Inventiones math. 53, 91 – 116 (1979)

Inventiones mathematicae

Division Values in Local Fields

Robert F. Coleman

Department of Mathematics, Princeton University, Princeton, N.J., U.S.A.

I. Introduction

In his work on cyclotomic fields Kummer observed that various formal operations on power series had number theoretic applications. Perhaps the most striking of these was Kummer's idea of taking logarithmic derivatives of p-adic numbers. After a long period of neglect, various refinements and generalizations of Kummer's idea have recently been used by Iwasawa [I_1] and Wiles [W] to study explicit reciprocity laws, and by Coates and Wiles [C] to study the arithmetic of elliptic curves with complex multiplication. Other applications of Kummer's observation include Iwasawa's explicit descriptions [I_1], [I_2] of the Galois structure of various modules connected with local cyclotomic fields. The aim of the present paper is to begin a deeper and more systematic study of the local analytic theory which underlies these relations between power series and p-adic numbers.

The central result of this paper is a general theorem on the interpolation of division values, proven in Sect. III. In Sect. IV and VI we present two important applications of this theorem which we shall now describe.

Let K be a fixed local field, i.e. a field which is complete with respect to a discrete valuation and whose residue field is finite. Let $\mathcal{O}_K$ be the ring of integers of K. Fix a local parameter π of $\mathcal{O}_K$, and let $\mathfrak{F}$ be a Lubin-Tate formal group, with endomorphism ring $\mathcal{O}_K$, which is associated with π (see [L]). For b in $\mathcal{O}_K$, we write $[b]$ for the endomorphism of $\mathfrak{F}$ given by b, and $\mathfrak{F}_n$ for the kernel of the endomorphism $[\pi^{n+1}]$. Now take H to be a fixed, complete, unramified extension of K, and let φ be the Frobenius element of the Galois group of H over K. We define the tower of fields

$$H_n = H(\mathfrak{F}_n) \quad (n = 0, 1, \ldots).$$

When $m \geqq n$, we write $N_{m,n}$ for the norm map from H_m to H_n. We now fix a generator $v = (v_n)$ of the Tate module $\varprojlim \mathfrak{F}_n$ as an $\mathcal{O}_K$-module (in other words, v_n is a generator of $\mathfrak{F}_n$ as an $\mathcal{O}_K$-module for each $n \geqq 0$, and $[\pi^{m-n}](v_m) = v_n$ for all

0020-9910/79/0053/0091/$05.20

$m \geqq n$). Let $\mathcal{O}_H$ be the ring of integers of H. As usual, we write $\mathcal{O}_H((T))$ for the ring of formal Laurent series, with finite poles, in an indeterminate T and with coefficients in $\mathcal{O}_H$. The Galois group of H over K operates on $\mathcal{O}_H((T))$ coefficientwise. Finally, if R is a ring, R^* will denote the multiplicative group of invertible elements of R. Our first application of the interpolation theorem is to coherent sequences of norms (finite or infinite). In particular we prove:

Theorem A. *Let $\alpha=(\alpha_n)$ be an element of $\varprojlim H_n^*$, where the inverse limit is taken with respect to the norm maps. Then there exists a unique power series $f_\alpha(T)$ in $\mathcal{O}^H((T))^*$ satisfying*

$$(\varphi^{-n} f_\alpha)(v_n)=\alpha_n \quad \text{for all } n \geqq 0.$$

The uniqueness of $f_\alpha(T)$ is obvious from the Weierstrass preparation theorem. The non-trivial part of the proof of Theorem A is establishing the existence of $f_\alpha(T)$. In the special case $H=K=\mathbb{Q}_p$, Theorem A plays a fundamental role in the paper [C], where an ad hoc proof of it is given.

Now assume that H is finite over K. Let λ be the logarithm map of the Lubin-Tate group $\mathfrak{F}$. If we write $\mathfrak{p}_n$ for the maximal ideal of the ring of integers of H_n, it is well known that λ converges on $\mathfrak{p}_n$. Let $T_{n/K}$ denote the trace map from H_n to K. We then define

$$\mathfrak{X}_n=\{a \in H_n\colon T_n(a\lambda(b)) \in \mathcal{O}_K \text{ for all } b \text{ in } \mathfrak{p}_n\}.$$

If $m \geqq n$, it is plain that the trace map $T_{m,n}$ from H_m to H_n maps $\mathfrak{X}_m$ into $\mathfrak{X}_n$. Our second application of the interpolation theorem is to coherent sequences of traces in $\mathfrak{X}_n$. By means of this result we are able to give a characterization of elements of $\mathfrak{X}_n$ which does not depend on λ. We also obtain:

Theorem B. *Let $\alpha=(\alpha_n)$ be an element of $\mathfrak{X}_\infty=\varprojlim \mathfrak{X}_n$, where the inverse limit is taken with respect to the trace maps. Then there exists a unique power series $g_\alpha(T)$ in $\mathcal{O}_H((T))$ satisfying*

$$\pi^{-(n+1)}(\varphi^{-n} g_\alpha)(v_n)=\alpha_n \quad \text{for all } n \geqq 0.$$

Conversely, suppose that a power series $g(T)$ in $\mathcal{O}_H((T))$ has the property that

$$T_{m,n}(g(v_m))=\pi^{m-n}(\varphi^{m-n} g)(v_n)$$

for all $m \geqq n$. Put $\alpha_n=\pi^{-(n+1)}(\varphi^{-n} g)(v_n)$ for each $n \geqq 0$. Then $\alpha=(\alpha_n)$ belongs to $\varprojlim \mathfrak{X}_n$.

In another paper, in which we will discuss Kummer's logarithmic derivative in detail, we will explain the connection between these results and the explicit reciprocity laws of Wiles. (See the remarks at the end of Sect. VI for further comments.) We also point out that, using Theorem 15 of this paper (which is a stronger version of Theorem A) one can prove in a constructive manner, the following fact, which, previously, was only obtainable indirectly via class field theory. Let $d=[H:K]$.

Proposition. *Let $m \geqq n \geqq 0$, and let $\beta \in H_n^*$. Then $\beta \in N_{m,n}(H_m^*)$ if and only if $N_{n/K}(\beta) \in (\pi^d)(1+\pi^{m+1}\mathcal{O}_K)$. Moreover, $N_{n/K}(H_n^*) = (\pi^d)(1+\pi^{n+1}\mathcal{O}_K)$.*

This proposition, however, will not be proven here.

I would like to thank John Coates for his encouragement and help throughout the preparation of this paper.

Notation. Throughout, K will be a fixed local field, and Ω will denote a fixed completion of the algebraic closure of K. All extensions of K will be assumed to lie in Ω. Let L be any such extension of K, and $\mathcal{O}_L$ the ring of integers of L. As usual, $L((T))$ and $L[[T]]$ will denote the field of formal Laurent series in T with coefficients in L and poles of finite order at zero, and the subring consisting of formal series without poles, respectively. The rings $\mathcal{O}_L((T))$ and $\mathcal{O}_L[[T]]$ are defined in a similar manner.

We write $|\ |$ for the absolute value on Ω, normalized so that $|a| = q^{-1}$, where a is any parameter of K and q is the order of the residue field of K. Let B denote the open ball of radius one with center the origin in Ω, and let B' be this open ball with the origin deleted. We write

$$L((T))_1$$

for the subset of $L((T))$ consisting of all power series which converge on B'. We shall always assume that $L((T))_1$ is endowed with the "compact-open" topology with respect to B'. In other words, a sequence $\{f_n\}$ in $L((T))_1$ converges to f if and only if, for each closed annulus A around zero in B', and for each $\varepsilon > 0$, there exists a positive integer $N = N(A, \varepsilon)$ such that $|f_n(a) - f(a)| < \varepsilon$ for all a in A and all $n \geqq N$. It is easy to see that, if $\{f_n\}$ converges to f, then the individual coefficients of the power series f_n converge in L to those of f. We recall several well known facts about power series in $L((T))_1$, when viewed as analytic functions. First, if $f = \sum_{i=-\infty}^{\infty} a_i \cdot T^i$ is any element of $L((T))_1$ then for $r = q^{-a}$, where a is a positive rational, we have,

$$\sup_{\substack{|x|=r \\ x \in \Omega}} |f(x)| = \sup_{n=0,1,\ldots} |a_n| \cdot r^n.$$

Second, elements of $L((T))_1$, satisfy the maximum principle, i.e. for any $f \in L((T))_1$ the maximum of f on any set of the form $\{x \in \Omega\colon q^{-a} \leqq |x| \leqq q^{-b}\}$, where $a > b$ are positive rationals, is attained on the set $\{x \in \Omega\colon |x| = q^{-a} \text{ or } |x| = q^{-b}\}$. Given positive reals r and ε, with $r < 1$, we define $S_L(r, \varepsilon)$ to be the set of all f in $L((T))_1$ such that $|f(x)| < \varepsilon$ for all x in Ω with $|x| = r$. It follows from the maximum principle that the $S_L(r, \varepsilon)$ form a sub-basis of neighborhoods of the origin in $L((T))_1$. Finally, if L is a complete subfield of Ω then $L[[T]]_1$ is a complete topological subgroup of $L((T))_1$, where $L[[T]]_1$ denotes $L((T))_1 \cap L[[T]]_1$ endowed with the restriction topology from $L((T))_1$.

We will have several occasions to take inverse limits of objects indexed by the non-negative integers. Therefore, we adopt the following notation: If $\{A_n, \gamma_{m,n}\}_{0 \leqq n \leqq m}$ is an inverse system, we let $\gamma_{\infty,m}$ denote the natural map from $\varprojlim A_n$ to A_m. If $a \in \varprojlim A_n$ we set $a_m = \gamma_{\infty,m}(a)$.

II. A Galois Structure on $H((T))_1$

Let K be as in the introduction. We shall study Lubin-Tate formal groups, with endomorphism ring $\mathcal{O}_K$. For a detailed discussion of these, see [L]. We simply recall that they arise in the following manner. Fix a local parameter π in $\mathcal{O}_K$. Let $\mathcal{G}_\pi$ denote the set of all formal power series $f(T)$ in $\mathcal{O}_K[[T]]$ satisfying (i) $f(T) \equiv \pi T \bmod$ degree 2, and (ii) $f(T) \equiv T^q \bmod \pi\mathcal{O}_K$. For each f in $\mathcal{G}_\pi$, there exists a unique formal group law $\mathfrak{F}_f(X, Y)$ in $\mathcal{O}_K[[X, Y]]$ such that $\mathfrak{F}_f(f(X), f(Y)) = f(\mathfrak{F}_f(X, Y))$. The endomorphism ring of $\mathfrak{F}_f$ is naturally isomorphic to $\mathcal{O}_K$. As usual, we write $[a] = [a]_{\mathfrak{F}_f}$ for the formal power series giving the endomorphism of $\mathfrak{F}_f$ corresponding to $a \in \mathcal{O}_K$. In particular, $[\pi] = f$. Finally, if f and g are any two elements of $\mathcal{G}_\pi$, the formal groups $\mathfrak{F}_f$, $\mathfrak{F}_g$ are isomorphic over $\mathcal{O}_K$. From now on, we fix one of these Lubin-Tate formal groups associated with π and K, and denote it simply by $\mathfrak{F}$.

