Korean J. Math. **18** (2010), No. 2, pp. 161–166

CIRCULAR UNITS OF ABELIAN FIELDS WITH A PRIME POWER CONDUCTOR

Jae Moon Kim and Jado Ryu*

Abstract. For an abelian extension K of $\mathbb{Q}$, let $C_W(K)$ be the group of Washington units of K, and $C_S(K)$ the group of Sinnott units of K. A lot of results about $C_S(K)$ have been found while very few is known about $C_W(K)$. This is mainly because elements in $C_S(K)$ are more explicitly defined than those in $C_W(K)$. The aim of this paper is to find a basis of $C_W(K)$ and use it to compare $C_W(K)$ and $C_S(K)$ when K is a subfield of $\mathbb{Q}(\zeta_{p^e})$, where p is a prime.

1. Introduction

For each positive integer n not congruent to 2 mod 4, we fix a primitive nth root of 1 in $\mathbb{C}$ by $\zeta_n = e^{\frac{2\pi i}{n}}$ so that $\zeta_n^{\frac{n}{m}} = \zeta_m$ whenever $m|n$. The field $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$ with $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^\times$, the multiplicative group consisting of the units of the ring $\mathbb{Z}_n$. So $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where φ is the Euler φ function.

We denote the unit group of the ring of integers of a number field K by $E(K)$. It is well known that $E(K)$ is a finitely generated abelian group whose free part is of rank $r_1 + r_2 - 1$, where r_1 is the number of real embeddings of K and r_2 is that of pairs of complex embeddings of K. And the torsion subgroup $W(K)$ of $E(K)$ consists of roots of unity in K and is a finite cyclic group. Thus

$$E(\mathbb{Q}(\zeta_n)) \simeq W(\mathbb{Q}(\zeta_n)) \oplus \mathbb{Z}^{\frac{1}{2}\varphi(n)-1}.$$

Note that $W(\mathbb{Q}(\zeta_n))$ is a cyclic group generated by $-\zeta_n$.

Received April 12, 2010. Revised June 3, 2010. Accepted June 7, 2010.
2000 Mathematics Subject Classification: 11R18, 11R27.
Key words and phrases: cyclotomic unit, Sinnot unit, Washington unit.
This work was supported by Inha University Reserch Grant.
*Corresponding author.

This structure theorem for $E(\mathbb{Q}(\zeta_n))$, however, does not provide with a basis for the unit group. In fact, even in the simplest case when $n = p$ is a prime, not any basis is known. Fortunately, the unit group has a special subgroup with explicitly described generators which is called the group of cyclotomic units. To be precise, let V_n be the multiplicative subgroup of $\mathbb{Q}(\zeta_n)^\times$ generated by $\{\pm\zeta_n, 1-\zeta_n^a | 1 \le a \le n-1\}$. The group of cyclotomic units of $\mathbb{Q}(\zeta_n)$ is then defined by $C(\mathbb{Q}(\zeta_n)) = V_n \cap E(\mathbb{Q}(\zeta_n))$. The elements in $C(\mathbb{Q}(\zeta_n))$ are called cyclotomic units. The most important property of the group of cyclotomic units is the following index formula:

$$[E(\mathbb{Q}(\zeta_n)) : C(\mathbb{Q}(\zeta_n))] = 2^b h_n^+$$

for some nonnegative integer b ([3]). Here h_n^+ is the class number of $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

For abelian extensions, the situation is quite different. In [4], for an abelian extension K, Sinnott defines $C_S(K)$, the group circular units of K by

$$C_S(K) = E(K) \cap \left\langle -1, \mathbf{N}_{\mathbb{Q}(\zeta_m)/K\cap\mathbb{Q}(\zeta_m)}\,(1-\zeta_m^a) \,\middle|\, m, a \in \mathbb{Z}, m > 1, m \nmid a \right\rangle.$$

In that paper, he computes the index $[E(K) : C_S(K)]$, showing how the class number of K is remarkably involved in the index.

