Università degli studi di Roma
"La Sapienza"
Facoltà di Scienze Matematiche Fisiche e Naturali

Dottorato di Ricerca in Matematica
XXXIII ciclo

Class group behaviour in cyclotomic extensions of abelian fields

Autore: Lorenzo Pagani

Relatore: René Schoof

Sapienza
Università di Roma

Contents

Introduction

Let K be a number field. Understanding the ideal class group Cl_K of the field K is a classical problem in algebraic number theory. Solving this problem is hard, especially if the discriminant of the field K is large. However, we can get interesting results focusing on the ℓ-part of Cl_K for a fixed prime ℓ rather than focusing on the full class group. In this thesis we restrict our attention to the fields appearing in cyclotomic $\mathbb{Z}_p$-extensions of abelian number fields K.

Why abelian fields? Denote by $X(K)$ the group of Dirichlet characters associated to an abelian number field K. For any Dirichlet character χ we define the L-function

$$L(s,\chi) = \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s},$$

where s is a complex variable with $\mathrm{Re}(s) > 1$. It is well known that $L(s,\chi)$ admits an holomorphic continuation on the complex plane if $\chi \neq 1$. While for $\chi = 1$, the function $L(s,1)$ is the classical Riemann zeta-function, which is meromorphic with a simple pole at $s = 1$. For any abelian number field K we have the Dedekind zeta-function:

$$\zeta_K(s) = \prod_{\chi \in X(K)} L(s,\chi).$$

The residue at $s = 1$ of the function $\zeta_K(s)$ is closely related to the class number of K and to the regulator of K. Further details can be found in[Has52] or [Was97, Chapter 4]. From the residue formula it is possible to deduce two important relations, we present them briefly below.

The first relation involves the minus part of the class number of K and Bernoulli numbers. Let $K^+ \subset K$ be the maximal real extension inside K. Then, the minus class number h_K^- is defined as the quotient h_K/h_{K^+} where h_K and h_{K^+} are the class numbers of K and K^+ respectively. Let $\mu(K)$ be the group of roots of unity in $K^\times$. Denote by W the cardinality of $\mu(K)$ and by Q the index $[O_K^\times : \mu(K)O_{K^+}^\times]$. Then we get

$$h_K^- = QW \prod_{\substack{\chi \in X(K) \\ \chi \text{ odd}}} \left(-\frac{1}{2} B_{1,\chi}\right).$$

Here $B_{1\chi}$ is the first generalized Bernoulli number associated to the character χ. In other words, letting f be the conductor of χ we have

$$B_{1,\chi} = \frac{1}{f} \sum_{a=0}^{f-1} a\chi(a).$$

Note that the index Q is equal to 1 or 2. Indeed, we have a morphism

$$O_K^\times/\mu(K)O_{K^+}^\times \longrightarrow \mu(K)/\mu(K)^2$$

defined by $u \mapsto u^{1-j}$ where j is complex conjugation. By [Was97, Theorem 4.12] this is injective.

The second relation can be derived from the residue formula as shown in [Sin80]. Sinnott introduced a group of units $\mathrm{Cyc}_K \subset O_K^\times$ usually called group of cyclotomic or circular units. The index $[O_K^\times : \mathrm{Cyc}_K]$ is related to the class number of K. In particular, if K is a real field we have

$$[O_K^\times : \mathrm{Cyc}_K] = 2^{[K:\mathbb{Q}]-1} h_K c_K,$$

where $c_K \in \mathbb{Q}$ is an easily computable constant.

These formulae are our main tool to study class numbers in this thesis.

Why cyclotomic $\mathbb{Z}_p$-extensions? We start by recalling the definition of $\mathbb{Z}_p$-extension. Let K be a number field. A $\mathbb{Z}_p$-extension is a field extension $\mathcal{K}|K$ whose Galois group is topologically isomorphic to the additive group of p-adic numbers. Moreover, $\mathcal{K}$ is said to be cyclotomic if it is the unique $\mathbb{Z}_p$-extension of K contained in the field obtained by adjoining all the p-power roots of unity to K. Hence, we have a tower of fields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset \mathcal{K}$$

such that $\mathrm{Gal}(K_n|K)$ is a cyclic group of order p^n. Let ℓ be a prime number, and let $\mathcal{A}_{n,\ell}$ be the ℓ-part of the class group Cl_{K_n}. Writing N for the norm maps we have a projective system

$$\mathcal{A}_{0,\ell} \xleftarrow{N} \mathcal{A}_{1,\ell} \xleftarrow{N} \mathcal{A}_{2,\ell} \xleftarrow{N} \dots$$

We distinguish two different situations: the case $\ell \neq p$ and the case $\ell = p$.

For $\ell \neq p$, Sinnott and Washington proved with different approaches that there exists a level n_0 such that the norm maps $N : \mathcal{A}_{n,\ell} \longrightarrow \mathcal{A}_{n_0,\ell}$ are isomorphisms for any $n \geq n_0$. See [Sin87] and [Was97, Section 16.3] for further details.

If $\ell = p$, the situation is more complicated. In [Iwa59], Iwasawa showed the existence of integers μ, λ and ν such that

$$\# \mathcal{A}_{n,p} = p^{\mu p^n + \lambda n + \nu}$$

for levels n sufficiently large. For $\mathbb{Z}_p$-extensions of abelian number fields the μ-invariant is zero as proved in [FW79]. Moreover, the $\mathbb{Q}_p$-vector space

$$\left(\varprojlim \mathcal{A}_{n,p}\right) \otimes_{\mathbb{Z}} \mathbb{Q}_p$$

has finite dimension λ. If K is a complex abelian number field, the Main Conjecture proven in [MW84] sets a relation between the characteristic polynomial of a topological generator of $\mathrm{Gal}(\mathcal{K}|K)$ acting on V and the p-adic L-functions $L_p(s, \omega^{-1}\chi)$ associated to $\chi \in X(K)$. Here ω is the Teichmüller character. In particular, for an odd character χ the function $L_p(s, \omega^{-1}\chi)$ is related to the χ^{-1}-eigenspace of V. On the other hand, if χ is even, then the p-adic L-function $L_p(s, \omega^{-1}\chi)$ is identically zero.

A natural question is whether the λ-invariant is zero when K is a real field. This problem is know as Greenberg's conjecture. Note that Greenberg's conjecture is equivalent to saying that the sequence of $\mathcal{A}_{n,p}$'s stabilizes. In other words, there exists a level n_0 such that the norm maps $N : \mathcal{A}_{n,p} \longrightarrow \mathcal{A}_{n_0,p}$ are isomorphisms for any $n \geq n_0$.

Our results. This thesis is divided into two parts.

In the first part we study the Greenberg's conjecture for a real quadratic field and its cyclotomic $\mathbb{Z}_2$-extension. In particular, we present an algorithm to check if the conjecture is true for the cyclotomic $\mathbb{Z}_2$-extensions of the fields $F = \mathbb{Q}(\sqrt{f})$ where f is a positive integer and $f < 10000$. This algorithm is an adaptation of the one described in [KS95].

Let F_n be the n-th level of the cyclotomic $\mathbb{Z}_2$-extension of F. We exploit the relation between cyclotomic units and class number. Since there is a 2-power factor in Sinnot's index formula, we define a group C_{F_n} such that $\mathrm{Cyc}_{F_n} \subset C_{F_n} \subset O_{F_n}^{\times}$ and

$$[O_{F_n^{\times}} : C_{F_n}] = \#\,\mathrm{Cl}_{F_n}\, c_F.$$

Here c_F is a constant equal to 1 or 1/2 depending on F. We define and study the $\mathbb{Z}_2[\mathrm{Gal}(F_n|F)]$-module

$$A_n = \frac{O_{F_n}^{\times}}{C_{F_n}} \otimes_{\mathbb{Z}} \mathbb{Z}_2\,.$$

Exploiting properties of finite Gorenstein rings we describe a procedure to check whether $\#A_n = \#A_{n+1}$ at low levels n. Although we are not able to compute the exact module structure of A_n, we can guarantee the existence of a level n_0 such that $\#A_{n_0} = \#A_{n_0+1}$ for the fields $F = \mathbb{Q}(\sqrt{f})$ with $1 < f < 10000$. In the range of our computations, it was always the case that n_0 does not exceed 11.

Finally, since the algebra $\mathbb{Z}_2[\mathrm{Gal}(F_n|F)]$ is local, we deduce that the natural morphisms $A_{n_0} \longrightarrow A_n$ are isomorphisms for all $n \geq n_0$. In other words, Greenberg's conjecture holds for the cyclotomic $\mathbb{Z}_2$-extensions of real quadratic fields $F = \mathbb{Q}(\sqrt{f})$ with $1 < f < 10000$.

In the second part of the thesis we study the ℓ-part of the class number in $\mathbb{Z}_p$-extensions with $\ell \neq p$ and $\ell \neq 2$. Let $\overline{\mathbb{F}}_\ell$ be an algebraic closure of the finite field $\mathbb{F}_\ell$. Denote by ζ_{p^n} a primitive p^n-th root of unity inside $\overline{\mathbb{F}}_\ell$. We define $\overline{\Theta}$ to be the $\mathbb{F}_\ell$-algebra of functions

$$f : \mu = \varinjlim \langle \zeta_{p^n} \rangle \longrightarrow \overline{\mathbb{F}}_\ell.$$

Let K be an imaginary abelian number field and let K_n be the n-th field in the cyclotomic $\mathbb{Z}_p$-extension of K. We denote by $\mathcal{A}_{n,\ell}$ the ℓ-part of the class group Cl_{K_n}, and we assume $q = 4$ if $p = 2$ or $q = p$ otherwise. Exploiting the relation between Bernoulli numbers and the minus class number, Washington introduced in [Was97, Section 16.3] certain rational functions $f_\chi \in \overline{\Theta}$ for any odd character $\chi \in X(K)$. These functions satisfy the following property: if ℓ divides $h^-_{K_n}/h^-_{K_{n-1}}$, then there exists an odd character $\chi \in X(K)$ and $\zeta \in \mu$ with order qp^n such that $f_\chi(\zeta) = 0$.

We explicitly compute an integer n_0 so that if $f_\chi(\zeta) = 0$ for some χ then the order of ζ is less than qp^{n_0}. Equivalently, ℓ does not divide $h^-_{K_n}/h^-_{K_{n-1}}$ if $n \geq n_0$. Finally, applying the reflection theorem we prove that ℓ does not divides $h_{K_n}/h_{K_{n-1}}$ if $n \geq n_0$.

In other words, we explicitly compute an integer n_0 such that for any $n \geq n_0$ the norm maps $N : \mathcal{A}_{n,\ell} \longrightarrow \mathcal{A}_{n_0-1,\ell}$ are actually isomorphisms.

References

[FW79] Ferrero B. and Washington L.C.: *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

[Has52] Hasse H.: *Über die Klassenzahl abelscher Zahlkörper*. Akademie-Verlag: Berlin, 1952.

[KS95] Kraft J. and Schoof R.: *Computing Iwasawa modules of real quadratic fields*, Compos. Math. **95** (1995), 135-155.

[Iwa59] Iwasawa K.: *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[MW84] Mazur B. and Wiles A.: *Class fields of abelian extensions of $\mathbb{Q}$*, Invent. Math. **76** (1984), 179-330.

[Sin80] Sinnott W.: *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181-234.

[Sin87] Sinnott W.: *Γ-transforms of rational function measures on $\mathbb{Z}_S$*, Invent. Math. **89** (1987), 139-157.

[Was97] Washington L.C.: *Introduction to cyclotomic fields*, Second Edition, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York, (1997).

GREENBERG'S CONJECTURE FOR REAL QUADRATIC FIELDS

LORENZO PAGANI

ABSTRACT. Let $\mathcal{A}_n$ be the 2-part of the ideal class group of the n-th layer of the cyclotomic $\mathbb{Z}_2$-extension of a real quadratic number field F. The cardinality of $\mathcal{A}_n$ is related to the index of cyclotomic units in the full group of units. We present a method to study the latter index. As an application we show that the sequence of the $\mathcal{A}_n$'s stabilizes for the real fields $F = \mathbb{Q}(\sqrt{f})$ for any integer $0 < f < 10000$. Equivalently Greenberg's conjecture holds for those fields.

INTRODUCTION

Let F be a number field. A $\mathbb{Z}_p$-extension is a field extension $\mathcal{F}|F$ whose Galois group is topologically isomorphic to the additive group of p-adic numbers. Moreover, $\mathcal{F}$ is said to be cyclotomic if it is the unique $\mathbb{Z}_p$-extension of F contained in the field obtained by adjoining all the p-power roots of unity to F. We have a tower of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset \mathcal{F}$$

such that $\mathrm{Gal}(F_n|F)$ is a cyclic group of order p^n. The p-parts $\mathcal{A}_n$ of the class group of the fields F_n give a projective system

$$\mathcal{A}_0 \xleftarrow{N} \mathcal{A}_1 \xleftarrow{N} \mathcal{A}_2 \xleftarrow{N} \dots$$

where N is the norm map. In [Iwa59], Iwasawa showed the existence of integers μ, λ and ν such that

$$\#\,\mathcal{A}_n = p^{\mu p^n + \lambda n + \nu}$$

for large enough n.

For abelian fields F, it is known that $\mu = 0$ as shown by Ferrero and Washington in [FW79]. Moreover, Greenberg in his thesis [Gre76] conjectured that $\lambda = 0$ whenever the field F is totally real and $\mathcal{F}$ is the cyclotomic $\mathbb{Z}_p$-extension. If Greenberg's conjecture holds, then there exists a level n_0 such that for any $n \geq n_0$ the norm maps $N : \mathcal{A}_n \longrightarrow \mathcal{A}_{n_0}$ are isomorphisms.

In this paper we restrict our attention to the case in which F is a real quadratic field and $\mathcal{F}$ is the cyclotomic $\mathbb{Z}_2$-extension of F. We are able to compute upper bounds for $\#\,\mathcal{A}_n$ exploiting properties of cyclotomic units and Gorenstein rings. This method is an adaptation of the algorithm described in [Cor97], [KS95] or [Sch02] to our situation. As a consequence of our computation we have the following.

Theorem. *Greenberg's conjecture is true for the cyclotomic $\mathbb{Z}_2$-extension of real quadratic fields $F = \mathbb{Q}(\sqrt{f})$ where f is an integer and $0 < f < 10000$.*

2010 *Mathematics Subject Classification.* Primary 11R29, 11Y40. Secondary 11R23.

Similar computational results for cyclotomic $\mathbb{Z}_3$-extensions of quadratic real fields were already known. They can be found in [Fuk96], [Tay96] and [KS95]. We follow the approach of the last article. In adapting it to our situation we encounter two main obstacles: the fact that for the field F_n the index of cyclotomic units inside the full group of units is equal to the class number h_{F_n} times a 2-power factor that grows as $2^{[F_n:\mathbb{Q}]}$. The second one is the fact that when F is a quadratic field, a $\mathbb{Z}_2[\mathrm{Gal}(F|\,\mathbb{Q})]$-module in general does not split as a part which is invariant with the action of $\mathrm{Gal}(F|\,\mathbb{Q})$ and a part which is anti-invariant. While it is true for $\mathbb{Z}_3[\mathrm{Gal}(F|\,\mathbb{Q})]$-modules since 2 and 3 are coprime.

We expect that the algorithm we describe can be extended to the case of cyclotomic $\mathbb{Z}_p$-extensions of real fields of degree p. Furthermore, we think that this case could be easier since all the cohomology groups we will encounter should be trivial if p is odd.

In section 1 we describe the group of cyclotomic units of F_n. We collect some auxiliary lemmas in section 2. In sections 3 and 4 we enlarge the group of cyclotomic units in order to get rid of the 2-power factor in the index formula. We introduce a group C_{F_n} contained in $O_{F_n}^\times$ and larger than cyclotomic units defined by Sinnott. We denote by A_n the 2-part of the quotient $O_{F_n}^\times/C_{F_n}$ and we study the $\mathrm{Gal}(F_n|F)$-module structure of A_n. In section 5 we use the properties of finite Gorenstein rings to give a description of the dual module of A_n. In sections 6 and 7 we explain an algorithm to get upper bounds for the modules A_n and we collect the results in section 8.

1. Cyclotomic units

In this section we recall the definition of the group of cyclotomic units following [Sin80, Section 4]. In the next sections we will enlarge this group taking the possible square roots of cyclotomic units. We denote by ζ_n the primitive n-th root of unity $\mathrm{e}^{\frac{2\pi i}{n}}$ for any integer $n \geq 1$.

Definition 1.1. Let K be an abelian number field. For any integer $n \geq 1$ we denote by $K_{(n)}$ the intersection $K \cap \mathbb{Q}(\zeta_n)$. Let D_K be the subgroup of $K^\times$ generated by -1 and the elements

$$\underset{\mathbb{Q}(\zeta_n)|K_{(n)}}{\mathrm{Norm}}\ (1-\zeta_n^a) \quad : \quad n \in \mathbb{Z}_{>2},\, a \in \{1,2,\dots,n-1\}\,.$$

The group of cyclotomic units is $D_K \cap O_K^\times$.

Remark 1.2. Let $G = \mathrm{Gal}(K|\,\mathbb{Q})$. It is easy to show that

$$D_K = \mathbb{Q}^\times \cdot \left\langle \underset{\mathbb{Q}(\zeta_n)|K_{(n)}}{\mathrm{Norm}}\ (1-\zeta_n) \right\rangle_{\mathbb{Z}[G]}$$

where n runs over the conductors of the possible subfields of K.

We focus on the case $K = F_n$. Fix $f \geq 3$ a squarefree integer, let $F_0 = \mathbb{Q}(\sqrt{f})$. Let $\mathbb{Q}_n$ be the n-th level of the cyclotomic $\mathbb{Z}_2$-extension over the rationals, namely $\mathbb{Q}_n = \mathbb{Q}(\zeta_{2^{n+2}})^+$. Then F_n is the field $\mathbb{Q}_n(\sqrt{f})$. We exclude the case $f = 2$ since $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$ and therefore the cyclotomic $\mathbb{Z}_2$-extensions of $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$ coincide. In this case it is well known that the 2-part of $\mathrm{Cl}_{\mathbb{Q}_n}$ is trivial. We fix the following notation:

let $\Gamma_n = \mathrm{Gal}(F_n|\,\mathbb{Q})$. We have that $\Gamma_n \cong G_n \times \Delta$, where $G_n = \mathrm{Gal}(F_n|F_0) \cong \mathrm{Gal}(\mathbb{Q}_n\,|\,\mathbb{Q})$ is cyclic of order 2^n while $\Delta = \mathrm{Gal}(F_n|\,\mathbb{Q}_n) \cong \mathrm{Gal}(F_0|\,\mathbb{Q})$ is cyclic of order 2.

We introduce some interesting units:

Definition 1.3. Fix an algebraic closure $\overline{\mathbb{Q}}$ of the rationals. For any integer $n \geq 1$ define the units:

(i) Let σ be the generator of Δ. For any positive squarefree integer f let $\delta_f \in \overline{\mathbb{Q}}$ be such that

$$\delta_f^2 = \begin{cases} \underset{\mathbb{Q}(\zeta_{4f})|F_0}{\mathrm{Norm}}(1-\zeta_{4f}), & \text{if } f \equiv 2,3 \bmod 4, \\ \underset{\mathbb{Q}(\zeta_f)|F_0}{\mathrm{Norm}}(1-\zeta_f)^{1-\sigma}, & \text{if } f \equiv 1 \bmod 4 \text{ and } f \text{ prime}, \\ \underset{\mathbb{Q}(\zeta_f)|F_0}{\mathrm{Norm}}(1-\zeta_f), & \text{otherwise.} \end{cases}$$

Note that δ_f is defined up to a sign and δ_f^2 lies in Cyc_{F_0}.

(ii) Let γ be a generator of $G_n \cong \mathrm{Gal}(\mathbb{Q}_n\,|\,\mathbb{Q})$. There exists an automorphism ϕ_c of $\mathbb{Q}(\zeta_{2^{n+2}})$ defined by $\phi_c(\zeta_{2^{n+2}}) = \zeta_{2^{n+2}}^c$ such that $\phi_{c|\,\mathbb{Q}_n} = \gamma$. Set

$$\beta_n = \zeta_{2^{n+2}}^{\frac{1-c}{2}} \frac{1-\zeta_{2^{n+2}}^c}{1-\zeta_{2^{n+2}}} \in O_{\mathbb{Q}_n}^\times.$$

Choosing a different ϕ_c changes the sign of β_n.

(iii) We define the element of $O_{F_{n+1}}^\times$

$$\eta_n = \underset{\mathbb{Q}(\zeta_{2^{n+3}f})^+|F_{n+1}}{\mathrm{Norm}} \left(\zeta_4(\zeta_{2^{n+3}f} - \zeta_{2^{n+3}f}^{-1})\right).$$

We summarize some useful properties of the above units:

Lemma 1.4. *The units in Definition 1.3 have the following properties:*

(a) Let γ be a generator of G_n. The square of β_n is a cyclotomic unit of $\mathbb{Q}_n$, namely

$$\beta_n^2 = \underset{\mathbb{Q}(\zeta_{2^{n+2}})|\,\mathbb{Q}_n}{\mathrm{Norm}} (1-\zeta_{2^{n+2}})^{\gamma-1}.$$

(b) The square of η_n is a cyclotomic unit of F_n, namely

$$\eta_n^2 = \underset{\mathbb{Q}(\zeta_{2^{n+2}f})|F_n}{\mathrm{Norm}} (1-\zeta_{2^{n+2}f}).$$

(c) If $f \equiv 1 \bmod 4$ and f is prime, then $\delta_f \in O_{F_0}^\times$.

(d) Let γ be a generator of G_{n+1}. We have that $\eta_n^{\gamma-1}$ lies in $O_{F_n}^\times$ for any f. Whereas $\eta_n \in O_{F_n}^\times$ if and only if $\mathrm{Norm}_{F_n|F_0}(\eta_n^2)$ is a square in $O_{F_0}^\times$. The last condition is satisfied if $f \equiv 1 \bmod 4$.

Proof. The first two parts are simple computations. They follow from the relations:

$$\left(\zeta_{2^{n+2}}^{\frac{1-c}{2}} \frac{1-\zeta_{2^{n+2}}^c}{1-\zeta_{2^{n+2}}}\right)^2 = \frac{(1-\zeta_{2^{n+2}}^c)(1-\zeta_{2^{n+2}}^{-c})}{(1-\zeta_{2^{n+2}})(1-\zeta_{2^{n+2}}^{-1})},$$

$$\left(\zeta_4(\zeta_{2^{n+3}f} - \zeta_{2^{n+3}f}^{-1})\right)^2 = (1-\zeta_{2^{n+2}f})(1-\zeta_{2^{n+2}f}^{-1}).$$

In order to prove part (c) we take ϕ an automorphism of $\mathbb{Q}(\zeta_f)$ such that $\phi_{|F_0}$ generates the group Δ. Let $s \in (\mathbb{Z}/f\mathbb{Z})^\times$ be the element defined by $\phi(\zeta_f) = \zeta_f^s$. Then up to a sign we get

$$\delta_f = \underset{\mathbb{Q}(\zeta_f)^+|F_0}{\text{Norm}} \left(\zeta_f^{\frac{s-1}{2}} \frac{1-\zeta_f}{1-\zeta_f^s} \right).$$

Similarly, for part (d) let γ be a generator of the group G_{n+1} and denote by $\widetilde{\gamma}$ an automorphism of $\mathbb{Q}(\zeta_{2^{n+3}f})$ such that $\widetilde{\gamma}_{|F_{n+1}} = \gamma$ and $\widetilde{\gamma}(\zeta_f) = \zeta_f$. Consider the unit of $O_{F_n}^\times$ defined as

$$\underset{\mathbb{Q}(\zeta_{2^{n+2}f})^+|F_n}{\text{Norm}} \left(\zeta_{2^{n+2}f}^{\frac{1-\widetilde{\gamma}}{2}} \frac{1-\zeta_{2^{n+2}f}^{\widetilde{\gamma}}}{1-\zeta_{2^{n+2}f}} \right).$$

Its square is exactly $\eta_n^{2(\gamma-1)}$ and therefore $\eta_n^{\gamma-1} \in O_{F_n}^\times$.

Let $N_n = \sum_{i=0}^{2^n-1} \gamma^i \in \mathbb{Z}[G_{n+1}]$. Assume now that the element $\text{Norm}_{F_n|F_0}(\eta_n^2) = \eta_n^{2N_n}$ is a square in $O_{F_0}^\times$. It follows that $\eta_n^{N_n} \in O_{F_0}^\times$ and we get that

$$\eta_n^{\gamma^{2^n}-1} = \left(\eta_n^{N_n}\right)^{\gamma-1} = 1.$$

Since γ^{2^n} generates $\text{Gal}(F_{n+1}|F_n)$, we have $\eta_n \in O_{F_n}^\times$.

For $f \equiv 1 \bmod 4$, we compute $\text{Norm}_{F_n|F_0}(\eta_n^2)$. Let ϕ_2 be the automorphism of $\mathbb{Q}(\zeta_{2^{n+2}f})$ such that $\phi_{2|\,\mathbb{Q}(\zeta_{2^{n+2}})} = \text{id}$ and $\phi_2(\zeta_f) = \zeta_f^2$. Then

$$\begin{aligned}\underset{F_n|F_0}{\text{Norm}}(\eta_n^2) = \underset{\mathbb{Q}(\zeta_{2^{n+2}f})|F_0}{\text{Norm}}(1-\zeta_{2^{n+2}f}) = \\ = \underset{\mathbb{Q}(\zeta_f)|F_0}{\text{Norm}} \left((1-\zeta_f)^{1-\phi_2^{-1}} \right) = \underset{\mathbb{Q}(\zeta_f)|F_0}{\text{Norm}} (1-\zeta_f)^{1-\phi_{2|F_0}}.\end{aligned}$$

Let χ_f be the quadratic Dirichlet character associated to F_0. Then $\phi_{2|F_0} = \text{id}$ if and only if $2 \in \ker \chi_f$. The last condition holds if and only if 2 splits in F_0, namely when $f \equiv 1 \bmod 8$. Therefore we get

$$\underset{F_n|F_0}{\text{Norm}}(\eta_n^2) = \begin{cases} 1, & \text{if } f \equiv 1 \bmod 8, \\ \delta_f^2, & \text{if } f \equiv 5 \bmod 8 \text{ and } f \text{ prime}, \\ \delta_f^{2(1-\sigma)} = \delta_f^4, & \text{otherwise.} \end{cases}$$

Notice that the right hand side is always a square in $O_{F_0}^\times$. This concludes the proof of the Lemma. □

Lemma 1.5. *Let $f \geq 3$ be an odd squarefree integer. The group of cyclotomic units for the field F_n is*

$$\text{Cyc}_{F_n} = \left\langle -1, \eta_n^2, \beta_n^2, \delta_f^2 \right\rangle_{\mathbb{Z}[G_n]}.$$

This is also true for F_0 if we put $\eta_0^2 = \text{Norm}_{F_n|F_0}(\eta_n^2)$ and $\beta_0 = -1$.

