CIRCULAR UNITS AND CLASS GROUPS OF ABELIAN FIELDS

RADAN KUČERA

ABSTRACT. The main aim of this paper is to give an exposition on circular units which contains definitions, basic properties (usually given without proofs), and some examples. Moreover, the paper is supplemented by some results to compare different groups of circular units (Proposition 2.2, Theorems 3.1 and 3.3) and these unpublished results are fully proven here.

1. Circular units in a cyclotomic field. The easiest situation where one can consider circular (sometimes called cyclotomic) units is the case of cyclotomic fields. Let \( n > 2 \) be a positive integer and \( \zeta_n = e^{2\pi i/n} \) be a primitive \( n \)th root of unity, for example \( \zeta_n = e^{2\pi i/n} \).

Let \( \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n) \) be the \( n \)th cyclotomic field. Since \( \mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n) \) for an odd \( n \), we can suppose that \( n \not\equiv 2 \pmod{4} \). We know that the ring of algebraic integers of \( \mathbb{Q}(\zeta_n) \) is equal to \( \mathbb{Z}[\zeta_n] \) and Dirichlet’s unit theorem gives the structure of the group \( E(\mathbb{Q}(\zeta_n)) \) of units of \( \mathbb{Z}[\zeta_n] \): it is isomorphic to the product of its torsion subgroup with \( \frac{1}{2} \phi(n) - 1 \) copies of \( \mathbb{Z} \). Moreover the torsion part \( E(\mathbb{Q}(\zeta_n))_{\text{tor}} \) is the cyclic group \( \langle -1, \zeta_n \rangle \) having \( 2n \) or \( n \) elements depending upon whether \( n \) is odd or even. But we do not know an explicit system of generators of the whole group \( E(\mathbb{Q}(\zeta_n)) \). Even worse, a computation of these so-called fundamental units for a given \( n \) is intractable already for modest values of \( n \).

However we know plenty of units of \( \mathbb{Q}(\zeta_n) \) explicitly, for example, \( 1 - \zeta_n^a \in E(\mathbb{Q}(\zeta_n)) \) for any integer \( a \) such that \( n \nmid a \) and \( n/(a, n) \) is not a prime power. Moreover \( a \)'s with \( n/(a, n) \) being a prime power can be also used to produce units: \( (1 - \zeta_n^a)/(1 - \zeta_n^b) \in E(\mathbb{Q}(\zeta_n)) \) for any integers \( a \) and \( b \) such that \( (a, n) = (b, n) \neq n \). These units altogether generate the so-called group of circular units \( C(\mathbb{Q}(\zeta_n)) \) of \( \mathbb{Q}(\zeta_n) \). It is easy to show that this group can be defined also by the intersection

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

where \( \langle \ldots \rangle \) means “generated as a multiplicative subgroup of \( \mathbb{Q}(\zeta_n) \).” Let us mention that \( -\zeta_n = (1 - \zeta_n)/(1 - \zeta_n^{-1}) \in C(\mathbb{Q}(\zeta_n)) \) and so \( E(\mathbb{Q}(\zeta_n))_{\text{tor}} \subseteq C(\mathbb{Q}(\zeta_n)) \).


©Association mathématique du Québec
For \( n = p \) being an odd prime, the group of circular units has been already studied by E. Kummer who discovered that (in modern language) the index of \( C(\mathbb{Q}^{(p)}) \) in \( E(\mathbb{Q}^{(p)}) \) is equal to the class number of the maximal real subfield \( \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \) of \( \mathbb{Q}^{(p)} \). This result has been generalized by W. Sinnott who proved in [S1] 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 \( \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \) of \( \mathbb{Q}^{(n)} \) and \( c \) involves explicitly the number \( s \) of ramified primes in \( \mathbb{Q}^{(n)} \) (i.e. primes dividing \( n \)): \( c = 0 \) for \( s = 1 \) and \( c = 2^{s-2} + 1 - s \) for \( s > 1 \).

If \( n = p^e \) is a prime power then it is easy to describe a \( \mathbb{Z} \)-basis of \( C(\mathbb{Q}^{(n)}) \), i.e., an independent system of generators of \( C(\mathbb{Q}^{(n)})/C(\mathbb{Q}^{(n)})_{\text{tor}} \). Such a basis is, for example, the set

\[
\left\{ \frac{1 - \zeta_a^n}{1 - \zeta_n^n} : 1 < a < \frac{n}{2}, (a, n) = 1 \right\},
\]

and the index formula can be obtained in this case just by computing the regulator of this basis (see [W, pp. 143-146]). The general case is much more complicated – again a basis is formed by a suitable set of the mentioned generators, but now it is difficult to describe which set of the generators one should take (see [GK] and [K1]). Nevertheless R. Gold and J. Kim have been able to use this ugly basis to obtain a nice result: the groups of circular units of cyclotomic fields satisfy Galois descent, i.e., if \( m | n \) then

\[
C(\mathbb{Q}^{(m)}) = C(\mathbb{Q}^{(n)}) \cap \mathbb{Q}^{(m)} = C(\mathbb{Q}^{(n)})_{\text{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}^{(m)})}. \]

2. Circular units in an abelian field. By an abelian field we have in mind a finite Galois extension of \( \mathbb{Q} \) whose Galois group is abelian. Due to the Kronecker-Weber theorem we know that any abelian field is a subfield of a cyclotomic field. Let \( K \) be an abelian field and let \( m \) be the conductor of \( K \) (i.e., \( \mathbb{Q}^{(m)} \) is the smallest cyclotomic field containing \( K \)). Let \( E(K) \) be the group of units (of the ring of integers) in \( K \). In contrast to the case of a cyclotomic field, it is not so clear how to define the group of circular units of \( K \). In fact we have several possible definitions giving different groups.

We can use the norm of \( \mathbb{Q}^{(m)}/K \) to map the group \( C(\mathbb{Q}^{(m)}) \) to \( E(K) \). By this procedure we obtain the so-called group of circular units of \( K \) of conductor level

\[
C_{\text{cl}}(K) = \langle \pm N_{\mathbb{Q}^{(m)}/K}(1 - \zeta_m^a) ; a \in \mathbb{Z}, \ m \nmid a \rangle \cap E(K).
\]

Since \( C(\mathbb{Q}^{(m)}) \) is of finite index in \( E(\mathbb{Q}^{(m)}) \), it is clear that \( C_{\text{cl}}(K) \) is of finite index in \( E(K) \).

But consider a generator \( N_{\mathbb{Q}^{(m)}/K}(1 - \zeta_m^a) \) of this group in the case when \( a \) and \( m \) are not relatively prime. We can suppose that our roots of unity satisfy \( \zeta_{st}^t = \zeta_s \) for any positive integers \( s, t \). Let \( r = m/(a, m) \) and \( b = a/(a, m) \). The following diagram of
R. Kučera

fields

\[
\begin{array}{c}
\mathbb{Q}^{(m)} \\
K \mathbb{Q}^{(r)} \\
\mathbb{Q}^{(r)} \\
\mathbb{Q}^{(r)} \cap K
\end{array}
\]

gives that

\[
N_{\mathbb{Q}^{(m)}/K}(1 - \zeta_m^a) = N_{\mathbb{Q}^{(m)}/K}(1 - \zeta_r^b) = N_{\mathbb{Q}^{(r)}/K \cap \mathbb{Q}^{(r)}}(1 - \zeta_p^b)[\mathbb{Q}^{(m)}, K \mathbb{Q}^{(r)}],
\]

which is a power of an explicit number.

