LOCAL UNITS MODULO CIRCULAR UNITS

R. COLEMAN

Abstract. In his paper, Some Modules in the Theory of Cyclotomic Fields [2],
Iwasawa obtained the remarkable theorem that the quotient of the $p$-adic cyclotomic
units by the completion of the circular units is isomorphic to the quotient of the
group ring by the Stickelberger ideal. He then used this to deduce some interesting
global results, the most striking of which is an explanation of the plus part of the
analytic class number formula under the assumption that the class group at the first
layer is cyclic, together with a regularity assumption.

In this note, we will show how with the results in our paper, Division Values in
Local Fields [1], it is now possible to give a substantially simpler proof of the above
theorem. We also describe, briefly, how one can obtain various global results of
Iwasawa from this Theorem, which are not included in either Lang’s [3], or

I. Notation. Let $\mathbb{Q}_p((T))$ denote the ring of Laurent series with finite poles over
$\mathbb{Q}_p$. Let $\mathbb{Q}_p((T))_1$ and $\mathbb{Q}_p[[T]]_1$ denote the subrings of $\mathbb{Q}_p((T))$ consisting of power
series which converge on the punctured open unit ball and on the open unit ball
respectively. Let $\mathbb{Z}_p((T))$ denote the subring of $\mathbb{Q}_p((T))$ with integer coefficients and
$\mathbb{Z}_p[[T]]$ the ring $\mathbb{Z}_p((T)) \cap \mathbb{Q}_p[[T]]_1$.

Let $S$ and $N$ denote the trace and norm operators defined in [1] on $\mathbb{Q}_p((T))_1$ and
$\mathbb{Z}_p((T))^\ast$ respectively. They are characterized by the formulas

\[
(1) \quad S(g)(1 - (1 - T)^p) = \sum_\zeta g(1 - \zeta(1 - T)),
\]

\[
(2) \quad N(f)(1 - (1 - T)^p) = \prod_\zeta f(1 - \zeta(1 - T)),
\]

where $\zeta$ runs over the $p$th roots of unity $\mu_p$. Let

\[
[a](T) = 1 - (1 - T)^a, \quad \varphi g = g \circ [p],
\]

\[
D = (1 - T) \frac{d}{dT}, \quad \delta f = \frac{Df}{f}, \quad \text{for } g \in \mathbb{Q}_p[[T]]_1 \text{ and } f \in \mathbb{Z}_p((T))^\ast.
\]

We then have the identities

\[
(3) \quad S \log(f) = \log(N(f)),
\]

\[
(4) \quad S Dg = p D S g,
\]

\[
(5) \quad S \delta(h) = p \delta N(h),
\]

\[
(6) \quad S \varphi(g) = pg,
\]

Received by the editors September 20, 1982 and, in revised form, December 20, 1982.
1980 Mathematics Subject Classification. Primary 12A35.
for \( f \in \mathbb{Z}_p[[T]]^0 = \{ f \in \mathbb{Z}_p[[T]] : f(0) = 1 \mod p \}, \ g \in \mathbb{Q}_p[[T]] \), \( h \in \mathbb{Z}_p((T))^* \).

Let \( \Phi_p = \mathbb{Q}_p(\mu_{p^{n+1}}), \Phi_\infty = \bigcup \Phi_n, \ G = \text{Gal}(\Phi_\infty/\mathbb{Q}_p) \). Let \( R = \mathbb{Z}_p[[G]] \) denote the completed group ring of \( G \) over \( \mathbb{Z}_p \). Let \( \chi : G \to \mathbb{Z}_p^* \) denote the canonical character of \( G \), giving its action on roots of unity of \( p \)-power order. Let \( \xi = (\xi_n) \) be a fixed generator of \( \mathbb{T}_p(G_m) \). If \( a \in \mathbb{Z}_p^* \) we set \( a(\xi) = (\xi_n^a) \).