As in the introduction we let $\mathfrak{F}_n$ denote the kernel of the endomorphism $[\pi^{n+1}]$ of $\mathfrak{F}$. Let H denote a fixed complete (not necessarily finite), unramified extension of K. We put

$$H_n = H(\mathfrak{F}_n), \qquad H_\infty = \bigcup_{n \geqq 0} H_n.$$

Let G_n be the Galois group of H_n over H, and G_∞ the Galois group of H_∞ over H. The action of G_∞ on $\mathfrak{F}_\infty = \bigcup_{n \geqq 0} \mathfrak{F}_n$ gives rise to a continuous homomorphism

$$\kappa\colon G_\infty \to U_K, \tag{1}$$

defined by $\sigma(u) = [\kappa(\sigma)](u)$ for all σ in G_∞ and u in $\mathfrak{F}_\infty$; here U_K denotes the group of units of $\mathcal{O}_K$. By Lubin-Tate Theory, κ is, in fact, an isomorphism. Write $R_n = \mathcal{O}_H[G_n]$ for the group ring of G_n with coefficients in $\mathcal{O}_H$. Let $R_\infty = \varprojlim R_n$, the projective limit being taken with respect to the restriction maps. Intuitively, R_∞ may be viewed as the continuous analogue of the ordinary group ring $\mathcal{O}_H[G_\infty]$. There is a natural injection of $\mathcal{O}_H[G_\infty]$ into R_∞, and we identify $\mathcal{O}_H[G_\infty]$ with its image under this injection. Of course, R_∞ is endowed with the natural topology, arising from viewing each R_n as the product of an appropriate number of copies of $\mathcal{O}_H$. Relative to this topology, $\mathcal{O}_H[G_\infty]$ is a dense subset of R_∞.

The general philosophy behind our work is to translate problems about the arithmetic of the field H_∞ into problems about the structure of the power series ring $H((T))_1$. One of the main benefits of this translation is that it enables us to use differentiation to study the arithmetic of H_∞. As mentioned in the Introduction, the origins of this idea go back to Kummer's work on cyclotomic fields. The following result is of fundamental importance for this translation.

Theorem 1. *There exists a unique, continuous, R_∞-module structure on $H((T))_1$ such that, for all f in $H((T))_1$, we have*

$$\sigma(f) = f \circ [\kappa(\sigma)], \qquad a(f) = a \cdot f, \tag{2}$$

for all σ in G_∞ and all a in $\mathcal{O}_K$.

For the proof we will need the following technical result:

Given $f \in H((T))_1$, we define V_f to be the set of all $g \in H((T))_1$ such that $|g(x)| < \sup_{|y|=|x|} |f(y)|$ for all $x \in B'$. Plainly f belongs to V_f. Also let P_m denote the projection from $H((T))_1$ to itself given by associating to a Laurent series, its terms of degree $<m$. This map is obviously continuous and, by the remarks in the introduction, carries V_f into itself.

Lemma 2. *Suppose $f \in H((T))_1$. Then,* (i) *if $f \in S_H(r, \varepsilon)$ for positive reals r and ε, with $r<1$, then $V_f \subseteq S_H(r, \varepsilon)$.* (ii) *$V_f$ is a complete subspace of $H((T))_1$.* (iii) *If g belongs to $T\mathcal{O}_H[[T]]$, and the coefficient of T in g is a unit in $\mathcal{O}_H$, then $f \circ g \in V_f$.* (iv) *If $\{g_i\}$ is a sequence of elements of V_f then $\lim_{i \to \infty} P_m(g_i) = 0$ for all integers m if and only if $\lim_{i \to \infty} g_i = 0$.*

Proof. Part (i) follows immediately from the definitions.

It is clear that V_f is a closed subspace of $H((T))_1$. Moreover, it is easy to see that V_f is contained in $T^{-N} \cdot H[[T]]_1$, if f is. Since the latter space is complete, (ii) follows. Next, (iii) is an immediate consequence of the fact that g determines an isometry of B'. Finally, for (iv), it is clear from the above that $g_i - P_m(g_i)$ belongs to V_f, so (iv) will follow easily from the assertion: For positive reals r and ε, $r<1$, there exists a positive integer $N = N(f, r, \varepsilon)$ such that $V_f \cap T^N H[[T]]_1 \subseteq S_H(r, \varepsilon)$. This in turn follows from the assertion: For positive reals r and ε, with $r = q^{-a}$, where a is a positive rational, we have, $S_H(r, \varepsilon) \cap T^m H[[T]]_1 \subseteq S_H(s, \varepsilon(s/r)^m)$ for positive real $s<r$. But this is an easy consequence of the maximum principle.

We also need:

Lemma 2a. *Let $\{a_i\}_{i=1}^{\infty}$ be a sequence of distinct elements of B' such that $\prod_{i=1}^{\infty} a_i = 0$ and let $\{g_n\}_{i=1}^{\infty}$ be a sequence of elements of $\mathcal{O}_\Omega[[T]]$. Then if $\lim_{n \to \infty} g_n(a_i) = 0$ for all $i \geqq 1$, it follows that $\lim_{n \to \infty} g_n = 0$ in $\Omega((T))_1$.*

Proof. Suppose that $\{g_n\}$ does not converge to zero. Then we claim that without loss of generality we may suppose that $|g_n(0)| > \delta$ for some positive real δ, and for all $n \geqq 1$. Indeed, since all the g_n lie in $\mathcal{O}_\Omega[[T]]$, there must exist a smallest k such that $c_{n,k}$ does not converge to zero, where $c_{n,k}$ is the coefficient of T^k in g_n. The conditions of the lemma do not change it we replace g_n by $T^{-k}(g_n - P_k(g_n))$. Our claim is then established by choosing an appropriate subsequence of $\{g_n\}$.

The lemma will follow from the following assertion: Set $A_m = \prod_{i=1}^{m} |a_i| \cdot \prod_{i=1}^{m} |(a_i - a_j)|$ and let $f \in \mathcal{O}_\Omega[[T]]$. Then, if $|f(a_i)| < A_m$, for $1 \leqq i \leqq m$, we have $|f(0)| < \prod_{i=1}^{m} |a_i|$. We prove this assertion by induction on m. If $m=1$ then $|a_1| = A_1 > |f(a_1)| = |f(0) + (f(a_1) - f(0))|$, so as $|f(a_1) - f(0)| < |a_1|$, the assertion follows in this case. Now suppose the assertion true for $m \geqq 1$. Expand f around a_{m+1} so that $f(T) = f(a_{m+1}) + (T - a_{m+1}) g(T)$ for some $g \in \mathcal{O}_\Omega[[T]]$. Evaluating this expression at a_i and using the hypothesis that $|f(a_i)| < A_{m+1}$, for

all $1 \leqq i \leqq m+1$, we find

$$|a_i - a_{m+1}| \cdot |g(a_i)| < A_{m+1}$$

for $1 \leqq i \leqq m$. Since $|a_j| < 1$ and $a_i \neq a_{m+1}$, for $i, j \leqq m+1$, $i \neq m+1$, it follows that

$$g(a_i) < A_{m+1}(|a_i - a_{m+1}|)^{-1} < A_m$$

for all $1 \leqq i \leqq m$. Thus by induction $|g(0)| < \prod_{i=1}^{m} |a_i|$. Therefore $|f(0)| = |f(a_{m+1}) - a_{m+1} \cdot g(0)| < \prod_{i=1}^{m+1} |a_i|$ as asserted.

Let $\mathfrak{F}_n' = \{u \in \mathfrak{F}_n : u \neq 0\}$, for all $0 \leqq n \leqq \infty$. Since $\prod_{u \in \mathfrak{F}_\infty} u = 0$, Lemma 2a has the following consequence, which will play an important role in the rest of the paper.

Uniqueness Principle. *If f and g are in $\mathcal{O}_H((T))$ and $f(u) = g(u)$ for all $u \in \mathfrak{F}_\infty'$ then $f = g$.*

Proof of Theorem 1. To simplify notation in the proof, we put $M = H((T))_1$. It follows from (iii) of Lemma 2 that $f \circ [\kappa(\sigma)]$ also belongs to M. Thus (2) defines an $\mathcal{O}_H[G_\infty]$-module structure on M, whence the uniqueness is plain, because $\mathcal{O}_H[G_\infty]$ is dense in R_∞.

We now turn to existence. We conclude from (iii) of Lemma 2 that ωf lies in V_f, for all ω in $\mathcal{O}_H[G_\infty]$. Since V_f is a complete subspace of M, if we can show that

$$\lim_{i \to \infty} \omega_i f = 0, \tag{4}$$

for any sequence $\{\omega_i\}$ of elements of $\mathcal{O}_H[G_\infty]$ such that $\lim_{i \to \infty} \omega_i = 0$, and for any f in M, then we will be able to extend the map $\omega \mapsto \omega f$ by continuity to a continuous map from R_∞ into V_f. This will give the desired action of R_∞ on M. Suppose for the moment that we have already established (4). To show that the map $R_\infty \times M \to M$, given by $(\omega, f) \mapsto \omega f$, is continuous, we need only verify that

$$\lim_{i \to \infty} \omega_i f_i = 0, \tag{5}$$

for any sequence (ω_i, f_i) in $R_\infty \times M$ such that $\lim_{i \to \infty} (\omega_i, f_i) = (\omega, 0)$ or $(0, f)$, for some $\omega \in R_\infty$ or $f \in M$. In the first case, $\lim_{i \to \infty} f_i = 0$, and since $\omega_i f_i \in V_{f_i}$ for all i, (5) follows from (i) of Lemma 2. In the second case, what we have just shown implies that $\lim_{i \to \infty} \omega_i (f_i - f) = 0$, and so (5) follows from the continuity of the map $\omega \mapsto \omega f$.

Thus, to complete the proof, we must establish (4). Suppose first that $f \in \mathcal{O}_H((T))$. Now R_∞ acts continuously on the additive group of H_∞ in the natural way. Thus $\lim_{i \to \infty} \omega_i(b) = 0$ for all $b \in H_\infty$. Taking $b = f(u)$, where u is any non-zero element of $\mathfrak{F}_\infty$, we conclude that $\lim_{i \to \infty} \omega_i(f(u)) = 0$. But $\omega_i(f(u)) = (\omega_i f)(u)$, be-

cause $\sigma(u)=[\kappa(\sigma)](u)$ for all σ in G_∞. From this and Lemma 2a, (4) follows in this case. Clearly this also implies that (4) holds for all f in $c.\ \mathcal{O}_H((T))$, where c is any element of H.

Now, for each integer $m\geqq 0$, there exists a $c_m\neq 0$ in H such that $P_m(f)$ is in $c_m\cdot\mathcal{O}_H((T))$. Thus, by what we have already shown $\lim_{i\to\infty}\omega_i(P_m(f))=0$. But, it is easy to see that for any ω in $\mathcal{O}_H[G_\infty]$, we have $P_m(\omega f)=P_m(\omega P_m(f))$. Therefore, the above equation implies that $\operatorname{Lim}_{i\to\infty}P_m(\omega_i f)=0$. This together with Lemma 2 (iv) establishes (4), and the proof of the theorem is complete.

From now on, we shall always consider $H((T))_1$ as being endowed with the R_∞-module structure given by Theorem 1. Plainly, $H[[T]]_1$, $\mathcal{O}_H((T))$ and $\mathcal{O}_H[[T]]$ are then R_∞-submodules of $H((T))_1$.

III. The Trace Operator

We use the same notation as in the previous sections. In particular, H denotes an arbitrary complete, unramified extension of K, and $H_n=H(\mathfrak{F}_n)$, $(n=0,1\ldots)$. For brevity, we write $\mathcal{O}_n$ for the ring of integers of H_n, and $\mathfrak{p}_n$ for the maximal ideal of $\mathcal{O}_n$.

We denote the sum of two elements X and Y under the formal group law of $\mathfrak{F}$ by $X[+]Y$. For $f\in H((T))_1$, n a positive integer, $u\in\mathfrak{F}_\infty$ we define the elements f_{π^n} and ${}_uf$ of $H_0((T))$ by

$$f_{\pi^n}=f\circ[\pi^n],\qquad {}_uf(T)=f(T[+]u).$$

(Note that these elements are not necessarily in $H_0((T))_1$.)

As in the introduction, let $v=(v_n)$ be a generator for the Tate-module of $\mathfrak{F}$ as an $\mathcal{O}_K$-module.

Lemma 3. *If $f\in\mathcal{O}_H[[T]]$ and ${}_uf=f$ for all $u\in\mathfrak{F}_0$ then there exists a unique $g\in\mathcal{O}_H[[T]]$ such that $g_\pi=f$.*

Proof. Uniqueness is obvious since $[\pi]$ has a power series inverse in $H[[T]]$.

