On a modification of the group of circular units of a real abelian field

Michal Bulant\textsuperscript{a,1}, Radan Kučera\textsuperscript{a,1}

\textsuperscript{a}Faculty of Science, Masaryk University, Kotlářská 2, Brno, 611 37, Czech Republic

Abstract

For a real abelian field $K$, Sinnott’s group of circular units $C_K$ is a subgroup of finite index in the full group of units $E_K$ playing an important role in Iwasawa theory. Let $K_\infty/K$ be the cyclotomic $\mathbb{Z}_p$-extension of $K$, and $h_{K_n}$ be the class number of $K_n$, the $n$-th layer in $K_\infty/K$. Then for $p \neq 2$ and $n$ going to infinity, the $p$-parts of the quotients $[E_{K_n} : C_{K_n}]/h_{K_n}$ stabilize. Unfortunately this is not the case for $p = 2$, when the group $C_{1,K}$ of all units of $K$, whose squares belong to $C_K$, is usually used instead of $C_K$. But $C_{1,K}$ is better only for index formula purposes, not having the other nice properties of $C_K$. The main aim of this paper is to offer another alternative to $C_K$ which can be used in cyclotomic $\mathbb{Z}_p$-extensions even for $p = 2$ still keeping almost all nice properties of $C_K$.

Keywords: Real abelian field; $\mathbb{Z}_p$-extension; group of circular units.

2000 MSC: 11R20

Introduction

Let $K$ be a real abelian field of conductor $m > 1$. For any integer $f$ let $\zeta_f$ be a primitive $f$-th root of unity. W. Sinnott in [7] defined a group $D'_K$ of circular numbers of $K$ which is generated by $-1$ and all conjugates of numbers

$$N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f)\cap K}(1 - \zeta_f)$$

for all $f > 1$. Then Sinnott’s group of circular units is, by definition, the intersection $C_K = D'_K \cap E_K$, where $E_K$ is the full group of units in $K$. It appeared later (see [6]) that restraining to $f | m$ is better since this new group $D_K$, still having the same intersection $C_K$ with $E_K$, is finitely generated.

Sinnott’s group $C_K$ improves many previous versions of groups of cyclotomic units due to Kummer, Hasse, Leopoldt, Gillard and others (an overview of these
groups can be found for example in [5], while [4] compares them for \( K \) being a compositum of quadratic fields). Sinnott’s group \( C_K \) is used in plenty of interesting modern applications. It comes with the following advantages:

- It has an explicit finite set of generators constructed out of the numbers (1).
- Its Galois module structure is described by the distribution relations satisfied by these generators, and is easier to control than e.g. the one of the full group of units \( E_K \).
- The index \( [E_K : C_K] \) is explicitly related to the class number \( h_K \) of \( K \). More precisely one can define the constant \( c_K \) by the formula \( [E_K : C_K] = c_K h_K \). Then Sinnott gives an explicit formula for \( c_K \) and proves that \( [K : \mathbb{Q}] \cdot c_K \) is an integer. In fact, most of the technical work in [7] consists in controlling this \( c_K \).
- For \( p \neq 2 \) this \( C_K \) is the Galois module to consider in Iwasawa Theory because in the cyclotomic \( \mathbb{Z}_p \)-extension \( K_{\infty} = \bigcup K_n \) of \( K \) the \( p \)-parts of constants \( c_{K_n} \) stabilize when \( n \) tends to infinity.
- Finally it is proven in [6] that Sinnott’s version agrees with Thaine’s one, the later being constructed to apply the Euler System machinery to cyclotomic fields.

In view of all these properties, it is now admitted by experts that \( C_K \) is optimal apart for the 2-part of the constant \( c_K \). But, because of this 2-part, the group \( C_K \) is of no use in Iwasawa theory with \( p = 2 \). Indeed, in Sinnott’s formula for \( c_K \) the factor \( \frac{1}{[K : \mathbb{Q}] - 1} \) appears. This factor is not bounded in the cyclotomic \( \mathbb{Z}_2 \)-extension of \( K_n \) and corresponds to a non trivial \( \mu \)-invariant in the limit of the quotients \( E_{K_n} / C_{K_n} \) (recall that \( p = 2 \)). To remedy this, Sinnott in [7] already proposed to use \( C_{1,K} \) which is, by definition, the group of all units in \( E_K \) whose squares lie in \( C_K \). The group \( C_{1,K} \) is really being used in papers devoted to Iwasawa theory (see [1]). However this ad hoc \( C_{1,K} \) has none of the above nice properties of the initial \( C_K \) and is only better for index formula purposes.

