ABSTRACT

Title of dissertation: CLASS NUMBERS OF REAL CYCLOTOMIC FIELDS OF CONDUCTOR pq

Eleni Agathocleous, Doctor of Philosophy, 2009

Dissertation directed by: Professor Lawrence Washington
Department of Mathematics

The class numbers $h^+$ of the real cyclotomic fields are very hard to compute. Methods based on discriminant bounds become useless as the conductor of the field grows and that is why other methods have been developed, which approach the problem from different angles. In this thesis we extend a method of Schoof that was designed for real cyclotomic fields of prime conductor to real cyclotomic fields of conductor equal to the product of two distinct odd primes. Our method calculates the index of a specific group of cyclotomic units in the full group of units of the field. This index has $h^+$ as a factor. We then remove from the index the extra factor that does not come from $h^+$ and so we have the order of $h^+$. We apply our method to real cyclotomic fields of conductor $< 2000$ and we test the divisibility of $h^+$ by all primes $< 10000$. Finally, we calculate the full order of the $l$-part of $h^+$ for all odd primes $l < 10000$. 
CLASS NUMBERS OF REAL CYCLOTOMIC FIELDS OF CONDUCTOR pq

by

Eleni Agathocleous

Dissertation submitted to the Faculty of the Graduate School of the University of Maryland, College Park in partial fulfillment of the requirements for the degree of Doctor of Philosophy
2009

Advisory Committee:
Professor Lawrence Washington Chair/Advisor
Associate Professor Harry Tamvakis
Associate Professor Niranjan Ramachandran
Professor Joel Cohen
Professor William Gasarch
Acknowledgments

First and foremost I would like to thank my advisor, Professor Lawrence Washington, for his continuous guidance, support and excellent advice, for replying to every single e-mail that I sent and for all the hours that he spent on the improvement of this thesis. In every way, this document would not exist without him. I would also like to thank Professors Harry Tamvakis, Niranjan Ramachandran, Joel Cohen and William Gasarch for agreeing to serve on my committee.

I also wish to thank Haralambos Kafkarides for his continuous support and encouragement, as well as my parents, Athos and Maro, my sister Nasia, and Maria-Eleni. Finally I would like to thank all of my friends in College Park and in Washington DC and especially Christos Economides and Christina Aristidou, for all their help and support and for making my stay here pleasant and fun!
# Table of Contents

0 **Introduction** 1

1 Extension of Schoof’s Method 7
   1.1 Schoof’s Method 7
   1.2 Finite Gorenstein Rings 9
   1.3 Extension of the Method to Real Cyclotomic Fields of Conductor $pq$
      1.3.1 Cyclotomic Units 13
      1.3.2 Leopoldt’s Cyclotomic Units and the Decomposition of the Class Number of a Real Abelian Field 15
      1.3.3 A New Cyclotomic Unit $\eta$ 18
      1.3.4 The module $B = E/H = E/\pm \eta^G$ 26

2 The Computational Part and an Example 33
   2.1 Reformulating Theorem 1.1 in terms of Polynomials 33
   2.2 The Decomposition of the modules $B[M]^{\perp}$ 35
   2.3 Gröbner Bases 37
   2.4 The Algorithm 42
      2.4.1 Step 1 42
      2.4.2 Step 2 43
      2.4.3 Step 3 44
   2.5 An Example 48

3 Tables and Discussion of the Results 55

4 Conclusion and Future Projects 59

Appendix 61

Bibliography 80
Chapter 0

Introduction

Let $Q(\zeta_m)$ be the cyclotomic field of conductor $m$ and denote by $C$ its ideal class group and by $h = |C|$ its class number. In the same way let $C^+$ and $h^+$ denote the ideal class group and class number of the maximal real subfield $Q(\zeta_m)^+$. The natural map $C^+ \rightarrow C$ is an injection [30, Theorem 4.14] and we have the well known result $h = h^+ h^-$. The relative class number $h^-$ is easy to compute as there is an explicit and easily computable formula for its order [30, Theorem 4.17]. Schoof in [24] determined the structure and computed the order of $h^-$ for a large number of cyclotomic fields of prime conductor. The number $h^+$ however is extremely hard to compute. The class number formula is not so useful as it requires that the units of $Q(\zeta_m)^+$ be known. Methods that use the classical Minkowski bound become useless as $m$ grows, and other methods based on Odlyzko’s discriminant bounds (see [20] and [21]) are only applicable to fields with small conductor. Masley in [19] computed the class numbers for real abelian fields of conductor $\leq 100$ and Van der Linden in [29] was able to calculate the class number of a large collection of real abelian fields of conductor $\leq 200$. For fields of larger conductor however, the above methods can not be effective. As a result, other methods and techniques were developed that approach the problem from a different angle.

One of these methods is introduced by Schoof in [25] and is designed for real
cyclotomic fields of prime conductor. It is the goal of this thesis to extend his
method to real cyclotomic fields of conductor equal to the product of two distinct
odd primes. Schoof developed an algorithm that computes the order of the module
\( B = \text{Units}/(\text{Cyclotomic Units}) \), which is precisely equal to \( h^+ \) in his case where the
conductor of the field is a prime number. In our case the order of \( B \) is \( h^+ \), by
Sinnott’s formula that we give in Section 1.3, and therefore we could still work
with the same \( B \) as Schoof’s. The complicated structure of the group of cyclotomic
units however when the conductor is not prime, as we will see in 1.3.1, forces us to
provide a replacement for the group of cyclotomic units and therefore for \( B \). Schoof
calculated the various \( l \)-parts of \( h^+ \) by proving that the order of each \( l \)-part equals the
order of the finite module \( B[M]^\perp \), \( M \) being some power of \( l \). He then proved that the
various \( B[M]^\perp \) are isomorphic to \( I/\{f_\mathfrak{R}(\eta)\}_{\mathfrak{R}} \), where \( I \) is the augmentation ideal
of the group ring \( R = (\mathbb{Z}/MZ)[G] \), \( G \) is the galois group of the extension \( Q(\zeta_p)^+/Q \)
and the maps \( f_\mathfrak{R} \in \text{Hom}_R(E/\{\pm 1\}, R) \) correspond to the frobenius elements of
unramified prime ideals \( \mathfrak{R} \) which split completely in the extension \( Q(\zeta_p)^+(\zeta_{2M}) \).
These maps are evaluated on \( \eta \), which is a generator of the group of cyclotomic
units. To facilitate his calculations, he broke each module \( B[M]^\perp \) into its Jordan-
Hölder factors and expressed these factors in terms of polynomials so as to compute
their order. He applied his method to real cyclotomic fields of prime conductor \( p < 
10000 \) and he calculated the \( l \)-part of \( h^+ \) for the largest subgroup of \( B_l \) whose Jordan-
Hölder factors have order < 80000. One of the great advantages of his method is
that it did not exclude the primes dividing the order of the extension, as opposed
to other methods that we discuss below. However, since he computed the order of
the largest subgroup of $B_p$ whose Jordan-Hölder factors have order less than 80000, there is a slight probability that he did not get the full $l$-part of $h^+$ but only part of it.

Many of the other methods employ the well known Leopoldt's decomposition of the class number $h^+$ of a real abelian field $K$, see [17], which derives from his decomposition of the cyclotomic units into the product of the cyclotomic units of all cyclic subfields $K_\xi$ of $K$. More specifically, we have that $h^+ = Q \prod h_\chi$, where the product runs over all non-trivial characters $\chi$ irreducible over the rationals, each 'class number' $h_\chi$ is the index of the cyclotomic units of $K_\chi$ in its full group of units $E_\chi$ and $Q$ is some value which equals 1 in the case where the extension $K/Q$ is cyclic of prime order, but which is very hard to compute in the general case.

Gras and Gras in [12] used the above decomposition of cyclotomic units and proved that for each cyclic subfield $K_\chi$ of $K$, there is a unit $\varepsilon$ in the full group of units $E_\chi$ of $K_\chi$ which is of the form $\varepsilon = \eta^m$, where $\eta$ is a cyclotomic unit, and $\varepsilon$ has the property that $m$ equals the order of the 'class number' of the specific cyclic subfield $K_\chi$. In the same paper we find a method that checks whether the $m$-th root of a unit belongs to a subfield of $K$. This method has been employed by Schoof in [25] and Hakkarainen in [13] and we use it here as well, in the third step of our algorithm, modified however, in order to fit our case. In a different paper by Gras, see [11], one can find some interesting results proved for a special case of real abelian fields. Gras worked with cubic, cyclic extensions and proved that for any $Z'$-submodule $F$ of the full group of units $E$ there exists an element $\omega$ in the group ring $Z' = Z[G]/(1 + \sigma + \sigma^2) \cong Z[\zeta_3]$ with the property that $[E:F] = N_{Q(\sqrt{-3})/Q}(\omega)$. 

3
This element $\omega$ is associated with the class number of these extensions and, together with other facts proved in this article, Gras was able to calculate the class number for cubic, cyclic extensions of conductor $< 4000$.

Recently in his thesis, Hakkarainen in [13] also used Leopoldt’s decomposition to prove whether a prime $l$ divides $h^+$, and since he worked with arbitrary real abelian fields $K$ he could not draw exact conclusions about the $l$-part of $h^+$ for the primes that divide the degree of the extension $K/Q$. In order to prove the divisibility of $h^+$ by a prime $l$ not dividing the degree, it sufficed to prove that $l$ divides any of the ‘class numbers’ of the cyclic sub-extensions of $K$, since in Leopoldt’s decomposition of the class number, any prime dividing $h^+$ that does not divide the degree of the extension can only come from the ‘class numbers’ of the cyclic sub-extensions. In practice Hakkarainen checked the divisibility of $h^+$ by all primes $< 10000$. He used the method of Schwarz, see [27], in order to exclude the primes that do not divide $h^+$ and used some ideas from van der Linden to search for units that are $l$-th powers in the full group of units. Finally, he employed a method from [12] that we mentioned above, to verify the divisibility of $h^+$ by $l$. He applied his method to real abelian number fields of conductor $< 2000$. In this thesis we apply our algorithm to the fields of conductor $pq$ that appear in Hakkarainen’s tables. We verify all the primes that he obtained and we also complete his results in the sense that we verify the divisibility of $h^+$ by the exact power of those primes $l < 10000$ that also happen to divide the degree of the extension.

There are also other methods that approach the problem of computing $h^+$ in different ways to the ones described above. Aoki, in [3], describes a method for
computing annihilators of the ideal class group. The method for the annihilators of the plus part of the ideal class group that he describes in this paper involve the construction of maps like the ones used in Schoof [25] for the description of his modules whose order give the \( l \)-part of \( h^+ \). The image of these maps in Aoki’s paper, when applied on cyclotomic units give higher annihilators for the \( l \)-part of \( h^+ \). These ideas are based on the work of Thaine [28], as well as on the work of V. Kolyvagin and K. Rubin. In another paper by Aoki and Fukuda [4], an algorithm is introduced for the calculation again of the \( l \)-part of \( h^+ \), but for odd primes not dividing the degree of the extension.

Cornacchia in [7] studied a Galois module \( L \) introduced by Anderson in [2], whose structure is related to both the circular units and the Stickelberger ideal. Cornacchia studied this module for cyclotomic fields of prime conductor. He decomposed Anderson’s module into its \( \chi \)-components, where \( \chi \) is a \( l \)-adic character of the subgroup \( D \) of the galois group \( G \) with \((|D|, l) = 1\) and then proved that
\[
L^\text{dual}_\chi \cong (\mathbb{Z}[G]/M)/J_\chi,
\]
where \( J_\chi \) is an ideal generated by homomorphisms representing maps from the group of \( l \)-units into \( \mathbb{Z}_\chi[G]/M \), where \( M \) is some sufficiently large power of \( l \). By applying his results with \( l = 2 \), he was able to calculate the 2-part of \( h^+ \) for cyclotomic fields of prime conductor < 10000. Some of Cornacchia’s ideas are also employed by Schoof in [25] that we have already discussed above.

In Chapter 1 that follows the introductory part of this thesis, we discuss in more detail the method of Schoof. We stress the difficulties that arise when one tries to apply it to cyclotomic fields of non-prime conductor and we show how to generalize it in order to apply it to our case of cyclotomic fields of conductor \( pq \). We
present a new unit and calculate the index of the subgroup that it generates, in the full group of units. This group will replace the group of cyclotomic units that was used for the fields of prime conductor. We then reformulate the main theorems of Schoof in order to match our generalized case. In Chapter 2 we describe the results of Chapter 1 in terms of polynomials so that we can perform our calculations, and we give some basic facts about Gröbner Bases since our polynomials are in two variables. We then describe the three steps of the algorithm and give an example. In Chapter 3 we present and discuss the tables with our results and in Chapter 4 we finish with the conclusion and future projects that can follow from this work.
Chapter 1

Extension of Schoof’s Method to Real Cyclotomic Fields of Conductor pq

As was already explained in the introduction, the methods for calculating the class number $h^+$ of a real cyclotomic field which are based on discriminant bounds become useless as the conductor of the field grows. That is why other techniques were developed that approached the problem from a different angle. One of these is Schoof’s method presented in [25], which focuses on the real cyclotomic fields $\mathbb{Q}(\zeta_p)^+$ with prime conductor $p$. We will give a brief description of the method below so that the reader can understand the changes one has to make in order to generalize it to fields of non-prime conductor. A complete and formal description of our method for real cyclotomic fields of conductor $pq$ will start from Section 3, right after the definition and some properties of finite Gorenstein Rings in Section 2, which we will need to support the theoretical part of our method.

1.1 Schoof’s Method

For the fields $\mathbb{Q}(\zeta_p)^+$ that Schoof focused on, we have that $h^+ = [E:H]$, where $E$ is the group of units of $\mathbb{Q}(\zeta_p)^+$ and $H$ is its subgroup of cyclotomic units. The quotient $B = E/H$ is a finite $\mathbb{Z}[G]$-module, where $G = \text{Gal}(\mathbb{Q}(\zeta_p)^+ / \mathbb{Q})$ is a cyclic group of order $(p - 1)/2$ and we see that $|B| = h^+$. Let $l$ be any prime number.
As the order of $B$ is the product of its $l$-parts, Schoof studied the modules $B[M]^{\perp}$ instead, where $M$ is a power of $l$, since as we will see in the next section, for finite Gorenstein rings $R$ and any finite $R$-module $A$ we have that

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

and therefore $|A| = |A^{\text{dual}}| = |A^{\perp}|$. Now, for each $B[M]^{\perp}$ Schoof found the order of its simple Jordan-Hölder factors since the product of those factors gives the order of $B[M]^{\perp}$. First, he expressed the modules $B[M]^{\perp}$ in a way that facilitated the calculations. For $I$, the augmentation ideal of the ring $R = (Z/MZ)[G]$, he proved that $B[M]^{\perp} \cong I/\{f_R(\eta)\}_{(\mathfrak{R})}$ where $\eta$ is a generator of the group of cyclotomic units $H$, $f_R$ is the Frobenius group ring element that corresponds to an unramified prime ideal $\mathfrak{R}$ which splits completely in the extension $Q(\zeta_p)^{\pm}(\zeta_2)^M)/Q$, and $\mathfrak{R}$ runs through all such unramified prime ideals. Since he studied the $l$-parts of $B$ he worked in $Z_l$ and he used the isomorphism

$$Z_l[G] \cong Z_l[x]/(x^{(p-1)/2} - 1)$$

where $x \leftrightarrow \sigma : \zeta_p + \zeta_p^{-1} \mapsto \zeta_p^g + \zeta_p^{-g}, g$ a primitive root modulo $p$. The Frobenius maps he wrote as polynomials in the variable $x$. More specifically, for each fixed $l$ he wrote the order of $G$ as $ml^a$ with $(m, l) = 1$, so that the polynomial $x^m - 1$ could be written as a product of irreducible polynomials $\phi$ in $Z_l[x]$. This gave the following isomorphism of $Z_l$-algebras

$$Z_l[G] \cong Z_l[x]/(x^{(p-1)/2} - 1) \cong Z_l[x]/((x^{l^a})^m - 1) \cong \prod_{\phi} Z_l[x]/(\phi(x^{l^a}))$$

where the factors $Z_l[x]/(\phi(x^{l^a}))$ are complete local $Z_l[G]$-algebras with maximal ideals $(l, \phi(x))$ and residue fields isomorphic to $F = F_l[x]/(\phi(x))$. The order of $F$
is \( l^f \), where \( f \) is the degree of \( \phi \). Using the above decomposition of the ring \( \mathbb{Z}_l[G] \), one can write the \( l \)-part of any finite \( \mathbb{Z}_l[G] \)-module \( A \) as

\[
A \otimes \mathbb{Z}_l \cong \prod_{\phi} A_{\phi}
\]

where

\[
A_{\phi} = A \otimes_{\mathbb{Z}_l[G]} \mathbb{Z}_l[x]/(\phi(x^l)).
\]

As a finite module, \( A \) admits a Jordan-Hölder filtration with simple factors, each of which is isomorphic to some \( F \). All these hold in particular for the module \( B = E/H \) and the various \( B[M]^\perp \) described above. A Jordan-Hölder factor of \( B[M]^\perp \) has order \( l^f \) and it corresponds to the unique subfield of \( Q(\zeta_p)^+ \) of degree equal to the order of \( x \) in \( F_l[x]/(\phi(x)) \). Schoof examined the divisibility of \( h^+ \) by all primes \( < 80,000 \), for all cyclotomic fields of prime conductor \( p < 10,000 \), and calculated all the Jordan-Hölder factors of the various \( B[M]^\perp \) which had order \( \leq 80,000 \).

