COMPOSITIO MATHEMATICA

ROBERT GOLD
JAEMOON KIM

Bases for cyclotomic units

Compositio Mathematica, tome 71, nº 1 (1989), p. 13-27
<http://www.numdam.org/item?id=CM_1989__71_1_13_0>

© Foundation Compositio Mathematica, 1989, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (http://http://www.compositio.nl/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques
http://www.numdam.org/

Compositio Mathematica **71**: 13–28, 1989.
© *1989 Kluwer Academic Publishers. Printed in the Netherlands.*

Bases for cyclotomic units

ROBERT GOLD and JAEMOON KIM

Department of Mathematics, The Ohio State University, Columbus, Ohio, U.S.A.

Received 24 May 1988; accepted 2 November 1988

Section 0. Introduction

Let n be an integer, $n \not\equiv 2 \pmod 4$ and let $\zeta_n = e^{2\pi i/n}$, a primitive nth root of unity. Clearly with this choice we have $\zeta_n^{n/m} = \zeta_m$ for any $m|n$. Let E_n be the group of units of the field $\mathbb{Q}(\zeta_n)$, V_n the subgroup of $\mathbb{Q}(\zeta_n)^\times$ generated by

$$\{\pm\zeta_n, 1 - \zeta_n^a \colon 1 \leqslant a < n\}, \tag{1}$$

and $U_n = E_n \cap V_n$. Then U_n is the group of cyclotomic units of $\mathbb{Q}(\zeta_n)$. It is known that U_n is of finite index in E_n([13]). In particular $\operatorname{rank}_{\mathbb{Z}} U_n = \operatorname{rank}_{\mathbb{Z}} E_n = \frac{1}{2}\phi(n) - 1$.

Our goal in this paper is to provide a basis (minimal set of generators) for U_n, and to use this basis to show that $U_n^G = U_m$ for all $m|n$ where $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$.

There are relations among the elements of (1).

$$1 - \zeta_n^{-a} = -\zeta_n^{-a}(1 - \zeta_n^a) \tag{A}$$

$$1 - \zeta_m^a = \sum_{i=0}^{(n/m)-1} (1 - \zeta_n^{a+mi}) \quad \text{if} \quad m|n. \tag{B}$$

The first one is immediate and the second one comes from the identity

$$X^d - 1 = \prod_{i=0}^{d-1} (X - \zeta_d^i).$$

It had been conjectured by Milnor (unpublished) that every relation among the cyclotomic units is a consquence of (A) and (B), and H. Bass [1] claimed to have proved the conjecture. After a few years, V. Ennola [2] proved that twice any relation is a combination of (A) and (B), but not every relation is such a combination.

We will begin by finding a basis of the universal punctured even distribution $(A_n^0)^+$, which is the abelian group with generators

$$\left\{g\left(\frac{a}{n}\right): \frac{a}{n} \in \frac{1}{n}\,\mathbb{Z}/\mathbb{Z}, \frac{a}{n} \neq 0\right\}$$

and relations

$$g\left(\frac{-a}{n}\right) = g\left(\frac{a}{n}\right) \tag{A_1}$$

$$g\left(\frac{a}{m}\right) = \sum_{i=0}^{(n/m)-1} g\left(\frac{a+mi}{n}\right) \quad \text{if } m|n \text{ and } \frac{a}{m} \neq 0. \tag{B_1}$$

We introduce a theorem on $(A_n^0)^+$ which we use later and we refer the reader to L. Washington [5] for details.

THEOREM. *Let $n \not\equiv 2 \bmod 4$. Then there is a split exact sequence*

$$0 \to (\mathbb{Z}/2\mathbb{Z})^{2^{r-1}-r} \to (A_n^0)^+ \xrightarrow{\varphi} V_n/\langle \pm\zeta_n\rangle \to 0,$$

where $\varphi(g(a/n)) = 1 - \zeta_n^a \bmod(\pm\zeta_n)$ and r is the number of distinct prime factors of n.

Section 1. Basis of $(A_n^0)^+$

Let n be an integer, $n \not\equiv 2 (\bmod 4)$, and $p_1^{e_1} \ldots p_r^{e_r}$ be its prime factorization. Let $K_i = \mathbb{Q}(\zeta_{p_i^{e_i}})$. If p_i is odd, $\mathrm{Gal}(K_i/\mathbb{Q})$ is cyclic. Let σ_i be a fixed generator of $\mathrm{Gal}(K_i\mathbb{Q})$, or the corresponding element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ which fixes $\mathbb{Q}(\zeta_{n/p_i^{e_i}})$. Under the natural isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

which maps a to $\gamma: \zeta_n \mapsto \zeta_n^a$, we may view σ_i as an element of $(\mathbb{Z}/n\mathbb{Z})^\times$, or even a positive integer $< n$, relatively prime to n, since they form a set of representatives. If p_i is even, $\mathrm{Gal}(K_i/\mathbb{Q}) = \langle \tilde{\sigma}_i \tau\rangle$ where $\tilde{\sigma}_i$ is a fixed element of order 2^{e-2} and τ is the element of order 2 corresponding to complex conjugation. We let

$$\sigma_i^k = \begin{cases} \tilde{\sigma}_i^k & \text{if } 0 \leqslant k < 2^{e-2} \\ \tilde{\sigma}_i^k \tau & \text{if } 2^{e-2} \leqslant k < 2^{e-1}. \end{cases}$$

Then we consider the σ_i^k's as elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ as before.

LEMMA 1. Suppose $(b, n) = 1$. Then

$$\sum_{k=0}^{\varphi(p_i^{e_i})-1} g\left(\frac{b\sigma_i^k}{n}\right) = g\left(\frac{b}{n/p_i^{e_i}}\right) - g\left(\frac{c}{n/p_i^{e_i}}\right) \in (A^0_{n/p_i^{e_i}})^+ \qquad (B_2)$$

for some c.

