UNIVERSITY OF CALIFORNIA, SAN DIEGO

Higher Order Integral Stark-Type Conjectures

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Caleb J. Emmons

Committee in charge:

Professor Cristian Popescu, Chair
Professor Benjamin Grinstein
Professor Rafael Núñez
Professor Harold Stark
Professor Audrey Terras

2006

The dissertation of Caleb J. Emmons is approved, and it is acceptable in quality and form for publication on microfilm:

Chair

University of California, San Diego

2006

To my parents, and my brother.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

First and foremost I would like to thank my advisor, Cristian Popescu. Our weekly conversations were invaluable, and you always seemed to know an improbable amount of mathematics, including the right way to think about algebra. You also knew just when to give me a little push. The only thing you denied me was the pleasure some people seem to take in complaining about their advisors.

Thanks are in order for Harold Stark, without whom there would be no Stark conjectures, for the inspiration, the classes, the concrete examples, and for teaching me about p, $\mathfrak{p}$, $\mathfrak{P}$, $\wp$; and to Audrey Terras, for the classes with colored chalk, the discussions, the enthusiasm and the advice.

For a constant diet of nonsense I am thankful for my friends Tony, Tom, and Yummy Maki Yummy Box. I am also in debt to Stefan Erickson for the good ideas and for being an excellent conference companion. Thank you Colleen for righting my course—truly this document would not exist without you. Also a shout-out to Brynna, who insisted that I thank her, and also was unfailing in her excitement about my thesis topic, or at least adamant that I be excited about it.

To my family for being proud of me—from "Read book!" through "Read dissertation?" you have always given me the best help, advice, and love—thanks!

For love, support and a vision of the future beyond graduate school, thank you Jenny. You make me happy!

Finally, I would like to thank my high school mathematics teacher and mentor Annie Cavagnaro for truly getting me started in math, sharing your sense of wonder and throwing some awesome GEEK parties.

VITA

1978	Born, Santa Barbara, California
2000	B. S., Mathematics, University of California, Davis
2000–2006	Teaching assistant, University of California, San Diego
2002	M. A., Mathematics, University of California, San Diego
2004	C. Phil., Mathematics, University of California, San Diego
Fall 2004	Associate Instructor, University of California, San Diego
2006	Ph. D., Mathematics, University of California, San Diego

ABSTRACT OF THE DISSERTATION

Higher Order Integral Stark-Type Conjectures

by

Caleb J. Emmons

Doctor of Philosophy in Mathematics

University of California San Diego, 2006

Professor Cristian Popescu, Chair

The Stark conjectures attempt to capture the leading terms at $s = 0$ of the S-incomplete Artin L-functions attached to an abelian extension of number fields as the image under a regulator map of an evaluator built out of S-units. We introduce a new conjecture of Popescu, which extends Rubin's higher order of vanishing Stark-type conjecture by removing the hypothesis that S contains splitting primes.

We prove that the evaluator attached to an extension K/k can be written as a linear combination of evaluators arising in subextensions which do have splitting primes, linking the original conjecture of Rubin with its extension. This allows a cohomological proof of the extended conjecture when the original is known for the subextensions and S has "enough" finite unramifying primes. We study extensions of exponent 2 where we prove Rubin's conjecture under the hypothesis that an auxiliary smoothing set T is sufficiently large, and achieve new partial results towards the conjecture in general for these extensions. The consequences of a

Stark-type conjecture of Burns are studied, leading to weaker sufficient inequalities for extensions of prime exponent.

In the appendix, we prove a series of equivalences for when a cyclic Kummer extension of K is central extension over k, which is an analogue of Coates' condition for achieving an abelian extension.

Chapter 1

Introduction and history

1.1 Introduction for non-number theorists

To begin, we work through a very specific example to introduce the reader to the flavor of all the objects we will be concerned with in the remainder of the dissertation. Although I may use technical language occasionally, even the non-mathematical reader should be able to get an idea of the material. The most basic objects in number theory are probably the ring[1] of integers

$$\mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, 4, ...\}$$

and the field[2] of rational numbers (fractions)

$$\mathbb{Q} = \left\{ \frac{c}{d} \;\middle|\; c, d \in \mathbb{Z}, d \neq 0 \right\}.$$

Number theory studies not only these objects (e.g. factoring integers into

[1] A *ring* is basically a set of objects together with operations +, - and ×.
[2] A *field* is basically a set of objects together with operations +, -, × and ÷.

primes), but also asks what happens when we add in elements which were not there before. For example, one can learn a lot of number theory and geometry by studying the Gaussian integers

$$\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$$

i.e., the ring we get by adding the new number "$\sqrt{-1}$" to $\mathbb{Z}$.

