Akademie věd České republiky

Teze doktorské disertační práce
k získání vědeckého titulu „doktor věd“
ve skupině věd fyzikálně-matematických

A study of class groups of abelian fields by means of circular units

(Studium grupy tříd ideálů abelovských
těles pomocí kruhových jednotek)

Komise pro obhajoby doktorských disertací v oboru
„Matematické struktury“

Radan Kučera

Přírodovědecká fakulta Masarykovy Univerzity v Brně

Brno, 29. února 2004

Resumé

Při řešení diofantických rovnic bývá někdy užitečné rozšířit obor celých čísel, v němž hledáme řešení, a to na okruh všech celých algebraických čísel v nějakém konečném rozšíření tělesa racionálních čísel. To však má za následek, že ztrácíme jednoznačný rozklad na součin ireducibilních prvků, neboť uvažovaný okruh už nemusí být okruhem s jednoznačným rozkladem. Naštěstí však jde o Dedekindův okruh, takže jeho libovolný nenulový ideál lze zapsat jako součin prvoideálů, a to jednoznačně až na pořadí. Díky tomu lze často úvahy prováděné v okruzích s jednoznačným rozkladem provést i zde: místo prvků rozkládáme hlavní ideály jimi generované. Problémem však je, že přejít od součinu ideálů zpět k součinu prvků lze jen tehdy, jde-li o hlavní ideály. Proto je tedy nutné mít přehled o tom, které z ideálů jsou hlavní. Faktorizací pologrupy všech nenulových ideálů podle podpologrupy těch hlavních vzniká tzv. grupa tříd ideálů, což je konečná grupa. Znalost její struktury v některých případech umožňuje danou diofantickou rovnici vyřešit. Popsat grupu tříd ideálů nebo alespoň její řád – počet tříd ideálů – je však obtížný úkol, proto jakékoli i částečné informace jsou cenné.

Ve speciálním případě, kdy uvažované konečné rozšíření tělesa racionálních čísel je abelovské, tj. Galoisovo s komutativní Galoisovou grupou, je možné v grupě všech jednotek okruhu celých algebraických čísel definovat podgrupu tzv. kruhových jednotek. Ukazuje se, že existují jisté hluboké souvislosti mezi grupou tříd ideálů na jedné straně a faktorgrupou grupy všech jednotek podle podgrupy těch kruhových na straně druhé.

Těmto souvislostem je právě věnována tato doktorská disertační práce, jejímž jádrem je soubor devíti uveřejněných vědeckých prací. Tento soubor je doplněn komentářem, který je psán jako přehledný výklad o kruhových jednotkách a jejich využití při zkoumání grupy tříd ideálů abelovského tělesa. Proto je možné práci použít jako úvod do problematiky kruhových jednotek, jehož cílem je provést čtenáře od úvodních definic až po pokročilé partie, kdy se na grupu tříd ideálů i na faktorgrupu jednotek díváme jako na Galoisovy moduly a porovnáváme anihilátory těchto modulů. Stojí za zmínku, že tato velmi abstraktní teorie má své konkrétní výsledky: Thaineova věta (v disertaci uvedena jako Theorem 8a) hraje klíčovou roli v nedávném Mihăilescově důkaze Catalanovy hypotézy, která tvrdí, že 8 a 9 jsou jediná dvě po sobě jdoucí přirozená čísla, která jsou obě alespoň druhou mocninou nějakého přirozeného čísla.

Poslední kapitola disertace naznačuje další zobecnění: Starkova hypotéza, zhruba řečeno, předpokládá, že jednotky analogické kruhovým jednotkám by měly existovat pro abelovské rozšíření libovolného číselného tělesa, nejen tělesa racionálních čísel (kromě racionálních čísel, kde jde právě o kruhové

jednotky, jsou zatím známy jen tzv. eliptické jednotky pro imaginární kvadratická tělesa). Chinburgova hypotéza pak doplňuje v této situaci vztah mezi grupou tříd ideálů a grupou jednotek. Zesílenou variantou této hypotézy je tzv. „lifted root number conjecture“, jejíž důkaz ve speciálním případě cyklického rozšíření racionálních čísel lichého prvočíselného stupně, provedený pomocí kruhových jednotek, obsahuje disertace v přiloženém článku [**8**].

Introduction

The dissertation thesis consists of the set of nine published research papers [**1**-**9**] and of the annotation, which is written as an exposition on circular units. The following text is a reduced variant of this exposition. To make it more reader-friendly, some examples and statements are included though they have not been published yet (for example Theorems 3 or 5), so due to the rules of the Academy of Sciences of the Czech Republic these results cannot be considered as a part of the thesis. To clearly indicate which results form the thesis they are numbered by roman numbers (Theorems I to XV) instead of arabic ones.

In accordance with the rules of the Academy of Sciences of the Czech Republic, the list of the most important author's papers having a relation to the investigated problems is embodied in the thesis. This list can be found on page **??**; it contains the included papers [**1**–**9**] and six other papers [10–15].

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 be a positive integer and ζ_n be a primitive nth root of unity, e.g. $\zeta_n = e^{2\pi i/n}$. Let $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta_n)$ be the nth cyclotomic field. Since $\mathbb{Q}^{(2n)} = \mathbb{Q}^{(n)}$ for an odd n, we can suppose that $n \not\equiv 2 \pmod 4$. We know that the ring of algebraic integers of $\mathbb{Q}^{(n)}$ is equal to $\mathbb{Z}[\zeta_n]$ and Dirichlet's unit theorem gives the structure of the group $E(\mathbb{Q}^{(n)})$ of units of $\mathbb{Z}[\zeta_n]$: it is isomorphic to the product of its torsion subgroup with $\frac{1}{2}\varphi(n)-1$ copies of $\mathbb{Z}$. Moreover the torsion part $E(\mathbb{Q}^{(n)})_{\rm tor}$ is the cyclic group $\langle -1, \zeta_n\rangle$ having $2n$ or n elements depending whether n is odd or even. But we do not know an explicit system of generators of the whole group $E(\mathbb{Q}^{(n)})$. 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 $\mathbb{Q}^{(n)}$ explicitly, for example, $1-\zeta_n^a \in E(\mathbb{Q}^{(n)})$ for any integer a such that $n \nmid a$ and $\frac{n}{(a,n)}$ is not a prime power. Moreover a's with $\frac{n}{(a,n)}$ being a prime power can be also used to produce units: $\frac{1-\zeta_n^a}{1-\zeta_n^b} \in E(\mathbb{Q}^{(n)})$ 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 $C(\mathbb{Q}^{(n)})$ of $\mathbb{Q}^{(n)}$. It is easy to show that this group can be defined also by the intersection

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

where $\langle\ldots\rangle$ means generating in the multiplicative group $\mathbb{Q}^{(n)\times}$. Let us mention that $-\zeta_n = \frac{1-\zeta_n}{1-\zeta_n^{-1}} \in C(\mathbb{Q}^{(n)})$ and so $E(\mathbb{Q}^{(n)})_{\rm tor} \subseteq C(\mathbb{Q}^{(n)})$.

