A simple proof of a lemma of Coleman

BY A. SAIKIA

Department of Pure Mathematics and Mathematical Statistics
Cambridge, CB2 1SB


1. Introduction

Let $p$ be an odd prime. The results in this paper concern the units of the infinite extension of $\mathbb{Q}_p$ generated by all $p$-power roots of unity. Let

$$\Phi_n = \mathbb{Q}_p(\mu_{p^{n+1}})$$

where $\mu_{p^{n+1}}$ denote the $p^{n+1}$-th roots of 1. Let $\wp_n$ be the maximal ideal of the ring of integers of $\Phi_n$ and let $U_n$ be the units congruent to 1 modulo $\wp_n$. Let $\zeta_n$ be a fixed primitive $p^{n+1}$-th root of unity such that $\zeta_p = \zeta_{n-1} \forall n \geq 1$. Put $\pi_n = \zeta_n - 1$. Thus $\pi_n$ is a local parameter for $\Phi_n$. Let

$$\mathfrak{S}_n = \text{Gal}(\Phi_n/\mathbb{Q}_p).$$

Kummer already exploited the obvious fact that every $u_0 \in U_0$ can be written in the form

$$u_0 = f_0(\pi_0)$$

where $f_0(T)$ is some power series in $\mathbb{Z}_p[[T]]$. Here of course, the power series $f_0(T)$ is not uniquely determined. Let

$$U_\infty = \lim_{\leftarrow} U_n$$

the inverse limit being with respect to norm maps. Coates and Wiles (see [3]) discovered that any unit $u = (u_n) \in U_\infty$ has a unique power series $f_u(T)$ in $\mathbb{Z}_p[[T]]$ with $f_u(\pi_n) = u_n$. The uniqueness of such a power series is obvious by Weierstrass Preparation Theorem, but the existence is in no way obvious. They worked with the formal group of height one attached to an elliptic curve with complex multiplication at an ordinary prime, but their ideas apply to any Lubin-Tate group defined over $\mathbb{Z}_p$.

Almost immediately, Coleman [4] gave a totally different proof of the existence of the $f_u(T)$, which holds for all Lubin-Tate groups. We refer to such a power series as a Coleman power series. In this paper we adopt the same approach as [3]. We first prove the
following result which is stronger than the original one in [3].

**Theorem 1.** Given $u \in U_\infty$, there exists a unique power series $f_u(T) \in R$ such that

$$f_u(\zeta_n - 1) = u_n \quad \forall n \geq 0.$$ 

Let

$$\Phi_\infty = Q_p(\mu^\infty), \quad \mathcal{G}_\infty = \text{Gal}(\Phi_\infty/Q_p).$$

We define the Iwasawa algebra $\mathcal{G}_\infty$ by

$$\Lambda(\mathcal{G}_\infty) = \lim_{\leftarrow} \mathbb{Z}_p[\mathcal{G}_\infty/H],$$

where $H$ runs over the open subgroups of $\mathcal{G}_\infty$. Each $U_n$ is a $\mathbb{Z}_p$-module because it is pro-$p$, and so also is $U_\infty$. Thus $U_\infty$ is a compact $\mathbb{Z}_p$-module on which $\mathcal{G}_\infty$ act continuously. We can therefore extend this action to an action of the whole Iwasawa algebra $\Lambda(\mathcal{G}_\infty)$. Let $T_p(\mu)$ be given by

$$T_p(\mu) = \lim_{\leftarrow} \mu_{p^{n+1}}$$

where the inverse limit is with respect to the $p$-power maps or the norm maps (these are the same on $\mu_{p^{n+1}}$) in the tower $\Phi_n$ ($n = 0, 1, 2, \ldots$). Hence $T_p(\mu)$ is a free $\mathbb{Z}_p$-module of rank 1 with generator $(\zeta_n)$.

In section 3, we define a canonical $\mathcal{G}_\infty$-homomorphism

$$l_\infty : U_\infty \longrightarrow \Lambda(\mathcal{G}_\infty)$$

which is of fundamental importance in the Iwasawa theory of the $\Phi_n$ (where $n = 0, 1, 2, \ldots$). A second aim of the present paper is to show that the original method of Coates and Wiles can also be used to give a short proof of the following result of Coleman [4], [5].

**Theorem 2.** There is an exact sequence of $\Lambda(\mathcal{G}_\infty)$-modules

$$0 \longrightarrow T_p(\mu) \longrightarrow U_\infty \xrightarrow{l_\infty} \Lambda(\mathcal{G}_\infty) \xrightarrow{r_\infty} T_p(\mu) \longrightarrow 0.$$ 

For the definition of $r_\infty$, see section 3. Coleman’s proof ([4], [5]) of Theorem 2 is rather elaborate, especially his determination of the cokernel of $l_\infty$. In addition, there is interest in giving a different and simple proof because of the importance of the result in the Iwasawa theory of cyclotomic fields. Indeed, the proof of the first part of the “main
conjecture” on cyclotomic fields is the precise determination of the image under $l_\infty$ of the submodule of $U_\infty$ given by the cyclotomic units. This gives by far the simplest proof of a celebrated theorem of Iwasawa [8].

