ON WASHINGTON GROUP OF CIRCULAR UNITS OF SOME COMPOSITA OF QUADRATIC FIELDS

MICHAL BULANT

ABSTRACT. Circular units emerge in many occasions in algebraic number theory as they have tight connection (first discovered by E. Kummer) to the class group of the respective number field.

For example, E. Kummer has shown that in the case of cyclotomic field with prime conductor the index of the group of circular units in the full group of units is equal to the class number of the maximal real subfield of that field. His result was later generalized so we are now able to obtain information about class groups by the study of circular units.

In contrast to the case of cyclotomic field it is not clear how to define the group of circular units of a general abelian number field K. In the literature there eventually turned up several possible definitions of a group of circular units.

One of these definitions (which appeared in the Washington's book *Introduction to cyclotomic fields* – [7]) constructs the group of circular units to be as large as possible — it considers all circular units of the respective cyclotomic superfield which are lying already in the field K.

This definition has some nice properties but also serious difficulties: generally we do not know neither explicit generators of the group nor the index of the group in the full group of units.

In this paper we present results about this index for some classes of abelian fields — namely for composita of quadratic fields satisfying an additional condition — obtained by the study of the relation between Washington group of circular units and the well-known Sinnott's group of circular units. Methods of this paper use and slightly extend approach appeared in [4].

1. INTRODUCTION

For the understanding of the arithmetic of any algebraic number field K it is necessary to be able to work with its group of units $E(K)$. Unfortunately it is not feasible to find a basis of the non-torsion part of $E(K)$ (so called fundamental units) in the general case. We are therefore trying to approximate the group $E(K)$ by an appropriate subgroup with a known set of independent generators. In the case of abelian extension of rational numbers this role is usually played by so-called circular units which are defined in the next section.

Throughout the whole paper we shall assume the field K to be an abelian field, i.e. a finite Galois extension of $\mathbb{Q}$ with commutative Galois group. Often we will also work with cyclotomic fields; by the n^{th} cyclotomic field we understand the field $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$ is a primitive n^{th} root of unity.

2. CIRCULAR UNITS IN ABELIAN FIELDS

Let us first consider the case of a cyclotomic field $K = \mathbb{Q}^{(n)}$. Although we do not know explicit system of independent generators of $E(\mathbb{Q}^{(n)})$ we are able to construct a subgroup of $E(\mathbb{Q}^{(n)})$ of sufficiently low finite index – namely the group of circular units $C(\mathbb{Q}^{(n)})$ formed by the units of the form $1 - \zeta_n^a$:

$$C(\mathbb{Q}^{(n)}) = \langle 1 - \zeta_n^a;\, a \in \mathbb{Z},\, n \nmid a\rangle \cap E(\mathbb{Q}^{(n)}).$$

A natural question arises — how to generalize this definition to the case of a general abelian number field? Unfortunately there is no unique way of definition of circular units in this case

1991 *Mathematics Subject Classification.* 11R29(primary), 11R27, 11R20.
Key words and phrases. circular units, abelian field, class number.
The author was financially supported by the Grant Agency of the Czech Republic, grant 201/04/0381.

(for the review and comparison of several possible definitions see [4]). Probably the best known definition of circular units is the one due to Sinnott (see [6]):

$$C_S(K) = \langle \pm \mathrm{N}_{\mathbb{Q}^{(r)}/\mathbb{Q}^{(r)}\cap K}(1-\zeta_r^a); 1 < r \mid n, (a,r)=1\rangle \cap E(K).$$

Another possible definition appeared in the book [7]:

$$C_W(K) = K \cap C(\mathbb{Q}^{(n)}).$$

Trivially $C_S(K) \subseteq C_W(K)$.