Since we want to have a good approximation of \(E(K)\) by some explicitly generated subgroup, we take as many explicit generators as possible. Therefore we can use the previous computation to enlarge the group and get an equivalent form of Sinnott’s definition of the group of circular units of \(K\) (the fact that the following definition is equivalent to the definition of Sinnott in [S2] is proven in [L, Proposition 1]). Sinnott’s group \(C_S(K)\) of circular units of \(K\) can be defined by the intersection

\[
C_S(K) = \langle \pm {N_{\mathbb{Q}^{(r)}/\mathbb{Q}^{(r)} \cap K}}(1 - \zeta_p^a); \; 1 < r \mid m, (a, r) = 1 \rangle \cap E(K).
\]

It is clear that \(C_{cl}(K) \subseteq C_S(K)\). Sinnott proved in [S2] that the index of \(C_S(K)\) in \(E(K)\) is a multiple of the class number \(h_K^+\) of the maximal real subfield \(K \cap \mathbb{R}\) of \(K\) but his formula contains a non-explicit factor, namely the index of Sinnott’s module \(U\).

This module is a submodule of the rational group ring \(\mathbb{Q}[G]\), where \(G = \text{Gal}(K/\mathbb{Q})\) is the Galois group of \(K\), and is defined by means of inertia subgroups and Frobenius automorphisms of ramified primes (for the precise definition, see [S2, Proposition 2.3]). Sinnott’s formula reads

\[
[E(K) : C_S(K)] = h_K^+ \mathbb{Q} \frac{\prod_{p|m} [K_p : \mathbb{Q}]}{[K : \mathbb{Q}]} 2^{-g} (e^+ Z[G] : e^+ U)
\]

(see [S2, Theorem 4.1]), where \(Q \in \{1, 2\}\) is Hasse’s unit index (so \(Q = 1\) if \(K\) is real), \(K_p\) is the maximal subfield of \(K\) unramified at all finite primes different from \(p\), \(e^+ = (1 + j)/2 \in \mathbb{Q}[G]\) is the idempotent given by the complex conjugation \(j \in G\) (so \(e^+ = 1\) if \(K\) is real), and \((:\)\) is the generalized index (defined by means of the absolute value of the determinant of the transition matrix between bases of the two modules); finally \(g = 1 - [K : \mathbb{Q}]\) if \(K\) is real but otherwise \(g\) is not determined in full. If \(K\) is imaginary we only know that \(g\) is an integer between the number of primes \(p|m\) with \(K_p\) imaginary and the number of them with \([K_p : \mathbb{Q}]\) even (see [S2, Proposition 4.1]).

The small problem concerning the unknown \(g\) can be overcome by a slight modification of the definition of \(C_S(K)\) (see [K3]) but the problem of determining the index
(e^* \mathbb{Z}[G] : e^* U) is serious: Sinnott proved in [S2, Proposition 5.1] that this index is an integer which can be divisible only by primes dividing the degree \([K : \mathbb{Q}]\) (he proved even more: this index can be divisible only by primes dividing the degree \([K : K]\), where \(K\) is the genus field of \(K\) in the narrow sense, and also by 2 if \(K\) is imaginary, see [S2, Corollary on p. 225]) but the precise value of this index is known only for some special cases of \(K\): for example, if \(K\) is real with \(G\) cyclic (see [S2, Theorem 5.3]); or if \(K\) is ramified at most at two finite primes (see [S2, Theorem 5.1]); or if the compositum \(K \mathbb{K}_p\) is equal to \(K\) for each prime \(p|m\), where \(\mathbb{K}_p\) is the maximal subfield of \(\mathbb{K}\) unramified at all finite primes different from \(p\) (see [S2, Theorem 5.4]); or if \(K\) is a compositum of quadratic fields (see [K2]); or if the degree of \(K\) is the square of an odd prime (see [Kr]).

We have seen that, similarly to the case of cyclotomic fields, \(C_S(K)\) is again defined by means of explicit generators and its finite index is described by a formula containing the class number of the maximal real subfield but we lose one nice property, namely we do not have Galois descent in general. Since we want to keep the definition for cyclotomic fields as a special case, there is just one way how to get Galois descent, namely by putting \(C_W(K) = K \cap C(\mathbb{Q}(m))\). It is easy to see that \(C_S(K) \subseteq C_W(K)\).

Since this definition is mentioned in [W, p. 143], we are calling \(C_W(K)\) the Washington group of circular units of \(K\). But using this definition we lose the other good properties of circular units: we have neither explicit generators nor a formula for the index (more precisely, the author is not aware of any published formula for \([E(K) : C_W(K)]\) which would cover infinitely many abelian fields \(K\) with \(C_W(K) \neq C_S(K)\) - a formula of this kind for a very special class of abelian fields is given by Proposition 2.2 below).

There is another definition of circular units which can be found in the literature (see [Gb, pp. 152–153]). This approach uses cyclic subfields of \(K\) and goes back to Hasse (see [H, pp. 38, 22], where slightly different numbers are considered). This group is smaller but it has the advantage of an easier Galois module structure. Let \(L\) be the set of all cyclic subfields \(L \neq \mathbb{Q}\) of \(K\), i.e., of all subfields \(L \subseteq K\) whose Galois group \(\text{Gal}(L/\mathbb{Q})\) is a nontrivial cyclic group. Let \(f_L\) be the conductor of \(L\). The group of circular units of cyclic subfields of \(K\) is defined by

\[
C_{cs}(K) = \langle \pm N_{\mathbb{Q}(f_L)/L}(1 - \zeta_{f_L}) ; L \in L, a \in \mathbb{Z}, (a, f_L) = 1 \rangle \cap E(K).
\]

Since we have

\[
N_{\mathbb{Q}(f_L)/L}(1 - \zeta_{f_L}) = N_{\mathbb{Q}(f_L) \cap K/L}(N_{\mathbb{Q}(f_L)/}\mathbb{Q}(f_L)\cap K(1 - \zeta_{f_L}))
\]

it is easy to see that \(C_{cs}(K) \subseteq C_S(K)\).

