)h$$

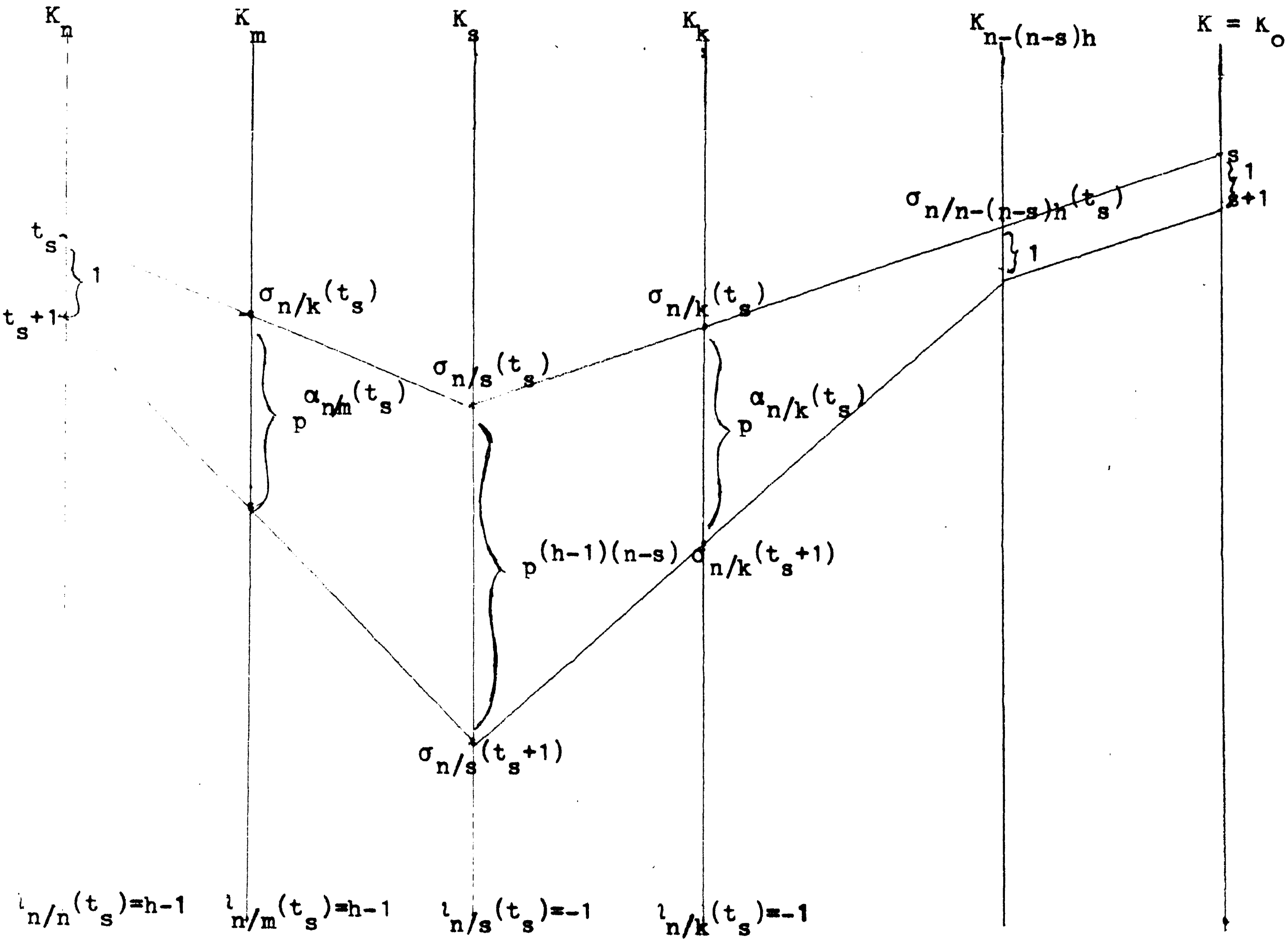
$$\alpha_{n/k}(t_s) = 0 \qquad \text{for } n-(n-s)h \geq m \geq 0$$