Let us now discuss the construction of the basis for the group of circular units and the index in the full group of units. W. Sinnott has proved in [5] that

$$[E(\mathbb{Q}^{(n)}) : C(\mathbb{Q}^{(n)})] = 2^c \cdot h^+_{\mathbb{Q}^{(n)}},$$

where $h^+_{\mathbb{Q}^{(n)}}$ is the class number of the maximal real subfield of $\mathbb{Q}^{(n)}$ and c is given by an explicit function of the number of primes ramified in $\mathbb{Q}^{(n)}$. In [6], Sinnott has also stated the formula for the index $[E(K) : C_S(K)]$ in the case of a general abelian field – in this case the formula unfortunately contains a non-explicit factor which has been calculated only in some special cases so far, e.g. when K is a compositum of quadratic fields (see [3, Proposition 1] and Proposition 2). In the case of the alternative definition $C_W(K)$ we are not aware of any explicit formula for the index.

Construction of a basis of the group of circular units is generally even more complicated than the calculation of the index described above. The easiest case is that of cyclotomic field of a prime power conductor, $K = \mathbb{Q}^{(n)}$, where $n = p^l$, p being a prime, l any positive integer. In this case, a basis is the set

$$\left\{\frac{1-\zeta_n^a}{1-\zeta_n}; 1 < a < \frac{n}{2}, (a,n)=1\right\}.$$

In the case of a general cyclotomic field the situation is much more complicated — similar bases were found independently by R. Gold and J. Kim (see [1]) and by R. Kučera ([2]). As we shall need this basis for our purpose later we present here the construction described in [2, Theorem 6.1]. In our description we limit ourselves to the case where the conductor of K is a product of disctinct primes.

Proposition 1. *Let $n = p_1 \cdot p_2 \cdots p_l$ be the conductor of K ($p_1 < p_2 < \cdots < p_l$ being primes). Further let $X = \{a \in \mathbb{Z}; 0 < a < n\}$ and M be the set defined by*

$$\begin{aligned} M = X \setminus \Bigg(&\left\{a \in X; \exists i \in \{1,\dots,l\} : p_i \nmid a \,\wedge\, \frac{a}{(a,n)} \equiv -1 \pmod{p_i}\right\} \\ &\cup \Big\{a \in X;\, a \mid n \,\wedge\, 2 \nmid \#\{i \in \{1,\dots,l\}; p_i \nmid a\}\Big\} \\ &\cup \bigcup_{k=1}^{l} \left\{a \in X; p_k \nmid a \,\wedge\, \left\langle \frac{a}{(a,n)\cdot p_k}\right\rangle > \frac{1}{2} \,\wedge\, \forall i \in \{k+1,\dots,l\} : a \equiv (a,n) \pmod{p_i}\right\}\Bigg) \end{aligned}$$

Then the set

$$\left\{1-\zeta_n^a;\ a \in M \wedge \forall i \in \{1,\dots,l\} : \frac{n}{p_i} \nmid a\right\} \cup \left\{\frac{1-\zeta_{p_i}^{\frac{ap_i}{n}}}{1-\zeta_{p_i}};\ a \in M \wedge \frac{n}{p_i} \mid a\,,\ i = 1,\dots,l\right\}$$

forms a system of independent generators of the non-torsion part of the group $C(\mathbb{Q}^{(n)})$.

Proof. See [2, Theorem 6.1]. □

3. Compositum of real quadratic fields

Now let K be a compositum of real quadratic fields, such that $K = \mathbb{Q}(\sqrt{p}; p \in J)$, where J is a set of positive primes $p \equiv 1 \pmod 4$ satisfying for any distinct $p, q \in J$ the relation $(p/q) = 1$ (p is a quadratic residue modulo q – and vice-versa).

For any $\emptyset \neq T \subseteq J$ we now define $n_T = \prod_{p\in T} p$, $K_T = \mathbb{Q}(\sqrt{p}\,; p \in T)$, and $\mathbb{Q}^T = \mathbb{Q}(\zeta_T)$, where $\zeta_T = e^{2\pi i/n_T}$. Further, for any $p \in J$ let σ_p be a generator of $\mathrm{Gal}\left(\mathbb{Q}^J/\mathbb{Q}^{J\setminus\{p\}}\right)$.