In the next example we shall need the following well-known norm relations: let \(n\) and \(m\) be positive integers, \(n \neq 2 \equiv m \pmod{4}\), \(n|m\). Then

\[
N_{\mathbb{Q}(m)/\mathbb{Q}(n)}(1 - \zeta_m) = (1 - \zeta_n)^{\prod_p(1 - \text{Frob}(p)^{-1})},
\]

where the product is taken over all primes \(p \mid m, p \nmid n\), and \(\text{Frob}(p)\) means the Frobenius automorphism of \(p\) (an empty product equals 1).
Example 2.1. Let us compute all mentioned groups of circular units for

\[ K = \mathbb{Q}(\sqrt{13}, \sqrt{17}). \]

It is easy to see that the conductor of \( K \) is \( 13 \cdot 17 = 221 \) and that \( \text{Gal}(\mathbb{Q}(\sqrt{221})/\mathbb{Q}) = \langle \sigma, \tau \rangle \), where \( \zeta_{13}^\sigma = \zeta_{13}, \zeta_{17}^\sigma = \zeta_{17}, \zeta_{13}^\tau = \zeta_{13}^2 \), and \( \zeta_{17}^\tau = \zeta_{17} \). We have \( \text{Gal}(\mathbb{Q}(\sqrt{221})/K) = \langle \sigma^2, \tau^2 \rangle \), so \( \text{Gal}(K/\mathbb{Q}) = \{1, \sigma|_K, \tau|_K, \sigma \tau|_K\} \). Let

\[ \eta_1 = N_{\mathbb{Q}(\sqrt{221})/K}(1 - \zeta_{221}). \]

Then, using the norm relations (2.3), we have

\[ \eta_1^{1+\sigma} = N_{\mathbb{Q}(\sqrt{221})/\mathbb{Q}(\sqrt{13})}(1 - \zeta_{221}) = N_{\mathbb{Q}(13)/\mathbb{Q}(\sqrt{13})}(1 - \zeta_{13})^{1-\text{Frob}(17)^{-1}} = 1, \]

since the Legendre symbol \( (\frac{13}{17}) = 1 \) and so \( \text{Frob}(17) \) on \( \mathbb{Q}(\sqrt{13}) \) is trivial. Similarly \( \eta_1^{1+\tau} = 1 \). Hence all conjugates of \( \eta_1 \) are \( \eta_1^\sigma = \eta_1^\tau = \eta_1^{-1} \) and \( \eta_1^{\sigma \tau} = \eta_1 \). Let

\[ \eta_2 = N_{\mathbb{Q}(13)/\mathbb{Q}(\sqrt{13})}(1 - \zeta_{13})^{1-\tau} \]

be the quotient of the only two conjugates of the norm \( N_{\mathbb{Q}(\sqrt{13})/\mathbb{Q}}(1 - \zeta_{13}) \), which is not a unit, since \( N_{\mathbb{Q}(\sqrt{13})/\mathbb{Q}}(N_{\mathbb{Q}(13)/\mathbb{Q}(\sqrt{13})}(1 - \zeta_{13})) = 13 \). Similarly, let

\[ \eta_3 = N_{\mathbb{Q}(17)/\mathbb{Q}(\sqrt{17})}(1 - \zeta_{17})^{1-\sigma}. \]

Then

\[ C_S(K) = \langle -1, \eta_1, \eta_2, \eta_3 \rangle. \]

Since \([\mathbb{Q}(\sqrt{221}): K]\mathbb{Q}(13)] = \frac{1}{2} \varphi(17) = 8\) and \([\mathbb{Q}(\sqrt{221}): K\mathbb{Q}(17)] = \frac{1}{2} \varphi(13) = 6\), we have

\[ C_{\text{cl}}(K) = \langle -1, \eta_1, \eta_2^8, \eta_3^6 \rangle \]

and \([C_S(K) : C_{\text{cl}}(K)] = 48\). The nontrivial cyclic subfields of \( K \) are \( \mathbb{Q}(\sqrt{13}), \mathbb{Q}(\sqrt{17}), \)

and \( \mathbb{Q}(\sqrt{221}) \). Since \( \text{Gal}(K/\mathbb{Q}(\sqrt{221})) = \{1, \sigma \tau|_K\} \) and \( \eta_1^{\sigma \tau} = \eta_1 \), we have

\[ C_{\text{cs}}(K) = \langle -1, \eta_1^2, \eta_2, \eta_3 \rangle \]

and \([C_S(K) : C_{\text{cs}}(K)] = 2\). We have obtained that neither \( C_{\text{cs}}(K) \subseteq C_{\text{cl}}(K) \) nor \( C_{\text{cl}}(K) \subseteq C_{\text{cs}}(K) \). The determination of the Washington group of circular units is more complicated since it is not given by a system of generators. We have

\[ \eta_1 = \prod_{1 \leq a < 221 \atop \left(\frac{a}{221}\right) = 1} (1 - \zeta_{221}^a) = \prod_{1 \leq a < 221 \atop a \equiv 1, 3, 9 \pmod{13}} \eta_1 \]

where

\[ \varepsilon_1 = \prod_{1 \leq a < 221 \atop a \equiv 1, 3, 9 \pmod{13}} (1 - \zeta_{221}^a), \]

and
since the number of factors is even and the Chinese remainder theorem gives that $\sum a$ is divisible by both 13 and 17. Similarly

$$N_{\mathbb{Q}(\sqrt{13})/\mathbb{Q}}(1 - \zeta_{13}) = -(1 - \zeta_{13})^2(1 - \zeta_{13}^3)^2(1 - \zeta_{13}^9)^2$$

and

$$N_{\mathbb{Q}(\sqrt{17})/\mathbb{Q}}(1 - \zeta_{17}) = \zeta_{17}^2(1 - \zeta_{17})^2(1 - \zeta_{17}^2)^2(1 - \zeta_{17}^4)^2(1 - \zeta_{17}^8)^2.$$  

Hence $\eta_2 = \varepsilon_2^3$ and $\eta_3 = \varepsilon_3^3,$ where

$$\varepsilon_2 = \frac{(1 - \zeta_{13})(1 - \zeta_{13}^3)(1 - \zeta_{13}^9)}{(1 - \zeta_{13}^2)(1 - \zeta_{13}^3)(1 - \zeta_{13}^9)}$$

and

$$\varepsilon_3 = \frac{\zeta_{17}(1 - \zeta_{17})(1 - \zeta_{17}^2)(1 - \zeta_{17}^4)(1 - \zeta_{17}^8)}{\zeta_{17}^2(1 - \zeta_{17}^2)(1 - \zeta_{17}^4)(1 - \zeta_{17}^8)(1 - \zeta_{17}^3)}$$

Since $\eta_1^6 = \eta_1^{-1},$ we have $\varepsilon_1^6 = \pm \varepsilon_1^{-1}$ and $\varepsilon_1^2 = \pm \varepsilon_1^{-1},$ which gives $\varepsilon_1^2 = \varepsilon_1^2 = \varepsilon_1$ and so $\varepsilon_1 \in K.$ It is easy to check that $\varepsilon_2^7 = -\varepsilon_2^{-1}$ and $\varepsilon_3 = -\varepsilon_3^{-1},$ and again $\varepsilon_2, \varepsilon_3 \in K.$ Since clearly $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in C(\mathbb{Q}(\sqrt{21})),$ we have

$$\langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle \subseteq C_W(K).$$

The problem is to prove the other inclusion. Using the software package PARI we can compute the class number $h_K$ and the system of fundamental units of $K$: we have $h_K = 1$ and

$$E(K) = \langle -1, \sqrt{17} - \sqrt{3}, \sqrt{13} - 3, \sqrt{17} - 4 \rangle.$$  

Moreover we compute

$$\varepsilon_1 = \frac{\sqrt{17} - \sqrt{3}}{2}, \quad \varepsilon_2 = \frac{\sqrt{13} - 3}{2}, \quad \varepsilon_3 = 4 - \sqrt{17}.$$  

Hence the inclusion $C_W(K) \subseteq E(K)$ gives

$$C_W(K) = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$$

and $[C_W(K) : C_S(K)] = 8.$ \(\square\)

The following proposition generalizes Example 2.1 and computes the index $[E(K) : C_W(K)]$ for an infinite family of abelian fields.

