MATHEMATICS OF COMPUTATION
Volume 67, Number 223, July 1998, Pages 1225–1245
S 0025-5718(98)00939-9

MINUS CLASS GROUPS OF THE FIELDS OF THE l-TH ROOTS OF UNITY

RENÉ SCHOOF

Abstract. We show that for any prime number $l > 2$ the minus class group of the field of the l-th roots of unity $\overline{\mathbf{Q}_p}(\zeta_l)$ admits a finite free resolution of length 1 as a module over the ring $\widehat{\mathbf{Z}}[G]/(1+\iota)$. Here ι denotes complex conjugation in $G = \mathrm{Gal}(\overline{\mathbf{Q}_p}(\zeta_l)/\overline{\mathbf{Q}_p}) \cong (\mathbf{Z}/l\mathbf{Z})^*$. Moreover, for the primes $l \le 509$ we show that the minus class group is cyclic as a module over this ring. For these primes we also determine the structure of the minus class group.

Introduction

Let l be an odd prime and let ζ_l denote a primitive l-th root of unity. In this paper we study the cyclotomic fields $\mathbf{Q}(\zeta_l)$ and the class groups Cl_l of their rings of integers $\mathbf{Z}[\zeta_l]$. The class group Cl_l splits in a natural way into two parts: the natural map from the class group Cl_l^+ of the ring of integers of the subfield $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ to Cl_l is injective [24, p.40]. Its cokernel, the *minus class group of* $\mathbf{Q}(\zeta_l)$, is denoted by Cl_l^-. There is an exact sequence

$$0 \longrightarrow Cl_l^+ \longrightarrow Cl_l \longrightarrow Cl_l^- \longrightarrow 0.$$

About the groups Cl_l^+ little is known. For small primes l they are trivial [23]. See [3], [21] for a numerical study of these groups. In this paper we consider the other groups, the minus class groups Cl_l^-, which are easier to handle. There is, first of all, an explicit and easily computable formula for their cardinalities h_l^-. See [24, p.42]:

$$h_l^- = 2l \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi},$$

where the product runs over the characters $\chi : (\mathbf{Z}/l\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ which are odd, i.e. which satisfy $\chi(-1) = -1$. The numbers $B_{1,\chi}$ are generalized Bernoulli numbers; they are defined in section 1.

Around 1850, E. E. Kummer [9], [10] used this formula to compute the minus class numbers h_l^- for the primes $l < 100$. These calculations were extended by D. H. Lehmer and J. M. Masley [15] in 1978 to the primes $l \le 509$. The numbers h_l^- grow very rapidly with l. For instance, h_{491}^- already has 138 decimal digits.

The class number h_l^- alone does, of course, not determine the structure of the group Cl_l^-. If h_l^- is squarefree, the group Cl_l^- is cyclic, but in general h_l^- has

Received by the editor March 28, 1994 and, in revised form, December 2, 1996.
1991 *Mathematics Subject Classification.* Primary 11R18, 11R29, 11R34.
Key words and phrases. Cyclotomic fields, class groups, cohomology of groups.

multiple factors. It is a natural problem to try and determine the *structure* of the minus class groups. Kummer [12] addressed this problem in 1853. He showed, for instance, that for $l = 29$ the minus class group is isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$. He claimed moreover that the minus class group of $\mathbf{Q}(\zeta_{31})$ is cyclic of order 9. Only in 1870 he gave a rigorous proof of this fact [11]. It involves a lenghty calculation in the field $\mathbf{Q}(\zeta_{31})$. His claim that the group Cl_{71}^- is cyclic of order $7^2 \cdot 79241$ is correct, but has, as far as I know, never been justified previously [6].

In this paper we study the structure of the minus class groups Cl_l^- as Galois modules. Since complex conjugation ι acts as -1 on Cl_l^-, it is natural to study Cl_l^- as a module over the ring $\widehat{\mathbf{Z}}[G]/(1+\iota)$ where $\widehat{\mathbf{Z}}$ denotes the profinite ring $\varprojlim \mathbf{Z}/n\mathbf{Z}$ and $G = \mathrm{Gal}(\mathbf{Q}(\zeta_l)/\mathbf{Q}) \cong (\mathbf{Z}/l\mathbf{Z})^*$. We prove the following:

Theorem I. *Let l be an odd prime. Then there exist an exact sequence of $\widehat{\mathbf{Z}}[G]/(1+\iota)$-modules*

$$0 \longrightarrow L \xrightarrow{\Theta} L \longrightarrow Cl_l^- \longrightarrow 0$$

where L is free of finite rank over $\widehat{\mathbf{Z}}[G]/(1+\iota)$.

Theorem I is an immediate consequence of Theorems 2.2*(i)* and 3.2*(i)*. For small l we can be more precise:

Theorem II. *For $l \leq 509$ one can take L of rank 1 in Theorem I. In other words, the minus class group is isomorphic to $\widehat{\mathbf{Z}}[G]/(1+\iota,\Theta)$ as a $\widehat{\mathbf{Z}}[G]/(1+\iota)$-module. Moreover, for Θ one can take the modified Stickelberger element introduced in section 1.*

Theorem II is proved in section 4. In the course of the proof we determine completely the structure of the minus class groups Cl_l^- as abelian groups for $l \leq 509$. As an example we mention Cl_{491}^-, which we show to be isomorphic to a product of six cyclic groups:

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/982\mathbf{Z} \times \mathbf{Z}/10802\mathbf{Z} \times \mathbf{Z}/186801892626658241556648 17/ \\ /2058040549987866811619637044179381826025758157958832119412282729825 86/ \\ /25221939971178506931727800584004906\mathbf{Z}.$$

Theorem II probably holds for several other primes l, but is definitely not true in general. It does, for instance, not hold for $l = 3299$. This follows from the fact that, when $l \equiv 3 \pmod 4$, the minus class group Cl_l^- is cyclic over $\widehat{\mathbf{Z}}[G]/(1+\iota)$ if and only if the class group of the quadratic subfield $\mathbf{Q}(\sqrt{-l}) \subset \mathbf{Q}(\zeta_l)$ is a cyclic group. Since the class group of $\mathbf{Q}(\sqrt{-3299})$ is isomorphic to $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}$, the group Cl_{3299}^- is *not* cyclic as a $\widehat{\mathbf{Z}}[G]/(1+\iota)$-module [13, p.80].

Finally, we single out a particularly simple consequence of our results. Roughly speaking, it says that for prime divisors p of $l-1$, the p-part of Cl_l^- is cyclic whenever it is small.

Theorem III. *Let l and p be odd primes and let M denote the p-part of the minus class group of $\mathbf{Q}(\zeta_l)$. If $\#M$ divides $(l-1)^2$, then M is a cyclic group.*

Theorem III is proved in section 2. Applying it with $l = 31$, $p = 3$ and $l = 71$, $p = 7$ respectively we obtain a proof of Kummer's claims. The condition that

$\#M$ divide $(l-1)^2$ cannot be relaxed further: in section 4 we show that the 5-part of the minus class group of $\mathbf{Q}(\zeta_{101})$ is isomorphic to $\mathbf{Z}/125\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$.

Our method is, in some sense, a finite version of Iwasawa theory. It is closely related to V. A. Kolyvagin's work [7]. In order to obtain information about the structure of a certain χ-eigenspace of the p-part of a minus class group, we "deform" the Dirichlet character χ and study the extension L corresponding to $\chi\psi$, where ψ is some character of p-power order. The generalized Bernoulli numbers $B_{1,\chi\psi}$ contain information about the χ-eigenspace of the class group of this extension. This information is obtained by viewing the field L as a "truncated" $\mathbf{Z}_p$-extension and by studying the χ-part of the minus class group of L by mimicking techniques from Iwasawa theory. The main results are Theorem III and the two criteria for cyclicity, Theorems 2.3 and 3.3.

The main difficulty in extending Theorem II to primes $l > 509$ is the size of the class numbers. For larger l one is bound to encounter composite numbers that cannot be factored within reasonable time. Sooner or later one will also encounter χ-parts that are *not* cyclic Galois modules. In these cases the methods of this paper do not apply.

The paper is organized as follows. In section 1 we briefly recall some well known facts concerning $\mathbf{Z}[G]$-modules when G is a finite abelian group. In this section we also discuss some elementary properties of Stickelberger elements and generalized Bernoulli numbers. Even though there are similarities between the structure of the odd and even parts of the minus class groups, the differences are sufficiently big to merit separate treatment. In section 2 we consider the p-parts of minus class groups for odd primes p. In section 3 we do the same for $p = 2$. Finally, in section 4, we present the numerical results and prove Theorem II.

We need to know the complete prime decomposition of the class numbers h_l^- for $l \leq 509$. In the appendix a table of the prime factorizations of these numbers is given. This table is complete and supersedes the one computed by Lehmer and Masley [15]. The present table contains also the factorizations of the unfactored composite numbers in their table. I thank Arjen Lenstra, Peter Montgomery, Bob Silverman and Herman te Riele for computing the unknown prime factors, François Morain for several primality proofs and Pietro Cornacchia for catching an error in Table 4.4.

1. Preliminaries

In this section we recall some elementary facts concerning modules over group rings $\mathbf{Z}[G]$ when G is a finite abelian group. In addition we recall some basic properties of Stickelberger elements and generalized Bernoulli numbers.

Let G be a finite abelian group. For a G-module M, we denote by M^G the subgroup of G-invariant elements of M. Now fix a prime p and let

$$G \cong \pi \times \Delta,$$

where π is the p-part of G and Δ is the maximal subgroup of G of order prime to p. We write the group ring $\mathbf{Z}_p[G]$ as $\mathbf{Z}_p[\Delta][\pi]$. By the orthogonality relations there is an isomorphism of rings

$$\mathbf{Z}_p[\Delta] \cong \prod_{\chi} O_\chi.$$

Here χ runs over the characters $\chi : \Delta \longrightarrow \overline{\mathbf{Q}}_p^*$ up to $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-conjugacy. The rings O_χ are unramified extensions of $\mathbf{Z}_p$ generated by the values of χ. They are $\mathbf{Z}_p[\Delta]$-algebras via the rule $\sigma \cdot x = \chi(\sigma)x$ for $x \in O_\chi$ and $\sigma \in \Delta$. The ring isomorphism is given by mapping $\sigma \in \Delta$ to $\chi(\sigma)$ in each component O_χ. The residue field of O_χ is $\mathbf{F}_p(\zeta_d)$ where d is the order of χ.

