A simple proof of a lemma of Coleman

By A. SAIKIA
Department of Pure Mathematics and Mathematical Statistics
Cambridge, CB2 1SB

(*appeared in Math. Proc. Camb. Phil. Soc. vol. 130 (2001)*)

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

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

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 Φ_n and let U_n be the units congruent to 1 modulo $\wp_n$. Let ζ_n be a fixed primitive p^{n+1}-th root of unity such that $\zeta_n^p = \zeta_{n-1}\ \forall n \geq 1$. Put $\pi_n = \zeta_n - 1$. Thus π_n is a local parameter for Φ_n. Let

$$\mathcal{G}_n = \mathrm{Gal}\,\big(\Phi_n/\mathbb{Q}_p\big).$$

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*

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

Let

$$\Phi_\infty = \mathbb{Q}_p\big(\mu_{p^\infty}\big), \;\; \mathcal{G}_\infty = \mathrm{Gal}\big(\Phi_\infty/\mathbb{Q}_p\big).$$

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

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

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_∞. Thus U_∞ 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 $\Lambda\big(\mathcal{G}_\infty\big)$. 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 Φ_n ($n = 0, 1, 2, \ldots$). Hence $T_p(\mu)$ is a free $\mathbb{Z}_p$-module of rank 1 with generator (ζ_n).

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

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

which is of fundamental importance in the Iwasawa theory of the Φ_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 $\Lambda\big(\mathcal{G}_\infty\big)$-modules*

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

For the definition of r_∞, see section 3. Coleman's proof ([4], [5]) of Theorem 2 is rather elaborate, especially his determination of the cokernel of l_∞. 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_∞ of the submodule of U_∞ 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

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

for the cyclotomic character, which is defined by

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

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

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

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

Let χ be the restriction of ψ to Δ, so that χ generates the group of characters of Δ. Write e_i for the orthogonal idempotent of χ^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 Δ acts via χ^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 γ_0 of Γ so that

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

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

$$\gamma_0.x = (1+T)x \qquad \forall x \in C.$$

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

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

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

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

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

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

(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

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

$$\theta(T) = T + \dots \quad .$$

Then we have

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

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 χ be the restriction of the cyclotomic character ψ to Δ. Then*

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

Proof. Since $v_0 = \theta(\zeta_0 - 1) \Rightarrow v_0^\sigma = \theta(\zeta_0^\sigma - 1)$, by the definition of χ we have $v_0^\sigma = \theta\big([\chi(\sigma)]_{\hat{G}_m}(\zeta_0 - 1)\big)$. 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_∞ which were first written down in [3].

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

Proof. The minimal polynomial of $(\beta - v_n)$ over Φ_{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_∞. From now, we will denote this element by α, i.e.

$$\alpha = \Big((\beta - v_n)\Big) \in U_\infty, \qquad \alpha_i = \alpha^{e_i} \in U_\infty^{(i)} \qquad (3).$$

It is very useful to us because of the following :

PROPOSITION 2.3. $U_\infty^{(i)} = R\alpha_i, \quad i \not\equiv 0, 1 \bmod (p-1)$.

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 $i \equiv 0, 1 \bmod (p-1)$.

Let M_n denote the maximal abelian p-extension of Φ_n. Let

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

Then M_∞ is the maximal abelian p-extension of Φ_∞. Put

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

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

$$1 \longrightarrow U_n \longrightarrow X_n \longrightarrow \mathbb{Z}_p \longrightarrow 1 \qquad (4)$$

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

$$1 \longrightarrow U_\infty \longrightarrow X_\infty \longrightarrow \mathbb{Z}_p \longrightarrow 1 \qquad (5)$$

By definition, Γ_n acts on X_∞ by conjugation and it is easy to see (cf [9]) that $(\gamma_0^{p^n}-1)X_\infty$ correspond to the commutator subgroup of $\mathrm{Gal}(M_\infty/\Phi_n)$. Hence

$$X_\infty/(\gamma_0^{p^n}-1)X_\infty = \mathrm{Gal}(M_n/\Phi_\infty) \qquad (6)$$

We have an exact sequence of Galois groups

$$1 \longrightarrow \mathrm{Gal}\big(M_n/\Phi_\infty\big) \longrightarrow \mathrm{Gal}\big(M_n/\Phi_n\big) = X_n \longrightarrow \mathrm{Gal}\big(\Phi_\infty/\Phi_n\big) \longrightarrow 1 \quad (7)$$

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

$$U_n^{(i)} \simeq U_\infty^{(i)}/(\gamma_0^{p^n}-1)U_\infty^{(i)}, \quad i \not\equiv 0 \bmod (p-1). \quad (8)$$

For $i \not\equiv 0, 1 \bmod (p-1)$, $U_n^{(i)}$ is a free $\mathbb{Z}_p$-module of rank p^n. It follows easily from the structure theory of R-modules that $U_\infty^{(i)}$ is a free R-module of rank 1. Then one can use logarithmic derivatives mod p (as explained in [3]) to show that that α_i generates $U_\infty^{(i)}$ as an R-module.