As we see above, one of the great advantages of Schoof’s Method, which will also apply in our method as well, is that it does not exclude the primes dividing the order of the group, in contrast to other methods that we have already discussed in the introduction.

1.2 Finite Gorenstein Rings

In this section we give the definition and some basic properties of finite Gorenstein rings that we will need later on. We follow Schoof [25].

Let \( R \) be a finite commutative ring and \( A \) any \( R \)-module. Define

\[
A^\perp = Hom_R(A, R) \quad \text{and} \quad A^{\text{dual}} = Hom_Z(A, Q/Z).
\]
Both of these groups are $R$-modules.

**Definition 1.1.** The ring $R$ is Gorenstein if the $R$-module $R^{\text{dual}}$ is free of rank 1 over $R$.

Let $R$ be a finite Gorenstein ring. For any $M \in \mathbb{Z}$, any finite abelian group $G$, and any irreducible polynomial $g(x) \in R[x]$, we have that the rings $\mathbb{Z}/MZ$, $(\mathbb{Z}/MZ)[G]$ and $R[x]/(g(x))$ are finite Gorenstein rings.

In the next proposition we prove a fact that we already mentioned above and which we will also use in the next chapter.

**Proposition 1.1.** Let $R$ be a finite Gorenstein ring and let $\chi : R \to \mathbb{Q}/\mathbb{Z}$ denote a generator of the $R$-module $\text{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$. Then, for every $R$-module $A$, the map $\Phi : A^{\perp} \to A^{\text{dual}} : f \mapsto \chi \cdot f$ is an isomorphism of $R$-modules.

**Proof:** For any $R$-module $A$ we have the canonical isomorphism $\text{Hom}_R(A, \text{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \cong \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$.

We also have the $R$-isomorphism $R \cong \text{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ via the map that maps 1 to $\chi$. Hence $A^{\perp} = \text{Hom}_R(A, R) \cong \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) = A^{\text{dual}}$ via the map $\Phi$ given in the statement above. \square

We will also need the two propositions below. The first one shows that any finite $R$-module is Jordan-Hölder isomorphic to its dual, and together with Proposition 1.1. above, justifies the use of the Jordan-Hölder factors of $B^{\perp}$ instead of $B$.

**Proposition 1.2.** Let $R$ be a finite Gorenstein ring. Any finite $R$-module is Jordan-Hölder isomorphic to its dual.
Proof: Consider the exact sequence

\[ 0 \rightarrow mA \rightarrow A \rightarrow A/mA \rightarrow 0. \]

Since the functor \( A \rightarrow A^{\text{dual}} \) from the category of finite \( Z/MZ \)-modules to itself is exact, we apply it to the sequence above and we obtain the exact sequence

\[ 0 \rightarrow (A/mA)^{\text{dual}} \rightarrow A^{\text{dual}} \rightarrow (mA)^{\text{dual}} \rightarrow 0. \]

We therefore have that

\[ (A/mA)^{\text{dual}} \cong A^{\text{dual}}/(mA)^{\text{dual}} \cong A^{\text{dual}}[m] = \{ a \in A^{\text{dual}} : \mu a = 0 \text{ for all } \mu \in m \}. \]

This implies that

\[ |A/mA| = |(A/mA)^{\text{dual}}| = |A^{\text{dual}}[m]| \]

and both are vector spaces over \( R/m \). Hence, they have the same dimension and therefore the same number of simple Jordan-Hölder factors \( R/m \). If \( mA = 0 \) then we are done by the above. If \( A/mA = 0 \) then there are no Jordan-Hölder factors of \( R/m \) for \( A \) or for \( A^{\text{dual}} \). Now suppose \( A \neq mA \neq 0 \). We need the following definition

**Definition 1.2.** If the simple factor modules of a composition series of a module \( M \) are \( Q_1, Q_2, ..., Q_n \), we define

\[ jh(M) = Q_1 \oplus Q_2 \oplus ... \oplus Q_n \]

By induction, we may assume the proposition for all modules of order smaller than \(|A|\). In particular,

\[ jh(mA) = jh((mA)^{\text{dual}}) \quad \text{and} \quad jh(A/mA) = jh((A/mA)^{\text{dual}}). \]
From the two exact sequences above and by [23, Lemma 7.86] we have that
\[ jh(A) = jh(mA) \oplus jh(A/mA) \text{ and } jh(A^{\text{dual}}) = jh((A/mA)^{\text{dual}}) \oplus jh(mA^{\text{dual}}). \]
But since
\[ jh(A/mA) = jh(A^{\text{dual}}/mA^{\text{dual}}) \text{ and } jh(mA) = jh(mA^{\text{dual}}). \]
we have that \( jh(A) = jh(A^{\text{dual}}) \) and this complete the proof of the proposition. \( \Box \)

**Proposition 1.3.** Let \( R \) be a finite Gorenstein ring and \( I \) an ideal of \( R \). Suppose there is an ideal \( J \subset R \) and a surjection \( g : R/J \to I^\perp \) with the property that \( \text{Ann}_R(J) \) annihilates \( R/I \). Then \( g \) is an isomorphism.

**Proof:** We have that \( |I| = |I^\perp| \leq |R/J| = |(R/J)^\perp| = |\text{Ann}_R(J)| \). The last equality follows from the fact that \((R/J)^\perp\) is isomorphic to \( \text{Ann}_R(J) \). 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 \( g \) is an isomorphism. \( \Box \)

This concludes our brief introduction to finite Gorenstein rings. We continue with the theoretical outline of our method.

### 1.3 Extension of the Method to Real Cyclotomic Fields of Conductor \( pq \)

From our description of Schoof’s method in Section 1, one sees that the first thing that needs to be considered is the group of units that will replace the group of cyclotomic units that we have in the case of prime conductor. This subject will be
dealt with in 1.3.1. The second step will be to reformulate the main theorem which describes the modules $B[M]^{\perp}$ in terms of the augmentation ideal and the frobenius maps. This we will present in 1.3.2. In Chapter 2, we will describe everything in terms of polynomials so that we can perform our calculations.

1.3.1 Cyclotomic Units

The group of cyclotomic units of the fields $Q(\zeta_m)^+$ for $m$ not a prime number, and therefore for the fields $Q(\zeta_{pq})^+$, has a complicated structure. Sinnott in [26] defined the cyclotomic units attached to an abelian field $K$ as follows:

**Definition 1.3.** Let $K$ be an abelian field and let $K_m = K \cap Q(\zeta_m)$. Let $a$ be an integer not divisible by $m$. The number $N_{Q(\zeta_m)/K_m}(1 - \zeta_m^a)$ lies in $K^*$. Denote by $D_m$ the group generated in $K^*$ by $-1$ and all such elements $N_{Q(\zeta_m)/K_m}(1 - \zeta_m^a)$. The circular units $H$ are defined by $H = E \cap D_m$, where $E$ is the full group of units of $K$.

In the same paper, Sinnott calculated their index in the full group of units to be

$$[E : H] = 2^b h^+$$

where $b = 0$ if $g = 1$ and $b = 2^{g-2} + 1 - g$ if $g \geq 2$ and $g$ is the number of distinct prime numbers of the conductor $m$.

Kučera and Conrad investigated the group of cyclotomic units described in the definition above, for $K$ being the cyclotomic field of conductor $m$. Kučera in [14] found a basis for $H$ and showed that every cyclotomic unit can be written as
a product of a root of unity and elements in that basis. Similarly, Conrad in [6] constructed a basis $B$ for $H$, with the property that $B_d \subset B_m$ for $d|m$.

In the case where $m$ is an odd prime power, the following units $\xi_a$ together with $-1$ were proven to form a system of independent generators for the group of cyclotomic units of $\mathbb{Q}(\zeta_m)^+$

$$\xi_a = \zeta_m^{(1-a)/2} \frac{1 - \zeta_m^a}{1 - \zeta_m}, \quad 1 < a < \frac{1}{2}m, \quad (a, m) = 1.$$  

For a proof of this see for example [30, Lemma 8.1].

When $m$ is not a prime power however, a set similar to the above does not work since for example the unit $(1 - \zeta_m)$ is not of that form or even worse, this set might be of infinite index in the group of units and hence does not give full rank. In this case, other sets of independent units were introduced which, even though they do not generate the full group of cyclotomic units, they are of finite index in the full group of units. See for example Ramachandra’s set of independent units in [22] and Levesque’s system of independent units in [18], which is a generalization of Ramachandra’s units with smaller index in the full group of units.

In earlier work, Leopoldt in [17] had also studied the group of cyclotomic units. His approach was to decompose it into the product of the groups of cyclotomic units that come from all cyclic subfields of the field in hand. The index of this product of groups in the full group of units however contains a factor whose value is not always known. We will explain Leopoldt’s decomposition of the cyclotomic units in more detail below, since many of the methods for computing prime divisors of $h^+$ adopt this decomposition as it is less complicated to work with the cyclic subfields and
their units, instead of the whole field.

Finally, for a detailed presentation and comparison of the various groups of cyclotomic units and their index in the full groups of units, for the special case of a compositum of real quadratic fields, see [15].

1.3.2 Leopoldt’s Cyclotomic Units and the Decomposition of the Class Number of a Real Abelian Field

Let \( \xi \) denote a rational character of \( G \) irreducible over \( Q \) and for each such \( \xi \neq \xi_0 \) let \( \text{Ker}(\xi) = \{ \alpha \in G | \xi(\alpha) = \xi(1) \} \). Then the fields \( K_\xi \) fixed by \( \text{Ker}(\xi) \) are cyclic of conductor \( f_\xi \) and with cyclic galois group \( G_\xi = G/\text{Ker}(\xi) \) of order \( g_\xi \). For each Dirichlet character \( \chi \) let \( e_\chi = \frac{1}{|G|} \sum_{\alpha \in G} \chi(\alpha^{-1})\alpha \) be its corresponding idempotent and therefore denote by \( e_\xi = \sum_{\chi \in [\xi]} e_\chi \) the orthogonal idempotent of the algebra \( Q[G] \) that corresponds to \( \xi \), with equivalence class denoted by \([\xi]\). We should also explain here that two characters \( \xi \) belong to the same equivalence class if they generate the same cyclic subgroup.

**Definition 1.4.** A real unit \( \varepsilon \) is a \( \xi \)-unit if and only if \( \varepsilon^2 \in K_\xi \) and \( N_{K_\xi/L}(\varepsilon^2) = 1 \) for all proper subfields \( L \) of \( K_\xi \).

For each \( \xi \neq \xi_0 \) let \( E_\xi \subset K_\xi \) be the group of proper \( \xi \)-units of \( K_\xi \). In other words, \( E_\xi \) is the set of \( \xi \)-units that lie in \( K_\xi \). Denote by \( F_\xi \) the group generated by the element \( \theta_\xi = \eta_\xi^\gamma_\xi \), where \( \eta_\xi \) and \( \gamma_\xi \) are defined as follows:

For every automorphism \( \alpha \in \text{Gal}(Q(\zeta_{f_\xi})^+ \cap K_\xi) \) we choose an extension \( \bar{\alpha} \in \text{Gal}(Q(\zeta_{f_\xi})^+ \cap K_\xi) \). For each \( \alpha \in \text{Gal}(Q(\zeta_{f_\xi})^+ \cap K_\xi) \) we choose an extension \( \bar{\alpha} \in \text{Gal}(Q(\zeta_{f_\xi})^+ \cap K_\xi) \).
\[ \text{Gal}(Q(\zeta_{f\xi})/K_{\xi}) \text{ and we define} \]

\[ \eta_{\xi} = \prod_{\alpha} \alpha(\zeta_{f\xi} - \zeta_{f\xi}^{-1}). \]

Let \( \alpha_{\xi} \) be a generator of \( G_{\xi} \) and for every \( \xi \neq \xi_0 \) define

\[ \gamma_{\xi} = \prod_{r|g_{\xi}} (1 - \alpha_{\xi}^{g_{\xi}/r}) \]

where the product runs over all prime divisors \( r \) of \( g_{\xi} \). The element \( \eta_{\xi}^{\gamma_{\xi}} \) is in \( K_{\xi} \) and we have that

\[ \eta_{\xi}^{[G:\gamma_{\xi}]\gamma_{\xi}} = \pm \eta_{\xi}^{u_{\xi}} \]

where

\[ u_{\xi} = \sum_{\alpha \in G} \xi(\alpha^{-1})s \quad \text{and} \quad \eta = \prod_{\xi \neq \xi_0} \eta_{\xi}^{\gamma_{\xi}}. \]

We have \( F_{\xi} = \langle (\pm \theta_{\xi})^s | \alpha \in G_{\xi} \rangle \) and we see that \( F_{\xi} \) is a subgroup of \( E_{\xi} \). Let \( E_{\xi}^0 \) denote the group of \( \xi \)-units. It is a result of Leopoldt that

\[ [E : \prod_{\xi \neq \xi_0} E \cap E_{\xi}^0] = Q_K < \infty \]

and also that \( Q_K \) divides \( g^{\theta - 1} \) and \([E_{\xi}^0 : E_{\xi}]\) is some power of 2. We therefore have that

\[ [E : \prod_{\xi \neq \xi_0} E_{\xi}] = 2^a_K Q_K = Q_K^+ \]

for some \( a_K \). We can now state a main result of Leopoldt:

\[ h^+ = \frac{Q_K^+}{\sqrt{\prod_{\xi \neq \xi_0} d_{\xi}}} \prod_{\xi \neq \xi_0} h_{\xi} \]

where \( h_{\xi} = [E_{\xi} : F_{\xi}] \) and \( d_{\xi} \) is the discriminant of the cyclotomic polynomial \( \Phi_{g_{\xi}}(x) \).

Rearranging we get

\[ h^+ = Q_K^+ g^{(2 - q)/2} \prod_{\xi \neq \xi_0} \sqrt{d_{\xi}} \prod_{\xi \neq \xi_0} h_{\xi} \]
Since the discriminants $d_\xi$ are only divisible by the primes dividing the order of $G$, then so is the factor

$$Q_K^+g^{(2-g)/2} \prod_{\xi \neq \xi_0} \sqrt{d_\xi}.$$ 

Therefore, if we have that a prime $l$ divides some $h_\xi$ and $(l, |G|) = 1$, then we know that $l|h^+$. If $l$ happens to be a divisor of $|G|$ however, then this $l$ might be canceled out by the above factor. Therefore for this case, the formula for $h^+$ above does not give us exact information, except of course from the cases that $Q_K^+$ can be computed.

Gillard in [8], [9] and [10] also studied the cyclotomic units introduced by Leopoldt. In [8] he worked with the unit

$$\Theta = \prod_{\xi \neq \xi_0} \theta_\xi$$

where the product runs over all rational, non-trivial, irreducible characters of $G$ and the $\theta_\xi$ are as above, and calculated the index of $\pm \Theta^I$ in the full group of units, where $I$ is the augmentation ideal of $\mathbb{Z}[G]$. One could adopt this unit and generalize Schoof’s method by letting $B = E/\pm \Theta^I$. We applied our method to Gillard’s unit but we saw that for fields with big conductor, its complicated structure made the computational part take too long.

Given all the above and the complexity of the group of cyclotomic units for fields of non-prime conductor, we decided to work instead with a unit $\eta$ that we introduce below. We prove that the group $H = \pm \eta^{\mathbb{Z}[G]}$ is of finite index in the full group of units and modify the method of Schoof accordingly.
1.3.3 A New Cyclotomic Unit $\eta$

Let $p$ and $q$ be distinct odd primes. From now on, $E$ will denote the group of units of the real cyclotomic field $Q(\zeta_{pq})^+$ and $O$ its ring of integers. Without loss of generality we will always assume that $p < q$. Choose and fix $g$ and $h$, primitive roots modulo $p$ and $q$ respectively. Denote by $\eta(g,h)$ the following real unit of $Q(\zeta_{pq})^+$:

$$\eta(g,h) = \zeta_p^{-g} (1 - \zeta_p^{p+q})^2 \frac{\zeta_p^{-g/2}}{\zeta_p^{-1/2}} \frac{\zeta_q^{-h/2}}{\zeta_q^{-1/2}} \frac{1 - \zeta_q^h}{1 - \zeta_q}$$

and by $H(g,h)$ the group $\pm \eta Z[G]$. We will usually omit the subscripts and just write $H$ and $\eta$ since we will let $\eta_\alpha$ denote the unit $\eta$ with the galois element $\alpha$ acting on it.

With this notation in mind, we are ready to prove a statement about the regulator of the units $\{\eta_\alpha\}_{\alpha \in G}$.