One beautiful aspect of Stark-type conjectures is that they can use magical-looking sums to learn about arithmetic in certain rings. For example we will see that the sums

$$\frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15} + \frac{1}{17} - \ldots = \frac{\pi}{4}, \tag{1.1}$$

$$\frac{1}{1} - \frac{1}{5} - \frac{1}{7} + \frac{1}{11} + \frac{1}{13} - \frac{1}{17} - \frac{1}{19} + \frac{1}{23} + \frac{1}{25} - \ldots = \frac{\ln(2+\sqrt{3})}{\sqrt{3}}, \tag{1.2}$$

and

$$\frac{1}{1} + \frac{1}{3} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} - \frac{1}{13} - \frac{1}{17} - \frac{1}{19} + \frac{1}{21} + \ldots = \frac{\pi}{\sqrt{5}} \tag{1.3}$$

can actually give us information about factorization in $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{3}]$ and $\mathbb{Z}[\sqrt{-5}]$, respectively.

Let d be a squarefree[3] integer, such that 4 divides $(d-3)$. Consider the field we get by adding $\sqrt{d}$ to $\mathbb{Q}$:

$$\mathbb{Q}(\sqrt{d}) = \{\alpha + \beta\sqrt{d} \mid \alpha, \beta \in \mathbb{Q}\}.$$

[3]Squarefree means that d is not divisible by n^2 for any $n > 1$. For such a number it is not hard to see that $\sqrt{d}$ is not in $\mathbb{Q}$.

The ring of integers of this field is

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

It is natural to investigate the ways in which this new ring $\mathbb{Z}[\sqrt{d}]$ is like or unlike $\mathbb{Z}$.

To start with, $\mathbb{Z}[\sqrt{d}]$ may or may not have unique factorization. For example, in $\mathbb{Z}[\sqrt{-5}]$ we have the following factorizations of 6:

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{1.4}$$

Yet within the ring, 2 does not divide either of the numbers on the right hand side. Thus "factorization into prime numbers" fails.[4] In order to recover unique factorization, the notion of an *ideal* was introduced. An ideal $\mathfrak{A} \subseteq \mathbb{Z}[\sqrt{d}]$ is any subset that is closed under internal addition ($a+b \in \mathfrak{A}$ for all $a, b \in \mathfrak{A}$) and external multiplication ($r \cdot a \in \mathfrak{A}$ for all $r \in \mathbb{Z}[\sqrt{d}]$, $a \in \mathfrak{A}$). We call an ideal *principal* if $\mathfrak{A} = (\alpha)\mathbb{Z}[\sqrt{d}]$ is generated by one element. We call two ideals $\mathfrak{A}$ and $\mathfrak{B}$ *pricipally equivalent* if there exist γ and δ in $\mathbb{Z}[\sqrt{d}]$ such that $(\gamma)\mathfrak{A} = (\delta)\mathfrak{B}$. We then look at the class group

$$Cl_d = \{\text{ideals of } \mathbb{Z}[\sqrt{d}]\}/(\text{principal equivalence})$$

and define the class number h_d to be the cardinality of the class group. We have the following theorem:

$$\mathbb{Z}[\sqrt{d}] \text{ has unique factorization} \quad \Longleftrightarrow \quad h_d = 1. \tag{1.5}$$

[4]The mistaken assumption that certain number rings had the property of unique factorization led to incorrect "proofs" of Fermat's Last Theorem in the 1800s; FLT was finally settled during the 1990s.

Another way in which $\mathbb{Z}[\sqrt{d}]$ may differ from $\mathbb{Z}$ is that it may have infinitely many units. The units (i.e. invertible elements) of $\mathbb{Z}$ are simply ± 1. However, in $\mathbb{Z}[\sqrt{3}]$ for example, we have the equation

$$(2+\sqrt{3})(2-\sqrt{3}) = 1, \tag{1.6}$$

and thus $\varepsilon_3 = 2+\sqrt{3}$ is a unit of $\mathbb{Z}[\sqrt{3}]$. (And of course, if we square, cube, etc. both sides of equation (1.6), we learn that any power of ε_3 is also a unit.)