Notation.

We fix the following notation. We write

$$\psi : \mathcal{G}_\infty \xrightarrow{\sim} \mathbb{Z}_p^X$$

for the cyclotomic character, which is defined by

$$\zeta^\sigma = \zeta^{\psi(\sigma)} \quad \forall \sigma \in \mathcal{G}_\infty, \; \forall \zeta \in \mu_{\infty}. $$

Since $\mathbb{Z}_p^X = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$, we have the corresponding decomposition under the isomorphism $\psi$

$$\mathcal{G}_\infty = \Delta \times \Gamma,$$

where $\Delta$ is cyclic of order $p - 1$ and $\Gamma$ is isomorphic to $\mathbb{Z}_p$. Clearly, $\Gamma = \text{Gal}(\Phi_\infty/\Phi_0)$ and $\Delta$ is isomorphic to $\text{Gal}(\Phi_0/\mathbb{Q}_p)$ under restriction.

Let $\chi$ be the restriction of $\psi$ to $\Delta$, so that $\chi$ generates the group of characters of $\Delta$. Write $e_i$ for the orthogonal idempotent of $\chi^i$ in $\mathbb{Z}_p[\Delta]$, i.e.

$$e_i = \frac{1}{p - 1} \sum_{\sigma \in \Delta} \chi^i(\sigma)\sigma^{-1}.$$

If $A$ is any $\mathbb{Z}_p[\Delta]$-module, we denote by $A^{(i)} = e_i A$ the submodule of $A$ on which $\Delta$ acts via $\chi^i$. Then we have the decomposition

$$A = \bigoplus A^{(i)}.$$

Let $R$ be the ring of formal power series in an indeterminate $T$ with coefficient in $\mathbb{Z}_p$. We fix a topological generator $\gamma_0$ of $\Gamma$ so that

$$\Lambda(\Gamma) \xrightarrow{\sim} R, \quad \gamma_0 \mapsto 1 + T.$$

Suppose $C$ is a compact $\mathbb{Z}_p$ module on which $\Gamma$ acts continuously. Then $C$ has a unique $R$-module structure such that

$$\gamma_0 x = (1 + T)x \quad \forall x \in C.$$
2. Existence of Coleman Power Series

We exploit some basic facts about Lubin-Tate groups to prove the existence of Coleman Power series. For an account of Lubin-Tate groups see [1], [9] or [10]. Let $G$ be any Lubin-Tate formal group over $\mathbb{Z}_p$ which is attached to the local parameter $p$ of $\mathbb{Z}_p$. If $a \in \mathbb{Z}_p$, we write $[a]_G(T)$ for the formal power series in $\mathbb{Z}_p[[T]]$ corresponding to the endomorphism $[a]$ of $G$. Hence

$$[a]_G(T) = aT + \ldots$$

If $G$ is the formal multiplicative group $\hat{G}_m$, we have

$$[p]_{\hat{G}_m}(T) = (1 + T)p - 1.$$ 

However, it is more convenient for us to use the unique Lubin-Tate group $B$ such that

$$[p]_B(T) = Tp + pT.$$ 

Then it is easy to see (cf. [13])

$$[\xi]_B(X) = \xi X \quad \forall \xi \in \mu_{p-1}. \quad (1)$$

(For a proof, see [13].) By Lubin-Tate theory, $\hat{G}_m$ and $B$ are isomorphic over $\mathbb{Z}_p$, and we fix an isomorphism

$$\theta : \hat{G}_m \sim \rightarrow B$$

$$\theta(T) = T + \ldots .$$

Then we have

$$[a]_B(\theta(T)) = \theta([a]_{\hat{G}_m}(T)). \quad (2)$$

For each $n \geq 0$ let $B_{p^{n+1}}$ denote the kernel of the endomorphism $[p^{n+1}]_B$ of $B$. We put $v_n = \theta(\zeta_n - 1)$ so that $v_n$ is a generator of $B_{p^{n+1}}$.

**Lemma 2.1.** Let $\chi$ be the restriction of the cyclotomic character $\psi$ to $\Delta$. Then

$$v^\sigma_0 = \chi(\sigma)v_0 \quad \forall \sigma \in \Delta.$$ 

**Proof.** Since $v_0 = \theta(\zeta_0 - 1) \Rightarrow v^\sigma_0 = \theta(\zeta^\sigma_0 - 1)$, by the definition of $\chi$ we have

$$v^\sigma_0 = \theta([\chi(\sigma)]_{\hat{G}_m}(\zeta_0 - 1)).$$

Then the assertion follows using (1) and (2).
The main idea of our proof of Theorems 1 and 2 is to use certain explicit elements of $U_\infty$ which were first written down in [3].

**Lemma 2.2.** Let $\beta$ denote the unique $(p-1)$-th root of $(1-p)$ satisfying $\beta \equiv 1 \mod p$. Then $N_{m,n}(\beta - v_m) = \beta - v_n$ and $(\beta - v_n) \in U_\infty$.