Proof. Let $p_i = p, e_i = e$ and $\sigma_i = \sigma$ for simplicity. From the relation (B_1) in Section 0, we have

$$g\left(\frac{b}{n/p^e}\right) = \sum_{i=0}^{p^e-1} g\left(\frac{b + i(n/p^e)}{n}\right)$$

$$= \sum_{(b+i(n/p^e),n)=1} g\left(\frac{b + i(n/p^e)}{n}\right) + \sum_{(b+i(n/p^e),n)\neq 1} g\left(\frac{b + i(n/p^e)}{n}\right).$$

But, since σ fixes $\mathbb{Q}(\zeta_{n/p^e}), \sigma \equiv 1 (\text{mod } n/p^e)$. Thus

$$\sum_{(b+i(n/p^e),n)=1} g\left(\frac{b + i(n/p^e)}{n}\right) = \sum_{k=0}^{\varphi(p^e)-1} g\left(\frac{b\sigma^k}{n}\right).$$

On the other hand, let i_0 be such that

$$\begin{cases} b + i_0(n/p^e) \equiv 0 & \text{mod } p \\ b + i_0(n/p^e) \not\equiv 0 & \text{mod } p^2 \\ 0 \leqslant i_0 < p^e \end{cases}$$

and let $b + i_0(n/p^e) = cp$. Then $(c, n) = 1$ and $\{i_0 + tp\}$ is the set of all solutions for

$$\begin{cases} b + i(n/p^e) \equiv 0 & \text{mod } p \\ 0 \leqslant i < p^e \end{cases}$$

as t runs through all integers satisfying $0 \leqslant i_0 + tp < p^e$. Hence

$$\sum_{(b+i(n/p^e),n)\neq 1} g\left(\frac{b + i(n/p^e)}{n}\right) = \sum_t g\left(\frac{c + t(n/p^e)}{n/p}\right) = g\left(\frac{c}{n/p^e}\right). \qquad \text{Q.E.D.}$$

Let $n = p_1^{e_1} \cdots p_r^{e_r}$ as before and let

$$I_n = \begin{Bmatrix} (i_1, \dots, i_r) \mid 0 \leqslant i_r \leqslant \frac{1}{2}\varphi(p_r^{e_r}) - 1 & \text{and} \\ 0 \leqslant i_l \leqslant \varphi(p_l^{e_l}) - 1 & \text{for } l < r \end{Bmatrix}$$

and $I'_n = \{(i_1, \ldots, i_r) \in I_n$ satisfying one of the following$\}$

$$\begin{cases} i_r \neq 0 & & \text{and } i_l \neq 0 \text{ for all } l \leqslant r-1 \\ i_r = 0, & 1 \leqslant i_{r-1} \leqslant \frac{1}{2}\varphi(p_{r-1}^{e_{r-1}}) - 1 & \text{and } i_l \neq 0 \text{ for } l \leqslant r-2 \\ i_r = i_{r-1} = 0, & 1 \leqslant i_{r-2} \leqslant \frac{1}{2}\varphi(p_{r-2}^{e_{r-2}}) - 1 & \text{and } i_l \neq 0 \text{ for } l \leqslant r-3 \\ \vdots & & \\ i_r = i_{r-1} = \cdots = i_2 = 0, & 1 \leqslant i_1 \leqslant \frac{1}{2}\varphi(p_1^{e_1}) - 1 & \\ i_r = i_{r-1} = \cdots = i_2 = i_1 = 0. & & \end{cases}$$

Note that

$$\#(I'_n) = \tfrac{1}{2}(\varphi(p_r^{e_r}) - 1)(\varphi(p_{r-1}^{e_{r-1}}) - 1) \ldots (\varphi(p_1^{e_1}) - 1) + \tfrac{1}{2}.$$

Let T_n be the group generated by

$$\left\{ g\left(\frac{\sigma_1^{i_1} \ldots \sigma_r^{i_r}}{n}\right) \mid (i_1, \ldots, i_r) \in I'_n \right\}$$

and let

$$T'_n = \prod_{\substack{(d,n/d)=1 \\ d \neq 1,n}} T_d,$$

where T_d is defined similarly to T_n.

THEOREM 1. $(A_n^0)^+ = T_n \times T'_n = \prod_{\substack{(d,n/d)=1 \\ d>1}} T_d.$

REMARK. Since the number of generators of T_n is at most $\#(I'_n) = \frac{1}{2}\Pi(\varphi(p_i^{e_i}) - 1) + \frac{1}{2}$, $T_n \times T'_n$ is generated at most by $\mathrm{rank}_{\mathbb{Z}} V_n + 2^{r-1} - r$ elements, which is the minimum number of generators of $(A_n^0)^+$. Hence this theorem provides a basis of $(A_n^0)^+$.

Proof of theorem. By induction on r. By using the relations (A_1) and (B_1) with $m = p^k$, we can prove the theorem for $r = 1$ easily. Assume the theorem holds for n a product of $r - 1$ distinct primes. It is not hard to see $(A_n^0)^+ = T_n \times T_n^l$ if and only if $g(\sigma_1^{i_1} \ldots \sigma_r^{i_r}/n) \in T_n \times T'_n$ for every $(i_1, \ldots, i_r) \in I_n$. As a matter of notation, we let

$$g\left(\frac{\sigma_1^{i_1} \ldots \sigma_r^{i_r}}{n}\right) = g_{i_1 \ldots i_r}.$$

If $(i_1, \ldots, i_r) \in I'_n$, then $g_{i_1 \ldots i_r} \in T_n$ by definition. We prove $g_{i_1 \ldots i_r} \in T_n \times T'_n$ for $(i_1, \ldots, i_r) \in I_n - I'_n$ case by case.