Proof. We prove the statement for $n \geq 1$. The case $n = 0$ is similar and easier. Define the following units:

$$\begin{aligned} a_t &= \underset{\mathbb{Q}(\zeta_{2^{n+2}f})|F_n}{\mathrm{Norm}}(1-\zeta_{2^{n+2}f}), \quad 0 \leq t \leq n, \\ b_t &= \underset{\mathbb{Q}(\zeta_{2^{n+2}})|\mathbb{Q}_n}{\mathrm{Norm}}(1-\zeta_{2^{n+2}}), \quad 1 \leq t \leq n, \\ d_f &= \underset{\mathbb{Q}(\zeta_{f'})|F_0}{\mathrm{Norm}}(1-\zeta_{f'}). \end{aligned}$$

where f' is the conductor of F_0, namely $f' = f$ if $f \equiv 1 \bmod 4$ or $f' = 4f$ if $f \equiv 3 \bmod 4$. Notice that $\mathrm{Norm}_{F_n|F_t}(a_n) = a_t$ and $\mathrm{Norm}_{\mathbb{Q}_n|\mathbb{Q}_t}(b_n) = b_t$. Combining this information with Remark 1.2 we get that

$$D_{F_n} = \mathbb{Q}^\times \cdot \langle a_n, b_n, d_f \rangle_{\mathbb{Z}[\Gamma_n]}.$$

Moreover, we can consider only the G_n-conjugates. Indeed, let σ be the generator of Δ, then $a_n^{1+\sigma}$ lies in $\langle -1, b_n \rangle_{\mathbb{Z}[G_n]}$, the element b_n is Δ-invariant and $d_f^{1+\sigma} \in \mathbb{Q}^\times$. Let γ be a generator of G_n, then

$$D_{F_n} = \mathbb{Q}^\times \cdot \left\langle a_n^{\gamma^i}, b_n^{\gamma^j}, d_f \ : \ 0 \leq i < 2^n, \ 0 \leq j < 2^n \right\rangle_{\mathbb{Z}}.$$

By Lemma 1.4 we have $a_n = \eta_n^2$ and $b_n^{\gamma-1} = \beta_n^2$. Therefore

$$D_{F_n} = \mathbb{Q}^\times \cdot \left\langle (\eta_n^2)^{\gamma^i}, b_n, (\beta_n^2)^{\gamma^j}, d_f \ : \ 0 \leq i < 2^n, \ 0 \leq j < 2^n - 1 \right\rangle_{\mathbb{Z}}.$$

According to [Sin80, Lemma 4.1], an element $u \in D_{F_n}$ lies in Cyc_{F_n} if and only if $\mathrm{Norm}_{F_n|\mathbb{Q}}(u) = \pm 1$. We compute the norm of the generators:

$$\begin{aligned} &\underset{F_n|\mathbb{Q}}{\mathrm{Norm}}((\eta_n^2)^{\gamma^i}) = 1, \\ &\underset{F_n|\mathbb{Q}}{\mathrm{Norm}}((\beta_n^2)^{\gamma^j}) = 1, \\ &\underset{F_n|\mathbb{Q}}{\mathrm{Norm}}(b_n) = 4, \\ &\underset{F_n|\mathbb{Q}}{\mathrm{Norm}}(d_f) = \begin{cases} f^{2^n}, & \text{if } f \equiv 1 \bmod 4 \text{ and } f \text{ prime}, \\ 1, & \text{otherwise.} \end{cases} \end{aligned}$$

Assume now that $f \equiv 1 \bmod 4$ and f prime. The elements with norm ± 1 in D_{F_n} are

$$\mathrm{Cyc}_{F_n} = \left\langle -1, (\eta_n^2)^{\gamma^i}, (\beta_n^2)^{\gamma^j}, b_n^{2^n}/2, d_f^2/f \right\rangle_{\mathbb{Z}}.$$

Note that

$$\frac{d_f^2}{f} = \frac{d_f^{1+\sigma} d_f^{1-\sigma}}{f} = d_f^{1-\sigma} = \delta_f^2.$$

Consider now the element $b_n^{2^n}/2$. Let $N_n = \sum_{i=0}^{2^n-1} \gamma^i \in \mathbb{Z}[G_n]$, then $2^n - N_n$ lies in the augmentation ideal. In particular, we have $2^n - N_n = (\gamma - 1)x$ for some $x \in \mathbb{Z}[G_n]$. So

$$\frac{b_n^{2^n}}{2} = \frac{b_n^{N_n} b_n^{2^n - N_n}}{2} = b_n^{(\gamma-1)x} = (\beta_n^2)^x.$$

We conclude that

$$\mathrm{Cyc}_{F_n} = \left\langle -1, \eta_n^2, \beta_n^2, \delta_f^2 \right\rangle_{\mathbb{Z}[G_n]}.$$

In the remaining cases d_f has norm 1. Therefore, we get that

$$\mathrm{Cyc}_{F_n} = \left\langle -1, (\eta_n^2)^{\gamma^i}, (\beta_n^2)^{\gamma^j}, b_n^{2^n}/2, d_f \right\rangle_{\mathbb{Z}}.$$

By Definition 1.3 we have that $d_f = \delta_f^2$. Moreover we can show as above that $b_n^{2^n}/2$ lies in the $\mathbb{Z}[G_n]$-submodule generated by β_n^2. We finally get

$$\mathrm{Cyc}_{F_n} = \left\langle -1, \eta_n^2, \beta_n^2, \delta_f^2 \right\rangle_{\mathbb{Z}[G_n]}.$$

□

Remark 1.6. The assumption f odd can be made without losing any generality. Indeed, since $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$ the cyclotomic $\mathbb{Z}_2$-extensions of $\mathbb{Q}(\sqrt{f})$ and $\mathbb{Q}(\sqrt{2f})$ differ only at the 0-th level.

The relation between cyclotomic units and the class number is given by Sinnott's index formula. As stated in [Sin80, Theorem 4.1] we have:

$$[O_{F_n}^\times : \mathrm{Cyc}_{F_n}] = \begin{cases} 2^{2^{n+1}-1} h_{F_n}, & \text{if } f \equiv 1 \bmod 4 \text{ and } f \text{ prime}, \\ 2^{2^{n+1}-2} h_{F_n}, & \text{otherwise.} \end{cases} \tag{S}$$

Remark 1.7. Note that [Sin80, Theorem 4.1] actually states that

$$[O_{F_n}^\times : \mathrm{Cyc}_{F_n}] = 2^{2^{n+1}-j} h_{F_n} c_{F_n}$$

where c_{F_n} is a rational number and $j = 1$ if $f \equiv 1 \bmod 4$ and f prime or $j = 2$ otherwise. We give the definition of c_{F_n} and we show that $c_{F_n} = 1$ in Appendix A.

Since we want to exploit the connection between the cyclotomic units index and the 2-part of the class number, we need to get rid of the 2-power factor appearing in Sinnott's index formula. In the following sections we work with a larger group of units C_{F_n}.

2. Auxiliary lemmas

In this section we collect some auxiliary lemmas. We need them in the following sections.

Lemma 2.1. *Let $K \subset L$ be a Galois extension of number fields with group G. Let W be the set of 2^k-th roots of unity inside $L^\times$ for a fixed positive integer k. Then, the kernel of the natural morphism*

$$\iota : O_K^\times / O_K^{\times 2^k} \longrightarrow O_L^\times / O_L^{\times 2^k}$$

is isomorphic to a subgroup of $\mathrm{H}^1(G, W)$. The definition of such cohomology groups can be found in [CF93, Section 4].

Proof. Consider the exact sequence

$$0 \longrightarrow W \longrightarrow L^\times \xrightarrow{2^k} L^{\times 2^k} \longrightarrow 0$$

and take G-invariants. We get

$$K^\times \xrightarrow{2^k} L^{\times 2^k} \cap K \longrightarrow \mathrm{H}^1(G, W) \longrightarrow 0.$$

The rightmost zero is a consequence of Hilbert's Theorem 90. Then

$$\ker\left(K^\times/K^{\times 2^k} \to L^\times/L^{\times 2^k}\right) \cong \mathrm{H}^1(G, W).$$

Finally, we consider the natural commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker \iota & \longrightarrow & \dfrac{O_K^\times}{O_K^{\times 2^k}} & \xrightarrow{\iota} & \dfrac{O_L^\times}{O_L^{\times 2^k}} \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{H}^1(G, W) & \longrightarrow & \dfrac{K^\times}{K^{\times 2^k}} & \longrightarrow & \dfrac{L^\times}{L^{\times 2^k}}. \end{array}$$

Since the central vertical map is injective, we can identify the kernel of ι with a subgroup of $\mathrm{H}^1(\mathrm{Gal}(L|K), W)$. □

Lemma 2.2. *Let A, B be free $\mathbb{Z}$-modules such that $A \subset B$. Then, the morphisms induced by the inclusion*

$$\iota_k : A/2^k A \longrightarrow B/2^k B$$

are injective for each $k \geq 1$ if and only if ι_1 is injective.

Proof. We prove it by induction. Let $k \geq 1$. Consider the exact sequence

$$0 \longrightarrow \frac{\mathbb{Z}}{2\,\mathbb{Z}} \xrightarrow{2^k} \frac{\mathbb{Z}}{2^{k+1}\,\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{2^k\,\mathbb{Z}} \longrightarrow 0$$

where the left map is induced by the multiplication by 2^k, while the right one is the natural quotient. Tensoring with the free module A we get the exact sequence

$$0 \longrightarrow \frac{A}{2A} \xrightarrow{2^k} \frac{A}{2^{k+1}A} \longrightarrow \frac{A}{2^k A} \longrightarrow 0.$$

We have a similar exact sequence tensoring with the module B instead of A. From the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \dfrac{A}{2A} & \xrightarrow{2^k} & \dfrac{A}{2^{k+1}A} & \longrightarrow & \dfrac{A}{2^k A} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \iota_1} & & \downarrow{\scriptstyle \iota_{k+1}} & & \downarrow{\scriptstyle \iota_k} & & \\ 0 & \longrightarrow & \dfrac{B}{2B} & \xrightarrow{2^k} & \dfrac{B}{2^{k+1}B} & \longrightarrow & \dfrac{B}{2^k B} & \longrightarrow & 0 \end{array}$$

we deduce that if ι_1 and ι_k are both injective, then ι_{k+1} is injective too. □

Lemma 2.3. *Let $C_{\mathbb{Q}_n}$ be the $\mathbb{Z}[G_n]$-submodule of $O^\times_{\mathbb{Q}_n}$ generated by -1 and β_n. Then, the natural morphisms*

$$\iota : \frac{C_{\mathbb{Q}_n}}{\pm C^{2^k}_{\mathbb{Q}_n}} \longrightarrow \frac{O^\times_{F_n}}{\pm O^{\times 2^k}_{F_n}}$$

are injective for any $n, k \geq 1$.

Proof. According to Lemma 2.2, it is enough to prove the statement for

$$\iota : \frac{C_{\mathbb{Q}_n}}{\pm C^{2}_{\mathbb{Q}_n}} \longrightarrow \frac{O^\times_{F_n}}{\pm O^{\times 2}_{F_n}}.$$

By [Was97, Theorem 8.2] the index $[O^\times_{\mathbb{Q}_n} : C_{\mathbb{Q}_n}]$ is equal to the class number of $\mathbb{Q}_n$ and it is odd. Therefore, the natural map

$$C_{\mathbb{Q}_n}/\pm C^{2^k}_{\mathbb{Q}_n} \cong O^\times_{\mathbb{Q}_n}/\pm O^{\times 2^k}_{\mathbb{Q}_n}$$

is an isomorphism.

Since -1 is not a square in $O^\times_{F_n}$, the kernel of ι is isomorphic to the kernel of the map

$$\frac{O^\times_{\mathbb{Q}_n}}{O^{\times 2}_{\mathbb{Q}_n}} \longrightarrow \frac{O^\times_{F_n}}{O^{\times 2}_{F_n}}.$$

So, Lemma 2.1 states that $\ker \iota$ is isomorphic to a subgroup of $\mathrm{H}^1(\Delta, \pm 1)$. The cardinality of $\mathrm{H}^1(\Delta, \pm 1)$ is 2.

Let γ be a generator of G_n and let $N_n = \sum_{i=0}^{2^n-1} \gamma^i \in \mathbb{Z}[G_n]$. Then, the morphism of $\mathbb{Z}[G_n]$-modules

$$\pi : \frac{\mathbb{Z}[G_n]}{(N_n)} \longrightarrow \frac{C_{\mathbb{Q}_n}}{\pm 1}$$

defined by $1 \mapsto \beta_n$ is an isomorphism. Indeed, π is a surjective morphism between free $\mathbb{Z}$-modules of same rank. In particular, π induces an isomorphism

$$\frac{\mathbb{Z}[G_n]}{(2, N_n)} \cong \frac{C_{\mathbb{Q}_n}}{\pm C^2_{\mathbb{Q}_n}}.$$

Since ι is G_n-equivariant, we identify $\ker \iota$ with an ideal of the algebra $\mathbb{Z}[G_n]/(2, N_n)$. The only ideal of cardinality 2 is the one generated by

$$\underset{\mathbb{Q}_n | \mathbb{Q}_1}{\mathrm{Norm}} = \sum_{i=0}^{2^{n-1}-1} \gamma^{2i}$$

We deduce that ι is injective if and only if

$$\beta_1 = \underset{\mathbb{Q}_n | \mathbb{Q}_1}{\mathrm{Norm}}(\beta_n) \notin \pm O^{\times 2}_{F_n}.$$

Note that $\beta_1 = 1 + \sqrt{2}$ up to Galois conjugation and $\mathbb{Q}(\sqrt{\beta_1})$ has complex Galois closure. Therefore, it cannot be contained in F_n. We conclude that ι is injective. □

Lemma 2.4. *Fix $n \geq 1$. Let γ be a generator of G_n. For any $0 \leq m \leq n$ let N_m be the element in $\mathbb{Z}[G_n]$ defined as $\sum_{i=0}^{2^m-1} \gamma^i$. Then*

$$\mathrm{Ext}^1{}_{\mathbb{Z}[G_n]}\left(\frac{\mathbb{Z}[G_n]}{(N_m)}, \frac{\mathbb{Z}[G_n]}{(N_n)}\right) = 0.$$

Proof. Consider the exact sequence of $\mathbb{Z}[G_n]$-modules

$$0 \longrightarrow (N_m) \longrightarrow \mathbb{Z}[G_n] \longrightarrow \mathbb{Z}[G_n]/(N_m) \longrightarrow 0.$$

We apply the functor $\mathrm{Hom}_{\mathbb{Z}[G_n]}(-, \mathbb{Z}[G_n]/(N_n))$. We get the following exact sequence

$$\mathrm{Hom}\left(\mathbb{Z}[G_n], \frac{\mathbb{Z}[G_n]}{(N_n)}\right) \xrightarrow{\iota} \mathrm{Hom}\left((N_m), \frac{\mathbb{Z}[G_n]}{(N_n)}\right) \longrightarrow \mathrm{Ext}^1\left(\frac{\mathbb{Z}[G_n]}{(N_m)}, \frac{\mathbb{Z}[G_n]}{(N_n)}\right) \longrightarrow 0.$$

It suffices to prove that ι is surjective. We identify

$$\mathrm{Hom}_{\mathbb{Z}[G_n]}\left(\mathbb{Z}[G_n], \frac{\mathbb{Z}[G_n]}{(N_n)}\right) \cong \frac{\mathbb{Z}[G_n]}{(N_n)}$$

via the $\mathbb{Z}[G_n]$-module isomorphism $\phi \mapsto \phi(1)$. Similarly we have an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G_n]}\left((N_m), \frac{\mathbb{Z}[G_n]}{(N_n)}\right) \cong \left\{ y \in \frac{\mathbb{Z}[G_n]}{(N_n)} \ : \ \frac{\gamma^{2^n}-1}{N_m} y = 0 \right\}$$

that maps $\phi \mapsto \phi(N_m)$. Via these identifications the map ι became the morphism

$$\frac{\mathbb{Z}[G_n]}{(N_n)} \longrightarrow \left\{ y \in \frac{\mathbb{Z}[G_n]}{(N_n)} \ : \ \frac{\gamma^{2^n}-1}{N_m} y = 0 \right\}$$

induced by the multiplication by N_m.

Let π be the ring surjective morphism

$$\pi : \mathbb{Z}[T] \longrightarrow \mathbb{Z}[G_n]/(N_n)$$

such that $\pi(T) = \gamma$. Let $y \in \mathbb{Z}[G_n]/(N_n)$ such that it is annihilated by $(\gamma^{2^n}-1)/(N_m)$. Take $y(T) \in \mathbb{Z}[T]$ so that $\pi(y(T)) = y$. Then, there exists a polynomial $q(T)$ that satisfies

$$\frac{T^{2^n}-1}{\left(\sum_{i=0}^{2^m-1} T^i\right)} y(T) = \left(\sum_{i=0}^{2^n-1} T^i\right) q(T).$$

This relation is equivalent to

$$(T-1)y(T) = \left(\sum_{i=0}^{2^m-1} T^i\right) q(T).$$

Since $T-1$ and $\sum_{i=0}^{2^m-1} T^i$ are coprime, the polynomial $q(T)$ is divisible by $(T-1)$. Let $q' = \pi(q(T)/(T-1))$. It follows that $y = N_m q'$. Therefore ι is surjective. □

3. The ramified and the inert case

In this section we restrict our attention to the case in which f is a positive odd squarefree integer and $f \not\equiv 1 \bmod 8$. In this case there is only one prime ideal of $O_{F_0}^\times$ lying above 2. Therefore [Was97, Proposition 13.2] states that there is only one prime ideal that ramifies in the cyclotomic $\mathbb{Z}_2$-extension of F_0. By [Was97, Theorem 10.4] the class number h_{F_n} is even if and only if h_{F_0} is. In particular, if h_{F_0} is odd, then Greenberg's conjecture holds. Therefore, we may assume $2|h_{F_0}$.

Remark 3.1. Under the assumption $2|h_{F_0}$ we have that $\eta_n \in O_{F_n}^\times$. If $f \equiv 5 \bmod 8$ it follows from Lemma 1.4. While if $f \equiv 3 \bmod 4$ we exploit the fact that $2|h_{F_0}$. Indeed, Sinnott's index formula (S) implies that the index $[O_{F_0}^\times : \mathrm{Cyc}_{F_0}]$ is even. Since the unit δ_f^2 is positive under any real embedding of F_0 and since $\mathrm{Cyc}_{F_0} = \langle -1, \delta_f^2 \rangle_{\mathbb{Z}}$, it follows that δ_f^2 is a square in $O_{F_0}^\times$. Then, Lemma 1.4 implies that $\eta_n \in O_{F_n}^\times$ since $\mathrm{Norm}_{F_n|F_0}(\eta_n^2) = \delta_f^2$.

Definition 3.2. Let $f \not\equiv 1 \bmod 8$ be a positive odd squarefree integer. Let $F_0 = \mathbb{Q}(\sqrt{f})$ and assume that $2|h_{F_0}$. For any $n \geq 1$ we define the $\mathbb{Z}[G_n]$-module

$$C_{F_n} = \langle -1, \eta_n, \beta_n \rangle_{\mathbb{Z}[G_n]}.$$

Furthermore, we define $C_{F_0} = \left\langle -1, \underset{F_n|F_0}{\mathrm{Norm}}(\eta_n) \right\rangle_{\mathbb{Z}}$. It is convenient to set the following notation: $\eta_0 = \mathrm{Norm}_{F_n|F_0}(\eta_n)$ and $\beta_0 = -1$.

Notice that for any $0 \leq m \leq n$ we have inclusions $C_{F_m} \subset C_{F_n}$. Indeed, we have up to sign that $\mathrm{Norm}_{F_n|F_m}(\eta_n) = \eta_m$ and $\mathrm{Norm}_{F_n|F_m}(\beta_n) = \beta_m$. Moreover, we have that up to a sign

$$\eta_0 = \underset{F_n|F_0}{\mathrm{Norm}}(\eta_n) = \begin{cases} \delta_f^2, & \text{if } f \equiv 5 \bmod 8 \text{ and } f \text{ not prime,} \\ \delta_f, & \text{otherwise.} \end{cases}$$

This equality is obtained computing the norm of η_n^2 and then taking the square root.

Proposition 3.3. *Let $f \not\equiv 1 \bmod 8$ be a positive odd squarefree integer. Let $F_0 = \mathbb{Q}(\sqrt{f})$. Assume that $2|h_{F_0}$. Then, for any $n \geq 0$ we have the inclusions*

$$\mathrm{Cyc}_{F_n} \subset C_{F_n} \subset O_{F_n}^\times$$

and the index $[O_{F_n}^\times : C_{F_n}]$ is equal to h_{F_n} when $f \equiv 5 \bmod 8$ or is equal to $h_{F_n}/2$ when $f \equiv 3 \bmod 4$.

Let γ be a generator of G_n and let $N_n = \sum_{i=0}^{2^n-1} \gamma^i \in \mathbb{Z}[G_n]$. Then, we have an isomorphism of $\mathbb{Z}[G_n]$-modules

$$\pi : \mathbb{Z}[G_n] \oplus \frac{\mathbb{Z}[G_n]}{(N_n)} \longrightarrow \frac{C_{F_n}}{\pm 1}$$

defined by $(x, y) \mapsto \eta_n^x \beta_n^y$.

Proof. The inclusion $C_{F_n} \subset O_{F_n}^\times$ follows from Lemma 1.4 and Remark 3.1. While the inclusion $\mathrm{Cyc}_{F_n} \subset C_{F_n}$ is straightforward from Lemma 1.5 and the fact that up to a sign

we have

$$\operatorname*{Norm}_{F_n|F_0}(\eta_n) = \begin{cases} \delta_f^2, & \text{if } f \equiv 5 \bmod 8 \text{ and } f \text{ not prime,} \\ \delta_f, & \text{otherwise.} \end{cases}$$

Since π is a surjective morphism between free modules of the same rank, it is an isomorphism.

In order to prove the statement about the index, we consider the image of $\mathrm{Cyc}_{F_n} / \pm 1$ via π^{-1}. If $f \equiv 5 \bmod 8$ and f is not prime, by Proposition 1.5 we have

$$\pi^{-1}(\mathrm{Cyc}_{F_n} / \pm 1) = \langle 2, N_n \rangle_{\mathbb{Z}[G_n]} \oplus \langle 2 \rangle_{\mathbb{Z}[G_n]/(N_n)}$$

Therefore we get

$$[C_{F_n} : \mathrm{Cyc}_{F_n}] = [\pi^{-1}(C_{F_n}/ \pm 1) : \pi^{-1}(\mathrm{Cyc}_{F_n} / \pm 1)] = 2^{2^{n+1}-2}.$$

Combining this with Sinnott's index formula we deduce that $[O_{F_n}^{\times} : C_{F_n}] = h_{F_n}$.

On the other hand, if $f \equiv 5 \bmod 8$ and f prime or if $f \equiv 3 \bmod 4$, we have

$$\pi^{-1}(\mathrm{Cyc}_{F_n} / \pm 1) = \langle 2 \rangle_{\mathbb{Z}[G_n]} \oplus \langle 2 \rangle_{\mathbb{Z}[G_n]/(N_n)}$$

hence the index $[C_{F_n} : \mathrm{Cyc}_{F_n}] = 2^{2^{n+1}-1}$. Again combining this with Sinnott's index formula we prove the Proposition. □

Corollary 3.4. *Let $f \not\equiv 1 \bmod 8$ be a positive odd squarefree integer. Let $F_0 = \mathbb{Q}(\sqrt{f})$. Assume that $2|h_{F_0}$. Let $0 \leq m \leq n$. Then, the natural inclusion induces an isomorphism*

$$C_{F_m} \cong C_{F_n}^{\mathrm{Gal}(F_n|F_m)}.$$

Proof. By Proposition 3.3, we have an isomorphism

$$\pi : \mathbb{Z}[G_n] \oplus \frac{\mathbb{Z}[G_n]}{(N_n)} \longrightarrow \frac{C_{F_n}}{\pm 1}.$$

We deduce that π induces an isomorphism

$$\operatorname*{Norm}_{F_n|F_m} \cdot \left(\mathbb{Z}[G_n] \oplus \frac{\mathbb{Z}[G_n]}{(N_n)} \right) \cong \left(\frac{C_{F_n}}{\pm 1} \right)^{\mathrm{Gal}(F_n|F_m)}.$$

It follows that the group $(C_{F_n}/ \pm 1)^{\mathrm{Gal}(F_n|F_m)}$ is generated by $\mathrm{Norm}_{F_n|F_m}(\eta_n) = \eta_m$ and $\mathrm{Norm}_{F_n|F_m}(\beta_n) = \beta_m$. We conclude that $C_{F_n}^{\mathrm{Gal}(F_n|F_m)} = \langle -1, \eta_m, \beta_m \rangle = C_{F_m}$. □

Definition 3.5. Let $f \not\equiv 1 \bmod 8$ be a positive odd squarefree integer. Let $F_0 = \mathbb{Q}(\sqrt{f})$. Assume that $2|h_{F_0}$. For any $n \geq 0$ we define the $\mathbb{Z}_2[G_n]$-module

$$A_n = \frac{O_{F_n}^{\times}}{C_{F_n}} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \,.$$

The cardinality of A_n is closely related to the 2-part of the class number of F_n. Furthermore, for any $m \leq n$ there are natural morphisms $A_m \longrightarrow A_n$ induced by the inclusions $O_{F_m}^{\times} \longrightarrow O_{F_n}^{\times}$. By Corollary 3.4 the morphisms $A_m \longrightarrow A_n$ are injective.

