Journal of Pure and Applied Algebra 53 (1988) 125–137
North-Holland

COHOMOLOGY OF CLASS GROUPS OF CYCLOTOMIC FIELDS; AN APPLICATION TO MORSE-SMALE DIFFEOMORPHISMS

René SCHOOF
Dipartimento di Matematica, Università di Pisa, 56100 Pisa, Italy

Communicated by J.D. Stasheff
Received 4 December 1986

The obstruction group SSF came up in the topological investigations of Shub and Franks. It was studied by Bass and Lenstra; the latter showed that

$$\mathrm{SSF} \cong \bigoplus_{n \geq 1} \mathrm{Pic}\left(\mathbb{Z}\left[\zeta_n, \frac{1}{n}\right]\right).$$

In this paper the structure of SSF as an abelian group is determined. It is proved that

$$\mathrm{SSF} \cong \bigoplus_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$$

confirming a conjecture of Lenstra.

1. Introduction

Let M be a compact smooth manifold. In [9] Shub and Sullivan showed that if a diffeomorphism $f: M \to M$ is 'Morse-Smale', then the eigenvalues of f_* acting on $H_*(M, \mathbb{Q})$ are roots of unity. In the course of proving some kind of converse to this theorem, Shub and Franks [5] introduced a certain obstruction group which was baptized SSF by Bass [1]. It is defined as follows:

Let $\mathscr{C}$ denote the category with objects pairs (H, u) where H is a finitely generated abelian group and $u \in \mathrm{Aut}(H)$ is such that $u \otimes \mathbb{Q}$ has only roots of unity as its eigenvalues; the $\mathscr{C}$-morphisms are defined in the obvious way. A pair (H, u) is called a permutation module if H has a $\mathbb{Z}$-basis permuted by u. Let $K_0(\mathscr{C})$ denote the Grothendieck group of $\mathscr{C}$ and let $P \subset K_0(\mathscr{C})$ denote the subgroup generated by the classes of the permutation modules. We define

$$\mathrm{SSF} = K_0(\mathscr{C})/P.$$

In [7] Lenstra showed that there is a natural isomorphism

$$\mathrm{SSF} \cong \bigoplus_{n \geq 1} \mathrm{Pic}\left(\mathbb{Z}\left[\frac{1}{n}, \zeta_n\right]\right). \tag{1}$$

Here ζ_n denotes a primitive nth root of unity. In this paper we will prove the following theorem:

Theorem 1.1. *There is an isomorphism of abelian groups*

$$\mathrm{SSF} \cong \bigoplus_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

This result was conjectured by H.W. Lenstra, c.f. [1,7]. In fact, in [7] Lenstra determined the structure of SSF as an abelian group except for its 2-part. In this paper we determine the structure of the 2-part of SSF. For the sake of completeness, a self-contained proof of Theorem 1.1, including a discussion of the odd part of SSF, is given in Section 4. For a related computation see [2].

In Section 2 we discuss the Galois cohomology of class groups of abelian number fields with special attention for their 2-parts. In Section 3 we apply the results of Section 2 to the class groups of the fields in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\zeta_{116})$.

For every commutative ring R with 1 we denote by R^* the group of units of R. For a prime p we denote by $\mathbb{Z}_p$ the ring of p-adic integers and by $\mathbb{Q}_p$ the field of p-adic numbers; for an abelian group A, its p-part $A \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is denoted by A_p. For a prime power $q > 1$ we denote by $\mathbb{F}_q$ a field of q elements. For every commutative ring R with 1 and every abelian group G we denote for every subgroup H of G by I_H the kernel of $R[G] \to R[G/H]$. For a finite group G, a $\mathbb{Z}[G]$-module M and an integer q we denote by $\hat{H}^q(G, M)$ the qth Tate cohomology group of G with values in M. For every $n \in \mathbb{Z}_{\geq 1}$, we let ζ_n denote a primitive nth root of unity and we will also write i for ζ_4.

2. Cohomological triviality of class groups

In this section we will study the Galois cohomology of the class groups of abelian number fields. We will investigate in which cases the 2-parts of the minus class groups of abelian number fields are cohomologically trivial. For the class field theory and cohomology theory that we will use see [3].

We will first prove two general lemmas.

We introduce some notation: Let G denote a finite p-group and let Δ denote a finite abelian group of order prime to p. For every character $\chi : \Delta \to \overline{\mathbb{Q}}_p^*$ and every $\mathbb{Z}_p[\Delta]$-module M. We denote by $M(\chi)$ the χ-part of M, i.e. $M(\chi) = \mathrm{Hom}_{\mathbb{Z}_p[\Delta]}(O_\chi, M)$ where O_χ is the unramified extension $\mathbb{Z}_p[\mathrm{im}\,\chi]$ of $\mathbb{Z}_p$: it is a module over $\mathbb{Z}[\Delta]$ as follows: for $\delta \in \Delta$ and $x \in O_\chi$ we define $\delta \cdot x = \chi(\delta) \cdot x$.

Lemma 2.1. (i) *For every $\mathbb{Z}[G \times \Delta]$-module M we have that $\hat{H}^q(G, M)^\Delta \cong \hat{H}^q(G, M^\Delta)$ for all $q \in \mathbb{Z}$.*

(ii) *For every $\mathbb{Z}_p[G \times \Delta]$-module M and every character $\chi : \Delta \to \overline{\mathbb{Q}}_p^*$ it holds that $\hat{H}^q(G, M(\chi)) \cong \hat{H}^q(G, M)(\chi)$ for all $q \in \mathbb{Z}$.*

Proof. (i) It is trivial that the inclusion $M^{\Delta} \to M$ induces a map $\hat{H}^q(G, M^{\Delta}) \xrightarrow{f} \hat{H}^q(G, M)^{\Delta}$. The Δ-trace map $M \to M^{\Delta}$ induces a map $\hat{H}^q(G, M)^{\Delta} \xrightarrow{g} \hat{H}^q(G, M^{\Delta})$. Clearly both fg and gf are just multiplication by $\#\Delta$ which is a bijection on the cohomology groups, since these groups, being killed by $\#G$ have order coprime to $\#\Delta$.