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 [43] 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 is given explicitly by 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 $C(\mathbb{Q}^{(n)})/C(\mathbb{Q}^{(n)})_{\rm tor}$, such a basis is, for example, the set

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

and the index formula can be obtained in this case just by computing the regulator of this basis (see [46, pp. 143-146]). The general case is much more complicated since the relations among the generators of the group

$$U_n = \langle 1 - \zeta_n^a;\, a = 1, \ldots, n-1 \rangle$$

are more and more difficult with the increasing number of prime divisors of n. It is easy to prove that the torsion part $(U_n)_{\mathrm{tor}}$ of U_n equals to the cyclic group $\langle -1, \zeta_n \rangle$ and that the generators of U_n satisfy the following relations:

$$\begin{aligned} 1 - \zeta_n^{n-a} &= -\zeta_n^{-a}(1 - \zeta_n^a) && \text{for any } a = 1, \ldots, n-1, \\ 1 - \zeta_n^{ma} &= \prod_{i=0}^{m-1} (1 - \zeta_n^{a+i(n/m)}) && \text{for any } m|n \text{ and any } a = 1, \ldots, \frac{n}{m} - 1. \end{aligned}$$

Let A_n be the free abelian group generated by $n-1$ independent generators e_a, where $a = 1, \ldots, n-1$. Let B_n be its subgroup of relations of even distribution, i.e. the subgroup generated by the following elements

$$\begin{aligned} & e_{n-a} - e_a && \text{for any } a = 1, \ldots, n-1, \\ & e_{ma} - \sum_{i=0}^{m-1} e_{a+i(n/m)} && \text{for any } m|n \text{ and any } a = 1, \ldots, \frac{n}{m} - 1. \end{aligned}$$

So we have a surjective homomorphism $A_n/B_n \to U_n/(U_n)_{\mathrm{tor}}$. If we take $e_{n-a} + e_a$ instead of $e_{n-a} - e_a$ in the definition of B_n, we obtain the subgroup of relations of odd distribution B_n'. These odd distribution relations are satisfied by Gauss sums (or by generators of Stickelberger ideal). The distribution relations are also called Davenport-Hasse relations due to the paper [25]. These relations appear in number theory also in other connections and there is quite a rich literature concerning them. Already in the 60s H. Hasse (in [33]) and J. Milnor (unpublished, mentioned in [16]) posed a question whether all relations satisfied by circular numbers $1 - \zeta_n^a$ and by Gauss sums (modulo its torsional subgroups) belong to the group B_n and B_n', respectively. In 1966 in [16] H. Bass gave a proof of this fact for circular numbers, but in 1972 in [26] V. Ennola showed that Bass overlooked that there are problems with 2-torsion, for example if $n = 105$ then the quotient group A_n/B_n has a nontrivial 2-torsion. In 1975 K. Yamamoto studied the problem for Gauss sums in [47] where he finds the correct description of the torsional part of A_n/B_n' but there is a gap in his proof of the key lemma. In 1980 C.-G. Schmidt proved that for any positive integer n both $(A_n/B_n)_{\mathrm{tor}}$ and $(A_n/B_n')_{\mathrm{tor}}$ are elementary 2-groups and found their order using cohomology of groups. Finally in 1989 in [27] R. Gold and J. Kim used

the mentioned result of Schmidt to construct a $\mathbb{Z}$-basis of $C(\mathbb{Q}^{(n)})$. But their proof contains a gap concerning 2-torsion. Independently, the author of this thesis has obtained $\mathbb{Z}$-bases of $C(\mathbb{Q}^{(n)})$ and of the Stickelberger ideal of the n-th cyclotomic field. The summary of these results was published in 1989 in [10] and the papers containing complete proofs appeared in 1992: $\mathbb{Z}$-bases of general odd and even distributions, a special case of them being A_n/B_n and A_n/B'_n, are constructed in [**1**], while [**2**] uses the results of [**1**] to give the mentioned $\mathbb{Z}$-bases of $C(\mathbb{Q}^{(n)})$ and of the Stickelberger ideal. This construction is described by the following

Theorem I. ([**2**, Theorem 6.1]) Let $n \not\equiv 2 \pmod 4$ and let $n = p_1^{r_1} \dots p_s^{r_s}$ be the prime decomposition of n (so $p_1, \dots, p_s$ are different primes, $r_1, \dots, r_s$ are positive integers). We put $q_i = p_i^{r_i}$ and we define

$$\begin{aligned}
X &= \{a \in \mathbb{Z};\, 0 < a < n,\, \forall i \in \{1, \dots, s\} : (p_i | a \implies q_i | a)\},\\
N_1 &= \big\{a \in X \cup \{0\};\, (a = 0 \text{ or } a \mid n),\, 2 \nmid \#\{k \in \{1, \dots, s\};\, q_k \nmid a\}\big\},\\
N_2 &= \big\{a \in X;\, \exists i \in \{1, \dots, s\}\colon (q_i \nmid a,\, \tfrac{a}{(n,a)} \equiv -1 \pmod{q_i})\big\},\\
N_3 &= \bigcup_{k=1}^{s} \big\{a \in X;\, q_k \nmid a,\, \langle \tfrac{a}{q_k(n,a)} \rangle > \tfrac{1}{2},\\
&\qquad\qquad \forall i \in \{k{+}1, \dots, s\}\colon a \equiv (n, a) \pmod{q_i}\big\},
\end{aligned}$$

and finally

$$M = X - (N_1 \cup N_2 \cup N_3).$$

For any $a \in X$ we put

$$v_a = \begin{cases} \frac{1-\zeta_n^a}{1-\zeta_n^{n/q_i}} & \text{if there is } i \in \{1, \dots, s\} \text{ such that } n | a q_i,\\ 1 - \zeta_n^a & \text{otherwise.} \end{cases}$$

Then the set $\{v_a;\, a \in M\}$ forms a $\mathbb{Z}$-basis of $C(\mathbb{Q}^{(n)})$. □

This construction is rather technical but the independent construction of Gold and Kim has similar features, so it seems that there is no easier description of a $\mathbb{Z}$-basis of $C(\mathbb{Q}^{(n)})$. Nevertheless Gold and 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

$$C(\mathbb{Q}^{(m)}) = C(\mathbb{Q}^{(n)}) \cap \mathbb{Q}^{(m)} = C(\mathbb{Q}^{(n)})^{\mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}^{(m)})}.$$

Circular units in an abelian field

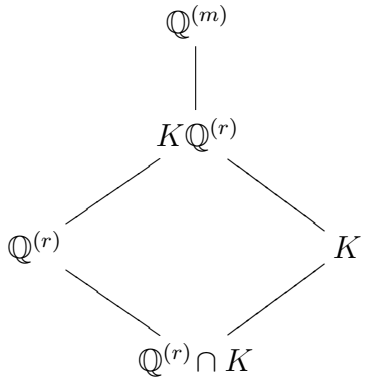
By an abelian field we have in mind a finite Galois extension of $\mathbb{Q}$ whose Galois group is abelian. Due to the Kronecker-Weber theorem we know that any abelian field is a subfield of a cyclotomic field. Let K be an abelian field and let m be the conductor of K (i.e. $\mathbb{Q}^{(m)}$ is the 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

$$C_{\mathrm{cl}}(K) = \langle \pm \mathrm{N}_{\mathbb{Q}^{(m)}/K}(1-\zeta_m^a);\, a \in \mathbb{Z},\, m \nmid a \rangle \cap E(K).$$

