Evaluating Zeta Functions of Abelian Number Fields at Negative Integers

Dylan Attwell-Duval

Master of Science

Department of Mathematics and Statistics

McGill University

Montreal, Quebec

December, 2009

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Master of Science

Acknowledgements

First and foremost I would like to thank my supervisor, Professor Eyal Goren. His guidance and encouragement has been outstanding for my entire tenure at McGill thus far and I would not have been able to complete this work without his help. Additionally I would like to thank the following professors who had an especially great impact on my undergraduate academic career and without whom I would not be here today: Prof. Almut Buchard, Prof. Stephen Kudla and Prof. Dror Bar-Natan.

I would also like to thank all the generous philanthropists who donate to McGill or indeed any academic institution, for without your support the pursuit of knowledge for a living would be all but an impossibility. In particular, I have personally benefitted from the donations of Max Binz and Lorne Trottier during my stay at McGill.

Finally I would like to thank all four of my parents. My success is nothing more then the fruition of your labours.

Abstract

In this thesis we study abelian number fields and in particular their zeta functions at the negative integers. The prototypical examples of abelian number fields are the oft-studied cyclotomic fields, a topic upon which many texts have been almost exclusively dedicated to (see for example [26] or nearly any text on global class field theory).

We begin by building up our understanding of the characters of finite abelian groups and how they are related to Dedekind zeta functions. We then use tools from number theory such as the Kronecker-Weber theorem and Bernoulli numbers to find a simple algorithm for determining the values of these zeta functions at negative integers. We conclude the thesis by comparing the relative complexity of our method to two alternative methods that use completely different theoretical tools to attack the more general problem of non-abelian number fields.

Abrégé

Dans cette thèse nous étudions les corps de nombres abéliens et en particulier leurs fonctions zeta aux entiers négatifs. Les exemples-type de corps de nombres abéliens sont les corps cyclotomiques que l'on étudie fréquemment, un sujet auquel de nombreux textes ont été entièrement consacrés (voir par exemple [26] ou presque tous les textes sur la théorie globale des corps de classes).

Nous commençons par construire notre comprehension des caractères des groupes abéliens finis et de ce qui les lie aux fonctions zeta de Dedekind. Ensuite nous utilisons des outils de théorie des nombres comme le théorème de Kronecker-Weber et les nombres de Bernouilli pour trouver un algorithme simple pour déterminer les valeurs de ces fonctions zeta aux entiers négatifs. Nous concluons la thèse en comparant la complexité relative de notre méthode à deux méthodes alternatives qui utilisent des outils théoriques complètement différents pour attaquer le problème plus général des corps de nombres non-abéliens.

TABLE OF CONTENTS

List of Tables

Introduction

The end result of this project is the development of an efficient algorithm that researchers in the field can use to evaluate Dedekind zeta functions of abelian number fields at negative integers. This should serve the community well as there appears to be a distinct lack of numerical data regarding zeta values at negative integers, despite there being great overall interest in these numbers. Indeed the only known similar work comes from [12] where Goren uses PARI to calculate these values. Goren notes that problems do arise with his method as PARI is limited by the precision of its analytic estimations, and he produces an example where PARI returns an incorrect value for a certain zeta function at -23. The work of this thesis expands on the work of Goren in the context of abelian number fields (although there is some discussion regarding the more general case) and approaches the problem from the point of view of L-functions, which ends up circumventing the issue of analytic estimation and precision. This allows researchers interested in calculating these values to be confident in the results for relatively large negative integers and also to be able to compute these values quickly. Indeed, using the same zeta function that PARI was unable to evaluate at -23 through analytic approximation, the author was able to evaluate at -199 in under 1.3 seconds and the fraction returned had a denominator satisfying the necessary prime divisor conditions (see Chapter 5) which suggests the legitimacy of the returned value.

The main motivation for the thesis problem is the fact that the values of these zeta functions at negative integers have a habit of popping up in many

different sections of number theory as part of some intrinsic property that people may wish to know.

One common example, as we shall see in section 6 of this text, is that they appear in the coefficients of certain normalized Eisenstein series of Hilbert modular forms. Another place in the theory of modular forms in which these values occur is calculating volumes of certain orbifolds that arise in the study of Siegel modular forms. For instance, we have the symplectic group $Sp(2g, \mathbb{Z})$ acting on the Siegel upper half plane $\mathcal{H}_g$ with volume measured by a metric generalizing the Poincaré metric. If we normalize the volume to give the Euler characteristic of this space, we have

$$\text{vol}(Sp(2g, \mathbb{Z})\backslash\mathcal{H}_g) = \zeta(-1)\zeta(-3)\ldots\zeta(1-2g)$$

where ζ is the usual Riemann-zeta function, the most basic example of a Dedekind zeta function (see [25]).

Another example arises in the theory of motives. In [4], $\zeta_K(1-n)$ appears in the volume of hyperbolic $(2n-1)$-simplices defined over K. More generally, the author studies various covolumes arising from products of $2m$ hyperbolic planes modulo the action of certain arithmetic groups. In the formula given for such volumes, we see $\zeta_K(-1)\zeta_K(-3)\ldots\zeta_K(1-2m)$ appearing, similar to the result above.

A final motivating example comes from the field of Hilbert modular surfaces. If K is a real quadratic field, then [24] shows the volume of $\Gamma_K\backslash\mathcal{H}_1^2$ as $2\zeta_K(-1)$ where Γ_K is the Hilbert modular group associated to K. This is particularly interesting because it is also shown (see pg. 72 of [24]) that the dimension of certain cusp forms S_k associated with a Hilbert modular group

can be expressed in terms of this volume,

$$\dim(S_k) = \frac{(k-1)^2}{4}\mathrm{vol}(\Gamma\backslash\mathcal{H}_1^2) + \sum_{\sigma}\chi(M_\sigma, V_\sigma),$$

where the $\chi(M_\sigma, V_\sigma)$ are certain contributions that arise from the cusps. Zeta values at -1 also show up in Hilbert modular surfaces in regards to the intersection numbers of line bundles of modular forms. For instance, in [5] we have the equation

$$\mathcal{M}_k(\mathbb{C})^2 = k^2\zeta_K(-1),$$

which gives the self intersection number of the line bundle of modular forms $\mathcal{M}_k$ on the desingularization of the compactification of the quasi-projective algebraic variety $\Gamma_k\backslash\mathcal{H}_1^2$.

Another topic that is closely related to the evaluation of abelian zeta functions is the study of Dirichlet L-series. These objects play a prominent role in this thesis as do the generalized Bernoulli numbers which are closely related to the valuation of L-series at negative integers as we shall see in Chapter 1. Both of these objects also appear frequently in various subfields of number theory. Perhaps the best example is the relation between generalized Bernoulli numbers and the class number of cyclotomic fields and their subfields. As discussed in chapter 5 of [26], we have the result of Kummer that for p an odd prime number, the class number of $\mathbb{Q}(\omega_p)$ is divisible by p if and only if it divides the relative class number, if and only if it divides the numerator of B_j for $2 \leq j \leq p-3$, where the B_j are regular Bernoulli numbers (ω_p being a primitive p^{th} root of unity). A corollary to this is Kummer's famous theorem that there are infinitely many irregular primes. Generalized Bernoulli numbers also play a prominent role in the theory of p-adic L-functions and in particular appear in formulas for evaluation of such objects at negative integers.

Dirichlet L-series also appear in the context of elliptic curves and modular forms. In general, we have different types of L-series for these objects, such as the Hasse-Weil L-function associated with elliptic curves which encodes data regarding the number of points on a curve over finite fields. However these L-functions can sometimes be related, such as in chapter 4 of [17] which discusses Shimura's famous theorem relating forms of half integer weight to those of even integer weight. In this theorem we have a modular form g arising from a congruence subgroup depending on a certain Dirichlet character χ. This form has an associated Dirichlet series arising from its Fourier expansion coefficients and it turns out that it can be written as the product $L(\chi, s)L(\chi, s-(k-2))$. In particular, when D is the discriminant of a negative quadratic field $\mathbb{Q}(\sqrt{-n})$ where n is square free, then this is equal to the Hasse-Weil L-function of the elliptic curve E_n defined by the equation $y^2 = x^3 - nx$.

Having been thoroughly motivated towards the usefulness of being able to calculate the values of L-functions and zeta functions at negative integers, we proceed to discuss the scope of the project. Chapters 1 and 2 are dedicated to reviewing Dirichlet characters and other number theory concepts that are essential in both understanding and solving the thesis problem. This includes introducing the associated L-functions and their continuation to the whole plane, as well as using the theory developed to prove Dirichlet's wonderful theorem on primes in an arithmetic sequence.

The third chapter is a proof of the classical Kronecker-Weber theorem using the contents of the previous chapters. The formulation of the theorem given is particularly useful from a computational standpoint because it gives an explicit cyclotomic field that an abelian field can be embedded into.

The fourth chapter details the procedure involved in solving the problem and lists some results obtained from this method as well as working through an

example by hand. More explicitly, we use the results of the first three chapters to construct the character group of the Galois group of an abelian number field over $\mathbb{Q}$ and then use the characters and their corresponding L-functions to find special values of the zeta functions. We also deduce an upper bound on the running time for a fixed field and variable negative integer using this approach and find that the problem can be solved with a number of operations that is linear with respect to the size of the negative integer. In particular we have the following result.

Theorem 4.3.2. *Let K be a totally real abelian number field of degree m over $\mathbb{Q}$ and conductor f. Assume its group of Dirichlet characters are known, as are all necessary Bernoulli polynomials. Then the operation cost of determining $\zeta_K(1-k)$ in a rational form is bounded by $3k \cdot m \cdot f + C(m, f)$ for some constant $C(m, f)$ depending on m and f.*

The final two chapters give an overview of how to solve the problem for non-abelian number fields using completely different methods then those discussed in the rest of the thesis. Although these approaches are able to solve a more general problem then the one focused on here, the operational complexity of solving the abelian case through these methods turns out be much greater then the method we develop in the earlier chapters. As shown in the text, if n is the degree of the extension field over $\mathbb{Q}$ then we describe a method using the functional equation relating $\zeta_K(k)$ to $\zeta_K(1-k)$. We find that the operation cost of using this method is bounded by a function that is approximately an n-degree polynomial in k. The second alternative method that we describe relies on Hilbert modular forms and we find that this method has an operation cost that is at best bounded by a function that is $o(\log(k)k^n + k^3)$, where $1-k$

is the value at which we wish to evaluate the zeta function of the field. We summarize these two results formally below.

Theorem 5.0.3. *Let K be a totally real number field over $\mathbb{Q}$ of degree m. Assume that in the ring of integers $\mathcal{O}_K$, all prime ideals, their norms, and their ramification indices over $\mathbb{Z}$ are known. Then $\zeta_K(1-k)$ can be computed and fully reduced to a rational in $O(k^m M_k^{\frac{1}{k-1}})$ where M_k is the bound on the denominator obtained from (5.0.2). Furthermore, the precision to which irrational values need to be computed in the calculations can be bounded by a function that is $O(k\log(k)+\log(M_k))$.*

Theorem 6.0.3. *Let K be a totally real number field over $\mathbb{Q}$ of degree m. Assume that bases of modular forms for sufficiently large weights have been precalculated with Fourier expansion about $i\infty$. Then $\zeta_K(1-k)$ can be calculated and fully reduced to a rational number with $o(k^m \log(k)+f(k))$ operations, where $f(k)$ is a function of k that is at best cubic in k.*

Clearly the large difference in computational complexity between the method focused on in this text for abelian number fields and the above two methods for the more general case lends itself to the conclusion that implementation of the abelian only method would be worthwhile even if a more general method already existed. Indeed using this method would allow a researcher interested in abelian number fields and their zeta functions to produce more results at a faster rate then otherwise possible.

Appendix A includes a brief discussion of various computational techniques and algorithms that are already implemented into current computing programs and are used to solve the thesis problem. The final appendix includes a copy

of the program written in MAGMA to calculate the values given in Chapter 4.

CHAPTER 1

Dirichlet Characters and Finite Abelian Extensions

In this chapter, we follow the texts of [26, 19, 14]. Many of the shorter proofs will be given, although most will be similar to ones found in the aforementioned texts. The reader will be referred to a text when proofs are omitted for brevity.

1.1 Characters of Finite Abelian Groups

We begin with an arbitrary finite abelian group G. A *character* on G is a group homomorphism $\chi : G \to \mathbb{C}^\times$. The set of all such characters will be denoted $\widehat{G}$. The first observation that we can make about characters is that χ maps G to a subset of the roots of unity. This follows from the fact that if $g \in G$ has finite order n, then $\chi(g)^n = \chi(g^n) = \chi(e) = 1$ and so $\chi(g)$ satisfies some cyclotomic equation.

We can induce a group structure on $\widehat{G}$ by defining multiplication in the natural way, namely

$$\chi\phi : G \to \mathbb{C}^\times,$$

$$\chi\phi(g) := \chi(g)\phi(g),$$

whenever χ and ϕ are two characters of G. It is easy to see that if $\psi\chi(g) = \chi(g)$ $\forall\ g \in G$, then ψ must be identically 1 on G and that such a ψ is a well-defined character on G. Likewise, given any character χ, one checks immediately that the map $\chi^{-1}(g) = \overline{\chi(g)}$ is also a character on G and gives the inverse element of χ in our group $\widehat{G}$. We will often denote χ^{-1} as $\overline{\chi}$ for obvious reasons.

We now proceed to prove a few general facts about the character group $\widehat{G}$ that will be useful in the proceeding discussion of Dirichlet characters. Henceforth, ω_n will always denote the primitive n^{th} root of unity $e^{\frac{2\pi i}{n}}$ unless noted otherwise.

Proposition 1.1.1. *If $G =< g >$ is a finite cyclic group, then $G \cong \widehat{G}$.*

Proof. Assume $|G| = n$. Note that any $\chi \in \widehat{G}$ is completely determined by its value on g, since $\chi(g^m) = \chi(g)^m$. It is then routine to check that any map sending g to an n^{th} root of unity induces a character on G and all such characters can be obtained in this manner. Hence the map $\psi : G \to \widehat{G}$, $\psi(g^m)(g) = (\omega_n)^m$ is an isomorphism of groups. □

Proposition 1.1.2. *If $G \cong A \times B$ is the direct product of two finite abelian groups, then $\widehat{G} \cong \widehat{A} \times \widehat{B}$.*

Proof. Define the group homomorphisms $\mu : \widehat{G} \to \widehat{A} \times \widehat{B}$ as $\mu(\chi) = (\chi|_A, \chi|_B)$ and $\tau : \widehat{A} \times \widehat{B} \to \widehat{G}$ as $\tau((\chi, \psi))(g) = \chi(a)\psi(b)$ where $g = ab$ is the unique decomposition of g into a product of $a \in A$ and $b \in B$. One easily checks that μ and τ are inverses of each other. □

Corollary 1.1.3. *For all finite abelian groups G, $G \cong \widehat{G}$. Furthermore, $G \cong \widehat{\widehat{G}}$ canonically.*

Proof. Since G is finite and abelian, G can be decomposed into a finite direct product of finite cyclic groups. Proposition (1.1.2) applied inductively along with (1.1.1) completes the proof of the first statement. The second statement follows from the map $g \to \psi_g$, where $\psi_g(\chi) = \chi(g)$ for all $\chi \in \widehat{G}$. □

We now begin to explore the relationship between subgroups and quotients of G and the corresponding subgroups in $\widehat{G}$.

Proposition 1.1.4. *Let $H \leq G$ be a subgroup of finite abelian group G. Then $\widehat{G/H} \cong \{\chi \in \widehat{G} \mid \chi(h) = 1 \quad \forall\ h \in H\} =: H^{\perp} \leq \widehat{G}$. Furthermore, we have $H \leq H' \leq G$ iff $H'^{\perp} \leq H^{\perp}$.*

Proof. Clearly every element of $H^{\perp}$ induces a distinct character on G/H by the first isomorphism theorem. On the other hand, every character of G can be restricted to a character of H and this restriction is a homomorphism from $\widehat{G}$ to $\widehat{H}$ with kernel $|H^{\perp}|$. By (1.1.3), $|H^{\perp}| \geq |G|/|H| = |\widehat{G/H}|$ and so equality must hold. It is immediately clear from the definitions that $H \leq H'$ implies $H^{\perp} \geq H'^{\perp}$. For the converse, it suffices to show that given any $g \in G \backslash H$, there exists a character that is trivial on H but non-trivial on g. Supposing not, then by the earlier calculation, $|G/ < g, H > | = | < g, H >^{\perp} | = |H^{\perp}| = |G/H|$ which is clearly false when $g \notin H$. □

The proof of the previous theorem gives us a nice characterization of $\widehat{H}$ for any subgroup $H \leq G$ and suggests the duality between subgroups of G and $\widehat{G}$.

Corollary 1.1.5.

(i) $\widehat{H} \cong \widehat{G}/H^{\perp}$.

(ii) For every $H \leq G$, we have the subgroup $H^{\perp} \leq \widehat{G}$ and this mapping is a bijective, inclusion reversing one.

Proof. (i) follows from the proof of (1.1.4). (ii) The fact that the map is inclusion reversing and injective follows from the second part of (1.1.4). Since

$G \cong \widehat{G}$, the number of subgroups in each group is the same. This proves bijectivity. □

The final result of this section can be considered as an "orthogonality" condition on the characters of G. This property will be useful in the subsequent sections.

Proposition 1.1.6. *Assume G is a finite abelian group of order n. Let $\chi, \psi \in \widehat{G}$ and $a, b \in G$, then*

(i) $\sum_{g \in G} \chi(g)\overline{\psi(g)} = n\delta(\chi, \psi)$, *where $\delta(\chi, \psi) = 1$ if $\chi = \psi$ and 0 otherwise.*

(ii) $\sum_{\tau \in \widehat{G}} \tau(a)\overline{\tau(b)} = n\delta(a, b)$, *where $\delta(a, b) = 1$ if $a = b$ and 0 otherwise.*

In particular, the characters of G form an orthonormal basis for $L^2(G)$ with inner product $< f, h >= \frac{1}{|G|} \sum_{g \in G} f(g)\overline{h(g)}$.

Proof. (i) In the case where $\psi = \chi$, the result is obvious, as we are just summing one n times. Otherwise observe that $\chi\overline{\psi}$ is a non-trivial element of $\widehat{G}$, so it suffices to show that if χ is any non-trivial character, then $\sum_{g \in G} \chi(g) = 0$. To this end, observe that since χ is non-trivial, $\exists\ g' \in G$ st. $\chi(g) \neq 1$ and so

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g'g) = \chi(g') \sum_{g \in G} \chi(g).$$

Therefore $(1 - \chi(g'))\sum_{g \in G} \chi(g) = 0$ and the result follows.

(ii) This result follows immediately from (i) and the second statement in (1.1.3). □

1.2 Dirichlet Characters

We now focus our study of characters onto a specific class of finite abelian groups, namely the groups $(\mathbb{Z}/N\mathbb{Z})^\times$. These groups share the following interesting relationship: If $M, N \in \mathbb{N}$ are such that $M|N$ then any character χ of $(\mathbb{Z}/M\mathbb{Z})^\times$ induces a character of $(\mathbb{Z}/N\mathbb{Z})^\times$ by composition $\chi \circ \pi$, where π is reduction modulo M. Alternatively, using the language developed in the previous section we can say that if ψ is a character of $(\mathbb{Z}/N\mathbb{Z})^\times$, and $\psi \in \{\overline{1+kM}|\ k \in \mathbb{Z} \text{ st. } (1+kM, N) = 1\}^\perp$, then ψ is induced by its preimage under the isomorphism in (1.1.4), where we identify $(\mathbb{Z}/M\mathbb{Z})^\times$ with G/H in that theorem. It is easy to see that these two characterizations agree.

Given χ in the character group of $(\mathbb{Z}/N\mathbb{Z})^\times$, the previous observation leads us to define the *conductor* f_χ to be the smallest $M \in \mathbb{N}$ such that χ is induced by some character on $(\mathbb{Z}/M\mathbb{Z})^\times$ or equivalently, the smallest M st. $\chi(\overline{a}) = \chi(\overline{a+kM})$ whenever both $\overline{a}$ and $\overline{a+kM} \in (\mathbb{Z}/N\mathbb{Z})^\times$. We call a character of $(\mathbb{Z}/N\mathbb{Z})^\times$ *primitive* if its conductor equals N. Note that every character of $(\mathbb{Z}/N\mathbb{Z})^\times$ is induced by a unique primitive character of conductor dividing N, which can be shown by noting that if χ is well-defined modulo M and L, then it is well-defined modulo $\gcd(M, L)$. Furthermore, it is clear that distinct characters of $(\mathbb{Z}/N\mathbb{Z})^\times$ are induced by distinct primitive characters.

Finally, we define the collection of *Dirichlet characters* to be the set of all primitive characters and *Dirichlet characters mod N* denoted D_N to be the set of all primitive characters whose conductors divide N.

There is a natural group structure on the set of Dirichlet characters that restricts to a group structure on D_N. Given ψ, χ of conductor f_ψ and f_χ, define $\psi\chi$ as follows: ψ and χ both induce characters of $(\mathbb{Z}/lcm(f_\psi, f_\chi)\mathbb{Z})^\times$. Let γ be the character on $(\mathbb{Z}/lcm(f_\psi, f_\chi)\mathbb{Z})^\times$ defined by $\gamma(a) = \psi(a)\chi(a)$ (Where

we have identified the Dirichlet characters with the characters they induce). Then define $\psi\chi$ as the primitive character that induces γ.

It is clear that inverses and the identity element exist under this action. That this action is in fact associative requires some minor work, but follows from the fact that if $N = lcm(f_\chi, f_\psi, f_\phi)$, then $\chi(\psi\phi)$ and $(\chi\psi)\phi$ are both primitive by definition, and induce equivalent characters on $(\mathbb{Z}/N\mathbb{Z})^\times$. Dirichlet characters mod N are clearly closed under this action, as the conductors all divide N. Furthermore, the identity element has conductor 1, and χ and $\overline{\chi}$ share the same conductor for any character χ, thus Dirichlet characters mod N are a subgroup, and it is easy to see that this subgroup is isomorphic to the character group of $(\mathbb{Z}/N\mathbb{Z})^\times$ under the obvious map of induced characters. We will henceforth identify D_N with the character group of $(\mathbb{Z}/N\mathbb{Z})^\times$ without further comment.

Before moving on, we give a brief description of how Dirichlet characters can be decomposed.

Proposition 1.2.1.

(i) Assume (N,M) = 1. Then $D_{NM} = D_N D_M$, where we consider D_N and D_M as subgroups of the larger group under the inclusion mapping.
(ii) If χ and ψ are two Dirichlet characters of relatively prime conductor, then $f_{\chi\psi} = f_\chi f_\psi$.
(iii) If $f_\chi = n = \prod p_i^{\alpha_i}$, then $\chi = \prod \chi_{p_i}$, where χ_{p_i} are Dirichlet characters of conductor dividing ${p_i}^{\alpha_i}$.

Proof. (i) Since (N,M) = 1, $D_N \cap D_M = \{1\}$, the trivial character. Since $|D_N||D_M| = |(\mathbb{Z}/N\mathbb{Z})^\times||(\mathbb{Z}/M\mathbb{Z})^\times| = |(\mathbb{Z}/MN\mathbb{Z})^\times| = |D_{NM}|$, the result follows.

(ii) Clearly the conductor of $\chi\psi$ divides $f_\chi f_\psi$ so assume it is strictly less, say N, and $f_\chi \nmid N$. Then if $M = lcm(N, f_\psi)$, $\chi = \chi\psi \cdot \overline{\psi} \in D_M$ but f_χ does not divide M. Hence we have a contradiction.
(iii) Apply (i) inductively to get $D_n = \prod D_{p_i^{\alpha_i}}$. The result is then obvious. $\square$

Switching now to a more concrete algebraic setting where our study of Dirichlet characters can be applied, consider identifying the Galois group of $\mathbb{Q}(\omega_N)$ with $(\mathbb{Z}/N\mathbb{Z})^\times$. We can then identify the character group with the Dirichlet characters mod N. Suppose K is a subfield of $\mathbb{Q}(\omega_N)$. Then by Galois theory there corresponds a unique subgroup $H \leq (\mathbb{Z}/N\mathbb{Z})^\times$ that characterizes K (namely the largest subgroup that fixes K). By (1.1.4), the character group of $\mathrm{Gal}(K/\mathbb{Q})$ embeds naturally into D_N as the subgroup of characters that act trivially on H. Conversely, given any subgroup Y of D_N we get the fixed field of $Y^\perp := \{\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q}) \mid \chi(\sigma) = 1 \ \forall\ \chi \in Y\}$.

Proposition 1.2.2. *Under the above identification, let K, K' be two subfields of $\mathbb{Q}(\omega_N)$ and let Y, Y' be the corresponding subgroups of D_N. Then*
(i) $K \subseteq K'$ iff $Y \subseteq Y'$.
(ii) The group generated by Y and Y' corresponds to the field KK'.

Proof. (i) $K \subseteq K'$ iff $H' \leq H$ iff $Y \leq Y'$ by (1.1.4) and general Galois theory.
(ii) The subgroup $Y_0 = \{\chi \in D_N | \chi(h) = 1 \quad \forall\ h \in H \cap H'\}$ is the one that corresponds to KK'. On the other hand $H \cap H'$ is the largest subgroup contained in both H and H', hence by (1.1.5), Y_0 is the smallest subgroup containing both Y and Y' and hence is generated by them. $\square$

We conclude from (1.1.5 (ii)) and general Galois theory, that the map discussed above is a bijection between subgroups of D_N and subfields of $\mathbb{Q}(\omega_N)$. We also note that the size of the subgroups is equal to the degree of the corresponding subfield over $\mathbb{Q}$. Moreover, if $K \subseteq \mathbb{Q}(\omega_M) \subset \mathbb{Q}(\omega_N)$, then the image of the character group of $\mathrm{Gal}(K/\mathbb{Q})$ in D_N is equal to its image in D_M followed by the inclusion of D_M into D_N. Indeed let H' be the subgroup corresponding to K in $\mathrm{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^\times$ and let H be the subgroup corresponding to K in $\mathrm{Gal}(\mathbb{Q}(\omega_M)/\mathbb{Q}) = (\mathbb{Z}/M\mathbb{Z})^\times$. Then H' contains $S := \{\overline{1+mk} | k \in \mathbb{Z}\}$ which is the subgroup corresponding to $\mathbb{Q}(\omega_M)$. Hence any character identically 1 on H' is induced by a character which is identically 1 on the image of H' under the quotient map $(\mathbb{Z}/N\mathbb{Z})^\times/S$ which is precisely $H \leq (\mathbb{Z}/M\mathbb{Z})^\times$. Hence every character of $H' \leq (\mathbb{Z}/N\mathbb{Z})^\times$ is induced by a character of $H \leq (\mathbb{Z}/M\mathbb{Z})^\times$ and it follows that the image of H' in D_M is equal to its image in D_N followed by inclusion.

We will see in the Chapter 3 that any finite abelian Galois extension K of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\omega_N)$. Assuming this fact for now, it follows that the character group of $\mathrm{Gal}(K/\mathbb{Q})$ can be identified with some subgroup of D_N. We use this observation along with what we have just proved to give the following minimality condition on N.

Proposition 1.2.3. *Let K be as above and say $\mathbb{X}_K \leq D_N$ is the character group of Gal$(K/\mathbb{Q})$. Define $f_K = lcm\{f_\chi | \chi \in \mathbb{X}_K\}$. Then f_K is the minimal integer such that K is contained in the f_K^{th}-cyclotomic field and every cyclotomic field containing K also contains ω_{f_K}.*

Proof. By (1.2.2), K is contained in a subfield of $\mathbb{Q}(\omega_N)$ iff $\mathbb{X}_K$ is contained in the subfield's corresponding subgroup in D_N. By the discussion above, the corresponding subgroup for the M^{th}-cyclotomic field is $D_M \leq D_N$ (Assuming

$M|N$ otherwise the M^{th}-cyclotomic field is not a subfield of the N^{th}). Since D_M is precisely the group of Dirichlet characters whose conductors divide M, it follows that the smallest D_M that could possibly contain $\mathbb{X}_K$ is indeed D_{f_K}. Since $K \subseteq \mathbb{Q}(\omega_N)$, all Dirichlet characters in question have order dividing N so clearly f_K must divide N, proving the proposition. □

The number f_K in the above proposition is known as the *conductor* of K.

We can get another nice result on abelian number fields if we introduce the concept of even and odd Dirichlet characters. Say χ is *even* if $\chi(-1) = 1$ and *odd* if $\chi(-1) = -1$. It is clear that the value of χ does not depend on the modulus on which it is defined.

Proposition 1.2.4. *Let K be an abelian number field, and let $\mathbb{X}_K$ be the corresponding group of Dirichlet characters. Then K is totally real iff $\mathbb{X}_K$ consists entirely of even characters.*

Proof. Assume $K \subseteq \mathbb{Q}(\omega_N)$ so that $\mathbb{X}_K \leq D_N$. Every totally real subfield of $\mathbb{Q}(\omega_N)$ is contained in $L = \mathbb{Q}(\omega_N + \omega_N^{-1})$. It is easy to see that L is the fixed field of $\{1, -1\} \leq (\mathbb{Z}/N\mathbb{Z})^\times$ and hence the subgroup of D_N corresponding to L is precisely all even characters. By (1.2.2), L contains K iff $\mathbb{X}_K$ consists entirely of even characters. □

Although most of our work with Dirichlet characters will come to fruition after we have introduced L-functions, we conclude this chapter with a few number theoretic results that use what we have developed to better understand the relationship between abelian number fields and their corresponding group

of characters. The following theorem shows that we can recover ramification indices of primes through this identification.

Theorem 1.2.5. *Let X be a subgroup of $D_n = \prod D_{p_i^{\alpha_i}}$ (where $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ is the prime decomposition of n), and K the corresponding subfield of $\mathbb{Q}(\omega_n)$. Let X_{p_j} be the image of X under the homomorphism that projects D_n onto $D_{p_j^{\alpha_j}}$. Then the ramification index of p_j in K equals $|X_{p_j}|$.*

Proof. Let $n = p_j^{\alpha_j} m$ and define L to be the subfield $\mathbb{Q}(\omega_m)K$ contained in $\mathbb{Q}(\omega_n)$. Since p_j is unramified in $\mathbb{Q}(\omega_m)$, the ramification index of p in L is the same as the index in K. By (1.2.2 (ii)), the group of characters of L is generated by X and D_m. It is easy to see that this character group is also generated by D_m and X_{p_j}. Hence $L = \mathbb{Q}(\omega_m) \cdot F$ where F is some subfield of $\mathbb{Q}(\omega_{p_j^{\alpha_j}})$ and $[F : \mathbb{Q}] = |X_{p_j}|$ since $D_m \cap X_{p_j} = \{1\}$. Since p_j ramifies completely in $\mathbb{Q}(\omega_{p_j^{\alpha_j}})$, it also ramifies completely in F and the result follows. □

In the next section we will have reason to observe another characterization of Dirichlet characters which we introduce now. Given $\chi \in D_n$, we can induce a function from $\mathbb{Z}$ to $\mathbb{C}$, which sends n to $\chi(n \mod f_\chi)$ when $(n, f_\chi) = 1$ and 0 otherwise. It is obvious that this function completely determines χ and vice versa, so we will identify this function as χ. Note that viewing the Dirichlet characters as functions on $\mathbb{Z}$, if $(a, f_\chi) = 1 = (a, f_\psi)$ then $\chi\psi(a) = \chi(a)\psi(a)$ but in general this need not be true. For example, if χ has conductor f_χ, then $\chi\overline{\chi}(f_\chi) = 1 \neq 0 = \chi(f_\chi)\overline{\chi}(f_\chi)$. It is pivotal to remember that the product of two Dirichlet characters is always the primitive character induced by the product in some character group. We will henceforth identify Dirichlet characters with the functions they induce when it suits us. The following corollary and theorem make use of this identification.