Definition. Let M be a $\mathbf{Z}_p[G]$-module and let $\chi : \Delta \longrightarrow \overline{\mathbf{Q}}_p^*$ be a character. Equivalently, χ is a character of G of order prime to p. The χ-*eigenspace* $M(\chi)$ or χ-*part* of M is defined by

$$M(\chi) = M \otimes_{\mathbf{Z}_p[\Delta]} O_\chi.$$

We have a decomposition into eigenspaces of M:

$$M \cong \prod_\chi M(\chi),$$

where χ runs over the characters $\chi : \Delta \longrightarrow \overline{\mathbf{Q}}_p^*$ up to $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-conjugacy. Each eigenspace $M(\chi)$ is a module over the local ring $O_\chi[\pi]$. The residue field of this ring is equal to the residue field of O_χ which is $\mathbf{F}_p(\zeta_d)$, where d is the order of χ.

We frequently use the following properties of the Tate cohomology groups [2]. Let M be a G-module and let $P \subset \pi$. The natural action of P on the Tate cohomology groups $\widehat{H}^q(P, M)$ is trivial, but Δ acts, in general, in a non-trivial way. Note that the groups $\widehat{H}^q(P, M)$ are $\mathbf{Z}_p[\Delta]$-modules, because they are killed by $\#P$.

Lemma 1.1. *Let p be a prime and let G be a finite abelian group. Let π and Δ be as above and let P be a subgroup of π.*

(i) For every $\mathbf{Z}[G]$-module M we have that $\widehat{H}^q(P, M^\Delta) \cong \widehat{H}^q(P, M)^\Delta$ for all $q \in \mathbf{Z}$.

(ii) For every $\mathbf{Z}_p[G]$-module M and every character $\chi : \Delta \longrightarrow \overline{\mathbf{Q}}_p^*$ we have that

$$\widehat{H}^q(P, M(\chi)) \cong \widehat{H}^q(P, M)(\chi) \qquad \text{for all } q \in \mathbf{Z}.$$

Proof. *(i)* Since the actions of Δ and P commute, the inclusion $i : M^\Delta \hookrightarrow M$ and the Δ-norm map $N : M \to M^\Delta$ are P-morphisms. The maps $i \cdot N$ and $N \cdot i$ induce multiplication by $\#\Delta$ on $\widehat{H}^q(P, M)^\Delta$ and $\widehat{H}^q(P, M^\Delta)$ respectively. Since $\#\Delta$ and $\#P$ are coprime, multiplication by $\#\Delta$ is an isomorphism and *(i)* follows.

(ii) Since the actions of Δ and P commute, the eigenspaces $M(\chi)$ are P-modules. Taking the sum over the characters $\chi : \Delta \longrightarrow \overline{\mathbf{Q}}_p^*$, up to $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-conjugacy, of the natural maps $\widehat{H}^q(P, M(\chi)) \longrightarrow \widehat{H}^q(P, M)(\chi)$, we obtain precisely the map $\bigoplus_\chi \widehat{H}^q(P, M(\chi)) \longrightarrow \widehat{H}^q(P, M)$ induced by the isomorphism $\bigoplus_\chi M(\chi) \longrightarrow M$. This proves *(ii)*. ☐

The remainder of this section is devoted to properties of Stickelberger elements and generalized Bernoulli numbers. Let $f \not\equiv 2 \pmod 4$ be a conductor and let $G = (\mathbf{Z}/f\mathbf{Z})^*$. The *Stickelberger element* θ_f of conductor f is given by

$$\theta_f = \sum_{\substack{a=1 \\ \gcd(a,f)=1}}^{f} \left(\frac{a}{f} - \frac{1}{2}\right) [a]^{-1} \in \mathbf{Q}[G].$$

For any prime number p we write $G = \pi \times \Delta$ as above. We have $\mathbf{Q}_p[G] \cong \bigoplus_\chi K_\chi[\pi]$ where the sum runs over the characters $\chi : \Delta \longrightarrow \overline{\mathbf{Q}}_p^*$ up to $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-conjugacy and K_χ is the quotient field of O_χ. We denote the algebra homomorphism

$\mathbf{Q}_p[G] \longrightarrow K_\chi[\pi]$ induced by χ again by χ. For every character $\chi \neq \omega$, the image $\frac{1}{2}\chi(\theta_f)$ of $\frac{1}{2}\theta_f$ in $K_\chi[\pi]$ is an element of the subring $O_\chi[\pi]$. Here $\omega : (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow \overline{\mathbf{Q}}_p^*$ denotes the Teichmüller character. It is the character that gives the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the group μ_p of p-th roots of unity. Note that $\omega = 1$ when $p = 2$. For odd p the element $\frac{1}{2}\theta_f$ annihilates the χ-part of the p-part of the ideal class group of $\mathbf{Q}(\zeta_f)$. This is Stickelberger's Theorem [24, Chpt.6]. For $p = 2$, C. Greither [4] has shown the same when π is cyclic and the conductor f is odd.

For any character φ of G of conductor f, the generalized Bernoulli number $B_{1,\varphi}$ is simply the value of the algebra homomorphism $\mathbf{Q}_p[G] \longrightarrow \overline{\mathbf{Q}}_p$ induced by φ evaluated on the Stickelberger element:

$$B_{1,\varphi} = \varphi(\theta_f) = \sum_{\substack{a=1 \\ \gcd(a,f)=1}}^{f} \left(\frac{a}{f} - \frac{1}{2}\right) \varphi(a)^{-1} \in \overline{\mathbf{Q}}_p.$$

Finally we assume that $f = l$ is prime, so that $G = (\mathbf{Z}/l\mathbf{Z})^*$ and we introduce the modified Stickelberger element $\Theta \in \widehat{\mathbf{Z}}[G]/(1+\iota)$ that occurs in Theorem II. We have that $\widehat{\mathbf{Z}}[G]/(1+\iota) \cong \prod_p \mathbf{Z}_p[G]/(1+\iota)$. Moreover, each factor $\mathbf{Z}_p[G]/(1+\iota)$ is isomorphic to $\prod_\chi O_\chi[\pi_p]$, where the χ run over all odd characters of order prime to p when p is odd and all characters of odd order when $p = 2$ respectively. Here π_p denotes the p-part of G. Therefore it suffices to describe the various components $\chi(\Theta)$ of Θ: if $p = l$ and $\chi = \omega$ or if $p = 2$ and $\chi = 1$, we let $\chi(\Theta) = 1$. In all other cases $\chi(\Theta) = \frac{1}{2}\chi(\theta_l)$.

The modified Stickelberger element $\Theta \in \widehat{\mathbf{Z}}[G](1+\iota)$ annihilates Cl_l^-. The order of $\widehat{\mathbf{Z}}[G](1+\iota, \Theta)$ is equal to the minus class number h_l^-.

2. Odd primes p

In this section we study the p-parts of the minus class groups of complex abelian number fields for odd primes p. We show that certain eigenspaces of these groups are cohomologically trivial Galois modules. This puts restraints on their structure. We derive an easily applicable criterion for these eigenspaces to be cyclic Galois modules.

In this section $p \neq 2$ is a prime. We fix a complex abelian number K field with $G = \mathrm{Gal}(K/\mathbf{Q})$. Let π denote the p-part of G and $F = K^\pi$ its fixed field. We fix an odd character $\chi : G \longrightarrow \overline{\mathbf{Q}}_p{}^*$ of order prime to p, which is not equal to the Teichmüller character ω . Since $p \neq 2$, we have that $Cl_K^-(\chi) = Cl_K(\chi)$. Therefore we work, in this section, with the class group Cl_K itself rather than the minus class group Cl_K^-.

Theorem 2.1. *Let $P \subset G$ be a subgroup of π with fixed field $E = K^P$. Suppose that that for all primes r that are ramified in $E \subset K$ we have that $\chi(r) \neq 1$. Then*

(i) the eigenspace $Cl_K(\chi)$ is a cohomologically trivial $O_\chi[P]$-module;

(ii) the natural map $Cl_E(\chi) \longrightarrow Cl_K(\chi)^P$ is bijective and the norm map $Cl_K(\chi) \longrightarrow Cl_E(\chi)$ is surjective.

Proof. *(i)* It suffices to show that $\widehat{H}^q(P, Cl_K(\chi)) = 0$ for all $q \in \mathbf{Z}$. Let O_K denote the ring of integers of K, let C_K denote the idèle class group of K and let U_K denote the group of unit idèles, i.e. the group of K-idèles that have trivial valuation at all finite primes. We have the exact sequence of G-modules [2]

$$0 \longrightarrow O_K^* \longrightarrow U_K \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 0.$$

We show that the χ-parts of the Tate P-cohomology groups of these modules are all zero. For the unit group O_K^* we have the following exact sequence [24, p.39]

$$0 \longrightarrow \{1,-1\} \longrightarrow \mu_K \times O_{K^+}^* \longrightarrow O_K^* \longrightarrow Q \longrightarrow 0.$$

Here O_{K^+} is the ring of integers of the maximal real subfield K^+ of K and μ_K denotes the group of roots of unity in K. The group Q has order at most 2. Complex conjugation acts trivially on $\{1,-1\}$, on Q and on $O_{K^+}^*$. Since χ is an odd character, we have, by Lemma 1.1, that $\widehat{H}^q(P, O_K^*)(\chi) \cong \widehat{H}^q(K, \mu_K)(\chi)$ for all $q \in \mathbf{Z}$. Since χ is not the Teichmüller character, the χ-part of μ_K is zero so that, by Lemma 1.1, $\widehat{H}^q(P, O_K^*)(\chi) = 0$ for all $q \in \mathbf{Z}$.

By *global* class field theory there are natural isomorphisms $\widehat{H}^q(P, C_K) \cong \widehat{H}^{q-2}(P, \mathbf{Z})$ for all $q \in \mathbf{Z}$. Since G acts trivially on $\mathbf{Z}$, it follows from Lemma 1.1 that $\widehat{H}^q(P, C_K)(\chi) = 0$ for all $q \in \mathbf{Z}$.