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

But consider a generator $\mathrm{N}_{\mathbb{Q}^{(m)}/K}(1-\zeta_m^a)$ 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 $r = \frac{m}{(a,m)}$ and $b = \frac{a}{(a,m)}$. The following diagram of fields



gives that

$$\mathrm{N}_{\mathbb{Q}^{(m)}/K}(1-\zeta_m^a) = \mathrm{N}_{\mathbb{Q}^{(m)}/K}(1-\zeta_r^b) = \mathrm{N}_{\mathbb{Q}^{(r)}/K\cap\mathbb{Q}^{(r)}}(1-\zeta_r^b)^{[\mathbb{Q}^{(m)}:K\mathbb{Q}^{(r)}]}, \qquad (1)$$

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 want to 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 [44] is proven in [36, Proposition 1]). Sinnott group $C_{\mathrm{S}}(K)$ of circular units of K can be defined by the intersection

$$C_{\mathrm{S}}(K) = \langle \pm \mathrm{N}_{\mathbb{Q}^{(r)}/\mathbb{Q}^{(r)}\cap K}(1-\zeta_r^a);\, 1<r \mid m,\, (a,r)=1\rangle \cap E(K). \qquad (2)$$

It is clear that $C_{\mathrm{cl}}(K) \subseteq C_{\mathrm{S}}(K)$. Sinnott proved in [44] that the index of $C_{\mathrm{S}}(K)$ 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 $G = \mathrm{Gal}(K/\mathbb{Q})$ 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 [44, Proposition 2.3]). Sinnott's formula reads

$$[E(K) : C_{\mathrm{S}}(K)] = h_K^+ \, Q \, \frac{\prod_{p|m}[K_p:\mathbb{Q}]}{[K:\mathbb{Q}]} \, 2^{-g} \, (e^+\mathbb{Z}[G] : e^+U) \qquad (3)$$

(see [44, Theorem 4.1]), where $Q \in \{1,2\}$ is Hasse 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, $e^+ = \frac{1+j}{2} \in \mathbb{Q}[G]$ 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 [44, Proposition 4.1]).

The author of this thesis has found out that the problem concerning the unknown g can be overcome by the following slight modification of the definition (**??**) of $C_{\mathrm{S}}(K)$. By an adaptation of Sinnott's computation we obtain

Theorem II. ([**5**, Theorem]) Let P be the set of all rational primes p such that $p \not\equiv 3 \pmod 4$ and $\sqrt{p} \in K$. Let $C'_{\mathrm{S}}(K)$ be defined as

$$\langle \{\sqrt{p};\, p \in P\} \cup \{\pm \mathrm{N}_{\mathbb{Q}^{(r)}/\mathbb{Q}^{(r)}\cap K}(1-\zeta_r^a);\, 1<r \mid m,\, (a,r)=1\}\rangle \cap E(K).$$

Then

$$[E(K) : C'_{\mathrm{S}}(K)] = h_K^+ \, Q \, \frac{\prod_{p|m}[K_p:\mathbb{Q}]}{[K:\mathbb{Q}]} \, 2^{-g'-g''} \, (e^+\mathbb{Z}[G] : e^+U),$$

where g' is the number of primes $p|m$ such that the degree $[K_p:\mathbb{Q}]$ is even and $g'' = 1-[K:\mathbb{Q}]$ if K is real and $g''=0$ if K is imaginary. □

The problem to determine the index $(e^+\mathbb{Z}[G] : e^+U)$ is serious: Sinnott proved in [44, 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 $[\overline{K} : K]$, where $\overline{K}$ is the genus field of K in the narrow sense, and also by 2 if K is imaginary, see [44, 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 [44, Theorem 5.3]); or if K is ramified at most at two finite primes (see [44, Theorem 5.1]); or if the compositum $K\overline{K}_p$ equals $\overline{K}$ for each prime $p|m$, where $\overline{K}_p$ is the maximal subfield of $\overline{K}$ unramified at all finite primes different from p (see [44, Theorem 5.4]); or if K is a compositum of quadratic fields (see Theorem IV in the next section); or if the degree of K is the square of an odd prime (see [35]) etc.

We have seen that, similarly to the case of cyclotomic fields, $C_{\mathrm{S}}(K)$ 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 to get Galois descent, namely to put $C_{\mathrm{W}}(K) = K \cap C(\mathbb{Q}^{(m)})$. It is easy to see that $C_{\mathrm{S}}(K) \subseteq C_{\mathrm{W}}(K)$. Since this definition is mentioned in [46, p. 143], we are calling $C_{\mathrm{W}}(K)$ 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 $[E(K) : C_{\mathrm{W}}(K)]$ which would cover infinitely many abelian fields K with $C_{\mathrm{W}}(K) \neq C_{\mathrm{S}}(K)$ - a formula of this kind for a very special class of abelian fields is given by Proposition 2 below).

The natural question to characterize all abelian fields having the property $C_{\mathrm{S}}(K) = C_{\mathrm{W}}(K)$ is an open problem. The author of the thesis made a small step in this direction by enlarging the class of all cyclotomic fields as follows:

Theorem III. ([**6**, Proposition]) Let K be a compositum of any finite number of imaginary abelian fields, each of them being ramified at one prime. Then $C_{\mathrm{S}}(K) = C_{\mathrm{W}}(K)$. □

There is another definition of circular units which can be found in the literature (see [28, pp. 152-153]). This approach uses cyclic subfields of K and goes back to Hasse (see [32, 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 $\mathcal{L}$ be the set of all cyclic subfields $L \neq \mathbb{Q}$ of K, i.e. of all subfields $L \subseteq K$ whose Galois group $\mathrm{Gal}(L/\mathbb{Q})$ 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

$$C_{\mathrm{cs}}(K) = \langle \pm \mathrm{N}_{\mathbb{Q}^{(f_L)}/L}(1-\zeta_{f_L}^a);\ L \in \mathcal{L},\ a \in \mathbb{Z},\ (a, f_L) = 1 \rangle \cap E(K).$$

Since we have

$$\mathrm{N}_{\mathbb{Q}^{(f_L)}/L}(1-\zeta_{f_L}^a) = \mathrm{N}_{\mathbb{Q}^{(f_L)}\cap K/L}(\mathrm{N}_{\mathbb{Q}^{(f_L)}/\mathbb{Q}^{(f_L)}\cap K}(1-\zeta_{f_L}^a)),$$

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

Example 1. Let us construct 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 $\mathrm{Gal}(\mathbb{Q}^{(221)}/\mathbb{Q}) = \langle \sigma, \tau \rangle$, where $\zeta_{13}^{\sigma} = \zeta_{13}$, $\zeta_{17}^{\sigma} = \zeta_{17}^3$, $\zeta_{13}^{\tau} = \zeta_{13}^2$, and $\zeta_{17}^{\tau} = \zeta_{17}$. We have $\mathrm{Gal}(\mathbb{Q}^{(221)}/K) = \langle \sigma^2, \tau^2 \rangle$, so $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma|_K, \tau|_K, \sigma\tau|_K\}$. Let

$$\begin{aligned}
\eta_1 &= \mathrm{N}_{\mathbb{Q}^{(221)}/K}(1-\zeta_{221}),\\
\eta_2 &= \mathrm{N}_{\mathbb{Q}^{(13)}/\mathbb{Q}(\sqrt{13})}(1-\zeta_{13})^{1-\tau},\\
\eta_3 &= \mathrm{N}_{\mathbb{Q}^{(17)}/\mathbb{Q}(\sqrt{17})}(1-\zeta_{17})^{1-\sigma}.
\end{aligned}$$

Then

$$\begin{aligned}
C_{\mathrm{S}}(K) &= \langle -1, \eta_1, \eta_2, \eta_3 \rangle,\\
C_{\mathrm{cl}}(K) &= \langle -1, \eta_1, \eta_2^8, \eta_3^6 \rangle,\\
C_{\mathrm{cs}}(K) &= \langle -1, \eta_1^2, \eta_2, \eta_3 \rangle,\\
C_{\mathrm{W}}(K) &= \langle -1, \sqrt{\eta_1}, \sqrt{\eta_2}, \sqrt{\eta_3} \rangle.
\end{aligned}$$

Hence $[C_{\mathrm{S}}(K) : C_{\mathrm{cl}}(K)] = 48$, $[C_{\mathrm{S}}(K) : C_{\mathrm{cs}}(K)] = 2$ and $[C_{\mathrm{W}}(K) : C_{\mathrm{S}}(K)] = 8$. □

The following proposition generalizes Example 1 and computes the index $[E(K) : C_{\mathrm{W}}(K)]$ for an infinite family of abelian fields.