(i) $g_{i_1 \ldots i_r} \in T_n \times T'_n$ if $i_r \neq 0$.

Proof. If none of $i_1, \ldots, i_{r-1}$ is 0, then $(i_1, \ldots, i_r) \in I'_n$ so $g_{i_1 \ldots i_r} \in T_n$. Suppose only one of $i_1, \ldots, i_{r-1}$ is 0, say i_1. Then for $j \neq 0$, $g_{i_2 \ldots i_r} \in T_n$ since $(j, i_2, \ldots i_r) \in I'_n$. Also,

$$\sum_{j=0}^{\varphi(p_1^{e_1})-1} g_{ji_2 \ldots i_r} \in T'_n$$

by the relation (B_2) in Lemma 1. Thus $g_{0i_2 \ldots i_r} \in T_n \times T'_n$. If two of $i_1, \ldots, i_{r-1}$ are 0, say $i_1 = i_2 = 0$, use the relation (B_2) again:

$$\sum_{j=0}^{\varphi(p_1^{e_1})-1} g_{j0i_3 \ldots i_r} \in T'_n.$$

Since $g_{j0i_3 \ldots i_r} \in T_n \times T'_n$ if $j \neq 0$ by the previous case, $g_{00i_3 \ldots i_r} \in T_n \times T'_n$. Then argue similarly for the case when there are exactly three zeros, and then four zeros and so on.

(ii) For each $l, 1 \leqslant l \leqslant r, g_{i_1 \ldots i_r} \in T_n \times T'_n$ if $i_r = i_{r-1} = \cdots = i_{l+1} = 0$ and $1 \leqslant i_l \leqslant \frac{1}{2}\varphi(p_l^{e_l}) - 1$.

Proof. We prove when $l = r - 1$ (the proof of the rest is quite similar to this case). We have to show $g_{i_1 \ldots i_{r-1}0} \in T_n \times T'_n$ when $1 \leqslant i_{r-1} \leqslant \frac{1}{2}\varphi(p_{r-1}^{e_{r-1}}) - 1$ and $i_1, i_2, \ldots, i_{r-2}$ arbitrary.

If none of $i_1, i_2, \ldots i_{r-2}$ is 0, then by the definition of I'_n, we are done. If only one of them is 0, say $i_1 = 0$, use the relation (B_2) again:

$$\sum_{j=0}^{\varphi(p^{e_1})-1} g_{ji_2 \ldots i_{r-1}0} \in T'_n.$$

Since $g_{ji_2 \ldots i_{r-1}0} \in T_n$ for $j \neq 0, g_{0i_2i_2 \ldots i_{r-1}0} \in T_n \times T'_n$. Then prove when there are exactly two zeros and proceed as we did in case (i).

(iii) Let $\delta_j = 0$ or $\frac{1}{2}\varphi(p_j^{e_j})$. If $(i_1, \ldots, i_r) \neq (\delta_1, \ldots, \delta_r)$, then $g_{i_1 \ldots i_r} \in T_n \times T'_n$.

Proof. Since case (i) treats the case $i_r \neq 0$, we assume $i_r = 0$ and prove

$$g_{i_1 \ldots i_{r-1}0} \in T_n \times T'_n \text{ when } (i_1, \ldots, i_{r-1}, 0) \neq (\delta_1, \ldots, \delta_{r-1}, 0).$$

First, we claim that $g_{i_1\ldots i_{r-1}0} \in T_n \times T'_n$ when $i_{r-1} \neq \delta_{r-1}$. If $1 \leqslant i_{r-1} \leqslant \frac{1}{2}\varphi(p_{r-1}^{e_{r-1}}) - 1$, the result follows from case (ii). Suppose $\frac{1}{2}\varphi(p_{r-1}^{e_{r-1}}) + 1 \leqslant i_{r-1} \leqslant \varphi(p_{r-1}^{e_{r-1}}) - 1$. Consider

$$\sum_{j=0}^{\varphi(p_r^{e_r})-1} g_{i_1\ldots i_{r-1}j} = g_{i_1\ldots i_{r-1}0} + \sum_{j=1}^{\frac{1}{2}\varphi(p_r^{e_r})-1} g_{i_1\ldots i_{r-1}j}$$

$$+ g_{i_1\ldots i_{r-1}\varphi(p_r^{e_r})/2} + \sum_{j=\frac{1}{2}\varphi(p_r^{e_r})+1}^{\varphi(p_r^{e_r})-1} g_{i_1\ldots i_{r-1}j}. \tag{$*$}$$

But $\Sigma_{j=1}^{\frac{1}{2}\varphi(p_r^{e_r})-1} g_{i_1\ldots i_{r_1}j} \in T_n \times T'_n$ by (i). Let $i'_l = i_l + \frac{1}{2}\varphi(p_l^{e_l})$. Then by the relation (A_1) in Section 0,

$$\sum_{j=\frac{1}{2}\varphi(p_r^{e_r})+1}^{\varphi(p_r^{e_r})-1} g_{i_1\ldots i_{r-1}j} = \sum_{j'=1}^{\frac{1}{2}\varphi(p_r^{e_r})-1} g_{i'_1\ldots i'_{r-1}j'} \in T_n \times T'_n$$

by (i). Also, since $1 \leqslant i'_{r-1} \leqslant \frac{1}{2}\varphi(p_{r-1}^{e_{r-1}})$,

$$g_{i_1\ldots i_{r-1}\varphi(p_r^{e_r})/2} = g_{i'_1\ldots i'_{r-1}0} \in T_n \times T'_n.$$

Since the left side of $(*)$ is in T'_n by Lemma 1, so is the right side. Therefore $g_{i_1\ldots i_{r-1}0} \in T_n \times T'_n$ when $i_{r-1} \neq \delta_{r-1}$.