Lemma 3.6. *Let $f \not\equiv 1 \bmod 8$ be a positive odd squarefree integer. Let $F_0 = \mathbb{Q}(\sqrt{f})$. Assume that $2|h_{F_0}$. Let $0 \leq m \leq n$ and set $N_m = \sum_{i=0}^{2^m-1} \gamma^i \in \mathbb{Z}[G_n]$. Then, the natural map $A_m \longrightarrow A_n$ induces an isomorphism*

$$\frac{A_m}{A_0} \cong \frac{A_n}{A_0}[N_m].$$

Here $(A_n/A_0)[N_m]$ denotes the kernel of the map $A_n/A_0 \to A_n/A_0$ induced by the multiplication by N_m.

Proof. We consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_{F_0} & \longrightarrow & O_{F_0}^\times & \longrightarrow & \frac{O_{F_0}^\times}{C_{F_0}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C_{F_n} & \longrightarrow & O_{F_n}^\times & \longrightarrow & \frac{O_{F_n}^\times}{C_{F_n}} & \longrightarrow & 0 \end{array}$$

By Corollary 3.4 we have that $C_{F_0} = C_{F_n}^{G_n}$. Hence, the rightmost vertical map is injective. Therefore, the snake lemma gives us the following exact sequence:

$$0 \longrightarrow \frac{C_{F_n}}{C_{F_0}} \longrightarrow \frac{O_{F_n}^\times}{O_{F_0}^\times} \longrightarrow \frac{O_{F_n}^\times}{C_{F_n} O_{F_0}^\times} \longrightarrow 0.$$

The cardinality of the rightmost group of the exact sequence is h_{F_n}/h_{F_0}.

According to Proposition 3.3 the group C_{F_n}/C_{F_0} is isomorphic as $\mathbb{Z}[G_n]$-module to $\mathbb{Z}[G_n]/(N_n) \oplus \mathbb{Z}[G_n]/(N_n)$.

We apply the functor $\mathrm{Hom}_{\mathbb{Z}[G_n]}(\mathbb{Z}[G_n]/(N_m), -)$ to get

$$0 \longrightarrow \frac{C_{F_n}}{C_{F_0}}[N_m] \longrightarrow \frac{O_{F_n}^\times}{O_{F_0}^\times}[N_m] \longrightarrow \frac{O_{F_n}^\times}{C_{F_n} O_{F_0}^\times}[N_m] \longrightarrow 0.$$

By Lemma 2.4 the sequence is exact. Furthermore, we have the following commutative diagram whose rows are exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{C_{F_m}}{C_{F_0}} & \longrightarrow & \frac{O_{F_m}^\times}{O_{F_0}^\times} & \longrightarrow & \frac{O_{F_m}^\times}{C_{F_m} O_{F_0}^\times} & \longrightarrow & 0\,. \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \frac{C_{F_n}}{C_{F_0}}[N_m] & \longrightarrow & \frac{O_{F_n}^\times}{O_{F_0}^\times}[N_m] & \longrightarrow & \frac{O_{F_n}^\times}{C_{F_n} O_{F_0}^\times}[N_m] & \longrightarrow & 0 \end{array}$$

The leftmost vertical map is an isomorphism. Indeed, the map π described in Proposition 3.3 induces an isomorphism

$$\frac{C_{F_n}}{C_{F_0}}[N_m] \cong \underset{F_n|F_m}{\mathrm{Norm}} \cdot \left(\frac{\mathbb{Z}[G_n]}{(N_n)} \oplus \frac{\mathbb{Z}[G_n]}{(N_n)} \right).$$

Since up to a sign $\mathrm{Norm}_{F_n|F_m}(\eta_n) = \eta_m$ and $\mathrm{Norm}_{F_n|F_m}(\beta_n) = \beta_m$, we get the desired isomorphism.

We prove that also the central vertical map is an isomorphism. The map

$$\frac{O_{F_m}^\times}{O_{F_0}^\times} \longrightarrow \frac{O_{F_n}^\times}{O_{F_0}^\times}[N_m]$$

is clearly injective. Take $x \in O_{F_n}^\times$ such that $x^{N_m} \in O_{F_0}^\times$. Then $1 = (x^{N_m})^{\gamma-1} = x^{\gamma^{2^m}-1}$. Therefore $x \in O_{F_m}^\times$ and the surjectivity follows. Hence, we have an isomorphism

$$\frac{O_{F_m}^\times}{C_{F_m}O_{F_0}^\times} \cong \frac{O_{F_n}^\times}{C_{F_n}O_{F_0}^\times}[N_m].$$

Since we are interested in the 2-part of the class group, we tensor by $\mathbb{Z}_2$ and we get

$$\frac{A_m}{A_0} \cong \frac{A_n}{A_0}[N_m].$$

□

Proposition 3.7. *Let $f \not\equiv 1 \bmod 8$ be a positive odd squarefree integer. Let $F_0 = \mathbb{Q}(\sqrt{f})$. Assume that $2|h_{F_0}$. Assume there exists an integer $n_0 \geq 0$ such that A_{n_0} and A_{n_0+1} have the same cardinality. Then, for any $n \geq n_0$ the natural maps $A_{n_0} \longrightarrow A_n$ are isomorphisms.*

Proof. Fix $n > n_0$. By Lemma 3.6 we have

$$\frac{A_{n_0}}{A_0} \cong \frac{A_n}{A_0}[N_{n_0}] \subset \frac{A_n}{A_0}[N_{n_0+1}] \cong \frac{A_{n_0+1}}{A_0}.$$

The hypothesis $\#A_{n_0} = \#A_{n_0+1}$ implies that $\#(A_{n_0}/A_0) = \#(A_{n_0+1}/A_0)$ too. Indeed, the natural maps $A_0 \longrightarrow A_n$ are injective by the fact that $C_{F_0} = C_{F_n}^{G_n}$. Since all the modules are finite we get

$$\frac{A_n}{A_0}[N_{n_0}] = \frac{A_n}{A_0}[N_{n_0+1}] \quad \text{and} \quad N_{n_0}\frac{A_n}{A_0} = N_{n_0+1}\frac{A_n}{A_0}.$$

The algebra $\mathbb{Z}_2[G_n]$ is local with maximal ideal $\mathfrak{M} = (2, \gamma - 1)$. Note that

$$N_{n_0}\frac{A_n}{A_0} = N_{n_0+1}\frac{A_n}{A_0} = (1+\gamma^{2^{n_0}})N_{n_0}\frac{A_n}{A_0} \subset \mathfrak{M}N_{n_0}\frac{A_n}{A_0}.$$

Therefore Nakayama's lemma implies that $N_{n_0}(A_n/A_0) = 0$. Hence

$$\frac{A_{n_0}}{A_0} \cong \frac{A_n}{A_0}[N_{n_0}] = \frac{A_n}{A_0}.$$

It follows that $A_{n_0} \cong A_n$. □

In order to understand the structure of A_n we study its 2^k-torsion part for a fixed positive integer k. If k is big enough we have that $A_n = A_n[2^k]$.

Consider the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{C_{F_n}}{\pm 1} & \longrightarrow & \frac{O_{F_n}^{\times}}{\pm 1} & \longrightarrow & \frac{O_{F_n}^{\times}}{C_{F_n}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 2^k} & & \downarrow{\scriptstyle 2^k} & & \downarrow{\scriptstyle 2^k} & & \\ 0 & \longrightarrow & \frac{C_{F_n}}{\pm 1} & \longrightarrow & \frac{O_{F_n}^{\times}}{\pm 1} & \longrightarrow & \frac{O_{F_n}^{\times}}{C_{F_n}} & \longrightarrow & 0. \end{array}$$

The rows are exact. Therefore, snake lemma gives us the exact sequence of $\mathbb{Z}[G_n]$-modules

$$0 \longrightarrow A_n[2^k] \longrightarrow \frac{C_{F_n}}{\pm C_{F_n}^{2^k}} \longrightarrow \frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}} \longrightarrow 0. \tag{3.1}$$

Proposition 3.8. *Let $f \not\equiv 1 \bmod 8$ be a positive odd squarefree integer. Let $F_0 = \mathbb{Q}(\sqrt{f})$. Assume that $2|h_{F_0}$. Let X_{F_n} be the $\mathbb{Z}[G_n]$-submodule of C_{F_n} generated by -1 and η_n. Let $C_{\mathbb{Q}_n}$ be the $\mathbb{Z}[G_n]$-submodule of C_{F_n} generated by -1 and β_n. For a fixed positive integer k we denote by Y_n the cokernel of the morphism*

$$\frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} \longrightarrow \frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}}$$

induced by the inclusion $C_{\mathbb{Q}_n} \subset C_{F_n}$. Then, we have an exact sequence of $\mathbb{Z}[G_n]$-modules

$$0 \longrightarrow A_n[2^k] \longrightarrow \frac{X_{F_n}}{\pm X_{F_n}^{2^k}} \longrightarrow Y_n \longrightarrow 0.$$

Proof. Consider the natural commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} & \longrightarrow & \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} & \longrightarrow & 0\,. \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_n[2^k] & \longrightarrow & \frac{C_{F_n}}{\pm C_{F_n}^{2^k}} & \longrightarrow & \frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}} & \longrightarrow & 0 \end{array}$$

By Lemma 2.3 the rightmost map is injective. Moreover,

$$\frac{C_{F_n}}{\pm 1} = \frac{C_{\mathbb{Q}_n}}{\pm 1} \oplus \frac{X_{F_n}}{\pm 1}$$

as shown in Proposition 3.3. Then, applying the snake lemma we get

$$0 \longrightarrow A_n[2^k] \longrightarrow \frac{X_{F_n}}{\pm X_{F_n}^{2^k}} \longrightarrow Y_n \longrightarrow 0.$$

□

4. The split case

In this section we define the counterparts of C_{F_n} and A_n in the case f is a positive squarefree integer and $f \equiv 1 \bmod 8$. Later, we prove that if there exists a level $n_0 \geq 0$ such that $\#A_{n_0} = \#A_{n_0+1}$, then $A_{n_0} \cong A_n$ for any $n \geq n_0$. Finally, we describe the 2^k-torsion part of A_n for a fixed positive integer k.

Definition 4.1. Let $f \geq 3$ be a squarefree integer such that $f \equiv 1 \bmod 8$. Let $\delta'_f = \delta_f$ if f is prime or $\delta'_f = \delta_f^2$ otherwise. We define

$$C_{F_n} = \left\langle -1, \eta_n, \beta_n, \delta'_f \right\rangle_{\mathbb{Z}[G_n]}$$

for any $n \geq 1$. We put $C_{F_0} = \left\langle -1, \delta'_f \right\rangle_{\mathbb{Z}}$. It is convenient to set $\eta_0 = \mathrm{Norm}_{F_n|F_0}(\eta_n) = \pm 1$ and $\beta_0 = -1$.

For any $0 \leq m \leq n$ the module C_{F_m} is contained in C_{F_n}. Indeed, up to a sign we have that $\mathrm{Norm}_{F_n|F_m}(\eta_n) = \eta_m$ and $\mathrm{Norm}_{F_n|F_m}(\beta_n) = \beta_m$.

Proposition 4.2. *Let $f \geq 3$ be a squarefree integer such that $f \equiv 1 \bmod 8$. For any $n \geq 0$, we have inclusions*

$$\mathrm{Cyc}_{F_n} \subset C_{F_n} \subset O_{F_n}^{\times}$$

and the index $[O_{F_n}^{\times} : C_{F_n}]$ is equal to h_{F_n}.

Let $N_n = \sum_{i=0}^{2^n-1} \gamma^i \in \mathbb{Z}[G_n]$. Then, we have an isomorphism of $\mathbb{Z}[G_n]$-modules

$$\pi : \frac{\mathbb{Z}[G_n]}{(N_n)} \oplus \frac{\mathbb{Z}[G_n]}{(N_n)} \oplus \mathbb{Z} \longrightarrow \frac{C_{F_n}}{\pm 1}$$

defined by $(x, y, z) \mapsto \eta_n^x \beta_n^y {\delta'_f}^z$.

Proof. The fact that

$$\mathrm{Cyc}_{F_n} \subset C_{F_n} \subset O_{F_n}^{\times}$$

follows clearly from Lemmas 1.4 and 1.5.

Recall that $\mathrm{Norm}_{F_n|F_0}(\eta_n) = \pm 1$ when $f \equiv 1 \bmod 8$. Therefore, π is well defined. Moreover, since π is a surjective morphism between free modules of the same rank, it is an isomorphism.

In order to prove the statement about the index, we consider the image of $\mathrm{Cyc}_{F_n} / \pm 1$ via π^{-1}. By proposition 1.5 we have

$$\pi^{-1}(\mathrm{Cyc}_{F_n} / \pm 1) = \langle 2 \rangle_{\mathbb{Z}[G_n]/(N_n)} \oplus \langle 2 \rangle_{\mathbb{Z}[G_n]/(N_n)} \oplus \left\langle 2^j \right\rangle_{\mathbb{Z}}$$

where $j = 1$ if f is prime and $j = 0$ otherwise. It follows that $[C_{F_n} : \mathrm{Cyc}_{F_n}] = 2^{2^{n+1}-2+j}$. Finally, combining this result with Sinnott's index formula for the field F_n we get that the index $[O_{F_n}^{\times} : C_{F_n}]$ is equal to h_{F_n}. □

Corollary 4.3. *Let $f \geq 3$ be a positive squarefree integer such that $f \equiv 1 \bmod 8$. Let $0 \leq m \leq n$. Then, the natural inclusion induces an isomorphism*

$$C_{F_m} \cong C_{F_n}^{\mathrm{Gal}(F_n|F_m)}.$$

Proof. By Proposition 4.2, we have an isomorphism

$$\pi : \frac{\mathbb{Z}[G_n]}{(N_n)} \oplus \frac{\mathbb{Z}[G_n]}{(N_n)} \oplus \mathbb{Z} \longrightarrow \frac{C_{F_n}}{\pm 1}.$$

So, π induces an isomorphism

$$\underset{F_n|F_m}{\mathrm{Norm}} \cdot \left(\frac{\mathbb{Z}[G_n]}{(N_n)} \oplus \frac{\mathbb{Z}[G_n]}{(N_n)} \right) \oplus \mathbb{Z} \cong \left(\frac{C_{F_n}}{\pm 1} \right)^{\mathrm{Gal}(F_n|F_m)}.$$

It follows that the group $(C_{F_n}/\pm 1)^{\mathrm{Gal}(F_n|F_m)}$ is generated by $\mathrm{Norm}_{F_n|F_m}(\eta_n) = \eta_m$, $\mathrm{Norm}_{F_n|F_m}(\beta_n) = \beta_m$ and δ'_f. We conclude that $C_{F_n}^{\mathrm{Gal}(F_n|F_m)} = \langle -1, \eta_m, \beta_m, \delta'_f \rangle$. Hence we have $C_{F_n}^{\mathrm{Gal}(F_n|F_m)} = C_{F_m}$. □

Definition 4.4. Let $f \geq 3$ be a squarefree integer such that $f \equiv 1 \bmod 8$. For any $n \geq 0$ we define the $\mathbb{Z}_2[G_n]$-module

$$A_n = \frac{O_{F_n}^\times}{C_{F_n}} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \,.$$

The cardinality of A_n is equal to the 2-part of the class number h_{F_n}. Moreover, for any $0 \leq m \leq n$ the inclusions $O_{F_m}^\times \longrightarrow O_{F_n}^\times$ induce natural morphisms $A_m \longrightarrow A_n$. By Corollary 4.3, these morphisms are injective.

Proposition 4.5. *Let $f \geq 3$ be a squarefree integer so that $f \equiv 1 \bmod 8$. Let $0 \leq m \leq n$ and let $N_m = \sum_{i=0}^{2^m-1} \gamma^i \in \mathbb{Z}[G_n]$. Then, the natural morphism $A_m \longrightarrow A_n$ induces an isomorphism*

$$\frac{A_m}{A_0} \cong \frac{A_n}{A_0}[N_m].$$

Furthermore, if there exists an integer $n_0 \geq 0$ such that A_{n_0} and A_{n_0+1} have the same cardinality, then for any $n \geq n_0$ the natural morphisms $A_n \longrightarrow A_{n_0}$ are isomorphisms.

We omit the proof as it is similar to the one of Lemma 3.6 and the one of Proposition 3.7.

Fix now an integer $k > 0$. In order to study the 2^k-torsion part $A_n[2^k]$ we need the following Lemma:

Lemma 4.6. *Let $C_{\mathbb{Q}_n}$ be the $\mathbb{Z}[G_n]$-submodule of C_{F_n} generated by -1 and β_n. Then, the natural morphisms*

$$\frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} \oplus \frac{O_{F_0}^\times}{\pm O_{F_0}^{\times 2^k}} \longrightarrow \frac{O_{F_n}^\times}{\pm O_{F_n}^{\times 2^k}}$$

are injective for any $n, k \geq 1$.

Proof. As a consequence of Lemma 2.2, it suffices to show that the map

$$\iota : \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2}} \oplus \frac{O_{F_0}^\times}{\pm O_{F_0}^{\times 2}} \longrightarrow \frac{O_{F_n}^\times}{\pm O_{F_n}^{\times 2}}$$

is injective.

Consider the following commutative diagram of $\mathbb{Z}[G_n]$-modules:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^2} & \longrightarrow & \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^2} & \longrightarrow & 0\,. \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker\iota & \longrightarrow & \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^2} \oplus \frac{O_{F_0}^\times}{\pm O_{F_0}^{\times 2}} & \longrightarrow & \frac{O_{F_n}^\times}{\pm O_{F_n}^{\times 2}} & & \end{array}$$

The rows are exact. Moreover, by Lemma 2.3 the rightmost vertical map is injective. Using the snake lemma we can identify $\ker\iota$ with a subgroup of $O_{F_0}^\times/\pm O_{F_0}^{\times 2}$. Therefore, the cardinality of $\ker\iota$ is at most 2.

We know that

$$\frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^2} \oplus \frac{O_{F_0}^\times}{O_{F_0}^{\times 2}} \cong \frac{\mathbb{Z}[G_n]}{(2, N_n)} \oplus \frac{\mathbb{Z}}{2\,\mathbb{Z}}.$$

So the only $\mathbb{Z}[G_n]$-submodules with 2 elements are the following:

$$\langle(\beta_1, 1)\rangle\,, \quad \langle(1, \varepsilon)\rangle\,, \quad \langle(\beta_1, \varepsilon)\rangle\,,$$

where ε is a fundamental unit of F_0. Note that $\beta_1 \notin \pm O_{F_n}^{\times^2}$ by Lemma 2.3.

Assume that $\ker\iota$ is generated by $(1, \varepsilon)$. Then, the unit ε lies in $\pm O_{F_n}^{\times 2}$. Since the fundamental unit ε is defined up to a sign, we assume that there exists $z \in O_{F_n}^\times$ such that $\varepsilon = z^2$. Otherwise, if $\varepsilon = -z^2$ we consider $-\varepsilon$ as a fundamental unit. Note that the extension $F_0(z)$ has degree 2 over F_0. Therefore, $z \in F_1 = F_0(\sqrt{2})$. So $z = x + \sqrt{2}y$ for some $x, y \in F_0$. The relation $z^2 = \varepsilon$ gives us two cases: or $x^2 = \varepsilon$ or $2y^2 = \varepsilon$. The first case is impossible as ε is a fundamental unit. On the other hand, if there exists $y \in F_0$ such that $2y^2 = \varepsilon$, then $(y^{-1})^2 = 2\varepsilon^{-1}$. Since $(y^{-1})^2$ lies in $2O_{F_0}$ and the prime 2 splits in O_{F_0}, we get that $y^{-1} \in 2O_{F_0}$. Note that

$$\pm 4 = \operatorname*{Norm}_{F_0|\,\mathbb{Q}}(2\varepsilon^{-1}) = \left(\operatorname*{Norm}_{F_0|\,\mathbb{Q}}(y^{-1})\right)^2 \in 16\,\mathbb{Z}\,.$$

This leads to a contradiction.

Assume that $\ker\iota$ is generated by (β_1, ε). Then, the unit $\beta_1\varepsilon$ lies in $\pm O_{F_n}^{\times 2}$. So there exists $z \in O_{F_n}^\times$ such that

$$\beta_1\varepsilon = z^2, \quad \text{or} \quad \beta_1\varepsilon = -z^2.$$

Consider γ a generator of $G_n = \mathrm{Gal}(F_n|F_0)$. Then

$$(z^{1+\gamma})^2 = (\pm z^2)^{1+\gamma} = \operatorname*{Norm}_{\mathbb{Q}_1\,|\,\mathbb{Q}}(\beta_1)\varepsilon^2 = -\varepsilon^2.$$

This leads to a contradiction with the fact that F_n is a real field.

We conclude that $\ker\iota = 1$.

□

We conclude this section describing $A_n[2^k]$.

Proposition 4.7. *Let $f \geq 3$ be a squarefree integer such that $f \equiv 1 \bmod 8$. Let X_{F_n} be the $\mathbb{Z}[G_n]$-submodule of C_{F_n} generated by -1 and η_n. Let $C_{\mathbb{Q}_n}$ be the $\mathbb{Z}[G_n]$-submodule of C_{F_n} generated by -1 and β_n. For a fixed positive integer k, we denote by Y_n the cokernel of the natural morphism*

$$\frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} \oplus \frac{C_{F_0}}{\pm C_{F_0}^{2^k}} \longrightarrow \frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}}$$

induced by the inclusions $C_{\mathbb{Q}_n} \subset C_{F_n}$ and $C_{F_0} \subset C_{F_n}$. Then, we have an exact sequence of $\mathbb{Z}[G_n]$-modules

$$0 \longrightarrow \frac{A_n[2^k]}{A_0[2^k]} \longrightarrow \frac{X_{F_n}}{\pm X_{F_n}^{2^k}} \longrightarrow Y_n \longrightarrow 0.$$

Proof. Notice that we can describe the 2^k-torsion of A_n with an exact sequence similar to the one in (3.1). In other words, we have

$$0 \longrightarrow A_n[2^k] \longrightarrow \frac{C_{F_n}}{\pm C_{F_n}^{2^k}} \longrightarrow \frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}} \longrightarrow 0.$$

In particular, the map

$$\frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} \oplus \frac{C_{F_0}}{\pm C_{F_0}^{2^k}} \longrightarrow \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} \oplus \frac{C_{F_0}}{\pm O_{F_0}^{\times 2^k} \cap C_{F_0}}$$

induced by the identity on the first component and by the natural quotient on the second component has kernel isomorphic to $A_0[2^k]$.

We consider the natural commutative diagram whose rows are exact:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_0[2^k] & \longrightarrow & \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} \oplus \frac{C_{F_0}}{\pm C_{F_0}^{2^k}} & \longrightarrow & \frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} \oplus \frac{C_{F_0}}{\pm O_{F_0}^{\times 2^k} \cap C_{F_0}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_n[2^k] & \longrightarrow & \frac{C_{F_n}}{\pm C_{F_n}^{2^k}} & \longrightarrow & \frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}} & \longrightarrow & 0.
\end{array}$$

By Lemma 4.6 the rightmost vertical map is injective. Furthermore, we have an isomorphism

$$\frac{C_{F_n}}{\pm 1} \cong \frac{X_{F_n}}{\pm 1} \oplus \frac{C_{\mathbb{Q}_n}}{\pm 1} \oplus \frac{C_{F_0}}{\pm 1}$$

as observed in Proposition 4.2. Therefore, applying the snake lemma we get the exact sequence

$$0 \longrightarrow \frac{A_n[2^k]}{A_0[2^k]} \longrightarrow \frac{X_{F_n}}{\pm X_{F_n}^{2^k}} \longrightarrow Y_n \longrightarrow 0.$$

□

5. The dual module

In this section we recall the definition and some properties of finite Gorenstein rings. We use them to describe the dual of $C_{F_n}/\pm O_{F_n}^{\times 2^k} \cap C_{F_n}$ in terms of Galois groups.

Definition 5.1. Let R be a commutative finite ring. For any R-module A, we have the group $A^\perp = \mathrm{Hom}_R(A,R)$ and the dual group $A^{\mathrm{dual}} = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$. They are R-modules via $(r\phi)(a) = \phi(ra)$ for any $r \in R$ and $a \in A$. The ring R is said to be Gorenstein if R^{dual} is a free R-module of rank one.

We state below the properties of Gorenstein rings we need.

Proposition 5.2. *Let R be a finite Gorenstein ring. Then*

(a) For every R-module A, the map

$$A^\perp = \mathrm{Hom}_R(A,R) \to A^{\mathrm{dual}} = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$$

defined by $\psi \mapsto \phi \circ \psi$ is an isomorphism of R-modules. Here $\phi : R \to \mathbb{Q}/\mathbb{Z}$ denotes a generator of R^{dual}. In particular if A is finite, then $\#A = \#A^\vee$.

(b) The functor $A \to A^\perp$ from the category of finite R-module to itself is exact.

These properties are shown in [Sch02, Proposition 1.1].

Remark 5.3. Let $R_k = \mathbb{Z}/2^k\mathbb{Z}[G_n]$. It is a finite Gorenstein ring. We made explicit the isomorphism described in the Proposition above. Let $\phi : R_k \longrightarrow \mathbb{Z}/2^k\mathbb{Z}$ be the homomorphism that maps an element $\sum_{g\in G_n} x_g g$ to x_1. Then ϕ generates the R_k-module $\mathrm{Hom}_{R_k}(R_k, \mathbb{Z}/2^k\mathbb{Z})$ which is isomorphic to R_k^{dual}. If ψ is an element of $\mathrm{Hom}_{R_k}(A, R_k)$ that maps a to $\sum_{g\in G_n} x_g g$, then the composition $\phi \circ \psi : A \longrightarrow \mathbb{Z}/2^k\mathbb{Z}$ maps a to x_1.

Lemma 5.4. *Let R be a finite Gorenstein ring and let A be an R-module. Assume there exists $r \in R$ such that $r(A^\perp) = 0$. Then, the module rA is trivial.*

Proof. Consider the exact sequence of R-modules

$$0 \longrightarrow A[r] \longrightarrow A \xrightarrow{r} A \longrightarrow A/rA \longrightarrow 0.$$

The dual map $A^\perp \longrightarrow A^\perp$ induced by the multiplication by r on A is the multiplication by r on $A^\perp$. Therefore, applying the functor $(-)^\perp$ we get the exact sequence

$$0 \longrightarrow (A/rA)^\perp \longrightarrow A^\perp \xrightarrow{r} A^\perp \longrightarrow A[r]^\perp \longrightarrow 0.$$

Since r annihilates $A^\perp$, we get $(A/rA)^\perp \cong A^\perp$. By the faithfulness of $(-)^\perp$, we deduce that the natural quotient $A \longrightarrow A/rA$ is an isomorphism. This implies that $rA = 0$. □

We give now two corollaries of Propositions 3.8 and 4.7.

