

## CLASS NUMBERS OF REAL CYCLOTOMIC FIELDS OF PRIME CONDUCTOR

RENÉ SCHOOF

ABSTRACT. The class numbers  $h_l^+$  of the real cyclotomic fields  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  are notoriously hard to compute. Indeed, the number  $h_l^+$  is not known for a single prime  $l \geq 71$ . In this paper we present a table of the orders of certain subgroups of the class groups of the real cyclotomic fields  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  for the primes  $l < 10,000$ . It is quite likely that these subgroups are in fact *equal* to the class groups themselves, but there is at present no hope of proving this rigorously. In the last section of the paper we argue —on the basis of the Cohen-Lenstra heuristics— that the probability that our table is actually a table of class numbers  $h_l^+$ , is at least 98%.

### INTRODUCTION

Let  $l > 2$  be a prime number and let  $\zeta_l$  denote a primitive  $l$ -th root of unity. The ideal class group  $Cl_l$  of the ring of integers of the cyclotomic field  $\mathbf{Q}(\zeta_l)$  is a finite abelian group of order  $h_l$ , the *class number* of  $\mathbf{Q}(\zeta_l)$ . The group  $Cl_l$  naturally splits into two parts; there is a natural exact sequence

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

where  $Cl_l^+$  denotes the class group of the ring of integers of the real cyclotomic field  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . Its order, the *class number* of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ , is denoted by  $h_l^+$ . The quotient group  $Cl_l^-$  is rather well understood. Already in the 19th century, E.E. Kummer [12], [13] computed the orders of the groups  $Cl_l^-$  for  $l < 100$ . Nowadays it is rather easy to compute these numbers for much larger values of  $l$ . See [19] for the structure of the groups  $Cl_l^-$  and [5] for a study of the extension of  $Cl_l^-$  by  $Cl_l^+$ . The present paper is concerned with the groups  $Cl_l^+$ .

The groups  $Cl_l^+$  are not well understood, and there is at present no practical method to compute their orders, not even for relatively small  $l$ . Methods that inspect all ideals of norm less than the classical Minkowski bound become useless as  $l$  grows: for  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  the Minkowski bound is  $(\frac{l-1}{2})!(\frac{l-1}{2})^{-(l-1)/2}l^{(l-3)/4}$ , which exceeds  $10^{28}$  when  $l > 100$ . Algorithms that proceed by searching for fundamental units are not very efficient either, because the rank of the unit group of the ring of integers of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  is  $(l-3)/2$ , which is at least 49 when  $l > 100$ . This is too large to be of much use. Using Odlyzko's discriminant bounds, F. van der Linden computed in [22] the groups  $Cl_l^+$  for  $l \leq 163$ . For  $l \geq 71$  his results are only valid under assumption of the Generalized Riemann Hypothesis for zeta functions of number fields. Van der Linden's results are the best known: strictly speaking,

---

Received by the editor November 7, 2000 and, in revised form, July 9, 2001.  
2000 *Mathematics Subject Classification*. Primary 11R18, 11Y40.

the largest prime  $l$  for which the class number of  $\mathbf{Q}(\zeta_l)$  is known is  $l = 67$ . The class number of  $\mathbf{Q}(\zeta_{71})$  is unknown at present. Assuming the Generalized Riemann Hypothesis improves the situation only marginally: determining the class number of  $\mathbf{Q}(\zeta_{167})$  is beyond the scope of any known method.

In view of this sorry state of affairs, we proceed in the following experimental way. Let  $G_l$  denote the Galois group of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  over  $\mathbf{Q}$ . This is a cyclic group of order  $(l-1)/2$ . Let  $B_l$  denote the quotient of the unit group of the ring of integers of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  by its subgroup of cyclotomic units. It follows from the so-called class number formula [23] that

$$\#Cl_l^+ = \#B_l.$$

This result can be refined as follows. Both groups  $B_l$  and  $Cl_l^+$  are finite  $\mathbf{Z}[G_l]$ -modules and hence admit Jordan-Hölder filtrations with simple factors. An application of the class number formula for  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  and its subfields shows that the submodules of  $B_l$  and  $Cl_l^+$  all of whose simple Jordan-Hölder factors have some fixed order  $q$ , have the same number of elements as well.

The simple Jordan-Hölder factors of the ring  $\mathbf{Z}[G_l]$  are 1-dimensional vector spaces over the finite residue fields of  $\mathbf{Z}[G_l]$ . On heuristic grounds one expects that when  $l$  varies, the smaller factors have a higher probability of occurring than the larger ones. Therefore we computed only the small Jordan-Hölder factors of  $B_l$  for primes  $l$  in a certain range. More precisely, our computation gives the following.

**Main result.** *A table of all the simple Jordan-Hölder factors of order less than 80,000 of all groups  $B_l$  for  $l < 10,000$ . Moreover, we give their multiplicities and hence the order  $\tilde{h}_l^+$  of the largest subgroup of  $B_l$  all of whose Jordan-Hölder factors have order less than 80,000. The number  $\tilde{h}_l^+$  is also the order of the largest subgroup  $\tilde{Cl}_l^+$  of  $Cl_l^+$  all of whose Jordan-Hölder factors have order less than 80,000.*

This is a rather extensive calculation. We checked the more than 85 million simple Jordan-Hölder factors of the rings  $\mathbf{Z}[G_l]$  with  $l < 10,000$  that have order less than 80,000. Both bounds are rather arbitrary. It turned out that only 354 of the factors appear in the Jordan-Hölder filtration of the group  $B_l$  for some field  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . The largest one has order 1451. For each occurring Jordan-Hölder factor we computed the multiplicity with which it occurs in  $B_l$ . More precisely, we determined for all  $l < 10,000$  the Galois module structure of the largest submodule of  $B_l$  all of whose Jordan-Hölder factors have order less than 80,000. This submodule is not necessarily isomorphic to the Galois module  $\tilde{Cl}_l^+$ , but it has the same order  $\tilde{h}_l^+$ .

We can say with certainty that  $\tilde{h}_l^+$  divides  $h_l^+$  and that either  $h_l^+$  is equal to  $\tilde{h}_l^+$  or that  $h_l^+ > 80,000 \cdot \tilde{h}_l^+$ . But we do not know for sure whether  $\tilde{h}_l^+ = h_l^+$  for a single  $l \geq 71$  (or  $l \geq 167$  if we assume the Generalized Riemann Hypothesis). Nevertheless, an informal calculation based on the Cohen-Lenstra heuristics indicates that it is not at all unlikely that actually  $\tilde{h}_l^+ = h_l^+$  for all primes  $l$  in our range. Proving this rigorously seems completely out of reach however.

Note that we do *not* claim to have computed the  $p$ -part of  $h_l^+$  for all primes  $p < 80,000$ . We show, for instance, that  $\tilde{h}_{167}^+ = 1$ , but we have not even checked that  $h_{167}^+ = 1$  is not divisible by 3! Indeed, since the relevant Jordan-Hölder factors all have order  $3^{41}$ , once 3 divides  $h_{167}^+$ , then so does  $3^{41}$ . The heuristics indicate

that it is extremely improbable that  $Cl_{167}^+$  admits any simple Jordan-Hölder factors of order as large as  $3^{41}$ .

In section 1 we briefly discuss finite Gorenstein rings. Our main examples are finite group rings. In section 2 we give a description of the Galois modules  $B_l$  that is suitable for actual computation. In section 3 we explain how the calculations were performed. In section 4 we present the results of the calculations. The “Main Table” contains the numbers  $\tilde{h}_l^+$ . In section 5 we show that, even if the Galois modules  $B_l$  and  $Cl_l^+$  need not be isomorphic, their Galois cohomology groups are. For  $l < 10,000$ , they can readily be computed from the data given in section 4. Finally, in section 6, we present the heuristic arguments that lead to the assertion that with 98% probability, the Main Table is actually a table of class numbers of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  for  $l < 10,000$ .

Initially computations were performed on Macintoshes at the Universities of Sassari and Trento in Italy. PARI was used to do the multi-precision computations described in section 3. I thank Stéphane Fermigier, who some years later translated my Pascal programs into C and ran them on a powerful Connection Machine in Paris, Larry Washington for several useful remarks, Francesco Pappalardi and Don Zagier for their help with the estimates in section 6, and Silvio Levy for the production of Figure 6.1.

### 1. FINITE GORENSTEIN RINGS

In this section we discuss some elementary properties of finite *Gorenstein* rings. The properties of these rings play a role in the next section.

Let  $R$  be a finite commutative ring. For any  $R$ -module  $A$ , the additive group  $A^\perp = \text{Hom}_R(A, R)$  is an  $R$ -module via  $(\lambda f)(a) = \lambda f(a) = f(\lambda a)$  for  $\lambda \in R$ ,  $a \in A$ . Similarly, the dual group  $A^{\text{dual}} = \text{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$  is an  $R$ -module via  $(\lambda f)(a) = f(\lambda a)$  for  $\lambda \in R$ ,  $a \in A$ .

The ring  $R$  is said to be *Gorenstein* if the  $R$ -module  $R^{\text{dual}}$  is free of rank 1 over  $R$ . For any positive  $M \in \mathbf{Z}$ , the ring  $\mathbf{Z}/M\mathbf{Z}$  is a Gorenstein ring. If  $R$  is a finite Gorenstein ring, and  $g(X) \in R[X]$  is a monic polynomial, then  $R[X]/(g(X))$  is also a finite Gorenstein ring. In particular, for any  $M > 0$  and any finite abelian group  $G$ , the group ring  $(\mathbf{Z}/M\mathbf{Z})[G]$  is Gorenstein.

The following proposition collects some well-known consequences of the Gorenstein property.

**Proposition 1.1.** *Let  $R$  be a finite Gorenstein ring. Then*

(i) *For every  $R$ -module  $A$ , the map*

$$A^\perp = \text{Hom}_R(A, R) \longrightarrow \text{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z}) \cong A^{\text{dual}}$$

*defined by  $f \mapsto \chi \cdot f$  is an isomorphism of  $R$ -modules. Here  $\chi : R \longrightarrow \mathbf{Q}/\mathbf{Z}$  denotes a generator of the  $R$ -module  $\text{Hom}_{\mathbf{Z}}(R, \mathbf{Q}/\mathbf{Z})$ .*

(ii) *The functor  $A \mapsto A^\perp$  from the category of finite  $R$ -modules to itself is exact. Moreover,  $(A^\perp)^\perp \cong A$*

(iii) *The map  $I \mapsto \text{Ann}_R(I)$  is an inclusion-reversing bijection from the set of ideals of  $R$  to itself. One has that  $\text{Ann}_R \text{Ann}_R(I) = I$  for every ideal  $I$ . In addition,  $\text{Ann}_R(I + J) = \text{Ann}_R(I) \cap \text{Ann}_R(J)$  and  $\text{Ann}_R(I \cap J) = \text{Ann}_R(I) + \text{Ann}_R(J)$  for all ideals  $I, J$  of  $R$ .*

*Proof.* Let  $A$  be an  $R$ -module. The canonical isomorphism

$$\mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbf{Z}}(R, \mathbf{Q}/\mathbf{Z})) \cong \mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$$

and the  $R$ -isomorphism  $R \cong \mathrm{Hom}_{\mathbf{Z}}(R, \mathbf{Q}/\mathbf{Z})$  given by  $1 \mapsto \chi$  imply (i). Part (ii) follows from the fact that the functor  $A \mapsto A^{\mathrm{dual}} = \mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$  from the category of finite  $\mathbf{Z}/M\mathbf{Z}$ -modules to itself is exact. The canonical map  $A \rightarrow (A^{\mathrm{dual}})^{\mathrm{dual}}$  is easily seen to induce an isomorphism of  $R$ -modules  $A \cong (A^\perp)^\perp$ . Since  $(R/I)^\perp \cong \mathrm{Ann}_R(I)$ , we have that  $\#I \cdot \#\mathrm{Ann}_R(I) = \#R$ . Applying this to  $\mathrm{Ann}_R(I)$  gives that  $\#\mathrm{Ann}_R(I) = \#\mathrm{Ann}_R(\mathrm{Ann}_R(I))$ . Therefore the inclusion  $I \subset \mathrm{Ann}_R(\mathrm{Ann}_R(I))$  is an equality. The remaining statements in part (iii) easily follow from this.

This proves the proposition.  $\square$

For finite group rings  $R = (\mathbf{Z}/M\mathbf{Z})[G]$  we make Prop.1.1 (i) more explicit. Let  $\chi : R \rightarrow \mathbf{Z}/M\mathbf{Z}$  denote the homomorphism that maps a group ring element  $\sum_{\sigma \in G} x_\sigma[\sigma]$  to its coefficient  $x_1$ . Then  $\chi$  generates the  $R$ -module  $\mathrm{Hom}_{\mathbf{Z}}(R, \mathbf{Z}/M\mathbf{Z})$ , which is naturally isomorphic to  $R^{\mathrm{dual}}$ . If  $f \in \mathrm{Hom}_R(A, R)$  maps  $a \in A$  to  $\sum_{\sigma \in G} x_\sigma[\sigma]$ , then the homomorphism  $\chi \cdot f : A \rightarrow \mathbf{Z}/M\mathbf{Z}$  of Prop.1.1 (i) maps  $a$  to  $x_1$ .

The following proposition concerns relations between the structures of certain  $R$ -modules and their duals.

