COMPOSITIO MATHEMATICA

JAMES S. KRAFT
RENÉ SCHOOF

Computing Iwasawa modules of real quadratic number fields

Compositio Mathematica, tome 97, n° 1-2 (1995), p. 135-155.
<http://www.numdam.org/item?id=CM_1995__97_1-2_135_0>

Compositio Mathematica **97:** 135–155, 1995.

Computing Iwasawa modules of real quadratic number fields

Dedicated to Frans Oort on the occasion of his 60th birthday

JAMES S. KRAFT[1] and RENÉ SCHOOF[2]
[1] *Department of Mathematics, Ithaca College, Ithaca, NY 14850, USA*
e-mail:kraft@ithaca.edu
[2] *Dipartimento di Matematica, 2[a] Università di Roma, "Tor Vergata", I-00133 Roma, Italy*
e-mail: schoof@volterra.science.unitn.it

Received 9 February 1995; accepted in final form 18 April 1995

Abstract. Let p be an odd prime and let X denote the projective limit of the p-parts of the ideal class groups of the fields in the cyclotomic $\mathbf{Z}_p$-extension of a real quadratic number field F. We present a method to compute the structure of X. As an illustration of the method we compute X for $p = 3$ and all real quadratic fields $\mathbf{Q}(\sqrt{f})$ of conductor $f < 10000$ and $f \not\equiv 1 \pmod 3$. For all fields we find that X is finite. In other words, Iwasawa's λ-invariant is zero in these cases, which confirms a conjecture of Greenberg's.

1. Introduction

Let F be a number field and let p be an odd prime. Let

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots$$

denote the cyclotomic $\mathbf{Z}_p$-extension of F. In other words, $F_n = F\mathbf{Q}_n$ where $\mathbf{Q}_n$ is the unique subfield of degree p^n of the field of p^{n+1}th roots of unity $\mathbf{Q}(\zeta_{p^{n+1}})$. We let $F_\infty = \cup_n F_n$.

The p-parts A_n of the class groups of the rings of integers of the fields F_n form a projective system

$$A_0 \xleftarrow{N} A_1 \xleftarrow{N} A_2 \xleftarrow{N} \cdots,$$

where N denotes the norm map. By K. Iwasawa's theorem [12], there exist three integers $\mu, \lambda, \nu \in \mathbf{Z}$, which depend on the number field F and the prime p, such that

$$\#A_n = p^{\mu p^n + \lambda n + \nu} \quad \text{for } n \text{ sufficiently large.}$$

For abelian number fields F, the μ-invariant is zero by the Ferrero–Washington theorem [12]. Moreover, the $\mathbf{Q}_p$-vector space

$$V = \left(\varprojlim A_n\right) \otimes \mathbf{Q}_p$$

has finite dimension λ.

If F is a complex abelian field, the Main Conjecture [7] implies that the characteristic polynomial of a topological generator of $\mathrm{Gal}(F_\infty/F)$ acting on V is closely related to the p-adic L-functions $L_p(s, \omega\chi^{-1})$ associated to the characters χ of $\mathrm{Gal}(F/\mathbf{Q})$. Here ω denotes the Teichmüller character.

When χ is an odd character, the character $\omega\chi^{-1}$ is even and the p-adic L-function $L_p(s, \omega\chi^{-1})$ is related to the χ^{-1}-eigenspace of V. When χ is even however, the p-adic L-function is identically zero [12]. One expects that the corresponding eigenspace is trivial in this case. In other words, Iwasawa's λ-invariant should be zero for *real* abelian number fields F. This means that the projective limit $\varprojlim A_n$ is *finite*. Equivalently, the sequence of class groups $A_0, A_1, A_2, \ldots$, stabilizes, i.e., there is an index n_0 such that the norm map $N: A_n \to A_{n_0}$ is an isomorphism for all $n \geqslant n_0$.

In his thesis [4], R. Greenberg has studied this question. He gave a sufficient criterion for λ to be zero. Using his criterion the λ-invariant has been shown to be zero in a handful of examples [1, 6]. In this paper we present an efficient algorithm to compute the groups A_n in the cyclotomic $\mathbf{Z}_p$-extension of an abelian number field. The method is based on properties of cyclotomic units and exploits the fact that certain group rings are Gorenstein rings. The algorithm not only enables us to verify in any given case that $\lambda = 0$, but it also gives the structure of $\varprojlim A_n$ as a Galois module. This is a consequence of our Proposition 2.6 which says that, when $\lambda = 0$, the group of units modulo cyclotomic units becomes actually *isomorphic* to A_n when n is sufficiently large .

Although our method applies in greater generality, we restrict our attention to the simplest non-trivial case: F is a real quadratic field and $p = 3$. The algorithm is inspired by the one used in [8]. As an illustration of the method we have computed the groups A_n for the fields $\mathbf{Q}(\sqrt{f})$ of conductor $f < 10000$ with $f \not\equiv 1 \pmod 3$. We know of only one non-trivial case where the structure of the groups A_n had been computed previously: for $\mathbf{Q}(\sqrt{257})$ and $p = 3$, Greenberg [5] has shown that $A_n \cong \mathbf{Z}/3\mathbf{Z}$ for all n. It is not difficult to extend our computations much further.

For the case $f \equiv 1 \pmod 3$ see the papers by T. Fukuda, K. Komatsu and H. Taya (see [11] and the references there). We will apply our methods to this somewhat different case in a separate paper.

The results of the calculations are presented in Table 5.2. It turns out that the sequence of groups $A_0, A_1, A_2, \ldots$, stabilizes in all cases. As a consequence we can confirm Greenberg's conjecture in all cases:

THEOREM. *The Iwasawa λ-invariants associated to the $\mathbf{Z}_3$-extension of the real quadratic fields $\mathbf{Q}(\sqrt{f})$ of conductor $f < 10000$ with $f \not\equiv 1 \pmod 3$ are all equal to zero.*

In Section 2 we discuss some properties of cyclotomic units. In Sections 3 and 4 we present our algorithm and in Section 5 we give the results of our computations. For the cohomology and class field theory that we use, see [2].

2. Cyclotomic units

In this section we study the cyclotomic units in the $\mathbf{Z}_p$-extension of a real quadratic field in some detail. First we introduce some notation.

Let $F = \mathbf{Q}(\sqrt{f})$ be a real quadratic field of conductor f. Let σ denote the non-trivial automorphism of F and let $\chi(x) = (\frac{f}{x})$ be the Dirichlet character associated to F. Let p be an odd prime and let

$$F = F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots$$

be the cyclotomic $\mathbf{Z}_p$ extension of F: every F_n is of the form $F\mathbf{Q}_n$ where $\mathbf{Q}_n$ is the nth layer in the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. The field F_n is contained in $\mathbf{Q}(\zeta_{p^{n+1}f})$ and is abelian over $\mathbf{Q}$. Let $G_n = \mathrm{Gal}(F_n/F_0)$; it is a cyclic group of order p^n.

For any $n \geqslant 0$, let O_n^* denote the unit group of the ring of integers O_n of F_n, let Cyc_n denote the subgroup of O_n^* of cyclotomic units and Cl_n the ideal class group of O_n. We use the definition of Cyc_n as in Sinnott's paper [10, Sect. 4].

All these groups admit an action by the Galois group $\mathrm{Gal}(F_n/\mathbf{Q}_n) \cong \mathrm{Gal}(F/\mathbf{Q}) = \{\sigma, \mathrm{id}\}$. We use this action to split the modules into an invariant and anti-invariant piece. The anti-invariant pieces are important for us. They are defined as follows: $O_n^*(\chi) = (O_n^* \otimes \mathbf{Z}_p)^{\sigma-1}$ and similarly $\mathrm{Cyc}_n(\chi) = (\mathrm{Cyc}_n \otimes \mathbf{Z}_p)^{\sigma-1}$ and $Cl_n(\chi) = (Cl_n \otimes \mathbf{Z}_p)^{\sigma-1}$.