Let $U_d = \mathbb{Z}[\sqrt{d}]^\times$ be the group of units. The Dirichlet Unit Theorem in this situation (again $4|(d-3)$) says

$$U_d = \begin{cases} \{\pm 1\} & \text{if } d < -1 \\ \{\pm 1, \pm\sqrt{-1}\} & \text{if } d = -1 \\ \{\pm 1\} \times \langle \varepsilon_d \rangle & \text{if } d > 0, \end{cases}$$

where ε_d is called the *fundamental unit* for $\mathbb{Q}(\sqrt{d})$ and is a generator of an infinite cyclic group.

Our goal was to study the arithmetic of $\mathbb{Z}[\sqrt{d}]$ via infinite sums. To this end, define a function $\chi_d : \mathbb{Z} \to \{0, \pm 1\}$ in the following manner. Let $\chi_d(1) = 1$. If p is a prime number, put

$$\chi_d(p) = \begin{cases} 0 & \text{if } p \mid 4d \\ 1 & \text{if } p \nmid 4d, p|(x^2-4d) \text{ for some } x \in \mathbb{Z} \\ -1 & \text{otherwise.} \end{cases}$$

Then extend χ_d multiplicatively:

$$\chi_d(mn) = \chi_d(m) \cdot \chi_d(n).$$

(Later we will recognize χ_d as the unique nontrivial Dirichlet character associated to our abelian field extension.)

We define an L-function via

$$\begin{aligned} L(s, \chi_d) &= \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s} \\ &= \frac{\chi_d(1)}{1^s} + \frac{\chi_d(2)}{2^s} + \frac{\chi_d(3)}{3^s} + \frac{\chi_d(4)}{4^s} + \frac{\chi_d(5)}{5^s} + \dots, \end{aligned}$$

where s is a complex variable. This series initially converges absolutely and uniformly on compact subsets of $\Re e(s) > 1$, but it may be analytically continued to the whole complex plane. Moreover, these sums even converge at $s = 1$.

At this point the enterprising reader can return to the sums (1.1), (1.2), and (1.3) and work out that these are equal to $L(1, \chi_{-1})$, $L(1, \chi_3)$ and $L(1, \chi_{-5})$ respectively.

Now we state an amazing theorem which links the value of these L-functions at $s = 1$ to the class number and the group of units. (This theorem arises from writing the L-functions as a ratio of *zeta functions*. We will pursue this approach extensively and in much greater generality in Chapter 4.)

Theorem 1.1.1. *If d is an integer, $4|(d-3)$, and χ_d is as above, then*

$$L(1, \chi_d) = \begin{cases} \frac{\pi}{\sqrt{4|d|}} h_d & \text{if } d < -1 \\ \frac{\pi}{4} h_{-1} & \text{if } d = -1 \\ \frac{\ln(\varepsilon_d)}{\sqrt{d}} h_d & \text{if } d > 0. \end{cases}$$

At this point, if we focus on $d = -5$, we can write a computer program that sums for example the first one-hundred-thousand[5] terms of series (1.3), and outputs

[5] One can get bounds on how many terms are needed, *etc.* We are not attempting to focus on this aspect. Here one-hundred-thousand terms is easily sufficient.

the value

$$\texttt{approx} = 1.4049429462081752786309227\,28$$

and compare this to

$$\texttt{Pi/sqrt(20)} = 0.70248147310407263931563746\,43$$

According to Theorem 1.1.1, the ratio of these two numbers must be the class number. That is

$$h_{-5} = 2.$$

And we could conclude via (1.5) that $\mathbb{Z}[\sqrt{-5}]$ does *not* have unique factorization. Notice that we could conclude this entirely numerically, without recourse to actually finding an instance of non-unique factorization such as equation (1.4).

Similarly, if we sum the first terms of the series (1.1) it quickly converges to $\pi/4$ and we learn that $h_{-1} = 1$, i.e. that the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ *do* have unique factorization.

Exercise: Given the value of the sum (1.2) and that $\varepsilon_3 = 2 + \sqrt{3}$, use Theorem 1.1.1 to determine h_3, and hence by (1.5) whether $\mathbb{Z}[\sqrt{3}]$ has unique factorization.

This long example has illustrated the connections between values of certain L-functions at $s = 1$ and quantities arising from the unit group and the class group of the associated field. This is the concern of the Stark conjectures. In the next section and those following, we shall generalize these ideas in the following ways: by replacing the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ with an arbitrary finite abelian extension of number fields K/k, by moving our point of interest[6] (via the functional equation) from $s = 1$ to $s = 0$, and by introducing auxiliary sets of primes S and T.

