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

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 $C^+ \longrightarrow C$ 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 ≤ 100 and Van der Linden in [29] was able to calculate the class number of a large collection of real abelian fields of conductor ≤ 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=Units/(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 $I/\{f_{\Re}(\eta)\}_{\{\Re\}}$, where I is the augmentation ideal of the group ring $R = (Z/MZ)[G]$, G is the galois group of the extension $Q(\zeta_p)^+/Q$ and the maps $f_{\Re} \in Hom_R(E/\{\pm 1\}, R)$ correspond to the frobenius elements of unramified prime ideals $\Re$ which split completely in the extension $Q(\zeta_p)^+(\zeta_{2M})$. These maps are evaluated on η, 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_ξ of K. More specifically, we have that $h^+ = Q\prod_\chi h_\chi$, where the product runs over all non-trivial characters χ irreducible over the rationals, each 'class number' h_χ is the index of the cyclotomic units of K_χ in its full group of units E_χ 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_χ of K, there is a unit ε in the full group of units E_χ of K_χ which is of the form $\varepsilon = \eta^m$, where η is a cyclotomic unit, and ε has the property that m equals the order of the 'class number' of the specific cyclic subfield K_χ. 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 ω in the group ring $Z' = Z[G]/(1+\sigma+\sigma^2) \cong Z[\zeta_3]$ with the property that $[E{:}F] = N_{Q(\sqrt{-3})/Q}(\omega)$.

This element ω 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 χ-components, where χ is a l-adic character of the subgroup D of the galois group G with $(|D|,l)$=1 and then proved that $L_{\chi}^{dual} \cong (Z[G]_{\chi}/M)/J_{\chi}$, where J_{χ} is an ideal generated by homomorphisms representing maps from the group of l - units into $Z_{\chi}[G]/M$, 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 $Q(\zeta_p)^+$ 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 $Q(\zeta_p)^+$ that Schoof focused on, we have that $h^+ = [E{:}H]$, where E is the group of units of $Q(\zeta_p)^+$ and H is its subgroup of cyclotomic units. The quotient $B = E/H$ is a finite $Z[G]$-module, where $G = Gal(Q(\zeta_p)^+/Q)$ 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

$$Hom_R(A, R) = A^{\perp} \cong A^{dual} = Hom_Z(A, Q/Z)$$

and therefore $|A| = |A^{dual}| = |A^{\perp}|$. 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 $B[M]^{\perp} \cong I/\{f_{\Re}(\eta)\}_{\{\Re\}}$ where η is a generator of the group of cyclotomic units H, $f_{\Re}$ is the frobenius group ring element that corresponds to an unramified prime ideal $\Re$ which splits completely in the extension $Q(\zeta_p)^+(\zeta_{2M})/Q$, and $\Re$ 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 ϕ 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 ϕ. Using the above decomposition of the ring $Z_l[G]$, one can write the l-part of any finite $Z_l[G]$-module A as

$$A \otimes Z_l \cong \prod_{\phi} A_\phi$$

where

$$A_\phi = A \otimes_{Z_l[G]} Z_l[x]/(\phi(x^{l^a})).$$

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

$$A^\perp = Hom_R(A, R) \text{ and } A^{dual} = Hom_Z(A, Q/Z).$$

Both of these groups are R-modules.

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

Let R be a finite Gorenstein ring. For any $M \in Z$, any finite abelian group G, and any irreducible polynomial $g(x) \in R[x]$, we have that the rings Z/MZ, $(Z/MZ)[G]$ 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 $\chi : R \to Q/Z$ denote a generator of the R-module $Hom_Z(R, Q/Z)$. Then, for every R-module A, the map $\Phi : A^{\perp} \to A^{dual} : f \mapsto \chi \cdot f$ is an isomorphism of R-modules.*

Proof: For any R-module A we have the canonical isomorphism

$$Hom_R(A, Hom_Z(R, Q/Z)) \cong Hom_Z(A, Q/Z).$$

We also have the R-isomorphism $R \cong Hom_Z(R, Q/Z)$ via the map that maps 1 to χ. Hence $A^{\perp} = Hom_R(A, R) \cong Hom_Z(A, Q/Z) = A^{dual}$ via the map Φ 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. The idea of the second one we will use in the third step of our algorithm.

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

$$0 \to mA \to A \to A/mA \to 0.$$

Since the functor $A \to A^{dual}$ 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

$$0 \to (A/mA)^{dual} \to A^{dual} \to (mA)^{dual} \to 0.$$

We therefore have that

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

This implies that

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

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^{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,

$$jh(mA) = jh((mA)^{dual}) \qquad and \qquad jh(A/mA) = jh((A/mA)^{dual}).$$

From the two exact sequences above and by [23, Lemma 7.86] we have that

$$jh(A) = jh(mA) \oplus jh(A/mA) \text{ and } jh(A^{dual}) = jh((A/mA)^{dual}) \oplus jh(mA^{dual}).$$

But since

$$jh(A/mA) = jh(A^{dual}/mA^{dual}) \qquad \text{and} \qquad jh(mA) = jh(mA^{dual}).$$

we have that $jh(A) = jh(A^{dual})$ and this complete the proof of the proposition. $\square$

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 $Ann_R(J)$ annihilates R/I. Then g is an isomorphism.*

Proof: We have that $|I| = |I^{\perp}| \leq |R/J| = |(R/J)^{\perp}| = |Ann_R(J)|$. The last equality follows from the fact that $(R/J)^{\perp}$ is isomorphic to $Ann_R(J)$. Since $Ann_R(J) \subset I$, we also have that $|I| \geq |Ann_R(J)|$, so that we must have equality everywhere, and g is an isomorphism. $\square$

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 ξ_a together with -1 were proven to form a system of independent generators for the group of cyclotomic units of $Q(\zeta_m)^+$

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

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 ξ denote a rational character of G irreducible over Q and for each such $\xi \neq \xi_0$ let $Ker(\xi) = \{\alpha \in G | \xi(\alpha) = \xi(1)\}$. Then the fields K_ξ fixed by $Ker(\xi)$ are cyclic of conductor f_ξ and with cyclic galois group $G_\xi = G/Ker(\xi)$ of order g_ξ. For each Dirichlet character χ 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 ξ, with equivalence class denoted by $[\xi]$. We should also explain here that two characters ξ belong to the same equivalence class if they generate the same cyclic subgroup.

Definition 1.4. *A real unit ε is a ξ-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_ξ.*

For each $\xi \neq \xi_0$ let $E_\xi \subset K_\xi$ be the group of proper ξ-units of K_ξ. In other words, E_ξ is the set of ξ-units that lie in K_ξ. Denote by F_ξ the group generated by the element $\theta_\xi = \eta_\xi^{\gamma_\xi}$, where η_ξ and γ_ξ are defined as follows:

For every automorphism $\alpha \in Gal(Q(\zeta_{f_\xi})^+/K_\xi)$ we choose an extension $\bar{\alpha} \in$

$Gal(Q(\zeta_{f_\xi})/K_\xi)$ and we define

$$\eta_\xi = \prod_\alpha \bar{\alpha}(\zeta_{f_\xi} - \zeta_{f_\xi}^{-1}).$$

Let α_ξ be a generator of G_ξ 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_ξ. The element $\eta_\xi^{\gamma_\xi}$ is in K_ξ and we have that

$$\eta_\xi^{|G|\cdot\gamma_\xi} = \pm\eta^{u_\xi}$$

where

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

We have $F_\xi = \langle(\pm\theta_\xi)^\alpha|\alpha \in G_\xi\rangle$ and we see that F_ξ is a subgroup of E_ξ. Let E_ξ^0 denote the group of ξ-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^{g-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:

$$h^+ = \frac{Q_K^+}{\sqrt{\frac{g^{g-2}}{\prod_{\xi\neq\xi_0} d_\xi}}} \prod_{\xi\neq\xi0} h_\xi$$

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

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

Since the discriminants d_ξ 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_ξ 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 θ_ξ are as above, and calculated the index of $\pm\Theta^I$ in the full group of units, where I is the augmentation ideal of $Z[G]$. 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 η that we introduce below. We prove that the group $H = \pm\eta^{Z[G]}$ is of finite index in the full group of units and modify the method of Schoof accordingly.

1.3.3 A New Cyclotomic Unit η

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 $Q(\zeta_{pq})^+$:

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

and by $H_{(g,h)}$ the group $\pm\eta_{(g,h)}^{Z[G]}$. We will usually omit the subscripts and just write H and η since we will let η_α denote the unit η with the galois element α 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 $H = \pm\eta^{Z[G]} = \pm\eta_{(g,h)}^{Z[G]}$ 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:*

$$[E:H] = \frac{2^{|G|-1}h^+}{|G|}\cdot$$

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

where the characters χ in the first product are the even characters χ_p of conductor p and those in the second product are the even characters χ_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 χ an even Dirichlet character and note that for any root of unity ζ 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 η_α is:

$$R = R(\{\eta_\alpha\})$$

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

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

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

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

$$= \pm\frac{1}{|G|}\prod_{\chi\neq 1}\frac{1}{2}\sum_{\substack{1\leq\beta\leq pq\\(\beta,pq)=1}}\chi(\beta)\big[log|1-\zeta_{pq}^{\beta(p+q)}|^2 + log|\frac{1-\zeta_p^{g\beta}}{1-\zeta_p^{\beta}}| + log|\frac{1-\zeta_q^{h\beta}}{1-\zeta_q^{\beta}}|\big]\ (*)$$

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

Lemma 1.1. *For $m|n \in Z^+$, if f_χ 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 $\chi : (Z/nZ)^\times \to C^\times$ can be factored through $(Z/(n/m)Z)^\times$, therefore $f_\chi|\ (n/m)$, contradiction. Hence such a exists and since $a \equiv 1\ mod(n/m)$ we have that $\zeta_n^{bm} = \zeta_n^{abm}$, hence

$$\sum_{\substack{1\leq b\leq n\\(b,n)=1}}\chi(b)\ log|1-\zeta_n^{bm}| = \sum_{\substack{1\leq b\leq n\\(b,n)=1}}\chi(b)\ log|1-\zeta_n^{abm}| =$$

$$\chi(a)^{-1}\cdot\sum_{\substack{ab(mod\ \ n)\\(ab,n)=1}}\chi(ab)log|1-\zeta_n^{abm}| = \chi(a)^{-1}\cdot\sum_{\substack{1\leq b\leq n\\(b,n)=1}}\chi(b)log|1-\zeta_n^{bm}|.$$

Since $\chi(a)^{-1} \neq 1$, we have that

$$\sum_{\substack{1 \leq b \leq m \\ (b,m)=1}} \chi(b)\ log|1-\zeta_n^{bm}| = 0,$$

as we wanted. $\square$

Lemma 1.2. *Let $n = mm'$ with $(m, m') = 1$ and assume $f_\chi|\ m$. 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 $f_\chi|\ m$, χ 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 $\zeta_n^{bm'} = \zeta_m^b$ we have that $\zeta_n^{bm'}$ depends only on a and it is clear that χ also only depends on a. The lemma now follows. $\square$

Lemma 1.3. *Let $P, Q, g \in Z^+$ with $f_\chi|P$ and $g|P$. 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 as $b = a + cP$ 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

$$1 - x^Q = \prod_{0 \leq c \leq Q-1} (1 - \zeta_{PQ}^{cP} x)$$

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 χ only depend on a, the lemma follows. $\square$

Lemma 1.4. *Let $n \in Z^+$ and assume $f_\chi |\ n$. Then*

$$\sum_{\substack{1\le b\le n\\(b,n)=1}} \chi(b)\ log|1-\zeta_n^b| = \prod_{p|n}(1-\chi(p)) \sum_{1\le b\le n} \chi(b) log|1-\zeta_n^b|.$$

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 $\prod_{p|n}(1-\chi(p))$, the right hand side equals

$$\sum_{\substack{1\le b\le n\\(b,n)=1}} \chi(b)\ log|1-\zeta_n^b| - \sum_{p_i} \chi(p_i) \sum_{1\le b\le n} \chi(b) log|1 - \zeta_n^b| +$$

$$\sum_{p_i\neq p_j} \chi(p_ip_j) \sum_{1\le b\le m} \chi(b) log|1-\zeta_n^b| - \ ...$$

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 $f_\chi |\ (n/p_i)$ and by Lemma 1.3 above with g =1, the sum becomes equal to

$$\sum_{1\le b\le n} \chi(b) log|1 - \zeta_n^b| - \sum_{p_i} \sum_{\substack{1\le b\le m\\p_i|b}} \chi(b) log|1 - \zeta_n^b| + \ ... \ =$$

$$\sum_{\substack{1\le b\le n\\(b,n)=1}} \chi(b) log|1 - \zeta_n^b|. \quad \square$$

We can now continue with the proof of Proposition 1.3.