**Proposition 2.2.** Let $p \equiv q \equiv 1 \pmod{4}$ be different primes such that $(\frac{p}{q}) = 1$ and let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q}).$ Then we have $[E(K) : C_W(K)] = h_K.$

**Proof.** The conductor of $K$ is $pq$ and $\text{Gal}(\mathbb{Q}(\sqrt{pq})/\mathbb{Q}) = \langle \sigma, \tau \rangle,$ where $\sigma$ and $\tau$ are chosen to satisfy $\text{Gal}(\mathbb{Q}(\sqrt{pq})/\mathbb{Q}(\sqrt{p})) = \langle \sigma \rangle$ and $\text{Gal}(\mathbb{Q}(\sqrt{pq})/\mathbb{Q}(\sqrt{q})) = \langle \tau \rangle.$ Then $\sigma(q-1)/2 \tau(p-1)/2$ is the complex conjugation and $\text{Gal}(\mathbb{Q}(\sqrt{pq})/K) = \langle \sigma^2, \tau^2 \rangle,$ so $\text{Gal}(K/\mathbb{Q}) = \{1, \sigma | K, \tau | K, \sigma \tau | K \}.$ Let

$$\eta_1 = N_{\mathbb{Q}(\sqrt{pq})/K}(1 - \zeta_{pq}), \quad \eta_2 = N_{\mathbb{Q}(\sqrt{pq})/\mathbb{Q}(\sqrt{p})}(1 - \zeta_p)^{1-\tau}$$

and
and \( \eta_3 = N_{Q(\sqrt{q})/Q}\left(1 - \zeta_q\right)^{1-\sigma}. \)

Since \( \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1 \), the norm relations give \( \eta_1^{1+\tau} = \eta_3^{1+\sigma} = 1 \) and

\[
C_S(K) = \langle -1, \eta_1, \eta_2, \eta_3 \rangle.
\]

Similarly as in Example 2.1 we obtain that \( \eta_1, \eta_2, \) and \( \eta_3 \) are squares in \( \mathbb{Q}^{(pq)} \). Indeed,

\[
\eta_1 = \prod_{i=0}^{(q-3)/2} \prod_{j=0}^{(p-3)/2} (1 - \zeta_{pq})^{\sigma_2 i \tau_2 j} = \prod_{i=0}^{(q-5)/4} \prod_{j=0}^{(p-3)/2} (-\zeta_{pq}^{-1}(1 - \zeta_{pq})^2)^{\sigma_1 i \tau_2 j} = \eta_1^2,
\]

with

\[
\varepsilon_1 = \prod_{i=0}^{(q-5)/4} \prod_{j=0}^{(p-3)/2} \left(\zeta_{pq}^{(pq-1)/2}(1 - \zeta_{pq})\right)^{\sigma_1 i \tau_2 j};
\]

moreover,

\[
\eta_2 = \prod_{i=0}^{(p-3)/2} (1 - \zeta_p)^{(-\tau)^i} = \prod_{i=0}^{(p-3)/2} (-\zeta_p^{-1}(1 - \zeta_p)^2)^{(-\tau)^i} = \eta_2^2,
\]

and \( \eta_3 = \varepsilon_3^2 \), where

\[
\varepsilon_2 = \prod_{i=0}^{(p-3)/2} \left(\zeta_p^{(p-1)/2}(1 - \zeta_p)^{(-\tau)^i}\right), \quad \varepsilon_3 = \prod_{i=0}^{(q-3)/2} \left(\zeta_q^{(q-1)/2}(1 - \zeta_q)^{(-\sigma)^i}\right).
\]

Since \( \eta_1^{\sigma} = \eta_1^{(-1)} = \eta_1^{-1} \), we have \( \varepsilon_1^{\sigma} = \pm \varepsilon_1^{-1} \) and \( \varepsilon_1^{-1} = \pm \varepsilon_1^{-1} \), which gives \( \varepsilon_1^{\sigma} = \varepsilon_1^{-1} = \varepsilon_1 \), and so \( \varepsilon_1 \in K \). Moreover,

\[
\varepsilon_2^{1+\tau} = (\zeta_p^{(p-1)/2}(1 - \zeta_p)^{1-\tau(p-1)/2}) \frac{\zeta_p^{(p-1)/2}(1 - \zeta_p)}{\zeta_p^{(p-1)/2}(1 - \zeta_p^{-1})} = -1
\]

and similarly \( \varepsilon_3^{1+\sigma} = -1 \), so \( \varepsilon_2, \varepsilon_3 \in K \). Clearly \( \varepsilon_1, \varepsilon_2, \varepsilon_3 \in C\left(\mathbb{Q}^{(pq)}\right) \), so we have

\[
\langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle \subseteq C_W(K).
\]

To prove the other inclusion we shall use a basis of \( C\left(\mathbb{Q}^{(pq)}\right) \) obtained in [GK] or [K1]: a basis of \( C\left(\mathbb{Q}^{(pq)}\right) \) is formed by

\[
\begin{align*}
&u_j = (1 - \zeta_p)^{1-\tau_j}, \quad j = 1, 2, \ldots, (p-3)/2, \\
u_i = (1 - \zeta_q)^{1-\sigma_i}, \quad i = 1, 2, \ldots, (q-3)/2, \\
w_{0,j} = (1 - \zeta_{pq})^{\tau_j}, \quad j = 0, 1, \ldots, (p-3)/2, \\
w_{i,j} = (1 - \zeta_{pq})^{\sigma_i \tau_j}, \quad i = 1, 2, \ldots, (q-3)/2, \quad j = 0, 1, \ldots, p-3.
\end{align*}
\]