Corollary 1.2.6. *Let L be a field associated with some group $\mathbb{X}_L$ of Dirichlet characters. Then p ramifies in L iff $\exists\ \chi \in \mathbb{X}_L$ st. $\chi(p) = 0$.*

Proof. By (1.2.5), p ramifies in L iff $\exists\ \chi \in X$ whose conductor divides p iff $\chi(p) = 0$. □

Theorem 1.2.7. *Let $\mathbb{X}_K$ be a group of Dirichlet characters, K the associated field. Let $Y = \{\chi \in \mathbb{X}_K | \chi(p) \neq 0\}$ and $Z = \{\chi \in \mathbb{X}_K | \chi(p) = 1\}$. Then $e = [\mathbb{X}_K : Y], f = [Y : Z]$, and $g = [Z : 1]$ are the ramification index for p in K, the residue degree, and the number of primes lying over p respectively. Furthermore, $\mathbb{X}_K/Y$ and $\mathbb{X}_K/Z$ are isomorphic to the inertia and decomposition groups respectively.*

Proof. See [26] pg. 25-26. □

1.3 Zeta Functions and L-Functions

We now begin the study of Dedekind zeta functions, and in particular, those attached to abelian field extensions of $\mathbb{Q}$. Our work with Dirichlet characters will help immensely in the study of these objects and bring to light many useful facts about them. We begin with an informal definition: Given any sequence $\{a_n\}_{n=1}^{\infty} \subset \mathbb{C}$, define the associated *Dirichlet series* as

$$\sum_{n=1}^{\infty} \frac{a_n}{n^z},$$

where $z = x + iy$ is a complex variable. The following lemma found in [19] gives conditions for when this series converges to a holomorphic function in some half plane.

Lemma 1.3.1. *Suppose the partial sums of $\sum a_n$ form an infinite sequence $\{S_N\}$ that is $O(N^r)$ for some real $r \geq 0$. Then the Dirichlet series associated with $\{a_n\}_{n=1}^{\infty}$ converges for all $z = x + iy$ with $x > r$, and is analytic there.*

Proof. See [19] pg. 182-183. □

We now introduce one of the two types of Dirichlet series we will be focusing on. Let K be a number field and define its *Dedekind zeta function* as the Dirichlet series

$$\zeta_K(z) = \sum_{n=1}^{\infty} \frac{j_n}{n^z} = \sum_{I \lhd \mathcal{O}_K} \frac{1}{||I||^z},$$

where j_n is the number of ideals in $\mathcal{O}_K$ of norm n. The following theorem along with (1.3.1) shows that $\zeta_K(z)$ is well-defined and analytic on $\{\Re(z) > 1\}$.

Theorem 1.3.2. *Let K be a number field of degree n over $\mathbb{Q}$ and let $i(t)$ denote the number of ideals in $\mathcal{O}_K$ of norm $\leq t$. Then*

$$i(t) = h\kappa t + O(t^{1-\frac{1}{n}}),$$

where h is the class number of K, and $\kappa = \dfrac{2^{s_1+s_2}\pi^{s_2} reg(\mathcal{O}_K)}{w\sqrt{|\Delta(\mathcal{O}_K)|}}$. Here s_1, s_2 are the number of real and half the number of complex embeddings respectively of K, w is the number of roots of unity in K, $\Delta(\mathcal{O}_K)$ is the discriminant of the ring of integers, and $reg(\mathcal{O}_K)$ is the regulator (see [19] for a definition of the regulator).

Proof. See chapter 6 of [19]. □

The case when $K = \mathbb{Q}$ reduces to the usual zeta function $\zeta(z) = \sum \frac{1}{n^z}$ and the study of this function will be pivotal in the study of the more general case. Having proven that all ζ_K are defined on a half plane, we now show that they can also be represented by a Euler product over the same domain.

Proposition 1.3.3. *For* $\Re(z) > 1$,

$$\zeta_K(z) = \prod_{\substack{P \lhd \mathcal{O}_K \\ P \text{ prime}}} (1 - \frac{1}{||P||^z})^{-1}.$$

Proof. Since $\sum_P \frac{1}{||P||^{|z|}} \leq \sum_{I \lhd \mathcal{O}_K} \frac{1}{||I||^{|z|}} = \zeta_K(|z|) < \infty$, the Euler product converges to a limit on $\Re(z) > 1$ and the order does not need to be specified because convergence is absolute. Let S_N be the partial product over all primes in $\mathcal{O}_K$ of norm $\leq N$. Then

$$S_N = \prod_{||P|| \leq N} (1 + \frac{1}{P^z} + \frac{1}{P^{2z}} + ...) = \sum_{\substack{I \lhd \mathcal{O}_K \\ ||I|| \leq N}} \frac{1}{||I||^z} + A_N(z)$$

where $A_N(z)$ is some analytic function of absolute value $\leq \sum_{\substack{I \lhd \mathcal{O}_K \\ ||I|| > N}} \frac{1}{||I||^{|z|}}$. Note that we are justified in rearranging the terms of the infinite sums because $\sum_{t=0}^{\infty} \frac{1}{m^{tz}}$ converges absolutely when $m > 1$ and $\Re(z) > 0$. Letting $N \to \infty$, we conclude that the norm of $A_N(z)$ goes to zero and so $S_N(z) \to \zeta_K(z)$. $\square$

Restricting ourselves to the case when K is an abelian extension of $\mathbb{Q}$ (or in fact any Galois extension), (1.3.3) gives us a nice characterization of ζ_K in terms of the primes $p \in \mathbb{Z}$ because the splitting of a prime in a Galois extension is uniform. Indeed, assume p splits into r_p distinct primes and the inertial degree of p over any prime of $\mathcal{O}_K$ is f_p, then by (1.3.3) we have for

$\Re(z) > 1$,

$$\zeta_K(z) = \prod_p (1 - \frac{1}{p^{f_p z}})^{-r_p}.$$

When K is an abelian extension of $\mathbb{Q}$, it is this decomposition of ζ_K that will allow us to use L-functions to analytically continue ζ_K. Before introducing this concept however, we are going to follow [14] and [19] in proving a few common facts about ζ that will be used later to prove Dirichlet's famous theorem on primes in an arithmetic sequence.

Proposition 1.3.4. *The Riemann zeta-function $\zeta(z)$ can be extended to a meromorphic function on $\{\Re(z) > 0\}$ that has a simple pole of residue 1 at $z = 1$ and is otherwise analytic.*

Proof. Consider the two functions

$$f(z) := 1 + \frac{-1}{2^z} + \frac{1}{3^z} + \frac{-1}{4^z} + \frac{1}{5^z} + \frac{-1}{6^z} + ...$$

$$\text{and } g(z) := 1 + \frac{1}{2^z} + \frac{-2}{3^z} + \frac{1}{4^z} + \frac{1}{5^z} + \frac{-2}{6^z} + ...$$

By (1.3.1), $f(z)$ and $g(z)$ are well-defined analytic functions when $\Re(z) > 0$. Because the ζ series converges absolutely for $\Re(z) > 1$, reordering terms in a clever manner yields the identities

$$(1 - 2^{1-z})\zeta(z) = f(z)$$

$$\text{and } (1 - 3^{1-z})\zeta(z) = g(z).$$

Hence we have two meromorphic extensions of ζ which must agree since the half plane is simply connected. Since both f and g are analytic, it follows that if ζ has a pole at z_0, then $\exists\ n, m \in \mathbb{Z}$ such that $1 + \frac{2\pi i n}{\ln(2)} = z_0 = 1 + \frac{2\pi i m}{\ln(3)}$. Rearranging the identity, it follows that $\ln(\frac{3^n}{2^m}) = 0$, implying $3^n = 2^m$. Clearly this is possible iff $n = m = 0$. The next proposition will complete the proof. $\square$

Proposition 1.3.5. *Assume $s > 1$ is real. Then*

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1.$$

Proof. Fix $s > 1$. Then the function t^{-s} is strictly decreasing on $(1, \infty)$ and hence for all non-zero $n \in \mathbb{N}$ we have

$$(n+1)^{-s} < \int_n^{n+1} t^{-s} dt < n^{-s}.$$

Summing this inequality over all positive integers n,

$$\zeta(s) - 1 < \int_1^{\infty} t^{-s} dt < \zeta(s).$$

Evaluating the integral gives $(s-1)^{-1}$ and so we can conclude that $(s-1)(\zeta(s)-1) < 1 < (s-1)\zeta(s)$. Taking limits proves the result. □

Proposition 1.3.6. *For $\Re(z) > 1$, $\ln \zeta(z) = \sum_p p^{-z} + R(z)$, where $R(z)$ is analytic and bounded on the half space and p runs through all primes.*

Proof. Since $\zeta(z)$ has a Euler product expansion on the restricted domain, we know $\ln \zeta(z) = -\sum_p \ln(1 - \frac{1}{p^z})$ converges absolutely (Of course we are taking a branch of ln that is real along the reals). Furthermore, as $|\frac{1}{p^z}| \leq \frac{1}{2}$ for all p, we can apply the Taylor expansion of $-\ln(1-x) = \sum_{n \geq 1} \frac{x^n}{n}$ which also converges absolutely. Therefore

$$\ln \zeta(z) = \sum_p \sum_{n \geq 1} \frac{1}{n p^{zn}},$$

and since the series are absolutely convergent, we can rearrange to get

$$\ln \zeta(z) = \sum_p p^{-z} + \sum_p \sum_{n \geq 2} \frac{1}{n p^z n}.$$

It remains to show that the second series is uniformly bounded on the half plane. Indeed,

$$\sum_p \sum_{n\geq 2} \left| \frac{1}{np^{zn}} \right| \leq \sum_p |p^{-2}(1-p^{-1})^{-1}| \leq \sum_p |p^{-2}|(1-2^{-1})^{-1} < 2\zeta(2).$$

□

Finally, we come to *Dirichlet L-functions*. Let χ be a Dirichlet character viewed as a function from $\mathbb{Z}$ to $\mathbb{C}$. Define its associated L-function as

$$L(z,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^z}.$$

By (1.1.6), $\sum_{n=1}^{f_\chi} \chi(n) = 0$ if χ is non-trivial, so (1.3.1) tells us that $L(z,\chi)$ is an analytic function on $\Re(z) > 0$ because the partial sums of the numerators S_N are bounded by a constant (namely $\max\{|S_1|, \ldots, |S_{f_{\chi^{-1}}}|\}$). In the case where $\chi = 1$, we note that $L(z,1) = \zeta(z)$. This observation motivates the following proposition, which generalizes (1.3.3).

Proposition 1.3.7. *For* $\Re(z) > 1$, $L(z,\chi) = \prod_p (1 - \frac{\chi(p)}{p^z})^{-1}$.

Proof. Since $|\chi(n)|$ is either one or zero, the terms in the sum of $L(z,\chi)$ are bounded by those of $L(z,1) = \zeta(z) = \zeta_{\mathbb{Q}}$. Using the fact that χ is multiplicative, the proof then follows almost verbatim to the proof of (1.3.2) in the special case where $K = \mathbb{Q}$. □

Recall from the previous section that for every abelian number field K we have an associated subgroup of Dirichlet characters X. We saw that a number of intrinsic properties of the field K can be recovered from studying the characters in X. We will now see that ζ_K is also recoverable from X.

Theorem 1.3.8. *Let K and X be as above. For $\Re(z) > 1$,*

$$\zeta_K(z) = \prod_{\chi \in X} L(z, \chi).$$

Proof. From what we have proven so far, we know that $\zeta_K = \prod_p (1 - \frac{1}{p^{f_p z}})^{-r_p}$ and $L(z, \chi) = \prod_p (1 - \frac{\chi(p)}{p^z})^{-1}$. Since convergence is absolute, there is no problem in rearranging the factors in a finite product of L-functions. Thus we write suggestively

$$\prod_{\chi \in X} L(z, \chi) = \prod_p \prod_{\chi \in X} (1 - \frac{\chi(p)}{p^z})^{-1}.$$

Hence it suffices to show that for every prime $p \in \mathbb{N}$,

$$\prod_{\chi \in X} (1 - \frac{\chi(p)}{p^z})^{-1} = (1 - \frac{1}{p^{f_p z}})^{-r_p}.$$

Fixing p, it is clear that if $\chi(p) = 0$, then χ contributes nothing to the product above, so recalling notation from theorem (1.2.7), we are interested in the subgroups Y and $Z \subseteq X$. By (1.2.7), $r_p = |Z|$ is the number of $\chi \in Y$ such that $\chi(p) = 1$. Furthermore, f_p is the order of Y/Z, which means $|Y| = f_p r_p$ and since p does not divide the conductor of any character in Y, $\chi(p)^{f_p} = \chi^{f_p}(p) = 1$ for all $\chi \in Y$. The map $\mu : Y \to \{f_p^{th} - \text{roots of unity}\}$ which sends χ to $\chi(p)$ is therefore well-defined. Moreover, μ is easily seen to be a group homomorphism because $\chi\psi(p) = \chi(p)\psi(p)$ for all $\chi, \psi \in Y$. We know that the kernel is X and it follows from the size of Y that μ must be surjective and every f_p^{th} root of unity must have r_p elements in its pre-image. We therefore conclude

$$\prod_{\chi \in X} (1 - \frac{\chi(p)}{p^z})^{-1} = \prod_{\chi \in Y} (1 - \frac{\chi(p)}{p^z})^{-1} = (\prod_{n=0}^{f_p - 1} (1 - \frac{\omega_{f_p}^n}{p^z}))^{-r_p} = (1 - \frac{1}{p^{f_p z}})^{-r_p}.$$

□

1.4 Extending L-Functions

In Theorem (1.3.8), we saw that we can reconstruct the zeta function of an abelian number field K just by understanding a certain group of Dirichlet characters. In the current section, we are going to use this relationship to extend the domain of definition of ζ_K, by first showing that we can extend every Dirichlet L-function to a meromorphic function on $\mathbb{C}$ and then taking the necessary finite product. We follow the proof found in [14] pg. 261 - 264.

Before we get started, we prove two lemmas that will be used in our foray into analytic continuation.

Lemma 1.4.1. *Let $P(x)$ be a polynomial with complex coefficients and $P(0)$ equal to 0. Let $Q(x)$ be a polynomial with non-negative real coefficients and a non-zero constant term. Let $k \in \mathbb{R}$ be arbitrary. Then the function*

$$f(z) := \int_0^\infty \frac{P(e^{-t})t^{z+k}}{Q(e^{-t})}dt$$

is well-defined and analytic on $A_k := \{z \in \mathbb{C} \mid \Re(z) > -(k+1)\}$.

Proof. It suffices to show that f is complex differentiable on A_k and to this end, we consider the integrand function $h(z,t)$. The derivative with respect to z of h is $\dfrac{P(e^{-t})\ln(t)t^{z+k}}{Q(e^{-t})}$. Note that $\left|\dfrac{P(e^{-t})}{e^{-t}}\right|$ is bounded on $(0,\infty)$ because it is continuous and approaches a finite limit as t goes to ∞. Likewise, $|Q(e^{-t})|$ is bounded from below by $Q(0)$ due to the restrictions on the coefficients and approaches this limit for large t. We conclude that if z is restricted to some open subspace $A_{k,\epsilon} = \{z \in \mathbb{C}| -(k+1)+\epsilon < \Re(z) < 1/\epsilon\}$ for small $\epsilon > 0$, then

$$|h'(z,t)| < g_\epsilon(t) := \begin{cases} C \cdot e^{-t} |\ln(t)| t^{\epsilon-1} & \text{for } t \in (0,1] \\ C \cdot e^{-t} \ln(t) t^{1/\epsilon+k} & \text{for } t \in (1,\infty). \end{cases}$$

for some sufficiently large C. If $g_\epsilon(t) \in L^1((0,\infty))$, then f would be complex differentiable on $A_{k,\epsilon}$ with $\dfrac{\partial f}{\partial z} = \displaystyle\int_0^\infty \frac{P(e^{-t})\ln(t)t^{z+k}}{Q(e^{-t})} dt$. Since $\epsilon > 0$ is arbitrary, this would suffice to show f is analytic on all of A_k.

We show $g_\epsilon(t)$ is in L^1 by first noting that

$$\begin{aligned} \lim_{t\to 0^+} t^{\epsilon/2} \cdot \ln(t) &= \lim_{t\to 0^+} \frac{\ln(t)}{\frac{1}{t^{\epsilon/2}}} \\ &= \lim_{t\to 0+} \frac{\frac{1}{t}}{\frac{-\epsilon/2}{t^{1+\epsilon/2}}} \quad \text{by L'Hopital's.} \\ &= 0 \end{aligned}$$

and so there exists some constant B st. $|\ln(t)| < Bt^{-\epsilon/2}$ for all $t \in (0,1]$. Furthermore, for $t > 1$, $|\ln(t)| < t$ so we must have

$$\begin{aligned} \int_0^\infty g_\epsilon(t)dt &= \int_0^1 g_\epsilon(t)dt + \int_1^\infty g_\epsilon(t)dt \\ &\leq BC \int_0^1 t^{\epsilon/2-1} + C\int_1^\infty e^{-t}t^{1/\epsilon+k+1}dt. \end{aligned}$$

Since both of the integrals above are easily seen to be finite from basic analytic methods, we conclude $g_\epsilon \in L^1((0,\infty))$ and the proof is complete. □

Lemma 1.4.2. *Let $F(t) = \dfrac{P(e^{-t})}{Q(e^{-t})}$ with $P(x)$ and $Q(x)$ as in (1.4.1). Then $\dfrac{\partial^n F(t)}{\partial t^n} = \dfrac{P_n(e^{-t})}{Q_n(e^{-t})}$, where $P_n(x)$ and $Q_n(x)$ also satisfy the conditions of (1.4.1). Moreover, $F(t)$ and all of its derivatives are bounded as $t \to 0$ and all such functions are $o(t^{-m})$ for any fixed $m \in \mathbb{N}$.*

Proof. By induction, the first statement holds if it holds for $n = 1$. Writing $P(x) = xP_0(x)$, we have

$$\frac{\partial F(t)}{\partial t} = e^{-t}\frac{-(P_0(e^{-t}) + P_0'(e^{-t}))Q(e^{-t}) + e^{-t}Q'(e^{-t})P_0(e^{-t})}{Q(e^{-t})^2}.$$

Replacing e^{-t} with x in the above numerator, and observing that the derivative of polynomials is again a polynomial, we see that the numerator satisfies the conditions of (1.4.1). Furthermore Q^2 satisfies the conditions of (1.4.1) if Q does hence the first claim holds. The proof of (1.4.1) shows that any function of the same form as F is bounded on $[0, \infty)$. Since all derivatives of F are also of this form, in particular they are all bounded as $t \to 0$. The last part of the lemma follows from basic facts about the decay rate of the exponential e^{-t} and the fact that denominator is always bounded from below as t goes to ∞. □

We now introduce the Γ-function, which will be used later in the thesis and will give us a dry run at analytic continuation. Define

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt.$$

(1.4.1) tells us that Γ is analytic on $\{\Re(z) > 0\}$. However if $\Re(z) > 1$, integration by parts gives us

$$\Gamma(z) = -e^{-t}t^{z-1}|_0^\infty + (z-1)\int_0^\infty e^{-t}t^{z-2}dt = (z-1)\Gamma(z-1).$$

Therefore Γ satisfies the functional equation $\Gamma(z+1) = z\Gamma(z)$ and we use this to analytically continue Γ in the following way. For $k \in \mathbb{N}$, define the function

$$\Gamma_k(z) = \frac{1}{z(z+1)...(z+k-1)}\int_0^\infty e^{-t}t^{z+k-1}dt = \frac{1}{z(z+1)...(z+k-1)}\Gamma(z+k).$$

We note that for $\Re(z) > 0$, $\Gamma_k(z) = \Gamma(z)$ because by repeated use of the functional equation, $\Gamma(k+z) = z(z+1)...(z+k-1)\Gamma(z)$. Thus for each k, Γ_k

gives an analytic continuation of Γ to $\Re(z) > -k$ and since we can choose k arbitrarily large, we see that gamma extends to a meromorphic function on $\mathbb{C}$ with poles at the non-positive integers. The Γ-function will henceforth represent this extended function. It is well known that the Γ-function has no zeros, and this fact will be used but not proved. For a proof see [2].

We now head forth and use the Γ-function to analytically continue L-functions. Let χ be a Dirichlet character of conductor f_χ. For $\Re(z) > 1$ and $n \in \mathbb{N}$ we have from a simple change of variables that

$$\chi(n)n^{-z}\Gamma(z) = \int_0^\infty \chi(n)e^{-t}n^{-1}(\frac{t}{n})^{z-1}dt = \int_0^\infty \chi(n)e^{-nt}t^{z-1}dt. \tag{1.1}$$

Summing (1.1) over all positive integers, we get

$$L(z,\chi)\Gamma(z) = \sum_{n=1}^{\infty}\int_0^\infty \chi(n)e^{-nt}t^{z-1}dt. \tag{1.2}$$

Fixing z momentarily, we note that

$$\sum_{n=1}^{\infty}\int_0^\infty |\chi(n)e^{-nt}t^{z-1}|dt = \int_0^\infty (\sum_{n=1}^{\infty}(e^{-t})^n)t^{|z|-1}dt = \int_0^\infty \frac{e^{-t}}{1-e^{-t}}t^{|z|-1}.$$

The integrand clearly decays fast enough at ∞ to be integrable, so the only question is its behavior near 0. $(1-e^{-t})^{-1}$ has a simple pole at 0 of residue 1 as can be seen from its Taylor expansion. It follows that the integrand behaves like $e^{-t}t^{|z|-2}$ plus some function that is bounded near 0. Since $|z| > 1$, $t^{|z|-2}$ is integrable on $(0, M)$ for any positive M. Hence the summation in (1.2) can be moved inside the integral because the integrand is in L^1, and since the pointwise convergence is absolute, we may reorder the sum as we please. In

particular,

$$\begin{aligned} L(z,\chi)\Gamma(z) &= \int_0^\infty \sum_{n=1}^{f_\chi} \chi(n) \sum_{k=0}^{\infty} e^{-t(n+kf_\chi)} t^{z-1} dt \\ &= \int_0^\infty \sum_{n=1}^{f_\chi} \frac{\chi(n)e^{-tn}}{1-e^{-tf_\chi}} t^{z-1} dt. \end{aligned} \tag{1.3}$$

A change of variables from t to $2t$ in (1.3) gives

$$2^{1-z} L(z,\chi)\Gamma(z) = 2\int_0^\infty \sum_{n=1}^{f_\chi} \frac{\chi(n)e^{-2tn}}{1-e^{-2tf_\chi}} t^{z-1} dt.$$

Subtracting this result from (1.3), and defining the normalized function $L^\star(z,\chi) = (1-2^{1-z})L(z,\chi)$ gives us

$$\begin{aligned} L^\star(z,\chi)\Gamma(z) &= \int_0^\infty \sum_{n=1}^{f_\chi} \chi(n)\left(\frac{e^{-tn}}{1-e^{-tf_\chi}} - \frac{2e^{-2tn}}{1-e^{-2tf_\chi}}\right) t^{z-1} dt \\ &= \int_0^\infty \sum_{n=1}^{f_\chi} \chi(n) \frac{e^{-tn} - e^{-tn-2tf_\chi} - 2e^{-2tn} + 2e^{-2tn-tf_\chi}}{(1-e^{-tf_\chi})(1-e^{-2tf_\chi})} t^{z-1} dt \\ &= \int_0^\infty \sum_{n=1}^{f_\chi} \chi(n) e^{-tn} \frac{(1-e^{-tf_\chi})(1+e^{-tf_\chi}) - 2e^{-tn}(1-e^{-tf_\chi})}{(1-e^{-tf_\chi})(1-e^{-2tf_\chi})} t^{z-1} dt \\ &= \int_0^\infty \frac{\sum_{n=1}^{f_\chi} \chi(n) e^{-tn}(1+e^{-tf_\chi} - 2e^{-tn})}{(1-e^{-2tf_\chi})} t^{z-1} dt \end{aligned} \tag{1.4}$$

Replace e^{-t} in (1.4) with the indeterminant x and note that for every n, $1 + x^{f_\chi} - 2x^n$ is 0 when $x = 1$. It follows that the integrand in (1.4) can be written in the form $\dfrac{P(x)}{1+x+...+x^{2f_\chi-1}} t^{z-1} = \dfrac{P(x)}{Q(x)} t^{z-1}$, where P and Q satisfy the hypotheses of (1.4.1).

Let $F_{\chi,0}(t) := \frac{P(e^{-t})}{Q(e^{-t})}$, and $F_{\chi,n}$ as its n^{th} derivative. (1.4) can then be written as

$$L^\star(z,\chi)\Gamma(z) = \int_0^\infty F_{\chi,0} t^{z-1} dt$$

Applying integration by parts with $u = F_{\chi,0}(t)$ and $dv = t^{z-1}dt$ and using (1.4.2),

$$\begin{aligned} L^\star(z,\chi)\Gamma(z) &= \frac{1}{z}F_{\chi,0}(t)t^z|_0^\infty - \frac{1}{z}\int_0^\infty F_{\chi,1}(t)t^z dt \\ \Rightarrow zL^\star(z,\chi)\Gamma(z) &= -\int_0^\infty F_{\chi,1}(t)t^z dt \\ \Rightarrow L^\star(z,\chi)\Gamma(z+1) &= -\int_0^\infty F_{\chi,1}(t)t^z dt \end{aligned} \tag{1.5}$$

Lemma (1.4.1) says that (1.5) defines an analytic function for $\{\Re(z) > -1\}$ and therefore $\dfrac{-1}{(1-2^{z-1})\Gamma(z+1)}\displaystyle\int_0^\infty F_{\chi,1}(t)t^z dt$ provides an extension of $L(z,\chi)$ to $\{\Re(z) > -1\}$. (1.4.2) lets us repeatedly use the integration by parts method above to extend $L(z,\chi)$ to the entire plane. By (1.3.1), (1.3.4) and the proof of (1.1.6 (i)), we know where the poles of the L-functions are in the half plane $\{\Re(z) > 0\}$. Since Γ is non-zero we note that our extended L-functions do not pick up any new poles in the extended domain. We conclude by summarizing our results in the following theorem.

Theorem 1.4.3. *Let everything be as above, and suppose $k \in \mathbb{N}$ is an arbitrary positive integer. Then the formula*

$$L(z,\chi) = \frac{(-1)^k}{(1-2^{1-z})\Gamma(z+k)}\int_0^\infty F_{\chi,k}(t)t^{z+k-1}dt$$

extends χ's associated L-function to the half plane $\{z \in \mathbb{C} \mid \Re(z) > k\}$. If χ is the trivial character, the extended function has a unique simple pole at 1 of residue 1. Otherwise χ is non-trivial and the extension is analytic everywhere it is defined.

It should be mentioned that (1.4.3) also allows us to extend the domain of definition of every zeta function corresponding to an abelian number field through the relation $\zeta_K(z) = \prod L(z,\chi)$. We are particularly interested in

the values of ζ_K at the negative integers and we will momentarily see how to calculate these values for any L-function by computing Taylor expansions. We begin by introducing a special class of sequences:

Define the sequence $\{B_n\}_{n=0}^{\infty}$ by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n(\frac{t^n}{n!}).$$

This sequence is known as the *Bernoulli numbers*. We define the *generalized Bernoulli numbers* $B_{n,\chi}$ from the expansion

$$\sum_{a=1}^{f_\chi} \frac{\chi(a)te^{at}}{e^{f_\chi t} - 1} = \sum_{n=0}^{\infty} B_{n,\chi}(\frac{t^n}{n!}).$$

The terminology is derived from the fact that for the trivial character,

$$\sum_{n=0}^{\infty} B_{n,1}(\frac{t^n}{n!}) = \frac{te^t}{e^t - 1} = \frac{t}{e^t - 1} + t$$

and hence $B_{n,1} = B_n$ for all $n \neq 1$.

Corollary 1.4.4. *Let n be a positive integer and χ some Dirichlet character. Then $L(1 - n, \chi) = -B_{n,\chi}/n$.*

Proof. In the formula given in (1.4.3), let $n = k$ and $z = 1 - n$. Then

$$L(1 - n, \chi) = \frac{(-1)^n}{(1 - 2^n)\Gamma(1)} \int_0^{\infty} F_{\chi,n}(t)dt,$$

where $F_{\chi,n}$ is the n^{th} derivative of the function

$$\begin{aligned} F_{\chi,0} &= \sum_{a=1}^{f_\chi} \chi(a)(\frac{e^{-ta}}{1 - e^{-tf_\chi}} - \frac{2e^{-2ta}}{1 - e^{-2tf_\chi}}) \\ &= \frac{1}{t}\sum_{k=0}^{\infty}(-1)^k B_{k,\chi}\frac{t^k}{k!} - \frac{1}{t}\sum_{k=0}^{\infty}(-1)^k 2^k B_{k,\chi}\frac{t^k}{k!} \\ &= \sum_{k=1}^{\infty}(-1)^k(1 - 2^k)B_{k,\chi}\frac{t^{k-1}}{k!}. \end{aligned}$$

Therefore by the fundamental theorem of calculus and (1.4.2), we conclude

$$\begin{aligned} L(1-n,\chi) &= \frac{(-1)^n}{1-2^n}F_{\chi,n-1}(0) \\ &= \frac{(-1)^n(-1)^{n-1}(1-2^n)B_{n,\chi}}{n(1-2^n)} \\ &= \frac{-B_{n,\chi}}{n}. \end{aligned}$$

□

Some restrictions on the values of $B_{n,\chi}$ can be made by observing the parity of the function $f_\chi(t) = \sum_{a=1}^{f_\chi} \frac{\chi(a)te^{at}}{e^{f_\chi t}-1}$. Indeed, assume first that χ is not the trivial character and substitute $-t$ for t in the above expression to get

$$\begin{aligned} f_\chi(-t) &= -\sum_{a=1}^{f_\chi} \frac{\chi(a)te^{-at}}{e^{-f_\chi t}-1} \\ &= -\sum_{a=1}^{f_\chi} \frac{\chi(a)te^{(f_\chi-a)t}}{1-e^{f_\chi t}} \\ &= \sum_{a=1}^{f_\chi} \frac{\chi(f_\chi-a)e^{at}}{e^{f_\chi t}-1} \\ &= \chi(-1)f_\chi(t). \end{aligned}$$

Hence the parity of f_χ agrees with the parity of χ. If χ is the trivial character, we have

$$\begin{aligned} f_1(t) - \frac{t}{2} &= \frac{t}{e^t-1} + \frac{t}{2} \\ &= \frac{te^{-t}}{1-e^{-t}} + \frac{t}{2} \\ &= \frac{(-t)}{e^{-t}-1} - \frac{t}{2} \\ &= f_1(-t) + \frac{t}{2}, \end{aligned}$$

so in this case $f_1 - t/2$ is even. Since even and oddness is reflected in the power series expansion by zeros in the appropriate coefficients, we have proved the following lemma.

Lemma 1.4.5. *Let χ be a Dirichlet character and $n \geq 1$ an arbitrary integer.*

(i) If χ is non-trivial and even, then $B_{2n-1,\chi} = 0$.

(ii) If χ is non-trivial and odd, then $B_{2n,\chi} = 0$.

(iii) If $\chi = 1$ is the trivial character, then $B_{2n-1,1} = 1/2$ if $n = 1$ and 0 otherwise.

Corollary 1.4.6. *Let K be an abelian number field over $\mathbb{Q}$. Then $\zeta_K(-n) = 0$ for all even $n \geq 2$ and if K is not totally real then $\zeta_K(-n) = 0$ for all positive $n \in \mathbb{N}$.*

Proof. Assume K is not totally real and let $\mathbb{X}_K$ be the set of Dirichlet characters corresponding to K. By proposition (1.2.4), $\mathbb{X}_K$ contains an odd character ψ and of course $\mathbb{X}_K$ contains the trivial character. By (1.4.5) and (1.4.4), either $L(1-n,1) = 0$ or $L(1-n,\psi) = 0$ for all $n \geq 2$. The first statement follows from the fact that every character group contains the trivial character. □

Before ending this section, we prove a result regarding generalized Bernoulli numbers that will allow them to be computed quickly and uniformly. This result will be useful in chapter 5 when we develop an efficient algorithm to find these numbers.