We use *local* class field theory to compute the cohomology of U_K. See also [20]. By Shapiro's lemma we have

$$\widehat{H}^q(P, U_K) \cong \bigoplus_v \widehat{H}^q(P_r, O_w^*) = \bigoplus_r \bigoplus_{v|r} \widehat{H}^q(P_r, O_w^*)$$

where v runs over the prime ideals of E and r runs over ordinary prime numbers. The ring O_w is the ring of integers of the completion K_w of K at a prime w of K over v. We have $\mathbf{Q}_r \subset E_v \subset K_w$ with Galois groups $G_r = \mathrm{Gal}(K_w/\mathbf{Q}_r)$, $P_r = \mathrm{Gal}(K_w/E_v)$ and $H_r = \mathrm{Gal}(E_v/\mathbf{Q}_r)$. Since G is abelian, the decomposition groups P_r and H_r only depend on the prime r. Since $\widehat{H}^q(P_r, O_w^*)$ vanishes when v is unramified in K, it suffices to consider only primes r that are ramified in $E \subset K$. For each prime ideal v of F dividing a ramified prime r, there is an exact sequence of G_r-modules

$$0 \longrightarrow O_w^* \longrightarrow K_w^* \longrightarrow \mathbf{Z} \longrightarrow 0.$$

Consider the long exact sequence of Tate P_r-cohomology groups. By Lemma 1.1, the group H_r acts trivially on the cohomology groups $\widehat{H}^q(P_r, \mathbf{Z})$. By local class field theory there are natural isomorphisms $\widehat{H}^q(P_r, K_w^*) \cong \widehat{H}^{q-2}(P_r, \mathbf{Z})$ for all $q \in \mathbf{Z}$, so that H_r also acts trivially on the groups $\widehat{H}^q(P_r, K_w^*)$. Let Δ_r denote the maximal subgroup of H_r of order prime to p. Then Δ_r and P_r have coprime orders, so that the long cohomology sequence remains exact when we take Δ_r-invariants. It follows that $\widehat{H}^q(P_r, O_w^*)$ is Δ_r-invariant. Therefore Δ_r acts trivially on the sum $\bigoplus_{v|r} \widehat{H}^q(P_r, O_w^*)$. Since $\chi(r) \neq 1$ for all ramified primes r, we see that $\Delta_r \not\subset \ker(\chi)$. This implies that the χ-part of $\bigoplus_{v|r} \widehat{H}^q(P_r, O_w^*)$ is zero.

It follows that $\widehat{H}^q(G, U_K)(\chi) = 0$ for all $q \in \mathbf{Z}$. Combining all this and using Lemma 1.1 one more time, we deduce that $\widehat{H}^q(P, Cl_K(\chi)) = 0$ for all $q \in \mathbf{Z}$. This proves *(i)*.

(ii) It is easy to see that the natural map $C_E/N(C_K) \longrightarrow\!\!\!\!\rightarrow Cl_E/N(Cl_K)$ is surjective. Since $\chi \neq 1$, the group $C_E/N(C_K) = \widehat{H}^0(P, C_K) \cong \widehat{H}^{-2}(P, \mathbf{Z})$ has trivial χ-part, and it follows that the norm map $N : Cl_K(\chi) \longrightarrow\!\!\!\!\rightarrow Cl_E(\chi)$ is surjective. Notice that in order to prove surjectivity of this norm map we have not really used the condition on χ, but merely the fact that χ is not trivial.

The P-cohomology groups of each module in the exact sequence $0 \longrightarrow O_K^* \longrightarrow U_K \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 0$ have trivial χ-parts. Since the natural maps $O_E^* \rightarrow {O_K^*}^P$, $U_E \rightarrow U_K^P$ and $C_E \rightarrow C_K^P$ are all isomorphisms, so is $Cl_E(\chi) \rightarrow Cl_K(\chi)^P$. This proves *(ii)*. □

Theorem 2.2. *If for all primes r that are ramified in $F \subset K$ we have that $\chi(r) \neq 1$, then*

(i) there is an exact sequence of $O_\chi[\pi]$-modules

$$0 \longrightarrow O_\chi[\pi]^d \xrightarrow{\Theta} O_\chi[\pi]^d \longrightarrow Cl_K(\chi) \longrightarrow 0$$

where d is the O_χ-rank of $Cl_F(\chi)$;

(ii) we have

$$\#Cl_K(\chi) = \#O_\chi/(\prod_\psi B_{1,\chi^{-1}\psi})$$

where ψ runs over all characters $\psi : \pi \longrightarrow \overline{\mathbf{Q}}_p^{\,*}$.

Proof. By Nakayama's lemma there is a surjective $O_\chi[\pi]$ morphism $O_\chi[\pi]^d \twoheadrightarrow Cl_K(\chi)$. By Theorem 2.1, the class group $Cl_K(\chi)$ and hence the kernel of this map are cohomologically trivial. Now one copies the proof of [2, p.113, Thm.8] with $\mathbf{Z}$ replaced by the discrete valuation ring O_χ. It follows that the kernel is a projective $O_\chi[\pi]$-module. Since $O_\chi[\pi]$ is local, the kernel is therefore free. It has rank d since it is of finite index in $O_\chi[\pi]^d$. This proves *(i)*.

Part *(ii)* is a generalization of the Theorem of B. Mazur and A. Wiles [7], [16], [17], [18]. By D. Solomon's Theorem [22, p.472], we have for every subgroup $P \subset \pi$ with cyclic quotient π/P,

$$\#Cl_{K^P}(\chi)[N_{P'}/N_P] = \#O_\chi/(\prod_{ker\ \psi = P} B_{1,\chi^{-1}\psi}).$$

Here the ψ run over the characters of G for which $\ker \psi = P$. Here P' denotes the unique subgroup of π containing P as a subgroup of index p and N_P and $N_{P'}$ denote the norm maps $\sum_{\sigma \in P} \sigma$ and $\sum_{\sigma \in P'} \sigma$ respectively. In the exceptional case $P = \pi$ the group P' is not defined and we simply put $N_{P'} = 0$. By $Cl_K^P[N_{P'}/N_P]$ we denote the kernel of the relative norm map $N_{P'}/N_P$ from the class group $Cl_{K^P}(\chi)$ to itself.

Put $S_\chi = \prod_P N_P O_\chi[\pi]/N_{P'} O_\chi[\pi]$. Here P runs over the subgroups of π with cyclic quotient π/P. The natural map

$$g : O_\chi[\pi] \longrightarrow S_\chi$$

becomes an isomorphism when we take the tensor product with the quotient field K_χ of O_χ. Therefore g is injective and has finite cokernel.

All modules occurring in the exact sequence of part *(i)* are cohomologically trivial. Therefore it remains exact when we apply the functor $\prod_P N_P(-)/N_{P'}(-)$ to it. We obtain the following diagram with exact rows.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & O_\chi[\pi]^d & \xrightarrow{\Theta} & O_\chi[\pi]^d & \longrightarrow & Cl_K(\chi) & \longrightarrow & 0 \\
 & & \downarrow g & & \downarrow g & & \downarrow & & \\
0 & \longrightarrow & S_\chi^d & \longrightarrow & S_\chi^d & \longrightarrow & \prod_P N_P Cl_K(\chi)/N_{P'} Cl_K(\chi) & \longrightarrow & 0
\end{array}$$

Theorem 2.1*(i)* and *(ii)* and an application of the snake lemma then gives that

$$\#Cl_K(\chi) = \prod_P \#(N_P Cl_K(\chi)/N_{P'} Cl_K(\chi)) = \prod_P \#(Cl_{K^P}(\chi)[N_{P'}/N_P])$$

and the result follows from Solomon's Theorem. □

It is not difficult to express the order of $Cl_K(\chi)$ in terms of the matrix Θ of Theorem 2.1*(i)*. One has [1, III, sect.9, Prop.6]

$$\#Cl_K(\chi) = \#O_\chi/(\prod_\psi \psi(\det(\Theta))).$$

Here ψ runs over the characters of π, and $\psi(\det(\Theta))$ indicates the value of the natural extension of ψ to an algebra homomorphism $O_\chi[\pi] \longrightarrow \overline{\mathbf{Q}}_p$ on $\det(\Theta) \in O_\chi[\pi]$.

Next we deduce a sufficient condition for the eigenspace $Cl_K(\chi)$ to be a cyclic $O_\chi[\pi]$-module.

Theorem 2.3. *Suppose that for all primes r that are ramified in $F \subset K$ we have that $\chi(r) \neq 1$. If one of the following conditions holds:*

- *$B_{1,\chi^{-1}} = pu$ for some unit $u \in O_\chi^*$;*
- *there exists a character $\varphi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \overline{\mathbf{Q}}_p^{\,*}$ of order $p^k > 1$ such that $B_{1,\chi^{-1}\varphi} = (1-\zeta_{p^k})u$ for some unit u in $O_\chi[\zeta_{p^k}]$,*

then there is an isomorphism of $O_\chi[\pi]$-modules

$$Cl_K(\chi) \cong O_\chi[\pi]/(\theta_\chi).$$

In particular, $Cl_K(\chi)$ is a cyclic $O_\chi[\pi]$-module.

Proof. We first show that $Cl_F(\chi)$ is a cyclic O_χ-module. If $B_{1,\chi^{-1}} = pu$ for some unit $u \in O_\chi^*$, it follows from Theorem 2.2*(ii)* that $\#Cl_F(\chi)$ is equal to the order of the residue field $O_\chi/(p)$. Therefore $Cl_F(\chi)$ is cyclic over O_χ.

In the other case, let $E = \overline{\mathbf{Q}}^{\ker\varphi} F$ and let $P = \mathrm{Gal}(E/F)$. Then P is cyclic and we let $F \subset E' \subset E$ be the unique subfield of E of index p. Since $\varphi \neq 1$, it follows from Theorem 2.1*(ii)* that the norm map $N_{E/E'} : Cl_E(\chi) \longrightarrow Cl_{E'}(\chi)$ is surjective. To compute the order of the kernel of $N_{E/E'}$, we observe that

$$\mathrm{Norm}(B_{1,\chi^{-1}\varphi}) = \mathrm{Norm}(1-\zeta_{p^k}) = p$$

(here the Norm is the $\mathbf{Q}_p(\zeta_{p^k})/\mathbf{Q}_p$-norm). By Solomon's Theorem [22, Thm. II, 1], we conclude that $Cl_E(\chi)[N_{E/E'}]$ has the same order as the residue field $O_\chi/(p)$ of R_χ. Therefore so does $Cl_E(\chi)/(N_{E/E'})$. By Nakayama's lemma, $Cl_E(\chi)$ is therefore cyclic over the group ring $O_\chi[P]$. It follows that $Cl_F(\chi)$ is cyclic over O_χ in this case as well.

To complete the proof, we observe that, by Theorem 2.1, $Cl_K(\chi)$ is cohomologically trivial and the π-norm map induces an O_χ-isomorphism between $Cl_F(\chi)$ and $Cl_K(\chi)$ modulo the augmentation ideal of $O_\chi[\pi]$. It follows from Nakayama's lemma that $Cl_K(\chi)$ is cyclic over $O_\chi[\pi]$. By Stickelberger's theorem there is therefore a surjection $O_\chi[\pi]/(\theta_\chi) \longrightarrow\!\!\!\!\rightarrow Cl_K(\chi)$, which is an isomorphism because both groups have the same order by Theorem 2.2. This proves Theorem 2.3. □

In the case the p-group π is cyclic of order p^e, say, we can be a little bit more explicit. We have the usual isomorphism of local rings, familiar in Iwasawa theory

$$O_\chi[\pi] \cong O_\chi[T]/((1+T)^{p^e}-1),$$

where $1+T$ corresponds to some generator of π. The maximal ideal of this local ring is (T,p). For $i \geq 0$, we let $\omega_i(T) = (1+T)^{p^i}-1$.