Another subgroup of the unit group of an abelian extension K is mentioned by Washington in [5], which we denote by $C_W(K)$. It is simply defined by

$$C_W(K) = C(\mathbb{Q}(\zeta_n))^{Gal(\mathbb{Q}(\zeta_n)/K)},$$

where n is the conductor of K. But in this case it is not easy to compute the index $[E(K) : C_W(K)]$ since the generators of $C_W(K)$ are not explicit enough. It is clear that $C_W(K)$ contains $C_S(K)$. However, the index $[C_W(K) : C_S(K)]$ has not been successfully determined except for a few special cases ([1],[2]).

The aim of this paper to compare $C_W(K)$ with $C_S(K)$ when the conductor of K is a prime power(Theorem 2.5, Theorem 2.8). The method given in this paper seems to be useful in generalizing our results to abelian fields with arbitrary conductors. We will achieve our goal by finding a basis of $C_W(K)$(Theorem 2.4).

We finish this section with the index formula discovered by Sinnott ([4]).

THEOREM 1.1. *Let K be a subfield of $Q(\zeta_{p^e})$. then*

$$[E(K) : C_S(K)] = \begin{cases} 2^{[K:\mathbb{Q}]-1} h_K & \text{if } K \text{ is real} \\ h_{K^+} & \text{if } K \text{ is imaginary} \end{cases},$$

where K^+ is the maximal real subfield of K.

2. Main result

We begin this section with an obvious property of a free abelian group.

LEMMA 2.1. *Let M be a free abelian group with a basis $\{x_1, x_2, \cdots, x_n\}$. Then $\{x_1, x_2, \cdots, x_{i-1}, x_i^*, x_{i+1}, \cdots, x_n\}$ also serves as a basis of M, where $x_i^* = x_i + \sum_{j \neq i} m_j x_j$ for some integers m_j.*

Now we consider the cyclotomic field $\mathbb{Q}(\zeta_{p^e})$. Let $p^e = q$, $\varphi(q) = \varphi$ and $\zeta_q = \zeta$. Then $\mathbb{Q}(\zeta_q)^+$ is a cyclic extension of $\mathbb{Q}$ of degree $\frac{\varphi}{2}$. Let σ be a generator of $Gal(\mathbb{Q}(\zeta_q)^+/\mathbb{Q})$. An extension of σ to $\mathbb{Q}(\zeta_q)$ is also denoted by σ. For each integer i, put $v(i) = \frac{1-\zeta^{\sigma^i}}{1-\zeta}\zeta^{(1-\sigma^i)/2}$. Note that $v(0) = 1$, and that

$$\begin{aligned} \sigma^k(v(i)) &= \sigma^k\left(\frac{1-\zeta^{\sigma^i}}{1-\zeta}\zeta^{(1-\sigma^i)/2}\right) \\ &= \frac{1-\zeta^{\sigma^{i+k}}}{1-\zeta^{\sigma^k}}\zeta^{(\sigma^k-\sigma^{i+k})/2} \\ &= \left(\frac{1-\zeta^{\sigma^{i+k}}}{1-\zeta}\zeta^{(1-\sigma^{i+k})/2}\right) \times \left(\frac{1-\zeta}{1-\zeta^{\sigma^k}}\frac{1}{\zeta^{(1-\sigma^k)/2}}\right) \\ &= \frac{v(i+k)}{v(k)}. \end{aligned}$$

Since $1-\zeta_n^{-a} = -\zeta_n^{-a}(1-\zeta_n^a)$, we have

$$\begin{aligned}\overline{v(i)} &= \frac{1-\zeta^{-\sigma^i}}{1-\zeta^{-1}}\zeta^{-(1-\sigma^i)/2} \\ &= \frac{-\zeta^{-\sigma^i}(1-\zeta^{\sigma^i})}{-\zeta^{-1}(1-\zeta)}\zeta^{-(1-\sigma^i)/2} \\ &= \frac{1-\zeta^{\sigma^i}}{1-\zeta}\zeta^{(1-\sigma^i)/2} \\ &= v(i),\end{aligned}$$

where $\overline{v(i)}$ is the complex conjugation of $v(i)$. Hence $v(i)$ is an element of $C_W(\mathbb{Q}(\zeta_q)^+)$. The next theorem says that these elements generate $C_W(\mathbb{Q}(\zeta_q)^+)$.