Define the *Bernoulli Polynomials* $B_n(X)$ as

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!}.$$

Observe that since $\dfrac{t}{e^t-1} = \displaystyle\sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$ and $e^{Xt} = \displaystyle\sum_{n=0}^{\infty} X^n \frac{t^n}{n!}$, one can easily express the Bernoulli polynomials in terms of the Bernoulli numbers,

$$B_n(X) = \sum_{i=0}^{\infty} \binom{n}{i} B_i X^{n-i}.$$

Proposition 1.4.7. *Let F be any multiple of conductor f_χ of the Dirichlet character χ. Then*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right).$$

Proof.

$$\sum_{n=0}^{\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) \frac{t^n}{n!} = \sum_{a=1}^{F} \frac{\chi(a)}{F} \sum_{n=0}^{\infty} B_n\left(\frac{a}{F}\right) \frac{(Ft)^n}{n!} = \sum_{a=1}^{F} \chi(a) \frac{te^{(a/F)Ft}}{e^{Ft}-1}.$$

Let $g = F/f$ and $a = b + cf_\chi$, so that a running from 1 to F is equivalent to b running from 1 to f_χ and c running from 0 to $g-1$. Also note that $\chi(a) = \chi(b)$. It follows that we can rewrite the last line in our equality above as

$$\sum_{b=1}^{f_\chi} \sum_{c=0}^{g-1} \chi(b) \frac{te^{(b+cf_\chi)t}}{e^{f_\chi g t}-1} = \left(\sum_{b=1}^{f_\chi} \chi(b) \frac{te^{bt}}{e^{f_\chi g t}-1}\right)\left(\sum_{c=0}^{g-1} e^{cf_\chi t}\right).$$

But the final factor above is just a finite geometric series and can be evaluated directly as $\dfrac{e^{f_\chi g t}-1}{e^{f_\chi t}-1}$ and the result follows by definition of $B_{n,\chi}$. □

1.5 Odds and Ends

We conclude this chapter with a few nice results that can be easily obtained through the language we have developed in the previous sections.

A set of positive primes A is said to have *Dirichlet density* if

$$\lim_{s \to 1^+} -\frac{\sum_{p \in A} p^{-s}}{\ln(s-1)}$$

exists. If the limit does exist, we say it is the *Dirichlet density* $d(A)$ of A.

Observe that if A is finite then $d(A) = 0$ and if A and B are disjoint sets, then $d(A \cup B) = d(A) + d(B)$, assuming both terms on the right hand side exist. The set of all primes in $\mathbb{N}$ has Dirichlet density 1, as (1.3.5) and (1.3.6) combine to show that

$$\begin{aligned} 1 &= \lim_{s \to 1^+} -\frac{\ln(\zeta_{\mathbb{Q}}(s))}{\ln(s-1)} \\ &= \lim_{s \to 1^+} -\frac{\sum p^{-s} + R(s)}{\ln(s-1)} \\ &= \lim_{s \to 1^+} -\frac{\sum p^{-s}}{\ln(s-1)}. \end{aligned}$$

We will use the concept of Dirichlet density to prove Dirichlet's famous theorem on primes; we need only the following lemma.

Lemma 1.5.1. *Let K be an arbitrary number field of degree m over $\mathbb{Q}$. Then $\zeta_K(z)$ has a simple pole at $z = 1$.*

Proof. We know that when $K = \mathbb{Q}$ the lemma holds and in fact ζ has a residue of 1 at $z = 1$. Recall our original definition of $\zeta_K(z) = \sum_n \frac{j_n}{n^z}$, when $\Re(z) > 1$. Recalling notation from (1.3.2), we may then add and subtract $h\kappa\zeta(z)$ to get

$$\zeta_K(z) = \sum_{n=1}^{\infty} \frac{j_n - h\kappa}{n^z} + h\kappa\zeta(z)$$

By (1.3.2), $\sum_{n=1}^{N} j_n = i(N) = h\kappa N + O(N^{1-\frac{1}{m}})$ and it follows from (1.3.1) that the series above converges to an analytic function on $\Re(z) > 1 - \frac{1}{m}$. Hence $z\zeta_K(z)$ converges to $h\kappa$ as z goes to 0. □

Theorem 1.5.2. *Assume $a, b \in \mathbb{N}$ satisfy $(a, b) = 1$. Then the set $A_{a,b}$ of all primes in $\mathbb{N}$ that are congruent with a modulo b has Dirichlet density $1/\phi(b)$.*

Proof. The proof of proposition (1.3.6) generalizes immediately to the following result: Let χ be any Dirichlet character. Then for $\Re(z) > 1$, $\ln L(z,\chi) = \sum \chi(p)p^{-z} + R_\chi(z)$, where $R_\chi(z)$ is analytic and bounded as $z \to 0$.

Using this, we note that when $\Re(z) > 1$ we have

$$\begin{aligned}\sum_{\chi \in D_b} \chi(a^{-1}) \ln L(z,\chi) &= \sum_p \frac{\sum_{\chi \in X} \chi(a^{-1}p)}{p^z} + \sum_{\chi \in D_b} R_\chi \\ &= \sum_{p \equiv a(b)} \frac{\phi(b)}{p^z} + \sum_{\chi \in D_b} R_\chi,\end{aligned}$$

where the last equality comes from (1.1.6). Applying (1.6.1) and the fact that $\zeta_{\mathbb{Q}(\omega_b)}(z) = \prod_{\chi \in D_b} L(z,\chi)$, we see that if χ is non-trivial, $L(1,\chi)$ is not 0. In particular $\ln L(1,\chi)$ is finite and so we conclude that

$$\begin{aligned}1 &= \lim_{z \to 1^+} -\frac{\ln(\zeta(z))}{\ln(z-1)} \\ &= \lim_{z \to 1^+} -\sum_{\chi \in D_b} \frac{\chi(a^{-1}) \ln L(z,\chi)}{\ln(z-1)} \\ &= \lim_{z \to 1^+} -\sum_{p \equiv a(b)} \frac{\frac{\phi(b)}{p^z}}{\ln(z-1)} - \sum_{\chi \in D_b} \frac{R_\chi}{\ln(z-1)} \\ &= \lim_{z \to 1^+} -\phi(b) \frac{\sum_{p \equiv a(b)} \frac{1}{p^z}}{\ln(z-1)}.\end{aligned}$$

Therefore $d(A_{a,b}) = 1/\phi(b)$. □

We now use Dirichlet's theorem to show how the splitting of rational primes in an abelian number field completely determines the field. In fact a much more general statement holds but this weaker result will be sufficient for the purposes of this thesis. See the discussion in [19] regarding polar density to find a proof of the more general statement.

Theorem 1.5.3. *Suppose K and L are two subfields of some cyclotomic field, and let A and B be the set of primes in $\mathbb{Q}$ that split completely in K, L respectively. If $A\backslash B \cup B\backslash A$ is finite, then $K = L$.*

Proof. Choose $N \in \mathbb{N}$ large enough so that $\mathbb{Q}(\omega_N) \supseteq K$ and L. Assume H_K and H_L are the corresponding subgroups in $(\mathbb{Z}/N\mathbb{Z})^\times$. Lemma (4.1.0) tells us that aside from the primes dividing N, $p \in A$ iff $\overline{p} \in H_K$ and likewise $p \in B$ iff $\overline{p} \in H_L$. By (1.6.2), if $H_K \neq H_L$, there are infinitely many primes that are in one but not the other. Hence $A\backslash B \cup B\backslash A$ is finite iff $K = L$. □

CHAPTER 2
Tools from Number Theory

We use this chapter to introduce some of the concepts from number theory that will be needed for proofs in the subsequent chapters. The reader should by no means consider this an exhaustive detailing of these algebraic objects, as we develop them only to the extent needed for this thesis.

2.1 Fractional Ideals

We follow [15] in giving a brief introduction to the concept of fractional ideals in the context of a number field K with ring of integers $\mathcal{O}$. The main purpose of this section will serve to provide background for introducing the different of a number field, which will be introduced in the subsequent section and is needed in our proof of the Kronecker-Weber theorem.

A *fractional ideal* of K is a nonzero finitely generated $\mathcal{O}$-submodule of K, where $\mathcal{O}$ is some Dedekind ring and K is its field of fractions. If $\mathcal{M}$ is a fractional ideal, then we define $\mathcal{M}^{-1} := \{x \in K \mid x\mathcal{M} \subseteq \mathcal{O}\}$. It is easy to see that if $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{N}^{-1} \subseteq \mathcal{M}^{-1}$ and also $\mathcal{O}^{-1} = \mathcal{O}$.

It is clear that if $I \lhd \mathcal{O}$ is any nonzero ideal, then I is also a fractional ideal. Conversely, any fractional ideal entirely contained in $\mathcal{O}$ is clearly an ideal, which we may denote as an *integral ideal* when necessary to avoid confusion. Another obvious example would be $y\mathcal{O}$ for any $y \in K$. We will see that when $\mathcal{O}$ is a PID, all fractional ideals of K can be expressed in this manner, and so the concept of PIDs extends from ideals to fractional ideals.

Proposition 2.1.1. *If $\mathcal{M}$ is a fractional ideal then so is $\mathcal{M}^{-1}$.*

Proof. $\mathcal{M}^{-1}$ is clearly an $\mathcal{O}$-submodule of K from the definition. Since $\mathcal{M}$ is finitely generated, say by $\{\frac{a_1}{b_1}, \frac{a_2}{b_2}..., \frac{a_n}{b_n}\}$, it is easy to see that $0 \neq b_1 b_2 ... b_n \in \mathcal{M}^{-1}$ and so $\mathcal{M}^{-1}$ is nonzero. It remains to show $\mathcal{M}^{-1}$ is finitely generated. Taking any $m \in \mathcal{O}$, we have $m\mathcal{M}^{-1} \subseteq \mathcal{O}$ and hence $\mathcal{M}^{-1} \subseteq m^{-1}\mathcal{O}$. Since $\mathcal{O}$ is noetherian, it follows that $\mathcal{M}^{-1}$ is finitely generated. □

Define the product of two fractional ideals in the obvious way, namely $\mathcal{MN}$ is the set of all $x \in K$ such that x can be written as a finite sum, $\sum a_i b_i$, with $a_i \in \mathcal{M}$ and $b_i \in \mathcal{N}$. Given this definition, we see that if $\{a_i\}$ and $\{b_j\}$ are finite sets generating $\mathcal{M}$ and $\mathcal{N}$, then $\{a_i b_j\}$ generates their product. Since $\mathcal{OM} = \mathcal{M} = \mathcal{MO}$, the following proposition is all that remains to show the set of fractional ideals is an abelian group under the above multiplication.

Proposition 2.1.2. $\mathcal{MM}^{-1} = \mathcal{O}$.

Proof. It is clear from the definitions that $\mathcal{MM}^{-1} \subseteq \mathcal{O}$. We make use of the following 2 claims to prove the reverse inclusion.

Claim 1: Let $S \subset \mathcal{O}$ be a multiplicative set and $\mathcal{M}_S = S^{-1}\mathcal{M}$ be the localization of $\mathcal{M}$ with respect to S. Then $(\mathcal{M}^{-1})_S = (\mathcal{M}_S)^{-1}$ and $\mathcal{M}_S\mathcal{N}_S = (\mathcal{MN})_S$.

Proof: Let $x \in (\mathcal{M}^{-1})_S$. Then $\exists\ s \in S$ st. $sx \in \mathcal{M}^{-1}$. Hence $sx\mathcal{M} \subseteq \mathcal{O}$ which implies $x\mathcal{M}_S \subseteq \mathcal{O}_S$. Conversely suppose $x \in (\mathcal{M}_S)^{-1}$ and write $\mathcal{M} = k_1\mathcal{O} + \ldots + k_n\mathcal{O}$ for some $k_i \in K$. It follows that $xk_i \in \mathcal{O}_S$ for all i, say $xk_i = \frac{a_i}{s_i}$ for $a_i \in \mathcal{O}$ and $s_i \in S$. Hence $sx \in \mathcal{M}^{-1}$ where s is the product of the s_i, and so $x \in (\mathcal{O}^{-1})_S$. The second part of the claim is proved similarly.

Claim 2: If $\mathcal{O}$ is a PID, then every fractional ideal is generated by a single element.

Proof: Let $\mathcal{M}$ be any fractional ideal. Using the fact that $\mathcal{M}$ is finitely generated, we conclude there is a $k \in \mathcal{O}$ st. $k\mathcal{M} \subseteq \mathcal{O}$. Hence $k\mathcal{M} = (x)$ is an integral ideal, and it follows $\mathcal{M} = \frac{k}{x}\mathcal{O}$.

Returning to the proof of the proposition, suppose $\mathcal{M}\mathcal{M}^{-1}$ is a proper integral ideal of $\mathcal{O}$. Then it is contained in some prime ideal P. Localizing at P we see that $(\mathcal{M}\mathcal{M}^{-1})_P \subseteq P \cdot \mathcal{O}_P$ while by claims (1) and (2) we have $(\mathcal{M}\mathcal{M}^{-1})_P = (\mathcal{M}_P)(\mathcal{M}_P)^{-1} = (x\mathcal{O}_P)(x^{-1}\mathcal{O}_P) = \mathcal{O}_P$. This is a contradiction. □

The following theorem shows that the unique prime factorization of ideals in $\mathcal{O}$ extends in a natural way to factorization of all fractional ideals.

Theorem 2.1.3. *Let $\mathcal{M}$ be any fractional ideal in Dedekind ring $\mathcal{O}$. Then $\mathcal{M}$ can be expressed uniquely as a product*

$$\mathcal{M} = P_1^{\alpha_1} P_2^{\alpha_2} ... P_k^{\alpha_k}$$

with each P_i a distinct prime ideal and each $\alpha_i \in \mathbb{Z}$.

Proof. See [15] pg. 18. □

Before moving on to differents in the next section, we introduce the concept of a dual basis. Let $K \subset L$ be two number fields and consider the K-bilinear quadratic form $T = T_K^L : L \times L \to K$.

Theorem 2.1.4. *The trace map is non-degenerate.*

Proof. We assume that there exists $x \in L$ such that $T(x, \cdot)$ is the zero map and show x must be zero. Let $\alpha \in L$ be a primitive element over K, ie. $L = K(\alpha)$. We can then write x as a polynomial in α, say

$$x = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1},$$

where $b_i \in K$ and $n = [L : K]$. Letting $A := (a_{ij})$ be the $n \times n$ matrix defined by $a_{ij} = T(\alpha^{i-1}\alpha^{j-1})$, we conclude that if x is not zero then A must have determinant zero, as $\sum_{i=1}^{n} b_{i-1}T(\alpha^{i-1}\alpha^{j-1}) = T(x\alpha^{j-1}) = 0$ for all j and hence

$$[b_0, ..., b_1].A = \vec{0}.$$

On the other hand, let

$$f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$$

be the minimal polynomial for $\alpha = \alpha_1$ over K, where all of the α_i lie in some splitting field. Then we have the *Vandermonde* matrix

$$V := \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{pmatrix}$$

and one can check that $V^t.V = A$. On the other hand, it is well known that $\det(V) = \prod_{i<j}(\alpha_i - \alpha_j)$ and since L is a separable extension of K, we must have $\det(A) = \det(V)^2 \neq 0$. Hence x must be zero. □

Since L is a finite dimensional vector space of K, it follows from (2.1.4) and general linear algebra that every K-linear functional in L^* is of the form $f(x) = T(xy)$ for some unique $y \in L$ and it is clear that any such y defines a

linear functional as above. In particular, given a basis $\{\alpha_1, ..., \alpha_n\}$ of L over K, we can consider the functionals $f_i \in L^*$ such that $f_i(\alpha_j) = \delta_{ij}$ for $i = 1, ..., n$. We define the *dual basis* with respect to $\{\alpha_1, ..., \alpha_n\}$ to be $\{\beta_1, ..., \beta_n\}$, where $f_i(x) = T(x\beta_i)$. It is easy to see by the linearity of the trace that the dual basis is in fact a basis. The final proposition of this section shows that we can calculate dual bases explicitly when the given basis is monogenous.

Proposition 2.1.5. *Suppose $\alpha \in L$ st. $L = K[\alpha]$. Let f be the monic irreducible polynomial for α over K and write $f(x) = (x - \alpha)g(x)$. Then*

$$g(x) = \beta_0 + \beta_1 x + ... + \beta_{n-1}x^{n-1} \in L[x]$$

and

$$\left\{ \frac{\beta_0}{f'(\alpha)}, ..., \frac{\beta_{n-1}}{f'(\alpha)} \right\}$$

is the dual basis to $\{1, \alpha, ..., \alpha^{n-1}\}$.

Proof. We follow the proof outlined in the exercises of [19]. Let $\sigma_1, ..., \sigma_n$ be the n distinct embeddings of L in $\mathbb{C}$ that fix K and for simplicity, assume σ_1 is the identity. Define $g_i(x) = \sigma_i(g(x))$ and $\alpha_i = \sigma_i(\alpha)$, so that $f(x) = (x - \alpha_i)g_i(x)$ in $\mathbb{C}[x]$. It is easy to see that $g_i(\alpha_j) = 0$ if $i \neq j$ and is equal to $f'(\alpha_i)$ if $i = j$. Let V be the Vandermonde matrix defined with respect to the α_i and $N =(\ \sigma_i(\beta_{j-1}/f'(\alpha))\ )$. Then

$$N.V^t = \left(\sum_{k=1}^{n} \sigma_i(\beta_{k-1}/f'(\alpha))\alpha_j^{k-1} \right) = (g_i(\alpha_j)/(f'(\alpha_i))) = I_n.$$

Hence $N = (V^t)^{-1}$ and so

$$I_n = V^t.N = \left(\sum_{k=1}^{n} \alpha_k^{i-1}\sigma_k(\beta_{j-1}/f'(\alpha)) \right) = (T(\alpha^{i-1}\frac{\beta_{j-1}}{f'(\alpha)})).$$

□

2.2 Differents

We start with $L|K$ a separable extension of fields, $\mathcal{O}_K$ a Dedekind subring of K and $\mathcal{O}_L$ its integral closure in L. Let A be an $\mathcal{O}_K$-submodule of L. We define the *complimentary set* $\mathcal{A}^* := \{x \in L \mid T(xA) \subseteq \mathcal{O}_K\}$. We note that A^* is an $\mathcal{O}_K$-module, as $T((mx)A) = mT(xA)$. Furthermore, if $A \subseteq B$ are two such $\mathcal{O}_K$-modules, then $B^* \subseteq A^*$.

Proposition 2.2.1. *Let $\{\alpha_1, ..., \alpha_n\}$ be a basis for L over K and consider the $\mathcal{O}_K$-submodule*

$$A := \alpha_1\mathcal{O}_K + ... + \alpha_n\mathcal{O}_K.$$

Then $A^* = \beta_1\mathcal{O}_K + ... + \beta_n\mathcal{O}_K$, where $\{\beta_1, ..., \beta_n\}$ is the corresponding dual basis.

Proof. Suppose $x \in A$. Then $x = c_1\alpha_1 + ... + c_n\alpha_n$ and by definition of the dual basis, $T(x\beta_i) = c_i \in \mathcal{O}_K$. Hence A^* certainly contains $\beta_1\mathcal{O}_K + ... + \beta_n\mathcal{O}_K$. Conversely, if $y \in A^*$, then let $d_k = T(\alpha_k y)$. It follows that $y = d_1\beta_1 + ... + d_n\beta_n$ and since each d_k is in $\mathcal{O}_K$, we have the reverse containment. □

We observe from the definitions that if $\mathcal{M}$ is an $\mathcal{O}_L$-submodule of L, then its complimentary set is as well. This motivates the following proposition.

Proposition 2.2.2. *If $\mathcal{M}$ is a fractional ideal, so is $\mathcal{M}^*$.*

Proof. It remains to show $\mathcal{M}^*$ is nonzero and finitely generated. Pick $s \in K$ such that $s\mathcal{M} = I \lhd \mathcal{O}_L$. I contains a basis for L over K, say $\{\alpha_1, ..., \alpha_n\}$ and hence $\mathcal{M}$ contains the $\mathcal{O}_K$ module $A = \frac{\alpha_1}{s_1}\mathcal{O}_K + ... + \frac{\alpha_n}{s_n}\mathcal{O}_K$. Thus $A^*\mathcal{O}_L \supseteq$

$A^* \supseteq \mathcal{M}^*$, and $A^*\mathcal{O}_L$ is finitely generated by (2.2.1). Since $\mathcal{O}_L$ is noetherian, $\mathcal{M}^*$ is finitely generated, and clearly nonzero since $\mathcal{M}^{-1} \subseteq \mathcal{M}^*$. □

Following the previous proposition, we place special emphasis on the fractional ideal $\mathcal{C} = \mathcal{O}_L^*$ which contains $\mathcal{O}_L^{-1} = \mathcal{O}_L$ by denoting it *Dedekind's complimentary module* or the *inverse different* for reasons that will soon become clear. Note of course that $\mathcal{C}$ depends explicitly on $\mathcal{O}_K$ and its integral closure in L so our notation is somewhat lacking, however clarification will be provided when confusion may arise. In any case, define the *different* $\mathcal{D} = \mathcal{C}^{-1}$. Again, the same remarks regarding notation applies to the different, for example we may write $\mathcal{D}_{L|K}$ or even $\mathcal{D}_{\mathcal{O}_L|\mathcal{O}_K}$ to specify the fields or Dedekind rings. Observe that $\mathcal{D} \subset \mathcal{O}_L$ so that the different is in fact an integral ideal.

Proposition 2.2.3.

(i) For a tower of fields $K \subseteq L \subseteq M$, one has $\mathcal{D}_{M|K} = \mathcal{D}_{L|K}\mathcal{D}_{M|L}$ (here $\mathcal{D}_{L|K}$ is identified with the ideal of $\mathcal{O}_M$ generated by $\mathcal{D}_{L|K} \subseteq \mathcal{O}_L$.

(ii) For any multiplicative subset S of $\mathcal{O}_K$, one has $\mathcal{D}_{S^{-1}\mathcal{O}_L|S^{-1}\mathcal{O}_K} = S^{-1}\mathcal{D}_{L|K}$.

(iii) If $P|p$ are prime ideals of $\mathcal{O}_L, \mathcal{O}_K$ respectively, and $\mathcal{O}_P|\mathcal{O}_p$ are the associated completions, then $\mathcal{D}_{\mathcal{O}_L|\mathcal{O}_K}\mathcal{O}_P = \mathcal{D}_{\mathcal{O}_P|\mathcal{O}_p}$.

Proof. (i) We assume that $\mathcal{O}_K$ is the Dedekind ring of K that these differents are defined with respect to and that $\mathcal{O}_L$ and $\mathcal{O}_M$ are the integral closures of $\mathcal{O}_K$ in their respective fields. It clearly suffices to show $\mathcal{C}_{M|K} = \mathcal{C}_{L|K}\mathcal{C}_{M|L}$, where again we identify $\mathcal{C}_{L|K}$ with the fractional ideal of M generated by $\mathcal{C}_{L|K} \subset L$.

Therefore suppose $x \in \mathcal{C}_{L|K}$ and $y \in \mathcal{C}_{M|L}$. Then

$$\begin{aligned} T_K^M(xy\mathcal{O}_M) &= T_K^L(T_L^M(xy\mathcal{O}_M)) \\ &= T_K^L(xT_L^M(y\mathcal{O}_M)) \\ &\subseteq T_K^L(x\mathcal{O}_L) \\ &\subseteq \mathcal{O}_K \end{aligned}$$

and so we have $\supseteq$. To get the reverse containment, suppose $z \in \mathcal{C}_{M|K}$ and $y \in \mathcal{D}_{L|K}$. Now we know $T_K^L(T_L^M(z)\mathcal{O}_L) = T_K^M(z\mathcal{O}_L)$ lies in $\mathcal{O}_K$, so $T_L^M(z) \in \mathcal{C}_{L|K}$. Hence $T_L^M(yz) = yT_L^M(z)$ must lie in $\mathcal{O}_L$. Therefore $\mathcal{D}_{L|K}\mathcal{C}_{M|K} \subseteq \mathcal{C}_{M|L}$, which suffices since $\mathcal{D}_{L|K} = (\mathcal{C}_{L|K})^{-1}$.

(ii) Again it suffices to prove $\mathcal{C}_{S^{-1}\mathcal{O}_L|S^{-1}\mathcal{O}_K} = S^{-1}\mathcal{C}_{\mathcal{O}_L|\mathcal{O}_K}$ by the first claim in (2.1.1). Suppose $x \in \mathcal{C}_{S^{-1}\mathcal{O}_L|S^{-1}\mathcal{O}_K}$. Then $T(x\mathcal{O}_L) \subset S^{-1}\mathcal{O}_K$, so by the usual finitely generated argument, we can find some $s \in S$ st. $sx \in \mathcal{C}_{\mathcal{O}_L|\mathcal{O}_K}$ which gives $\subseteq$. On the other hand if $y \in S^{-1}\mathcal{C}_{\mathcal{O}_L|\mathcal{O}_K}$, then $T(yS^{-1}\mathcal{O}_L) = S^{-1}T(y\mathcal{O}_L) \subseteq S^{-1}\mathcal{O}_K$.

(iii) See [22] pg. 196. □

An immediate corollary to (2.2.3 (iii)) is that the different can be determined locally, ie. $\mathcal{D}_{L|K} = \prod_P \mathcal{O}_L \cap \mathcal{D}_{L_P|K_p}$.

We now come to the property of the different that will be most useful to us in the sequel. Let $\alpha \in \mathcal{O}_L$ and $f(x) \in \mathcal{O}_K[x]$ the minimal polynomial for α. We define the *different of* α as

$$\delta_{L|K}(\alpha) = \begin{cases} f'(\alpha) & \text{if } L = K[\alpha]. \\ 0 & \text{if } L \neq K[\alpha]. \end{cases}$$

Proposition 2.2.4. *If* $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, *then* $\mathcal{D}_{L|K} = (\delta_{L|K}(\alpha))$.

Proof. Apply (2.1.5) and (2.2.1) to get $\mathcal{C} = f'(\alpha)^{-1}(\beta_0\mathcal{O}_K + ... + \beta_{n-1}\mathcal{O}_K)$, where the β_j satisfy the equation $\beta_0 + ... + \beta_{n-1}x^{n-1} = f(x)/(x-\alpha)$. Now $\beta_{n-1} = 1$ and $\beta_{k-1} - \alpha\beta_k = a_k$ for all $k < n$, where $f(x) = a_0 + ... + a_{n-1}x^{n-1} + x^n$. It is easy to determine the β_j recursively, and it turns out

$$\beta_{n-i} = \alpha^{i-1} + a_{n-1}\alpha^{i-2} + ... + a_{n-i+1}.$$

Since the a_i are all in $\mathcal{O}_K$, we have $\beta_0\mathcal{O}_K + ... + \beta_{n-1}\mathcal{O}_K = \mathcal{O}_K[\alpha] = \mathcal{O}_L$. Thus $\mathcal{D}_{L|K} = \mathcal{C}^{-1} = (f'(\alpha))$. □

It turns out that in general, $\mathcal{D}_{L|K}$ is the ideal generated by the differents of all the elements in $\mathcal{O}_L$ but this fact will not be needed. The interested reader is again directed to [22] for more details.

2.3 Ramification Groups

This introduction follows the directed exercises found in [19]. The motivation for introducing ramification groups is to prove a special case of Hilbert's formula (2.3.9), which will be used in the proof of the Kronecker-Weber theorem in the next section when we try to embed an arbitrary abelian field into a cyclotomic one. In what follows, assume L is a Galois extension of K, with Galois group G. Let $\mathcal{O}_K$, $\mathcal{O}_L$ be the corresponding number rings, and assume $Q \lhd \mathcal{O}_L$ is a prime that extends $P \lhd \mathcal{O}_K$. Let D and T be the corresponding decomposition and inertia subgroups.

Define the *ramification groups* for $m \geq 0$:

$$V_m(Q|P) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \mod Q^{m+1} \quad \forall \alpha \in \mathcal{O}_L\}.$$

Note that when no confusion will arise, we will simplify the notation to V_m. We now develop some preliminary results on ramification groups that will be useful in future proofs.

Proposition 2.3.1. *The ramification groups are normal in D and are all eventually the trivial subgroup.*

Proof. It is clear from the definition that $V_0 = T$ and that the ramification subgroups form a descending chain. Since G is finite, the chain must stabilize. Thus it suffices to show the intersection of the ramification groups is trivial.

$$\begin{aligned} \bigcap_{m\geq 0} V_m &= \{\sigma \in G : \sigma(\alpha) \equiv \alpha \mod Q^{m+1} \quad \forall m, \forall \alpha \in \mathcal{O}_L\} \\ \Rightarrow \sigma \in \bigcap_{m\geq 0} V_m &\Leftrightarrow \sigma(\alpha) - \alpha \in \bigcap_{m\geq 0} Q^{m+1} = \{0\} \quad \forall\ \alpha \in \mathcal{O}_L \\ &\Leftrightarrow \sigma = 1. \end{aligned}$$

Now suppose $\tau \in D$ and $\sigma \in V_m$. Then $\forall\ \alpha \in \mathcal{O}_L$, $\sigma\tau^{-1}(\alpha) - \tau^{-1}(\alpha) \in Q^{m+1}$ and so $\tau\sigma\tau^{-1}(\alpha) - \alpha \in \tau(Q^{m+1}) = Q^{m+1}$ which implies $\tau\sigma\tau^{-1} \in V_m$. Hence $V_m \lhd D$. □

We next prove for $m \geq 1$ that if $\sigma \in V_{m-1}$, it suffices to check its action on any element $\pi \in Q\backslash Q^2$ in order to determine if σ is in V_m.

Proposition 2.3.2. *Let $\pi \in Q\backslash Q^2$ and $m \geq 1$. If $\sigma \in V_{m-1}$, then $\sigma \in V_m \Leftrightarrow \sigma(\pi) \equiv \pi \mod Q^{m+1}$.*

Proof. One direction is obvious, so assume $\sigma(\pi) \equiv \pi \mod Q^{m+1}$ and we will fix $\alpha \in \mathcal{O}_L$. Suppose first that $\alpha \in \pi\mathcal{O}_L$, then $\alpha = \pi k$ for some k and

$$\begin{aligned}
\sigma(\alpha) - \alpha &= \sigma(\pi k) - \pi k \\
&= \sigma(\pi)\sigma(k) - \pi k \\
&= (\pi + \beta_1)(k + \beta_2) - \pi k \quad \text{where } \beta_1 \in Q^{m+1} \ \& \ \beta_2 \in Q^m \\
&= \beta_1\beta_2 + \beta_1 k + \beta_2\pi \\
&\equiv 0 \mod Q^{m+1}.
\end{aligned}$$

Now assume $\alpha \in Q$. Then $(\alpha) = Q \cdot J$ and $(\pi) = Q \cdot I$ where I is relatively prime with Q. By the Chinese Remainder Theorem, $\exists\ \beta \in I \backslash Q$ and hence $\alpha\beta \in (\pi)$.

$$\begin{aligned}
\Rightarrow \beta\sigma(\alpha) - \beta\alpha &= (\sigma(\beta) + k)\sigma(\alpha) - \beta\alpha \quad \text{for some } k \in Q^m \\
&= k\sigma(\alpha) + \sigma(\beta\alpha) - \beta\alpha \\
&\equiv k\sigma(\alpha) \mod Q^{m+1} \quad \text{by above} \\
&\equiv 0 \quad \text{because } \alpha \in Q \ \& \ k \in Q^m \\
\Rightarrow \beta(\sigma(\alpha) - \alpha) &\equiv 0 \mod Q^{m+1} \\
\Rightarrow \sigma(\alpha) - \alpha &\equiv 0 \quad \text{since } \beta \notin Q.
\end{aligned}$$

Finally we let α be arbitrary. Let L_T be the inertia field corresponding to Q and we note that since Q ramifies completely over L_T, the inclusion map $\mathcal{O}_{L_T} \hookrightarrow \mathcal{O}_L$ induces an isomorphism of residue fields. In particular, $\exists\ \beta \in \mathcal{O}_{L_T}$ st. $\beta \equiv \alpha \mod Q$. Since σ fixes L_T we have

$$\begin{aligned}
\sigma(\alpha) &= \sigma(\alpha - \beta) + \beta \\
&\equiv \alpha - \beta + \beta \mod Q^{m+1} \quad \text{since } \alpha - \beta \in Q \\
&\equiv \alpha.
\end{aligned}$$

□

Corollary 2.3.3. *Fix $\pi \in Q \backslash Q^2$. Then $\forall\ \sigma \in T$, $\sigma \in V_m \Leftrightarrow \sigma(\pi) \equiv \pi \mod Q^{m+1}$.*

Proof. One direction is obvious and for the other, simply apply the above proposition inductively. □

The next two propositions explore the relationship between consecutive ramification groups and in particular how they are influenced by the residue field $\mathcal{O}_L/Q$.