By the Weierstrass Preparation theorem [24], every non-zero $f(T) \in O_\chi[[T]]/((1+T)^{p^e}-1)$ is the residue class of a polynomial of the form $p^\mu u(T)h(T)$ where μ is a non-negative integer, $u(T)$ a unit and $h(T) = T^\lambda + a_{\lambda-1}T^{\lambda-1} + \ldots + a_1T + a_0$ is a *Weierstrass polynomial* of degree $\lambda < p^e$. This means that $a_i \equiv 0 \pmod p$ for $i = 0, 1, \ldots, \lambda-1$.

Proposition 2.4. *Suppose that for all primes r that are ramified in $F \subset K$ we have that $\chi(r) \neq 1$. Suppose that the Galois group π is cyclic of order p^e and that $Cl_F(\chi)$ is a cyclic O_χ-module. If for some character ψ of π of order p, for some $\lambda < p-1$ and for some unit $u \in O_\chi[\zeta_p]$, we have that $B_{1,\chi^{-1}\psi} = (1-\zeta_p)^\lambda u$, then*

$$Cl_K(\chi) \cong (O_\chi/(p^e))^{\lambda-1} \times O_\chi/(p^e B_{1,\chi^{-1}})$$

as an O_χ-module.

Proof. We write $O_\chi[\pi] = O_\chi[T]/(\omega_e(T))$ as above. Since $Cl_F(\chi)$ is a cyclic O_χ-module, it follows from Theorem 2.1 that the eigenspace $Cl_K(\chi)$ is a cohomologically trivial cyclic $O_\chi[\pi]$-module. Therefore $Cl_K(\chi) \cong O_\chi[\pi]/(p^\mu f(T))$ for some Weierstrass polynomial $f(T)$. Since $Cl_F(\chi) \cong O_\chi[\pi]/(T) \cong O_\chi/(p^\mu f(0))$, we have that $p^\mu f(0) = B_{1,\chi^{-1}}$, up to a p-adic unit. Similarly, for the subfield $F \subset E \subset K$ of degree p over F we have that $Cl_E \cong O_\chi[T]/(f(T), \omega_1(T))$. Applying Solomon's Theorem [22, Thm. II, 1], we find that, up to a p-adic unit, $f(1-\zeta_p) = B_{1,\chi^{-1}\psi} = (1-\zeta_p)^\lambda$.

Since $\lambda < p-1$, this implies $\mu = 0$ and $\deg(f) = \lambda$. Since $O_\chi[T]/(f(T), \omega_e(T))$ is cohomologically trivial, we have the following exact sequence

$$0 \longrightarrow O_\chi[T]/(f(T), \omega_e(T)/T) \xrightarrow{T} O_\chi[T]/(f(T), \omega_e(T)) \longrightarrow O_\chi/(f(0)) \longrightarrow 0.$$

We analyze the ideal $(f(T), \omega_e(T)/T)$. Consider for $0 \leq i < e$ the quotient

$$\frac{\omega_{i+1}(T)}{\omega_i(T)} = (1+T)^{p^i(p-1)} + \ldots + (1+T)^{p^i} + 1.$$

Since $\lambda < p-1$ we have that $T^{p-1} \equiv Tpg(T) \pmod{f(T)}$ for some polynomial $g(T) \in O_\chi[T]$. This implies that $\omega_{i+1}/\omega_i = p + pTh(T)$ for some $h(T) \in O_\chi[T]$. Therefore

$$\frac{\omega_e(T)}{T} = \prod_{i=0}^{e-1} \frac{\omega_{i+1}}{\omega_i} \equiv p^e \cdot u(T) \pmod{f(T)}$$

where $u(T)$ is some unit in $O_\chi[T]/(\omega_e(T))$. This shows that the ideals $(f(T), \omega_e(T)/T)$ and $(f(T), p^e)$ are equal and that there is an isomorphism of O_χ-modules

$$O_\chi[T]/(f(T), \omega_e(T)/T) \cong (O_\chi/p^e O_\chi)^\lambda.$$

To complete the proof, we observe that $f(0) \in O_\chi[T]/(f(T), \omega_e(T))$ is the image of

$$\frac{f(T)-f(0)}{T} \in O_\chi[T]/(f(T), \omega_e(T)/T) = O_\chi[T]/(f(T), p^e),$$

under the multiplication by T map. Since f is monic, this implies that $f(0)$ has order p^e. Therefore $1 \in O_\chi[T]/(\omega_e(T), f(T))$ has, up to p-adic unit, order $f(0)p^e$.

This completes the proof $\square$

The following simple result often suffices to determine the structure of the p-part of the minus class group of $\mathbf{Q}(\zeta_l)$ when p divides $l-1$. Note that the proof does not rely on the theorems of Mazur-Wiles, Kolyvagin or Solomon.

Theorem III. *Let l and p be odd primes and let M be the p-part of the minus class group of $\mathbf{Q}(\zeta_l)$. If $\#M$ divides $(l-1)^2$, then M is a cyclic group.*

Proof. Let π denote the p-part of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_l)/\mathbf{Q})$; it is a cyclic group of order p^e. Let F be the fixed field of π, let χ be a character of G of order prime to p and let $M(\chi)$ be the corresponding eigenspace of M. We assume that $M(\chi) \neq 0$. Since the condition of Theorem 2.1 is satisfied for $K = \mathbf{Q}(\zeta_l)$, there is an exact sequence

$$0 \longrightarrow O_\chi[\pi]^d \xrightarrow{\Theta} O_\chi[\pi]^d \longrightarrow M(\chi) \longrightarrow 0,$$

where d is the O_χ-rank of $Cl_F(\chi)$. Let $q = p^a$ denote the number of elements in the residue field of O_χ. We write $\det(\Theta) = p^\mu u(T) f(T) \in O_\chi[\pi] \cong O_\chi[T]/(\omega_e(T))$ for some Weierstrass polynomial $f(T) = T^\lambda + a_{\lambda-1}T^{\lambda-1} + \ldots + a_1 T + a_0$ and some unit $u(T)$. Then $\#M(\chi) = \#O_\chi/(\prod_{\zeta^{p^e}=1} p^\mu f(\zeta - 1))$, so that

$$\#M(\chi) \geq q^{\mu p^e + \min(\lambda, p-1)e+1}$$

and hence

$$2e \geq a(\mu p^e + \min(\lambda, p-1)e + 1).$$

Since $2e < p^e + 1$, we have $\mu = 0$. Since $M(\chi) \neq 0$, this implies that $\lambda > 0$. Moreover, since $a \cdot \min(\lambda, p-1) < 2$, we have that $\lambda = 1$ and $a = 1$ so that $O_\chi = \mathbf{Z}_p$. This shows that, up to a unit, $f(T) = \det(\Theta) = T - \beta$ for some $\beta \in p\mathbf{Z}_p$. Since d is the O_χ-rank of $Cl_F(\chi)$, any surjection $O_\chi[\pi]^d \twoheadrightarrow Cl_l(\chi)$ is an isomorphism modulo the maximal ideal $\mathfrak{m}$ of the local ring $O_\chi[\pi]$. This implies that all entries of the matrix Θ are contained in $\mathfrak{m}$ so that $\det(\Theta) \in \mathfrak{m}^d$.

It follows that $d = 1$, so that $M(\chi) \cong \mathbf{Z}_p[T]/((1+T)^{p^e} - 1, T - \beta) \cong \mathbf{Z}_p/p^e\beta\mathbf{Z}_p$ is a cyclic group. We conclude the proof by observing that $\#M(\chi) \geq p^{e+1}$, so that only one eigenspace $M(\chi)$ is non-trivial and hence $M = M(\chi)$. $\square$

3. The 2-part

In this section we study the 2-part of the minus class group of a complex abelian number field K. We show that certain eigenspaces of the 2-part are cohomologically trivial Galois modules. This has consequences for their structure. Finally we prove a criterion for cyclicity of these eigenspaces as Galois modules.

Let $G = \mathrm{Gal}(K/\mathbf{Q})$, let $\iota \in G$ denote complex conjugation and let K^+ denote the fixed field of ι. We have inclusions of idèle class groups $C_{K^+} \subset C_K$ and of idèle unit groups $U_{K^+} \subset U_K$. There is a natural map $Cl_{K^+} \longrightarrow Cl_K$. We define

$$U_K^- = U_K/U_{K^+},$$
$$C_K^- = C_K/C_{K^+},$$
$$Cl_K^- = Cl_K/\mathrm{im}\, Cl_{K^+},$$
$$\mu_K^- = \mu_K \cap U_K^-.$$

Note that U_K^- is isomorphic to the submodule $U_K^{1-\iota}$ of U_K. The intersection $\mu_K \cap U_K^-$ is taken inside U_K.

A diagram chase involving the exact sequence $0 \longrightarrow O_K^* \longrightarrow U_K \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 0$ and the analogous sequence for K^+ shows that there is an exact sequence [19]

$$0 \longrightarrow \mu_K^- \longrightarrow U_K^- \longrightarrow C_K^- \longrightarrow Cl_K^- \longrightarrow 0.$$

It is important to use the definition of the minus class group Cl_K^- that we give here. Often the minus class group of an abelian number field K is defined to be the kernel of the norm map $N : Cl_K \longrightarrow Cl_{K^+}$. The present definition differs at most in the 2-part. It has several advantages: as we will see below, it is easy to compute the Galois cohomology of Cl_K^-; the results for the 2-part are very similar to the results for the odd parts. I don't know how to do the calculations using the other definition.

Another advantage over the usual definition is the following. It is easy to deduce the following formula for the order of Cl_K^- from the usual class number formula:

$$\#Cl_K^- = \frac{2}{[\mu_K : \mu_K^-]} \#\mu_K \prod_{\chi\ odd} -\frac{1}{2} B_{1,\chi}.$$

This formula does not involve the unit index "Q_K" of Hasse [5, Ch.20], which is, in general, difficult to compute. This time there is the factor $2/[\mu_K : \mu_K^-]$, which is either 1 or 2, but this quantity is easy to compute; it captures, in some sense, only the easy aspects of the unit index Q_K and its calculation is precisely the content of Hasse's Satz 22 in [5].

In this secton we fix a complex abelian number field K with $G = \mathrm{Gal}(K/\mathbf{Q})$. Let π be the 2-part of G with fixed field $k = K^\pi$. We fix a non-trivial character χ of G of odd order. We denote the fixed field of K under ι by K^+. Note that $k \subset K^+$.

Theorem 3.1. *Let $P \subset \pi$ be a 2-group that does not contain ι and let $E = K^P$. Let E^+ be the fixed field of E under ι. If all primes r that ramify in $E^+ \subset K$ satisfy $\chi(r) \neq 1$, then*

(i) $Cl_K^-(\chi)$ is a cohomologically trivial $O_\chi[P]$-module;

(ii) the natural map $Cl_E^-(\chi) \longrightarrow Cl_K^-(\chi)^P$ is bijective and the norm map $N : Cl_K^-(\chi) \longrightarrow Cl_E^-(\chi)$ is surjective.

