PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 89, Number 1, September 1983

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 Stickleberger 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 Washington's [4] books.

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

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

$$\mathcal{S}(g)\big(1-(1-T)^p\big) = \sum_{\zeta} g(1-\zeta(1-T)), \tag{1}$$

$$\mathcal{N}(f)\big(1-(1-T)^p\big) = \prod_{\zeta} f(1-\zeta(1-T)), \tag{2}$$

where ζ runs over the pth roots of unity μ_p. Let

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

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

We then have the identities

$$\mathcal{S}\operatorname{Log}(f) = \operatorname{Log}(\mathcal{N}f), \tag{3}$$

$$\mathcal{S}Dg = pD\mathcal{S}g, \tag{4}$$

$$\mathcal{S}\delta(h) = p\delta\mathcal{N}(h), \tag{5}$$

$$\mathcal{S}\varphi(g) = pg, \tag{6}$$

Received by the editors September 20, 1982 and, in revised form, December 20, 1982.
1980 *Mathematics Subject Classification.* Primary 12A35.

0002-9939/82/0000-1451/$03.00

$$D(g \circ [a]) = a(Df) \circ [a], \tag{7}$$

$$\delta(h \circ [a]) = a(\delta h) \circ [a], \tag{8}$$

for $f \in \mathbf{Z}_p[[T]]^0 = \{f \in \mathbf{Z}_p[[T]]: f(0) = 1 \bmod p\}$, $g \in \mathbf{Q}_p[[T]]_1$, $h \in \mathbf{Z}_p((T))^*$.

Let $\Phi_n = \mathbf{Q}_p(\mu_{p^{n+1}})$, $\Phi_\infty = \cup \Phi_n$, $G = \mathrm{Gal}(\Phi_\infty/\mathbf{Q}_p)$. Let $R = \mathbf{Z}_p[[G]]$ denote the completed group ring of G over $\mathbf{Z}_p$. Let χ: $G \to \mathbf{Z}_p^*$ denote the canonical character of G, giving its action on roots of unity of p-power order. Let $\zeta = (\zeta_n)$ be a fixed generator of $T_p(\mathbf{G}_m)$. If $a \in \mathbf{Z}_p^*$ we set $a(\zeta) = (\zeta_n^a)$.

As in [1] we may give the multiplicative group $\mathbf{Z}_p[[T]]^0$ and the additive group $\mathbf{Q}_p((T))_1$ 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^ω and ωg for f as an element of $\mathbf{Z}_p[[T]]^0$ and g as an element of $\mathbf{Q}_p((T))_1$. These actions are consistent with evaluation at the points $1 - \zeta_n$. Finally, if $a \in \mathbf{Z}_p^*$ 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 ζ) of R-modules*

$$0 \to T_p(\mathbf{G}_m) \to \mathbf{Z}_p[[T]]^0 \to \mathbf{Z}_p[[T]] \to T_p(\mathbf{G}_m) \to 0$$

(when $(p \neq 2)$) where the first map is given by $a(\zeta) \to (1 - T)^a$, the second by $f \mapsto (1 - \varphi/p)\mathrm{Log}\, f$ and the third by $g \mapsto Dg(0)(\zeta)$. (When $p = 2$ there is a similar exact sequence with $T_p(\mathbf{G}_m)$ replaced by $\mu_2 \oplus T_2(\mathbf{G}_m)$ in each case.)

LEMMA 2. $\mathbf{Z}_p[[T]] = R(1 - T) + \varphi(\mathbf{Z}_p[[T]])$.

PROOF. If $a \in \mathbf{Z}$, $a \geqslant 0$, $(a, p) = 1$ then

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

and is monic of degree a. If $a \in \mathbf{Z}$, $a \geqslant 0$ then

$$(-1)^a [p]^a = \varphi\big((-1)^a T^a\big) \in \varphi \mathbf{Z}_p[[T]]$$

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

Let $\mathcal{V} = \{g \in \mathbf{Z}_p[[T]]: \mathbb{S}(g) = 0\}$. 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

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

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 $\omega\zeta_n = 0$ for all $n \geqslant 0$, but this implies $\omega\Phi_\infty = 0$ which implies $\omega = 0$.

COROLLARY. *$D\mathcal{V} = \mathcal{V}$ and in fact the map $f \mapsto Df \otimes \zeta$ is an R-module isomorphism*

$$\mathcal{V} \tilde{\to} \mathcal{V} \otimes T_p(\mathbf{G}).$$

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 $\mathbf{Z}_p \cap \mathcal{V} = \varnothing$.