Corollary 5.5 (of Proposition 3.8)**.** *Let $f \not\equiv 1 \bmod 8$ be an odd positive squarefree integer. Assume that the class number of $F_0 = \mathbb{Q}(\sqrt{f})$ is even. Let $R_k = \mathbb{Z}/2^k\mathbb{Z}[G_n]$ for some positive integer k. Then*

$$A_n[2^k]^\perp \cong \frac{R_k}{\{\psi(\eta_n) \ : \ \psi \in Y_n^\perp\}}.$$

Moreover

$$Y_n^{\perp}=\left\{\psi\in\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k}\cap C_{F_n}}\right)^{\perp}\ :\ \psi(\beta_n)=0\right\}.$$

Proof. From the definition of Y_n and the fact that $(-)^{\perp}$ is an exact functor on the category of finite R_k-module we deduce that the sequence

$$0\longrightarrow Y_n^{\perp}\longrightarrow\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k}\cap C_{F_n}}\right)^{\perp}\longrightarrow\left(\frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{\times 2^k}}\right)^{\perp}$$

is exact. Since $C_{\mathbb{Q}_n}/\pm 1$ is generated by β_n we get that

$$Y_n^{\perp}=\left\{\psi\in\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k}\cap C_{F_n}}\right)^{\perp}\ :\ \psi(\beta_n)=0\right\}.$$

By Proposition 3.8 and by the exactness of the functor $(-)^{\perp}$ we get an exact sequence of R_k-modules

$$0\longrightarrow Y_n^{\perp}\longrightarrow\left(\frac{X_{F_n}}{\pm X_{F_n}^{2^k}}\right)^{\perp}\longrightarrow A_n[2^k]^{\perp}\longrightarrow 0.$$

Due to Proposition 3.3 we have $X_{F_n}/\pm X_{F_n}^{2^k}\cong R_k$. Therefore we can identify $\left(X_{F_n}/\pm X_{F_n}^{2^k}\right)^{\perp}$ with R_k via the isomorphism that maps ψ to $\psi(\eta_n)$. Via this identification we get the exact sequence

$$0\longrightarrow\{\psi(\eta_n)\ :\ \psi\in Y_n^{\perp}\}\longrightarrow R_k\longrightarrow A_n[2^k]\longrightarrow 0.$$

□

Corollary 5.6 (of Proposition 4.7)**.** *Let $f\equiv 1 \bmod 8$ be a squarefree integer so that $f\geq 3$. Let $R_k=\mathbb{Z}/2^k\mathbb{Z}[G_n]$ for some positive integer k. Then*

$$\left(\frac{A_n[2^k]}{A_0[2^k]}\right)^{\perp}\cong\frac{I_k}{\{\psi(\eta_n)\ :\ \psi\in Y_n^{\perp}\}}$$

where $I_k\subset R_k$ is the augmentation ideal. Moreover

$$Y_n^{\perp}=\left\{\psi\in\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k}\cap C_{F_n}}\right)^{\perp}\ :\ \psi(\beta_n)=\psi(\delta_f')=0\right\}.$$

Proof. The proof is essentially the same as the one of Corollary 5.5. By Proposition 4.7 the module $Y_n^\perp$ fits in the exact sequences

$$0 \longrightarrow Y_n^\perp \longrightarrow \left(\frac{X_{F_n}}{\pm X_{F_n}^{2^k}}\right)^\perp \longrightarrow \left(\frac{A_n[2^k]}{A_0[2^k]}\right)^\perp \longrightarrow 0,$$

$$0 \longrightarrow Y_n^\perp \longrightarrow \left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}}\right)^\perp \longrightarrow \left(\frac{C_{\mathbb{Q}_n}}{\pm C_{\mathbb{Q}_n}^{2^k}} \oplus \frac{C_{F_0}}{\pm C_{F_0}^{2^k}}\right)^\perp.$$

From the second one we deduce that $\psi \in \left(C_{F_n}/\pm O_{F_n}^{\times 2^k} \cap C_{F_n}\right)^\perp$ lies in $Y_n^\perp$ if and only if it is trivial when evaluated both in β_n and δ'_f.

Since $X_{F_n}/\pm X_{F_n}^{2^k} \cong R_k/(N_n)$ we have an isomorphism $(X_{F_n} \pm X_{F_n}^{2^k})^\perp \cong I_k$ defined by mapping ψ to $\psi(\eta_n)$. Under this identification $Y_n^\perp$ is mapped to

$$\left\{\psi(\eta_n) \ : \ \psi \in Y_n^\perp\right\} \subset I_k.$$

This concludes the proof of the Corollary. □

We conclude this section describing the elements of $\left(C_{F_n}/\pm O_{F_n}^{\times 2^k} \cap C_{F_n}\right)^\perp$.

Definition 5.7. Fix $f \geq 3$ an odd squarefree integer. Let r be a prime that completely splits in $F_n(\zeta_4) = \mathbb{Q}(\zeta_{2^{n+2}}, \sqrt{f})$. In other words, $r \equiv 1 \bmod 2^{n+2}$ and f is a square modulo r. Let $k \leq n+1$ be a positive integer. Choose a prime $\mathfrak{R}$ of $F_n(\zeta_4)$ dividing r and a primitive 2^k-root of unity ζ_{2^k}. For any $u \in C_{F_n}$ we define $\log_r(u)$ as the element of $\mathbb{Z}/2^k\mathbb{Z}$ such that

$$u^{\frac{r-1}{2^k}} \equiv \zeta_{2^k}^{\log_r(u)} \bmod \mathfrak{R}.$$

We define $f_r \in \left(C_{F_n}/\pm O_{F_n}^{\times 2^k} \cap C_{F_n}\right)^\perp$ as

$$f_r(u) = \sum_{g \in G_n} \log_r(u^g) g^{-1}.$$

Notice that the definition of f_r depends both on a choice of a primitive 2^k-th root of unity and of a prime $\mathfrak{R}$. If we choose a different ζ_{2^k} we are multiplying f_r by an invertible element of $\mathbb{Z}/2^k\mathbb{Z}$. While if we change $\mathfrak{R}$ we are multiplying f_r by an element of G_n. Therefore f_r is well defined up to an invertible element of R_k. If we want to stress the choice of the ideal $\mathfrak{R}$ we write $f_{\mathfrak{R}}$ instead of f_r.

Proposition 5.8. *Let $\mathcal{P}_n$ be the set of prime numbers that split completely in $F_n(\zeta_4)$. Let $0 < k \leq n+1$. Then*

$$\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}}\right)^\perp = \langle f_r \ : \ r \in \mathcal{P}_n \rangle_{R_k}.$$

Proof. Consider the natural map

$$\iota : O_{F_n}^\times / O_{F_n}^{\times 2^k} \longrightarrow F_n(\zeta_4)^\times / F_n(\zeta_4)^{\times 2^k}.$$

As a consequence of Proposition 2.1 we have that the $\ker \iota$ is isomorphic to a subgroup of $\mathrm{H}^1(\mathrm{Gal}(F_n(\zeta_4)|F_n), \langle \zeta_{2^k} \rangle)$. Since $\mathrm{Gal}(F_n(\zeta_4)|F_n)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and is generate by complex conjugation we get that $\mathrm{H}^1(\mathrm{Gal}(F_n(\zeta_4)|F_n), \langle \zeta_{2^k} \rangle)$ has order 2. Therefore, $\#\ker \iota \leq 2$. Since $\zeta_{2^{n+2}} \in F_n(\zeta_4)$ we have that -1 is a 2^k-power in $F_n(\zeta_4)$ but not in $O_{F_n}^\times$. Hence

$$\iota : O_{F_n}^\times / \pm O_{F_n}^{\times 2^k} \longrightarrow F_n(\zeta_4)^\times / F_n(\zeta_4)^{\times 2^k}$$

is injective.

We can identify $C_{F_n}/\pm O_{F_n}^{\times 2^k} \cap C_{F_n}$ with a subgroup of $F_n(\zeta_4)^\times / F_n(\zeta_4)^{\times 2^k}$. Then, Kummer theory gives us an isomorphism

$$\mathrm{Gal}\left(F_n(\zeta_4, \sqrt[2^k]{C_{F_n}})|F_n(\zeta_4)\right) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}}, \frac{\mathbb{Z}}{2^k\,\mathbb{Z}}\right).$$

This isomorphism depends on the choice of a 2^k-primitive root of unity. On the other hand, since R_k is finite Gorenstein we have the isomorphism described in Remark 5.3:

$$\mathrm{Hom}_{R_k}\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}}, R_k\right) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}}, \frac{\mathbb{Z}}{2^k\,\mathbb{Z}}\right).$$

Choose a prime ideal $\mathfrak{R} \subset O_{F_n(\zeta_4)}^\times$ that divides $r \in \mathcal{P}_n$. It is easy to check that the image under Kummer isomorphism of the Frobenius morphism associated to $\mathfrak{R}$ and the image of $f_{\mathfrak{R}}$ under the isomorphism given by the Gorenstein ring properties coincide.

Recall that the Chebotarëv density theorem states that every element of the Galois group $\mathrm{Gal}(F_n(\zeta_4, \sqrt[2^k]{C_{F_n}})|F_n(\zeta_4))$ is a Frobenius morphism associated to a prime that splits completely in $F_n(\zeta_4)$. Therefore we get

$$\left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^k} \cap C_{F_n}}\right)^\perp = \{f_{\mathfrak{R}} \ : \ \mathfrak{R}|r \,\text{and}\, r \in \mathcal{P}_n\} = \langle f_r \ : \ r \in \mathcal{P}_n \rangle_{R_k}.$$

□

6. The algorithm

We explain in this section how we implement the above ideas on a computer. It is possible to find an upper bound for the cardinality of A_n. In this section we fix a level n and the integer $k = n+1$. Let π be the the isomorphism

$$\pi : R_{n+1} = \frac{\mathbb{Z}}{2^{n+1}\,\mathbb{Z}}[G_n] \longrightarrow \frac{\mathbb{Z}_2[X]}{(2^{n+1}, X^{2^n} - 1)}$$

that maps γ to X. Via this isomorphism we translate the results of Corollaries 5.5 and 5.6 in terms of polynomials so that a computer can easily handle them. For any $u \in C_{F_n}$ and $r \in \mathcal{P}_n$ we define the polynomial

$$f_r^u(X) = \sum_{i=0}^{2^n-1} \log_r(u^{\gamma^{-i}}) X^i \in \frac{\mathbb{Z}_2[X]}{(2^{n+1}, X^{2^n} - 1)}.$$

Note that $\pi(f_r(u)) = f_r^u(X)$.

Assume f to be a positive odd squarefree integer such that $f \not\equiv 1 \bmod 8$ and $2|h_{F_0}$. We want to find a collection of elements inside $Y_n^{\perp}$. We compute primes $r_1, r_2, \dots$ that are congruent to 1 modulo $2^{n+2}f$. This implies that those primes split completely in $\mathbb{Q}(\zeta_{2^{n+2}f})$ and consequently in $F_n(\zeta_4)$. Since $\beta_n \in C_{F_n}/\pm 1$ is annihilated by N_n, the elements $f_{r_i}(\beta_n)$ lie in the augmentation ideal of R_{n+1}. In particular, $\gamma - 1$ divides $f_{r_i}(\beta_n)$. For any pair (r_i, r_j) we define

$$g_{i,j} = \frac{f_{r_i}(\beta_n)}{\gamma - 1} f_{r_j} - \frac{f_{r_j}(\beta_n)}{\gamma - 1} f_{r_i}.$$

This is an element of $Y_n^{\perp}$. Indeed, $g_{i,j}(\beta_n) = 0$. Let $J^{(1)}$ be the zero ideal of R_{n+1}. For any $i \geq 2$, we compute the R_{n+1}-ideals

$$J^{(i)} = J^{(i-1)} + (g_{i,j}(\eta_n) \ : \ 1 \leq j < i).$$

Since R_{n+1} is a finite ring, the ideals $J^{(i)}$ stabilize in finitely many steps to an ideal J_n. By Corollary 5.5 there is a surjective homomorphism

$$\frac{R_{n+1}}{J_n} \longrightarrow A_n[2^{n+1}]^{\perp}.$$

On a computer this strategy looks like the following: for a prime $r_i \equiv 1 \bmod 2^{n+2}f$ we compute the polynomials $f_{r_i}^{\beta_n}(X)$ and $f_{r_i}^{\eta_n}(X)$. Then, for any $j < i$ we have

$$\pi(g_{i,j}(\eta_n)) = \frac{f_{r_i}^{\beta_n}(X)}{X - 1} f_{r_j}^{\eta_n}(X) - \frac{f_{r_j}^{\beta_n}(X)}{X - 1} f_{r_i}^{\eta_n}(X).$$

If M is an integer sufficiently large, then π induces an isomorphism

$$\frac{R_{n+1}}{J_n} \xrightarrow{\pi} \frac{\mathbb{Z}_2[X]}{(2^{n+1}, X^{2^n} - 1, \pi(g_{i,j}(\eta_n)) \ : \ 1 \leq j < i \leq M)}. \tag{6.1}$$

Let 2^{m_0} be the cardinality of the 2-part of h_{F_0}. We compute the ideals $J_n \subset R_{n+1}$ for $n = 1, 2, \dots$ until the hypotheses of the following Lemma are satisfied.

Lemma 6.1. *Let $f \not\equiv 1 \bmod 8$ be an odd squarefree integer. Assume that $2|h_{F_0}$. Let 2^{m_0} be the cardinality of A_0. Assume that there exists an integer m such that $2^m \in J_m$. Then, we have a surjective morphism of $\mathbb{Z}[G_m]$-modules*

$$\frac{R_{m+1}}{J_m} \longrightarrow A_m^{\perp}.$$

Moreover, assume that one of the following properties holds.

(a) The cardinality of R_{m+1}/J_m is strictly less than 2^{m+m_0},
(b) the element $N_{m-1} \in R_{m+1}$ lies in the ideal J_m.

Then, the natural morphisms $A_{m-1} \longrightarrow A_n$ are isomorphisms for any $n \geq m - 1$.

Proof. We have a surjection of $\mathbb{Z}[G_m]$-modules

$$\frac{R_{m+1}}{J_m} \longrightarrow A_m[2^{m+1}]^{\perp}$$

Since 2^m lies in J_m we get that 2^m annihilates $A_m[2^{m+1}]^\perp$. By Lemma 5.4 the element 2^m annihilates $A_m[2^{m+1}]$ and Nakayama's lemma implies that $A_m[2^{m+1}] = A_m$. So, we are getting an upper bound for the cardinality of the full module A_m.

Assume that (a) holds. Then, we have

$$2^{m_0} = \#A_0 \leq \#A_1 \leq \cdots \leq \#A_m < 2^{m+m_0}.$$

Therefore, there exists a level $m' < m$ so that $\#A_{m'} = \#A_{m'+1}$. Proposition 3.7 implies that $A_{m'} \cong A_n$ for any $n \geq m'$.

Assume that (b) holds. Then N_{m-1} annihilates $A_m^\perp$ and its submodule $(A_m/A_0)^\perp$. So, the element N_{m-1} annihilates A_m/A_0 too. By Lemma 3.6, we conclude that

$$\frac{A_{m-1}}{A_0} \cong \frac{A_m}{A_0}[N_{m-1}] = \frac{A_m}{A_0}.$$

We get that $\#A_{m-1} = \#A_m$ since the natural morphisms $A_0 \longrightarrow A_n$ are injective for any positive n. Finally, Proposition 3.7 implies that $A_{m-1} \cong A_n$ for any $n \geq m-1$. □

Assume now that $f \geq 3$ is a positive squarefree integer and $f \equiv 1 \bmod 8$. We find several primes $r_1, r_2, \ldots$ that are congruent to 1 mod $2^{n+2}f$. Since δ'_f is annihilated by $\gamma - 1$, the elements $f_{r_i}(\delta'_f) \in R_{n+1}$ are divisible by N_n. Fix $i \geq 2$. Let H_i be the subset of $(C_{F_n}/\pm O_{F_n}^{n+1} \cap C_{F_n})^\perp$ whose elements are

$$\frac{f_{r_j}(\delta'_f)}{2^{s(j,l)}N_n} f_{r_l} - \frac{f_{r_l}(\delta'_f)}{2^{s(j,l)}N_n} f_{r_j}$$

where $1 \leq j < l \leq i$ and $s(j,l) \leq n+1$ is the largest integer such that both $f_{r_j}(\delta'_f)$ and $f_{r_l}(\delta'_f)$ are congruent to 0 modulo $2^{s(j,l)}$. The elements of H_i are trivial when evaluated in δ'_f. For any pair of elements $h_j, h_l \in H_i$ we define

$$g_{h_j,h_l} = \frac{h_j(\beta_n)}{\gamma - 1} h_l - \frac{h_l(\beta_n)}{\gamma - 1} h_j.$$

Note that g_{h_j,h_l} is trivial when evaluated in both δ'_f and β_n. Therefore, the functions g_{h_j,h_l} lie in $Y_n^\perp$. Let $J^{(i)}$ be the R_{n+1}-ideal

$$J^{(i)} = \left(g_{h_j,h_l}(\eta_n) \ : \ h_j, h_l \in H_i\right).$$

It is easy to check that we have inclusions $J^{(i)} \subset J^{(i+1)}$. So the ideals $J^{(i)}$ stabilize in finitely many steps to an ideal J_n. Let $I_{n+1} \subset R_{n+1}$ be the augmentation ideal. By Corollary 5.6 there is a surjective morphism

$$\frac{I_{n+1}}{J_n} \longrightarrow \left(\frac{A_n[2^{n+1}]}{A_0[2^{n+1}]}\right)^\perp.$$

Furthermore, if M is a sufficiently large integer then π induces an isomorphism

$$\frac{I_{n+1}}{J_n} \xrightarrow{\pi} \frac{(X-1)\,\mathbb{Z}_2[X]}{(2^{n+1}(X-1), X^{2^n} - 1, \pi(g_{h_j,h_l}(\eta_n)) \ : \ h_j, h_l \in H_M)}.$$

Then, dividing by $X-1$ we get an isomorphism

$$\frac{I_{n+1}}{J_n} \longrightarrow \frac{\mathbb{Z}_2[X]}{\left(2^{n+1}, \frac{X^{2^n}-1}{X-1}, \frac{\pi(g_{h_j,h_l}(\eta_n))}{X-1} \ : \ h_j, h_l \in H_M\right)} \tag{6.2}$$

The polynomials $\pi(g_{h_j,h_l}(\eta_n))$ can be computed using combinations of $f_{r_i}^{\eta_n}(X)$, $f_{r_i}^{\beta_n}(X)$ and $f_{r_i}^{\delta'_f}(X)$.

For $n = 1, 2, \ldots$ we compute the ideal J_n until the hypotheses of the next Lemma are satisfied.

Lemma 6.2. *Let $f \not\equiv 1 \bmod 8$ and $2|h_{F_0}$. Let 2^{m_0} be the cardinality of A_0. Assume that there exists an integer $m \geq m_0$ such that $2^{m-m_0} \in J_m$. Then, we have a surjective morphism of $\mathbb{Z}[G_m]$-modules*

$$\frac{I_{m+1}}{J_m} \longrightarrow \left(\frac{A_m}{A_0}\right)^{\perp}.$$

Moreover, assume that one of the following properties holds.

(a) The cardinality of I_{m+1}/J_m is strictly less than 2^m,
(b) the element $N_{m-1} \in R_{m+1}$ annihilates I_{m+1}/J_m.

Then, the natural morphisms $A_{m-1} \longrightarrow A_n$ are isomorphisms for any $n \geq m-1$.

Proof. We have a surjection of $\mathbb{Z}[G_m]$-modules

$$\frac{I_{m+1}}{J_m} \longrightarrow \left(\frac{A_m[2^{m+1}]}{A_0}\right)^{\perp}.$$

Since 2^{m-m_0} lies in J_m we have that 2^{m-m_0} annihilates $(A_m[2^{m+1}]/A_0)^{\perp}$. By Lemma 5.4 the element 2^{m-m_0} annihilates $A_m[2^{m+1}]/A_0$. It follows that 2^m annihilates $A_m[2^{m+1}]$ and Nakayama's lemma implies that $A_m[2^{m+1}] = A_m$.

Assume that (a) holds. Then, we have

$$2^{m_0} = \#A_0 \leq \#A_1 \leq \cdots \leq \#A_m < 2^{m+m_0}.$$

Therefore, there exists a level $m' < m$ so that $\#A_{m'} = \#A_{m'+1}$. Proposition 4.5 implies that $A_{m'} \cong A_n$ for any $n \geq m'$.

Assume that (b) holds. Then N_{m-1} annihilates $(A_m/A_0)^{\perp}$. So, the element N_{m-1} annihilates A_m/A_0 too. By Proposition 4.5, we conclude that

$$\frac{A_{m-1}}{A_0} \cong \frac{A_m}{A_0}[N_{m-1}] = \frac{A_m}{A_0}.$$

We get that $\#A_{m-1} = \#A_m$ since the natural morphisms $A_0 \longrightarrow A_n$ are injective for any positive n. Finally, Proposition 4.5 implies that $A_{m-1} \cong A_n$ for any $n \geq m-1$. □

We conclude this section giving explicit formulae for the polynomials $f_r^{\eta_n}(X)$, $f_r^{\beta_n}(X)$ and $f_r^{\delta'_f}(X)$. Assume $f \equiv 3 \bmod 4$. Let χ_{-f} be the Dirichlet quadratic character for the field $\mathbb{Q}(\sqrt{-f})$. We have an isomorphism $\ker \chi_{-f} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_f), \mathbb{Q}(\sqrt{-f}))$. Notice that $F_{n+1} = \mathbb{Q}(\zeta_{2^{n+3}}, \sqrt{-f})^+$, therefore we get

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^{n+3}f})^+ | F_{n+1}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{2^{n+3}f}) | \mathbb{Q}(\zeta_{2^{n+3}}, \sqrt{-f})) \cong \ker \chi_{-f}.$$

We get that

$$\eta_n = \prod_{a\in\ker\chi_{-f}} \left(\zeta_4(\zeta_{2^{n+3}}\zeta_f^a - \zeta_{2^{n+3}}^{-1}\zeta_f^{-a})\right).$$

Moreover, a generator γ of G_n can be chosen as the inverse of the restriction to F_n of $\phi \in \mathrm{Gal}(\mathbb{Q}(\zeta_{2^{n+2}},\zeta_f)|\,\mathbb{Q}(\zeta_f))$ defined by $\phi(\zeta_{2^{n+2}}) = \zeta_{2^{n+2}}^3$. It follows that

$$f_r^{\eta_n}(X) = \sum_{i=0}^{2^n-1} \log_r\left(\prod_{a\in\ker\chi_{-f}} \left(\zeta_4^{3^i}\left(\zeta_{2^{n+3}}^{3^i}\zeta_f^a - \zeta_{2^{n+3}}^{-3^i}\zeta_f^{-a}\right)\right)\right) X^i.$$

On the other hand if $f \equiv 1 \bmod 4$, let χ_f be the quadratic character for the field $\mathbb{Q}(\sqrt{f})$. As above we have that $F_{n+1} = \mathbb{Q}(\zeta_{2^{n+3}},\sqrt{f})^+$ and the group $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^{n+3}f})^+|F_{n+1})$ is isomorphic to $\ker\chi_f$. Therefore

$$f_r^{\eta_n}(X) = \sum_{i=0}^{2^n-1} \log_r\left(\prod_{a\in\ker\chi_{f}} \left(\zeta_4^{3^i}\left(\zeta_{2^{n+3}}^{3^i}\zeta_f^a - \zeta_{2^{n+3}}^{-3^i}\zeta_f^{-a}\right)\right)\right) X^i.$$

In both cases, we have

$$f_r^{\beta_n}(X) = \sum_{i=0}^{2^n-1} \log_r\left(\zeta_{2^{n+2}}^{\frac{3^i-3^{i+1}}{2}} \frac{1-\zeta_{2^{n+2}}^{3^{i+1}}}{1-\zeta_{2^{n+2}}^{3^i}}\right) X^i.$$

Finally, if $f \equiv 1 \bmod 8$ we have

$$f_r^{\delta_f'}(X) = f_r^{\delta_f^2}(X) = \log_r\left(\prod_{a\in\ker\chi_f}(1-\zeta_f^a)\right)\sum_{i=0}^{2^n-1} X^i$$

when f is not prime. While if f is prime we get

$$f_r^{\delta_f'}(X) = f_r^{\delta_f}(X) = \log_r\left(\prod_{a\in\ker\chi_f/\pm1} \zeta_f^{a\frac{s-1}{2}} \frac{1-\zeta_f^a}{1-\zeta_f^{as}}\right)\sum_{i=0}^{2^n-1} X^i$$

where s is an element in $(\mathbb{Z}/f\mathbb{Z})^\times$ but not in $\ker\chi_f$. See the proof of Lemma 1.4 part (c) for an explicit form of δ_f.

Remark 6.3. Notice that we restrict our attention to primes $r \equiv 1 \bmod 2^{n+2}f$. We do that in order to simplify the computation of the above polynomials. Indeed, for such primes $\zeta_{2^{n+3}f}$ lies in $\mathbb{F}_{r^2}$. Otherwise, $\zeta_{2^{n+2}f}$ lies in a larger subfield of $\mathbb{F}_{r^{\varphi(f)}}$. So, computing $f_r^{\eta_n}(X)$ became harder without the assumption $r \equiv 1 \bmod 2^{n+2}f$.