DEFINITION. The nth cyclotomic unit $\eta_n \in F_n$ is defined by

$$\eta_n = \underset{\mathbf{Q}(\zeta_{f'p^{n+1}})/F_n}{\mathrm{Norm}} \left(1 - \zeta_{f'}\zeta_{p^{n+1}}\right)^{1-\sigma};$$

here $f' = f/p$ when p divides f (or equivalently: when $\chi(p) = 0$) and $f' = f$ otherwise.

From now on we assume that

$$\chi(p) = \left(\frac{f}{p}\right) \neq 1.$$

It follows from [10, Thm. 4.1 and Thm. 5.3] that in this case the index $[O_n^* : \mathrm{Cyc}_n]$ is, up to a p-adic unit, equal to the class number $\#Cl_n$. It follows from the distribution relations for the cyclotomic units, that, up to exponents of the form $\chi(p) - 1$, the cyclotomic units η_k, for $k < n$ and the cyclotomic unit $\mathrm{Norm}_{\mathbf{Q}(\zeta_f)/F_0}(1 - \zeta_f)^{1-\sigma}$ are all norms of η_n. Therefore η_n generates $\mathrm{Cyc}_n(\chi)$ as a $\mathbf{Z}_p[G_n]$-module. In other words, the map

$$\mathbf{Z}_p[G_n] \to \mathrm{Cyc}_n(\chi)$$

given by $x \mapsto \eta_n^x$ is surjective. Since both $\mathbf{Z}_p[G_n]$ and $\mathrm{Cyc}_n(\chi)$ are free $\mathbf{Z}_p$-modules of rank p^n, the map is an isomorphism and we see that $\mathrm{Cyc}_n(\chi)$ is free of rank 1 over $\mathbf{Z}_p[G_n]$ generated by η_n.

For convenience sake we let

$$\begin{aligned} A_n &= Cl_n(\chi), \\ B_n &= O_n^*(\chi)/\mathrm{Cyc}_n(\chi), \\ C_n &= \mathrm{Hom}(B_n, \mathbf{Q}/\mathbf{Z}). \end{aligned}$$

The groups B_n and C_n have the same order as A_n:

$$h_n = \#A_n = \#B_n = \#C_n.$$

This follows from the decomposition of the zeta-function of F_n into a product of L-series [12]. In general, the groups A_n and B_n are *not* isomorphic. Recall that the action of the Galois group G_n on C_n is given by

$$\gamma(f)(u) = f(\gamma^{-1}(u)), \quad \gamma \in G_n, u \in B_n.$$

In order to study the growth of the class groups A_n in the $\mathbf{Z}_p$-extension, we may as well study the groups B_n, which are easier to compute. It turns out to be even more convenient to study the *dual* groups C_n.

For any $n \geqslant m \geqslant 0$ let $G_{n,m}$ denote the group $\mathrm{Gal}(F_n/F_m)$. It is a cyclic group of order p^{n-m}.

LEMMA 2.1. *Let $n \geqslant m \geqslant 0$. Then the natural map*

$$B_m \longrightarrow B_n^{G_{n,m}}$$

is an isomorphism.

Proof. Since $\mathrm{Cyc}_n(\chi)$ is a free $\mathbf{Z}_p[G_n]$-module, the cohomology group $H^1(G_{n,m}, \mathrm{Cyc}_n(\chi))$ is trivial. Now apply the snake lemma to the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Cyc}_m(\chi) & \longrightarrow & O_m^*(\chi) & \longrightarrow & B_m & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Cyc}_n(\chi)^{G_{n,m}} & \longrightarrow & O_n^*(\chi)^{G_{n,m}} & \longrightarrow & B_n^{G_{n,m}} & \longrightarrow & 0 \end{array}$$

This proves the lemma. □

The following proposition enables us to decide whether the sequence of groups

$$B_0 \hookrightarrow B_1 \hookrightarrow B_2 \hookrightarrow \cdots$$

stabilizes.

PROPOSITION 2.2. (Stabilization.) *If $\#B_m = \#B_{m+1}$ for some $m \geqslant 0$, then the natural map $B_m \to B_n$ is an isomorphism for all $n \geqslant m$.*

Proof. Let $n \geqslant m+1$ and let γ denote a generator of $G_{n,m}$. The group ring $\mathbf{Z}_p[G_{n,m}]$ is a local ring with maximal ideal $\mathfrak{m} = (\gamma - 1, p)$. By Lemma 2.1 the groups B_m and B_{m+1} are precisely the invariants of $G_{n,m}$ and its subgroup $G_{n,m+1}$ respectively. In other words $B_m = \ker(\gamma - 1)$ and $B_{m+1} = \ker(\gamma^p - 1)$. Since these groups have the same cardinality, the same is true for $(\gamma - 1)B_n$ and $(\gamma^p - 1)B_n$. This implies that

$$(\gamma - 1)B_n$$

$$= (\gamma^p - 1)B_n = (\gamma^{p-1} + \cdots + \gamma + 1)(\gamma - 1)B_n \subset \mathfrak{m}(\gamma - 1)B_n.$$

By Nakayama's Lemma we therefore have that $(\gamma - 1)B_n = 0$. This implies that B_n is $G_{n,m}$-invariant and hence equal to B_m as required. □

In the computations we will use the following, obviously equivalent, form of Proposition 2.2:

COROLLARY 2.3. *If $\#C_m = \#C_{m+1}$ for some $m \geqslant 0$, then the norm map $A_n \to A_m$ is an isomorphism for all $n \geqslant m$.*

We now study the structure of the groups C_n in some more detail. It is convenient to introduce the projective limit

$$C = \varprojlim C_n.$$

Here the transition maps $C_n \to C_m$ (for $n \geqslant m$) are the duals of the natural maps $B_m \hookrightarrow B_n$. The group C is a module over the projective limit of the rings $\mathbf{Z}_p[G_n]$, which is isomorphic to the Iwasawa algebra $\Lambda = \mathbf{Z}_p[[T]]$. Here $1+T$ corresponds to the topological generator $1+p$ of the projective limit $1 + p\mathbf{Z}_p$ of the groups $G_n \cong 1 + p\mathbf{Z}/p^{n+1}\mathbf{Z}$. One has that

$$\mathbf{Z}_p[G_n] = \Lambda/(\omega_n) \quad \text{for each } n \geqslant 0,$$

where ω_n denotes $(1+T)^{p^n} - 1$.

THEOREM 2.4.

(i) *There is an isomorphism of Λ-modules*

$$C \cong \Lambda/I \quad \textit{for some } \Lambda\textit{-ideal } I.$$

Moreover, for each $n \geqslant 0$ we have

$$C_n \cong \Lambda/(\omega_n, I).$$

(ii) *For every $k, n \geqslant 0$, there is a canonical G_n-isomorphism*

$$C_n/p^k C_n \cong \mathbf{Z}/p^k\mathbf{Z}[G_n]/\{f(\eta_n) : f \in \mathrm{Hom}_{G_n}(O_n^*(\chi), \mathbf{Z}/p^k\mathbf{Z}[G_n])\}.$$

Proof. (i) Since C/TC is dual to the cyclic group B_0, it follows from Nakayama's Lemma that C is a cyclic Λ-module. The fact that $C_n \cong \Lambda/(\omega_n, I)$ follows by dualizing from Lemma 2.1.