**Proposition 1.2.** *Let  $R$  be a finite Gorenstein ring. Then we have the following.*

(i) *Any finite  $R$ -module is Jordan-Hölder isomorphic to its dual.*

*Let  $I \subset R$  be an ideal.*

(ii) (P. Cornacchia) *The modules  $R/I$  and  $(R/I)^\perp$  are isomorphic  $R$ -modules if and only if  $\mathrm{Ann}_R(I)$  is principal.*

(iii) *If  $R/I$  has a Jordan-Hölder filtration of length at most 2, then  $(R/I)^\perp \cong R/I$ .*

(iv) *Suppose that there are an ideal  $J \subset R$  and a surjection  $g : R/J \rightarrow I^\perp$  with the property that  $\mathrm{Ann}_R(J)$  annihilates  $R/I$ . Then  $J = \mathrm{Ann}_R(I)$  and  $g$  is an isomorphism.*

*Proof.* For any finite  $R$ -module  $A$  and any maximal ideal  $\mathfrak{m}$  of  $R$ , the dual of  $A/\mathfrak{m}A$  is isomorphic to  $A^{\mathrm{dual}}[\mathfrak{m}] = \{a \in A^{\mathrm{dual}} : \lambda a = 0 \text{ for all } \lambda \in \mathfrak{m}\}$ . Therefore  $A$  has a simple Jordan-Hölder factor isomorphic to  $R/\mathfrak{m}$  if and only if  $A^{\mathrm{dual}}$  has. Part (i) now follows by induction.

(ii) I owe this part to Pietro Cornacchia. Since  $(R/I)^\perp \cong \mathrm{Ann}_R(I)$ , the condition that  $\mathrm{Ann}_R(I)$  is principal is clearly necessary. Conversely, if  $\mathrm{Ann}_R(I)$  is principal, it is isomorphic to an  $R$ -module of the form  $R/J$  for some ideal  $J \subset R$ . Since  $I$  annihilates  $\mathrm{Ann}_R(I)$ , we have that  $I \subset J$ . This shows that there is a surjection of  $R$ -modules  $R/I \rightarrow \mathrm{Ann}_R(I) \cong (R/I)^\perp$ . Since both sides have the same cardinality, we have an isomorphism, and (ii) follows.

(iii) If the length of  $R/I$  is 1, then  $I$  is maximal, so that  $\mathrm{Ann}_R(I)$  is minimal and hence principal. If the length of  $R/I$  is 2, we distinguish two cases. If there is only one maximal ideal  $\mathfrak{m}$  satisfying  $I \subset \mathfrak{m} \subset R$ , then any element in  $\mathrm{Ann}_R(I) - \mathrm{Ann}_R(\mathfrak{m})$  generates  $\mathrm{Ann}_R(I)$ , so that  $\mathrm{Ann}_R(I)$  is principal. If there are two distinct maximal ideals  $\mathfrak{m}, \mathfrak{m}'$  containing  $I$ , then  $I = \mathfrak{m} \cap \mathfrak{m}'$ . Denoting by  $\alpha$  and  $\alpha'$  generators of  $\mathrm{Ann}_R(\mathfrak{m})$  and  $\mathrm{Ann}_R(\mathfrak{m}')$  respectively, we have by Prop.1.1 (iii) that  $\mathrm{Ann}_R(I) = \langle \alpha, \alpha' \rangle$ . But this ideal is generated by the sum  $\alpha + \alpha'$ . Indeed,  $1 = \mu + \mu'$  for some  $\mu \in \mathfrak{m}$  and  $\mu' \in \mathfrak{m}'$ , and hence  $\alpha = \mu'(\alpha + \alpha')$  and  $\alpha' = \mu(\alpha + \alpha')$ . So, in all cases, the ideal  $\mathrm{Ann}_R(I)$  is principal, and the result follows from (ii).

(iv) We have that  $\#I = \#I^\perp \leq \#(R/J) = \#\text{Ann}_R(J)$ . Since  $\text{Ann}_R(J) \subset I$ , we also have that  $\#I \geq \#\text{Ann}_R(J)$ , so that we must have equality everywhere, and (iv) follows.  $\square$

When  $R = (\mathbf{Z}/M\mathbf{Z})[G]$ , the isomorphism  $A^\perp \cong A^{\text{dual}}$  of Prop.1.1 (i) induces a  $G$ -action on  $A^{\text{dual}} = \text{Hom}_{\mathbf{Z}}(A, \mathbf{Q}/\mathbf{Z})$  which is given by  $(\sigma f)(a) = f(\sigma(a))$ . This action is the *inverse* of the usual action [3, IV, sect.1] of  $G$  on  $A^{\text{dual}}$ .

## 2. CYCLOTOMIC UNITS

In this section we fix a prime  $l > 2$  and let  $\zeta_l$  denote a primitive  $l$ -th root of unity. We give a description of the group of units modulo cyclotomic units associated to  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  that is suitable for explicit computation.

We let  $K = \mathbf{Q}(\zeta_l + \zeta_l^{-1})$ , we let  $O$  denote the ring of integers of  $K$ , and we put  $G = \text{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/l\mathbf{Z})^*/\{\pm 1\}$ . The group  $\text{Cyc}$  of *cyclotomic units* is the multiplicative  $\mathbf{Z}[G]$ -module generated by the unit

$$\eta = \frac{\zeta_l^g - \zeta_l^{-g}}{\zeta_l - \zeta_l^{-1}}.$$

Here  $g$  denotes a primitive root modulo  $l$ . The group  $\text{Cyc}$  does not depend on the choice of  $g$ . It contains the unit  $-1$ , and the  $G$ -homomorphism  $\mathbf{Z}[G] \rightarrow \text{Cyc}/\{\pm 1\}$  given by  $x \mapsto \eta^x$  induces a  $G$ -isomorphism  $\mathbf{Z}[G]/(\text{Norm}) \cong \text{Cyc}/\{\pm 1\}$ . Note that multiplication by  $[g] - 1$  induces an  $G$ -isomorphism  $\mathbf{Z}[G]/(\text{Norm}) \cong I$ . Here  $I$  denotes the augmentation ideal of  $\mathbf{Z}[G]$ , and  $\text{Norm} = \sum_{\sigma \in G} [\sigma] \in \mathbf{Z}[G]$ . Finally we put

$$B = O^*/\text{Cyc}.$$

It is well-known [23, Thm.8.2] that the  $G$ -module  $B$  is finite and has the same order as the class group of  $K$ .

In this section we let  $M > 1$  denote a power of a prime  $p$ . We put  $F = K(\zeta_{2M})$  and  $\Delta = \text{Gal}(F/K)$ . First we prove a lemma.

**Lemma 2.1.** *The kernel of the natural map*

$$j : O^*/O^{*M} \rightarrow F^*/F^{*M}$$

*is trivial if  $p$  is odd. It has order 2 and is generated by  $-1$  if  $p = 2$ .*

*Proof* (Cf. [23, Prop.15.47]). We fix an embedding  $F \subset \mathbf{C}$ . This embedding identifies  $K$  with a subfield of  $\mathbf{R}$ . Suppose  $x > 0$  in  $O^* \subset \mathbf{R}^*$  is in the kernel of  $j$ . Then  $x = y^M$  for some  $y \in F^*$ . Since the  $M$ -th roots of unity are contained in  $F$ , we may assume that  $y \in \mathbf{R}$ , so that the complex conjugation automorphism in  $\Delta$  fixes  $y$ . Since  $\Delta$  is commutative, this implies that  $\sigma(y) \in \mathbf{R}$  for all  $\sigma \in \Delta$ . Therefore  $\sigma(y) = \pm y$  for all  $\sigma \in \Delta$ .

If  $p \neq 2$ , the order of  $\Delta$  is odd and hence  $\Delta$  fixes  $y$ . It follows that  $y \in K^*$  and hence  $x \in O^{*M}$ . Since  $-1$  is an  $M$ -th power as well, the map  $j$  is injective in this case. If  $p = 2$ , we have that  $y^2 \in K^*$ . More precisely, since the quadratic subfields of  $F$  are  $\mathbf{Q}(i)$ ,  $\mathbf{Q}(\sqrt{2})$  and  $\mathbf{Q}(\sqrt{-2})$ , Kummer theory implies that  $y^2 \in \langle -1, 2 \rangle K^{*2}$ . Since  $y$  is a unit, this implies that  $y^2 = \pm u^2$  for some  $u \in O^*$ , and hence  $x = u^M$ . On the other hand,  $-1$  is the  $M$ -th power of  $\zeta_{2M}$  but  $-1$  is not even a square in  $K$ . This shows that the kernel of  $j$  is the cyclic group of order 2 generated by  $-1$ , as required.  $\square$

Next we associate to any prime ideal  $\mathfrak{R}$  of degree 1 of the field  $F = K(\zeta_{2M})$  a  $G$ -homomorphism  $f_{\mathfrak{R}} : O^*/\{\pm 1\} \rightarrow (\mathbf{Z}/M\mathbf{Z})[G]$ . Let  $\mathfrak{r}$  denote the prime of  $K$  over which  $\mathfrak{R}$  is lying and let  $r$  denote the prime number over which  $\mathfrak{r}$  lies. The prime  $r$  satisfies  $r \equiv \pm 1 \pmod{l}$  and  $r \equiv 1 \pmod{2M}$ . Consider the diagram below.

$$\begin{array}{ccccccc}
 O^* & \xrightarrow{f_1} & (O/rO)^* & \xrightarrow[\cong]{f_2} & (O_F/rO_F)^{\Delta} & & \\
 & & \downarrow f_3 & & \downarrow f_3 & & \\
 & & \mu_M(O/rO) & \xleftarrow[\cong]{f_2} & \mu_M(O_F/rO_F)^{\Delta} & \xleftarrow[\cong]{f_4} & (\mathbf{Z}/M\mathbf{Z})[\Omega]^{\Delta} \xleftarrow[\cong]{f_5} (\mathbf{Z}/M\mathbf{Z})[G]
 \end{array}$$

Here  $O_F$  denotes the ring of integers of  $F$  and  $\Omega$  denotes  $\text{Gal}(F/\mathbf{Q})$ . There is an exact sequence  $0 \rightarrow \Delta \rightarrow \Omega \rightarrow G \rightarrow 0$ . By  $\mu_M(A)$  we denote the group of  $M$ -th roots of unity of a commutative ring  $A$ . The map  $f_1$  is simply reduction modulo the ideal  $rO$ . The maps  $f_2$  are induced by the inclusion maps. The vertical maps  $f_3$  are given by raising to the power  $(r-1)/M$ . The map  $f_4$  is the restriction of the  $\Omega$ -homomorphism  $(\mathbf{Z}/M\mathbf{Z})[\Omega] \rightarrow \mu_M(O_F/rO_F)$  that maps  $1 \in (\mathbf{Z}/M\mathbf{Z})[\Omega]$  to the unique element in  $O_F/rO_F$  that is congruent to  $\zeta_{2M}$  modulo  $\mathfrak{R}$  and congruent to 1 modulo all other primes of  $F$  that lie over  $r$ . By the Chinese Remainder Theorem and the fact that  $r$  is completely split in  $F$ , this map and hence the map  $f_4$  are isomorphisms. Finally, the isomorphism  $f_5$  is given by multiplication by the  $\Delta$ -norm  $\sum_{\sigma \in \Delta} [\sigma]$ .

We define the  $G$ -homomorphism  $f_{\mathfrak{R}}$  by  $f_{\mathfrak{R}} = f_5^{-1} f_4^{-1} f_3 f_2 f_1$ . Since  $\zeta_{2M} \in F^*$ , we have that  $f_{\mathfrak{R}}(-1) = 0$ , so that  $f_{\mathfrak{R}}$  factors through the quotient  $O^*/\{\pm 1\}$ :

$$f_{\mathfrak{R}} : O^*/\{\pm 1\} \rightarrow (\mathbf{Z}/M\mathbf{Z})[G].$$

Rather than giving a direct description of the  $G$ -module  $B$ , we give, for every prime power  $M$ , a description of the dual of the  $M$ -torsion of  $B$ .

**Theorem 2.2.** *Let  $M > 1$  be a power of a prime  $p$  and let  $I$  denote the augmentation ideal of the ring  $(\mathbf{Z}/M\mathbf{Z})[G]$ . There is a natural isomorphism of  $G$ -modules*

$$B[M]^{\perp} \cong I/\{f_{\mathfrak{R}}(\eta) : \mathfrak{R} \in S\}.$$

Here  $S$  denotes the set of unramified prime ideals  $\mathfrak{R}$  of  $K(\zeta_{2M})$  of degree 1.