Then

\[
\varepsilon_1^{\sigma} = \prod_{i=0}^{(q-5)/4} \prod_{j=0}^{(p-3)/2} \left(\zeta_{pq}^{(pq-1)/2}(1 - \zeta_{pq})\right)^{\sigma i \tau_2 j} = \xi_1 \prod_{i=0}^{(q-5)/4} \prod_{j=0}^{(p-3)/2} w_{2i+1,2j}
\]
for a suitable root of unity $\xi_1$ and

$$\varepsilon_1 = \pm \varepsilon_1^{-\sigma} = \pm \xi_1^{-1} \prod_{i=0}^{(q-5)/4} \prod_{j=0}^{(p-3)/2} w_{2i+1,2j}^{-1},$$

where we have used only elements of the last row of our basis. Similarly we obtain

$$\varepsilon_2 = \xi_2 \prod_{i=1}^{(p-3)/2} u_i^{(-1)^{i+1}}$$

and

$$\varepsilon_3 = \xi_3 \prod_{i=1}^{(q-3)/2} v_i^{(-1)^{i+1}}$$

for suitable roots of unity $\xi_2$ and $\xi_3$, using only elements of the first row and of the second row, respectively. Clearly $\langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$ is of finite index in $C_W(K)$, so for any $\rho \in C_W(K)$ there is a positive integer $n$ such that $\rho^n \in \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$. Hence there are $a_1, a_2, a_3 \in \mathbb{Z}$ such that $\rho^n = \pm \varepsilon_1^{a_1} \varepsilon_2^{a_2} \varepsilon_3^{a_3}$. Using the previous decomposition of $\varepsilon_1, \varepsilon_2, \varepsilon_3$ into the basis elements and the fact that $\rho$ can also be decomposed in this basis, we obtain that $n|a_1, n|a_2$, and $n|a_3$, which gives $\rho \in \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$. So

$$C_W(K) = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$$

and $[C_W(K) : C_S(K)] = 8$.

Sinnott’s index formula gives

$$[E(K) : C_S(K)] = 8h_K,$$

due to the fact that $Q = 1$ and $e^+ = 1$ because $K$ is real, and $(\mathbb{Z}[G] : U) = 1$ due to [S2, Theorem 5.1]. Comparing the indices gives the proposition. $\Box$

3. A comparison of different groups of circular units. In this section we shall compare the groups of circular units defined above. Let $K$ be an abelian field of conductor $m$. We have seen that

$$\begin{align*}
C_W(K) \\
\downarrow \\
C_S(K) \\
\downarrow \\
C_{cl}(K) \\
\downarrow \\
C_{cs}(K)
\end{align*}$$

and Example 2.1 shows that there is no inclusion between $C_{cl}(K)$ and $C_{cs}(K)$ in general. Though we are not able to compute the precise values of indices between these four groups of circular units, we derive at least partial information, namely we show which primes could be divisors of these indices.

By means of the identity (2.1), it is easy to see that for any $\eta \in C_{cl}(K)$ we have $\eta |[\mathbb{Q}(m):K] \in C_S(K)$. Therefore if a prime $\ell$ divides the index $[C_S(K) : C_{cl}(K)]$ then $\ell$ divides $[\mathbb{Q}(m):K] = \varphi(m)/[K : \mathbb{Q}]$. 


Theorem 3.1. Let $\overline{K}$ be the genus field of $K$ in the narrow sense. Let $\ell$ be an odd prime dividing the index $[C_W(K) : C_S(K)]$. Then $\ell \mid [\overline{K} : K]$.

Proof. Let $m = \prod_{i=1}^s p_i^{n_i}$ be the prime decomposition of the conductor of $K$. Since $\overline{K}$ is the maximal abelian field having the same ramification indices over $\mathbb{Q}$ as $K$, [W, Theorem 3.5] implies that $\overline{K} = \prod_{i=1}^s T_i$ for suitable $T_i \subseteq \mathbb{Q}(p_i^{n_i})$. Let $R_i$ be the maximal subfield of $\mathbb{Q}(p_i^{n_i})$ such that $[R_i : \mathbb{Q}]$ is a power of 2. Then $R_i$ is imaginary and

$$L = \overline{K} \prod_{i=1}^s R_i = \prod_{i=1}^s (T_iR_i)$$

is a compositum of imaginary abelian fields, each of them being ramified only at one finite prime. This means that $L$ satisfies the conditions of [K4], so the Proposition of [K4] gives $C_W(L) = C_S(L)$. Since $C_W(K) \subseteq C_W(L)$, we have

$$(C_W(K))^{[L : K]} = N_{L/K}(C_W(L)) \subseteq N_{L/K}(C_W(L)) = N_{L/K}(C_S(L)) \subseteq C_S(K).$$

Therefore $\ell \mid [C_W(K) : C_S(K)]$ implies $\ell \mid [L : K] = [L : \overline{K}] \cdot [\overline{K} : K]$. Since $[L : \overline{K}]$ is a power of 2, the theorem follows.

Corollary 3.2. If $\ell$ is an odd prime dividing the index $[C_W(K) : C_S(K)]$, then $\ell \mid [K : \mathbb{Q}]$.

Proof. Using the notation of the previous theorem, the mentioned Theorem 3.5 of [W] implies that $[T_i : \mathbb{Q}]$ is equal to the ramification index of $p_i$ in $K/\mathbb{Q}$, so $[T_i : \mathbb{Q}] \mid [K : \mathbb{Q}]$. Therefore $[\overline{K} : \mathbb{Q}] = \prod_{i=1}^s [T_i : \mathbb{Q}] \mid [K : \mathbb{Q}]^s$. Since $[\overline{K} : K] \mid [\overline{K} : \mathbb{Q}]$ and $\ell \mid [\overline{K} : K]$, we have $\ell \mid [K : \mathbb{Q}]$.

Theorem 3.3. Let $\ell$ be a prime dividing the index $[C_S(K) : C_{cs}(K)]$. Then $\ell \mid [K : \mathbb{Q}]$.

Proof. Let $n = [K : \mathbb{Q}]$ and $\eta \in C_S(K)$. The theorem will be proved if we show that $\eta^n \in C_{cs}(K)$. Let $G = \text{Gal}(K/\mathbb{Q})$ and $X$ be the group of characters of $G$. For any $\chi \in X$ let

$$e_\chi = \frac{1}{n} \sum_{\sigma \in G} \chi(\sigma)^{-1} \in \mathbb{C}[G]$$

be the corresponding idempotent and let $\mathbb{Q}(\chi)$ be the field generated by the values of $\chi$. For any $\tau \in \text{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ we can consider the conjugate $\chi^\tau$ of the character $\chi$ defined by $\chi^\tau(\sigma) = (\chi(\sigma))^\tau$. It is easy to see that the relation “to be the conjugate of” is an equivalence relation on $X$, and that two characters in $X$ are conjugate if and only if they have the same kernel. For any class $T$ of conjugate characters, we denote the common kernel of $\chi \in T$ by $\ker T$ and we define $e_T = \sum_{\chi \in T} e_\chi$. It is easy to see that $e_T \in \mathbb{Q}[G]$ and that for any $\sigma \in \ker T$ we have $\sigma e_T = e_T$. So there is $r_T \in \mathbb{Z}[G]$ such that $n e_T = r_T r_T^* e_T$, where $s_T = \sum_{\sigma \in \ker T} \sigma$.