**Proof.** The minimal polynomial of $(\beta - v_n)$ over $\Phi_{n-1}$ is

$$(\beta - x)^p + p(\beta - x) = v_{n-1}.$$ 

Noting that $p$ is odd, we get

$$N_{n,n-1}(\beta - v_n) = \beta^p + p\beta - v_{n-1} = \beta - v_{n-1}.$$ 

We stress that it is quite miraculous that one can write down such explicit element of $U_\infty$. From now, we will denote this element by $\alpha$, i.e.

$$\alpha = \left((\beta - v_n)\right) \in U_\infty,$$

$$\alpha_i = \alpha^{e_i} \in U^{(i)}_\infty \quad (3).$$

It is very useful to us because of the following:

**Proposition 2.3.** $U^{(i)}_\infty = R\alpha_i, \quad i \neq 0, 1 \mod (p-1).$

This is very well known and is given in detail in [3]. Hence we only sketch the proof before turning to the more delicate case of $i \equiv 0, 1 \mod (p-1)$.

Let $M_n$ denote the maximal abelian $p$-extension of $\Phi_n$. Let

$$M_\infty = \cup_{n \geq 0} M_n.$$ 

Then $M_\infty$ is the maximal abelian $p$-extension of $\Phi_\infty$. Put

$$X_n = \text{Gal}(M_n/\Phi_n), \quad X_\infty = \text{Gal}(M_\infty/\Phi_\infty).$$ 

By local class field theory, we have an exact sequence of Galois modules for all $n \geq 0$

$$1 \rightarrow U_n \rightarrow X_n \rightarrow \mathbb{Z}_p \rightarrow 1 \quad (4)$$

Passing to the projective limit, we have an exact sequence of $\mathbb{Z}_\infty$-modules

$$1 \rightarrow U_\infty \rightarrow X_\infty \rightarrow \mathbb{Z}_p \rightarrow 1 \quad (5)$$
By definition, $\Gamma_n$ acts on $X_\infty$ by conjugation and it is easy to see (cf [9]) that $(\gamma_0^p - 1)X_\infty$ correspond to the commutator subgroup of $\text{Gal}(M_\infty/\Phi_n)$. Hence

$$X_\infty/(\gamma_0^p - 1)X_\infty = \text{Gal}(M_n/\Phi_n) \quad (6)$$

We have an exact sequence of Galois groups

$$1 \to \text{Gal}(M_n/\Phi_n) \to \text{Gal}(M_n/\Phi_n) = X_n \to \text{Gal}(\Phi_\infty/\Phi_n) \to 1 \quad (7)$$

But $\Delta$ acts trivially on $\text{Gal}(\Phi_\infty/\Phi_n)$. By (4), (5), (6) and (7)

$$U^{(i)}_n \simeq U^{(i)}_\infty/(\gamma_0^p - 1)U^{(i)}_\infty, \quad i \not\equiv 0 \pmod{(p - 1)}. \quad (8)$$

For $i \neq 0, 1 \pmod{(p - 1)}$, $U^{(i)}_n$ is a free $\mathbb{Z}_p$-module of rank $p^n$. It follows easily from the structure theory of $R$-modules that $U^{(i)}_\infty$ is a free $R$-module of rank 1. Then one can use logarithmic derivatives mod $p$ (as explained in [3]) to show that that $\alpha_i$ generates $U^{(i)}_\infty$ as an $R$-module.

We will now find suitable generators for $U^{(1)}_\infty$ and $U^{(0)}_\infty$.

**Proposition 2.4.** $U^{(1)}_\infty = T_p(\mu)R\alpha_1$.

By (8), we have $U^{(1)}_\infty/(\gamma_0 - 1)U^{(1)}_\infty \simeq U^{(1)}_0$. By Nakayama’s lemma, it suffices to produce elements in $U^{(1)}_\infty$ that project down to $\mathbb{Z}_p$-generators of $U^{(1)}_0$. We know that $U^{(1)}_0$ is a $\mathbb{Z}_p$-module of rank 1 and torsion $\mu_p$. Logarithmic derivative mod $p$ of $(\beta - v_0)^{e_1}$ is nonzero (its value is $-1/\beta$, as deduced in [3]), so it is not a $p$-th power in $U^{(1)}_0$. If $(\beta - v_0)^{e_1}$ is not a $p$-th root of 1, then the $p$-th roots of unity and $(\beta - v_0)^{e_1}$ will generate $U^{(1)}_0$ as a $\mathbb{Z}_p$-module. All we need now is the following:

**Lemma 2.5.** $(\beta - v_0)^{e_1}$ is not a $p$-th root unity.

**Proof.** We have

$$(\beta - v_0)^{e_1p} = \prod_{\sigma \in \Delta} (\beta - v_0)_{\mathbb{F}_p}^{p\chi(\sigma)\sigma^{-1}}$$

$$= \prod_{\sigma \in \Delta} \left(1 - \frac{p}{p - 1}\chi(\sigma)\beta^{-1}\chi(\sigma^{-1})v_0\right) \mod p\psi_0^2$$

$$= \prod_{\sigma \in \Delta} \left(1 - \frac{p}{p - 1}\beta^{-1}v_0\right) \mod p\psi_0^2$$

$$= 1 - \beta^{-1}pv_0 \mod p\psi_0^2.$$
Hence \( (\beta - \nu_0)^{\xi_1} \) cannot be a \( p \)-th root of unity.