Proposition 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 $[E(K) : C_{\mathrm{W}}(K)] = h_K$.

Proof. See the thesis. □

Circular units in a compositum of quadratic fields

In this chapter we shall suppose that our abelian field K is of a special form, namely that K is a compositum of a finite number of quadratic fields such that -1 is not a square of the genus field $\overline{K}$ of K in the narrow sense. This condition can be written equivalently as follows: either 2 does not ramify in K and $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_s})$, where $d_1, \ldots, d_s$ with $s \geq 1$ are square-free integers all congruent to 1 modulo 4, or 2 ramifies in K and there is uniquely determined $x \in \{2, -2\}$ such that $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_s})$, where $d_1, \ldots, d_s$ with $s \geq 1$ are square-free integers such that $d_i \equiv 1 \pmod 4$ or $d_i \equiv x \pmod 8$ for each $i \in \{1, \ldots, s\}$. In the former case, let

$$J = \{p \in \mathbb{Z};\ p \equiv 1 \pmod 4,\ |p| \text{ is a prime ramifying in } K\},$$

and, in the latter case, let

$$J = \{x\} \cup \{p \in \mathbb{Z};\ p \equiv 1 \pmod 4,\ |p| \text{ is a prime ramifying in } K\}.$$

For any $p \in J$, let

$$n_{\{p\}} = \begin{cases} |p| & \text{if } p \text{ is odd,} \\ 8 & \text{if } p \text{ is even.} \end{cases}$$

For any $S \subseteq J$ let (by convention, an empty product is 1)

$$n_S = \prod_{p \in S} n_{\{p\}}, \quad \zeta_S = e^{2\pi i / n_S}, \quad \mathbb{Q}^S = \mathbb{Q}^{(n_S)} = \mathbb{Q}(\zeta_S), \quad \overline{K}_S = \mathbb{Q}(\sqrt{p};\ p \in S).$$

It is easy to see that $\overline{K}_J = \overline{K}$ and that n_J is the conductor of K. Let us define

$$\varepsilon_S = \begin{cases} 1 & \text{if } S = \emptyset, \\ \frac{1}{\sqrt{p}} \operatorname{N}_{\mathbb{Q}^S/\overline{K}_S}(1 - \zeta_S) & \text{if } S = \{p\}, \\ \operatorname{N}_{\mathbb{Q}^S/\overline{K}_S}(1 - \zeta_S) & \text{if } \#S > 1, \end{cases}$$

$K_S = K \cap \overline{K}_S$ and $\eta_S = \operatorname{N}_{\overline{K}_S/K_S}(\varepsilon_S)$ for any $S \subseteq J$. It is easy to see that ε_S and η_S are units in $\overline{K}_S$ and K_S, respectively. For any $p \in J$ let σ_p be the non-trivial automorphism in $\operatorname{Gal}(\overline{K}_J/\overline{K}_{J\setminus\{p\}})$. Then $G = \operatorname{Gal}(\overline{K}_J/\mathbb{Q})$ can be considered as a (multiplicative) vector space over $\mathbb{F}_2$ with $\mathbb{F}_2$-basis $\{\sigma_p;\ p \in J\}$.

Let us denote the maximal real subfield of K by K^+. Let

$$X = \{\xi \in \widehat{G};\ \xi(\sigma) = 1 \text{ for all } \sigma \in \operatorname{Gal}(\overline{K}_J/K^+)\},$$

where $\widehat{G}$ is the character group of G. Then X can be viewed also as the group of all Dirichlet characters corresponding to K^+. For any $\chi \in X$ let

$$S_\chi = \{p \in J;\, \chi(\sigma_p) = -1\}.$$

Let W be the group of roots of unity in K. It is easy to see that the group generated by W and by

$$\{\eta_S^\sigma;\, S \subseteq J,\, \sigma \in G\}$$

coincides with the group $C'_{\mathrm{S}}(K)$ defined above in Theorem II.

Theorem IV. ([**4**, Theorem 1 and Proposition 1]) Let

$$B = \{\eta_{S_\chi};\, \chi \in X,\, \chi \neq 1\}.$$

Then B is a basis of $C'_{\mathrm{S}}(K)$. Moreover

$$[E : C'_{\mathrm{S}}(K)] = \left(\prod_{\substack{\chi \in X \\ \chi \neq 1}} \frac{2 \cdot [K : K_{S_\chi}]}{[K : K^+]} \right) \cdot (\#X)^{-\frac{1}{2}(\#X)} \cdot Qh^+$$

and the index of Sinnott module (cf. (**??**))

$$(e^+\mathbb{Z}[G] : e^+U) = [K^+ : \mathbb{Q}]^{-[K^+:\mathbb{Q}]/2} \cdot \prod_{\chi \in X} [K : K_{S_\chi}].$$

□

Theorem IV shows a way to get a divisibility relation for the class number – it is enough to prove a divisibility statement for the index $[E : C'_{\mathrm{S}}(K)]$.

Theorem V. ([**4**, Theorem 2]) Let us denote $n = \#J$ and $2^l = [K : \mathbb{Q}]$. If K is real then

$$2^{2^l - 1 - l - n - \binom{l}{2}} \mid [E : C'_{\mathrm{S}}(K)],$$

and if K is imaginary then

$$2^{2^{l-1} - l - n - \binom{l}{2}} \mid [E : C'_{\mathrm{S}}(K)].$$

□

Theorems IV and V can give a result concerning divisibility h^+ by a high power of 2 as the following special case shows.

Corollary VI. ([**4**, Example]) Let us suppose $k = K_J$ and

$$\#\{p \in J;\, p < 0\} > 1.$$

Let us denote $n = \#J$. Then

$$2^{2^{n-2}-n-\binom{n}{2}-1} \mid h^+.$$

□

P. E. Conner and J. Hurrelbrink in their book [22] characterize the parity of the class number of any biquadratic field up to the following cases:

- $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, where p and q are different primes, $p \equiv q \equiv 1 \pmod 4$, the Legendre symbol $\left(\frac{p}{q}\right) = 1$;
- $\mathbb{Q}(\sqrt{p}, \sqrt{2})$, where p is a prime, $p \equiv 1 \pmod 8$.

The problem of characterizing fields with an even class number among these fields is equivalent to the problem of characterizing fields $\mathbb{Q}(\sqrt{pq})$ (in the first case) and $\mathbb{Q}(\sqrt{2p})$ (in the second case) with a class number divisible by 4 (e.g., see [22, the remarks following (21.5) and (19.8)]). Theorem IV made possible to obtain the following criterions by means of a careful study of square roots of circular units.