Now let $\mathcal{M} = \{f \in \mathbf{Z}_p((T))^*: \mathcal{N}(f) = f\}$. By Theorem 16 of [**1**], for each element $\alpha = (\alpha_n) \in \varprojlim \Phi_n^*$ there is a unique element $f_\alpha \in \mathcal{M}$ such that

$$f_\alpha(1 - \zeta_n) = \alpha_n,$$

and the map $\alpha \mapsto f_\alpha$ is a Galois-isomorphism.

Let $\mathcal{M}^0 = \mathcal{M} \cap \mathbf{Z}_p[[T]]^0$. Then $\mathcal{M}^0 \cong \operatorname{Lim} U_n$ where U_n is the group of principal units in Φ_n.

THEOREM 4. *We have an exact sequence of R-modules.*

$$0 \to T_p(\mathbf{G}_m) \to \mathcal{M} \to \mathcal{V} \to T_p(\mathbf{G}_m) \to 0$$

where the maps are as in Theorem 1 (*if* $p \neq 2$). (*Again there is a similar statement when* $p = 2$.)

PROOF. As $(1 - T) \in \mathcal{M}^0$, we only need check that $\mathcal{M}^0$ is the inverse image of $\mathcal{V}$ under the map $f \mapsto (1 - \varphi/p)\operatorname{Log}(f)$. However, using (3) and (6) we deduce

$$\mathcal{S}(1 - \varphi/p)\operatorname{Log} f = \operatorname{Log} \mathcal{N}(f) - \operatorname{Log} f = \operatorname{Log}(\mathcal{N}(f)/f).$$

So f is in the inverse image of $\mathcal{V}$ iff $(\mathcal{N}(f)/f \in \operatorname{Ker}(\operatorname{Log}) = 1)$ (if $p \neq 2$).

III. The image of the circular units. Let C_n denote the completion in Φ_n^* of the group of circular units in $\mathbf{Q}(\mu_{p^{n+1}})$. Thus C_n is generated topologically by the elements

$$T^{1-\sigma(a)}|_{T=1-\zeta_n} = [a](T)|_{T=1-\zeta_n} = \frac{1 - \zeta_n}{1 - \zeta_n^a},$$

with $a \in \mathbf{Z}_p^*$. Let $C_n^0 = C_n \cap U_n$.

Let $\mathcal{C} = \varprojlim C_n$ considered as a subgroup of $\mathcal{M}$ and $\mathcal{C}^0 = \mathcal{C} \cap \mathcal{M}^0$. It follows that $\mathcal{C}^0 \cong \varprojlim C_n^0$. Clearly $\mathcal{C}^0$ is an R-submodule of $\mathcal{M}^0$ generated over R by the elements

$$\omega(a)T^{1-\sigma(a)} \qquad (a \in \mathbf{Z}_p^*)$$

where $\omega: \mathbf{Z}_p^* \to \mu_{p-1}$ is the Teichmüller character.

Let

$$\theta_n = \sum_{a=1}^{p^{n+1}} B_1\left(\left\langle a/p^{n+1}\right\rangle\right)\sigma_a$$

denote the nth Stickleberger element, where $B_1(x) = x - \frac{1}{2}$, the first Bernoulli polynomial. Let $\theta = (\theta_n) \in \mathbf{Q}_p[[G]] \supseteq R$. Then the Stickleberger ideal is $\mathcal{S} = R\theta \cap R$. In fact, one knows $\mathcal{S}$ is generated over R by the elements

$$(1 - a\sigma^{-1}(a))\theta, \qquad a \in \mathbf{Z}_p^*.$$

There is an involution $\omega \to \omega^*$ of the ring $\mathbf{Q}_p[[G]]$ induced by

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

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

PROPOSITION 5 (KUMMER-IWASAWA).

$$\frac{\zeta_n}{\zeta_n - 1} - \frac{\zeta_{n-1}}{\zeta_{n-1} - 1} = \theta^*\zeta_n.$$

PROOF. This follows immediately from the equation

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

PROPOSITION 6. $\mathcal{V}/((1-\varphi)\delta\mathcal{C}^0) \cong R/\mathcal{S}^*$ *as* R*-modules.*

PROOF. $(1-\varphi)\delta\mathcal{C}^0$ is generated by the elements

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

By Proposition 5

$$\begin{aligned}(1-a\sigma(a))(1-\varphi)\delta(T)|_{1-\zeta_n} &= (1-a\sigma(a))(\theta^*\zeta_n)\\ &= ((1-a\sigma(a))\theta^*(1-T))|_{1-\zeta_n}\end{aligned}$$

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 $(1-\varphi)\delta\mathcal{C}^0$ is the span of $(1-a\sigma(a))\theta^*\mathcal{V}$ which is $\mathcal{S}^*\mathcal{V}$. 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

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

It is not hard to see that

$$R/I \otimes T_p(\mathbf{G}_m) \cong R/I(-1).$$

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

COROLLARY.

$$\mathcal{V}/(1-\varphi/p)\mathrm{Log}(\mathcal{C}^0) \cong R/\mathcal{S}^*(-1).$$

Finally using this and Theorem 4 we deduce

THEOREM 7. *There is an exact sequence*

$$0 \to \mathcal{M}^0/\mathcal{C}^0 \to R/\mathcal{S}^*(-1) \to T_p(\mathbf{G}_m) \to 0$$

of R*-modules.*

Taking " $+$ " parts we obtain

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

where $\mathcal{M}^+ = (\mathcal{M}^0)^+$, $\mathcal{C}^+ = (\mathcal{C}^0)^+$.