*Proof.* Let  $R = (\mathbf{Z}/M\mathbf{Z})[G]$ . Applying the Snake Lemma to the following diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \text{Cyc}/\{\pm 1\} & \longrightarrow & O^*/\{\pm 1\} & \longrightarrow & B \longrightarrow 0 \\
 & & \downarrow M & & \downarrow M & & \downarrow M \\
 0 & \longrightarrow & \text{Cyc}/\{\pm 1\} & \longrightarrow & O^*/\{\pm 1\} & \longrightarrow & B \longrightarrow 0
 \end{array}$$

gives rise to the exact sequence of  $R$ -modules

$$0 \rightarrow B[M] \rightarrow \text{Cyc} / \pm \text{Cyc}^M \rightarrow O^* / \pm O^{*M}.$$

By Prop.1.1(ii), taking  $R$ -duals is exact and we obtain the exact sequence

$$\text{Hom}_R(O^* / \pm O^{*M}, R) \rightarrow \text{Hom}_R(\text{Cyc} / \pm \text{Cyc}^M, R) \rightarrow \text{Hom}_R(B[M], R) \rightarrow 0.$$

Let  $F = K(\zeta_{2M})$ . By Lemma 2.1, we can identify the group  $O^*/\pm O^{*M}$  with a subgroup of  $F^*/F^{*M}$ . Therefore, by Kummer theory,

$$\text{Gal}(F(\sqrt[M]{O^*})/F) \cong \text{Hom}_{\mathbf{Z}}(O^*/\{\pm 1\}, \mu_M) \cong \text{Hom}_{\mathbf{Z}}(O^*/\{\pm 1\}, \mathbf{Z}/M\mathbf{Z}).$$

The last isomorphism depends on a choice of a primitive  $M$ -th root of unity in  $K(\zeta_{2M})$ . The group

$$\text{Hom}_{\mathbf{Z}}(O^*/\{\pm 1\}, \mathbf{Z}/M\mathbf{Z})$$

is naturally isomorphic to

$$\text{Hom}_{\mathbf{Z}}(O^*/\pm O^{*M}, \mathbf{Q}/\mathbf{Z})$$

which is in turn isomorphic to

$$\text{Hom}_R(O^*/\pm O^{*M}, R).$$

This last isomorphism follows from Prop.1.1 (i) and is made completely explicit by the remark following that proposition. We claim that the homomorphisms  $f_{\mathfrak{R}}$  that were introduced above correspond exactly to the Frobenius elements of the primes over  $\mathfrak{R}$  in  $\text{Gal}(F(\sqrt[M]{O^*})/F)$ . To see this, we let  $\varepsilon \in O^*$  and we note that

$$f_{\mathfrak{R}}(\varepsilon) = \sum_{\sigma \in G} x_{\sigma}[\sigma] \in (\mathbf{Z}/M\mathbf{Z})[G],$$

where  $x_{\sigma}$  is determined by  $\sigma^{-1}(\varepsilon)^{(r-1)/M} \equiv \zeta_M^{x_{\sigma}} \pmod{\mathfrak{R}}$ . The homomorphism in  $\text{Hom}_{\mathbf{Z}}(O^*/\pm O^{*M}, \mathbf{Z}/M\mathbf{Z})$  that corresponds to it maps  $\varepsilon$  to  $x_1$ . To this homomorphism Kummer theory associates the automorphism  $\tau$  in  $\text{Gal}(F(\sqrt[M]{O^*})/F)$  for which  $\tau(\sqrt[M]{\varepsilon})/\sqrt[M]{\varepsilon}$  is the unique lift of  $\varepsilon \pmod{\mathfrak{R}}$  to  $\zeta_M^{x_1} \in \mu_M \subset F^*$ . That implies that  $\tau(\sqrt[M]{\varepsilon}) \equiv \sqrt[M]{\varepsilon}^{\tau} \pmod{\mathfrak{R}}$ . It follows that  $f_{\mathfrak{R}}$  corresponds to the Frobenius element of the prime  $\mathfrak{R}$ .

By Chebotarev’s Density Theorem every element of  $\text{Hom}_R(O^*/\{\pm 1\}, R)$  is of the form  $f_{\mathfrak{R}}$  for some prime  $\mathfrak{R}$  of degree 1. Since  $\text{Cyc}/\{\pm 1\}$  is isomorphic to the augmentation ideal of  $\mathbf{Z}[G]$ , the  $G$ -norm kills every  $R$ -homomorphism

$$\text{Cyc}/\pm \text{Cyc}^M \longrightarrow R.$$

Therefore the map  $\text{Hom}_R(\text{Cyc}/\pm \text{Cyc}^M, R) \longrightarrow I$  given by  $f \mapsto f(\eta)$  is well defined. Since it is injective and since the orders of the two groups are equal, it is an isomorphism of  $R$ -modules. It follows that

$$B[M]^{\perp} \cong I/\{f(\eta) : f \in \text{Hom}_R(O^*/\pm O^{*M}, R)\} = I/\{f_{\mathfrak{R}}(\eta) : \mathfrak{R} \in S\}.$$

This proves the theorem. □

### 3. THE COMPUTATIONS

In this section we apply Theorem 2.2 and explain how the tables in section 4 were obtained.

Let  $l$  be an odd prime and let  $G = \text{Gal}(\mathbf{Q}(\zeta_l + \zeta_l^{-1})/\mathbf{Q})$ . The group  $G$  is naturally isomorphic to the cyclic group  $G = (\mathbf{Z}/l\mathbf{Z})^*/\{\pm 1\}$ . We choose a primitive root  $g \pmod{l}$ . Then the ring homomorphism  $\mathbf{Z}[X]/(X^{(l-1)/2} - 1) \xrightarrow{\cong} \mathbf{Z}[G]$  that maps the variable  $X$  to the automorphism given by  $\zeta_l + \zeta_l^{-1} \mapsto \zeta_l^g + \zeta_l^{-g}$  is an isomorphism.

Any finite  $\mathbf{Z}[G]$ -module  $A$  is a product of its  $p$ -parts  $A \otimes \mathbf{Z}_p$ . Each  $p$ -part is a module over the ring  $\mathbf{Z}_p[G] \cong \mathbf{Z}_p[X]/(X^{(l-1)/2} - 1)$ . We write  $(l - 1)/2 = p^a m$ , where  $p^a$  is the order of the  $p$ -part  $\pi$  of  $G$ . There is a natural isomorphism

$\mathbf{Z}_p[G] \cong \mathbf{Z}_p[X]/(X^m - 1)[\pi]$ . Since  $p$  does not divide  $m$ , we can write  $X^m - 1 = \prod_{\varphi} \varphi(X)$  as a product of distinct irreducible polynomials  $\varphi(X) \in \mathbf{Z}_p[X]$ . This gives rise to natural isomorphisms of  $\mathbf{Z}_p$ -algebras

$$\begin{aligned} \mathbf{Z}_p[G] &\cong \mathbf{Z}_p[X]/(X^{(l-1)/2} - 1) \cong \mathbf{Z}_p[X]/(X^m - 1)[\pi] \cong \prod_{\varphi} \mathbf{Z}_p[X]/(\varphi(X))[\pi] \\ &\cong \mathbf{Z}_p[X]/(X^{p^a m} - 1) \cong \prod_{\varphi} \mathbf{Z}_p[X]/(\varphi(X^{p^a})). \end{aligned}$$

The ring homomorphisms

$$\mathbf{Z}_p[X]/(\varphi(X))[\pi] \xrightarrow{\cong} \mathbf{Z}_p[X]/(\varphi(X^{p^a}))$$

that map  $X$  to  $X^{p^a}$  and a generator of  $\pi$  to  $X^m$  provide explicit isomorphisms between the corresponding factors of the two products. The rings  $\mathbf{Z}_p[X]/(\varphi(X^{p^a}))$  can therefore be viewed as group rings with coefficients in an extension of  $\mathbf{Z}_p$ . They are complete local  $\mathbf{Z}_p[G]$ -algebras with maximal ideals  $(p, \varphi(X))$  and residue fields isomorphic to  $\mathbf{F}_p[X]/(\varphi(X))$ . The orders of the residue fields are given by  $q = p^f$ , where  $f = \deg \varphi$ .

The decomposition of the ring  $\mathbf{Z}_p[G]$  enables us to write each  $p$ -part of  $A$  as  $A \otimes \mathbf{Z}_p \cong \prod_{\varphi} A_{\varphi}$  where the ‘‘eigenspace’’  $A_{\varphi}$  is given as  $A_{\varphi} = A \otimes \mathbf{Z}_p \otimes_{\mathbf{Z}_p[G]} \mathbf{Z}_p[X]/(\varphi(X^{p^a}))$ . Each eigenspace  $A_{\varphi}$  is a module over the corresponding  $\mathbf{Z}_p[G]$ -algebra  $\mathbf{Z}_p[X]/(\varphi(X^{p^a}))$ . It admits a filtration with simple subquotients, all of which are isomorphic to the residue field  $\mathbf{F}_q = \mathbf{F}_p[X]/(\varphi(X))$ .

The residue fields of the ring  $\mathbf{Z}[G]$  are precisely the residue fields of the various local rings  $\mathbf{Z}_p[X]/(\varphi(X^{p^a}))$ . Every finite  $\mathbf{Z}[G]$ -module admits a Jordan-Hölder filtration whose simple factors are one-dimensional vector spaces over these residue fields. The *order* of such a simple Jordan-Hölder factor is the order  $q = p^f$  of the residue field and its *degree*  $d$  is the order of  $X$  modulo  $\varphi(X)$ . This implies that  $d$  divides  $(l - 1)/2$ . The order of  $p \pmod{d}$  is equal to  $f$ . Therefore  $d$  divides  $q - 1$  as well.

This applies in particular to the module  $B$  of units of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  modulo cyclotomic units and to the ideal class group. It also applies to the modules  $B[M]^{\perp}$  that were discussed in section 2. By Prop.1.2 (i), the simple Jordan-Hölder factors of  $B$  are precisely the ones of the various  $B[M]^{\perp}$ . Simple Jordan-Hölder factors of  $B$  of degree  $d$  are invariant under the unique subgroup of  $G$  of index  $d$ . They ‘‘appear’’ in the group of units modulo cyclotomic units associated to the unique subfield of degree  $d$  in  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . It seems difficult to predict, in general, which simple factors the module  $B$  admits. However, there is the following general result.

**Proposition 3.1.** *Let  $l > 2$  be a prime. The module  $B = O^*/\text{Cyc}$  does not admit any simple Jordan-Hölder factors of degree  $d = 1$ . In particular, it does not admit any such factors of order  $q = 2$ .*

*Proof.* Let  $M > 1$  be a power of a prime  $p$  and let  $(l - 1)/2 = p^a m$  with  $p$  not dividing  $m$ . By Prop.5.1 (i), the  $G$ -invariants of  $B$  and hence of its  $p$ -part  $B \otimes \mathbf{Z}_p$  are zero. This implies that the co-invariants  $B \otimes \mathbf{Z}_p$  modulo  $(X - 1)(B \otimes \mathbf{Z}_p)$  are zero and hence, by Nakayama’s Lemma, that the module  $(B \otimes \mathbf{Z}_p)/(X^{p^a} - 1)(B \otimes \mathbf{Z}_p)$  is also zero. In other words  $B_{\varphi} = 0$  for  $\varphi = X - 1$ . This shows that  $B$  does not admit any Jordan-Hölder factors of degree  $d = 1$ .



Simple Jordan-Hölder factors of order  $q = 2$  do not occur since their degrees  $d$  must divide  $q - 1 = 1$ . This proves the proposition.  $\square$

We formulate the results of the previous section in terms of polynomials. Let  $M > 1$  be a power of a prime  $p$ , let  $S$  denote the set of primes  $r$  for which  $r \equiv \pm 1 \pmod{l}$  and  $r \equiv 1 \pmod{2M}$ , and let  $r \in S$ . In terms of the isomorphism  $\mathbf{Z}[G] \cong \mathbf{Z}[X]/(X^{(l-1)/2} - 1)$  mentioned above, we have that

$$f_{\mathfrak{R}}(\eta) = \sum_{k=1}^{(l-1)/2} \log_r \left( \frac{\zeta_l^{g^k} - \zeta_l^{-g^k}}{\zeta_l^{g^{k-1}} - \zeta_l^{-g^{k-1}}} \right) \cdot X^k \in (\mathbf{Z}/M\mathbf{Z})[X]/(X^{(l-1)/2} - 1).$$

Here  $\log_r(x)$  denotes the element  $i \in \mathbf{Z}/M\mathbf{Z}$  for which  $\zeta_M^i$  is congruent to  $x^{(r-1)/M}$  modulo the prime  $\mathfrak{R}$ . Notice that changing the choice of the prime  $\mathfrak{R}$  over  $\mathfrak{r}$  only changes the choice of  $\zeta_M$  and therefore multiplies  $f_{\mathfrak{R}}(\eta)$  by a unit of  $\mathbf{Z}/M\mathbf{Z}$ . Changing the prime  $\mathfrak{r}$  over  $r$ , on the other hand, changes the choice of  $\zeta_l$  and multiplies  $f_{\mathfrak{R}}(\eta)$  by a power of  $X$ . Therefore  $f_{\mathfrak{R}}(\eta)$  depends, up to units, only on the prime  $r$ . Since  $\eta$  has norm  $\pm 1$ , the element  $f_{\mathfrak{R}}(\eta)$  is contained in the augmentation ideal  $I \subset (\mathbf{Z}/M\mathbf{Z})[X]/(X^{(l-1)/2} - 1)$ . This is the ideal generated by  $X - 1$ . Dividing by  $X - 1$  gives an isomorphism  $I \rightarrow (\mathbf{Z}/M\mathbf{Z})[X]/((X^{(l-1)/2} - 1)/(X - 1))$ . We denote the image of  $f_{\mathfrak{R}}(\eta)$  in this ring by  $f_r(X)$ . Up to multiplication by units, this polynomial only depends on the prime  $r$ . We have that

$$f_r(X) = \sum_{k=1}^{(l-1)/2} \log_r \left( \zeta_l^{g^k} - \zeta_l^{-g^k} \right) \cdot X^k \in (\mathbf{Z}/M\mathbf{Z})[X] \Big/ \left( \frac{X^{(l-1)/2} - 1}{X - 1} \right).$$

**Theorem 3.2.** *Using the notation above, we have that*

$$B[M]^\perp \cong (\mathbf{Z}/M\mathbf{Z})[X] \Big/ \left\langle \frac{X^{(l-1)/2} - 1}{X - 1}, f_r(X) : r \in S \right\rangle.$$

*Proof.* Here  $B[M]^\perp = \text{Hom}_R(B[M], R)$ , where  $R = (\mathbf{Z}/M\mathbf{Z})[G]$ . The result is immediate from Theorem 2.2.  $\square$

Next we fix a prime  $l$  and a prime power  $q = p^f$ , and we explain how to compute the part of  $B$  that admits a Jordan-Hölder filtration with simple factors of order  $q$ . In the range of our calculations we have that  $l < 10,000$  and  $q < 80,000$ .