**Proposition 1.4.** Let $E$ be the group of units of $Q(\zeta_{pq})^+$ and $H = \pm \eta Z[G] = \pm \eta Z[G]_{(g,h)}$ as above, where $g$ and $h$ are any two fixed primitive roots modulo $p$ and $q$ respectively.

The index $[E:H]$ is always finite and it equals:

$$[E : H] = \frac{2^{[G] - h^+}}{|G|}.$$

$$\prod_{\chi = \chi_p \neq 1} \frac{1}{2} \left[ 2(\chi(g)^{-1} - 1) + (\chi(g^{-1}) - 1)(q-1) \right] \prod_{\chi = \chi_q \neq 1} \frac{1}{2} \left[ 2(\chi(p)^{-1} - 1) + (\chi(h^{-1}) - 1)(p-1) \right]$$

where the characters $\chi$ in the first product are the even characters $\chi_p$ of conductor $p$ and those in the second product are the even characters $\chi_q$ of conductor $q$.

**Proof:** Define $f$ by $f(\alpha) = log|\eta_\alpha|$. We see that $\sum_\alpha f(\alpha) = log|\prod_\alpha \eta_\alpha| = 0$.

Denote by $\chi$ an even Dirichlet character and note that for any root of unity $\zeta$ we have that $log|\zeta^i(1 - \zeta^j)| = log|1 - \zeta^j|$, where $i$ and $j$ are arbitrary. The regulator $R$
of the units \(\eta_\alpha\) is:

\[
R = R(\{\eta_\alpha\})
\]

\[
= \pm \det(\log|\eta_{\alpha\beta}|)_{\alpha,\beta \neq 1}
\]

\[
= \pm \det(f(\alpha\beta))_{\alpha,\beta \neq 1}
\]

\[
= \pm \det(f(\beta\alpha^{-1}))_{\alpha,\beta \neq 1} \quad \text{(by rearranging the rows)}
\]

\[
= \pm \frac{1}{|G|} \prod_{\chi \neq 1} \sum_{\beta \in G} \chi(\beta)f(\beta) \quad \text{(by [30, Lemma 5.26(c)])}
\]

\[
= \pm \frac{1}{|G|} \prod_{\chi \neq 1} \frac{1}{2} \sum_{1 \leq \beta \leq p, (\beta, pq) = 1} \chi(\beta)[\log|1 - \zeta_{pq}^{\beta(\rho+\omega)}|^2 + \log|1 - \zeta_{pq}^{\beta}| + \log|1 - \zeta_{pq}^{\beta h\beta}|] \quad (*)
\]

Before we continue with the proof of the proposition, we need the following lemmas (the proofs are taken from [30]).

**Lemma 1.1.** For \(m|n \in \mathbb{Z}^+\), if \(f_\chi\) does not divide \((n/m)\) then

\[
\sum_{1 \leq b \leq n, (b,n) = 1} \chi(b) \log|1 - \zeta_{n}^{bm}| = 0.
\]

**Proof:** We need an \(a \equiv 1 \mod n/m\) with \((a,n) = 1\) and \(\chi(a) \neq 1\). If no such \(a\) exists then for every \(a \equiv 1 \mod (n/m)\), if \((a,n) = 1\) then \(\chi(a) = 1\). But this means that the character \(\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to C^\times\) can be factored through \((\mathbb{Z}/(n/m)\mathbb{Z})^\times\), therefore \(f_\chi\mid (n/m)\), contradiction. Hence such \(a\) exists and since \(a \equiv 1 \mod (n/m)\) we have that \(\zeta_{n}^{bm} = \zeta_{n}^{abm}\), hence

\[
\sum_{1 \leq b \leq n, (b,n) = 1} \chi(b) \log|1 - \zeta_{n}^{bm}| = \sum_{1 \leq b \leq n, (b,n) = 1} \chi(b) \log|1 - \zeta_{n}^{abm}| =
\]

\[
\chi(a)^{-1} \cdot \sum_{ab \equiv 1 \mod n} \chi(ab)\log|1 - \zeta_{n}^{abm}| = \chi(a)^{-1} \cdot \sum_{1 \leq b \leq n, (b,n) = 1} \chi(b)\log|1 - \zeta_{n}^{bm}|.
\]
Since \( \chi(a)^{-1} \neq 1 \), we have that
\[
\sum_{\substack{1 \leq b \leq m \\ (b,m) = 1}} \chi(b) \log|1 - \zeta_n^b| = 0,
\]
as we wanted. \( \square \)

**Lemma 1.2.** Let \( n = mm' \) with \( (m, m') = 1 \) and assume \( f_\chi \mid m \). Then
\[
\sum_{1 \leq b \leq n, (b,n) = 1} \chi(b) \log|1 - \zeta_n^{bm'}| = \phi(m') \cdot \sum_{1 \leq a \leq m, (a,m) = 1} \chi(a) \log|1 - \zeta_m^a|.
\]

*Proof:* Since \( f_\chi \mid m \), \( \chi \) factors through \((Z/mZ)^\times\) and for every \( b \) with \( (b,n) = 1 \) there is a \( 0 \leq c < m' \) and an \( 1 \leq a < m \) such that \( (a,m) = 1 \) and \( b = a + cm \).

Conversely, for every \( a \) with \( (a,m) = 1 \) there are \( \phi(m') \) different choices for \( c \) such that \( (b = a + cm, n) = 1 \). Since \( \zeta_n^{bm'} = \zeta_n^b \) we have that \( \zeta_n^{bm'} \) depends only on \( a \) and it is clear that \( \chi \) also only depends on \( a \). The lemma now follows. \( \square \)

**Lemma 1.3.** Let \( P, Q, g \in Z^+ \) with \( f_\chi \mid P \) and \( g \mid P \). Then
\[
\sum_{1 \leq b \leq PQ, (b,g) = 1} \chi(b) \log|1 - \zeta_{PQ}^b| = \sum_{1 \leq a \leq P, (a,g) = 1} \chi(a) \log|1 - \zeta_P^a|.
\]

*Proof:* We can write \( b = a + cP \) for \( 1 \leq a \leq P \) and \( 0 \leq c \leq Q - 1 \). Then \( (b, g) = 1 \) if and only if \( (a, g) = 1 \). Also, from the polynomial identity
\[
1 - x^Q = \prod_{0 \leq c \leq Q-1} (1 - \zeta_{PQ}^{cx})
\]
we get the identity
\[
1 - \zeta_P^a = 1 - (\zeta_{PQ}^a)^Q = 1 - \zeta_P^a = \prod_{0 \leq c \leq Q-1} (1 - \zeta_{PQ}^{a+cP}).
\]
Since the values of the character \( \chi \) only depend on \( a \), the lemma follows. \( \square \)
Lemma 1.4. Let \( n \in \mathbb{Z}^+ \) and assume \( f_\chi \mid n \). Then

\[
\sum_{1 \leq b \leq n} \chi(b) \log |1 - \zeta_n^b| = \prod_{p \mid n} (1 - \chi(p)) \sum_{1 \leq b \leq n} \chi(b) \log |1 - \zeta_n^b|.
\]

Proof Let \( n = \prod_i p_i^{e_i} \) with \( e_i \geq 1 \) be the prime factorization of \( n \). When we expand the product \( \prod_{p \mid n} (1 - \chi(p)) \), the right hand side equals

\[
\sum_{1 \leq b \leq n} \chi(b) \log |1 - \zeta_n^b| - \sum_{p_i} \chi(p_i) \sum_{1 \leq b \leq n} \chi(b) \log |1 - \zeta_n^b| + \\
\sum_{p_i \neq p_j} \chi(p_i p_j) \sum_{1 \leq b \leq m} \chi(b) \log |1 - \zeta_n^b| - ...
\]

We see that only those primes with \( (f_\chi, p_i) = 1 \) appear in the sum above since otherwise \( \chi(p_i) = 0 \). Therefore, we have that \( f_\chi \mid (n/p_i) \) and by Lemma 1.3 above with \( g = 1 \), the sum becomes equal to

\[
\sum_{1 \leq b \leq n} \chi(b) \log |1 - \zeta_n^b| - \sum_{p_i} \sum_{1 \leq b \leq m} \chi(b) \log |1 - \zeta_n^b| + ... = \\
\sum_{1 \leq b \leq n} \chi(b) \log |1 - \zeta_n^b|.
\]

We can now continue with the proof of Proposition 1.3.

For a character \( \chi \) and the first summand in the brackets in (\#) above, we have

\[
2 \sum_{1 \leq \beta \leq pq} \chi(\beta) \log |1 - \zeta_{pq}^{\beta(p+q)}| = \\
2\chi(p+q)^{-1} \sum_{\beta \mid (p+q) \text{ mod } (pq)} \chi(\beta (p+q)) \log |1 - \zeta_{pq}^{\beta(p+q)}| \\
= 2\chi(p+q)^{-1}(1 - \chi(q))(1 - \chi(p)) \sum_{1 \leq \beta \leq pq} \chi(\beta) \log |1 - \zeta_{pq}^{\beta}|
\] (by Lemma 1.4).
To this sum, for characters of conductor $p$ or $q$, we apply Lemma 1.3. The first sum in (*)& now equals:

\[
\begin{cases}
2\chi(p + q)^{-1} \sum_{1 \leq \beta \leq pq} \chi(\beta) \log |1 - \zeta_{pq}^\beta|, & \text{if } f_x = pq \\
2\chi(q)^{-1}(1 - \chi(q)) \sum_{1 \leq \alpha \leq p} \chi(\alpha) \log |1 - \zeta_p^\alpha|, & \text{if } f_x = p \\
2\chi(p)^{-1}(1 - \chi(p)) \sum_{1 \leq \alpha \leq q} \chi(\alpha) \log |1 - \zeta_q^\alpha|, & \text{if } f_x = q
\end{cases}
\]

For a character $\chi$ and the second summand we have

\[
\sum_{1 \leq \beta \leq pq \atop (\beta, pq) = 1} \chi(\beta) \left[ \log |1 - \zeta_p^\beta| - \log |1 - \zeta_p^\beta| \right]
\]

\[
= \chi(g)^{-1} \sum_{g \beta \equiv 1 \pmod{pq} \atop (\beta, pq) = 1} \chi(g\beta) \log |1 - \zeta_p^{g\beta}| - \sum_{1 \leq \beta \leq pq \atop (\beta, pq) = 1} \chi(\beta) \log |1 - \zeta_p^\beta|
\]

\[
= (\chi(g^{-1}) - 1) \sum_{1 \leq \alpha \leq pq \atop (\alpha, pq) = 1} \chi(\alpha) \log |1 - \zeta_p^\alpha|.
\]

If $f_x = pq$ then

\[
\sum_{1 \leq \alpha \leq pq \atop (\alpha, pq) = 1} \chi(\alpha) \log |1 - \zeta_p^\alpha| = \sum_{1 \leq \alpha \leq pq \atop (\alpha, pq) = 1} \chi(\alpha) \log |1 - \zeta_p^\alpha| = 0 \quad \text{(by Lemma 1.1)}.
\]

Similarly, by applying Lemma 1.1 to the second summand for characters of conductor $q$, we also get 0. For the characters of conductor $p$, we apply Lemma 1.2 to the second summand. All of the above give the following:

\[
\begin{cases}
0, & \text{if } f_x = pq \\
(\chi(g^{-1}) - 1)(q - 1) \sum_{1 \leq \alpha \leq p} \chi(\alpha) \log |1 - \zeta_p^\alpha|, & \text{if } f_x = p \\
0, & \text{if } f_x = q
\end{cases}
\]

Similarly, the third summand equals:
\[
\begin{aligned}
&= \begin{cases} 
0, & \text{if } f_\chi = pq \\
0, & \text{if } f_\chi = p \\
(\chi(h^{-1}) - 1)(p - 1) \sum_{1 \leq \alpha \leq q} \chi(\alpha) \log|1 - \zeta_\alpha^p|, & \text{if } f_\chi = q
\end{cases} \\
&\text{Putting all three together and denoting by } \chi_{pq}, \chi_p \text{ and } \chi_q \text{ the characters of conductor } pq, p \text{ and } q \text{ respectively, we have that }
\end{aligned}
\]

Therefore the above equals

\[
= \pm \frac{1}{|G|} \sum_{1 \leq \beta \leq pq} \chi(\beta) \log|1 - \zeta_\beta^{pq}|.
\]

The product over all characters of the term \(\chi(p + q)^{-1}\) will give \(\pm 1\) since the value of each \(\chi\) is canceled out by that of \(\bar{\chi}\). Therefore \(R\) equals

\[
\prod_{\chi = \chi_p \neq 1} \frac{1}{2} [2\chi(q)^{-1} (1 - \chi(q)) + (\chi(g^{-1}) - 1)(q - 1)] \sum_{1 \leq \alpha \leq p} \chi(\alpha) \log|1 - \zeta_\alpha^p|.
\]

The \(L\)-series attached to each even character \(\chi\) satisfies

\[
L(1, \chi) = -\frac{\tau(\chi)}{f_\chi} \sum_{1 \leq b \leq f_\chi} \bar{\chi}(b) \log|1 - \zeta_b^f|.
\]

Therefore \(R\) is now equal to

\[
R = \pm \frac{1}{|G|} \prod_{\chi = \chi_{pq} \neq 1} \frac{-f_\chi}{\tau(\chi)} L(1, \bar{\chi}).
\]
\[
\prod_{\chi = \chi_p \neq 1} \frac{1}{2} \left[ 2(\chi(q)^{-1}) + (\chi(g^{-1}) - 1)(q - 1) \right] \frac{(-f_\chi)}{\tau(\chi)} L(1, \chi).
\]
\[
\prod_{\chi = \chi_q \neq 1} \frac{1}{2} \left[ 2(\chi(p)^{-1}) + (\chi(h^{-1}) - 1)(p - 1) \right] \frac{(-f_\chi)}{\tau(\chi)} L(1, \chi) = \pm \frac{1}{|G|} \prod_{\chi \neq \chi_{even}} \tau(\chi)L(1, \chi).
\]
\[
\prod_{\chi = \chi_p \neq 1} \frac{1}{2} \left[ 2(1 - \chi(q)) + (\chi(g^{-1}) - 1)(q - 1) \right] \prod_{\chi = \chi_q \neq 1} \frac{1}{2} \left[ 2(1 - \chi(p)) + (\chi(h^{-1}) - 1)(p - 1) \right].
\]

The class number formula for a real number field \( K \) of degree \( n \), discriminant \( d \), class number \( h^+ \) and regulator \( R^+ \), is given by the formula
\[
\frac{2^{[G]} h^+ R^+}{2 \sqrt{|d|}} = \prod_{1 \neq \chi_{even}} L(1, \chi).
\]

By applying this formula to the above, we have that \( R \) is now equal to
\[
R = \frac{2^{[G]} h^+ R^+}{|G|}.
\]
\[
\prod_{\chi = \chi_p \neq 1} \frac{1}{2} \left[ 2(\chi(q)^{-1}) + (\chi(g^{-1}) - 1)(q - 1) \right] \prod_{\chi = \chi_q \neq 1} \frac{1}{2} \left[ 2(\chi(p)^{-1}) + (\chi(h^{-1}) - 1)(p - 1) \right].
\]

Therefore,
\[
\frac{R}{R^+} = \frac{2^{[G]} h^+}{|G|}.
\]
\[
\prod_{\chi = \chi_p \neq 1} \frac{1}{2} \left[ 2(\chi(q)^{-1}) + (\chi(g^{-1}) - 1)(q - 1) \right] \prod_{\chi = \chi_q \neq 1} \frac{1}{2} \left[ 2(\chi(p)^{-1}) + (\chi(h^{-1}) - 1)(p - 1) \right].
\]

So now, by [30, Lemma 4.15], we have that
\[
[E : H] = \frac{R}{R^+} = \frac{2^{[G]} h^+}{|G|}.
\]
\[
\prod_{\chi = \chi_p \neq 1} \frac{1}{2} \left[ 2(\chi(q)^{-1}) + (\chi(g^{-1}) - 1)(q - 1) \right] \prod_{\chi = \chi_q \neq 1} \frac{1}{2} \left[ 2(\chi(p)^{-1}) + (\chi(h^{-1}) - 1)(p - 1) \right]
\]
as desired.
To show that \([E:H]\) is always finite it suffices to show that the regulator is never zero. Assume it is zero. Then for some character of conductor \(p\) the sum
\[
2(\chi(q)^{-1} - 1) + (\chi(g^{-1}) - 1)(q - 1)
\]
is zero or for some character of conductor \(q\) the sum
\[
2(\chi(p)^{-1} - 1) + (\chi(h^{-1}) - 1)(p - 1)
\]
is zero. But
\[
2(\chi(q)^{-1} - 1) + (\chi(g^{-1}) - 1)(q - 1) = 0
\]
\[
\Leftrightarrow
\]
\[
2\chi(q)^{-1} + (q - 1)\chi(g)^{-1} = 2 + (q - 1)
\]
which never happens as \(\chi(g)^{-1}\) can never equal 1, since \(g\) is a primitive root. Similarly for a character of conductor \(q\). Therefore, the regulator is never zero and this completes the proof of Proposition 1.3. \(\Box\)

Denote by \(P\) the factor
\[
\frac{2^{|G|-1}}{|G|} \prod_{\chi=\chi_p \neq 1} \left[2(\chi(q)^{-1} - 1) + (\chi(g^{-1}) - 1)(q - 1)\right] \prod_{\chi=\chi_q \neq 1} \left[2(\chi(p)^{-1} - 1) + (\chi(h^{-1}) - 1)(p - 1)\right]
\]
which appears in the index \([E:H]\) in Proposition 1.3 above. We now have
\[
[E : H] = P \cdot h^+.
\]
One can take advantage of the fact that any choice of primitive roots \(g\) and \(h\) give a finite index, and for each field \(Q(\zeta_{pq})^+\) one can choose the pair \((g,h)\) with the property that \(P_{(g,h)}\) is divisible by the smallest number of distinct primes. Furthermore,
for the primes that appear in this $P_{(g,h)}$ one can check to see if those primes divide the greatest common divisor of all the $P_{(g,h)}$ for every pair of primitive roots $(g,h)$. In the case that a prime $l$ does not divide the greatest common divisor, there is some pair $(g_0, h_0)$ for which $l$ does not divide $P_{(g_0,h_0)}$. We can therefore repeat the first part of our algorithm that we explain in the next chapter, for this pair $(g_0, h_0)$ and for this prime $l$. If $l$ does not come up as a possible divisor for this pair of primitive roots this means that it only divides $P_{(g,h)}$ for the initial choice of $g$ and $h$ and not the class number. Hence, we do not need to consider this $l$ in the next steps of the algorithm. These facts are very useful in the computations described in the next chapter, since they narrow down the number of primes that one needs to check to see if they divide $h^+$ and hence speed up the calculations.