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

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

By (8), we have $U_\infty^{(1)}/(\gamma_0-1)U_\infty^{(1)} \simeq U_0^{(1)}$. By Nakayama's lemma, it suffices to produce elements in $U_\infty^{(1)}$ that project down to $\mathbb{Z}_p$-generators of $U_0^{(1)}$. We know that $U_0^{(1)}$ is a $\mathbb{Z}_p$-module of rank 1 and torsion μ_p. Logarithmic derivative mod p of $(\beta - v_0)^{e_1}$ is nonzero (its value is $-\frac{1}{\beta}$, as deduced in [3]), so it is not a p-th power in $U_0^{(1)}$. 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 $U_0^{(1)}$ as a $\mathbb{Z}_p$-module. All we need now is the following :

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

Proof. We have

$$\begin{aligned}
(\beta - v_0)^{e_1 p} &= \prod_{\sigma\in\Delta} (\beta - v_0)^{\frac{p}{p-1}\chi(\sigma)\sigma^{-1}} \\
&= \prod_{\sigma\in\Delta} \Big(1 - \frac{p}{p-1}\chi(\sigma)\beta^{-1}\chi(\sigma^{-1})v_0\Big) \mod p\wp_0^2 \\
&= \prod_{\sigma\in\Delta} (1 - \frac{p}{p-1}\beta^{-1}v_0) \mod p\wp_0^2 \\
&= 1 - \beta^{-1}pv_0 \mod p\wp_0^2.
\end{aligned}$$

Hence $(\beta - v_0)^{e_1}$ cannot be a p-th root of unity.

So (ζ_n) and α_1 generate $U_\infty^{(1)}$ over R.

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

PROPOSITION 2.6. $\left(\left(\frac{\zeta_n^{\gamma_0}-1}{\zeta_n-1}\right)^{e_0}\right)$ generates $U_\infty^{(0)}$ 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 Φ_n of order prime to p.
Let $\hat{\Phi}_n^\times$ denote th p-adic completion of the multiplicative group of $\Phi_n^\times$. Then,

$$\hat{\Phi}_n^\times \simeq U_n \times \mathbb{Z}_p.$$

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

$$1 \longrightarrow U_\infty^\Gamma \longrightarrow X_\infty^\Gamma \longrightarrow \mathbb{Z}_p \longrightarrow (U_\infty)_\Gamma \longrightarrow (X_\infty)_\Gamma \longrightarrow \mathbb{Z}_p \longrightarrow 1.$$

Since $X_\infty^\Gamma = 0$ (cf [6]) we have

$$1 \longrightarrow \mathbb{Z}_p \longrightarrow U_\infty^{(0)}/(\gamma_0 - 1)U_\infty^{(0)} \longrightarrow X_\infty^{(0)}/(\gamma_0 - 1)X_\infty^{(0)} \xrightarrow{f} \mathbb{Z}_p \longrightarrow 1 \quad (9)$$

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

$$1 \longrightarrow U_0' \longrightarrow \mathrm{Gal}\big(M_0/\Phi_\infty\big) \longrightarrow \mathbb{Z}_p \longrightarrow 1$$

and by (6),

$$1 \longrightarrow U_0'^{(0)} \longrightarrow X_\infty^{(0)}/(\gamma_0 - 1)X_\infty^{(0)} \xrightarrow{f} \mathbb{Z}_p \longrightarrow 1.$$

But f is an isomorphism as $U_0'^{(0)} = 1$. Then (9) tells us that

$$\mathbb{Z}_p \simeq U_\infty^{(0)}/(\gamma_0 - 1)U_\infty^{(0)}.$$

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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_n & \longrightarrow & \hat{\Phi}_n^\times & \xrightarrow{valuation} & \mathbb{Z}_p & \longrightarrow & 1 \\ & & {\scriptstyle \gamma_0-1}\downarrow & & {\scriptstyle \gamma_0-1}\downarrow & & {\scriptstyle \gamma_0-1}\downarrow & & \\ 1 & \longrightarrow & U_n & \longrightarrow & \hat{\Phi}_n^\times & \xrightarrow{valuation} & \mathbb{Z}_p & \longrightarrow & 1 \end{array}$$