As in [1] we may give the multiplicative group \( \mathbb{Z}_p[[T]]^0 \) and the additive group \( \mathbb{Q}_p((T))^1 \) continuous \( R \)-module structures such that in each case the effect of \( \sigma \in G \) on \( f \) is \( f \circ \chi(\sigma) \). If \( \omega \in R \) write \( f^\omega \) and \( \omega g \) for \( f \) as an element of \( \mathbb{Z}_p[[T]]^0 \) and \( g \) as an element of \( \mathbb{Q}_p((T))^1 \). These actions are consistent with evaluation at the points \( 1 - \xi_n \). Finally, if \( a \in \mathbb{Z}_p^* \) we let \( \sigma(a) \) denote the element \( G \) such that \( \chi(\sigma(a)) = a \).

II. The structure of the local units. The following result is not difficult and follows immediately from Theorem 2.2 of [1].

**Theorem 1.** There is an exact sequence (depending only on \( \xi \)) of \( R \)-modules

\[
0 \to \mathbb{T}_p(G_m) \to \mathbb{Z}_p[[T]]^0 \to \mathbb{Z}_p[[T]] \to \mathbb{T}_p(G_m) \to 0
\]

(when \( p \neq 2 \)) where the first map is given by \( a(\xi) \to (1 - T)^a \), the second by \( f \to (1 - \chi/p) \log f \) and the third by \( g \to Dg(0)(\xi) \). (When \( p = 2 \) there is a similar exact sequence with \( \mathbb{T}_p(G_m) \) replaced by \( \mu_2 \oplus T_2(G_m) \) in each case.)

**Lemma 2.** \( \mathbb{Z}_p[[T]] = \mathbb{R}(1 - T) + \varphi(\mathbb{Z}_p[[T]]) \).

**Proof.** If \( a \in \mathbb{Z}, a \geq 0, (a, p) = 1 \) then

\[
(T - 1)^a = (-1)^a \sigma(a)(1 - T) \in R(1 - T)
\]

and is monic of degree \( a \). If \( a \in \mathbb{Z}, a \geq 0 \) then

\[
(-1)^a[p]^a = \varphi((-1)^aT^a) \in \varphi\mathbb{Z}_p[[T]]
\]

and is monic of degree \( pa \). It follows that \( R(1 - T) + \varphi(\mathbb{Z}_p[[T]]) \) contains a monic polynomial of every nonnegative degree and hence is dense in \( \mathbb{Z}_p[[T]] \); since it is also closed the lemma follows.

Let \( \mathcal{V} = \{ g \in \mathbb{Z}_p[[T]] : \bar{S}(g) = 0 \} \). Clearly \( 1 - T \in \mathcal{V} \).

**Theorem 3.** \( \mathcal{V} \) is a principal \( R \)-module generated by \( 1 - T \).

**Proof.** By (6) we see immediately that

\[
\mathcal{V} \cap \varphi(\mathbb{Z}_p[[T]]) = 0.
\]

It follows from Lemma 2 that \( \mathcal{V} = R(1 - T) \). To be sure \( \mathcal{V} \) is not a torsion module, suppose \( \omega(1 - T) = 0 \). Evaluating we deduce \( \omega \xi_n = 0 \) for all \( n \geq 0 \), but this implies \( \omega \Phi_\infty = 0 \) which implies \( \omega = 0 \).

**Corollary.** \( D\mathcal{V} = \mathcal{V} \) and in fact the map \( f \mapsto Df \otimes \xi \) is an \( R \)-module isomorphism

\[
\mathcal{V} \sim \mathcal{V} \otimes T_p(G).
\]
Proof. The first assertion follows from the theorem, the fact that
\[ D(1 - T) = -(1 - T) \]
(7) and compactness. The second assertion follows from (7), compactness and the fact that \( Z_p \cap \mathbb{V} = \varnothing \).

Now let \( \mathcal{R} = \{ f \in Z_p((T))^*: \mathcal{R}(f) = f \} \). By Theorem 16 of [1], for each element \( \alpha = (\alpha_n) \in \lim \Phi_n^* \) there is a unique element \( f_\alpha \in \mathcal{R} \) such that
\[ f_\alpha(1 - \zeta_n) = \alpha_n, \]
and the map \( \alpha \mapsto f_\alpha \) is a Galois-isomorphism.

Let \( \mathcal{R}_0 = \mathcal{R} \cap Z_p[[T]]^0 \). Then \( \mathcal{R}_0 \simeq \lim U_n \) where \( U_n \) is the group of principal units in \( \Phi_n \).