In the case of a compositum of quadratic field we are able to calculate the required index:

Proposition 2. *Let $K = \mathbb{Q}(\sqrt{p}; p \in J)$, where J is as above. Then*

$$[E(K) : C_S(K)] = 2^{2^{\#J}-1} \cdot h_K,$$

where h_K is the class number of K.

Proof. See [3, Theorem 1], especially Remark following the proof of Theorem 1. Considering our restrictions put on the field K we obtain the formula $[E(K) : C] = 2^{2^{\#J}-\#J-1} \cdot h_K$ where the group C considered in [3] is slightly enlarged group $C_S(K)$. From the discussions on pages 148–149 we finally obtain $[C : C_S(K)] = 2^{\#J}$. □

From the previous section we know that the group $C_S(K)$ of circular units of K (in Sinnott's sense) is generated by -1 and all conjugates of $\eta_T, \emptyset \neq T \subseteq J$, where

$$\eta_T = \begin{cases} \mathrm{N}_{\mathbb{Q}^T/K_T}(1-\zeta_T)^{1-\sigma_p} = \prod_{i=0}^{p-2}(1-\zeta_p)^{(-\sigma_p)^i}, & \text{if} \quad T = \{p\} \\ \mathrm{N}_{\mathbb{Q}^T/K_T}(1-\zeta_T), & \text{if} \quad \#T > 1 \end{cases}$$

For our calculations we shall need the following well-known norm relation:

Lemma 3. *Let m and n be positive integers, $m \not\equiv 2 \pmod 4$, $n \not\equiv 2 \pmod 4$, and $m \mid n$. Then*

$$\mathrm{N}_{\mathbb{Q}^{(n)}/\mathbb{Q}^{(m)}}(1-\zeta_n) = (1-\zeta_m)^{\prod_p (1-\mathrm{Frob}(p)^{-1})},$$

where p is running through prime factors of n not dividing m and $\mathrm{Frob}(p)$ is the Frobenius automorphism of p on $\mathbb{Q}^{(m)}$.

Corollary 4. *For any nonempty set $T \subseteq J$ and any prime $p \in T$*

$$\eta_T^{1+\sigma_p} = 1.$$

Proof. If $\#T > 1$ Lemma 3 gives

$$\begin{aligned}\eta_T^{1+\sigma_p} &= \mathrm{N}_{K_T/K_{T\setminus\{p\}}}(\mathrm{N}_{\mathbb{Q}^T/K_T}(1-\zeta_T)) = \mathrm{N}_{\mathbb{Q}^T/K_{T\setminus\{p\}}}(1-\zeta_T) = \\ &= \mathrm{N}_{\mathbb{Q}^{T\setminus\{p\}}/K_{T\setminus\{p\}}}(\mathrm{N}_{\mathbb{Q}^T/\mathbb{Q}^{T\setminus\{p\}}}(1-\zeta_T)) = \mathrm{N}_{\mathbb{Q}^{T\setminus\{p\}}/K_{T\setminus\{p\}}}(1-\zeta_{T\setminus\{p\}})^{1-\mathrm{Frob}(p)^{-1}} = 1,\end{aligned}$$

since the restriction of $\mathrm{Frob}(p)$ to $K_{T\setminus\{p\}}$ is trivial as $(p/q) = 1$ for any $q \in T \setminus \{p\}$. The proof of the assertion in the situation when $\#T = 1$ is very similar. □

Proposition 5. *If $K = \mathbb{Q}(\sqrt{p}; p \in J)$, where J is a set of positive primes $p \equiv 1 \pmod 4$ such that for any distinct $p, q \in J$ we have $(p/q) = 1$, then*

$$C_S(K) = \langle -1, \eta_T; \emptyset \neq T \subseteq J\rangle.$$

Proof. We have to show that by omitting conjugates of η_T we do not lose anything. But for any $p \in T$ we have $\eta_T^{\sigma_p} = \eta_T^{-1}$ by the previous corollary. □