THEOREM 2.2. *The set* $\left\{v(i)\middle|1 \le i \lneq \frac{\varphi}{2}\right\}$ *forms a basis of the free part of* $C_W(\mathbb{Q}(\zeta_q)^+)$. *That is*

$$C_W(\mathbb{Q}(\zeta_q)^+) = \left\langle \pm v(i)\middle|1 \le i \lneq \frac{\varphi}{2}\right\rangle.$$

Proof. See [5]. □

Now we find a basis of $C_S(K)$ and $C_W(K)$, where K is a subfield of $\mathbb{Q}(\zeta_q)^+$. Put $[K:\mathbb{Q}] = r$, and $[\mathbb{Q}(\zeta_q)^+ : K] = t$. So $tr = \frac{1}{2}\varphi$. For each i, $1 \le i \lneq r$, let $v_K(i) = \mathbf{N}_{\mathbb{Q}(\zeta_q)^+/K} v(i)$, where $\mathbf{N}_{\mathbb{Q}(\zeta_q)^+/K}$ is the norm from $\mathbb{Q}(\zeta_q)^+$ to K.

In this case, the generators of $C_S(K)$ given is section 1 can be written more explicitly. Namely,

$$C_S(K) = \left\langle \pm \mathrm{N}_{\mathbb{Q}(\zeta_q)/K}\left(\frac{1-\zeta_q^i}{1-\zeta_q}\right) | 1 \le i < \varphi \right\rangle.$$

Since $\mathrm{N}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}(\zeta_q)^+}\left(\frac{1-\zeta_q^a}{1-\zeta_q}\right) = \frac{1-\zeta_q^a}{1-\zeta_q}\cdot\frac{1-\zeta_q^{-a}}{1-\zeta_q^{-1}} = \left(\frac{1-\zeta_q^a}{1-\zeta_q}\right)^2 \zeta_q^{1-a}$, we have $\mathrm{N}_{\mathbb{Q}(\zeta_q)/K}\left(\frac{1-\zeta_q^{\sigma^i}}{1-\zeta_q}\right) = v_K(i)^2$. Hence we have the following theorem.

THEOREM 2.3. *The set* $\{v_K(i)^2 | 1 \le i < r\}$ *forms a basis of the free part of* $C_S(K)$. *That is*

$$C_S(K) = \left\langle \pm v_K(i)^2 | 1 \le i < r \right\rangle.$$

The next theorem describes a basis of $C_W(K)$.

THEOREM 2.4. *The set* $\left\{v_K(i)\middle|1 \le i \lneq r\right\}$ *forms a basis of the free part of* $C_W(K)$. *That is*

$$C_W(K) = \left\langle \pm v_K(i)\middle|1 \le i \lneq r \right\rangle.$$

Proof. Since $Gal(\mathbb{Q}(\zeta_q)^+/K)$ is generated by σ^r, we have

$$\begin{aligned} v_K(i) &= \prod_{0\le m\lneq t} \sigma^{mr}(v(i)) \\ &= \prod_{0\le m\lneq t} \frac{v(i+mr)}{v(mr)} \\ &= v(i) \prod_{1\le m\lneq t} \frac{v(i+mr)}{v(mr)}. \end{aligned}$$