(ii) It is trivial that the canonical map $M(\chi) \hookrightarrow M$ induces a map $\hat{H}^q(G, M(\chi)) \to \hat{H}^q(G, M)(\chi)$. Since Δ is abelian of order coprime to $\#G$, the composite map $\bigoplus_{\chi} M(\chi) \to M$ is an isomorphism and so is $\bigoplus_{\chi} \hat{H}^q(G, M(\chi)) \to \bigoplus_{\chi} \hat{H}^q(G, M)(\chi)$. This proves (ii). □

Lemma 2.2. *Let O be a finite extension of $\mathbb{Z}_p$ and let M be a finite $O[G]$-module. The following are equivalent*:

(i) *M is a cohomologically trivial $O[G]$-module*;

(ii) *There is an exact sequence*

$$0 \to F \to F \to M \to 0$$

where F is $O[G]$-free of rank equal to the number of generators of $M/I_G M$ as an O-module.

Proof. It is trivial that (ii) implies (i); to prove the converse we observe that since G is a p-group, the ring $O[G]$ is a local ring with maximal ideal $\mathfrak{m}$ and residue field k isomorphic to the residue field of the local ring O. By Nakayama's lemma there is an $O[G]$-surjection $F \twoheadrightarrow M$ where F is $O[G]$-free of $O[G]$-rank equal to $\dim_k M/\mathfrak{m}M = \mathrm{rk}_O M/I_G M$. This gives us an exact sequence $0 \to A \to F \to M \to 0$ where A is O-free since F is and where A is cohomologically trivial since both M and F are. It follows from an analogue of [3, Theorem 8, p. 113] (replace $\mathbb{Z}$ by O and give the same proof) that A is an $O[G]$-projective module. Since $O[G]$ is a local ring, A is in fact free and since M is finite, it has the same rank as F. This proves Lemma 2.2. □

For future reference we mention the following well-known results. In the notation of Lemma 2.2, let M be a finite $O[G]$-module sitting in an exact sequence $0 \to F \xrightarrow{\theta} F \to M \to 0$, where F is free of finite rank. It is well known that up to a p-adic unit, the order of M is given by

$$\#M = \underset{O/\mathbb{Z}_p}{\mathrm{Norm}} \left(\prod_{\chi \in \hat{G}} \chi(\det \theta) \right), \tag{2}$$

here $\hat{G}$ denotes $\mathrm{Hom}(G, \overline{\mathbb{Q}}_p^*)$ and $\chi \in \hat{G}$ is linearly extended to a ring homomorphism $\chi : O[G] \to \overline{\mathbb{Q}}_p^*$. In fact, for every subgroup H of G we have

$$\#M/I_H M = \underset{O/\mathbb{Z}_p}{\mathrm{Norm}} \left(\prod_{\chi \in (G/H)^{\wedge}} \chi(\det \theta) \right). \tag{3}$$

Next we apply the above in the case where G and Δ are Galois groups of number fields. We introduce some notation: let F be a number field; by 0_F we denote the ring of integers of F, by 0_F^* its units and by Cl_F its class group. Let C_F denote the idèle class group $\mathbb{A}_F^*/F^*$ of F and let U_F denote the unit idèles: $U_F = (x \in \mathbb{A}_F^* : |x|_v = 1$ for all finite valuations v of $F)$. If E/F is a finite abelian extension of number fields with $G = \mathrm{Gal}(E/F)$ we let $G_\mathfrak{p} \subset G$, for a prime $\mathfrak{p}$ of F, denote the decomposition group of any prime $\mathfrak{q}$ in E over $\mathfrak{p}$.

Lemma 2.3. *Let L/k be a finite abelian extension of number fields with* $\mathrm{Gal}(L/k) = G \times \Delta$ *where G is a p-group and Δ has order prime to p. Let $\chi : \Delta \to \overline{\mathbb{Q}}_p^*$ denote a character.*

(i) $\hat{H}^q(G, C_L)(\chi) = 0$ *for all* $q \in \mathbb{Z}$, *if* $\chi \neq 1$.

(ii) $\hat{H}^q(G, U_L)(\chi) = 0$ *for all* $q \in \mathbb{Z}$, *if* $\chi(\Delta_\mathfrak{p}) \neq 1$ *for every prime* $\mathfrak{p}$ *of k ramified in* L^Δ/k.

Proof. (i) By *global* class field theory there is for every $q \in \mathbb{Z}$ a canonical isomorphism

$$\hat{H}^q(G, C_L) \cong \hat{H}^{q-2}(G, \mathbb{Z}).$$

Since $\mathbb{Z}$ is Δ-invariant it follows from Lemma 2.1(i) that $\hat{H}^q(G, \mathbb{Z})$ is Δ-invariant as well and (i) follows.