Proposition 2.3.4. *T/V_1 can be embedded into $(\mathcal{O}_L/Q)^\times$.*

Proof. Fix $\pi \in Q \backslash Q^2$ and let $\sigma \in T$ be arbitrary. Then $\pi\mathcal{O}_L = Q \cdot I$ with Q and I relatively prime, so by the CRT, $\exists\ x \in \mathcal{O}_L$, such that $x \equiv 0 \mod I$ and $x \equiv \sigma(\pi) \mod Q^2$.

$\Rightarrow x \in Q \cap I = (\pi)$

$\Rightarrow x = \pi\alpha \quad$ for some $\alpha \in \mathcal{O}_L$

$\Rightarrow \sigma(\pi) \equiv \pi\alpha \mod Q^2$.

Hence $\forall\ \sigma \in T$, $\exists\ \alpha \in \mathcal{O}_L$ st. $\sigma(\pi) \equiv \pi\alpha \mod Q^2$ and clearly α is uniquely determined mod Q. Now fix σ and let α_σ denote such an element as above. Note that $\alpha \notin Q$ since $\pi \notin Q^2$ and by (2.3.2), $\alpha \equiv 1$ iff $\sigma \in V_1$. Furthermore,

$$\begin{aligned} \alpha_{\sigma\tau}\pi &\equiv \sigma\tau(\pi) \\ &\equiv \sigma(\alpha_\tau \pi) \\ &\equiv \sigma(\alpha_\tau) \cdot \alpha_\sigma \pi \mod Q^2. \end{aligned}$$

Since $(\alpha_\tau - \sigma(\alpha_\tau))\alpha_\sigma\pi \in Q^2$, this implies $\alpha_{\sigma\tau}\pi \equiv \alpha_\sigma\alpha_\tau\pi$.

Finally let $\varphi : T \to (\mathcal{O}_L/Q)^\times, \varphi(\sigma) = \overline{\alpha_\sigma}$. Then φ is well-defined as α_σ is unique mod Q and the above shows φ is a group homomorphism with kernel V_1. Hence φ induces the desired embedding. $\square$

Corollary 2.3.5. *T/V_1 is cyclic of order dividing $q^{f(Q|q)} - 1$, where $q \in \mathbb{Z}$ is the prime lying under Q.*

Proposition 2.3.6. *For $m \geq 2, V_{m-1}/V_m \hookrightarrow \mathcal{O}_L/Q$ as an additive group.*

Proof. We proceed similarly to the previous proposition. Fix $\pi \in Q \backslash Q^2$ so that $(\pi) = Q \cdot I$ with Q and I relatively prime ideals. Let $\sigma \in V_{m-1}$ be arbitrary. Then $\sigma(\pi) = \pi + \beta$ for some $\beta \in Q^m$. By the CRT, $\exists\ x$ st. $x \equiv \beta \mod Q^{m+1}$ and $x \equiv 0 \mod I^m$.

$\Rightarrow x \in Q^m I^m$

$\Rightarrow x \in (\pi^m)$

$\Rightarrow \sigma(\pi) \equiv \pi + \beta \equiv \pi + \pi^m \alpha \mod Q^{m+1}$, where $\pi^m \alpha = x$.

It follows that for any $\sigma \in V_{m-1}$, $\exists\ \alpha$ st. $\sigma(\pi) \equiv \pi + \alpha\pi^m \mod Q^{m+1}$ and α is easily seen to be unique mod Q. Let α_σ denote such an element for each $\sigma \in V_{m-1}$,

$$\begin{aligned} \pi + \alpha_{\sigma\tau}\pi^m &\equiv \sigma\tau(\pi) \mod Q^{m+1} \\ &\equiv \sigma(\pi + \alpha - \tau\pi^m) \\ &\equiv \pi + \alpha\sigma\pi^m + \sigma(\alpha_\tau \pi^m). \end{aligned}$$

Considering the last term above,

$$\begin{aligned}
\sigma(\alpha_\tau\pi^m) - \alpha_\tau\pi^m &\equiv \sigma(\alpha_\tau)(\pi+\delta)^m - \alpha_\tau\pi^m \mod Q^{m+1} \quad \text{for some } \delta \in Q^m. \\
&\equiv \sigma(\alpha_\tau)(\pi^m - \alpha_\tau\pi^m) \quad \because m \geq 2. \\
&\equiv (\sigma(\alpha_\tau) - \alpha_\tau)\pi^m \\
&\equiv 0 \quad \because \sigma \in V_{m-1} \subset T.
\end{aligned}$$

Hence $\alpha_{\sigma\tau} \equiv \alpha_\sigma + \alpha_\tau \mod Q^{m+1}$ and therefore the map $\psi : V_{m-1} \to \mathcal{O}_L/Q$, $\psi(\sigma) = \alpha_\sigma$ is well defined and induces an injective group homomorphism from V_{m-1}/V_m into the additive group $\mathcal{O}_L/Q$. □

Corollary 2.3.7. *$V_1(Q|P)$ is the Sylow q-subgroup of $T(Q|P)$, where $q \in \mathbb{Z}$ is the prime lying under Q (and P).*

Proof. By (2.3.4), T/V_1 embeds into $(\mathcal{O}_L/Q)^\times$ which has order relatively prime to q. Thus T/V_1 contains the Sylow q-subgroup of T. On the other hand, by (2.3.6) and (2.3.1) $V_m/V_{m+1} \hookrightarrow \bigoplus_1^{f(Q|q)} \mathbb{Z}/q\mathbb{Z}$ and for sufficiently large n, $V_n = 1$.

$\therefore |V_1| = \prod_{i=1}^{n} |V_i/V_{i+1}|$ is a product of powers of q. □

Before moving on to proving a special case of Hilbert's formula, we give a strengthened version of (2.3.4) which will be used in the next section. In what follows, assume $\phi = \phi(Q|P)$ is any map in the decomposition group D such that $\phi(\alpha) \equiv \alpha^{||P||} \mod Q \quad \forall\ \alpha \in \mathcal{O}_L$.

Proposition 2.3.8. *Assume T/V_1 is abelian. Then the embedding of (2.3.4) actually maps T/V_1 into $(\mathcal{O}_K/P)^\times$.*

Proof. Fix π in $Q\backslash Q^2$ and $\sigma \in V_{m-1}, m \geq 1$. From the proof of (2.3.4) and (2.3.6), $\exists\ \alpha$ st. $\sigma(\pi) \equiv \alpha\pi \mod Q^{m+1}$. We claim that in fact $\sigma(x) \equiv \alpha x \mod Q^{m+1}$ for any $x \in Q$ (So that α does not depend on π). Indeed, suppose first that $x \in (\pi)$, say $x = \pi k$. Then

$$\begin{aligned}
\sigma(x) &= \sigma(\pi)\sigma(k) \\
&\equiv \alpha\pi\sigma(k) \mod Q^{m+1} \\
&= \alpha\pi(k+\beta) \quad \text{for some } \beta \in Q^m \\
&\equiv \alpha\pi k \\
&\equiv \alpha x \mod Q^{m+1}.
\end{aligned}$$

Next assume $x \in Q$ and choose a δ st. $\delta \in I\backslash Q$ where $Q \cdot I = (\pi)$. Then $\delta x \in (\pi)$ and $\sigma(\delta x) \equiv \alpha\delta x \mod Q^{m+1}$ by above, so

$$\begin{aligned}
\delta\sigma(x) - \sigma(\delta x) &= \sigma(x)(\delta - \sigma(\delta)) \\
&\equiv 0 \mod Q^{m+1} \quad \text{because } x \in Q \text{ and } \sigma \in V_{m-1}. \\
\Rightarrow \delta\sigma(x) &\equiv \delta\alpha x \mod Q^{m+1} \\
\Rightarrow \sigma(x) &\equiv \alpha x \quad \text{since } \delta \notin Q.
\end{aligned}$$

In particular, suppose $\sigma \in T = V_0$. Then $\phi^{-1}(\pi)$ lies in Q since π does. Hence

$$\phi\sigma\phi^{-1}(\pi) \equiv \phi(\alpha\phi^{-1}(\pi)) \equiv \alpha^{||P||}\pi \mod Q^2.$$

By assumption, T/V_1 is abelian, so $\phi\sigma\phi^{-1} = \sigma \in T/V_1$ and hence $\overline{\sigma} = \overline{\phi\sigma\phi^{-1}}$. Thus we deduce that $\alpha = \alpha^{||P||}$ in $(\mathcal{O}_L/Q)^\times$. Hence the induced embedding $\overline{\varphi}$ actually sends T/V_1 into $(\mathcal{O}_K/P)^\times$. □

We now prove a special case of Hilbert's formula. Our additional assumption will be that the prime $Q \lhd \mathcal{O}_L$ is completely ramified over $P \lhd \mathcal{O}_K$. The

general case follows easily from this special case combined with the tower formula for differents (2.2.3), but we shall not have need for it. In what follows, let $\mathcal{O}_Q$ and $\mathcal{O}_P$ denote the valuation rings in the complete fields L_Q and K_P respectively.

Theorem 2.3.9. *Assume P is completely ramified in L and let Q^k be the exact power of Q dividing the different $\mathcal{D}_{L/K}$. Then*

$$k = \sum_{m \geq 0} (|V_m| - 1).$$

Proof. By the remark following (2.2.3), as α, β run over the primes in $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively, we have

$$\mathcal{D}_{L/K} = \prod_{\alpha} \prod_{\beta|\alpha} (\mathcal{D}_{L_\beta/L_\alpha} \cap \mathcal{O}_L).$$

In particular, $Q^k = \mathcal{D}_{L_Q/L_P} \cap \mathcal{O}_L$. Let $\pi \in Q \backslash Q^2$ be arbitrary, then $K(\pi) = L$ and π generates the unique maximal ideal of $\mathcal{O}_Q$. Applying proposition 6.8 in chapter 2 of [22], $\mathcal{O}_Q$ is generated as an $\mathcal{O}_P$ module by $\{w_j \pi^i\}$, where $0 \leq i \leq e(Q|P) - 1$ and the w_j are representatives of a basis for $\mathcal{O}_L/Q$ over $\mathcal{O}_K/P$. Since $e(Q|P) = [L : K]$, $\mathcal{O}_L/Q = \mathcal{O}_K/P$ and so $\{1, \pi, ..., \pi^{e-1}\}$ forms such a basis. In particular, $\mathcal{O}_Q = \mathcal{O}_P[\pi]$ so $\mathcal{O}_Q$ is monogenous. By (2.2.4), this implies $\mathcal{D}_{L_Q/K_P} = (f'(\pi))$ where f is the minimum polynomial for π over K_P. Since $[L_Q : K_P] = e(Q|P) f(Q|P) = [L : K]$, f is also the minimum polynomial for π over K. Therefore Q^k is the exact power of Q dividing $(f'(\pi)) \lhd \mathcal{O}_L$.

Now suppose $\sigma \in V_{m-1} \backslash V_m$, so $(\pi - \sigma(\pi))\mathcal{O}_L$ is exactly divisible by Q^m. Since $f'(\pi) = \prod_{\sigma \in G} (\pi - \sigma(\pi))$ and P ramifies completely in L, $G = D = T$ and so

$$k = \sum_{m \geq 1} m |V_{m-1} - V_m| = \sum_{m \geq 0} |V_m - 1|,$$

where the last equality comes from a simple counting argument (if $\sigma \in V_{m-1} \backslash V_m$, then σ will contribute to exactly m terms on the right hand side of the equality). $\square$

CHAPTER 3
The Kronecker-Weber Theorem

Given a suitable function $f(x)$ whose roots generate an abelian extension K of $\mathbb{Q}$, our next order of business is to systematically find a suitable N_K such that K embeds into $\mathbb{Q}(\omega_{N_K})$. Such an N exists in general, as guaranteed by the Kronecker-Weber theorem and we now prove there exists a suitable N that depends only on the degree of the extension $[K:\mathbb{Q}]$ and the primes of $\mathbb{Z}$ that ramify in K. The proof will follow the directed exercises found in chapter 4 of [19].

Theorem 3.0.1. *Let K be an abelian extension of $\mathbb{Q}$ st. $[K:\mathbb{Q}] = n = \prod_{i=1}^{k} q_i^{r_i}$ and let $A := \{p_1, p_2, ..., p_t\}$ be the set of all primes of $\mathbb{Z}$ that ramify in K. If $2 \in A$ then define m to be $2\prod p_i$, otherwise let $m = \prod p_i$. Then $K \subseteq \mathbb{Q}(\omega_{mn})$.*

Proof. Observe first that since $G = \mathrm{Gal}(K/\mathbb{Q})$ is abelian, we have

$$G \cong S_{q_1} \times S_{q_2} \times ... \times S_{q_k}$$

where each S_{q_i} is the Sylow q_i-subgroup of G. Hence $K = L_{q_1}L_{q_2}...L_{q_k}$, where L_{q_i} is the fixed field of $\prod_{j\neq i} S_{q_j}$ and $[L_{q_i} : \mathbb{Q}] = |S_{q_i}| = q_i^{r_i}$. Clearly then it is enough to show each $L_{q_i} \subseteq \mathbb{Q}(\omega_t)$ for some $t|nm$ because if a and b are positive integers, we have the identity $\mathbb{Q}(\omega_a)\mathbb{Q}(\omega_b) = \mathbb{Q}(\omega_{lcm(a,b)})$. Let t be the product of the primes that ramify in L_{q_i} with $q_i^{r_i}$ (and an additional factor of 2 if 2 ramifies in L_{q_i}). We note that the primes ramifying in L_{q_i} form a subset of the primes ramifying in L, and certainly $q_i^{r_i}$ divides m. Hence t divides

nm and we have reduced the problem to the case where K is an extension of $\mathbb{Q}$ of prime power degree.

Henceforth we assume $[K : \mathbb{Q}] = q^r$ for some prime q. The next step is to reduce to the case where q is the only prime that ramifies in K.

Suppose $p \neq q$ ramifies in K. Let P be a prime of K lying over p and let $e = e(P|p)$ be the ramification index. Recall from (2.3.7) that the ramification group $V_1(P|p)$ is the Sylow p-subgroup of the inertia group $T(P|p)$. Since $T \leq G$ and $|G| = q^r$, we must have $V_1 = \{1\}$. By (2.3.8), T/V_1 embeds into $(\mathbb{Z}/p\mathbb{Z})^\times$ and hence $e = |T|$ divides $p - 1$. Since $\mathrm{Gal}(\mathbb{Q}(\omega_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ which is cyclic of order $p - 1$, we deduce $\exists!$ subfield $L \subseteq \mathbb{Q}(\omega_p)$ of degree e over $\mathbb{Q}$. Clearly p ramifies completely in L since it does in $\mathbb{Q}(\omega_p)$. Observe that the only primes ramifying in LK are the ones ramifying in K, since the only prime that ramifies in $\mathbb{Q}(\omega_p)$ and hence L, is p.

Let $U \lhd \mathcal{O}_{LK}$ be a prime lying over P and let $K' \subseteq LK$ be the fixed field of $T(U|p)$. Then p is unramified in K' since it is the inertia field of U over p, as are all primes that are unramified in K. The canonical mapping of $\mathrm{Gal}(LK/\mathbb{Q})$ into $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ via restriction embeds $T(U|p)$ into $T(P|p) \times \mathrm{Gal}(L/\mathbb{Q})$, which is a subgroup of order e^2 and in particular is a power of q. Hence we note once again that $V_1(U|p) = \{1\}$ by its Sylow subgroup characterization and therefore by (2.3.7), $T(U|p) \cong T(U|p)/V_1(U|p) \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$. In particular, this shows $T(U|p)$ is cyclic. Combining this fact with the embedding of $T(U|p)$ into $T(P|p) \times \mathrm{Gal}(L/\mathbb{Q})$, which is a group of exponent e, we deduce $|T(U|p)| \leq e$. On the other hand the ramification degree of p in $\mathcal{O}_{LK}$ is at least the ramification degree of p in $\mathcal{O}_K$ which is precisely e, thus $|T(U|p)| = e$.

Since $|T(U|p)| = e$, we can conclude that U must be unramified over L. Furthermore, $[LK : K'] = |T(U|p)| = e = [L : \mathbb{Q}]$. As observed earlier, q is totally ramified in L and unramified in K', hence $L \cap K' = \mathbb{Q}$ and thus $[LK' : K'] = [L : \mathbb{Q}] = e$. It follows that $LK' = LK$. Finally note that

$$\begin{aligned}
[K' : \mathbb{Q}] &= \frac{[LK' : \mathbb{Q}]}{[LK' : K']} \\
&= \frac{[LK : L][L : \mathbb{Q}]}{[LK' : K']} \\
&= [K : L \cap K] \\
&= q^t, \text{ for some } t \leq r.
\end{aligned}$$

Thus we have found a field K' such that the only possible primes that ramify in K' are the primes that ramify in K, with the exception of q. Furthermore, $[K' : \mathbb{Q}]$ divides $[K : \mathbb{Q}]$ and since $LK' = LK$ for some field $L \subseteq \mathbb{Q}(\omega_q)$, if K' lies in the s^{th}-cyclotomic field, then K must lie in the sq^{th}-cyclotomic field. Applying this argument repeatedly for every prime in K not equal to p, we reduce to the case where K is a finite extension of $\mathbb{Q}$ of prime power order p^r and p is the only prime that ramifies in K. Thus it suffices to show that K lies in $\mathbb{Q}(\omega_{p^{r+1}})$ when $p \neq 2$ and $\mathbb{Q}(\omega_{2^{r+2}})$ otherwise.

Case 1: $p = 2, [K : \mathbb{Q}] = 2^r$.

Subcase 1: $r = 1$.

Since K is a quadratic extension, $K = \mathbb{Q}(\sqrt{m})$ for some squarefree integer m. It is well known (see for example [19] pg. 33) that the discriminant of a quadratic number field satisfies the following formula:

$$\Delta\mathbb{Q}(\sqrt{m}) = \begin{cases} m & \text{if } m \equiv 1 \bmod 4 \\ 4m & \text{if } m \equiv 2, 3 \bmod 4. \end{cases}$$

As 2 is the only prime that ramifies in K, the discriminant Δ must be a power of 2 (Up to a sign). It follows by inspection that the only possibilities for a squarefree m are $m = 2, -1$, or -2. In any case, $\mathbb{Q}(\omega_8) \supset \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$ hence $\mathbb{Q}(\omega_8) \supset K$. This completes the proof of the first subcase.

Subcase 2: $r > 1$.

Since $[K : K \cap \mathbb{R}]$ is either 1 or 2, then necessarily $[K \cap \mathbb{R} : \mathbb{Q}] \geq 2$. Using the fact that $\mathrm{Gal}(K \cap \mathbb{R}/\mathbb{Q})$ is abelian and divisible by 2, it must have a subgroup of index 2. Thus $K \cap \mathbb{R}$ contains a quadratic subfield, and by the previous subcase, that subfield must be $\mathbb{Q}(\sqrt{2})$.

Let $L = \mathbb{Q}(\omega_{2^{r+2}}) \cap \mathbb{R}$, so $[L : \mathbb{Q}] = 2^r$ and 2 is the only prime that ramifies in L as it is the only prime that ramifies in $\mathbb{Q}(\omega_{2^{r+2}})$. By the above comments, L also contains $\mathbb{Q}(\sqrt{2})$ and this is the unique quadratic subfield contained in L. The Galois group of L is cyclic as it is isomorphic to the cyclic group $(\mathbb{Z}/2^{r+2}\mathbb{Z})^\times/\{\pm 1\}$. Let σ be a generator and extend σ to $\tau \in \mathrm{Gal}(LK/\mathbb{Q})$. Let F be the fixed field of τ. Clearly $[F : \mathbb{Q}]$ is a power of 2, and we conclude either 1 or 2, for if $[F : \mathbb{Q}] > 2$, $F \supset \mathbb{Q}(\sqrt{2})$, contradicting the fact that $F \cap L = \mathbb{Q}$ since τ restricted to L is σ. Hence from the discussion in subcase 1, $F = \mathbb{Q}$, $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$.

Next we note that the canonical embedding of $\mathrm{Gal}(LK/\mathbb{Q})$ into $\mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$ sends τ to $(\sigma, \tau|_K)$. We conclude that τ has order 2^r. Indeed, τ has order at least that of $(\sigma, 1)$, which generates a subgroup of order 2^r, but on the other hand the group $\mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$ has exponent 2^r. Finally, note that

$$\begin{aligned}
|\mathrm{Gal}(LK/\mathbb{Q})| &= |<\tau>||\mathrm{Gal}(LK/\mathbb{Q})/<\tau>| \\
&= 2^r[F:\mathbb{Q}] \\
&= \begin{cases} 2^r & \text{if } F = \mathbb{Q} \\ 2^{r+1} & \text{if } F = \mathbb{Q}(\sqrt{-1}) \text{ or } \mathbb{Q}(\sqrt{-2}). \end{cases}
\end{aligned}$$

In any case, it follows that $LK = LF \subseteq L(\sqrt{-1}, \sqrt{-2}) = \mathbb{Q}(\omega_{2^{r+2}})$ and in particular, $\mathbb{Q}(\omega_{2^{r+2}}) \supset K$. This concludes the proof in the case that $p = 2$.

Case 2: $p \neq 2, [K:\mathbb{Q}] = p^r$.

Before we can draw the desired conclusion in general, we are going to make use of the material found in section (2.2) regarding the different of a number field. Assume first that $r = 1$ and let $P \lhd K$ be a prime lying over p. Then p ramifies in K and since K is Galois over $\mathbb{Q}$, the subgroup $T(P|p) \leq \mathrm{Gal}(K/\mathbb{Q})$ is non-trivial. But $G = \mathrm{Gal}(K/\mathbb{Q})$ has prime order p and hence $T(P|p)$ is the whole group. In particular p ramifies completely in K. Now fix some element $\alpha \in P \backslash P^2$. Because $P \cap \mathbb{Q} = P^2 \cap \mathbb{Q} = (p)$, this implies $\alpha \notin \mathbb{Q}$ and since $[K:\mathbb{Q}]$ has prime order, we must have $\mathbb{Q}(\alpha) = K$. Hence the minimum polynomial

$$f(x) = x^p + a_{p-1}x^{p-1} + ... + a_0 \tag{3.1}$$

for α over $\mathbb{Q}$ lies in $\mathbb{Z}[x]$ and has degree p.

Since p is totally ramified in K, by Hilbert's formula (2.3.9) we know the exact power k of P dividing the different $\mathcal{D}_{K/\mathbb{Q}}$ is equal to

$$k = \sum_{m \geq 0} |V_m| - 1.$$

Note that since G is cyclic of order p, every V_m has order either p or 1. Hence $p-1|k$.

On the other hand, the exact power P dividing $\mathcal{D}_{K/\mathbb{Q}}$ is equal to the exact power dividing the ideal $(f'(\alpha)) \lhd K$ (See the proof of (2.3.9)). Substituting α into (3.1) and reducing mod P, followed by mod P^2, up to mod $P^p = (p)$ we see respectively that $a_0, a_1, ..., a_{p-1} \in P \cap \mathbb{Q} = (p)$. Thus every term in

$$f'(\alpha) = p\alpha^{p-1} + (p-1)a_{p-1}\alpha^{p-2} + ... + a_1$$

generates an ideal divisible by P. Moreover, the power k_i of P dividing $(ia_{p-i}\alpha^i)$ must be congruent with $i \bmod p$ for $1 \leq i \leq p$ (here $a_p = 1$) since $P^p = (p)$. In particular each k_i is distinct and hence $k = \min\{k_1, ..., k_p\}$. Keeping this in mind, we note that $k_p = p+p-1 < 3(p-1)$ and $k_i \geq p > p-1 \ \forall \ i$. Thus the divisibility condition $p-1|k$ immediately implies $k = 2(p-1)$. Since primes of K divide $\mathcal{D}_{K/\mathbb{Q}}$ iff they ramify over $\mathbb{Q}$, we conclude that $\mathcal{D}_{K/\mathbb{Q}} = P^{2(p-1)}$

We now temporarily leave our current case, and consider the case when $r = 2$, again with the assumption that P is a prime of K lying over p. We note once again that since p must ramify, $e(P|p) = p^2$ or p. Clearly the first case holds, since in the latter, the corresponding inertia field would give a non-trivial field extension of $\mathbb{Q}$ with no ramified primes. Indeed the same reasoning holds for any $r \geq 1$, so we always have p ramifying completely. By the Sylow p-subgroup characterization of $V_1(P|p)$, we conclude $V_1 = T(P|p) = \mathrm{Gal}(K/\mathbb{Q})$. Let $k' > 1$ be the smallest integer such that $V_{k'} \neq \mathrm{Gal}(K/\mathbb{Q})$. By (2.3.6), we know V_{k-1}/V_k embeds into the additive group $\mathcal{O}_K/P \cong \mathbb{Z}/p\mathbb{Z}$ for $k \geq 2$ and hence $|V_{k'}| = p$. Let $H \leq \mathrm{Gal}(K/\mathbb{Q})$ be an arbitrary subgroup such that $|H| = p$ and let K_H be the corresponding fixed field. Applying our results

from the case when $r = 1$ to H_k with the tower formula for differents (2.2.3), we get

$$\begin{aligned}\mathcal{D}_{K/\mathbb{Q}} &= \mathcal{D}_{K/K_H} \cdot \mathcal{D}_{K_H/\mathbb{Q}} \\ &= \mathcal{D}_{K/K_H} \cdot Q^{2(p-1)}\mathcal{O}_K \\ &= \mathcal{D}_{K/K_H} \cdot P^{2p(p-1)}.\end{aligned}$$

where $Q = P \cap K_H$. This shows that $\mathcal{D}_{K/K_H}$ is independent of the choice of H. On the other hand, if k is the maximum power of P dividing $\mathcal{D}_{K/K_H}$, then

$$k = \sum_{m \geq 0} |V_m \cap H| - 1$$

again by the Hilbert Formula for completely ramified primes. This implies if $H \neq V_{k'}$, then $k = k'(p-1)$ while $H = V_{k'}$ implies $k \geq (k'+1)(p-1)$. These observations can only be reconciled by the conclusion that $V_{k'}$ is the unique subgroup of order p and hence $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/p^2\mathbb{Z}$.

Returning back to the case where $r = 1$, we use what we have just shown. Assume now that there are two distinct number fields $K \neq K'$ such that $[K : \mathbb{Q}] = [K' : \mathbb{Q}] = p$ and p is the only prime that ramifies in either extension (thus it ramifies in both). Then KK' is a number field that must satisfy the conclusions just drawn for the case when $r = 2$, that is to say $\mathrm{Gal}(KK'/\mathbb{Q})$ is cyclic which is clearly absurd. Hence K is unique and so it remains to find a field that satisfies the conditions on K. Inspection reveals that the unique subgroup $H \leq \mathrm{Gal}(\mathbb{Q}(\omega_{p^2})/\mathbb{Q})$ of order $p-1$ fixes an abelian number field of degree p over $\mathbb{Q}$ and p is the only prime that ramifies in it. Hence K must be this fixed field, which we will denote K^* for future reference and clearly $K = K^* \subset \mathbb{Q}(\omega_{p^2})$, proving the assertion for the case that $r = 1$.

It remains to show the theorem is true for $r > 1$ and p an odd prime; we proceed similarly to the case when $p = 2$. Let L be the unique subfield of $\mathbb{Q}(\omega_{p^{r+1}})$ with degree p^r over $\mathbb{Q}$ (Note that we have uniqueness as the Galois group is isomorphic to $(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times$, which is well known to be cyclic of order $p^r(p-1)$ for any odd prime). Then $\mathbb{Z}/p^r\mathbb{Z} \cong \mathrm{Gal}(L/\mathbb{Q}) =< \sigma >$, so extend σ to $\tau \in \mathrm{Gal}(LK/\mathbb{Q})$ and let F be the fixed field of τ. Then F is abelian over $\mathbb{Q}$, $[F : \mathbb{Q}] = p^t$ for some t, and p is the only prime that ramifies in F, which it does completely. As in the case with $p = 2$, we conclude $F \cap L = \mathbb{Q}$ and in fact, if $F \neq \mathbb{Q}$ then F contains K^* by uniqueness, as does K and more importantly L. Hence $F = \mathbb{Q}$, so by the Fundamental Theorem for Galois Theory, $< \tau >$ equals $\mathrm{Gal}(LK/\mathbb{Q})$. Since $\mathrm{Gal}(LK/\mathbb{Q})$ embeds into $\mathrm{Gal}(L/\mathbb{Q})\times\mathrm{Gal}(K/\mathbb{Q})$, the latter group being a group of exponent p^r, we have $p^r = |\sigma| \leq |\tau| \leq p^r$. We conclude that $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(LK/\mathbb{Q})$ and therefore $K = L$. Hence $K \subset \mathbb{Q}(\omega_{p^{r+1}})$. □

We can immediately strengthen this theorem slightly with the following lemma.

Lemma 3.0.2. *Let K be a field contained in the N^{th}-cyclotomic field. Suppose $m \in \mathbb{Z}$ is a prime that does not ramify in K. Writing $N = m^k N'$ for some $k \in \mathbb{N}$ and $(m, N') = 1$, then $K \subseteq \mathbb{Q}(\omega_{N'})$.*

Proof. The proof revolves around the inertia subgroup T_m of $\mathrm{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$. The fixed field of T_m is the largest subfield of $\mathbb{Q}(\omega_N)$ in which m does not ramify, and the degree of that field over $\mathbb{Q}$ must be less then or equal to $\frac{\varphi(N)}{\varphi(m^k)} = \varphi(N')$ since m ramifies completely in the $(m^k)^{th}$ cyclotomic field, which is contained in $\mathbb{Q}(\omega_N)$. Since $\mathbb{Q}(\omega_{N'})$ satisfies both the degree and ramification

conditions, it follows that it is the fixed field of T_m. By hypothesis, m does not ramify in K, so $K \subseteq \mathbb{Q}(\omega_{N'})$ as claimed. $\square$

Corollary 3.0.3. *Let K be an abelian extension of $\mathbb{Q}$ and let $A := \{p_1, p_2, ..., p_t\}$ be the set of all primes of $\mathbb{Z}$ that ramify in K. Assume $[K : \mathbb{Q}] = n = (\prod_{i=1}^{t} p_i^{r_i}) \cdot n' = \mu \cdot n'$, where $(n', p_i) = 1 \; \forall \; p_i \in A$. If $2 \in A$ then define m to be $2\prod p_i$, otherwise let $m = \prod p_i$. Then $K \subseteq \mathbb{Q}(\omega_{m\mu})$.*

Proof. Apply theorem (3.0.1), followed by lemma (3.0.2) to all primes dividing n that do not ramify in K. $\square$

CHAPTER 4

Zeta Functions at Negative Integers for Abelian Number Fields

4.1 Determining Characters

We have seen from (3.0.1) that given an abelian extension K of $\mathbb{Q}$, we can find a suitable $N \in \mathbb{N}$, depending only on the degree $[K : \mathbb{Q}]$ and the primes that ramify, such that $\mathbb{Q}(\omega_N) \supseteq K$. Finding this N is a critical first step in our quest to determine the character group of K and ultimately its Dedekind zeta function, as we have a firm understanding of the character group of $(\mathbb{Z}/N\mathbb{Z})^\times$ and its quotient groups (see section 1). Note that in this section we will always mean "Dirichlet character" or "Dirichlet character group" when we say "character" or "character group", unless otherwise noted.

Recall from (1.3.8) that if $K \subseteq \mathbb{Q}(\omega_N)$, then for $\Re(z) > 1$ we have the formula

$$\zeta_K(s) = \prod_{\chi \in \widehat{G}} L(s, \chi).$$

The goal of this section will thus be to develop a systematic way in which we can produce all the elements in $\widehat{G}$, under the assumption that the Galois group G of K is known to be a quotient group of the Galois group of $\mathbb{Q}(\omega_N)$.