Remark 6.4. In general we do not expect that the surjective morphisms

$$\frac{R_{n+1}}{J_n} \longrightarrow A_n[2^{n+1}]^\perp, \quad \text{if } f \not\equiv 1 \bmod 8 \text{ and } 2|h_{F_0},$$

$$\frac{I_{n+1}}{J_n} \longrightarrow \left(\frac{A_n[2^{n+1}]}{A_0[2^{n+1}]}\right)^\perp, \quad \text{if } f \equiv 1 \bmod 8,$$

are actually isomorphisms. Indeed, letting $L_n = \mathbb{Q}(\zeta_{2^{n+2}f})^+$ it is easy to check that

$$\left(\frac{C_{F_n}}{\pm O_{L_n}^{\times 2^{n+1}} \cap C_{F_n}}\right)^{\perp} = \left\langle f_r \ : \ r \equiv 1 \bmod 2^{n+2}f \right\rangle_{R_{n+1}} \subset \left(\frac{C_{F_n}}{\pm O_{F_n}^{\times 2^{n+1}} \cap C_{F_n}}\right)$$

The proof of this fact is similar to the one of Proposition 5.8. Taking the dual, we have that the cokernel of the above inclusion is the dual of the kernel of the natural morphism

$$\iota : \frac{C_{F_n}}{\pm O_{F_n}^{\times 2^{n+1}} \cap C_{F_n}} \longrightarrow \frac{C_{F_n}}{\pm O_{L_n}^{\times 2^{n+1}} \cap C_{F_n}}.$$

Usually $\ker \iota$ is not trivial. We know from Lemma 2.1 that $\ker \iota$ can be identified with a subgroup of $\mathrm{H}^1(\mathrm{Gal}(L_n|F_n), \{\pm 1\})$. Since $\mathrm{Gal}(L_n|F_n)$ is isomorphic to $\ker \chi_f$ or $\ker \chi_{-f}$, we can deduce that the cardinality of $\ker \iota$ does not exceed 2^t where t is the number of prime factors that divide the integer f.

7. Some examples

In this section we show two examples. The first one is an example of what usually happens. While, the second one is an example where the group A_n grows a little in the $\mathbb{Z}_2$-tower.

Example. Let $f = 949$. Then, $f \equiv 5 \mod 8$ and the class number of $F_0 = \mathbb{Q}(\sqrt{f})$ is 2. Therefore, the cardinality of A_0 is 2. For several $r \equiv 1 \bmod 2^{n+2}f$ we compute the polynomials $f_r^{\eta_n}(X)$ and $f_r^{\beta_n}(X)$ in $\mathbb{Z}_2[X]/(2^{n+1}, X^{2^n} - 1)$. It is convenient to express such polynomials using the new parameter $T = X - 1$. Consider the level $n = 1$.

r	$f_r^{\eta_n}(T)$	$f_r^{\beta_n}(T)/T$
22777	T	3
45553	$3T + 2$	3
60737	$3T$	3
68329	$2T + 2$	2
136657	$3T$	1
151841	0	2

The polynomials

$$\frac{f_{r_i}^{\beta_n}(T)}{T} f_{r_j}^{\eta_n}(T) - \frac{f_{r_j}^{\beta_n}(T)}{T} f_{r_i}^{\eta_n}(T)$$

generate the ideal $(2) \subset \mathbb{Z}_2[T]/(4, (T-1)^2-1)$. As shown in Section 6 we have a surjective homomorphism

$$\frac{\mathbb{Z}_2[T]}{(2, T^2)} \longrightarrow A_1[4]^{\perp}.$$

We deduce that 2 annihilates $A_1[4]$. Hence $A_1[4] = A_1$.

Consider the level $n = 2$. We compute the following polynomials

r	$f_r^{\eta_n}(T)$	$f_r^{\beta_n}(T)/T$
45553	$2T^3+5T+2$	$2T^2+2T+3$
60737	$7T^3+6T^2+T+4$	$5T^2+5T+5$
136657	$4T^3+5T$	$7T^2+5T+3$
151841	T^3+7T^2+2T	$6T^2+6T+6$
182209	$6T^3+4T^2+2T+4$	$4T^2+7T$
273313	$6T^3+2T^2+3T+6$	$5T^2+7T+1$

Note that the polynomials

$$\frac{f_{r_i}^{\beta_n}(T)}{T}f_{r_j}^{\eta_n}(T)-\frac{f_{r_j}^{\beta_n}(T)}{T}f_{r_i}^{\eta_n}(T)$$

generate the ideal $(2,T^2)\subset\mathbb{Z}_2[T]/(8,(T-1)^4-1)$. So, we get a surjective morphism

$$\frac{\mathbb{Z}_2[T]}{(2,T^2)}\longrightarrow A_2[8]^{\perp}.$$

We conclude that $A_2[8]=A_2$ and $A_2\leq 4$. The hypotheses of Lemma 6.1 are satisfied. We can deduce that $A_1\cong A_n$ for any $n\geq 1$.

Example. Let $f=6817$. In this case, $f\equiv 1 \bmod 8$ and the field $F_0=\mathbb{Q}(\sqrt{f})$ has class number 2. For $n=1,2,\dots$ we compute ideals J_n' of $\mathbb{Z}_2[X]$ such that we have a surjective morphism

$$\frac{\mathbb{Z}_2[X]}{J_n'}\longrightarrow\left(\frac{A_n[2^{n+1}]}{A_0[2^{n+1}]}\right)^{\perp}.$$

The ideals J_n' are the ones appearing in (6.2). We collect below those ideals using the parameter $T=X-1$.

n	$J_n'\subset\mathbb{Z}_2[T]$	$[\mathbb{Z}_2[T]:J_n']$
1	$(4,T+2)$	4
2	$(8,4T,2T^2,T^3+2T+4)$	64
3	$(8,4T,2T^2,T^4)$	128
4	$(16,4T,2T^2,T^4)$	256
5	$(32,4T,2T^2,T^4)$	512
6	$(64,4T,2T^2,T^4+32)$	1024
7	$(64,4T,2T^2,T^4+32)$	1024

For $n=7$ the hypotheses of Lemma 6.2 are satisfied. Indeed, the polynomials 2^6 and $\sum_{i=0}^{2^6-1}(T+1)^i$ lies in J_7'. Note that via the isomorphism described in (6.2) the polynomial $\sum_{i=0}^{2^6-1}(T+1)^i$ is mapped to $N_6=\sum_{i=0}^{2^6-1}\gamma^i$. Therefore we get that for any $n\geq 6$ the natural morphisms $A_6\longrightarrow A_n$ are isomorphisms.

8. The main tables

We collect now the results we get. In all the cases we found that the modules A_n stabilize. As a consequence we get that Greenberg's conjecture hold in all cases.

Results for $f \equiv 3 \bmod 4$. Let $3 \leq f < 10000$ be a squarefree integer so that f is congruent to 3 modulo 4. Assume that the class number of $F_0 = \mathbb{Q}(\sqrt{f})$ is even. As presented in Section 6, we compute an ideal $J \subset \mathbb{Z}_2[X]$ such that for any positive n we have a surjective morphism

$$\frac{\mathbb{Z}_2[X]}{J} \longrightarrow A_n^{\perp}.$$

Denote by N the index $[\mathbb{Z}_2[X] : J]$. Let n_0 be the least integer such that the polynomial $\sum_{i=0}^{2^{n_0}-1} X^i$ lies in J. By Lemma 3.6, the natural morphisms $A_{n_0} \longrightarrow A_n$ are isomorphisms for all $n \geq n_0$.

We collect the ideals J in the following table. It is convenient to write the results with the parameter $T = X - 1$.

J	n_0	N	f
$(2, T)$	1	2	15, 35, 39, 55, 87, 91, 95, 111, 115, 143, 155, 159, 183, 203, 215, 235, 247, 259, 295, 299, 303, 319, 327, 335, 355, 371, 395, 403, 407, 415, 427, 447, 471, 515, 519, 535, 543, 551, 559, 583, 591, 611, 635, 655, 667, 671, 687, 695, 703, 707, 755, 763, 767, 807, 815, 831, 835, 851, 871, 879, 895, 899, 923, 951, 955, 995, 1007, 1027, 1043, 1047, 1055, 1079, 1099, 1111, 1115, 1119, 1135, 1147, 1159, 1167, 1191, 1195, 1199, 1211, 1219, 1247, 1255, 1263, 1267, 1315, 1339, 1355, 1363, 1379, 1383, 1391, 1403, 1415, 1527, 1535, 1555, 1591, 1603, 1623, 1639, 1643, 1651, 1655, 1671, 1703, 1711, 1727, 1735, 1739, 1795, 1807, 1835, 1839, 1883, 1891, 1895, 1903, 1915, 1919, 1939, 1943, 1959, 1963, 1983, 1991, 2031, 2051, 2059, 2071, 2095, 2103, 2119, 2127, 2155, 2167, 2171, 2183, 2195, 2199, 2215, 2219, 2271, 2279, 2291, 2315, 2319, 2323, 2327, 2335, 2391, 2395, 2407, 2435, 2443, 2455, 2463, 2479, 2483, 2487, 2491, 2495, 2507, 2515, 2519, 2559, 2587, 2611, 2615, 2623, 2627, 2631, 2723, 2735, 2743, 2779, 2815, 2823, 2831, 2855, 2867, 2899, 2923, 2935, 2947, 2951, 2959, 2983, 2987, 2991, 2995, 3035, 3039, 3047, 3063, 3071, 3095, 3103, 3107, 3127, 3131, 3155, 3183, 3207, 3215, 3223, 3227, 3235, 3263, 3279, 3287, 3295, 3327, 3351, 3379, 3415, 3419, 3427, 3439, 3455, 3487, 3523, 3543, 3551, 3563, 3595, 3599, 3611, 3635, 3639, 3679, 3683, 3687, 3695, 3711, 3715, 3743, 3755, 3763, 3787, 3799, 3811, 3831, 3839, 3899, 3903, 3935, 3959, 3979, 3991, 4031, 4043, 4055, 4087, 4103, 4115, 4119, 4135, 4143, 4163, 4187, 4195, 4279, 4287, 4291, 4295, 4303, 4315, 4331, 4343, 4351, 4359, 4367, 4379, 4399, 4415, 4435, 4479, 4511, 4531, 4535, 4555, 4571, 4595, 4619, 4627, 4631, 4647, 4667, 4687, 4699, 4727, 4735, 4739, 4747, 4771, 4791, 4819, 4835, 4839, 4843, 4847, 4855, 4863, 4867, 4907, 4911, 4915, 4927, 4955, 4963, 4979, 5007, 5063, 5071, 5079, 5095, 5111, 5123, 5127, 5131, 5143, 5155, 5191, 5195, 5199, 5223, 5255, 5263, 5267, 5299, 5315, 5363, 5367, 5411, 5435, 5447, 5455, 5459, 5515, 5539, 5567, 5579, 5583, 5587, 5599, 5603, 5611, 5615, 5631, 5671, 5703, 5707, 5747, 5755, 5759, 5771, 5799, 5803, 5815, 5847, 5855, 5919, 5935, 5951, 5959, 5971, 5991, 6019, 6023, 6031, 6071, 6087, 6107, 6115, 6119, 6127, 6139, 6155, 6159, 6179, 6187, 6207, 6227, 6283, 6295, 6331, 6371, 6383, 6395, 6407, 6415, 6423, 6431, 6455, 6467, 6487, 6515, 6527, 6535, 6539, 6583, 6587, 6595, 6623, 6631, 6635, 6639, 6663, 6711, 6731, 6739, 6743, ...

J	n_0	N	f
			...6751, 6767, 6799, 6807, 6835, 6879, 6927, 6931, 6943, 6979, 6995, 6999, 7003, 7023, 7067, 7071, 7087, 7091, 7099, 7111, 7115, 7135, 7143, 7147, 7167, 7171, 7183, 7195, 7235, 7255, 7271, 7279, 7291, 7295, 7303, 7311, 7319, 7355, 7363, 7367, 7379, 7391, 7415, 7423, 7427, 7431, 7435, 7439, 7447, 7483, 7495, 7543, 7555, 7615, 7627, 7631, 7647, 7651, 7655, 7671, 7711, 7715, 7739, 7747, 7763, 7783, 7787, 7795, 7799, 7807, 7819, 7835, 7855, 7859, 7863, 7891, 7895, 7915, 7979, 7991, 7999, 8003, 8027, 8031, 8035, 8047, 8063, 8079, 8095, 8131, 8135, 8203, 8207, 8223, 8247, 8251, 8267, 8315, 8327, 8335, 8339, 8359, 8367, 8383, 8391, 8399, 8411, 8471, 8479, 8491, 8495, 8503, 8507, 8511, 8567, 8579, 8583, 8587, 8603, 8611, 8615, 8639, 8659, 8727, 8735, 8751, 8759, 8767, 8791, 8795, 8843, 8851, 8871, 8879, 8903, 8915, 8935, 8939, 8947, 8983, 9019, 9031, 9047, 9055, 9083, 9107, 9111, 9115, 9119, 9131, 9155, 9183, 9211, 9235, 9259, 9263, 9287, 9327, 9335, 9347, 9355, 9383, 9395, 9451, 9487, 9535, 9543, 9599, 9607, 9611, 9647, 9655, 9659, 9663, 9667, 9671, 9683, 9687, 9731, 9755, 9759, 9763, 9827, 9847, 9895, 9903, 9935, 9943, 9983, 9995.
$(2, T^2)$	2	2^2	51, 123, 187, 287, 411, 451, 511, 623, 779, 1203, 1347, 1563, 1707, 1819, 1843, 1923, 1927, 2047, 2123, 2191, 2227, 2263, 2283, 2363, 2427, 2571, 2651, 2747, 2759, 2771, 2787, 2859, 2863, 2911, 2931, 3151, 3239, 3431, 3587, 3647, 3667, 3859, 4083, 4207, 4227, 4247, 4499, 4579, 4811, 5027, 5091, 5327, 5723, 5891, 5899, 5999, 6191, 6243, 6259, 6439, 6443, 6459, 6463, 6499, 6559, 6847, 6891, 7123, 7199, 7251, 7339, 7343, 7403, 7519, 7619, 7679, 7771, 7827, 7831, 7899, 8051, 8159, 8187, 8227, 8259, 8331, 8351, 8371, 8403, 8459, 8483, 8531, 8651, 8691, 8899, 9123, 9167, 9179, 9247, 9299, 9307, 9427, 9627, 9703, 9707, 9727, 9799, 9899, 9987.
$(4, 2T, T^2)$	2	2^3	195, 219, 231, 291, 555, 579, 715, 731, 759, 903, 915, 939, 943, 959, 979, 1003, 1015, 1131, 1139, 1227, 1235, 1271, 1295, 1311, 1371, 1407, 1411, 1463, 1495, 1551, 1595, 1631, 1635, 1679, 1767, 1803, 1855, 1967, 2015, 2067, 2247, 2307, 2343, 2355, 2419, 2603, 2607, 2639, 2679, 2715, 2755, 2795, 2967, 3027, 3199, 3219, 3335, 3355, 3367, 3423, 3435, 3443, 3515, 3759, 3815, 3835, 3891, 3939, 4155, 4171, 4183, 4191, 4223, 4267, 4319, 4411, 4427, 4431, 4467, 4495, 4503, 4543, 4615, 4623, 4763, 4823, 4891, 4939, 4983, 5035, 5207, 5215, 5235, 5291, 5307, 5371, 5403, 5487, 5555, 5595, 5627, 5663, 5699, 5719, 5727, 5731, 5735, 5767, 5811, 5871, 5883, 5955, 5963, 5979, 5995, 6063, 6231, 6303, 6315, 6319, 6391, 6411, 6479, 6483, 6695, 6747, 6787, 6843, 6895, 6951, 6955, 7031, 7131, 7223, 7231, 7239, 7287, 7383, 7419, 7531, 7579, 7683, 7903, 7959, 8115, 8139, 8195, 8215, 8255, 8571, 8607, 8695, 8711, 8859, 8891, 8911, 8943, 9147, 9195, 9271, 9303, 9407, 9447, 9455, 9483, 9507, 9515, 9571, 9695, 9699, 9715, 9815, 9915, 9919, 9951.
$(2, T^3)$	2	2^3	119, 339, 391, 679, 771, 1059, 1207, 1687, 2147, 2231, 2839, 3031, 3383, 4803, 4859, 4883, 5287, 5383, 5543, 6503, 6667, 6819, 6887, 7463, 7571, 7971, 8279, 8551, 9223, 9267, 9411, 9527, 9959.
$(4, 2T, T^2 + 2)$	2	2^3	267, 803, 843, 1691, 3291, 3579, 3867, 4299, 4307, 6059, 7179, 9771.
$(4, 2T, T^3)$	2	2^4	483, 615, 651, 663, 1095, 1435, 1455, 1491, 1599, 1615, 1659, 1751, 1771, 2055, 2139, 2255, 2387, 2431, 2555, 2567, 2667, 2703, 2847, 2895, 3115, 3143, 3471, 3495, 3507, 3567, 3619, 3655, 3731, 3783, 3895, 4015, 4439, 4471, 4551, 4683, 4711, 5015, 5151, 5335, 5343, 5451, 5467, 5523, 5691, 5695, 5863, 6015, 6251, 6351, 6495, 6519, 6531, 6603, 6643, 6735, 6839, 6923, 6935, 7055, 7107, 7503, 7527, 7539, 7599, 7707, 7743, 7815, 7843, 7931, 8007, 8099, 8323, 8439, 8535, 8763, 9255, 9331, 9367, 9399, 9443, 9499, 9579, 9615, 9635, 9723, 9863, 9879, 9911.

J	n_0	N	f
$(8, 2T+4, T^2+4)$	2	2^4	399, 1299, 1443, 1743, 2035, 2379, 2751, 2915, 2919, 3399, 3403, 3963, 3999, 4387, 4767, 5135, 5219, 5271, 5947, 6123, 6447, 6567, 6671, 7563, 7719, 7847, 8555, 8671, 9023, 9035, 9143, 9595, 9807, 9955.
$(4, T^2+2)$	2	2^4	699, 3091, 3139, 3827, 5163, 5739, 6611, 7811.
$(4, 2T^2, T^3+2T)$	2	2^5	255, 935, 987, 1479, 1887, 3111, 4123, 4215, 4795, 5019, 5423, 5559, 6919, 8043, 8155, 8455, 8499, 8823, 9051, 9095, 9215, 9231, 9379, 9939.
$(16, 2T+4, T^2+12)$	2	2^5	4251, 7511, 9823.
$(8, 2T+4, T^3)$	2	2^5	1351.
$(8, 4T, 2T^2+4, T^3+2T+4)$	2	2^6	2827, 3747, 6707, 9219.
$(16, 2T+4, T^3+8)$	2	2^6	7063.
$(8, 2T^2+4T+4, T^3+6T+4)$	2	2^7	4695, 6855.
$(8, 2T, T^2)$	3	2^4	323, 435, 455, 723, 795, 1507, 1515, 1763, 2955, 3043, 3055, 3387, 4035, 4071, 4147, 4395, 4755, 5159, 5395, 5495, 5511, 5551, 5619, 6051, 6055, 6235, 6335, 6815, 7015, 7635, 7851, 7887, 7939, 8015, 8239, 8319, 9003, 9039, 9139, 9191, 9415, 9519, 9591, 9979.
$(2, T^4)$	3	2^4	527, 1343, 1799, 2471, 3651, 3707, 4151, 4659, 5311, 6167, 6239, 6387, 6403, 7327, 7471, 7751, 8071, 8143, 8743, 8927.
$(4, 2T, T^4)$	3	2^5	791, 1011, 1547, 2359, 3503, 3603, 4407, 5083, 6215, 6307, 6755, 8407, 8435, 8755.
$(16, 2T+12, T^2+12)$	3	2^5	1239, 2019, 4971, 5795, 5943, 6771, 7059, 8083, 8515, 8635, 8683, 8799.
$(8, 4T, T^2+2T+4)$	3	2^5	1419, 3099, 4587, 4731, 5259, 6963, 7467, 7611, 9339.
$(8, 4T, T^2+2T)$	3	2^5	1947, 3531, 3819, 5379, 5907, 8643, 8987.
$(8, 4T, T^2+6)$	3	2^5	2563, 4443, 5251, 7387.
$(8, 2T, T^3)$	3	2^5	2807, 4487, 6103, 9079.
$(4, 2T^2, T^3)$	3	2^5	3459, 5331, 9363, 9651.
$(2, T^5)$	3	2^5	4039, 5667, 8519, 9071.
$(4, 2T, T^4+2)$	3	2^5	1779, 2643, 8023.
$(8, 4T, 2T^2, T^3)$	3	2^6	1155, 1995, 3135, 3615, 3795, 4199, 4515, 4895, 5115, 5187, 5655, 6135, 6195, 6355, 7035, 7095, 7755, 8103, 8151, 8547, 9015.
$(4, 2T^2, T^4+2T)$	3	2^6	595, 1695, 1955, 2159, 3451, 4403, 6035, 6339, 7259, 9831.
$(4, 2T, T^5)$	3	2^6	2635, 3955, 4371, 4559, 6715, 6851, 7347, 7663, 8655, 8895.
$(4, 2T^2, T^4)$	3	2^6	2091, 3723, 4991, 6987, 7567, 7667.
$(8, 2T+4, T^4)$	3	2^6	799, 4063, 4607.
$(8, 4T, 2T^2+4, T^3+2T)$	3	2^6	1335, 8395.
$(32, 2T+20, T^2+28)$	3	2^6	4807, 7359.
$(16, 4T+8, T^2+2T+8)$	3	2^6	2211.
$(8, T^2+6)$	3	2^6	3147.
$(8, 2T, T^4)$	3	2^6	3791.
$(4, 2T^2, T^4+2)$	3	2^6	6523.
$(8, T^2+4T+2)$	3	2^6	7323.
$(16, 2T+12, T^3+8)$	3	2^6	9991.
$(8, 4T, 2T^2, T^4)$	3	2^7	3255, 4935, 7995, 8855, 9435, 9471.
$(16, 4T+8, 2T^2+8, T^3+8)$	3	2^7	7315, 8815, 8835, 9735, 9779, 9867.
$(8, 2T^2+4, T^3+2T)$	3	2^7	1243, 2163, 4011, 4179.
$(4, 2T^3, T^4+2T^2+2T)$	3	2^7	3395, 6511, 8827.
$(4, 2T^2, T^5+2T)$	3	2^7	3995, 5055.
$(16, 4T+8, 2T^2, T^3+8)$	3	2^7	3883.
$(8, 4T, 2T^2+4, T^4+4)$	3	2^7	4539.
$(4, 2T^3, T^4+2T)$	3	2^7	5295.
$(4, 2T^3, T^4+2T^2)$	3	2^7	6347.
$(16, 4T+8, 2T^2, T^3)$	3	2^7	7779.
$(8, 4T, 2T^3, T^4)$	3	2^8	6279, 7455.
$(8, 2T^2+4, T^4+4T+4)$	3	2^8	8067, 8119.
$(4, T^4+2T^3+2T^2+2)$	3	2^8	2599.
$(8, 4T, 2T^3, T^4+2T^2)$	3	2^8	3315.
$(8, 4T, 2T^2, T^5)$	3	2^8	3927.

J	n_0	N	f
$(4, 2T^2, T^6)$	3	2^8	5763.
$(16, 4T+8, 2T^2+8, T^4)$	3	2^8	7395.
$(4, 2T^3, T^5+2T)$	3	2^8	8995.
$(8, 4T, 2T^3, T^5+2T^2)$	3	2^9	6783, 7735.
$(4, 2T^3, T^6+2T^2)$	3	2^9	9843.
$(4, 2T^4, T^6+2T^2)$	3	2^{10}	4947.
$(8, 4T, 2T^3, T^6)$	3	2^{10}	8211.
$(16, 8T, 4T^2+8, 2T^3+4T+8, T^4+4T+4)$	3	2^{10}	9691.
$(16, 2T+8, T^2)$	4	2^5	2135, 2235, 3311, 3535, 4255, 5359, 8355, 9159.
$(16, 2T, T^2)$	4	2^5	3983, 4047, 4355, 8787, 9795.
$(32, 2T+12, T^2+28)$	4	2^6	6683, 8931.
$(16, 4T, T^2+2T)$	4	2^6	4323.
$(32, 2T+28, T^2+28)$	4	2^6	5183.
$(16, 8T, T^2+6T+4)$	4	2^7	4827, 6267, 9523.
$(16, 4T, 2T^2, T^3)$	4	2^7	6555, 6699, 8715.
$(32, 4T+24, T^2+2T+24)$	4	2^7	2811, 7923.
$(16, 8T, T^2+2T+12)$	4	2^7	1387.
$(16, 8T, T^2+14)$	4	2^7	8907.
$(8, 4T, 2T^3+4, T^4+2T)$	4	2^8	1731.
$(16, 4T, 2T^2, T^4)$	4	2^8	2415.
$(16, 8T, 2T^2+4, T^3+2T)$	4	2^8	3059.
$(32, 2T+12, T^4+16)$	4	2^8	3247.
$(8, 4T, 2T^3+4, T^4+2T+4)$	4	2^8	3855.
$(16, 8T, 2T^2+8, T^3+4T)$	4	2^8	4899.
$(16, T^2+6)$	4	2^8	5339.
$(16, 8T, 2T^2+4T+8, T^3+8)$	4	2^8	6083.
$(16, T^2+12T+14)$	4	2^8	9563.
$(16, 8T, 2T^2+4T, T^3+4T)$	4	2^8	9835.
$(16, 2T^2+12, T^3+6T)$	4	2^9	3171.
$(8, 4T^2, 2T^3+4T+4, T^4+2T^2+2T+4)$	4	2^9	7871.
$(32, 4T+24, 2T^2+24, T^4+16)$	4	2^9	8295.
$(8, 4T, 2T^3+4, T^5+2T^2)$	4	2^9	8687.
$(16, 8T, 2T^2+4T+8, T^4)$	4	2^9	8979.
$(16, 2T^2+12, T^3+14T)$	4	2^9	9087.
$(8, 2T, T^8)$	4	2^{10}	3007.
$(8, 2T^3+4T+4, T^4+6T^2+2T)$	4	2^{10}	5911.
$(4, 2T, T^9)$	4	2^{10}	5983.
$(16, 8T, 4T^2, 2T^3, T^4)$	4	2^{10}	8463.
$(8, 2T^3+4T^2+4T+4, T^5+6T^2+4)$	4	2^{11}	4879.
$(8, 4T, 2T^3+4, T^{10}+2T^2)$	4	2^{14}	7967.
$(32, 2T+24, T^2+16)$	5	2^6	4611, 8347.
$(32, 2T+8, T^2+16)$	5	2^6	6915, 8723.
$(32, 2T+16, T^2)$	5	2^6	7955.
$(64, 2T+60, T^2+60)$	5	2^7	7051.
$(32, 4T+16, 2T^2, T^3)$	5	2^8	3243, 7215.
$(32, 8T, T^2+2T+8)$	5	2^8	9291.
$(32, 16T, T^2+6T+4)$	5	2^9	627.
$(32, 16T, 2T^2+8T+16, T^3+8T)$	5	2^{10}	4715.
$(64, 2T+48, T^2)$	6	2^7	6095.
$(64, 2T+8, T^2+48)$	6	2^7	7163.
$(64, 4T+16, T^2+2T+24)$	6	2^8	2451.
$(64, 4T+48, T^2+2T+40)$	6	2^8	6099.
$(128, 2T+28, T^2+60)$	6	2^8	8299.
$(64, 8T+32, T^2+2T+56)$	6	2^9	2739.
$(128, 4T+120, T^2+2T+120)$	6	2^9	7491.
$(64, 4T+16, 2T^2+32, T^3)$	6	2^9	9503.
$(64, 16T, T^2+2T+56)$	6	2^{10}	8283.
$(64, 32T, T^2+24T+54)$	6	2^{11}	1851.
$(128, 2T+104, T^2+112)$	7	2^8	1067.