IV. Applications to global questions. Let

$K = \cup \mathbf{Q}(\mu_{p^n})$.

M = the maximal pro-p abelian unramified outside p extension of K.

L = the maximal unramified extension of K contained in L.

A_n = p-Sylow subgroup of the class group of $\mathbf{Q}_p(\mu_{p^{n+1}})$.

$A_k = \mathrm{Lim}_{n\to\infty} A_n$.

E_n = the completion in Φ_n^* of the units in $\mathbf{Q}_p(\mu_{p^{n+1}})$.

$E_n^0 = E_n \cap U_n$,

$E_n^+ = (E_n^0)^+$, and

$\mathfrak{E}^+ = \varprojlim E_n^+ \subseteq \mathfrak{M}^0$.

It is well known [**4**, Corollary 3.6], that

$$\mathfrak{M}^+/\mathfrak{E}^+ \cong \mathrm{Gal}(M/L)^+ .$$

Therefore we have the following exact sequence of R-modules.

$$(*) \qquad 0 \to \mathfrak{E}^+/\mathcal{C}^+ \to \mathfrak{M}^+/\mathcal{C}^+ \to \mathrm{Gal}(M/K)^+ \to \mathrm{Gal}(L/K)^+ \to 0.$$

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

$$\mathrm{Gal}(L/K)^- \cong R^-/\mathfrak{S}^-,$$

and in fact

$$A_n^- \cong R_n^-/\mathfrak{S}_n^-.$$

From the perfect (Kummer) pairing

$$(**) \qquad \mathrm{Gal}(M/K)^+ \times A_k^- \to \mu_{p^\infty}$$

and the fact $|A_n| < \infty$, it is not hard to show

$$\mathrm{Gal}(M/K)^+ \cong R^+/(\mathfrak{S}^-)^*(-1).$$

THEOREM 8 (IWASAWA). *Assuming A_0 is a cyclic R-module and* $\mathrm{Gal}(L/K)$ *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

$$\mathfrak{E}^+/\mathcal{C}^+ \cong \mathrm{Gal}(L/K)^+ .$$

The theorem follows by descending to finite layers, once one knows:

LEMMA. *If* $\mathrm{Gal}(L/K)$ *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

$$0 \to E_m \to K_m \to P_m \to 0, \qquad 0 \to P_m \to I_m \to H_m \to 0$$

where $K_m = \mathbf{Q}(\mu_{p^{m+1}})$, P_m = principal ideals in K_m, I_m = ideals of K_m and H_m = class group K_m, and using the facts that

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

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

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

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

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

where $L'_m = p$-Hilbert class field of K_m, $L_m = KL'_m \subseteq L$, $X = \text{Gal}(L/K)$ and $\gamma_n = \gamma^{p^{n+1}}$, where γ is a fixed generator of $\text{Gal}(K/\mathbf{Q}(\mu_p))$. 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 $H^2(G, E_m) \cong H^2(G, X/(1 - \gamma_m)X)$ and

$$H^2(G, X/(1 - \gamma_m)X) = \frac{\{x \in \mathbf{Z}: (1 - \gamma_n)x \in (1 - \gamma_m)X\}}{(1 - \gamma_m)X + \nu_{m,n}X},$$

where $\nu_{m,n} = (1 - \gamma_m)/(1 - \gamma_n) = 1 + \gamma_n + \cdots + \gamma_n^{p^{m-n}-1}$. 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*

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

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

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

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

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

PROOF. This follows from Theorm 7, the fact that under these assumptions $A_k^+ = 0$, $\mathcal{E}^+/\mathcal{C}^+ = 0$ and the perfect Kummer pairing

$$\text{Gal}(M/K)^- \times \left(E_\infty \otimes \mathbf{Q}_p/\mathbf{Z}_p\right) \to \mu_{p^\infty}.$$

REFERENCES

1. R. Coleman, *Division values in local fields*, Invent. Math. **53** (1979), 91–116.
2. K. Iwasawa, *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan **20** (1964), 42–82.
3. S. Lang, *Cyclotomic fields*, Graduate Texts in Math., Springer-Verlag, New York, 1978.
4. L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., Springer-Verlag, New York, 1982.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02138

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