Now, suppose we have constructed a_i in $\mathcal{O}_H$ for $0\leqq i\leqq n-1$ so that

$$[\pi]^n\cdot f_n=f-\sum_{i=0}^{n-1}a_i[\pi]^i \tag{1}$$

for some $f_n\in\mathcal{O}_H[[T]]$ (this is trivial for $n=0$). Then as ${}_uf=f$ and ${}_u[\pi]=[\pi]$, for all $u\in\mathfrak{F}_0$, it follows that ${}_uf_n=f_n$. But then $(f_n-f_n(0))(u)=0$ for all u in $\mathfrak{F}_0$, so by Weierstrass preparation there exists an $f_{n+1}\in\mathcal{O}_H[[T]]$ such that $f_n=f_n(0)+[\pi]\cdot f_{n+1}$. Therefore we may set $a_n=f_n(0)$ and obtain (1) for $n+1$. In this manner we may construct a sequence $\{a_i\}$ of elements of $\mathcal{O}_H$ such that

$$f-\sum_{i=0}^{\infty}a_i[\pi]^i\in\bigcap_{n\geqq 0}[\pi]^n\mathcal{O}_H[[T]]=(0).$$

Setting $g=\sum_{i=0}^{\infty}a_iT^i$ we complete the proof of the lemma.

Theorem 4. *There exists a unique map* $\mathscr{S}$: $H((T))_1 \to H((T))_1$ *such that*

$$\mathscr{S}(f)_\pi = \sum_{u \in \mathfrak{F}_0} {}_u f. \tag{2}$$

Moreover, $\mathscr{S}$ *is continuous.*

Proof. As in Lemma 3 the uniqueness is plain.

For $f \in H((T))_1$ let $\mathscr{T}(f) = \sum_{u \in \mathfrak{F}_0} {}_u f$; $\mathscr{T}(f)$ is then in $H((T))$.

To prove the existence of $\mathscr{S}$, first suppose $f \in \mathcal{O}_H[[T]]$. It follows that $\mathscr{T}(f) \in \mathcal{O}_H[[T]]$ and that ${}_u\mathscr{T}(f) = \mathscr{T}(f)$ for all $u \in \mathfrak{F}_0$. Hence, by Lemma 3, $\mathscr{T}(f) = g_\pi$ for a unique $g \in \mathcal{O}_H[[T]]$. We set $\mathscr{S}(f) = g$ in this case. This defines $\mathscr{S}$ on $\mathcal{O}_H[[T]]$. It is clear that $\mathscr{S}$ is $\mathcal{O}_H$-linear, has its image in $\mathcal{O}_H[[T]]$ and satisfies (2). Therefore, we may extend $\mathscr{S}$ H-linearly to $H \otimes \mathcal{O}^H[[T]]$. Its image is then contained in $H[[T]]_1 = H((T))_1 \cap H[[T]]$ and (2) holds. Since $H \otimes \mathcal{O}_H[[T]]$ is dense in $H[[T]]_1$, if we verify that $\mathscr{S}$ is continuous on this set, then we may extend it by continuity to all of $H[[T]]_1$. (We use here that $H[[T]]_1$ is a complete topological group.) It follows immediately that $\mathscr{S}$ will be continuous, and since $\mathscr{T}$ is evidently continuous, that (2) will hold.

Since $\mathscr{S}$ is H-linear on $H \otimes \mathcal{O}_H[[T]]$ we need only verify continuity at the origin. Let r, ε be positive real numbers with $q^{-(q-1)^{-1}} < r < 1$. It suffices to show: If $f \in S_H(r, \varepsilon) \cap H \otimes \mathcal{O}_H[[T]]$ then $\mathscr{S}(f) \in S_H(r^q, \varepsilon)$. It is clear that ${}_u f$ is in $S_{H^0}(r, \varepsilon)$ if $u \in \mathfrak{F}_0$, since then $|u| < q^{-(q-1)^{-1}}$. Thus $\mathscr{T}(f)$ belongs to $S_H(r, \varepsilon)$. Also, if B_t denotes the ball of radius t around the origin in Ω, then it is easy to see that $[\pi](B_r) = B_{r^q}$. Hence as $\mathscr{S}(f) \in H[[T]]_1$ and satisfies (2) we have: $\mathscr{S}(f)(B_{r^q}) = \mathscr{T}(f)(B_r)$; and the above assertion follows immediately. Therefore, we may extend $\mathscr{S}$ to all of $H[[T]]_1$.

It remains to define $\mathscr{S}$ for f arbitrary in $H((T))_1$. However, if $f \in H((T))_1$, there exists a suitably large positive integer N such that $[\pi]^N \cdot f \in H[[T]]_1$. We then set

$$\mathscr{S}(f) = T^{-N} \mathscr{S}([\pi]^N \cdot f).$$

It is clear that $\mathscr{S}$ will now satisfy the requirements of the theorem.

Recall (cf. Theorem 1) that $H((T))_1$ has a canonical structure as an R_∞-module. If $m \geqq n$, $T_{m,n}$ denotes the trace map from H_m to H_n; also recall, $\mathfrak{F}_n' = \mathfrak{F}_n - \{0\}$, for $0 \leqq n \leqq \infty$.

Corollary 5. *The map* $\mathscr{S}$ *is a continuous* R_∞*-endomorphism of* $H((T))_1$*, which leaves invariant the submodules* $H[[T]]_1$, $\mathcal{O}_H((T))$ *and* $\mathcal{O}_H[[T]]$. *Moreover, for all* f *in* $H((T))_1$, *we have* (i) $\mathscr{S}(f)(v_n) = T_{n+1,n}(f(v_{n+1}))$ *for all* $n \geqq 0$; (ii) $\sum_{u \in \mathfrak{F}_{n-1}'} f(u) = (\mathscr{S}^n(f)_{\pi^n} - f)(0)$, $n < \infty$.

Proof. It is clear from the proof of Theorem 4 that $\mathscr{S}$ leaves invariant $\mathcal{O}_H((T))$, $\mathcal{O}_H[[T]]$, and $H[[T]]_1$.

Now

$$\sigma \mathscr{S}(f)_\pi = \sigma \sum_{v \in \mathfrak{F}_0} {}_v f = \sum_{v \in \mathfrak{F}_0} {}_{\sigma^{-1}(v)} \sigma f = \sum_{v \in \mathfrak{F}_0} {}_v \sigma f = \mathscr{S}(\sigma f)_\pi.$$

Thus $\sigma\mathscr{S}(f)=\mathscr{S}(\sigma f)$. Also, $\mathscr{S}$ is obviously H-linear, *a fortiori* $\mathcal{O}_H$-linear, and so it follows from the continuity of $\mathscr{S}$ that $\mathscr{S}$ is an R_∞-homomorphism.

(i) follows immediately from (2) since the conjugates of $f(v_n)$ over H_{n-1} are precisely the elements $f(v_n[+]u)$ of H_n, for $u\in\mathfrak{F}_0$.

By iterating (2) we obtain

$$\mathscr{S}^n(f)_{\pi^n}=\sum_{u\in\mathfrak{F}_{n-1}} {}_uf.$$

If we subtract f from both sides of this expression we cancel the pole and hence we may evaluate at zero to obtain (ii).

The trace operator also enjoys the following congruence property:

Lemma 6. *If* $f\in\mathcal{O}_H((T))$ *then*

$$\mathscr{S}^n(f)\equiv 0 \bmod \pi^n\mathcal{O}_H((T)).$$

Proof. The lemma follows easily from the case $n=1$ using induction and the $\mathcal{O}_H$-linearity of $\mathscr{S}$.

First suppose $f\in\mathcal{O}_H[[T]]$. Then since $f_\pi\equiv f(T^q) \bmod \pi$ and ${}_uf\equiv f \bmod \mathfrak{p}_0$ it follows from (2) that

$$\mathscr{S}(f)(T^q)\equiv q\cdot f\equiv 0 \bmod \mathfrak{p}_0$$

and hence mod π since the left hand side is in $\mathcal{O}_H[[T]]$. This implies the lemma for $f\in\mathcal{O}_H[[T]]$. Now suppose f arbitrary in $\mathcal{O}_H((T))$. There exists a positive integer N such that $[\pi]^N\cdot f\in\mathcal{O}_H[[T]]$. It is easily checked that

$$\mathscr{S}([\pi]^N\cdot f)=T^N\mathscr{S}(f).$$

Hence, the lemma follows immediately from the special case, $f\in\mathcal{O}_H[[T]]$; discussed above.

We now begin the proof of the general interpolation theorem mentioned in the introduction.

Let $\mathscr{H}$ denote the set of all Galois equivariant maps from $\mathfrak{F}'_\infty$ into H_∞ (i.e. w.r.t. G_∞). Then, $\mathscr{H}$ is naturally an R_∞-module where the action is given by $(\omega h)(u)=\omega(h(u))$ for $\omega\in R_\infty$, $h\in\mathscr{H}$ and $u\in\mathfrak{F}'_\infty$. Moreover, restriction from B' to $\mathfrak{F}'_\infty$ defines a continuous R_∞-homomorphism from $H((T))_1$ into $\mathscr{H}$. For a given R_∞-submodule A of $H((T))_1$, two natural questions arise; What is the kernel and what is the image of this homomorphism restricted to A?

If $A=H((T))_1$, the answers are that the kernel is $\lambda\cdot H((T))_1$, where λ is the logarithm of $\mathfrak{F}$ (see Sect. V), and the image is all of $\mathscr{H}$. It is more interesting to consider submodules of $H((T))_1$ defined by some "integrality" condition. Here we shall be mainly concerned with $\mathcal{O}_H((T))$.

Our uniqueness principle answers our first question for $A=\mathcal{O}_H((T))$; that is, the kernel is zero. To answer our second question, we introduce the following integral.

For $h \in \mathscr{H}$, we define

$$\int_{\mathfrak{F}} h = -\operatorname*{Lim}_{n \to \infty} \sum_{u \in \mathfrak{F}_n'} h(u)$$

whenever the limit exists. Let $L(\mathfrak{F})$ denote the subset of $\mathscr{H}$ on which this integral is defined. $L(\mathfrak{F})$ is clearly an R_∞-submodule of $\mathscr{H}$ and $\int_{\mathfrak{F}}$ defines a linear functional from $L(\mathfrak{F})$ into H. Let T_n denote the trace from H_n to H. It follows from the Galois equivariance that if $h \in L(\mathfrak{F})$,

$$\int_{\mathfrak{F}} h = -\sum_{n=0}^{\infty} T_n(h(v_n)) \tag{3}$$

(recall that v_n is a generator for $\mathfrak{F}_n$). The significance of this integral lies in the following mean-value property for elements of $\mathcal{O}_H[[T]]$.

Proposition 7. *If $f \in \mathcal{O}_H[[T]]$ then $f \in L(\mathfrak{F})$ and*

$$f(0) = \int_{\mathfrak{F}} f.$$

Proof. By Lemma 5 (ii) $-\sum_{u \in \mathfrak{F}_n'} f(u) = f(0) - \mathscr{S}^{n+1}(f)(0)$, so

$$\begin{aligned} \int_{\mathfrak{F}} f &= f(0) - \lim_{n \to \infty} \mathscr{S}^{n+1}(f)(0) \\ &= f(0), \end{aligned}$$

using Lemma 6.

For $g \in H((T))_1$ and $h \in \mathscr{H}$ we understand by $g \cdot h$, the element of $\mathscr{H}$ defined as the pointwise product of g and h as functions on $\mathfrak{F}_\infty'$. The previous proposition motivates us to define $\mathscr{H}_n$, $0 \leqq n \leqq \infty$ to be the set of all elements h of $\mathscr{H}$ such that $g \cdot h \in L(\mathfrak{F})$ and

$$\int_{\mathfrak{F}} g \cdot h \equiv 0 \bmod \pi^{n+1} \mathcal{O}_H$$

for all $g \in T\mathcal{O}_H[[T]]$, where we take $\pi^{\infty+1} = 0$.

We now state the main result of this section.