J	n_0	N	f
$(128, 2T+72, T^2+112)$	7	2^8	2595.
$(128, 2T+112, T^2+64)$	7	2^8	5835.
$(128, 4T+16, 2T^2+96, T^3+64)$	7	2^{10}	3003.
$(256, 128T, 2T^2+44T+68, T^3+62T+20)$	7	2^{16}	7535.
$(512, 2T+28, T^2+316)$	8	2^{10}	1023.
$(512, 2T+304, T^2+448)$	9	2^{10}	8679.
$(2048, 4T+1520, T^2+2T+744)$	11	2^{13}	3363.

Results for $f \equiv 5 \bmod 8$**.** Let $3 \leq f < 10000$ be a squarefree integer so that f is congruent to 5 modulo 8. Assume that the class number of $F_0 = \mathbb{Q}(\sqrt{f})$ is even. As presented in Section 6, we compute an ideal $J \subset \mathbb{Z}_2[X]$ such that for any positive n we have a surjective morphism

$$\frac{\mathbb{Z}_2[X]}{J} \longrightarrow A_n^{\perp}.$$

Denote by N the index $[J : \mathbb{Z}_2[X]]$. Let n_0 be the least integer such that the polynomial $\sum_{i=0}^{2^{n_0}-1} X^i$ lies in J. By Lemma 3.6, the natural morphisms $A_{n_0} \longrightarrow A_n$ are isomorphisms for all $n \geq n_0$.

We collect the ideals J in the following table. It is convenient to write the results with the parameter $T = X - 1$.

I	n_0	N	f
$(2, T^2)$	2	2^2	85, 365, 485, 493, 629, 949, 965, 1037, 1157, 1165, 1261, 1853, 2117, 2165, 2509, 2581, 2813, 2941, 3077, 3085, 3133, 3293, 3349, 3365, 3589, 3653, 3869, 4573, 4685, 4709, 4885, 5165, 5213, 5389, 5429, 5485, 5597, 5837, 5965, 6485, 6749, 7141, 7165, 7373, 8021, 8485, 8765, 8917, 8989, 9197, 9365, 9565, 9997.
$(4, 2T, T^2)$	2	2^3	165, 205, 221, 285, 429, 445, 741, 885, 901, 1405, 1517, 1717, 1749, 1965, 2013, 2045, 2085, 2109, 2245, 2301, 2365, 2613, 2685, 2845, 3005, 3029, 3165, 3237, 3597, 3685, 3765, 3845, 4069, 4085, 4453, 4565, 4645, 4717, 4773, 4965, 5045, 5069, 5133, 5245, 5629, 5645, 5685, 5757, 5829, 5885, 5917, 5933, 6149, 6213, 6285, 6341, 6357, 6365, 6445, 6549, 6605, 6773, 6837, 6989, 7045, 7157, 7221, 7365, 7405, 7445, 7485, 7733, 7813, 7837, 7869, 7885, 8333, 8357, 8493, 8565, 8749, 8853, 8877, 8965, 9005, 9077, 9141, 9285, 9309, 9381, 9469, 9701, 9885.
$(4, 2T, T^2+2)$	2	2^3	533, 685, 2285, 4141, 5317, 6109, 6437, 7261, 8285, 9965.
$(2, T^3)$	2	2^3	565, 1285, 1765, 3277, 4181, 4589, 5765, 8885, 9509.
$(4, 2T, T^3)$	2	2^4	861, 1533, 1645, 1869, 2093, 2485, 2821, 3157, 4277, 4445, 5285, 5405, 5453, 5621, 5781, 5957, 6141, 6293, 6573, 6789, 6853, 6965, 7805, 8029, 8165, 8277, 8533, 8589, 8733, 9269, 9373, 9453, 9541, 9709, 9717.
$(8, 2T+4, T^2+4)$	2	2^4	645, 957, 1005, 1205, 3205, 3333, 3405, 3741, 4245, 4605, 5141, 5709, 6061, 6501, 6613, 6645, 7005, 7845, 8205, 8621, 9861.
$(4, T^2+2T+2)$	2	2^4	1565, 2173, 4469, 4765, 7421, 9389.
$(4, 2T^2, T^3+2T)$	2	2^5	1085, 2765, 2877, 3565, 3813, 4893, 5901, 5989, 6685, 7189, 7453, 9085.
$(8, 4T, T^2+2T+6)$	2	2^5	1189, 1781, 4285, 5941, 9893.
$(8, 4T, T^2+2T+2)$	2	2^5	3973.
$(16, 2T+4, T^2+12)$	2	2^5	5205.
$(8, 4T, 2T^2+4, T^3+2T+4)$	2	2^6	2829.
$(8, 2T^2+4T+4, T^3+6T+4)$	2	2^7	9485.
$(8, 2T, T^2)$	3	2^4	1045, 1677, 2533, 3245, 5181, 5973, 6757, 6981, 7557, 7645, 7957, 8149, 8653, 8949, 9213, 9789, 9845.
$(2, T^4)$	3	2^4	2885, 2965, 6085, 7501, 7709.

I	n_0	N	f
$(4, 2T, T^4)$	3	2^5	2037, 2261, 4381, 4405, 5061, 5117, 5253, 6005, 6693, 7021, 7429, 7469, 7701, 7973, 8421, 9093, 9429, 9877.
$(8, 4T, T^2 + 4)$	3	2^5	2501, 4045, 5365, 7085, 7093, 8077, 9685, 9805.
$(8, 4T, T^2)$	3	2^5	1885, 3805, 3965, 7685, 8845.
$(16, 2T + 12, T^2 + 12)$	3	2^5	2445, 2717, 3021, 8805, 9581.
$(4, 2T^2, T^3)$	3	2^5	3341, 6245, 6893.
$(8, 4T, 2T^2, T^3)$	3	2^6	1365, 3045, 3885, 4389, 4485, 5005, 6405, 7917, 8645, 9165, 9597, 9933.
$(4, 2T^2, T^4 + 2T)$	3	2^6	357, 1173, 1309, 3621, 4301, 8517.
$(4, 2T, T^5)$	3	2^6	1581, 2373, 4029, 5797, 7797.
$(4, 2T^2, T^4)$	3	2^6	3485, 6205, 9061.
$(8, 4T, 2T^2 + 4, T^3 + 2T)$	3	2^6	5845, 9821.
$(4, 2T^2, T^4 + 2)$	3	2^6	7765, 9773.
$(16, 4T + 8, T^2 + 12)$	3	2^6	2405.
$(32, 2T + 20, T^2 + 28)$	3	2^6	3893.
$(4, 2T^2, T^5 + 2T)$	3	2^7	6477, 7285, 8789, 9741.
$(8, 2T^2 + 4, T^3 + 6T)$	3	2^7	805, 1469, 3605.
$(8, 4T, 2T^2, T^4)$	3	2^7	2805, 4053.
$(8, 2T^2 + 4T + 4, T^3 + 2T + 4)$	3	2^7	6461, 8365.
$(16, 4T + 8, 2T^2 + 8, T^3 + 8)$	3	2^7	5037.
$(16, 4T + 8, 2T^2, T^3)$	3	2^7	8005.
$(4, 2T^2, T^6)$	3	2^8	8245, 9605.
$(4, T^4 + 2T^3 + 2)$	3	2^8	1685.
$(8, 4T, 2T^3, T^4 + 2T^2)$	3	2^8	4845.
$(4, 2T^3, T^5 + 2T^2 + 2T)$	3	2^8	5397.
$(8, 4T, 2T^3, T^4)$	3	2^8	6765.
$(16, 4T + 8, 2T^2 + 8, T^4)$	3	2^8	7565.
$(8, 4T, 2T^2, T^5)$	3	2^8	8701.
$(16, 4T + 8, 2T^2 + 8, T^5)$	3	2^9	7077.
$(4, 2T^4, T^5 + 2T)$	3	2^9	7413.
$(16, 2T + 8, T^2)$	4	2^5	2005, 4981, 5109, 5605, 7437, 8605.
$(32, 2T + 12, T^2 + 28)$	4	2^6	2701.
$(32, 2T + 28, T^2 + 28)$	4	2^6	9645.
$(64, 2T + 52, T^2 + 28)$	4	2^7	1653, 4917, 8445.
$(16, 8T, T^2 + 4T + 8)$	4	2^7	2605.
$(16, 8T, T^2 + 4T + 12)$	4	2^7	3445.
$(16, 8T, 2T^2, T^3)$	4	2^8	4669.
$(32, 4T + 24, 2T^2 + 24, T^3 + 24)$	4	2^8	5565.
$(32, 8T + 16, T^2 + 4)$	4	2^8	7397.
$(16, 2T^2 + 12T + 12, T^3 + 10T + 12)$	4	2^9	9205.
$(16, 8T, 2T^3 + 4T^2 + 8, T^4 + 4T + 8)$	4	2^{11}	7293.
$(8, 2T^4 + 4T + 4, T^5 + 6T^2 + 6T)$	4	2^{13}	2397.
$(16, 4T, 2T^3, T^9 + 2T^2)$	4	2^{14}	9021.
$(32, 2T + 8, T^2 + 16)$	5	2^6	1221, 3477.
$(32, 2T + 24, T^2 + 16)$	5	2^6	7205, 9797.
$(32, 2T + 16, T^2)$	5	2^6	8229.
$(32, 8T, T^2 + 8)$	5	2^8	6565.
$(128, 2T + 20, T^2 + 28)$	5	2^8	8437.
$(64, 4T + 56, 2T^2 + 56, T^3 + 56)$	5	2^9	6045.
$(16, 8T, 2T^4 + 4T^3 + 4T^2 + 4T + 12, T^5 + 6T^3 + 6T^2 + 2T + 4)$	5	2^{14}	9445.
$(64, 2T + 56, T^2 + 48)$	6	2^7	2669.
$(64, 2T + 8, T^2 + 48)$	6	2^7	4173.
$(128, 2T + 92, T^2 + 60)$	6	2^8	1245.
$(128, 2T + 76, T^2 + 92)$	6	2^8	9669.
$(128, 2T + 120, T^2 + 112)$	7	2^8	5421.
$(256, 2T + 72, T^2 + 240)$	8	2^9	6805.
$(1024, 2T + 316, T^2 + 636)$	9	2^{11}	1605.
$(2048, 2T + 1036, T^2 + 2012)$	10	2^{12}	8045.

Results for $f \equiv 1 \bmod 8$. Let $3 \leq f < 10000$ be a squarefree integer so that f is congruent to 1 modulo 8. As presented in Section 6, we compute an ideal $J \subset \mathbb{Z}_2[X]$ such that for any positive n we have a surjective morphism

$$\frac{\mathbb{Z}_2[X]}{J} \longrightarrow \left(\frac{A_n}{A_0}\right)^{\perp}.$$

Denote by N the index $[\mathbb{Z}_2[X] : J]$. Let n_0 be the least integer such that the polynomial $\sum_{i=0}^{2^{n_0}-1} X^i$ lies in J. By Proposition 4.5, the natural morphisms $A_{n_0} \longrightarrow A_n$ are isomorphisms for all $n \geq n_0$.

We collect the ideals J in the following table. It is convenient to write the results with the parameter $T = X - 1$. We omit the integers f such that the ideal $J = \mathbb{Z}_2[T]$.

I	n_0	N	f
$(2, T)$	1	2	105, 145, 185, 217, 273, 329, 345, 385, 409, 481, 521, 553, 569, 665, 705, 713, 785, 809, 857, 865, 897, 953, 1001, 1129, 1145, 1209, 1265, 1281, 1337, 1385, 1417, 1465, 1505, 1545, 1657, 1729, 1745, 1769, 1817, 1833, 1865, 1905, 1937, 2065, 2121, 2137, 2153, 2185, 2249, 2289, 2345, 2377, 2505, 2521, 2553, 2561, 2585, 2617, 2633, 2681, 2697, 2705, 2729, 2769, 2785, 2905, 3081, 3161, 3209, 3241, 3297, 3337, 3345, 3353, 3441, 3601, 3633, 3657, 3665, 3745, 3769, 3785, 3801, 3809, 3905, 3913, 3945, 4081, 4089, 4209, 4345, 4385, 4393, 4433, 4465, 4553, 4585, 4697, 4809, 4865, 4929, 4945, 4953, 5033, 5129, 5177, 5305, 5353, 5369, 5497, 5505, 5545, 5585, 5609, 5649, 5665, 5673, 5705, 5745, 5777, 5801, 5817, 5889, 5897, 5993, 6041, 6097, 6153, 6161, 6169, 6217, 6265, 6329, 6385, 6513, 6649, 6721, 6785, 6873, 6937, 6945, 6985, 7033, 7097, 7177, 7193, 7241, 7273, 7305, 7329, 7385, 7449, 7505, 7521, 7545, 7553, 7657, 7705, 7761, 7777, 7833, 7849, 7945, 7969, 8009, 8057, 8065, 8113, 8137, 8185, 8305, 8321, 8329, 8337, 8377, 8441, 8465, 8497, 8617, 8665, 8697, 8769, 8785, 8841, 8953, 9017, 9089, 9105, 9145, 9161, 9169, 9185, 9193, 9289, 9321, 9353, 9361, 9433, 9545, 9577, 9593, 9665, 9681, 9705, 9737, 9785, 9817, 9865, 9889, 9905, 9913, 9985.
$(4, T+2)$	1	2^2	113, 497, 1601, 1777, 1841, 2369, 3073, 3121, 3137, 3473, 4177, 4193, 4721, 4817, 5761, 6353, 6481, 7153, 7313, 7489, 8209, 9569, 9649.
$(8, T+2)$	1	2^3	3089, 3313, 3521, 4513, 9793.
$(4, T)$	2	2^2	65, 137, 265, 777, 985, 1065, 1073, 1313, 1321, 1673, 1705, 1897, 2001, 2233, 2257, 2265, 2297, 2713, 2777, 2921, 2929, 2945, 2985, 3001, 3193, 3265, 3585, 3857, 3865, 3985, 4033, 4065, 4121, 4137, 4649, 4665, 4889, 5065, 5161, 5217, 5257, 5273, 5385, 5417, 5449, 5465, 5473, 5681, 6065, 6145, 6177, 6233, 6377, 6465, 6473, 6585, 6641, 6665, 6745, 6865, 6969, 7001, 7049, 7185, 7337, 7369, 7417, 7433, 7745, 7881, 7897, 8153, 8345, 8593, 8601, 8681, 8961, 8985, 9393, 9689, 9833, 9961.
$(2, T^2)$	2	2^2	697, 969, 2193, 3009, 3417, 3553, 3649, 3977, 4233, 4521, 5289, 5321, 5529, 6369, 7257, 7809, 7913, 7953, 8041, 8585, 8857, 9129, 9553.
$(2, T^3)$	2	2^3	337, 1457, 1553, 2129, 2449, 3729, 5233, 5969, 7121, 7409, 8249, 8401, 8481, 8977.
$(4, 2T, T^2)$	2	2^3	1241, 1513, 2993, 4161, 4505, 4785, 5785, 6105, 6953, 8177, 8265, 9673.
$(4, 2T, T^2+2)$	2	2^3	593, 881, 2689, 4049, 5945, 6689, 9137, 9417, 9697.
$(8, T+6)$	2	2^3	2593, 4417, 5297, 6049, 8561.
$(4, 2T, T^3)$	2	2^4	6601, 7345, 7665, 8905, 9177, 9345.
$(4, T^2+2)$	2	2^4	577, 2409, 2937.
$(4, T^2+2T+2)$	2	2^4	4001, 4657.

I	n_0	N	f
$(8, 2T+4, T^2)$	2	2^4	8569.
$(8, 2T+4, T^2+4)$	2	2^4	9881.
$(8, 2T, T^3+4)$	2	2^5	9377.
$(8, 4T, 2T^2+4, T^3+6T+4)$	2	2^6	2665.
$(8, 2T^2+4T+4, T^3+6T+4)$	2	2^7	5313.
$(8, T)$	3	2^3	41, 313, 457, 761, 1081, 1561, 1985, 1993, 2305, 2545, 2569, 2849, 2953, 2977, 3017, 3129, 3385, 3929, 4017, 4249, 4681, 4729, 4793, 4841, 4921, 5641, 5713, 6073, 6185, 6401, 6617, 6657, 7465, 7473, 7561, 7721, 7801, 8169, 8393, 8521, 8545, 8729, 8809, 9049, 9257, 9305, 9385, 9465, 9529, 9929.
$(8, T+4)$	3	2^3	257, 1153, 2513, 4289, 5201, 6209, 6449, 6529, 8081.
$(8, 2T, T^2)$	3	2^4	1105, 3201, 6409.
$(4, T^2)$	3	2^4	561, 6681.
$(4, T^2+2T)$	3	2^4	1353, 8313.
$(2, T^4)$	3	2^4	1921, 5729.
$(16, T+14)$	3	2^4	6433, 7217.
$(16, T+6)$	3	2^4	5393.
$(4, 2T, T^3+2)$	3	2^4	8161.
$(8, 2T, T^2+4)$	3	2^4	8273.
$(4, 2T, T^4)$	3	2^5	1785, 5865.
$(8, 4T, T^2+6)$	3	2^5	4273.
$(4, 2T^2, T^3)$	3	2^5	5617.
$(8, 4T, T^2+2T)$	3	2^5	8633.
$(16, 2T+12, T^2+12)$	3	2^5	8745.
$(4, 2T, T^5)$	3	2^6	3689, 7905.
$(8, 2T+4, T^4)$	3	2^6	3281.
$(8, 2T, T^4)$	3	2^6	6545.
$(16, 4T+8, T^2+8)$	3	2^6	7089.
$(16, 4T+8, T^2+2T+4)$	3	2^6	7689.
$(4, 2T^3, T^4)$	3	2^7	1649, 2737, 8449.
$(2, T^7)$	3	2^7	3937, 5921.
$(4, 2T^2, T^5+2T)$	3	2^7	4369.
$(8, 4T, 2T^2, T^4+2T)$	3	2^7	4641.
$(8, 4T, 2T^2, T^4+2T+4)$	3	2^7	7361.
$(4, 2T^3, T^4+2T^2)$	3	2^7	7633.
$(8, 2T, T^5)$	3	2^7	9401.
$(8, 4T, 2T^3, T^5+2T^2+2T)$	3	2^9	5593.
$(16, T)$	4	2^4	465, 609, 889, 1585, 2865, 3065, 3233, 3593, 4073, 4537, 4969, 4985, 5849, 7985, 8089, 8945, 9217, 9641, 9953.
$(16, T+8)$	4	2^4	1169, 1393, 1633, 4529, 9121.
$(16, T+12)$	4	2^4	4577, 6881, 7393.
$(16, T+4)$	4	2^4	5089.
$(16, 2T+8, T^2)$	4	2^5	3145, 5185.
$(16, 2T, T^2)$	4	2^5	3961, 4777.
$(16, 2T, T^2+8)$	4	2^5	2113.
$(32, T+14)$	4	2^5	7441.
$(8, T^2+6T+4)$	4	2^6	5073, 9473.
$(16, 2T+8, T^3+8)$	4	2^6	3761.
$(16, 2T, T^3)$	4	2^6	4305.
$(32, 2T+28, T^2+28)$	4	2^6	4745.
$(8, T^2+4T)$	4	2^6	5457.
$(32, 8T+16, T^2+24)$	4	2^8	1217.
$(16, 4T+8, T^3+2T^2+2T)$	4	2^8	6441.
$(32, 8T+16, T^2+4T+24)$	4	2^8	9281.
$(16, 8T, 4T^2, T^3+2T^2+2T)$	4	2^9	4633.
$(16, 2T^2+4, T^3+2T)$	4	2^9	7161.
$(4, 2T^3, T^7+2T^2+2T+2)$	4	2^{10}	6913.
$(8, 4T, 2T^3, T^6+2T)$	4	2^{10}	9809.
$(8, 4T^2, T^5+2T^3+6T+6)$	4	2^{12}	4801.

I	n_0	N	f
$(32, T)$	5	2^5	1113, 3289, 3433, 3545, 5657, 7321, 7673, 8297, 9497.
$(32, T+8)$	5	2^5	161, 2273.
$(32, T+16)$	5	2^5	2657, 2833.
$(32, T+24)$	5	2^5	353.
$(32, T+20)$	5	2^5	1249.
$(32, T+4)$	5	2^5	8257.
$(32, 2T+16, T^2)$	5	2^6	3705.
$(32, 2T, T^2+16)$	5	2^6	9273.
$(32, 4T, T^2+2T)$	5	2^7	7769.
$(64, 2T+44, T^2+28)$	5	2^7	9265.
$(32, 4T, T^3+2T^2+2T+24)$	5	2^9	7841.
$(64, 8T+48, T^2+6T)$	5	2^9	8385.
$(16, 8T, T^3+4T^2+4T+2)$	5	2^{10}	1889.
$(16, 4T^2, T^3+12T+12)$	5	2^{10}	9601.
$(64, T+32)$	6	2^6	721, 1057, 5569, 8369.
$(64, T)$	6	2^6	2201, 4441, 7265, 7609.
$(64, T+24)$	6	2^6	3409.
$(128, T+70)$	6	2^7	3361.
$(64, 2T+16, T^2)$	6	2^7	6497.
$(64, 2T, T^2+32)$	6	2^7	7793.
$(128, T+30)$	6	2^7	9233.
$(256, T+202)$	6	2^8	2177.
$(64, 4T+32, T^2+48)$	6	2^8	8609.
$(64, 2T+16, T^3+32)$	6	2^8	9521.
$(64, 4T, 2T^2, T^4+32)$	6	2^{10}	6817.
$(64, 16T, 2T^2+48, T^3)$	6	2^{11}	8897.
$(64, 8T, 4T^2, T^5+2T^3+2T)$	6	2^{15}	6001.
$(128, T+16)$	7	2^7	3841.
$(128, T)$	7	2^7	4265.
$(128, T+64)$	7	2^7	5873.
$(128, 2T+96, T^2)$	7	2^8	2145, 2329.
$(128, 2T+32, T^2)$	7	2^8	2465, 6305.
$(128, 2T, T^2)$	7	2^8	7081.
$(128, 2T+32, T^2+64)$	7	2^8	8241.
$(256, T+64)$	8	2^8	3217.
$(256, T+160)$	8	2^8	6769.
$(256, 16T, 8T^3, T^4+6T^3+14T^2+6T+224)$	8	2^{19}	4097.
$(512, T)$	9	2^9	1185.
$(512, T+256)$	9	2^9	4993.
$(512, 2T+176, T^2+192)$	9	2^{10}	2337.
$(512, 4T, 2T^2, T^3)$	9	2^{12}	7585.
$(2048, T)$	11	2^{11}	3881.
$(2048, 2T, T^2+1024)$	11	2^{12}	1201.
$(2048, 8T+256, T^2+4T+384)$	11	2^{14}	4481.
$(2048, 8T+256, 2T^2+1536, T^3+4T+128)$	11	2^{15}	3713.

Appendix A. Index formula

Let $f \geq 3$ be a squarefree integer. Let F_n be the n-th level field in the cyclotomic $\mathbb{Z}_2$-extension of the field $F_0 = \mathbb{Q}(\sqrt{f})$. Sinnott's index formula [Sin80, Theorem 4.1] states that

$$[O_{F_n}^{\times} : \mathrm{Cyc}_{F_n}] = \begin{cases} 2^{2^{n+1}-1} h_{F_n} c_{F_n}, & \text{if } f \equiv 1 \bmod 4 \text{ and } f \text{ is prime,} \\ 2^{2^{n+1}-2} h_{F_n} c_{F_n}, & \text{otherwise.} \end{cases}$$

The constant c_{F_n} is a positive rational number. In this appendix we explicit the definition of c_{F_n} and we prove that $c_{F_n}=1$.

We introduce the notation used in [Sin80]. Let $\Gamma_n=\mathrm{Gal}(F_n|\,\mathbb{Q})$.

- For any prime number p, let $T_p<\Gamma_n$ be the inertia subgroup at p. Let r be a positive squarefree integer. Denote by T_r the subgroup of Γ_n generated by T_p for any prime p that divides r.
- For any subgroup $H<\Gamma_n$ we put
$$s(H)=\sum_{h\in H}h.$$
- Let p be a prime number. We define $(p,F_n)^*\in\mathbb{Q}[\Gamma_n]$ as
$$(p,F_n)^*=\frac{s(T_p)}{\#T_p}\lambda_p^{-1}$$
where λ_p is a Frobenius morphism above p.
- Let $R=\mathbb{Z}[\Gamma_n]$. Let m be the product of distinct primes that divide the conductor of F_n. Define $U\subset\mathbb{Q}[\Gamma_n]$ as the R-module generated by
$$s(T_r)\prod_{p|\frac{m}{r}}(1-(p,F_n)^*)$$
where r runs over the positive divisor of m and p denotes a prime number. Then [Sin80, Proposition 2.3] states that U is a lattice in $\mathbb{Q}(\Gamma_n)$.

Let V be a finite dimensional $\mathbb{Q}$-vector space. Let $L,M\subset V$ be two lattices. Choose a $\mathbb{Q}$-linear automorphism ϕ of V such that $\phi(L)=M$. Then, we define
$$(L:M)=|\det(\phi)|.$$
The index $(L:M)$ does not depend on the choice of ϕ. By [Sin80, Lemmas 1.1 and 1.2] the index satisfies the following properties. Let $L,M,N\subset V$ be lattices then

$$(L:N)=(L:M)(M:N). \tag{$A1$}$$

Moreover, let $L,M\subset V$ be both lattices and R-modules. For any $\alpha\in\mathbb{Q}(\Gamma_n)$ let L_α be the kernel of the map $L\longrightarrow\alpha L$ induced by the multiplication by α. Define M_α similarly. Then

$$(L:M)=(L_\alpha:M_\alpha)(\alpha L:\alpha M). \tag{$A2$}$$

Finally, according to [Sin80, Theorem 4.1] we have $c_{F_n}=(R:U)$.

