RIMS Kôkyûroku Bessatsu
B12 (2009), 183–191

Local units are generated by certain cyclotomic units

By

Masanori Asakura*

§ 1. Introduction

Let H be a finite unramified extension of $\mathbb{Q}_p$ and O_H the ring of integers. Put $G_n := \mathrm{Gal}(H(\zeta_{p^n})/H)$ and $G := \varprojlim_n G_n$. Let

$$\mathbb{Z}_p[[G]] := \varprojlim_n \mathbb{Z}_p[G_n]$$

be the *Iwasawa algebra*. Letting q_H be the order of the residue field of H, we denote the group of $(q_H - 1)$-th roots of unity in H by μ_H. Note that μ_H is equal to the group of all roots of unity in H if $p \geq 3$, but not equal if $p = 2$. In what follows we fix a generator $(\zeta_{p^n})_n \in \mathbb{Z}_p(1)$. Let

$$U'_H := \varprojlim_n O_H[\zeta_{p^n}]^\times, \quad U_H := \varprojlim_n U'_H/p^n$$

where the limit in the former is taken with respect to the norm maps. We call U_H the group of *local units*. There is a natural inclusion $\mathbb{Z}_p(1) \to U_H$.

For $\eta \in \mu_H - \{1\}$ we put

$$C(\eta) := (1 - \eta^{1/p^n}\zeta_{p^n})_{n\geq 1} \in U_H \tag{1.1}$$

and call it the *cyclotomic unit*. Let H'/H be a finite unramified extension. The norm map for H'/H induces a map $N_{H'/H} : U_{H'} \to U_H$. For $\eta' \in \mu_{H'}$, we have $C(\eta') \in U_{H'}$ and hence the cyclotomic unit $N_{H'/H}C(\eta') \in U_H(r-1)$.

Recently I proved the following result to fix a mistake in my paper [1].

Theorem 1.1 ([2] Theorem 2.2). *Suppose $p \geq 2$. Then we have*

$$U_H = \mathbb{Z}_p(1) + \sum_{H', \eta' \in \mu_{H'} - \{1\}} \mathbb{Z}_p[[G]] N_{H'/H}(C(\eta')) \tag{1.2}$$

where H' runs over all finite unramified extensions of H.

Received April 23, 2008. Revised September 25, 2008.
2000 Mathematics Subject Classification(s): 11R23, 11S05
*Hokkaido University, Sapporo 060-0810, Japan.
e-mail: asakura@math.sci.hokudai.ac.jp

After I talked at the RIMS symposium "Algebraic Number Theory and related Topics", people asked me whether one really needs $H' \supsetneq H$ in the summation. The answer is "Yes" for example when $p = 3$ and $H = \mathbb{Q}_p$. However when $p \geq 5$ the answer is "No" :

Theorem 1.1 bis. *Suppose $p \geq 5$. Then we have*

$$U_H = \mathbb{Z}_p(1) + \sum_{\eta \in \mu_H - \{1\}} \mathbb{Z}_p[[G]]C(\eta). \tag{1.3}$$

In this article we give a proof of Theorem 1.1 bis together with a survey of the proof of Theorem 1.1. We will give an application of Theorem 1.1 bis to p-adic L-functions in §4.

Iwasawa's theorem asserts that the cyclotomic units are related to the p-adic L-functions. More precisely the characteristic ideal of the group of local units modulo "cyclotomic units" is generated by p-adic L-function (cf. [3] 4.4.1). In our discussion we take into account $C(\zeta_{p-1})$ etc. as cyclotomic units even when $H = \mathbb{Q}_p$, though they do not appear in the above sense. That is why I put "certain" in the title.

§ 2. Survey of Proof of Theorem 1.1

We recall the proof of Theorem 1.1 in case $p > 2$ from [2] (we omit the case $p = 2$ since the argument is slightly different).