Theorem 8. *If $h \in \mathscr{H}$ and $k \in \mathbb{Z}$, then $T^k \cdot h \in \mathscr{H}_n$, $0 \leqq n \leqq \infty$, if and only if there exists an $f \in T^{-k}\mathcal{O}_H[[T]]$ such that*

$$f(u) = h(u) \quad \text{for all } u \in \mathfrak{F}_n'.$$

We shall require a couple of lemmas.

Lemma 9. *If $\alpha_i \in \pi^{n-i}\mathfrak{p}_0\mathcal{O}_n$ for $0 \leqq i \leqq n < \infty$, then there exists an $f \in \mathcal{O}_H[[T]]$ such that $f(v_i) = \alpha_i$.*

Proof. This follows simply from the observation that if

$$g_{n,k}=\frac{[\pi^{n+1}]\cdot[\pi^k]}{[\pi^{k+1}]} \quad \text{for } 0\leqq k\leqq n,$$

then $g_{n,k}\in\mathcal{O}_H[[T]]$ and

$$g_{n,k}(v_i)=\begin{cases}0 & 0\leqq i\leqq n \quad i\neq k\\ \pi^{n-k}\cdot v_0 & i=k.\end{cases}$$

Lemma 10. *If $f\in\mathcal{O}_H[[T]]$ and $T^{-1}f(T)\in\mathscr{H}_n$, $n<\infty$ then there exists a $g\in\mathcal{O}_H[[T]]$ such that $g(u)=u^{-1}f(u)$, for $u\in\mathfrak{F}'_n$.*

Proof. Since $T^{-1}\cdot f(T)\in\mathscr{H}_n$,

$$\int_{\mathfrak{F}} f\equiv 0 \bmod \pi^{n+1}\mathcal{O}_H.$$

But, $\int_{\mathfrak{F}} f=f(0)$ by Proposition 7 and so the above congruence implies $f(0)\in\pi^{n+1}\mathcal{O}_H$. Let $f(0)=\pi^{n+1}b$, $b\in\mathcal{O}_H$ and let

$$g(T)=T^{-1}f(T)-bT^{-2}[\pi^{n+1}](T).$$

By construction, g satisfies the conditions of our lemma.

Proof of Theorem 8. Clearly it suffices to consider only the case $k=0$. First suppose $n<\infty$. Let $h\in\mathscr{H}_n$. On the one hand we observe that $T^r\cdot h\in\mathscr{H}_n$ for all $r\geqq 0$; so if there exists an $r\gg 0$ and an $f'\in\mathcal{O}_H[[T]]$, such that $f'(u)=u^r h(u)$ for $u\in\mathfrak{F}'_n$, then applying Lemma 10 iteratively we deduce that there exists an $f\in\mathcal{O}_H[[T]]$ satisfying the requirements of the Theorem. On the other hand, for r sufficiently large,

$$u_i^r h(u_i)\in\pi^{n-i}\mathfrak{p}_0\mathcal{O}_i \quad \text{for } 0\leqq i\leqq n.$$

Hence, by Lemma 9, there exists an f' such that $f'(v_i)=v_i^r\cdot h(v_i)$ for $0\leqq i\leqq n$, and by Galois equivariance $f'(u)=u^r\cdot h(u)$ for $u\in\mathfrak{F}'_n$. This together with the above observation completes the proof for $n<\infty$.

If $n=\infty$, then by what we have already proven, for each $m\geqq 0$, there exists an $f_m\in\mathcal{O}_H[[T]]$ such that $f_m(u)=h(u)$ for $u\in\mathfrak{F}'_\infty$. By Lemma 2a, $\{f_m\}$ is a Cauchy sequence. Let f be its limit in $\mathcal{O}_H[[T]]$ ($\mathcal{O}_H[[T]]$ is a complete subspace of $H((T))_1$). Then we must have $f(u)=h(u)$ for all $u\in\mathfrak{F}'_\infty$. This concludes the proof of the "if" part of the Theorem. The converse follows immediately from Proposition 7, and the fact that $T_m(\mathcal{O}_m)\subseteq\pi^m\mathcal{O}_H$ (which follows from Lemma 6 and Corollary 5 (i)).

IV. The Norm Operator

To simplify notation we set $\mathcal{O}_H[[T]]=I$. Let $\mathscr{M}$ denote the group of invertible elements in $\mathcal{O}_H((T))$ and $\mathscr{M}^o$ the group of principal units in I, i.e., the set of all $f\in I$ such that $f(0)\equiv 1 \bmod \pi\mathcal{O}_H$. Let p be the characteristic of the

residue field of K. Then $I^* = V \times \mathcal{M}^o$ where V is the group of roots of unity of order prime to p in H.

Let $\mathbb{Z}_p$ denote the p-adic integers and let $\mathcal{T}_\infty = \varprojlim \mathbb{Z}_p[G_n]$, where the inverse limit is taken with respect to the canonical restriction maps. $\mathbb{Z}_p$ acts in a natural way on $\mathcal{M}^o$ and we may give $\mathcal{M}^o$ the structure of a continuous $\mathcal{T}_\infty$-module such that

$$(f)^a = f^a \quad \text{and} \quad (f)^\sigma = f \circ [K(\sigma)]$$

for $a \in \mathbb{Z}_p$ and $\sigma \in G_\infty$. The proof of this fact runs along similar lines to the proof of Theorem 1, only in this case it is much simpler as $\mathcal{M}^o$ is complete.

For each $n \geqq 0$, let $\varepsilon_n : H((T))_1 \to H_n$ be the evaluation map; $f \mapsto f(v_n)$. It is clear that ε_n induces an R_∞-homomorphism. Also, if we restrict ε_n to $\mathcal{M}^o$ we obtain a $\mathcal{T}_\infty$-homomorphism from $\mathcal{M}^o$ into $1 + \mathfrak{p}_n \subseteq H_n^*$, where $\mathcal{T}_\infty$ acts on the multiplicative group $1 + \mathfrak{p}_n$ in the natural way.

Theorem 11. *There exists a unique map $\mathcal{N} : \mathcal{O}_H((T)) \to \mathcal{O}_H((T))$ which satisfies:*

$$\mathcal{N}(f)_\pi = \prod_{u \in \mathfrak{F}_0} {}_u f. \tag{1}$$

Moreover, $\mathcal{N}$ is continuous.

Proof. Uniqueness is plain.

For $f \in I$, let $\mathcal{Q}(f) = \prod_{u \in \mathfrak{F}_0} {}_u f$. It is easy to see that $\mathcal{Q}(f) \in I$ and that ${}_u\mathcal{Q}(f) = \mathcal{Q}(f)$ for all $u \in \mathfrak{F}$. Thus, by Lemma 3, there exists a unique $g \in I$ such that $g_\pi = \mathcal{Q}(f)$. In this case, set $\mathcal{N}(f) = g$. For f arbitrary in $\mathcal{O}_H((T))$ there exists a suitably large positive integer N such that $[\pi]^N \cdot f \in I$, we then set $\mathcal{N}(f) = T^{-q^N} \mathcal{N}([\pi]^N \cdot f)$. It follows easily now that $\mathcal{N}$ satisfies the requirements of the Theorem.

Continuity follows from the continuity of $\mathcal{Q}$ (cf. the proof of Theorem 4).

Let $N_{m,n}$ denote the norm from H_m to H_n, and N_n the norm from H_n to H. Let $v_T(f)$ denote the order of the zero of f at zero, for $f \in H((T))$.

Corollary 12. *The map $\mathcal{N}$ is multiplicative from the monoid $\mathcal{O}_H((T))$ into itself, and leaves invariant $\mathcal{M}$ and $\mathcal{M}^o$. Moreover, if $f \in \mathcal{O}_H((T))$ then;* (i) $v_T(\mathcal{N}(f)) = v_T(f)$. (ii) $\varepsilon_n \mathcal{N}(f) = N_{n+1,n}(\varepsilon_{n+1}(f))$. (iii) *$\mathcal{N}$ restricts to a continuous $\mathcal{T}_\infty$-endomorphism of $\mathcal{M}^o$.*

Proof. That $\mathcal{N}$ is multiplicative follows immediately from the fact that $\mathcal{Q}$ is. It follows that $\mathcal{N}$ leaves invariant $\mathcal{M} = \mathcal{O}_H((T))^x$. From the proof of Theorem 11, we see that $\mathcal{N}$ leaves invariant I, hence also $\mathcal{M} \cap I^x = V \times \mathcal{M}^o$. Since $\mathcal{M}^o$ is a pro-p group and V is a torsion group without p-torsion, it follows that $\mathcal{N}$ leaves invariant $\mathcal{M}^o$. Now, (i) and (ii) follow immediately from (1). Finally, (1) also implies that $\mathcal{N}(h^\sigma) = \mathcal{N}(h)^\sigma$ for $h \in \mathcal{M}^o$; hence (iii) follows from the continuity of $\mathcal{N}$.

Remark. If the characteristic of K is zero and $\mathcal{T}_\infty$ is identified with a subring of R_∞ in the natural way, then the usual logarithm series induces a $\mathcal{T}_\infty$-homomorphism of $\mathcal{M}^0$ into $H[[T]]_1$ such that $\operatorname{Log} \mathcal{N}(h) = \mathcal{S} \operatorname{Log}(h)$.

Let φ be the Frobenius automorphism of H_∞ over K_∞. For $f \in H((T))$ we define φf coefficientwise so that φ commutes with G_∞, $\mathscr{T}_\infty$, $\mathscr{S}$ and $\mathscr{N}$. (N.B., φ does not in general commute with R_∞.) The following congruences are enjoyed by $\mathscr{N}$.

Lemma 13. *Let $g \in 1+\pi^i I$, $i \geqq 1$, and $h \in \mathscr{M}$. Then*

(i) $\mathscr{N}(g) \equiv 1 \bmod \pi^{i+1} I$,

(ii) $\dfrac{\mathscr{N}^i(h)}{\varphi \mathscr{N}^{i-1}(h)} \equiv 1 \bmod \pi^i I$.

Proof. We first observe that ${}_u g \equiv g \bmod \pi^i \mathfrak{p}_0$, for $u \in \mathfrak{F}_0$. Hence $\mathscr{Q}(g) \equiv g^q \equiv 1 \bmod \pi^{i+1}$ since $\mathscr{Q}(g) \in I$. We deduce from (1) that $\mathscr{N}(g)_\pi \equiv 1 \bmod \pi^{i+1}$. To conclude the proof of (i), we must verify the statement: If $k \in I$ and $k_\pi \in \pi^n I$ then $k \in \pi^n I$. We proceed by induction on n. The statement is trivial for $n=0$. Suppose now $n>0$ and the statement is true for $n-1$. Set $k' = \pi^{1-n} k$. Then $k'_\pi \in \pi I$ and by induction $k' \in I$. As $[\pi](T) \equiv T^q \bmod \pi$ we have $k'(T^q) \in \pi I$, and so $k = \pi^{n-1} k' \in \pi^n I$. Thus we have (i)

We first prove (ii) for $i=1$. Suppose $f \in I$, then as $\mathscr{N}(f)_\pi (T) \equiv \mathscr{N}(f)(T^q) \bmod \pi$ and ${}_v f \equiv f \bmod \mathfrak{p}_0$, we may conclude from (1) that $\mathscr{N}(f)(T^q) \equiv f(T)^q \bmod \pi I$. But, $f(T)^q \equiv \varphi f(T^q) \bmod \pi I$; we deduce

$$\mathscr{N}(f) \equiv \varphi f \bmod \pi I, \tag{2}$$

for $f \in I$. It follows from (2) that $\mathscr{N}(f)/\varphi f \equiv 1 \bmod (\varphi f)^{-1} \cdot \pi I$, for $f \in \mathscr{M} \cap I$. But, by Corollary 12 (i) $v_T \mathscr{N}(f) = v_T f$ so that we actually have

$$\mathscr{N}(f)/\varphi f \equiv 1 \bmod \pi I, \tag{3}$$

for $f \in \mathscr{M} \cap I$. Since, for every $f \in \mathscr{M}$, either f or $f^{-1} \in I$, (3) follows immediately for any $f \in \mathscr{M}$. We obtain (ii) by applying (i) iteratively to (3).