So \((\zeta_n)\) and \(\alpha_1\) generate \( U^{(1)}_{\infty} \) over \( R \).

Now we find \( R \)-generator for \( U^{(0)}_{\infty} \):

**Proposition 2.6.** \( \left( \frac{\zeta_n^0 - 1}{\zeta_n - 1} \right)^{\xi_0} \) generates \( U^{(0)}_{\infty} \) as an \( R \)-module.

**Proof.** Clearly,

\[
\Phi_n^\times = U_n \times W \times (\zeta_n - 1)^\mathbb{Z},
\]

where \( W \) is the group of roots of unity in \( \Phi_n \) of order prime to \( p \).

Let \( \hat{\Phi}_n^\times \) denote the \( p \)-adic completion of the multiplicative group of \( \Phi_n^\times \). Then,

\[
\hat{\Phi}_n^\times \cong U_n \times \mathbb{Z}_p.
\]

Using the snake lemma for the exact sequence (5), we have

\[
1 \rightarrow U^\Gamma_{\infty} \rightarrow X^\Gamma_{\infty} \rightarrow \mathbb{Z}_p \rightarrow (U_{\infty})_{\Gamma} \rightarrow (X_{\infty})_{\Gamma} \rightarrow \mathbb{Z}_p \rightarrow 1.
\]

Since \( X^\Gamma_{\infty} = 0 \) ( cf [6] ) we have

\[
1 \rightarrow \mathbb{Z}_p \rightarrow U^{(0)}_{\infty}/(\gamma_0 - 1)U^{(0)}_{\infty} \rightarrow X^{(0)}_{\infty}/(\gamma_0 - 1)X^{(0)}_{\infty} \rightarrow \mathbb{Z}_p \rightarrow 1 \quad (9)
\]

Let \( U'_n \) be the units in \( U_n \) with norm 1 to \( \mathbb{Q}_p \). It is an easy exercise in local class field theory to show that

\[
U'_n = \{ u_n : \forall \ m \geq n \ \exists u_m \in U_m, \ N_{m,n}(u_m) = u_n \}
\]

But (4) implies that we have an exact sequence of Galois modules

\[
1 \rightarrow U'_0 \rightarrow \text{Gal}(M_0/\Phi_{\infty}) \rightarrow \mathbb{Z}_p \rightarrow 1
\]

and by (6),

\[
1 \rightarrow U^{(0)}_{0} \rightarrow X^{(0)}_{\infty}/(\gamma_0 - 1)X^{(0)}_{\infty} \rightarrow \mathbb{Z}_p \rightarrow 1.
\]

But \( f \) is an isomorphism as \( U^{(0)}_{0} = 1 \). Then (9) tells us that

\[
\mathbb{Z}_p \cong U^{(0)}_{\infty}/(\gamma_0 - 1)U^{(0)}_{\infty}.
\]
It is enough to find the image of $1_{\mathbb{Z}_p}$ in $U^{(0)}_{\infty}/(\gamma_0 - 1)U^{(0)}_{\infty}$. We have the following diagram

$$
\begin{array}{c c c c c}
1 & \longrightarrow & U_n & \longrightarrow & \Phi_n^* \\
\gamma_0 - 1 & \downarrow & \gamma_0 - 1 & \downarrow & \gamma_0 - 1 \\
1 & \longrightarrow & U_n & \longrightarrow & \Phi_n^* \\
\end{array}
$$

By the snake lemma, the image of $1_{\mathbb{Z}_p}$ in $U_n/(\gamma_0 - 1)U_n$ is $\frac{\gamma_0 - 1}{\zeta_0 - 1}$. Hence the image of $1_{\mathbb{Z}_p}$ in $U^{(0)}_{\infty}/(\gamma_0 - 1)U^{(0)}_{\infty}$ is $\left(\frac{\gamma_0 - 1}{\zeta_0 - 1}\right)^{\xi_0}$. By Nakayama’s lemma, $\left(\frac{\gamma_0 - 1}{\zeta_0 - 1}\right)^{\xi_0}$ generates $U^{(0)}_{\infty}$ as a $R$-module. This proves the proposition.

Theorem 1 is almost an immediate consequence of propositions (2.3), (2.4) and (2.6) as follows. These propositions tell us that $U_{\infty}$ is generated over $R$ by $\alpha = \left((\beta - v_n)\right)$, $x_1 = \left(\frac{\gamma_0 - 1}{\zeta_0 - 1}\right)$, $x_2 = (\zeta_n)$. But $\alpha, x_1, x_2$ clearly all have Coleman power series, namely $f_\alpha(T) = \beta - \theta(T)$, $f_{x_1}(T) = \frac{(1 + T)^{\psi(\gamma_0) - 1}}{T}$, and $f_{x_2}(T) = (1 + T)$. Also, it is easy to see that

$$
f_{u_1u_2}(T) = f_{u_1}(T)f_{u_2}(T)
$$

$$
f_\sigma(T) = f_u((1 + T)^{\psi(\sigma) - 1}) \quad \forall \sigma \in \mathcal{S}_\infty.
$$

Thus all the units in $U_{\infty}$ have a Coleman power series.