We need to show that $\eta^n \in C_{cs}(K)$. Let us recall that $L$ means the set of all cyclic subfields $L \neq \mathbb{Q}$ of $K$ and $f_L$ is the conductor of $L \in L$. Since $N_{\mathbb{Q}(\ell/L)}(1 - \zeta_{f_L}^a)$ is a unit if $f_L$ is not a prime power and is a $p$-unit whose absolute norm is equal to $p$ if $f_L$ is a power of a prime $p$, it is easy to prove that $C_{cs}(K) = D \cap E(K)$, where

$$D = \langle \pm N_{\mathbb{Q}(f_L/L)}(1 - \zeta_{f_L}^a) ; \ L \in L, a \in \mathbb{Z}, (a, f_L) = 1 \rangle \cup \{p; p|m\}.$$
We know $\eta \in E(K)$. Moreover, due to the definition of $C_S(K)$, $\eta$ is a multiplicative combination of Galois conjugations of $N_{Q(r)/Q(r)\cap K}(1 - \zeta_r)$, where $r > 1$ is a divisor of the conductor $m$ of $K$. So the theorem will be proved if we show that $N_{Q(r)/Q(r)\cap K}(1 - \zeta_r)^n \in D$.

The well-known identity $\sum_{\chi \in \chi} e_\chi = 1$ gives $n = \sum_T n_{eT} = \sum_T r_{T/sT},$ where $T$ runs over all classes of conjugate characters. Hence it is enough to show that for any class $T$ we have $N_{Q(r)/Q(r)\cap K}(1 - \zeta_r)^{sT} \in D$.

Let $T$ be a fixed class containing a character $\chi$ and let $M$ be the subfield of $K$ corresponding to $\ker T$. Since $\Gal(M/Q) \cong G/\ker T \cong \chi(G)$, it is easy to see that $M$ is a cyclic subfield of $K$. Moreover, we have $\alpha^{sT} = N_{K/M}(\alpha)$ for any $\alpha \in K$. So it is enough to show that $N_{K/M}(N_{Q(r)/Q(r)\cap K}(1 - \zeta_r)) \in D$. But the following diagram of fields

\[
\begin{array}{ccc}
\mathbb{Q}(r) & \xrightarrow{f} & \mathbb{Q}(r) \\
\downarrow & & \downarrow \\
M(\mathbb{Q}(r)\cap K) & \xrightarrow{f} & M(\mathbb{Q}(r)\cap K) \\
\downarrow & & \downarrow \\
\mathbb{Q}(r)\cap K & \xrightarrow{f} & \mathbb{Q}(r)\cap K \\
\downarrow & & \downarrow \\
M & \xrightarrow{f} & M \\
\end{array}
\]

gives that

$$N_{K/M}(N_{Q(r)/Q(r)\cap K}(1 - \zeta_r)) = N_{Q(r)/Q(r)\cap M}(1 - \zeta_r)^{[K:M(\mathbb{Q}(r)\cap K)]}.$$ 

If $\mathbb{Q}(r)\cap M = \mathbb{Q}$ then $N_{Q(r)/Q(r)\cap M}(1 - \zeta_r)$ is equal to 1 if $r$ is not a prime power and is equal to $p$ if $r$ is a power of a prime $p$. If $\mathbb{Q}(r)\cap M \neq \mathbb{Q}$ then $L = \mathbb{Q}(r)\cap M \in \mathcal{L}$ and the norm relations (2.3) give

$$N_{Q(r)/Q(r)\cap M}(1 - \zeta_r) = N_{Q(f_L)/L}(N_{Q(r)/Q(f_L)}(1 - \zeta_r))$$

$$= N_{Q(f_L)/L}(1 - \zeta_{f_L})^{\prod_p (1 - \frac{1}{\text{Frob}(p)^{1}})} \in D,$$

where the product is taken over all primes $p \mid r, p \nmid f_L$. The theorem is proved. \qed

4. **Annihilators of the class group of a real abelian field.** Let $K$ be a real abelian field, $p$ be an odd prime such that $p \nmid [K : \mathbb{Q}]$ and $G = \Gal(K/\mathbb{Q})$. Sinnott’s index formula (2.2) shows that there are some similarities between two finite groups: the class group $\text{Cl}(K)$ of $K$ and the quotient group $E(K)/C_S(K)$. More precisely, (2.2) gives that the $p$-Sylow subgroups of the mentioned groups are of the same order:

$$|\text{Cl}(K)_p| = |(E(K)/C_S(K))_p|.$$
Lemma 15.3] to cover the case minor imperfection can be easily repaired: it is not difficult to modify the proof of [W, Theorem 15.2] is weaker than Theorems 4.3 and 4.4 since, as Example 2.1 shows, (E(K)/C_S(K))_p is only a quotient group of (E(K)/C_{cl}(K))_p in general. But this minor imperfection can be easily repaired: it is not difficult to modify the proof of [W, Theorem 15.2] to cover the case δ ∈ C_S(K) instead of the used special case δ ∈ C_{cl}(K).

Thaine’s method has been generalized by K. Rubin in [R1], where he considers any abelian extension of number fields (instead of an abelian extension of Q) and any prime p (allowing p to divide the degree of the extension). To make the exposition easier we state his results only for the special case of a real abelian field K.

Example 4.1. If K = Q(√62501) and p = 3, then we have Cl(K)_p ≅ (Z/3Z)^2 while (E(K)/C_S(K))_p ≅ Z/9Z.

Corollary 3.2 shows

(E(K)/C_S(K))_p ≅ (E(K)/C_{W}(K))_p,

and Theorem 3.3 gives

(E(K)/C_S(K))_p ≅ (E(K)/C_{cs}(K))_p,

so it is not important which of these three groups of circular units we are considering.

A common algebraic property of Cl(K)_p and (E(K)/C_S(K))_p has been formulated by G. Gras in his conjecture:

Conjecture 4.2. Let K be a real abelian field, and let p be an odd prime such that p∤[K : Q]. Then the Z_p[G]-modules Cl(K)_p and (E(K)/C_{cs}(K))_p have isomorphic Jordan-Hölder series.

An important step in this direction has been made in 1977 by R. Greenberg who proved in [Gb] that the Main Conjecture of Iwasawa theory implies Conjecture 4.2. Therefore the proof of the Main Conjecture, given in 1984 by B. Mazur and A. Wiles [MW], is also a proof of Conjecture 4.2. These deep results have been obtained by extremely difficult techniques from algebraic geometry.

An astonishing turnaround appeared in 1988 when F. Thaine gave in [T] a very much simpler proof of the following corollary of Conjecture 4.2:

Theorem 4.3. Let K be a real abelian field, and let p be an odd prime such that p∤[K : Q]. If θ ∈ Z_p[G] annihilates (E(K)/C_S(K))_p, then θ also annihilates Cl(K)_p.

More precisely, Thaine proved more since his theorem covers also the case of p = 2:

Theorem 4.4. Let K be a real abelian field of odd degree [K : Q]. If θ ∈ Z_2[G] annihilates (E(K)/C_S(K))_2, then 2θ annihilates Cl(K)_2.