It is an immediate consequence of this lemma that the limit,

$$\mathscr{N}^\infty(f) \overset{\text{defn.}}{=} \operatorname*{Lim}_{i \to \infty} \varphi^{-i} \mathscr{N}^i(f)$$

exists for all $f \in \mathscr{M}$ and satisfies

$$\mathscr{N}(\mathscr{N}^\infty(f)) = \varphi \mathscr{N}^\infty(f) \quad \text{and} \quad \mathscr{N}^\infty(f)/f \equiv 1 \bmod \pi I \tag{4}$$

Example. Let $H = K = \mathbb{Q}_p$ be the field of p-adic numbers. Let $\mathfrak{F} = \mathbb{G}_m$ be the formal multiplicative group. Then $\mathbb{G}_m$ is a Lubin-Tate group over $\mathbb{Q}_p$ corresponding to the parameter p. We then have

$$\mathscr{N}^\infty(1-T) = (\varepsilon - 1) - T, \qquad \mathscr{N}^\infty(1-(1+T)^a) = 1-(1+T)^a$$

where ε is the unique element of $\mathbb{Z}_p$ which satisfies $\varepsilon^p = \varepsilon$ and $\varepsilon \equiv 2 \bmod p$, and where $(a, p) = 1$. Evaluating $(1-(1+T)^a)/T$ at $u_n = \zeta_n - 1$ $(\zeta_n^{p^{n+1}} = 1)$ we obtain of course the circular units.

Now set $\mathscr{M}_\infty = \{f \in \mathscr{M} / \mathscr{N}(f) = \varphi f\}$ and $\mathscr{M}_\infty^o = \mathscr{M}^o \cap \mathscr{M}_\infty$. We see from (4) that $\mathscr{M}_\infty$ is non-trivial and that $\mathscr{N}^\infty$ is a projector from $\mathscr{M}$ onto $\mathscr{M}_\infty$; in fact we have:

Proposition 14. (i) $\mathscr{M}_\infty = (\mathscr{N}^\infty(T))^{\mathbb{Z}} \times V \times \mathscr{M}_\infty^o$. (ii) *The sequence:*

$$(1) \to 1 + \pi I \to \mathscr{M}^o \underset{\iota}{\overset{\mathscr{N}^\infty}{\rightleftarrows}} \mathscr{M}_\infty^o \to (1)$$

is a split exact sequence of topological $\mathscr{T}_\infty$-modulues, where ι is the inclusion.

Proof. This follows immediately from Corollary 12 and Lemma 13.

Let $G(T) = \mathscr{N}^\infty(T)$. We then have $G \in T \cdot \mathscr{M}^o$.

We now prove the main result of this section.

Theorem 15. *Let $\alpha \in H_n^*$, then there exists an $f_\alpha \in \mathscr{M}$ such that*

$$\varepsilon_i f_\alpha = \varphi^i N_{n,i} \alpha \quad \text{for } 0 \leqq i \leqq n.$$

Proof. For all $\beta \in H_n$, let $h_\beta \in \mathscr{H}$ (cf. Sect. III) be defined as follows:

$$h_\beta(\sigma v_i) = \begin{cases} 0 & i > n, \\ \sigma \varphi^i N_{n,i} \beta & 0 \leqq i \leqq n, \end{cases} \quad \text{for } \sigma \in G_\infty.$$

First suppose $\alpha \in \mathscr{O}_n^*$. We will show $h_\alpha \in \mathscr{H}_n$, i.e., we will show

$$\int_{\mathfrak{F}} g \cdot h_\alpha \equiv 0 \bmod \pi^{n+1} \tag{5}$$

for all $g \in T \cdot I$. It is sufficient to verify (5) for all $g \in \{G(T)^k\}_{k \geqq 1}$. Indeed, the collection of $\mathscr{O}_H$-linear combinations of elements in this set is dense in $T \cdot I$, and (5) is clearly a continuous $\mathscr{O}_H$-linear condition on g. But, in view of the definition of $G(T)$ and Corollary 12 (ii)

$$G(T)^k \cdot h_\alpha = h_\gamma$$

where $\gamma = \varphi^{-n} G(u_n)^k \cdot \alpha$. As $\gamma \in \mathfrak{p}_n$, for $k \geqq 1$, we are reduced to proving

$$\int_{\mathfrak{F}} h_\beta \equiv 0 \bmod \pi^{n+1} \tag{6}$$

for all $\beta \in \mathfrak{p}_n$.

Now choose $f \in T \cdot I$ so that $\varepsilon_n f = \varphi^n \beta$. From Corollary 5 (ii), we deduce that

$$T_i(\varepsilon_i g) = (\mathscr{S}^{i+1}(g) - \mathscr{S}^i(g))(0),$$

for $g \in I$. Let $\mathscr{N}^{(i)}(f) = \varphi^{-i} \mathscr{N}^i(f)$, for $j \geqq 0$. Using (III, 3), Corollary 12 (ii) and Corollary 5 (i) we have

$$\int_{\mathfrak{F}} h_\beta = \sum_{i=0}^{n} T_i(\varphi^i N_{n,i}\beta)$$
$$= \sum_{i=0}^{n} (\mathscr{S}^{i+1}(\mathscr{N}^{(n-i)}(f)) - \mathscr{S}^i(\mathscr{N}^{(1-i)}(f)))(0)$$
$$= \mathscr{S}^{n+1}(f)(0) - \mathscr{N}^{(n)}(f)(0) + \sum_{i=0}^{n} \mathscr{S}^{i+1}(\mathscr{N}^{(n-(i-1))}(f) - \mathscr{N}^{(n-i)}(f))(0).$$

Now, $\mathscr{S}^{n+1}(f) \equiv 0 \bmod \pi^{n+1}$ by Lemma 6, $\mathscr{N}^{(n)}(f)(0) = 0$ since $1 \leqq v_T(f) = v_T(\mathscr{N}^{(n)}(f))$, by Corollary 12 (i), and

$$\mathscr{S}^{i+1}(\mathscr{N}^{(n-(i-1))}(f) - \mathscr{N}^{(n-i)}(f)) \equiv 0 \bmod \pi^{n+1} \cdot I$$

by Lemma 6 (ii) and Lemma 13 (ii). Hence we have (6) and so $h_\alpha \in \mathscr{H}_n$ for all $\alpha \in \mathcal{O}_n^*$. Thus by Theorem 8 there exists an $f_\alpha \in I$ such that $f_\alpha(u) = h_\alpha(u)$ for all $u \in \mathfrak{F}_n$ Actually, $f_\alpha \in I^*$ since $f_\alpha(0) \equiv \alpha \bmod \mathfrak{p}_n$. Thus we have Theorem 15 for $\alpha \in \mathcal{O}_n^*$.

It remains to consider β arbitrary in H_n^*. But, $H_n^* = (\varphi^{-n} G(v_n))^{\mathbb{Z}} \times \mathcal{O}_n^*$, as $G(T) \in T \cdot \mathscr{M}^o$. So if $\beta = (\varphi^{-n} G(v_n))^k \cdot \alpha$, where $k \in \mathbb{Z}$ and $\alpha \in \mathcal{O}_n^*$ we set

$$f_\beta = G(T)^k \cdot f_\alpha$$

where f_α is as above. This completes the proof of the theorem.

Let $X_\infty = \varprojlim H_n^*$ and $X_\infty^0 = \varprojlim 1 + \mathfrak{p}_n$, where the inverse limits are taken with respect to the maps, $N_{m,n}$ for $m \geqq n \geqq 0$. $X_\infty^0 \subseteq X_\infty$ and X_∞^o is naturally a $\mathscr{T}_\infty$-module.

Theorem 16. *There exists a unique map $\gamma (= \gamma_v)$ from X_∞ into $\mathscr{M}$ such that*

$$\begin{array}{ccc} X_\infty & \xrightarrow{\gamma} & \mathscr{M} \\ \downarrow{\scriptstyle N_{\infty,i}} & & \downarrow{\scriptstyle \varepsilon_i} \\ H_j^* & \xrightarrow{\varphi^i} & H_i^* \end{array} \tag{7}$$

commutes for all $i \geqq 0$.

Proof. The uniqueness of γ follows from our uniqueness principle.

We know from the previous theorem that for each positive integer n there exists a (non-unique) map $\gamma_n \colon X_\infty \to \mathscr{M}$, which makes (7) commute for all i such that $0 \leqq i \leqq n$. Also, it is easy to see that $v_{\mathfrak{p}_n}(b_n) = v_T(\gamma_n(b))$ and $v_{u_m}(b_m) = v_{\mathfrak{p}_n}(b_n)$ for all $b \in X_\infty$ and all $m \geqq n$ (H_∞/H is totally ramified). Thus for each $b \in X_\infty$ the sequence $\{\gamma_n(b)\}$ is contained in $T^k \mathcal{O}_H[[T]]$, for some $k \in \mathbb{Z}$. Lemma 2a implies that this sequence is Cauchy and if we set $\gamma(b)$ equal to its limit for each $b \in X_\infty$, we see immediately that γ makes (1) commute, for all $n \geqq 0$. This completes the proof of the Theorem.

Corollary 17. *γ is a topological isomorphism from X_∞ onto $\mathscr{M}_\infty$, which restricts to a topological $\mathscr{T}_\infty$-isomorphism from X_∞^o onto $\mathscr{M}_\infty^o$.*

Proof. As $\varepsilon_n \mathcal{N}(\gamma(b)) = N_{n+1,n}(\varepsilon_{n+1}\gamma(b)) = \varphi\varepsilon_n\gamma(b) = \varepsilon_n\varphi\gamma(b)$ for all $n \geqq 0$, it follows from our uniqueness principle that $\mathcal{N}\gamma(b) = \varphi\gamma(b)$ so that $\gamma(b) \in \mathcal{M}_\infty$ for all $b \varepsilon X_\infty$. Also, given $f \in \mathcal{M}_\infty$, the sequence $c_f = \{\varphi^{-1}\varepsilon_i(f)\}$ lies in X_∞. Moreover, the map $f \mapsto c_f$ is clearly the inverse of γ on $\mathcal{M}_\infty$ and is continuous. Hence, γ is a bijection from X_∞ to $\mathcal{M}_\infty$.

Obviously γ is a homomorphism, and by Lemma 2a, it is continuous. This together with the continuity of γ^{-1} implies that γ is a topological isomorphism onto $\mathcal{M}_\infty$.

Finally, it is plain that γ restricted to X_∞^o is a $\mathbb{Z}[G_\infty]$-homomorphism onto $\mathcal{M}_\infty^o$, so as γ is continuous, it follows that γ defines a topological $\mathcal{T}_\infty$-isomorphism from X_∞^o onto $\mathcal{M}_\infty^o$.

Corollary 18. $X_\infty \approx \mathfrak{k}((T))^*$, *where* $\mathfrak{k}$ *is the residue field of* H.

Proof. This follows immediately from the previous theorem and Proposition 14.

Remark. By means of this isomorphism, one can give $X_\infty \cup \{0\}$ the structure of a field. It can be shown that this is identical with Fontaine's construction [F], by means of which one can set up a correspondence between algebraic extensions of H_∞ and algebraic extensions of $\mathfrak{k}((T))$.

Corollary 19. *If* $[H:K] < \infty$ *then* $(\bigcap_{m \geqq n} N_{m,n}(1+\mathfrak{p}_m)) \cdot (1+\pi\mathcal{O}_n) = 1+\mathfrak{p}_n$, *for* $n \geqq 0$.

Proof. This follows immediately from the preceding Theorem, Proposition 14 and the compactness of $1+\mathfrak{p}_n$.

V. The Lubin-Tate Logarithm

We maintain the notations of the previous section. In this section we will study the logarithm associated with $\mathfrak{F}$. We begin with a technical lemma on the endomorphism $[\pi]$. Let $\mathfrak{p}_H$ denote the ideal $\pi\mathcal{O}_H$.