Let $\chi : G \to \mathbb{Z}_p^\times$ be the cyclotomic character defined by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi(\sigma)}$. We write $\sigma_a := \chi^{-1}(a)$. We choose an isomorphism of topological O_H-algebra

$$\Phi : O_H[[G]] \xrightarrow{\cong} \overbrace{O_H[[T]] \times \cdots \times O_H[[T]]}^{p-1 \text{ times}} \tag{2.1}$$

which is uniquely determined by

$$\Phi(\sigma_{1+p}) = (T + 1 + p, \cdots, T + 1 + p), \tag{2.2}$$

$$\Phi(\sigma_\eta) = (\eta, \eta^2, \cdots, \eta^{p-1}) \quad \text{for } \eta^{p-1} = 1. \tag{2.3}$$

We denote by $k_H := O_H/pO_H$ the residue field and put $k_H^0 := \ker(\mathrm{Tr} : k_H \to \mathbb{F}_p)$ the kernel of the trace map.

§ 2.1. Step 1 : Coleman's exact sequence and Nakayama's lemma

Put by U_{cycl} the right hand side of (1.2). We want to show $U_H = U_{\mathrm{cycl}}$. A key tool in the proof is Coleman's exact sequence

$$0 \longrightarrow \mathbb{Z}_p(1) \xrightarrow{i_1} U_H \xrightarrow{l_\infty} O_H[[G]] \xrightarrow{i_2} \mathbb{Z}_p(1) \longrightarrow 0 \tag{2.4}$$

of $\mathbb{Z}_p[[G]]$-modules ([4], see also [3]). Here the map i_1 is a natural inclusion. The map i_2 is the composition of the trace map $\mathrm{Tr}_{H/\mathbb{Q}_p} : O_H[[G]] \to \mathbb{Z}_p[[G]]$ with the $\mathbb{Z}_p$-linear map $\mathbb{Z}_p[[G]] \to \mathbb{Z}_p(1)$ such that $\sigma_\alpha \mapsto (\zeta_{p^n}^\alpha)_{n\geq 1}$. The map l_∞ will play an important role below (see [2] §2.1 for the definition).

Thus it is enough to show $\Phi l_\infty(U_H) = \Phi l_\infty(U_{\mathrm{cycl}})$. Since the both sides are $\mathbb{Z}_p[[T]] \times \cdots \times \mathbb{Z}_p[[T]]$-modules, it is enough to check it on each component

$$p_i \Phi l_\infty(U_{\mathrm{cycl}}) = p_i \Phi l_\infty(U_H) \quad 1 \leq \forall i \leq p-1 \tag{2.5}$$

where $p_i : O_H[[T]] \times \cdots \times O_H[[T]] \to O_H[[T]]$ is the i-th projection.

Since U_H is a finitely generated $\mathbb{Z}_p[[G]]$-module (which follows from (2.4)), $p_i\Phi l_\infty(U_H)$ and hence $p_i\Phi l_\infty(U_{\mathrm{cycl}})$ are finitely generated $\mathbb{Z}_p[[T]]$-modules. One can apply Nakayama's lemma to (2.5), and thus the assertion is reduced to show the following.

Claim 2.1. $p_i\Phi l_\infty(U_{\mathrm{cycl}}) \otimes_{\mathbb{Z}_p[[T]]} \mathbb{F}_p = p_i\Phi l_\infty(U_H) \otimes_{\mathbb{Z}_p[[T]]} \mathbb{F}_p$ *for* $1 \leq \forall i \leq p-1$.

We note that there is an isomorphism

$$p_i\Phi l_\infty(U_H) \otimes_{\mathbb{Z}_p[[T]]} \mathbb{F}_p \cong \begin{cases} k_H^0 \oplus k_H/k_H^0 T & i = 1 \\ k_H & 2 \leq i \leq p-1 \end{cases} \tag{2.6}$$

by (2.4) (the choice (2.2) is crucial in the above description).