The first question one comes upon when considering this problem is how to find the precise quotient group that $\mathrm{Gal}(K/\mathbb{Q})$ represents. That is to say, what subgroup $H \leq \mathrm{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ fixes K and how can we find it? For ease of notation, in what follows we identify H and $\mathrm{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ with their respective images under the canonical isomorphism into $(\mathbb{Z}/N\mathbb{Z})^\times$. It is well

known that the decomposition of unramified primes in $\mathbb{Q}(\omega_N)$ is determined entirely by congruency classes mod N. The following lemma shows this also holds for any subfield of $\mathbb{Q}(\omega_N)$ as well.

Lemma 4.1.1. *Assume $K \subseteq \mathbb{Q}(\omega_N)$ is an abelian extension of $\mathbb{Q}$. Let $H \leq (\mathbb{Z}/N\mathbb{Z})^\times$ be the corresponding subgroup fixing K and $p \in \mathbb{Q}$ any prime that does not divide N. Then the inertia index f_p of p in K is equal to the order of $\overline{p}$ in $(\mathbb{Z}/N\mathbb{Z})^\times/H$ and (p) splits into $\frac{|(\mathbb{Z}/N\mathbb{Z})^\times/H|}{f_p}$ distinct primes.*

Proof. Since p does not divide N, p does not divide the discriminant of $\mathbb{Q}(\omega_N)$ and so is unramified there and hence also in K. Thus it suffices to prove the statement about f_p, as $f_p \cdot r_p = |(\mathbb{Z}/N\mathbb{Z})^\times/H|$. Let φ be the Frobenius automorphism of p for $\mathbb{Q}(\omega_N)$ so that its restriction to K is the Frobenius automorphism for that field. Then f_p equals the order of $\varphi|_K$ in $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times/H$ and $\varphi|_K$ is sent to $\overline{p}$ under this isomorphism. The result follows. □

We can now use the lemma to determine the subgroup H. We consider the following procedure:

0. [Input] Irreducible, monic $f(x) \in \mathbb{Q}[x]$ such that f generates an abelian extension.

1. [Initialize] Set $D \leftarrow$ discriminant of f. $N \leftarrow \deg(f)$.
$H \leftarrow \{1\} \subset (\mathbb{Z}/N\mathbb{Z})^\times$. $m \leftarrow 2$.

2. For $p|D$, p prime, set $N \leftarrow N \cdot p$ if $p \neq 2$. $N \leftarrow N \cdot 4$ if $p = 2$.

3. If $(m, N) = 1$ and $m \notin H$, factor $f \mod q$, where q is any prime congruent to m mod N and $q \nmid D$. If f splits mod q, $H \leftarrow < H, m >$.

4. [Finished?] If $|H| = \phi(N)/\deg(f)$ then return N, H. Otherwise, $m \leftarrow m + 1$ and goto step 3.

We use the theory developed to check that if f generates K, then the above algorithm returns the subgroup of $\mathrm{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ that fixes K, where K is a subfield of $\mathbb{Q}(\omega_N)$. The latter fact follows immediately from (3.0.1) and the fact that primes ramify in K only if they divide the discriminant of any generating polynomial. To check that the subgroup is correct, note that (1.6.3) tells us that the Galois extension K is entirely characterized by the primes that split completely in it. On the other hand, (4.1.1) tells us that almost all primes in $\mathbb{Q}$ decompose in K entirely based on two factors, namely their congruency group mod N and the subgroup H. In particular, p splits completely in K iff $\overline{p} \in H \leq (\mathbb{Z}/N\mathbb{Z})^\times$. Hence to determine H, it suffices to find one prime in every congruency class of $(\mathbb{Z}/N\mathbb{Z})^\times$ and find its factorization into prime ideals of K. Of course since we are given a function f whose zeros generate K, this is no problem for any prime q of $\mathbb{Z}$ that does not divide the discriminant of f, as the factorization of (q) into ideals of K corresponds to the factorization of f modulo q. Thus the procedure outlined above is sound.

Before moving on, we remark that there are a number of ways to improve the efficiency of the above procedure in practice. In particular, finding a prime congruent to some unit of $\mathbb{Z}/N\mathbb{Z}$, while possible by Dirichlet's theorem, can be computationally quite expensive for large N. There are a few ways to minimize the number of times this needs to be done, such as evaluating f at small integers and factoring. Any primes appearing in this factorization must necessarily generate a subgroup of H, as long as they do not also divide the discriminant of f. One can also consider the order of the element m in $(\mathbb{Z}/N\mathbb{Z})^\times$. Depending on the order of H, this may rule out m being a possible element of H. Furthermore, the quotient group is isomorphic to the Galois group of K, hence one can use the exponent e of $\mathrm{Gal}(K/\mathbb{Q})$ to deduce that m^e

must lie in H for all m. Another approach is to note that if $< m >=< n >$, then $m \in H$ iff $n \in H$.

Now that we have a method to determine the precise subgroup H of $\mathrm{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ that fixes K, the next step in our journey will be to find the character group, $\widehat{G}$. Conveniently for us $G = (\mathbb{Z}/N\mathbb{Z})^\times/H$ so by (1.1.4), its corresponding group of characters is

$$\{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times} : \chi|_H \equiv 1\}.$$

Since we now know what the group H looks like in $(\mathbb{Z}/N\mathbb{Z})^\times$, $\widehat{G}$ can be determined by simply computing all the characters of $(\mathbb{Z}/N\mathbb{Z})^\times$ and then checking which ones are identically 1 on H. In fact we can get away with only computing the characters whose orders divide $[K : \mathbb{Q}]$. This is because the character group of G is isomorphic to G and hence only has $[K : \mathbb{Q}]$ elements in it. This is theoretically very convenient if N is easily factored because if $N = 2^{r_0}p_1^{r_1}...p_n^{r_n}$ is a prime decomposition, then

$$\widehat{(\mathbb{Z}/N\mathbb{Z})^\times} \cong \widehat{(\mathbb{Z}/2^{r_0}\mathbb{Z})^\times} \times \prod_{i=1}^{n} \widehat{(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times} \cong (\mathbb{Z}/2^{r_0}\mathbb{Z})^\times \times \prod_{i=1}^{n} (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$$

where by (1.1.1), the identification between $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times =< \overline{a_i} >$ and its character group is given by $\overline{a_i}^t \to \chi_{a_i^t}$, where $\chi_{a_i^t}$ is the unique primitive character that satisfies $\chi_{a_i^t}(a_i) = \omega^t_{p_i^{r_i-1}(p-1)}$ when considered as a map on $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$. Calculating $\widehat{G}$ when H is known thus reduces to finding generators of $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$, a topic that is discussed in Appendix A. We can then use these generators to find explicit representations for all appropriate elements of $\widehat{(\mathbb{Z}/N\mathbb{Z})^\times}$, and then check which elements act trivially on H.

The above argument has thus verified the soundness of the following algorithm, which returns $\widehat{G}$:

0. [Input] Irreducible, monic $f(x) \in \mathbb{Q}[x]$ such that f generates an abelian extension.

1. [Initialize] $N \leftarrow \prod p_i^{r_i}$, an integer such that $\mathbb{Q}(\omega_N)$ contains the splitting field of f. $H \leq (\mathbb{Z}/N\mathbb{Z})^\times$ corresponding to splitting field of f. $\widehat{G} \leftarrow \{1\}$. For primes $p_i|N$, construct Dirichlet character group A_i of $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$. $A \leftarrow \prod A_i$.

2. For $\psi \in A$, if $\psi(m) = 1 \ \forall \ m \in H$ then $\widehat{G} \leftarrow < \widehat{G}, \psi >$.

3. [Output] Return $\widehat{G}$.

Before moving on to an example of this theory in action, we should first note that a few additional pieces of information have fallen out along the way. Indeed, one notes that since we have given an explicit way to calculate all the Dirichlet characters mod N of $\mathrm{Gal}(K/\mathbb{Q})$, by (1.2.3) we can calculate the conductor and also the discriminant of K via the Conductor-Discriminant formula (See [26] pg. 28)

$$\Delta(K) = (-1)^{s_2} \prod_{\chi \in \widehat{G}} f_\chi,$$

where s_2 is half the number of complex embeddings of K.

Example:

We will now calculate an example to illustrate the above theory in practice.

Consider the monic, irreducible polynomial $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$. The corresponding resolvent polynomial is $h(x) = x^3 + 10x^2 - 4x - 40$ which has zeros at ± 2 and 10. It follows from general Galois theory that the splitting field K of f has Galois group isomorphic to V_4 and in particular is abelian over $\mathbb{Q}$. Thus the theory of the previous two sections applies and we use it

to determine a formula for $\zeta_K(s)$ on the right half plane $\Re(s) > 1$. Our first step is to find all the primes that ramify in K or equivalently, all primes that divide $\Delta(K)$. Since $\Delta(K)|\Delta(f)$, it suffices to find and factor $\Delta(f)$,

$$\Delta(f) = \Delta(h) = (10-2)^2(10+2)^2(2+2)^2 = 2^{14}3^2.$$

By (3.0.1), it follows that $K \subseteq \mathbb{Q}(\omega_{48})$. Let G be the Galois group for K over $\mathbb{Q}$ and identify $\mathrm{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ with $(\mathbb{Z}/48\mathbb{Z})^\times$. Let H be the subgroup of $(\mathbb{Z}/48\mathbb{Z})^\times$ that fixes K. Since H has order $\frac{\varphi(48)}{[K:\mathbb{Q}]} = 4$, there are precisely three non-trivial equivalence classes in $(\mathbb{Z}/48\mathbb{Z})^\times$ that cause f to split completely after reducing modulo any prime in that class. Recall that since we are dealing with Galois extensions, it suffices to find only one linear factor modulo any given prime to know that f splits completely (this is a fact that we used in the remarks following the algorithm to find H). Ideally one would have a computer program to do this by calculating $\mathrm{GCD}(f, x^{p-1} - 1) \bmod p$, but since we are doing this by hand, we will simply calculate the first few values of f and factor them. Any prime factors arising that are not 2 or 3 must necessarily lie in H.

$$f(0) = 1, \quad f(1) = -2^3, \quad f(2) = -23,$$
$$f(3) = -2^3, \quad f(4) = 97, \quad f(5) = 2^3 47.$$

Since $47 \cdot 23 \equiv 25 \bmod 48$, the above 6 calculations show that $H = \{\overline{1}, \overline{23}, \overline{25}, \overline{47}\}$.

Now that we have H, we can begin calculating characters. We first note that

$$\mathbb{Z}_{48}^\times \cong \mathbb{Z}_{16}^\times \times \mathbb{Z}_3^\times = < \overline{-1}, \overline{5} > \times < \overline{-1} >$$

and this isomorphism shows that the character group is generated by 3 elements $\{\chi_{-1}, \chi_5, \tau\}$, where

$$\chi_{-1}(\pm\overline{5}^m, \overline{-1}^n) = \pm 1$$
$$\chi_5(\pm\overline{5}^m, \overline{-1}^n) = i^m$$
$$\tau(\pm\overline{5}^m, \overline{(-1)}^n) = (-1)^n.$$

Under the above identification, H is sent to $\{(\overline{1}, \overline{1}), (\overline{7}, \overline{2}), (\overline{9}, \overline{1}), (\overline{15}, \overline{2})\}$ or writing in terms of generators, $H = \{(\overline{1}, \overline{1}), (\overline{-1} \cdot \overline{5}^2, \overline{-1}), (\overline{5}^2, \overline{1}), (\overline{-1}, \overline{-1})\}$. One easily checks that the subset of characters that act trivially on H is therefore $\{1, \chi_{-1}\tau, \chi_5^2, \chi_{-1}\chi_5^2\tau\}$ which we identify as $\widehat{G}$ (more specifically, we identify these characters with their associated primitive Dirichlet characters). If we view χ_5 as a character of $(\mathbb{Z}/16\mathbb{Z})^\times$, then one checks directly that

$$\begin{aligned} \chi_5^2(\overline{1}) &= 1 = \chi_5^2(\overline{9}) \\ \chi_5^2(\overline{5}) &= -1 = \chi_5^2(\overline{13}) \\ \chi_5^2(\overline{5}) &\neq \chi_5^2(\overline{1}) \end{aligned}$$

Since χ_5^2 is even, this shows it is well defined modulo 8 but not modulo 4 and hence is a primitive character mod 8. Hence we identify χ_5^2 as the character on $(\mathbb{Z}/8\mathbb{Z})^\times$ that sends -1 to 1 and 5 to -1. It is easy to see χ_{-1} and τ necessarily have conductors 4 and 3 respectively and since they are non-trivial, this defines them uniquely as Dirichlet characters mod 4 and mod 3 respectively. Thus $\chi_{-1}\tau$ is a primitive character mod 12 and likewise $\chi_{-1}\chi_5^2\tau$ is a primitive character mod 24. Hence the smallest cyclotomic field containing K is the 24^{th} and the discriminant $\Delta(K) = (-1)^r 2304 = (-1)^r 2^8 3^2$. Note that every character in H is even and therefore K is totally real, so $r = 0$ by (1.2.4).

Putting everything together we now have an expression for $\zeta_K(s)$ when $\Re(s) > 1$,

$$\zeta_K(s) = \prod_{\chi \in \widehat{G}} L(s, \chi).$$

For completeness sake, we compute the first few terms of the Dirichlet series corresponding to each element of $\widehat{G}$ below.

$$\begin{aligned}
L(s,1) &= 1 + \tfrac{1}{2^s} + \tfrac{1}{3^s} + \tfrac{1}{4^s} + \tfrac{1}{5^s} + \tfrac{1}{6^s} + \tfrac{1}{7^s} + \tfrac{1}{8^s} + \tfrac{1}{9^s} + \ldots \\
L(s, \chi_{-1}\tau) &= 1 + \tfrac{-1}{5^s} + \tfrac{-1}{7^s} + \tfrac{1}{11^s} + \tfrac{1}{13^s} + \tfrac{-1}{17^s} + \tfrac{-1}{19^s} + \tfrac{1}{23^s} + \ldots \\
L(s, \chi_5^2) &= 1 + \tfrac{-1}{3^s} + \tfrac{-1}{5^s} + \tfrac{1}{7^s} + \tfrac{1}{9^s} + \tfrac{-1}{11^s} + \tfrac{-1}{13^s} + \tfrac{1}{15^s} + \ldots \\
L(s, \chi_{-1}\chi_5^2\tau) &= 1 + \tfrac{1}{5^s} + \tfrac{-1}{7^s} + \tfrac{-1}{11^s} + \tfrac{-1}{13^s} + \tfrac{-1}{17^s} + \tfrac{1}{19^s} + \tfrac{1}{23^s} + \ldots
\end{aligned}$$

This concludes the example and the section. The astute reader may have noticed that $f = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})$ and so $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. With this knowledge in hand, the reader is invited to check any or all of the results found previously for this particular field by some other method. We shall return to this example in the sequel to determine ζ_K at odd negative integers.

4.2 Evaluating Abelian Zeta Functions

In 4.1, we saw how to find the Dirichlet character group of an arbitrary abelian number field K extending $\mathbb{Q}$. It is now a matter of simply putting together our earlier theory on characters in order to finally evaluate the corresponding zeta function at negative integers. Indeed, suppose now that K is a totally real abelian extension of $\mathbb{Q}$ and we want to determine $\zeta_K(1-n)$ for n a positive, even integer (the only interesting case by (1.4.6)). Then we can apply

the theory above to get X, the corresponding group of Dirichlet characters. By (1.4.4), $L(1-n,\chi) = -B_{n,\chi}/n$ and since $\zeta_K(1-n) = \prod_{\chi\in X} L(1-n,\chi)$, all that remains is to find the corresponding generalized Bernoulli numbers. Since we have X, we also have f, the conductor of K, which is a multiple of the conductor of any character χ in X. Hence we can apply (1.4.7) with $F = f$ and find $B_{n,\chi}$ by evaluating the necessary Bernoulli polynomials. We continue with our example of $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ from the last section to illustrate how this can be done in practice by calculating $\zeta_K(1-n)$ for $n \in \{2,4,6,8\}$.

Recall that $X = \{1, \chi_{-1}\tau, \chi_5^2, \chi_{-1}\chi_5^2\tau\}$ was our group of Dirichlet characters, with primitive modulus 1, 12, 8 and 24 respectively. The values of the characters are listed at the end of 4.1 and we use these values to determine the necessary functions below. For reference, the necessary Bernoulli polynomials are

$$\begin{aligned} B_2(X) &= X^2 - X + \tfrac{1}{6} \\ B_4(X) &= X^4 - 2X^3 + X^2 - \tfrac{1}{30} \\ B_6(X) &= X^6 - 3X^5 + \tfrac{5}{2}X^4 - \tfrac{1}{2}X^2 + \tfrac{1}{42} \\ B_8(X) &= X^8 - 4X^7 + \tfrac{14}{3}X^6 - \tfrac{7}{3}X^4 + \tfrac{2}{3}X^2 - \tfrac{1}{30} \end{aligned}$$

For the character 1:

$$\begin{aligned} B_{2,1} = 1/6 \quad B_{4,1} = -1/30 \\ B_{6,1} = 1/42 \quad B_{8,1} = -1/30. \end{aligned}$$

For the character $\chi_{-1}\tau$:

$$\begin{aligned} B_{2,\chi_{-1}\tau} = 4 \qquad B_{4,\chi_{-1}\tau} = -184 \\ B_{6,\chi_{-1}\tau} = 20172 \quad B_{8,\chi_{-1}\tau} = -4120688. \end{aligned}$$

For the character χ_5^2:

$$\begin{aligned} B_{2,\chi_5^2} = 2 \qquad B_{4,\chi_5^2} = -44 \\ B_{6,\chi_5^2} = 2166 \quad B_{8,\chi_5^2} = -196888. \end{aligned}$$

For the character $\chi_{-1}\chi_5^2\tau$:

$$B_{2,\chi_{-1}\chi_5^2\tau} = 12 \qquad B_{4,\chi_{-1}\chi_5^2\tau} = -2088$$
$$B_{6,\chi_{-1}\chi_5^2\tau} = 912996 \quad B_{8,\chi_{-1}\chi_5^2\tau} = -745928016.$$

Putting these results together, we conclude

$$\begin{array}{rcccl}
\zeta_K(-1) & = & (\frac{-1}{2})^4(\frac{1}{6})(4)(2)(12) & = & 1 \\
\zeta_K(-3) & = & (\frac{-1}{4})^4(\frac{-1}{30})(-184)(-44)(-2088) & = & \frac{22011}{10} \\
\zeta_K(-5) & = & (\frac{-1}{6})^4(\frac{1}{42})(20172)(2166)(912996) & = & \frac{2198584943}{3} \\
\zeta_K(-7) & = & (\frac{-1}{8})^4(\frac{-1}{30})(-4120688)(-196888)(-745928016) & = & \frac{98499651123679091}{20}
\end{array}$$

This concludes the example. Below is a list of zeta function values computed by the author using this method. All credit for the primitive polynomials used goes to [16]. The method used to calculate these values is quite effective in general and can be used to calculate $\zeta_K(1-n)$ for many different abelian K and n, particularly when K has a small conductor. In the calculations that follow, we have kept $n \leq 8$ as the zeta function values can grow quite rapidly, however calculating for larger n is not a problem in general. As we shall see in Chapter 5, the primes that can appear in the denominator of $\zeta_K(1-n)$ are very restricted by their ramification numbers in $\mathcal{O}_K$. In particular, if p is an odd prime that does not ramify in K, then p^t can divide the denominator only if n is congruent with 0 modulo $(p-1)p^{t-1}$. This provides an easy first check to see if the values listed in the following tables are reasonable. For a more precise result on potential denominators appearing, see (5.0.2).

We give an overview of the operational cost of calculating ζ_K after the tables.

Table 4–1: Zeta Values for Real Quadratic Fields

Field L	Conductor	$\zeta_L(1-k)$ for k value			
		2	4	6	8
$\mathbb{Q}(\sqrt{2})$	8	$\frac{1}{12}$	$\frac{11}{120}$	$\frac{361}{252}$	$\frac{24611}{240}$
$\mathbb{Q}(\sqrt{3})$	12	$\frac{1}{6}$	$\frac{23}{60}$	$\frac{1681}{126}$	$\frac{257543}{120}$
$\mathbb{Q}(\sqrt{5})$	5	$\frac{1}{30}$	$\frac{1}{60}$	$\frac{67}{630}$	$\frac{361}{120}$
$\mathbb{Q}(\sqrt{6})$	24	$\frac{1}{2}$	$\frac{87}{20}$	$\frac{3623}{6}$	$\frac{15540167}{40}$
$\mathbb{Q}(\sqrt{7})$	28	$\frac{2}{3}$	$\frac{113}{15}$	$\frac{88922}{63}$	$\frac{37040933}{30}$
$\mathbb{Q}(\sqrt{10})$	40	$\frac{7}{6}$	$\frac{1577}{60}$	$\frac{1264807}{126}$	$\frac{2150342537}{120}$
$\mathbb{Q}(\sqrt{11})$	44	$\frac{7}{6}$	$\frac{2153}{60}$	$\frac{2130727}{126}$	$\frac{4393611593}{120}$
$\mathbb{Q}(\sqrt{13})$	13	$\frac{1}{6}$	$\frac{29}{60}$	$\frac{33463}{1638}$	$\frac{467669}{120}$
$\mathbb{Q}(\sqrt{14})$	56	$\frac{5}{3}$	$\frac{2503}{30}$	$\frac{4013645}{63}$	$\frac{13406231743}{60}$
$\mathbb{Q}(\sqrt{15})$	60	2	$\frac{537}{5}$	$\frac{1957882}{21}$	$\frac{3749253437}{10}$
$\mathbb{Q}(\sqrt{17})$	17	$\frac{1}{3}$	$\frac{41}{30}$	$\frac{5791}{63}$	$\frac{29950897}{1020}$
$\mathbb{Q}(\sqrt{19})$	76	$\frac{19}{6}$	$\frac{14933}{60}$	$\frac{43171459}{126}$	$\frac{264948072293}{120}$
$\mathbb{Q}(\sqrt{21})$	21	$\frac{1}{3}$	$\frac{77}{30}$	$\frac{17971}{63}$	$\frac{8529317}{60}$
$\mathbb{Q}(\sqrt{22})$	88	$\frac{23}{6}$	$\frac{24889}{60}$	$\frac{96678263}{126}$	$\frac{795567059929}{120}$
$\mathbb{Q}(\sqrt{23})$	92	$\frac{10}{3}$	$\frac{7093}{15}$	$\frac{8794030}{9}$	$\frac{277506449593}{30}$
$\mathbb{Q}(\sqrt{26})$	104	$\frac{25}{6}$	$\frac{43679}{60}$	$\frac{241665385}{126}$	$\frac{2784046499279}{120}$
$\mathbb{Q}(\sqrt{29})$	29	$\frac{1}{2}$	$\frac{157}{20}$	$\frac{23537}{14}$	$\frac{63987797}{40}$
$\mathbb{Q}(\sqrt{30})$	120	$\frac{17}{3}$	$\frac{36451}{30}$	$\frac{265810697}{63}$	$\frac{4072124178091}{60}$
$\mathbb{Q}(\sqrt{31})$	124	$\frac{20}{3}$	$\frac{20714}{15}$	$\frac{318795140}{63}$	$\frac{1302061439737}{15}$
$\mathbb{Q}(\sqrt{33})$	33	1	$\frac{141}{10}$	$\frac{74231}{21}$	$\frac{84995021}{20}$
$\mathbb{Q}(\sqrt{34})$	136	$\frac{23}{3}$	$\frac{57241}{30}$	$\frac{529854263}{63}$	$\frac{10412874712441}{60}$
$\mathbb{Q}(\sqrt{35})$	140	$\frac{19}{3}$	$\frac{61733}{30}$	$\frac{619698979}{63}$	$\frac{12937658154773}{60}$
$\mathbb{Q}(\sqrt{37})$	37	$\frac{5}{6}$	$\frac{1129}{60}$	$\frac{115865}{18}$	$\frac{1193648689}{120}$
$\mathbb{Q}(\sqrt{38})$	152	$\frac{41}{6}$	$\frac{32867}{12}$	$\frac{1948118201}{126}$	$\frac{9589172296595}{24}$
$\mathbb{Q}(\sqrt{39})$	156	$\frac{26}{3}$	$\frac{9145}{3}$	$\frac{160764638}{9}$	$\frac{2913380886349}{6}$
$\mathbb{Q}(\sqrt{41})$	41	$\frac{4}{3}$	$\frac{448}{15}$	$\frac{733924}{63}$	$\frac{324649814}{15}$
$\mathbb{Q}(\sqrt{42})$	168	9	$\frac{7875}{2}$	$\frac{187933043}{7}$	$\frac{3386014695603}{4}$
$\mathbb{Q}(\sqrt{43})$	172	$\frac{21}{2}$	$\frac{86603}{20}$	$\frac{1285165781}{42}$	$\frac{40401626292363}{40}$
$\mathbb{Q}(\sqrt{46})$	184	$\frac{37}{3}$	$\frac{164999}{30}$	$\frac{2793813037}{63}$	$\frac{100499210339519}{60}$
$\mathbb{Q}(\sqrt{47})$	188	$\frac{28}{3}$	$\frac{86446}{15}$	$\frac{3135548908}{63}$	$\frac{29513322141443}{15}$
$\mathbb{Q}(\sqrt{51})$	204	13	$\frac{15591}{2}$	$\frac{1640393453}{21}$	$\frac{14524385798023}{4}$
$\mathbb{Q}(\sqrt{53})$	53	$\frac{7}{6}$	$\frac{775}{12}$	$\frac{5838037}{126}$	$\frac{3534518239}{24}$
$\mathbb{Q}(\sqrt{55})$	220	$\frac{46}{3}$	$\frac{153847}{15}$	$\frac{7464304726}{63}$	$\frac{191941033133827}{30}$
$\mathbb{Q}(\sqrt{57})$	57	$\frac{7}{3}$	$\frac{2867}{30}$	$\frac{4499857}{63}$	$\frac{15371694947}{60}$
$\mathbb{Q}(\sqrt{58})$	232	$\frac{33}{2}$	$\frac{246839}{20}$	$\frac{6664029233}{42}$	$\frac{381149526802599}{40}$
$\mathbb{Q}(\sqrt{59})$	236	$\frac{85}{6}$	$\frac{768827}{60}$	$\frac{21905188502}{126}$	$\frac{1299470610025307}{120}$
$\mathbb{Q}(\sqrt{101})$	101	$\frac{19}{6}$	$\frac{37103}{60}$	$\frac{28937887}{18}$	$\frac{2226607059623}{120}$
$\mathbb{Q}(\sqrt{102})$	408	$\frac{103}{3}$	$\frac{2637641}{30}$	$\frac{222678863623}{63}$	$\frac{39437718445100201}{60}$

Table 4–2: Zeta Values for Maximal Real Subfields of Cyclotomic Fields

$\mathbb{Q}(\omega_N) \cap \mathbb{R}$	$\zeta_L(1-k)$ for k value			
for N value	2	4	6	8
4	$\frac{-1}{12}$	$\frac{1}{120}$	$\frac{-1}{252}$	$\frac{1}{240}$
7	$\frac{-1}{21}$	$\frac{79}{210}$	$\frac{-7393}{63}$	$\frac{142490119}{420}$
9	$\frac{-1}{9}$	$\frac{199}{90}$	$\frac{-50353}{27}$	$\frac{2648750959}{180}$
11	$\frac{-20}{33}$	$\frac{1695622}{165}$	$\frac{-50936925341420}{693}$	35430104007633523 60091 / 165
13	$\frac{152}{39}$	$\frac{1267169036}{195}$	1240276106567774 8712 / 819	59025521778751543 656793084 2838 / 195
15	$\frac{4}{15}$	$\frac{2522}{15}$	$\frac{4407640828}{315}$	$\frac{340269200275141}{15}$
16	$\frac{5}{6}$	$\frac{87439}{60}$	$\frac{48311765405}{126}$	$\frac{244310433568546039}{120}$
17	$\frac{18688}{51}$	$\frac{881620409802368}{51}$	1352475062683584 0457019286738688 / 1071	17795542442597046 27562092728733716 31966079828288 / 51
19	$\frac{-93504}{19}$	5767476605519708 256 / 95	-5119156157611607 18506438938074297 7088 / 133	18413397545604044 16317587662574944 69060267417629241 1209648 / 95
20	$\frac{2}{3}$	$\frac{3793}{3}$	$\frac{20876972870}{63}$	$\frac{10185217266205657}{6}$
21	$\frac{16}{3}$	$\frac{196804168}{15}$	$\frac{410899105316076688}{9}$	20446810763679221 5223646112964 / 15
23	$\frac{-104701969}{69}$	889970097451703378 560647296 / 345	-3618692805791287 924081254713751795 948413147240878336 / 1449	292175794781557807 828066937175926062 043886219249144892 357648090668228016 1662528 / 345
24	1	$\frac{22011}{10}$	$\frac{2198584943}{3}$	$\frac{98499651123679091}{20}$
25	$\frac{5825408}{75}$	213348756242356715 34784 / 75	289950642256096734 915370498015699083 114421376 / 1575	149263554830026152 669338969074236752 652176352542322348 17113854960992 / 75
27	$\frac{-373312}{27}$	7115770421925672675 2 / 135	-9139896402993467 968375731369340208 9536 / 81	261578028875827566 082911644238632037 363978267384039608 982256 / 135
28	$\frac{416}{21}$	$\frac{28255169072}{105}$	331378288772961075 488 / 63	926499559520108082 759262963410616 / 105
29	$\frac{703717310464}{29}$	129104936823786628 709164020258049812 0704 / 145	139572973346296274 022424877684636598 262465579899802559 97770173424010395 648 / 203	249732457459989310 984049745691439521 171188300865993136 503087293044790076 678608338393458111 961685244235595215 6672 / 145

Table 4–3: Zeta Values for Totally Real Fields with Galois Group $\mathbb{Z}/3\mathbb{Z}$