Lemma 20. *The following assertions are true for each integer* $i \geqq 1$. (i) *If* g, h *are power series in* I, *with* g *arbitrary and* h *satisfying* $h(T) \equiv T^q \bmod \mathfrak{p}_H$, *then* $[\pi^i] \circ g \equiv [\pi^{i-1}] \circ \varphi g \circ h \bmod \mathfrak{p}_H^i$; (ii) *Let* N *be a positive integer, and* r, ε *positive reals, with* $r<1$. *If* f *belongs to* $S_H(r,\varepsilon) \cap T^N H[[T]]$, *then* $f_{\pi^i} \in S_H(r, \varepsilon q^{-iN} M_r^N)$, *where* M_r *is a positive real number depending only on* r.

Proof. The proof of (i) is by induction on i. It is true for $i=1$, because

$$[\pi] \circ g \equiv g^q \equiv \varphi g(T^q) \equiv \varphi g \circ h \bmod \mathfrak{p}_H.$$

Suppose that it is true for an integer $i \geqq 1$. Write

$$[\pi^i] \circ g = [\pi^{i-1}] \circ \varphi g \circ h + \pi^i k_1, \qquad [\pi](T) = T^q + \pi k_2.$$

where k_1, k_2 belong to I. Then, if we put $A = [\pi^{i-1}] \circ \varphi g \circ h$, we have

$$[\pi^{i+1}]\circ g=(A+\pi^i k_1)^q+\pi k_2(A+\pi^i k_1)$$
$$\equiv A^q+\pi k_2(A) \bmod \mathfrak{p}_H^{i+1},$$
$$\equiv[\pi^i]\circ\varphi g\circ h \bmod \mathfrak{p}_H^{i+1},$$

and so (i) follows.

To prove (ii) we first observe that if $h\in B$, then

$$|[\pi](b)|\leqq\max(q^{-1}|b|, |b|^q),$$

since $[\pi](T)=\pi T+T^q+\pi g(T)$, for some $g\in T^2\mathcal{O}_K[[T]]$. From this it follows that there exists a positive integer k_r, depending only on $r=|b|$, such that $|[\pi^{k_r}](b)|<q^{-(q-1)^{-1}}$. It also follows that $|[\pi](b)|<q^{-1}|b|$ if $|b|<q^{-(q-1)^{-1}}$. From these two facts we see that there exists a constant $C_r>0$, depending only on r, such that

$$|[\pi^i](b)|<q^{-i}C_r$$

if $|b|=r$. Now take f to be a power series in $S_H(r,\varepsilon)\cap T^N H[[T]]$, say $f(T)=T^N h(T)$. It is clear from the above that

$$|f_{\pi^i}(b)|<q^{-iN}C_r^N|h_{\pi^i}(b)|.$$

But $|[\pi^i](b)|<r$, and so if $r>0$,

$$|h([\pi^i](b))|<\sup_{|x|=r}\left|\frac{f(x)}{x^N}\right|<r^{-N}\varepsilon.$$

Combining these last two inequalities, assertion (ii) follows with $M_r=C_r/r$. This completes the proof of Lemma 20.

Let $\lambda=\lambda_{\mathfrak{F}}$ denote the logarithm of $\mathfrak{F}$. Thus, if $\mathbb{G}_a$ denotes the formal additive group, then λ is the unique power series in $K[[T]]$ which, gives an isomorphism

$$\lambda\colon \mathfrak{F}\xrightarrow{\sim}\mathbb{G}_a$$

over K, and which satisfies $\lambda(T)\equiv T$ mod degree 2. We have the following basic lemma about λ.

Lemma 21. (i) $\lambda=\lim_{n\to\infty}\pi^{-n}[\pi^n]$, *where the limit is taken in* $K((T))_1$; (ii) *If* g *and* h *satisfy the same hypotheses as in part* (i) *of Lemma* 20, *then,*

$$\lambda\circ g-\frac{\lambda\circ\varphi g\circ h}{\pi}\in I.$$

Proof. Let $K[[T]]_1=K[[T]]\cap K((T))_1$, endowed with the restriction topology. Put $h_n=\pi^{-n}[\pi^n]$. Since $K[[T]]_1$ is a complete, non-archimedean, topological ring, it suffices to show that $h_{n+1}-h_n$ tends to 0 as $n\to\infty$, to prove the existence of $\lim_{n\to\infty}h_n$. Put $g(T)=h_1(T)-T$. Obvously, $g(T)$ is divisible by T^2 in $K[[T]]_1$, and

$$\pi^{-n}g\circ[\pi^n]=h_{n+1}-h_n.$$

Applying (ii) of Lemma 20 with $N=2$, we conclude that the left hand side of this equation tends to zero as $n\to\infty$. Thus $h=\lim_{n\to\infty} h_n$ exists. Since $h(T)\equiv T \bmod$ degree 2, and $h\circ[\pi]=\pi h$, a simple argument based on the uniqueness of λ, which we omit, shows that we must have $h=\lambda$. This completes the proof of (i). Also (i) implies that

$$\lambda\circ g-\frac{\lambda\circ\varphi g\circ h}{\pi}=\lim_{n\to\infty}\left(\frac{[\pi^{n+1}]\circ g-[\pi^n]\circ\varphi g\circ h}{\pi^{n+1}}\right),$$

and the right hand side is in I by part (i) of Lemma 20. This completes the proof of Lemma 21.

For a more detailed discussion of λ, see [Fr] Chapt. 4 (also see [W]). Here we simply recall, without proof, the following basic facts. First, λ commutes with the action of $\mathcal{O}_K$ as endomorphism ring of $\mathfrak{F}$ and $\mathbb{G}_a$. Second, $\frac{d}{dT}\lambda$ belongs to $\mathcal{O}_K[[T]]$. Third, λ converges on B and if $|b|<q^{-(q-1)^{-1}}$, then

$$|\lambda(b)|=|b|. \tag{1}$$

Finally, the kernel of λ on B is the group $\mathfrak{F}_\infty$. We point out, however, that all of these facts follow easily from Lemma 21.

If $\mathcal{I}$ is any topologically nilpotent ideal in a topological $\mathcal{O}_K$-algebra R, we define $\mathfrak{F}(\mathcal{I})$ to be the topological group whose underlying topological space is $\mathcal{I}$ and whose addition law "$[+]$" is given by

$$a[+]b=\mathfrak{F}(a,b).$$

(N.B. This is consistent with our earlier use of $[+]$.)

Let $\mathcal{A}_\infty$ denote the closure of $\mathcal{O}_K[G_\infty]$ in R_∞. Let m denote the maximal ideal of I. We may give the group $\mathfrak{F}(m)$ the structure of a continuous $\mathcal{A}_\infty$-module such that the action of $\omega\in\mathcal{A}_\infty$ on an element f of $\mathfrak{F}(m)$ is denoted by $[\omega](f)$, and such that

$$[a](f)=[a]\circ f,\qquad [\sigma](f)=f\circ[\kappa(\sigma)],$$

for $a\in\mathcal{O}_K$, $\sigma\in G_\infty$. Once again, the proof of the existence and uniqueness of such a structure runs along similar lines to the proof of Theorem 1.

We shall henceforth always consider $\mathfrak{F}(m)$ endowed with this $\mathcal{A}_\infty$-module structure. It is plain that λ defines a continuous $\mathcal{A}_\infty$-module homomorphism from $\mathfrak{F}(m)$ into $H[[T]]_1$. The remainder of this section will be devoted to giving descriptions of $\mathfrak{F}(m)$ and of $\lambda(\mathfrak{F}(m))$. Let $\Theta: H[[T]]_1\to H[[T]]_1$ be the map defined by

$$\Theta(f)=f-\frac{\varphi f_\pi}{\pi}.$$

Let $\Theta_{\mathfrak{F}}: \mathfrak{F}(m)\to H[[T]]_1$ be the map defined by

$$\Theta_{\mathfrak{F}}(g)=\Theta(\lambda(g)).$$

Let

$$A=\left\{g\in I: g(0)\in\mathscr{J}_H, \frac{d}{dT}(g)(0)\in(1-\varphi)\,\mathcal{O}_H\right\},$$

where $\mathscr{J}_H=(1-\varphi)\,\mathcal{O}_H+\mathfrak{p}H$, if $q=2$, and $\mathscr{J}_H=\mathcal{O}_H$ otherwise. Finally let $\mathscr{C}=\mathfrak{F}_\infty\cap\mathfrak{F}(\mathfrak{p}_H)$. Since $[H_0:H]=q-1$, $\mathscr{C}=\{0\}$ unless $q=2$, in which case $\mathscr{C}=\mathfrak{F}_\pi$. We may now state:

Theorem 22. *The sequence*

$$0\to\mathscr{C}[+][\mathscr{A}_\infty]\,T\xrightarrow{\text{incl.}}\mathfrak{F}(m)\xrightarrow{\Theta_{\mathfrak{F}}}A\to 0$$

is an exact sequence of topological $\mathscr{A}_\infty$-modules, which splits when $q\neq 2$ or $H=K$.

Proof. The fact that $\Theta_{\mathfrak{F}}$ is a continuous $\mathscr{A}_\infty$-homomorphism follows from the fact that both λ and Θ obviously are.

We see that the image of $\Theta_{\mathfrak{F}}$ is contained in I from Lemma 2 (ii) and the fact that $\pi^{-1}\mathfrak{p}_H=\mathcal{O}_H$. To see that its image is A, we first observe:

$$\Theta_{\mathfrak{F}}(f)(0)=\lambda(f(0))-\frac{\varphi\lambda(f(0))}{\pi}. \tag{2}$$

By (1), $|\lambda(a)|=|a|$ if $a\in\mathfrak{p}_H$ and $q\neq 2$ or $a\in\mathfrak{p}_H^2$ and $q=2$; since $|\pi^i|=q^{-i}>q^{-(q-1)^{-1}}$ if $i\geqq 1$ and $q\neq 2$ or $i\geqq 2$ and $q=2$. Furthermore, if $q=2H=K$, $\frac{\lambda(\pi a)}{\pi}\equiv(1-\varphi)\,a \bmod \mathfrak{p}_H$. Thus $\lambda(\mathfrak{p}_H)=(1-\varphi)\,\mathfrak{p}_H+\mathfrak{p}_H^2$. Therefore the right hand side of (2) is in $\mathscr{J}_H$ and, in fact, $\Theta_{\mathfrak{F}}(\mathfrak{p}_H)=\mathscr{J}_H$. Second, we see easily

$$\left(\frac{d}{dT}\Theta_{\mathfrak{F}}(f)\right)(0)=(1-\varphi)\left(\frac{d}{dT}\lambda(f)\right)(0).$$

As $\lambda'\in\mathcal{O}_K[[T]]$, the right hand side of the above expression lies in $(1-\varphi)\mathcal{O}_H$ for all $f\in\mathfrak{F}(m)$ and this together with the above shows that the image of $\Theta_{\mathfrak{F}}\subseteq A$. To see the other inclusion we set $f_{\varepsilon,i}=\Theta_{\mathfrak{F}}(\varepsilon T^i)$ for each integer $i\geqq 1$ and each $\varepsilon\in V$, where V is the set of roots of unity in H of order prime to p. We see that

$f_{\varepsilon,i}(T)\equiv(\varepsilon-\varepsilon^q\pi^{i-1})\,T^i \bmod$ degree $i+1$. It follows from this that if $h\in A$ then there exist $a_{\varepsilon,i}\in\mathcal{O}_K$ and an $a\in\mathscr{J}_H$ such that

$$h=a+\sum_{v,i}a_{\varepsilon,i}\cdot f_{\varepsilon,i}.$$

It follows that for each i, $|a_{\varepsilon,i}|<\delta$ for all but finitely many ε where δ is any possitive real. From this and Lemma 20 (ii) it follows that the series $g=\sum_{v,i}^{\mathfrak{F}}[a_{v,i}](vT^i)$ converges in $\mathfrak{F}(m)$, where $\Sigma_{\mathfrak{F}}$ denotes summation in $\mathfrak{F}(m)$. From the continuity of $\Theta_{\mathfrak{F}}$ we see that $h-\Theta_{\mathfrak{F}}(g)=a$. Since $\Theta_{\mathfrak{F}}(\mathfrak{p}_H)=\mathscr{J}_H$ we deduce that $\Theta_{\mathfrak{F}}(\mathfrak{F}(m))=A$.