This paper is devoted to the construction of an alternative to \( C_K \). Let \( G = \text{Gal}(K/\mathbb{Q}) \), and let \( I_K \) be the ideal of \( \mathbb{Z}[G] \) generated by 2 and the augmentation ideal. Then it is classical that \( D_{K}^{1/2} \) is contained in the group of squares in \( K^\times \). We define a \( G \)-module \( B_K \subset K^\times \) by \( B_K^2 = D_K^{1/2} \) and \(-1 \in B_K \) hoping that the intersection \( B_K \cap E_K \) can be accepted as a good substitute to \( C_K \), even for the prime \( p = 2 \). Indeed, Corollary 5 provides an explicit system of generators of \( B_K \cap E_K \) and Theorem 14 shows that

\[
[E_{K_n} : (B_{K_n} \cap E_{K_n})] \cdot h_{K_n}^{-1}
\]

stabilizes when \( K_n \) runs through the finite steps in the cyclotomic \( \mathbb{Z}_p \)-tower of \( K \) for each prime \( p \) including \( p = 2 \). So we think that \( B_K \) is the proper group
of circular numbers to consider now, as one has $B_K^2 \subseteq D_K \subseteq B_K$ and as $B_K$ is optimal even for the 2-part of the index $[E_K : (B_K \cap E_K)]$. In Section 4 we show that this index is slightly more difficult to handle than the classical $[E_K : C_K]$. There is another index $[D_K : B_K^2]$ that appears here (see Corollary 9). This factor may change according to the arithmetic of the prime factors of $m$ even in the simpler case of a field $K = \mathbb{Q}(\zeta_m)^+$, the maximal real subfield of the $m$-th cyclotomic field. However, for any real abelian field, this index satisfy the inequalities

$$2^{1+g} \leq [D_K : B_K^2] \leq 2^{2g},$$

where $g$ is the number of primes ramified in $K/\mathbb{Q}$ (see Corollary 8). Hence, in the general case of an abelian field $K$, this index is as explicit and as under control as the Sinnott index $[E_K : C_K]$. Therefore we are convinced that this extra complication does not change the effectiveness of the new module $B_K \cap E_K$.

1. The group $B_K$ of a real abelian field $K$

Let $K$ be an abelian field of conductor $m > 1$ and let $G = \text{Gal}(K/\mathbb{Q})$. For any positive integer $f$ let $\zeta_f$ be a primitive $f$-th root of unity; we assume that these roots are chosen in such a way that $\zeta_n^f = \zeta_f$ for any positive integer $n$.

**Definition 1.** Let $E_K$ be the group of units of $K$. We define the group $D_K$ of circular numbers of $K$ as the $G$-module generated by $-1$ and by all circular numbers $\eta_f = N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f) \cap K}(1 - \zeta_f)$ for all $1 < f | m$. We denote $C_K = D_K \cap E_K$.

**Proposition 1.** $C_K$ is the Sinnott’s group of circular numbers of $K$.

**Proof.** See [6], Proposition 1.

**Lemma 2.** $D_K$ is the $G$-module generated by $-1$ and by all circular numbers $\eta_f$ for all $1 < f | m$, $(f, \frac{m}{f}) = 1$.

**Proof.** For any $f' > 1$ dividing $f$ such that $f'$ is divisible by each prime dividing $f$ we have

$$N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f) \cap K}(1 - \zeta_f) = 1 - \zeta_{f'},$$

and so

$$\eta_f = N_{\mathbb{Q}(\zeta_{f'})/\mathbb{Q}(\zeta_{f'}) \cap K}(1 - \zeta_{f'}) = N_{\mathbb{Q}(\zeta_f) \cap K/\mathbb{Q}(\zeta_{f'}) \cap K}(\eta_f)$$

and the lemma follows.

**Definition 2.** Let $I_K$ be the ideal of the group ring $\mathbb{Z}[G]$ generated by 2 and by the augmentation ideal. Explicitly

$$I_K = \left\{ \sum_{\sigma \in G} a_\sigma \sigma \bigg| a_\sigma \in \mathbb{Z}, 2 \bigg| \sum_{\sigma \in G} a_\sigma \right\}. $$
For any integer $t$ relatively prime to $m$ let $\sigma_t$ be the automorphism of $\mathbb{Q}(\zeta_m)$ determined by $\zeta_m^{\sigma_t} = \zeta_m^{t}$. Since each automorphism of $\mathbb{Q}(\zeta_m)$ can be written as $\sigma_t$ with an odd $t$, the following easy lemma implies a classical result for a real abelian field $K$ saying that $D_K^f := \{\beta^n \mid \beta \in D_K, \alpha \in I_K\}$ consists of squares in $K$.