Theorem VII. ([**3**, Theorem 1]) Let p and q be different primes such that $p \equiv q \equiv 1 \pmod 4$. Let h and h_1 be the class numbers of $k = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ and $k_1 = \mathbb{Q}(\sqrt{pq})$, respectively, and let e be the norm of the fundamental unit of k_1.

1. If $\left(\frac{p}{q}\right) = -1$, then h is odd, $h_1 \equiv 2 \pmod 4$ and $e = -1$.
2. Let us suppose $\left(\frac{p}{q}\right) = 1$ and fix $u, v \in \mathbb{Z}$ satisfying $u^2 \equiv p \pmod q$ and $v^2 \equiv q \pmod p$. Then the following assertions hold true:
   (a) if $\left(\frac{u}{q}\right) \neq \left(\frac{v}{p}\right)$, then h is odd, $h_1 \equiv 2 \pmod 4$ and $e = 1$;
   (b) if $\left(\frac{u}{q}\right) = \left(\frac{v}{p}\right) = -1$, then h is even, $h_1 \equiv 4 \pmod 8$ and $e = -1$;
   (c) if $\left(\frac{u}{q}\right) = \left(\frac{v}{p}\right) = 1$, then h is even and $4|h_1$ (resp. $8|h_1$ whenever $e = -1$).

□

Theorem VIII. ([**3**, Theorem 2]) Let p be a prime such that $p \equiv 1 \pmod 4$. Let h and h_1 be the class numbers of $k = \mathbb{Q}(\sqrt{p}, \sqrt{2})$ and $k_1 = \mathbb{Q}(\sqrt{2p})$, respectively, and let e be the norm of the fundamental unit of k_1.

1. If $p \equiv 5 \pmod 8$, then h is odd, $h_1 \equiv 2 \pmod 4$ and $e = -1$.
2. Let us suppose $p \equiv 1 \pmod 8$ and fix $v \in \mathbb{Z}$ satisfying $v^2 \equiv 2 \pmod p$. Then the following assertions hold true:

(a) if $\left(\frac{v}{p}\right) \neq (-1)^{\frac{p-1}{8}}$, then h is odd, $h_1 \equiv 2 \pmod 4$ and $e = 1$;

(b) if $\left(\frac{v}{p}\right) = -1$ and $p \equiv 9 \pmod{16}$, then h is even, $h_1 \equiv 4 \pmod 8$ and $e = -1$;

(c) if $\left(\frac{v}{p}\right) = 1$ and $p \equiv 1 \pmod{16}$, then h is even and $4|h_1$ (resp. $8|h_1$ whenever $e = -1$). □

Theorems VII and VIII have the following consequences.

Corollary IX. ([**3**, Corollary 1]) Let p and q be different primes such that $p \equiv q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$. Let us write $p = a^2 + b^2$ and $q = c^2 + d^2$, where a, c are odd and b, d are even. Then the class number h of $k = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ is even if and only if

$$\left(\tfrac{ad-bc}{q}\right) = (-1)^{\frac{q-1}{4}}.$$

□

Corollary X. ([**3**, Corollary 2]) Let p be a prime such that $p \equiv 1 \pmod 8$. Let us write $p = a^2 + b^2$, where a is odd and b is even. Then the class number h of $k = \mathbb{Q}(\sqrt{p}, \sqrt{2})$ is even if and only if $16|p - 1 + 2b$. □

Corollary XI. ([**3**, Corollary 3]) Let p be a prime. If $p \equiv 1 \pmod{16}$, then p can be written in the form $p = x^2 + 64y^2$ with $x, y \in \mathbb{Z}$ if and only if p can be written in the form $p = r^2 + 32s^2$ with $r, s \in \mathbb{Z}$. If $p \equiv 9 \pmod{16}$, then p can be written in the form $p = x^2 + 64y^2$ with $x, y \in \mathbb{Z}$ if and only if p cannot be written in the form $p = r^2 + 32s^2$ with $r, s \in \mathbb{Z}$. □

The previous results were a motivation for the following modification of the problem: consider fields of the same odd prime degree instead of quadratic fields. This change makes things much more difficult, nevertheless we have covered in [**7**] a particular case – the compositum of such fields each of them being ramified at exactly one prime.

Let p be an odd prime. Let $p_1, \ldots, p_s$ be different primes, all congruent to 1 modulo p. For each $i = 1, \ldots, s$ let K_i be the abelian field of conductor p_i and degree $[K_i : \mathbb{Q}] = p$. Let us consider the compositum $K = \prod_{i=1}^{s} K_i$. Then K is real and Sinnott's formula gives

$$[E(K) : C_{\mathrm{S}}(K)] = h_K \cdot 2^{p^s - 1}.$$

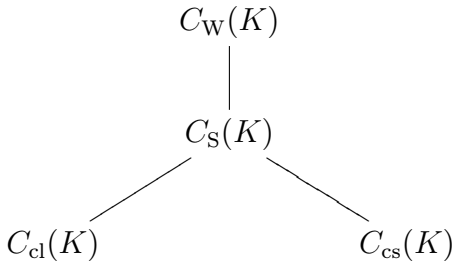
A careful estimate of the dimension of vector space $E(K)/(E(K)^p C_{\mathrm{S}}(K))$ over $\mathbb{F}_p$ gives the following

Theorem XII. ([**7**, Théorème 3.2]) The class number h_K of K is divisible by $p^{2^s - s^2 + s - 2}$. □

Let us notice that this problem has been attacked by different methods, too. In [23] G. Cornell proved $p^{p^{s-4}-1} \mid h_K$ and in [24] G. Cornell and M. Rosen proved $p^{s(s-3)/2} \mid h_K$. Theorem XII is stronger than these results if $s = 5$ and $p \leq 7$ or if $s = 6$ and $p \leq 5$ or if $s = 7, 8, 9, 10$ and $p = 3$.

A comparison of different groups of circular units in an abelian field

This section is devoted to a comparison of the groups of circular units defined above for a general case of an abelian field. Let K be an abelian field of conductor m. We have seen that



and Example 1 shows that there is no inclusion between $C_{\mathrm{cl}}(K)$ and $C_{\mathrm{cs}}(K)$ 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 prime could be a divisor of these indices.

Using the identity (**??**) it is easy to see that for any $\eta \in C_{\mathrm{cl}}(K)$ we have $\eta^{[\mathbb{Q}^{(m)}:K]} \in C_{\mathrm{S}}(K)$. Therefore if a prime l divides the index $[C_{\mathrm{S}}(K) : C_{\mathrm{cl}}(K)]$ then $l \mid [\mathbb{Q}^{(m)} : K] = \frac{\varphi(m)}{[K:\mathbb{Q}]}$.

Theorem 3. Let $\overline{K}$ be the genus field of K in the narrow sense. Let l be an odd prime dividing the index $[C_{\mathrm{W}}(K) : C_{\mathrm{S}}(K)]$. Then $l \mid [\overline{K} : K]$.

Proof. See the thesis. □

Corollary 4. If l is an odd prime dividing the index $[C_{\mathrm{W}}(K) : C_{\mathrm{S}}(K)]$ then $l \mid [K : \mathbb{Q}]$.

Proof. See the thesis. □

Theorem 5. Let l be a prime dividing the index $[C_{\mathrm{S}}(K) : C_{\mathrm{cs}}(K)]$. Then $l \mid [K : \mathbb{Q}]$.