By the snake lemma, the image of $1_{\mathbb{Z}_p}$ in $U_n/(\gamma_0-1)U_n$ is $\frac{\zeta_n^{\gamma_0}-1}{\zeta_n-1}$. Hence the image of $1_{\mathbb{Z}_p}$ in $U_\infty^{(0)}/(\gamma_0-1)U_\infty^{(0)}$ is $\left(\left(\frac{\zeta_n^{\gamma_0}-1}{\zeta_n-1}\right)^{e_0}\right)$. By Nakayama's lemma, $\left(\left(\frac{\zeta_n^{\gamma_0}-1}{\zeta_n-1}\right)^{e_0}\right)$ generates $U_\infty^{(0)}$ 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_∞ is generated over R by $\alpha = \Big((\beta - v_n)\Big)$, $x_1 = \left(\frac{\zeta_n^{\gamma_0}-1}{\zeta_n-1}\right)$, $x_2 = (\zeta_n)$. But α, 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

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

$$f_{u^\sigma}(T) = f_u\big((1+T)^{\psi(\sigma)} - 1\big) \qquad \forall \sigma \in \mathcal{G}_\infty.$$

Thus all the units in U_∞ have a Coleman power series.

It is useful to note that

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

and so the Weierstrass Preparation Theorem implies that

$$f_u\big((1+T)^p - 1\big) = \prod_{\eta \in \mu_p} f_u\big(\eta(1+T) - 1\big). \qquad (10)$$

3. *Coleman's Lemma*

Measures and Power Series

It is well known and almost obvious that the elements of $\Lambda(\mathcal{G}_\infty)$ are just the $\mathbb{Z}_p$-valued measures on $\mathcal{G}_\infty \simeq \mathbb{Z}_p^\times$ (see [11], [12]). On the other hand, we can identify the $\mathbb{Z}_p$-values measures on $\mathbb{Z}_p^\times$ i.e. $\Lambda\big(\mathbb{Z}_p^\times\big)$ 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 μ is a $\mathbb{Z}_p$-valued measures on $\mathbb{Z}_p$, the corresponding power series in R is given by

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

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

$$\tilde{\phi} : \Lambda\big(\mathbb{Z}_p\big) = \varprojlim \mathbb{Z}_p\big[\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p\big] \longrightarrow R$$

$$\tilde{\phi}(1_{\mathbb{Z}_p}) \longmapsto 1+T.$$

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

Proposition 3.1.

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

where

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

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

$$\int_{\mathbb{Z}_p} f d\tilde{\mu} = \int_{\mathbb{Z}_p^\times} f \mid_{\mathbb{Z}_p^\times} d\mu \ .$$

Conversely, if we have a measure μ on $\mathbb{Z}_p$ we get a measure μ^* on $\mathbb{Z}_p^\times$.
If $g : \mathbb{Z}_p^\times \longrightarrow C_p$ is a continuous function and $\epsilon_{\mathbb{Z}_p^\times}$ is the characteristic function of $\mathbb{Z}_p^\times$ then

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

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

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

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

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

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

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

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

LEMMA 3.2. $\mathrm{Ker}(l_\infty) = T_p(\mu)$.

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, $T_p(\mu) \subset \mathrm{Ker}\ l_\infty$.

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

$$f_u(0)^p = f_u(0) \equiv \ \mathrm{mod}\ p \Rightarrow u_0^p = f_u(0) = 1.$$

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

We can define a map

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

by the formula

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

We now proceed to show that $\mathrm{Im}(l_\infty) = \mathrm{Ker}(r_\infty)$ 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

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

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

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

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

It is obvious that $\delta_k : U_\infty \longrightarrow \mathbb{Z}_p$ 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)

$$\int_{\mathcal{G}_\infty} \psi^k(\sigma) dl_\infty(u) = D^k L(u)(T) \mid_{(T=0)} = (1 - p^{k-1})\delta_k(u). \quad (13)$$

By (13), we have

$$\int_{\mathcal{G}_\infty} \psi(\sigma) dl_\infty(u_\infty) = (1 - p^{1-1})\delta_1(u_\infty) = 0.$$

and hence Im $(l_\infty) \subset$ Ker (r_∞). The difficult part of the proof of the Theorem 2 is to show that Im $(l_\infty) =$ Ker (r_∞). 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 $k = 1, 2, \dots p-1$, and $\delta_p(\alpha) = p \times$* 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 α 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]) $Z = \lambda(X) = X + b_p X^p + \dots$ and $X = \phi(Z) = Z + a_p Z^p + \dots$. 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,* $pb_p \equiv 1 \bmod p^2$.