For a character χ and the first summand in the brackets in $(*)$ above, we have

$$2 \sum_{\substack{1\le \beta\le pq\\(\beta,pq)=1}} \chi(\beta)\ log|1-\zeta_{pq}^{\beta(p+q)}| =$$

$$2\chi(p+q)^{-1} \sum_{\substack{\beta(p+q)\ \ mod(pq)\\(\beta(p+q),pq)=1}} \chi(\beta(p+q))\ log|1-\zeta_{pq}^{\beta(p+q)}|$$

$$= 2\chi(p+q)^{-1}(1-\chi(q))(1-\chi(p)) \sum_{1\le\beta\le pq} \chi(\beta)\ log|1-\zeta_{pq}^{\beta}| \qquad (by\ Lemma\ 1.4).$$

To this sum, for characters of conductor p or q, we apply Lemma 1.3. The first sum in $(*)$ now equals:

$$= \begin{cases} 2\chi(p+q)^{-1}\sum_{1\leq\beta\leq pq}\chi(\beta)\ log|1-\zeta_{pq}^{\beta}| & , \quad iff_x = pq \\ 2\chi(q)^{-1}(1-\chi(q))\sum_{1\leq\alpha\leq p}\chi(\alpha)\ log|1-\zeta_{p}^{\alpha}| & , \quad if\ f_\chi = p \\ 2\chi(p)^{-1}(1-\chi(p))\sum_{1\leq\alpha\leq q}\chi(\alpha)\ log|1-\zeta_{q}^{\alpha}| & , \quad if\ f_\chi = q \end{cases}$$

For a character χ and the second summand we have

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

$$= \chi(g)^{-1} \sum_{\substack{g\beta(mod\ \ pq) \\ (\beta,pq)=1}} \chi(g\beta)log|1-\zeta_p^{g\beta}| - \sum_{\substack{1\leq\beta\leq pq \\ (\beta,pq)=1}} \chi(\beta)log|1\ -\ \zeta_p^{\beta}|$$

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

If $f_\chi = pq$ then

$$\sum_{\substack{1\leq\alpha\leq pq \\ (\alpha,pq)=1}} \chi(\alpha)log|1\ -\ \zeta_p^{\alpha}| = \sum_{\substack{1\leq\alpha\leq pq \\ (\alpha,pq)=1}} \chi(\alpha)log|1\ -\ \zeta_{pq}^{q\alpha}| = 0 \qquad (by\ Lemma 1.1).$$

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:

$$= \begin{cases} 0 & , \quad iff_\chi = pq \\ (\chi(g^{-1})-1)(q-1)\sum_{1\leq\alpha\leq p}\chi(\alpha)log|1\ -\ \zeta_p^{\alpha}| & , \quad if\ f_\chi = p \\ 0 & , \quad if\ f_\chi = q \end{cases}$$

Similarly, the third summand equals:

$$= \begin{cases} 0 \quad , \quad iff_\chi = pq \\ 0 \quad , \quad if \ f_\chi = p \\ (\chi(h^{-1})-1)(p-1)\sum_{1\leq\alpha\leq q}\chi(\alpha)log|1 \ - \ \zeta_q^\alpha| \quad , \quad if \ f_\chi = q \end{cases}$$

Putting all three together and denoting by χ_{pq}, χ_p and χ_q the characters of conductor pq, p and q respectively, we have that

$$R \ = \ \pm\frac{1}{|G|}\prod_{\chi=\chi_{pq}\neq 1}\frac{1}{2}\cdot 2\ \chi(p+q)^{-1}\sum_{1\leq\beta\leq pq}\chi(\beta)\ log|1-\zeta_{pq}^\beta|\cdot$$

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

$$\prod_{\chi=\chi_q\neq 1}\frac{1}{2}\big[2\chi(p)^{-1}\ (1-\chi(p))+(\chi(h^{-1})-1)(p-1)\big]\sum_{1\leq\alpha\leq q}\chi(\alpha)log|1-\zeta_q^\alpha|$$

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

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

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

$$\prod_{\chi=\chi_q\neq 1}\frac{1}{2}\big[2(\chi(p)^{-1}\ -1)+(\chi(h^{-1})-1)(p-1)\big]\sum_{1\leq\alpha\leq q}\chi(\alpha)log|1-\zeta_q^\alpha|.$$

The L-series attached to each even character χ satisfies

$$L(1,\chi) \ = \ -\frac{\tau(\chi)}{f_\chi}\sum_{1\leq b\leq f_\chi}\bar{\chi}(b)log|1 \ - \ \zeta_{f_\chi}^b|$$

therefore R is now equal to

$$R \ = \ \pm\frac{1}{|G|}\prod_{\chi=\chi_{pq}\neq 1}\frac{(-f_\chi)}{\tau(\overline{\chi})}L(1,\overline{\chi})\cdot$$

$$\prod_{\chi=\chi_p\neq 1}\frac{1}{2}\big[2(\chi(q)^{-1}1)+(\chi(g^{-1})-1)(q-1)\big]\frac{(-f_\chi)}{\tau(\overline{\chi})}L(1,\overline{\chi})\cdot$$

$$\prod_{\chi=\chi_q\neq 1}\frac{1}{2}\big[2(\chi(p)^{-1}-1)+(\chi(h^{-1})-1)(p-1)\big]\frac{(-f_\chi)}{\tau(\overline{\chi})}L(1,\overline{\chi}) \ =$$

$$\pm\frac{1}{|G|}\prod_{1\neq\chi even}\tau(\chi)L(1,\overline{\chi})\cdot$$

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

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

$$R \ = \ \frac{2^{|G|-1}h^+R^+}{|G|}\cdot$$

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

Therefore,

$$\frac{R}{R^+} = \frac{2^{|G|-1}h^+}{|G|}\cdot$$

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

So now, by [30, Lemma 4.15], we have that

$$[E:H] = \frac{R}{R^+} = \frac{2^{|G|-1}h^+}{|G|}\cdot$$

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

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. □

Denote by P the factor

$$\frac{2^{|G|-1}}{|G|}\cdot$$

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

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 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

$$\Phi : Z[G] \to E$$

$$: \quad \alpha \quad \mapsto \eta^a$$

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

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

Lemma 1.5. *The kernel of the natural map*

$$j : E/E^M \to F^*/F^{*M}$$

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

Proof: Fix an embedding $F \subset C$. Then $Q(\zeta_{pq})^+$ identifies with a subfield of R. Suppose $0 < x \in E \subset R$ is in $Ker j$. Then $x = y^M$, some $y \in F^*$. Since $\mu_M \subset F$ we may assume that $y \in$ R and therefore $conj(y)$=y, where $conj$ is complex conjugation in Δ. Since Δ commutative, $s(y)$=$s(conj(y))$=$conj(s(y))$ $\forall s \in \Delta$, therefore $s(y)$=$\pm y$ $\forall s \in \Delta$, since y and all its conjugates are real M-th roots of x. If $l \neq 2$ then M is odd. Assume $\exists s \in \Delta$ with $s(y)$=$-y$. Then x=$s(x)$=$s(y^M)$=$(s(y))^M$=$(-y)^M$=$-x$, contradiction. Therefore Δ fixes y and hence $y \in (Q(\zeta_{pq})^+)^*$ and $x \in E^M$. Since we took $x > 0$ we need to check for -1 as well. Since M odd, $(-1)^M = -1$ therefore $-1 \in E^M$ 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 $y^2 \in Q(\zeta_{pq})^{+*}$. The quadratic subextensions of $F/Q(\zeta_{pq})^+$ are $Q(\zeta_{pq})(i)$ and $Q(\zeta_{pq})^+(\sqrt{\pm 2})$ and hence

$y^2 = 2u^2$ or $= \pm u^2$, for some $u \in E$. If $y^2 = 2u^2$, then $2 = y^2\ v^2$, 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=$(y^2)^{2^{(k-1)}}$. 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 $kerj = \langle -1 \rangle$ of order two in this case. □

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

$$0 \rightarrow \Delta \rightarrow \Omega \rightarrow G \rightarrow 0.$$

Let $\Re$ be any prime ideal of F of degree 1, ρ a prime ideal of $Q(\zeta_{pq})^+$ and r a prime number such that $\Re \mid \rho \mid r$. 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:

$$\begin{tikzcd}
\varepsilon \in E \arrow[r, "f_1"] & \vec{\varepsilon} \in (O/rO)^* \arrow[r, "f_2"] \arrow[d, "f_3"] & (O_F/rO_F)^{*\Delta} \arrow[d, "f_3'"] & & \\
& \mu_M(O/rO) & \mu_M(O_F/rO_F)^{\Delta} \arrow[l, "f_2'"] & (Z/MZ)[\Omega]^{\Delta} \arrow[l, "f_4"] & (Z/MZ)[G] \arrow[l, "f_5"]
\end{tikzcd}$$

The map f_1 is reduction modulo the ideal rO and $\vec{\varepsilon} = (\varepsilon_1, ..., \varepsilon_g)$ where $\varepsilon_i \equiv \varepsilon\ mod\ \rho_i$ and the ρ_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 ζ_{2M} mod $\Re$ and congruent to 1 modulo all the other primes $\Re'$ that lie over r. There is such an $\varepsilon \in E$ with $f_3' f_2 f_1(\varepsilon) \equiv \zeta_{2M}(mod \Re)$ and $f_3' f_2 f_1(\varepsilon) \equiv 1(mod \Re')$, 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 Δ-norm $= \sum_{s \in \Delta} s$. The map f_5 is an isomorphism since $(Z/MZ)[\Omega]^{\Delta}$ is fixed by Δ. Let $f_{\Re} = f_5^{-1} f_4^{-1} f_3' f_2 f_1$. Since $-1 = {\zeta_{2M}}^M$ we have that $f_{\Re}(-1) = 0$ and hence $f_{\Re}$ factors through the quotient

$$f_{\Re} : E/ \pm E^M \rightarrow (Z/MZ)[G].$$

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

Proof: Let μ_M denote the M-th roots of unity and once we choose a primitive M-th root we have the isomorphism

$$Hom_Z(E/ \pm E^M, \mu_M) \cong Hom_Z(E/ \pm E^M, Z/MZ)$$

which is naturally isomorphic to $Hom_Z(E/ \pm E^M, Q/Z)$. The group $E/ \pm E^M$ is a module over the group ring $(Z/MZ)[G] = R$, hence

$$Hom_Z(E/ \pm E^M, Q/Z) \cong Hom_Z(E/ \pm E^M \otimes_R R, Q/Z)$$

and the Adjoint Isomorphism Theorem gives

$$Hom_Z(E/ \pm E^M \otimes_R R, Q/Z) \cong Hom_R(E/ \pm E^M, Hom_Z(R, Q/Z)).$$

By Definition 1.1. we have that

$$Hom_Z(R, Q/Z) = R^{dual} \cong R$$

and we have therefore shown that

$$Hom_Z(E/\pm E^M, \mu_M) \cong Hom_R(E/\pm E^M, R).$$

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 $F(\sqrt[M]{E})/F$. Since $\Re$ splits completely, we can associate to it a uniquely determined element β in $Gal(F(\sqrt[M]{E})/F)$, namely the frobenius automorphism corresponding to $\Re$, such that $\beta(\sqrt[M]{\varepsilon}) \equiv (\sqrt[M]{\varepsilon})^r (mod\ \Re)$. From our definition of $f_\Re$ above we have $f_\Re(\varepsilon) = \sum_{s\in G} x_s s$ where x_s is determined by

$$s^{-1}(\varepsilon)^{(r-1)/M} \equiv \zeta_M^{x_s}\ mod\ \Re.$$

The corresponding homomorphism in $Hom_Z(E/\pm E^M, Z/MZ)$ maps ε to x_1. Since $\beta(\varepsilon)/\varepsilon$ is an M-th root of unity, we can write $\beta(\sqrt[M]{\varepsilon})/\sqrt[M]{\varepsilon} \equiv \zeta_M^{x_1}$ mod $\Re \Leftrightarrow \varepsilon^{(r-1)/M}$ $\equiv \zeta_M^{x_1}$ mod $\Re$. Therefore every $f_\Re$ corresponds to the frobenius map of $\Re$ in $Gal(F(\sqrt[M]{E})/F)$. From Kummer Theory we have that

$$Gal(F(\sqrt[M]{E})/F) \cong Hom_Z(E/\pm E^M, \mu_M)$$

and we showed above that $Hom_Z(E/\pm E^M, \mu_M) \cong Hom_R(E/\pm E^M, R)$. By Cebotarev's Density Theorem every element of $Hom_R(E/\pm E^M, R)$ is of the form $f_\Re$ for some prime $\Re$ of degree 1. This concludes the proof of the lemma. □

Theorem 1.1. *Let l and M be as above and let I denote the augmentation ideal of*

$R = (Z/MZ)[G]$. We have $B[M]^{\perp} \cong I/\{f_{\Re}(\eta) : \Re \in S\}$, where S denotes the set of unramified prime ideals $\Re$ of $Q(\zeta_{pq})^{+}(\zeta_{2M})$ of degree 1.