Proof. See the thesis. □

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 $G = \mathrm{Gal}(K/\mathbb{Q})$. Sinnott's index formula (**??**) shows that there are some similarities between two finite groups: namely the class group $\mathcal{C}l(K)$ of K and the quotient group $E(K)/C_{\mathrm{S}}(K)$. More precisely, (**??**) gives that the p-Sylow subgroups of the mentioned groups are of the same order: $|\mathcal{C}l(K)_p| = |(E(K)/C_{\mathrm{S}}(K))_p|$. But this result has been obtained via the analytical class number formula, so it is not clear whether these two groups have similar algebraic properties. Since G acts on these groups, both $\mathcal{C}l(K)_p$ and $(E(K)/C_{\mathrm{S}}(K))_p$ are $\mathbb{Z}_p[G]$-modules. But they are not isomorphic in general (even as groups), as we can see in the following

Example 6. If $K = \mathbb{Q}(\sqrt{62501})$ and $p = 3$ then we have $\mathcal{C}l(K)_p \cong (\mathbb{Z}/3\mathbb{Z})^2$ while $(E(K)/C_{\mathrm{S}}(K))_p \cong \mathbb{Z}/9\mathbb{Z}$. □

Corollary 4 shows that $(E(K)/C_{\mathrm{S}}(K))_p \cong (E(K)/C_{\mathrm{W}}(K))_p$, Theorem 5 gives that $(E(K)/C_{\mathrm{S}}(K))_p \cong (E(K)/C_{\mathrm{cs}}(K))_p$, so it is not important which of these three groups of circular units we are considering.

A common algebraic property of $\mathcal{C}l(K)_p$ and $(E(K)/C_{\mathrm{S}}(K))_p$ has been formulated by G. Gras in his

Conjecture 7. Let K be a real abelian field, p be an odd prime such that $p \nmid [K : \mathbb{Q}]$. Then the $\mathbb{Z}_p[G]$-modules $\mathcal{C}l(K)_p$ and $(E(K)/C_{\mathrm{cs}}(K))_p$ have isomorphic Jordan-Hölder series. □

An important step in this direction has been made by R. Greenberg who proved in [28] in 1977 that the Main Conjecture of Iwasawa theory implies Conjecture 7. Therefore the proof of Main Conjecture, given by B. Mazur and A. Wiles in [37] in 1984, is also a proof of Conjecture 7. These deep results has been obtained by extremely difficult techniques from algebraic geometry.

An astonishing turnaround appeared in 1988 when F. Thaine gave in [45] a very much simpler proof of the following corollary of Conjecture 7:

Theorem 8a. ([45, Theorem 3]) Let K be a real abelian field, p be an odd prime such that $p \nmid [K : \mathbb{Q}]$. If $\theta \in \mathbb{Z}_p[G]$ annihilates $(E(K)/C_{\mathrm{S}}(K))_p$ then θ annihilates $\mathcal{C}l(K)_p$, too. □

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

Theorem 8b. ([45, Theorem 3]) Let K be a real abelian field of odd degree $[K : \mathbb{Q}]$. If $\theta \in \mathbb{Z}_2[G]$ annihilates $(E(K)/C_{\mathrm{S}}(K))_2$ then 2θ annihilates $\mathcal{C}l(K)_2$. □

A nice exposition of Thaine's proof of Theorems 8 can be found in [46, §15.2]. (Attention: Washington uses the group $C_{\mathrm{cl}}(K)$ instead of $C_{\mathrm{S}}(K)$ here, so [46, Theorem 15.2] is weaker than Theorems 8 since, as Example 1 shows, $(E(K)/C_{\mathrm{S}}(K))_p$ is only a quotient group of $(E(K)/C_{\mathrm{cl}}(K))_p$ in general. But this minor imperfection can be easily repaired: it is not difficult to modify the proof of [46, Lemma 15.3] to cover the case $\delta \in C_{\mathrm{S}}(K)$ instead of the used special case $\delta \in C_{\mathrm{cl}}(K)$.)

Thaine's method has been generalized by K. Rubin in [39], where he considers any abelian extension of number fields (instead of an abelian extension of $\mathbb{Q}$) 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:

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 $\eta \equiv \varepsilon^2 \pmod{(1-\zeta_q)(1-\zeta_q^{-1})}$ and whose norm $\mathrm{N}_{K_q/K}(\eta) = 1$. 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 $\mathcal{C}l(K)_p$, and let V be a finitely generated submodule of $\mathbb{Z}[G]$-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 of $\mathbb{Z}[G]$-modules $\mathrm{Gal}(H/K)$ and $\mathcal{C}l(K)_p$, where G acts on $\mathrm{Gal}(H/K)$ via conjugation. Let $H' = H \cap K(\zeta_N)$. In [39] Rubin proves

Theorem 9. $\alpha(\varepsilon)$ annihilates $\mathrm{Gal}(H/H')$ for any $\varepsilon \in \mathcal{C}$. □

This theorem does not give an annihilator of $\mathcal{C}l(K)_p \cong \mathrm{Gal}(H/K)$ but only an annihilator of its submodule $\mathrm{Gal}(H/H')$. But we have control on their quotient $\mathrm{Gal}(H'/K)$, 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 $C_{\mathrm{S}}(K) \subseteq \mathcal{C}$ but, in general, $C_{\mathrm{W}}(K) \not\subseteq \mathcal{C}$.

Another important step further 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 $\mathcal{C}l(K)_p$ but also to bound their orders, so it gives not only a proof of

Theorems 8 but also a proof of Conjecture 7. A very nice introduction to Euler systems is [40], where the Main Conjecture for the pth cyclotomic field $\mathbb{Q}^{(p)}$ is proved. The Main Conjecture for all abelian fields including the case $p = 2$ was proven by C. Greither using these techniques in [29]. The recent monograph [41] of Rubin on Euler systems is written from a more general point of view and is meant for a more advanced reader.

Theorems 8 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 9 but the input of Theorem 9 is not an annihilator of a quotient of $E(K)$ but a $\mathbb{Z}[G]$-module homomorphism α. Therefore natural questions appear for a prime p which divides the degree: how can the annihilators of $\mathcal{C}l(K)_p$ and annihilators of $(E(K)/C_{\mathrm{S}}(K))_p$ 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 [**9**] we studied the easiest possible case of this situation, which is described in the rest of this chapter.

Let p be an odd prime and $l = p^k$ be its power. Let K be an abelian field of degree $[K : \mathbb{Q}] = l$ with cyclic Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. We want to study the p-Sylow subgroup $\mathcal{C}l(K)_p$ of the class group of K. Let $p_1, \ldots, p_s$ be all primes which ramify in $K/\mathbb{Q}$. We assume the following

Assumption 10. Each p_i ramifies totally and tamely in $K/\mathbb{Q}$ and $s > 1$.

In fact, the assumption $s > 1$ is quite natural since $\mathcal{C}l(K)_p$ is trivial if $s = 1$. The tameness of ramification is assumed just to make things notationally easier, for example it implies that $p_1 \equiv \cdots \equiv p_s \equiv 1 \pmod{l}$ and that $m = p_1 \ldots p_s$ is the conductor of K, but this assumption can be removed. The essential part of Assumption 10 is that each ramifying prime ramifies totally.