Proof. We know (see [13]) that

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

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

$$\begin{aligned}
\frac{1}{p}\big[p\big](X) &= X + \frac{1}{p}X^p. \\
\frac{1}{p^2}\big[p^2\big](X) &= X + \frac{1}{p}(1+p^{p-1})X^p + \ \dots \\
\frac{1}{p^3}\big[p^3\big](X) &= X + \frac{1}{p}(1+p^{p-1}+p^{2p-2})X^p + \ \dots \\
\frac{1}{p^4}\big[p^4\big](X) &= X + \frac{1}{p}\big(1+p^{p-1}+p^{2p-2}+p^{3p-3}\big)X^p + \ \dots
\end{aligned}$$

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

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

$$\begin{aligned}
\frac{d}{dZ}\log f_\alpha(X) &= \frac{1}{\lambda'(X)}\frac{-1}{\beta - X} \\
&= -\frac{1}{\beta}\phi'(Z)\big[1 + \frac{\phi(Z)}{\beta} + \frac{\phi(Z)^2}{\beta^2} + \dots\big] \\
&= h_\alpha(Z) \text{ (say).}
\end{aligned}$$

Since $\phi(Z) = Z + a_pZ^p + \dots$, we have $h_\alpha(Z) = -\frac{1}{\beta}[1 + pa_pZ^{p-1} + \dots]\times$ $[1 + \frac{(Z+a_pZ^p+\dots)}{\beta} + \frac{(Z+a_pZ^p+\dots)^2}{\beta^2} + \dots]$. It follows that

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

On the other hand,

$$\begin{aligned}
\delta_p(\alpha) &= \text{The coefficient of } Z^{p-1} \text{ in } h_\alpha(Z) \times\ (p-1)! \\
&= -\frac{(p-1)!}{\beta}\ \big[\ pa_p + \frac{1}{\beta^{p-1}}\ \big].
\end{aligned}$$

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

$$\begin{aligned}
\delta_p(\alpha) &= -\frac{(p-1)!}{\beta}\big[\ -pb_p + \frac{1}{1-p}\big] \\
&= \text{unit} \times \big[(-1 + \text{multiple of } \ p^{p-1}) + 1 + p + p^2 + \dots\big] \\
&\equiv p \times \text{unit} \mod (p^2).
\end{aligned}$$

This proves the proposition (3.3).

As

$$\mathbb{Z}_p[\Delta] = \bigoplus_{i=0}^{p-2} \mathbb{Z}_p[\Delta]e_i \simeq \bigoplus_{i=0}^{p-2} \mathbb{Z}_p.$$

where the map from $\mathbb{Z}_p[\Delta]e_i$ to $\mathbb{Z}_p$ is given by evaluation at χ^i, we obtain

$$\Lambda\big(\mathcal{G}_\infty\big) \simeq \mathbb{Z}_p[\Delta][[T]] \simeq \bigoplus_{i=0}^{p-2} \mathbb{Z}_p[[T]], \text{ with } \gamma_0 \mapsto 1 + T. \qquad (14)$$

Explicitly, the last isomorphism is given as follows :
Let $\mu \in \Lambda\big(\mathcal{G}_\infty\big)$ correspond to $h_\mu(T) = \sum_{n=0}^{\infty} c_nT^n$ in $\mathbb{Z}_p[\Delta][[T]]$, 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 α is the special element of U_∞ defined by (3). Let $l_\infty(\alpha)$ in $\Lambda(\mathcal{G}_\infty)$ correspond to $g(T) = \sum_{n=0}^{\infty} c_nT^n$ in $\mathbb{Z}_p[\Delta][[T]]$. Under the isomorphisms in (14),

$$l_\infty(\alpha) \longmapsto g(T) \longmapsto (\dots, g_i(T), \dots)$$

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

LEMMA 3.5. *For $i = 0, 2, 3, \dots p-2$, $g_i(T)$ is a unit in R and $g_1(T)$ can be written as $(1 + T - \psi(\gamma_0))h_1(T)$, where $h_1(T)$ is a unit.*