**Step 1.** For a given  $l$  we first decide whether  $B$  admits any Jordan-Hölder factors of order  $q$  at all. The possible degrees  $d$  of these factors all divide

$$\delta = \text{gcd}((l - 1)/2, q - 1).$$

By Prop.3.1 Jordan-Hölder factors of degree  $d = 1$  do not occur. Therefore the first step is trivial when  $\delta = 1$ . We use Theorem 3.2 with  $M = p$ . Since  $B^\perp/pB^\perp \cong B[p]^\perp$ , Nakayama’s Lemma and Prop.1.2 (i) imply that the module  $B$  admits no Jordan-Hölder factors of order  $q$  if and only if  $B[p]^\perp/\varphi B[p]^\perp$  is trivial for all divisors  $\varphi$  of  $X^m - 1$  of degree  $f$ . We check this for all  $\varphi$  simultaneously by calculating several polynomials

$$f_r(X) = \sum_{j=1}^{\delta} \log_r \left( \prod_{k \equiv j \pmod{\frac{l-1}{2\delta}}} (\zeta^{g^k} - \zeta^{-g^k}) \right) \cdot X^j$$

in the ring  $(\mathbf{Z}/p\mathbf{Z})[X]/(\frac{X^\delta-1}{X-1})$ . Here  $r \in S$  and  $g$  is the primitive root modulo  $l$  used above. The point is that every irreducible divisor  $\varphi$  of degree  $f$  of  $X^m - 1$  also divides  $\frac{X^\delta-1}{X-1}$ . It is important in practice to *first* compute the products over  $k \equiv j \pmod{(l-1)/2\delta}$  and only *then* their logarithms in  $\mathbf{Z}/p\mathbf{Z}$ .

Then one puts  $d_0 = \frac{X^\delta-1}{X-1}$  and computes  $d_i = \gcd(d_{i-1}, f_{r_i}(X))$  for various primes  $r_1, r_2, \dots \in S$ . Each  $d_i$  divides its predecessor  $d_{i-1}$ . As soon as  $d_i$  is not divisible by any irreducible polynomial of degree  $f$ , we stop. The formula of Theorem 3.2 implies that  $B[p]^\perp / \varphi B[p]^\perp = 0$  for all  $\varphi$  of degree  $f$ , and hence that  $B^\perp$  as well as  $B$  do not admit any Jordan-Hölder factors of order  $q$ . This is what happens most of the time. It is important that this part of the program is efficient. When  $d_i$  admits an irreducible divisor  $\varphi$  of degree  $f$  for ever larger values of  $i$ , we also stop, but this time we believe, on the basis of Theorem 2.2, that  $B$  admits a Jordan-Hölder factor corresponding to the polynomial  $\varphi$ , and we proceed to the second step of the algorithm.

The second and third steps of the algorithm are executed only very rarely. They need not be very efficient.

**Step 2.** Since the polynomials  $d_i$  of the first step divide  $X^{q-1} - 1 \in (\mathbf{Z}/p\mathbf{Z})[X]$ , they are squarefree. For each  $\varphi(X)$ , an irreducible factor of degree  $f$  that divides all  $d_i$ 's, we want to determine the structure of the eigenspace  $B_\varphi^\perp$ . We do the following. For  $M = p, p^2, p^3, \dots$  we compute a lift of  $\varphi(X)$  to an irreducible divisor of  $X^{q-1} - 1 \in \mathbf{Z}/M\mathbf{Z}[X]$ . We use the description of  $B[M]^\perp$  of Theorem 3.2 and take its  $\varphi$ -part. We let

$$f_r(X) = \sum_{j=1}^{p^a d} \log_r \left( \prod_{k \equiv j \pmod{\frac{l-1}{2dp^a}}} (\zeta_l^{g^k} - \zeta_l^{-g^k}) \right) \cdot X^j$$

in the ring  $(\mathbf{Z}/M\mathbf{Z})[X]/(\varphi(X^{p^a}))$ . Here  $d$  denotes the degree of the Jordan-Hölder factor corresponding to  $\varphi$ , and  $p^a$  is the exact power of  $p$  dividing  $(l-1)/2$ . We have that

$$B[M]_\varphi^\perp \cong (\mathbf{Z}/M\mathbf{Z})[X]/\langle \varphi(X^{p^a}), f_r(X) : r \in S \rangle,$$

where  $S$  denotes the set of primes that are congruent to 1 (mod  $M$ ) and congruent to  $\pm 1$  (mod  $l$ ).

Let  $R$  denote the finite local ring  $(\mathbf{Z}/M\mathbf{Z})[X]/(\varphi(X^{p^a}))$ . Note that  $R$  is isomorphic to the group ring  $(W/MW)[\pi]$ , where  $W$  denotes the  $p$ -adic ring  $\mathbf{Z}_p[X]/(\varphi(X))$ . We let  $I_0$  be the zero ideal of  $R$ , and then pick several primes  $r_1, r_2, \dots \in S$  and compute the  $R$ -ideals  $I_i = I_{i-1} + (f_{r_i}(X))$ . Each  $I_i$  contains its predecessor  $I_{i-1}$ . If our belief in the previous step was justified, the ideals  $I_i$  will stabilize at some nonunit ideal  $\mathcal{I}^{(M)}$  of  $R$ . There is a surjective homomorphism

$$R/\mathcal{I}^{(M)} \longrightarrow B[M]_\varphi^\perp,$$

which we then believe to be an isomorphism. We proceed in this way for  $M = p, p^2, \dots$  and compute the orders  $o(M)$  of the quotients  $(\mathbf{Z}/M\mathbf{Z})[X]/(\varphi(X^{p^a}) + \mathcal{I}^{(M)})$ . Since these rings are supposed to be isomorphic to  $B[M]_\varphi^\perp$ , the sequence  $o(p), o(p^2), \dots$  will be nondecreasing. For some  $M$  we will then find that  $o(pM) = o(M)$ . It follows that  $M$  annihilates  $(\mathbf{Z}/pM\mathbf{Z})[X]/(\varphi(X^{p^a}) + \mathcal{I}^{(pM)})$  and hence its quotient

$B[pM]_{\varphi}^{\perp}$ . Nakayama’s Lemma implies then that  $M$  annihilates  $B_{\varphi}^{\perp}$ . Therefore we have an explicit ideal  $\mathcal{I}^{(M)} \subset R$  and a surjection

$$R/\mathcal{I}^{(M)} \longrightarrow B_{\varphi}^{\perp},$$

which we believe to be an isomorphism. All computations are gcd computations in the rings  $R = (\mathbf{Z}/M\mathbf{Z})[X]/(\varphi(X^{p^a}))$ .

In the third and last step we attempt to *prove* that  $B_{\varphi}^{\perp}$  is actually isomorphic to the cyclic module  $R/\mathcal{I}^{(M)}$  that has been computed in the second step. The method can already be found in a paper by G. and M.-N. Gras [10].

**Step 3.** Let  $\varphi$  be as in Step 2. Let  $M$  be a power of  $p$  that kills  $B_{\varphi}^{\perp}$  and, as before, let  $R$  denote the ring  $(\mathbf{Z}/M\mathbf{Z})[X]/(\varphi(X^{p^a}))$ . Consider the exact sequence

$$0 \longrightarrow B[M] \longrightarrow \text{Cyc}/\pm \text{Cyc}^M \longrightarrow \text{Cyc}/\pm O^{*M} \longrightarrow 0,$$

where the first homomorphism is given by  $\varepsilon \mapsto \varepsilon^M$ . Recall that the  $(\mathbf{Z}/M\mathbf{Z})[G]$ -module  $\text{Cyc}/\pm \text{Cyc}^M$  is isomorphic to the augmentation ideal of  $(\mathbf{Z}/M\mathbf{Z})[G]$ . Since  $\varphi \neq X - 1$ , the  $\varphi$ -part  $R$  of  $(\mathbf{Z}/M\mathbf{Z})[G]$  is isomorphic to the  $\varphi$ -part of its augmentation ideal. Since  $M$  annihilates  $B_{\varphi}$ , we obtain the exact sequence

$$0 \longrightarrow B_{\varphi} \longrightarrow R \longrightarrow C_{\varphi} \longrightarrow 0$$

of  $R$ -modules. Here  $C$  denotes the  $G$ -module  $\text{Cyc}/\pm O^{*M}$ . By Step 2, the first condition of Prop.1.2 (iv) with  $J = \mathcal{I}^{(M)}$  is satisfied. We now check the second condition: we must show that the  $\text{Ann}_R(J)$  annihilates  $C_{\varphi}$ .

For every  $(\mathbf{Z}/M\mathbf{Z})[G]$ -module  $A$  we have that  $A_{\varphi} \cong \frac{X^{(l-1)/2}-1}{\varphi(X^{p^a})}A$ . Therefore  $\text{Ann}_R(J)$  annihilates  $C_{\varphi}$  if and only if  $\frac{X^{(l-1)/2}-1}{\varphi(X^{p^a})}\text{Ann}_R(J)$  annihilates  $C$ . This can be checked directly by a computation similar to the one explained below. In order to keep the objects as small as possible, we do something slightly more subtle. Let  $a'$  be the smallest exponent such that  $\varphi(X^{p^{a'}}) \in \mathcal{I}^{(M)}$ . Let  $R' = (\mathbf{Z}/M\mathbf{Z})[X]/(\varphi(X^{p^{a'}}))$  and let  $J'$  denote the image of the ideal  $\mathcal{I}^{(M)}$  in  $R'$ . The ring  $R'$  is isomorphic to the group ring  $(\mathbf{Z}/M\mathbf{Z})[X]/(\varphi(X))[\pi']$ , where  $\pi'$  is the unique quotient of  $\pi$  of order  $p^{a'}$ . We have that  $R/J \cong R'/J'$ . Since the rings  $R$  and  $R'$  are Gorenstein, we have that  $\#\text{Ann}_R(J) = \#\text{Ann}_{R'}(J')$ . This implies that  $\text{Ann}_R(J) = \frac{\varphi(X^{p^a})}{\varphi(X^{p^{a'}})}\text{Ann}_{R'}(J')$ . We conclude that

$$\text{Ann}_R(J) \text{ annihilates } C_{\varphi} \iff \frac{X^{(l-1)/2}-1}{\varphi(X^{p^{a'}})}\text{Ann}_{R'}(J') \text{ annihilates } \text{Cyc}/\pm O^{*M}.$$

In order to check this, we compute a finite set of generators  $g(X)$  of  $\text{Ann}_{R'}(J')$ . For each  $g(X)$  and  $j = 1, \dots, dp^{a'}$  we compute a high precision approximation  $u_j$  to  $\tau_j(\eta^x) \in \mathbf{R}$ , where  $x \in \mathbf{Z}[X]$  is a lift of the polynomial

$$\frac{X^{\frac{l-1}{2}} - 1}{\varphi(X^{p^{a'}})} \cdot g(X) \in (\mathbf{Z}/M\mathbf{Z})[X].$$

Here  $\tau_j$  denotes the embedding  $\mathbf{Q}(\zeta_l + \zeta_l^{-1}) \hookrightarrow \mathbf{R}$  given by  $\zeta_l + \zeta_l^{-1} \mapsto 2\cos(2g^j\pi/l)$ . Note that  $(X^{(l-1)/2} - 1)/\varphi(X^{p^{a'}})$  is divisible by the norm map

$$(X^{(l-1)/2} - 1)/(X^{dp^{a'}} - 1)$$

from  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  to its subfield of degree  $dp^{a'}$ . Therefore  $\tau_j(\eta^x) = \tau_{j'}(\eta^x)$  whenever  $j \equiv j' \pmod{dp^{a'}}$ .

Rounding off the coefficients of the polynomial  $\prod_{j=1}^{dp^{a'}}(t-u_j)$ , we obtain a polynomial  $F(t) \in \mathbf{Z}[t]$  that has  $\eta^x$  and its conjugates as zeroes. If  $M$  is odd, we compute the product  $\prod_{j=1}^{dp^{a'}}(t-\sqrt[M]{u_j}) \in \mathbf{R}[t]$ . It should have coefficients that are very close to integers. This already indicates that the roots of  $F(t)$  are  $M$ -th powers, but does not prove that they are  $M$ -th powers of elements in the field  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . To be sure of that, we round off the coefficients of  $F(t)$  and check that the resulting polynomial  $G(t) \in \mathbf{Z}[t]$  divides  $F(t^M)$ .