In the remainder of this chapter we reformulate Schoof’s main theorem that describes the module $B = E/H$ in terms of the various $B[M]^\perp$.

### 1.3.4 The module $B = E/H = E/\pm \eta Z[G]$  

We denote by $B$ be the $Z[G]$-module $E/H$, where $H = \pm \eta Z[G]$ as above. From Proposition 1.3 we have that the order of $B$ is finite and equals the index $[E : H]$. Therefore, by generalizing Schoof, we can calculate its order and then multiply by $1/P$ in order to get $h^+$, as desired.

Since $H$ is of finite index in $E$ we have that the map
Φ : Z[G] → E

: α ↦ η^a

is a homomorphism whose image H is of finite index and therefore Z-isomorphic to Z[G]^{-1}. We have that H ∼= Z[G]/N_G as Z[G]-modules, where N_G is the norm of G.

Let M > 1 denote a power of a prime l. We let F = Q(ζ_{pq})^+(ζ_{2M}) and Δ = Gal(F/Q(ζ_{pq})^+).

**Lemma 1.5.** The kernel of the natural map

\[ j : E/E^M → F^*/F^{*M} \]

is trivial if l odd and it has order two and is generated by -1 if l = 2.

**Proof:** Fix an embedding F ⊂ C. Then Q(ζ_{pq})^+ identifies with a subfield of R. Suppose 0 < x ∈ E ⊂ R is in Ker j. Then x = y^M, some y ∈ F^*. Since μ_M ⊂ F we may assume that y ∈ R and therefore conj(y) = y, where conj is complex conjugation in Δ. Since Δ commutative, s(y) = s(conj(y)) = conj(s(y)) ∀s ∈ Δ, therefore s(y) = ±y ∀s ∈ Δ, since y and all its conjugates are real M-th roots of x. If l ≠ 2 then M is odd. Assume ∃s ∈ Δ with s(y) = -y. Then x = s(x) = s(y^M) = (s(y))^M = (-y)^M = -x, contradiction. Therefore Δ fixes y and hence y ∈ (Q(ζ_{pq})^+)^* and x ∈ E^M. Since we took x > 0 we need to check for -1 as well. Since M odd, (-1)^M = -1 therefore -1 ∈ E^M as well and in this case j is an injection. If l = 2 we see that s(y^2) = s(y)^2 = y^2 therefore y^2 ∈ Q(ζ_{pq})^+. The quadratic subextensions of F/Q(ζ_{pq})^+ are Q(ζ_{pq})(i) and Q(ζ_{pq})^+(√±2) and hence
\[ y^2 = 2u^2 \text{ or } = \pm u^2, \text{ for some } u \in E. \] If \( y^2 = 2u^2 \), then \( 2 = y^2u^2 \), with \( v \) such that \( vu = 1 \), which can not happen since then \( (2) = (v)^2 \) as ideals but \( 2 \) does not ramify in \( Q(\zeta_{pq})^+ \). So we can only have the second case where \( x = y^M = (\sqrt{y})^{2(k-1)} \). For \( k \geq 2 \) we have \( x = u^2 \) and therefore \( x \in E^M \). When \( k = 1 \) we have \( x = y^2 = \pm u^2 \), but since \( x > 0 \) we still get \( x = u^2 \) which implies that \( x \in E^M \). For \(-1\), observe that \(-1 = \zeta_{2M}^M \) but \(-1 \) is not even a square in \( Q(\zeta_{pq})^+ \) which means \( kerj = (-1) \) of order two in this case. \( \square \)

Let \( \Omega = Gal(F/Q) \). We have the following exact sequence of galois groups

\[ 0 \to \Delta \to \Omega \to G \to 0. \]

Let \( \mathfrak{R} \) be any prime ideal of \( F \) of degree 1, \( \rho \) a prime ideal of \( Q(\zeta_{pq})^+ \) and \( r \) a prime number such that \( \mathfrak{R} \mid \rho \mid r \). We have \( r \equiv \pm 1 \mod (pq) \) and \( r \equiv 1 \mod (2M) \). Let \( g = |G| = \frac{(p-1)(q-1)}{2} \) and consider the following diagram:

\[
\begin{array}{cccc}
\varepsilon \in E & \xrightarrow{f_1} & \overline{\varepsilon} \in (O/rO)^* & \xrightarrow{f_2} \xrightarrow{f_3} (O_F/rO_F)^* \Delta \\
& & \mu_M(O/rO) & \xleftarrow{f_4} \mu_M(O_F/rO_F)^\Delta \\
& & \mu_M(O_F/rO_F)^\Delta & \xrightarrow{f_5} \xleftarrow{f_4} (Z/MZ)[\Omega]^\Delta \\
& & (Z/MZ)[\Omega]^\Delta & \xrightarrow{f_5} (Z/MZ)[G]
\end{array}
\]

The map \( f_1 \) is reduction modulo the ideal \( rO \) and \( \overline{\varepsilon} = (\varepsilon_1, ..., \varepsilon_g) \) where \( \varepsilon_i \equiv \varepsilon \mod \rho_i \) and the \( \rho_i \) are the primes dividing \( r \). The maps \( f_2 \) and \( f_2' \) are just inclusion maps. The vertical maps \( f_3 \) and \( f_3' \) raise the units to the power \( (r - 1)/M \) and therefore become \( M \)-th roots of unity in \( O/rO \) (respectively in \( O_F/rO_F \)). Here \( \mu_M(R) \) denotes the \( M \)-th roots of unity of a commutative ring \( R \). The map \( f_4 \) maps \( 1 \in (Z/MZ)[\Omega] \) to the unique element in \( \mu_M(O_F/rO_F) \) that is congruent to \( \zeta_{2M} \mod \mathfrak{R} \) and congruent
to 1 modulo all the other primes \( \mathfrak{R}' \) that lie over \( r \). There is such an \( \varepsilon \in E \) with 
\[ f'_3f_2f_1(\varepsilon) \equiv \zeta_{2M}(\text{mod} \mathfrak{R}) \quad \text{and} \quad f'_3f_2f_1(\varepsilon) \equiv 1(\text{mod} \mathfrak{R}'), \]
by the Chinese Remainder Theorem. Furthermore, since \( r \) splits completely in \( F \), the orders of the two groups are equal and therefore the map \( f_4 \) is an isomorphism. Finally, the map \( f_5 \) sends an element \( \bar{g} \in G \cong \Omega/\Delta \) to the sum of its inverse images and once we fix an inverse image \( g \), this comes down to multiplying \( g \) by the \( \Delta \)-norm = \( \sum_{s \in \Delta} s \). The map \( f_5 \) is an isomorphism since \( \mathbb{Z}/M\mathbb{Z})[\Omega]^{\Delta} \) is fixed by \( \Delta \). Let \( f_{\mathfrak{R}} = f^{-1}_5 f^{-1}_4 f'_3 f_2 f_1 \). Since \(-1 = \zeta_{2M}^M\) we have that \( f_{\mathfrak{R}}(-1) = 0 \) and hence \( f_{\mathfrak{R}} \) factors through the quotient 
\[ f_{\mathfrak{R}} : E/ \pm E^M \to (\mathbb{Z}/M\mathbb{Z})[G]. \]

**Lemma 1.6.** The maps \( f_{\mathfrak{R}} \) correspond to the frobenius elements of the primes over \( \mathfrak{R} \) in \( \text{Gal}(F(\sqrt{E})/F) \). Furthermore, every map in \( \text{Hom}_R(E/ \pm E^M, R) \) is of the form \( f_{\mathfrak{R}} \) for some \( \mathfrak{R} \in S \) where \( S \) denotes the set of unramified prime ideals \( \mathfrak{R} \) of \( Q(\zeta_p)+\zeta_{2M} \) of degree 1 and \( R = (\mathbb{Z}/M\mathbb{Z})[G] \).

**Proof:** Let \( \mu_M \) denote the \( M \)-th roots of unity and once we choose a primitive \( M \)-th root we have the isomorphism 
\[ \text{Hom}_{\mathbb{Z}}(E/ \pm E^M, \mu_M) \cong \text{Hom}_{\mathbb{Z}}(E/ \pm E^M, \mathbb{Z}/M\mathbb{Z}) \]
which is naturally isomorphic to \( \text{Hom}_{\mathbb{Z}}(E/ \pm E^M, Q/Z) \). The group \( E/ \pm E^M \) is a module over the group ring \( (\mathbb{Z}/M\mathbb{Z})[G] = R \), hence 
\[ \text{Hom}_{\mathbb{Z}}(E/ \pm E^M, Q/Z) \cong \text{Hom}_{\mathbb{Z}}(E/ \pm E^M \otimes_R R, Q/Z) \]
and the Adjoint Isomorphism Theorem gives 
\[ \text{Hom}_{\mathbb{Z}}(E/ \pm E^M \otimes_R R, Q/Z) \cong \text{Hom}_R(E/ \pm E^M, \text{Hom}_{\mathbb{Z}}(R, Q/Z)). \]
By Definition 1.1 we have that
\[ \text{Hom}_Z(R, Q/Z) = R^{\text{dual}} \cong R \]
and we have therefore shown that
\[ \text{Hom}_Z(E/ \pm E^M, \mu_M) \cong \text{Hom}_R(E/ \pm E^M, R). \]

Now, from Lemma 1.5 above, we can identify the group \( E/ \pm E^M \) with a subgroup of \( F^*/F^{*M} \). Consider the extension \( F(\sqrt[n]{E})/F \). Since \( \mathfrak{R} \) splits completely, we can associate to it a uniquely determined element \( \beta \) in \( \text{Gal}(F(\sqrt[n]{E})/F) \), namely the frobenius automorphism corresponding to \( \mathfrak{R} \), such that \( \beta(\sqrt[n]{\epsilon}) \equiv (\sqrt[n]{\epsilon})^r (\text{mod } \mathfrak{R}) \).

From our definition of \( f_{\mathfrak{R}} \) above we have \( f_{\mathfrak{R}}(\epsilon) = \sum_{s \in G} x_s s \) where \( x_s \) is determined by
\[ s^{-1}(\epsilon)^{(r-1)/M} \equiv \zeta_M^{x_s} \text{ mod } \mathfrak{R}. \]
The corresponding homomorphism in \( \text{Hom}_Z(E/\pm E^M, Z/MZ) \) maps \( \epsilon \) to \( x_1 \). Since \( \beta(\epsilon)/\epsilon \) is an \( M \)-th root of unity, we can write \( \beta(\sqrt[n]{\epsilon})/\sqrt[n]{\epsilon} \equiv \zeta_M^{x_1} \text{ mod } \mathfrak{R} \iff \epsilon^{(r-1)/M} \equiv \zeta_M^{x_1} \text{ mod } \mathfrak{R} \). Therefore every \( f_{\mathfrak{R}} \) corresponds to the frobenius map of \( \mathfrak{R} \) in \( \text{Gal}(F(\sqrt[n]{E})/F) \). From Kummer Theory we have that
\[ \text{Gal}(F(\sqrt[n]{E})/F) \cong \text{Hom}_Z(E/ \pm E^M, \mu_M) \]
and we showed above that \( \text{Hom}_Z(E/ \pm E^M, \mu_M) \cong \text{Hom}_R(E/ \pm E^M, R) \). By Cebotarev’s Density Theorem every element of \( \text{Hom}_R(E/ \pm E^M, R) \) is of the form \( f_{\mathfrak{R}} \) for some prime \( \mathfrak{R} \) of degree 1. This concludes the proof of the lemma. \( \square \)

**Theorem 1.1.** Let \( l \) and \( M \) be as above and let \( I \) denote the augmentation ideal of
$R = (Z/MZ)[G]$. We have $B[M]^\perp \cong I/\{f_{\mathfrak{R}}(\eta) : \mathfrak{R} \in S\}$, where $S$ denotes the set of unramified prime ideals $\mathfrak{R}$ of $Q(\zeta_{pq})^+(\zeta_{2M})$ of degree $1$.

**Proof:** Applying the Snake Lemma to the following diagram

\[
\begin{array}{cccccc}
0 & \rightarrow & H/\{\pm1\} & \rightarrow & E/\{\pm1\} & \rightarrow & B & \rightarrow & 0 \\
& & \downarrow^M & & \downarrow^M & & \downarrow^M & & \\
0 & \rightarrow & H/\{\pm1\} & \rightarrow & E/\{\pm1\} & \rightarrow & B & \rightarrow & 0
\end{array}
\]

yields the exact sequence of $R$-modules

\[
0 \rightarrow B[M] \rightarrow H/\pm H^M \rightarrow E/\pm E^M.
\]

Since $Q/Z$ is an injective $Z$-module, the contravariant functor $\text{Hom}_Z(\_, Q/Z)$ is an exact functor. Furthermore, from Proposition 1.1 we have that $A^\perp \cong A^{\text{dual}}$. From both of the above, we therefore get the exact sequence

\[
\text{Hom}_R(E/\pm E^M, R) \rightarrow \text{Hom}_R(H/\pm H^M, R) \rightarrow \text{Hom}_R(B[M], R) \rightarrow 0.
\]

which gives the isomorphisms

\[
\text{Hom}_R(B[M], R) = B[M]^\perp \cong \text{Hom}_R(H/\pm H^M, R)/\text{Hom}_R(E/\pm E^M, R).
\]

As we showed earlier,$$
H/\{\pm1\} \cong Z[G]/N_G$$

and similarly here

$$(Z/MZ)[G]/N_G \cong H/\pm H^M,$$

so the $G$-norm kills every $R$-homomorphism $f : H/\pm H^M \rightarrow R$. We see that
Hom}_R(H/ \pm H^M, R) \cong Hom}_R(R/N_G, R) \cong Ann_R(N_G) \cong I.

Furthermore, the map

\[ Hom_R(E/ \pm E^M, R) \to Hom_R(H/ \pm H^M, R) \to I \]

is given by restriction and then evaluation on \( \eta \). Therefore, by Lemma 1.6 we have that

\[ Hom_R(E/ \pm E^M, R) \cong \{ f_\mathfrak{R}(\eta) : \mathfrak{R} \in S \} \]

where \( S \) denotes the set of unramified prime ideals \( \mathfrak{R} \) of \( \mathbb{Q}(\zeta_{pq})^+(\zeta_2M) \) of degree 1.

From all of the above we obtain

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

as we wanted. \( \square \)

In the next chapter, we describe everything in terms of polynomials so that we can perform our calculations, and then we give an example.
Chapter 2

The Computational Part and an Example

In this chapter we will use Theorem 1.1 and express $B[M]^\perp$ in terms of polynomials, so that we can perform our calculations. In this chapter, $l$ will denote an odd prime.