(ii) By Shapiro's lemma we have

$$\hat{H}^q(G, U_L) \cong \prod_{\mathfrak{q} \text{ of } K} \hat{H}^q(G_\mathfrak{q}, 0_{L_\mathfrak{r}}^*) \text{ as } \Delta\text{-modules.}$$

where K denotes L^G and $\mathfrak{r}$ is a prime of L over $\mathfrak{q}$. It is well known that $\hat{H}^q(G_\mathfrak{q}, 0_{L_\mathfrak{r}}^*) = 0$ whenever $\mathfrak{q}$ is unramified in L/K or equivalently if $\mathfrak{p}$ is unramified in L^Δ/k; here $\mathfrak{p}$ denotes the prime of k over which $\mathfrak{q}$ lies. There is an exact sequence of $\Delta_\mathfrak{p} \times G_\mathfrak{q}$-modules

$$0 \to 0_{L_\mathfrak{r}}^* \to L_\mathfrak{r}^* \to \mathbb{Z} \to 0.$$

By *local* class field theory there is for every $q \in \mathbb{Z}$ a canonical isomorphism

$$\hat{H}^q(G_\mathfrak{q}, L_\mathfrak{r}^*) \cong \hat{H}^{q-2}(G_\mathfrak{q}, \mathbb{Z}).$$

By Lemma 2.1 the groups $\hat{H}^q(G_\mathfrak{q}, \mathbb{Z})$ and $\hat{H}^q(G_\mathfrak{q}, L_\mathfrak{r}^*)$ have trivial $\Delta_\mathfrak{p}$-action. Since $\gcd(\#\Delta_\mathfrak{p}, \#G_\mathfrak{q}) = 1$ we see that the same is true for $\hat{H}^q(G_\mathfrak{q}, 0_{L_\mathfrak{r}}^*)$. It follows that the χ-part of $\hat{H}^q(G_\mathfrak{q}, 0_{L_\mathfrak{r}}^*)$ is 0 whenever $\chi(\Delta_\mathfrak{p}) \neq 1$. This proves the lemma. □

We introduce some more notation; let K be a CM-field with maximal real subfield K^+ and let σ denote the non-trivial K^+-automorphism of K. By μ_K we denote the group of roots of unity in K; we let $U_K^- = (\sigma - 1)U_K = \{\sigma(u)/u \in U_K\}$ and we observe that $(\sigma - 1)U_K = U_K/U_K^+$. By C_K^- we denote $(\sigma - 1)C_K$ which is isomorphic to C_K/C_K^+ and finally by $\mathrm{Cl}_K{}^-$ we denote $\mathrm{Cl}_K/\mathrm{im}(Cl_{K^+})$.

Lemma 2.4. *For every* CM*-field* K *there is an exact sequence*

$$0 \to \mu_K \cap U_K^- \to U_K^- \to C_K^- \to \mathrm{Cl}_K^- \to 0.$$

Proof. From the diagram

$$\begin{array}{ccccccc} U_{K^+} & \longrightarrow & C_{K^+} & \longrightarrow & \mathrm{Cl}_{K^+} & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ U_K & \longrightarrow & C_K & \longrightarrow & \mathrm{Cl}_K & \longrightarrow & 0 \end{array}$$

we obtain an exact sequence

$$U_K^- \to C_K^- \to \mathrm{Cl}_K^- \to 0$$

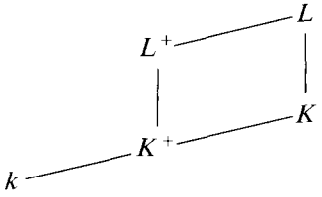
and from the diagram

$$\begin{array}{ccccccc} & & & & 0 & & 0 \\ & & & & \downarrow & & \downarrow \\ & & & & U_K^- & \longrightarrow & C_K^- \\ & & & & \downarrow & & \downarrow \\ 0 & \longrightarrow & 0_K^* & \longrightarrow & U_K & \longrightarrow & C_K \end{array}$$

we see that $\ker(U_K^- \to C_K^-) = 0_K^* \cap U_K^-$. If $\varepsilon \in 0_K^* \cap U_K^-$, then $\varepsilon = \sigma(u)/u$ for some $u \in U_K$; therefore $\sigma(\varepsilon) \cdot \varepsilon = 1$ and it follows that ε is a root of unity. We conclude that $0_K^* \cap U_K^- = \mu_K \cap U_K^-$. This proves the lemma. □

Theorem 2.5. *Let* L/K *be a 2-power degree extension of complex abelian number fields. Let* k *be a subfield of* K^+ *such that* $[K^+ : k]$ *is odd.*

Let Δ *denote* $\mathrm{Gal}(K^+/k)$ *and let* $\chi : \Delta \to \overline{\mathbb{Q}}_2^*$ *be a nontrivial character. Put* $O_\chi = \mathbb{Z}_2[\mathrm{im}\,\chi]$ *and* $G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(L^+/K^+)$.



If $\chi(\Delta_\mathfrak{p}) \neq 1$ *for all primes* $\mathfrak{p}$ *of* k *over which primes ramify in* L/K^+, *then*

(i) *For every field* $K \subset F \subset L$ *with* $H = \mathrm{Gal}(L/F)$ *we have*

$$\mathrm{Cl}_{F,2}^-(\chi) \cong \mathrm{Cl}_{L,2}^-(\chi)/I_H \mathrm{Cl}_{L,2}^-(\chi) \text{ as } O_\chi[G/H]\text{-modules.}$$

(ii) *There is an exact sequence of* $O_\chi[G]$*-modules*

$$0 \to O_\chi[G]^r \to O_\chi[G]^r \to \mathrm{Cl}_{L,2}^-(\chi) \to 0$$

where $r = \mathrm{rank}_{O_\chi} \mathrm{Cl}_{K,2}^-(\chi)$.

Proof. Let F be a subfield, $K \subset F \subset L$. Let $H = \mathrm{Gal}(L/F)$ and let N_H denote the H-norm map.