**Theorem 4.** We have an exact sequence of \( R \)-modules.
\[ 0 \to T_p(G_m) \to \mathcal{R} \to \mathcal{V} \to T_p(G_m^0) \to 0 \]
where the maps are as in Theorem 1 (if \( p \neq 2 \)). (Again there is a similar statement when \( p = 2 \).)

**Proof.** As \( (1 - T) \in \mathcal{R}_0 \), we only need check that \( \mathcal{R}_0 \) is the inverse image of \( \mathcal{V} \) under the map \( f \mapsto (1 - \varphi/p)\log(f) \). However, using (3) and (6) we deduce
\[ \mathcal{S}(1 - \varphi/p)\log f = \log \mathcal{R}(f) - \log f = \log(\mathcal{R}(f)/f). \]
So \( f \) is in the inverse image of \( \mathcal{V} \) iff \( (\mathcal{R}(f)/f) \in \Ker(\log) = 1 \) (if \( p \neq 2 \)).

**III. The image of the circular units.** Let \( C_n \) denote the completion in \( \Phi_n^* \) of the group of circular units in \( Q(\mu_{p^n+1}) \). Thus \( C_n \) is generated topologically by the elements
\[ T^{1-\sigma(a)}|_{T=1-\zeta_n} = [a](T)|_{T=1-\zeta_n} = \frac{1 - \zeta_n}{1 - \zeta_n}, \]
with \( a \in Z_p^* \). Let \( C_n^0 = C_n \cap U_n \).

Let \( \mathcal{C} = \lim C_n \) considered as a subgroup of \( \mathcal{R} \) and \( \mathcal{C}_0 = \mathcal{C} \cap \mathcal{R}_0 \). It follows that \( \mathcal{C}_0 \simeq \lim C_n^0 \). Clearly \( \mathcal{C}_0 \) is an \( R \)-submodule of \( \mathcal{R}_0 \) generated over \( R \) by the elements
\[ \omega(a)T^{1-\sigma(a)} \quad (a \in Z_p^*) \]
where \( \omega: Z_p^* \to \mu_{p-1} \) is the Teichmüller character.

Let
\[ \theta_n = \sum_{a=1}^{p^{n+1}} B_1((a/p^{n+1}))\sigma_a \]
denote the \( n \)th Stickleber element, where \( B_1(x) = x - \frac{1}{2} \), the first Bernoulli polynomial. Let \( \theta = (\theta_n) \in Q_p[[G]] \supseteq R \). Then the Stickleberger ideal is \( \mathcal{S} = R\theta \cap R \). In fact, one knows \( \mathcal{S} \) is generated over \( R \) by the elements
\[ (1 - aa^{-1}(a))\theta, \quad a \in Z_p^*. \]
There is an involution $\omega \to \omega^*$ of the ring $\mathbb{Q}_p[[G]]$ induced by

$$\sigma \to \sigma^{-1}, \quad \sigma \in G.$$  

If $I$ is an $R$-submodule of $\mathbb{Q}_p[[G]]$ we set $I^* = \{\omega^*: \omega \in I\}; I^*$ is also an $R$-module.

**Proposition 5 (Kummer-Iwasawa).**

$$\frac{\xi_n}{\xi_n - 1} - \frac{\xi_{n-1}}{\xi_{n-1} - 1} = \theta^* \xi_n.$$

**Proof.** This follows immediately from the equation

$$p^{n+1} \xi_n = (\xi_n - 1) \left( \sum_{a=1}^{p^{n+1}} a^a \xi_n^a \right).$$

**Proposition 6.** $\mathbb{C}/((1 - \varphi)\mathbb{C}^0) \cong R/\mathbb{S}^*$ as $R$-modules.

**Proof.** $(1 - \varphi)\mathbb{C}^0$ is generated by the elements

$$(1 - \varphi)\delta(\omega(a)T^{1-\sigma(a)}) = (1 - \varphi)(1 - a\sigma(a))\delta(T) = (1 - a\sigma(a))(1 - \varphi)\delta(T).$$

By Proposition 5

$$(1 - a\sigma(a))(1 - \varphi)\delta(T)|_{1-\xi_n} = (1 - a\sigma(a))(\theta^* \xi_n)$$

$$= ((1 - a\sigma(a))\theta^*(1 - T))|_{1-\xi_n}$$

as $(1 - a\sigma(a))\theta^* = ((1 - a\sigma^{-1}(a))\theta)^* \in R$. It follows that

$$(1 - a\sigma(a))(1 - \varphi)\delta(T) = (1 - a\sigma(a))\theta^*(1 - T).$$

Thus $(1 - \varphi)\mathbb{C}^0$ is the span of $(1 - a\sigma(a))\theta^*\mathbb{C}$ which is $\mathbb{S}^*\mathbb{C}$. The proposition now follows immediately from Theorem 3.