If  $M$  is a power of 2, there are sign ambiguities. The numbers  $u_i$  all have the same sign. If they are negative, we change their signs. Then, for all  $2^{d2^{a'}-1}$  possible choices of signs, we consider the polynomial  $(t-\sqrt[M]{u_1})\prod_{j=2}^{d2^{a'}}(t\pm\sqrt[M]{u_j}) \in \mathbf{R}[t]$ . Only one of these has coefficients that are very close to integers. We then check that the polynomial  $G(t) \in \mathbf{Z}[t]$  obtained by rounding off these coefficients divides  $F(t^M)$ . In either case, if the approximations are sufficiently accurate, we have proved that  $\eta^x$  is an  $M$ -th power in  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . It follows from Proposition 1.2 (i) that  $B_\varphi^\perp$  is actually isomorphic to  $R/\mathcal{I}^{(M)}$ , as required.

**Example.** For  $l = 4297$  and  $q = 4$  the order of the 2-part  $\pi$  of the Galois group  $G_l$  is 4. In the notation used above, this means that  $a = 2$ . The only simple Jordan-Hölder factor of order 4 corresponds to the polynomial  $\varphi = X^2 + X + 1$ . We find in the first step that  $\varphi$  divides all the gcd's  $d_i$  and we are led to believe that  $B_\varphi$  is nontrivial. The eigenspace  $B_\varphi$  is a module over the ring  $\mathbf{Z}_2[X]/(\varphi(X^4)) \cong W[\pi] \cong W[T]/((1+T)^4-1)$ . Here  $W = \mathbf{Z}_2[\zeta]$ , where  $\zeta = X^4$  is a cube root of unity. As in Iwasawa theory, the polynomial  $1+T = X^3$  corresponds to a generator of  $\pi$ .

Since the maximal ideal of the local ring  $W[\pi] \cong W[T]/((1+T)^4-1)$  is equal to  $(T, 2)$ , the parameter  $T$  is convenient for doing computations. Every element of  $W[\pi]$  can be written as a unit times a “Weierstrass polynomial” of the form  $2^\mu(T^\lambda + \dots + a_0)$  with  $a_i \equiv 0 \pmod{2}$  for  $0 \leq i < \lambda$ . These Weierstrass polynomials are not unique in general. The polynomials  $f_r$  that are listed below are such Weierstrass polynomials associated to the polynomials  $f_r$  of Thm.2.3 (and are only well defined up to units).

Next we perform the second step for  $M = 2, 4, 8, \dots$ . For  $M = 2$ , we compute the ideal  $\mathcal{I}^{(2)}$  of  $(W/2W)[\pi]$  generated by the polynomials  $f_r$  in the table. Already the first polynomial  $T^2$  generates  $\mathcal{I}^{(2)}$ . After five more tries, we believe that adding more polynomials  $f_r$  will not enlarge the ideal any further. So, the module  $(W/2W)[\pi]/(T^2) \cong W[T]/(T^2, 2)$  of order  $4^2$  admits a homomorphism onto  $B_\varphi^\perp[2]$  which we believe to be an isomorphism.

$M = 2.$		$M = 4.$	
$r$	$f_r \in (W/2W)[\pi]$	$r$	$f_r \in (W/4W)[\pi]$
17189	$T^2$	111721	$2(1 + \zeta)T + T^2$
111721	$T^2$	171881	$2\zeta T + T^2$
171881	$T^2$	180473	$2(1 + \zeta)T + T^2$
180473	$T^2$	214849	$2(1 + \zeta)T + T^2$
214849	$T^2$	283601	$2(1 + \zeta)T + 2T^2 + T^3$
283601	$T^3$	378137	$2T + T^2$

$M = 8.$

$r$	$f_r \in (W/8W)[\pi]$
214849	$4 + (2 + 6\zeta)T + T^2$
283601	$4\zeta + (2 + 2\zeta)T + 2T^2 + T^3$
687521	$4 + (2 + 2\zeta)T + T^2$
833617	$4 + (2 + 2\zeta)T + T^2$
893777	$4\zeta + (2 + 6\zeta)T + (4 + 4\zeta)T^2 + T^3$
1031281	$6T + T^2$
1306289	$4\zeta + (4 + 6\zeta)T + T^2$
1727393	$4 + (6 + 2\zeta)T + T^2$

$M = 16.$

$r$	$f_r \in (W/16W)[\pi]$
214849	$(4 + 8\zeta) + (10 + 6\zeta)T + T^2$
687521	$4 + (10 + 2\zeta)T + T^2$
1727393	$(12 + 8\zeta) + (14 + 2\zeta)T + T^2$
1864897	$(8 + 4\zeta) + (4 + 6\zeta)T + T^2$
1925057	$(12 + 8\zeta) + (14 + 2\zeta)T + T^2$
2062561	$(12 + 12\zeta) + (14 + 8\zeta)T + 10\zeta T^2 + T^3$
3102433	$(4 + 4\zeta) + (2 + 4\zeta)T + (2 + 12\zeta)T^2 + T^3$
3300097	$(12 + 4\zeta) + (4 + 4\zeta)T + T^2$

For  $M = 4$ , we find the ideal  $\mathcal{I}^{(4)} = (T^2, 2T)$  of  $(W/4W)[\pi]$ . The ideal  $\mathcal{I}^{(4)}$  is already generated by the first two polynomials  $f_r$ . Once again we believe that adding more polynomials  $f_r$  will not enlarge the ideal any further. Therefore the module  $(W/4W)[\pi]/(T^2, 2T) \cong W[T]/(T^2, 2T, 4)$  of order  $4^3$  admits a homomorphism onto  $B_\varphi^\perp[4]$  which we believe to be an isomorphism.

For  $M = 8$  the polynomials  $f_r$  generate the ideal

$$\mathcal{I}^{(8)} = (T^2 + 2T, 2T + 4(\zeta + 1))$$

of  $(W/8W)[\pi]$ . It follows that the module

$$(W/8W)[\pi]/(T^2 + 2T, 2T + 4(\zeta + 1)) \cong W[T]/(T^2 + 2T, 2T + 4(\zeta + 1), 8)$$

of order  $4^4$  admits a homomorphism onto  $B_\varphi^\perp[8]$ . Actually, already the first two polynomials  $f_r$  generate  $\mathcal{I}^{(8)}$ . We suspect once again that this map is, in fact, an isomorphism.

For  $M = 16$  we find that the polynomials  $f_r$  generate the ideal

$$\mathcal{I}^{(16)} = (T^2 + 2T, 2T + 4(\zeta + 1), 8)$$

of  $(W/16W)[\pi]$ . The module

$$(W/16W)[\pi]/(T^2 + 2T, 2T + 4(\zeta + 1), 8) \cong W[T]/(T^2 + 2T, 2T + 4(\zeta + 1), 8)$$

admits a surjective homomorphism onto  $B_\varphi^\perp[16]$ . This module is isomorphic to the one we found for  $M = 8$ . Since it is killed by 8, we have that  $B_\varphi^\perp = B_\varphi^\perp[8]$ .

This concludes Step 2. We now suspect that  $B_\varphi^\perp$  is isomorphic to  $R/J$  with  $R = (O/8O)[\pi]$  and  $J = (T^2 + 2T, 2T + 4(\zeta + 1))$ .

Finally we do the computations of Step 3. First we observe that  $\varphi(X^2) = \zeta^2(T^2 + 2T)$  is in  $J$ . Therefore, in the notation used above, we have that  $a' = 1$ .

So  $R/J \cong R'/J'$  with  $R' = (W/8W)[\pi'] = (W/8W)[T]/(T^2 + 2T)$  and  $J' = (2T - 4(\zeta + 1))$ . Here  $\pi'$  denotes the order 2 quotient of  $\pi$ . One checks that  $\text{Ann}_{R'}(J') = (4, T + 2\zeta)$ . The elements  $x \in \mathbf{Z}[G]$  introduced above are

$$x = \frac{X^{2148} - 1}{X^4 + X^2 + 1} \cdot g(X),$$

with  $g(X) = 4$  and  $g(X) = T + 2\zeta = X^3 - 1 + 2X^2$ . We raise  $\eta$  to the symbolic power  $(X^{2148} - 1)/(X^4 + X^2 + 1)$  and compute its image under  $\tau_j$  for  $j = 1, 2, \dots, 6$ . In other words, we compute  $\tau_j(N(\eta)^{X^2-1})$  for  $j = 1, 2, \dots, 6$ . Here  $N$  denotes the norm map from  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  to its degree 6 subfield. The resulting real numbers appear to be the zeroes of the following polynomial in  $\mathbf{Z}[t]$ :

$$\begin{aligned} F(t) = & t^6 + 900176138747448t^5 + 185766377755735633731676590t^4 \\ & + 127973707497873453310375901520t^3 - 2553521583555102412987t^2 \\ & + 207337205736t - 1. \end{aligned}$$

Let  $\varepsilon$  denote a zero of  $F(t)$  in the degree 6 subfield of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . We raise it to the symbolic powers  $g(X) = 4$  and  $T + 2\zeta$  and then check whether they are 8th powers. When  $g(X) = 4$ , this boils down to checking whether  $\varepsilon$  is a square. Indeed, the square root of  $\varepsilon$  turns out to be a zero of the polynomial

$$G_1(t) = t^6 + 1142996t^5 + 22804194t^4 + 70290306t^3 - 2208643t^2 + 17182t + 1.$$

In addition,  $G_1(t)$  divides  $F(t^2)$ .

Next, the 8th root of  $\varepsilon^{T+2\zeta}$  is a root of the polynomial

$$G_2(t) = t^6 + 17182t^5 + 64470t^4 + 51544t^3 - 17173t^2 - 6t + 1,$$

and  $G_2(t)$  divides  $H(t^8)$ , where  $H(t)$  denotes the minimum polynomial of  $\varepsilon^{T+2\zeta}$ .

This shows that  $\varepsilon^4$  and  $\varepsilon^{T+2\zeta}$  are 8th powers in  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . With this computation we have now verified the second condition of Prop.1.2 (iv) and we can conclude that the module  $B_\varphi^\perp$  is actually isomorphic to  $(W/8W)[\pi]/(T^2 + 2T, 2T - 4(\zeta + 1)) \cong W[T]/(T^2 + 2T, 2T - 4(\zeta + 1), 8)$ .

#### 4. TABLES

In this section we discuss the numerical results. Recall that for an odd prime  $l$ , the number  $\tilde{h}_l^+$  denotes the order of the largest submodule of  $B_l$  or of  $Cl_l^+$  that admits a Jordan-Hölder filtration with simple factors of order  $q < 80,000$ .

TABLE 4.1. Small  $\tilde{h}_l^+$ .

$\tilde{h}_l^+$	freq	%	$\tilde{h}_l^+$	freq	%	$\tilde{h}_l^+$	freq	%
1	925	75.3%	8	8	0.7%	15	0	0.0%
3	37	3.0%	9	12	1.0%	16	12	1.0%
4	47	3.8%	11	14	1.1%	17	6	0.5%
5	33	2.7%	12	0	0.0%	19	6	0.5%
7	26	2.1%	13	13	1.0%	20	0	0.0%

TABLE 4.2. Large  $\tilde{h}_l^+$ .

$l$	$\tilde{h}_l^+$	$l$	$\tilde{h}_l^+$	$l$	$\tilde{h}_l^+$	$l$	$\tilde{h}_l^+$
1231	211	4481	291	2417	697	9421	3388
1459	247	3121	305	5557	1387	6577	5321
3931	256	7489	448	5051	1451	3547	16777
4297	256	641	495	7753	1875	7841	26944
1297	275	9551	541	3301	2416	8017	130473

There are 1228 odd primes  $l$  less than 10,000. For 925 of these we have that  $\tilde{h}_l^+ = 1$ . The remaining 303 primes  $l$  are listed in the Main Table, at the end of the paper. The numbers  $\tilde{h}_l^+$  are in the second column. They are given as a product of the orders of their simple Jordan-Hölder factors. The degrees  $d$  of the Jordan-Hölder factors are indicated in the third column. They are listed in the same order as the Jordan-Hölder factors themselves. If a simple Jordan-Hölder factor  $\mathbf{F}_p[X]/(\varphi(X))$  of order  $q$  occurs with multiplicity greater than 1, we write  $q^{s_0} \cdot q^{s_1} \cdot q^{s_2} \cdots$  with corresponding degrees  $d, dp, dp^2, \dots$  to indicate that the orders of  $B_\varphi^\perp$  modulo  $\varphi(X^{p^i})$  are  $q^{s_0 + \dots + s_i}$  for  $i = 0, 1, 2, \dots$ . Finally, an asterisk in the Main Table indicates that the corresponding subfield of degree  $d$  belongs to one of the families of abelian number fields of small degree that we discuss below. A simplified form of the Main Table already appeared in [23, p.366]. Note however that the value of  $\tilde{h}_l^+$  for  $l = 9829$  given there is false. The correct value is  $\tilde{h}_{9829}^+ = 5$ .

We single out some of the numerical results. Table 4.1 contains the frequencies of the primes  $l$  for which  $\tilde{h}_l^+ \leq 20$ . Since simple Jordan-Hölder factors cannot have order 2 by Prop. 3.1, we always have that  $\tilde{h}_l^+ \not\equiv 2 \pmod{4}$ .

Table 4.2 contains the largest values of  $\tilde{h}_l^+$  that we found for  $l < 10,000$ .