Then, by Lemma 2.1 and Theorem 2.2, we have

$$C_W(\mathbb{Q}(\zeta_q)^+) = \left\langle \pm v_K(i)\middle|1 \le i \lneq r \right\rangle \oplus \left\langle v(i)\middle| r \le i \lneq \frac{\varphi}{2} \right\rangle.$$

Let $D = \left\langle \pm v_K(i)\middle|1 \le i \lneq r \right\rangle$. Being a norm from $\mathbb{Q}(\zeta_q)^+$ to K, $v_K(i)$ must be fixed by $Gal(\mathbb{Q}(\zeta_q)^+/K)$, and thus an element in $C_W(K)$. Hence $D < C_W(K) < C_W(\mathbb{Q}(\zeta_q)^+)$ and D is direct summand of $C_W(\mathbb{Q}(\zeta_q)^+)$. Also note that D is of finite index in $C_W(K)$ since $\mathrm{rank}_{\mathbb{Z}} D = r - 1 = \mathrm{rank}_{\mathbb{Z}} C_W(K)$. Therefore $D = C_W(K) = \left\langle \pm v_K(i)\middle|1 \le i \lneq r \right\rangle$. □

THEOREM 2.5. *Let* K *be a real subfield of* $\mathbb{Q}(\zeta_{p^e})$ *with* $[K : \mathbb{Q}] = r$. *Then*

(1) $[C_W(K) : C_S(K)] = 2^{r-1}$

(2) $[E(K) : C_W(K)] = h_K$.

Proof. From Theorem 2.3 and 2.4, we get (1). (2) follows from the index formula given in the Theorem 1.1. □

To study Washington units for imaginary subfields of $\mathbb{Q}(\zeta_q)$, we need the unit index. For an imaginary abelian field K (with an arbitrary conductor), we define $Q_E(K)$ by $Q_E(K) = [E(K) : W(K)E(K^+)]$ as usual. The index $Q_E(K)$ is called the unit index of K, and it is known that $Q_E(K) = 1$ or 2. Similarly, we define $Q_C(K)$ by $Q_C(K) = [C_W(K) : W(K)C_W(K^+)]$.

LEMMA 2.6. *Let* K *be an imaginary abelian field. Then* $Q_C \middle| Q_E$.

Proof. Note that the kernel of composition

$$C_W(K) \longrightarrow E(K) \longrightarrow E(K)/W(K)E(K^+)$$

is $W(K)C_W(K^+)$. Hence $Q_C \Big| Q_E$. □

COROLLARY 2.7. *If K is an imaginary subfield of $\mathbb{Q}(\zeta_q)$, then*

$$C_W(K) = W(K)C_W(K^+).$$

Proof. Since $Q_E(K)$ is 1 in this case, so is $Q_C(K)$. The result follows from this. □

THEOREM 2.8. *Let K be an imaginary subfield of $\mathbb{Q}(\zeta_q)$. Then*
(1) $[E(K) : C_W(K)] = h_{K^+}$
(2) $[C_W(K) : C_S(K)] = 1$.

Proof. Since $E(K) = W(K)E(K^+)$ and $C_W(K) = W(K)C_W(K^+)$, we have $[E(K) : C_W(K)] = [E(K^+) : C_W(K^+)] = h_{K^+}$ by Theorem 2.5. And (2) follows from the index formula in the Theorem 1.1. □

References

[1] C. Greither, *Über relativ-invariante Kreiseinheiten und Stickelberger-Elemente*, Manuscripta Math. **80**(1993), 27–43.
[2] R. Kučera, *On the Stickelberger ideal and circular units of some genus fields*, Tatra Mt. Math. Publ. **20**(2000), 93–104.
[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 Math. **74**, Springer-Verlag, New York/Berline, 1980.

Department of Mathematics
Inha University
Incheon 402-751, Korea
E-mail: jmkim@inha.ac.kr

Department of Mathematics
Inha University
Incheon 402-751, Korea
E-mail: jdryu@inha.ac.kr