Defining Poly. of L	$\Delta(L)$	f_L	$\zeta_L(1-k)$ for k value			
			2	4	6	8
$x^3 - x^2 - 2x + 1$	49	7	$\frac{-1}{21}$	$\frac{79}{210}$	$\frac{-7393}{63}$	$\frac{142490119}{420}$
$x^3 - 3x^2 + 1$	81	9	$\frac{-1}{9}$	$\frac{199}{90}$	$\frac{-50353}{27}$	$\frac{2648750959}{180}$
$x^3 - x^2 - 4x - 1$	169	13	$\frac{-1}{3}$	$\frac{11227}{390}$	$\frac{-6701911}{63}$	$\frac{285307394787}{780}$
$x^3 - x^2 - 6x + 7$	361	19	-1	$\frac{4087}{10}$	$\frac{-2758494229}{399}$	$\frac{21696966762367}{20}$
$x^3 - x^2 - 10x + 8$	961	31	$\frac{-28}{3}$	$\frac{228614}{15}$	$\frac{-99594088828}{63}$	25449589228520 107 / 15
$x^3 - x^2 - 12x - 11$	1369	37	-7	$\frac{433513}{10}$	$\frac{-221736281617}{21}$	47656335484644 2353 / 20
$x^3 - x^2 - 14x - 8$	1849	43	$\frac{-76}{3}$	$\frac{2259086}{15}$	$\frac{-3642576372076}{63}$	34457376574661 36863 / 15
$x^3 - x^2 - 20x + 9$	3721	61	$\frac{-133}{3}$	$\frac{44689099}{30}$	-163363743993 283 / 63	25844144369029 57878499 / 60
$x^3 - 21x - 35$	3969	63	$\frac{-133}{3}$	$\frac{54922771}{30}$	-232363717924 243 / 63	41917356766362 98283451 / 60
$x^3 - 21x - 28$	3969	63	$\frac{-268}{3}$	$\frac{33153134}{15}$	-243557105345 068 / 63	10603027430450 27729167 / 15
$x^3 - x^2 - 22x - 5$	4489	67	$\frac{-193}{3}$	$\frac{86578159}{30}$	-458598853953 703 / 63	10556987395909 112777959 / 60
$x^3 - x^2 - 24x + 27$	5329	73	-79	$\frac{52419793}{10}$	-56088011483407 / 3	12739034108512 472635513 20
$x^3 - x^2 - 26x - 41$	6241	79	$\frac{-199}{3}$	$\frac{263038561}{30}$	-279663868280 9089 / 63	12491724617245 5242369881 / 60
$x^3 - x^2 - 30x - 27$	8281	91	-151	$\frac{245053849}{10}$	-443471130819 8401 / 21	34746761977954 8497499169 / 20
$x^3 - x^2 - 30x + 64$	8281	91	-244	$\frac{143202074}{5}$	-463012615730 5204 / 21	87852692367837 183805597 / 5
$x^3 - x^2 - 32x + 79$	9409	97	$\frac{-367}{3}$	$\frac{1106690017}{30}$	-382058060539 1311 /9	27151388632213 94547219817 / 60
$x^3 - x^2 - 34x + 61$	10609	103	$\frac{-637}{3}$	$\frac{1748682187}{30}$	-519680594883 20827 / 63	66830236704102 99899397907 / 60
$x^3 - x^2 - 36x + 4$	11881	109	-412	$\frac{506359526}{5}$	-337151605764 22012 / 21	13168356762005 16884427643 / 5
$x^3 - 39x - 26$	13689	117	$\frac{-1732}{3}$	$\frac{2525603738}{15}$	-315353992461 87196 / 9	11431665301467 456456028309 / 15
$x^3 - 39x - 91$	12689	117	$\frac{-775}{3}$	$\frac{4167470617}{30}$	-210566899697 242225 / 63	45192917950857 895244795137 / 60
$x^3 - x^2 - 42x - 80$	16129	127	-724	$\frac{1483081754}{5}$	-181158205363 739284 / 21	13037468271122 531491373677 / 5
$x^3 - x^2 - 44x + 64$	17689	133	-844	$\frac{2049626174}{5}$	-301015461002 723884 / 21	26056263648538 002464811367 / 5
$x^3 - x^2 - 44x - 69$	17689	133	-463	$\frac{3490141513}{10}$	-288255304152 127513 / 21	10305476148963 5750747736673 / 20
$x^3 - x^2 - 46x - 103$	19321	139	$\frac{-1075}{3}$	$\frac{13731622573}{30}$	-139926868073 2591525 / 63	59901546632470 2816956443573 / 60

Table 4–4: Zeta Values for Totally Real Fields with Galois Group $\mathbb{Z}/4\mathbb{Z}$

Defining Poly. of L	$\Delta(L)$	f_L	$\zeta_L(1-k)$ for k value			
			2	4	6	8
$x^4 - x^3 - 4x^2 + 4x + 1$	1125	15	$\frac{4}{15}$	$\frac{2522}{15}$	$\frac{4407640828}{315}$	$\frac{340269200275141}{15}$
$x^4 - 5x^2 + 5$	2000	20	$\frac{2}{3}$	$\frac{3793}{3}$	$\frac{20876972870}{63}$	10185217266205 657 / 6
$x^4 - 4x^2 + 2$	2048	16	$\frac{5}{6}$	$\frac{87439}{60}$	$\frac{48311765405}{126}$	24431043356854 6039 / 120
$x^4 - x^3 - 6x^2 + x + 1$	4913	17	$\frac{8}{3}$	$\frac{1501748}{51}$	$\frac{2927442275768}{63}$	73243738598296 001578 / 51
$x^4 - x^3 - 9x^2 + 9x + 11$	6125	35	$\frac{52}{15}$	$\frac{949826}{15}$	$\frac{49198405871884}{315}$	11258341497525 2128393 / 15
$x^4 - 10x^2 + 20$	8000	40	$\frac{82}{15}$	$\frac{2428121}{15}$	2137806681069 34 / 315	16687460276546 64809441 / 30
$x^4 - x^3 - 14x^2 + 14x + 31$	15125	55	$\frac{40}{3}$	$\frac{4494500}{3}$	1419781907968 600 / 63	19811806913720 486943010 / 3
$x^4 - 12x^2 + 18$	18432	48	$\frac{73}{3}$	$\frac{95783699}{30}$	4279294971376 273 / 63	17527951011130 38776232779 / 60
$x^4 - x^3 - 11x^2 - 9x + 3$	19773	39	24	$\frac{19584396}{5}$	8977618187208 344 / 91	24645236534309 6067651798 / 5

Table 4–5: Zeta Values for Totally Real Fields with Galois Group V_4

Defining Poly. of L	$\Delta(L)$	f_L	$\zeta_L(1-k)$ for k value			
			2	4	6	8
$x^4 - 6x^2 + 4$	1600	40	$\frac{7}{15}$	$\frac{17347}{30}$	$\frac{30591886909}{315}$	19104870944296 627 / 60
$x^4 - 4x^2 + 1$	2304	24	1	$\frac{22011}{10}$	$\frac{2198584943}{3}$	98499651123679 091 / 20
$x^4 - 2x^3 - 7x^2 + 8x + 1$	3600	60	$\frac{8}{5}$	$\frac{49404}{5}$	$\frac{882041504056}{105}$	69715885206206 0102 / 5
$x^4 - 9x^2 + 4$	4225	65	$\frac{32}{15}$	$\frac{260536}{15}$	$\frac{82993232144192}{4095}$	69485025875424 35588 / 15
$x^4 - 5x^2 + 1$	7056	84	$\frac{16}{3}$	$\frac{1600984}{15}$	$\frac{21490136139376}{63}$	32546621594258 3464892 / 15
$x^4 - 11x^2 + 9$	7225	85	$\frac{24}{5}$	$\frac{567932}{5}$	$\frac{40694841858728}{105}$	22019245136208 58970862 / 85
$x^4 - 2x^3 - 9x^2 + 10x - 1$	10816	104	$\frac{25}{3}$	$\frac{13933601}{30}$	$\frac{224565569919235}{63}$	32043823294539 226431761 / 60
$x^4 - 13x^2 + 16$	11025	105	$\frac{48}{5}$	$\frac{2500344}{5}$	$\frac{138658645437552}{35}$	30825584395650 60149532 / 5
$x^4 - 8x^2 + 9$	12544	56	$\frac{40}{3}$	$\frac{12444916}{15}$	$\frac{515365535956360}{63}$	24442627868625 910571618 / 15
$x^4 - 2x^3 - 13x^2 + 14x + 19$	14400	120	$\frac{68}{5}$	$\frac{6342474}{5}$	$\frac{258092617601908}{15}$	22844617807790 149112117 / 5
$x^4 - 7x^2 + 4$	17424	132	28	$\frac{13964358}{5}$	1063508156680 388 / 21	96175598435029 555420979 / 5
$x^4 - 2x^3 - 11x^2 + 12x + 2$	18496	136	$\frac{92}{3}$	$\frac{51631382}{15}$	4430749437475 652 / 63	76755540987789 83710699547 / 255
$x^4 - 2x^3 - 15x^2 + 16x + 29$	19600	140	$\frac{304}{15}$	$\frac{55806632}{15}$	2953621171930 1968 / 315	69199790931405 5866713796 / 15

Table 4–6: Zeta Values for Totally Real Fields with Galois Group $\mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$

Defining Poly. of L	$\Delta(L)$	f_L	$\zeta_L(1-k)$ for k value 2	4	6	8
$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$	11^4	11	$\frac{-20}{3}$	$\frac{1695622}{165}$	$\frac{-50936925341420}{693}$	35430104007633 52360091 / 165
$x^5 - 10x^3 - 5x^2 + 10x - 1$	5^8	25	$\frac{-284}{3}$	$\frac{75880707482}{75}$	-323390421080 746279844 / 63	80051769877718 65469117042898 4741 / 75
$x^5 - x^4 - 12x^3 + 21x^2 + x - 5$	31^4	31	$\frac{-1100}{3}$	$\frac{309701488762}{15}$	-113882933598 0948622297100 / 1953	10163787098630 16583409976241 4772821 / 15
$x^5 - x^4 - 16x^3 - 5x^2 + 21x + 9$	41^4	41	$\frac{-8260}{3}$	1638136374 4922 / 15	-173470767772 05604627361620 / 63	18315962070440 54002921082832 793469532221 / 615
$x^6 - x^5 - 7x^4 + 2x^3 + 7x^2 - 2x - 1$	$5^3 7^4$	35	$\frac{296}{105}$	$\frac{323983108}{105}$	1480010171093 980136 / 315	64429551550124 89926691699051 4 / 105
$x^6 - x^5 - 5x^4 + 4x^3 + 6x^2 - 3x - 1$	13^5	13	$\frac{152}{39}$	$\frac{1267169036}{195}$	1240276106567 7748712 / 819	59025521778751 54365679308428 38 / 195
$x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1$	$3^3 7^5$	21	$\frac{16}{3}$	$\frac{196804168}{15}$	4108991053160 76688 / 9	2044681076367 9221522364611 2964 / 15
$x^6 - 9x^4 - 4x^3 + 9x^2 + 3x - 1$	$3^8 5^3$	45	$\frac{584}{45}$	$\frac{4684354132}{45}$	1597596534176 91918344 / 135	51932881033449 69766273179394 3706 / 45
$x^6 - 7x^4 + 14x^2 - 7$	$2^6 7^5$	28	$\frac{416}{21}$	$\frac{28255169072}{105}$	3313782887729 61075488 / 63	9264995595201 0808275926296 3410616 / 105
$x^6 - 10x^4 + 24x^2 - 8$	$2^9 7^4$	56	$\frac{172}{7}$	$\frac{15035749102}{35}$	2302301465742 03691276 / 21	84074373571736 22417959576628 88871 / 35
$x^6 - 6x^4 + 9x^2 - 3$	$2^6 3^9$	36	$\frac{248}{9}$	$\frac{4260546220}{9}$	3390359299869 26764664 / 27	25970047479897 91263682736547 64070 / 9
$x^6 - 12x^4 + 36x^2 - 8$	$2^9 3^8$	72	$\frac{988}{9}$	$\frac{651668657926}{45}$	7455530109650 5483439164 / 27	20330218772719 59860596946113 264468883 / 45
$x^6 - x^5 - 12x^4 + 13x^3 + 19x^2 - 10x - 5$	$5^3 13^4$	65	$\frac{1952}{15}$	3509833061 008 / 195	1216031865704 999876258144 / 315	13908910897658 53223193979292 2475996744 / 195
$x^6 - 2x^5 - 12x^4 + 18x^3 + 23x^2 - 16x + 1$	$2^6 3^3 7^4$	84	$\frac{3176}{21}$	3183713247 668 / 105	5556257655245 83835088488 / 63	23112029124940 82359665358012 8489656554 / 105
$x^6 - x^5 - 14x^4 + 9x^3 + 35x^2 - 16x - 1$	$7^4 13^3$	91	$\frac{4448}{21}$	7375467141 872 / 105	2705817875336 9225906888672 / 819	13995403996071 05177965891499 44274360056 / 105
$x^6 - 12x^4 - 5x^3 + 36x^2 + 30x + 1$	$3^9 7^3$	63	$\frac{3088}{9}$	7590315348 616 / 45	3470339635049 726273455504 / 27	38176738036607 58949338084940 79837810468 / 45
$x^6 - 14x^4 + 56x^2 - 56$	$2^9 7^5$	56	$\frac{9680}{21}$	4092601761 8312 / 105	3071280716806 0491025006160 / 63	54956633713560 67650913360396 360931329156 / 105

Table 4–7: Number of Fields for which $\zeta_L(1-k)$ is an Integer

Quadratic Fields $\mathbb{Q}(\sqrt{m})$	♯ of Fields Counted	k-value 2	4	6	8
m squarefree in $[2, 199]$	121	19	3	1	1
m squarefree in $[200, 399]$	121	26	4	4	2
m squarefree in $[400, 599]$	123	26	2	3	1
m squarefree in $[600, 799]$	123	34	7	2	3
m squarefree in $[800, 999]$	119	32	2	0	2
m squarefree in $[1000, 1199]$	122	27	5	0	1
m squarefree in $[1200, 1399]$	124	27	1	3	1
m squarefree in $[1400, 1599]$	123	30	3	1	2
m squarefree in $[1600, 1799]$	119	26	3	0	2
m squarefree in $[1800, 1999]$	119	29	4	1	1
Totals	1214	276	34	15	16
$\mathbb{Q}(\omega_m + \omega_m^{-1})$ $m \not\equiv 2 \mod 4$					
m in $[4, 99]$	72	16	5	5	5
m in $[100, 199]$	75	24	14	12	14
m in $[200, 299]$	75	31	22	17	22
m in $[300, 399]$	75	37	23	20	23
m in $[400, 499]$	75	40	33	30	33
Totals	372	148	97	84	97

4.3 Evaluating Running Times

We now consider the operation costs of calculating such results in general. More precisely, fix some abelian number field K of degree m over $\mathbb{Q}$. Assume $\mathbb{X}_K$ is the group of Dirichlet characters corresponding to K and K has conductor f. Given some even integer $k \geq 2$, we wish to put a bound on the number of arithmetic operations needed to calculate $\zeta_K(1-k)$. We assume that all Bernoulli polynomials have been precalculated.

Observing that $\zeta_K(1-k) = (-1/k)^m \prod B_{k,\chi}$ where the product runs over $\chi \in \mathbb{X}_K$, we consider the cost of computing $B_{k,\chi}$. Indeed by (1.4.7), we have

$$B_{k,\chi} = f^{k-1} \sum_{a=1}^{f} \chi(a) B_k\left(\frac{a}{f}\right)$$

and we note that each $B_k(X)$ is a k degree polynomial. It takes 1 division and $k-1$ multiplications to determine the values $\left\{\frac{a}{f}, (\frac{a}{f})^2, \ldots, (\frac{a}{f})^k\right\}$. Since we are assuming the coefficients of the Bernoulli polynomials have already been determined, it only costs at most k more instance of multiplication and k instances of addition to fully evaluate $B_k(\frac{a}{f})$. We then multiply our answer with $\chi(a)$ and repeat this process at most $f-1$ times since $\chi(f) = 0$ (note that in general many additional iterations can be skipped as $\chi(a)$ will attain 0 when $(a, f_\chi) \neq 1$). After calculating each term in the sum, we must add the terms and multiply by f^{k-1}, which is a cost of $f-1$ additions and $k-1$ multiplications. We conclude that the total arithmetic cost to compute $B_{k,\chi}$ is no more then $(f-1)(3k+2)+k-1$ operations, which is bounded by $3kf$ operations when k is large. Since we need to do this for m different characters, followed by multiplication by $(-1/k)^m$, the total cost of calculating $\zeta_K(1-k)$ in this manner is bounded by $3mkf$ arithmetic operations for sufficiently large k.

This is a very nice result and shows that $\zeta_K(1-k)$ can be computed in linear time with respect to k once $\mathbb{X}_K$ is known. It should be noted that we have ignored the time it takes to process algebraic relationships between the factors which arise from the values attained by the characters in $\mathbb{X}_K$. It is a theorem of Siegel and Klingen that $\zeta_K(1-k)$ is always rational, and so ideally we would want any program that calculates these values to produce a ratio of two integers as an output. So far we have only discussed how to create an output that would include products and sums of Dirichlet characters evaluated at various integers. There is however a very convenient way to pass to the former state from the latter which we now consider.

We first note that because our final solution is necessarily a rational number, it follows that $[L:\mathbb{Q}]\zeta_K(1-k) = \mathrm{Tr}_{\mathbb{Q}}^{L}(\zeta_K(1-k))$, where L is some number field containing all the algebraic integers appearing in $\zeta_K(1-k)$. Hence, instead of trying to simplify through various algebraic relations, we can just consider the trace of the various terms appearing in $\zeta_K(1-k)$. However, the only non-rational algebraic numbers appearing in the output of our algorithm are the evaluation of certain Dirichlet characters, which of course are all roots of unity that divide the exponent of the group $\mathrm{Gal}(K/\mathbb{Q})$. Hence the question reduces to finding the $\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\omega_N)}(\omega)$, where ω is some arbitrary root of unity lying inside of $\mathbb{Q}(\omega_N)$ (clearly ω is necessarily a power of ω_N, but this shall not be important).

Certainly it is enough to assume $\omega = \omega_N$, because of the trace identity

$$\mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\omega_N)}(\omega) = [\mathbb{Q}(\omega_N):\mathbb{Q}(\omega)] \cdot \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\omega)}(\omega).$$

Now recall that the trace of ω_N is in fact the negative of the coefficient on the term $x^{\phi(N)-1}$ appearing in the N^{th} cyclotomic polynomial. In general, determining the coefficients of cyclotomic polynomials is a very deep question

however the following lemma shows that the coefficient we are interested in is entirely determined by the prime factorization of N.

Lemma 4.3.1. *Let $\Psi_N(x)$ denote the N^{th} cyclotomic polynomial. If N is not squarefree, then the coefficient corresponding to $x^{\phi(N)-1}$ in $\Psi_N(x)$ is 0. Otherwise let N factor into t distinct primes. Then the coefficient on $x^{\phi(N)-1}$ is $(-1)^{t+1}$.*

Proof. Assume $N = p_1^{\alpha_1} \dots p_t^{\alpha_t}$ is the prime factorization of N and let $N' = p_1 \dots p_t$. It is a well known fact (see for example the exercises in [8]) that $\Psi_N(x) = \Psi_{N'}(x^{\frac{N}{N'}})$ and this fact alone proves the first statement. Hence assume $N = N'$. Recall the general definition of the N^{th} cyclotomic polynomial as

$$\Psi_N(x) = \frac{x^N - 1}{\prod\limits_{\substack{d|N \\ d \neq N}} \Psi_d(x)}.$$

It follows easily that the sum of all the zeros of Ψ_N will be the negative of the sum of all the zeros of all the Ψ_d for $d|N, d \neq N$. The proof now follows from induction on t. If $t = 0$, then $N = 1$ and $\Psi_N(x) = x - 1$, so the coefficient is $(-1)^1$ as claimed. Suppose the claim holds for all $t < t'$. Then if N is square free with t' distinct primes dividing it, we have from the previous remarks that the sum of all zeros of Ψ_N equals the negative of the following sum,

$$1 - \left(\sum_{\substack{q_1 | N \\ q_1 \text{ prime}}} 1 \right) + \left(\sum_{\substack{q_1, q_2 | N \\ q_1 < q_2 \text{ prime}}} 1 \right) - \ldots + (-1)^{t'-1} \left(\sum_{\substack{q_1, \ldots, q_{t'-1} | N \\ q_1 < \ldots < q_{t'-1} \text{ prime}}} 1 \right).$$

But this expression is easily seen to be $\sum_{i=0}^{t'-1} (-1)^i \binom{t'}{i}$. Using the binomial expansion of $0 = (1 + (-1))^{t'}$ completes the proof. □

We conclude from this analysis that reducing our algebraic expression of $\zeta_K(1-k)$ to a rational number can be done with very little additional operational cost. Indeed there will be only m Dirichlet characters (whose image is contained in the m^{th} roots of unity), and so the number of different roots of unity in the unsimplified expression of $\zeta_K(1-k)$ is bounded by m and in particular is independent of k. The above argument shows that we can replace these roots by certain integers and then divide the resulting expression by the least common multiple of their primitive moduli to get an equivalent expression for $\zeta_K(1-k)$. This concludes the section and we summarize our findings in the theorem below.

Theorem 4.3.2. *Let K be a totally real abelian number field of degree m over $\mathbb{Q}$ and conductor f. Assume its group of Dirichlet characters are known, as are all necessary Bernoulli polynomials. Then the operation cost of determining $\zeta_K(1-k)$ in a rational form is bounded by $3k \cdot m \cdot f + C(m,f)$ for some constant $C(m,f)$ depending on m and f.*

4.4 A Final Result

Before moving on, we use the program constructed earlier in the chapter to provide numerical evidence for a certain conjecture.

Given a totally real number field L and a prime $p > 2$, we consider the following statement:

$$C(L,p) : \zeta_L(2-p) \text{ is not } p-\text{integral.}$$

This condition is considered in [13], where it is noted that by the ABC conjecture (see [23]), if L is a real quadratic field of class number 1, then $C(L,p)$ is

expected to fail precisely $1/p$ of the times. The following tables extend those given in [13] in providing numerical evidence for this result. Explicitly, there are 1029 primes between 1 and 10,000, 832 from 10,000 to 20,000, 776 from 20,000 to 30,000 and 785 from 30,000 to 40,000 such that $\mathbb{Q}$ adjoined with the square root of such a prime has class number one. The table below lists the number of such primes l for which $C(\mathbb{Q}(\sqrt{l}), p)$ fails to hold, for p prime from 3 to 13, and calculates the ratio between this value and the expected number for each interval. Note that from 1-10,000, [13] lists $C(\mathbb{Q}(\sqrt{l}), 7)$ failing 165 times, however our program found it to fail only 161 times over the same interval. All other values that are listed both here and in [13] agree.

Table 4–8: Condition $C(L, p)$ Verification

p	$C(\mathbb{Q}(\sqrt{l}), p)$ fails in [1,10000]	Predicted	Ratio
3	312	343	0.91
5	196	205.8	0.95
7	161	147	1.10
11	92	93.5	0.98
13	66	79.2	0.83
p	$C(\mathbb{Q}(\sqrt{l}), p)$ fails in [10000,20000]	Predicted	Ratio
3	251	277.3	0.91
5	170	166.4	1.02
7	116	118.9	0.98
11	67	75.6	0.89
13	65	64	1.02
p	$C(\mathbb{Q}(\sqrt{l}), p)$ fails in [20000,30000]	Predicted	Ratio
3	236	258.7	0.91
5	165	155.2	1.06
7	106	110.9	0.96
11	68	70.5	0.96
13	62	59.7	1.04
p	$C(\mathbb{Q}(\sqrt{l}), p)$ fails in [30000,40000]	Predicted	Ratio
3	251	261.7	0.96
5	146	157	1.00
7	112	112.1	0.96
11	56	71.4	0.78
13	68	60.4	1.13

CHAPTER 5
A Functional Equation Approach

We conclude this thesis with a brief survey of two alternative methods of calculating the value of zeta functions at negative integers. These methods are more general then the one described in detail within this thesis, as they apply to totally real number fields that need not be abelian Galois extensions of $\mathbb{Q}$. The theorems and results used in this section will not be proven as their proofs go beyond the scope of this text, however references will be provided.

In what follows, assume we have the following notation. K is an arbitrary number field, with $[K : \mathbb{Q}] = N$, discriminant $\Delta(K)$, s_1 real embeddings into $\mathbb{C}$ and $2s_2$ complex embeddings. We begin with the following key result regarding the zeta function of K.

Theorem 5.0.1. *$\zeta_K(s)$ can be extended to a meromorphic function on $\mathbb{C}$ that satisfies the following functional equation:*

$$A^s\Gamma\left(\frac{s}{2}\right)^{s_1}\Gamma(s)^{s_2}\zeta_K(s) = A^{1-s}\Gamma\left(\frac{1-s}{2}\right)^{s_1}\Gamma(1-s)^{s_2}\zeta_K(1-s), \qquad (5.1)$$

where

$$A = 2^{-s_2}\pi^{-N/2}\sqrt{|\Delta(K)|}.$$

Proof. See [18]. □

A few preliminary observations can be made regarding (5.1) above. We first note that if $\Re(s) > 1$, then using the fact that $\zeta_K(s)$ is finite, we have that the left hand side of (5.1) is finite. On the other hand, recall from section (1.4) that Γ has poles at the negative integers. It follows that either ζ_K is 0 at all negative integers, or $s_2 = 0$, in which case ζ_K is still necessary 0 at all negative even integers. This is a generalization of result (1.4.6).

Because we are focused on negative integer values of ζ_K, we should re-arrange (1) to solve for $\zeta_K(1-s)$ in the case where $s_2 = 0$ (ie. K is totally real) and $s \geq 2$ is an even integer. In that case, we can use the fact that $\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(n) = (n-1)!$, and the functional equation for Γ to get

$$\begin{aligned}
\zeta_K(1-s) &= A^{2s-1}\Gamma\left(\frac{s}{2}\right)^N \Gamma\left(\frac{1-s}{2}\right)^{-N} \zeta_K(s) \\
&= A^{2s-1}\left(\frac{(s/2-1)!}{\frac{2}{1-s}\cdot\frac{2}{3-s}\cdot\ldots\cdot\frac{2}{-1}\Gamma(1/2)}\right)^N \zeta_K(s) \\
&= (-1)^{Ns/2}A^{2s-1}\left(\frac{((s/2-1)!)\cdot 1\cdot 3\cdot\ldots\cdot(s-1)}{\sqrt{\pi}2^{s/2}}\right)^N \zeta_K(s) \\
&= (-1)^{Ns/2}A^{2s-1}\left(\frac{(s/2-1)!s!}{\sqrt{\pi}2^s(s/2)!}\right)^N \zeta_K(s) \\
&= (-1)^{Ns/2}\frac{(2(s-1)!)^N}{\sqrt{|\Delta(K)|}}\left(\frac{|\Delta(K)|}{\pi^N 2^N}\right)^s \zeta_K(s). \qquad (5.2)
\end{aligned}$$

For notational purposes, we will denote $\dfrac{|\Delta(K)|}{\pi^N 2^N}$ as C_K in the above equation. Using the fact that $\zeta_K(s) = \displaystyle\sum_{I \lhd \mathcal{O}_K} \frac{1}{||I||^s}$, (5.2) gives us a very convenient way of calculating $\zeta_K(1-s)$ assuming we can evaluate the necessary infinite sum. Unfortunately, even if one can determine all the ideals and their norms, it may not be obvious how to determine the infinite sum in general. Thus it appears that while one could approximate $\zeta_K(1-s)$ arbitrarily well in this manner, it is unclear how to get an exact result. However, results from the study of modular forms will come to our aid in this matter which we now discuss.

As noted in 4.3, a famous theorem of Siegel and Klingen states that $\zeta_K(-n)$ is always rational. While this alone is not sufficient for our purposes, Andreatta and Goren showed that one can determine the possible integers appearing in the denominator of $\zeta_K(1-s)$ by considering the ramification of certain primes in $\mathcal{O}_K$. We consider their result in more detail as soon as we introduce the necessary notation.

Let K be a totally real number field with $[K:\mathbb{Q}] = N$ as above. Let p be some arbitrary prime of $\mathbb{Q}$. Then for every prime $P \lhd \mathcal{O}_K$ lying over p, one can consider the complete field L_P lying over $\mathbb{Q}_p$. Let B_P be the maximal abelian subextension of $\mathbb{Q}_p$ contained in L_P. Define $e'(P|p) = m_P \cdot p^{\beta_P}$ with $(m_P, p) = 1$ to be the ramification index of p in the ring of integers of B_P. Define $e_p^t := \min\{m_P \mid P \text{ lies over } p\}$ and $e_p^w := \min\{p^{\beta_P} \mid P \text{ lies over } p\}$. It turns out that for $p \neq 2$, e_p^t is the index of some subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ and in particular divides $p-1$. Finally, let $l(n)$ be the exponent of the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Theorem 5.0.2. *Let $s > 1$ be an even integer. Suppose that $2^{-N}\zeta_K(1-s)$ is not p-integral and let $n = -val_p(2^{-N}\zeta_K(1-s))$. Then*

i. if $p \neq 2$,

$$s \equiv 0 \mod \frac{p-1}{e_p^t} \cdot \left\lceil \frac{p^{n-1}}{e_p^w} \right\rceil;$$

ii. if $p = 2$,

$$s \equiv 0 \mod \left\lceil \frac{2^{l(n)}}{e_2^w} \right\rceil.$$

Proof. See pg. 92 of [1]. □

Note that one can use the fact $e'(P|p)$ divides the ramification index $e(P|p)$ to put bounds on the size of e_p^t and e_p^w without actually considering the p-adic extensions of $\mathbb{Q}_p$.

This theorem allows us to use (5.2) to compute the exact values of $\zeta_K(1-s)$ instead of just arbitrarily good approximations. Indeed, since we can put a bound on the size of the denominator, say M_s, it follows that $\zeta_K(1-s)\cdot M_s$ must be an integer. Our equation becomes

$$M_s \cdot \zeta_K(1-s) = M_s \cdot (-1)^{Ns/2} \frac{(2(s-1)!)^N}{\sqrt{|\Delta(K)|}} (C_K)^s \zeta_K(s). \tag{5.3}$$

Since the left hand side is an integer, it follows that we only need to approximate the right hand side to the nearest integer in order to know the true value. In what follows we will put an upper bound on how well $\zeta_K(s)$ needs to be approximated.