1.2 A brief history of Stark-type conjectures

Leonhard Euler (1707-1783) was among the first to systematically study values of analytically defined objects. In particular, he investigated what is now called the *Riemann zeta function*:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

and deduced its product formula

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

For this reason, the factors in the product are called *Euler factors*.

About a century later, Johann Lejeune Dirichlet (1805-1859) introduced a periodic function (a *Dirichlet character*) into the numerator of the zeta function and called the result an L-function. We have already seen examples of these in the previous section and learned that their special values are quite useful for learning about arithmetic.[7]

These days, L-functions are attached not to periodic functions of the natural numbers, but rather to characters of a Galois group, a view which encompasses

[6]This move will require us to examine derivatives of the L-functions, but this is not a fundamental change, as we are really interested merely in capturing the leading coefficient in the power series expansion about the specified point.

[7]Dirichlet's foremost use of L-functions was to prove his theorem on primes in progression: for any relatively prime natural numbers a and b, the set $\{ax + b \mid x \text{ a natural number}\}$ contains infinitely many prime numbers.

the earlier definition by recognizing $(\mathbb{Z}/n\mathbb{Z})^\times$ as the Galois group of the cyclotomic field of n^{th} roots of unity over $\mathbb{Q}$.

The importance of L-functions is that they provide a character-by-character factorization of the *Dedekind zeta function.* Named after Richard Dedekind (1831-1916), this function is attached to a number field K, and can be given by the Euler product

$$\zeta_K(s) = \prod_{\mathfrak{p} \text{ a prime of } K} \frac{1}{1 - N\mathfrak{P}^{-s}}.$$

(See Section 2.2 for the notations.) If $K = \mathbb{Q}$ we recover Riemann zeta.

We have

$$\zeta_K(s) = \prod_{\chi} L(s, \chi), \tag{1.7}$$

where the product runs over all the characters attached to the Galois group of $K/\mathbb{Q}$. We shall reëncounter this formula in greater generality.

These zeta and L-functions have functional equations relating their values at s and $1 - s$. In the previous section we studied values at $s = 1$. However, it turns out one obtains simpler formulae if one turns attention to $s = 0$. By the functional equation, these are equivalent.

Expanding $\zeta_K(s)$ in a power series at $s = 0$ gives the analytic class number formula

$$\zeta_K(s) = \frac{-h_K R_K}{w_K} s^d + O(s^{d+1}). \tag{1.8}$$

The leading term of the zeta function encodes the class number (h_K), the number of roots of unity in K (w_K) and a regulator (R_K) arising from the unit group of K. Also appearing is d, the $\mathbb{Z}$-rank of the unit group.

Harold Stark was perhaps the first to suspect that a natural rational factorization of the regulator occurred in terms of the unit group. In a series of papers in the 1970s and early 1980s Stark promulgated the Stark conjectures. These provide a framework to investigate the natural question of how the leading term of $\zeta_K(s)$ factors into the leading terms of the L-functions at $s = 0$. Write the power series of each L-function at $s = 0$ as

$$L(s, \chi) = c(\chi) s^{r(\chi)} + O(s^{r(\chi)+1}).$$

By combining equations (1.7) and (1.8) we know

$$d = \sum_{\chi} r(\chi) \tag{1.9}$$

and

$$\frac{-h_K R_K}{w_K} = \prod_{\chi} c(\chi). \tag{1.10}$$

One main question is whether we can realize each $c(\chi)$ as arising from a χ-piece of R_K times some rational number.

Furthermore, if this question is answered in the affirmative, what then can we say about the rational number? In a certain very specific case, Stark gave an *integral* conjecture which bounds the denominators of these numbers. This conjecture allows one to construct so-called *Stark units* out of the values of the first derivatives of the L-functions at $s = 0$. These Stark units are very useful and mysterious objects in number theory. In some cases taking roots of Stark units leads to a solution of Hilbert's 12th Problem—explicit class field theory via special functions. Hilbert had in mind the well known theory of exponentional function $\exp(x)$ over $\mathbb{Q}$ and the j-function coming from the theory of complex multiplication over imaginary quadratic fields. Stark suggests that at times we may use character combinations of $\exp(L'(s,\chi))$ as our special function.