Now we assume $g_{i_1\ldots i_l i_{l+1}\ldots i_{r-1}0} \in T_n \times T'_n$ when $(i_{l+1},\ldots,i_{r-1},0) \neq (\delta_{l+1},\ldots,\delta_{r-1},0)$, and we will show $g_{i_1\ldots i_l i_{l+1}\ldots i_{r-1}0} \in T_n \times T'_n$ if $i_l \neq \delta_l$ and $(i_{l+1},\ldots,i_{r-1},0) \neq (\delta_{l+1},\ldots,\delta_{r-1},0)$.

Suppose $1 \leqslant i_l \leqslant \frac{1}{2}\varphi(p_l^{e_l}) - 1$. If all of $i_{l+1},\ldots i_{r-1}$ are 0, the result follows from case (ii). Suppose only one of them, say i_t, is $\frac{1}{2}\varphi(p_t^{e_t})$. Consider

$$\sum_{j=0}^{\varphi(p_t^{e_t})-1} g_{i_1\ldots i_l 0\ldots 0 j 0\ldots 0} \in T'_n.$$

Since $g_{i_1\ldots i_l 0\ldots 0} \in T_n \times T'_n$ by (ii) and since $\Sigma_{j\neq 0,\frac{1}{2}\varphi(p_t^{e_t})} g_{i_1\ldots i_l 0\ldots 0 j 0} \in T_n \times T'_n$ by assumption, $g_{i_1\ldots i_l 0\ldots 0\varphi(p_t^{e_t})/2 0\ldots 0} \in T_n \times T'_n$. Then we can prove the case when two of $i_{l+1},\ldots,i_{r-1}$ are non zero δ, then three nonzero δ, and so on.

Suppose $\frac{1}{2}\varphi(p_l^{e_l}) + 1 \leqslant i_l \leqslant \varphi(p_l^{e_l}) - 1$. Consider

$$\sum_{j=0}^{\varphi(p_r^{e_r})-1} g_{i_1\ldots i_l \delta_{l+1}\ldots\delta_{r-1}j}$$

$$= g_{i_1\ldots i_l\delta_{l+1}\delta_{r-1}0} + \sum_{j=1}^{\frac{1}{2}\varphi(p_r^{e_r})-1} g_{i_1\ldots i_l\delta_{l+1}\ldots\delta_{r-1}j}$$

$$+ g_{i_1\ldots i_l\delta_{l+1}\ldots\delta_{r-1}\varphi(p_r^{e_r})/2} + \sum_{j=\frac{1}{2}\varphi(p_r^{e_r})+1}^{\varphi(p_r^{e_r})-1} g_{i_1\ldots i_l\delta_{l+1}\ldots\delta_{r-1}j}. \qquad (**)$$

By arguing similarly as before, we can show that every term but the first of the right side of (**) belongs to $T_n \times T'_n$. Since the left side of (**) is also in $T_n \times T'_n$, we conclude that $g_{i_1\ldots i_l\delta_{l+1}\ldots\delta_{r-1}0} \in T_n \times T'_n$.

(iv) $g_{\delta_1\ldots\delta_{r-1}0} \in T_n \times T'_n$

Proof. We know that $g_{0\ldots 0} = g(1/n) \in T_n$. If only one δ_i is different from 0, say δ_1, consider

$$\sum_{j=0}^{\varphi(p_1^{e_1})-1} g_{j0\ldots 0} \in T'_n.$$

Since every term except $g_{(\varphi(p_1^{e_1})/2)0\ldots 0}$ belongs to $T_n \times T'_n$, so does $g_{(\varphi(p_1^{e_1})/2)0\ldots 0}$. Then prove the case when there are two non zeros, and so on.

This finishes the proof of Theorem 1.

Section 2. Basis of U_n

Let $n = p_1^{e_1} \ldots p_r^{e_r}$ be an integer $\not\equiv 2 (\operatorname{mod} 4)$ as before. To find a basis of U_n, we eliminate certain generators of T_n. To be precise, let

$$I''_n = \begin{cases} I'_n - \{(0, 0 \ldots, 0)\} & \text{if } r = \text{odd} \\ I'_n & \text{if } r = \text{even} \end{cases}$$

$$\tilde{g}\left(\frac{a}{n}\right) = \begin{cases} g^{(a/n)} & \text{if } n \text{ is composite} \\ g^{(a/p^e)} - g^{(1/p^e)} & \text{if } n = p^e \end{cases}$$

$$\tilde{T}_n = \text{group generated by } \left\{ \tilde{g}\left(\frac{\sigma_1^{i_1} \ldots \sigma_r^{i_r}}{n}\right) \,\middle|\, (i_1, \ldots, i_r) \in I''_n \right\}$$

$$\tilde{T}'_n = \prod_{\substack{d|n \\ (d,n/d)=1 \\ d\neq 1,n}} \tilde{T}_d, \quad \text{where } \tilde{T}_d \text{ is defined similarly to } \tilde{T}_n.$$

REMARK. The passage from g to $\tilde{g}$ takes account of the fact that $1 - \zeta_n$ is a unit if and only if n is not a prime power. When n is a power of p, $1 - \zeta_n$ is a divisor of p.