2.1 Reformulating Theorem 1.1 in terms of Polynomials

Let $l$ be a fixed odd prime, $M > 1$ some fixed power of $l$ and $G$ denotes the galois group of $\mathbb{Q}(\zeta_{pq})^+$. The group $G$ is of order $(p-1)(q-1)/2$ and we have the isomorphisms

$$G \cong \left( (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \right)/\{\pm 1\} \cong \langle \sigma, \tau : \sigma^{(p-1)} = 1, \tau^{(q-1)} = 1, \sigma^{(p-1)/2}\tau^{(q-1)/2} = 1 \rangle$$

where $\sigma : \zeta_p \mapsto \zeta_p^\gamma$ and $\tau : \zeta_q \mapsto \zeta_q^\delta$ with $\gamma$ and $\delta$ being fixed primitive roots modulo $p$ and $q$ respectively. The last of the three relations is the relation for complex conjugation. The primitive roots $\gamma$ and $\delta$ will be fixed throughout and will always represent the generators of $(\mathbb{Z}/p\mathbb{Z})^\times$ and $(\mathbb{Z}/q\mathbb{Z})^\times$ respectively. We see that

$$Z[G] \cong Z[x, y]/(x^{p-1} - 1, y^{q-1} - 1, x^{(p-1)/2}y^{(q-1)/2} - 1)$$

via the map that sends $\sigma$ to $x$ and $\tau$ to $y$. Similarly,

$$(Z/M\mathbb{Z})[G] \cong (Z/M\mathbb{Z})[x, y]/(x^{p-1} - 1, y^{q-1} - 1, x^{(p-1)/2}y^{(q-1)/2} - 1).$$
Using this notation, the maps $f_\mathcal{R}$ that were introduced in the previous chapter can now be expressed as polynomials in the variables $x$ and $y$ as follows:

$$f_\mathcal{R}(x, y) = \sum_{1 \leq i \leq p-1} \sum_{1 \leq j \leq (q-1)/2} \log_l(\eta_{i,j}) \cdot x^i \cdot y^j$$

where

$$\eta_{i,j} = \zeta_p^{-\gamma_i} \zeta_q^{-\delta_j} (1 - \zeta_p^{\gamma_i} \zeta_q^{\delta_j} )^2 \frac{\zeta_p^{-g\gamma_i/2}}{(1 - \zeta_p^{\gamma_i})} \frac{\zeta_q^{-h\delta_j/2}}{(1 - \zeta_q^{\delta_j})}.$$

Here, $\log_l$ denotes the discrete log which gives $\log_l(\eta) = s$ where $s \in \mathbb{Z}/MZ$ is such that $\eta^{(r-1)/M} \equiv \zeta_M^s \mod \mathcal{R}$.

We note here that the second sum in the definition of $f_\mathcal{R}(x, y)$ goes from 1 up to $(q - 1)/2$ since we are in the real subfield of $Q(\zeta_{pq})$.

Given the above, we can now reformulate Theorem 1.1 of the previous chapter as follows:

**Theorem 2.1.** Let $l$ be a fixed prime and let $M > 1$ be some fixed power of $l$.

Denote by $R$ the ring

$$(Z/MZ)[x, y]/(x^{p-1} - 1, y^{q-1} - 1, x^{(p-1)/2}y^{(q-1)/2} - 1)$$

and let $B[M]^\perp$ be as in Theorem 1.1. Then

$$B[M]^\perp \cong (x - 1, y - 1) \big/ \{f_\mathcal{R}(x, y) : \mathcal{R} \in S\}$$

where $S = \{\text{the degree 1 prime ideals of } Q(\zeta_{pq})^\perp(\zeta_{2M})\}$.

**Proof:** From our polynomial description of $Z[G]$ above, it follows that $(x - 1, y - 1)$ is the augmentation ideal of $(Z/MZ)[G]$. The result is now immediate from Theorem 1.1. □
We have now expressed the modules $B[M]^{\perp}$ in terms of polynomials. Another step that is necessary for our calculating of their orders, especially for fields with big conductors, is to find a way to break down these modules into smaller pieces. This we handle in the next section.

2.2 The Decomposition of the modules $B[M]^{\perp}$

Let $\tilde{G}$ denote the Galois group of the extension $Q(\zeta_{pq})/Q$. We can write $Z_l[\tilde{G}]$ as follows: for the same fixed prime $l$ as above, write $p - 1 = m_1 l^{a_1}$ and $q - 1 = m_2 l^{a_2}$ where $l^{\alpha_1} || p - 1$ and $l^{\alpha_2} || q - 1$. Since now $l$ does not divide $m_1$ and $m_2$, we have that

$$Z_l[\tilde{G}] \cong Z_l[x, y]/(x^{p-1} - 1, y^{q-1} - 1) \cong \prod_{\phi_x, \phi_y} Z_l[x, y]/(\phi_x(x^{a_1}), \phi_y(y^{a_2})) \cong \prod_{\phi_x} Z_l[x]/(\phi_x(x^{a_1})) \otimes \prod_{\phi_y} Z_l[y]/(\phi_y(y^{a_2}))$$

where the product runs over all irreducible divisors $\phi_x$ of $x^{m_1} - 1$ and $\phi_y$ of $y^{m_2} - 1$. We see that $Z_l[x]/(\phi_x(x^{m_1}))$ and $Z_l[y]/(\phi_y(y^{m_2}))$ are complete local $Z_l[\tilde{G}]$-algebras with maximal ideals $(l, \phi_x(x))$ and $(l, \phi_y(y))$, respectively, and the orders of their residue fields are $l^{f_1}$ and $l^{f_2}$, where $f_1 = \deg(\phi_x(x))$ and $f_2 = \deg(\phi_y(y))$. Let $\Delta$ denote the subgroup of $\tilde{G}$ of order prime to $l$. From the decomposition of $Z_l[\tilde{G}]$ above, we can write any finite $Z_l[\tilde{G}]$-module $A$ as a product of its $\phi$-parts

$$A_{\phi_x, \phi_y} = A \otimes_{Z_l[\tilde{G}]} \left( Z_l[x]/(\phi_x(x^{a_1})) \otimes \prod_{\phi_y} Z_l[y]/(\phi_y(y^{a_2})) \right).$$
The simple Jordan-Hölder factors of each \( A_{\phi_x, \phi_y} \) over \( Z_l[\Delta] \) are the same as those over \( Z_l[\tilde{G}] \) since we ‘removed’ the powers of \( x \) and \( y \) dividing the order of \( \tilde{G} \).

All of the above about the module \( A \) also hold in particular for \( B \), the various \( B[M]^{\perp} \) and their \( \phi \)-parts \( B[M]^{\perp}_{\phi_x, \phi_y} \). Therefore, when we want to find the Jordan-Hölder factors of \( B \) we can start by taking all combinations of degrees \( f_1 \) and \( f_2 \). Since \( x \) and \( y \) are non-zero elements in the corresponding residue fields \( \left[ Z_l[x]/(\phi_x(x^{l^{a_1}})) \right]/(l, \phi_x(x)) \) and \( \left[ Z_l[y]/(\phi_y(y^{l^{a_2}})) \right]/(l, \phi_y(y)) \), we must have that the orders of \( x \) and \( y \) in the ring attached to \( \phi_x \) and \( \phi_y \) must divide \((l^{f_1} - 1)\) and \((l^{f_2} - 1)\) respectively. Let \( d_1 = \gcd(p - 1, l^{f_1} - 1) \) and \( d_2 = \gcd(q - 1, l^{f_2} - 1) \) and let

\[
R_{d_1, d_2} = (Z/MZ)[x, y]/((x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1).
\]

Since the rings \( R_{d_1, d_2} \) and \( R_{\phi_x, \phi_y} \) are direct summands of \( R \), any map from their modules \( B[M]_{d_1, d_2} \) and \( B[M]_{\phi_x, \phi_y} \), respectively, to \( R \) will end up in these smaller rings. Therefore we can refer to \( B[M]^{\perp}_{d_1, d_2} \) and \( B[M]^{\perp}_{\phi_x, \phi_y} \) as \( R_{d_1, d_2} \) and \( R_{\phi_x, \phi_y} \) modules, respectively.

We see that, instead of going all the way down to the various \( B[M]^{\perp}_{\phi_x, \phi_y} \) and looking for the simple Jordan-Hölder factors, one could evaluate directly the order of the various \( R_{d_1, d_2} \)-modules

\[
B[M]^{\perp}_{d_1, d_2} \cong (x - 1, y - 1)/(x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1, cnj, f_{\mathbb{R}}(x, y) : \mathbb{R} \in S \quad (i)
\]

where \( S \) is as in Theorem 2.1 and \( cnj \) denotes the conjugation relation

\[
 cnj = x^{(p-1)/2}y^{(q-1)/2} - 1
\]

as above. We have that \((1 \pm c)/2\) are idempotents in \( (Z/MZ)[\tilde{G}] \) for \( M \) odd, where
c denotes complex conjugation. Therefore, the conjugation relation in the ideal

\[ J = \langle (x^{\ell_1})^{d_1} - 1, (y^{\ell_2})^{d_2} - 1, cnj, f_\mathcal{R}(x, y) : \mathcal{R} \in S \rangle \quad (ii) \]

from (i) above, makes \( B[M]_{d_1,d_2}^1 \) a \((Z/MZ)[G]\)-module. Note that here, the polynomials \( f_\mathcal{R} \) are restrictions of the frobenius elements of Theorem 2.1 to this smaller extension determined by the set of polynomials \((x^{\ell_1})^{d_1} - 1\) and \((y^{\ell_2})^{d_2} - 1\). They are therefore of the form

\[ f_\mathcal{R}(x, y) = \sum_{1 \leq i \leq d_1 \ell_1} \sum_{1 \leq j \leq d_2 \ell_2} \log_l \left( \prod_{m \equiv i \mod (d_1 \ell_1)} \eta(m, n) \right) \cdot x^i \cdot y^j \quad (iii). \]

### 2.3 Gröbner Bases

Before we continue with the outline of the algorithm, one last thing that needs to be discussed is the way we handle the appearance of two variables \( x \) and \( y \) in our calculations of the ideals \( J \) defined in the previous section, in order to get a description of the various \( B[M]_{d_1,d_2}^1 \) and to also calculate their order. We use the theory for Gröbner Bases, which we present here by following [1]. As before, \( d_1 = \gcd(p - 1, \ell_1 - 1) \) will be the order of \( x \) and \( d_2 = \gcd(q - 1, \ell_2 - 1) \) will be the order of \( y \) in the ring \( R_{d_1,d_2} \), where \( f_1 \) and \( f_2 \) are the degrees of some irreducible polynomials \( \phi_x \) and \( \phi_y \) respectively. Again, let \( B[M]_{d_1,d_2}^1 \) be the corresponding \( R_{d_1,d_2} \)-module and

\[ J = \langle (x^{\ell_1})^{d_1} - 1, (y^{\ell_2})^{d_2} - 1, cnj, f_\mathcal{R}(x, y) : \mathcal{R} \in S \rangle \]

the corresponding ideal. All the computations for the calculation of the frobenius polynomials were performed in PARI and the computations for a basis for the ideal
In MATHEMATICA, which allows the computations of bases for ideals whose elements are polynomials in more than one variable and their coefficients are in any ring \((Z/MZ)\), not necessarily a field.

In this section, \(R = A[x, y]\) will denote a polynomial ring in two variables \(x\) and \(y\) with coefficients in a Noetherian ring \(A\). Hence \(R\) is Noetherian as well. This \(R\) is not necessarily related to the various rings \(R_{d_1, d_2}\) of the previous section. We use \(R\) more generally. Because of the appearance of more than one variable in our polynomials, we need to agree on the order of the variables and also find a way to compare every element. We call a power product an element of the form \(x^a y^b\) with \(a, b\) non-negative integers and we denote by \(T^2\) the set of all power products of the polynomial ring \(R_{d_1, d_2}\) defined in the previous section as

\[
R_{d_1, d_2} = (Z/MZ)[x, y]/(x^{d_1} - 1, y^{d_2} - 1).
\]

Following the definition of term order given in [1], we define a total order on \(T^2\) as follows:

**Definition 2.1.** By a term order on \(T^2\) we mean a total order \(<\) on \(T^2\) which satisfies the following conditions:

(i) \(1 < x^a y^b\) for all \(1 \neq x^a y^b \in T^2\)

(ii) If \(x^{a_1} y^{b_1} < x^{a_2} y^{b_2}\) then \((x^{a_1} y^{b_1}) (x^c y^d) < (x^{a_2} y^{b_2}) (x^c y^d)\) for all \((x^c y^d) \in T^2\).

The type of term order that we use here is the lexicographical order on \(T^2\) which we define below:

**Definition 2.2.** The lexicographical order on \(T^2\) with \(x > y\) is defined as:
For \((a_1, b_1), (a_2, b_2)\) with \(a_i, b_i\) positive integers, we define \(x^{a_1}y^{b_1} < x^{a_2}y^{b_2}\) if and only if \((a_1 < a_2\) or \((a_1 = a_2\) and \(b_1 < b_2))\). We therefore have

\[1 < y < y^2 < y^3 < ... < x < xy < xy^2 < ... < x^2 < ...\]

Now that we have chosen a term order on our polynomial ring, for each polynomial

\[f = c_1x^{a_1}y^{b_1} + c_2x^{a_2}y^{b_2} + ... + c_nx^{a_n}y^{b_n}\]

with \(c_i \neq 0\) in \((Z/MZ)\) and \(x^{a_1}y^{b_1} > x^{a_2}y^{b_2} > ... > x^{a_n}y^{b_n}\), we can define:

- \(lp(f) = x^{a_1}y^{b_1}\), the leading power product of \(f\),
- \(lc(f) = c_1\), the leading coefficient of \(f\),
- \(lt(f) = c_1x^{a_1}y^{b_1}\), the leading term of \(f\).

Since the coefficients are not necessarily in a field, we need to ‘re-define’ division.

**Definition 2.3.** Let \(G\) be a set of polynomials in \(R\), \(G = \{g_1, g_2, ..., g_n\}\). We say that \(f\) reduces to \(h\) modulo the set \(G\) in one step, denoted

\[f \xrightarrow{G} h,\]

if and only if

\[h = f - (c_1x^{a_1}y^{b_1}f_1 + ... + c_sx^{a_s}y^{b_s}f_s)\]

for \(c_1, ..., c_s \in R\) and with \(lp(f) = x^{a_i}y^{b_i}lp(f_i)\) for all \(i\) such that \(c_i \neq 0\) and \(lt(f) = c_1x^{a_1}y^{b_1}lt(f_1) + ... + c_sx^{a_s}y^{b_s}lt(f_s)\).
**Definition 2.4.** Let \( f, h \) and \( f_1, f_2, \ldots, f_s \) be polynomials in \( R \), with \( f_i \neq 0 \ \forall \ 1 \leq i \leq s \), and let \( F = \{f_1, f_2, \ldots, f_s\} \). We say that \( f \) reduces to \( h \) modulo \( F \), denoted

\[
 f \xrightarrow{F} h ,
\]

if and only if there exist polynomials \( h_1, \ldots, h_{t-1} \in R \) such that

\[
 f \xrightarrow{F} h_1 \xrightarrow{F} h_2 \xrightarrow{F} \cdots \xrightarrow{F} h_{t-1} \xrightarrow{F} h .
\]

We note that if

\[
 f \xrightarrow{F} h ,
\]

then \( f - h \in \langle f_1, \ldots, f_s \rangle \).

We will now give the statement of a theorem ([1, Theorem 4.14]) which basically serves as the definition for a Gröbner Basis. We need to state first that the leading term ideal of an ideal \( V \) of a ring \( R \), denoted by \( LT(V) \), is defined as:

\[
 LT(V) = \langle \{lt(v) : v \in V \} \rangle .
\]

**Theorem 2.2.** Let \( V \) be an ideal of \( R \) and let \( G = \{g_1, \ldots, g_n\} \) be a set of non-zero polynomials in \( V \). The following are equivalent:

(i) \( LT(G) = LT(V) \).

(ii) For any polynomial \( f \in R \) we have

\[
 f \in V \text{ if and only if } \quad f \xrightarrow{G} 0
\]

(iii) For all \( f \in V \), \( f = h_1g_1 + \cdots + h_ng_n \) for some polynomials \( h_1, \ldots, h_n \in R \), such that \( lp(f) = \max_{1 \leq i \leq n}(lp(h_i)lp(g_i)) \).
Definition 2.5. A set $G$ of non-zero polynomials contained in an ideal $V$ of a ring $R$ is called a Gröbner basis for $V$ if and only if $G$ satisfies any one of the three equivalent conditions of Theorem 2.2 above. Obviously $G$ is a Gröbner basis for $\langle G \rangle$.