It is useful to note that

$$
f_u((1 + T)^p - 1) \mid_{T = \zeta_n - 1} = f_u(\zeta_n - 1 - 1) = u_{n-1} = N_{n,n-1}f_u(\zeta_n - 1) = \prod_{\eta \in \mu_p} f_u(\eta \zeta_n - 1) = \prod_{\eta \in \mu_p} f_u(\eta(1 + T) - 1) \mid_{T = \zeta_n - 1}
$$

and so the Weierstrass Preparation Theorem implies that

$$
f_u((1 + T)^p - 1) = \prod_{\eta \in \mu_p} f_u(\eta(1 + T) - 1). \quad (10)
$$
Measures and Power Series

It is well known and almost obvious that the elements of $\Lambda(G_\infty)$ are just the $\mathbb{Z}_p$-valued measures on $G_\infty \simeq \mathbb{Z}_p^\times$ (see [11], [12]). On the other hand, we can identify the $\mathbb{Z}_p$-values measures on $\mathbb{Z}_p^\times$ i.e. $\Lambda(\mathbb{Z}_p^\times)$ with a subset of $R = \mathbb{Z}_p[[T]]$ as follows. There is a 1-1 correspondence between $\mathbb{Z}_p$-valued measures on $\mathbb{Z}_p$ and power series in $R$. If $\mu$ is a $\mathbb{Z}_p$-valued measures on $\mathbb{Z}_p$, the corresponding power series in $R$ is given by

$$h_\mu(T) = \sum_{n=0}^{\infty} \left( \int_{\mathbb{Z}_p} \left( \frac{x}{n} \right) d\mu \right) T^n = \int_{\mathbb{Z}_p} \left( 1 + T \right)^x d\mu.$$

The fact that this is a bijection follows from Mahler’s theorem for continuous functions on $\mathbb{Z}_p$ (see [9] for details). On the other hand, there is a topological isomorphism of $\mathbb{Z}_p$-algebra

$$\tilde{\phi} : \Lambda(\mathbb{Z}_p) \rightarrow R, \quad \tilde{\phi}(1_\mathbb{Z}_p) \mapsto 1 + T.$$

It is well known that $\tilde{\phi}(\mu) = h_\mu(T)$ for all $\mu$ in $\Lambda(\mathbb{Z}_p)$.

**Proposition 3.1.**

$$\Lambda(\mathbb{Z}_p^\times) = \{ \mu \in \Lambda(\mathbb{Z}_p) | W(h_\mu) = h_\mu \}.$$

where

$$W(h)(T) = h(T) - \frac{1}{p} \sum_{\eta \in \mathbb{Z}_p} h(\eta(1 + T) - 1).$$

**Proof.** Any measure $\mu$ on $\mathbb{Z}_p^\times$ can be extended to a measure $\tilde{\mu}$ on $\mathbb{Z}_p$, as follows. Let $C_p$ be the completion of an algebraic closure of $\mathbb{Q}_p$. If $f : \mathbb{Z}_p \rightarrow C_p$ is a continuous function, we define

$$\int_{\mathbb{Z}_p} f d\mu = \int_{\mathbb{Z}_p^\times} f |_{\mathbb{Z}_p^\times} d\mu.$$

Conversely, if we have a measure $\mu$ on $\mathbb{Z}_p$ we get a measure $\mu^*$ on $\mathbb{Z}_p^\times$.

If $g : \mathbb{Z}_p^\times \rightarrow C_p$ is a continuous function and $\epsilon_{\mathbb{Z}_p^\times}$ is the characteristic function of $\mathbb{Z}_p^\times$ then

$$\int_{\mathbb{Z}_p^\times} g d\mu^* = \int_{\mathbb{Z}_p^\times} \tilde{g} \epsilon_{\mathbb{Z}_p^\times} d\mu.$$

Here $\tilde{g}$ is any continuous extension of $g$ to $\mathbb{Z}_p$.

We have

$$\Lambda(\mathbb{Z}_p^\times) = \{ \mu \in \Lambda(\mathbb{Z}_p) | \mu^* = \mu \}.$$
It is well known that $\mu_h^* = \mu_{W(h)}$ (see [9] or [12]) where $\mu_h$ is the measure associated with the power series $h \in R$. So the proposition is proved.

Given a unit $u$ in $U_\infty$, let $f_u(T)$ be its Coleman power series. Define

$$L(u)(T) = \log f_u(T) - \frac{1}{p} \log f_u((1 + T)^p - 1). \quad (11)$$

Using (10), it is easy to see that $L(u)(T) \in R$ and $W(L(u))(T) = L(u)(T)$.