Note that

$$(A_n^0)^+ = G_1 \times G_2 \times G_3, \text{ where}$$

$$G_1 = \tilde{T}_n \times \tilde{T}'_n$$

$$G_2 = \text{group generated by } \left\{ g\left(\frac{1}{p_i^{e_i}}\right) \,\middle|\, 1 \leqslant i \leqslant r \right\}$$

$$G_3 = \text{group generated by } \left\{ g\left(\frac{1}{p_{i_1}^{e_{r_1}} \cdots p_{i_l}^{e_{r_l}}}\right) \,\middle|\, l \geqslant 3, \text{odd} \right\}.$$

THEOREM 2. $U_n = \varphi(G_1) \times \langle -\zeta_n \rangle$, *where* $\varphi\colon (A_n^0)^+ \to V_n \bmod \langle -\zeta_n \rangle$ *is as in the theorem of Section* 0.

REMARK. Since G_1 is generated by at most $\operatorname{rank}_{\mathbb{Z}} U_n$ elements, this theorem provides a basis of U_n.

Before we prove Theorem 2, we need several lemmas.

LEMMA 2. $2g(1/n) \in G_1$ if *n is composite.*

Proof. If r is even, there is nothing to prove. So we assume r is odd. Let $m_i = \frac{1}{2}\varphi(p_i^{e_i}) - 1$, $M_i = \varphi(p_i^{e_i}) - 1$ and let

$$\sum_{0 \leqslant i_1 \leqslant m_1} \sum_{0 \leqslant i_2 \leqslant m_2} \cdots \sum_{0 \leqslant i_r \leqslant m_r} g_{i_1 \ldots i_r} = R_0$$

and for each $l, 1 \leqslant l \leqslant r$, let

$$\sum_{m_1+1 \leqslant i_1 \leqslant M_1} \cdots \sum_{m_l+1 \leqslant i_l \leqslant M_l} \sum_{0 \leqslant i_{l+1} \leqslant m_{l+1}} \cdots \sum_{0 \leqslant i_r \leqslant m_r} g_{i_1 \ldots i_r} = R_l.$$

Then $R_i + R_{i+1} \in \tilde{T}'_n$ for each $i = 1, 2, \ldots r-1$ by Lemma 1. Hence $R_0 + R_r = (R_0 + R_1) - (R_1 + R_2) + (R_2 + R_3) - \cdots + (R_{r-1} + R_r) \in \tilde{T}'_n$. But since $R_0 = R_r$, we have $2R_0 \in \tilde{T}'_n$. And in the sum of R_0, every term except $g_{0\ldots 0}$ belongs to $\tilde{T}_n \times \tilde{T}'_n$. Therefore $2g_{0\ldots 0} = 2g(1/n) \in \tilde{T}_n \times \tilde{T}'_n = G_1$. Q.E.D.

LEMMA 3. *The given generators of* $G_1 \times G_2$ *are linearly independent over* $\mathbb{Z}$.

Proof. In the proof of Theorem 1, we used the fact $(0, \ldots, 0) \in I'_n$ only in step (iv). But since $2g(1/n) \in G_1$ by Lemma 2, $2g_{\delta_1 \ldots \delta_r} \in G_1$. Thus $G_1 \times G_2$ is of finite index in $(A_n^0)^+$, hence $\varphi(G_1 \times G_2)$ is of finite index in V_n. Since G_1 is mapped to U_n and since G_2 is mapped to nonunits, $\varphi(G_1)$ is of finite index in U_n. Since $\varphi(G_1)$ is generated at most by $\operatorname{rank}_{\mathbb{Z}} U_n$ elements, the generators of $\varphi(G_1)$ are linearly independent. Therefore the given generators of G_1 are linearly independent and so are the generators of $G_1 \times G_2$. Q.E.D.

LEMMA 4. *Let $r \geqslant 3$ odd. Then there is a unique $R \in (A_n^0)^+$ such that $R \neq 0, 2R = 0$ and R is of the form*

$$R = g\left(\frac{1}{n}\right) + \sum_{\tilde{g}(a/n) \in G_1} \tilde{f}\left(\frac{a}{n}\right)\tilde{g}\left(\frac{a}{n}\right)$$

with $\tilde{f}(a/n) \in \mathbb{Z}$.

Proof. Uniqueness is immediate by Lemma 3. We prove existence by induction on r. Suppose $r = 3$. Since $\mathrm{Tor}(A_n^0)^+ \simeq \mathbb{Z}/2\mathbb{Z}$ by the theorem in Section 0, there is an $R \neq 0$ such that $2R = 0$. Since $(A_n^0)^+ = G_1 \times G_2 \times G_3$, we may write

$$R = mg\left(\frac{1}{n}\right) + \sum_{\tilde{g}(a/n) \in G_1} \tilde{f}\left(\frac{a}{n}\right)\tilde{g}\left(\frac{a}{n}\right) + \sum_{i=1}^{3} f\left(\frac{1}{p_i^{e_i}}\right) g\left(\frac{1}{p_i^{e_i}}\right)$$

Since $2g(1/n) \in G_1$,

$$2g\left(\frac{1}{n}\right) = \sum_{\tilde{g}(a/n) \in G_1} \tilde{h}\left(\frac{a}{n}\right)\tilde{g}\left(\frac{a}{n}\right)$$

with $\tilde{h}(a/n) \in \mathbb{Z}$. Thus we may assume $m = 0$ or 1. But if $m = 0$, then

$$0 = 2R = \sum \tilde{f}\left(\frac{a}{n}\right)\tilde{g}\left(\frac{a}{n}\right) + \sum f\left(\frac{1}{p_i^{e_i}}\right) g\left(\frac{1}{p_i^{e_i}}\right)$$

implies $\tilde{f}(a/n) = f(1/p_i^{e_i}) = 0$ by the linear independence (Lemma 3), which forces $R = 0$. Hence $m = 1$ and

$$R = g\left(\frac{1}{n}\right) + \sum \tilde{f}\left(\frac{a}{n}\right)\tilde{g}\left(\frac{a}{n}\right) + \sum f\left(\frac{1}{p_i^{e_i}}\right) g\left(\frac{1}{p_i^{e_i}}\right).$$

Now apply the map φ to both sides to obtain

$$1 = \varphi\left(g\left(\frac{1}{n}\right)\right) \times \prod \varphi\left(\tilde{g}\left(\frac{a}{n}\right)\right)^{\tilde{f}(a/n)} \times \prod \varphi\left(g\left(\frac{1}{p_i^{e_i}}\right)\right)^{f(1/p_i^{e_i})}.$$

Since the first two terms of the right side are units, $f(1/p_i^{e_i}) = 0$ and R has the desired form.