Lemma 6. *For any nonempty set $T \subseteq J$ the unit η_T is a square in the appropriate field K_T.*

Proof. For $T = \{p\}$ we have

$$\eta_{\{p\}} = \prod_{i=0}^{p-2}(1-\zeta_p)^{(-\sigma_p)^i} = \prod_{i=0}^{(p-3)/2}\left(-\zeta_p^{-1}(1-\zeta_p)^2\right)^{(-\sigma_p)^i} = \varepsilon_{\{p\}}^2,$$

where $\varepsilon_{\{p\}} = \displaystyle\prod_{i=0}^{(p-3)/2}(\zeta_p^{(p-1)/2}(1-\zeta_p))^{(-\sigma_p)^i}$ is clearly an element of $\mathbb{Q}^{\{p\}}$.

For $T=\{p_1,p_2,\dots,p_t\}\subseteq J$ (where $t\geq 2,\ p_1=\min T$) we have (index i in all subscripts running over the set $\{1,\dots,t\}$).

$$\eta_T=\prod_{\substack{1\leq a\leq n_T\\ \forall\, i:(a/p_i)=1}}\left(1-\zeta_T^a\right)=\prod_{\substack{1\leq a\leq n_T\\ \forall\, i:(a/p_i)=1\\ \left\langle\frac{a}{p_1}\right\rangle<\frac12}}\left(1-\zeta_T^a\right)\left(1-\zeta_T^{-a}\right)=\prod_{\substack{1\leq a\leq n_T\\ \forall\, i:(a/p_i)=1\\ \left\langle\frac{a}{p_1}\right\rangle<\frac12}}\left(-\zeta_T^{-a}\cdot\left(1-\zeta_T^a\right)^2\right)=\varepsilon_T^2$$

where again

$$\varepsilon_T=\prod_{\substack{1\leq a\leq n_T\\ \forall\, i:(a/p_i)=1\\ \left\langle\frac{a}{p_1}\right\rangle<\frac12}}\zeta_T^{\frac{n_T-1}{2}a}\left(1-\zeta_T^a\right)$$

is an element of $\mathbb{Q}^T$ (by $\langle x\rangle=x-[x]$ we denote the fractional part of a real number x).

It remains to show that for every nonempty $T\subseteq J$ the unit ε_T is an element of K_T. As $\mathrm{Gal}\left(\mathbb{Q}^T/K_T\right)=\langle\sigma_p^2;\,p\in T\rangle$ it is sufficient to prove that $\varepsilon_T^{\sigma_p^2}=\varepsilon_T$ for any $p\in T$. But from the above corollary we obtain $(\varepsilon_T^2)^{1+\sigma_p}=\eta_T^{1+\sigma_p}=1$, hence $\varepsilon_T^{\sigma_p}=\pm\varepsilon_T^{-1}$, and $\varepsilon_T^{\sigma_p^2}=\varepsilon_T$. $\square$

As the unit ε_T is clearly also circular in $\mathbb{Q}^T$, we obtain that $\varepsilon_T\in C_W(K_T)\subseteq C_W(K)$ for any nonempty $T\subseteq J$. Let us now form a subgroup D of $C_W(K)$ generated by these ε_T's:

$$D=\langle -1,\varepsilon_T;\emptyset\neq T\subseteq J\rangle.$$

Our present goal is to show that D is in fact equal to $C_W(K)$ (i.e. we are going to prove the inclusion $C_W(K)\subseteq D$). As the conductor of K is n_J we have to consider a basis of the group $C(\mathbb{Q}^{(n_J)})$. Due to the special form of the conductor n_J (it is a product of distinct primes) we can describe this basis in a more compact form. In fact we shall describe only a subset of the basis in the following as it is fully sufficient for our purposes.