§ 2.2. Step 2 : p-adic polylogarithm

We want to show Claim 2.1. The following is a key formula (see [2] (2.20)):

$$p_i\Phi l_\infty(N_{H'/H}C(\eta'))|_{T=(1+p)^j-(1+p)} = -\mathrm{Tr}_{H'/H}\ l_{1-j}^{(p)}(\eta') \quad \text{for } j \equiv i \bmod p-1. \tag{2.7}$$

Here $l^{(p)}(z)$ is the p-adic polylog. The congruence relation

$$l_i^{(p)}(\eta) \equiv \frac{1}{1-\eta^{p^m}} \sum_{\substack{1\leq n\leq p^m-1 \\ (n,p)=1}} \frac{\eta^n}{n^i} \mod p^m O_H, \quad m \geq 1 \tag{2.8}$$

is well-known (cf. loc.cit. (2.17)). Let us rewrite Claim 2.1 more explicitly. If $2 \leq i \leq p-1$, it follows from (2.7) and (2.8) that one can rewrite Claim 2.1 in the following way:

Claim (A) *Suppose* $2 \leq i \leq p-1$. *Then the following elements*

$$\mathrm{Tr}_{H'/H} \frac{1}{1-(\eta')^p} \sum_{n=1}^{p-1} \frac{(\eta')^n}{n^{1-i}} \mod pO_H$$

generate k_H *as* $\mathbb{F}_p$*-module.*

The case $i = 1$ is more delicate. Let us write

$$p_1 \Phi l_\infty(C(\eta')) = q_0(\eta') + q_1(\eta')T + \cdots \ \text{in } O_{H'}[[T]],$$

$$p_1 \Phi l_\infty(N_{H'/H} C(\eta')) = \mathrm{Tr}_{H'/H} q_0(\eta') + \mathrm{Tr}_{H'/H} q_1(\eta')T + \cdots \ \text{in } O_H[[T]].$$

Again by (2.7), one can show the following ([2] Lem. 2.7):

$$q_0(\eta') = \frac{-\eta'}{1-\eta'} - \frac{-(\eta')^p}{1-(\eta')^p} \in O_{H'}, \tag{2.9}$$

$$q_0(\eta') - p q_1(\eta') \equiv -l^{(p)}_{1-p}(\eta') \mod p^2 O_{H'}, \tag{2.10}$$

$$p \mathrm{Tr}_{H'/\mathbb{Q}_p} q_1(\eta') \equiv \mathrm{Tr}_{H'/\mathbb{Q}_p} l^{(p)}_{1-p}(\eta') \mod p^2 \mathbb{Z}_p \tag{2.11}$$

((2.11) follows from (2.9) and (2.10) together with the fact $\mathrm{Tr}_{H'/\mathbb{Q}_p} q_0(\eta') = 0$). Claim 2.1 in case $i = 1$ is equivalent to say that $p_1 \Phi l_\infty(U_{\mathrm{cycl}}) \to k_H^0 \oplus k_H/k_H^0 T \cong k_H^0 \oplus \mathbb{F}_p$ is surjective, and it is explicitly written in the following way:

Claim (B) *The following elements*

$$\mathrm{Tr}_{H'/H}\left(\frac{-\eta'}{1-\eta'} - \frac{-(\eta')^p}{1-(\eta')^p}\right) \mod pO_H$$

generate k_H^0 as $\mathbb{F}_p$-module. Moreover there are some $\eta'_i \in \mu_{H'} - \{1\}$ and $a_i \in \mathbb{Z}_p$ such that

$$\sum_i a_i \mathrm{Tr}_{H'/H}\left(\frac{-\eta'_i}{1-\eta'_i} - \frac{-(\eta'_i)^p}{1-(\eta'_i)^p}\right) \equiv 0 \mod pO_H$$

and

$$\sum_i a_i \left(\frac{1}{p} \mathrm{Tr}_{H'/\mathbb{Q}_p}(l^{(p)}_{1-p}(\eta'_i))\right) \not\equiv 0 \mod p\mathbb{Z}_p \quad \text{(cf. (2.8))}.$$

§ 2.3. Step 3 : Claims (A) and (B)

The proof of Theorem 1.1 is reduced to show Claim (A) and Claim (B) in the previous section. The proof of Claim (A) is easy and we use only the set $\mu_H - \{1\}$ to supply generators of k_H ([2] Prop.2.6).

The former part of Claim (B) is trivial and we do not need H' either. The latter part of Claim (B) is the technical heart. The proof can be seen in [2] Prop.2.8 which is about 3 pages long of quite elementary calculations. There we need to assume $[H' : \mathbb{Q}_p] \geq 2$ to find η'_i. If $H \neq \mathbb{Q}_p$ then one can take $H' = H$ so that we do not need H' in the summation in (1.2). However if $p = 3$ and $H = \mathbb{Q}_p$, then we do need H' to show Claim (B) (see Remark after Claim (C) below).