Proof: Applying the Snake Lemma to the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H/\{\pm 1\} & \longrightarrow & E/\{\pm 1\} & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow^{M} & & \downarrow^{M} & & \downarrow^{M} & & \\ 0 & \longrightarrow & H/\{\pm 1\} & \longrightarrow & E/\{\pm 1\} & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

yields the exact sequence of R-modules

$$0 \longrightarrow B[M] \longrightarrow H/\pm H^{M} \longrightarrow E/\pm E^{M}.$$

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

$$Hom_{R}(E/\pm E^{M}, R) \longrightarrow Hom_{R}(H/\pm H^{M}, R) \longrightarrow Hom_{R}(B[M], R) \longrightarrow 0.$$

which gives the isomorphisms

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

As we showed earlier,

$$H/\{\pm 1\} \cong Z[G]/N_{G}$$

and similarly here

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

so the G-norm kills every R-homomorphism $f : H/\pm H^{M} \to R$. 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 η. Therefore, by Lemma 1.6 we have that

$$Hom_R(E/\pm E^M, R) \cong \{f_{\Re}(\eta) : \Re \in S\}$$

where S denotes the set of unramified prime ideals $\Re$ of $Q(\zeta_{pq})^+(\zeta_{2M})$ of degree 1. From all of the above we obtain

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

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 $Q(\zeta_{pq})^{+}$. The group G is of order $(p-1)(q-1)/2$ and we have the isomorphisms

$$G \cong \Big((Z/pZ)^{\star} \times (Z/qZ)^{\star}\Big)/\{\pm\mathbf{1}\} \cong$$

$$\langle \sigma, \tau : \sigma^{(p-1)} = 1, \tau^{(q-1)} = 1, \sigma^{(p-1)/2}\tau^{(q-1)/2} = 1\rangle$$

where $\sigma : \zeta_p \mapsto \zeta_p^{\gamma}$ and $\tau : \zeta_q \mapsto \zeta_q^{\delta}$ with γ and δ being fixed primitive roots modulo p and q respectively. The last of the three relations is the relation for complex conjugation. The primitive roots γ and δ will be fixed throughout and will always represent the generators of $(Z/pZ)^{\times}$ and $(Z/qZ)^{\times}$ 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 σ to x and τ to y. Similarly,

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

Using this notation, the maps $f_{\Re}$ that were introduced in the previous chapter can now be expressed as polynomials in the variables x and y as follows:

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

where

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

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

We note here that the second sum in the definition of $f_{\Re}(x,y)$ 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

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

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

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. $\square$

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 $l^{a_1}||p-1$ and $l^{a_2}||q-1$. Since now l does not divide m_1 and m_2, we have that

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

$$Z_l[x,y]/((x^{l^{a_1}})^{m_1}-1, (y^{l^{a_2}})^{m_2}-1) \cong$$

$$\prod_{\phi_x,\phi_y} Z_l[x,y]/(\phi_x(x^{l^{a_1}}), \phi_y(y^{l^{a_2}})) \cong$$

$$\prod_{\phi_x} Z_l[x]/(\phi_x(x^{l^{a_1}})) \otimes \prod_{\phi_y} Z_l[y]/(\phi_y(y^{l^{a_2}}))$$

where the product runs over all irreducible divisors ϕ_x of $x^{m_1}-1$ and ϕ_y of $y^{m_2}-1$. We see that $Z_l[x]/(\phi_x(x^{l^{a_1}}))$ and $Z_l[y]/(\phi_y(y^{l^{a_2}}))$ 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 Δ 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 ϕ-parts

$$A_{\phi_x,\phi_y} = A \otimes_{Z_l[\tilde{G}]} \Big(Z_l[x]/(\phi_x(x^{l^{a_1}})) \otimes \prod_{\phi_y} Z_l[y]/(\phi_y(y^{l^{a_2}})) \Big).$$

The simple Jordan-Hölder factors of each A_{ϕ_x,ϕ_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 ϕ-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 $\Big[Z_l[x]/(\phi_x(x^{l^{a_1}}))\Big]/(l,\phi_x(x))$ and $\Big[Z_l[y]/(\phi_y(y^{l^{a_2}})\Big]/(l,\phi_y(y))$, we must have that the orders of x and y in the ring attached to ϕ_x and ϕ_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_{ϕ_x,ϕ_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_{ϕ_x,ϕ_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

$$B[M]^{\perp}_{d_1,d_2} \cong (x-1,y-1)/\langle (x^{l^{a_1}})^{d_1}-1, (y^{l^{a_2}})^{d_2}-1, cnj, f_{\Re}(x,y) : \Re \in S\rangle \qquad (i)$$

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

$$J = \langle (x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1, cnj, f_{\Re}(x,y) : \Re \in S \rangle \qquad (ii)$$

from (i) above, makes $B[M]^{\perp}_{d_1,d_2}$ a $(Z/MZ)[G]$-module. Note that here, the polynomials $f_{\Re}$ are restrictions of the frobenius elements of Theorem 2.1 to this smaller extension determined by the set of polynomials $(x^{l^{a_1}})^{d_1} - 1$ and $(y^{l^{a_2}})^{d_2} - 1$. They are therefore of the form

$$f_{\Re}(x,y) = \sum_{1 \le i \le d_1 l^{a_1}} \sum_{1 \le j \le d_2 l^{a_2}} log_l\Big(\prod_{\substack{m \equiv i mod(d_1 l^{a_1}) \\ n \equiv j mod(d_2 l^{a_2})}} \eta_{(m,n)} \Big) \cdot x^i \cdot y^j \qquad (iii).$$

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 $B[M]^{\perp}_{d_1,d_2}$ and to also calculate their order. We use the theory for Gröbner Bases, which we present here by following [1]. As before, $d_1 = gcd(p-1, l^{f_1} - 1)$ will be the order of x and $d_2 = gcd(q-1, l^{f_2} - 1)$ 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 ϕ_x and ϕ_y respectively. Again, let $B[M]^{\perp}_{d_1,d_2}$ be the corresponding R_{d_1,d_2}-module and

$$J = \langle (x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1, cnj, f_{\Re}(x,y) : \Re \in S \rangle$$

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

J 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

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

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 $f_1, f_2, ..., f_s$ be polynomials in R, with $f_i \neq 0 \ \forall \ 1 \leq i \leq s$, and let $F = \{f_1, f_2, ..., f_s\}$. We say that f reduces to h modulo F, denoted*

$$f \xrightarrow{F} h \ ,$$

if and only if there exist polynomials $h_1, ..., h_{t-1} \in R$ 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 $f - h \in \langle f_1, ..., f_s \rangle$.

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 $G = \{g_1, ..., g_n\}$ 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

$$f \in V \text{ if and only if}$$

$$f \xrightarrow{G} 0$$

(iii) For all $f \in V$, $f = h_1 g_1 + ... + h_n g_n$ for some polynomials $h_1, ..., h_n \in R$, such that $lp(f) = max_{1 \leq i \leq n}(lp(h_i) lp(g_i))$. $\square$

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.* $\square$

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 $B[M]^{\perp}_{d_1,d_2}$ 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 $T = \langle (x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1, N_d \rangle$. We therefore see that

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

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 $Q(\zeta_{pq})^+$ 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 Z/lZ where, as above, $gcd(m_i, l)$=1 for i=1,2 and $m_1 l^{a_1} = p - 1$ and $m_2 l^{a_2} = q - 1$. As before, let (f_1, f_2) be a pair of degrees of irreducible polynomials ϕ_x, ϕ_y respectively, which appear in the factorization of $Z[\tilde{G}]$. Let $d_1 = gcd(p-1, l^{f1} - 1)$ and $d_2 = gcd(q-1, l^{f_2} - 1)$. For various primes r with $r \equiv \pm 1 (mod\ pq)$ and $r \equiv 1 (mod\ 2l)$ we calculate the frobenius elements $f_{\Re}$ 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 $f_{\Re_i}$ that we calculated above and we let $J_i = J_{i-1} + (f_{\Re_i})$. This ascending chain of ideals will computationally stabilize at some ideal $J^l \subseteq (x-1, y-1)$ in R_{d_1,d_2}. If J^l 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 $J^l \subset (x-1, y-1)$ then the corresponding $B[l]^{\perp}_{d_1,d_2}$ is not trivial, if J^l 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^l 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 $(x-1, y-1)/J^l$ 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 $f_{\mathfrak{R}}$ now lie in (Z/MZ) and we have to make sure that the primes r satisfy $r \equiv 1(mod\ 2M)$ for the specific power M of l. As before, let $R_{d_1,d_2} = (Z/MZ)[x, y]/((x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1)$, and denote by I_M its augmentation ideal. As in Step 1, for each M we have that the sequence of ideals

$$J_0 \subset J_1 \subset ... \subset J_i \subset ...$$

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

$$... \to I_{lM}/J^{lM} \to I_M/J^M \to ...$$

we have that the orders of the modules I_M/J^M are non-decreasing. Since $B[M]^{\perp}_{d_1,d_2}$ is finite and its order is bounded above by $|B_{d_1,d_2}|$ which is finite and independent 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, $|I_{lM}/J^{lM}| = |I_M/J^M|$ hence $I_{lM}/J^{lM} \cong I_M/J^M$. Therefore M annihilates I_{lM}/J^{lM} and therefore it also annihilates its quotient $\Big(I_{lM}/J^{lM}\Big)/\langle f_{\Re}(x,y) : \Re \in S\rangle \cong B[lM]^{\perp}_{d_1,d_2}$. This implies that $M(B[lM]^{dual}_{d_1,d_2}) = 0$ which gives $M(B[lM]_{d_1,d_2}) = 0$ since as finite abelian groups, $B[lM]^{dual}_{d_1,d_2}$ and $B[lM]_{d_1,d_2}$ are isomorphic. Therefore $B[Ml]_{d_1,d_2} = B[M]_{d_1,d_2}$ and

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

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 $B^{dual}_{d_1,d_2}$ are isomorphic as finite abelian groups, we obtain $MB^{\perp}_{d_1,d_2} = 0$.

2.4.3 Step 3

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

$$g : (x-1, y-1)/((x^{l^{a_1}})^{d_1} - 1, (y^{l^{a_2}})^{d_2} - 1, J^M) \to B^{\perp}_{d_1,d_2}$$

is actually an isomorphism.