For each $i = 1, \ldots, s$, let K_i be the unique subfield of the p_ith cyclotomic field $\mathbb{Q}^{(p_i)}$ of degree $[K_i : \mathbb{Q}] = l$. Then the genus field of K is $\overline{K} = \prod_{i=1}^{s} K_i$. Let us choose and fix a generator σ of G and for each $i = 1, \ldots, s$ let $\sigma_i \in \mathrm{Gal}(\overline{K}/\mathbb{Q})$ 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 $\mathbb{Z}/l\mathbb{Z}$ as follows: if $i \neq j$ then $\sigma_j^{a_{ij}}|_{K_j}$ is the Frobenius automorphism of p_i on K_j and the main diagonal is determined by the condition that A has zero row sums, i.e. $a_{ii} = -\sum_{j \neq i} a_{ij}$.

Assumption 10 implies that $C_{\mathrm{S}}(K) = C_{\mathrm{cs}}(K)$ is the $\mathbb{Z}[G]$-module $\langle -\eta \rangle_G$ generated by $-\eta$, where $\eta = \mathrm{N}_{\mathbb{Q}_m/K}(1 - \zeta_m)$. Sinnott's index formula (**??**) gives $[E(K) : C_{\mathrm{S}}(K)] = l^{-1} h_K$ since $(\mathbb{Z}[G] : U) = 1$ due to the cyclicity of K (see [44, Theorem 5.3]). This implies that l divides the class number h_K but genus theory gives even more: $l^{s-1} | h_K$. Using class field theory, this can be seen as follows: let H be the Hilbert p-class field of K so $\mathrm{Gal}(H/K) \cong \mathcal{C}l(K)_p$

via 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 it is a p-extension of K, we have $\overline{K} \subseteq H$, which means $l^{s-1} = [\overline{K} : K] \mid [H : K] = |\mathcal{C}l(K)_p|$, the pth 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 $\mathrm{Gal}(L/K)$ which is the case if and only if σ acts trivially on $\mathrm{Gal}(L/K)$. Therefore $\mathrm{Gal}(H/\overline{K})$ is the minimal subgroup of $\mathrm{Gal}(H/K)$ whose quotient in $\mathrm{Gal}(H/K)$ has trivial action of σ, which means $\mathrm{Gal}(H/\overline{K}) = (\sigma - 1)\,\mathrm{Gal}(H/K) \cong (\sigma - 1)\mathcal{C}l(K)_p$. So we call $(\sigma - 1)\mathcal{C}l(K)_p$ the non-genus part of $\mathcal{C}l(K)_p$. Having a good understanding for $\mathrm{Gal}(\overline{K}/K)$, it is precisely $(\sigma - 1)\mathcal{C}l(K)_p$ which we want to study.

If $s > 2$ then the divisibility relation $l^{s-1} | h_K = l \cdot [E(K) : C_{\mathrm{S}}(K)]$ means that there are units in $E(K)$, not belonging to $C_{\mathrm{S}}(K)$, whose pth power is in $C_{\mathrm{S}}(K)$. In [**9**], we have searched for such units in

$$\langle 1 - \zeta_m^a;\, a \in \mathbb{Z},\, m \nmid a \rangle \cap K$$

and proved

Theorem XIII. ([**9**, Theorem 1]) There is $\varepsilon \in K^\times$ which is a unit outside of $\{p_1, \ldots, p_s\}$ and satisfies

$$\varepsilon^{(\sigma-1)^{s-1}} = \eta \qquad \text{and} \qquad \mathrm{N}_{K/\mathbb{Q}}(\varepsilon) = \prod_{i=1}^{s} p_i^{(-1)^{s-1} A_i},$$

where $0 \leq A_i < l$ is a lift of the (i,i)-th minor of A. Moreover, we have $\varepsilon^{\sigma-1} \in C_{\mathrm{W}}(K)$ and $|(E(K)/\langle \varepsilon^{\sigma-1} \rangle_G)_p| = |(\sigma - 1)\mathcal{C}l(K)_p|$, 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 $C_{\mathrm{W}}(K)$ but the opposite inclusion does not hold true in general: if all A_i's are zero then $\varepsilon \in C_{\mathrm{W}}(K)$ but $\varepsilon \notin \langle \varepsilon^{\sigma-1} \rangle_G$.

Similarly to the situation of Theorem 8a, 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 XIV. ([**9**, Theorem 2]) If $\theta \in \mathbb{Z}_p[G]$ annihilates $\mathbb{Z}[G]$-module $(E(K)/\langle \varepsilon^{\sigma-1} \rangle_G)_p$ then θ annihilates $(\sigma - 1)\mathcal{C}l(K)_p$, too. □

Theorem XIV has been proved by a modification of methods of Rubin. Since ε 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.

The Lifted Root Number Conjecture

The main theme of the previous chapters consists in the fact that there are some deep connections between the unit group and the class group of an abelian field. However this is only a very special case of a much more general picture. This chapter should show the contribution of the author to this general context. Unfortunately, going to this depth demands to be little bit more vague.

We have seen that we have circular units in any number field K which is an abelian extension of $\mathbb{Q}$. Roughly speaking, Stark conjecture expects the existence of numbers having similar properties for any abelian extension of number fields.

For any Galois extension K/F of number fields, Chinburg defined in [21] an invariant $\Omega = \Omega(3, K/F)$ in the class group of the integral group ring $\mathbb{Z}[G]$, where $G = \mathrm{Gal}(K/F)$. The so-called Root Number Conjecture (RNC for short) states that Ω is the root number class; in particular Ω is conjecturally zero if G is abelian or of odd order. The invariant Ω measures, very roughly speaking, the discrepancy of Galois module structure between the unit group and the class group of K, but the actual description is much more subtle, involving the canonical class of K/F and so-called Tate sequences.

In [31], a lifted invariant was presented. This new invariant, let us call it $\omega(K/F)$, exists if the Stark conjecture holds for K. It lies in a relative K-group $K_0T(\mathbb{Z}[G])$, and it maps to $\Omega(3, K/F)$ under the canonical epimorphism from the $K_0T(\mathbb{Z}[G])$ to the class group of $\mathbb{Z}[G]$. At least for absolutely abelian K, the lifted invariant exists, and the so-called Lifted Root Number Conjecture (LRNC) states that it is zero. The lifted conjecture has the great advantage to localize well, that is, it is equivalent to a collection of local statements $\omega_p = 0$ with p running through all prime numbers. More details can be found in the survey article [30]. Burns and Flach introduced in [18] so-called equivariant Tamagawa numbers $T\Omega(\mathbb{Q}(0)_K, \mathbb{Z}[G])$, which are actually obtained from a more general construction by specializing to the motive $\mathbb{Q}(0)_K$, and Burns has proved in [17] that $T\Omega(\mathbb{Q}(0)_K, \mathbb{Z}[G])$ agrees with $\omega(K/F)$ up to an involution of $\mathbb{Z}[G]$ when G is abelian and $\omega(K/F)$ is defined. So actually LRNC is a special case of the Equivariant Tamagawa Number Conjecture.

Ritter and Weiss proved in [38] that $\omega(K/F)$ is zero for the case that $F = \mathbb{Q}$ and K is abelian of odd prime degree p over $\mathbb{Q}$ such that $K/\mathbb{Q}$ is tame and at most 2 primes ramify in K. The principal result of [**8**] removes the latter restriction:

Theorem XV. ([**8**, Theorem 6]) The Lifted Root Number Conjecture holds for all cyclic tame extensions of $\mathbb{Q}$ of odd prime degree p. □

The tameness condition was presumably not necessary, but we had not done the extra calculations. Anyway, the only prime which might ramify wildly is p. It should be mentioned here that in [19] D. Burns and C. Greither proved LRNC up to its 2-primary part for all absolutely abelian fields K, using rather involved methods; but it is hoped that the explicit approach of [**8**] retains some interest. For example, the method of trees derived in [**8**], which we have also used in [**9**], has been successfully used by A. Hayward in [34].