**Lemma 3.** If $K$ is real then for any $1 < f \mid m$ and any odd integer $t$ relatively prime to $m$ we have

$$
\frac{1-\zeta_f^t}{1-\zeta_f} \zeta_f^{(1-t)/2} \in \mathbb{Q}(\zeta_f)^+
$$

and so

$$
\eta_f^{\sigma_t^{-1}} = \varepsilon_{f,t}, \quad \text{where} \quad \varepsilon_{f,t} = N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f)^+} \left( \frac{1-\zeta_f^t}{1-\zeta_f} \zeta_f^{(1-t)/2} \right). \tag{2}
$$

**Proof.** This is obvious.

**Definition 3.** If $K$ is real, we define $B_K$ to be the subgroup of the multiplicative group $K^\times$ satisfying $-1 \in B_K$ and $B_K^2 = D_K^f$.

We shall use the notation introduced in (2) more generally: for any $1 < f \mid m$ and any odd integer $t$ relatively prime to $f$ let

$$
\varepsilon_{f,t} = N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f)^+} \left( \frac{1-\zeta_f^t}{1-\zeta_f} \zeta_f^{(1-t)/2} \right).
$$

**Lemma 4.** If $K$ is real then $B_K$ is the submodule of the $G$-module $K^\times$, which is (as a subgroup of $K^\times$) generated by $-1$, by $\eta_f$, and by $\varepsilon_{f,t}$ for all $1 < f \mid m$, $(f, \frac{m}{2}) = 1$, $1 < t < f$, $(t, 2f) = 1$.

**Proof.** Lemmas 2 and 3 show that $B_K$ is the $G$-submodule of $K^\times$ generated by $-1$, by $\eta_f$, and by $\varepsilon_{f,t}$ for all $1 < f \mid m$, $(f, \frac{m}{2}) = 1$, and all odd integers $t$ relatively prime to $m$. For any odd integer $s$ relatively prime to $f$ we have

$$(\varepsilon_{f,t}^{\sigma_s^{-1}})^2 = \eta_f^{\sigma_s^{-1}(\sigma_t^{-1})} = \eta_f^{\sigma_s^{-1} - (\sigma_t^{-1}) - (\sigma_t - 1)} = (\varepsilon_{f,st} \cdot \varepsilon_{f,s}^{-1} \cdot \varepsilon_{f,t}^{-1})^2$$

and so

$$
\varepsilon_{f,t}^{\sigma_s^{-1}} = \pm \varepsilon_{f,st} \cdot \varepsilon_{f,s}^{-1} \cdot \varepsilon_{f,t}^{-1},
$$

which together with (2) gives that $B_K$ is the subgroup of $K^\times$ generated by $-1$, by $\eta_f$, and by $\varepsilon_{f,t}$ for all $1 < f \mid m$, $(f, \frac{m}{2}) = 1$, and all odd integers $t$ relatively prime to $m$. The lemma follows since $\varepsilon_{f,t} = \varepsilon_{f,s}^1$ for any odd integers $t, s$ relatively prime to $f$ such that $t \equiv s \pmod{f}$.

**Corollary 5.** $B_K \cap E_K$ is (as a subgroup of $E_K$) generated by $-1$, by $\eta_f$ for all $f \mid m$, $(f, \frac{m}{2}) = 1$, such that $f$ is divisible by at least two primes, and by $\varepsilon_{f,t}$ for all $1 < f \mid m$, $(f, \frac{m}{2}) = 1$, $1 < t < f$, $(t, 2f) = 1$. 


Proposition 7. Let \( K \not= \mathbb{Q} \) be a real abelian field. Then we have \( D_K \subseteq B_K \), \( C_K \subseteq B_K \cap E_K \), and the inclusion gives the isomorphism of the quotients

\[
(B_K \cap E_K)/C_K \cong B_K/D_K,
\]

which are 2-elementary groups.

Proof. Since \( 2 \in I_K \) we have \( D_K \subseteq B_K \). Moreover \( B_K^2 = D_K^1 \subseteq D_K \) hence \( B_K/D_K \) is 2-elementary. Since the numbers \( \eta_f \) belong to \( D_K \), Lemma 4 and Corollary 5 give \( D_K : (B_K \cap E_K) = B_K \). As \( D_K \cap B_K \cap E_K = D_K \cap E_K = C_K \), the proposition follows.