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

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

Recall that the $(Z/MZ)[G]$-module $H/\pm H^m$ is isomorphic to $(Z/MZ)[G]/N_G$. Furthermore, since M annihilates $B^{\perp}_{d_1,d_2} \cong Hom_{R_{d_1,d_2}}(B_{d_1,d_2}, R_{d_1,d_2})$ 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

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

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

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

We need the following: For any ideal $J \subseteq R$, R some finite Gorenstein ring, duality yields a surjection $R \cong Hom_R(R,R) \to Hom_R(J,R)$. 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

$$Hom_{R_{d_1,d_2}}(I_M, R_{d_1,d_2}) \cong R_{d_1,d_2}/Ann_{R_{d_1,d_2}}(I_M) = R_{d_1,d_2}/N_d.$$

Therefore, the kernel of the map

$$Hom_{R_{d_1,d_2}}(I_M, R_{d_1,d_2}) \to Hom_{R_{d_1,d_2}}(J^M, R_{d_1,d_2})$$

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

$$\Psi : B_{d_1,d_2} \hookrightarrow (I_M/J^M)^{\perp} \cong Ann_{(R_{d_1,d_2}/N_d)}(J^M).$$

Assume that $Ann_{R_{d_1,d_2}/(N_d)}(J^M)$ annihilates $\Big(R_{d_1,d_2}/N_d\Big)/\psi(B_{d_1,d_2})$. Then

$$Ann_{R_{d_1,d_2}/N_d}(J^M) \subseteq \psi(B_{d_1,d_2}).$$

But now we have that

$$|Ann_{R_{d_1,d_2}/N_d}(J^M)| \leq |\psi(B_{d_1,d_2})| = |B_{d_1,d_2}| = |\Psi(B_{d_1,d_2})| \leq |Ann_{(R_{d_1,d_2}/N_d)}(J^M)|.$$

Therefore we have that the orders of I_M/J^M and $B^{\perp}_{d_1,d_2}$ are equal and hence g is an isomorphism. From the second exact sequence above we have that

$$\Big(R_{d_1,d_2}/N_d\Big)/\psi(B_{d_1,d_2}) \cong (H/\pm E^M)_{d_1,d_2}.$$

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

To find the annihilator $Ann_{R_{d_1,d_2}/N_d}(J^M)$ 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

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

Then, we apply each generator $h(x,y)$ of the annihilator to the unit η_{d_1,d_2}, where η_{d_1,d_2} is the unit η with the 'norm' element $\frac{(x^{p-1}-1)(y^{q-1}-1)}{(x^{l^{a_1}d_1}-1)(y^{l^{a_2}d_2}-1)}$ applied to it. If $\eta^{h(x,y)}_{d_1,d_2}$ 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 η_d^h the unit $\eta_{d_1,d_2}^{h(x,y)}$ that we already described above and by G_d the quotient of G containing the coset representatives of the embeddings in G, which map ζ_p to $\zeta_p^{g^i}$ and ζ_q to $\zeta_q^{h^i}$, for $1 \le i \le l^{a_1}d_1$ and $\le j \le l^{a_2}d_2$.

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

$$P(X) = \prod_{a \in G_d} (X - (a(\eta_d^h))^{1/M})$$

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

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

$$T(X) = X^{M/N} - (\eta_d^h)^{1/N}$$

is irreducible in $Q(\zeta_{pq})^+$. Since $M/N \ge 3$, $T(X)$ has at least one complex root. Therefore $(\eta_d^h)^{1/M}$ 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. □

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 $GCD(P_{(g,h)}) = 2^{32}$ 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:

$$x^2 - 1 = (x + 1)(x + 2)$$

$$y^{22} - 1 = (y + 1)(y + 2)(y^5 + 2y^3 + y^2 + 2y + 2)(y^5 + 2y^3 + 2y^2 + 2y + 1)(y^5 + 2y^4 + 2y^3 + 2y^2 + 1)(y^5 + y^4 + 2y^3 + y^2 + 2)$$

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

$P_{(g',h')}$ but not of $GCD(P_{(g,h)})$ and therefore it is possible that it might only divide $P_{(g',h')}$ and not h^+. The pair $(g_0, h_0) = (5(mod7), 7(mod67))$ 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 $M = 3, 3^2, ...$ 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 $|I_M/J^M|$.

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

$M = 3$

$r_1 = 7521823$

$f_{\Re_1} = (y^5+y^4+2y^3+2y^2+2y+2)x^5+(2y^5+2y^4+2y^3+2y^2+y+2)x^4+(2y^5+y^4+y^2+1)x^3+(2y^5+2y^4+2y^3+2y^2+y+2)x^2+(y^5+y^4+y^3+2y+1)x+(y^5+y^4+y^3+2y)$

$r_2 = 8889427$

$f_{\Re_2} = (2y^5 + 2y^4 + y^3 + 2y^2 + y + 2)x^5 + (2y^5 + 2y^3 + 2y^2 + 2y)x^4 + (2y^5 + 2y^4 + y^3 + 2y + 2)x^3 + (y^5 + 2y^3 + 2y^2 + 2y)x^2 + (2y^4 + y)x + (y^5 + 2y^4 + 2y^3 + 2y^2 + y)$

$r_3 = 9573229$

$f_{\Re_3} = (y^4+2y^3+2y+1)x^5+(y^4+y^3+y^2)x^4+(y^5+2y^2+y+2)x^3+(2y^4+2y^3)x^2+(2y^5 + 2y^4 + y^3 + y + 2)x + (y^5 + y^3 + 1)$

$r_4 = 10257031$

$f_{\Re_4} = (y^5 + y + 2)x^5 + (2y^5 + 2y^4 + 2y^3 + 2y^2)x^4 + (2y^4 + 2y^3 + y^2 + 2y)x^3 + (y^5 + y^2 + y + 1)x^2 + (2y^5 + 2y^4 + y^2 + 2y + 2)x + (2y^5 + y^4 + 2y^3 + y^2 + y)$

$r_5 = 20514061$

$f_{\Re_5} = (2y^5 + y^3 + y^2 + 2y + 1)x^5 + (2y^4 + y^3 + y^2 + 2y + 2)x^4 + (2y^5 + y^4 + 2y^3 + y + 2)x^3 + (y^2 + y)x^2 + (2y^5 + y^2 + 2y + 1)x + (y^5 + 2y^3 + y^2 + y)$

$r_6 = 22565467$

$f_{\Re_6} = (2y^4 + y^3 + y^2 + 2)x^5 + (2y^5 + 2y^3 + y + 1)x^4 + (y^5 + y^4 + y^3 + y^2 + 2y + 1)x^3 + (2y^4 + 2y^3 + y^2 + y + 2)x^2 + (y^5 + 2y^4 + 2y^3 + y^2 + 2)x + (2y^5 + 2y^4 + y^3 + y^2 + 1)$

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

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 $Z/3Z$ we have that $|I_M/J^M| = 3$.

$M = 3^2$

$r_1 = 7521823$

$f_{\Re_1} = (4y^5 + 7y^4 + 5y^3 + 8y^2 + 5y + 2)x^5 + (5y^5 + 8y^4 + 5y^3 + 2y^2 + 4y + 8)x^4 + (8y^5 + 4y^4 + 6y^3 + 7y^2 + 6y + 4)x^3 + (2y^5 + 8y^4 + 2y^3 + 2y^2 + y + 8)x^2 + (y^5 + 7y^4 + y^3 + 3y^2 + 8y + 7)x + (y^5 + 4y^4 + 7y^3 + 3y^2 + 2y + 6)$

$r_2 = 8889427$

$f_{\Re_2} = (2y^5 + 2y^4 + y^3 + 2y^2 + 4y + 5)x^5 + (2y^5 + 3y^4 + 8y^3 + 2y^2 + 5y + 3)x^4 + (2y^5 +$

$8y^4+y^3+5y+5)x^3+(7y^5+6y^4+5y^3+2y^2+2y+6)x^2+(6y^5+2y^4+3y^2+y)x+$

$(y^5+2y^4+5y^3+2y^2+y+6)$

$r_3 = 9573229$

$f_{\Re_3} = (4y^4+8y^3+5y+1)x^5+(3y^5+7y^4+7y^3+7y^2+6y)x^4+(y^5+6y^3+5y^2+y+2)x^3+$

$(6y^5+5y^4+5y^3+3y^2+3y+3)x^2+(5y^5+5y^4+y^3+7y+8)x+(4y^5+3y^4+7y^3+3y^2+6y+7)$

$r_4 = 10257031$

$f_{\Re_4} = (y^5+3y^4+y+2)x^5+(2y^5+5y^4+2y^3+8y^2)x^4+(6y^5+2y^4+5y^3+y^2+5y)x^3+$

$(4y^5+7y^2+y+4)x^2+(8y^5+5y^4+6y^3+y^2+2y+8)x+(8y^5+7y^4+8y^3+4y^2+4y+6)$

$r_5 = 20514061$

$f_{\Re_5} = (5y^5+3y^4+7y^3+7y^2+2y+4)x^5+(5y^4+7y^3+4y^2+2y+2)x^4+(5y^5+$

$4y^4+8y^3+3y^2+y+2)x^3+(3y^5+6y^4+3y^3+y^2+y+3)x^2+(8y^5+6y^4+3y^3+$

$7y^2+8y+7)x+(4y^5+3y^4+8y^3+7y^2+7y+6)$

$r_6 = 22565467$

$f_{\Re_6} = (3y^5+5y^4+y^3+y^2+3y+2)x^5+(5y^5+6y^4+8y^3+7y+7)x^4+(y^5+7y^4+$

$7y^3+4y^2+8y+1)x^3+(3y^5+5y^4+2y^3+7y^2+7y+8)x^2+(7y^5+2y^4+8y^3+7y^2+$

$5)x+(2y^5+5y^4+y^3+y^2+7)$

$J^M = (y^2-3y+2, 3-x-2y) = ((y-1)(y-2), -2(y-1)-(x-1))$ 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 $M = 3^3$.

$M = 3^3$

$r_1 = 7521823$

$f_{\Re_1} = (13y^5 + 7y^4 + 14y^3 + 26y^2 + 14y + 20)x^5 + (5y^5 + 17y^4 + 5y^3 + 11y^2 + 13y + 26)x^4 + (17y^5 + 4y^4 + 24y^3 + 16y^2 + 6y + 4)x^3 + (20y^5 + 8y^4 + 11y^3 + 11y^2 + y + 26)x^2 + (y^5 + 25y^4 + 19y^3 + 21y^2 + 26y + 7)x + (10y^5 + 22y^4 + 25y^3 + 3y^2 + 2y + 6)$

$r_2 = 8889427$

$f_{\Re_2} = (20y^5 + 2y^4 + y^3 + 11y^2 + 22y + 23)x^5 + (2y^5 + 12y^4 + 26y^3 + 11y^2 + 14y + 21)x^4 + (2y^5 + 26y^4 + y^3 + 18y^2 + 14y + 23)x^3 + (16y^5 + 15y^4 + 14y^3 + 20y^2 + 11y + 15)x^2 + (6y^5 + 11y^4 + 21y^2 + 19y)x + (10y^5 + 11y^4 + 23y^3 + 11y^2 + 10y + 24)$

$r_3 = 9573229$

$f_{\Re_3} = (9y^5 + 4y^4 + 17y^3 + 18y^2 + 5y + 19)x^5 + (12y^5 + 16y^4 + 7y^3 + 7y^2 + 15y)x^4 + (10y^5 + 24y^3 + 14y^2 + 10y + 20)x^3 + (24y^5 + 5y^4 + 5y^3 + 3y^2 + 12y + 12)x^2 + (5y^5 + 5y^4 + 19y^3 + 9y^2 + 7y + 26)x + (13y^5 + 21y^4 + 25y^3 + 12y^2 + 6y + 16)$

$r_4 = 10257031$

$f_{\Re_4} = (10y^5 + 3y^4 + 18y^3 + 19y + 2)x^5 + (20y^5 + 14y^4 + 2y^3 + 17y^2 + 9y + 9)x^4 + (24y^5 + 2y^4 + 23y^3 + 10y^2 + 14y + 9)x^3 + (22y^5 + 9y^4 + 9y^3 + 7y^2 + 10y + 22)x^2 + (26y^5 + 5y^4 + 15y^3 + y^2 + 2y + 26)x + (17y^5 + 16y^4 + 26y^3 + 4y^2 + 22y + 15)$