Suppose the lemma is true for all d less than r. For any d of the form $p_{i_1}^{e_{i_1}}\mathrm{cdots}p_{i_l}^{e_{i_l}}$ with $3 \leqslant l < r, l$ odd, there is an element $R_d \in (A_n^0)^+$ such that

$R_d \neq 0, 2R_d = 0$ and R_d is of the form.

$$R_d = g\left(\frac{1}{d}\right) + \sum \cdots$$

by the induction hypothesis. Note that R_d's are linearly independent, i.e. $R_{d_1} + \cdots + R_{d_s} \neq 0$ for any distinct choice of $d, \ldots, d_s$, for otherwise, $g(1/d_1)$ would be expressed by other generators of $G_1 \times G_2 \times G_3$, which is impossible. So we have

$$\binom{r}{3} + \binom{r}{5} + \cdots + \binom{r}{r-2} = 2^{r-1} - r - 1$$

independent elements of $\mathrm{Tor}(A_n^0)^+$. But since

$$\mathrm{Tor}(A_n^0)^+ \simeq (\mathbb{Z}/2\mathbb{Z})^{2^{r-1}-r},$$

there is one more generator of $\mathrm{Tor}(A_n^0)^+$, say R_1. We can write

$$R_1 = cg\left(\frac{1}{n}\right) + \sum_{\tilde{g}(a/n) \in G_1} \tilde{f}\left(\frac{a}{n}\right)\tilde{g}\left(\frac{a}{n}\right) + \sum_{g(1/p_i^{e_i} \in G_2} f\left(\frac{1}{p_i^{e_i}}\right) g\left(\frac{1}{p_i^{e_i}}\right)$$
$$+ \sum_{g(1/a) \in G_3} f\left(\frac{1}{d}\right) g\left(\frac{1}{d}\right).$$

As in the case $r = 3$, we may assume $c = 0$ or 1. Suppose $c = 0$. Then

$$R_1 - \sum f\left(\frac{1}{d}\right) R_d$$

in an element of $\mathrm{Tor}(A_n^0)^+$ with $f(1/d) = 0$ for any $g(1/d) \in G_3$. Then, by Lemma 3,

$$R_1 - \sum f\left(\frac{1}{d}\right) R_d = 0$$

which is impossible since R_1 is not in the span of R_d's. Hence $c = 1$ and R_1 is of the form

$$R_1 = g\left(\frac{1}{n}\right) + \sum \tilde{f}\left(\frac{a}{n}\right)\tilde{g}\left(\frac{a}{n}\right) + \sum f\left(\frac{1}{p_i^{e_i}}\right) g\left(\frac{1}{p_i^{e_i}}\right) + \sum f\left(\frac{1}{d}\right) g\left(\frac{1}{d}\right).$$

Since $f(1/p_i^{e_i}) = 0$ as in the case $r = 3$, we get a desired element

$$R = R_1 - \sum f\left(\frac{1}{d}\right) R_d.$$

Proof of Theorem 2. It is easy to prove if n is a prime power, so we assume n is composite. By step (iv) in the proof of Theorem 1, it is enough to show that $\varphi(g(1/n)) \in \varphi(G_1)$. But this is obvious by Lemma 4. Just apply φ to R to obtain

$$1 = \varphi\left(g\left(\frac{1}{n}\right)\right) \times \prod \varphi\left(\tilde{g}\left(\frac{a}{n}\right)\right)^{\tilde{f}(a/n)}. \qquad \text{Q.E.D.}$$

COROLLARY 1. *Suppose m and n are integers,* $\not\equiv 2 (\mathrm{mod}\, 4)$, *and* $(m, n) = 1$. *Then*

$$U_{mn}^G = U_n$$

where $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n))$ and U_{mn}^G is the subgroup of U_{mn} fixed under the action of G.

Proof. By Theorem 2, we can extend a basis $\{\eta_1, \dots, \eta_s\}$ of $U_n \mathrm{mod}\langle -\zeta_n\rangle$ to a basis $\{\eta_1 \dots, \eta_s, \varepsilon_1, \dots, \varepsilon_t\}$ of $U_{mn} \mathrm{mod}\langle -\zeta_{mn}\rangle$. Let

$$\delta = \pm \zeta_{mn}^c \eta_1^{a_1} \dots \eta_s^{a_s} \varepsilon_1^{b_1} \dots \varepsilon_t^{b_t} \in U_{mn}^G.$$

Then since $\delta^\sigma = \delta$ for any $\sigma \in G$,

$$\delta^{\varphi(m)} = N_{\mathbb{Q}(\zeta_{mn})/\mathbb{Q}(\zeta_n)} \delta \in U_n.$$