Proposition 6. Let \( K \) be a real abelian field of conductor \( m > 1 \). Then \( D_K/B_K^2 \) is a 2-elementary group generated by (the classes containing) \(-1\) and \( \eta_f \) for all \( 1 < f \mid m \), \( (f, q) = 1 \). Moreover, the Galois action on \( D_K/B_K^2 \) is trivial and we have the following exact sequence

\[
1 \to C_K/(B_K^2 \cap E_K) \to D_K/B_K^2 \to (\mathbb{Z}/2\mathbb{Z})^g \to 1,
\]

(3)

where \( g \) is the number of primes dividing \( m \).

Proof. The inclusion \( D_K \subseteq B_K \) implies that \( D_K/B_K^2 \) is 2-elementary, and by the definition of \( B_K \) we obtain that the Galois action is trivial. The statement concerning the generators of \( D_K/B_K^2 \) is given by Lemma 2.

Since \( B_K^2 \cap C_K = B_K^2 \cap D_K \cap E_K = B_K^2 \cap E_K \), the left-hand-side mapping in the sequence (3) is injective. A reasoning similar to the one used in the proof of Corollary 5 gives that the sequence, where the right-hand-side mapping is given by the \( p \)-adic valuations at all primes \( p \mid m \), is exact.

Corollary 8. The 2-rank of \( D_K/B_K^2 \) satisfies

\[
1 + g \leq \dim_{\mathbb{F}_2} D_K/B_K^2 \leq 2^g.
\]

Proof. The upper bound follows from the number of generators in Proposition 7, the lower bound from the exact sequence (3) and the fact that \(-1 \in C_K \) but \(-1 \notin B_K^2 \).

Corollary 9. The index of the group of circular units \( C_K \) in \( B_K \cap E_K \) satisfies

\[
[(B_K \cap E_K) : C_K] = 2^{[K:Q]+g} : [D_K : B_K^2]^{-1}.
\]

Proof. We have \( C_K = D_K \cap E_K \subseteq B_K \cap E_K \subseteq E_K \), and \( \text{rank}_\mathbb{Z} C_K = \text{rank}_\mathbb{Z} E_K = [K : \mathbb{Q}] - 1 \), hence \(-1 \in B_K \) and \(-1 \notin B_K^2 \) yields

\[
\dim_{\mathbb{F}_2} (B_K \cap E_K)/(B_K^2 \cap E_K) = 1 + \text{rank}_\mathbb{Z} E_K = [K : \mathbb{Q}].
\]
Therefore
\[ [(B_K \cap E_K) : C_K] \cdot [C_K : (B_K^2 \cap E_K)] = [(B_K \cap E_K) : (B_K^2 \cap E_K)] = 2^{[K:Q]} \]

The exact sequence (3) gives the result.

The following proposition recalls the well-known behaviour of groups $D_K$ in field extensions and shows that our groups $B_K$ behave equally well.

**Proposition 10.** Let $K \subseteq L$ be abelian fields of conductors $m$, $m'$, respectively, and let $R$ be the subgroup of $\mathbb{Q}^\times$ generated by all primes $p \mid m'$, $p \nmid m$. Then
\[ D_K \subseteq D_L, \quad N_{L/K}(D_L) \subseteq D_K \cdot R. \]
Moreover, if $K$ and $L$ are real then
\[ B_K \subseteq B_L, \quad N_{L/K}(B_L) \subseteq B_K \cdot R. \]

**Proof.** Let $1 < f \mid m'$, $f \not\equiv 2 \pmod{4}$. Denoting $M = (\mathbb{Q}(\zeta_f) \cap L)K$ we have the following diagram of fields:

\[
\begin{array}{cccc}
L & \quad & M \\
\downarrow & & \downarrow \\
\mathbb{Q}(\zeta_f) & \quad & \mathbb{Q}(\zeta_f) \cap L \\
\downarrow & & \downarrow \\
\mathbb{Q}(\zeta_f) \cap K & \quad & \\
& & \\
\end{array}
\]

and so
\[ N_{L/K}(N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f) \cap L}(1 - \zeta_f)) = N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f) \cap K}(1 - \zeta_f)^{[L:M]}, \]
If $(m, f) = 1$ then $\mathbb{Q}(\zeta_f) \cap K = \mathbb{Q}$ and this norm belongs to $R$. Let us suppose $(m, f) > 1$. Since $\mathbb{Q}(\zeta_f) \cap K = \mathbb{Q}(\zeta_f) \cap \mathbb{Q}(\zeta_m) \cap K = \mathbb{Q}(\zeta_{(m,f)}) \cap K$, the norm above is equal to
\[ N_{\mathbb{Q}(\zeta_{(m,f)})/\mathbb{Q}(\zeta_{(m,f)}) \cap K}(1 - \zeta_{(m,f)})^{[L:M]} \prod_p (1 - \text{Frob}_p^{-1}) \in D_K \]
where the product is taken over all primes $p \mid f$, $p \nmid m$, and $\text{Frob}_p$ means the Frobenius automorphism of $p$. Hence
\[ N_{L/K}(D_L) \subseteq D_K \cdot R \quad \text{and} \quad N_{L/K}(D_L^{12}) = N_{L/K}(D_L)^{1K} \subseteq D_K^{1K} \cdot R^2 \quad (4) \]
as $R^{1K} = R^2$. If $f \mid m$ then
\[ N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f) \cap K}(1 - \zeta_f) = N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f) \cap K}(N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f) \cap L}(1 - \zeta_f)) \in D_L \]
so $D_K \subseteq D_L$ and $D_L^{1K} \subseteq D_L^{1L}$. If $K$ and $L$ are real then taking square roots in the last relation together with (4) gives the result concerning $B_K$, $B_L$. 
2. Another characterization of the group $B_K$