§ 3. Proof of Theorem 1.1 bis

As we have seen in the previous section, we may assume $H = \mathbb{Q}_p$. Then all we have to do is to show the latter statement of Claim (B) without H', namely

Claim (C) *Suppose $p \geq 5$ and $H = \mathbb{Q}_p$. Then there is some $\eta \in \mu_{\mathbb{Q}_p} - \{1\}$ such that*

$$\frac{1}{p}\, l_{1-p}^{(p)}(\eta) \not\equiv 0 \mod p\mathbb{Z}_p.$$

Remark. The above is no longer true if $p = 3$. In fact, one has

$$\frac{1}{3}\, l_{-2}^{(3)}(\eta) \equiv \frac{\eta + 2^2\eta^2 + 4^2\eta^4 + 5^2\eta^5 + 7^2\eta^7 + 8^2\eta^8}{3(1-\eta^9)} \mod 3$$

by the congruence relation (2.8). Since $p = 3$, η must be -1 and then the right hand side vanishes.

Proof of Claim (C). Recall from (2.8) the congruence relation

$$l_r^{(p)}(\eta) \equiv \frac{1}{1-\eta^{p^2}} \sum_k \frac{\eta^k}{k^r} \mod p^2\mathbb{Z}_p.$$

where k runs over the integers such that $1 \leq k \leq p^2 - 1$ and $(p, k) = 1$. Put

$$l_r^*(x) := \sum_k \frac{x^k}{k^r} \in \mathbb{Z}_p[x].$$

Then $l_r^*(\eta) = (1 - \eta^{p^2}) l_r^{(p)}(\eta) \bmod p^2$. We want to show $l_{1-p}^*(\eta) \not\equiv 0 \bmod p^2$ for some $\eta \neq 1$. Since $l_0^*(\eta) = \sum_{i=0}^{p-1}\sum_{j=1}^{p-1} \eta^{j+ip} = (\sum_{i=0}^{p-1} \eta^{ip})(\sum_{j=1}^{p-1} \eta^j) = 0$, we may switch $l_{1-p}^*(x)$ with $l_{1-p}^*(x) - l_0^*(x)$. Let

$$l(x) := \sum_k \frac{k^{p-1} - 1}{p} x^k \in \mathbb{Z}[x].$$

Then $l_{1-p}^*(x) - l_0^*(x) = pl(x)$. Thus it suffices to show

$$l(\eta) \not\equiv 0 \mod p \quad \text{for some } \eta \neq 1, \tag{3.1}$$

equivalently

$$l(m) \not\equiv 0 \mod p \quad \text{for some } 2 \leq m \leq p-1. \tag{3.2}$$

Let $\bar{l}(x)$ be the image of $l(x)$ via the natural map $\mathbb{Z}[x] \to \mathbb{F}_p[x]/(x^{p-1} - 1)$. Write

$$\bar{l}(x) = c_0 + c_1 x + \cdots + c_{p-2} x^{p-2} \quad (c_i \in \mathbb{F}_p).$$

Then

$$l(m) \equiv 0 \bmod p \quad \text{for } 2 \leq \forall m \leq p-1 \Leftrightarrow \bar{l}(m) = 0 \quad \text{for } 2 \leq \forall m \leq p-1$$
$$\Leftrightarrow c_0 = c_1 = \cdots = c_{p-2}.$$

We will show that this is impossible.

Lemma 3.1.

$$c_0 = \left(\sum_{i=1}^{p-1} \frac{i^{p-1}-1}{p} \right) - 1, \tag{3.3}$$

$$c_k = c_0 + \frac{k^{p-1}-1}{p} - \sum_{i=1}^{k-1} i^{p-2}, \quad 1 \leq k \leq p-2 \tag{3.4}$$

where the sum "$\sum_{i=1}^{k-1}$" is zero if $k = 1$ by convention.