A nice exposition of Thaine’s proof of Theorems 4.3 and 4.4 can be found in [W, §15.2]. (Attention: Washington uses the group C_{cl}(K) instead of C_S(K) here, so [W, Theorem 15.2] is weaker than Theorems 4.3 and 4.4 since, as Example 2.1 shows, (E(K)/C_S(K))_p is only a quotient group of (E(K)/C_{cl}(K))_p in general. But this minor imperfection can be easily repaired: it is not difficult to modify the proof of [W, Lemma 15.3] to cover the case δ ∈ C_S(K) instead of the used special case δ ∈ C_{cl}(K).)
Let $\mathcal{S}$ be the set of all odd primes which split completely in $K$. For any $q \in \mathcal{S}$, let $K_q = K(\zeta_q + \zeta_q^{-1})$ and let $\mathcal{C}(q)$ be the set of all $\varepsilon \in K^\times$ such that there exists $\eta \in E(K_q)$ which satisfies the congruence $\eta \equiv \varepsilon^2 (\mod (1 - \zeta_q)(1 - \zeta_q^{-1}))$ and whose norm is $N_{K_q/K}(\eta) = 1$. The group of Rubin’s special numbers of $K$ is defined as

$$\mathcal{C} = \{\varepsilon \in K^\times; \varepsilon \in \mathcal{C}(q) \text{ for almost all } q \in \mathcal{S}\}.$$ 

Let $N$ be a power of a prime $p$, large enough to kill $\text{Cl}(K)_p$, and let $V$ be a finitely generated submodule of the $\mathbb{Z}[G]$-module $K^\times/(K^\times)^N$. Let $\alpha : V \to (\mathbb{Z}/N\mathbb{Z})[G]$ be a $\mathbb{Z}[G]$-module homomorphism. Let $H$ denote the Hilbert $p$-class field of $K$, i.e., $H$ is the maximal unramified abelian $p$-extension of $K$. Then the Artin map gives an isomorphism between the $\mathbb{Z}[G]$-modules $\text{Gal}(H/K)$ and $\text{Cl}(K)_p$, where $G$ acts on $\text{Gal}(H/K)$ via conjugation. Let $H' = H \cap K(\zeta_N)$. In [R1] Rubin proves the following theorem:

**Theorem 4.5.** The element $\alpha(\varepsilon)$ annihilates $\text{Gal}(H/H')$ for any $\varepsilon \in \mathcal{C}$.

This theorem does not give an annihilator of $\text{Cl}(K)_p \cong \text{Gal}(H/K)$ but only an annihilator of its submodule $\text{Gal}(H/H')$. But we have control on their quotient $\text{Gal}(H'/K)$, because $H'$ can be computed without knowledge of $H$: $H'$ is the maximal subextension of $K(\zeta_N)/K$ unramified over $K$. For example, if $p$ is not ramified in $K$ then we have $H' = K$. Concerning Rubin’s special numbers, we have $\mathcal{C}_S(K) \subseteq \mathcal{C}$ but, in general, $\mathcal{C}_W(K) \not\subseteq \mathcal{C}$.

Another important further step has been made by V. Kolyvagin who discovered how Thaine’s method can be strengthened and introduced what he called “Euler systems.” Roughly speaking, Thaine’s method is just the first step in Kolyvagin’s inductive procedure and the advantage of an Euler system is that it allows to bound not only the exponents of the eigenspaces of $\text{Cl}(K)_p$ but also to bound their orders, so it gives not only a proof of Theorems 4.3 and 4.4 but also a proof of Conjecture 4.2. A very nice introduction to Euler systems is in [R2], where the Main Conjecture for the $p$th cyclotomic field $\mathbb{Q}(\zeta_p)$ is proved. The Main Conjecture for all abelian fields including the case $p = 2$ was proven in [Gr] by C. Greither using these techniques. The recent monograph [R3] of Rubin on Euler systems is written from a more general point of view and is meant for a more advanced reader.

Theorems 4.3 and 4.4 cover only the case of a prime $p$ which does not divide the degree of the field $K$. The primes dividing the degree are covered by Theorem 4.5 but the input of Theorem 4.5 is not an annihilator of a quotient of $E(K)$ but a $\mathbb{Z}[G]$-module homomorphism $\alpha$. Therefore natural questions appear for a prime $p$ which divides the degree: how can the annihilators of $\text{Cl}(K)_p$ and the annihilators of $(E(K)/\mathcal{C}_S(K))_p$ be compared? Moreover, in general, these two modules are not of the same order, so can one change them to get some interesting modules that have the same order? These questions were a starting point of joint research with C. Greither. In [GrK] we studied the easiest possible case of this situation, which is described in the following section.

**5. Annihilators of the class group of some cyclic abelian fields.** Let $p$ be an odd prime and $\ell = p^k$ be a given power. Let $K$ be an abelian field of degree $[K : \mathbb{Q}] = \ell$ with cyclic Galois group $G = \text{Gal}(K/\mathbb{Q})$. We want to study the $p$-Sylow subgroup
Cl(K)\_p of the class group of K. Let p_1, \ldots, p_s be all primes which ramify in K/Q. We assume the following hypothesis:

Assumption 5.1. Each p_i ramifies totally and tamely in K/Q and s > 1.

In fact, the assumption s > 1 is quite natural since Cl(K)\_p is trivial if s = 1. The essential part of Assumption 5.1 is that each ramifying prime ramifies totally and tamely.

Assumption 5.1 gives that p_1 \equiv \cdots \equiv p_s \equiv 1 \pmod{\ell} and that m = p_1 \cdots p_s is the conductor of K. For each i = 1, \ldots, s, let K_i be the unique subfield of the p_i-th cyclotomic field \( \mathbb{Q}^{(p_i)} \) of degree \([K_i : \mathbb{Q}] = \ell\). Then the genus field of K is \( \overline{K} = \prod_{i=1}^{s} K_i \). Let us choose and fix a generator \( \sigma \) of \( G \) and for each \( i = 1, \ldots, s \) let \( \sigma_i \in \text{Gal}(\overline{K}/\mathbb{Q}) \) be determined by the conditions \( \sigma_i|_{K} = \sigma \) and \( \sigma_i|_{K_j} = 1 \) for each \( j \neq i \). We define an \( s \times s \) matrix \( A = (a_{ij}) \) over \( \mathbb{Z}/\ell\mathbb{Z} \) as follows: if \( i \neq j \) then \( a_{ij} = -1 \), otherwise \( a_{ii} = -\sum_{j \neq i} a_{ij} \).