The Noetherian property of the ring $R$ and Theorem 2.2 above, yield the following Theorem ([1, Corollary 4.1.17]):

**Theorem 2.3.** Let $J \subseteq R[x, y]$ be a non-zero ideal. Then $J$ has a finite Gröbner Basis. □

Denote by $G_J$ a Gröbner basis for our ideal $J$ of the ring $R_{d_1, d_2}$ as above. We see that the order of $B[M]_{d_1, d_2}$ is the order of the quotient

$$(x - 1, y - 1)/ \langle G_J \rangle.$$

In the last step of the algorithm we will also need to compute the annihilator of some ideal $\langle G_J \rangle$ over the finite ring $R_{d_1, d_2}/N_d$, where $N_d$ is the polynomial in $R_{d_1, d_2}$ representing the norm element. For this we follow a method outlined in [1, Proposition 4.3.11] and we calculate the ideal quotient

$$T : \langle G_J \rangle = \{ f \in R_{d_1, d_2}/N_d : f \langle G_J \rangle \subseteq T \}$$

where $T = \langle (x^{d_1})^{d_1} - 1, (y^{d_2})^{d_2} - 1, N_d \rangle$. We therefore see that

$$\text{Ann}_{R_{d_1, d_2}/N_d}(\langle G_J \rangle) = T : \langle G_J \rangle.$$

We are now ready to describe the steps of the algorithm.
2.4 The Algorithm

2.4.1 Step 1

Fix distinct odd primes $p$ and $q$ and an odd prime $l$. The product $pq$ is the conductor of the field $\mathbb{Q}(\zeta_{pq})^+$ whose class number $h^+$ we want to calculate and $M = l$ is the prime that we check to see if it divides $h^+$. Factor $x^{m_1} - 1$ and $y^{m_2} - 1$ into irreducibles in $\mathbb{Z}/l\mathbb{Z}$ where, as above, $\gcd(m_i, l) = 1$ for $i = 1, 2$ and $m_1l^{a_1} = p - 1$ and $m_2l^{a_2} = q - 1$. As before, let $(f_1, f_2)$ be a pair of degrees of irreducible polynomials $\phi_x, \phi_y$ respectively, which appear in the factorization of $\mathbb{Z}[\tilde{G}]$. Let $d_1 = \gcd(p - 1, l^{f_1} - 1)$ and $d_2 = \gcd(q - 1, l^{f_2} - 1)$. For various primes $r$ with $r \equiv \pm 1 \pmod{pq}$ and $r \equiv 1 \pmod{2l}$ we calculate the frobenius elements $f_R$ as in (ii). Let $J_0$ denote the zero ideal of $R_{d_1, d_2}$ together with the conjugation relation $cnj$. We pick several frobenius polynomials $f_{R_i}$ that we calculated above and we let $J_i = J_{i-1} + (f_{R_i})$. This ascending chain of ideals will computationally stabilize at some ideal $J' \subseteq (x - 1, y - 1)$ in $R_{d_1, d_2}$. If $J'$ happens to equal the whole augmentation ideal $(x - 1, y - 1)$ of $R_{d_1, d_2}$, then the module $B[l]_{d_1, d_2}$ is trivial. If however, for some pair of degrees $(f_1, f_2)$ we have a strict inclusion $J' \subset (x - 1, y - 1)$ then the corresponding $B[l]_{d_1, d_2}$ is not trivial, if $J'$ has indeed stabilized at the correct ideal $J$. Hence we believe that $l$ divides the index $[E:H]$.

As expected, in most cases the ideal $J'$ is the whole augmentation ideal and so we do not continue to steps 2 and 3 for this prime $l$. When we do get a non-trivial quotient $(x - 1, y - 1)/J'$ for some $l$ however, we do not proceed to the next step right away but we follow first the procedure outlined right after the proof of
Proposition 1.1.3. That is, for each prime $l$ that appears in the factor $P_{(g,h)}$ for the
specific pair of $(g,h)$ with which we run step 1, but does not appear in the greatest
common divisor of all the $P_{(g,h)}$, we run step 1 again with a pair of primitive roots
$(g_0,h_0)$ for which $l$ does not divide $P_{(g_0,h_0)}$. If $l$ gives a non-trivial factor, then we
proceed to the next steps. We follow this procedure because it is computationally
much faster to run step 1 with the same pair of primitive roots $(g,h)$ for all primes,
instead of trying to determine which pair is best for each prime and then running
the test. Furthermore, most primes will give a trivial factor anyway and therefore
it is not worth trying to find the best pair $(g,h)$ for each one of them.

2.4.2 Step 2

In this step we repeat the procedure of step 1 but with higher powers of $l$, i.e.
for $M = l^2, l^3$, etc, and only for those primes which ‘passed’ step 1. The coefficients
of the frobenius polynomials $f_R$ now lie in $(Z/MZ)$ and we have to make sure that
the primes $r$ satisfy $r \equiv 1 \pmod{2M}$ for the specific power $M$ of $l$. As before, let
$R_{d_1,d_2} = (Z/MZ)[x,y]/((x^{d_1})^{d_1} - 1, (y^{d_2})^{d_2} - 1)$, and denote by $I_M$ its augmentation
ideal. As in Step 1, for each $M$ we have that the sequence of ideals

$$ J_0 \subset J_1 \subset \ldots \subset J_i \subset \ldots $$

will stabilize at some ideal $J^M$ and from the sequence of surjective maps

$$ \ldots \rightarrow I_{IM}/J^M \rightarrow I_M/J^M \rightarrow \ldots $$

we have that the orders of the modules $I_M/J^M$ are non-decreasing. Since $B[M]_{d_1,d_2}$
is finite and its order is bounded above by $|B_{d_1,d_2}|$ which is finite and indepen-
dent of $M$, the orders of the quotients $I_M/J^M$ will have to stabilize. We will have that for some power $M$ of $l$, $|I_M/J^M| = |I_M/J^M| \text{ hence } I_M/J^M \cong I_M/J^M$.

Therefore $M$ annihilates $I_M/J^M$ and therefore it also annihilates its quotient $\left(I_M/J^M\right)/\langle f(x,y) : \mathcal{R} \in S \rangle \cong B[lM]_{d_1,d_2}^\perp$. This implies that $M(B[lM]_{d_1,d_2}^\perp) = 0$ which gives $M(B[lM]_{d_1,d_2}) = 0$ since as finite abelian groups, $B[lM]_{d_1,d_2}^\perp$ and $B[lM]_{d_1,d_2}$ are isomorphic. Therefore $B[M]_{d_1,d_2} = B[M]_{d_1,d_2}$ and

$$|MB_{d_1,d_2}| = |B_{d_1,d_2}/B[M]_{d_1,d_2}| = |B_{d_1,d_2}|/|B[M]_{d_1,d_2}| = |MB_{d_1,d_2}|.$$  

Therefore $(MB_{d_1,d_2})/l(MB_{d_1,d_2}) = 0$ and by Nakayama’s Lemma, $MB_{d_1,d_2} = 0$.

Again, since $B_{d_1,d_2}$ and $B_{d_1,d_2}^\perp$ are isomorphic as finite abelian groups, we obtain $MB_{d_1,d_2}^\perp = 0$.

2.4.3 Step 3

In the third and last step we determine the structure and hence the order of the module $B_{d_1,d_2}^\perp$, by showing that the surjective map

$$g : (x - 1, y - 1)/((x^{m_1})^{d_1} - 1, (y^{m_2})^{d_2} - 1, J^M) \rightarrow B_{d_1,d_2}^\perp$$

is actually an isomorphism.

Let $M$ be as in step 2, i.e. the power of $l$ which annihilates $B_{d_1,d_2}^\perp$. Consider the exact sequence:

$$0 \rightarrow B[M] \xrightarrow{\psi} H/ \pm H^M \rightarrow H/ \pm E^M \rightarrow 0$$

Recall that the $(Z/MZ)[G]$-module $H/ \pm H^m$ is isomorphic to $(Z/MZ)[G]/N_G$. Furthermore, since $M$ annihilates $B_{d_1,d_2}^\perp \cong Hom_{R_{d_1,d_2}}(B_{d_1,d_2}, R_{d_1,d_2})$ that implies
that $M$ also annihilates $B_{d_1,d_2}$. Therefore, tensoring by $R_{d_1,d_2}$ we obtain the following exact sequence of $R_{d_1,d_2}$-modules

$$0 \longrightarrow B_{d_1,d_2} \xrightarrow{\psi} R_{d_1,d_2}/N_d \longrightarrow (H/ E^M)_{d_1,d_2} \longrightarrow 0.$$ 

With the ideals $I_M, J^M \subseteq R_{d_1,d_2}$ as above, we have the exact sequence

$$0 \to J^M \to I_M \to I_M/J^M \to 0$$

which yields the following exact sequence of $R_{d_1,d_2}$-duals

$$0 \to \text{Hom}_{R_{d_1,d_2}}(I_M/J^M, R_{d_1,d_2}) \to \text{Hom}_{R_{d_1,d_2}}(I_M, R_{d_1,d_2}) \to \text{Hom}_{R_{d_1,d_2}}(J^M, R_{d_1,d_2}) \to 0.$$ 

We need the following: For any ideal $J \subseteq R$, $R$ some finite Gorenstein ring, duality yields a surjection $R \cong \text{Hom}_R(R, R) \to \text{Hom}_R(J, R)$. Therefore every $R$-homomorphism from $J$ to $R$ is given by multiplication by some element of $R$ and so from the last exact sequence we have that

$$\text{Hom}_{R_{d_1,d_2}}(I_M, R_{d_1,d_2}) \cong R_{d_1,d_2}/\text{Ann}_{R_{d_1,d_2}}(I_M) = R_{d_1,d_2}/N_d.$$ 

Therefore, the kernel of the map

$$\text{Hom}_{R_{d_1,d_2}}(I_M, R_{d_1,d_2}) \to \text{Hom}_{R_{d_1,d_2}}(J^M, R_{d_1,d_2})$$

is $\text{Ann}_{(R_{d_1,d_2}/N_d)}(J^M)$ and we have that $(I_M/J^M)^\perp = \text{Hom}_{R_{d_1,d_2}}(I_M/J^M, R_{d_1,d_2}) \cong \text{Ann}_{(R_{d_1,d_2}/N_d)}(J^M)$. From the surjection $g : I_M/J^M \to B_{d_1,d_2}$ that we established from step 2 we have an injection

$$\Psi : B_{d_1,d_2} \hookrightarrow (I_M/J^M)^\perp \cong \text{Ann}_{(R_{d_1,d_2}/N_d)}(J^M).$$
Assume that \( \text{Ann}_{R_{d_1,d_2}/(N_d)}(J^M) \) annihilates \( (R_{d_1,d_2}/N_d)/\psi(B_{d_1,d_2}) \). Then
\[
\text{Ann}_{R_{d_1,d_2}/N_d}(J^M) \subseteq \psi(B_{d_1,d_2}).
\]

But now we have that
\[
|\text{Ann}_{R_{d_1,d_2}/N_d}(J^M)| \leq |\psi(B_{d_1,d_2})| = |B_{d_1,d_2}| = |\Psi(B_{d_1,d_2})| \leq |\text{Ann}_{(R_{d_1,d_2}/N_d)}(J^M)|.
\]

Therefore we have that the orders of \( I_M/J^M \) and \( B_{d_1,d_2}^+ \) are equal and hence \( g \) is an isomorphism. From the second exact sequence above we have that
\[
(R_{d_1,d_2}/N_d)/\psi(B_{d_1,d_2}) \cong (H/ \pm E^M)_{d_1,d_2}.
\]

Hence, if we show that \( \text{Ann}_{R_{d_1,d_2}/N_d}(J^M) \) annihilates \( (H/ \pm E^M)_{d_1,d_2} \), we will have proved that \( g \) is an isomorphism.

To find the annihilator \( \text{Ann}_{R_{d_1,d_2}/N_d}(J^M) \) we find a Gröbner basis \( G_{J^M} \) for the ideal \( J^M \) and then we calculate the ideal quotient as explained before step 1 above. That is, we calculate the ideal quotient
\[
T : \langle G_J \rangle = \{ f \in R_{d_1,d_2}/N_d : f \langle G_J \rangle \subseteq T \}
\]
where \( T = \langle (x^{a_1})^{d_1} - 1, (y^{a_2})^{d_2} - 1, N_d \rangle \). We therefore see that
\[
\text{Ann}_{R_{d_1,d_2}/N_d}(\langle G_J \rangle) = T : \langle G_J \rangle.
\]

Then, we apply each generator \( h(x,y) \) of the annihilator to the unit \( \eta_{d_1,d_2} \), where \( \eta_{d_1,d_2} \) is the unit \( \eta \) with the ‘norm’ element \( \frac{(x^{p-1})^{d_1}(y^{q-1})^{d_2}}{(x^{n_1}+d_1-1)(y^{n_2}+d_2-1)} \) applied to it. If \( \eta_{d_1,d_2}^h(x,y) \) is an \( M \)-th power of a unit in \( E \) then we are done. To see whether it is an \( M \)-th power we follow a method similar to the one in Gras and Gras [12] that we also
mentioned in the Introduction. We reformulate here the main proposition from [12]
in order to make it applicable to our case and we prove it again, only for the case
that \( l \) is odd since we only calculate the odd \( l \)-parts of \( h^+ \).

We denote by \( \eta^h_d \) the unit \( \eta^{h(x,y)}_{d_1,d_2} \) that we already described above and by \( G_d \)
the quotient of \( G \) containing the coset representatives of the embeddings in \( G \), which
map \( \zeta_p \) to \( \zeta_p^{a^i} \) and \( \zeta_q \) to \( \zeta_q^{h^j} \), for \( 1 \leq i \leq l^{a_1}d_1 \) and \( 1 \leq j \leq l^{a_2}d_2 \).

**Proposition 2.1.** Let \( M \) be a fixed power of an odd prime \( l \) as above and consider
the polynomial

\[
P(X) = \prod_{a \in G_d} (X - (a(\eta^h_d))^{1/M})
\]

where \( (a(\eta^h_d))^{1/M} \) denotes the real \( M \)-th root of \( a(\eta^h_d) \). If \( P \) has coefficients in \( Z \) then
\( \eta^h_d \) is an \( M \)-th power in \( Q(\zeta_{pq})^+ \).

**Proof:** Let \( N \) be the largest power of \( l \) for which the unit \( (\eta^h_d)^{1/N} \) lies in
\( Q(\zeta_{pq})^+ \). If \( M = N \) then we are done so we assume \( N < M \). Then \( (\eta^h_d)^{1/N} \) is not
an element of \( (Q(\zeta_{pq})^+)^l \) and therefore by [16, Chapter VIII, Theorem 16] we have
that the polynomial

\[
T(X) = X^{M/N} - (\eta^h_d)^{1/N}
\]
is irreducible in \( Q(\zeta_{pq})^+ \). Since \( M/N \geq 3 \), \( T(X) \) has at least one complex root.
Therefore \( (\eta^h_d)^{1/M} \) has at least one Galois conjugate that is not real. But \( P(X) \in Z[X] \) implies that the Galois conjugates are roots of \( P(X) \) which are real. Therefore
we have a contradiction. \( \Box \)
2.5 An Example

We finish Chapter 2 with an example. We choose the field of conductor \(7 \cdot 67 = 469\) for which we agree with Hakkarainen that 3 is the only odd prime < 10000 which divides \(h^+\). He only obtained however a \(3^1\) dividing \(h^+\), whereas our results show that that the 3-part of \(h^+\) has order \(3^2\).

Let \(l = 3\), \(p = 7\), \(q = 67\) and \(Q(\zeta_{pq})^+\) the real cyclotomic field of conductor \(pq = 469\). We first compute the factor \(P_{(g,h)}\) for all pairs of primitive roots \((g, h)\) and then their greatest common divisor. From the calculations we have that \(\text{GCD}(P_{(g,h)}) = 2^{32}\) and so we see that it is best to run the test with the pair \((g', h') = (3(mod 7), 7(mod 67))\) for which \(P_{(g', h')}\) has the smallest number of factors. In particular, \(P_{(g', h')} = 2^{98} \cdot 17^2\).

Next, we decompose the group ring \(Z[G]\) as we show in Section 2.2. We have that \(x^{p-1} - 1 = (x^3)^2 - 1\) and \(y^{q-1} - 1 = (y^3)^{22} - 1\) and so the polynomials that we factor into irreducibles in \(Z/3Z\) are \(x^2 - 1\) and \(y^{22} - 1\). We have the following factorization:

\[
x^2 - 1 = (x + 1)(x + 2)
\]
\[
y^{22} - 1 = (y + 1)(y + 2)(y^5 + 2y^3 + y^2 + 2y + 2)(y^5 + 2y^3 + 2y^2 + 2y + 1)(y^5 + 2y^4 + 2y^3 + 2y^2 + 2)(y^5 + y^4 + 2y^3 + y^2 + 2)
\]

and so we run step 1 for all possible degrees \(d_1\) and \(d_2\) which in this case are \(d_1 = 2\) and \(d_2 = 2\) and 22.

Step 1 gave the primes 2, 3 and 17 to be the only primes < 10000 that are possible divisors of the index. Since we chose not to calculate the 2-part of \(h^+\), the only primes we have to consider are therefore 3 and 17. Before proceeding to step 2 however, we run step 1 again for the prime 17 because it did appear as a factor of
but not of $\gcd(P_{(g, h)})$ and therefore it is possible that it might only divide $P_{(g', h')}$ and not $h^+ \mod 7$. The pair $(g_0, h_0) = (5 \mod 7, 7 \mod 67)$ does not have 17 as a factor of $P_{(g_0, h_0)}$ and step 1 for 17 with this pair of primitive roots only gives trivial Jordan-Hölder factors. Therefore we proceed to the next steps only for the prime 3.