One then has

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

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

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



According to lemma (6.5) below 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, $n \geq m \geq k$, all terms of $\mathrm{Norm}_{n/m}(x)$ of which the valuation falls below the lower line in the picture above. In §7 below we shall show that in fact for $x \in \pi_m A_m$

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

and for $x \in \pi_k A_k$

(6.4.6) $\mathrm{Norm}_{k/k-1}(x) \equiv \mathrm{Tr}_{k/k-1}(x) \bmod \pi_{k-1}^{\sigma_{n/k-1}(t_s)}$ if $v_k(x) = \sigma_{n/k}(t_s)$ and $s \geq k > 0$

6.5. Lemma.

Let $t > t' \geq 1$, $\sigma_{m/k}(t) = s$, $\sigma_{m/k}(t') = s'$. 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).

7.1. Proposition.

Let F, K_n, h, α_n be as in theorem (6.1). Then for every $s \geq \alpha_n = n - [\frac{n-1}{h}]$, there is a t_s such that

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

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

(iii) The induced map

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

is surjective.

Proof. Let $n = \ell h + r$, $1 \leq r \leq h$. For $s \geq n$ take $t_s = \frac{p^n-1}{p-1} + (s-n)p^n$.

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

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

(7.1.1) $$\sigma^o_{j/j-1}(\sigma_{n/j}(t_s)) \geq \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)}$$

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

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

Now $$\sigma^o_{j/j-1}(\sigma_{n/j}(t_s)) = \left[\frac{(m_j+1)(p-1)+p^{(n-j)(h-1)}t_s}{p}\right] \geq$$

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

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

$$= p^{h+sh-jh+j-2} + \ldots + p^{(n-j+1)(h-1)+1} +$$

$$+ 2p^{(n-j+1)(h-1)}$$

$$\leq p^{j-1}$$

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

p^{h-1}. Finally if $i \geqq 2p^{h-1}$, then $v_{j-1}(a_i) + i\sigma_{n/j}(t_s) \geq p^{2(h-1)}\sigma_{n/j}(t_s)$ $\geqq 2p^{h-1}\sigma_{n/j}(t_s) \geq p^{h-1}\sigma_{n/j}(t_s) + p^{h-1}.p^{\alpha_{n/j}(t_s)} = p^{h-1}\sigma_{n/j}(t_s) + p^{\alpha_{n/j-1}(t_s)}$ because $\sigma_{n/j}(t_s) \geq p^{\alpha_{n/j}(t_s)}$. This proves (7.1.2).

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

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

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

(7.1.5) $$\sigma^o_{j/j-1}(2\sigma_{n/j}(t_s)) \geq \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)}$$

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

$\sigma^o_{j/j-1}(2\sigma_{n/j}(t_s)) = \sigma_{n/j-1}(t_s) + p^{-1}\sigma_{n/j}(t_s)$. As $\sigma_{n/j}(t_s) \geq p^{\alpha_{n/j}(t_s)}$, and

$\alpha_{n/j-1}(t_s) = \alpha_{n/j}(t_s) - 1$, this proves (7.1.5) for $s \geq j > n-(n-s)h$. If

$n-(n-s)h \geq j > 0$, then $\sigma_{n/j}(t_s) \geq p$ and hence $\sigma_{j/j-1}(2\sigma_{n/j}(t_s)) \geq$

$\sigma_{j/j-1}(\sigma_{n/j}(t_s)) + 1 = \sigma_{n/j-1}(t_s) + 1 = \sigma_{n/j-1}(t_s) + p^{\alpha_{n/j-1}(t_s)}$.