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

$$\begin{aligned}
g_i\big(\psi^k(\gamma_0) - 1\big) &= \sum_{n=0}^{\infty} \chi^k(c_n)\big(\psi^k(\gamma_0) - 1\big)^n \\
&= \int_{\mathcal{G}_\infty} \psi^k dl_\infty(\alpha) \\
&= (1 - p^{k-1})\delta_k(\alpha) \quad \text{by (13)}
\end{aligned}$$

Then it follows from proposition (3.3) that for $i = 2, 3, \ldots p-2$, $g_i\big(\psi^i(\gamma_0) - 1\big)$ is a unit. Hence $g_i(T)$ is a unit. With $i = p-1$, we have

$$g_0\big(\psi^{p-1}(\gamma_0) - 1\big) = (1 - p^{p-2})\ \delta_{p-1}(\alpha) = \text{a unit.}$$

This implies that $g_0(T)$ is also a unit. We have

$$g_1\big(\psi(\gamma_0) - 1\big) = (1 - p^0)\delta_1(\alpha) = 0.$$

So $g_1(T)$ can be written as $(1 + T - \psi(\gamma_0))h_1(T)$. But $g_1\big(\psi^p(\gamma_0) - 1\big)$ is $p \times$ unit by proposition (3.3). It is clear that $\psi^p(\gamma_0) - \psi(\gamma_0) = p \times$ a unit . But

$$h_1\big(\psi^p(\gamma_0) - 1\big)\big(\psi^p(\gamma_0) - \psi(\gamma_0)\big) = p \times \text{ a unit.}$$

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 $r_\infty \subset$ Im l_∞.

Proof: Consider $r_\infty(\mu) = 0$. By definition, $\int_{\mathcal{G}_\infty} \psi d\mu = 0$. Let $\mu \in \Lambda(\mathcal{G}_\infty)$ correspond to $(f_0, f_1, \ldots, f_{p-2})$ in $\bigoplus_{i=0}^{p-2} \mathbb{Z}_p[[T]]$ under (14). Then

$$\int_{\mathcal{G}_\infty} \psi d\mu = f_1\big(\psi(\gamma_0) - 1\big) = 0.$$

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,

$$\begin{aligned} f(T) &= \sum_{i=0}^{p-2} \lambda_i(T)g_i(T)e_i \\ &= \Big(\sum_{i=0}^{p-2} \lambda_i(T)e_i\Big)\Big(\sum_{j=0}^{p-2} g_j(T)e_j\Big). \end{aligned}$$

But $\Lambda(\mathcal{G}_\infty) \xrightarrow{\sim} \bigoplus_{i=0}^{p-2} \mathbb{Z}_p[[T]]$ is a $\mathbb{Z}_p$-algebra isomorphism. Hence

$$\mu_f = x\ .l_\infty(\alpha)$$

where x is some element of $\Lambda(\mathcal{G}_\infty)$. But U_∞ is a $\Lambda(\mathcal{G}_\infty)$ module and l_∞ is a $\Lambda(\mathcal{G}_\infty)$-homomorphism from U_∞ 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 Im $l_\infty \subset$ Ker r_∞. 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

[**1**] J. W. S. Cassels and A. Frohlich. *Algebraic Number Theory* (Academic Press) 1967.

[**2**] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39** (1977), 223–251.

[**3**] J. Coates and A. Wiles. On p-adic L-functions and Elliptic Units. *J. Austral. Math. Soc.* (Series A) **26** (1978), 1–25.

[**4**] R. Coleman. Division Values in Local Fields. *Invent. Math.* **53** (1979) 91–116.

[**5**] R. Coleman. The Arithmetic of Lubin-Tate Division Towers. *Duke. Math. Journal* **48** (1981), 449–466.

[**6**] K. Iwasawa. On $\mathbb{Z}_l$-extensions of Algebraic Number Fields. *Ann. of Math.* 2 **(98)** (1973), 246–326.

[**7**] K. Iwasawa. On p-adic L-functions *Ann. of Math.* (2) **99** (1969), 198–205.

[**8**] K. Iwasawa. On Some Modules in the Theory of Cyclotomic Fields *J. Math. Soc. Japan* Vol. 16
(1964), 42–82.

[**9**] S. Lang. *Cyclotomic Fields* (Springer-Verlag, 1978).

[**10**] J. Lubin and J. Tate. Formal Complex Multiplication in Local Fields *Ann. of Math.* **8** (1965), 380–387.

[**11**] K. J. P. Serre. Sur le residu de la fonction zêta p-adique d'un corps de nombres *C. R. Acad. Sci. Paris*, **287** (1978), 183–188.

[**12**] L. Washington. *Introduction to Cyclotomic Fields* (Springer Verlag, 1997).

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