We first consider the maximum size of $\zeta_K(s)$ for s an even integer at least 2. Writing the function as an infinite product, we have

$$\begin{aligned}
\zeta_K(s) &= \prod_{\substack{P \lhd \mathcal{O}_K \\ P \text{ prime}}} (1 - ||P||^{-s})^{-1} \\
&= \prod_{\substack{p \in \mathbb{N} \\ p \text{ prime}}} \prod_{\substack{P \lhd \mathcal{O}_K \\ P \text{ prime} \\ P|(p)}} (1 - ||P||^{-s})^{-1} \\
&\leq \prod_{\substack{p \in \mathbb{N} \\ p \text{ prime}}} \prod_{\substack{P \lhd \mathcal{O}_K \\ P \text{ prime} \\ P|(p)}} (1 - p^{-s})^{-1} \\
&\leq \prod_{\substack{p \in \mathbb{Z} \\ p \text{ prime}}} (1 - p^{-s})^{-N} \\
&= \zeta_{\mathbb{Q}}(s)^N \\
&\leq (\frac{\pi^2}{6})^N.
\end{aligned}$$

We introduce the following truncated product as our estimate of $\zeta_K(s)$,

$$Z_K(s,T) := \prod_{\substack{p \text{ prime in } \mathbb{N} \\ p \leq T}} \prod_{\substack{P \lhd \mathcal{O}_K \\ P \text{ prime \& } P|(p)}} (1 - ||P||^{-s})^{-1}.$$

It is clear that for fixed s, as $T \to \infty$, $Z_K(s,T) \to \zeta_K(s)$ and this convergence is monotone increasing. We would like to find a bound on the difference between them as a function of s and T, say $E_0(s,T)$. Working towards this goal, we calculate

$$\begin{aligned}
\zeta_K(s) - Z_K(s,T) &= Z_K(s,T)((\prod_{\substack{p \text{ prime in } \mathbb{N} \\ p > T}} \prod_{\substack{P \lhd \mathcal{O}_K \\ P \text{ prime \& } P|(p)}} (1 - ||P||^{-s})^{-1}) - 1) \\
&< \zeta_K(s)((\prod_{\substack{p \text{ prime in } \mathbb{N} \\ p > T}} (1 - p^{-s})^{-N}) - 1) \\
&< (\frac{\pi^2}{6})^N((1 + \sum_{n>T} \frac{1}{n^s})^N - 1)
\end{aligned}$$

where the last line has used our bound on ζ_K and bounded the infinite product by an infinite sum. It is very easy to bound this infinite sum, as it is well known to be less then the integral $\displaystyle\int_T^\infty \frac{dx}{x^s}$ which is readily seen to be $\dfrac{1}{(s-1)T^{s-1}}$. Thus we have

$$\zeta(s) - Z_K(s,T) < \left(\frac{\pi^2}{6}\right)^N \left(\left(1 + \frac{1}{(s-1)T^{s-1}}\right)^N - 1\right).$$

The other source of error in an analytic estimation of the right hand side of (5.3) will come from rounding π and $\sqrt{|\Delta(K)|}$. Let $F(s,n,m)$ denote the the value of $\dfrac{(2(s-1)!)^N}{\sqrt{|\Delta(K)|}}(C_K)^s$ when π and $\sqrt{|\Delta(K)|}$ are rounded to n and m decimal points of accuracy respectively (recall $C_K = \dfrac{|\Delta(K)|}{\pi^N 2^N}$) and define $E_1(s,n,m)$ as the difference $\dfrac{(2(s-1)!)^N}{\sqrt{|\Delta(K)|}}(C_K)^s - F(s,n,m)$. Again we would like to find a bound for $|E_1(s,n,m)|$. Let ϵ_1 denote the difference between π

and its rounded decimal expansion and likewise define ϵ_2 as the corresponding difference for $\sqrt{|\Delta(K)|}$. Then $|\epsilon_1| < 10^{-n}$ and $|\epsilon_2| < 10^{-m}$ and so we have

$$\begin{aligned}
&|E_1(s,n,m)| \\
&\quad = \frac{(2(s-1)!)^N |\Delta(K)|^s}{2^{Ns}} \left| \frac{1}{\sqrt{\Delta(K)}\pi^{Ns}} - \frac{1}{(\sqrt{\Delta(K)} - \epsilon_2)(\pi - \epsilon_1)^{Ns}} \right| \\
&\quad = \frac{(2(s-1)!)^N |\Delta(K)|^s}{2^{Ns}\sqrt{|\Delta(K)|}\pi^{Ns}} \left| 1 - \frac{1}{(1 - \epsilon_2/\sqrt{|\Delta(K)|})(1 - \epsilon_1/\pi)^{Ns}} \right|.
\end{aligned}$$

Let us assume that $n \geq 2\log_{10}(Ns+1)$ and that m is at least 1. Then it is easy to show by expanding that $(1-\epsilon_1/\pi)^{Ns}$ lies between $(1-(Ns+1)|\epsilon_1|/\pi)$ and $(1+(Ns+1)\epsilon_1/\pi)$. Under this assumption, we have

$$\begin{aligned}
&\left| 1 - \frac{1}{(1 - \frac{\epsilon_2}{\sqrt{|\Delta(K)|}})(1 - \frac{\epsilon_1}{\pi})^{Ns}} \right| \\
&< \frac{\pi\sqrt{|\Delta(K)|}}{(\sqrt{|\Delta(K)|} - |\epsilon_2|)(\pi - (Ns+1)|\epsilon_1|)} - \frac{\pi\sqrt{|\Delta(K)|}}{(\sqrt{|\Delta(K)|} + |\epsilon_2|)(\pi + (Ns+1)|\epsilon_1|)} \\
&= 2\pi\sqrt{|\Delta(K)|}\frac{\pi|\epsilon_2| + (Ns+1)|\epsilon_1|\sqrt{|\Delta(K)|}}{(\pi^2 - (Ns+1)^2|\epsilon_1|^2)(|\Delta(K)| - |\epsilon_2|^2)} \\
&\leq 2\pi\sqrt{|\Delta(K)|}\frac{\pi|\epsilon_2| + \sqrt{|\epsilon_1||\Delta(K)|}}{(\pi^2 - |\epsilon_1|)(|\Delta(K)| - |\epsilon_2|^2)} \\
&\leq \frac{2}{\pi\sqrt{|\Delta(K)|}}\frac{\pi|\epsilon_2| + \sqrt{|\epsilon_1||\Delta(K)|}}{(1-1/98)(1-1/100)} \\
&< \frac{25}{12}(|\epsilon_2|/\sqrt{|\Delta(K)|} + \sqrt{|\epsilon_1|}/\pi).
\end{aligned}$$

We now return to equation (5.3) and rewrite it as

$$\begin{aligned}
M_s \cdot \zeta_K(1-s) &= M_s \cdot (-1)^{Ns/2}(F(s,n,m) + E_1(s,n,m))(Z_K(s,T) + E_0(s,T)) \\
&= (-1)^{Ns/2} M_s (F(s,n,m)Z_K(s,T) + E_1(s,n,m)Z_K(s,T) \quad (5.4) \\
&\quad + E_0(s,T)(F(s,n,m) + E_1(s,n,m))).
\end{aligned}$$

Note that the first term in (5.4) is what one would calculate in practice, while the remaining two are error terms. Because we know that the actual value must be an integer, it suffices to find T, n and m that ensure the error terms are sufficiently small, say less then $\frac{1}{10M_s}$. Looking at the first error term, recall that $Z_K < \zeta_K \leq 2^N$, while the calculations above show that if $n \geq 2\log_{10}(Ns)$ and $m \geq 1$,

$$|E_1(s,n,m)| < \frac{(2(s-1)!)^N}{\sqrt{|\Delta(K)|}}(C_K)^s \frac{25}{12}(|\epsilon_2|/\sqrt{|\Delta(K)|} + \sqrt{|\epsilon_1|}/\pi).$$

Hence for the first error term to be less then $1/10M_s$, it suffices to have

$$(|\epsilon_2|/\sqrt{|\Delta(K)|} + \sqrt{|\epsilon_1|}/\pi) \leq \frac{6\sqrt{|\Delta(K)|}}{4^N \cdot 125 \cdot ((s-1)!)^N (C_K)^s M_s}$$

Letting $\alpha = \min(n/2, m)$, we certainly have $2 \cdot 10^{-\alpha} < (|\epsilon_2|/\sqrt{|\Delta(K)|} + \sqrt{|\epsilon_1|}/\pi)$ and so

$$\alpha > -\log_{10}\left(\frac{6\sqrt{|\Delta(K)|}}{4^N \cdot 125 \cdot ((s-1)!)^N (C_K)^s M_s}\right) / \log_{10}(2).$$

Letting β_s be the right hand side of the above inequality, we get explicit values for n and m that will guarantee the first error term is sufficiently small, namely $n \geq \max(2\log_{10}(Ns), 2\beta_s)$ and $m \geq \max(1, \beta_s)$. We remark that by considering Stirling's approximation of the factorial function,

$$\sqrt{2\pi s}\left(\frac{s}{e}\right)^s e^{\frac{1}{12s+1}} < s! < \sqrt{2\pi s}\left(\frac{s}{e}\right)^s e^{\frac{1}{12s}} \quad \text{for } s \geq 1,$$

it is clear that β_s will be $O((s-1)\log(s-1) + \log(M_s))$ as s gets large and in particular the precision to which π and $\sqrt{|\Delta(K)|}$ need to be known will be at least slightly worse then a linear function of s.

Turning our attention to the second error term, recall that

$$E_0(s,T) < \left(\frac{\pi^2}{6}\right)^N \left(\left(1 + \frac{1}{(s-1)T^{s-1}}\right)^N - 1\right).$$

Hence it suffice to find T such that

$$\left(\frac{\pi^2}{6}\right)^N \left(\left(1+\frac{1}{(s-1)T^{s-1}}\right)^N - 1\right) \frac{(2(s-1)!)^N}{\sqrt{|\Delta(K)|}}(C_K)^s < \frac{1}{10M_s}.$$

In order to avoid messy formulas, we assume $(s-1)T^{s-1} \geq N^2 - N$ (a fairly mild assumption in the long run) and use this assumption to justify replacing $(1+\frac{1}{(s-1)T^{s-1}})^N$ with $1+\frac{N+1}{(s-1)T^{s-1}}$. This simplifies the inequality to

$$\frac{N+1}{(s-1)T^{s-1}} < \frac{6^N\sqrt{|\Delta(K)|}}{10\cdot 2^N\pi^{2N}M_s((s-1)!)^N(C_K)^s}$$

$$\Rightarrow \left(\frac{10\cdot(N+1)\cdot 2^N\pi^{2N}M_s((s-1)!)^N(C_K)^s}{(s-1)6^N\sqrt{|\Delta(K)|}}\right)^{\frac{1}{s-1}} < T.$$

Once again using Stirling's approximation of the factorial function, one notes that as $s\to\infty$, the left hand side of the above inequality is $O(M_s^{\frac{1}{s-1}}(s-1)^N)$ so in particular, evaluating ζ_K in this way uses a T value that grows with s at least as fast as an N degree polynomial. Hence we have the following theorem.

Theorem 5.0.3. *Let K be a totally real number field over $\mathbb{Q}$ of degree m. Assume that in the ring of integers $\mathcal{O}_K$, all prime ideals, their norms, and their ramification indices over $\mathbb{Z}$ are known. Then $\zeta_K(1-k)$ can be computed and fully reduced to a rational in $O(k^m M_k^{\frac{1}{k-1}})$ where M_k is the bound on the denominator obtained from (5.0.2). Furthermore, the precision to which irrational values need to be computed in the calculations can be bounded by a function that is $O(k\log(k)+\log(M_k))$.*

We conclude this section with an example that illustrates the above in practice. According to the table of zeta values for quadratic extensions given in chapter 4, $\zeta_{\mathbb{Q}(\sqrt{7})}(1-4) = \frac{113}{15}$. Let us check this using the method above. Set $K=\mathbb{Q}(\sqrt{7})$ and $N=2$. The only primes that ramify in K are 2 and 7. Since

K is an abelian extension of $\mathbb{Q}$, we have $e_2^w = 2$, $e_7^t = 2$, and all else equal to 1. Using (5.0.2) we consider the possible primes p and their powers that could divide the denominator of $2^{-2}\zeta_K(1-4)$. If $p \neq 2, 7$, then $4 \equiv 0 \mod (p-1)$. Clearly the only possibilities are 3 and 5, both of which can appear to only a single power since 6 and 20 are both greater then 4. p could not be 7 because $4 \not\equiv 0 \mod (6/2)$. For $p = 2$ we must have $2^{l(n)}/2 \leq 4$, where n is the power of 2 appearing, and so $n \leq 5$. It follows that $M_4 = 2^3 \cdot 3 \cdot 5 = 120$ is such that $\zeta_K(1-4) \cdot M_4$ is an integer. Subbing in the values $N = 2$, $|\Delta(K)| = 28$ and $s = 4$ into the necessary inequalities above, we see that $T > 28.2$ and $\beta_4 \cong 16.1$ so $m \geq 15.1$ and $n \geq 32.2$. Set $m = n = 33$ for simplicity and $T = 29$, which gives a value of $Z_K(4, 29) = 1.093978\ldots$. Plugging the necessary values into MAGMA, we get

$$M_4 \cdot (-1)^2 \cdot F(4, 31, 31) \cdot Z_K(4, 26) = 903.9962\ldots$$

which obviously rounds to 904. Hence $\zeta_K(3) = \frac{904}{120} = \frac{113}{15}$ exactly as predicted.

CHAPTER 6
A Modular Function Approach

In this section we give a brief description of how one can determine zeta function values at negative integers via the theory of Hilbert modular forms. This section will follow and refer to the material given in [11] and [17]. In what follows, assume L is a totally real number field (as we have seen earlier this is the only interesting case), $[L : \mathbb{Q}] = n$, $\{\tau_1, \ldots, \tau_n\}$ are the distinct embeddings of L into $\mathbb{C}$ and let $\mathbb{H}$ denote the complex upper half-plane. For an arbitrary matrix $\mu = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(L)^+$, let $\tau_j(\mu) = \begin{pmatrix} \tau_j(a) & \tau_j(b) \\ \tau_j(c) & \tau_j(d) \end{pmatrix}$. Furthermore, if $z = (z_1, \ldots, z_n) \in \mathbb{H}$ we have a natural action $\mu z = (\tau_1(\mu)z_1, \ldots, \tau_n(\mu)z_n)$ where each $\tau_i(\mu)$ acts on z_i as a fractional linear transformation in the usual way.

For an arbitrary fractional ideal $\mathcal{A}$ of L, define the algebraic group

$$GL(\mathcal{O}_L \oplus \mathcal{A})^+ = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, d \in \mathcal{O}_L, b \in \mathcal{A}, c \in \mathcal{A}^{-1}, ad - bc \in (\mathcal{O}^\times)^+ \right\},$$

where $(\mathcal{O}_L^\times)^+$ denotes the group of all totally positive units of $\mathcal{O}_L$.

Given a matrix $\delta = \left(\begin{smallmatrix} \delta_1 & \delta_2 \\ \delta_3 & \delta_4 \end{smallmatrix}\right) \in GL_2(\mathbb{R})^+$, for $z \in \mathbb{H}$ we define

$$j(\delta, z) = (\delta_3 z + \delta_4)(\det \delta)^{-1/2}.$$

For a vector $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbb{Z}^n$ and a matrix $\mu \in GL_2(L)^+$, let

$$j_{\mathbf{k}}(\mu, z) = \prod_{i=1}^{n} j(\tau_i(\mu), z_i)^{k_i}$$

with $z = (z_1, \ldots, z_n) \in \mathbb{H}^n$.

It is clear that our definition of j agrees with the concept of *factor of automorphy* associated with usual modular forms. We use $j_{\mathbf{k}}$ to extend this concept to holomorphic functions on $\mathbb{H}^n$ in what follows. Let $f : \mathbb{H}^n \to \mathbb{C}$ and put

$$(f|_{\mathbf{k}}\mu)(z) = j_{\mathbf{k}}(\mu, z)^{-1} f(\mu z).$$

For $\Gamma \subseteq GL(\mathcal{O}_L \oplus \mathcal{A})^+$ of finite index, we say that f as above is a *Hilbert modular form* of weight $\mathbf{k}$ and level Γ if it is holomorphic, $f|_{\mathbf{k}}\mu = f \ \forall \mu \in \Gamma$, and f satisfies a certain holomorphy condition at infinity. This holomorphy condition generalizes the concept of q-expansions at the cusps for usual modular forms and amounts to having an expansion

$$f(z) = \sum_{\nu \in M^*} a_\nu e^{2\pi i \mathrm{Tr}(\nu \cdot z)},$$

where $M = \{a : \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma\}$, M^* is its complimentary $\mathcal{O}_L$-module and $\mathrm{Tr}(\nu \cdot z)$ equals $\tau_1(\nu)z_1 + \ldots + \tau_n(\nu)z_n$ (see [11] for details).

The primary examples of Hilbert modular forms that we are interested in are the *Eisenstein series*, which we introduce now. Fix a fractional ideal $\mathcal{B}$ of L. Let A be some class of fractional ideals in the class group of L and let $\mathcal{A}$ be an arbitrary representative. For $k \in \mathbb{Z}$, k even and ≥ 2, let $\mathbf{k}$ equal $(k, k, \ldots, k)$ and define the Eisenstein series of weight $\mathbf{k}$ and class A as

$$G_{\mathbf{k},A} := ||\mathcal{A}||^k \sum\nolimits'_{(\alpha,\beta) \in \mathcal{A}\mathcal{B} \oplus \mathcal{A}} \mathbb{N}(\alpha z + \beta)^{-k},$$

where $\alpha z + \beta = (\tau_1(\alpha)z_1 + \tau_1(\beta), \ldots, \tau_n(\alpha)z_1 + \tau_n(\beta))$, $\mathbb{N}(z) = z_1 \cdots z_n$ and the sum is restricted in the following sense: we define $(\alpha, \beta) \sim (\alpha', \beta')$ if there exists $\epsilon \in \mathcal{O}_L^\times$ st. $\alpha = \epsilon\alpha'$ and $\beta = \epsilon\beta'$. This is clearly an equivalence relation on the non-zero pairs and the restricted sum takes one element from each equivalence class. Note that this is well defined because the algebraic norm of a unit is always 1 and one easily sees that the value of this function does not change when $\mathcal{A}$ is replaced by $\eta\mathcal{A}$ for any $\eta \in L$. Finally, this sum necessarily converges under the given conditions on $\mathbf{k}$ assuming $n > 1$ and also for $n = 1$ if $k \geq 4$ (in which case we are reduced to the usual Eisenstein series of modular forms on $SL_2(\mathbb{Z})$).

One can check from the definitions that multiplication on the right by any $\mu \in GL(\mathcal{O}_L \oplus \mathcal{B}^{-1})^+$ is an automorphism for $\mathcal{A}\mathcal{B} \oplus \mathcal{A}$ that preserves the equivalence relation defined above. This can be used to obtain the following result.

Proposition 6.0.1. *The Eisenstein series defined as above is a Hilbert modular form of weight* $\mathbf{k}$ *and level* $GL(\mathcal{O}_L \oplus \mathcal{B})^+$.

Proof. See pg. 69 of [11]. □

As before, let A be an ideal class in the class group of L and let $\mathcal{B}$ be any integral ideal. We define the two functions

$$\zeta_A(k) = \sum_{\substack{\mathcal{A} \in A \\ \mathcal{A} \subset \mathcal{O}_L}} ||\mathcal{A}||^{-k}; \quad \sigma_{k-1,A}(\mathcal{B}) = \sum_{\substack{\mathcal{A} \in A \\ \mathcal{B} \subseteq \mathcal{A} \subseteq \mathcal{O}_L}} ||\mathcal{A}||^{k-1}.$$

One notes immediately that summing the ζ_A as A runs through all the ideal classes gives the usual ζ_L and likewise summing all the $\sigma_{k-1,A}$ gives a function that generalizes the usual σ_{k-1} function on $\mathbb{N}$ to ideals of $\mathcal{O}_L$. We shall call

this function σ'_{k-1}, and explicitly it is defined as $\sigma'_{k-1}(I) = \sum_{I \subseteq \mathcal{A} \subseteq \mathcal{O}_L} ||\mathcal{A}||^{k-1}$. It turns out that the ζ_A and $\sigma_{k-1,A}$ functions appear quite prominently in the Fourier expansion of the $G_{\mathbf{k},A}$, while $\zeta_{\mathbb{Q}}$ and σ_{k-1} appear in the q-expansion of the usual Eisenstein series modular forms, hence one may suspect that there may be a parallel between the coefficients of these two different types of modular forms. Indeed this is the case, and it is this relationship that one can exploit to determine special values of ζ_L. More explicitly, after multiplying the series $\sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^k}$ by an appropriate normalization constant, we get a modular form $E_k(z)$ of weight k (assuming $k \geq 4$) with q-expansion $\zeta_{\mathbb{Q}}(1-k)/2 + \sum_{m\in\mathbb{N}} \sigma_{k-1}(m)q^m$ (see [17]). On the other hand, if we define

$$E^{L,*}_{\mathbf{k}} = \frac{1}{c} \sum_{A \in Cl(L)} G_{\mathbf{k},A},$$

where $c = \frac{(2\pi i)^{kn}}{(k-1)!^n} \Delta_L^{1/2-k}$ is a normalizing constant, we see immediately that $E^{L,*}_{\mathbf{k}}$ is a Hilbert modular form of weight $\mathbf{k}$ and level $GL(\mathcal{O}_L \oplus \mathcal{B})^+$. More importantly, the Fourier expansion about the cusp $(i\infty, \ldots, i\infty)$ is

$$E^{L,*}_{\mathbf{k}} = \frac{\zeta_L(1-k)}{2^n} + \sum_{\substack{\nu \in \mathcal{B}\mathcal{D}_L^{-1} \\ \nu \gg 0}} \sigma'_{k-1}((\nu)\mathcal{B}^{-1}\mathcal{D}_L) e^{2\pi i \mathrm{Tr}(\nu z)},$$

where $\mathcal{D}_L$ is the different of $\mathcal{O}_L$ and $\nu \gg 0$ means that ν must be totally positive.

The similarities are apparent, especially if one takes $\mathcal{B} = \mathcal{O}_L$, which we will now consider. Let $\Phi : \mathbb{H} \to \mathbb{H}^n$ be the diagonal map, $z \to (z, z, \ldots, z)$. Then by (6.0.1) and the fact that $GL(\mathcal{O}_L \oplus \mathcal{O}_L)^+ \supseteq SL_2(\mathbb{Z})$, we have that the function $E^{L,*}_{\mathbf{k}} \circ \Phi : \mathbb{H} \to \mathbb{C}$ is a modular form of weight kn and the q-expansion at $i\infty$ can be expressed as

$$E^{L,*}_{\mathbf{k}} \circ \Phi = \frac{\zeta_L(1-k)}{2^n} + \sum_{m=1}^{\infty} a_k(m) q^m,$$

where

$$a_k(m) = \sum_{\substack{\nu \in (\mathcal{D}_L^{-1})^+ \\ \mathrm{Tr}(\nu) = m}} \sigma'_{k-1}((\nu)\mathcal{D}_L) = \sum_{\substack{\nu \in (\mathcal{D}_L^{-1})^+ \\ \mathrm{Tr}(\nu) = m}} \sum_{(\nu)\mathcal{D}_L \subseteq I \subseteq \mathcal{O}_L} ||I||^{k-1}.$$

This is a truly elegant result and the reader is again directed to [11] for full details. The usefulness of the above expression comes from the fact that it is very easy to construct a basis for the vector space of modular forms of weight nk. In fact the set $\{E_4^i E_6^j\}$ where $i, j \in \mathbb{N}$ st. $4i + 6j = nk$ forms such a basis (See [17] pg. 118) and each of these basis elements has a q-expansion that is easily computable for a large number of terms (because we have a formula for the expansions of E_4 and E_6). Using this method to calculate $\zeta_L(1-k)$ is still limited however to ones ability to calculate the $a_k(m)$. To be able to calculate $E_{\mathbf{k}}^{L,*} \circ \Phi$ in terms of the basis, one needs to be able to calculate explicitly the $a_k(m)$ for at least $j + 1$ distinct values of n, where j is the dimension of the space of weight kn modular forms. Hence using this modular approach is very fruitful when a lot of additional information is already known about L, for example its different and its lattice structure. One especially nice case is when L is a quadratic extension, then the ring of integers of L is monogenous and (2.2.4) shows that $D_L = (\sqrt{\Delta_L})$. Using this and the well-understood structure of the ring of integers of quadratic fields and their ideals, one can calculate $\zeta_L(1-k)$ for certain k using explicit formulas such as *Siegel's formula*:

$$\zeta_L(-1) = \frac{1}{60} \sum_{\substack{a \in \mathbb{Z} \\ a \equiv \Delta_L \mod 2 \\ |a| < \sqrt{\Delta_L}}} \sigma_1\left(\frac{\Delta_L - a^2}{4}\right).$$

The methodology for determining the above formula is mapped out in [11] and the interested reader is directed to [6] for more formulae like the one above.

We conclude this section with another discussion of how expensive it is to calculate zeta function values in this way. As usual, we fix a number field L with $[L : K] = n \geq 2$ and we let $k \in \mathbb{N}$ vary over positive even integers at least 2. We assume that the structure of the field L and its ring of integers is a precalculation, so we do not concern ourselves with finding the different, determining the ideal structure of $\mathcal{O}_L$, or finding totally positive elements of a certain trace as these things are independent of k. The final result will not be as precise for this section as in previous analysis because as we shall see, the amount of computation needed actually depends on the structure of certain modular groups.

As noted above, the complex vector space V of modular forms of weight nk has a basis $\{E_4^i E_6^j\}$ where i and j are positive integers such that $4i + 6j = nk$ and we assume the E_i's are normalized such that

$$E_4 = \frac{1}{120} + \sum_{t=1}^{\infty} \sigma_3(t) q^t \text{ and } E_6 = \frac{-1}{252} + \sum_{t=1}^{\infty} \sigma_5(t) q^t.$$

It is not hard to prove that the dimension of this vector space can be expressed as

$$\text{Dim}(V) = \begin{cases} \left\lfloor \frac{nk}{12} \right\rfloor + 1 & \text{if } nk \not\equiv 2 \mod 12 \\ \left\lfloor \frac{nk}{12} \right\rfloor & \text{else.} \end{cases}$$

In particular we note that the dimension m is $\sim nk/12$.

We shall see shortly that each of these basis elements will need to have *at least* the first $m + 1$ terms in their q-expansions calculated explicitly. This requires calculating powers of E_4 and E_6 up to approximately $nk/4$ and $nk/6$ respectively. We give a brief analysis of how many operations that requires. Assume that E_4's and E_6's q-expansions are already known to a sufficiently high degree (it is fair to assume this would be a precalculation). Finding the

product modulo q^{m+1} of two expansions of the form $a_0 + a_1 q + \ldots + a_m q^m$ and simplifying requires $(m+1)(m+2)/2$ instances of multiplication and $(m+1)(m+2)/2 - (m+1)$ instances of addition for a total of $(m+1)^2$ operations. Thus it takes approximately $5nk/12 \cdot (m+1)^2 \approx 5m(m+1)^2$ operations to find all the necessary powers of E_4 and E_6. We then have to multiply powers of E_4 with powers of E_6, which we do between $m-2$ and m times and each time we require $(m+1)^2$ more operations. In any case, the total cost of finding the first $m+1$ terms in the q-expansion of every basis element will be $O(m^3)$.

Returning to the problem at hand, for simplicity of notation we denote the function $E_{\mathbf{k}}^{L,*} \circ \Phi = f$ and $\{E_4^i E_6^j\} = \{g_i\}_{i=1}^m$, so that we are looking to find constants $d_i \in \mathbb{C}$ st. $f = \sum_{i=1}^m d_i g_i$. Let v_i be m-tuples with j^{th} coordinate equal to the coefficient on q^{j-1} in the q expansion of g_i. We claim that the v_i's form a basis for $\mathbb{C}^m$. Indeed if not, then there exists non-trivial linear relations between the first m coefficients in the g_i's and thus there exists a non-zero weight nk cusp form whose zero at infinity is of order at least m. Letting Δ be the usual discriminant form of weight 12, it follows that we can divide our cusp form by Δ^{m-1} to get a new non-trivial cusp form whose weight lies in $\{0, 4, 6, 8, 10, 14\}$. But no such cusp forms exist (See [17] pg. 117) and hence we have a contradiction.

Let now v_i' be the $(m-1)$-tuples st. v_j' is equal to v_j with the first term removed. It follows from above that there exists at least one subset of the v_i' that form a $\mathbb{C}^{m-1}$ basis, and such a subset can be found by applying a Gaussian elimination algorithm to the m by $(m-1)$ matrix whose rows are the v_i'. As remarked in Appendix A when discussing resultants of polynomials, Gaussian elimination of a t by t matrix has an operation cost that is $O(t^3)$, and we conclude that the cost of finding the desired basis is $O(m^3)$. Let us suppose

that $v'_1, \ldots, v'_{m-1}$ are all linearly independent. Then we can find $c_1, \ldots, c_{m-1}$ such that

$$g_m - \sum_{i=1}^{m-1} c_i g_i = A_0 + 0 \cdot q + 0 \cdot q^2 + \ldots + 0 \cdot q^{m-1} + A_m q^m + \ldots.$$

What we are looking for in the above expression is the first non-zero term after A_0. If A_j is such a term, it follows that if we define w_i to be the m-tuple v'_i with the q^j coefficient of g_i appended to the end of the vector, then the w_i's will form a basis for $\mathbb{C}^m$. Note that such an A_j necessarily exists because the expression above is a weight nk modular form and the constant functions are not. Unfortunately it is possible that A_m will in fact be zero, and if this were the case then we would would have to go back and find the coefficient of the next term in the q-expansion of each basis element and find A_{m+1} above and hope it is not zero. Obviously if it were zero then we would have to continue doing this, which is why it was mentioned earlier that we need to calculate coefficients at least up to the q^m term for each basis element.

Let us ignore this issue and assume for simplicity that A_m is not zero. Then we can solve for the d_i above by applying Gauss-Jordan elimination to the augmented matrix $(A|B)$, where the columns of A are the w_i and the $B = (a_k(1), a_k(2), \ldots a_k(m-1), a_k(m))$ (of course if A_m is zero, we replace the last coordinate of B with $a_k(j)$, where A_j is as above).

We now consider the issue of evaluating the $a_k(i)$ for $1 \leq i \leq m$, which as discussed above is the best case scenario. This question breaks down into two problems, namely how many totally positive elements of trace less then m could lie in $\mathcal{D}_L^{-1}$ and how many arithmetic operations does it take to evaluate $\sigma_{k-1}(\nu\mathcal{D})$ for some ν satisfying these conditions? We consider each problem in turn.

For some $d \in \mathbb{N}$, $d \cdot \mathcal{D}_L^{-1}$ is an integral ideal. Applying Minkowski's lattice theory, we can consider $I = d \cdot \mathcal{D}_L^{-1}$ as a complete lattice in $\mathbb{R}^n$ whose fundamental mesh has volume $\sqrt{|\Delta_L|}[\mathcal{O}_L : I]$ (See [22] pg. 31). We wish to estimate the number of elements in I that lie in the first quadrant and whose trace lies between d and md. This is equivalent to finding the number of lattice points that lie inside the simplex whose edges consist of $\{(dm, 0, 0, \ldots, 0), (0, dm, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, dm)\}$ but outside the one whose edges are $\{(d, 0, \ldots, 0), \ldots (0, 0, \ldots, d)\}$. The number of points in each simplex will be approximately the ratio of their volumes to the volume of the fundamental mesh. It is well known that the simplices above have volume $(dm)^n/n!$ and $d^n/n!$ respectively. Hence the number of lattice points that lie in the first simplex but not the second will be approximately

$$d^n \frac{m^n - 1}{n!\sqrt{|\Delta_L|}[\mathcal{O}_L : I]}.$$

Using Stirling's approximation to the factorial function (See previous section) and the fact that $m \approx nk/12$, the above expression is $O(k^n)$. We conclude that when determining $a_k(i)$ for i from 1 to m, we will have to consider the value of σ'_{k-1} at a number of ideals that grows with k in polynomial time. Note that if we wished to put an explicit bound on the number of such elements instead of just an estimate, we could proceed by first finding the maximum length of a vector contained in the lattice spanned by I, say c. We would then replace the lengths dn and d in the two simplices by $dn + c$ and $\max(d - c, 0)$ respectively. Calculating the volume ratios would then put a maximum value on the number of lattice points in the first simplex and a minimum on the second. It is clear however that we would still end up with a function that grows like an n-degree polynomial in k.

Turning now to issue of evaluating σ'_{k-1}, we note that this function satisfies the same sort of multiplicative property on ideals that the usual σ_{k-1} satisfies on integers, namely $\sigma'_{k-1}(P^e) = (||P||^{(k-1)(e+1)} - 1)/(||P||^{k-1} - 1)$ when P is some prime ideal, and $\sigma'_{k-1}(IJ) = \sigma'_{k-1}(I)\sigma'_{k-1}(J)$ when I and J are relatively prime ideals. Since we are assuming that factoring ideals of $\mathcal{O}_L$ is free, it follows that the number of arithmetic operations needed to evaluate $\sigma'_{k-1}(J)$ is bounded by a constant times the number prime ideals dividing J, hence we consider just how many this could be. We first note that using the AM-GM inequality, we can put a bound on the norm of any fractional ideal generated by a totally positive element whose trace is less then m. Indeed for such a ν we have

$$k/12 + 1/n \geq (m/n) \geq \frac{\mathrm{Tr}(\nu)}{n} = \frac{\sum_{i=1}^{n} \tau_i(\nu)}{n} \geq \sqrt[n]{N(\nu)}.$$

In particular the norm of $\nu\mathcal{D}_L$ is bounded by say $(k/3)^n$ times the norm of $\mathcal{D}_L$. We conclude that the number of prime ideals that could possibly divide $\nu\mathcal{D}_L$ is $o(\log(k))$.

It follows from our that the operation cost of evaluating all the necessary arithmetic functions to determine $a_k(i)$ for $1 \leq i \leq m$ will be $o(k^n \log(k))$. We conclude the section with a summary of the results.

Theorem 6.0.2. *Let K be a totally real number field over $\mathbb{Q}$ of degree m. Assume that bases of modular forms for sufficiently large weights have been precalculated with Fourier expansion about $i\infty$. Then $\zeta_K(1-k)$ can be calculated and fully reduced to a rational number with $o(k^m \log(k) + f(k))$ operations, where $f(k)$ is a function of k that is at best cubic in k.*

Conclusion

The motivation of this thesis was to construct an algorithm that could compute Dedekind zeta function values at negative integers for abelian number fields. We have now managed to construct such an algorithm that runs in linear time for a fixed field and have used it to calculate values for many different fields.

Further analysis into this topic could be fruitful as there are a number of different avenues to pursue. As discussed in chapters 5 and 6, there is the issue of calculating these zeta values for non-abelian fields, and it would be interesting to try and come up with an algorithm that is more effective then the ones described in this thesis, which essentially run in polynomial time of degree equal to the degree of the extension field over $\mathbb{Q}$.