$r_5 = 20514061$

$f_{\Re_5} = (14y^5 + 3y^4 + 25y^3 + 16y^2 + 11y + 22)x^5 + (18y^5 + 23y^4 + 16y^3 + 22y^2 + 2y + 20)x^4 + (23y^5 + 22y^4 + 17y^3 + 21y^2 + 10y + 20)x^3 + (21y^5 + 6y^4 + 12y^3 + 19y^2 + y + 3)x^2 + (17y^5 + 15y^4 + 21y^3 + 7y^2 + 26y + 16)x + (13y^5 + 3y^4 + 26y^3 + 25y^2 + 7y + 24)$

$r_6 = 22565467$

$f_{\Re_6} = (12y^5 + 23y^4 + 19y^3 + 10y^2 + 12y + 11)x^5 + (14y^5 + 24y^4 + 8y^3 + 25y + 7)x^4 + (10y^5 + 16y^4 + 7y^3 + 4y^2 + 8y + 1)x^3 + (21y^5 + 5y^4 + 20y^3 + 16y^2 + 16y + 8)x^2 +$

$(25y^5+2y^4+8y^3+16y^2+5)x+(20y^5+14y^4+y^3+y^2+16)$

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

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 $(d_1, d_2) = (2{,}22)$ the frobenius polynomials give exactly the same ideals J^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 $B^{\perp}_{d_1,d_2}$. 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 $B^{\perp}_{d_1,d_2}$ 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 Z, then the unit $\eta^{h_i}_{d_1,d_2}$ 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 *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_χ, 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

$f = p \cdot q$	GCD	extra 'non trivial' primes	$\tilde{h}^{+}$
321=3·107	1	3	3
427=7·61	1	5	5 $*$
469=7·67	1	3	3^2 $*$
473=11·43	$3^4 \cdot 5^2 \cdot 7^4$	-	1 $*$
481=13·37	$7 \cdot 19$	-	19
551=19·29	5	-	5
629=17·37	$3^4 \cdot 19$	5	5·19
697=17·41	$3^3 \cdot 7$	-	3
703=19·37	$3^{16} \cdot 5$	13,37	13·37
753=3·251	1	11	11
763=7·109	3^4	13	13
779=19·41	5^2	41	41
785=5·157	$3^2 \cdot 79$	-	3 $*$
793=13·61	$3^{20} \cdot 5 \cdot 7$	37	$3 \cdot 37$ $*$
817=19·43	1	5	5
869=11·79	1	79	79
889=7·127	$3^4 \cdot 7^2$	-	7 $*$
923=13·71	3^3	61	61
985=5·197	$3^3 \cdot 11$	-	3
1101=3·367	1	3	3 $*$
1139=17·67	$3^7 \cdot 11^7$	89	89
1141=7·163	1	19	19
1159=19·61	$3^3 \cdot 7$	73	73
1207=17·71	3^2	17	17
1211=7·173	1	7	7
1241=17·73	$3^4 \cdot 7 \cdot 37 \cdot 109$	5	5
1243=11·113	$5 \cdot 37$	41	41
1257=3·419	1	3	3
1261=13·97	7^3	5,97	$5 \cdot 7^2 \cdot 97$
1271=31·41	$3^3 \cdot 5^6$	7,11,31	$7 \cdot 11 \cdot 31$
1313=13·101	$3 \cdot 5^2$	31	31
1339=13·103	$3^7 \cdot 17^5$	13	$3^2 \cdot 13$ $*$
1343=17·79	5	17	17
1355=5·271	$3^3 \cdot 5$	37	37
1385=5·277	$3^2 \cdot 139$	5,7	$5 \cdot 7$
1387=19·73	$3^4 \cdot 7 \cdot 101$	17,19,37	$17^2 \cdot 19 \cdot 37$
1393=7·199	1	5	5

Table 3.2: Main Table Continued

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

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 η 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 θ_ξ introduced in 1.3.1 for the cyclic subfield K_ξ. 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^+.

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 $Q(\zeta_{7\cdot 67})^+$ 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}$105396109733503507390551867013258435444498076254086208
515231384896204081 8.0000000000000...X^{35} + 27770849867391781929153039 12
3424870200502519195159225493647320919842008162255027094008168821939260 9
4301873763494728581933647064840838030277079 12.999999999999...X^{34}
− 4430311868472799003847513079501905099728766646454366030912016726639832
8507586815778745045238775196878181746855466988401029075529237875580382 30
83385780057005333105063502390932593708031080 73.99999999999999...X^{33}
+ 176693037355891254273323143703633528959881636956778825389053993886
574361330101078950441893914805001001154219295199549799824378107250660467 44
37039663537598308569264697053786233006407395642316829728774221942366554 37
4835898726936353471.9999999999999999999...X^{32} −
118245613631805832148856824695260705266257885134607987346024885714514899678
176750537049883090503527837025590471059902844954818523209405684251889015 83
1436318652596929848061438500207199081829437469925906650429326841995685 49
7316062065767284819240169537850440399816658 7.999999999999999999999999...X^{31}
+ 1978293496742157460348417170288169109794370841890033837498196523028671961
996005769427730405407273553703690433505961560132089854762069408810804766455 6
519943952901000535380338895861380139505767328320003719182346767882843002779
4951449225535243180779144073622039411067088845962815384860602 6
06562850804.99999999999999...X^{30} −
1100986919646893842326499440503297743785765745863955446122109852469541195 6
945547983250818259235527169394413721311579115829136617621706592899306 03
3949326520673731884670469894890533505382331569679213674145664772117902700
3805013772244142995792886020866062662916391622852789395239936636190579552
691900938377936514261659250579 39.9999999999999999999999...X^{29}
+ 244569892095091938314892448208938554039722356072854135212377617586443 43
5295118703188184741730974218486051268622037022411339175699547300030154 98

22871951434808167003997676218121580379254248395187778623595659125887565

9144008994973509254995244645129122374274147428637264962970738335343754798

22052730106174422447999541680198098262634253583479514

62720834.9999999999999999999...X^{28} −

27436557356034724128817446413685197948411808135909544354956975329494

09658663429195537590532690585714627579052010736384406792449715211

830899443498069308081112093388139161566491176370470803796910045906

39062772914726090816222586097268188753238380117211292581206347558

8805233021652751637749047645330208638460261019340244710959505344578

950453410226765875375141682295733378024307.9999999999999999999999999...X^{27} +

1613833366410763456456079717682426881164960451134616497662425

9264664017926930928966218958385895844971621398414514983675560806018

314570324869426678376784580375358215022645037911552476248093144775954324

0428862589069909709277555574873995672921653833932239895

0227124445025992932357641918834159111777166513035099430412014766

182764644397830940824

106683696118474387368543296400134823122482

9066548852444606.999999999999999...X^{26} −

4635403380089426272687801176816126323523597073205882181607656464952

804237328200654528788008026512153298866596835293708740267998580

72192210761589694075573487972643504346241703333113864485939162487248273831860

101946569761033802036467623592502743899710074709

9533754932095601765376279

790241648911878694250657530670049416410336886981131314297229

45230283119643948817127450925446877388955069437370113489918117

67905811768733006359.9999999999999999999...X^{25} +

50899063110951250423796046159121202507656267532409988489050811463

3668686165594547366288881222528181685735138872258060202981093

13465302975573130916478674683007868313011051254351607975506640715533383343

9463881645430045092733661777763690407426317660215950141

7980859007538637711136389083127731633054913821014347446263744108364228

938341996620673770825795048143607897932141759534782075608277752455490052

5566788329116051179378877188854154366370240913982.9999999999999999999...X^{24}

− 5398119935249082433570676523479132330706396424724716453378713669237

476845788734699180849758842401074787620140528731948245702262735095285899995

298560235552687177840055539914947106344057255369974108447567317902898711

21673876993955497181429163486515190178070

1884260717587061121123220763142136

612078227048756373203381588548524020344713102805265

6947959101722036031788094928

196109362903309473140516916736651107209084857400607372816

$815403486090651898726604560788383410000851.99999999999999999...X^{23} +$

158794135161858492808221573642293390388034850618205212157567206301013364623 7408

603950699437258119398797754848594984798527674225391992367398716199 1415

122803086410614730800312204656870113825483147781145605286551416265400969 3504

980606118005902254701829510521608474316697043832153791320913553233218166470

434808229035033913403366851484001148848858511672796887762543236185242090 7033

746700991764400675932782747130231194120545243089720137701989926563913343 5283

$5573285106539261179170543773811 1.99999999999999999999999999...X^{22}$

$- 8308712221877523088156990053528236708613978193396102432559314274627119526 7514266$

730221317898876884562113916697267062962781022247188542079041675602451760220580 4334383

12943530601136037173054504544189723650468575320836738854571867828954370018346 74741075

414316988311448253222789038932402000866737315026659281317426073003709932655095 2394634

397980189007138105169271123492878198129100039112660655511481769898138387370219 8348255

7462695352294137620832434469873559275278736204041134595257381857660556853922

$42779.99999999999999999...X^{21} +$

120584137475532259592432281208804542491906512490530661694 7104

106388674287957889920805049429751273161780809729692406981449550085427823351034 4895142

408595028057505647146552927045988326969654572352060153468413116803838624580068 6799119

011274247617426689085269580563111930239335241523331476182910238513375501103660 5603310

630911620794767755122052528829813956296205566576835922961643481629343047397892 1556963

722102709672908828819449235238644002348762939242604074528541685887971592851694 4145821

$616787877917806811948551742478033.999999999999...X^{20} -$

304088457686204204604361030323565508159719530999093127005226591795922168535268 0990765

251733430390182540956274438530161045957732159648883665463962990342091018234174 1299532

229863234454409165457246349784032948001875737300845790388810441179332786445057 8653552

391027956873466482528565942490020973242959266543473675476484759460181704506105 3454860

028427779176072576999308288136472522405544215548564819167560004996275048161732 9861903

9179331947200179844379632630563670740654848601563739493053638554498201286522977722157

3707035475082579.9999999999999999...X^{19} + 1917121787682851735092003419251040393260657

9976687109767673185665043316428571408373265130731585960504716418901631760956500847844

8006685227335908452359751739690697756445817385234799971309088239121436295656646452659

5315987002960658253514596884313472583135074775410859355587659180962871141232196112811

4854942361692352372785405175064365551231050979738127206689968883321965222941176791700

5168668340860477307592266966272649037191197406934134774079333467962530727583332113608

522364533511432634938575869311555547065109036992934

42644012173667.99999999999999999999...X^{18} −

2026763519321103866016748293034278165944217773244601197543323303320079351724021444

182230586040049633121202060270092694320291991686770046379835946549453291648234372395

3898267498925934914124958598650336595532473817022538170954066813999114377538517874638

8354788537965053917406982792063090785128654115342540310284672720683829695195304043524

3468944393302585074578321843293496794139160191788871081360341641210921293415253067061

3611962869152327845273253870042788690874315200401710962434664778746031530742529446119

81371725885087108568548335.9999999999999999...X^{17} +

535668941859072585978725512282002226721529589025692932829381547406837254997654566455

6733369503623674837069567594895489692631025192849018682143444185147188095486600433990

1512783580637695244327060782898715861562114856328077210148879050918309426104668240619

1765587050547231795199255905328775244072810392504786000177539364069462937527206950834

1648571840489820237816066540234578433382301812676272828956635596527874389809520643751

0783066623491115427083153881949555749222036155204794173896588485185399508900875954391

985314532366326054789.99999999999999999999...X^{16} −

101362433911685028852435019920245977154707329574475329291897016991484427435476188899

1341581683292456979783750358523191222712109880575581846295624373840529377868965489435

3872749172904383498710307472955063247838883594728141385608917207081812339740208863584

1634796680068903845422340879997902375702627749694838988861479080809384556957297984455

6739635216541074527296953954215013223906692782193168126440197594782655472201612260017

2435983819117816797928821206284212914103169415017789647384306194603474711104666363638

08090.00000000000000000000...X^{15} +

59721161492936066593669336726847798596152542824393514318260531323566263014608528553

3820862745600780461677453335369346831115705872080456411701101638721363076270707839997

9461985549170100998537836301395496168276005359879139732904573351143168424380286497852

0282418578000158173341313576081777769575212330285247504526715501731394326336712846927