Proof. Note that $\mathrm{Gal}(K/E^+) \cong P \times \{1, \iota\}$. The proof follows the pattern of the proof of Theorem 2.1.

(i) It suffices to show that $\widehat{H}^q(P, Cl_K^-(\chi)) = 0$ for all $q \in \mathbf{Z}$. Consider the exact sequence

$$0 \longrightarrow \mu_K^- \longrightarrow U_K^- \longrightarrow C_K^- \longrightarrow Cl_K^- \longrightarrow 0.$$

We show that the χ-parts of the P-cohomology groups of the first three modules are trivial. Lemma 1.1 then implies that $\widehat{H}^q(P, Cl_K^-(\chi)) = 0$ for all $q \in \mathbf{Z}$.

Since χ has odd order, it acts trivially on the 2-part of μ_K^- and therefore on its P-cohomology groups. This shows that $\widehat{H}^q(P, \mu_K^-)(\chi) = 0$ for all $q \in \mathbf{Z}$. By *global* class field theory $\widehat{H}^q(P, C_K)$ and $\widehat{H}^q(P, C_{K^+})$ are isomorphic to $\widehat{H}^{q-2}(P, \mathbf{Z})$ and have therefore trivial G-action and, since $\chi \neq 1$, trivial χ-parts. It follows that $\widehat{H}^q(P, C_{K^-})(\chi) = 0$ for all $q \in \mathbf{Z}$.

By *local* class field theory and the fact that $\chi(r) \neq 1$ for the primes r that ramify in $E \subset K$ and $E^+ \subset K^+$ we have that $\widehat{H}^q(P, U_K)$ and $\widehat{H}^q(P, U_{K^+})$ have trivial χ-parts. The proofs are similar to the proof of part *(i)* of Theorem 2.1.

(ii) The natural map $C_E^-/N(C_K^-) \longrightarrow Cl_E^-/N(Cl_K^-)$ is surjective. We saw already in the proof of part *(i)* that $C_E^-/N(C_K^-) = \widehat{H}^0(P, C_K^-)$ has trivial χ-part. Therefore the norm map $N : Cl_K^-(\chi) \longrightarrow\!\!\!\!\rightarrow Cl_E^-(\chi)$ is surjective. Note that we only used the fact that $\chi \neq 1$ to prove this.

To prove the second statement, we consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_E^- & \longrightarrow & U_E^- & \longrightarrow & C_E^- & \longrightarrow & Cl_E^- & \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & \mu_K^{-\,P} & \longrightarrow & U_K^{-\,P} & \longrightarrow & C_K^{-\,P} & \longrightarrow & Cl_K^{-\,P} & \longrightarrow 0 \end{array}$$

An easy diagram chase shows that the first three vertical arrows are injective and have cokernels with trivial χ-parts. By the proof of part *(i)*, the P-cohomology groups of each of the modules μ_K^-, U_K^-, C_K^- and Cl_K^- have trivial χ-parts as well. This easily implies that the rightmost map induces an isomorphism $Cl_E^-(\chi) \longrightarrow Cl_K^-(\chi)^P$ as required. □

Theorem 3.2. *If all primes r that ramify in $k \subset K$ satisfy $\chi(r) \neq 1$, then*

(i) there is an exact sequence

$$0 \longrightarrow (O_\chi[\pi]/(1+\iota))^d \xrightarrow{\Theta} (O_\chi[\pi]/(1+\iota))^d \longrightarrow Cl_K^-(\chi) \longrightarrow 0;$$

(ii) If, in addition, the prime 2 is not ramified in the field K, then

$$\#Cl_K^-(\chi) = O_\chi/(\prod_\psi \frac{1}{2} B_{1,\chi^{-1}\psi}),$$

where the product runs over the odd *characters ψ of G of 2-power order.*

Proof. Choose $\sigma \in \pi$ so that $\langle\sigma\rangle$ is a direct summand of π containing ι. Let 2^e denote the order of σ and let P be a complement of $\langle\sigma\rangle$ in π: we have $\pi = P \times \langle\sigma\rangle$. The eigenspace $Cl_K^-(\chi)$ is a $O_\chi[\pi]$-module on which $\iota = \sigma^{2^{e-1}}$ acts as -1. Therefore $Cl_K^-(\chi)$ is a module over the ring $O_\chi[P \times \langle\sigma\rangle]/(1+\iota) \cong O_\chi[\zeta_{2^e}][P]$.

By Theorem 3.1, $Cl_K^-(\chi)$ is a cohomologically trivial P-module. Let $O_\chi[\zeta_{2^e}][P]^d \twoheadrightarrow Cl_K^-(\chi)$ be a surjective $O_\chi[\zeta_{2^e}][P]$-homomorphism. The kernel is a cohomologically trivial torsion-free $O_\chi[\zeta_{2^e}][P]$-module. As in the proof of Theorem 2.3, we copy the proof of [2, p.113, Thm.8] with $\mathbf{Z}$ replaced by the discrete valuation ring $O_\chi[\zeta_{2^e}]$. It follows that the kernel is projective and hence free over the local ring $O_\chi[\zeta_{2^e}][P]$. Since the quotient is finite, the kernel has rank d. This proves *(i)*.

(ii) We proceed with induction with respect to the order of π. Since 2 is unramified we may apply C. Greither's Theorem [4, p.453, Thms. A and B] and we see that the result holds when π is cyclic. Suppose π is not cyclic. Writing $\pi = \langle\sigma\rangle \times P$ as in part *(i)*, the group P is not trivial. Let $\tau \in P$ be an element of order 2. The fixed fields K^τ and $K^{\tau\iota}$ of τ and $\tau\iota$ are both complex abelian number fields containing k. The set of odd characters of G is the disjoint union of the sets of odd characters of $\mathrm{Gal}(K^\tau/\mathbf{Q})$ and $\mathrm{Gal}(K^{\tau\iota}/\mathbf{Q})$.

By induction, the result holds for the fields K^τ and $K^{\tau\iota}$. By Theorem 3.1*(i)*, $M = Cl_K^-(\chi)$ is cohomologically trivial, both as a $\{1,\tau\}$-module and as a $\{1,\tau\iota\}$-module. Moreover, by part *(ii)* of that theorem, $(1+\tau)M$ and $(1+\tau\iota)M$ are isomorphic to the χ-part of the 2-part of the minus class group of K^τ and $K^{\tau\iota}$

respectively. Since ι acts as -1 on M, it follows from the cohomological triviality of M that $\#M = \#(1+\tau)M \cdot \#(1-\tau)M = \#(1+\tau)M \cdot \#(1+\tau\iota)M$. This proves *(ii)*. □

Finally we prove a sufficient condition for the eigenspace $Cl_K^-(\chi)$ to be a cyclic $O_\chi[\pi]/(1+\iota)$-module.

Theorem 3.3. *Suppose that all primes r that ramify in $k \subset K$ satisfy $\chi(r) \neq 1$. If there exists an odd character φ of odd conductor and of order 2^k for which each of the following two conditions hold:*

- $\frac{1}{2}B_{1,\chi^{-1}\varphi} = (1-\zeta_{2^k})u$ *for some unit* $u \in O_\chi[\zeta_{2^e}]^*$,
- $\chi(r) \neq 1$ *for all primes r dividing the conductor of φ,*

then $Cl_K^-(\chi)$ is a cyclic $O_\chi[\pi]/(1+\iota)$-module.

Proof. Let k_φ denote the composite field $k\mathbf{Q}^{\ker\varphi}$ and let K_φ denote $K\mathbf{Q}^{\ker\varphi}$. Both fields $k_\varphi \subset K_\varphi$ are complex. Put $\pi' = \mathrm{Gal}(K_\varphi/k)$ and $P = \mathrm{Gal}(K_\varphi/k_\varphi)$. We have that $\iota \notin P$.

Since 2 is not ramified, it follows from Greither's Theorem that the order of $Cl_{k_\varphi}^-(\chi)$ is equal to the order of $O_\chi/(\mathrm{Norm}(\frac{1}{2}B_{1,\chi^{-1}\varphi}))$. Here the Norm is the $O_\chi[\zeta_{2^k}]/O_\chi$-Norm. Since $\mathrm{Norm}(\frac{1}{2}B_{1,\chi^{-1}\varphi}) = \mathrm{Norm}(1-\zeta_{2^k}) = 2$, we see that the order of $Cl_{k_\varphi}^-(\chi)$ is equal to the order of the residue field of O_χ. Therefore $Cl_{k_\varphi}^-(\chi)$ is a cyclic Galois module. By Theorem 3.1, applied to $E = k_\varphi \subset K_\varphi$, the eigenspace $Cl_{K_\varphi}^-(\chi)$ is a cohomologically trivial P-module and the P-norm map induces an isomorphism between $Cl_{k_\varphi}^-(\chi)$ and $Cl_{K_\varphi}^-(\chi)$ modulo the P-augmentation ideal. Therefore another application of Nakayama's Lemma implies that $Cl_{K_\varphi}^-(\chi)$ is a cyclic $O_\chi[P]$-module and hence a cyclic $O_\chi[\pi']/(1+\iota)$-module. Therefore its quotient $Cl_K^-(\chi)$ is a cyclic $O_\chi[\pi]/(1+\iota)$-module, as required. □

If the group π is cyclic, then $O_\chi[\pi]/(1+\iota) \cong O_\chi[\zeta_{2^e}]$ where $\#\pi = 2^e$. Since the ring $O_\chi[\zeta_{2^e}]$ is a discrete valuation ring, the structure of finite modules over $O_\chi[\pi]/(1+\iota)$ is particularly simple.

Proposition 3.4. *Suppose that π is cyclic and that $Cl_K^-(\chi)$ is cyclic over $O_\chi[\pi]$. If $\#Cl_K^-(\chi) = 2^{ft}$, where 2^f is the order of the residue field $O_\chi/(2)$, then there is an isomorphism of $O_\chi[\zeta_{2^e}]$-modules*

$$Cl_K^-(\chi) \cong O_\chi[\zeta_{2^e}]/((1-\zeta_{2^e})^t)$$

and there is an isomorphism of abelian groups

$$Cl_K^-(\chi) \cong (\mathbf{Z}/2^r\mathbf{Z})^{f(2^{e-1}-s)} \times (\mathbf{Z}/2^{r+1}\mathbf{Z})^{fs}$$

where $r, s \in \mathbf{Z}$ are determined by $t = r2^{e-1} + s$ and $0 \le s < 2^{e-1}$.