Since H is a 2-group, the cohomology groups of $\mu_L \cap U_L^-$ and $\mu_{L,2} \cap U_L^-$ are isomorphic. The Galois group $\mathrm{Gal}(\bar{F}/F)$ acts via a quotient group of 2-power order on $\mu_{L,2}$, so, the group Δ, being of odd order, must act trivially on $\mu_{L,2}$. Since $\chi \neq 1$, we deduce from Lemma 2.1(ii) that

$$\hat{H}^q(H, \mu_L \cap U_L^-)(\chi) = 0, \qquad \text{for all } q \in \mathbb{Z}. \tag{4}$$

From the exact sequence $0 \to U_L^+ \to U_L \to U_L^- \to 0$ and the fact that $\chi(\Delta_\mathfrak{p}) \neq 1$ for all primes $\mathfrak{p}$ of k over which primes in L are ramified over K^+, we conclude from Lemma 2.3(ii) that

$$\hat{H}^q(H, U_L^-)(\chi) = 0, \qquad \text{for all } q \in \mathbb{Z}. \tag{5}$$

From the long cohomology sequence of the above sequence we obtain the exact sequence $0 \to U_F^- \to (U_L^-)^H \to H^1(H, U_L^+) \ldots$, which gives us that

$$((U_L^-)^H / U_F^-)(\chi) = 0. \tag{6}$$

From the long cohomology sequence of the exact sequence

$$0 \to \mu_L \cap U_L^- \to U_L^- \to U_L^- / \mu_L \cap U_L^- \to 0$$

we find an exact sequence

$$\cdots \to (U_L^-)^H \to (U_L^- / \mu_L \cap U_L^-)^H \to H^1(H, \mu_L \cap U_L^-) \to \cdots$$

and (4) with $q = 1$ and (6) imply that

$$\mathrm{cok}(U_F^- / \mu_F \cap U_F^- \to (U_L^- / \mu_L \cap U_L^-)^H)(\chi) = 0. \tag{7}$$

From the exact sequence $0 \to C_{L^+} \to C_L \to C_L^- \to 0$ and the fact that $\chi \neq 1$, we conclude by Lemma 2.3(i) that

$$\hat{H}^q(H, C_L^-)(\chi) = 0, \qquad \text{for all } q \in \mathbb{Z} \tag{8}$$

and from the long cohomology sequence of this sequence and the fact that $H^1(H, C_{L^+}) \simeq \hat{H}^{-1}(H, \mathbb{Z}) = 0$ we conclude that

$$(C_L^-)^H = C_F^-. \tag{9}$$

From Lemma 2.4 we obtain the exact sequence

$$0 \to \mu_L \cap U_L^- \to U_L^- \to C_L^- \to \mathrm{Cl}_L^- \to 0$$

and it follows from (4), (5) and (8) that $\hat{H}^q(H, \mathrm{Cl}_L^-)(\chi) = 0$ for all $q \in \mathbb{Z}$ and hence

that $\mathrm{Cl}_{L,2}^{-}(\chi)$ is a cohomologically trivial G-module.

From the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & U_F^-/\mu_F \cap U_F^- & \longrightarrow & C_F^- & \longrightarrow & \mathrm{Cl}_F^- \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & (U_L^-/\mu_L \cap U_L^-)^H & \longrightarrow & (C_L^-)^H & \longrightarrow & (\mathrm{Cl}_L^-)^H \longrightarrow H^1(H, U_L^-/\mu_L \cap U_L^-) \end{array}$$

and (7) and (9) we conclude:

$$\text{The map } \mathrm{Cl}_{F,2}^{-}(\chi) \to (\mathrm{Cl}_{L,2}^{-}(\chi))^H \text{ is injective.} \tag{10}$$

From the diagram

$$\begin{array}{ccccccc} U_L^- & \longrightarrow & C_L^- & \longrightarrow & \mathrm{Cl}_L^- & \longrightarrow & 0 \\ \downarrow{\scriptstyle N_H} & & \downarrow{\scriptstyle N_H} & & \downarrow{\scriptstyle N_H} & & \\ U_F^- & \longrightarrow & C_F^- & \longrightarrow & \mathrm{Cl}_F^- & \longrightarrow & 0 \end{array}$$

and the fact that $(C_F^-/N_H C_L^-)(\chi) = \hat{H}^0(H, C_L^-)(\chi) = 0$, it follows that the map $N_H : \mathrm{Cl}_{L,2}^{-}(\chi) \to \mathrm{Cl}_{F,2}^{-}(\chi)$ is surjective. By (10) the kernel of this map is equal to the kernel of $N_H : \mathrm{Cl}_{L,2}^{-}(\chi) \to \mathrm{Cl}_{L,2}^{-}(\chi)$ which, since $\hat{H}^{-1}(H, \mathrm{Cl}_{L,2}^{-}(\chi)) = 0$, is equal to $I_H \mathrm{Cl}_{L,2}^{-}(\chi)$. This proves (i).

We have already proved that $\mathrm{Cl}_{L,2}^{-}(\chi)$ is cohomologically trivial. When we apply (i) with $H = G$ we find that $\mathrm{Cl}_{L,2}^{-}(\chi)/I_G \mathrm{Cl}_{L,2}^{-}(\chi) \simeq \mathrm{Cl}_{F,2}^{-}(\chi)$. Part (ii) now follows easily from Nakayama's Lemma. □

3. Minus class groups in a special $\mathbb{Z}_2$-extension

In this section we will study the 2-parts of the minus class groups of the fields $\mathbb{Q}(\zeta_{29 \cdot 2^m})$ where $m \in \mathbb{Z}$ is at least 4. We let E denote the subfield of $\mathbb{Q}(\zeta_{29})$ which is of degree 7 over $\mathbb{Q}$ and we put $\Delta = \mathrm{Gal}(E/\mathbb{Q})$.