Now suppose $\Theta_{\mathfrak{F}}(g)=0$. Let $f=\lambda(g)$; then $\Theta(f)=0$. Suppose $f\neq 0$. If aT^k is the first non-vanishing term of $f(T)$ we conclude, by examining the coefficient of T^k in $\Theta(f)$ as above, that $k=1$ and $a\in K$. But, then $f-a\lambda$ satisfies the same conditions as f, has no linear term and therefore must be zero. Hence we

conclude, $\Theta_{\mathfrak{F}}(g)=0$ if and only if $\lambda(g)=a\lambda$ for some $a\in K$. Since the kernel of λ on $\mathfrak{F}(m)$ is $\mathscr{C}$, we have immediately that $g\in\mathscr{C}[+][\mathscr{A}_\infty]T$, as asserted.

As for the splitting, first observe that $[\sigma]T=[\kappa(\sigma)](T)$, $\sigma\in G_\infty$, so that $[\mathscr{A}_\infty]_T=[\mathscr{O}_K]_T$. We define $P\colon \mathfrak{F}(m)\to\mathscr{C}[+][\mathscr{A}_\infty]_T$ by setting $P(f)=[f(0)](\alpha)[+]\left[\frac{d}{dT}(f)(0)\right](T)$, where α is the generator of $\mathscr{C}$ (recall $|\mathscr{C}|\leqq 2$). It is easy to see that P is an $\mathscr{O}_K[G_\infty]$ homomorphism, hence as P is clearly continuous, P is an $\mathscr{A}_\infty$-homomorphism. It is also plain that P is a projector onto the kernel of $\Theta_{\mathfrak{F}}$.

To see that the sequence is topologically exact, we first observe that all the maps are continuous and that the first group is compact. Therefore, we only need to show that $\Theta_{\mathfrak{F}}$ is an open mapping. But this follows immediately from the facts that $\Theta_{\mathfrak{F}}(\mathfrak{F}(\pi^n m))\supseteq\pi^{n+1}A$ and that $\Theta_{\mathfrak{F}}(\mathfrak{F}(T^k\cdot\mathscr{O}_H[[T]]))=T^k\mathscr{O}_H[[T]]$ for $n\geqq 1$ and $k\geqq 2$. These facts, in turn, may be proven by arguments similar to those given above. This completes the proof of the Theorem.

Corollary 23. *When $q\neq 2$ or $H=K$, $\mathfrak{F}(m)$ is $\mathscr{A}_\infty$-isomorphic to $\mathscr{C}\oplus\mathscr{A}_\infty/\mathscr{I}_1\oplus A$, where $\mathscr{I}_1$ is the closed ideal in $\mathscr{A}_\infty$ generated topologically by $\{1-\kappa(\sigma)^{-1}\sigma\}_{\sigma\in G_\infty}$.*

Proof. From the previous theorem we see that it is sufficient to show that the kernel of the map $\omega\mapsto[\omega]T$ from $\mathscr{A}_\infty$ to $\mathfrak{F}(m)$ is precisely $\mathscr{I}_1$. Because $[\sigma]T=[\kappa(\sigma)](T)$ we see that there is a unique map $\mathscr{K}_1\colon \mathscr{A}_\infty\to\mathscr{O}_K$ such that $[\omega]T=[\mathscr{K}_1(\omega)]T$. It is also clear that the map $\mathscr{K}_1$ is a continuous surjective ring homomorphism whose kernel is identical with that of $\omega\mapsto[\omega]T$. We see easily that $\mathscr{I}_1$ is contained in the kernel of $\mathscr{K}_1$. Now $\mathscr{I}_1+\mathscr{O}_K=\mathscr{A}_\infty$ since $\mathscr{I}_1+\mathscr{O}_K$ is closed and contains $\mathscr{O}_K[G_\infty]$; hence as $\mathscr{K}_1(a)=a$ for $a\in\mathscr{O}_K\subseteq\mathscr{A}_\infty$ it follows that $\mathscr{I}_1$ is the kernel of $\mathscr{K}_1$ and our proof is complete.

Now let $\Xi\colon T^2\mathscr{O}_H[[T]]\to T^2H[[T]]_1$ be defined by

$$\Xi f=\sum_{i=0}^{\infty}\frac{\varphi^i f_{\pi^i}}{\pi^i}$$

That Ξ is a well defined continuous map follows from Lemma 20 (ii). It is also plain that Ξ is an $\mathscr{A}_\infty$ homomorphism. For $b\in\mathscr{O}_H$ set

$$\rho(b)=b\lambda+\sum_{i=0}^{\infty}\varphi^i a\left(\frac{[\pi^i]}{\pi^i}-\lambda\right),$$

where $a=(1-\varphi)b$. The series converges by Lemma 20(ii) since $[\pi^i]-\pi^i\lambda=(T-\lambda)\circ[\pi^i]$.

Theorem 24. *Let $h\in H[[T]]_1$. Then $h\in\lambda\mathfrak{F}(m)$ if and only if there exists elements $a\in\pi\mathscr{I}_H$, $b\in\mathscr{O}_H$ and $f\in T^2\cdot\mathscr{O}_H[[T]]$ such that*

$$h=a+\rho(b)+\Xi(f).$$

Moreover, $\lambda(\mathfrak{F}(T^k\cdot\mathscr{O}_H[[T]]))=\Xi(T^k\cdot\mathscr{O}_H[[T]])$, for $k\geqq 2$.

Proof. We see easily that

$$\Theta\Xi(f)=f,\quad \Theta\rho(b)=(1-\varphi)bT\quad\text{and}\quad\Theta(\pi\mathscr{I}_H)=\mathscr{I}_H,\tag{3}$$

where $f \in T^2 \cdot I$, $b \in \mathcal{O}_H$. Let $\mathscr{E}$ denote the set of all elements of the form $a+\rho(b)+\Xi(f)$, where a, b and f are as above. It follows from (3) that $\Theta\mathscr{E}=A$. Thus by Theorem 22, $\mathscr{E}+\operatorname{Ker}\Theta=\lambda(\mathfrak{F}(\mathfrak{m}))+\operatorname{Ker}\Theta$. Therefore since $\mathscr{E} \supseteq \{\rho(b)\}_{b\in\mathcal{O}_K} = \mathcal{O}_K \cdot \lambda(\mathfrak{F}(\mathfrak{m})) \cap \operatorname{Ker}\Theta$, to prove the first part of the theorem, we need only show that $\mathscr{E} \subseteq \lambda(\mathfrak{F}(\mathfrak{m}))$. We know from the proof of Theorem 22 that $\operatorname{Ker}\Theta = K \cdot \lambda$. Let $g=a+\rho(b)+\Xi(f)$ be an element of $\mathscr{E}$. Suppose $g=\lambda(h)+c\lambda$ with $h\in\mathfrak{m}$ and $c\in K$. We then see that

$$b=\frac{d}{dT}\rho(b)(0)=\frac{d}{dT}(g)(0)=c\lambda'(0)+\lambda'(h)(0)\cdot h'(0).$$

So as $\lambda' \in \mathcal{O}_K[[T]]$ and $\lambda'(0)=1$ we see that $b \equiv c \bmod \mathcal{O}_H$. But, $b\in\mathcal{O}_H$ so that $c\in\mathcal{O}_H\cap K=\mathcal{O}_K$ and $g=\lambda([c](T)[+]h)$. Thus $\mathscr{E}\subseteq\lambda(\mathfrak{F}(\mathfrak{m}))$.

As for the second assertion, it follows from (4), the fact that $\lambda(T^k I) \subseteq T^k H[[T]]_1$, and the fact that Θ is an injection on $T^k H[[T]]_1$, for $k \geqq 2$.

Corollary 25 (Iwasawa). *If $\mathfrak{p}_n$ is the maximal ideal of the ring of integers in $\mathbb{Q}_p(\mathfrak{p}_n)$ where ζ_n is a primitive p^{n+1}-st root of unity, then*

$$(1-a^{-1}\sigma(a))\,\gamma_n \in \operatorname{Log}(1+\mathfrak{p}_n)$$

for $a\in\mathbb{Z}_p^*$, where $\sigma(a)$ is the element of Gal $(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p)$ such that $\sigma(a)\,\zeta_n=\zeta_n^a$, and where

$$\gamma_n=\sum_{i=0}^{n}\frac{\zeta_n^{p^i}-1}{p^i}.$$

Proof. We first note that if we set $H=K=\mathbb{Q}_p$, $\pi=p$ and $\mathfrak{F}=\mathbb{G}_m$ then $H_n=\mathbb{Q}_p(\zeta_n)$. Now let $\sigma=\kappa^{-1}(a)$ and set

$$g(T)=(1-a^{-1}\sigma)\,T=T-a^{-1}((1+T)^a-1).$$

Clearly $g\in T^2\mathbb{Z}_p[[T]]$; and so by Lemma 20 (ii) we may set

$$f(T)=\Xi g=\sum_{i=0}^{\infty}\frac{g([p^i])}{p^i} \qquad ([p](T)=(T+1)^p-1).$$

Thus by the above Theorem, $f(T)=\operatorname{Log}(1+h(T))$ for some h in $T^2\mathbb{Z}_p[[T]]$. Therefore

$$f(\zeta_n-1)=\operatorname{Log}(1+h(\zeta_n-1))\in\operatorname{Log}(1+\mathfrak{p}_n).$$

But it is plain that

$$f(\zeta_n-1)=(1-a^{-1}\sigma(a))\,\gamma_n.$$

This completes the proof of the corollary.

Remark. Iwasama's original proof of this fact [I_1] involved the explicit reciprocity laws. He went on the show, by means of an index computation, that for p odd,

$$\mathrm{Log}(1+\mathfrak{p}_n)=p\mathbb{Z}_p+\mathscr{I}_1\gamma_n,$$

where $\mathscr{I}_1$ is as in Corollary 23. In another paper, we will show how this result fits into a general picture and can be extended to the case of arbitrary division towers of Lubin-Tate formal groups of height one.

VI. The Dual of the Image of the Logarithm

In this section H shall denote a *finite* unramified extension of K. Since G_n acts on $\mathfrak{p}_n$ we may make $\mathfrak{F}(\mathfrak{p}_n)$ into an $\mathcal{O}_K[G_n]$-module and hence a continuous $\mathscr{A}_\infty$-module in the natural way. It is clear that λ then defines an $\mathscr{A}_\infty$-module homomorphism from $\mathfrak{F}(\mathfrak{p}_n)$ into H_n^+.

In order to study the image of $\mathfrak{F}(\mathfrak{p}_n)$ under λ, and its dual, we introduce for each $n\geqq 0$, a continuous $\mathscr{A}_\infty$-homomorphism $L_n\colon TH[[T]]_1\to H_n$ defined by

$$L_n(f)=\sum_{i=0}^{n}\frac{\varphi^i\varepsilon_{n-i}(f)}{\pi^i}$$

We have immediately

$$L_n(f)=\varepsilon_n(f)+\pi^{-1}\varphi L_{n-1}(f) \tag{1}$$

for $n\geqq 1$, and also

$$L_n(\Theta(f))=\varepsilon_n f,$$

where Θ is as in the previous section. From this and Theorem 22, we deduce

$$L_n(A')=\varepsilon_n\lambda(T\cdot I)=\lambda(\mathfrak{p}_n)\overset{\text{defn.}}{=}\mathscr{L}_n, \tag{2}$$

where $A'=\{f\in A/f(0)=0\}$.