Proof. This follows from the fact that $O_\chi[\zeta_{2^e}]$ is a discrete valuation ring with uniformizing element $1-\zeta_{2^e}$. □

4. Tables

In this section we present the proof of Theorem II. An essential ingredient is the table of class numbers h_l^- given in the appendix. We briefly explain the notation.

TABLE 4.1

l			l		
233	$p_{14} \cdot p_{29}$	PM	419	$p_{16} \cdot p_{30} \cdot p_{49}$	PM, HtR
269	$p_{16} \cdot p_{31}$	PM	433	$p_{14} \cdot p_{34}$	PM
317	$p_{25} \cdot p_{49}$	HtR	439	$p_{11} \cdot p_{21} \cdot p_{23} \cdot p_{24}$	PM, PM, PM
337	$p_{13} \cdot p_{15} \cdot p_{15}$	PM, PM	449	$p_{18} \cdot p_{84}$	PM
359	$p_{13} \cdot p_{30} \cdot p_{45}$	PM, HtR	463	$p_{18} \cdot p_{21} \cdot p_{25}$	PM, BS
379	$p_{22} \cdot p_{24}$	BS	467	$p_{19} \cdot p_{49} \cdot p_{55}$	PM, AL
383	$p_{19} \cdot p_{24} \cdot p_{46}$	PM, HtR	479	$p_{20} \cdot p_{27} \cdot p_{70}$	PM, AL
389	$p_{24} \cdot p_{60}$	AL	487	$p_{30} \cdot p_{49}$	HtR
397	$p_{8} \cdot p_{26} \cdot p_{27}$	PM, BS	499	$p_{15} \cdot p_{18} \cdot p_{47}$	PM, PM
401	$p_{16} \cdot p_{18} \cdot p_{31}$	PM, PM	503	$p_{12} \cdot p_{14} \cdot p_{112}$	PM, PM
409	$p_{12} \cdot p_{52}$	PM	509	$p_{16} \cdot p_{28} \cdot p_{101}$	PM, AL

Let l be an odd prime. We have $l-1 = 2^e \cdot m$ with m odd. For every divisor d of $l-1$ which itself is divisible by 2^e we define

$$h_l^-(d) = \prod_{\operatorname{ord}(\chi)=d} -\frac{1}{2}B_{1,\chi}$$

where the product runs over the characters $\chi : (\mathbf{Z}/l\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ of order d; except when $d = l-1$, in which case we multiply this product by l, and when $d = 2^e$, in which case we multiply it by 2. In the rare occasion when $l-1$ is equal to 2^e, the only possible value for d is $l-1 = 2^e$ and we put

$$h_l^-(d) = 2l \prod_{\operatorname{ord}(\chi)=d} -\frac{1}{2}B_{1,\chi}.$$

This last case occurs only when l is a Fermat prime i.e., when $l = 3$, 5, 17, 257, 65537 or has more than 2 500 000 decimal digits.

The numbers $h_l^-(d)$ are listed in the appendix. They are rational integers [5], [24] and they are related to the minus class number h_l^- by

$$h_l^- = \#Cl_l^- = \prod_{2^e|d|l-1} h_l^-(d).$$

In [15] D. H. Lehmer and J. M. Masley presented a table with the numbers $h_l^-(d)$ for $l \leq 509$. Of most of these numbers the complete prime factorization was given, but their table contains 22 unfactored composite numbers. These were factored by Peter Montgomery (PM), Bob Silverman (BS), Herman te Riele (HtR) and Arjen Lenstra (AL). The most laborious factorization, for $l = 467$, was performed by Arjen Lenstra, who factored a 103 digit factor of h_{467}^- into a product of two primes of 49 and 55 digits respectively. We list the various contributions in Table 4.1. By p_n we denote a prime factor of n decimal digits. The order in which the initials are given corresponds to the order of the prime factors. In order to prove Theorem II and, at the same time, determine the structure of Cl_l^- as an abelian group, we study the table of numbers $h_l^-(d)$ of the appendix. Clearly, if a prime p divides the class number h_l^- exactly once, the p-part of Cl_l^- is cyclic as a group and hence as a Galois module. This happens for most large prime divisors. All other cases are listed below. Tables 4.2, 4.3 and 4.4 contain the prime pairs (p, l) with $l \leq 509$ for which p^2 divides h_l^-. We discuss each table in some detail.

The class group Cl_l^- is a product of its p-parts and each p-part is a product of eigenspaces $Cl_l(\chi)$. The minus class group Cl_l^- is a cyclic Galois module if and only if for each prime p, each eigenspace $Cl_l^-(\chi)$ is cyclic over the local ring $O_\chi[\pi]$, where π is the p-part of $G = \mathrm{Gal}(\mathbf{Q}(\zeta_l)/\mathbf{Q})$.

TABLE 4.2. Primes p not dividing $l-1$

l	p	d	f	$h_l(d)$	class group	
41	11	40	2	11^2	11×11	
131	3	26	3	3^3	$3 \times 3 \times 3$	
139	47	46	1	47^2	2209	Thm.2.3 with $r = 283$
	277	46	1	277	277	
		138	1	277	277	
149	3	4	2	3^2	3×3	
151	11	30	2	11^2	11×11	
157	157	156	1	157^2	157×157	Thm.2.2
211	281	14	1	281	281	
		70	1	281	281	
227	2939	226	1	2939^3	$2939 \times 2939 \times 2939$	Thm.2.2
241	47	16	2	47^2	47×47	
277	47	276	2	47^2	47×47	
281	11	40	2	11^2	11×11	
	41	40	1	41^2	1681	Thm.2.3 with $r = 83$
293	3	4	2	3^2	3×3	
313	37	24	2	37^2	37×37	
337	17	16	1	17^2	17×17	Thm.2.2
353	353	352	1	353^2	353×353	Thm.2.2
379	379	42	1	379	379	
		378	1	379	379	
397	23	132	2	23^2	23×23	
401	41	80	2	41^2	41×41	
409	5	24	2	5^2	5×5	
419	3	2	1	3^2	9	Thm.2.3 with $r = 7$
443	3	26	3	3^6	$9 \times 9 \times 9$	Thm.2.3 with $r = 7$
457	5	24	2	5^2	5×5	
467	467	466	1	467^2	467×467	Thm.2.2
479	5	2	1	5^2	25	Thm.2.3 with $r = 11$
487	7	2	1	7	7	
		6	1	7	7	
	37	18	1	37^2	37×37	Thm.2.2
491	3	2	1	3^2	9	Thm.2.3 with $r = 7$
	11	10	1	11^3	11×121	Thm.2.2, Thm.2.3 with $r = 23$
	491	98	1	491	491	
		490	1	491^2	491×491	Thm.2.2

In Table 4.2 we have listed all pairs (p, l) for which p is odd and p^2 divides h_l^-, but p does not divide $l-1$. In this case the p-part π of the Galois group of $\mathbf{Q}(\zeta_l)$ over $\mathbf{Q}$ is trivial and an eigenspace $Cl_l(\chi)$ is cyclic as a Galois module if and only if it is a cyclic O_χ-module. It turns out that in all cases every $Cl_l(\chi)$ is cyclic as an O_χ-module.

To explain the table, we first note that in the case $l = p$, the Teichmüller eigenspace $Cl_l^-(\omega)$ is always trivial. Therefore we only have contributions for the

TABLE 4.3. Odd primes p dividing $l-1$

ℓ	p	d	$h_0, h_1, \ldots$	group	
31	3	2	3, 3	9	
71	7	2	7, 7	49	
101	5	4	5, 25, 25	25×125	Prop.2.4, $\lambda = 2$
131	5	2	5, 5	25	
137	17	8	17, 17	289	
139	3	2	3, 3	9	
157	13	12	13, 13	169	
181	5	4	25, 5	125	Prop.2.4, $\lambda = 1$
199	3	2	9, 3, 3	81	
211	3	2	3, 3	9	
	7	6	7, 7	49	
283	3	2	3, 3	9	
307	3	2	3, 3, 3	27	
331	3	2	3, 9	3×9	Thm.2.3, $\theta = T^2 - 15T + 3$
	3	10	81, 81	$9 \times 9 \times 9 \times 9$	Prop.2.4, $\lambda = 1$
337	7	16	49, 49	49×49	Prop.2.4, $\lambda = 1$
367	3	2	9, 3	27	Prop.2.4, $\lambda = 1$
379	3	2	3, 3, 3, 3	81	
409	17	8	17, 17	289	
421	5	4	25, 5	125	Prop.2.4, $\lambda = 1$
439	3	2	3, 27	9×9	Thm.2.3, $\theta = T^2 - 3T - 3$
461	5	4	25, 25	5×125	Thm.2.3 with $r = 11$; Prop.2.4, $\lambda = 2$
463	7	2	7, 7	49	
	7	6	7, 7	49	
499	3	2	3, 3	9	

characters $\chi \neq \omega$. Let d be a divisor of $l-1$ for which p divides $h_l^-(d)$. Then for all characters χ of order d the ring O_χ has a residue field with p^f elements where f is the order of p modulo d. If p^f happens to be the exact power of p dividing $h_l^-(d)$, then it is clear that for exactly one character χ of order d the eigenspace $Cl_l^-(\chi)$ is isomorphic to $O_\chi/(2)$ while all others are trivial. These cases are listed without comment. In the remaining cases we apply the theorem of Mazur and Wiles which is the case with trivial π of Theorem 2.2. If the precise power of p dividing $h_l^-(d)$ is p^{fa} and for precisely a characters χ of order d the generalized Bernoulli number $B_{1,\chi^{-1}}$ is divisible by p, then each eigenspace $Cl_l^-(\chi)$ is either isomorphic to $O_\chi/(2)$ or is zero. In particular, each $Cl_l(\chi)$ is a cyclic Galois module. This happens in all but seven cases. In the remaining seven cases we use Theorem 2.3 and show that each eigenspace is a cyclic O_χ module by computing an additional Bernoulli number $B_{1,\chi^{-1}\varphi}$ where φ is a suitable even character of order p and conductor r.

In Table 4.3 we have listed all pairs (p, l) with $p \neq 2$ dividing $l-1$. We'll see below that in this case the class number h_l^- is automatically divisible by p^2, so that Table 4.3 actually contains all pairs (p, l) for which p divides $\gcd(h_l^-, l-1)$. In order to explain the contents of the table, we fix p and l and we let p^e be the exact power of p dividing $l-1$.