Thus $L(u)(T)$ gives us a measure $\mu_{L(u)}$ on $\mathbb{Z}_p^\times$. We get a corresponding measure $l_\infty(u)$ on $\mathcal{G}_\infty$ via the isomorphism $\psi : \mathcal{G}_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times$ where

$$\int_{\mathcal{G}_\infty} f(\sigma) dl_\infty(u)(\sigma) = \int_{\mathbb{Z}_p^\times} f(\psi^{-1}(x)) d\mu_{L(u)}(x). \quad (12)$$

This gives us a map

$$l_\infty : U_\infty \longrightarrow \Lambda(\mathcal{G}_\infty).$$

**Lemma 3.2.** $\text{Ker}(l_\infty) = T_p(\mu)$.

**Proof.** Given $\xi \in T_p(\mu)$, we have $\xi = (\zeta_n)^a$ for some $a \in \mathbb{Z}_p$ and $f_\xi(T) = (1 + T)^a$. Hence $L_\xi(T) = \log(1 + T)^a - \frac{1}{p} \log(1 + T)^{ap} = 0$. Thus, $T_p(\mu) \subset \text{Ker} l_\infty$.

Conversely, suppose $l_\infty(u) = 0$. Then $L(u)(T) = 0$. Therefore, $f_u(T)^p = f_u((1 + T)^p - 1)$. Substituting $T = \zeta_n - 1$, we find that $u_n^p = u_{n-1}$. With $T = 0$, we get

$$f_u(0)^p = f_u(0) \equiv_{\mod p} u_0^p = f_u(0) = 1.$$  

Hence we have $\text{Ker} l_\infty \subset T_p(\mu)$.

We can define a map

$$r_\infty : \Lambda(\mathcal{G}_\infty) \longrightarrow T_p(\mu)$$

by the formula

$$r_\infty(\mu) = (\zeta_n)^{\int_{\mathcal{G}_\infty} \psi(\sigma)d\mu}.$$  

We now proceed to show that $\text{Im}(l_\infty) = \text{Ker}(r_\infty)$ using the ideas of logarithmic derivatives as introduced in [2].

**Logarithmic Derivatives**
Let $\hat{G}_a$ be the formal additive group with parameter $Z$. We have the logarithm map

$$\hat{G}_m \xrightarrow{\sim} G_a$$

$$Z = \log(1 + T) = T - \frac{T^2}{2} + \ldots$$

Clearly, we have $\frac{d}{dZ} = (1 + T) \frac{d}{dT}$. Let $D$ be the operator $(1 + T) \frac{d}{dT}$ on $R$ (see [3]). The $k$-th logarithmic derivative of a unit $u \in U_\infty$ is defined as

$$\delta_k(u) = D^k \log f_u(T) \mid_{T=0}, \quad k = 1, 2, 3, \ldots$$

It is obvious that $\delta_k : U_\infty \rightarrow \mathbb{Z}_p$ is a homomorphism of $\mathbb{Z}_p$ modules, and one sees easily that $\delta_k(u^\sigma) = \psi^k(\sigma) \delta_k(u)$.

For any element $h \in R$, we have (see [9])

$$\int_{\mathbb{Z}_p} x^k d\mu_h = D^k h(0)$$

Hence, by (11) and (12)

$$\int_{G_\infty} \psi^k(\sigma) d\ell_\infty(u) = D^k L(u)(T) \mid_{(T=0)} = (1 - p^{k-1}) \delta_k(u). \quad (13)$$

By (13), we have

$$\int_{G_\infty} \psi(\sigma) d\ell_\infty(u_\infty) = (1 - p^{1-1}) \delta_1(u_\infty) = 0.$$

and hence $\text{Im} (l_\infty) \subset \text{Ker} (r_\infty)$. The difficult part of the proof of the Theorem 2 is to show that $\text{Im} (l_\infty) = \text{Ker} (r_\infty)$. The key to our approach is the following result. Recall that $\alpha \in U_\infty$ is our special unit defined by (3).

**Proposition 3.3.** $\delta_k(\alpha)$ is a unit for $k = 1, 2, \ldots p - 1$, and $\delta_p(\alpha) = p \times \text{ a unit.}$

Logarithmic derivatives are intrinsic, i.e., they do not depend on the Lubin-Tate group we use to calculate them. We will calculate logarithmic derivatives of the unit $\alpha$ using the Lubin-Tate group $B$ which we introduced in section 2.