Let us place ourselves in the setting of Stark's orginal integral conjecture. For the precise definitions of all the terms to follow, consult the following chapter. Let K/k be an abelian extension of number fields, with Galois group G. Let $\widehat{G}$ denote the dual group of G. We introduce a finite set of primes S of the base field k, which contains all of the infinite and ramifying primes. For the purposes of this discussion we shall assume the cardinality of S is at least 3. This set S modifies the L-functions, class groups, and unit groups as described later. We let w_K denote the number of roots of unity in K.

CONJECTURE (The First Order Abelian Stark Conjecture):
Suppose further that S contains at least one prime v_0 which splits completely in K/k. Fix a prime w_0 of K which divides v_0. Then Stark predicts that there is a unique element $\varepsilon \in K$ with the following properties:
(i) (ε evaluates derivatives of the L-functions) for each χ in $\widehat{G}$,

$$L'_S(0,\chi) = \frac{-1}{w_K} \sum_{\sigma \in G} \chi(\sigma) \log |\varepsilon^\sigma|_{w_0},$$

(ii) (ε is an S-unit)

$$|\varepsilon|_w = 1 \text{ for all } w \text{ not lying above a prime in } S,$$

and
(iii) (abelian condition) the extension

$$K(\varepsilon^{1/w_K})/k$$

is abelian.

Stark proved this conjecture in [Sta80] under the assumption that $k = \mathbb{Q}$ or $k = \mathbb{Q}(\sqrt{-d})$ (i.e. the two cases in which the solution to Hilbert's 12th Problem is already known.) The next major contribution to the subject was the publication of John Tate's book *Les conjectures de Stark sur les fonctions L d'Artin en s=0* [Tat84], in which a representation-theoretic approach to the conjectures was highlighted.

The splitting prime v_0 forces the nontrivial L-functions to vanish with order at least one. In some cases the first derivative of the L-function captures the leading term of its power series expansion at $s = 0$, but at other times is does not. It is a natural question, therefore, to ask for a similar integral-type conjecture in the cases of higher order of vanishing. Karl Rubin made such a conjecture when he published [Rub96] in 1996. Rubin supposes that S contains $r \geq 1$ primes which split completely in K/k and then predicts that the r^{th} derivatives of the L-functions are captured under a regulator of an element in a sublattice of the r^{th} exterior power (over $\mathbb{Z}[G]$) of the $(S, T)-$modified unit group $U_{K,S,T}$. (See chapter 3). We shall call this the standard (Rubin) conjecture and denote it by $B(K/k, S, T, r)$. There is extensive support for Rubin's conjecture. Consult [Pop04].

Rubin's conjecture uses an auxiliary *smoothing* set of primes T. (Such a set was first introduced by Gross [Gro88].) By varying T one recaptures the condition (iii) of Stark's original integral conjecture. The connection is made via a theorem we describe in Appendix A. It is condition (iii) that at times implies a solution to Hilbert's 12th problem via Stark units. Stark originally formulated this condition merely by asking that $K(\varepsilon^{1/w_K})/K/k$ be a central extension. For a discussion and a proof of what is required to achieve a central extension, also see Appendix A.

Yet there remains the question of integrality when some of the vanishing at $s = 0$ is produced by non-split primes. Discussions between David Dummit and Stark led Stark to formulate *The Extended First Order Abelian Stark Question* in 2001. This question predicted a formula similar to, but more complicated than, (i) in cases when there was not necessarily a split prime in S but all L-functions vanished with order at least one at $s = 0$. Stefan Erickson investigated and proved certain cases of this question in his dissertation [Eri05].

The next step was to create a conjecture which merged the Extended First Order Question with Rubin's higher order integral conjecture. Cristian Popescu put forward a suggestion in 2003 (a forthcoming article by Popescu introducing this new conjecture is slated to be submitted for publication this year [Pop06]). This *extended* conjecture is outlined in Chapter 3, where we denote it by $\widetilde{B}(K/k, S, T)$. (There are a slight variants to B and $\widetilde{B}$ also introduced and referred to as conjectures C and $\widetilde{C}$.)

We shall examine this extended conjecture in detail. Our main goals will be to (1) examine its functoriality under change of fields, and sets S and T, (2) prove that the extended conjecture follows from knowing the standard conjecture under certain circumstances (and vice versa that the standard follows from the extended) and (3) prove the extended conjecture outright when possible.

Chapter 2

The objects of study

In this chapter, we carefully define all notations and objects we will be studying throughout this dissertation. The reader who is already familiar with the higher order integral Stark conjecture of Rubin may wish to skim Sections 2.3 and 2.7 before proceeding directly to Chapter 3. Many results of this chapter are of a technical nature and may be skipped upon a first reading and referred back to as necessary.