Now for each integer $n$ there is an automorphism $\omega \to \omega(n)$ of $R$ characterized by

$$\sigma \to \chi(\sigma)^n \sigma, \quad \sigma \in G.$$  

It is not hard to see that

$$R/I \otimes T_p(G_\mathbb{m}) \cong R/I(-1).$$  

Hence we deduce from the above theorem and the corollary to Theorem 3.

**Corollary.**

$$\mathbb{C}/(1 - \varphi/p)\log(\mathbb{C}^0) \cong R/\mathbb{S}^*(-1).$$

Finally using this and Theorem 4 we deduce

**Theorem 7.** There is an exact sequence

$$0 \to \mathcal{M}/\mathbb{C}^0 \to R/\mathbb{S}^*(-1) \to T_p(G_\mathbb{m}) \to 0$$

of $R$-modules.

Taking $"+"$ parts we obtain

$$\mathcal{M}^+/\mathbb{C}^+ = R^+/((\mathbb{S}^*)^+(-1)) = R^+/((\mathbb{S}^-)^*(-1))$$

where $\mathcal{M}^+ = (\mathcal{M}^0)^+, \mathbb{C}^+ = (\mathbb{C}^0)^+.$
IV. Applications to global questions. Let
\[ K = \bigcup \mathbb{Q}(\mu_{p^n}). \]
\[ M = \text{the maximal pro-}p\text{ abelian unramified outside } p\text{ extension of } K. \]
\[ L = \text{the maximal unramified extension of } K \text{ contained in } L. \]
\[ A_n = p\text{-Sylow subgroup of the class group of } \mathbb{Q}_p(\mu_{p^n+1}). \]
\[ A_k = \operatorname{Lim}_{n\to\infty} A_n. \]
\[ E_n^0 = \text{the completion in } \Phi_n^* \text{ of the units in } \mathbb{Q}_p(\mu_{p^n+1}). \]
\[ E_n^+ = (E_n^0)^+, \text{ and} \]
\[ \mathfrak{g}_+^+ = \operatorname{Lim}_{n\to\infty} E_n^+ \subseteq \mathfrak{e}^0. \]

It is well known [4, Corollary 3.6], that
\[ \mathfrak{e}^+ / \mathfrak{g}_+^+ \cong \text{Gal}(M/L)^+. \]

Therefore we have the following exact sequence of \( R \)-modules.
\[ 0 \to \mathfrak{g}_+^+ / \mathfrak{e}_+^+ \to \mathfrak{e}^+ / \mathfrak{e}_+^+ \to \text{Gal}(M/K)^+ \to \text{Gal}(L/K)^+ \to 0. \]

If one supposes \( A_0 \) (= \( p \)-Hilbert class group) is a cyclic \( R \)-module then it is not hard to show using Stickleberger's Theorem, the analytic class number formula, and Iwasawa's index formula for the Stickleberger ideal that
\[ \text{Gal}(L/K)^- \cong R^- / \mathfrak{s}^-, \]
and in fact
\[ A_n^- \cong R_n^- / \mathfrak{s}_n^- . \]

From the perfect (Kummer) pairing
\[ \text{Gal}(M/K)^+ \times A_k \to \mu_{p^n}, \]
and the fact \( |A_n| < \infty \), it is not hard to show
\[ \text{Gal}(M/K)^+ \cong R^+ / (\mathfrak{s}^-)^*(-1). \]

**Theorem 8 (Iwasawa).** Assuming \( A_0 \) is a cyclic \( R \)-module and \( \text{Gal}(L/K) \) has no nontrivial finite \( R \)-submodules, we have
\[ E_n^0 / C_n^0 \cong A_n^+, \]
(noncanonically) which implies the plus part of the class number formula.