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

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

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

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

for all $t \geq 1$. As $\sigma_{n/j}(t_s) \geq p$ for all $s \geq j > 0$ 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

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

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

If $s > j > n-(n-s)h$, we have $(s-j)p^jp^{h-1} - (s-j+1)p^{j-1} \geq 3p^{j-1}$ and $(n-s)(h-1) - (s-j+1) \leq j-1$ because $s \geq n - \ell > n - \frac{n}{h}$. This proves (7.1.3) in this case. If $s > n-(n-s)h \geq j > 0$, then $\alpha_{n/j-1}(t_s) = 0$ and $(s-j)p^jp^{h-1} \geq$

$\geq (s-j+1)p^{j-1} + 1$. It remains to prove (7.1.3) in the case $s = j$. We have to prove that

$$p^{h-1}.p^{(n-s)(h-1)}.t_s \geq p^{-1}.p^{(n-s)(h-1)}.t_s + p^{s-1} + p^{-1}.p^{(n-s)(h-1)}$$

or equivalently

$$t_s \geq \frac{p^{n-(n-s)h}+1}{p^h-1}$$

as $t_s = (p-1)^{-1}(p^{n-(n-s)h} + 1)$, this follows from the fact that $(p-1)^{-1}(p^f-1) \geq (p^h-1)^{-1}(p^f+1)$ if $f \geq 1$, and $h \geq 2$ and the fact that $n-(n-s)h = n-nh+sh \geq n-nh+(n-\ell)h = n-\ell h = r \geq 1$ because $s \geq n - \ell$ and $n = \ell h+r$, $1 \leq r \leq h$. 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 $z \in A_o = A_K = Z_p$. According to (6.4.5) and (5.5) we have

$$\text{(7.1.6)} \quad \text{Norm}_{n/s}(z\mu_n^{t_s}) \equiv \pm z^{p^{(n-s)h}} a^{n-s}. \mu_{n-s}^{\sigma_{n/s}(t_s)} \mod \mu_{n-s}^{\sigma_{n/s}(t_s+1)}$$

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

For $k \leq s$, it is $Tr_{k/k-1}$ which is the most important part of $F\text{-}Norm_{k/k-1}$ according to (6.4.6). We wish to apply (4.5) and shall therefore need to show that for $s \geq k > n-(n-s)h$

$$(7.1.7)\quad Tr_{k/k-1}\left(p^{s-k}\mu_k^{p^{-(s-k)}\sigma_{n/s}(t_s)}\right) \equiv p^{s-k+1}\mu_{k-1}^{p^{-(s-k+1)}\sigma_{n/s}(t_s)} \mod \mu_{k-1}^{\sigma_{n/k-1}(t_s+1)}$$

(Note that $v_k(p^{s-k}) + p^{-(s-k)}\sigma_{n/s}(t_s) = \sigma_{n/k}(t_s)$ for $s \geq k \geq n-(n-s)h$; further $n-(n-s)h \geq r \geq 1$, and for $k \leq n-(n-s)h$, $\sigma_{n/k}(t_s)$ contains no factors p so that we cannot apply (the second formula of) lemma (4.5) for $k \leq n-(n-s)h$).

If $s \geq k > n-(n-s)k$, 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

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

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

$$(7.1.8)\qquad v_{k-1}(p^{p-1}\mu_{k-1}^{-1}) \geq p^{\alpha_{n/k-1}(t_s)}$$

We have

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

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

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

$$(7.1.9)\quad \mathrm{Norm}_{n/\ell(s)}(z\mu_n^{t_s}) \equiv \pm z^{p^{(n-s)h}} . a^{n-s} . p^{s-\ell(s)} . \mu_{\ell(s)}^{t_s}$$

$$\mathrm{mod}\ \mu_{\ell(s)}^{\sigma_{n/\ell(s)}(t_s+1)}$$

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

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

It follows from (4.2.1) that $v_{\ell(s)-1}(\mathrm{Tr}_{\ell(s)/\ell(s)-1}(\mu_{\ell(s)}^{t_s})) =$