(ii) Let $n \geqslant 0$ and let p^k be a power of p. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Cyc}_n(\chi) & \longrightarrow & O_n^*(\chi) & \longrightarrow & B_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p^k} & & \downarrow{\scriptstyle p^k} & & \downarrow{\scriptstyle p^k} & & \\ 0 & \longrightarrow & \mathrm{Cyc}_n(\chi) & \longrightarrow & O_n^*(\chi) & \longrightarrow & B_n & \longrightarrow & 0 \end{array}$$

By the snake lemma this gives an exact sequence

$$0 \to B_n[p^k] \to \mathrm{Cyc}_n(\chi)/\{p^k\text{th powers}\} \to O_n^*(\chi)/\{p^k\text{th powers}\}.$$

All Galois modules in this sequence are killed by p^k. Therefore they are $\mathbf{Z}/p^k\mathbf{Z}[G_n]$-modules. The finite ring $R_n = \mathbf{Z}/p^k\mathbf{Z}[G_n]$ is a Gorenstein ring (see appendix of [7] for definition and basic properties). This means that $\mathrm{Hom}_{\mathbf{Z}}(R_n, \mathbf{Q}/\mathbf{Z})$ is a free R_n-module of rank 1. Therefore the canonical isomorphism $\mathrm{Hom}_{G_n}(M, \mathrm{Hom}_{\mathbf{Z}}(R_n, \mathbf{Q}/\mathbf{Z})) \cong \mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Q}/\mathbf{Z})$ gives rise to an isomorphism

$$\mathrm{Hom}_{G_n}(M, R_n) \xrightarrow{\cong} \mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Q}/\mathbf{Z}),$$

for every finite R_n-module M. The isomorphism is given by $f \mapsto \psi \circ f$ for some chosen R_n-generator $\psi\colon R_n \to \mathbf{Q}/\mathbf{Z}$. This shows that the contravariant functor $\mathrm{Hom}_{G_n}(-, R_n)$ is exact. Applying it to the exact sequence above gives us the exact sequence

$$\mathrm{Hom}_{G_n}(O_n^*(\chi), R_n) \to \mathrm{Hom}_{G_n}(\mathrm{Cyc}_n(\chi), R_n) \to C_n/p^kC_n \to 0.$$

Since $\mathrm{Cyc}_n(\chi)$ is free with generator η_n, we can identify $\mathrm{Hom}_{G_n}(\mathrm{Cyc}_n(\chi), R_n)$ with the ring R_n itself via $f \mapsto f(\eta_n)$. We obtain

$$C_n/p^kC_n \cong R_n/\{f(\eta_n) : f \in \mathrm{Hom}_{G_n}(O_n^*(\chi), R_n)\}$$

as required. □

For computational purposes, it is convenient to make part (ii) of this theorem more explicit. We can exhibit many G_n-homomorphisms $f\colon O_n^*(\chi) \to \mathbf{Z}/p^k\mathbf{Z}[G_n]$ as follows: let r be a prime number which is split in F_n and which is 1 (mod p^k). We have the *reduction modulo r map*

$$f_r : O_n^* \to (O_n/rO_n)^* \cong \bigoplus_{\mathfrak{p}|r} (O_n/\mathfrak{p})^*.$$

For every $\mathfrak{p}$, raising to the power $(r-1)/p^k$ gives a surjective homomorphism $(O/\mathfrak{p})^* \to \mathbf{Z}/p^k\mathbf{Z}$. Since all primes $\mathfrak{p}$ over r are permuted by the Galois group G_n, we obtain, by taking χ-parts, a G_n-homomorphism

$$f_r : O_n^*(\chi) \to \mathbf{Z}/p^k\mathbf{Z}[G_n]$$

which we also denote by f_r.

PROPOSITION 2.5. *Let $k \geqslant 1$ and $n \geqslant 0$. Every G_n-homomorphism $f\colon O_n^*(\chi) \to \mathbf{Z}/p^k\mathbf{Z}[G_n]$ is of the form f_r for some prime r which is split in $F_n(\zeta_{p^k})$.*

Proof. Let $\kappa = \max(k-1, n)$. Then both O_n^* and ζ_{p^k} are contained in $F_\kappa(\zeta_p)$. By Kummer theory we have the following diagram:

$$\begin{array}{c}
\varphi_r \in \mathrm{Gal}(F_\kappa(\zeta_p, \sqrt[p^k]{O_n^*(\chi)})/F_\kappa(\zeta_p)) \\
\downarrow \cong \\
\mathrm{Hom}(O_n^*(\chi)/O_n^*(\chi) \cap (O_{F_\kappa(\zeta_p)}^*)^{p^k}, \mu_{p^k}) \\
\downarrow \cong \\
\mathrm{Hom}(O_n^*(\chi)/O_n^*(\chi)^{p^k}, \mu_{p^k}) \\
\downarrow \cong \\
\mathrm{Hom}(O_n^*(\chi)/O_n^*(\chi)^{p^k}, \mathbf{Q}/\mathbf{Z}) \\
\downarrow \cong \\
f_r \in \mathrm{Hom}_{G_n}(O_n^*(\chi), \mathbf{Z}/p^k\mathbf{Z}[G_n])
\end{array}$$

Here the Frobenius element φ_r of r is mapped to the homomorphism f_r. The second isomorphism follows from the fact that the map $F_n^*/(F_n^*)^{p^k} \to F_\kappa(\zeta_p)^*/(F_\kappa(\zeta_p)^*)^{p^k}$ is injective, because its kernel, which is isomorphic to $H^1(\mathrm{Gal}(F_\kappa(\zeta_p), F_n), \mu_{p^k})$ is trivial. This follows from the exact restriction-inflation sequence

$$0 \to H^1(G_{\kappa,n}, \mu_{p^k}^{\Delta}) \to H^1(\mathrm{Gal}(F_\kappa(\zeta_p), F_n), \mu_{p^k}) \to H^1(\Delta, \mu_{p^k})$$

and the fact that $\Delta = \mathrm{Gal}(F_\kappa(\zeta_p), F_\kappa)$ has order prime to p and that $\mu_{p^k}^{\Delta} = \{1\}$.

By the Cebotarev density theorem, every element in $\mathrm{Hom}(O_n^*(\chi), \mathbf{Z}/p^k\mathbf{Z}[G_n])$ is of the form f_r. This proves the proposition. □

This gives us an explicit description of the modules C_n/p^kC_n:

$$C_n/p^kC_n \cong \mathbf{Z}/p^k\mathbf{Z}[G_n]/\{f_r(\eta_n) : r \text{ is split in } F_n(\zeta_{p^k})\}.$$

Next we explain how to recover the structure of the class groups A_n and the maps $A_m \to A_n$ from the structure of the Λ-module C. First we establish the following remarkable relation between the class groups A_n and the groups of units modulo cyclotomic units B_n:

PROPOSITION 2.6. *Suppose that the sequence of modules C_n stabilizes: $C = C_n$ if for $n \geqslant n_0$ (i.e. "$\lambda = 0$"). Then there is an isomorphism of G_n-modules*

$$A_n \cong B_n \quad \text{for } n \geqslant n_0.$$

Proof. Let $n \geqslant m \geqslant 0$. Let $G_{n,m} = \mathrm{Gal}(F_n/F_m)$. Since $\chi \neq 1$, the χ-part of the $G_{n,m}$-cohomology groups of the idèle class group of F_n is trivial. Since $\chi(p) \neq 1$, the χ-part of the $G_{n,m}$-cohomology groups of the group of unit idèles of F_n is also trivial [9, Sect. 4]. This implies that there is a canonical isomorphism

$$\hat{H}^q(G_{n,m}, O_n^*(\chi)) \cong \hat{H}^{q-2}(G_{n,m}, A_n), \quad \text{for all } q \in \mathbf{Z}.$$

Since the group $\mathrm{Cyc}_n(\chi)$ is cohomologically trivial and since G_n is cyclic this implies that there is a G_m-isomorphism

$$\hat{H}^q(G_{n,m}, B_n) \cong \hat{H}^q(G_{n,m}, A_n), \quad \text{for all } q \in \mathbf{Z}.$$

Since $\lambda = 0$, the groups A_n and B_n stabilize. Therefore there is an integer N such that Nth power of the maximal ideal $\mathfrak{m} = (p, T)$ of Λ kills both A_n and B_n for all n. Take $m \geqslant N$ and $n = 2m$. Then both ω_m and the $G_{n,m}$-norm are contained in $\mathfrak{m}^N$. Therefore $\hat{H}^0(G_{n,m}, B_n) = B_n$ and $\hat{H}^0(G_{n,m}, A_n) = A_n$.