Lemma 3.1. *Let K be a real number field satisfying $E \subset K \subset \mathbb{Q}(\zeta_{29 \cdot 2^m})$. Suppose $\chi : \Delta \to \overline{\mathbb{Q}}_2^*$ is a non-trivial character. Then*

$$\mathrm{Cl}_{K,2}(\chi) = 0.$$

Proof. We first show that E has class number 1: the root discriminant of E equals $29^{6/7}$ and Odlyzko's discriminant bounds in Diaz y Diaz's tables [4] imply at once that $h(E) = 1$. Next we consider arbitrary K satisfying the conditions stated in the lemma.

Let $G = \mathrm{Gal}(K/E)$; clearly G is a 2-group and $\mathrm{Gal}(K/\mathbb{Q}) \cong \Delta \times G$. The only primes

ramified in K/E are over 2 and 29. Since 29 is ramified in $E/\mathbb{Q}$ and since 2 is inert in this extension it follows from Lemma 2.3 that

$$\hat{H}^q(G, C_K)(\chi) = \hat{H}^q(G, U_K)(\chi) = 0$$

so

$$\hat{H}^q(G, \mathrm{Cl}_{K,2}(\chi)) = \hat{H}^{q+2}(G, 0_K^*)(\chi).$$

Since $\mathrm{Cl}_E = 0$ it follows that

$$0 = \ker(\mathrm{Cl}_E \to \mathrm{Cl}_K) = \ker(H^1(G, 0_K^*) \to H^1(G, U_K))$$

and since $H^1(G, U_K)(\chi) = 0$ we see that

$$H^1(G, 0_K^*)(\chi) = \hat{H}^{-1}(G, \mathrm{Cl}_{K,2}(\chi)) = 0.$$

Now $\hat{H}^{-1}(G, \mathrm{Cl}_{K,2}(\chi)) = \mathrm{Cl}_{K,2}(\chi)/I_G\mathrm{Cl}_{K,2}(\chi)$ because $\mathrm{Cl}_{E,2}(\chi) = 0$. Nakayama's lemma implies that $\mathrm{Cl}_{K,2}(\chi) = 0$ and that proves the lemma. □

Lemma 3.2. *The O_χ-module $\mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi)$ is isomorphic to $O_\chi/2O_\chi$ for one non-trivial character $\chi : \Delta \to \bar{\mathbb{Q}}_2^*$ while it is zero for the, up to $\mathrm{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2)$-conjugacy, only other such character.*

Proof. The only complex number fields contained in $E(\mathrm{i})$ are $\mathbb{Q}(\mathrm{i})$ and $E(\mathrm{i})$ itself. Since $\mathbb{Q}(\mathrm{i})$ has class number one it follows that

$$\mathrm{Cl}^-_{E(\mathrm{i}),2} \cong \mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi_1) \times \mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi_2)$$

where χ_1 and χ_2 denote the, up to $\mathrm{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2)$-conjugacy, two non-trivial characters of Δ. The class group of E, the maximal real subfield of $E(\mathrm{i})$, is trivial by Lemma 3.1. This implies that $\mathrm{Cl}^-_{E(\mathrm{i}),2} = \mathrm{Cl}_{E(\mathrm{i})} = \ker(\mathrm{Cl}_{E(\mathrm{i})} \xrightarrow{N} \mathrm{Cl}_E)$ and we can compute that $\#\mathrm{Cl}^-_{E(\mathrm{i})} = 56$ by calculating the appropriate generalized Bernoulli numbers. Both $\mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi_1)$ and $\mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi_2)$ are modules over $O_{\chi_1} = \mathbb{Z}_2[\mathrm{im}(\chi_1) = \mathrm{im}(\chi_2)] \cong \mathbb{Z}_2[\zeta_7]$, the unique unramified extension of degree 3 of $\mathbb{Z}_2$. The ring O_χ has a residue field with 8 elements and it follows that (say) $\mathrm{Cl}^-_{E(\mathrm{i}),2} = O_\chi/2O_\chi$ and $\mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi_2) = 0$. This proves Lemma 3.2. □

We let $\chi : \Delta \to \bar{\mathbb{Q}}_2^*$ denote the character for which according to Lemma 3.2 we have that $\mathrm{Cl}^-_{E(\mathrm{i}),2} = \mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi) \neq 0$.

Next let $m \in \mathbb{Z}_{\geq 1}$ and let $K = \mathbb{Q}(\zeta_{29 \cdot 2^{m+3}})$ and put $G = \mathrm{Gal}(K/E(\mathrm{i})) \cong \mathrm{Gal}(K/E(\zeta_{2^{m+3}})) \times \mathrm{Gal}(K/\mathbb{Q}(\zeta_{29}, \mathrm{i}))$.

We identify the group ring $O_\chi[G]$ with $O_\chi[[t, T]]/((1+t)^4 - 1, (1+T)^{2^{m+1}} - 1)$ where $1+t$ corresponds to a generator of $\mathrm{Gal}(K/E(\zeta_{2^{m+3}}))$ and $1+T$ to a generator of $\mathrm{Gal}(K/\mathbb{Q}(\zeta_{29}, i))$.

Theorem 3.3. *For $m \in \mathbb{Z}_{\geq 1}$ there is an isomorphism of O_χ-modules*

$$\mathrm{Cl}^-_{K,2}(\chi) \cong O_\chi[t]/((1+t)^4 - 1, 2^m\phi)$$

where $\phi \in O_\chi[t]$ is a polynomial of degree 2 for which $\phi = t^2 \pmod 2$.