1287616610431308988547037268886382074593335735196101110260858108857822229134241390551

$$
\begin{aligned}
&128761661043130898854703726888638207459333573519610111026085810885782222913424139055 1\\
&57160452000346488215196073238994104481022436375499337274439190 91\\
&799902022.99999999999999999...X^{14} -\\
&111361035113030029032738024590529431560899640677321107018240769034672273741743782265 0\\
&558137696951673375803379761101666268834281860124474959960373527479248023284566747776 7\\
&832067316404180473198584378595470367989308622414979793263434793978511339567422408454 0\\
&490159324828042607336098363596185264328057511535218196628854620830568280631389854086 5\\
&964940422297399380703290853927335805379923549676325499047193767246447776311260084310 6\\
&7998218884069974273857510691573668240922262908737480 90.00000000000000000...X^{13}\\
&+ 6465601402186598739007057334906139759471710315645952726680769090528324225046043443 99\\
&958391836528018732138208574741235010948951103929933085512734807757963564046175530272 8\\
&683139421202823966410829693470287667951764391748435883742813253617336867585689731481 6\\
&609364081473496161061565605508477891624460877163701249289125901271820720939010340894 1\\
&786980646157502078891952679249099700563831656858255340555828644373999505776342137714 4\\
&557320465850068610815480247868670797.99999999999999...X^{12}\\
&- 5818605356870885651866318880487971181745757048428154704869932789216597\\
&459246891276319056040177246303005761385938983437637142057433352669448923223658831214 1\\
&410724330966763178190698033846666552581653694784862091512805180988111405275758992553 6\\
&577301784980009433533647905526597057048205343586793886440014030353735810276252533485 0\\
&686425837536104150880423687944431556057051043399316413857531311565297337299110692421 4\\
&146821039862428287566917.999999999999999999...X^{11} +\\
&131110925619705388917607834791319024281334448648125167732975040016527230382526955234\\
&383044772374980740880898184992400037437056519675110896623013805802069350925794727590\\
&820896465283358215002233294319717031444437678528584021813028598207757014505951154837 0\\
&152453967247879540212044122583577715100766366785248752239808120798065630723497486623 8\\
&77795931748923750913392181747378526651118473964838023986850\\
&64422448767.9999999999999999999...X^{10} -\\
&909474067895683378810285132078240966226505709872181887965916383224362761281040843599\\
&128493089924850288390052933150041100514048768146122177594075145031301307702979186284 7\\
&775699652228749773857041129209691537236611805644260252702112118826954636958546475488\\
&422851568478475261793582907892754103186334396853246242122169825193362075184869603308 7\\
&8166440270616746274345798028675702456027.9999999999999999999...X^9\\
&+ 176739211755797998563653104637832269737532689739418149012469637060044787235820915916\\
&880670127291040115175383234682663352854957205628912681549433322236419550437768538484 0
\end{aligned}
$$

$6270994579567105826186628630022334483776702764466446067465765073740430659624243721013$

$3995310945813119367215129500442393535731351514208374899864492110122831280776853109887$

$2232721956.999999999999999999...X^8$

$-\,65274757334172621479128510263463237191222269239121501908800436848962885124912 6099$

$2356410503251533197071320985431238900026379909638366238936828447318242566479079755298$

$4271003363630879810830587416416880997880556244386795556435694803174806463521568668685$

$0548631710603022252698451842868508226703884547724700749139$

$752145077.999999999999999999...X^7 +$

$6744021837689285973643592359276310834317181369396656322433294280938617222 0$

$8202893128845163762850394102799060156012499261529400885644584178167369937304103710323$

$1925425582417118208469836230889537822530265640633892485649784491041654311559825288768$

$2284211202099582256077372425824895429369319.9999999999999999999999...X^6 -$

$1025126431787393766526278523671634301432741812966804454565977365590147800114067463154$

$3867085330526751988943702226653381050931226202182806548258736102222544935001492417398$

$0309116260824256363205432630135532227460183269861456311731966290752888$

$49723174311.9999999999999999999...X^5 +$

$3895616738408948387452492067199750820294391411243785437186808708187635300231802548611$

$2811896925417145106942262817253314633511638023755800217943816178217969183157822943 49$

$1255864594969703607587648041602282351424049 3.99999999999999999...X^4 -$

$1919477621972238921416569923816738286616270503347859689882716712002476643106377753236$

$3357027201809923544166917503835266360259733051369432380094595343098 6$

$68329951.9999999999...X^3 +$

$2759195015225947121386622622817076298230828468678209042668958020865811100023772635242$

$235329885506112480130 03.999999999999...X^2 -$

$9725119391640237294676247676043381733577096594322186 31.99999999999999...X$

$+\,0.999999999999...$

$P_2(X) = X^{36} + -10539610973350350739055186701325843544449807625408620851523138 4$

$8962040818.000000000000...X^{35} +$

$27770849867391781929153039123424870200502519195159225493647320919842008 16$

$2255027094008168821939260943018737634947285819336470648408380302 7$

$707912.9999999999999...X^{34}$

$-\,443031186847279900384751307950190509972876664645436603091201672663 98$

$328507586815778745045238775196878181746855466988401029075529237875580382$

$3083385780057005333105063502390932593708031080 73.9999999999...X^{33} +$

176693037355891254273323143703633528959881636956778825389053993886

574361330101078950441893914805001001154219295199549799824378107250 66

046744370396635375983085692646970537862330064073956423168297287742219 42366

554374835898726936353471.99999999999999999999...X^{32} −

118245613631805832148856824695260705266257885134607987346024885714514899678

176750537049883090503527837025590471059902844954818523209405684251889015 8314

363186525969298480614385002071990818294374699259066504293268419956854973 1606

206576728481924016953785044039981665 87.99999999999999999999...X^{31} +

197829349674215746034841717028816910979437084189003383749819652302867196 1996

005769427730405407273553703690433505961560132089854762069408810804766455 65199

439529010005353803388958613801395057673283200037191823467678828430027794 9514492

255352431807791440736220394110670888459628153848606026065628508 04.99999999999...X^{30} −

110098691964689384232649944050329774378576574586395544612210985246954119569455 4798325081

825923552716939441372131157911582913661762170659289930603394932652067373188 46704

698948905335053823315696792136741456647721179027003805013772244142995792886 020866

062662916391622852789395239936636190579552691900938377936514261 65925

057939.99999999999999999999...X^{29} +

244569892095091938314892448208938554039722356072854135212377617586443435295 1187

031881847417309742184860512686220370224113391756995473000301549822871951434 80816

700399767621812158037925424839518777862359565912588756591440089949735092549 9524464

512912237427414742863726496297073833534375479822052730106174422447999541680 1980982

626342535834795146272 0834.99999999999999999...X^{28} −

274365573560347241288174464136851979484118081359095443549569753294940965 8663

429195537590532690585714627579052010736384406792449715211830899443498069 30808

111209338813916156649117637047080379691004590639062772914726090816222586 0972

681887532383801172112925812063475588805233021652751637749047645330208 6384

602610193402447109595053445789504534102267658753751416822957333 78024

307.99999999999999999999...X^{27} +

161383336641076345645607971768242688116496045113461649766242592646640179 26930

928966218958385895844971621398414514983675560806018314570324869426678376 78458

037535821502264503791155247624809314477595432404288625890699097092775555 748739

956729216538339322398950227124445025992932357641918834159111777166513035 09943

041201476618276464439783094082410668369611847438736854329

640013482312248290665488524446 06.999999999999999...X^{26} −

4635403380089426272687801176816126323523597073205882181607656464952804237
3

2820065452878800802651215329886659683529370874026799858072192210761589694
0

7557348797264350434624170333311386448593916248724827383186010194656976103
38

0203646762359250274389971007470995337549320956017653762797902416489118786
94

2506575306700494164103368869811313142972294523028311964394881712745092544
68

$7738895506943737011348991811767905811768733006359.999999999999999...X^{25}+$

5089906311095125042379604615912120250765626753240998848905081146336686861
65

5945473662888812225281816857351388722580602029810931346530297557313091647
86

7468300786831301105125435160797550664071553338334394638816454300450927336
61

7777636904074263176602159501417980859007538637711136389083127731633054913
821

0143474462637441083642289383419966206737708257950481436078979321417595347
820

$756082777524554900525566788329116051179378877188854154366370240913982.99999$

$99999999999999...X^{24}-$

5398119935249082433570676523479132330706396424724716453378713669237476845
78

8734699180849758842401074787620140528731948245702262735095285899952985602
3555

2687177840055539914947106344057255369974108447567317902898711216738769939
5549

7181429163486515190178070188426071758706112112322076314213661207822704875
63732

0338158854852402034471310280526569479591017220360317880949281961093629033
094

7314051691673665110720908485740060737281681540348609065189872660456078838
341

$000851.9999999999999999999999999...X^{23}+$

1587941351618584928082215736422933903880348506182052121575672063010133646
23740

8603950699437258119398797754848594984798527674225391992367398716199141512
2803

0864106147308003122046568701138254831477811456052865514162654009693504980
6061

1800590225470182951052160847431669704383215379132091355323321816647043480
822

9035033913403366851484001148848858511672796887762543236185242090703374670
099

1764400675932782747130231194120545243089720137701989926563913343528355732
85

$1065392611791705437738111.999999999999999999999...X^{22}-$

8308712221877523088156990053528236708613978193396102432559314274627119526
7514

2667302213178988768845621139166972670629627810222471885420790416756024517
60220

5804334383129435306011360371730545045441897236504685753208367388545718678
2895

4370018346747410754143169883114482532227890389324020008667373150266592813
17426

0730037099326550952394634397980189007138105169271123492878198129100039112
6606

5551148176989813838737021983482557462695352294137620832434469873559275278
7362

$0404113459525738185766055685392242779.999999999999999999...X^{21}+$

12058413747553225959243228120880454249190651249053066169471041063886742879578
89920805049429751273161780809729692406981449550085427823351034489514240859502
805750564714655292704598832696965457235206015346841311680383862458006867991190
11274247617426689085269580563111930239335241523331476182910238513375501103660
56033106309116207947677551220525288298139562962055665768359229616434816293430
47397892155696372210270967290882881944923523864400234876293924260407452854168
58879715928516944145821616787877917806811948551742478033.99999999999999...X^{20} −
30408845768620420460436103032356550815971953099909312700522659179592216853526
8099076525173343039018254095627443853016104595773215964888366546396299034209101
82341741299532229863234454409165457246349784032948001875737300845790388810441
179332786445057865355239102795687346648252856594249002097324295926654347367547
6484759460181704506105345486002842777917607257699930828813647252240554421554856
4819167560004996275048161732986190391793319472001798443796326305636707406548
486015637394930536385544982012865229777221573707035475082579.99999999
9999999999999999...X^{19} +
19171217876828517350920034192510403932606579976687109767673185665043316
42857140837326513073158596050471641890163176095650084784480066852273359084
523597517396906977564458173852347999713090882391214362956566464526595315987
002960658253514596884313472583135074775410859355587659180962871141232196112
81148549423616923523727854051750643655512310509797381272066899688833219652
22941176791700516866834086047730759226696627264903719111974069341347740793
3346796253072758333211360852236453351143263493857586931155554706510903699
293442644012173667.9999999999999...X^{18} −
20267635193211038660167482930342781659442177732446011975433233033200793517
240214441822305860400496331212020602700926943202919916867700463798359465494
53291648234372395389826749892593491412495859865033659553247381702253817095406
6813999114377538517874638835478853796505391740698279206309078512865411534254
0310284672720683829695195304043524346894439330258507457832184329349679413916
0191788871081360341641210921293415253067061361196286915232784527325387004278
8690874315200401710962434664778746031530742529446119813717258850871085685
48335.99999999999999999999...X^{17} +
5356689418590725859787255122820022267215295890256929328293815474068372549976
54566455673336950362367483706956759489548969263102519284901868214344418514718
809548660043399015127835806376952443270607828987158615621148563280772101488790

5091830942610466824061917655870505472317951992559053287752440728103925047860000

17753936406946293752720695083416485718404898202378160665402345784333

8230181267627282895663559652787438980952064375107830666234911154270831538819495555