Let $\lambda : B \xrightarrow{\sim} \hat{G}_a$ be the normalized logarithm map and $\phi : \hat{G}_a \xrightarrow{\sim} B$ be the exponential map. We have (as shown in [13]) $Z = \lambda(X) = X + b_p X^p + \ldots$ and $X = \phi(Z) = Z + a_p Z^p + \ldots$. Also $D = \frac{d}{dZ} = \frac{1}{\lambda'(X)} \frac{d}{dX}$ and $\lambda(\phi(Z)) = Z$. Therefore, $\frac{1}{\lambda'(X)} = \phi'(Z)$.
We need the following lemma to calculate $\delta_p(\alpha)$:

**Lemma 3.4.** With notation as above, $pb_p \equiv 1 \mod p^2$.

**Proof.** We know (see [13]) that

$$\lambda(X) = \lim_{n \to \infty} \frac{1}{p^n} [p^n]_B(X).$$

We now calculate the coefficient of $X^p$ in $\lambda(X)$.

\[
\begin{align*}
\frac{1}{p} [p] (X) &= X + \frac{1}{p} X^p. \\
\frac{1}{p^2} [p^2] (X) &= X + \frac{1}{p} (1 + p^{p-1}) X^p + \ldots \\
\frac{1}{p^3} [p^3] (X) &= X + \frac{1}{p} (1 + p^{p-1} + p^{2p-2}) X^p + \ldots \\
\frac{1}{p^4} [p^4] (X) &= X + \frac{1}{p} (1 + p^{p-1} + p^{2p-2} + p^{3p-3}) X^p + \ldots
\end{align*}
\]

It is clear that if the coefficient of $X^p$ in $\frac{1}{p^n} [p^n]_B(X)$ is $c_n$, then $c_n \equiv \frac{1}{p} \mod p^{p-2}$. Thus, $b_p \equiv \frac{1}{p} \mod (p^{p-2})$, i.e. $pb_p \equiv 1 \mod (p^{p-1})$. This proves the lemma.

**Proof of the Proposition 3.3.** Recalling that $X = \phi(Z)$, $f_\alpha(X) = \beta - X$ and $\frac{d}{dZ} = \frac{1}{X(Z) \frac{d}{dX}}$, we obtain

$$\frac{d}{dZ} \log f_\alpha(X) = \frac{1}{X(Z) \beta - X} = -\frac{1}{\beta} \phi'(Z) \left[ 1 + \phi(Z) \frac{\phi(Z)^2}{\beta^2} + \ldots \right] = h_\alpha(Z) \text{ (say).}$$

Since $\phi(Z) = Z + a_p Z^p + \ldots$, we have $h_\alpha(Z) = -\frac{1}{\beta} \left[ 1 + pa_p Z^{p-1} + \ldots \right] \times [1 + \frac{(Z + a_p Z^p + \ldots)}{\beta} + \frac{(Z + a_p Z^p + \ldots)^2}{\beta^2} + \ldots]$. It follows that

$$\delta_k(\alpha) = -\frac{(k - 1)!}{\beta^k} \quad \text{for} \quad k = 1, \ldots, p - 1.$$

On the other hand,

$$\delta_p(\alpha) = \text{The coefficient of} \ Z^{p-1} \text{ in } h_\alpha(Z) \times (p - 1)!$$

$$= -\frac{(p - 1)!}{\beta} \left[ pa_p + \frac{1}{\beta^{p-1}} \right].$$

12
We have \( X = \phi(\lambda(X)) = \lambda(X) + a_p(\lambda(X))^p + \ldots \). Substituting the expression for \( \lambda(X) \) in terms of \( X \), we get \( X = X + b_pX^p + a_p(X + b_pX^p + \ldots)^p + \ldots \). Now it is clear that \( a_p = -b_p \). Hence

\[
\delta_p(\alpha) = -\frac{(p-1)!}{p} \left[ -pb_p + \frac{1}{1-p} \right] = \text{unit} \times \left[ (-1 + \text{multiple of } p^{p-1}) + 1 + p + p^2 + \ldots \right] \equiv p \times \text{unit} \mod (p^2).
\]

This proves the proposition (3.3).

As

\[
Z_p[\Delta] = \bigoplus_{i=0}^{p-2} Z_p[\Delta]e_i \simeq \bigoplus_{i=0}^{p-2} Z_p,
\]

where the map from \( Z_p[\Delta]e_i \) to \( Z_p \) is given by evaluation at \( \chi^i \), we obtain

\[
\Lambda(\mathcal{S}_\infty) \simeq Z_p[\Delta][[T]] \simeq \bigoplus_{i=0}^{p-2} Z_p[[T]], \text{ with } \gamma_0 \mapsto 1 + T. \quad (14)
\]

Explicitly, the last isomorphism is given as follows:

Let \( \mu \in \Lambda(\mathcal{S}_\infty) \) correspond to \( h_\mu(T) = \sum_{n=0}^{\infty} c_n T^n \) in \( Z_p[\Delta][[T]] \), then \( h_\mu(T) = \sum_{i=0}^{p-2} h_i(T)e_i \), where \( h_i(T) = \sum_{n=0}^{\infty} \chi^i(c_n) T^n \).

Recall that \( \alpha \) is the special element of \( U_\infty \) defined by (3). Let \( l_\infty(\alpha) \in \Lambda(\mathcal{S}_\infty) \) correspond to \( g(T) = \sum_{n=0}^{\infty} c_n T^n \) in \( Z_p[\Delta][[T]] \). Under the isomorphisms in (14),

\[
l_\infty(\alpha) \mapsto g(T) \mapsto (\ldots, g_i(T), \ldots)
\]

where \( g_i(T) = \sum_{n=0}^{\infty} \chi^i(c_n) T^n \).