Proof. The only primes that ramify in the extension K over $E(\mathrm{i})$ are the primes over 2 and 29; since 2 is inert in E over $\mathbb{Q}$, Theorem 2.7(ii) applies and we find an exact sequence

$$0 \to \Phi \to \Phi \to \mathrm{Cl}^-_{K,2}(\chi) \to 0$$

where Φ is $O_\chi[G]$-free of rank $= \mathrm{rk}_{O_\chi}\mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi)$. By Lemma 3.2, this rank is equal to one and therefore

$$X = \mathrm{Cl}^-_{K,2}(\chi) \cong O_\chi[[t, T]]/((t+1)^4 - 1, (1+T)^{2^{m-1}} - 1, F(t, T)) \tag{11}$$

for some power series $F(t, T)$ in $O_\chi[[t, T]]$. By Theorem 2.5(i) we have

$$\mathrm{Cl}^-_{E(\mathrm{i}),2}(\chi) \cong X/I_G X \cong O_\chi[t, T]/(t, T, F(t, T)) \cong O_\chi/(F(0,0))$$

and Lemma 3.2 gives that $F(0,0) = 2 \cdot \text{unit}$.

Let H denote $\mathrm{Gal}(K/\mathbb{Q}(\zeta_{29\cdot 16})) \subset G$ and let

$$Y = X/I_H X \cong O_\chi[t, T]/((t+1)^4 - 1, (T+1)^4 - 1, F(t, T)).$$

The order of Y is by (3) equal to

$$\underset{O_\chi/\mathbb{Z}_2}{\mathrm{Norm}} \prod_{\zeta^4=1} \prod_{\xi^4=1} F(\zeta - 1, \xi - 1).$$

Since 2 divides $F(0,0)$ we see that

$$\begin{aligned} &2 \text{ divides } F(\zeta-1, \xi-1) && \text{if } \{\zeta, \xi\} \subset \{-1, 1\}, \\ &\mathrm{i}-1 \text{ divides } F(\zeta-1, \xi-1) && \text{otherwise} \end{aligned}$$

and we find that the order of Y is at least

$$\underset{O_\chi/\mathbb{Z}_2}{\mathrm{Norm}} (2^4 \cdot (\mathrm{i}-1)^{16-4}) = 2^{30}.$$

The power of 2 dividing $h^-_{\mathbb{Q}(\zeta_{29\cdot 16})}$ is exactly 2^{30} as one finds in [8] or in the tables in [10]. Since $Y \hookrightarrow \mathrm{Cl}^-_{\mathbb{Q}(\zeta_{29\cdot 16})}$ we conclude that $\# Y = 2^{30}$ and that

$$F(\zeta-1, \xi-1) = \begin{cases} 2 \cdot \text{unit} & \text{if } \{\zeta, \xi\} \subset \{-1, 1\}, \\ (\mathrm{i}-1) \cdot \text{unit} & \text{otherwise} \end{cases} \tag{12}$$

We write $F(t, T) = \sum_{k \geq 0} f_k(t) T^k$ and we have that 2 divides $f_0(0) = F(0,0)$. By the above

$$f_1(0)(\mathrm{i}-1) + f_0(0) \equiv F(0, \mathrm{i}-1) \equiv (\mathrm{i}-1) \cdot \text{unit} \pmod 2$$

so $f_1(0)$ is a unit in O_χ and f_1 is a unit in $O_\chi[[t]]$. Applying Weierstrass' Preparation Theorem to powerseries with coefficients in the complete local ring $O_\chi[[t]]/((1+t)^4 - 1)$ (see [6]) we find that we may assume that $F(t, T) = T - g(t)$ for some

powerseries $g(t) \in O_\chi[[t]]$. Equation (11) now becomes

$$X = O_\chi[[t]]/((1+t)^4 - 1, (g+1)^{2^{m+1}} - 1). \tag{13}$$

We write $g(t) = t \cdot h(t) + g(0)$ and since $g(0) = F(0,0)$ is divisible by 2 we obtain that for $k \geq 2$

$$(g+1)^{2^k} + 1 \equiv g^{2^k} + 2g^{2^{k-1}} + 2 \equiv t^{2^k} h^{2^k} + 2g^{2^{k-1}} + 2 \pmod 4.$$

Since $t^{2^k} \equiv 2t^{2^k - 2} \mod (4, (t+1)^4 - 1)$ we conclude that $(g+1)^{2^k} + 1 = 2 \cdot \text{unit} \pmod{(t+1)^4 - 1}$ and we find that $X = O_\chi[[t]]/((t+1)^4 - 1, 2^{m-1}((g+1)^4 - 1))$. One easily checks that

$$(g+1)^4 - 1 \equiv 2t^2 h^2 (h^2 + 1) \mod (4, (t+1)^4 - 1). \tag{14}$$

Up to a unit we have that $F(i-1, 0) = g(i-1)$ so by (12) that $(i-1)h(0) + g(0) \equiv (i-1) \cdot \text{unit} \pmod 2$. Since $g(0) \equiv 0 \pmod 2$ we find that $h(0) \not\equiv 0 \pmod 2$. Up to a unit we have that $F(i-1, i-1) = (i-1) - g(i-1)$ so by (12) we have $(i-1) \cdot \text{unit} = (i-1) - g(i-1) = (i-1) - (i-1)h(i-1) - g(0) \equiv (i-1)(1 - h(0)) \pmod 2$. We conclude that $h(0) \not\equiv 1 \pmod 2$. And hence from (14) and the Weierstrass Preparation Theorem that $(g+1)^4 - 1 \equiv 2 \cdot \varphi \cdot \text{unit} \mod ((t+1)^4 - 1)$ where φ is a Weierstrass polynomial of degree 2. This proves Theorem 3.3. □

Proposition 3.4. *Let $m \in \mathbb{Z}_{\geq 1}$; The χ-part of the 2-part of the class group of $\mathbb{Q}(\zeta_{29 \cdot 2^{m+3}})$ has a direct summand isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$.*