Let as usually T be any nonempty subset of J. We have to distinguish two cases. If $\#T>1$ let us define

$$B_T=\left\{1-\zeta_T^a\,;\,1\leq a\leq n_T,\,(a,n_T)=1,\left\langle\frac{a}{\min T}\right\rangle<\frac12,\,\forall p\in T:\ a\not\equiv\pm1\pmod p\right\}$$

and if $T=\{p\}$, let

$$B_{\{p\}}=\left\{\frac{1-\zeta_p^j}{1-\zeta_p}\,;\,2\leq j\leq\frac{p-1}{2}\right\}$$

From the description of the basis of $C(\mathbb{Q}^{(n)})$ in Proposition 1 it is easy to see that the union

$$\bigcup_{\emptyset\neq T\subseteq J}B_T$$

is a subset of the basis of $C(\mathbb{Q}^{(n_J)})$ and that the sets B_T are clearly pairwise disjoint. We are going to show (separately for the two mentioned cases) that for any nonempty T the element ε_T is an element of $\mathbb{Q}^T$ generated by B_T (modulo torsion).

Keeping the notation $T=\{p_1,p_2,\dots,p_t\}\subseteq J$, $t\geq 2$, $p_1=\min T$, we have

$$\eta_T^{\sigma_{p_1}\cdots\sigma_{p_t}}=\prod_{\substack{1\leq a\leq n_T\\ \forall\, i:(a/p_i)=-1}}\left(1-\zeta_T^a\right)=\prod_{\substack{1\leq a\leq n_T\\ \forall\, i:(a/p_i)=-1\\ \left\langle\frac{a}{p_1}\right\rangle<\frac12}}\left(-\zeta_T^{-a}\left(1-\zeta_T^a\right)^2\right)$$

Using Corollary 4 we obtain $\eta_T^{\sigma_{p_1}\cdots\sigma_{p_t}} = \eta_T^{(-1)^t}$. Combining these two formulas we obtain another expression for ε_T, namely

$$\varepsilon_T = \pm \prod_{\substack{1\le a\le n_T \\ \forall\, i:(a/p_i)=-1 \\ \left\langle \frac{a}{p_1}\right\rangle < \frac{1}{2}}} \left(\zeta_T^{\frac{n_T-1}{2}a}\left(1-\zeta_T^a\right)\right)^{(-1)^t}.$$

From this expression it can be easily seen (as -1 is a quadratic residue modulo every $p \in T$) that ε_T is generated by B_T modulo roots of unity.

Now, let $T = \{p\}$. We have

$$\varepsilon_{\{p\}} = \prod_{i=0}^{(p-3)/2} (\zeta_p^{(p-1)/2}(1-\zeta_p))^{(-\sigma_p)^i} = \xi \cdot \prod_{i=0}^{(p-3)/2} (1-\zeta_p)^{(\sigma_p^i-1)\cdot(-1)^i}$$

for a suitable root of unity ξ. For a given i $(0 \le i \le (p-3)/2)$ let $1 \le j < p$ satisfies $(1-\zeta_p)^{\sigma_p^i} = 1-\zeta_p^j$. For $2 \le j \le (p-1)/2$ the unit $(1-\zeta_p)^{\sigma_p^i-1}$ clearly belongs to $B_{\{p\}}$. If $j=1$, then $(1-\zeta_p)^{\sigma_p^i-1} = 1$, and if $j = p-1$, then $(1-\zeta_p)^{\sigma_p^i-1} = \frac{1-\zeta_p^{-1}}{1-\zeta_p} = -\zeta_p^{-1}$, i.e. a root of unity. Finally, for $(p+1)/2 \le j \le p-2$ we obtain

$$(1-\zeta_p)^{\sigma_p^i-1} = \frac{1-\zeta_p^j}{1-\zeta_p} = -\zeta_p^j \cdot \frac{1-\zeta_p^{p-j}}{1-\zeta_p}.$$

Since $2 \le p-j \le (p-1)/2$, the last fraction belongs to $B_{\{p\}}$ and we have proved that $\varepsilon_{\{p\}}$ is again generated by the elements of $B_{\{p\}}$ modulo roots of unity.