Assumption 5.1 implies that \( C_S(K) = C_{cs}(K) \) is the \( \mathbb{Z}[G] \)-module \((\mathbb{Z}^l)^{s}\langle -\eta \rangle \) generated by \(-\eta\), where \( \eta = N_{Q_m/K}(1 - \zeta_m) \). Sinnott’s index formula (2.2) gives

\[
[E(K) : C_S(K)] = \ell^{-1} h_K
\]

since \((\mathbb{Z}[G] : U) = 1\) due to the cyclicity of \( K \) (see [S2, Theorem 5.3]). This implies that \( \ell \) divides the class number \( h_K \) but genus theory gives even more: \( \ell^{s-1} | h_K \). With the use of class field theory, this can be seen as follows: let \( H \) be the Hilbert \( p \)-class field of \( K \) so \( \text{Gal}(H/K) \cong Cl(K)_p \) via the Artin map. Since the genus field \( \overline{K} \) is the maximal unramified extension of \( K \) which is abelian over \( \mathbb{Q} \) and in our case is a \( p \)-extension of \( K \), we have \( \overline{K} \subseteq H \), which means

\[
\ell^{s-1} = [\overline{K} : K] | [H : K] = |Cl(K)_p|,
\]

the \( p \)th part of \( h_K \). For any field \( L \) such that \( K \subseteq L \subseteq H \), we have that \( L \) is abelian over \( \mathbb{Q} \) if and only if \( G \) acts trivially on \( \text{Gal}(L/K) \), which is the case if and only if \( \sigma \) acts trivially on \( \text{Gal}(L/K) \). Therefore \( \text{Gal}(H/\overline{K}) \) is the minimal subgroup of \( \text{Gal}(H/K) \) whose quotient in \( \text{Gal}(H/\overline{K}) \) has trivial action of \( \sigma \), which means

\[
\text{Gal}(H/\overline{K}) = (\sigma - 1) \text{Gal}(H/K) \cong (\sigma - 1) Cl(K)_p.
\]

So we call \((\sigma - 1) Cl(K)_p\) the non-genus part of \( Cl(K)_p \). Since we have a good understanding of \( \text{Gal}(\overline{K}/K) \), it is precisely \((\sigma - 1) Cl(K)_p\) which we want to study.

If \( s > 2 \) then the divisibility relation \( \ell^{s-1} | h_K = \ell \cdot [E(K) : C_S(K)] \) means that there are units in \( E(K) \), not belonging to \( C_S(K) \), whose \( p \)th power is in \( C_S(K) \). In [GrK], we have searched for such units in \( \langle 1 - \zeta_m^a ; a \in \mathbb{Z}, m \nmid a \rangle \cap K \) and proved the following result:

Theorem 5.2. There is \( \varepsilon \in K^\times \) which is a unit outside of \( \{p_1, \ldots, p_s\} \) and satisfies

\[
\varepsilon^{(\sigma-1)^{s-1}} = \eta \quad \text{and} \quad N_{K/Q}(\varepsilon) = \prod_{i=1}^{s} p_i^{A_i},
\]
where \( 0 \leq A_i < l \) is a lift of the \((i, i)\)-th minor of \( A \). Moreover, we have \( \varepsilon^{\sigma-1} \in C_W(K) \) and

\[
|\left( E(K) / \langle \varepsilon^{\sigma-1} \rangle_p \right) G_p | = |(\sigma - 1) Cl(K)_p |,
\]

where \( \langle \varepsilon^{\sigma-1} \rangle_G \) means the \( \mathbb{Z}[G] \)-module generated by \( \varepsilon^{\sigma-1} \).

Therefore \( \langle \varepsilon^{\sigma-1} \rangle_G \) is a submodule of \( C_W(K) \) but the opposite inclusion does not hold true in general: if all \( A_i \)'s are zero then \( \varepsilon \in C_W(K) \) but \( \varepsilon \not\in \langle \varepsilon^{\sigma-1} \rangle_G \).

Similarly to the situation of Theorem 4.3, we have two \( \mathbb{Z}_p[G] \)-modules of the same cardinality, so the question is whether they have some common algebraic properties. An answer is given by the following theorem:

**Theorem 5.3.** If \( \theta \in \mathbb{Z}_p[G] \) annihilates \( \left( E(K) / \langle \varepsilon^{\sigma-1} \rangle_p \right)_G \), then \( \theta \) also annihilates \( (\sigma - 1) Cl(K)_p \).

Theorem 5.3 has been proved by a modification of methods of Rubin. Since \( \varepsilon \) is not a special number in Rubin’s sense, it was necessary to introduce a new weakened version of specialness and to show that the standard machinery of Thaine and Rubin can be adapted to this change.
la seule possibilité pour obtenir une descente galoisienne. Ce groupe de Washington contient les trois autres groupes discutés ci-dessus, mais ne jouit pas des autres bonnes propriétés : nous ne connaissons pas de générateurs explicites et nous n’avons pas de formule pour l’indice.

La troisième section est consacrée à l’étude des indices relatifs de ces quatre groupes d’unités circulaires. Bien que nous ne soyons pas capables de calculer précisément ces valeurs, nous avons au moins des informations partielles, c’est-à-dire que nous montrons quels premiers peuvent diviser ces indices.

Dans la quatrième section, nous fixons un corps réel abélien \( K \) et un nombre premier \( p \), et nous comparons deux modules galoisiens apparaissant naturellement : la \( p \)-partie du groupe de toutes les unités modulo le groupe des unités circulaires, et la \( p \)-partie du groupe de classes de \( K \). Si nous supposons que \( p \) ne divise pas le degré absolu de \( K \), il n’est pas important de choisir le groupe de Sinnott, le groupe du niveau conducteur ou le groupe des sous-corps cycliques, vu que les trois groupes produisent à isomorphismes près les mêmes \( p \)-parties pour le quotient. Considérons maintenant ce module fini et la \( p \)-partie du groupe de classes. Ils ont les mêmes ordres, mais en général ils ne sont pas isomorphes. Le théorème de Thaine affirme que tout annulateur du premier module est un annulateur du second (sous l’hypothèse que \( p \) est impair et copremier au degré du corps). L’approche de Thaine a été généralisée par Rubin qui ne suppose plus que \( p \) est copremier au degré du corps (et qui considère un corps de nombres quelconque comme corps de base au lieu de \( \mathbb{Q} \)). Cependant, Rubin construit des annulateurs du groupe de classes qui ne proviennent pas d’annulateurs du groupe quotient d’unités, mais plutôt à partir d’un homomorphisme convenable de modules : les annulateurs sont leurs valeurs en des unités spéciales.

Dans la dernière section, nous décrivons un cas très particulier de la situation précédente non couvert par le théorème de Thaine; nous supposons que \( K \) est un corps cyclique dont le degré absolu est une puissance de \( p \) et dont les premiers ramifiés se ramifient totalement ou modérément. Pour ce type de corps de nombres, on peut construire au moyen de générateurs explicites un autre groupe d’unités circulaires. Ce dernier groupe est encore un sous-groupe du groupe des unités circulaires de Washington mais il contient strictement le groupe de Sinnott. Si nous considérons la \( p \)-partie du groupe de toutes les unités du corps modulo ce dernier groupe d’unités, alors l’ordre de ce quotient est le même que celui de la partie du groupe de classes correspondant à la partie non-genre (« non-genus part »). De plus, comme dans le théorème de Thaine, nous avons que tout annulateur du premier module est un annulatur du second.

Acknowledgements. The author wants to thank both the organizers of the conference for their support during the conference and the Grant Agency of the Czech Republic for the grant 201/01/0471. The author is grateful to T. Metsänkylä for very useful discussions which helped to improve this text.

REFERENCES

Circular units and class groups of abelian fields


R. Kučera
Department of Mathematics
Faculty of Science
Masaryk University
Janáčkovo nám. 2A
602 00 Brno, Czech Republic.
E-mail: kucera@math.muni.cz