It is well-known that the Stark units of a real abelian field are given by circular numbers (see the fundamental book [8] of J. Tate, pages 79–80). To be more precise, let us fix a real abelian field $K$ of conductor $m > 1$. The $S,T$-Stark unit $\eta_{K/Q,S,T,1,(\infty_K)}$ of $K/Q$, which appears in the rank 1 case of the Rubin-Stark conjecture for a real abelian field $K$, can be described as follows. If the set $S$ is minimal, i.e. if it consists only of the archimedean place $\infty_Q$ and of all primes ramified in $K/Q$, and $T = \{t\}$ for an odd unramified prime $t$ then it is given by

$$\eta_{K/Q,S,T,1,(\infty_K)} = N_{Q(\zeta_m)/K}((1 - \zeta_m)^{1-t\text{Frob}_t^{-1}}),$$

see [2], pages 102 and 113. Of course, it belongs to the group $D_{Q(\zeta_m)}$ of circular numbers of $K$. The answer “not always” is given by the following proposition which describes the group $B_K$ defined in the previous section in terms of these Stark units of subfields of $K$, since Proposition 6 and Corollaries 9 and 8 give

$$[B_K : D_K] \geq 2^{[K : \mathbb{Q}]+g-2g}.$$

Recall that $G$ denotes the Galois group of $K/\mathbb{Q}$.

**Proposition 11.** $B_K$ is equal to the $G$-module generated by $-1$ and by

$$N_{Q(\zeta_f)/Q(\zeta_f)\cap K}((1 - \zeta_f)^{1-t\text{Frob}_t^{-1}}) = N_{Q(\zeta_f)/Q(\zeta_f)\cap K}\left(\frac{1-\zeta_f}{(1-\zeta_f)^s}\right)^{\text{Frob}_t^{-1}}$$

for all $1 < f | m$, $(f, \frac{m}{f}) = 1$, and all odd primes $t \nmid f$.

**Proof.** Let $B'_K$ be the $G$-module generated by the mentioned generators. To show that $B'_K = B_K$ let us fix $f > 1$, $f | m$, $(f, \frac{m}{f}) = 1$. For any odd integer $t$ relatively prime to $f$ let $\sigma_t$ denotes the automorphism of $Q(\zeta_f)$ sending each root of unity to its $t$-th power. For any positive integers $s,t$ which are relatively prime to $2f$ we have

$$\frac{1-\zeta_f^s}{(1-\zeta_f)^s} = \left(\frac{1-\zeta_f}{(1-\zeta_f)^s}\right)^s \left(\frac{1-\zeta_f}{(1-\zeta_f)^t}\right)^t$$

and so decomposing any positive integer $t$ relatively prime to $2f$ into a product of primes we obtain

$$N_{Q(\zeta_f)/Q(\zeta_f)\cap K}\left(\frac{1-\zeta_f}{(1-\zeta_f)^s}\right) \in B'_K.$$

Since

$$\frac{1-\zeta_f^{2s-1}}{(1-\zeta_f)^{2s-1}} \cdot \left(\frac{1-\zeta_f^{2s+1}}{(1-\zeta_f)^{2s+1}}\right)^{-1} = (1 - \zeta_f)(1 - \zeta_f^{-1})$$

we have

$$\eta_f = N_{Q(\zeta_f)/Q(\zeta_f)\cap K}(1 - \zeta_f) = N_{Q(\zeta_f)/Q(\zeta_f)\cap K}\left((1 - \zeta_f)(1 - \zeta_f^{-1})\right) \in B'_K.$$
Moreover
\[
\frac{1-\zeta_f^t}{1-\zeta_f} \frac{\zeta_f^{(1-t)/2}}{(1-\zeta_f)} \cdot \left(-\left(1 - \zeta_f\right)(1 - \zeta_f^{-1})\right)^{(t-1)/2}
\]
and so
\[
\varepsilon_{f,t} = \pm N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f)} \cap K \left(\frac{1-\zeta_f^t}{(1-\zeta_f)^t}\right) \cdot \eta_f^{(t-1)/2} \in B'_K.
\]
Lemma 4 gives \(B_K = B'_K\).