In step 2 we repeat the same procedure as in step 1 but with higher powers of 3. For each $M = 3, 3^2, \ldots$ we determine the ideal $J^M$ at which all the ideals $J_i$ stabilize. We stop when for some $M$ we have that $|I_M/J^M| = |I_{3M}/J^{3M}|$. Below we show the Frobenius polynomials obtained for $M = 3, 3^2$ and $3^3$ for the pair of degrees $(d_1, d_2) = (2, 2)$, the ideals $J^M$ at which the ideals $J_i$ stabilize and the order of the quotients $|I_M/J^M|$. 

$$(d_1, d_2) = (2, 2)$$

$M = 3$

$r_1 = 7521823$

$$f_{R_1} = (y^5 + y^4 + 2y^3 + 2y^2 + 2y + 2)x^5 + (2y^5 + 2y^4 + 2y^3 + 2y^2 + y + 2)x^4 + (2y^5 + y^4 + y^2 + 1)x^3 + (2y^5 + 2y^4 + 2y^3 + 2y^2 + y + 2)x^2 + (y^5 + y^4 + y^3 + 2y + 1)x + (y^5 + y^4 + y^3 + 2y)$$

$r_2 = 8889427$

$$f_{R_2} = (2y^5 + 2y^4 + y^3 + 2y^2 + y + 2)x^5 + (2y^5 + 2y^3 + 2y^2 + 2y)x^4 + (2y^5 + 2y^4 + y^3 + 2y + 2)x^3 + (y^5 + 2y^3 + 2y^2 + 2y)x^2 + (2y^4 + y)x + (y^5 + 2y^4 + 2y^3 + 2y^2 + y)$$

$r_3 = 9573229$

$$f_{R_3} = (y^4 + 2y^3 + 2y + 1)x^5 + (y^4 + y^3 + y^2)x^4 + (y^5 + 2y^2 + y + 2)x^3 + (2y^4 + 2y^3)x^2 + (2y^5 + 2y^4 + y^3 + y + 2)x + (y^5 + y^3 + 1)$$

49
\( r_4 = 10257031 \)

\[ f_{\mathbb{R}_4} = (y^5 + y + 2)x^5 + (2y^5 + 2y^4 + 2y^3 + 2y^2)x^4 + (2y^4 + 2y^3 + y^2 + 2y)x^3 + (y^5 + y^2 + y + 1)x^2 + (2y^5 + 2y^4 + y^2 + 2y + 2)x + (2y^5 + y^4 + 2y^3 + y^2 + y) \]

\( r_5 = 20514061 \)

\[ f_{\mathbb{R}_5} = (2y^5 + y^3 + y^2 + 2y + 1)x^5 + (2y^4 + y^3 + y^2 + 2y + 2)x^4 + (2y^5 + y^4 + 2y^3 + y + 2)x^3 + (y^2 + y)x^2 + (2y^5 + y^2 + 2y + 1)x + (y^5 + 2y^3 + y^2 + y) \]

\( r_6 = 22565467 \)

\[ f_{\mathbb{R}_6} = (2y^4 + y^3 + y^2 + 2)x^5 + (2y^5 + 2y^3 + y + 1)x^4 + (y^5 + y^4 + y^3 + y^2 + 2y + 1)x^3 + (2y^4 + 2y^3 + y^2 + y + 2)x^2 + (y^5 + 2y^4 + 2y^3 + y^2 + 2)x + (2y^5 + 2y^4 + y^3 + y^2 + 1) \]

\[ J^M = (y^2 - 1, y - x) \equiv ((y + 1)(y - 1), (y - 1) - (x - 1)) \text{ in } \mathbb{Z}/3\mathbb{Z}. \]

From the second polynomial in \( J^M \) we see that the two generators of the augmentation ideal \( I_M \) become equivalent in \( I_M/J^M \). From the first one we have that \( y(y - 1) \equiv -(y - 1) \) in \( J^M \) therefore we can only have constants in front of the only generator of \( I_M/J^M \). Since we are in \( \mathbb{Z}/3\mathbb{Z} \) we have that \( |I_M/J^M| = 3 \).

\[ M = 3^2 \]

\( r_1 = 7521823 \)

\[ f_{\mathbb{R}_1} = (4y^5 + 7y^4 + 5y^3 + 8y^2 + 5y + 2)x^5 + (5y^5 + 8y^4 + 5y^3 + 2y^2 + 4y + 8)x^4 + (8y^5 + 4y^4 + 6y^3 + 7y^2 + 6y + 4)x^3 + (2y^5 + 8y^4 + 2y^3 + 2y^2 + y + 8)x^2 + (y^5 + 7y^4 + y^3 + 3y^2 + 8y + 7)x + (y^5 + 4y^4 + 7y^3 + 3y^2 + 2y + 6) \]

\( r_2 = 8889427 \)

\[ f_{\mathbb{R}_2} = (2y^5 + 2y^4 + y^3 + 2y^2 + 4y + 5)x^5 + (2y^5 + 3y^4 + 8y^3 + 2y^2 + 5y + 3)x^4 + (2y^5 + 4y^4 + 6y^3 + 8y^2 + 7y + 6)x^3 + (2y^5 + 2y^4 + y^3 + 2y^2 + 7y + 2)x^2 + (y^5 + 7y^4 + y^3 + 3y^2 + 4y + 4)x + (y^5 + 4y^4 + 7y^3 + 3y^2 + 2y + 6) \]
\[8y^4 + y^3 + 5y + 5)x^3 + (7y^5 + 6y^4 + 5y^3 + 2y^2 + 2y + 6)x^2 + (6y^5 + 2y^4 + 3y^2 + y)x + \\
(y^5 + 2y^4 + 5y^3 + 2y^2 + y + 6)
\]

\[r_3 = 9573229\]

\[f_{R_3} = (4y^4 + 8y^3 + 5y + 1)x^5 + (3y^5 + 7y^4 + 7y^3 + 7y^2 + 6y)x^4 + (y^5 + 6y^3 + 5y^2 + y + 2)x^3 + \\
(6y^5 + 5y^4 + 3y^2 + 3y + 3)x^2 + (5y^5 + 5y^4 + y^3 + 7y + 8)x + (4y^5 + 3y^4 + 7y^3 + 3y^2 + 6y + 7)
\]

\[r_4 = 10257031\]

\[f_{R_4} = (y^5 + 3y^4 + y + 2)x^5 + (2y^5 + 5y^4 + 2y^3 + 8y^2)x^4 + (6y^5 + 2y^4 + 5y^3 + y^2 + 5y)x^3 + \\
(4y^5 + 7y^2 + y + 4)x^2 + (8y^5 + 5y^4 + 6y^3 + y^2 + 2y + 8)x + (8y^5 + 7y^4 + 8y^3 + 4y^2 + 4y + 6)
\]

\[r_5 = 20514061\]

\[f_{R_5} = (5y^5 + 3y^4 + 7y^3 + 7y^2 + 2y + 4)x^5 + (5y^4 + 7y^3 + 4y^2 + 2y + 2)x^4 + (5y^5 + \\
4y^4 + 8y^3 + 3y^2 + y + 2)x^3 + (3y^5 + 6y^4 + 3y^3 + y^2 + y + 3)x^2 + (8y^5 + 6y^4 + 3y^3 + \\
7y^2 + 8y + 7)x + (4y^5 + 3y^4 + 8y^3 + 7y^2 + 7y + 6)
\]

\[r_6 = 22565467\]

\[f_{R_6} = (3y^5 + 5y^4 + y^3 + y^2 + 3y + 2)x^5 + (5y^5 + 6y^4 + 8y^3 + 7y + 7)x^4 + (y^5 + 7y^4 + \\
7y^3 + 4y^2 + 8y + 1)x^3 + (3y^5 + 5y^4 + 2y^3 + 7y^2 + 7y + 8)x^2 + (7y^5 + 2y^4 + 8y^3 + 7y^2 + \\
5)x + (2y^5 + 5y^4 + y^3 + y^2 + 7)
\]

\[J^M = (y^2 - 3y + 2, 3 - x - 2y) = ((y - 1)(y - 2), -2(y - 1) - (x - 1)) \text{ in } Z/9Z.
\]

The same reasoning as above for the ideal \(J^3\) applies here as well and we have that \(|I_M/J^M| = 3^2\). Since \(|I_3/J^3|\) is strictly smaller than \(|I_{3^2}/J^{3^2}|\) we need to continue as above with \(M = 3^3\).

\[M = 3^3\]
\[ r_1 = 7521823 \]
\[ f_{r_1} = (13y^5 + 7y^4 + 14y^3 + 26y^2 + 14y + 20)x^5 + (5y^5 + 17y^4 + 5y^3 + 11y^2 + 13y + 26)x^4 + (17y^5 + 4y^4 + 24y^3 + 16y^2 + 6y + 4)x^3 + (20y^5 + 8y^4 + 11y^3 + 11y^2 + y + 26)x^2 + (y^5 + 25y^4 + 19y^3 + 21y^2 + 26y + 7)x + (10y^5 + 22y^4 + 25y^3 + 3y^2 + 2y + 6) \]
\[ r_2 = 8889427 \]
\[ f_{r_2} = (20y^5 + 2y^4 + y^3 + 11y^2 + 22y + 23)x^5 + (2y^5 + 12y^4 + 26y^3 + 11y^2 + 14y + 21)x^4 + (2y^5 + 26y^4 + y^3 + 18y^2 + 14y + 23)x^3 + (16y^5 + 15y^4 + 14y^3 + 20y^2 + 11y + 15)x^2 + (6y^5 + 11y^4 + 21y^2 + 19y)x + (10y^5 + 11y^4 + 23y^3 + 11y^2 + 10y + 24) \]
\[ r_3 = 9573229 \]
\[ f_{r_3} = (9y^5 + 4y^4 + 17y^3 + 18y^2 + 5y + 19)x^5 + (12y^5 + 16y^4 + 7y^3 + 7y^2 + 15y)x^4 + (10y^5 + 24y^3 + 14y^2 + 10y + 20)x^3 + (24y^5 + 5y^4 + 5y^3 + 3y^2 + 12y + 12)x^2 + (5y^5 + 5y^4 + 19y^3 + 9y^2 + 7y + 26)x + (13y^5 + 21y^4 + 25y^3 + 12y^2 + 6y + 16) \]
\[ r_4 = 10257031 \]
\[ f_{r_4} = (10y^5 + 3y^4 + 18y^3 + 19y + 2)x^5 + (20y^5 + 14y^4 + 2y^3 + 17y^2 + 9y + 9)x^4 + (24y^5 + 2y^4 + 23y^3 + 10y^2 + 14y + 9)x^3 + (22y^5 + 9y^4 + 9y^3 + 7y^2 + 10y + 22)x^2 + (26y^5 + 5y^4 + 15y^3 + y^2 + 2y + 26)x + (17y^5 + 16y^4 + 26y^3 + 4y^2 + 22y + 15) \]
\[ r_5 = 20514061 \]
\[ f_{r_5} = (14y^5 + 3y^4 + 25y^3 + 16y^2 + 11y + 22)x^5 + (18y^5 + 23y^4 + 16y^3 + 22y^2 + 2y + 20)x^4 + (23y^5 + 22y^4 + 17y^3 + 21y^2 + 10y + 20)x^3 + (21y^5 + 6y^4 + 12y^3 + 19y^2 + y + 3)x^2 + (17y^5 + 15y^4 + 21y^3 + 7y^2 + 26y + 16)x + (13y^5 + 3y^4 + 26y^3 + 25y^2 + 7y + 24) \]
\[ r_6 = 22565467 \]
\[ f_{r_6} = (12y^5 + 23y^4 + 19y^3 + 10y^2 + 12y + 11)x^5 + (14y^5 + 24y^4 + 8y^3 + 25y + 7)x^4 + (10y^5 + 16y^4 + 7y^3 + 4y^2 + 8y + 1)x^3 + (21y^5 + 5y^4 + 20y^3 + 16y^2 + 16y + 8)x^2 + \]
\[(25y^5 + 2y^4 + 8y^3 + 16y^2 + 5)x + (20y^5 + 14y^4 + y^3 + y^2 + 16)\]

\[J^M = (9(y - 1), 2 - 3y + y^2, 3 - x - 2y) \text{ in } \mathbb{Z}/27\mathbb{Z}.\]

We see here that \(J^{3^3}\) is generated by the same polynomials as \(J^{3^2}\) but it has the extra polynomial \(9(y - 1)\) which reduces the number of constants to 9 instead of 27. Therefore \(|I_{3^2}/J^{3^2}| = |I_{3^3}/J^{3^3}| = 9\) and so, as expected, the orders of these quotients stabilize with \(M = 3^2\).

For the pair of degrees \((d_1, d_2) = (2,2)\) the frobenius polynomials give exactly the same ideals \(I^M\) as above and therefore we only need to consider the case for \((d_1, d_2) = (2,2)\). We now proceed to step 3 of the algorithm where we prove that \(I_M/J^M\) is isomorphic to \(B_{d_1,d_2}^+\). To do this, we first compute a set of generators for the ideal \(Ann_{R_{d_1,d_2}/N_d}(\langle G_{J^M} \rangle)\) where \(M = 3^2\) is the power of 3 that kills \(B_{d_1,d_2}^+\) and \(G_{J^M}\) is a Gröbner basis for the ideal \(J^M\). We found the following three polynomials to be the generators of \(Ann_{R_{d_1,d_2}/N_d}(\langle G_{J^M} \rangle)\):

\[h_1(x, y) = (3y^5 + 3y^4 + 3y^3 + 3y^2 + 3y + 3)x^4 + (-3y^5 - 3y^4 - 3y^3 - 3y^2 - 3y - 3)x^3 + (3y^5 + 3y^4 + 3y^3 + 3y^2 + 3y + 3)x + (-3y^5 - 3y^4 - 3y^3 - 3y^2 - 3y - 3),\]

\[h_2(x, y) = (3y^3 + 3y^2 - 3y - 3)x^5 + (3y^4 + 3y^3 - 3y^2 - 3y)x^4 + (3y^5 + 3y^4 - 3y^3 - 3y^2)x^3 + (3y^5 - 3y^4 - 3y^3 + 3)x^2 + (-3y^5 - 3y^4 + 3y + 3)x + (-3y^5 + 3y^2 + 3y - 3),\]

\[h_3(x, y) = (y^4 + 4y^2 - 2)x^5 + (y^5 - 3y^4 + 4y^3 - 3y^2 - 2y - 3)x^4 + (3y^5 + 4y^4 + 3y^3 - 2y^2 + 3y + 1)x^3 + (4y^5 - 2y^3 + y)x^2 + (-3y^5 - 2y^4 - 3y^3 + y^2 - 3y + 4)x + (-2y^5 + 3y^4 + y^3 + 3y^2 + 4y + 3).\]

For each \(h_i\) we form the polynomial \(P_i(X)\) of Proposition 2.1. If the coefficients of each \(P_i\) lie in \(\mathbb{Z}\), then the unit \(n_{d_1,d_2}^h\) and all its conjugates are 9-th powers in
$Q(\zeta_{pq})^+$ and we are done. The $P_i$ were calculated with a precision of 2000. They are big polynomials with very large integer coefficients and therefore we do not present them here. The reader can find them in the Appendix. Since all the $P_i$ have integer coefficients this implies that $3^2$ is the order of the 3-part of $h^+$. 
Chapter 3

Tables and Discussion of the Results

We present all our results in the Main Table below. For each field of conductor \( pq \) we present the greatest common divisor of the \( P_{(g,h)} \) for all pairs of primitive roots \((g, h)\), in the column \( GCD \). Since we do not calculate the 2-part of \( h^+ \), we leave out the powers of 2 from the \( GCD \). Therefore, if a ‘1’ appears in the column \( GCD \) for some field, this means that no odd primes divide the greatest common divisor of the various \( P_{(g,h)} \). However, there are always powers of 2 in the \( GCD \), as we see from our calculations of the index \([E : H]\) in chapter 1. In the column \textit{extra ‘nontrivial’ primes} we present all the primes that step 1 gave to be possible divisors of \( h^+ \), besides the ones that already appear in the column \( GCD \). The symbol \( \tilde{h}^+ \) in the fourth column, denotes the odd part of \( h^+ \) for all primes \( l < 10000 \).

We have verified the results of Hakkarainen for the fields of conductor \( pq \), for the primes \( l \) that do not divide the degree of the extension. We mark with an asterisk the fields whose class number we found to be divisible by a prime \( l \) which also divides the degree of the extension. From those fields, there are three cases where the primes that appear as possible divisors of \( h^+ \) in Hakkarainen’s results, i.e. divisors of a relative class number \( h_\chi \), in our case they were only divisors of the \( GCD \) and therefore not of \( h^+ \). In other words, although these primes do divide the index \([E : H]\), we found that they come from \( GCD \) and not from \( h^+ \). These are
the fields of conductor $11 \cdot 43$ where we found that $3$ does not divide $h^+$, the field of conductor $7 \cdot 211$ where we found that $7$ does not divide $h^+$ and the field of conductor $17 \cdot 103$ where we found that $17$ does not divide $h^+$. For the field of conductor $7 \cdot 67$ we found that the $3$-part of $h^+$ is $3^2$. Finally, for the fields of conductor $13 \cdot 61$ and $13 \cdot 103$ we found that $3$ and $3^2$ respectively are also divisors of $h^+$.