Proof.

$$\begin{aligned} \bar{l}(x) &= \sum_{i=1}^{p-1} \sum_{j=0}^{p-1} \frac{(i+jp)^{p-1}-1}{p} x^{i+jp} \\ &= \sum_{i=1}^{p-1} \sum_{j=0}^{p-1} \frac{(i+jp)^{p-1}-1}{p} x^{i+j} \\ &= \sum_{i=1}^{p-1} \sum_{j=0}^{p-1} \left(\frac{i^{p-1}-1}{p} - i^{p-2} j \right) x^{i+j} \end{aligned}$$

where the last equality follows from $(i+jp)^{p-1} \equiv i^{p-1} - pi^{p-2}j \bmod p^2$.

$$\begin{aligned} c_0 &= \sum_{i+j=p-1,\ 2(p-1)} \left(\frac{i^{p-1}-1}{p} - i^{p-2} j \right) \\ &= \sum_{i=1}^{p-1} \left(\frac{i^{p-1}-1}{p} - i^{p-2}(p-1-i) \right) + \left(\frac{(p-1)^{p-1}-1}{p} - (p-1)^{p-2}(p-1) \right). \end{aligned}$$

The second term is zero (modulo p). Noting $\sum_{i=1}^{p-1} i^{p-2} = 0$, one has

$$c_0 = \sum_{i=1}^{p-1} \left(\frac{i^{p-1}-1}{p} + i^{p-1} \right) = \sum_{i=1}^{p-1} \left(\frac{i^{p-1}-1}{p} \right) - 1.$$

Let $1 \le k \le p-2$. Then

$$\begin{aligned} c_0 &= \sum_{i+j=k,\ p-1+k} \left(\frac{i^{p-1}-1}{p} - i^{p-2}j \right) \\ &= \sum_{i=1}^{k} \left(\frac{i^{p-1}-1}{p} - i^{p-2}(k-i) \right) + \sum_{i=k}^{p-1} \left(\frac{i^{p-1}-1}{p} - i^{p-2}(p-1+k-i) \right) \\ &= \sum_{i=1}^{p-1} \left(\frac{i^{p-1}-1}{p} - i^{p-2}(k-i) \right) + \frac{k^{p-1}-1}{p} + \sum_{i=k}^{p-1}(-i^{p-2}(p-1)). \end{aligned}$$

Noting $\sum_{i=1}^{p-1} i^{p-2} = 0$, the first term is equal to c_0 and the third term is equal to $-\sum_{i=1}^{k-1} i^{p-2}$. Thus one has (3.4). □

Lemma 3.2. *There is some $1 \le k \le p-2$ such that*

$$c_k - c_0 = \frac{k^{p-1}-1}{p} - \sum_{i=1}^{k-1} i^{p-2} \not\equiv 0 \mod p.$$

Proof. Let $B_i(x)$ be the Bernoulli polynomial

$$B_m(x) := \sum_{i=0}^{m} \binom{m}{i} B_i x^{m-i}, \qquad \frac{x}{e^x-1} = \sum_{i=0}^{\infty} B_i \frac{x^i}{i!}.$$

As is well-known, $(B_m(k) - B_m)/m = 1 + 2^{m-1} + \cdots + (k-1)^{m-1}$ for an integer $k \ge 1$. Put

$$a(x) := \frac{1}{p}\left(x^{p-1} - 1 - \prod_{i=1}^{p-1}(x-i) \right) - \frac{B_{p-1}(x) - B_{p-1}}{p-1} \in \mathbb{Z}[\frac{1}{(p-1)!}][x].$$

The degree of $a(x)$ is $p-1$ and the leading coefficient is $1/(1-p)$. We have

$$a(k) = \frac{k^{p-1}-1}{p} - \sum_{i=1}^{k-1} i^{p-2}$$

for $1 \le k \le p-1$. Now suppose that $a(k) \equiv 0 \bmod p$ for all $1 \le k \le p-2$. Since $a(p-1) \equiv 0 \bmod p$, $a(x) \bmod p$ has roots $x = 1, 2, \cdots, (p-1)$, which means

$$a(x) \equiv x^{p-1} - 1 \mod p. \tag{3.5}$$

This is impossible. In fact a direct calculation shows

$$\prod_{i=1}^{p-1}(x-i) = x^{p-1} - \frac{1}{2}p(p-1)x^{p-2} + \left(\frac{1}{8}p^2(p-1)^2 - \frac{1}{12}p(p-1)(2p-1) \right) x^{p-3} + \cdots.$$