This implies that $A_n \cong B_n$ as G_n-modules for large n and therefore for each $n \geqslant n_0$. This proves the proposition. □

PROPOSITION 2.7. *Suppose that the sequence of modules C_n stabilizes: $C = C_n$ if for $n \geqslant n_0$. Then*

(i) *there is for each $m \geqslant 0$ an exact sequence*

$$0 \to A_m^{\text{dual}} \to C \xrightarrow{\omega_m} C \to B_m^{\text{dual}} \to 0.$$

(ii) *For every $0 \leqslant m \leqslant m'$ there is a commutative diagram:*

$$\begin{array}{ccc} A_{m'}^{\text{dual}} & \xrightarrow{\cong} & C[\omega_{m'}] \\ \downarrow{\scriptstyle j_{m,m'}^{\text{dual}}} & & \downarrow{\scriptstyle N_{m',m}} \\ A_m^{\text{dual}} & \xrightarrow{\cong} & C[\omega_m] \end{array}$$

Here $j_{m,m'}$ denotes the natural map $A_m \to A_{m'}$.

Proof. Suppose that $N \geqslant n_0$ is so large that $\mathfrak{m}^N$ kills C. Let $n \geqslant m + N$. Then the norm map norm $N_{n,m}$ is contained in $\mathfrak{m}^N$ and the kernel of the map $\omega_m\colon\ C \to C$ is the zeroth $G_{n,m}$-Tate cohomology group of C_n. By cohomological duality, this group is dual to $\hat{H}^1(G_{n,m}, B_n) \cong \hat{H}^1(G_{n,m}, O_n^*(\chi))$. Since $\chi(p) \neq 1$ the χ-part of the cohomology groups of the idèle units of F_n is trivial. This implies that

$$\ker(A_m \to A_n) \cong H^1(G_{n,m}, O_n^*(\chi)).$$

Therefore $C[\omega_m]$ is dual to $\ker(A_m \to A_n)$, which is just A_m if n is sufficiently large. This proves part (i).

To prove (ii) it suffices to observe that the following diagram is commutative

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_{m'}^{\text{dual}} & \longrightarrow & C & \xrightarrow{\omega_{m'}} & C & \longrightarrow & B_{m'}^{\text{dual}} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle j_{m,m'}^{\text{dual}}} & & \downarrow{\scriptstyle N_{m',m}} & & \downarrow{\scriptstyle \text{id}} & & \downarrow{\scriptstyle \text{Res}} & & \\
0 & \longrightarrow & A_m^{\text{dual}} & \longrightarrow & C & \xrightarrow{\omega_m} & C & \longrightarrow & B_m^{\text{dual}} & \longrightarrow & 0
\end{array}$$

We leave this straightforward verification to the reader. □

It is well known that A_m is in general not isomorphic to B_m. Therefore Proposition 2.6 does not hold for every $n \geqslant 0$. By Proposition 2.7 the group A_0 is dual to the kernel of $T\colon\ C \to C$ while B_0 is dual to the cokernel C/TC. Note that $\ker(T)$ can be non-cyclic even though $\operatorname{cok}(T)$ is always cyclic. For instance, if $I = \mathfrak{m}^j$, then

$$\begin{aligned}
\operatorname{coker}(T) &\cong \mathbf{Z}/p^j\mathbf{Z}, \\
\ker(T) &\cong \underbrace{\mathbf{Z}/p\mathbf{Z} \times \cdots \times \mathbf{Z}/p\mathbf{Z}}_{j \text{ times}}.
\end{aligned}$$

Two explicit examples of such ideals I are provided by $f = 32009$ and $f = 62501$. In both cases $I = \mathfrak{m}^2$ and the sequence of class groups stabilizes at level 1.

3. Upper bounds

In this section and the next we explain how we compute the groups C_n. In this section we discuss our method to obtain *upper bounds* for the modules C_n. In practice these upper bounds are actually sharp, but this is only verified by means of the calculations explained in Section 4 where we discuss our method to obtain rigorous *lower bounds* for the C_n.

By Proposition 2.5 we have the following explicit expression:

$$C_n/p^kC_n = \mathbf{Z}/p^k\mathbf{Z}[G_n]/\{f_r : r \text{ is split in } F_n(\zeta_{p^k})\},$$

where we have written f_r for $f_r(\eta_n)$. This result enables us to compute the modules C_n at every level n: to calculate C_n/p^kC_n for a given prime power p^k, we compute many elements $f_{r_1}, f_{r_2}, \ldots$. If we have computed "enough" of them, we have found the full ideal $\{f_r : r \text{ is split in } F_n(\zeta_{p^k})\}$ and hence, by Proposition 2.5, we know C_n/p^kC_n. If C_n/p^kC_n is already killed by p^{k-1}, then apparently $C_n = C_n/p^kC_n$ and we have found C_n itself. In practice we can rarely be sure to have computed sufficiently many elements f_r, but, in any case, C_n/p^kC_n is a *quotient* of $\mathbf{Z}/p^k\mathbf{Z}[G_n]/\langle f_{r_1}, f_{r_2}, \ldots\rangle$. If in addition p^{k-1} annihilates C_n/p^kC_n, we have therefore rigorously computed an "upper bound" for $C_n = C_n/p^kC_n$.

To investigate the behaviour in the $\mathbf{Z}_p$-extension, we compute the modules $C_0, C_1, C_2, \ldots$, as explained above. If one finds that $C_n = C_{n+1}$ for a certain n, then by Corollary 2.3 the modules C_n stabilize at this point: $C_m = C_n$ for each $m \geqslant n$ and $C = C_n$.

In practice, one simply computes the groups C_m/p^kC_m for some reasonably large k at some moderately high levels $m = n$ and $m = n + 1$. When $C_{n+1}/p^kC_{n+1} = C_n/p^kC_n$ and this group is killed by p^{k-1} one knows that $C_n = C_n/p^kC_n$ and that, most likely, $C = C_n$. One can recover the structure of the groups A_n and B_n at every level, by applying Proposition 2.7.

What do the f_r look like on a computer? Identifying the generator $p + 1$ of G_n with X, we write

$$\mathbf{Z}/p^k\mathbf{Z}[G_n] \cong \mathbf{Z}/p^k\mathbf{Z}[X]/(X^{p^n} - 1).$$

In this way the elements f_r become polynomials in X. The "logarithmic map" $\log_{\mathfrak{p}} : (O_n/\mathfrak{p})^* \to \mathbf{Z}/p^k\mathbf{Z}$ can be computed as follows: we choose (once and for all) a generator ζ for the subgroup of p^kth roots of unity in $\mathbf{Z}/r\mathbf{Z}$. Then $\log_{\mathfrak{p}}(x)$ is the discrete logarithm with respect to ζ of $x^{(r-1)/p^k}$. Finally, rather than fixing a cyclotomic unit $1 - \zeta_{p^{n+1}}\zeta_f$ and permuting the prime ideals $\mathfrak{p}$ with the Galois group, we fix one prime ideal $\mathfrak{p}$ over r and permute the cyclotomic units with the Galois group. The choices of ζ and $\mathfrak{p}$ are not important; they only change f_r by a unit.