If d and d' are two divisors of $l-1$ that only differ by a power of p, then $B_{1,\varphi^{-1}} \equiv B_{1,\varphi'^{-1}}$ modulo $(1-\zeta_{p^e})$ for all characters φ of order d and φ' of order d'. Therefore, as Lehmer observed [14, Thm.5], either both $h_l^-(d)$ and $h_l^-(d')$ are divisible by p

TABLE 4.4. $p = 2$

ℓ	d	ord(χ)	2^e	f	$h_l^-(d)$	2–class group	r
29	28	7	4	3	8	$2 \times 2 \times 2$	
113	112	7	16	3	8	$2 \times 2 \times 2$	
163	6	3	2	2	4	2×2	
197	28	7	4	3	8	$2 \times 2 \times 2$	
239	14	7	2	3	8^2	$4 \times 4 \times 4$	3
277	12	3	4	2	4^2	$2 \times 2 \times 2 \times 2$	3
311	62	31	2	5	32^2	$2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$	
337	336	21	16	6	64	$2 \times 2 \times 2 \times 2 \times 2 \times 2$	
349	12	3	4	2	4^2	$2 \times 2 \times 2 \times 2$	7
373	124	31	4	5	32	$2 \times 2 \times 2 \times 2 \times 2$	
397	12	3	4	2	4^3	$4 \times 4 \times 2 \times 2$	3
421	60	15	4	4	16	$2 \times 2 \times 2 \times 2$	
463	14	7	2	3	8	$2 \times 2 \times 2$	
491	14	7	2	3	8^2	$2 \times 2 \times 2 \times 2 \times 2 \times 2$	

or none is. For this reason we have ordered the class numbers as follows: for each divisor d of $l-1$ which is itself not divisible by p but for which $h_l^-(d)$ is divisible by p, we list, for $i = 0, 1, \ldots, e$ the p-part h_i of $h_l^-(dp^i)$. By Lehmer's observation, each h_i is divisible by p. We note in passing that this implies that h_l^- is divisible by p^2.

For each character χ of order d the residue field of O_χ has order p^f where f is the order of p modulo d. In all but one case either $h_0 = p^f$ or $h_1 = p^f$. In the latter case we have that, up to a unit, $B_{1,\chi^{-1}\psi} = 1 - \zeta_p$ for the characters ψ of conductor l and order p. In either case Theorem 2.3 applies and we see that $Cl_l(\chi)$ is cyclic over $O_\chi[\pi]$. The only exception is $l = 461$ with $p = 5$. In this case $h_0 = h_1 = 25$. In this case we have applied Theorem 2.3 with φ a character of order 5 and conductor 11. It turns out that in this exceptional case $Cl_l(\chi)$ is a cyclic $O_\chi[\pi]$-module as well.

In most cases we can apply Theorem III and conclude that the eigenspace is a cyclic group. These cases are listed without comment. In the cases $(l, p) = (101, 5)$, $(337, 7)$, $(461, 5)$ and $(331, 3)$ (the latter for $d = 10$) an application of Proposition 2.4 immediately gives the structure of $Cl_l(\chi)$. Finally, in the cases $(l, p) = (439, 3)$ and $(331, 3)$ (the latter for $d = 2$) we have explicitly computed the Stickelberger element θ and applied Theorem 2.3 directly.

Finally we discuss the contents of Table 4.4. Let χ be a character of $(\mathbf{Z}/l\mathbf{Z})^*$ of odd order. The 2-part of Cl_l^- is a module over $O_\chi[\pi]/(1+\iota) \cong O_\chi[\zeta_{2^e}]$. Here 2^e is the exact power of 2 dividing $l-1$. It is well known that $Cl_l^-(\chi)$ is trivial when $\chi = 1$. This implies that the prime $p = 2$ never divides h_l^- with multiplicity 1. Therefore Table 4.4 actually contains all primes $l \leq 509$ for which h_l^- is even.

It turns out that $Cl_l^-(\chi)$ is in all cases a cyclic Galois module. This follows from several applications of Theorem 3.3. In all but 4 cases we have that $\prod_\psi \frac{1}{2} B_{1,\chi^{-1}\psi} = 2u$ for some unit $u \in O_\chi$. Here the product runs over the odd characters ψ of 2-power order and conductor l. In this case $Cl_l^-(\chi) \cong O_\chi/(2)$ which is a vector space of dimension f over $\mathbf{F}_2$. Here f is the degree of $\mathbf{F}_2(\zeta_d)$ over $\mathbf{F}_2$ and d is the order of χ. In the remaining cases we applied Theorem 3.3 with an odd quadratic character φ of conductor r. Here $r \equiv 3 \pmod 4$ is a prime for which $\chi(r) \neq 1$.

The structure of $Cl_l^-(\chi)$ then follows easily from Theorem 3.4.

Appendix

l	d	$h_l^-(d)$
3	2	1
5	4	1
7	2	1
	6	1
11	2	1
	10	1
13	4	1
	12	1
17	16	1
19	2	1
	6	1
	18	1
23	2	3
	22	1
29	4	1
	28	2^3
31	2	3
	6	3
	10	1
	30	1
37	4	1
	12	1
	36	37
41	8	1
	40	11^2
43	2	1
	6	1
	14	1
	42	211
47	2	5
	46	139
53	4	1
	52	4889
59	2	3
	58	$59 \cdot 233$
61	4	1
	12	1
	20	41
	60	1861
67	2	1
	6	1
	22	67
	66	12739
71	2	7
	10	1
	14	7

l	d	$h_l^-(d)$
	70	79241
73	8	89
	24	1
	72	134353
79	2	5
	6	1
	26	53
	78	377911
83	2	3
	82	279405653
89	8	113
	88	118401449
97	32	3457
	96	$577 \cdot 206209$
101	4	5
	20	5^2
	100	$5^2 \cdot 101 \cdot 601 \cdot 18701$
103	2	5
	6	1
	34	1021
	102	$103 \cdot 17247691$
107	2	3
	106	$743 \cdot 9859 \cdot 2886593$
109	4	17
	12	1
	36	1009
	108	9431866153
113	16	17
	112	$2^3 \cdot 11853470598257$
127	2	5
	6	13
	14	43
	18	3079
	42	547
	126	$883 \cdot 626599$
131	2	5
	10	5
	26	$3^3 \cdot 53$
	130	$131 \cdot 1301 \cdot 4673706701$
137	8	17
	136	$17 \cdot 47737 \cdot 46890540621121$
139	2	3
	6	3
	46	$47^2 \cdot 277$
	138	$277 \cdot 967 \cdot 1188961909$
149	4	3^2

l	d	$h_l^-(d)$
	148	$149 \cdot 5129663383200408/$
		$/05461$
151	2	7
	6	1
	10	281
	30	11^2
	50	25951
	150	$1207501 \cdot 312885301$
157	4	5
	12	13
	52	3148601
	156	$13 \cdot 157^2 \cdot 1093 \cdot 1873 \cdot 4/$
		$/18861$
163	2	1
	6	2^2
	18	181
	54	365473
	162	$23167 \cdot 441845817162679$
167	2	11
	166	$499 \cdot 5123189985484229/$
		$/035947419$
173	4	5
	172	$20297 \cdot 231169 \cdot 725717/$
		$/29362851870621$
179	2	5
	178	$1069 \cdot 144586673923349/$
		$/48286764635121$
181	4	5^2
	12	37
	20	$5 \cdot 41$
	36	2521
	60	$61 \cdot 1321$
	180	5488435782589277701
191	2	13
	10	11
	38	51263
	190	$612771091 \cdot 3673395066/$
		$/9733713761$
193	64	192026280449
	192	$6529 \cdot 15361 \cdot 29761 \cdot 91/$
		$/969 \cdot 10369729$
197	4	5
	28	$2^3 \cdot 1877$
	196	$7841 \cdot 939830268487086/$
		$/6656225611549$
199	2	3^2
	6	3

l	d	$h_l^-(d)$
	18	$3 \cdot 19$
	22	727
	66	25645093
	198	$207293548177 \cdot 31681904128/$
		$/39$
211	2	3
	6	$3 \cdot 7$
	10	41
	14	281
	30	181
	42	$7 \cdot 421$
	70	$71 \cdot 281 \cdot 12251$
	210	$1051 \cdot 113981701 \cdot 4343510221$
223	2	7
	6	43
	74	17909933575379
	222	$11757537731851 \cdot 342480448/$
		$/3726447$
227	2	5
	226	$2939^3 \cdot 1692824021974901 \cdot$
		$\cdot 13444015915122722869$
229	4	17
	12	13
	76	$705053 \cdot 47824141$
	228	$457 \cdot 7753 \cdot 41415390332169/$
		$/2666991589$
233	8	1433
	232	$233 \cdot 79933937980769 \cdot 13046/$
		$/0082041199033205724304 89$
239	2	$3 \cdot 5$
	14	2^6
	34	511123
	238	$14136487 \cdot 123373184789 \cdot 2/$
		$/2497399987891136953079$
241	16	47^2
	48	2359873
	80	$15601 \cdot 126767281$
	240	$13921 \cdot 518123008737871423/$
		$/891201$
251	2	7
	10	11
	50	348270001
	250	$9631365977251 \cdot 3696311145/$
		$/67755437243663626501$
257	256	$257 \cdot 20738946049 \cdot 1022997/$
		$/744563911961561298 69818/$
		$/3419037149697$

l	d	$h_l^-(d)$
263	2	13
	262	$263 \cdot 787 \cdot 385927 \cdot 41875910095567886732818944462994807426018628 3$
269	4	13
	268	$40170973189 \cdot 8625962877077617 \cdot 8297860832320483544484903227261$
271	2	11
	6	1
	10	31
	18	37
	30	1201
	54	751928131
	90	$21961 \cdot 7288651$
	270	$271 \cdot 811 \cdot 1621 \cdot 15391 \cdot 20238391 \cdot 666587726641$
277	4	17
	12	2^4
	92	$89977 \cdot 1371353 \cdot 30697273$
	276	$47^2 \cdot 829 \cdot 4873333 \cdot 1776834909244716811072486129$
281	8	17
	40	$11^2 \cdot 41^2 \cdot 401$
	56	64523056921
	280	$3235961 \cdot 977343139976233968569461075411406081$
283	2	3
	6	3
	94	$2064523 \cdot 39341481709417$
	282	$283 \cdot 548464664749065479915789619426609807667 3$
293	4	3^2
	292	$293 \cdot 38901409 \cdot 52561753 \cdot 354041533 \cdot 19844792749 \cdot 702405569982494626097/$ $/54079833$
307	2	3
	6	3
	18	$3 \cdot 37$
	34	$137 \cdot 443 \cdot 1429$
	102	$307 \cdot 10191268178209$
	306	$613 \cdot 919 \cdot 512412441029648479897766391339165893563$
311	2	19
	10	41
	62	$2^{10} \cdot 9918966461$
	310	$311 \cdot 856882084088129553550988747251311805392434897275868681$
313	8	233
	24	37^2
	104	$65386361 \cdot 30358065621833$
	312	$155288017 \cdot 82941207961 \cdot 986685963782009603919680953$
317	4	13
	316	$143803113090284713760723 3 \cdot 80977059904098206005745297705028094003 97/$ $/943027841$
331	2	3
	6	3^2
	10	3^4