Therefore one has

$$a(x) \equiv \left(-\frac{1}{2}x^{p-2} + \frac{1}{12}x^{p-3} + \cdots\right) + \left(x^{p-1} + (p-1)B_1x^{p-2} + \binom{p-1}{2}B_2x^{p-3} + \cdots\right)$$
$$\equiv x^{p-1} + \frac{1}{4}x^{p-3} + \cdots \mod p$$

which contradicts (3.5). □

Lemmas 3.1 and 3.2 implies that there is some k such that $c_0 \not\equiv c_k \bmod p$ and it proves (3.2). This completes the proof of Claim (C) and hence Theorem 1.1 bis.

§ 4. Application to special values of p-adic L-functions

Let $L_p(s,\chi)$ denote the p-adic L-function which is characterized as a p-adic analytic function on $\mathbb{Z}_p$ such that

$$L_p(1-r,\chi\omega^r) = (1-\chi(p)p^{r-1})L(1-r,\chi), \quad r > 0 \tag{4.1}$$

where $L(s,\chi)$ is the Dirichlet L-function and $\omega : (\mathbb{Z}/p)^\times \to \mathbb{Z}_p^\times$ is the Teichmüller character. Due to Iwasawa's theorem, for each $1 \le i \le p-1$ there is a $G_{\chi\omega^i}(T) \in \mathrm{Frac}O_H[\mathrm{Image}\chi][[T]]$ such that

$$G_{\chi\omega^i}(1+p)^r - (1+p)) = -L_p(1-r,\chi\omega^i) \quad (r \in \mathbb{Z}_p). \tag{4.2}$$

(Note that if $\chi\omega^i$ is odd then $G_{\chi\omega^i} = 0$ as $L_p(s,\chi\omega^i) = 0$.) On the other hand let $F_\eta^{(i)}(T) = p_i\Phi l_\infty(C(\eta)) \in O_H[[T]]$ for $\eta \in \mu_H - \{1\}$. As we have seen in (2.7), we have

$$F_\eta^{(i)}((1+p)^j - (1+p)) = -l_{1-j}^{(p)}(\eta) \quad \text{for } j \equiv i \bmod p-1.$$

The p-adic polylogarithms are expressed as p-adic L-functions and vice versa. Therefore $F_\eta^{(i)}(T)$ are expressed as a linear combination of $G_{\chi\omega^i}(T)$ (see [2] (2.16) for details). Thus Theorem 1.1 bis implies the following (cf. loc.cit. Rem. 2.3).

Theorem 4.1. *Suppose $p \ge 5$. Then we have*

$$\sum_\chi \mathbb{Z}_p[\mathrm{Image}\chi][[T]]G_{\chi\omega^i}(T) \supset \begin{cases} O_H[[T]] & 2 \le i \le p-1 \\ O_H^0 + TO_H[[T]] & i = 1 \end{cases}$$

where χ runs over all Dirichlet characters whose conductors are divisors of $\sharp\mu_H = q_H - 1$.

As a simple consequence, one has the following: For each $2 \le i \le p-1$ there exists at least one Dirichlet character χ whose conductor is a divisor of $p-1$ such that $G_{\chi\omega^i}(T)$ is a unit in $\mathbb{Z}_p[[T]]$, in other words, $G_{\chi\omega^i}((1+p)^r - (1+p)) = -L_p(1-r,\chi\omega^i)$ is not divided by p for any $r \in \mathbb{Z}_p$.

References

[1] Asakura, M., Surjectivity of p-adic regulators on K_2 of Tate curves. *Invent. Math.* **165** (2006), 267–324.

[2] ———, Erratum "Surjectivity of p-adic regulators on K_2 of Tate curves". *Invent. Math.* **165** (2008), 213–229.

[3] Coates, J. and Sujatha, R., *Cyclotomic fields and zeta values.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[4] Coleman, R., Local units modulo circular units. *Proc. Amer. Math. Soc.* **89** (1983), no. 1, 1–7.