We only give the formula for $p = 3$. The condition $\chi(p) \neq 1$ means that $f \not\equiv 1 \pmod 3$. When $f \equiv 2 \pmod 3$ we get

$$f_r(\eta_n) = \sum_{y \in \mathbf{Z}/3^n\mathbf{Z}} \sum_{\substack{x \in (\mathbf{Z}/f\mathbf{Z})^* \\ (\frac{f}{x})=1}} \log_r \left(\frac{(1 - \zeta^{4^y}\zeta_f^x)(1 - \zeta^{-4^y}\zeta_f^x)}{(1 - \zeta^{4^y}\zeta_f^{gx})(1 - \zeta^{-4^y}\zeta_f^{gx})} \right) \cdot X^y. \qquad (1)$$

Here $g \in (\mathbf{Z}/f\mathbf{Z})^*$ satisfies $(\frac{f}{g}) = -1$ and ζ is a primitive 3^{n+1}th root of 1 modulo r. We have written $\log_r$ for $\log_{\mathfrak{p}}$; the summation over x corresponds to the norm to $F_n(\zeta_3) = \mathbf{Q}(\zeta, \sqrt{f})$.

The four factors inside the logarithm are projections into the correct χ-eigenspace: the factors in the numerator correspond to the norm to $F_n = \mathbf{Q}_n(\sqrt{f})$. The denominator is just σ applied to the numerator, where σ generates $\mathrm{Gal}(\mathbf{Q}(\sqrt{f})/\mathbf{Q})$. In other words, the quantity in the log is just $(1+\tau)(1-\sigma)$ applied to $(1-\zeta^{4y}\zeta_f^x)$. Here τ is the non-trivial automorphism of $\mathbf{Q}(\zeta_3)$. For computational purposes, the formulas should be modified a little. It is not difficult to see that, up to a 3-adic unit, we have

$$f_r(\eta_n) = \sum_{y \in \mathbf{Z}/3^n\mathbf{Z}} \log_r \left(\prod_{x \in (\mathbf{Z}/f\mathbf{Z})^*} (\zeta^{4y} - \zeta_f^x)^{\left(\frac{f}{x}\right)} \right) \cdot X^y \in \mathbf{Z}/3^k\mathbf{Z}[X]/(X^{3^n}-1). \quad (2)$$

When $f \equiv 0 \pmod 3$, the resulting formulas are practically the same as the ones for the case $f \equiv 2 \pmod 3$. There are slight differences because of the definition of the cyclotomic units. The analogue of formula (1) of the previous section is:

$$f_r(\eta_n) = \sum_{y \in \mathbf{Z}/3^n\mathbf{Z}} \sum_{\substack{x \in (\mathbf{Z}/f\mathbf{Z})^* \\ (\frac{f'}{x})=1}} \log_r \left(\frac{(1-\zeta^{4y}\zeta_{f'}^x)(1-\zeta^{-4y}\zeta_{f'}^{-x})}{(1-\zeta^{4y}\zeta_{f'}^{-x})(1-\zeta^{-4y}\zeta_{f'}^x)} \right) \cdot X^y. \quad (1')$$

Here f' denotes $f/3$. Since $\mathbf{Q}(\sqrt{f})$ is a real quadratic field, $\mathbf{Q}(\sqrt{-f'})$ is complex and $(\frac{-1}{f'}) = -1$. So, in terms of the formula in the case $f \equiv 2 \pmod 3$, we have taken $g = -1$ in this case. The sum over x corresponds to the norm to $\mathbf{Q}(\zeta, \sqrt{f'}) = F_n(\zeta_3, \sqrt{f'})$. The products within the numerator and denominator correspond to the norm from $F_n(\zeta_3, \sqrt{f'})$ to $\mathbf{Q}_n(\sqrt{3f'}) = F_n$. Finally we project the unit into the χ-eigenspace by applying $1-\sigma$.

As in the case $f \equiv 2 \pmod 3$, we modify the formula a little bit. Proceeding as before, we find the following expression:

$$f_r(\eta_n) = \sum_{y \in \mathbf{Z}/3^n\mathbf{Z}} \log_r \left(\prod_{x \in (\mathbf{Z}/f'\mathbf{Z})^*} (\zeta^{4y} - \zeta_{f'}^x)^{\left(\frac{f'}{x}\right)} \right) X^y$$
$$\in \mathbf{Z}/3^k\mathbf{Z}[X]/(X^{3^n}-1). \quad (2')$$

Notice that this time $\left(\frac{f'}{x}\right)$ is an odd character.

When f is large, computing the product in (2) and (2′) is a lot of work. It is important to *first* compute the products and *then* take their logarithms (only 3^n of them). Usually, it is not necessary to take n large than 0 or 1, because the class groups are all trivial or stabilize immediately. Occasionally, however, one may wish to consider $n = 2, 3, 4, \ldots$: In these cases it might be useful to have a table of the quadratic residue symbols modulo f. So far, we have always recomputed

all of them for each new auxiliary prime r. The choice of k hardly effects the running times when n is small: computing modulo 3^{10} is as efficient as computing modulo 3; only computing the few discrete logarithms is a lot slower when k is large.

In order to compute the ideal generated by the f_r in the ring $\mathbf{Z}/p^k\mathbf{Z}[X]/(X^{p^n}-1)$ it is convenient to convert everything to the parameter $T = X - 1$. Then the ring becomes isomorphic to $\mathbf{Z}/p^k\mathbf{Z}[T]/(\omega_n)$ where $\omega_n = (1+T)^{p^n} - 1$. This is a finite local ring with maximal ideal (p, T). It is a Gorenstein ring and its unique minimal ideal is generated by $p^{k-1}T^{p^n-1}$.

In our case

$$f_r \in \mathbf{Z}/3^k\mathbf{Z}[T]/((1+T)^{3^n} - 1).$$

In practice, we apply the Weierstraß-Preparation Theorem and compute the "distinguished parts" of f_r, i.e. we compute a Weierstraß polynomial $\tilde{f}_r$ such that $f_r = \tilde{f}_r$ up to a unit.

EXAMPLE 3.1. This is an example of what usually happens: let $f = 761$. In this case $h_0 = 3$. We take, somewhat arbitrarily, $p^k = 27$ and $n = 1$. So, the coefficients of the f_r are computed modulo 27 and the f_r are elements of the ring $\mathbf{Z}/27\mathbf{Z}[T]/(T^3 + 3T^2 + 3T)$.

r	$\tilde{f}_r$
82189	$3T^2 + 9T + 9$
164377	$T + 12$
328753	$T^2 + 12T + 9$
575317	T
616411	$T + 21$
739693	$3T^2 + 18T$
904069	$T^2 + 21T + 21$
986257	T

It is easily seen that the f_r generate the maximal ideal $\mathfrak{m}$ of $\Lambda/(\omega_1)$ in this case. Therefore

$$C_1 \cong \Lambda/\mathfrak{m} \cong \mathbf{Z}/3\mathbf{Z} \cong C_0.$$

By Proposition 2.2, this implies that $C = C_1 = C_0$. Note that, since $\Lambda/\langle \tilde{f}_{r_1}, \ldots, \tilde{f}_{r_t} \rangle$ is certainly an *upper bound* for C, we have a complete proof in this case: the tower of class groups stabilizes immediately at level 0. All the norm maps in the towers are isomorphisms and all the maps $j_{m,m'}: A_m \to A_{m'}$ are zero ($m < m'$).