3. Behavior of the unit groups in \(\mathbb{Z}_p\)-extensions

Let \(K\) be a real abelian field and \(p\) be a prime. Let
\[
K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty = \bigcup_{n=0}^{\infty} K_n
\]
be the cyclotomic \(\mathbb{Z}_p\)-extension of \(K\). Then all fields \(K_n\) are real abelian, so we can consider the groups \(B_{K_n}, C_{K_n}, D_{K_n},\) and \(E_{K_n}\). To simplify our notation let us write \(B_n := B_{K_n}, C_n := C_{K_n}, D_n := D_{K_n},\) and \(E_n := E_{K_n}\). The aim of this section is to study the behavior of relative indices between these groups in the tower.

We shall use the following standard terminology (see [9], page 118). Let \(q = p\) if \(p\) is odd and \(q = 4\) if \(p = 2\). A Dirichlet character is called a character of the first kind if its conductor is not divisible by \(pq\), and a character of the second kind if it is even and both its conductor and its order are powers of \(p\) (including \(p^0\)). By definition, the trivial character is of both kinds. So the characters of the second kind are exactly the Dirichlet characters of finite layers in the \(\mathbb{Z}_p\)-extension of \(\mathbb{Q}\). It is well-known that each Dirichlet character can be uniquely written as a product of a character of the first kind and a character of the second kind.

Having any real abelian field \(K'\), we can decompose each Dirichlet character corresponding to \(K'\) in the mentioned way. If we choose \(K\) to be the real abelian field whose group of Dirichlet characters consists of the obtained characters of the first kind, then the \(\mathbb{Z}_p\)-extension \(K_\infty\) of \(K\) is equal to the \(\mathbb{Z}_p\)-extension \(K'_\infty\) of \(K'\). As all our results concern the behavior of groups of units at a sufficiently large level, we can suppose without loss of generality that all Dirichlet characters of our fixed real abelian field \(K\) are of the first kind.

**Proposition 12.** There is a positive integer \(r\) such that
\[
[D_n : B_n^2] = [D_r : B_r^2]
\]
for all \(n \geq r\).

**Proof.** Let \(m\) be the maximal divisor of the conductor of \(K\) that is not divisible by \(p\). Since each Dirichlet character of our fixed real abelian field \(K\) is of the first kind, we see that the conductor of \(K\) is \(m\) or \(mq\). Let \(n\) be any positive integer.
The conductor of $K_n$ is $mp^n$ and Proposition 7 describes the generators of $D_n/B_n^2$: besides the generator $\eta_{1,n} = -1$ we have the generator

$$\eta_{f,n} = N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_f) \cap K_n}(1 - \zeta_f)$$

for each $1 < f \mid mp^n$, $(f, mp^n/f) = 1$.

On one hand, if $f \mid m$ then $p \nmid f$, so $\mathbb{Q}(\zeta_f) \cap K_n = \mathbb{Q}(\zeta_f) \cap K$, the generator $\eta_{f,n} = \eta_{f,1}$ does not depend on $n$, and

$$N_{K_{n+1}/K_n}(\eta_{f,n+1}) = \eta_{f,n}^p.$$  

On the other hand, if $f \nmid m$ then we have $\mathbb{Q}(\zeta_{pf}) \cap K_{n+1} \neq \mathbb{Q}(\zeta_f) \cap K_n$ because the group of Dirichlet characters of the former intersection contains all characters of second kind of conductor $qp^{n+1}$ which is not the case for the group of Dirichlet characters of the latter one. Therefore we have the following diagram of fields:

$$
\begin{array}{ccc}
\mathbb{Q}(\zeta_{pf}) & \xrightarrow{p} & K_{n+1} \\
\downarrow & & \downarrow p \\
\mathbb{Q}(\zeta_f) & \xrightarrow{p} & \mathbb{Q}(\zeta_{pf}) \cap K_{n+1} \\
& & \downarrow p \\
\mathbb{Q}(\zeta_f) \cap K_n & & \\
\end{array}
$$

and

$$N_{K_{n+1}/K_n}(\eta_{pf,n+1}) = N_{K_{n+1}/K_n}(N_{\mathbb{Q}(\zeta_{pf})/\mathbb{Q}(\zeta_{pf}) \cap K_{n+1}}(1 - \zeta_{pf}))$$

$$= N_{\mathbb{Q}(\zeta_{pf})/\mathbb{Q}(\zeta_f) \cap K_n}(1 - \zeta_{pf})$$

$$= \eta_{f,n}$$

because $p \mid f$ implies

$$N_{\mathbb{Q}(\zeta_{pf})/\mathbb{Q}(\zeta_f)}(1 - \zeta_{pf}) = 1 - \zeta_f.$$  