74922203615520479417389658848518539950890087595439198531453233

$66326054789.99999999999999999999...X^{16} -$

10136243391168502885243501992024597715470732957447532929189701699148442743

476188899134158168329245697978375035852319122271210988057558184629562437384

52937786896548943538727491729043834987103074729550632478388835947281413856

891720708181233974020886358416347966800689038454223408799979023757026277749

69483898886147908080938455695729798445567396352165410745272969539542150132

3906692782193168126440197594782655472201612260017243598381911781679792882

206284212914103169415017789647384306194603474711104666

$6363808090.0000000000000000...X^{15} +$

59721161492936066593669336726847798596152542824393514318260531323566263014

852855338208627456007804616774533353693468311157058720804564117011016387213

30762707078399979461985549170100998537836301395496168276005359879139732904573

35114316842438028649785202824185780001581733413135760817777695752123302852

50452671550173139432633671284692712876166104313089885470372688863820745933357

519610111026085810885782222913424139055157160452000346488215196073238994104

$4810224363754993372744391909179990202 2.99999999999999...X^{14} -$

111361035113030029032738024590529431560899640677321107018240769034672273741743

8226505581376969516733758033797611016662688342818601244749599603735274792480232

845667477767832067316404180473198584378595470367989308622414979793263434793978

1339567422408454049015932482804260733609836359618526432805751153521819662885462

830568280631389854086596494042229739938070329085392733580537992354967632549904

7193767246447776311260084310679982188840699742738575106915736682409222629087

$3748090.000000000000000...X^{13} +$

6465601402186598739007057334906139759471710315645952726680769090528324225046

434439995839183652801873213820857474123501094895110392993308551273480775796356

404617553027286831394212028239664108296934702876679517643917484358837428132533

6173368675856897314816609364081473496161061565605508477891624460877163701249288

91259012718207209390103408941786980646157502078891952679249099700563831656855

82553405558286443739995057763421377144557320465850068610815480247868686

$70797.99999999999999999...X^{12} -$

5818605356870885651866318880487971181745757048428154704869932789216597459

2468912763190560401772463030057613859389834376371420574333526694489232236588

31214141072433096676317819069803384666655258165369478486209151280518098811140

5275758992553657730178498000943353364790552659705704820534358679388644001403

035373581027625253348506864258375361041508804236879444315560570510433993164

1385753131156529733729911069242141468210398624282

$87566917.999999999999999999...X^{11}$ +

13111092561970538891760783479131902428133444864812516773297504001652723038

25269552343830447723749807408808981849924000374370565196751108966230138058

020693509257947275908208964652833582150022332943197170314444376785285840218

13028598207757014505951154837015245396724787954021204412258357771510076636678

524875223980812079806563072349748662387779593174892375091339218174737852665

$111847396483802398685064422448767.9999999999999999999...X^{10}$ −

909474067895683378810285132078240966226505709872181887965916383224362761281

0408435991284930899248502883900529331500411005140487681461221775940751450313

013077029791862847775699652228749773857041129209691537236611805644260252702112

118826954636958546475488422851568478475261793582907892754103186334396853246

24212216982519336207518486960330878166440270616746274345798028675

$702456027.9999999999999999999...X^9$ +

176739211755797998563653104637832269737532689739418149012469637060

04478723582091591688067012729104011517538323468266335285495720562

8912681549433322236419550437768538484062709945795671058261866286300

2233448377670276446644606746576507374043065962424372101339953109458131

19367215129500442393535731351514208374899864492110122831280776853

$1098872232721956.99999999999999999999999...X^8$ −

652747573341726214791285102634632371912222692391215019088004368489628851249

126099235641050325153319707132098543123890002637990963836623893682844

731824256647907975529842710033636308798108305874164168809978805562

44386795556435694803174806463521568668685054863171060302225269845184

$2868508226703884547724700749139752145077.99999999999999...X^7$ +

674402183768928597364359235927631083431718136939665632243329428093

861722208202893128845163762850394102799060156012499261529400885644584178

16736993730410371032319254255824171182084698362308895378225302656406

33892485649784491041654311559825288768228421120209958225607737242582489

$5429369319.99999999999999999999...X^6 -$

$1025126431787393766526278523671634301432741812966804454565977365590147800114067463154386708533052675198894370222665338105093122620218280654825873610222254493500149241739803091162608242563632054326301355322274601832698614563117319662907528884972317 4311.999999999999999...X^5 +$

$389561673840894838745249206719975082029439141124378543718680870818763530023180254861128118969254171451069422628172533146335116380237558002179438161782179691831578229434912558645949697036075876480416022823514240493.9999999999999999...X^4 -$

$19194776219722389214165699238167382866162705033478596898827167120024766431063777532363357027201809923544166917503835266360259733051369432380094595343098668329951.99999999999999...X^3 +$

$27591950152259471213866226228170762982308284686782090426689580208658111000237726352422353298855061124801300 3.9999999999999...X^2 -$

$97251193916402372946762476760433817335770965943221863 1.999999999999999999...X$

$+ 0.9999999999999999999...$

$$P_3(X) = X^{36} - 2406464386389170129394221071694993222298355204852212616883081323193 6.000000000000000...X^{35} +$$

$1595726284114729204562729210009462193993953331116050144287270766445559467906345698954034916320699325112405252581679324589224000289568 92.000000000000000000...X^{34} -$

$178028518743796308125950833819354208358098164216406932767712037232617221579148674766547414526363847556202832947133444465948533751431779566343122929892951463362047963995790077790151397525717118485616080.00000...X^{33} +$

$5472934858782283870631192200195812179924079411531371317624535730539396143980851281478916568214307265765012554080222169773949797242226473101870572733572460600114939579555889125016187277752481738787519120812761425189675465048367295308996648354056884330295954963167885 46.00000000000000000000...X^{32} -$

$27429260212073484922905824276732610776309185128535163584204511339613825006998570541950823491140675220135291183038171099886297404125559639131185031359178045327664592518655073219977826166126715330402496481135419824634588788812139626744744658715347136338818674389128999422833987260301822258371945451354358109028790 46.0000000000...X^{31} +$

$34367498800254466187192214802289080747739123342843998347694786587193628597 93$

5134950923917995172128169819323436173478276089619813965361577041342774708445

5090801762283178202937620485748829965721521638170666244185995364604676453 8

568357550697063503535566797225844568725979615570068474780728462562384640357 2

60142923172020180103915764102371852635785720886132338804080.0000000000000...X^{30} −

1487011444126533907518535800280260670214179828038864022563880080198112896 87

294589638764388375877863797623135548306041165257204446409850149227466289288 3

046777498753582385463627953208041479296809943769408955693767664425766203461 79

353828589384444073688479353814555808400826033458623651618187840254423986483 93

244958706842220081441751793794329909743289632112580638058957031316841800676 237

950657277727334.00000000000000...X^{29} +

171245320006634550172848659455034496787055688558364100421878397649717004142959 1396

558042575085257767284592914335755926491382138885897118887513142060609108688 09

548877737763125276661624121181201719756811210983058696919400305228448094305 742

836841321475946750958652842735496170939701857813735424755441189878090245951 489

780852754626051439009907405938307534245594163723560199206814980280355348721 378

2025189545859517879483581225034092714927879.00000000000000000...X^{28} −

224895857777814526955733443433189753060398671860994174427349542715994513019 1231

260073614271916439315285041737571625831749834227217482635520686666830903797 9398

678859147968343657593298891222691267427010084867916751556890423227085284757 679

162189215549684727209333777027750887755237670593960331325173862022630667578 2200

734359868736133851180837044926888958250620965352169687472191723784537562089 77272

48309238899891423635567919072977932729418899938758641301289889474650624503 7

596.00000000000000000000...X^{27} +

786294887684746821571138407617254664563691273112253520211230634824206665218 9111879

475864259101434666503120118305848403307795652501733784897679825454762314886 6294217

098212433170747572347262468775683351484897712183162489317097546072234501990 3798061

070899847982711012347816937976997091345679740975891228476773423998673459208 49952705

105485053347212953353704058226325634730936060257628908643581360106702821828 028986

080407936518111860295796593648778869093604552234883966741634129216027708988 37453340

2676565071216287.000000000000000...X^{26} −

135020574670345872027591656788257526881771718674167238406711158629069566664 5415013

448637630220440410976114131308993658126632028805339744693099166462849706248 624080

620016813133129669654317632493845312725843437786769161703595295013716719173 650775

025042627653761574595703936066706320999003343132876720350240406495565145772 7092490

274141410153288261598406483139571714337687310919263018951924098354068703786085820
40190214179701755809511917787238228389472677541939480906015124284705590526324810
95678160156745988896364129522634530194697163096030876618.0000000000000...X^{25} +
579777224309996847689204054340610259100271018987027284522652064685083570982232638
016604025717607565288310047643774578840842050898697063086780887549349953775940810
492161621544866669896024962675783555402649389566991694270987616096262537845497121
7077991310322306870743144972784349475235851240592429999574370530074710914103385110
6803636261642020913313697349761293432435274401786981252486112791937201768136904519
2638649590615542655487400028843817293342940181335202917884193914955509267165994896
5004138793338428495247514229793747409988503122595489971317715828120694928935820513
4558.0000000000000...X^{24} −
277550252803765601244769074448973127151272984492396807657236224311199527136308395755
73174366958405196862297123459814081644071641659581761060384921705578796802474341392
07855121371388107767396380134825393544075686544689351282101187634628524486928867676
84293677951173711150592202509159123002017352583036314612197480420388509038218589331
64461524231332797028074164524407498850318622343879501001555206259186601283281085972
16540901529523083022823456412441033201806108760527891765420784920496424787650798809
01653071032172684032279039906807813095064714663541293605912369829440583071769791815
3157355232544986.0000000000000000...X^{23} +
390143649073387235730548493511021548110061067034871641964756416270881091358221380832
029921259255481409327980168093660717325929757743062573096467778774883794427383817073
266565081956520153887093922636517654682090426360045420461457162335084979266691341870
1765879150498643168419468842524802971089634450090492671660328095557973987301374042
375517212176613245593232425357785057885274473086777141672741471233972019683863858247
8784480564050931481246622046785187955139951254532571846122588781897729619595358998
29598772264195793483073795009992467261755999740418278840753679857975653327267335921
4847503894314917624314279176816148205.000000000000000000000...X^{22} −
13876225330015935376747544290180634281430637976621153697906926415031623794004567927
99860272624304257019730728452172157572736098255459414130109890403427342828658177494
477533124377588951938127288201633705312806201137432234724744369301726594263063838284
81154505659159242373888017695610992545275438133563359871303660744232304016198614414
653966601298602122781655097705551091923790584176573823662673641738724517461487963035
865861861247180129906769176868374382414978297549540223825289698575508259045315449864
5173412841041199555519980097654463881218287222930643691345887740033254978717742424065

0765499164481023415686077150958397150206524998026558448 0.0000000000000000...X^{21} +
144917416579149590686631540180204500441879783435197923421508897671257009124248897975 87
562063569031802823211266308370905619880944246572251253965107501908740329318284810335 2
481540789449155877748437827708183129797219314958885658307922485352058854230191881450
476626590562240038257480389354546934446944665198761287483727655912121619607538055294
715177814296616475531864960286317477979610625006409327735506671042619426581751927131
494957259628261537554541741325474549663275032898935132626747461891632330967394244909
535759880278308725960083665825535424010885132510472556761521033339176009871399934 92
892334116497544880902470293753337078967648396548157854834143448 1719
920011.0000000000000000...X^{20} −
114352679944609717476743233736481473895507894115350273064979418098182134537627318
414594384514761245087659155406373732100982308971410767360687950605219456261865763
318495292872880842998288309175154707607241436306335589788327714290525029388134522
713472152418134796803722254873305059278323929015548431587189951343537215159981016
773228699240592482676832702393129600380164719374744010598371206838889219160915523
784156611966713560411485201731180865137579419041621690264615572380503340697583174
825219046526441358661877229452566022512623248987236980843585779101870555896330571
93831406708363417882110109412625794311106715554571679804716949315354423547030 9
51483348429993104772.0000000000000000...X^{19} +
225585987524393776546420131409326222831095342608396655459859894911167008348178912
902971907151271867330241292963009091986571904857724164373490870731792811871305469 1
839646984343452007672576028281385382046999886500031055589368841812644066552644160 0
479747176526627221907885415616709050747628152210634177500511354145973561997299907 05
449113128398742287116808881963376827759700756823018662237558288098014945803776288 6
448829700443549595092033913733874030231342299837885936549340393183130139244225512
331989011336457943065535146813481090169622346812704008869986850494259220510633309 8
683804686539744803927002865978833488351445568613368156614273633741542782048920 18
0594126601207.00000000000000000000...X^{18} −
600471526598053769498065254943793131139164393447946013569403157713431352830739574
056881010149310952846365049304434783019457630193943325289376052908256140964427078
677280827171116187253239385817741582520542911178642574948897180767417047034862019
952822382456787469953336676272189360917044667273262469909419931593006135484905942 1
523264824688519394072645785137267541024437903262282451631154072335233905767475862 5
393400172779118142486361979166221122179554307604148073986395664182647038692085655