EXAMPLE 3.2. $f = 4749$. Here's an example where the class groups grow a little bit in the $\mathbf{Z}_3$-extension. The class group of $\mathbf{Q}(\sqrt{f})$ is cyclic of order 3. We compute the following elements at level 1 modulo 27:

r	$\tilde{f}_r$
683857	$T+6$
769339	$T+24$
1282231	$3T+18$
1367713	$T+6$
1624159	$T+24$
2222533	$T+6$
2393497	$T+15$

All polynomials have 3 as a zero modulo 9. We move to level 2 and compute the following elements modulo the ideal $(\omega_2, 81)$:

r	$\tilde{f}_r$
769339	$T+24$
1282231	$T^5+60T^4+63T^3+3T^2+39T+45$
3846691	$T+51$
4359583	$T+24$
5898259	$T+24$
6667597	$T+51$
7180489	$T+51$

Once more, all polynomials $\tilde{f}_r$ have 3 as a zero; this time modulo 27. Once more, we move up one level in the $\mathbf{Z}_3$-extension. At level 3, modulo the ideal $(\omega_3, 243)$ we find

r	$\tilde{f}_r$
769339	$T+186$
3846691	$T+240$
16925437	$T+240$
22310803	$T^2+102T+36$
23849479	$T+78$
27696169	$T+240$
36158887	$T+105$

This time the polynomials again generate the ideal $(T-3, 27)$. Since the computations were done modulo 3^5, we conclude that the module $C_3/3^5C_3$ is equal to C_3. Since we tried so many primes r we are actually led to believe that the class groups stabilize at this point and that

$$C \cong C_3 \cong \Lambda/(T-3, 27) \cong \mathbf{Z}/27\mathbf{Z}.$$

Taking covariants we see that $C_0 \cong C/TC \cong \mathbf{Z}/3\mathbf{Z}$. Similarly $C_1 \cong C/\omega_1 C \cong \mathbf{Z}/9\mathbf{Z}$ and $C_2 = C \cong \mathbf{Z}/27\mathbf{Z}$. Using Proposition 2.7 one easily sees that A_0, A_1, A_2 are cyclic of order 3, 9 and 27 respectively. The maps $A_0 \hookrightarrow A_1 \hookrightarrow A_2$ are injective. It is not difficult to see that, in general, all ideal classes in A_k become only trivial in A_{k+3}.

EXAMPLE 3.3. $f = 6396$. This is a somewhat "exotic" example. We computed the following polynomials modulo 27 at level 1.

r	$\tilde{f}_r$
230257	$T^2 + 21T + 3$
287821	$T^2 + 24T + 21$
462949	$T^2 + 24T + 21$
1036153	$T^2 + 21T + 12$
1093717	$T^2 + 6T + 21$
1266409	$9T$
1381537	$T^2 + 3T + 21$

The polynomials $\tilde{f}_r$ generate the Λ-ideal $(T^2 + 3, 3T, 9)$. At level 2 we find, computing modulo 27,

r	$\tilde{f}_r$
230257	$T^2 + 12T + 12$
287821	$T^2 + 15T + 21$
462949	$T^2 + 24T + 21$
1036153	$T^2 + 21T + 12$
1093717	$T^2 + 6T + 12$
1266409	$T^3 + 3T^2 + 21T$
1381537	$T^2 + 12T + 3$

The $\tilde{f}_r$ generate the same ideal as before. This proves that C is isomorphic to a quotient of $\Lambda/(T^2 + 3, 3T, 9)$. In the next section we describe the computations that prove that actually $C \cong \Lambda/(T^2 + 3, 3T, 9)$.

4. Lower bounds

Our method to prove that the Λ-modules $\Lambda/(f_{r_1}, \ldots, f_{r_t})$ that we have computed using the method of Section 3 are actually equal to the module C, is similar to the one employed by G. Gras and M.-N. Gras in [3]. It is based on very accurate approximations of the cyclotomic units in $\mathbf{R}$. If one only wants to show that $\lambda = 0$, one can avoid the computations of this section as follows. If $\lambda > 0$, then by

Proposition 2.2 we have that $\#C_n \geqslant p^{n+1}$ for every $n \geqslant 0$. Therefore it suffices to show that $\#C_n \leqslant p^n$ for some n and this can be done using the method of the previous section.

Let p^k be a power of p and let $n \geqslant 0$. We let

$$R_n = \mathbf{Z}/p^k\mathbf{Z}[G_n].$$

We saw in the proof of Theorem 2.4 that this ring is a Gorenstein ring and that the R_n-module $\mathrm{Hom}_{\mathbf{Z}}(R_n, \mathbf{Q}/\mathbf{Z})$ is free over R_n of rank 1. For every finite R_n-module M there is an isomorphism $\mathrm{Hom}_{\mathbf{Z}}(M, \mathbf{Q}/\mathbf{Z}) \cong \mathrm{Hom}_{R_n}(M, \mathrm{Hom}_{\mathbf{Z}}(R_n, \mathbf{Q}/\mathbf{Z})) \cong \mathrm{Hom}_{R_n}(M, R_n)$. Because of our identification of $\mathrm{Hom}_{\mathbf{Z}}(R_n, \mathbf{Q}/\mathbf{Z})$ with R_n, this is, in general, not an isomorphism of R_n-modules. For instance, when M is an R_n-ideal I, we have that $\mathrm{Hom}(I, \mathbf{Q}/\mathbf{Z}) \cong \mathrm{Hom}_{R_n}(I, R_n) \cong \mathrm{Ann}(I)$, but the natural actions of G_n on $\mathrm{Hom}(I, \mathbf{Q}/\mathbf{Z})$ and $\mathrm{Ann}(I)$ do not agree. One is the inverse of the other.

Let $\hat{}\colon R_n \to R_n$ denote the involution of R_n induced by $\sigma \mapsto \sigma^{-1}$ for $\sigma \in G_n$. If $A \subset R_n$ is any subset, then $\hat{A}$ denotes the subset $\{\hat{x} : x \in A\}$.

Our method is based on the following proposition.

PROPOSITION 4.1. *Let $n \geqslant 0$ and let p^k be a power of p that annihilates C_n (and hence B_n). Let R_n denote the group ring $\mathbf{Z}/p^k\mathbf{Z}[G_n]$ and let I_n be an R_n-ideal that annihilates C_n. Then $C_n \cong R_n/I_n$ if and only if* $\mathrm{Ann}(\hat{I}_n)$ *annihilates the module* $\mathrm{Cyc}_n(\chi)/O_n^*(\chi)^{p^k}$.

Proof. From the diagram of the proof of Theorem 2.4 we obtain the exact sequence

$$0 \to B_n \to \mathrm{Cyc}_n(\chi)/\mathrm{Cyc}_n(\chi)^{p^k} \to \mathrm{Cyc}_n(\chi)/O_n^*(\chi)^{p^k} \to 0,$$

where the first arrow is given by $\varepsilon \mapsto \varepsilon^{p^k}$.

Since $\mathrm{Cyc}_n(\chi)/\mathrm{Cyc}_n(\chi)^{p^k}$ is free of rank 1 over R_n, we see that $\mathrm{Ann}(\hat{I}_n)$ annihilates the module $\mathrm{Cyc}_n(\chi)/O_n^*(\chi)^{p^k}$ if and only if $B_n \cong J$ for some R_n-ideal J containing $\mathrm{Ann}(\hat{I}_n)$. Since R_n is a Gorenstein ring, this means that $C_n \cong \mathrm{Hom}_{R_n}(\hat{J}, R_n) \cong R_n/\mathrm{Ann}(\hat{J})$ and that C_n admits a surjective R_n-morphism $C_n \to R_n/\mathrm{Ann}(\mathrm{Ann}(I_n))$. Since $I_n = \mathrm{Ann}(\mathrm{Ann}(I_n))$, we see that $\mathrm{Ann}(\hat{I}_n)$ annihilates $\mathrm{Cyc}_n(\chi)/O_n^*(\chi)^{p^k}$ if and only if there is a surjective R_n-morphism $C_n \to R_n/I_n$. The proposition now follows from the fact that I_n kills C_n. □