Hence

$$(\pm \zeta_{mn}^c)^{\phi(m)} \prod_{i=1}^{s} \eta_i^{a_i \phi(m)} \prod_{j=1}^{t} \varepsilon_j^{b_j \phi(m)}$$

$$= \pm \zeta_n^e \eta_1^{d_1} \dots \eta_s^{d_s}.$$

Therefore, $b_1 = b_t = 0$ and

$$\delta = \pm \zeta_{mn}^c \eta_1^{a_1} \dots \eta_s^{a_s}.$$

Since $\delta, \eta_1^{a_1} \dots \eta_s^{a_s} \in U_{mn}^G$, $\pm \zeta_{mn}^c \in U_{mn}^G$. Thus

$$\delta = \pm \zeta_n^f \eta_1^{a_1} \dots \eta_s^{a_s} \in U_n. \qquad \text{Q.E.D.}$$

Section 3. Basis of U_{pn} when $p|n$

In this section we will show $U_{pn}^G = U_n$, where $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{pn})/\mathbb{Q}(\zeta_n))$ by extending a basis of U_n to that of U_{pn}. When $p \mid n$, Corollary 1 in Section 2 proves it. So we assume $p \mid n$ and let $n = p_1^{e_1} \dots p_r^{e_r} p^e$ be the usual prime factorization of n with $e > 0$. As before we let σ_i be a fixed generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{e_i}}/\mathbb{Q}))$ for $i = 1, \dots, r$ and let σ be a fixed generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{e+1}})/\mathbb{Q})$. If p_i is even then we define σ_i^k as in Section 1. For each $d \mid n$ such that $(d, (n/d)) = 1$ and $(d, p) = 1$, say, $d = p_{i_1}^{e_{i_1}} \dots p_{i_t}^{e_{i_t}}$, let $\tilde{T}_d''$ be the subgroup of $(A_n^0)^+$ generated by

$$\left\{ \tilde{g}^{\sigma_{i_1}^{j_1} \dots \sigma_{i_t}^{j_t} \sigma^j / dp^{e+1}} : \begin{array}{l} \tfrac{1}{2}\varphi(p^e) \leqslant j \leqslant \tfrac{1}{2}\varphi(p^{e+1}) - 1, \\ 1 \leqslant j_l \leqslant \varphi(p_l^{e_l} - 1 \\ \text{if } p \neq 2, \text{ and } 1 \leqslant j \leqslant 2^{e-2} \text{ if } p = 2 \\ \text{for } 1 \leqslant l \leqslant t \end{array} \right\}.$$

and let

$$\tilde{T}_n'' = \prod_d \tilde{T}_d''.$$

Then it is easy to check that $\tilde{T}_n''$ is generated at most (actually, exactly by the following theorem) by $\mathrm{rank}_{\mathbb{Z}}\, U_{pn} - \mathrm{rank}_{\mathbb{Z}}\, U_n$ elements.

THEOREM 3. $U_{pm} = \varphi(\tilde{T}_n \times \tilde{T}_n' \times \tilde{T}_n'') \times \langle -\zeta_{pn} \rangle$.

Proof. We prove this only when p is odd. The proof for the even case is almost the same. We will show $U_{dp^{e+1}} = \varphi(\tilde{T}_{dp^e} \times \tilde{T}_{dp^e}' \times \tilde{T}_{dp^e}'')$ for each d with $(d, p) = 1$ $(d, n/d) = 1$ by induction on $w(d)$ = number of distinct prime factors of d.

Let $w(d) = 0 (d = 1)$. By Theorem 2, it is enough to show

$$\tilde{g}_j = \tilde{g}\left(\frac{\sigma^j}{p^{e+1}}\right) \in \tilde{T}_{p^e} \times \tilde{T}_{p^e}''$$

for $1 \leqslant j \leqslant \frac{1}{2}\varphi(p^{e+1}) - 1$, hence for $1 \leqslant j \leqslant \frac{1}{2}\varphi(p^e) - 1$ be definition of $\tilde{T}_{p^e}''$. First we need a Lemma.

LEMMA 5. *For any j, $1 \leqslant j \leqslant \frac{1}{2}\varphi(p^e) - 1$,*

$$\sum_{k=0}^{p-1} \tilde{g}_{j+k\varphi(p^e)} = \tilde{g}\left(\frac{\sigma^j}{p^e}\right) + \sum_{k=0}^{p-1} \tilde{g}_{k\varphi(p^e)}.$$

Proof. Immediate from the relation (B_1) since

$$\sigma^{k\varphi(p^e)} \equiv 1 \bmod p^e \text{ for } 0 \leqslant k \leqslant p - 1.$$

In the left side of Lemma 5, every term except for $\tilde{g}_j(k=0)$ belongs to $\tilde{T}''_{p^e}$ since for $1 \leqslant k \leqslant (p-1)/2$,

$$\tilde{g}_{j+k\varphi(p^e)} \in \tilde{T}''_{p^e}$$

by the definition of $\tilde{T}''_{p^e}$, and for $(p+1)/2 \leqslant k \leqslant p-1$ we have

$$\tilde{g}_{j+k\varphi(p^e)} = \tilde{g}_{j+k\varphi(p^e)-\frac{1}{2}\varphi(p^{e+1})} \in \tilde{T}''_{p^e}$$

Similarly,

$$\sum_{k=1}^{p-1} \tilde{g}_{k\varphi(p^e)} \in \tilde{T}''_{p^e}.$$

Since $\tilde{g}_0 = 1$ and since $\tilde{g}(\sigma^j/p^e) \in \tilde{T}_{p^e}$,

$$\tilde{g}_j = \tilde{g}\left(\frac{\sigma^j}{p^e}\right) + \sum_{k=0}^{p-1} \tilde{g}_{k\varphi(p^e)} - \sum_{k=1}^{p-1} \tilde{g}_{j+k\varphi(p^e)} \in \tilde{T}_{p^e} \times \tilde{T}''_{p^e}.$$

This settles the case $d = 1$.