The polynomials of the third step, which are used to prove that the unit $\alpha(\eta_d^h)$ is an $M$-th power in $E$ by showing that their coefficients are in $Z$, were computed with very high precision. That is why we get hundreds of decimals which are all 9’s or all 0’s. We did not continue to prove rigorously that the coefficients are indeed integers. However, to a very small number of fields with small polynomials we did apply the method outlined in Schoof [25], which proves that the coefficients of these polynomials are integers. This method requires that we round off the coefficients of $P(X)$ and then show that this new polynomial divides $P(X^M)$. This proved to be too time consuming for large polynomials and this is why we did not apply it to most of our fields.
Table 3.1: Main Table

<table>
<thead>
<tr>
<th>$f = p \cdot q$</th>
<th>GCD</th>
<th>extra 'non trivial' primes</th>
<th>$\tilde{h}^+$</th>
</tr>
</thead>
<tbody>
<tr>
<td>321 = 3 · 107</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>427 = 7 · 61</td>
<td>1</td>
<td>5</td>
<td>5 *</td>
</tr>
<tr>
<td>469 = 7 · 67</td>
<td>1</td>
<td>3</td>
<td>3² *</td>
</tr>
<tr>
<td>473 = 11 · 43</td>
<td>3⁴ · 5² · 7⁴</td>
<td>-</td>
<td>1 *</td>
</tr>
<tr>
<td>481 = 13 · 37</td>
<td>7 · 19</td>
<td>-</td>
<td>19</td>
</tr>
<tr>
<td>551 = 19 · 29</td>
<td>5</td>
<td>-</td>
<td>5</td>
</tr>
<tr>
<td>629 = 17 · 37</td>
<td>3⁴ · 19</td>
<td>5</td>
<td>5 · 19</td>
</tr>
<tr>
<td>697 = 17 · 41</td>
<td>3³ · 7</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>703 = 19 · 37</td>
<td>3¹⁶ · 5</td>
<td>13,37</td>
<td>13 · 37 *</td>
</tr>
<tr>
<td>753 = 3 · 251</td>
<td>1</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>763 = 7 · 109</td>
<td>3⁴</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>779 = 19 · 41</td>
<td>5²</td>
<td>41</td>
<td>41</td>
</tr>
<tr>
<td>785 = 5 · 157</td>
<td>3² · 79</td>
<td>-</td>
<td>3 *</td>
</tr>
<tr>
<td>793 = 13 · 61</td>
<td>3²⁰ · 5 · 7</td>
<td>37</td>
<td>3 · 37 *</td>
</tr>
<tr>
<td>817 = 19 · 43</td>
<td>1</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>869 = 11 · 79</td>
<td>1</td>
<td>79</td>
<td>79</td>
</tr>
<tr>
<td>889 = 7 · 127</td>
<td>3⁴ · 7²</td>
<td>-</td>
<td>7 *</td>
</tr>
<tr>
<td>923 = 13 · 71</td>
<td>3³</td>
<td>61</td>
<td>61</td>
</tr>
<tr>
<td>985 = 5 · 197</td>
<td>3³ · 11</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>1101 = 3 · 367</td>
<td>1</td>
<td>3</td>
<td>3 *</td>
</tr>
<tr>
<td>1139 = 17 · 67</td>
<td>3⁷ · 11⁷</td>
<td>89</td>
<td>89</td>
</tr>
<tr>
<td>1141 = 7 · 163</td>
<td>1</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>1159 = 19 · 61</td>
<td>3³ · 7</td>
<td>73</td>
<td>73</td>
</tr>
<tr>
<td>1207 = 17 · 71</td>
<td>3²</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>1211 = 7 · 173</td>
<td>1</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>1241 = 17 · 73</td>
<td>3⁴ · 7 · 37 · 109</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>1243 = 11 · 113</td>
<td>5 · 37</td>
<td>41</td>
<td>41</td>
</tr>
<tr>
<td>1257 = 3 · 419</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>1261 = 13 · 97</td>
<td>7³</td>
<td>5,97</td>
<td>5 · 7² · 97</td>
</tr>
<tr>
<td>1271 = 31 · 41</td>
<td>3³ · 5⁶</td>
<td>7,11,31</td>
<td>7 · 11 · 31</td>
</tr>
<tr>
<td>1313 = 13 · 101</td>
<td>3 · 5²</td>
<td>31</td>
<td>31</td>
</tr>
<tr>
<td>1339 = 13 · 103</td>
<td>3⁷ · 17⁵</td>
<td>13</td>
<td>3² · 13 *</td>
</tr>
<tr>
<td>1343 = 17 · 79</td>
<td>5</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>1355 = 5 · 271</td>
<td>3³ · 5</td>
<td>37</td>
<td>37</td>
</tr>
<tr>
<td>1385 = 5 · 277</td>
<td>3² · 139</td>
<td>5,7</td>
<td>5 · 7</td>
</tr>
<tr>
<td>1387 = 19 · 73</td>
<td>3⁴ · 7 · 101</td>
<td>17,19,37</td>
<td>17² · 19 · 37</td>
</tr>
<tr>
<td>1393 = 7 · 199</td>
<td>1</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
Table 3.2: Main Table Continued

<table>
<thead>
<tr>
<th>( f = p \cdot q )</th>
<th>GCD</th>
<th>extra ‘non trivial’ primes</th>
<th>( \tilde{h}^+ )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1465 = 5·293</td>
<td>( 3^2 \cdot 7^2 )</td>
<td>-</td>
<td>( 3^2 )</td>
</tr>
<tr>
<td>1477 = 7·211</td>
<td>( 3^2 \cdot 5^2 \cdot 7^2 )</td>
<td>11</td>
<td>11 *</td>
</tr>
<tr>
<td>1509 = 3·503</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>1513 = 17·89</td>
<td>( 11^3 \cdot 17 \cdot 41 )</td>
<td>13</td>
<td>13 · 17</td>
</tr>
<tr>
<td>1591 = 37·43</td>
<td>( 3^{26} \cdot 7^8 \cdot 11 \cdot 19 \cdot 487 )</td>
<td>43</td>
<td>43</td>
</tr>
<tr>
<td>1623 = 3·541</td>
<td>1</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>1641 = 3·547</td>
<td>1</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>1651 = 13·127</td>
<td>( 3^3 \cdot 7 )</td>
<td>5</td>
<td>( 5^2 )</td>
</tr>
<tr>
<td>1687 = 7·241</td>
<td>1</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>1735 = 5·347</td>
<td>( 3 \cdot 29 )</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>1739 = 37·47</td>
<td>( 23^5 )</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>1751 = 17·103</td>
<td>( 3^7 \cdot 17^7 )</td>
<td>-</td>
<td>1 *</td>
</tr>
<tr>
<td>1761 = 3·587</td>
<td>1</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>1765 = 5·353</td>
<td>( 3^2 \cdot 59 )</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>1865 = 5·373</td>
<td>( 3^2 \cdot 11 \cdot 17 )</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>1903 = 11·173</td>
<td>( 3^3 )</td>
<td>173</td>
<td>173</td>
</tr>
<tr>
<td>1921 = 17·113</td>
<td>( 3^3 \cdot 19 )</td>
<td>17, 29</td>
<td>17^3 · 29</td>
</tr>
<tr>
<td>1937 = 13·149</td>
<td>( 3^2 \cdot 5^2 \cdot 7 )</td>
<td>109</td>
<td>3 · 109 *</td>
</tr>
</tbody>
</table>
Chapter 4

Conclusion and Future Projects

In this thesis we studied the class number $h^+$ of real cyclotomic fields. In particular, we studied a pre-existing method introduced by Schoof [25] who calculated the $l$-part of $h^+$ for cyclotomic fields of prime conductor, and we extended this method to fields of conductor $pq$, $p$ and $q$ being distinct odd primes. We calculated the odd part of $h^+$ for all odd primes less than 10000, for cyclotomic fields of conductor $< 2500$. Our results verify the results of Hakkarainen [13] who studied the divisibility of $h^+$ by odd primes less than 10000, for fields of conductor $< 2000$. Our results also complete his results in the sense that they give the full order of the $l$-parts of $h^+$ for each odd prime $l < 10000$, including the primes dividing the degree of the field.

One can apply the second and third step of our algorithm to the prime $l = 2$ and therefore calculate the 2-part of $h^+$ which we did not complete here, as well as to primes $l > 10000$. For fields of conductor $> 2000$ the computations become very time consuming. Therefore, if one is to calculate the $l$-parts of $h^+$ for these fields, one could set an upper bound to the degrees $d_1$ and $d_2$. Schoof in [25] for example calculated the Jordan-Hölder factors of order up to 80000. Furthermore, one could apply our method to fields of conductor equal to the product of more than two distinct odd primes, by adjusting accordingly the unit $\eta$ and the description.
of the galois group $G$ in terms of polynomials. Of course we see that a larger number of primes dividing the conductor implies a more complicated unit and more variables. Therefore the calculations are expected to become very time consuming as the conductor of the field grows.

One of the reasons that the primes that divide the degree of the field are avoided in many methods for computing $h^+$, lies in the difficulty of computing the factor $Q_K^+$ that we discussed in Subsection 1.3.1. Our method could help in calculating this value, by applying the method to Leopoldt’s cyclotomic unit $\theta_{\xi}$ introduced in 1.3.1 for the cyclic subfield $K_{\xi}$. We could do that for every $\xi \neq \xi_0$ and only for the primes that divide the order of the galois group since only those primes appear in the index $Q_K^+$. We then divide this product with the product we find by applying the method to our unit. The result is the order of $Q_K^+$. 

60
Appendix

We present here the three polynomials $P_i$, $i = 1, 3$, which have integers coefficients and therefore prove that the units $\eta_{d_1,d_2}^{h_i}$ are 9-th powers in the field $\mathbb{Q}(\zeta_{767})^+$. of the Example of Chapter 2. The dots at the end of each coefficient indicate that the series of 9’s or 0’s continues.

\[ P_1(X) = X^{36}105396109733505357905518767013258435444498076254086208 \]
\[ 5152313848962040818.000000000000...X^{35} + 277084986739178192915303912 \]
\[ 34248702065025191051592254936473209198420081622550270940081688219392609 \]
\[ 430187363494728581933647064480483830327707912.9999999999...X^{34} \]
\[ - 443031186847279900384751307950190509972876666445436603091201672639832 \]
\[ 85075868157787450452387751968781874685546698840102907552923787558038230 \]
\[ 83385780057005333305665023900325370803108073.99999999999999...X^{33} \]
\[ + 176693073558912542732314370363352895988163695677882538905399886 \]
\[ 57436133010107895044183931480500100115421929519954979982437810725066046744 \]
\[ 37039663575798308569264970705378623230640739564231682972877422194236655437 \]
\[ 483589726936335471.999999999999999...X^{32} - 118245613631805832148856824695260705266257885134607987346024885714514899678 \]
\[ 17675053704988309050352783702559047105990284495481852320940568425188901583 \]
\[ 143631865259692984806143850020719908182943746992950665042932648199568549 \]
\[ 73160620657672848192401695378504403998166587.99999999999999999999999...X^{31} + 197829349674215740348417170288169109794370841890033837498196532028671961 \]
\[ 99600576942773054054072739537036904335059615601329098547620694988108047664556 \]
\[ 519943952901000535380388959861380139050576732832000371982346767882843002779 \]
\[ 49514492255352431807791440736220394110670888459628153848606026 \]
\[ 06562850804.999999999999999...X^{30} - 1100986919646893844232649494405032977437875765748639554461221098524695411956 \]
\[ 945547983250812592552716939413721311579115829136617621706592899300603 \]
\[ 394932652067373188467046989489053350538233156967921367414564772117902700 \]
\[ 380501377224414299579288602086606262016391622852789395239936636190579552 \]
\[ 691900938770654126165925057939.99999999989999999999999999999999...X^{29} \]
\[ + 244560892005091938314894248280893855403972235607285413521237761758644343 \]
\[ 5295118703188147173097421848605126862203702241133917569954730003015498 \]
\[
\begin{align*}
&1287616610431308985470372688638207459335735196101110260851088578222913421390511 \\
&5716045200346488215196073238994104481022436375499337274439190911 \\
&799902022.99999999999999999\ldots X^{14} + \\
&111361033003209327380245905294315608964067732110701820407690346727237417437822650 \\
&55813760959167337580337976110166626883281860124474959960373527492480232845667477767 \\
&83206731640148037198584378595470367989308622414979732634347939785113395674242048450 \\
&49015932482804260736998363599618526243280575115352181966288564208305682860313898540865 \\
&96494042229799380732985392733580579923549676325499047193767246447763112600843106 \\
&79821888406997427385751069157366824092226290873748090.00000000000000000\ldots X^{13} + \\
&+ 646560140218659873990705733490613975947171031564595272668076909502832242504604344399 \\
&958391813652801873213828085747412350109489511039299330855127348077579635640461755302728 \\
&683139421288728996403470278676791517643917484358837428132536173368675856897314816 \\
&6093640814739496161016556050584778916246408771637012492891259012718207209390103408941 \\
&7868964615750207889192679249997005683165685825534055528644373995057763421377144 \\
&55732046585069810815480247868070979.99999999999999\ldots X^{12} - \\
&- 5818065356870885651866318880487971181745750748428154704869932789216597 \\
&459246891276319056040177246263030057613859389834376371420574333526694489223236588312141 \\
&410724330966731819069803338466665525816536697488562091518051898811114052757589925536 \\
&5773017849800943353634790552697057048206343586793886400414030353735810276255334850 \\
&6864258375361041588042368744341556057051043959531641385753113156297372991106924214 \\
&14682103986242827566917.99999999999999999\ldots X^{11} + \\
&+ 1311109256197053889176078347913190242813344486481251677329750400160527230382526955234 \\
&383047723749074899208998149924000374370565196751108996230138058020693550295794727590 \\
&8209866465283358215002239249197170314444376785285840218130285982077570415059511548370 \\
&152453967247875490212044122538577715100766366785248752239808120798065307234974866238 \\
&7779531748923750913392181747378526651118473964838023986850 \\
&6422448767.99999999999999999\ldots X^{10} - \\
&- 90947406789568337881028512072840662265070987218218879659163832243626721821040843599 \\
&128493089924580288390529331500411005140487681461221775940751450313013077029791862847 \\
&775699522287497738570411292096915372366118056442602527021121882695463695546475488 \\
&4228515684784752617935829078927541038186334396853246242122169825193362075184686033087 \\
&816644207616746274347598028675702456027.99999999999999999\ldots X^{9} + \\
&+ 1767392117557979985636310467832269737532628973941814901246963700004478723582081951916 \\
&8806701272910401157538323468266335285495720562891261851494333222364195504377685384840 \\
&65
\]
\[ P_2(X) = X^{36} + -10539610973350350739055186701325843544498076254086208515231384 \\
8962040818.00000000000...X^{35} + \\
2777084986791781929153093123424870200502519159252549364732091984200816 \\
225502709400618882193926094301873763494728591933647064840830027 \\
707912.99999999999...X^{34} \\
- -4430311868472799003847513079501905099728766646453660309120167266398 \\
3285057681577874504523877519687818174685946988401029075529237875580382 \\
30833857805700533310506350239093529370803108073.99999999999...X^{33} + \\
66
$F_3(X) = X^{36} - 24064643863891701293942210716949932222983552048522$

126188838013231936.000000000000000...$X^{35} +$

15957262841147292045627292100094621939939533111160514428727076644555

94679063456985940349146320609933512405252581679324589220002895

6892.000000000000000000...$X^{34} -$

17802851874396308125950838319354208358098816421640693276771203723261722

1579148674766745147526363847556208239471334444465948533751431779566343

1292989295146336204796399579001774525717118485616080.0000...$X^{33} +$

547293485872283870631192200195812179924097941153137317316245357053996143

980851281478916568214307265765012554080222169773949797242264731018705727

335724606001149395795588891250161872775248173878751912081276142518967546

5048367295308906643540568843302959496316788546.00000000000000000000...$X^{32} -$

27429260212073484922908524276732610776309185128535163584204511339613825006

598570515908234911406752013529118303817099886297401425559639131185031359

178045327664592518655703219977826166126715330420496811354198246345887888121

3962674741465871543713633881867438912899942283398726030182225837194

54513453819092879046.00000000000000000000...$X^{31} +$

34367488800254466187192214802289087477391233423489334769478658719362859793
\[01652642749922669333297044183339965015096448464067477467160477801777799807209.000000000000000000000000...X^4 - \\
303938261488705611777211589894600794475486588216070620854915411559057677 \times 0 \]
\[058829854807683896143792723308786012747817013045755535315127173359875017116368602817154332519429087031300595104795308839696340787777032430303002327123228151024616.000000000000000000000000...X^3 + \\
2015981132559587594135125685403431560511283940800605998939443219832982005667630742881765303775495382816182643990532786361737343191705339282527390260450008802732629807452562042502502.000000000000000000000000...X^2 - \\
89793570702950544044491770018423201654711117118847664696249393305809252599781219837593748.000000000000000000000000...X + 1.00000000000000000000000000000000...\]
Bibliography