Proposition A.1. *Let $f\geq 3$ be an odd squarefree integer. Let F_n be the n-th level in the cyclotomic $\mathbb{Z}_2$-extension of $F_0=\mathbb{Q}(\sqrt{f})$. Then $c_{F_n}=1$.*

Proof. First of all, we assume $n=0$. Since the group $\mathrm{Gal}(F_0|\,\mathbb{Q})$ is cyclic, the proposition follows from [Sin80, Theorem 5.4].

Fix a level $n\geq 1$. Define $U_f\subset\mathbb{Q}(\Gamma_n)$ be the R-module generated by
$$s(T_r)\prod_{p|\frac{f}{r}}(1-(p,F_n)^*).$$

We compute separately the indices $(R : U_f)$ and $(U_f : U)$.

Recall that if $p|f$ then $T_p = \Delta$, where $\Delta = \mathrm{Gal}(F_n|\,\mathbb{Q}_n)$. We have

$$s(\Delta)(1-(p,F_n)^*) = s(\Delta)(1-\frac{s(\Delta)}{2}\lambda_p^{-1}) = s(\Delta)(1-\lambda_p^{-1}) \in R.$$

Therefore, we deduce that

$$U_f = s(\Delta)R + \prod_{p|f}(1-(p,F_n)^*)R.$$

Denote by e_Δ the element $s(\Delta)/2$. For any p that divides f we have

$$(1-e_\Delta)(1-(p,F_n)^*) = (1-e_\Delta).$$

Moreover, $(1-e_\Delta)s(\Delta) = 0$. Let $x \in U_f$, there exist $u, v \in R$ such that the element x is equal to $s(\Delta)u + \prod_{p|f}(1-(p,F_n)^*)v$. Then $(1-e_\Delta)x = (1-e_\Delta)v$ and hence

$$(1-e_\Delta)U_f = (1-e_\Delta)R.$$

Note that for any R-module $M \subset \mathbb{Q}(\Gamma_n)$ the kernel of the map $M \longrightarrow (1-e_\Delta)M$ induced by the multiplication by $1-e_\Delta$ is exactly M^Δ.

We show that $U_f^\Delta = R^\Delta$. Indeed, it is clear that $R^\Delta = s(\Delta)R$. Then, take $x \in U_f^\Delta$. There exist $u, v \in R$ such that $x = s(\Delta)u + \prod_{p|f}(1-(p,F_n)^*)v$ and $(1-e_\Delta)v = 0$. Therefore, the element v is divisible by $s(\Delta)$. It follows that

$$U_f^\Delta = s(\Delta)R + \prod_{p|f}(1-(p,F_n)^*)s(\Delta)R = s(\Delta)R + \prod_{p|f}(1-\lambda_p^{-1})s(\Delta)R = s(\Delta)R.$$

Finally, from the Equation (A2) we deduce

$$(R : U_f) = (R^\Delta : U_f^\Delta)((1-e_\Delta)R : (1-e_\Delta)U_f) = 1.$$

We compute now the index $(U_f : U)$. Let $U_f(T_2)$ be the R-submodule of U generated by

$$s(T_{2r})\prod_{p|\frac{2f}{2r}}(1-(p,F_n)^*)$$

where r runs over the positive divisor of f. Then, we get

$$U = U_f(T_2) + (1-(2,F_n)^*)U_f.$$

By [Sin80, Lemma 5.1] the index $(U_f : U)$ is equal to the cardinality of the quotient

$$B = \frac{U_f^{T_2}}{U_f(T_2) + (1-\lambda_2^{-1})U_f^{T_2}}.$$

Notice that the inertia group T_2 is Γ_n if $f \equiv 1 \bmod 4$ or $T_2 = \mathrm{Gal}(F_n|F_0)$ if $f \equiv 3 \bmod 4$. Then, it is easy to show that

$$U_f(T_2) = s(\Gamma_n)R + s(T_2)\prod_{p|f}(1-(p,F_n)^*)R.$$

Recall that $U_f^{\Delta} = R^{\Delta}$ and $(1-e_{\Delta})U_f = (1-e_{\Delta})R$ as shown previously. Consider the following commutative diagram whose rows are exact

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^{\Delta} & \longrightarrow & R & \xrightarrow{1-e_{\Delta}} & (1-e_{\Delta})R & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \lambda'} & & \downarrow{\scriptstyle \lambda} & & \| & & \\ 0 & \longrightarrow & R^{\Delta} & \longrightarrow & U_f & \xrightarrow{1-e_{\Delta}} & (1-e_{\Delta})R & \longrightarrow & 0 \end{array}$$

The application λ' is the multiplication by $\prod_{p|f}(1-\lambda_p^{-1})$ while the application λ is the multiplication by $\prod_{p|f}(1-(p,F_n)^*)$. The commutativity of the diagram follows from the relations

$$\begin{aligned} s(\Delta)(1-(p,F_n)^*) &= s(\Delta)(1-\lambda_p^{-1}) \\ (1-e_{\Delta})(1-(p,F_n)^*) &= 1-e_{\Delta} \end{aligned}$$

for any p prime divisor of f. We take T_2-invariants in order to get the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^{\Gamma_n} & \longrightarrow & R^{T_2} & \xrightarrow{1-e_{\Delta}} & ((1-e_{\Delta})R)^{T_2} & \longrightarrow & 0\,. \\ & & \downarrow{\scriptstyle \lambda'} & & \downarrow{\scriptstyle \lambda} & & \| & & \\ 0 & \longrightarrow & R^{\Gamma_n} & \longrightarrow & U_f^{T_2} & \xrightarrow{1-e_{\Delta}} & ((1-e_{\Delta})R)^{T_2} & \longrightarrow & 0 \end{array}$$

By [Sin80, Lemma 5.2] we have that $\mathrm{H}^1(T_2, R^{\Delta}) = 0$. It follows the exactness of the diagram's rows. We deduce from the diagram that

$$U_f^{T_2} = R^{\Gamma_n} + \lambda\left(R^{T_2}\right) = s(\Gamma_n)R + s(T_2)\prod_{p|f}(1-(p,F_n)^*)R.$$

In other words, we get that $U_f^{T_2} = U_f(T_2)$. Then, the cardinality of B and the index $(U_f : U)$ are equals to 1.

By Equation (A1), we conclude that

$$c_{F_n} = (R:U) = (R:U_f)(U_f:U) = 1.$$

□

References

[CF93] Cassels J.W.S. and Fröhlich A.: *Algebraic number theory*, Academic Press, San Diego (1993).

[Cor97] Cornacchia P.: *Anderson's module for cyclotomic fields of prime conductor*, J. Number Theory **67** (1997), 252-276.

[FW79] Ferrero B. and Washington L.C.: *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

[Fuk96] Fukuda T.: *Cyclotomic units and Greenberg's conjecture for real quadratic fields*, Math. Comp. **65** (1996), 1339-1348.

[Gre76] Greenberg, R.: *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263-284.

[KS95] Kraft J. and Schoof R.: *Computing Iwasawa modules of real quadratic fields*, Compos. Math. **95** (1995), 135-155.

[Iwa59] Iwasawa K.: *On* Γ*-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[Sch02] Schoof R.: *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. **73** (2003), 913-937.

[Sin80] Sinnott W.: *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181-234.

[Tay96] Taya H.: *Computation of* $\mathbb{Z}_3$*-invariants of real quadratic fields*, Math. Comp. **65** (1996), 779-784.

[Was97] Washington L.C.: *Introduction to cyclotomic fields*, Second Edition, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York, (1997).

Dipartimento di matematica, università di Roma "La Sapienza", piazzale Aldo Moro 5, 00185 Roma Italy

Email address: pagani@mat.uniroma1.it

STABILIZATION OF THE PRIME PARTS OF THE CLASS GROUP IN INFINITE CYCLOTOMIC EXTENSIONS

LORENZO PAGANI

ABSTRACT. Let p and ℓ be distinct primes. Let $\mathcal{A}_{K_n}$ be the ℓ-part of the ideal class group of th n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of an abelian number field K. Let $n_0 \geq 0$ be the least integer such that $\mathcal{A}_{K_n} \cong \mathcal{A}_{K_{n_0}}$ for any $n \geq n_0$. First, we study the relative class number of the field K_n exploiting the relation between Bernoulli numbers and class number. Then, by the reflection theorem we find an explicit upper bound for n_0.

INTRODUCTION

Let K be an abelian number field. Let p be a prime number. A $\mathbb{Z}_p$-extension of K is a Galois extension $K \subset \mathcal{K}$ whose Galois group is topologically isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$. Since the only closed subgroups of $\mathbb{Z}_p$ are $p^n\,\mathbb{Z}_p$ for $n \geq 0$, we have a tower of fields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset \mathcal{K}.$$

such that the group $\mathrm{Gal}(K_n|K)$ is cyclic of order p^n.

We will focus on the cyclotomic $\mathbb{Z}_p$-extension, namely the unique $\mathbb{Z}_p$-extension

$$\mathcal{K} \subset \bigcup_{n\geq 1} K(\zeta_{p^n})$$

where ζ_{p^n} is a primitive root of unity of order p^n for any n.

Fix a prime $\ell \neq p$. Let $\mathcal{A}_{K_n}$ be the ℓ-part of the ideal class group of the field K_n. Then in [Sin87] and [Was97, Section 16.3] it has been proved in different ways that there exists a level n_0 such that for any $n \geq n_0$ the norm maps $\mathcal{A}_{K_n} \longrightarrow \mathcal{A}_{K_{n_0}}$ are isomorphisms.

Following the ideas contained in [Was97, Section 16.3] we find an upper bound for the integer n_0. Examples of a similar application can be found in [FS95] where the authors focus on cyclotomic $\mathbb{Z}_3$-extensions of imaginary fields and describe an algorithm to compute the relative class numbers in the tower. Another example is [FK11] where the main interest is the cyclotomic $\mathbb{Z}_2$-extension over the rationals.

In this paper we do not make assumptions on the field K, or on the prime p. We compute an explicit bound for the integer n_0. The bound we get depends on both the primes p and ℓ and on the conductor of the field K.

Theorem. *Let p be a prime integer and set $q = 4$ if $p = 2$ or $q = p$ otherwise. Let ℓ be an odd prime different from p. Let K be an abelian field with conductor not divisible*

2010 *Mathematics Subject Classification.* Primary 11R18, 11R29.

by qp. Denote by $\mathfrak{f}$ be the conductor of $K(\zeta_\ell)$ and by t be the exponent of $\mathrm{Gal}(K(\zeta_\ell)|\,\mathbb{Q})$. *Fix an integer $c \geq 1$ such that for any $n \geq c$ the primes above ℓ in the field extension $\mathbb{Q}(\zeta_t, \zeta_{p^c}) \subset \mathbb{Q}(\zeta_t, \zeta_{p^n})$ are inert. Then*

$$n_0 \leq (\varphi(p-1)+1)c + 1 + \varphi(p-1)\log_p\left(\frac{\varphi(q)}{2}f\right).$$

Here φ is Euler totient function and f is the largest divisor of $\mathfrak{f}$ which is coprime to p.

The used approach involve Bernoulli numbers in order to deal with the relative class number of K_n. Recall that the relative class number is the quotient between the class number of K_n and the one of K_n^+. Then, we apply the reflection theorem to study the class number of K_n^+. A different strategy for a similar problem can be found in [Hor02] and [Hor05] where cyclotomic units are used instead of Bernoulli numbers.

We organize the paper as follows. Sections 1 and 4 cover some preliminaries about Bernoulli numbers and reflection theorem. In section 2 we present the main results contained in [Was97, Section 16.3]. We prove theorems about the stabilization of the relative class number in cyclotomic $\mathbb{Z}_p$-extensions in section 3 and about the full class number in section 5.

1. Analytic class number formula

Let ℓ be a prime number. Let $\mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$ be the ring of ℓ-adic integers and its fraction field respectively. Let $\overline{\mathbb{Q}}_\ell$ be a fixed algebraic closure of $\mathbb{Q}_\ell$ and let $\overline{\mathbb{Z}}_\ell$ be the integral closure of $\mathbb{Z}_\ell$ inside $\overline{\mathbb{Q}}_\ell$. Furthermore, we fix $\overline{\mathbb{Q}}$ an algebraic closure of the rationals and we fix an embedding $\overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}}_\ell$. We denote by ζ_n a primitive n-th root of unity in $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_\ell$.

Let K be an abelian number field with conductor $\mathfrak{f}$. For any $a \in (\mathbb{Z}/\mathfrak{f}\mathbb{Z})^\times$ let ϕ_a be the automorphism of $\mathbb{Q}(\zeta_\mathfrak{f})$ defined by $\phi_a(\zeta_\mathfrak{f}) = \zeta_\mathfrak{f}^a$ where $\zeta_\mathfrak{f}$ is a primitive root of unity of order $\mathfrak{f}$. For any group character $\chi : \mathrm{Gal}(K|\,\mathbb{Q}) \longrightarrow \overline{\mathbb{Q}}^\times$ we define the Dirichlet character

$$\chi' : (\mathbb{Z}/\mathfrak{f}\mathbb{Z})^\times \longrightarrow \overline{\mathbb{Q}}^\times$$

such that $\chi'(a) = \chi(\phi_{a|K})$ where $\phi_{a|K}$ is the restriction of the automorphism ϕ_a to K. We denote by $X(K)$ the group of such Dirichlet characters. Let $X(K)^-$ be the set of odd characters contained in $X(K)$.

For any Dirichlet character χ different from the trivial one we recall the definition of the first generalized Bernoulli number. Let f be the conductor of χ, then the first Bernoulli number is

$$B_{1,\chi} = \frac{1}{f}\sum_{a=0}^{f-1} a\chi(a)$$

where we put $\chi(a) = 0$ whenever a is not invertible modulo f. The Bernoulli number $B_{1,\chi}$ satisfies the following integrality property.

Lemma 1.1. *Let χ be a Dirichlet character of conductor f and order d. Assume that the conductor of χ is not a prime power. Then $B_{1,\chi} \in \mathbb{Z}[\zeta_d]$.*

Proof. Let r be a prime divisor of f. Let $f = r^n m$ with m and r coprime. Since we have a decomposition

$$(\mathbb{Z}/f\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/r^n\mathbb{Z})^\times,$$

there exist characters χ_m and χ_r of conductor m and r^n respectively such that $\chi = \chi_m\chi_r$.

Now we write $B_{1,\chi}$ as

$$B_{1,\chi} = \frac{1}{f}\sum_{a=0}^{f-1} a\chi(a) = \frac{1}{f}\sum_{b=0}^{r^n-1}\sum_{a=0}^{m-1}(b+ar^n)\chi_m(b+ar^n)\chi_r(b+ar^n) =$$
$$= \frac{1}{f}\sum_{b=0}^{r^n-1} b\chi_r(b)\sum_{a=0}^{m-1}\chi_m(b+ar^n) + \frac{1}{m}\sum_{b=0}^{r^n-1}\chi_r(b)\sum_{a=0}^{m-1} a\chi_m(b+ar^n).$$

For any $b \in \mathbb{Z}$ we claim that

$$\sum_{a=0}^{m-1}\chi_m(b+ar^n) = 0.$$

Indeed, since m and r^n are coprime, the set $\{b+ar^n : 0 \le a < m\}$ is a set of representatives for the integers modulo m. Therefore, we get that

$$\sum_{a=0}^{m-1}\chi_m(b+ar^n) = \sum_{a=0}^{m-1}\chi_m(a).$$

It is a well known fact that the right hand side term is zero.

We conclude that

$$B_{1,\chi} = \frac{1}{m}\sum_{b=0}^{r^n-1}\chi_r(b)\sum_{a=0}^{m-1} a\chi_m(b+ar^n).$$

Hence for any $r|f$ we get that r^n divides $fB_{1,\chi}$ in $\mathbb{Z}[\zeta_d]$. We deduce that $B_{1,\chi}$ lies in $\mathbb{Z}[\zeta_d]$. □

We recall now the analytic class number formula. It is proven in [Was97, Theorem 4.17]. For any imaginary abelian number field K, let K^+ be the maximal real field contained in K. We defined the relative class number h_K^- as the quotient h_K/h_{K^+}, where h_K is the cardinality of the class group of K.

Theorem 1.2 (Analytic class number formula)**.** *Let K be an abelian imaginary number field. Denote by $\mu(K)$ the group of roots of unity contained in K. Let $W_K = \#\mu(K)$ and let $Q_K = [O_K^\times : \mu(K)O_{K^+}^\times]$. Then*

$$h_K^- = Q_K W_K \prod_{\chi\in X(K)^-}\left(-\frac{1}{2}B_{1,\chi}\right).$$

Remark 1.3. Notice that h_K^- is actually an integer as shown in [Was97, Proposition 4.11]. Furthermore, [Was97, Theorem 4.12] states that Q_K can be 1 or 2.

Fix p a prime integer. Let $q=4$ if $p=2$ or $q=p$ if $p\neq 2$. Fix an odd prime $\ell\neq p$. Let K be an imaginary abelian number field. Denote by K_n the n-th level of the cyclotomic $\mathbb{Z}_p$-extension of K. We recall that the n-th level of the cyclotomic $\mathbb{Z}_p$-extension of the rationals $\mathbb{Q}_n$ is the unique real subfield of $\mathbb{Q}(\zeta_{qp^n})$ of degree p^n over $\mathbb{Q}$. As shown in [Was75, Lemma 1] we have the following.

Lemma 1.4. *Let K be an abelian number field. Let K_n be the n-th level of the cyclotomic $\mathbb{Z}_p$-extension of K. Then, there exists an abelian number field K' whose conductor is not divisible by qp and an integer $e\geq 0$ such that $K_n=K'_{n+e}$ for all sufficiently large n.*

Therefore, we will assume from now on that the conductor of K is not divisible by qp. Under this assumption we have that $K\cap\mathbb{Q}_n=\mathbb{Q}$. So, the field K_n is the compositum $K\,\mathbb{Q}_n$. Moreover, we have a natural isomorphism

$$\mathrm{Gal}(K_n|\,\mathbb{Q})\cong\mathrm{Gal}(K|\,\mathbb{Q})\times\mathrm{Gal}(\mathbb{Q}_n\,|\,\mathbb{Q}).$$

It follows that any Dirichlet character in $X(K_n)^-$ can be written uniquely as $\chi\psi$ where $\chi\in X(K)^-$ and $\psi\in X(\mathbb{Q}_n)$.

We can regard Dirichlet characters as ℓ-adic characters composing with the fixed embedding $\overline{\mathbb{Q}}^\times\subset\overline{\mathbb{Q}}_\ell^\times$. According to the analytic class number formula we get

$$\frac{h^-_{K_n}}{h^-_{K_{n-1}}}=u_n\frac{W_{K_n}}{W_{K_{n-1}}}\prod_{\chi\in X(L)^-}\prod_{\substack{\psi_n\in X(\mathbb{Q}_n)\\ \mathrm{ord}\psi_n=p^n}}B_{1,\chi\psi_n}\tag{1.1}$$

where u_n is a suitable ℓ-adic unit.

Remark 1.5. Let t be the exponent of $\mathrm{Gal}(K|\,\mathbb{Q})$ and let $\chi\psi_n$ be a character appearing in equation (1.1). Let f be the conductor of χ. Then, the conductor of $\chi\psi_n$ is $f'qp^n$ where $f'=f$ if p and f are coprime, or $f'=f/q$ otherwise. Therefore, $B_{1,\chi\psi_n}\in\mathbb{Z}_\ell[\zeta_t,\zeta_{p^n}]$. The latter statement is trivial if the conductor of $\chi\psi_n$ is coprime to ℓ, otherwise it is a consequence of Lemma 1.1. Furthermore, if $B_{1,\chi\psi_n}$ lies in the maximal ideal of $\mathbb{Z}_\ell[\zeta_t,\zeta_{p^n}]$ we get that ℓ divides $h^-_{K_n}/h^-_{K_{n-1}}$.

2. "Polynomials" with p-adic exponents

The residue field of $\overline{\mathbb{Z}}_\ell$ can be identified with an algebraic closure $\overline{\mathbb{F}}_\ell$ of the finite field $\mathbb{F}_\ell$. Therefore, we have a surjective morphism

$$\overline{\mathbb{Z}}_\ell\longrightarrow\overline{\mathbb{F}}_\ell.$$

For any positive n let $\zeta_{p^n}\in\overline{\mathbb{Z}}_\ell$ be a primitive p^n-th root of unity. We denote by $\overline{\zeta}_{p^n}$ the residue class of ζ_{p^n}. Since $\ell\neq p$, the element $\overline{\zeta}_{p^n}$ is a primitive p^n-th root of unity.

Definition 2.1. Let K be an abelian number field and let t be the exponent of $\mathrm{Gal}(K|\,\mathbb{Q})$. Let k be the residue field of $\mathbb{Z}_\ell[\zeta_t]$. We define $\overline{\Theta}$ to be the k-algebra of functions from $\mu=\varinjlim\langle\overline{\zeta}_{p^n}\rangle\subset\overline{\mathbb{F}}_\ell$ to $\overline{\mathbb{F}}_\ell$.

For any $a\in\mathbb{Z}_p$ we have the function U^a in $\overline{\Theta}$ such that

$$U^a:\overline{\zeta}_{p^n}\longrightarrow\overline{\zeta}^a_{p^n}.$$

Let $\Theta \subset \overline{\Theta}$ be the k-subalgebra generated by U^a for any $a \in \mathbb{Z}_p$.

We explain how the elements of Θ resemble polynomials in Lemma 2.4.

First we need to define the constant c. Let $c \geq 1$ be an integer such that for any $n \geq c$ all the primes above ℓ in the fields extension $\mathbb{Q}(\zeta_t, \zeta_{p^c}) \subset \mathbb{Q}(\zeta_t, \zeta_{p^n})$ are inert. Recall that t is the exponent of $\mathrm{Gal}(K|\mathbb{Q})$. The existence of c follows from the fact that a prime $\ell \neq p$ is unramified in a $\mathbb{Z}_p$-extension and there are only finitely many primes dividing ℓ. We suggest a method to find such c. We follow the idea in [FS95].

Lemma 2.2. *Let t be a positive integer. Denote by t' the largest divisor of t coprime to ℓ and let d be the order of ℓ inside $(\mathbb{Z}/t'\mathbb{Z})^\times$. Define*

$$c = v_p(\ell^{p-1} - 1) + v_p(d),$$

where v_p is the p-adic valuation normalized such that $v_p(p) = 1$. Then, the primes above ℓ in the extension $\mathbb{Q}(\zeta_t, \zeta_{p^c}) \subset \mathbb{Q}(\zeta_t, \zeta_{p^n})$ are inert for any $n \geq c$.

Proof. First of all, it suffices to prove the statement for t' instead of t. Indeed, all the relevant residue degree remain unchanged. So we may assume $t = t'$.

Let x be the least common multiple between d and $p-1$. Let $y = v_p(d)$, then we get that $x = (p-1)p^y s$ for some s coprime to p. Note that

$$v_p((\ell^{p-1})^{p^y s} - 1) = v_p((\ell^{p-1})^{p^y} - 1) = v_p(\ell^{p-1} - 1) + y = c.$$

Therefore we have that both $\ell^x \equiv 1 \bmod t'$ and $\ell^x \equiv 1 \bmod p^c$, but $\ell^x \not\equiv 1 \bmod p^{c+1}$. By [Was97, Theorem 2.13] we deduce that the primes above ℓ in the field extension $\mathbb{Q}(\zeta_{t'}, \zeta_{p^c}) \subset \mathbb{Q}(\zeta_{t'}, \zeta_{p^{c+1}})$ are inert since the extension has prime degree.

Finally, we assume by contradiction that there is a prime $\mathfrak{l}$ in $\mathbb{Q}(\zeta_{t'}, \zeta_{p^c})$ dividing ℓ that does not remain prime in $\mathbb{Q}(\zeta_{t'}, \zeta_{p^n})$. Then, taking the decomposition field F, we get a non trivial extension $\mathbb{Q}(\zeta_{t'}, \zeta_{p^c}) \subset F$ in which the prime $\mathfrak{l}$ splits completely. This leads to a contradiction. Indeed, the field $\mathbb{Q}(\zeta_{t'}, \zeta_{p^{c+1}})$ is contained in F and we have shown above that $\mathfrak{l}$ is inert. □

Remark 2.3. Fix $n \geq c$. Let t be the exponent of $\mathrm{Gal}(K|\mathbb{Q})$ and let k be the residue field of $\mathbb{Z}_\ell[\zeta_t]$. The fact that all the prime above ℓ are inert in the extension $\mathbb{Q}(\zeta_t, \zeta_{p^c}) \subset \mathbb{Q}(\zeta_t, \zeta_{p^n})$ is equivalent to say that the extension $k(\zeta_{p^c}) \subset k(\zeta_{p^n})$ has degree p^{n-c}. Moreover, we have an isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_t, \zeta_{p^n})|\,\mathbb{Q}(\zeta_t, \zeta_{p^c})) \cong \mathrm{Gal}(k(\overline{\zeta}_{p^n})|k(\overline{\zeta}_{p^c})).$$

It depends on the particular embedding $\overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}}_\ell$ we fixed.

The following Lemma is [Was97, Lemma 16.13].

Lemma 2.4. *Let $P \in \Theta$. Assume $P \neq 0$. Then P has finitely many zeroes in μ.*

Proof. Let $d_1, \ldots, d_s \in \mathbb{Z}_p$ distinct, and let $c_1, \ldots, c_s \in k$ such that

$$P = \sum_{i=1}^{s} c_i U^{d_i}.$$

Let M be a positive integer such that the exponents d_i are all different modulo p^M. Assume that P has infinitely many zeroes in μ. In particular, we can find a p^n-th root of unity $\zeta \in \mu$ such that $n > M + c$ and $P(\zeta) = 0$.

Notice that our choice of n implies that $\zeta^{d_i - d_j} \in k(\zeta_{p^c})$ if and only if $i = j$. Therefore, letting Tr be the trace map from $k(\zeta)$ to $k(\overline{\zeta}_{p^c})$, we get

$$0 = \mathrm{Tr}(\zeta^{-d_j} P(\zeta)) = \mathrm{Tr}\left(\sum_{i=1}^{s} c_i \zeta^{d_i - d_j}\right) = p^{n-c} c_j.$$

Since p is invertible in $\overline{\mathbb{F}}_\ell$, we get that $c_j = 0$ for any j. □

An interesting relation between some Bernoulli numbers and element of $\overline{\Theta}$ can be found in [Was97, Section 16.3] and in the appendix of [FS95].