For any positive integer $n$, the conductors of $K_{n+1}$ and $K_n$ are divisible by the same primes and so by Propositions 10 and 7 the norm induces the linear mapping $\hat{\mathbb{N}}_n : D_{n+1}/B_{n+1}^2 \to D_n/B_n^2$ of vector spaces over $\mathbb{F}_2$.

At first, let us assume $p \neq 2$. Then for any $f \mid m$, $(f, m/f) = 1$, we have

$$\hat{\mathbb{N}}_n(\eta_{f,n+1}) = \eta_{f,n}^p = \eta_{f,n} \in D_n/B_n^2.$$ 

Therefore $\hat{\mathbb{N}}_n : D_{n+1}/B_{n+1}^2 \to D_n/B_n^2$ is surjective and so

$$[D_{n+1} : B_{n+1}^2] \geq [D_n : B_n^2].$$

Due to Corollary 8 the upper bound of this index is $2^{2^g}$, where $g$ is the number of prime divisors of $pm$. Hence the sequence of indices $[D_n : B_n^2]$ must stabilize.
Now, let us assume that \( p = 2 \). Let \( D'_n \) be the \( G \)-submodule of \( D_n \) generated by all \( \eta_{f,n} \) with \( p \mid f \). Then \( D_n \) is the sum (not necessarily direct) of its submodules \( D_1 \) and \( D'_n \). Considering \( D_n/B_n^2 \) as a vector space over \( \mathbb{F}_2 \), we see that \( D_n/B_n^2 \) is the sum (not necessarily direct) of its subspaces \( U_n = D_1B_n^2/B_n^2 \) and \( V_n = D'_nB_n^2/B_n^2 \). We have seen that \( \hat{N}_n(U_{n+1}) = 0 \) and \( \hat{N}_n(V_{n+1}) = V_n \). Hence \( \dim_{\mathbb{F}_2} V_n \) is non-decreasing and bounded from above by \( 2^k \), so it must stabilize. Since \( B_n \subseteq B_{n+1} \) due to Proposition 10, \( \dim_{\mathbb{F}_2} U_n \) is non-increasing, so it must also stabilize. Let \( k \) be the least positive integer such that \( \dim_{\mathbb{F}_2} U_n = \dim_{\mathbb{F}_2} U_k \) for all \( n \geq k \). Then \( \hat{N}_n(V_{n+1}) = V_n \) gives \( V_{n+1} \cap \ker \hat{N}_n = 0 \) for any \( n \geq k \). Since \( U_{n+1} \subseteq \ker \hat{N}_n \) we have \( V_{n+1} \cap U_{n+1} = 0 \) and so \( D_{n+1}/B_{n+1}^2 \) is the direct sum \( U_{n+1} \oplus V_{n+1} \), hence \( [D_{n+1} : B_{n+1}^2] = 2^{\dim_{\mathbb{F}_2} U_k + \dim_{\mathbb{F}_2} V_k} \) is independent of \( n \).

**Corollary 13.** The product

\[
[(B_n \cap E_n) : C_n] \cdot 2^{-[K_n : \mathbb{Q}]}
\]

is constant for sufficiently large \( n \).

**Proof.** This follows from Corollary 9 and Proposition 12 since the set of primes dividing the conductor of \( K_n \) for any \( n \geq 1 \) is the set of prime divisors of \( pm \).

**Theorem 14.** Let \( K \) be a real abelian field and \( p \) be a prime. Let

\[
K = K_0 \subset K_1 \subset K_2 \subset \ldots K_\infty = \bigcup_{n=0}^{\infty} K_n
\]

be the cyclotomic \( \mathbb{Z}_p \)-extension of \( K \). Then there is a constant \( c \in \mathbb{Q} \) depending only on \( K_\infty \) such that for any sufficiently large \( n \) we have

\[
[E_n : (B_n \cap E_n)] = c \cdot h_n,
\]

where \( h_n \) is the class number of \( K_n \).