Most of the 354 simple Jordan-Hölder factors of  $B_l$ , occur with multiplicity 1. There are 35 exceptions. In Tables 4.3 and 4.4 we present the Galois module structure of the eigenspaces  $B_\varphi^\perp$  whose Jordan-Hölder filtration has length at least 2. Here  $q = p^f$  denotes the order of the simple factors, while  $d$  indicates their degree. In all but three cases there is only one polynomial of degree  $f$ . The exceptions are  $l = 7351, 7753$  and  $8563$ . In these cases there are two polynomials and two eigenspaces  $B_\varphi^\perp$ , only one of which is nontrivial. The order of the  $p$ -part  $\pi$  of  $G_l$  is given in the column indicated by  $\pi$ . The order of  $B_\varphi^\perp$  is given in the column indicated by “#”. Its Galois module structure is given in the last column. In the last column  $W$  denotes the ring  $\mathbf{Z}_2[\zeta_3]$  except when  $l = 3931$ , when it stands for the ring  $\mathbf{Z}_2[\zeta_5]$ . The variable  $T$  is as in Iwasawa theory: the polynomial  $1 + T$  corresponds to a generator of the  $p$ -part  $\pi$  of  $G_l$ . We do not specify the generator.

It is not difficult to derive the Galois module structure of  $B_l$  from the tables. Usually  $B_\varphi$  is isomorphic to  $B_\varphi^\perp$ . Indeed, by Prop.1.2 (iii), we have that  $B_\varphi \cong B_\varphi^\perp$  whenever the length of  $B_\varphi^\perp$  is at most 2. This leaves only the six modules in Table 4.4. One checks that the annihilators of the corresponding ideals are principal for  $l = 2089, 7489$  and  $9337$ . In these cases Prop.1.2 (ii) applies and we still have that  $B_\varphi \cong B_\varphi^\perp$ . In the remaining cases  $B_\varphi$  is not cyclic as a Galois module. It is isomorphic to the annihilator of the module listed in the rightmost column:  $B_\varphi$  is isomorphic to  $(T^2 + 3T + 3, 3T) \subset (\mathbf{Z}/9\mathbf{Z})[\pi]$  for  $l = 7873$  and to

TABLE 4.3.  $B_\varphi^\perp$  of length 2.

$l$	$q$	$d$	$\pi$	$\#$	$B_\varphi^\perp$
349	4	3	2	$4^2$	$W[T]/(T^2, 2)$
709	4	3	2	$4^2$	$W[T]/(T^2, 2)$
937	4	3	4	$4^2$	$W[T]/(T + 2\zeta, 4)$
1129	3	2	3	$3^2$	$\mathbf{Z}_3[T]/(T, 9)$
1777	4	3	8	$4^2$	$W[T]/(T, 4)$
2081	5	2	5	$5^2$	$\mathbf{Z}_5[T]/(T - 5, 25)$
3137	3	2	1	$3^2$	$\mathbf{Z}/9\mathbf{Z}$
3229	3	2	3	$3^2$	$\mathbf{Z}_3[T]/(T + 3, 9)$
3931	16	5	1	$16^2$	$W/4W$
4261	4	3	2	$4^2$	$W[T]/(T^2, 2)$
4357	4	3	2	$4^2$	$W[T]/(T + 2\zeta, 4)$
4409	3	2	1	$3^2$	$\mathbf{Z}/9\mathbf{Z}$
4561	4	3	8	$4^2$	$W[T]/(T^2, 2)$
4933	3	2	9	$3^2$	$\mathbf{Z}_3[T]/(T - 3, 9)$
5281	3	2	3	$3^2$	$\mathbf{Z}_3[T]/(T - 3, 9)$
5521	3	2	3	$3^2$	$\mathbf{Z}_3[T]/(T, 9)$
6247	4	3	1	$4^2$	$W/4W$
6637	3	2	3	$3^2$	$\mathbf{Z}_3[T]/(T - 3, 9)$
7057	7	2	7	$7^2$	$\mathbf{Z}_7[T]/(T + 7, 49)$
7351	7	3	49	$7^2$	$\mathbf{Z}_7[T]/(T, 49)$
7573	3	2	3	$3^2$	$\mathbf{Z}_3[T]/(T, 9)$
7687	4	3	1	$4^2$	$W/4W$
7753	5	4	1	$5^2$	$\mathbf{Z}/25\mathbf{Z}$
8017	3	2	3	$3^2$	$\mathbf{Z}_3[T]/(T + 3, 9)$
8563	7	3	1	$7^2$	$\mathbf{Z}/49\mathbf{Z}$
8581	3	2	3	$3^2$	$\mathbf{Z}_3[T]/(T - 3, 9)$
9109	4	3	2	$4^2$	$W[T]/(T + 2 + 2\zeta, 4)$
9181	5	2	5	$5^2$	$\mathbf{Z}_5[T]/(T + 5, 25)$
9601	4	3	64	$4^2$	$W[T]/(T + 2 + 2\zeta, 4)$

TABLE 4.4.  $B_\varphi^\perp$  of length 3 and 4.

$l$	$q$	$d$	$\pi$	$\#$	$B_\varphi^\perp$
2089	3	2	9	$3^3$	$\mathbf{Z}_3[T]/(T - 3, 27)$
4297	4	3	4	$4^4$	$W[T]/(T^2 + 2T, 2T - 4(\zeta + 1), 8)$
7489	4	3	32	$4^3$	$W[T]/(T + 2 + 4\zeta, 8)$
7873	3	2	3	$3^3$	$\mathbf{Z}_3[T]/(T^2, 3T, 9)$
8761	3	2	3	$3^4$	$\mathbf{Z}_3[T]/(T^2, 3T, 27)$
9337	4	3	4	$4^3$	$W[T]/(T + 4 - 2\zeta, 8)$

$(T^2 + 3T + 3, 9T) \subset (\mathbf{Z}/27\mathbf{Z})[\pi]$  for  $l = 8761$ . For  $l = 4297$ , we have seen in section 3 that  $B_\varphi^\perp$  is a module over the ring  $(W/8W)[\pi/\pi^2]$ . One finds that  $B_\varphi$  is isomorphic to the ideal  $(T + 2\zeta, 4) \subset (W/8W)[\pi/\pi^2]$ . Here  $\zeta$  denotes a cube root of unity and  $W = \mathbf{Z}_2[\zeta]$ .



It is not true in general that the Galois modules  $B_l$  and  $Cl_l^+$  are isomorphic. Indeed, for  $l = 7687$ , the 2-part of the class group  $Cl_l^+$  is killed by 2, while  $B_l$  is not [2]. We prove in section 5 that the  $G_l$ -modules  $Cl_l^+$  and  $B_l$  have isomorphic Galois cohomology groups. In contrast to the case of minus class groups  $Cl_l^-$  that usually have trivial Galois cohomology groups [19], the cohomology groups of  $Cl_l^+$  may be nontrivial. It is not difficult to compute them from the information in Tables 4.3 and 4.4. We leave this to the reader.

Our results are consistent with existing tables. They agree first of all with the results of Van der Linden [22] that we mentioned in the introduction. The simple Jordan-Hölder factors of degree  $d$  are precisely the ones that occur as factors of the class groups of the subfields of degree  $d$  of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . Our results are consistent with various tables [7], [8], [16] of class numbers of cyclic number fields of small degree  $d$ . In all cases we tried, our results were confirmed by the PARI-program [1]. Finally, recent computations by Y. Koyama and K. Yoshino [11] are consistent with our tables.

There are several families of abelian number fields known of low degree with explicitly known units. The units and regulators of these fields are small, so that their class groups are relatively large. See [6], [14] for connections between these units and certain modular curves. For instance, when  $l = n^2 + 1$  or  $l = n^2 + 4$  for some  $n \in \mathbf{Z}$ , the quadratic subfield of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  is given by  $\mathbf{Q}(\sqrt{n^2 + 1})$  with unit  $\varepsilon = n + \sqrt{n^2 + 1}$ , and by  $\mathbf{Q}(\sqrt{n^2 + 4})$  with  $\varepsilon = (n + \sqrt{n^2 + 4})/2$  respectively. The “simplest cubics” [18] form a similar family of degree 3. The conductor is of the form  $l = n^2 + 3n + 9$  and the cubic fields are generated by a root of the polynomial  $X^3 - nX^2 - (n + 3)X - 1$ . M.-N. Gras [8], [9] constructed such families of degree 4 (with conductors  $l = n^2 + 16$ ) and 6 (with conductors  $l = n^2 + 108$  and  $l = 16n^2 + 12n + 9$ ). Emma Lehmer [15] did so for degrees 5 (with conductors  $l = n^4 + 5n^3 + 15n^2 + 25n + 25$ ) and 8 (with conductors  $l = n^4 + 16$ ). The class numbers of Emma Lehmer’s degrees 5 and 8 have been computed in [17], [20] for all  $l < 10^{10}$ . There are no similar families known for degree 7, 9 or larger, but see [21].

In the range of our computations we encountered several members of these families of number fields. These are indicated with an asterisque in the Main Table.

### 5. GALOIS COHOMOLOGY

Let  $l > 2$  be a prime. In this section we show that the Galois cohomology groups of the module  $B$  of units modulo cyclotomic units are naturally isomorphic to those of the class group of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . See [3] for class field theory and cohomology of groups.

**Proposition 5.1.** *Let  $H$  be a subgroup of  $G = \text{Gal}(\mathbf{Q}(\zeta_l + \zeta_l^{-1})/\mathbf{Q})$ . Let  $O$  denote the ring of integers of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ , let  $B$  denote the group of units  $O^*$  modulo its subgroup of cyclotomic units and let  $Cl$  denote the class group of  $O$ . Then:*

(i) *The sequence of  $H$ -invariants*

$$0 \longrightarrow \text{Cyc}^H \longrightarrow O^{*H} \longrightarrow B^H \longrightarrow 0$$

*is exact; in particular,  $B^G = 0$ .*

(ii) *There are canonical isomorphisms*

$$\widehat{H}^q(H, Cl) \xrightarrow{\cong} \widehat{H}^{q+2}(H, B), \quad \text{for each } q \in \mathbf{Z}.$$

In particular, for each choice of a generator of  $H$  there are natural isomorphisms  $\widehat{H}^q(H, Cl) \cong \widehat{H}^q(H, B)$  for each  $q \in \mathbf{Z}$ .

*Proof.* Let  $g$  be a primitive root modulo  $l$  and let  $\sigma \in G$  denote the automorphism given by  $\sigma(\zeta_l + \zeta_l^{-1}) = \zeta_l^g + \zeta_l^{-g}$ . It is a generator of  $G$ . Let  $e$  denote the order of  $H$  and let  $ee' = (l - 1)/2 = \#G$ . There is an exact sequence of  $H$ -modules

$$0 \longrightarrow \{\pm 1\} \longrightarrow \text{Cyc} \longrightarrow I \longrightarrow 0.$$

Here  $I$  denotes the augmentation ideal of  $\mathbf{Z}[G]$ , and the  $H$ -homomorphism  $\text{Cyc} \longrightarrow I$  is given by  $\eta \mapsto [\sigma] - 1$ . Since  $\widehat{H}^0(H, I) \cong H^1(H, \mathbf{Z}) = 0$ , the natural map  $\widehat{H}^0(H, \{\pm 1\}) \longrightarrow \widehat{H}^0(H, \text{Cyc})$  is surjective. The  $G$ -norm of  $\eta$  being  $-1$ , the  $H$ -norm of the cyclotomic unit  $\eta^{(\sigma^{e'} - 1)/(\sigma - 1)}$  is  $-1$  as well. This implies that the latter map is zero, and we conclude that

$$(1) \quad \widehat{H}^0(H, \text{Cyc}) = 0 \quad \text{and} \quad \#\widehat{H}^{-1}(H, \text{Cyc}) = e.$$

The last equality follows from the fact that  $B = O^*/\text{Cyc}$  is finite, so that the Herbrand quotient of  $\text{Cyc}$  is equal to that of  $O^*$ , which is equal to  $e$ .

Let  $U$  denote the group of unit idèles of  $k = \mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . Since  $k$  is only ramified at its unique prime over  $l$  and since it is totally and tamely ramified at this prime, we have that  $\widehat{H}^q(H, U) \cong \widehat{H}^q(H, \mathbf{F}_l^*)$  for every  $q \in \mathbf{Z}$ . Therefore there are natural isomorphisms

$$(2) \quad \widehat{H}^{-1}(H, U) \cong \mu_e(\mathbf{F}_l) \quad \text{and} \quad \widehat{H}^0(H, U) \cong \mathbf{F}_l^*/(\mathbf{F}_l^*)^e.$$

Here  $\mu_e$  denotes the group of  $e$ -th roots of unity. We claim that the composite map  $\alpha_2\alpha_1$  in

$$\widehat{H}^{-1}(H, \text{Cyc}) \xrightarrow{\alpha_1} \widehat{H}^{-1}(H, O^*) \xrightarrow{\alpha_2} \widehat{H}^{-1}(H, U)$$

is an isomorphism. To see this, we consider the cyclotomic unit  $\varepsilon = \eta^{2(\sigma^{e'} - 1)/(\sigma - 1)}$ . It has  $H$ -norm 1. We compute its image in  $\mu_e(\mathbf{F}_l)$ . Since  $(\zeta_l^g - \zeta_l^{-g})/(\zeta_l - \zeta_l^{-1}) \equiv g \pmod{(\zeta_l - 1)}$ , we see that  $\varepsilon \equiv g^{2e'} \pmod{(\zeta_l - 1)}$ . Therefore the image of  $\varepsilon$  generates  $\mu_e(\mathbf{F}_l)$ , and it follows that the map  $\alpha_2\alpha_1$  is surjective. By (1) and (2) both groups  $\widehat{H}^{-1}(H, \text{Cyc})$  and  $\widehat{H}^{-1}(H, U)$  have order  $e$ . Therefore the map  $\alpha_2\alpha_1$  is actually an isomorphism. It follows that  $\alpha_1$  is injective and that  $\alpha_2$  is surjective.