$= \frac{p^{\ell(s)-1}-1}{p-1} + p^{\ell(s)-1}$ and (using induction one finds)

$$(7.1.10)\qquad v_o(\mathrm{Tr}_{\ell(s)/0}(\mu_{\ell(s)}^{t_s})) = \ell(s)$$

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

$$(7.1.11)\qquad \mathrm{Norm}_{n/o}(z\mu_n^{t_s}) \equiv \pm z^{p^{(n-s)h}} a^{n-s} p^s b \quad \mathrm{mod}\ p^{s+1}$$

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

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

7.3. Corollary (of the proof of Theorem (6.1)).

Let L be an unramified algebraic extension of $\mathbb{Q}_p$; let $L_n = K_n.L$ where K_n is as in theorem (6.1). Then theorem (6.1) also holds with K_n replaced by L_n

7.4. Corollary.

Let L be an unramified algebraic extension of $\mathbb{Q}_p$, and let $\ldots - L_n - \ldots - L_1 - L$ be an extension such that there exists a finite unramified extension K' of L such that $L_n.K' = K'.K_n$. Then theorem (6.1) also holds with K_n replaced by L_n.

Proof. Consider the commutative diagram

$$\begin{array}{ccc} F(L_n) & \xleftarrow{\ \mathrm{Norm}_{K'_n/L_n}\ } & F(K'.L_n) = F(K'_n) \\ {\scriptstyle \mathrm{Norm}_{L_n/L}} \downarrow & & \downarrow {\scriptstyle \mathrm{Norm}_{K'_n/K'}} \\ F(L) & \xleftarrow{\ \mathrm{Norm}_{K'/L}\ } & F(K') \end{array}$$

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

$\mathrm{Norm}_{K'/L}(F^{\alpha_n}(K')) = F^{\alpha_n}(L)$. 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 Γ-extension $\ldots - K_n - \ldots - K_{i+1} - K_i$ of K_i. It is not difficult to check that theorem (6.1) is not true for this Γ-extension, if i is large enough even if F is defined over Z_p.

8.2. More General Γ-Extension.

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

γ_n = smallest natural number such that $\mathrm{Norm}_{n/o}(F(K_n)) \subset F^{\gamma_n}(K)$

δ_n = largest natural number such that $F^{\delta_n}(K) \subset \mathrm{Norm}_{n/o}(F(K_n))$

Then one can prove

If the residue field of K is algebraically closed then the differences $\delta_n - \frac{(h-1)}{h} n\, e_K$ and $\gamma_n - \frac{(h-1)}{h} n\, e_K$ are bounded independently of n. (cf [3]).

REFERENCES.

[1]. Fröhlich, A (1968), Formal Groups. Lecture Notes in Mathematics 74, Springer.

[2]. Hazewinkel, M (1969), Abelian Extensions of Local Fields. Thesis, Amsterdam.

[3]. Hazewinkel, M ( ), On Norm Maps for one Dimensional Formal Groups.II: Γ-Extensions of Local Fields with Algebraically Closed Residue Field (in preparation).

[4]. Lazard, M (1955), Sur les Groupes de Lie Formels à un Paramètre. Bull. Soc. Math. France 94, 251-274.

[5]. Lubin, J (1964), One Parameter Formal Lie Groups over -adic integer Rings. Ann. of Math. 80, 464-484.

[6]. Lubin, J and J. Tate (1965), Formal Complex Multiplication in Local Fields. Ann. of Math. 81, 380-387.

[7]. Mazur, B (1969), Rational Points of Abelian Varieties with Values in Towers of Number Fields. Mimeographed, Harvard.

[8]. Serre, J.P. (1962), Corps Locaux. Hermann.

[9]. Tate, J (1967), p-divisible Groups. Proc. of a Conference on Local Fields held at Driebergen, ed. by T.A. Springer. Springer, 158-183.

Michiel Hazewinkel
Econometric Institute, Netherlands School of Economics, Burg. Oudlaan 50, ROTTERDAM-3016. The Netherlands.