Lemma 7. *$[C_W(K) : D]$ is finite.*

Proof. From Proposition 5 and the definition of D we know that $\operatorname{rank} C_S(K) = \operatorname{rank} D$. Moreover, as $C_S(K) \subseteq C_W(K) \subseteq E(K)$, and $\operatorname{rank} C_S(K) = \operatorname{rank} E(K)$ by Proposition 2 we obtain $\operatorname{rank} D = \operatorname{rank} C_W(K)$.

□

Proposition 8. *Let $K = \mathbb{Q}(\sqrt{p}; p \in J)$, where J is a set of positive primes $p \equiv 1 \pmod 4$ such that for any distinct $p, q \in J$ we have $(p/q) = 1$. Then*

$$C_W(K) = \langle -1, \varepsilon_T; \emptyset \ne T \subseteq J\rangle.$$

Proof. Denote as above the set $\langle -1, \varepsilon_T; \emptyset \ne T \subseteq J\rangle$ by D. From the previous lemma we know that there is a positive integer f such that for any $w \in C_W(K)$ we have $w^f \in D$, i.e.

$$w^f = \pm \prod_{\emptyset \ne T \subseteq J} \varepsilon_T^{f_T}$$

for suitable $f_T \in \mathbb{Z}$. From the expression of w and ε_T in basis of $C(\mathbb{Q}^{(n_J)})$ we obtain (as the sets B_T are pairwise disjoint and each ε_T is a multiplicative combination of some elements of B_T with exponents ± 1) that $f \mid f_T$ for any T, hence $w \in D$. □

Theorem. *Let $K = \mathbb{Q}(\sqrt{p}; p \in J)$, where J is a set of positive primes $p \equiv 1 \pmod 4$ such that for any distinct $p, q \in J$ we have $(p/q) = 1$.*

Then the Washington group of circular units of K is of finite index in the full group of units and

$$[E(K) : C_W(K)] = h_K,$$

where h_K is the class number of K.

Proof. From Proposition 2 we know that the Sinnott group $C_S(K)$ is of finite index in $E(K)$ and that in our case

$$[E(K) : C_S(K)] = 2^{2^{\#J}-1} \cdot h_K.$$

As $C_W(K) = \langle -1, \varepsilon_T; \emptyset \neq T \subseteq J \rangle$, $C_S(K) = \langle -1, \varepsilon_T^2; \emptyset \neq T \subseteq J \rangle$, and $\operatorname{rank} C_W(K) = \operatorname{rank} C_S(K) = 2^{\#J} - 1$, we have

$$[C_W(K) : C_S(K)] = 2^{2^{\#J}-1},$$

and therefore $[E(K) : C_W(K)] = h_K$. □

References

[1] R. Gold and J. Kim. Bases for cyclotomic units. *Compositio Math.*, 71:13–27, 1989.

[2] R. Kučera. On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field. *J. Number Theory*, 40(3):284–316, March 1992.

[3] R. Kučera. On the Stickelberger ideal and circular units of a compositum of quadratic fields. *J. Number Theory*, 56(1):139–166, January 1996.

[4] R. Kučera. Circular units and class groups of abelian fields. In *Comptes Rendus de la conférence internationale Maroc-Québec (Mai 2003) "Théorie des nombres et applications"*, pages 130–143, 2004.

[5] W. Sinnott. On the Stickelberger ideal and the circular units of a cyclotomic field. *Ann. of Math.*, 108:107–134, 1978.

[6] W. Sinnott. On the Stickelberger ideal and the circular units of an abelian field. *Invent. Math.*, 62:181–234, 1980.

[7] L. C. Washington. *Introduction to Cyclotomic Fields.* Number 83 in GTM. Springer, 2nd edition, 1997.

Department of Mathematics, Faculty of Science,
Masaryk University, Janáčkovo nám. 2a, 602 00 Brno,
Czech Republic

E-mail address: bulant@math.muni.cz