**Proof.** Sinnott proved (see [7], Theorem on page 182) that there is \( c_0 \in \mathbb{Q} \), depending only on \( K_\infty \) such that

\[
[E_n : C_n] = c_0 \cdot h_n \cdot 2^{[K_n : \mathbb{Q}]}
\]

for all sufficiently large \( n \). According to Corollary 13 there is \( c_1 \in \mathbb{Q} \) such that

\[
[(B_n \cap E_n) : C_n] = c_1 \cdot 2^{[K_n : \mathbb{Q}]}
\]

for all sufficiently large \( n \). Taking the quotient gives the theorem.

Note that in the theorem mentioned above Sinnott also defined

\[
C_{1,K_n} = \{ \varepsilon \in E_n \mid \varepsilon^2 \in C_n \}
\]

and proved that there is \( c' \in \mathbb{Q} \) such that

\[
[E_n : C_{1,K_n}] = c' \cdot h_n,
\]

for any sufficiently large \( n \). Although Proposition 6 implies that \( B_n \cap E_n \subseteq C_{1,K_n} \), this group \( C_{1,K_n} \) is not given by means of explicit generators while Corollary 5 describes explicit generators of \( B_n \cap E_n \).
In the previous section we have shown that \( B_K \cap E_K \) has a better behavior in \( \mathbb{Z}_p \)-extensions than Sinnott’s group of circular units \( C_K \). But this cannot be said about all properties of this group. For instance, it seems to be more difficult to find the index \( [E_K : (B_K \cap E_K)] \) than \( [E_K : C_K] \). Let us restrict ourselves only to the case \( K = \mathbb{Q}(\zeta_m)^+ \), \( 1 < m \not\equiv 2 \pmod{4} \), and write \( m = \prod_{i=1}^{g} p_i^{e_i} \), where \( p_1, \ldots, p_g \) are different primes dividing \( m \). The index of the group of circular units is computed in [7], Theorem 4.1 and for our \( K \) the result is:

\[
[E_K : C_K] = h_K \cdot 2^{[K : \mathbb{Q}] - 1} \cdot \prod_{i=1}^{g} \left[ K_{p_i} : \mathbb{Q} \right] \cdot (R : U),
\]

where \( h_K \) is the class number of \( K \) and \( K_{p_i} = \mathbb{Q}(\zeta_{p_i^{e_i}})^+ \). It is easy to compute

\[
\prod_{i=1}^{g} \left[ K_{p_i} : \mathbb{Q} \right] = 2^{1-g},
\]

so

\[
[E_K : C_K] = h_K \cdot 2^{[K : \mathbb{Q}] - g} \cdot (R : U),
\]

and [7], Theorem 5.4 gives

\[
(R : U) = \begin{cases} 
1 & \text{if } g = 1, \\
2^{g-2} - 1 & \text{otherwise.}
\end{cases}
\]

Therefore, for maximal real subfields of cyclotomic fields, the index \( [E_K : C_K] \) is determined by the class number, the absolute degree, and the number of ramified primes.

We can show that this is not the case for the index \( [E_K : (B_K \cap E_K)] \), which seems to be of more delicate matter. We were able to do it only for \( g \leq 3 \). Denoting \( x = \dim_{\mathbb{F}_2} D_K / B_K^2 \), Corollaries 9 and 8 give

\[
[(B_K \cap E_K) : C_K] = 2^{[K : \mathbb{Q}] + g - x}
\]

and \( 1 + g \leq x \leq 2^g \). In the case \( g = 1 \) this gives \( x = 2 \). Using the basis of the group of circular units of a cyclotomic field described in [3] we have obtained the following results which we only mention here without proof. If \( m = p_1 p_2 \) is a product of two different odd primes then \( x = 4 \). If \( m = p_1 p_2 p_3 \) is a product of three different odd primes then we need to distinguish the following four cases

- \( p_1 \equiv p_2 \equiv p_3 \equiv 1 \pmod{4} \): always \( x = 8 \);
- \( p_1 \equiv p_2 \equiv -p_3 \equiv 1 \pmod{4} \): if \( \left( \frac{p_2}{p_1} \right) = 1 \) then \( x = 8 \) else \( x = 7 \);
- \( p_1 \equiv -p_2 \equiv -p_3 \equiv 1 \pmod{4} \): if \( \left( \frac{p_2}{p_1} \right) = \left( \frac{p_3}{p_1} \right) = 1 \) then \( x = 8 \) else \( x = 7 \);
- \( p_1 \equiv p_2 \equiv p_3 \equiv 3 \pmod{4} \): always \( x = 7 \).

This example shows that to determine the exact power of 2 dividing the index \( [E_K : (B_K \cap E_K)] \) for the maximal real subfield of a cyclotomic field one needs to know more than only the class number, the absolute degree and the number of ramified primes.
Acknowledgments

The authors thank the referee for his very useful comments which helped to rewrite the paper to this version.

References