**Proof.** Since the two terms in the middle of \((*)\) are isomorphic cyclic \( R \)-modules if it is not hard to show
\[ \mathfrak{g}_+^+ / \mathfrak{e}_+^+ \cong \text{Gal}(L/K)^+. \]
The theorem follows by descending to finite layers, once one knows:

**Lemma.** If \( \text{Gal}(L/K) \) has no finite \( R \)-submodules, then \( N_{m,n} E_m = E_n \).

**Proof.** Analyzing the long exact sequences in group cohomology arising from the short exact sequences
\[ 0 \to E_m \to K_m \to P_m \to 0, \quad 0 \to P_m \to I_m \to H_m \to 0 \]
where $K_m = \mathbb{Q}(\mu_{p^{m-1}})$, $P_m = \text{principal ideals in } K_m$, $I_m = \text{ideals of } K_m$ and $H_m = \text{class group } K_m$, and using the facts that

$$H^1(G, K_m) = H^1(G, I_m) = \text{Image } (H^0(G, P_m) \to H^0(G, H_m)) = 0$$

where $G = \text{Gal}(K_m/K_n)$, one deduces

$$E_n/N_{m,n} E_m = H^2(G, E_m) \approx H^2(G, H_m) = H^2(G, A_m).$$

The last equality follows from the fact that $G$ is a $p$-group. Now

$$A_m = \text{Gal}(L'_m/K_m) \approx \text{Gal}(L_m/K) = X/(1 - \gamma_n)X$$

where $L'_m = p$-Hilbert class field of $K_m$, $L_m = KL'_m \subseteq L$, $X = \text{Gal}(L/K)$ and $\gamma_n = \gamma^{p^{m-1}}$, where $\gamma$ is a fixed generator of $\text{Gal}(K/\mathbb{Q}(\mu_p))$. The first isomorphism follows from class field theory, the second from the fact that $K/K_m$ is totally ramified at a prime above $p$ and the third from the fact that there is only one prime above $p$ in $K_m$. Thus $H^2(G, E_m) \approx H^2(G, X/(1 - \gamma_m)X)$ and

$$H^2(G, X/(1 - \gamma_m)X) = \left\{ \frac{x \in \mathbb{Z}}{(1 - \gamma_n)x \in (1 - \gamma_m)X} \right\},$$

where $\nu_{m,n} = (1 - \gamma_m)/(1 - \gamma_n) = 1 + \gamma_n + \cdots + \gamma_n^{p^{m-1}-1}$. However, if $x, x' \in X$ are such that $(1 - \gamma_n)x = (1 - \gamma_m)x'$, then

$$(1 - \gamma_n)y = 0$$

where $y = x - \nu_{m,n} x'$. Since $X/(1 - \gamma_n)X = A_n$ is finite, it follows that $1 - \gamma_n$ is prime to the support of $X$, hence $Ry$ is a finite submodule of $X$. Our assumption on $\text{Gal}(L/K) = X$ implies $Y = 0$ so that $H^2(G, X/(1 - \gamma_m)X)$ and hence $E_n/N_{m,n} E_m$ is trivial.

**Theorem 9.** If $\text{Gal}(L/K)^+ = 0$, then

$$R^-/S^- \approx \text{Gal}(L/K)^-. $$

**Proof.** This follows from $(*)$, $(**)$ and the plus part of the analytic class number formula.

**Theorem 10.** Suppose $\text{Gal}(L/K)^+ = 0$ then

$$L = K\left(\left\{ (\epsilon^a)^{1/p^{n-1}} : n > 0, \epsilon \in C_n^+ ; \alpha \in R, \alpha(S^*(-1))^+ \subseteq p^nR \right\}\right)$$

(here $C_n^+$ denotes the plus part of the global circular units).

**Proof.** This follows from Theorem 7, the fact that under these assumptions $A_k^+ = 0, S^+ / C^+ = 0$ and the perfect Kummer pairing

$$\text{Gal}(M/K)^- \times (E_{\infty} \otimes Q_p/Z_p) \to \mu_{p^\infty}.$$
REFERENCES


DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138

Current address: Department of Mathematics, University of California, Berkeley, California 94720