Since  $\alpha_1$  is injective, the long cohomology sequence associated to the short exact sequence  $0 \longrightarrow \text{Cyc} \longrightarrow O^* \longrightarrow B \longrightarrow 0$  gives rise to the exact sequence

$$0 \longrightarrow \text{Cyc}^H \longrightarrow O^{*H} \longrightarrow B^H \longrightarrow 0,$$

and (i) follows.

The proof of (ii) involves some more computations. Consider the exact sequence

$$0 \longrightarrow \text{Cyc} \longrightarrow U \longrightarrow U/\text{Cyc} \longrightarrow 0.$$

Since the cohomology of the cyclic group  $H$  is periodic, it follows from (1) and the fact that the map  $\alpha_2\alpha_1 : \widehat{H}^{-1}(H, \text{Cyc}) \longrightarrow \widehat{H}^{-1}(H, U)$  is bijective that

$$\widehat{H}^q(H, U/\text{Cyc}) = 0, \quad \text{for all odd } q \in \mathbf{Z},$$

and that the maps

$$(3) \quad \widehat{H}^q(H, U) \xrightarrow{\cong} \widehat{H}^q(H, U/\text{Cyc})$$

are isomorphisms for all even  $q \in \mathbf{Z}$ .

Let  $C$  denote the idèle class group of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  and consider the two exact sequences

$$\begin{aligned} 0 \longrightarrow B \longrightarrow U/\text{Cyc} \longrightarrow U/O^* \longrightarrow 0, \\ 0 \longrightarrow U/O^* \longrightarrow C \longrightarrow Cl \longrightarrow 0. \end{aligned}$$

The composite map

$$\widehat{H}^0(H, U) \xrightarrow{\cong} \widehat{H}^0(H, U/\text{Cyc}) \xrightarrow{\alpha_3} \widehat{H}^0(H, U/O^*) \xrightarrow{\alpha_4} \widehat{H}^0(H, C)$$

is an isomorphism. This follows from *class field theory*, since the Artin map identifies  $\widehat{H}^0(H, C)$  with the Galois group of the fixed field of  $H$  over  $\mathbf{Q}$  and  $\widehat{H}^0(H, U)$  with the inertia group of the unique prime over  $l$ . Under this identification the map above is identified with the inclusion map, which is an isomorphism since the prime over  $l$  is totally ramified.

It follows that  $\alpha_3$  is injective and that  $\alpha_4$  is surjective. Together with the facts that  $H^1(H, U/\text{Cyc}) = 0$  and that, by class field theory,  $H^1(H, C) = 0$ , this gives rise to the following natural isomorphisms and exact sequences:

$$\begin{aligned} H^1(H, U/O^*) &\xrightarrow{\cong} H^2(H, B), \\ \widehat{H}^0(H, Cl) &\xrightarrow{\cong} H^1(H, U/O^*), \\ 0 \longrightarrow \widehat{H}^0(H, U/\text{Cyc}) &\xrightarrow{\alpha_3} \widehat{H}^0(H, U/O^*) \longrightarrow H^1(H, B) \longrightarrow 0, \\ 0 \longrightarrow \widehat{H}^{-1}(H, Cl) &\longrightarrow \widehat{H}^0(H, U/O^*) \xrightarrow{\alpha_4} \widehat{H}^0(H, C) \longrightarrow 0. \end{aligned}$$

We obtain at once a canonical isomorphism

$$\widehat{H}^0(H, Cl) \xrightarrow{\cong} H^2(H, B).$$

Since the composite map  $\alpha_4\alpha_3$  is an isomorphism, an easy diagram chase shows that the composite map

$$\widehat{H}^{-1}(H, Cl) \longrightarrow \widehat{H}^0(H, U/O^*) \longrightarrow H^1(H, B)$$

is an isomorphism as well. The second statement of part (ii) now follows from the periodicity of the cohomology of cyclic groups. □

### 6. HEURISTICS

In this section we estimate the probability that the Main Table of the numbers  $\tilde{h}_l^+$  is actually a table of class numbers of the fields  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  for  $l < 10,000$ . Confronting the numerical data with the Cohen-Lenstra heuristics, we argue that this probability exceeds 98%.

Note that the Cohen-Lenstra heuristics [4] do not really apply to our situation. The heuristics apply typically to large sets of cyclic number fields of *fixed* degree. They say something about the average behavior of the class groups when the conductors of such fields vary in large intervals. Our situation is rather the opposite, since the conductors  $l$  are at most 10,000 and the main point of this section is to estimate the behavior of the Jordan-Hölder factors of the ideal class groups  $Cl_l^+$  that have very large order. As a consequence, we expect that the estimates that we derive from the Cohen-Lenstra heuristics systematically *overestimate* the probability that certain simple Jordan-Hölder factors occur in the class groups or in the groups  $B_l$  associated to the fields  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . This is fine for our main application, which is the justification of our claim that the Main Table is actually a table of

class numbers of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  for  $l < 10,000$ . It makes the estimates even more conservative. On the other hand, some of the other predictions that follow from our application of the Cohen-Lenstra heuristics appear to be off in a systematic way.

Having said that, we proceed in a somewhat nonrigorous fashion. We estimate the probability for simple Jordan-Hölder factors of the rings  $\mathbf{Z}[G_l]$  to occur in the class groups of the fields  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ . Let  $M$  be a simple Jordan-Hölder factor of the group ring  $\mathbf{Z}[G_l]$  of order  $q$  and degree  $d > 1$ . Recall that this implies  $d$  divides  $q - 1$  as well as  $(l - 1)/2$ , that  $q = p^f$  is a power of a prime  $p$  and that  $f$  is the order of  $p \pmod{d}$ . The module  $M$  is a residue field of the ring  $\mathbf{Z}[G_l]$ . More precisely, it is a residue field of the unique quotient ring of  $\mathbf{Z}[G_l]$  that is isomorphic to  $\mathbf{Z}[\zeta_d]$ . The ring  $\mathbf{Z}[\zeta_d]$  admits  $\phi(d)/f$  residue fields of order  $q$ . Here  $\phi$  denotes Euler's  $\phi$ -function. The number of residue fields of order  $q$  of the ring  $\mathbf{Z}[G_l]$  is obtained by summing the quantities  $\phi(d)/f$  over the divisors  $d > 1$  of  $\gcd((l - 1)/2, q - 1)$  for which the order of  $p \pmod{d}$  is  $f$ .

According to Cohen-Lenstra [4, Example 5.10], the probability that  $M$  does *not* occur in a "random  $\mathbf{Z}[\zeta_d]$ -module modulo a random principal ideal" is equal to  $\prod_{k \geq 2} (1 - q^{-k})$ . According to the heuristics, the parts of the class groups of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  all of whose simple Jordan-Hölder factors are isomorphic to  $M$  behave statistically as such modules. Therefore, the chance that for a given prime  $l$ , the class group of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  does *not* admit any simple Jordan-Hölder factors of order  $q$  at all is at least

$$P(q; l) = \prod_{k \geq 2} (1 - q^{-k})^{\sum_d \phi(d)/f},$$

where  $d$  runs over the divisors  $d > 1$  of  $\gcd((l - 1)/2, q - 1)$  for which the order of  $p \pmod{d}$  is  $f$ . Note that  $P(q; l)$  only depends on  $l \pmod{2(q - 1)}$ .

Next we also vary  $l$ . The proportion of primes  $l$  in a long interval for which the class group of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  does not admit any Jordan-Hölder factors of order  $q$  is given by

$$P(q) = \frac{1}{\phi(2(q - 1))} \sum_{l \in (\mathbf{Z}/(2(q - 1)\mathbf{Z}))^*} P(q; l).$$

It would actually be more natural to fix  $d$  as well as  $q$  and consider the proportion  $P(q, d)$  of primes  $l$  in a long interval for which the class group of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  does not admit any Jordan-Hölder factors of degree  $d$  and order  $q$ . In these terms,  $P(q) = \sum_d P(q, d)$ , where  $d$  runs over the divisors of  $q - 1$  modulo which  $p$  has order  $f$ . We haven't done so because of the limited amount of numerical material available: only 1228 fields.

It follows that the proportion of primes  $l$  for which a simple Jordan-Hölder factor of order  $q$  occurs in the class group of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  is at most  $1 - P(q)$ . Since there are 1228 odd primes  $l < 10,000$ , the sum  $1228 \sum_q (1 - P(q))$ , with  $q$  running over the prime powers  $q < 80,000$ , is then the expected number of simple Jordan-Hölder factors, not counting multiplicities, that we should find as factors of the class groups in the range of our computations. Its value, 406.4... out of the 85 million that are a priori possible, is somewhat larger than 354, the actual number that we found, but the order of magnitude is about right. Similarly, the predicted proportion of primes  $l$  for which the class number of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  is 1 is at least  $\prod_q P(q) \approx 71.3\%$ .

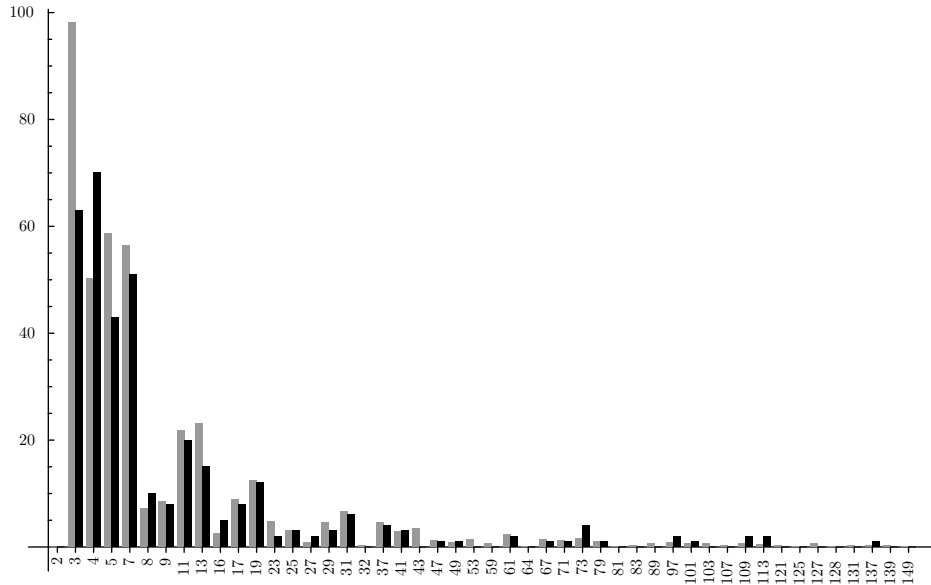


FIGURE 6.1. Distribution of the Jordan-Hölder factors of order  $q < 150$  in  $B_l$  for  $l < 10,000$ .

This is not very much smaller than the proportion of 75.3% of primes  $l$  with  $\tilde{h}_l^+ = 1$  that we found.

In Figure 6.1 we present a histogram counting the number of primes  $l < 10,000$  for which the class group of the field  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  admits a simple Jordan-Hölder factor of order  $q < 150$  (black columns) and the expected number  $1228(1 - P(q))$  (grey columns). Note that 347 of the 354 simple Jordan-Hölder factors are accounted for by this histogram. The seven missing Jordan-Hölder factors have orders 151, 211, 313, 421, 541, 883 and 1451 respectively.