7411331830561956105840210086096760096846511980245234161013564479876674580110

5488089104959751973772683058772195310389620174598530597736774240793374574252

15028622308091035.9999999999999999999...X^{17} +

3995882659161289574976283655965092664769417882361058576055097919292960238735561

3704418002801866455956683373058201967813338701763010401309931696485172093059713 3

2786172477747532474437905686265708214286233949678432948540139394437666097926142

4361557992882590800118579818971410755668026248230226788999341661378095741649 08

7410473181944896365354204252412300381749612260932917198767881207673450664083 94

0465149274174417445628310709870260708509637567570793672770129596038175032354 2

8239858642642695276205531947027416338547972071442562679121074490002371219524835

8738796341075722348384185426419462378196339600973085727386662959094508176024 5

7520316394778428977 27.000000000000000000000000...X^{16} −

1134517026740990420310489493576726738575489996272669749601459772550035180904852 4

2085595136510471543049221534221476500651433806506898430426144196288618973686 7

8305815894811431090296481879608501725882675834172856066315233190011661233824

8803064312886579640310346385443800634467054861707175741619128938998371000387 24

0109635949205506442672418252821523539414303841163084421253217905873298671101 81

6054897833107538539501045821448301384606655155697975240478744083992600444777439

7083503769829544042305850684174664546412002076924950712806336777346332115050

8807843770106999729657397324688178366495762781157758035862441431640024320104 1

394494.000000000000000...X^{15} +

8518996424162506866024883506849190407865570997022262516668267983302834141355

0504605927964219199624986433918766835250825859101951657790100007480140930582

1574254550912333739044048756990846478180906904839397598322238194706220130840 8

6134155136240696975262220580127588001538963591666359549586413532868891636848 6

2361361360245979883699844125208464132107202926845886419196091049336870063498 97

0750603206304929532034717697248383139849711341287638567346106095690631122921570

4895059088351172693485775877134649943008578690452921348185289678129070777806 9

94235995350919122535165233223931153578821950449093777384 81

244078.00000000000000000...X^{14} −

66175264184508928562274899215743343392438805709892693860274074991459976116685778 49

1690314850062977827838789169011372289098285285326720485020358610712513436155 63

7191116515089601237974222406562407619397292142280291460275597450475335029710399

0151936769958893597876047859023718985656968481830410772968624774069098741754912

1198184775679433681400696410108097040534619009719507683489216015969893857831753 8

3545818601493660232060459023282829226031431740375747766686956172133306089838797

1027024100766461878651228727587087974991438604725598851966206487932603968560 55

3253135891845500429180967 8.00000000000000000000...X^{13} +

135950910228573910245619538874836757724129434703742980251640524686290438

496871909101065668107361384692999446779252590875550770728236852092406934 95

331712569902234361285088895921041726347518072589629709538922891479 51

041840556236296271908979094339057450536655275755253664584408608629768732

627325645478688763524081400895949086731925379783775225824399209511858 9

05882391698628636016013800545622412792379043924984570016664898558488188 7

349820168054924347897377779990957010093015294684460666880939364503526 5

16278162079286478297925195337447241268153048867752 7

507848559.0000000000000000...X^{12} −

819682964214547056992719404381478433216517867397217592888842541819738

342193063153740553066411292836044429514323882089087434550192735627 9

104549424968641733506360614435320416250088610068526497896648229703

058833975370420792690477906601852466377835852252389814138738053247873898

895226140751603496338082633327218408421569298344878150016877 3

065882774056015187150319276001180662688818670585896581360562018 53

234758284619489329866033814038533201930365707443955173254231857161737 50

680327357015728412826837263453548713943261333522607 24

550.00000000000000000000...X^{11} +

180399963598756220747502594736176300151211594483663351894658885 76

531209921878780710321634097656103116900207633013617750593959229294

140128409668505229687094689850988597771603821751724551018904075962

276139348734575844859596878183902403258351784503052021605531581835

034636535752228390519143617058075592003069286367312298498608291702

402031462763350503016282309718620719962438690869163361668228757430 8

668857513936136532573186041030122111143197070322946861071693979695

671907552650554272971439072130050 09.00000000000000000000000

0000...X^{10} −

182670956843113405502285131031824422856129421281674877307496623615 9

162075922480937025554957473405539579250673853912025189135934321510 1

755686763389006222013082262491316988118730017018307513244469532542 2

4339834387412521868674518472745611073783431658759916419099460667231420539542341459048879969268862866629763823862499090486906465680275584908498503976681762330562033566437843926426697857403829886494132076264879974602615545285650074835993990744447651962283240162185754.0000000000000...X^9 +

93479075478851752320002772351696919610883080319453089870799837546078876388296426337963136027678778605331647811893649357350562978398070839295755758389130741841994397928618646674858215387456675479915939213507719075632405369180429395420487488657099455766283779123077500844177884409476292744296171865071596496926725760454504447395880502639085643886000359364349643853542692443888667641653913709455911126159826422523925418179154686830067072.00000000000000000000...X^8 −

236159568135318764994616174107978354538070567097252418448351115990430253782518536384290869055365647902574571971794053048830634590047190569529316409624557903868473163185748366499539473766246877799221313811527088753284571553416469521228075535787429013027288030854818063538639189635291834407590252941876412240211978863134120761468558844431646405378329790086139139808395626171937533528410235240074006891137800000000000000000000000...X^7 +

234619024918022407819044406857725286005352982321851960168659627957296067390332512237669772542511405819426723199173295407744863882977938903565054298665575864850334017149631346360724185916245017602528618692636180162040775942992513540106869624662145064149788114838563864792674945586140932974617774838685969278503473153166949091971633711264968234889433573977549061133073991900.00000000000000000000...X^6 −

10368686785999052373406710480057299699540327576286864389173924398335246126929792793835875203781949258202497211328596237655743449851682780371387500086670092740938891449776195522496378777992696932799657007866473168548625042284205018838968762136056238145614092852567089057436010664406742011512403632046871268071132620593019142343223180000000000000000000000000...X^5 +

114557702580640856805484300982801127535444262136834596118306321415304786734017911562600299945152840691764560641478302328343666677780703552203571749317849843254689636513092905304976505666333160495001075355138113111

0165264274999226693332970441833399650150964484640674774671604778017777

99807209.000000000000000000...X^4 −

3039382614887056117772115898946007944754865882160706208549154115590576770

5882985480768389614379272330878601274781701304575553531512717335598750

1711636860281715433251942908703130059510479530883969634078777703243030

30023271232281510246l6.000000000000000000000000...X^3 +

2015981132559587594135125685403431560511283940800605998939443219832982000

5667630742881765303775495382816182643990532786361733743191705339282527390

2604500088027326298074525620425025020.00000000000000000000...X^2 −

8979935707029505440444917700184232016547111711884766469624939333058092520

599781219837593748.000000000000000000...X + 1.000000000000000000000000000...

Bibliography

[1] W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, USA , 1994.

[2] G. Anderson: Another Look at the Index Formulas of Cyclotomic Number Theory, *Journal of Number Theory* **60** (1996), 142-164.

[3] M. Aoki: Notes on the Structure of the Ideal Class Groups of Abelian Number Fields, *Proc. Japan Acad.* **81**, Ser. A (2005), 69-74.

[4] M. Aoki, T. Fukuda: An Algorithm for Computing p-Class Groups of Abelian Number Fields, *Algorithmic Number Theory, Lecture Notes in Comput. Sci.* **4076**, Springer, Berlin (2006), 56-71.

[5] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier: User's Guide to PARI-GP (version 2.3.0), Université Bordeaux I, Bordeaux 2000.

[6] M. Conrad: Construction of Bases for the Group of Cyclotomic Units, *Journal of Number Theory* **81** (2000), 1-15.

[7] P. Cornacchia: Anderson's Module for Cyclotomic Fields of Prime Conductor, *Journal of Number Theory* **67** (1997), 252-276.

[8] R. Gillard: Unités Cyclotomiques, *Séminaire de Théorie des Nombres* (1978), Grenoble.

[9] R. Gillard: Unités Elliptiques et Unités Cyclotomiques, *Math. Ann.* **243** (1979), 181-189.

[10] R. Gillard: Unités Elliptiques et Groupes de Classes, *Ann. Inst. Fourier* **36** (1986), 29-41.

[11] M-N. Gras: Méthodes et algorithmes pour le calcul numérique du nombre de classes des unités des extensions cubiques cycliques de $\mathbf{Q}$, *Journal reine angew. Math.* **277** (1975), 89-116.

[12] G. and M-N. Gras: Calcul du nombre de classes et des unités des extensions abéliennes réelles de $\mathbf{Q}$, *Bulletin des Sciences Math.* **101** (1977), 97-129.

[13] T. Hakkarainen: On the Computation of the Class Numbers of Real Abelian Fields, Dissertation, University of Turku, 2007.

[14] R. Kučera: On Bases of the Stickelberger Ideal and of the Group of Circular Units of a Cyclotomic Field, *Journal of Number Theory* **40** (1992), 284-316.

[15] R. Kučera: Different Groups of Circular Units of a Compositum of Real Quadratic Fields, *Acta Arithmetica* **67** (1994), no.2, 123-140.

[16] S. Lang, *Algebra*, Addison-Wesley Pub. Co., Reading, Mass., 1967.

[17] H. Leopoldt: Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, Abh. Deutsch. Akad. Wiss. Berlin. Kl. Math. Nat., 1953, no. 2 (1954).

[18] C. Levesque: On Improving Ramachandra's Unit Index, *in Number Theory*, R. A. Mollin (Ed), pp. 325-338, W. de Gruyter, Berlin, New York, 1990.

[19] J. Masley: Class Numbers of Real Cyclic Number Fields with Small Conductor, *Compositio Mathematica* **37** (1978), 297-319.

[20] A. Odlyzko: Lower Bounds for Discriminants of Number Fields, *Acta Arithmetica* **29** (1976), 275-297.

[21] A. Odlyzko: Lower Bounds for Discriminants of Number Fields II, *Tohôku Math. J.* **29** (1977), 209-216.

[22] K. Ramachandra: On the Units of Cyclotomic Fields, *Acta Arithmetica* **12** (1966), 165-173.

[23] J. Rotman, *Advanced Modern Algebra*, Prentice Hall, USA, 2002.

[24] R. Schoof: Minus Class Groups of the Fields of the l-th Roots of Unity, *Mathematics of Computation* **67** (1998), 1225-1245.

[25] R. Schoof: Class Numbers of Real Cyclotomic Fields of Prime Conductor, *Mathematics of Computation* **72** (2003), 913-937.

[26] W. Sinnott: On the Stickelberger Ideal and the Circular Units of a Cyclotomic Field, *Annals of Mathematics* **108** (1978), 107-134.

[27] W. Schwarz: Über die Klassenzahl abelscher Zahlkörper, PhD Thesis, University of Saarbrücken (1995).

[28] F. Thaine: On the Ideal Class Groups of Real Abelian Number Fields, *Annals of Mathematics* **128** (1988), 1-18.

[29] F. van der Linden: Class Number Computations of Real Abelian Number Fields, *Mathematics of Computation* **39** (1982), 693-707.

[30] L.C. Washington, *Introduction to Cyclotomic Fields; second edition*, Springer-Verlag, Berlin Heidenberg New York, 1997.

[31] Wolfram Research, Mathematica 6.0 for Linux x86, Champaign, Illinois 1988.