Another potential topic would be a study into when these values are integers. Some numerical results on the subject were given in chapter 4, but it would be interesting to try and find a theoretical reason for when and why these integer values occur. A good place to start on the subject might be to consider some of the results discussed in chapter 5, where we note that in [11] it is shown that one can put a bound on the possible denominators occurring by considering the ramification of certain primes. Other similar results can be found in the text, including a result that shows that if k and k' are two even integers satisfying certain congruence relations for a given prime, then there is a relationship between the values of that prime appearing in the denominator of $\zeta_L(1-k)$ and $\zeta_L(1-k)$. Hence one might suspect that under certain conditions, finding $\zeta_L(1-k)$ to be integral for one k could lead to

the same result for another. One interesting pattern that was observed by the author through the course of writing this thesis was that $\zeta_{\mathbb{Q}(\omega_{2^n})}(-1)$ was verified to be integral for $5 \leq n \leq 11$ and one might suspect for even higher n that this continues to hold. This result can be considered somewhat less surprising by the aforementioned theory in [11] from which it follows that for any n, the denominator of $\zeta_{\mathbb{Q}(\omega_{2^n})}(-1)$ has to divide 12. Furthermore all the Bernoulli numbers in the product of some zeta function for some field K will also be appearing in the product of the zeta function for any field containing K which might suggest why we see in Table 4-7 that the number of zeta values occurring as integers increases as the primitive root of unity increases. The aforementioned bounded denominator result however is unique to the powers of 2 and k value of 2, and so not surprisingly this result of integrality is not so common for other towers of values, for example $\zeta_{\mathbb{Q}(\omega_{2^n})}(-3)$ was verified to not be integral for $n \leq 11$ and $\zeta_{\mathbb{Q}(\omega_{3^n})}(-1)$ was also verified to not be integral for $n \leq 6$.

One final topic that could build on the results in this thesis is a discussion of the growth rate of these values, either as a function of $1-k$ or the degree of the field or as a function of the conductor. A brief look at some of the results given in chapter 4 certainly leads to the conclusion that these values can get quite large extremely rapidly. For example, in verifying integrality as discussed above, the value $\zeta_{\mathbb{Q}(\omega_{2048})}(-1)$ came out to be an integer with 1649 digits! This phenomena can most likely be explained by looking at the functional equation in chapter 5, where one notes that the equation for $\zeta_K(1-s)$ has the factor $|\Delta(K)|^{\frac{2s-1}{2}}$ appearing in it, so certainly fields with large discriminants are going to have larger zeta values then those with small discriminants, all other variables being equal. However it would still be interesting to see if one could use say the conductor of K, along with the way that primes split in the

corresponding cyclotomic field to get a very precise bound using the infinite product expansion of the zeta function.

Appendices

APPENDIX A
Computational Algorithms

In this section we proceed to give a brief synopsis of the general methods and algorithms utilized by programs such as MAGMA needed to run the program we have developed. Most of these routines are already built into common computing programs and so a brief overview is all that is given.

Generators of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ when p is a prime

It is well known that 5 and -1 serve to generate $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ for any $\alpha \geq 1$ so we restrict to the case when p is odd and hence $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group. The following lemma from [7] shows that finding generators of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ reduces to the case when $\alpha = 1$.

Lemma 1. *Let p be an odd prime, and let g be a primitive root modulo p. If g is not a primitive root modulo every power of p, then $g + p$ is.*

Proof. Let l be any prime dividing $(p-1)$. Then $g^{p^{\alpha-1}\frac{p-1}{l}} \equiv g^{\frac{p-1}{l}} \not\equiv 1 \mod p$, since g is a primitive root modulo p. Clearly then $g^{p^{\alpha-1}\frac{p-1}{l}} \not\equiv 1 \mod p^\alpha$. We conclude g is a primitive root of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ iff $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \mod p^\alpha$.

Claim: $x^p \equiv 1 \mod p^\alpha$ implies $x \equiv 1 \mod p^\beta$ for all $1 \leq \beta \leq \alpha - 1$.

Proof: Clearly it is enough to show the claim when $\beta = \alpha - 1$. When $\alpha = 2$, the result clearly follows from Fermat's little theorem. Assume we have proven the claim for all $2 \leq \alpha < N$ and $x^p \equiv 1 \mod p^N$. Then $x^p \equiv 1$

mod p^{N-1} and so by inductive assumption, x is of the form $1 + kp^{N-2}$. Then $1 \equiv x^p \equiv 1 + pkp^{N-2} \mod p^N$ since $N \geq 3$. Hence k is divisible by p and we are done.

Returning to the proof of the lemma, we can apply the claim repeatedly to the statement $g^{p^{\alpha-2}(p-1)} \equiv 1 \mod p^\alpha$ to get $g^{p-1} \equiv 1 \mod p^2$. If this holds, then $(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 - g^{p-2}p \not\equiv 1 \mod p^2$ and we conclude from the claim that $(g+p)$ is then a generator of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for every $\alpha \geq 1$. $\square$

The following algorithm from pg. 25 of [7] takes an odd prime p and finds a primitive root of $(\mathbb{Z}/p\mathbb{Z})^\times$.

0. [Input] p an odd prime

1. [Initialize a] set $a \leftarrow 1$ and let $p - 1 = p_1^{v_1} ... p_k^{v_k}$ be the complete factorization of $p - 1$.

2. [Initialize check] Set $a \leftarrow a + 1$ and $i \leftarrow 1$.

3. [Check p_i] Compute $e \leftarrow a^{\frac{(p-1)}{p_i}}$. If $e = 1$ go to step 2. Otherwise, set $i \leftarrow i + 1$.

4. [finished?] If $i > k$ output a and terminate the algorithm, otherwise goto step 3.

It is easy to see that this algorithm works because a is not a primitive root if and only if the order of a is a proper divisor of $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$. Hence the algorithm checks the congruency class of a raised to every maximal proper divisor of $p - 1$. Using the usual exponentiation by squaring method for calculating powers in $\mathbb{Z}/p\mathbb{Z}$, the running time of each check is on the order of $O(\log(p - 1))$ and must be done at most k times for each a. A simple bound

on the number of prime divisors of $p-1$ shows that k is $o(\log(p))$. Assuming the GRH we have a result due to Shoup (see [3] pg. 221) which says that as p runs over the primes, if $h(p)$ denotes the least positive primitive root mod p then $h(p) = O(\log(p)^6)$. Clearly the overall running time of the algorithm depends on the efficiency of factoring $p-1$ as well as the aforementioned bounds and when p is quite large, the former will dominate the calculation speed. On the other hand, if we ignore the factoring cost of $p-1$, we conclude that the running time will be on the order of $o(\log(p)^8)$ operations.

By lemma (1), if g is the output of this algorithm we need only check if g^{p-1} is congruent with 1 mod p^2 to find a generator for $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Hence this algorithm provides an effective method for determining primitive roots of $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ when factoring $p-1$ is not an issue.

Determining primes that split completely in Galois number fields

If a number field K is Galois over the rationals, then the primes of $\mathbb{Q}$ split uniformly in it, ie. $(p) = Q_1^e Q_2^e ... Q_r^e$ and every Q_i has the same inertial degree over p. Given then a function $f(x) \in \mathbb{Q}[x]$ whose roots generate K, if p does not divide the discriminant of f, then p splits completely in K iff f has a root modulo p. The following algorithm from [20] pg. 82 gives a method to determine whether f has a root modulo p.

0. [Input] $\overline{f}(x)$ and $h(x) = x^p - x \in \mathbb{Z}/p\mathbb{Z}[x]$.
1. Set $r(x) \leftarrow f(x) \mod h(x), f(x) \leftarrow h(x), h(x) \leftarrow r(x)$. If $h(x) = 0$ go to
2. Otherwise go to 1.
2. Return $g(x)$

The returned value is not a constant polynomial if and only if f has a zero modulo p and hence p splits completely in K. The algorithm works because it calculates the GCD of the polynomials f and $x^p - x = \prod_{a \in \mathbb{Z}/p\mathbb{Z}} (x - a)$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Letting $m = \max\{p, deg(f)\}$, then the algorithm runs in $O(m^2)$ $\mathbb{Z}/p\mathbb{Z}$-operations.

Determining the discriminant of a polynomial

We follow the introduction of the *resultant* in [8] to motivate the solution of this problem. Suppose $f(x) = a_n x^n + ... + a_1 x + a_0$ and $g(x) = b_m x^m + ... + b_1 x + b_0$ are two polynomials over some field $F[x]$ with roots $x_1, ..., x_n$ and $y_1, ..., y_m$ respectively in the algebraic closure of F. Consider the determinant of the following $(n+m) \times (n+m)$ matrix A:

$$R(f,g) := \det(A) = \begin{vmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & & & & & \\ & a_n & a_{n-1} & \cdots & a_1 & a_0 & & & & \\ & & a_n & a_{n-1} & \cdots & a_1 & a_0 & & & \\ & & & & \ddots & & & \ddots & & \\ & & & & a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & & & & \\ & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & & & \\ & & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & & \\ & & & & \ddots & & & & \ddots & \\ & & & & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 \end{vmatrix}.$$

Suppose $R(f,g) = 0$. Then there exists some $(m+n) \times 1$ row vector v, with

$$v := [\lambda_{m-1}, \lambda_{m-2}, \cdots, \lambda_0, \mu_{n-1}, \mu_{n-2}, \cdots, \mu_0]$$

such that $v.A = \vec{0}$. Defining the polynomials $r(x) = \lambda_{m-1} x^{m-1} + ... + \lambda_0$ and $s(x) = \mu_{n-1} x^{n-1} + ... + \mu_0$, we see by comparing coefficients that $v.A = \vec{0}$ is

equivalent to the identity $r(x)f(x) + s(x)g(x) = 0$. On the other hand, since $\deg(r) < \deg(g)$ and $\deg(s) < \deg(f)$, this identity can only hold if f and g share a common zero in the algebraic closure of F. Conversely, if f and g share a common non-trivial factor, say $h(x)$, then $r(x) = \frac{g(x)}{h(x)}$ and $s(x) = \frac{f(x)}{h(x)}$ have degrees strictly less then g and f respectively, and solve the identity above. We conclude that $R(f, g) = 0$ iff f and g have a common root.

Writing out explicitly $R(f, g) = \sum_{\sigma \in S_{n+m}} (-1)^{|\sigma|} a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot \ldots \cdot a_{n+m,\sigma(n+m)}$, it is clear that all of the non-zero terms in this sum will be comprised of m factors taken from the coefficients of f and n factors taken from the coefficients of g. Note that the coefficients of f are either a_n or a_n times an elementary symmetric function in the x_i and a similar statement holds for the coefficients of g. It follows that $R(f, g)$ is $a_n^m b_m^n$ times a function symmetric in both the x_i and y_j. Furthermore, $R(f, g)$ is homogenous of degree m in the x_i and degree n in the y_j.

We know that if $x_i = y_j$ then $R(f, g) = 0$, so $(x_i - y_j)$ must divide $R(f, g)$ for all i, j. Therefore

$$R(f, g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j) \times K,$$

where K is some symmetric function in the x_i and y_j. By our discussion above regarding the homogeneity of the terms of $R(f, g)$, we know that the x_i do not appear in powers larger then m and likewise the y_j do not appear in powers larger then n. Hence K must be independent of the x and y and therefore a constant. Considering the case where all the x_i are zero and $a_n = 1$, it is easy to see that $R(f, g) = b_0^n = (b_m(-1)^m(y_1 \ldots y_m))^n$ and so K must equal 1. We conclude by noting that the above formula for $R(f, g)$ can be written as

$$R(f, g) = a_n^m \prod_{i=1}^{n} g(x_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(y_j). \tag{A.1}$$

Returning now to our original problem of finding the discriminant of a polynomial $f \in \mathbb{Q}[x]$, we use the formula in $(A.1)$. One can represent $\Delta(f)$ using norms and derivatives as follows:

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{n-2} N_{\mathbb{Q}}^K(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} a_n^{n-2} \prod_{i=1}^{n} f'(\alpha_i)$$

where $\{\alpha = \alpha_1, ..., \alpha_n\}$ run through all of the zeros of f in its splitting field K. Setting $g = f'$ and looking at the first equality in $(A.1)$, we see that $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \frac{1}{a_n} R(f, f')$. We conclude that calculating the discriminant of f reduces to calculating the determinant of a $2n-1 \times 2n-1$ matrix. One relatively efficient method of doing this is to reduce the matrix to an upper triangular one via Gaussian elimination, and then multiply along the diagonal. By [9], computing a Gaussian elimination for a $k \times k$ matrix takes approximately $2k^3/3$ arithmetic operations, hence computing the discriminant of a polynomial f can be done in cubic time with respect to the degree of f.

Factoring and the Irreducibility of Polynomials over $\mathbb{Z}$

Given a polynomial $f \in \mathbb{Z}[x]$, the reader is most likely familiar with numerous situational techniques for checking the irreducibility of f such as Eisenstein's criteria, the rational root test and reducing modulo various primes. While these can be very quick checks to test for irreducibility, they are often not sufficient to determine irreducibility for a general polynomial and hence algorithms relying on more general techniques have been developed for use in computational algebra programs such as MAGMA or Maple. Of course, most programs also have a built in *Factorization* algorithm, and certainly being able to factor f over $\mathbb{Z}$ suffices to be able to determine its irreducibility. However

if one is only interested in irreducibility, it seems wasteful to factor if one can avoid it so it is still useful to explore fast algorithms that can determine irreducibility without factoring. In what follows we describe two algorithms, one which returns a probabilistic answer on irreducibility and one that can confirm irreducibility but not rule it out. See [27] and [21] respectively for complete details.

*Note that in what follows, we will always assume f is squarefree, since we can check the resultant $R(f, f')$ to determine otherwise.

We begin with a discussion of Landau's famous theorem on prime ideals of a number field, which is formalized on pg. 228 of [3] as follows:

Theorem 2. *Let K be an algebraic number field of degree n. Let $\pi_K(x)$ denote the number of prime ideals whose norm is $\leq x$. Let $\lambda(x) = (\log x)^{3/5}(\log\log x)^{-1/5}$. There is a $c > 0$ (depending on K) such that*

$$\pi_K(x) = li(x) + O(xe^{-c\lambda(x)}) \sim \frac{x}{\log x}.$$

One notes that this reduces to the usual statement of the prime number theorem when K is $\mathbb{Q}$. It follows quite easily that if $\pi_{K,i}$ for $1 \leq i \leq n$ with notation as above, denotes the number of prime ideals of K with inertial degree i, then $\pi_{K,1}(x) \sim \frac{x}{\log x}$. We conclude from this that

$$\lim_{x\to\infty} \frac{\pi_{K,1}(x)}{\pi(x)} = 1$$

where $\pi = \pi_{\mathbb{Q}}$.

One might wonder how this is relevant to the irreducibility of a polynomial f over $\mathbb{Z}$. Suppose f splits into r irreducible factors over the integers. Then

$$\begin{aligned}\mathbb{Q}[x]/(f(x)) &\cong \mathbb{Q}[x]/(f_1(x)) \times \cdots \times \mathbb{Q}[x]/(f_r(x)) \\ &\cong K_1 \times \cdots \times K_r\end{aligned}$$

where each K_j is the corresponding number field. Consider an arbitrary prime $p \in \mathbb{Z}$ that does not divide the discriminant of f and hence also none of the discriminants of its factors. It follows that each of the $\overline{f_j} \in \mathbb{Z}/p\mathbb{Z}[x]$ will decompose into irreducible factors that represent the splitting of the prime ideal (p) in the number field K_j. In particular, any linear factor in the decomposition of an $\overline{f_j}$ and hence in the decomposition of $\overline{f}$ corresponds to a prime ideal in K_j with prime norm. Fixing some large $N \in \mathbb{N}$ consider the following algorithm:

0. [Input] $f \in \mathbb{Z}[x]$.
1. [Initialize] $L \leftarrow 0$.
2. for primes in [1..N] do
3. $\overline{f} \leftarrow f \mod p, \quad G \leftarrow \mathrm{GCD}(x^p - x, \overline{f}), \quad L \leftarrow L + \deg(G)$.
4. [Output] $L/\pi_{\mathbb{Q}}(N)$

*Refer to earlier in the chapter for an efficient algorithm on calculating the required GCD. Also note that we are assuming f is squarefree.

In the above algorithm, L counts all linear factors appearing in the reduction of f modulo p, for any prime $p \leq N$. By the above discussion, this is equivalent to counting all prime ideals of all K_j with prime norm less then N, save a finite error term c_j arising from the reduction of primes dividing the

discriminant $\Delta(f_j)$. We conclude that if we let N go to infinity, the value of L/N would asymptotically approach r, as

$$\lim_{N\to\infty} \sum_{j=1}^{r} \frac{\pi_{K_j,1}(N) + c_j}{\pi_{\mathbb{Q}}(N)} = \sum_{j=1}^{r} 1.$$

Thus this algorithm allows one to guess with reasonable certainty whether or not f will be irreducible, depending on the choice of N. Of course no definite conclusion can be made for any fixed N, however this algorithm is extremely cheap to run and is therefore useful to consider for the following reason.

As we shall see shortly, there exist algorithms that can confirm irreducibility but are not guaranteed to do so in any finite amount of time. These algorithms run much faster then factoring algorithms but still not as fast as the one above as they rely on primality testing, possibly combined with searching for "small" divisors. Hence if we were to run our given algorithm and the output appeared to suggest f is almost certainly irreducible, then it is likely that we would save time if we used the deterministic algorithm before using a factorization algorithm. On the other hand, if we thought that f was most likely not irreducible, then it would probably be worthwhile to go straight to the factoring.

We now move on to describing a second irreducibility test, following the paper [21]. The test was originally implemented in the Maple algebra system and has likely gone through some improvements, however it is the author's understanding that most algebra systems currently use tests of a similar flavor to determine irreducibility over the integers. One final note is that primality testing is involved, so depending on the size of prime in question and the primality test used, we may again be left with only a probabilistic answer of irreducibility.

As usual, let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ be an arbitrary squarefree polynomial with a_n and $a_0 \neq 0$. The motivation behind our test is the following simple observation: if f were reducible, say $f(x) = f_1(x)f_2(x)$, then $f(n) = f_1(n)f_2(n)\ \forall\ n \in \mathbb{Z}$ and hence $f(n)$ should not be prime *too often*. More explicitly, this could only happen when all but one of f's factors are ± 1. Cauchy's bound on the roots of a polynomial comes in handy for considering when this could happen.

Lemma 3. *Let f be as above. Suppose $z \in \mathbb{C}$ is a root of f. Then $|z| < 1 + a_\infty/|a_d|$ where $a_\infty = \max\{a_0, \cdots, a_{n-1}, a_n\}$.*

Lemma 4. *Let f be as above and assume $a_n > 0, k > 0, k \in \mathbb{Z}$. Define $b = 1 + \lceil a_\infty/a_m \rceil$. If f_1 is any factor of f with degree$(f_1) = \delta$, then both $|f_1(b+k)|$ and $|f_1(-b-k)| > k^\delta$.*

The second lemma follows immediately from the first after considering the factorization of f over $\mathbb{C}$. The next theorem follows just as easily from the second lemma and the discussion above.

Theorem 5. *Let f, b and k be as above. If either $|f(b+k)|$ or $|f(-b-k)|$ is prime, then f is irreducible.*

It is intuitively clear how one might go about using theorem (5) to check irreducibility. Simply calculate b and start checking the primality of $f(n)$ for $n > b$. However, it is easy to see that this will not work in all cases. For example, the irreducible polynomial $x^2 + x + 2$ is never prime, in fact it is divisible by 2 at all values. In general we define the *fixed divisor* d of a

polynomial over $\mathbb{Z}$ to be the largest integer that divides $f(n)\ \forall\ n \in \mathbb{Z}$. Clearly 2 is the fixed divisor of $x^2 + x + 2$. The following lemma says that the fixed divisor is readily determinable.

Lemma 6. *Let $f \in \mathbb{Z}[x]$ have degree n. Then the fixed divisor d of f is $GCD(f(0), f(1), \cdots, f(n))$. More generally, d is the GCD of any $n+1$ consecutive values of f and is fixed under translation (ie. if $g(x) = f(x+t)$ for some integer t, then the fixed divisor of g equals the fixed divisor of f).*

Obviously it would be nice if once the fixed divisor is known, we could simply divide $f(b+k)$ by it and use the possible primality of the quotient to determine irreducibility. The next theorem says that we can do this assuming k is large enough.

Theorem 7. *Let f, b and k be as usual. Suppose $v | f(b+k)$ and $0 < v \leq k$. Then f is irreducible if either $v^{-1}f(b+k)$ or $v^{-1}f(-b-k)$ are prime.*

Note that theorem (7) not only says we may divide out by d as long as $k \geq d$, but in fact we may divide out by any divisor of $f(b+k)$ that is sufficiently small. This brings us to the basic procedure for some fixed N_1 and N_2:

0. [Input] $f \in \mathbb{Z}$ squarefree, non-zero constant, positive leading coefficient.
1. [Initialize] $n :=$ degree(f), $\quad b := \lceil 1 + a_\infty / a_n \rceil$,
$d :=$ GCD$(f(0), \cdots, f(n))$.
2. for k in $[d..d+N_1]$ do
3. $\quad u := |f(b+k)/d|$
4. $\quad$ if $u > 10^{N_2}$ return "LIMIT REACHED".

5. $g :=$ smallfactors$(u, k/d)$

6. for x in g do

7. if u/x is prime then return true.

8. $v := |f(-b-k)/d|$

9. if $v > 10^{N_2}$ return "LIMIT REACHED".

10. $g :=$ smallfactors$(u, k/d\ )$

11. for x in g do

12. if u/x is prime then return true

13. return "LIMIT REACHED".

Here we can consider the function smallfactors(a,b) as returning the set of all positive divisors of a whose size is less then b.

It is conjectured by Bourniakowsky that there are always infinitely many $n \in \mathbb{Z}$ for which $d^{-1}|f(n)|$ is prime if f is irreducible. Assuming this is true, it follows that the above algorithm would confirm the irreducibility of a polynomial in a finite amount of time if the arbitrary bound N_1 and N_2 were removed. An even stronger conjecture known as "Hypothesis H^+" which has been posed by Adleman and Odlyzko claims that the "gaps" between values at which $d^{-1}f(x)$ is prime are not too large. Confirmation of Hypothesis H^+ would lead to an irreducibility algorithm whose running time is polynomial in the time taken to run integer primality tests, which is itself polynomial time in the size of the integer.

In general, many improvements can be made to increase the effectiveness of the above procedure, such as decreasing the value of b by translating the polynomial or replacing it with its reciprocal. Theorem (7) can be very easily strengthened to show that the maximum value of v that may be divided out of $|f(b+k)|$ depends on the smallest degree of any factor of f. In particular, since

we can always find linear factors, we may assume that every factor dividing f has degree at least 2, and hence v may be chosen to be any factor dividing $|f(b+k)|$ of size less then k^2 instead of merely k.

This concludes the overview of Monagan's paper.

APPENDIX B
Programs

The following is the MAGMA code for the programs used to obtain the results in this thesis.

```
> KronWeb:= function(f);

> if not IsIrreducible(f) then       // First section just checking that function is suitable
>    print f, "is not irreducible.";
>    CycloDeg:= 0;
> elif not IsAbelian(GaloisGroup(f)) then       // This can be improved. See [10] for a
>    print f, "does not produce a Galois extension."; // method to determine abelianicity
>    CycloDeg:=0;                  // of Galois group directly that runs in polynomial time
> else

>    ExtDegree:= Degree(f);       // Initializing variables
>    DegreeDivs:= Factorization(ExtDegree);
>    DiscFactor:= Factorization(Integers()!Discriminant(f));


>    PrimeSet:={};
>    for prime in DiscFactor do
>       PrimeSet:= PrimeSet join prime[1];
>    end for;

>    m1:= 1;
>    for prime in PrimeSet do
>       m1:= m1 * prime;
>    end for;
>    if 2 in PrimeSet then
>       m1:= 2 * m1;
>    end if;

>    n1:=ExtDegree;       // Removing extraneous factors thanks to (3.1.2)
>    for x in DegreeDivs do
>       if x[1] notin PrimeSet then
>          while n1 mod x[1] eq 0 do
>             n1:= n1 div x[1];
>          end while;
>       end if;
>    end for;
```

```
>    CycloDeg:= n1 * m1;
> end if;

> return CycloDeg;       // Returns abelian extension that ℚ[x]/(f) can embed into

> end function;



> CharGroup:= function(N, f);

> PrimeFactors:= Factorization(N);       // Initializing variables
> ResidueGroup:= Integers(N);
> GalGroup, g:= UnitGroup(ResidueGroup);
> ResidueSubgroup:= sub<GalGroup | 0>;

> ImageGalGroup:=[ ];       // Constructing map between (ℤ/Nℤ)^×
> for t in GalGroup do       // and generic abelian group
>    ImageGalGroup:= Append(ImageGalGroup, <t,g(t)>);
> end for;

> y:=0;       // Finding subgroup of (ℤ/Nℤ)^× that fixes field
> while #ResidueSubgroup ne (#GalGroup div Degree(f)) do
>    y:= y +1;
>    if ImageGalGroup[y][1] notin ResidueSubgroup then       // This could be improved
>       k:= Integers()!ImageGalGroup[y][2];       // For example, the order of y must
>       while not IsPrime(k) do       // satisfy certain conditions to be in the subgroup
>          k:= k + N;
>       end while;
>       ResiduePoly:= PolynomialRing(FiniteField(k));
>       RelPrime:= GCD(ResiduePoly.1^(k-1)-1,ResiduePoly!f);
>       if RelPrime ne 1 then
>          ResidueSubgroup:= sub< GalGroup | ResidueSubgroup, ImageGalGroup[y][1]>;
>       end if;
>    end if;
> end while;

> ImageResidueSubgroup:=[ ];
> for x in ResidueSubgroup do
>    ImageResidueSubgroup:= Append(ImageResidueSubgroup, <x,g(x)>);
> end for;

> Gens:=Generators(ResidueSubgroup);
> DircGroup:= DirichletGroup(N, CyclotomicField(Degree(f)));

// This next step should NOT be necessary. When MAGMA constructs a group of Dirichlet
// characters, it is supposed to construct an isomorphic abelian group in which do to
// algebraic manipulation. However, I have found that with V2.11-13 currently on the
// McGill computers this construction can be faulty and so the following constructs the
// abelian group and the map between the two explicitly.

> T:=[ ];
> for i in Generators(DircGroup) do
>    T:= Append(T, Order(i));
```

```
> end for;
> IsoDirc:= AbelianGroup(T);
> G:={ <IsoDirc!0, DircGroup!1>};
> for i in [1..#Generators(IsoDirc)] do
>    for j in [1..Order(IsoDirc.i)-1] do
>       G:= G join {<j*IsoDirc.i, DircGroup.i^j>};
>    end for;
> end for;
> while #G ne Order(DircGroup) do
>    H:= G;
>    for elt1 in H do
>       for elt2 in H do
>          G:= G join{ <elt1[1] + elt2[1], elt1[2]*elt2[2]>};
>       end for;
>    end for;
> end while;
> psi:= map<IsoDirc -> DircGroup | G>;

> CharacterGroup:=[* *];       // Finding the subgroup of characters that act trivially on
> IsoCharacterGroup:=sub<IsoDirc| IsoDirc!0>;       // associated subgroup of (ℤ/Nℤ)^×
> for X in IsoDirc do
>    if #IsoCharacterGroup ne Degree(f) then
>       if (Degree(f) mod Order(X) eq 0) and X notin IsoCharacterGroup then
>          s:= 0;
>          for i in Gens do
>             if Evaluate(psi(X),g(i)) ne 1 then
>                s:=s+1;
>             end if;
>          end for;
>          if s eq 0 then
>             IsoCharacterGroup:= sub<IsoDirc| IsoCharacterGroup, X>;
>          end if;
>       end if;
>    end if;
> end for;

> Conductor:= 1;       // Replacing characters with their associated primitive characters
> for X in IsoCharacterGroup do       // and finding the conductor of the field
>    CharacterGroup:= Append(CharacterGroup, AssociatedPrimitiveCharacter(psi(X)));
>    Conductor:=LCM(Conductor, Modulus(AssociatedPrimitiveCharacter(psi(X))));
> end for;

> Disc:= 1;
> Complexfield:= 0;
> for X in CharacterGroup do
>    Disc := Disc * Modulus(X);
>    if X(-1) eq -1 then
>       Complexfield:= 1;
>    end if;
> end for;

> if Complexfield eq 1 then
>    Disc:= Disc * (-1)^(Degree(f) div 2);
> end if;
```

```
> if Complexfield eq 0 then
>    print “The field is totally real”;
> else
>    print “The field is not totally real”;
> end if;

> print “The discriminant is”, Disc;
> print “The field can be embedded in the”, Conductor,“th cyclotomic field.”;
> return CharacterGroup, Conductor;

> end function;



> DedekindZeta:= procedure(CharacterGroup,Conductor, k);

> ZetaValue:=1;
> BernoulliPoly:= BernoulliPolynomial(k);

> for X in CharacterGroup do
>    GenBernoulliNumber:= Conductorˆ(k-1) * (&+[Evaluate(X,a)*Evaluate(BernoulliPoly,
a/Conductor): a in [1..Conductor]]);
>    ZetaValue:= ZetaValue * (-1) * GenBernoulliNumber / k ;
> end for;

> print “The Zeta function at ”, 1-k,“ has a value of ”, ZetaValue;

> end procedure;
```

REFERENCES

[1] F. Andreatta and E.Z. Goren. Hilbert modular forms: mod p and p-adic aspects. *Memoirs of the American Mathematical Society*, 819, 2005.

[2] G.E. Andrews, R. Askey, and R. Roy. Special Functions, volume 71 of Encyclopedia of Mathematics and its Applications, 1999.

[3] E. Bach and J. Shallit. *Algorithmic number theory*. MIT Press Cambridge, MA, USA, 1996.

[4] F. Brown. Dedekind Zeta motives for totally real fields. *Arxiv preprint arXiv:0804.1654*, 2008.

[5] J.H. Bruinier. Arithmetic Hirzebruch-Zagier divisors and modular forms. In *Mathematisches Institut, Seminars*, pages 201–209. Universitätsverlag Göttingen, 2004.

[6] H. Cohen. Variations sur un theme de Siegel et Hecke. *Acta Arithmetica*, 30:63–93, 1976.

[7] H. Cohen. *A course in computational algebraic number theory*. Springer-Verlag, 1993.

[8] D.S. Dummit and R.M. Foote. *Abstract algebra*. Wiley, 1999.

[9] R.W. Farebrother. *Linear least squares computations*. CRC, 1988.

[10] P. Fernandez-Ferreiros and M. de los Angeles Gomez-Molleda. A method for deciding whether the Galois group is abelian. In *Proceedings of the 2000 international symposium on Symbolic and algebraic computation*, pages 114–120. ACM New York, NY, USA, 2000.

[11] E.Z. Goren. Lectures on Hilbert Modular Varieties and Modular Forms (2002) Providence, RI: American Mathematical Society. *CRM Monograph*

Series, 14.

[12] E.Z. Goren. Zeta values. http://www.math.mcgill.ca/goren/ZetaValues/zeta.html.

[13] E.Z. Goren. Hasse invariants for Hilbert modular varieties. *Israel Journal of Mathematics*, 122(1):157–174, 2001.

[14] K.F. Ireland and M. Rosen. *A classical introduction to modern number theory*. Springer Science & Business, 1990.

[15] G.J. Janusz. *Algebraic number fields*. American Mathematical Society, 1996.

[16] J. Johnes. Tables of number fields with prescribed ramification, June 2001. `http://hobbes.la.asu.edu/numberfields-old/`.

[17] N. Koblitz. *Introduction to elliptic curves and modular forms*. Springer, 1993.

[18] S. Lang. *Algebraic number theory*. Springer-Verlag, 1994.

[19] D.A. Marcus. *Number fields*. Springer, 1977.

[20] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of applied cryptography*. CRC, 1996.

[21] M.B. Monagan. A heuristic irreducibility test for univariate polynomials. *Journal of Symbolic Computation*, 13(1):47–57, 1992.

[22] J. Neukirch and N. Schappacher. *Algebraic number theory*. Springer, 1999.

[23] J.H. Silverman. Wieferich's criterion and the abc-conjecture. *Journal of number theory(Print)*, 30(2):226–237, 1988.

[24] G. van der Geer. *Hilbert modular surfaces*. Springer, 1988.

[25] G. van der Geer. Siegel modular forms and their applications. *The 1-2-3 of modular forms: lectures at a summer school in Nordfjordeid, Norway*, page 181, 2008.

[26] L.C. Washington. *Introduction to cyclotomic fields*. Springer Verlag, 1997.

[27] R.E. Zippel. *Effective polynomial computation*. Springer, 1993.