We use this proposition as follows: suppose we know that C_n is annihilated by p^k and that it is a quotient of R_n/I_n for some ideal I_n. To prove that $C_n \cong R_n/I_n$ we compute a finite set Σ of generators of the ideal $\mathrm{Ann}(\hat{I}_n) \subset R_n$ and we attempt to show that each $x \in \Sigma$ annihilates $\mathrm{Cyc}_n(\chi)/O_n^*(\chi)^{p^k}$, i.e.,

$$\eta_n^x \in O_n^{*p^k} \quad \text{for } x \in \Sigma.$$

To show this, we compute very accurate approximations $\eta^{(i)} \in \mathbf{R}$ to η_n and its conjugates. From these approximations we compute the minimal polynomial $F(Y) \in \mathbf{Z}[Y]$ of η_n. This polynomial has degree $2p^n$. For each $x \in \Sigma$ we pick a representative $x \in \mathbf{Z}[G_n]$ with small coefficients

$$x = \sum_{k=1}^{p^n} a_k \gamma^k, \quad a_k \in \mathbf{Z}, |a_k| < p^k/2...$$

Here $\gamma \in G_n$ is the generator corresponding to $p+1$ and $T+1$. Next we compute very accurate approximations $\varepsilon^{(i)} \in \mathbf{R}$ of

$$\varepsilon = \eta_n^x = \prod_{k=1}^{p^n} \gamma_k \left(\eta_n^{a_k}\right)$$

and use these to compute the minimum polynomial $G(Y) \in \mathbf{Z}[Y]$ of ε. Finally we compute the p^kth roots of the $\varepsilon^{(i)}$ and the polynomial

$$H(Y) = \prod_{i=1}^{2p^n} \left(Y - \sqrt[p^k]{\varepsilon^{(i)}}\right) \in \mathbf{R}[Y].$$

If indeed $\eta^x \in O_n^{*p^k}$, then the polynomial $H(Y)$ has integral coefficients. In practice one is quickly convinced when one finds that the coefficients of H are very close to integers. However, this time one does not yet know that the zeroes are contained in a field of degree $2p^n$. One can prove this by checking that the integral polynomial close to $H(Y)$ divides the polynomial $G(Y^{p^k})$. This completes the description of the method.

In practice the polynomials F, G and H have gigantic coefficients. Therefore it is necessary to use extremely accurate approximations of the cyclotomic units. For the sake of efficiency we begin our computation of the $\eta^{(i)}$ using only a moderate accuracy of 100 or so decimal digits, just enough to "recognize" the integral coefficients of the polynomial $F(Y) \in \mathbf{Z}[Y]$. Then we recompute the $\eta^{(i)}$ using Newton's method. This is very efficient and provides us without excessive effort with an accuracy of 500–5000 decimal digits. The computation of the polynomials $G(Y)$ and $H(Y)$ is then completed using these high accuracy approximations.

We discuss only one fairly small example. See Example 3.3 for the upper bounds in this case. We used UBASIC and PARI to do the calculations. In the cases where the class groups seemed to stabilize at level 2 in the tower, it was necessary to do the computations with an accuracy of several thousands of decimal digits.

EXAMPLE 4.2. $f = 6396$. In this case the Λ-ideal that we have found with the method of Section 3 is $(T^2+3, 3T, 9)$. Therefore C is a quotient of the module $\Lambda/(T^2+3, 3T, 9)$. Since $\omega_1 = T^3 + 3T^2 + 3T \in I$, we have $C = C_1$. We take $p^k = 9$.

We must show that $C_1 \cong R_1/I_1$. Here $R_1 = \mathbf{Z}/9\mathbf{Z}[T]/(T^3 + 3T^2 + 3T)$ and $I_1 = (T^2+3, 3T)$. The annihilator $\mathrm{Ann}(\hat{I}_1)$ is $(T^2, 3T)$. Let γ denote the generator of G_1 corresponding to $T + 1$. We have to show that

$$\eta_1^{3(\gamma-1)} \qquad \text{and} \qquad \eta_1^{(\gamma-1)^2}$$

are ninth powers in O_1^*. Equivalently, we must check the following:

$$\begin{aligned} \varepsilon &= \gamma(\eta_1)\eta_1^{-1} \quad \text{is a cube in } O_1^*? \\ \varepsilon' &= \gamma^2(\eta_1)\gamma(\eta_1)^{-2}\eta_1 \quad \text{is a ninth power in } O_1^*? \end{aligned}$$

To do this we first compute, for $i = 1, 2, \ldots, 6$, the approximations $\eta^{(i)} \in \mathbf{R}$ to η_1:

$$\begin{aligned} \eta^{(1)} = {} & 1067549470063620065824 2.740540292555723835910871383683 \\ & 866586357611513327567014852500109494561638321936678 \\ & 553478375272623757799072935037446942559837408645801 0 \\ & 5998766704\ldots \end{aligned}$$

$$\begin{aligned} \eta^{(2)} = {} & 0.000000000000000000000009367247402037542207472700 48 \\ & 395365574340460989450635312309224496356940245654 29 \\ & 544350150600582766365281775623597235308105397\ldots \end{aligned}$$

$$\begin{aligned} \eta^{(3)} = {} & -14078828366.722653076449023695048411081882917041 37 \\ & 123619543632215197836226002272135218032291828451139 \\ & 566857180404948859131441299479193352192051881 84 \\ & 15486098\ldots \end{aligned}$$

$$\begin{aligned} \eta^{(4)} = {} & -0.000000000071028637749689783839091047435124687 88 \\ & 097966942383833506669831583582299601465808086993 4 \\ & 992938698903368897373464795839691595355729114578\ldots \end{aligned}$$

$$\begin{aligned} \eta^{(5)} = {} & -0.000000000456363420961354843563600631834840808 9 \\ & 991434410573201591049897836806073242720662822771 6 \\ & 133011050860668167236331957902637317764363207334 4\ldots \end{aligned}$$

$$\eta^{(6)} = -2191236094.01788725227915662983172510155679831341663418602115097558316330285399177566667135173374772736159678225561342739344715401182934983315958530192358\ldots$$

Here $\gamma^{(i+1)}$ is the inverse of $\gamma^{(i)}$ for $i = 1, 3, 5$. The number $\eta^{(3)}$ is an approximation to $\gamma(\eta_1)$ and $\eta^{(5)}$ is an approximation to $\gamma^2(\eta_1)$.

The minimum polynomial is

$$F(Y) = Y^6 - 106754947006199305937 82Y^5 - 1736909869296141720428004235121 61Y^4 - 3293394052124122192489974559566706336043 72Y^3 - 1736909869296141720428004235121 61Y^2 - 106754947006199305937 82Y + 1.$$

The minimum polynomial of ε is

$$G(Y) = Y^6 + 233925293094998728761627513577 86Y^5 - 7216603741460643440710978894293329284723290832349 13Y^4 - 5472104274972539200423645787625957327745929397407 25519246576052Y^3 - 7216603741460643440710978894293329284723290832349 13Y^2 + 233925293094998728761627513577 86Y + 1$$

and the minimum polynomial of its cube roots is

$$H(Y) = Y^6 + 28596413658Y^5 - 89436172566759393Y^4 - 8179337463 87389632436Y^3 - 89436172566759393Y^2 + 28596413658Y + 1.$$

It divides $G(Y^3)$. Similarly, the minimum polynomial of ε' is given by

$$G'(Y) = Y^6 + 7216603741460643440477053601198330555961663318771 30Y^5 - 1280063596371034895331917342401311892871217918833759541688955207285148540737850055071600048 1Y^4 - 5207937212139095017490961472922001037290723881761745355373113259335257233979577714767781183581852836 04Y^3 - 1280063596371034895331917342401311892871217918833759541688955200147285148540737850055071600048 1Y^2$$

$$+72166037414606434404770536011983305559616633187 7$$
$$130Y + 1.$$

Finally, the polynomial $H'(Y)$, minimum polynomial of $\sqrt[9]{\varepsilon'}$ is equal to

$$H'(Y) = Y^6 + 383754Y^5 - 28596797409Y^4 - 204459959828Y^3$$
$$-28596797409Y^2 + 383754Y + 1.$$

It divides $G'(Y^9)$.