Now we assume $U_{dp^{e+1}} = \varphi(\tilde{T}_{dp^e} \times \tilde{T}'_{dp^e} \times \tilde{T}''_{dp^e})$ for each d with $\omega(d) < r$, and we will show that it is also true for $d = n/p^e$. By Theorem 2, it is enough to show that for each $d = p_{i_1}^{e_{i_1}} \dots p_{i_t}^{e_{i_t}}$

$$\tilde{g}_{j_i \dots j_t j} \in \tilde{T}_{dp^e} \times \tilde{T}'_{dp^e} \times \tilde{T}''_{dp^e}$$

for $(j_1, j_2, \dots, j_t, j) \in I''_{dp^{e+1}}$, but actually we will show this for all $(j_1, \dots, j_t, j) \in I_{dp^{e+1}}$ case by case.

(i) $\tilde{g}_{j_1 \dots j_t j} \in \tilde{T}_{dp^e} \times \tilde{T}'_{dp^e} \times \tilde{T}''_{dp^e}$ for $\frac{1}{2}\varphi(p^e) \leqslant j \leqslant \frac{1}{2}\varphi(p^{e+1}) - 1$ and j_l arbitrary

Proof. If none of j_l, $1 \leqslant l \leqslant t$, is 0, there is nothing to prove. Suppose exactly one of them, say j_1, is 0. Then

$$\sum_{k=0}^{\varphi(p_{i_1}^{e_{i_1}})-1} \tilde{g}_{kj_2 \dots j_t j} \in \tilde{T}_{(d/p_{i_1}^{e_{i_1}})p^e} \times \tilde{T}'_{(d/p_{i_1}^{e_{i_1}})p^e} \times \tilde{T}''_{(d/p_{i_1}^{e_{i_1}})p^e}$$

by Lemma 1 (with a slight modification), and the induction hypothesis. But since

$$\sum_{k=1}^{\varphi(p_{i_1}^{e_{i_p}})-1} \tilde{g}_{kj_2 \dots j_t j} \in \tilde{T}''_{dp^e}$$

by the definition of $\tilde{T}''_{dp^e}, g_{0j_2\dots j_tj} \in \tilde{T}_{dp^e} \times \tilde{T}'_{dp^e} \times \tilde{T}''_{dp^e}$. Then we can proceed as we did in step (i) of the proof of Theorem 1.

(ii) $\tilde{g}_{0j_1\dots j_tj} \in \tilde{T}_{dp^e} \times \tilde{T}'_{dp^e} \times \tilde{T}''_{dp^e}$ for $1 \leqslant j \leqslant \frac{1}{2}\varphi(p^l) - 1$ and j_l arbitrary.

Proof. From the relation (B_1), we have

$$\sum_{k=0}^{p-1} \tilde{g}_{0j_1\dots j_tj+k\varphi(p^e)} \in \tilde{T}_{dp^e} \times \tilde{T}'_{dp^e}.$$

We consider two cases $1 \leqslant k \leqslant (p-1)/2$ and $(p+1)/2 \leqslant k \leqslant p-1$ separately to show

$$\sum_{k=1}^{p-1} \tilde{g}_{j_1\dots j_tj+k\varphi(p^e)} \in \tilde{T}_{dp^e} \times \tilde{T}'_{dp^e} \times \tilde{T}''_{dp^e}$$

as in the proof of the case $w(d) = 0$. Thus we get the result.

(iii) $\tilde{g}_{j_1\dots j_tj} \in \tilde{T}_{dp^e} \times \tilde{T}'_{dp^e} \times \tilde{T}''_{dp^e}$ for $j = 0$ and j_l arbitrary.

Proof. Quite similar to the proof of (ii) by considering

$$\sum_{k=0}^{p-1} \tilde{g}_{j_1\dots j_tk\varphi(p^e)}.$$

This finishes the proof. Q.E.D.

COROLLARY 2. *Let $p \mid n$ for $n \not\equiv 2 \pmod 4$. Then*

$$U_{pn}^G = U_n,$$

where $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{pn})/\mathbb{Q}(\zeta_n))$.

Proof. Similar to Corollary 1.

COROLLARY 3. For any integers m and n, $m, n \neq 2 \pmod 4$, such that $n|m$, the natural map

$$E_n/U_n \to E_m/U_m$$

is an injection.

Proof. By Corollary 1 and 2.

Remark. As an application of Corollary 3 consider $\mathbb{Q}(\zeta_n)$, $\mathbb{Q}(\zeta_m)$ as two layers in the cyclotomic $\mathbb{Z}_p$-extension of some $\mathbb{Q}(\zeta_d)$. Greenberg's conjecture asserts that the p-primary part of E_n/U_n has bounded order as $n \uparrow \infty$. Assuming that

Greenberg's conjecture is true, Corollary 3 implies that the map $(E_n/U_n)_p \to (E_m/U_m)_p$ is an isomorphism for $m > n \gg 0$. It follows that the map in the opposite direction induced by the norm is the zero map for $m \gg n \gg 0$. Therefore the projective limit of $(E_n/U_n)_p$ is trivial. It follows that $(\varprojlim E_n/\varprojlim U_n)_p = 0$ or, in other words, $p \nmid [E_n' : U_n]$ for any n where $E_n' = \bigcap_{m \geqslant n} N_{m,n}(E_m)$.

References

1. H. Bass, Generators and relations for cyclotomic units, *Nagoya Math. J.* 27 (1966), 401–407.
2. V. Ennola, On relations between cyclotomic units, *J. Number Theory* 4 (1972), 236–247.
3. W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. of Math.* (2) 108 (1978), 107–134.
4. W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, *Invent. Math.* 62 (1980), 181–234.
5. L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1980.