l	d	$h_l^-(d)$
	22	$23 \cdot 67$
	30	$3^4 \cdot 61$
	66	17406850561
	110	476506973241784667381
	330	$270271 \cdot 2214751817123091258484738727402 71$
337	16	$7^2 \cdot 17^2 \cdot 353$
	48	238321
	112	$7^2 \cdot 894469355265098929$
	336	$2^6 \cdot 3246769 \cdot 3622267546801 \cdot 110537863229809 \cdot 225164259907777$
347	2	5
	346	$347 \cdot 195408694266623882825901218619535050093508672655696083443 3397/$ $/220152315402574339617$
349	4	5
	12	$2^4 \cdot 13$
	116	$421081 \cdot 943429 \cdot 2021708236660033$
	348	$2089 \cdot 17749 \cdot 29247661 \cdot 1668462979632017006413600428178285043 1997$
353	32	$6113 \cdot 9473$
	352	$353^2 \cdot 281249 \cdot 1380611233 \cdot 3001891553 \cdot 394388386054183213731974638871/$ $/81225470103134619777$
359	2	19
	358	$5862361010431 \cdot 813287316389858595758239885873 \cdot 589221908016876253 83/$ $/96098639061222102691527 23$
367	2	3^2
	6	3
	122	$733 \cdot 268738874461290742168853881$
	366	$39163 \cdot 127480330983805586375654833118494134773442493271686377913$
373	4	5
	12	61
	124	$2^5 \cdot 1117 \cdot 6218451821 \cdot 1699148567515153$
	372	$1489 \cdot 191953 \cdot 1242045986997940217894794016838264561405884776170767 89$
379	2	3
	6	$3 \cdot 13$
	14	1499
	18	$3 \cdot 991$
	42	$379 \cdot 547$
	54	$3 \cdot 29997973$
	126	$127 \cdot 757 \cdot 9199 \cdot 154412119$
	378	$379 \cdot 1087873417 \cdot 311135834438114660893 9 \cdot 2146703456839204462861 63$
383	2	17
	382	$300032351 \cdot 3000702226373096449 \cdot 290945169106342852317343 \cdot 250644232/$ $/277194809918140413062043676197070590 1$
389	4	41
	388	$389 \cdot 1553 \cdot 4847366257 \cdot 1280291672438054651779 73 \cdot 102774267926336708 3/$ $/436553331888094966227479155330120838665 97$
397	4	13
	12	2^6
	36	$109 \cdot 4861$

l	d	$h_l^-(d)$
	44	23910808769
	132	23^2 · 132189553 · 1917436489
	396	9901 · 14141557 · 28894150148400351045400753 · 241092554399010330726544957
401	16	64849
	80	41^2 · 476056112401
	400	401 · 462972001 · 3692494801 · 2106370412068801 · 166771329637484801 · 348925/ /0662765811145388290782801
409	8	5^2 · 17
	24	73 · 1321
	136	17 · 122181721 · 7960379881 · 29097077764969
	408	409 · 725945254273 · 6183699722087375941883228469840272721633145678440121
419	2	3^2
	22	647747
	38	1103 · 5410099
	418	2719452561369347 · 440305024994584776198045120721 · 38089642480704298751/ /25494615628571625716516342483
421	4	5^2
	12	37
	20	5 · 2521
	28	29 · 39509
	60	2^4 · 22064701
	84	70309 · 46085341
	140	409781 · 16521541 · 672896721281
	420	421 · 39901 · 3455761 · 57979541174101 · 2655579516751331409910861
431	2	3 · 7
	10	11 · 701
	86	676649 · 2709472364809333
	430	14621 · 7970051 · 112225988494992246639243672859450218083129490012657313/ /823968596573192207124531
433	16	842353
	48	4727329
	144	3457 · 3021564742348701537217
	432	433 · 12097 · 21601 · 47521 · 1403137 · 102550753 · 96686549358769 · 64340730822/ /61985367563988399449713
439	2	3 · 5
	6	3^3
	146	293 · 527207 · 7171667 · 50898521 · 327151064937209
	438	40139516617 · 607057872831881225737 · 15343765387604391577783 · 7611086694/ /50601851817037
443	2	5
	26	3^6 · 79 · 157
	34	367926037
	442	12377 · 2099059 · 309860291076943369037303413323285158985313526398152831/ /008871913595050372353059812436688273929
449	64	500402969557121
	448	168449 · 226736972834339969 · 772865886177933052632667046915246737827100/ /790144773744195236265619879496879953539649
457	8	41
	24	5^2 · 577
	152	1217 · 43777 · 23353152677443223648257268496337
	456	63841 · 28668613681009535839148397954381101468353560199403645535773916736/ /6347873193
461	4	5^2
	20	5^2 · 661
	92	461 · 463413261346674397069
	460	161461 · 3702458172193117785898149655903648058852928086226081699845637442/ /0371674719539068279993529581
463	2	7
	6	7
	14	2^3 · 7 · 29
	22	89 · 1123
	42	7 · 631 · 673
	66	4423 · 33642841
	154	463 · 664064207818594609257539327251
	462	8779 · 604417477499456083 · 334167173856936895861 · 1451125083064477390379041
467	2	7
	466	467^2 · 7842513546558078253 · 154987811800520892460672570209646897293261969/ /1231 · 4511882445351575687067360009368178199225508063847112361
479	2	5^2
	478	48757 · 62141 · 2560169 · 26756241308309805857 · 177581990178050932739148007· ·3939232521558670638697337486372397962981765904709957802472308181004309
487	2	7
	6	7
	18	37^2
	54	919 · 2647 · 10909
	162	105792786991 · 1355141213869532941
	486	58321 · 105290443 · 294594702996402697646390639203 · 90058027084074393088174/ /14913576150427261734980259
491	2	3^2
	10	11^3
	14	2^6 · 29
	70	1262296191031
	98	491 · 101566319 · 2311247713517
	490	491^2 · 8489251 · 17841391 · 74468731 · 18022473215169065702224279183302091210/ /994749548801576948376558921841
499	2	3
	6	3
	166	167 · 8170189 · 4568950377354424102616078873671968013
	498	628477 · 2498605441 · 476526575352703 · 125184090531384337 · 2313122953817705/ /5312162275545594472697442144611
503	2	3 · 7
	502	15061 · 182337132259 · 67961871500791 · 142639305944396395662911180592353348/ /442031813108145092050553010609968433975432 1688566291891565574466073368/ /455407
509	4	13
	508	1102305661663669 · 3595837345204924707130453993 · 285986765137386082677131/ /210874962327994154402550613015614414986549035966985 8574049275462019230/ /8152597

References

[1] Bourbaki, N.: Éléments de Mathématique, Algèbre, Hermann, Paris 1970.
[2] Cassels, J.W.S and Fröhlich, A.: *Algebraic Number Theory*, Academic Press, London 1967. MR **35:**6500
[3] Cornacchia, P.: Anderson's module and ideal class groups of abelian fields, J. Number Theory, to appear.
[4] Greither, C.: Class groups of abelian fields, and the main conjecture, *Ann. de l'Institut Fourier*, **42** (1992), 449–499. MR **93j:**11071
[5] Hasse, H.: *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin 1952. MR **14:**141a
[6] Iwasawa, K.: A note on ideal class groups, *Nagoya Math. J.* **27**, (1966), 239–247. MR **33:**5603
[7] Kolyvagin, V.A.: Euler Systems, in: *The Grothendieck Festschrift II*, Prog. Math. **87**, Birkhäuser, Boston 1990, 435–483. MR **92g:**11109
[8] Kummer, E.E.: *Collected papers*, Vol.I, Springer-Verlag, Berlin 1975. MR **57:**5650a
[9] Kummer, E.E.: Bestimmung der Anzahl nicht äquivalenter Classen für die aus λten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben, *J. für die reine und angewandte Math.* **40**, (1850), 93–116. (Coll.Papers 299–322)
[10] Kummer, E.E.: Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers, *J. de math. pures et appl.* **16**, (1851), 377–498. (Coll.Papers 363-484)
[11] Kummer, E.E.: Über die Irregularität von Determinanten, *Monatsberichte der Kön. Preuß. Ak. der Wiss. zu Berlin*, (1853), 194–200. (Coll.Papers 539–545)
[12] Kummer, E.E.: Über die aus 31sten Wurzeln der Einheit gebildeten complexen Zahlen, *Monatsberichte der Kön. Preuß. Ak. der Wiss. zu Berlin*, (1870), 755–766. (Coll.Papers 907–918)
[13] Lang, S.: *Cyclotomic fields*, Graduate Texts in Math. **59**, Springer-Verlag, New York 1978. MR **58:**5578
[14] Lehmer, D.H.: Prime factors of cyclotomic class numbers, *Math. Comp.* **31**, (1977), 599–607. MR **55:**5576
[15] Lehmer, D.H. and Masley, J.: Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$, *Math.Comp.* **32**, (1978), 577–582, with microfiche supplement. MR **58:**16594a
[16] Mazur, B. and Wiles, A.: Class fields of abelian extensions of $\mathbf{Q}$, *Invent. Math.* **76**, (1984), 179–330. MR **85m:**11069
[17] Perrin-Riou, B.: Travaux de Kolyvagin et Rubin, *Séminaire Bourbaki 1989–1990*, Exp. **717**, *Astérisque*, **189-190**, 69–106. MR **92f:**11085
[18] Rubin, K.: Kolyvagin's system of Gauss sums, In: *Arithmetic Algebraic Geometry*, Texel 1989, Prog. Math. **89**, Birkhäuser, Boston 1991. MR **92a:**11121
[19] Schoof, R.: Cohomology of class groups of cyclotomic fields; an application to Morse-Smale diffeomorphisms, *J. of Pure and Applied Algebra* **53**, (1988), 125–137. MR **89j:**11111
[20] Schoof, R.: The structure of the minus class groups of abelian number fields, In: Goldstein. C.: *Sém. de Théorie de Nombres, Paris 1988–1989*, Birkhäuser, Boston 1990, 185–204. MR **92e:**11126
[21] Schoof, R.: Class numbers of $\mathbf{Q}(\cos(2\pi/p))$, in preparation.
[22] Solomon, D.: On the class groups of imaginary abelian fields, *Ann. Institut Fourier* **40**, (1990), 467–492. MR **92a:**11133
[23] Van der Linden, F.: Class number computations of real abelian number fields, *Math. Comp.* **39**, (1982), 693–707. MR **84e:**12005
[24] Washington, L.C.: *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, New York 1982. MR **85g:**11001

Dipartimento di Matematica, 2ª Università di Roma "Tor Vergata", I-00133 Rome, Italy
E-mail address: schoof@wins.uva.nl