Let us mention that also Theorem XIII has impact on the development of this deep general framework. Theorem XIII shows that η is a $(\sigma-1)^{s-1}$-th "power" in $K^\times$ and it is proved by an explicit construction of ε in the group of circular numbers of the m-th cyclotomic field, where m is the conductor of K. This construction is rather technical but elementary from the point of view that in fact only some combinatorial methods are used. This construction inspired D. Burns and A. Hayward to derive the existence of ε by another way. They replaced the direct use of combinatorial methods with a reduction to the general Tamagawa number formalism and obtained the following advantages: their approach works equally well in the setting of global function fields, as well as to the extensions for which the associated L-functions have multiple-order zero at $s = 0$ (rather than only first-order zero is in setting of [**9**]). However it seems that the general Tamagawa number formalism does not allow to obtain a proof of Theorem XIV.

References

The dissertation thesis consists of the set of nine published research papers [**1**-**9**], while [10-15] are other papers of the author concerning circular units. The other references [16-47] have been used in the text.

[**1**] R. Kučera, *On bases of odd and even universal ordinary distributions*, J. Number Theory 40 (1992), 264-283.

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

[**3**] R. Kučera, *On the parity of the class number of a biquadratic field*, J. Number Theory 52 (1995), 43-52.

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

[**5**] R. Kučera, *A note on Sinnott's definition of circular units of an abelian field*, J. Number Theory 63 (1997), 403-407.

[**6**] R. Kučera, *On the Stickelberger ideal and circular units of some genus fields*, Tatra Mountains Math. Publ. 20 (2000), 93-104.

[**7**] C. Greither, S. Hachami and R. Kučera, *Racines d'unités cyclotomiques et divisibilité du nombre de classes d'un corps abélien réel*, Acta Arith. 96 (2001), 247-259.

[**8**] C. Greither and R. Kučera, *The lifted root number conjecture for fields of prime degree over the rationals: an approach via trees and Euler systems*, Annales de l'Institut Fourier 53 (2002), 735-777.

[**9**] C. Greither and R. Kučera, *Annihilators for the class group of a cyclic field of prime power degree*, Acta Arith. 112 (2004), 177-198.

[10] R. Kučera, *Bazis ideala Stickel'bergera i systema osnovnych krugovych jedinic*, in Kol'ca i moduli 3, Zapiski naučnych seminarov LOMI, 175, 69-74 (in Russian), Nauka, Leningrad 1989.

[11] R. Kučera, A basis for the Stickelberger ideal and the system of circular units of a cyclotomic field, J. Sov. Math. 57 (1991), No.6, 3485-3489.

[12] R. Kučera, Different groups of circular units of a compositum of real quadratic fields, Acta Arith. 67 (1994), 123-140.

[13] R. Kučera and J. Nekovář, Cyclotomic units in $\mathbb{Z}_p$-extensions, J. Algebra 171 (1995), 457-472.

[14] R. Kučera, A generalization of a unit index of Greither, Acta Math. et Informatica Univ. Ostraviensis 6 (1998), 149-154.

[15] R. Kučera, A Note on Circular Units in $\mathbb{Z}_p$-extensions, Journal de Théorie des Nombres de Bordeaux 15 (2003), 223-229.

[16] H. Bass, *Generators and relations for cyclotomic units*, Nagoya Math. J. 27 (1966), 401-407.

[17] D. Burns, *Equivariant Tamagawa numbers and Galois module theory I*, Compositio Math. 127 (2001), 304-337.

[18] D. Burns and M. Flach, *Equivariant Tamagawa numbers of motives*, preprint 1998

[19] D. Burns and C. Greither, *On the equivariant Tamagawa number conjecture for Tate motives*, Invent. Math. 153 (2003), 303-359.

[20] D. Burns and A. Hayward, *Explicit units and the equivariant Tamagawa number conjecture II*, preprint 2004,
available at `http://www.mth.kcl.ac.uk/~hayward`

[21] T. Chinburg, *On the Galois structure of algebraic integers and S-units*, Invent. Math. 74 (1983), 321-349.

[22] P. E. Conner and J. Hurrelbrink, "Class number parity", Ser. Pure Math. 8, World Sci., Singapore, 1988.

[23] G. Cornell, *Exponential growth of the l-rank of the class group of the maximal real subfield of cyclotomic fields*, Bull. Amer. Math. Soc. 1 (1983), 55-58.

[24] G. Cornell and M. Rosen, *The class group of an absolutely abelian l-extension*, Illinois J. Math. 32 (1988), 453-461.

[25] H. Davenport a H. Hasse, *Die Nullstellen der Kongruenzzetafunction in gewissen zyklischen Fällen*, J. reine angew. Math. 172 (1934), 151-182.

[26] V. Ennola, *On relations between cyclotomic units*, J. Number Theory 4 (1972), 236-247.

[27] R. Gold and J. Kim, *Bases for cyclotomic units*, Compositio Math. 71 (1989), 13-27.

[28] R. Greenberg, *On p-adic L-functions and cyclotomic fields, II*, Nagoya Math. J. **67** (1977), 139-158.

[29] C. Greither, *Class groups of abelian fields and the main conjecture*, Ann. Inst. Fourier **42** (1992), 449-499.

[30] K.-W. Gruenberg, J.Ritter and A. Weiss, *On Chinburg's root number conjecture*, Jbr. Dt. Math.-Vereinigung 100 (1998), 36-44.

[31] K.-W. Gruenberg, J.Ritter and A. Weiss, *A local approach to Chinburg's root number formula*, Proc. London Math. Soc. 79 (1999), 47-80.

[32] H. Hasse, "Über die Klassenzahl abelscher Zahlkörper", Akademie-Verlag, Berlin, 1952.

[33] H. Hasse, "Vorlesungen über Zalhentheorie", Berlin 1964.

[34] A. Hayward, *A class number formula for higher derivatives of abelian L-functions*, Compositio Math. 140 (2004), 99-129.

[35] P. Kraemer, *Circular units in a bicyclic field*, to appear in J. Number Theory.

[36] G. Lettl, *A note on Thaine's circular units*, J. Number Theory 35 (1990), 224-226.

[37] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76 (1984), 179-330.

[38] J. Ritter a A. Weiss, *The lifted root number conjecture for some cyclic extensions of* $\mathbb{Q}$, Acta Arith. 90 (1999), 313-340.

[39] K. Rubin, *Global units and ideal class groups*, Invent. math. 89 (1987), 511-526.

[40] K. Rubin, *The Main Conjecture*, in: S. Lang, Cyclotomic Fields I and II (combined 2nd edition), Springer 1990.

[41] K. Rubin, *Euler systems*, Ann. of Math. Studies 147, Princeton Univ. Press, Princeton, 2000.

[42] C.-G. Schmidt, *Die Relationenfaktorgruppen von Stickelberger-Elementen und Kreiszahlen*, J. reine angew. Math. 315 (1980), 60-72.

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

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

[45] F. Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. 128 (1988), 1-18.

[46] L. C. Washington, "Introduction to cyclotomic fields", Springer-Verlag, GTM 83, 1997.

[47] K. Yamamoto, *The gap group of multiplicative relationship of Gaussian sums*, Symp. Math. XV (1975), 427-440.