Definition 2.5. Let K be an imaginary abelian number field. Fix an odd character χ in $X(K)^-$. Let q_{c-1} be the conductor of $\chi\psi_{c-1}$, where ψ_{c-1} lies in $X(\mathbb{Q}_{c-1})$ and has order exactly p^{c-1}. For any $y \in \mathbb{Z}_p$ we define the following element of $\overline{\Theta}$:

$$f_{\chi,y}(U) = \left(\sum_{\substack{b \equiv y \bmod p^c \\ 0<b<q_{c-1}}} \chi(b) U^b\right) (U^{q_{c-1}} - 1)^{-1}.$$

We abuse the notation $\chi(b)$ to denote its residue class in the field k.

Proposition 2.6. *Let K be an imaginary abelian number field and let χ be an odd character in $X(K)^-$. Let $n \geq \max(2c-1, 2)$. Let R be a set of representatives in $\mathbb{Z}_p$ for the subgroup of roots of unity of order $\varphi(q)$ modulo ± 1. Let F_χ be the element of $\overline{\Theta}$ defined as*

$$F_\chi = \sum_{\alpha \in R} f_{\chi,\alpha}(U^{\alpha^{-1}}).$$

Then, the Bernoulli number $B_{1,\chi\psi_n}$ lies in the maximal ideal of $\mathbb{Z}_\ell[\zeta_t, \zeta_{p^n}]$ if and only if there exists a primitive qp^n-th root of unity ζ such that $F_\chi(\zeta) = 0$. Here $\chi\psi_n$ is a character appearing in the Equation (1.1).

The proof of this proposition is contained in [Was97, Section 16.3]. Let Q be the element of Θ defined as

$$Q = \prod_{\alpha \in R} (U^{\alpha^{-1} q_{c-1}} - 1).$$

We will study in the next section the zeroes of $F_\chi Q$. This is convenient since F_χ has the same zeroes as $F_\chi Q$. Furthermore, $F_\chi Q$ lies in Θ.

3. Stabilization of the ℓ-part of the relative class number

The stabilization of $h^-_{K_n}$ is related to the non-vanishing of some rationals function F_χ when evaluated in primitive roots of unity of order a power of p. In this section we exploit this relation. We deal with the case $p = 2$ and the case p odd separately.

Lemma 3.1. *Assume $p = 2$. Let K be an imaginary abelian number field with conductor $\mathfrak{f}$ not divisible by 8. Let f be the largest odd divisor of $\mathfrak{f}$. Let n be an integer such that*

$$2^n \geq 2^{2c-1} f.$$

Then $v_\ell(B_{1,\chi\psi_n}) = 0$ for any $\chi \in X(K)^-$.

Proof. Fix $\chi \in X(K)^-$. Let F_χ and Q be as in the previous section. The hypotheses imply that $n \geq \max(2c-1, 2)$. Then, by Proposition 2.6 it suffices to show that $F_\chi Q(\zeta) \neq 0$ for any 2^{n+2}-th root of unity $\zeta \in \mu$.

Note that

$$F_\chi Q = \sum_{\substack{b \equiv 1 \bmod 2^c \\ 0<b<q_{c-1}}} \chi(b) U^b$$

is actually a polynomial with coefficients in the field k since all the exponents are integers. We have that $\deg(F_\chi Q) < q_{c-1}$. The integer q_{c-1} can be bounded from above by the conductor $2^{c+1}f$ of the field K_{c-1}. Assume now that a primitive 2^{n+2}-th root of unity ζ is a zero of $F_\chi Q$ then we have

$$2^{n+2-c} = [k(\zeta) : k(\overline{\zeta}_{2^c})] \leq [k(\zeta) : k] \leq \deg(F_\chi Q) < 2^{c+1} f.$$

This leads to a contradiction. □

Lemma 3.2. *Assume p odd. Let K be an imaginary abelian number field with conductor $\mathfrak{f}$ not divisible by p^2. Let f be the largest divisor of $\mathfrak{f}$ coprime to p. Let n be an integer such that*

$$p^n \geq p^{c-1} \left(\frac{p-1}{2} p^c f \right)^{\varphi(p-1)}.$$

Then $v_\ell(B_{1,\chi\psi_n}) = 0$ for any $\chi \in X(K)^-$.

Proof. Fix $\chi \in X(K)^-$. Let F_χ and Q be as in the previous section. Notice that the hypothesis imply that $n \geq \max(2c-1, 2)$. Then, by Proposition 2.6 it suffices to show that $F_\chi Q(\zeta) \neq 0$ for any p^{n+1}-th root of unity $\zeta \in \mu$.

Recall that $F_\chi Q$ is the element

$$\sum_{\alpha \in R} \left(\sum_{\substack{b \equiv \alpha \bmod p^c \\ 0<b<q_{c-1}}} \chi(b) U^{\alpha^{-1} b} \prod_{\beta \in R \setminus \{\alpha\}} (U^{\beta^{-1} q_{c-1}} - 1) \right).$$

Computing explicitly the products in the above formula, we get that the exponents of U that appear are the following:

$$\sum_{\alpha \in R} \psi(\alpha) \alpha^{-1}.$$

Where ψ is a function from R to $\mathbb{Z}$ such that:

(a) there exists a unique $\gamma \in R$ such that $\psi(\gamma) \equiv \gamma \bmod p^c$,
(b) for any $\alpha \in R$ we have $0 \leq \psi(\alpha) \leq q_{c-1}$,
(c) for any $\alpha \in R \setminus \{\gamma\}$ we have $\psi(\alpha) \in \{0, q_{c-1}\}$.

Choose an embedding $\mathbb{Z}[\zeta_{p-1}] \longrightarrow \mathbb{Z}_p$. Let $\mathfrak{p}$ be the pre-image of $p\mathbb{Z}_p$. We get an isomorphism

$$\frac{\mathbb{Z}[\zeta_{p-1}]}{\mathfrak{p}^{n+1-c}} \longrightarrow \frac{\mathbb{Z}_p}{p^{n+1-c}\mathbb{Z}_p}.$$

We look for possible choices of ψ such that $\sum_{\alpha\in R}\psi(\alpha)\alpha^{-1}$ is congruent to 1 modulo p^{n+1-c} or equivalently

$$\sum_{\alpha\in R}\psi(\alpha)\alpha^{-1} \equiv 1 \bmod \mathfrak{p}^{n+1-c}.$$

It happens if and only if

$$N_\psi = \underset{\mathbb{Q}(\zeta_{p-1})|\mathbb{Q}}{\text{Norm}}\left(\sum_{\alpha\in R}\psi(\alpha)\alpha^{-1} - 1\right)$$

is divisible by p^{n+1-c}. Without losing any generality we make the following assumptions: fix an embedding $\mathbb{Q}(\zeta_{p-1}) \longrightarrow \mathbb{C}$. We assume that under this embedding any $\alpha \in R$ is such that the imaginary part of α^{-1} is positive, and $1 \in R$. This is possible since R is defined up to sign. We get rough estimates

$$|N_\psi| \leq \left(|\psi(1)-1| + \sum_{\alpha\in R\setminus\{1\}}|\psi(\alpha)|\right)^{\varphi(p-1)} < \left(\frac{p-1}{2}q_{c-1}\right)^{\varphi(p-1)}.$$

Since q_{c-1} is the conductor of a character of the field K_{c-1} we can bound it from above by the conductor $p^c f$ of K_{c-1}. Therefore, we get

$$|N_\psi| < \left(\frac{p-1}{2}p^c f\right)^{\varphi(p-1)} \leq p^{n+1-c}.$$

If p^{n+1-c} divides N_ψ then $N_\psi = 0$. In particular, we have

$$\sum_{\alpha\in R}\psi(\alpha)\alpha^{-1} = 1.$$

By the assumptions made on R and the fact that $\psi(\alpha)$ is positive, the only possibility is that $\psi(1) = 1$ and $\psi(\alpha) = 0$ for any $\alpha \neq 1$. We can conclude that

$$F_\chi Q = (-1)^{\frac{p-1}{2}}\chi(1)U + \sum_i c_i U^{d_i},$$

where d_i are element in $\mathbb{Z}_p$ that are not congruent to 1 modulo p^{n+1-c}, and c_i are coefficients in k.

Finally, assume that a p^{n+1}-th root of unity ζ is a zero of $F_\chi Q$. Then mimicking the proof of Lemma 2.4, we consider the field trace Tr from $k(\zeta)$ to $k(\overline{\zeta}_{p^c})$. We get

$$0 = \text{Tr}\left(\zeta^{-1}F_\chi Q(\zeta)\right) = (-1)^{\frac{p-1}{2}}\chi(1)p^{n+1-c}.$$

Since the right hand side of the equality is non-trivial in $\overline{\mathbb{F}}_\ell$ we get a contradiction. □

The strategy we use to prove the above Lemma is similar to the one used for proving [Hor02, Lemma 8 and 9].

So far we have shown:

Theorem 3.3. *Let K be an imaginary abelian number field with conductor $\mathfrak{f}$ not divisible by qp. Denote by f the largest divisor of $\mathfrak{f}$ which is coprime to p. Let n be an integer such that*

$$p^n \geq p^{c-1}\left(\frac{\varphi(q)}{2}p^c f\right)^{\varphi(p-1)}.$$

Then $v_\ell(h^-_{K_n}/h^-_{K_{n-1}}) = 0$, where K_n is the n-th level of the cyclotomic $\mathbb{Z}_p$-extension of K.

Proof. From the analytic class number formula (1.1) we deduce that

$$v_\ell\left(\frac{h^-_{K_n}}{h^-_{K_{n-1}}}\right) = v_\ell\left(\frac{W_{K_n}}{W_{K_{n-1}}}\right) + \sum_{\chi,\psi_n} v_\ell(B_{1,\chi\psi_n}).$$

By Lemmas 3.1 and 3.2 we have $v_\ell(B_{1,\chi\psi_n}) = 0$.

Recall that W_{K_n} is the cardinality of the group of roots of unity inside K_n. Assume that $W_{K_n}/W_{K_{n-1}}$ is divisible by ℓ. This implies that there exists an integer $s \geq 1$ such that ζ_{ℓ^s} lies in K_n but not in K_{n-1}. Let s be minimal. Since the degree $[K_{n-1} : K_n]$ is prime we have that

$$K_{n-1} \subset K_{n-1}(\zeta_{\ell^s}) = K_n.$$

We get a contradiction since the conductor of K_n is exactly $qp^n f$, while the conductor of $K_{n-1}(\zeta_{\ell^s})$ is a divisor of $qp^{n-1}f\ell$. □

4. Reflection theorem

We state in this section the reflection theorem. It permit us to get information on the full class group knowing the minus part. First of all we introduce some notation.

Let G be a finite abelian group with cardinality prime to ℓ. Let ϕ be a character

$$\phi : G \longrightarrow \overline{\mathbb{Q}}_\ell^\times.$$

We define $\mathcal{O}_\phi$ to be the local $\mathbb{Z}_\ell$-algebra generated by the image of G via ϕ. Then $\mathcal{O}_\phi$ is a G-module via the relation $g.x = \phi(g)x$ for any $g \in G$ and $x \in \mathcal{O}_\phi$. We say that two characters ϕ_1 and ϕ_2 are Galois conjugate if there exists an automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_\ell|\,\mathbb{Q}_\ell)$ such that $\phi_1 = \sigma \circ \phi_2$. We denote by $\mathcal{X}(G)$ the set of such characters up to Galois conjugation.

Since the cardinality of G is coprime to ℓ we have an isomorphism of $\mathbb{Z}_\ell[G]$-modules

$$\mathbb{Z}_\ell[G] \xrightarrow{\cong} \bigoplus_{\phi\in\mathcal{X}(G)} \mathcal{O}_\phi$$

defined by $g \mapsto (\phi(g))_\phi$. Finally, we remark that for any $\mathbb{Z}_\ell[G]$-module B we have a decomposition in $\mathbb{Z}_\ell[G]$-modules

$$B \cong \bigoplus_{\phi\in\mathcal{X}(G)} B(\phi)$$

where the summands $B(\phi)$ are defined as $B \otimes_{\mathbb{Z}_\ell[G]} \mathcal{O}_\phi$.

Lemma 4.1. *Let $K \subset L \subset M$ be an extension of abelian number fields. Let G and H be the Galois groups $\mathrm{Gal}(M|K)$ and $\mathrm{Gal}(M|L)$ respectively. Let $\mathcal{A}_L$ and $\mathcal{A}_M$ be the ℓ-parts of the class group of the respective fields. Assume that ℓ is coprime to the cardinality of G. Then, the natural map $\mathcal{A}_L \longrightarrow \mathcal{A}_M$ induces an isomorphism*

$$\mathcal{A}_L(\phi) \cong \mathcal{A}_M(\phi)^H$$

for any $\phi \in \mathcal{X}(G)$. In particular, we have that

$$\mathcal{A}_L \cong \bigoplus_{\substack{\phi \in \mathcal{X}(G) \\ \phi(H)=1}} \mathcal{A}_M(\phi).$$

Proof. Consider the composition of the following maps:

$$\mathcal{A}_L(\phi) \xrightarrow{\iota} \mathcal{A}_M(\phi) \xrightarrow{N} \mathcal{A}_L(\phi)$$

where ι is induced by the inclusion $L \subset M$ while N is induced by the norm map form M to L. The above composition maps $I \mapsto I^{\#H}$. Since the cardinality of H is coprime to ℓ, the map $N \circ \iota$ is an isomorphism. Therefore, the exact sequence

$$0 \longrightarrow \ker(N) \longrightarrow \mathcal{A}_M(\phi) \xrightarrow{N} \mathcal{A}_L(\phi) \longrightarrow 0$$

splits. It follows that $\mathcal{A}_M(\phi) \cong \mathcal{A}_L(\phi) \oplus \ker(N)$. Taking H-invariants we get the isomorphism $\mathcal{A}_M(\phi)^H \cong \mathcal{A}_L(\phi)^H \oplus \ker(N)^H$. It is clear that $\mathcal{A}_L(\phi)^H = \mathcal{A}_L(\phi)$. While $\ker(N)^H = \{1\}$. Indeed, let $x \in \ker(N)^H$, then

$$N(x) = x^{\#H} = 1.$$

It implies that $x = 1$ since taking the $\#H$-th power is an isomorphism. This proves the first part of the Lemma.

Recall that there is a bijection between $\mathcal{X}(G/H)$ and the characters of $\mathcal{X}(G)$ that are trivial on H. Therefore since $\mathcal{A}_L$ is a $\mathbb{Z}_\ell[G/H]$-module we get

$$\mathcal{A}_L = \bigoplus_{\phi \in \mathcal{X}(G/H)} \mathcal{A}_L(\phi) = \bigoplus_{\substack{\phi \in \mathcal{X}(G) \\ \phi(H)=1}} \mathcal{A}_L(\phi) \cong \bigoplus_{\substack{\phi \in \mathcal{X}(G) \\ \phi(H)=1}} \mathcal{A}_M(\phi)^H.$$

Finally, since ϕ is trivial on H we have that $\mathcal{A}_M(\phi)^H = \mathcal{A}_M(\phi)$. □

We state now the reflection theorem or Spiegelungssatz. We focus on the case of abelian fields. The classical statement can be found in [Leo58], while a generalization of it is in [Gra03, Section 2.5*b*].

Definition 4.2. Let L be an abelian number field. Assume that $\zeta_\ell \in L$. We define the Teichmüller character ω_ℓ as the group homomorphism

$$\omega_\ell : \mathrm{Gal}(L|\,\mathbb{Q}) \longrightarrow \langle \zeta_{\ell-1} \rangle \subset \overline{\mathbb{Q}}_\ell^\times$$

such that for any $g \in \mathrm{Gal}(L|\,\mathbb{Q})$ we have $g(\zeta_\ell) = \zeta_\ell^{\omega_\ell(g)}$.

Theorem 4.3 (Reflection theorem)**.** *Let $K \subset L$ be an extension of abelian number fields. Assume that $\zeta_\ell \in L$, and ℓ is coprime to the cardinality of $G = \mathrm{Gal}(L|K)$. Let ω_ℓ be the restriction of the Teichmüller character to G. For any character $\phi \in \mathcal{X}(G)$ let $\phi^* = \omega_\ell \phi^{-1}$. Then*

$$\dim_{\mathbb{F}_\ell}\left(\mathcal{A}_L[\ell](\phi^*)\right) - \dim_{\mathbb{F}_\ell}\left(\mathcal{A}_L[\ell](\phi)\right) \leq \dim_{\mathbb{F}_\ell}\left((O_L^\times/O_L^{\times\ell})(\phi)\right).$$

The proof relies on the fact that the maximal unramified extension of exponent ℓ can be described both via class field theory and Kummer theory.

Remark 4.4. Keep the notation of the above Theorem. Assume that K is a real field and $\phi \neq \omega_\ell$ is an odd character. Then

$$\dim_{\mathbb{F}_\ell}\left((O_L^\times/O_L^{\times\ell})(\phi)\right) = 0.$$

Indeed, let $\mu(L)$ be the subgroup of roots of unity inside L. Recall that he index $[O_L^\times : \mu(L)O_{L^+}^\times]$ is equal to 1 or 2 as in [Was97, Theorem 4.12]. Since ℓ is odd we get

$$\frac{O_L^\times}{O_L^{\times\ell}} \cong \frac{\mu(L)}{\mu(L)^\ell} \oplus \frac{O_{L^+}^\times}{O_{L^+}^{\times\ell}}.$$

Since ϕ is odd, it follows that $(O_{L^+}^\times/O_{L^+}^{\times\ell})(\phi) = 0$. Moreover, the G-module $\mu(L)/\mu(L)^\ell$ is cyclic of order ℓ and it is generated by ζ_{ℓ^s} for a suitable $s \geq 1$. Therefore, we get that

$$\frac{\mu(L)}{\mu(L)^\ell} = \frac{\mu(L)}{\mu(L)^\ell}(\omega_\ell).$$

5. An upper bound for n_0

We are now ready to prove the Theorem presented in the introduction.

Theorem 5.1. *Let p be a prime integer and set $q = 4$ if $p = 2$ or $q = p$ otherwise. Let ℓ be an odd prime different from p. Let K be an abelian field with conductor not divisible by qp. Denote by $\mathfrak{f}$ be the conductor of $K(\zeta_\ell)$ and by t be the exponent of $\mathrm{Gal}(K(\zeta_\ell)|\,\mathbb{Q})$. Fix an integer $c \geq 1$ such that for any $n \geq c$ the primes above ℓ in the field extension $\mathbb{Q}(\zeta_t, \zeta_{p^c}) \subset \mathbb{Q}(\zeta_t, \zeta_{p^n})$ are inert. Assume that*

$$p^n \geq p^{c-1}\left(\frac{\varphi(q)}{2}p^c f\right)^{\varphi(p-1)}$$

where f is the largest divisor of $\mathfrak{f}$ coprime to p.

Then, the natural morphism $\mathcal{A}_{K_{n-1}} \longrightarrow \mathcal{A}_{K_n}$ is an isomorphism. Here $\mathcal{A}_{K_n}$ denotes the ℓ-part of the class group of the n-th level K_n of the cyclotomic $\mathbb{Z}_p$ extension of K.

Proof. Let $L = K(\zeta_\ell)$. Then $L_n = K_n(\zeta_\ell)$ is the n-th level in the cyclotomic $\mathbb{Z}_p$-extension of L. Let $G = \mathrm{Gal}(L_n|K)$ and $H = \mathrm{Gal}(L_n|L_{n-1})$. Let $\sigma \in G$ be the automorphism induced by complex conjugation. Note that ℓ is coprime to the cardinality of G. Then we have

$$\mathcal{A}_{L_n} = \left(\bigoplus_{\substack{\phi\in\mathcal{X}(G)\\ \phi(\sigma)=1}} \mathcal{A}_{L_n}(\phi)\right) \oplus \left(\bigoplus_{\substack{\phi\in\mathcal{X}(G)\\ \phi(\sigma)=-1}} \mathcal{A}_{L_n}(\phi)\right).$$

According to Lemma 4.1 we deduce that the first summand can be identified with $\mathcal{A}_{L_n^+}$. Hence the second one has cardinality exactly $h^-_{L_n}$. We call $\mathcal{A}^-_{L_n}$ the second summand. We have a similar decomposition for the field L_{n-1} where the sums run over the characters that are trivial on H.

Let $\mathcal{X}_H(G)$ be the set of characters of $\mathcal{X}(G)$ that do not vanish on the whole subgroup H. Then we have

$$\frac{\mathcal{A}_{L_n}}{\mathcal{A}_{L_{n-1}}} \cong \left(\bigoplus_{\substack{\phi\in\mathcal{X}_H(G)\\ \phi(\sigma)=1}} \mathcal{A}_{L_n}(\phi) \right) \oplus \left(\bigoplus_{\substack{\phi\in\mathcal{X}_H(G)\\ \phi(\sigma)=-1}} \mathcal{A}_{L_n}(\phi) \right) \cong \frac{\mathcal{A}_{L_n^+}}{\mathcal{A}_{L_{n-1}^+}} \oplus \frac{\mathcal{A}^-_{L_n}}{\mathcal{A}^-_{L_{n-1}}}.$$

Here the second summand has cardinality equal to the ℓ-part of $h^-_{L_n}/h^-_{L_{n-1}}$, which is 1 by Theorem 3.3. Therefore, $\mathcal{A}_{L_n}(\phi)$ is trivial for any $\phi \in \mathcal{X}_H(G)$ such that $\phi(\sigma) = -1$.

Now let ψ be in $\mathcal{X}_H(G)$ and $\psi(\sigma) = 1$. Then the character $\psi^* = \omega_\ell \psi^{-1}$ still lies in $\mathcal{X}_H(G)$, but $\psi^*(\sigma) = -1$. We apply the reflection theorem on the character ψ^* to deduce that

$$\dim_{\mathbb{F}_\ell} (\mathcal{A}_L[\ell](\psi)) - \dim_{\mathbb{F}_\ell} (\mathcal{A}_L[\ell](\psi^*)) \leq 0.$$

The term involving $(O^\times_{L_n}/O^{\times\ell}_{L_n})(\psi^*)$ gives no contribution as shown in Remark 4.4. We have already shown that $\mathcal{A}_{L_n}(\psi^*)$ is trivial. Therefore, the above inequality implies that $\mathcal{A}_{L_n}[\ell](\psi)$ and hence $\mathcal{A}_{L_n}(\psi)$ are trivial. So, the natural morphism $\mathcal{A}_{L_{n-1}} \longrightarrow \mathcal{A}_{L_n}$ is an isomorphism.

Consider the extension $K_n \subset L_n$. Its degree is a divisor of $\ell - 1$, therefore it is coprime to ℓ. This suffices to prove that the morphism $N : \mathcal{A}_{L_n} \longrightarrow \mathcal{A}_{K_n}$ induced by the norm is surjective for any $n \geq 0$. Similarly, the extension $K_{n-1} \subset K_n$ has degree coprime to ℓ. Hence, the natural morphism $\iota : \mathcal{A}_{K_{n-1}} \longrightarrow \mathcal{A}_{K_n}$ is injective.

We have the following commutative diagram

$$\begin{array}{ccc} \mathcal{A}_{L_{n-1}} & \xrightarrow[\cong]{\iota} & \mathcal{A}_{L_n} \\ \Big\downarrow N & & \Big\downarrow N \\ \mathcal{A}_{K_{n-1}} & \xhookrightarrow{\iota} & \mathcal{A}_{K_n} \end{array}$$

from which it follows that $\mathcal{A}_{K_{n-1}} \cong \mathcal{A}_{K_n}$ as desired. □

Remark 5.2. We can find an upper bound for n_0 in this way: chose $\widetilde{n}$ minimal such that it satisfies the hypothesis of the above theorem. Then

$$n_0 \leq \widetilde{n} - 1 \leq (\varphi(p-1)+1)c + 1 + \varphi(p-1)\log_p\left(\frac{\varphi(q)}{2}f\right).$$

We conclude this section giving an example. It is the case $K = \mathbb{Q}$. In this setting we can choose the integer c as shown in Lemma 2.2. Namely $c = v_p(\ell^{p-1} - 1)$. Then we get

$$n_0 \leq (\varphi(p-1)+1)c + 1 + \varphi(p-1)\log_p\left(\frac{\varphi(q)}{2}\ell\right).$$

This result is comparable with [Hor02, Lemma 8]. Although in that article the approach is based on cyclotomic units, the key point is finding zeroes of rational functions similar to the ones defined in Section 2. Since the bound we get is similar to the one in [Hor02], we are led to think that there is a relation within $F_{\omega_\ell^{-1}}$ and the rational functions appearing in [Hor02]. We finally notice that the bound on n_0 is the same for the field $\mathbb{Q}(\zeta_\ell)$, therefore there is no reason to expect it to be sharp.

References

[FS95] Friedman E. and Sands J.W. (with an Appendix by Washington L.C.): *On the ℓ-adic Iwasawa λ-invariant in a p-extension*, Math. Comp. **64** (1995), 1659-1674.

[FK11] Fukuda T. and Komatsu K.: *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, III*, Int. J. Number Theory **7** (2011), 1627-1635.

[Gra03] Gras G.: *Class field theory. From theory to practice*, Springer Monographs in Math. (2003).

[Hor02] Horie K.: *Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field*, J. Lond. Math. Soc. **66** (2002), 257-275.

[Hor05] Horie K.: *The ideal class group of the basic $\mathbb{Z}_p$-extension over a quadratic imaginary field*, Tohoku Math. J. **57** (2005) 375-394.

[Leo58] Leopoldt H.W.: *Zur Struktur der l-Klassengruppe galoisscher Zahlkörper*, J. Reine Angew. Math. **199** (1958), 165-174.

[Sin87] Sinnott W.: *Γ-transforms of rational function measures on $\mathbb{Z}_S$*, Invent. Math. **89** (1987), 139-157.

[Was75] Washington L.C.: *Class numbers and $\mathbb{Z}_p$-extensions*, Math. Ann. **214** (1975), 171-193.

[Was97] Washington L.C.: *Introduction to cyclotomic fields*, Second Edition, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York (1997).

Dipartimento di matematica, università di Roma "La Sapienza", piazzale Aldo Moro 5, 00185 Roma Italy

Email address: pagani@mat.uniroma1.it