Proof. Let K denote $\mathbb{Q}(\zeta_{29 \cdot 2^{m+3}})$. Since $\mathrm{Cl}_{K^+,2}(\chi) = 0$ by Lemma 3.1, we see that the χ-part of the 2-part of the class group of K is precisely $\mathrm{Cl}^-_{K,2}(\chi)$. It therefore suffices by Theorem 3.3 to show that

$$X = O_\chi[t]/((1+t)^4 - 1, 2^m \varphi)$$

(where φ is a Weierstrass polynomial of degree 2) has a direct summand isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$. Clearly $X/2^m X \cong (O_\chi/2^m O_\chi)^4$ and since $\varphi \equiv T^2 \pmod 2$ we have that $X/2^{m+1}X \cong (O_\chi/2^m O_\chi)^2 \times (O_\chi/2^{m+1} O_\chi)^2$; since $O_\chi/2^m O_\chi \cong (\mathbb{Z}/2^m\mathbb{Z})^3$, this clearly implies that X has a copy of $\mathbb{Z}/2^m\mathbb{Z}$ as a direct summand. This proves Proposition 3.4. □

4. Proof of the main theorem

In this section we will prove Theorem 1.1, the main result of this paper. The determination of SSF is done in two steps: first the odd part is computed and then the 2-part. The odd part was already done by Lenstra in [7]; the 2-part is computed using Proposition 3.4.

Theorem 4.1. $\bigoplus_{n \geq 1} \mathrm{Pic}(\mathbb{Z}[\zeta_n, 1/n]) \cong \bigoplus_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$.

Proof. For every prime p, the p-part of $\bigoplus_{n\geq 1}\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\bigoplus_{m\geq 1}(\mathbb{Z}/p^m\mathbb{Z})^{(\aleph_0)}$. So, to prove the theorem it suffices to show that for every prime p and every positive integer m there exist infinitely many n such that $\mathbb{Z}/p^m\mathbb{Z}$ is a direct summand of $\mathrm{Pic}(\mathbb{Z}[\zeta_n, 1/n])$. First we consider the case where $p\neq 2$. Let m be a positive integer. By a result of Yamamoto [11] there exists a quadratic number field K with discriminant not divisible by p which has a subgroup of its class group isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$. Let f denote the absolute value of the discriminant of K. It is well known that $K\subset\mathbb{Q}(\zeta_f)$. Let G denote $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$, let $N\subset G$ be the subgroup $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/K)$ and let $\chi:\mathrm{Gal}(K/\mathbb{Q})\to\{\pm 1\}$ denote the non-trivial character of $\mathrm{Gal}(K/\mathbb{Q})$.

The cokernel of the norm map $\mathrm{Cl}_{\mathbb{Q}(\zeta_f)}\to\mathrm{Cl}_K$ is a quotient of $C_K/N(C_{\mathbb{Q}(\zeta_f)})=\hat{H}^0(N,C_K)\simeq\hat{H}^{-2}(N,\mathbb{Z})\simeq N$. Since G is abelian, the canonical action of $\mathrm{Gal}(K/\mathbb{Q})$ on N is trivial. Since $\chi\neq 1$ we conclude that $N_p(\chi)=0$ and therefore that the norm $\mathrm{Cl}_{\mathbb{Q}(\zeta_f),p}(\chi)\to\mathrm{Cl}_{K,p}(\chi)$ is surjective. Since $\mathrm{Cl}_{\mathbb{Q}}=0$ we have that $\mathrm{Cl}_{K,p}=\mathrm{Cl}_{K,p}(\chi)$ and it follows that $\mathrm{Cl}_{\mathbb{Q}(\zeta_f),p}(\chi)$ has a subgroup isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$. Let $G=\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$ and let G_l denote the decomposition group of a prime over l in $\mathbb{Q}(\zeta_f)$. There is an exact sequence of G-modules

$$\coprod_{l\mid f}\mathbb{Z}[G/G_l]\to\mathrm{Cl}_{\mathbb{Q}(\zeta_f)}\to\mathrm{Pic}\,\mathbb{Z}\left[\zeta_f,\frac{1}{f}\right]\to 0.$$

Since all primes that ramify in $\mathbb{Q}(\zeta_f)/\mathbb{Q}$ also ramify in $K/\mathbb{Q}$ we have that $G_l\not\subseteq\ker\chi$ and we conclude that $\mathbb{Z}_p[G/G_l](\chi)=0$ for every $l\mid f$. Tensoring the above exact sequence with $\mathbb{Z}_p$, and taking χ-eigenspaces gives us therefore an isomorphism

$$\mathrm{Cl}_{\mathbb{Q}(\zeta_f),p}(\chi)\cong\mathrm{Pic}\left(\mathbb{Z}\left[\zeta_f,\frac{1}{f}\right]\right)_p(\chi).$$

Suppose $\mathfrak{l}_1,\ldots,\mathfrak{l}_t$ are prime ideals of $\mathbb{Q}(\zeta_f)$ satisfying

(i) Each $\mathfrak{l}_j$ lies over a rational prime $l_j\not\equiv 1\pmod p$.

(ii) The classes of the ideals $\mathfrak{l}_j$ in $\mathrm{Pic}(\mathbb{Z}[\zeta_f,1/f])$ generate the subgroup $(\mathrm{Pic}(\mathbb{Z}[\zeta_f,1/f]))^{p^m}$.

Let L denote the product of the primes l_j. Since $(\mathrm{Pic}(\mathbb{Z}[\zeta_f,1/f]))^{p^m}$ is stable under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$, the classes of all conjugates of the primes $\mathfrak{l}_j$ generate $(\mathrm{Pic}(\mathbb{Z}[\zeta_f,1/f]))^{p^m}$ as well and we conclude that $\mathrm{Pic}(\mathbb{Z}[\zeta_f,1/(fL)])\simeq\mathrm{Pic}(\mathbb{Z}[\zeta_f,1/f])/(\mathrm{Pic}(\mathbb{Z}[\zeta_f,1/f]))^{p^m}$ and therefore also that $\mathrm{Pic}(\mathbb{Z}[\zeta_f,1/(fL)])$ has a direct summand isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$.