Recall that $T_{n/K}$ denotes the trace from H_n to K. We define the trace pairing

$$\langle\ ,\ \rangle_n\colon H_n\times H_n\to K$$

by setting $\langle a,b\rangle_n=T_{n/K}(ab)$. Thus $\langle\ ,\ \rangle_n$ is a symmetric, non-degenerate, K-bilinear pairing. We define $\mathfrak{X}_n=\{a\in H_n/\langle a,b\rangle_n\in\mathcal{O}_K$ for all $b\in\mathscr{L}_n\}$. Then $\mathfrak{X}_n$ is a compact $\mathscr{A}_\infty$-submodule of $H_n^+(\mathscr{L}_n\supseteq\mathfrak{p}_H^2\mathcal{O}_n$ by $(V,1))$.[1] We now prove:

Theorem 26. *If $\alpha\in H_n$ then $\alpha\in\mathfrak{X}_n$ if and only if there exists an element $f_\alpha\in T^{-1}\mathcal{O}_H[[T]]$ such that* $\mathrm{Res}_0 f_\alpha\in\mathcal{O}_K$ *and*

$$\varepsilon_i f_\alpha=\pi^{i+1}\varphi^i T_{n,i}(\alpha), \tag{3}$$

for $0\leqq i\leqq n$.

---

[1] In the following we let $\mathrm{Res}_0 f$ denote the coefficient of T^{-1} in f where $f\in H_\infty((T))$

Proof. Let $\alpha \in H_n$ and let $h_\alpha \in \mathscr{H}$ be defined by

$$h_\alpha(\sigma v_i) = \begin{cases} 0 & n < i \\ \sigma \pi^{i+1} \varphi^{i-n} T_{n,i}(\alpha) & 0 \leqq i \leqq n \end{cases}$$

for $\sigma \in G_\infty$. Let $g \in T \cdot I$. Then using (1), and the fact that $T_{i,i-1}(h_\alpha(v_i)) = \pi \varphi h_\alpha(v_{i-1})$ for $1 \leqq i \leqq n$, we have, $L_n g, \pi^{n+1}\alpha\rangle_n$

$$\langle L_n g, h_\alpha(v_n)\rangle_n = \langle \varepsilon_n g, h_\alpha(v_n)\rangle_n + \langle L_{n-1} g, h_\alpha(v_{n-1})\rangle_{n-1}.$$

Iterating this we get

$$\begin{aligned} \langle L_n g, \pi^{n+1}\alpha\rangle_n &= \sum_{i=0}^{n} \langle \varepsilon_i g, h_\alpha(v_i)\rangle_i \\ &= T_{H/K}\left(\sum_{i=0}^{n} T_i(g(v_i)\, h_\alpha(v_i))\right) \\ &= T_{H/K} \int_{\mathfrak{F}} g \cdot h_\alpha, \end{aligned}$$

by (III, 7). From (2) we deduce that $\alpha \in \mathfrak{X}_n$ if and only if

$$T_{H/K} \int_{\mathfrak{F}} g \cdot h_\alpha \equiv 0 \bmod \pi^{n+1} \mathcal{O}_K \tag{4}$$

for all $g \in A'$.

Suppose now that there exists an $f_\alpha \in T^{-1} \cdot I$ such that $\mathrm{Res}_0 f_\alpha \in \mathcal{O}_K$ and $f_\alpha(v_i) = \varphi^n h_\alpha(v_i)$ for $0 \leqq i \leqq n$. Then if $g \in A'$ we have by Proposition 7, setting $f'_\alpha = \varphi^{-n} f_\alpha$,

$$\frac{d}{dT}(g)(0) \cdot \mathrm{Res}_0 f'_\alpha = \int_{\mathfrak{F}} g \cdot f'_\alpha \equiv \int_{\mathfrak{F}} g \cdot h_\alpha \bmod \pi^{n+1} \mathcal{O}_H.$$

The last congruence follows from (III, 3) and the fact that $T_m(\mathcal{O}_m) \subseteq \pi^m \mathcal{O}_H$. Hence, h_α satisfies (4) as our hypothesis on g and f imply that the value on the left lies in $(1-\varphi)\mathcal{O}_K$. Therefore α belongs to $\mathfrak{X}_n$.

Conversely, suppose $\alpha \in \mathfrak{X}_n$, then (4) implies in particular,

$$T_{H/K}(a \cdot \int_{\mathfrak{F}} g \cdot h_\alpha) = T_{H/K} \int_{\mathfrak{F}} a \cdot g \cdot h_\alpha \equiv 0 \bmod \pi^{n+1} \mathcal{O}_K.$$

for all $a \in \mathcal{O}_H$ and all $g \in T^2 \cdot I$. This implies

$$\int_{\mathfrak{F}} g \cdot h_\alpha \equiv 0 \bmod \pi^{n+1} \mathcal{O}_H$$

for all $g \in T^2 \cdot I$, since H is unramified over K. Therefore $T \cdot h_\alpha \in \mathscr{H}_n$, and so by Theorem 8, there exists an $f'_\alpha \in T^{-1} \cdot I$ such that $f'_\alpha(u) = h_\alpha(u)$ for $u \in \mathfrak{F}_0$. We still need to investigate the residue of f'_α. By (4) with $g(T) = (1-\varphi)b \cdot T$, and Proposition 7, we have,

$$T_{H/K}((1-\varphi)b \cdot \mathrm{Res}_0 f'_\alpha) \equiv 0 \bmod \pi^{n+1} \mathcal{O}_K,$$

for all $b \in \mathcal{O}_H$. It is easy to see that this implies that $\mathrm{Res}_0 f_\alpha' = c + \pi^{n+1} d$, where $c \in \mathcal{O}_K$ and $d \in \mathcal{O}_H$. Let

$$f_\alpha = \varphi^n(f_\alpha'(T) - d(T^{-1}[\pi^{n+1}](T))).$$

It now follows that f_α satisfies the conditions of our theorem and the proof is complete.

Corollary 27 (Iwasawa). *With notation as in Corollary* 25: *If*

$$\alpha_n = p^{-(n+1)} \frac{\zeta_n}{\zeta_n - 1}$$

$$\beta_n = p^{-(n+1)} \sum_{i=0}^{n} \zeta_n^{p^i}$$

then α_n *and* $(1-\sigma)\beta_n$ *are elements of* $\mathfrak{X}_n$ *for all* $\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p)$.

Proof. Let

$$g(T) = \frac{T+1}{T} \quad \text{and} \quad h(T) = \sum_{i=0}^{\infty} [p^i](T).$$

This series converges by Lemma 20(ii). Let $\zeta_i = \zeta_n^{p^{n-i}}$, and define α_i, β_i analogously to α_n and β_n. Let $\tilde{\sigma} \in G_\infty$, such that $\tilde{\sigma}/H_n = \sigma$. It is then clear that,

$$\varepsilon_i g = g(\zeta_i - 1) = p^{i+1}\alpha_i$$
$$\varepsilon_i((1-\tilde{\sigma})h) = p^{i+1}(1-\sigma)\beta_i.$$

An easy computation shows $T_{n,i}(\alpha_n) = \alpha_i$ and $T_{n,i}(\beta_n) = \beta_i$. Hence the corollary follows from the previous theorem with α equal to either α_n or β_n and f_α equal to either g or f. (See remark at the end of this section.)

Recall that $\mathfrak{X}_\infty = \varprojlim \mathfrak{X}_n$, the inverse limit being taken with respect to the trace maps; also recall that $\mathscr{S}$ is the homomorphism introduced in III. We then have:

Theorem 28. *There exists a unique map* $\theta (= \theta_v)$ *from* $\mathfrak{X}_\infty$ *into* $\mathcal{O}_H((T))$ *such that the following diagrams commute for all* $n \geqq 0$.

$$\begin{array}{ccc} \mathfrak{X}_\infty & \xrightarrow{\theta} & \mathcal{O}_H((T)) \\ \downarrow{\scriptstyle T_{\infty,n}} & & \downarrow{\scriptstyle \varepsilon_n} \\ H_n & \xrightarrow{\pi^{n+1}\varphi^n} & H_n \end{array}$$

Proof. The proof is exactly analogous to the proof of Theorem 16, using Theorem 26 in place of Theorem 15.

Corollary 29. θ *defines a topological* $\mathscr{A}_\infty$*-isomorphism from* $\mathfrak{X}_\infty$ *onto* $\{f \in \mathcal{O}_H((T)) : \mathscr{S}(f) = \pi\varphi f\}$.

Proof. Let $\alpha \in \mathfrak{X}_\infty$. If $f = \theta(\alpha)$ then

$$\varepsilon_i \mathscr{S}(f) = T_{i+1,i}(\varepsilon_{i+1}(f)) = \varepsilon_i(\pi\varphi(f)).$$

Hence by our uniqueness principle $\mathscr{S}(f) = \pi\varphi f$. On the other hand if $g \in \mathcal{O}_H((T))$ and $\mathscr{S}(g) = \pi\varphi g$ then since $\mathscr{S}(g)_\pi$ has the same polar part as g by (III, 2) we see easily that $g \in T^{-1} \cdot I$ and that $\mathrm{Res}_0 g \in \mathcal{O}_K$. Thus by Theorem 26 $c_g = \{\pi^{-(n+1)}\varphi^{-(n+1)}\varepsilon_n g\} \in \mathfrak{X}_\infty$; and clearly the map $g \mapsto c_g$ is the inverse of θ. The remaining statements may be proven using arguments similar to those used in the proof of Corollary 17.

Remark. This theorem relates the modules $\mathfrak{X}_n$ to an eigenspace of the operator $\varphi^{-1}\mathscr{S}$. In the height one theory alluded to after Corollary 25 we show how the other eigenspaces are related to modules with interesting properties. For instance, the image of λ, and $\mathrm{Log}(1+T)$ correspond to the eigenspaces with eigenvalues $\pi^{-1}p$, and 1, respectively. In fact if f is as in Corollars 25, and, g and h are as in Corollary 27 then,

$$\mathscr{S}(\tilde{f}) = \tilde{f}, \quad \delta(g) = p \cdot g \quad \text{and} \quad \mathscr{S}((1-\tilde{\sigma})h) = p(1-\tilde{\sigma})h,$$

where $\tilde{f} = (1-a^{-1})p(1-p)^{-1} + f$. Using the above ideas we show (in the situation of Corollary 27) that

$$\mathfrak{X}_n = \mathscr{A}_\infty \alpha_n + \mathscr{I}_0 \beta_n$$

where $\mathscr{I}_0$ is the closed ideal in $\mathscr{A}_\infty$ generated topologically by $\{1-\sigma\}_{\sigma \in G_\infty}$. This result was originally proven, by Iwasawa [I$_2$], using the explicit reciprocity law.

Remark. Let $\delta: \mathscr{M} \to \mathcal{O}_H((T))$ be the intrinsic logarithmic derivation,

$$\delta: f \mapsto \frac{1}{\lambda'}\frac{f'}{f}.$$

$\left(\text{Here } g' = \dfrac{d}{dT}g.\right)$ It is not difficult to see that

$$\pi\delta\mathscr{N}f = \mathscr{S}\delta f.$$

Therefore, if $f \in \mathscr{M}_\infty$ then $\mathscr{S}(\delta f) = \pi\varphi\delta f$. By Theorem 16 and the previous theorem, we see that this allows us to define a homomorphism ψ from X_∞ into $\mathfrak{X}_\infty$. This homomorphism is intimately connected with the class field theory of H_∞ and will be discussed more fully in a subsequent paper.

References

[C] Coates, J., Wiles, A.: On p-adic L-functions and Elliptic Units. Journal Australian Math. Soc., A, **25**, 1–25 (1978)

[F] Fontaine, J.M.: Corps de Séries Formelles et Extensions Galoisiennes des Corps Locaux, Séminaire de Théorie des Nombres de Grenoble, 28–38 (1971–72)

[Fr] Fröhlich, A.: Formal Groups, Lecture Notes in Mathematics, No. 74. Berlin: Springer-Verlag 1968

[I_1] Iwasawa, K.: Explicit Formulas for the Norm Residue Symbol. Jour. Math. Soc. Japan **20**, 151–164 (1968)

[I_2] Iwasawa, K.: On Some Modules in the Theory of Cyclotomic Fields. Jour. Math. Soc. Japan **20**, 42–82 (1964)

[L] Lubin, J., Tate, J.: Formal Complex Multiplication in Local Fields. Ann. of Math. **81**, 380–387 (1965)

[W] Wiles, A.: Higher Explicit Reciprocity Laws. Ann. of Math. **107**, 235–254 (1978)

Received April 2, 1978/March 5, 1979