**Lemma 3.5.** For \( i = 0, 2, 3, \ldots, p - 2 \), \( g_i(T) \) is a unit in \( R \) and \( g_i(T) \) can be written as \( (1 + T - \psi(\gamma_0))h_1(T) \), where \( h_1(T) \) is a unit.

**Proof.** For \( k \equiv i \mod (p-1) \),

\[
g_i(\psi^k(\gamma_0) - 1) = \sum_{n=0}^{\infty} \chi^k(c_n)(\psi^k(\gamma_0) - 1)^n
= \int_{\mathcal{S}_\infty} \psi^k dl_\infty(\alpha)
= (1 - p^{k-1})\delta_k(\alpha) \quad \text{by (13)}
\]

13
Then it follows from proposition (3.3) that for \(i = 2, 3, \ldots, p - 2\), \(g_i(\psi^i(\gamma_0) - 1)\) is a unit. Hence \(g_i(T)\) is a unit. With \(i = p - 1\), we have
\[
g_0(\psi^{p-1}(\gamma_0) - 1) = (1 - p^{p-2}) \delta_{p-1}(\alpha) = a \text{ unit}.
\]
This implies that \(g_0(T)\) is also a unit. We have
\[
g_1(\psi(\gamma_0) - 1) = (1 - p^0)\delta_1(\alpha) = 0.
\]
So \(g_1(T)\) can be written as \((1 + T - \psi(\gamma_0))h_1(T)\). But \(g_1(\psi^p(\gamma_0) - 1)\) is \(p \times \text{unit}\) by proposition (3.3). It is clear that \(\psi^p(\gamma_0) - \psi(\gamma_0) = p \times \text{unit}\). But
\[
h_1(\psi^p(\gamma_0) - 1)(\psi^p(\gamma_0) - \psi(\gamma_0)) = p \times \text{unit}.
\]
Hence \(h_1(T)\) is a unit in \(R\).

Now we can finish the proof of Theorem 2 with the following lemma:

**Lemma 3.6.** \(Ker r_\infty \subset \text{Im } l_\infty\).

**Proof:** Consider \(r_\infty(\mu) = 0\). By definition, \(\int_{G_\infty} \psi d\mu = 0\). Let \(\mu \in \Lambda(G_\infty)\) correspond to \((f_0, f_1, \ldots, f_{p-2})\) in \(\bigoplus_{i=0}^{p-2} \mathbb{Z}_p[[T]]\) under (14). Then
\[
\int_{G_\infty} \psi d\mu = f_1(\psi(\gamma_0) - 1) = 0.
\]
This tells us that \(f_1(T) = (1 + T - \psi(\gamma_0))\tilde{\lambda}_1(T)\) for some \(\tilde{\lambda}_1(T) \in \mathbb{Z}_p[[T]]\). Since \(h_1(T)\) is a unit, we have \(\tilde{\lambda}_1(T) = \lambda_1(T)h_1(T)\). Thus
\[
f_1(T) = (1 + T - \psi(\gamma_0))\lambda_1(T)h_1(T) = \lambda_1(T)g_1(T).
\]
Also, \(g_i(T)\) is a unit for \(i = 0, 2, 3, \ldots, p - 2\). Hence \(f_i(T) = \lambda_i(T)g_i(T)\) for some \(\lambda_i(T) \in \mathbb{Z}_p[[T]]\). Then,
\[
f(T) = \sum_{i=0}^{p-2} \lambda_i(T)g_i(T)e_i
\]
\[
= \left(\sum_{i=0}^{p-2} \lambda_i(T)e_i\right) \left(\sum_{j=0}^{p-2} g_j(T)e_j\right).
\]
But \(\Lambda(G_\infty) \sim \bigoplus_{i=0}^{p-2} \mathbb{Z}_p[[T]]\) is a \(\mathbb{Z}_p\)-algebra isomorphism. Hence
\[
m_f = x l_\infty(\alpha)
\]
where \( x \) is some element of \( \Lambda(\mathcal{G}_\infty) \). But \( U_\infty \) is a \( \Lambda(\mathcal{G}_\infty) \) module and \( l_\infty \) is a \( \Lambda(\mathcal{G}_\infty) \)-homomorphism from \( U_\infty \) to \( \Lambda(\mathcal{G}_\infty) \). So,

\[
\mu_f = l_\infty(\alpha^x).
\]

This shows that

\[
\text{Ker } r_\infty \subset \text{Im } l_\infty.
\]

But we already saw that \( \text{Im } l_\infty \subset \text{Ker } r_\infty \). So we have completed the proof of Theorem 2.

**Remark.** This method should work for any Lubin-Tate group of height 1. When the height is greater than 1, one would require measure theory on the local ring of integers not isomorphic to \( \mathbb{Z}_p \).

**Acknowledgements.** The author thanks Prof. J. Coates for many helpful discussions at various stages of this paper.

**REFERENCES**