5. Results

We have computed the Iwasawa modules C for all quadratic fields $\mathbf{Q}(\sqrt{f})$ of conductor $f < 10000$ with $f \not\equiv 1 \pmod 3$. In this section we present the numerical results.

First of all, in every case C turns out to be finite. This implies that the sequence of class groups A_n stabilizes. In other words, the projective limit

$$\lim_{\leftarrow} A_n$$

is finite. Equivalently:

THEOREM 5.1. *For all quadratic fields $\mathbf{Q}(\sqrt{f})$ of conductor $f < 10000$ with $f \not\equiv 1 \pmod 3$ the Iwasawa invariants λ associated to the cyclotomic $\mathbf{Z}_3$-extension of $\mathbf{Q}(\sqrt{f})$ are zero.*

For any real quadratic field of conductor $f \not\equiv 1 \pmod 3$ with $A_0 = 0$, i.e. with class number not divisible by 3, the Iwasawa module C is trivial. This is an easy consequence of Nakayama's Lemma.

There are 144 real quadratic fields of conductor $f < 10000$ with $f \not\equiv 1 \pmod 3$ that have $A_0 \neq 0$. In these cases $C \cong \Lambda/I$ for some non-trivial Λ-ideal I. In 110 cases we found that I is equal to the maximal ideal $\mathfrak{m} = (T, 3)$ of Λ. In these cases all groups A_n, B_n and C_n have order 3 and all maps $A_m \to A_n$ are zero $(n > m)$. Splitting the cases $f \equiv 0, 2 \pmod 3$ we have $I = \mathfrak{m}$ in 45 out of 54 cases when $f \equiv 0 \pmod 3$ and in 65 out of 90 cases when $f \equiv 2 \pmod 3$.

The remaining 34 cases are listed in the table below. In the first column the Λ-ideal I for which $C \cong \Lambda/I$ is given. In the second column the group structure of C is given; this can be deduced easily from the ideal I in column 1. By $a_1 \times a_2 \times \cdots \times a_t$ we indicate the group $\mathbf{Z}/a_1\mathbf{Z} \times \mathbf{Z}/a_2\mathbf{Z} \times \cdots \times \mathbf{Z}/a_t\mathbf{Z}$. In column 3 we have listed the level n_0 where stabilization occurs: $C_n = C_{n_0}$ for all $n \geqslant n_0$. By Corollary 2.6 these entries can also be deduced easily from the ideals in column 1. The remaining columns contain the conductors of the quadratic fields and various frequencies.

Table 5.2.

I	C	n_0	freq.	$f \equiv 0 \pmod 3$	$f \equiv 2 \pmod 3$
$(T, 9)$	9	0	0 + 3		3137, 4409, 6809
$(T-3, 9)$	9	1	0 + 2		4481, 7709
$(T+3, 9)$	9	1	3 + 6	3957, 7032, 7053	1772, 2777, 7244, 8069, 8396, 8837
$(T^2, 3)$	3 × 3	1	1 + 2	8745	4001, 6401
$(T-3, 27)$	27	2	1 + 1	4749	5297
$(T-12, 27)$	27	2	0 + 6		473, 785, 2021, 3569, 3596, 7601
$(T+12, 27)$	27	2	0 + 2		5081, 6584
$(T+3, 27)$	27	2	2 + 1	5613, 9813	2429
$(T^3, 3)$	3 × 3 × 3	1	0 + 2		1937, 3305
$(T^2+3, 3T, 9)$	3 × 9	1	1 + 0	6396	
$(T^2-3, 9)$	9 × 9	2	1 + 0	5529	

The very first entry of Table 5.2 contains the only three cases where C/TC has order 9. In these cases stabilization happens to occur at level $n_0 = 0$. In the remaining 31 cases C/TC has order 3. Using Corollary 2.6 it is easy to figure out the behaviour of the class groups A_n and the maps $A_n \to A_{n'}$ in the $\mathbf{Z}_3$-extension of $\mathbf{Q}(\sqrt{f})$. The groups A_n "grow" and "become" isomorphic to A_{n_0} when $n \geqslant n_0$; the maps $A_n \to A_{n'}$ are zero when the difference $n' - n$ is sufficiently large. We only discuss the last entry of the table as an example.

Let $F = F_0 = \mathbf{Q}(\sqrt{5529})$. In this case

$$\begin{aligned} C_0 &= C/TC \cong \Lambda/(T, T^2-3, 9) = \Lambda/(T, 3) \cong \mathbf{Z}/3\mathbf{Z}, \\ C_1 &= C/\omega_1 C \cong \Lambda/(T^3+3T^2+3T, T^2-3, 9) = \Lambda/(3T, T^2-3, 9) \\ &\cong \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}, \\ C_2 &= C/\omega_2 C \cong \Lambda/(\omega_2, T^2-3, 9) = \Lambda/(T^2-3, 9) \cong \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}. \end{aligned}$$

The last line follows from the fact that $\omega_2 = (1+T)^9 - 1$ is contained in the ideal $I = (T^2-3, 9)$. Stabilization of the groups C_n occurs at level $n = 2$. We have that $C_n = C_2$ for $n \geqslant 2$.

By Corollary 2.6 the class groups A_n are dual to $C[\omega_n]$. It is easy to see that

$$\begin{aligned} A_0 &\cong \mathbf{Z}/3\mathbf{Z}, \\ A_1 &\cong \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}, \\ A_n &\cong \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}, \quad \text{for } n \geqslant 2. \end{aligned}$$

The kernels of the maps $j_{n,n'} : A_n \to A_{n'}$ are dual to $(C/N_{n,n'}C)[\omega_n]$. For all $n' \geqslant n+2$, the maps $j_{n,n'}$ are zero. For $n \geqslant 1$ the maps $j_{n,n+1}$ have kernels isomorphic to $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. Finally, $j_{0,1}$ is the zero map.

References

[1] Candiotti, A.: Computations of Iwasawa invariants and K_2, *Compositio Math.*, **29** (1971), 89–111.

[2] Cassels, J. W. S. and Fröhlich, A.: *Algebraic Number Theory*, Academic Press, London 1967.

[3] Gras, G. and Gras, M.-N.: Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\mathbf{Q}$, *Bulletin des Sciences Math.* **101** (1977), 97–129.

[4] Greenberg, R.: On the Iwasawa invariants of totally real number fields, *American J. of Math.* **98** (1976), 263–284.

[5] Greenberg, R.: A note on K_2 and the theory of $\mathbf{Z}_p$-extensions, *American J. of Math.* **100** (1978), 1235–1245.

[6] Kraft, J. S.: Iwasawa invariants of CM fields, *Journal of Number Theory* **32** (1989), 65–77.

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

[8] Schoof, R.: Class numbers of $\mathbf{Q}(\cos(2\pi/p))$, in preparation.

[9] Schoof, R.: The structure of minus class groups of abelian number fields, 185–204, in C. Goldstein, *Séminaire de Théorie de Nombres*, Paris 1988–1990, Progress in Math. **91**, Birkhäuser 1990.

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

[11] Taya, H.: Computation of $\mathbf{Z}_3$-invariants of real quadratic fields, *Math. Comp.*, to appear.

[12] Washington, L. C.: *Introduction to Cyclotomic Fields*, Graduate Texts in Math. **83**, Springer-Verlag, Berlin, Heidelberg, New York 1982.