Finally we turn to the Main Table. We recall that it contains the orders  $\tilde{h}_l^+$  of the subgroups of the class groups of  $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$  for  $l < L = 10,000$  that admit only Jordan-Hölder factors of order  $q < Q = 80,000$ . The chance  $\mathcal{P}$  that the numbers  $\tilde{h}_l^+$  that we found are equal to the class numbers is therefore

$$\prod_{l < L} \prod_{q > Q} P(q; l).$$

Recall that  $P(q; l)$  only depends on  $l \pmod{2(q-1)}$ . We estimate  $P(q; l)$  by dropping the condition that the order of  $p \pmod{d}$  is equal to  $f$  and by replacing  $\phi(d)/f$  by  $\phi(d)$ . This enlarges the exponent and hence makes the product smaller. Therefore the probability  $\mathcal{P}$  that the Main Table is a table of class numbers is at least

$$\prod_{q > Q} \prod_{k \geq 2} (1 - q^{-k})^{\sum_{1 < d | q-1} \phi(d) \#\{l < L : l \equiv 1 \pmod{2d}\}}.$$

Replacing  $\#\{l < L : l \equiv 1 \pmod{2d}\}$  by  $\pi(L)/\phi(2d)$  and taking a logarithm, we find that  $-\log(\mathcal{P})$  is (approximately) at most

$$\pi(L) \sum_{q>Q} e(q-1) \sum_{k \geq 2} -\log(1 - q^{-k}) \approx \pi(L) \sum_{n>Q} \frac{e(n)}{n^2}.$$

Here  $e(n) = 0$  when  $n + 1$  is *not* a prime power, while it denotes the number of divisors  $d > 1$  of  $n$ , weighting the even ones with weight  $1/2$ , when  $n + 1$  is a prime power. A partial summation argument gives that

$$\sum_{n>Q} \frac{e(n)}{n^2} \leq \sum_{n>Q} \frac{E(n)}{n^3},$$

where

$$\begin{aligned} E(n) &= \sum_{d \text{ odd}} \#\{q < n : q \text{ is a prime power and } q \equiv 1 \pmod{d}\} \\ &\quad + \frac{1}{2} \sum_{d \text{ even}} \#\{q < n : q \text{ is a prime power and } q \equiv 1 \pmod{d}\}. \end{aligned}$$

By the prime number theorem and Dirichlet's Theorem on primes in arithmetic progressions we have that

$$E(n) \approx \frac{n}{\log n} \sum_{d \leq n} \frac{1}{\psi(d)},$$

where  $\psi(d) = \phi(d)$  when  $d$  is odd, while  $\psi(d) = 2\phi(d)$  when  $d$  is even. The function  $\psi$  is multiplicative, and in order to estimate the average value of  $1/\psi(d)$  we compute

$$\left( \sum_{n \geq 1} \frac{1}{\psi(n)n^s} \right) / \left( \sum_{n \geq 1} \frac{1}{n n^s} \right), \quad \text{for } s \rightarrow 0.$$

Evaluating the Euler products, we find the value

$$c = \prod_{p \text{ odd}} \frac{p^2 - p + 1}{(p-1)p} = \frac{2}{3} \frac{\zeta(2)\zeta(3)}{\zeta(6)}.$$

Here  $\zeta(s)$  denotes the Riemann zeta function. It follows that  $1/\psi(d)$  is on the average  $c/d$ , and hence

$$E(n) \approx \frac{n}{\log n} c \sum_{d \leq n} \frac{1}{d} \approx cn.$$

This implies that  $-\log(\mathcal{P})$  is (approximately) at most

$$\pi(L) \sum_{n>Q} \frac{cn}{n^3} \approx c \frac{\pi(L)}{Q}.$$

Finally we substitute  $\pi(L) = 1228$  and  $Q = 80,000$ . Since  $c = \frac{2}{3} \frac{\zeta(2)\zeta(3)}{\zeta(6)} = 1.29573\dots$ , we find  $-\log(\mathcal{P}) \leq 0.019889$ , and it seems therefore reasonable to estimate the probability  $\mathcal{P}$  that the Main Table is a table of class numbers to be at least 98%.

MAIN TABLE

$l$	$\tilde{h}_l^+$	deg	$l$	$\tilde{h}_l^+$	deg	$l$	$\tilde{h}_l^+$	$\tilde{h}_l^+$
163	4	3*	2351	11	5	4639	4	3
191	11	5*	2381	11	10	4649	3	2
229	3	2*	2417	17·41	4*, 8*	4657	5	4
257	3	2*	2437	7	3	4729	3·13	2, 12
277	4	3	2473	5	4	4783	7	3
313	7	3*	2557	3·7·7	2, 3*, 6	4789	4	3
349	4·4	3*, 6	2617	13	4*	4793	5	4
397	4	3	2621	11	10	4801	4	3
401	5·9	2*, 8	2659	19	3*	4817	17	8
457	5	4*	2677	3	2	4861	7	6
491	8	7	2689	4	3	4889	5	2
521	27	26	2713	3	2	4933	3·3	2, 6
547	4	3	2753	9	8	4937	5	4
577	7	2*	2777	3	2	4993	5	4
607	4	3*	2797	4	3	5051	1451	5*
631	11	5	2803	4	3	5081	3	2
641	5·11·9	4*, 5, 8*	2857	3	2	5101	11	10
709	4·4	3*, 6	2917	3·7	2*, 6*	5119	31	3*
733	3	2*	2927	8	7	5197	4	3
761	3	2	3001	11·11	5, 10	5209	29	14
821	11	10	3037	4	3	5261	3	2
827	8	7	3041	13	4*	5273	7	2
829	47	46	3121	5·61	2, 20	5281	3·3	2, 6
853	4	3	3137	3 <sup>2</sup>	2*	5297	3	2
857	5	4*	3181	5	2	5333	3	2*
877	7·7	3*, 6*	3217	7	3	5413	23	11
937	4·4	3*, 6	3221	3	2	5417	7	2
941	16	5*	3229	3·3	2, 6	5437	31	6*
953	71	7	3253	5	2*	5441	11	10
977	5	4*	3271	4	3	5477	3	2*
1009	7·4	2, 3	3301	16·151	5, 15	5479	4	3
1063	13	3*	3313	19·7	3*, 6*	5501	11	5
1069	7	6*	3433	37	12	5521	3 <sup>2</sup>	2
1093	5	2*	3469	13	6	5531	8	7
1129	3 <sup>2</sup> ·7	2, 3*	3517	4	3	5557	19·73	3*, 6
1153	19	9	3529	19	3	5581	73	9
1229	3	2*	3547	19·883	3*, 9	5641	9	4*
1231	211	15	3571	7	3	5659	4	3
1297	11·25	2*, 8	3581	11	5	5701	101	10
1373	3	2*	3697	5	4	5741	3	2
1381	7	6	3727	4	3	5779	4	3
1399	4	3	3877	3	2	5821	3	2
1429	5	2	3889	3	2	5827	13	3
1459	13·19	3, 9	3931	16 <sup>2</sup>	5	5953	4·7	3, 3
1489	3·19	2, 3*	4001	3	2	6037	4·7	3, 6*
1567	7	3*	4049	23	11	6053	3	2
1601	7	2*	4073	5	4	6073	13	12
1697	17	4*	4099	4	3	6079	4	3
1699	4	3	4177	19	18	6113	5	2
1777	4 <sup>2</sup>	3	4201	11	5	6133	3	2
1789	4	3	4219	4·7	3, 3	6163	4	3
1831	7	3	4229	7	2*	6229	13	6
1861	11	5	4241	9	4*	6247	4 <sup>2</sup>	3
1873	25	8	4261	4·4	3, 6	6257	29	4*
1879	4	3	4297	4 <sup>2</sup> ·4 <sup>2</sup>	3*, 6*	6301	8	7
1889	49	16	4327	8	7	6337	97	48
1901	3	2	4339	7	3	6361	61	20
1951	4	3	4357	5·4·4	2*, 3, 6	6421	41	10
1987	7	3*	4409	3 <sup>2</sup>	2	6449	5	4
2029	7	2*	4441	5·5	2, 4	6481	5	2
2081	5·5	2, 10	4457	5	4	6521	5	4
2089	3·3·3	2, 6, 18	4481	3·97	2, 3 <sup>2</sup>	6529	13	12
2113	37	12	4493	3	2*	6553	4	3
2131	4	3	4561	4·4	3, 6	6577	17·313	4*, 8*
2153	5	2	4567	4	3	6581	11	5
2161	16	5	4591	19	9	6637	3·4·3	2, 3, 6
2213	3	2*	4597	3·7	2, 6*	6673	17	8
2311	4	3	4603	79	39	6709	4·7	3, 3

MAIN TABLE (continued)

$l$	$\bar{h}_l^+$	deg	$l$	$\bar{h}_l^+$	deg	$l$	$\bar{h}_l^+$	$\bar{h}_l^+$
6737	9	4	8011	4	3	9109	4·4	3, 6
6781	13	6	8017	3·19·3·7·109	2, 3*, 6*, 6*, 12	9127	31	3*
6833	8	7	8069	3	2	9133	3·7	2, 6*
6949	5	2	8101	13	2*	9161	5	4
6961	17	8	8161	5	4	9181	5·5	2, 10
6991	7	3	8191	4	3	9241	13	3
6997	3·7	2, 6*	8209	4	3	9277	7	3
7027	4	3	8269	37	3	9281	3	2
7057	3·7·7	2*, 2*, 14	8287	7	3	9283	4	3
7229	5	2*	8297	5·9	4*, 4*	9293	3	2
7297	4	3	8317	113	14	9319	4·7	3*, 3*
7333	13	6*	8377	5	4	9337	4·4·4	3, 6, 12
7351	7·7	3, 21	8389	19	6*	9377	5	4
7369	13	12	8431	31	15	9391	4	3
7411	131	65	8501	5	2	9413	3·27	2*, 26
7417	109	12	8563	7 <sup>2</sup>	3*	9421	4·11·7·11	3, 5, 6, 10
7481	3	2	8581	3·3	2, 6	9511	73	3
7489	7·4·4 <sup>2</sup>	3*, 3*, 6	8597	3	2	9521	113	28
7529	5	4	8629	4·7	3, 3	9551	541	5
7537	3	2	8647	4	3	9601	4·5·4	3, 4, 6
7561	37	6	8681	11	10	9613	7	6
7573	3 <sup>2</sup>	2*	8689	5	2	9649	4	3
7589	8	7	8713	3·67	2, 33	9689	29	28
7621	7	3	8731	4	3	9697	7·9	3, 4
7639	4	3	8761	3 <sup>3</sup> ·3	2, 6	9721	4	3
7673	3	2	8831	16	5	9749	3	2
7687	4 <sup>2</sup>	3	8837	3	2*	9817	17	4*
7753	3·25·5 <sup>2</sup>	2, 3, 4	8887	4	3	9829	5	2
7817	5	2	8893	7	6	9833	3	2
7841	421·8·8	5*, 7, 7	9001	31	10	9857	73	8
7867	4	3	9013	7	6	9907	31	3*
7873	3 <sup>2</sup> ·3	2, 6	9029	7	2*			
7879	4	3	9041	17	4*			
7937	41	4*	9049	7	2			

## REFERENCES

- [1] Batut, C., Belabas, K., Bernardi, D., Cohen, H., Olivier, M.: *User's guide to PARI-GP*, (version 2.0.16), Lab. A2X, Université Bordeaux I, Bordeaux 1999. <http://hasse.mathematik.tu-muenchen.de/ntsw/pari>
- [2] Berthier, T.: *Générateurs et structure du groupe des classes d'ideaux des corps de nombres abéliens*, Thèse Université de Franche-Comté (1994) N. d'ordre 417.
- [3] Cassels, J.W.S. and Fröhlich, A.: *Algebraic Number Theory*, Academic Press, San Diego 1993. MR **35**:6500 (1st. ed.)
- [4] Cohen, H. and Lenstra, H.W.: Heuristics on class groups of number fields, in *Number theory, Noordwijkerhout 1983*, 33–62. Lecture Notes in Math. **1068**, Springer-Verlag, Berlin 1984. MR **85j**:11144
- [5] Cornacchia, P.: Anderson's module for cyclotomic fields of prime conductor, *J. Number Theory* **67** (1997), 252–276. MR **98h**:11143
- [6] Darmon, H.: Note on a polynomial of Emma Lehmer, *Math. Comp.* **56** (1991), 795–800. MR **91c**:11149
- [7] Gras, M.-N.: Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de  $\mathbf{Q}$ . *Journal reine angew. Math* **277** (1975), 89–116. MR **52**:10675
- [8] Gras, M.-N.: Table numérique du nombre de classes et des unités dans les extensions cycliques réelles de degré 4 de  $\mathbf{Q}$ , *Publ. Math. Besançon 1977/78*, fasc. 2.
- [9] Gras, M.-N.: Special units in real sextic fields, *Math. Comp.* **48** (1987), 179–182. MR **88m**:11092
- [10] Gras, G. and Gras, M.-N.: Calcul du nombre de classes et des unités des extensions abéliennes réelles de  $\mathbf{Q}$ , *Bulletin des Sciences Math.* **101** (1977), 97–129. MR **58**:586
- [11] Koyama, Y. and Yoshino K.: Prime divisors of real class numbers of  $p^r$ th cyclotomic field and characteristic polynomials attached to them, preprint August 2000.



- [12] Kummer, E.E.: Bestimmung der Anzahl nicht äquivalenter Classen für die aus  $\lambda$ ten 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) MR **57**:5650
- [13] 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) MR **57**:5650
- [14] Lecacheux, O.: Unités d'une famille de corps liés à la courbe  $X_1(25)$ . *Ann. Inst. Fourier* **40** (1990), 237–253. MR **91i**:11065
- [15] Lehmer, E.: Connection between Gaussian periods and cyclic units, *Math. Comp.* **50** (1988), 535–541. MR **89h**:11067a
- [16] Mäki, S.: *The determination of units in real cyclic sextic fields*, Lecture Notes in Math. **797**, Springer-Verlag, Berlin Heidelberg New York 1980. MR **82a**:12004
- [17] Martinelli, L.: *I polinomi di Emma Lehmer*, Tesi di Laurea, Università di Trento, February 1997.
- [18] Shanks, D.: The simplest cubic fields, *Math. Comp.* **28** (1974), 1137–1152. MR **50**:4537
- [19] Schoof, R.: Minus class groups of the fields of the  $l$ -th roots of unity, *Math. Comp.* **67** (1998), 1225–1245. MR **98j**:11085
- [20] Schoof, R. and Washington, L.C.: Quintic polynomials and real cyclotomic fields with large class numbers, *Math. Comp.* **50** (1988), 543–556. MR **89h**:11067b
- [21] Thaine, F.: Jacobi sums and new families of irreducible polynomials of Gaussian periods, *Math. Comp.* **70** (2001), 1617–1640.
- [22] Van der Linden, F.: Class number computations of real abelian number fields, *Math. Comp.* **39**, (1982), 693–707. MR **84e**:12005
- [23] Washington, L.C.: *Introduction to Cyclotomic Fields; second edition*, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York 1997. MR **97h**:11130

DIPARTIMENTO DI MATEMATICA, 2<sup>a</sup> UNIVERSITÀ DI ROMA “TOR VERGATA”, I-00133 ROMA, ITALY

*E-mail address:* schoof@science.uva.nl