It follows from (i) that the degree $[\mathbb{Q}(\zeta_{fL}):\mathbb{Q}(\zeta_f)]$, being a divisor of $\prod_{j=1}^{t}(l_j-1)$, is prime to p. We write $\theta=[\mathbb{Q}(\zeta_{fL}):\mathbb{Q}(\zeta_f)]^{-1}\cdot\mathrm{Norm}$ and we conclude from the commuting diagram

$$\begin{array}{ccc}\mathrm{Pic}\,\mathbb{Z}\left[\zeta_f,\dfrac{1}{fL}\right] & \longrightarrow & \mathrm{Pic}\,\mathbb{Z}\left[\zeta_{fL},\dfrac{1}{fL}\right]\\ \| & \swarrow_{\theta} & \\ \mathrm{Pic}\,\mathbb{Z}\left[\zeta_f,\dfrac{1}{fL}\right] & & \end{array}$$

that $\mathrm{Pic}(\mathbb{Z}[\zeta_{fL}, 1/(fL)])$ has a copy of $\mathbb{Z}/p^m\mathbb{Z}$ as a direct summand.

The proof in the case where $p \neq 2$ is now completed since there are infinitely many sets of primes l_i satisfying conditions (i) and (ii). This is, since $p \neq 2$ and since the intersection of $\mathbb{Q}(\zeta_p)$ and the Hilbert class field of $\mathbb{Q}(\zeta_f)$ is precisely $\mathbb{Q}$, easily implied by the Čebotarev Density Theorem.

Now we finish the proof by taking care of the case where $p = 2$.

By Proposition 3.4 for every integer $m \geq 0$ the group $\mathrm{Cl}_{\mathbb{Q}(\zeta_{29 \cdot 2^{m+3}}),2}(\chi)$ has a direct summand isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$. Here χ denotes the character of conductor 29 and order 7 for which $\mathrm{Cl}_{\mathbb{Q}(\zeta_{29}),2}(\chi) \neq 0$. Put $f = 29 \cdot 2^{m+3}$ and let G denote the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ and let G_2 (resp. G_{29}) denote the decomposition group of a prime over 2 (resp. 29) in $\mathbb{Q}(\zeta_f)$.

There is an exact sequence

$$\mathbb{Z}[G/G_2] \times \mathbb{Z}[G/G_{29}] \to \mathrm{Cl}_{\mathbb{Q}(\zeta_f)} \to \mathrm{Pic}\left(\mathbb{Z}\left[\zeta_f, \frac{1}{f}\right]\right) \to 0.$$

Since 29 ramifies totally in $\mathbb{Q}(\zeta_{29})/\mathbb{Q}$ and since 2 is inert in $\mathbb{Q}(\zeta_{29})/\mathbb{Q}$ it follows, as before, that we have an isomorphism

$$\mathrm{Cl}_{\mathbb{Q}(\zeta_f),2}(\chi) \simeq \mathrm{Pic}\left(\mathbb{Z}\left[\zeta_f, \frac{1}{f}\right]\right)_2(\chi)$$

and we see that $\mathrm{Pic}(\mathbb{Z}[\zeta_f, 1/f])_2$ has a direct summand isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$.

Let k be a positive integer; the degree of the extension $\mathbb{Q}(\zeta_{f \cdot 29^k})/\mathbb{Q}(\zeta_f)$ is a power of 29 and hence odd. It follows that $\mathrm{Pic}(\mathbb{Z}[\zeta_f, 1/f])_2$ is a direct summand of $\mathrm{Pic}(\mathbb{Z}[\zeta_{f \cdot 29^k}, 1/(f \cdot 29^k)])$ and hence that $\mathbb{Z}/2^m\mathbb{Z}$ is a direct summand of $\mathrm{Pic}(\mathbb{Z}[\zeta_n, 1/n])$ for every n of the form $f \cdot 29^k$, $k \in \mathbb{Z}_{\geq 0}$. This proves the theorem. □

Theorem 4.1 combined with Lenstra's result (1) yields Theorem 1.1.

References

[1] H. Bass, Lenstra's calculation of $G_0(R\pi)$, and applications to Morse-Smale diffeomorphisms, In: Integral Representations and Applications, Lecture Notes in Mathematics 882 (Springer, Berlin, 1981) 287–318.

[2] A. Brumer, The class group of all cyclotomic integers. J. Pure Appl. Algebra 20 (1981) 107–111.

[3] J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory (Academic Press, New York, 1967).

[4] F. Diaz y Diaz, Tables minorant la racine n-ième du discriminant d'un corps de degré n, Publ. Math. Orsay 80.06 (Univ. Paris, Orsay, 1980).

[5] J. Franks and M. Shub, The existence of Morse-Smale diffeomorphisms, Topology 20 (1981) 273–290.

[6] S. Lang, Cyclotomic fields, Graduate Texts in Mathematics 59 (Springer, Berlin, 1978).

[7] H.W. Lenstra, Grothendieck groups of abelian group rings, J. Pure Appl. Algebra (1981) 173–193.

[8] G. Schruttka von Rechtenstamm, Tabelle der (Relativ)-Klassenzahlen der Kreiskörper deren φ-Funktion des Wurzelexponenten (Grad) nicht grösser als 256 ist, Abh. Deutschen Akad. Wiss. Berlin, Kl. Math. Phys. 2 (1964) 1–64.

[9] M. Shub and D. Sullivan, Homology theory and dynamical systems, Topology 14 (1975) 109–132.
[10] L.C. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics 83 (Springer, Berlin, 1982).
[11] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7 (1970) 57–76.