2.1 Basic notations

For a finite set $\mathcal{S}$, $|\mathcal{S}|$ or occasionally $\#\mathcal{S}$ will denote the cardinality of $\mathcal{S}$. For any rational number q and prime l we factor $q = l^m \cdot t$ with t relatively prime to l and set $\mathrm{ord}_l(q) = m$.

If A is a group and l is a prime number, $\mathrm{rk}_l(A)$ is defined to be $\mathrm{ord}_l|A/A^l|$, if this number is finite. Of course infinite groups can and often do have finite l-ranks (for example if they are abelian and finitely generated). It is also important to recognize that if A is a finite group, $\mathrm{ord}_l|A|$ is always at least $\mathrm{rk}_l(A)$, and may be strictly greater. For example, $\mathrm{ord}_2|\mathbb{Z}/32\mathbb{Z}| = 5$ while $\mathrm{rk}_2(\mathbb{Z}/32\mathbb{Z}) = 1$.

If H is a subgroup of A, then $(A : H)$ denotes the index of H in A. If M/k is an extension of fields, $[M : k]$ is the dimension of M as a k-vector space.

If G is another group, and A has a G-action, i.e., A is a module over the ring $\mathbb{Z}[G]$, then for $a \in A$ and $\lambda \in \mathbb{Z}[G]$ we shall write the action as either $\lambda \cdot a$ or a^{λ}, primarily depending on whether we were originally considering A as an additive or multiplicative group. (At times we even mix the two notations.) For any ring $D \subseteq \mathbb{C}$ we abbreviate $DA := D \otimes_{\mathbb{Z}} A$. (Almost always $D = \mathbb{Q}$ or $D = \mathbb{C}$.) The notation $\widehat{\mathrm{H}}^i(G, A)$ denotes the i^{th} Tate cohomology group of G with coefficients in A (c.f. [Cas67]).

2.2 Field extensions and factorization of primes

Throughout this dissertation, we will usually take K/k to be a finite abelian Galois extension of number fields. A *number field* is a finite extension of the rational numbers $\mathbb{Q}$. To say K/k is *Galois* means that $\mathrm{Aut}_k(K)$, the set of automorphisms of K which fix k, has cardinality equal to $[K : k]$. We call $G(K/k) := \mathrm{Aut}_k(K)$ the *Galois group*, and when K/k is fixed often use simply the letter G to denote it.

A number field k has a canonical ring associated to it, called the *ring of integers* of k, and denoted $\mathcal{O}_k$. This ring is defined to be the collection of elements of k which are the root of some monic polynomial with coefficients in $\mathbb{Z}$. As was pointed out in the introduction, studying the arithmetic of $\mathcal{O}_k$ is one of the main goals of number theory.

Primes, or *places*, of a number field k come in two flavors. The first type, called *finite* or *non-Archimedean* primes, can be identified simply with non-zero prime ideals of the ring of integers $\mathcal{O}_k$. The second type of prime is called *infinite* or *Archimedean*. An infinite prime v corresponds to an embedding $\iota_v : k \hookrightarrow \mathbb{C}$. If $\iota_v(k) \subseteq \mathbb{R}$ we say v is a *real place*; otherwise v is a *complex place*. Primes in general are denoted by the letters v or w. Finite primes shall occasionally be denoted with the letters $\mathfrak{p}$, $\mathfrak{P}$, p, $\mathfrak{q}$, *etc.*

A more holistic view is possible; we could take a prime (infinte or finite) to be defined as an equivalence class of absolute values on k. In particular, if v is a prime of k, then the completion, k_v, is $\mathbb{C}$, $\mathbb{R}$, or a finite extension of the p-adic numbers $\mathbb{Q}_p$, depending on whether v is a complex place, a real place, or a place of finite residue characteristic p, respectively. The normalized absolute value corresponding to a finite place $\mathfrak{p}$ of k is

$$|\alpha|_{\mathfrak{p}} = (N\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)},$$

where $N\mathfrak{p} = |\mathcal{O}_k/\mathfrak{p}|$ is the cardinality of the residue field, and $\mathrm{ord}_{\mathfrak{p}}$ is the natural extension to ideals of the ord function from the previous section. When v is a real infinite place, $|\alpha|_v$ is the usual $\mathbb{R}$-absolute value of the corresponding v-embedding of α. If v is complex, then $|\alpha|_v = |\iota_v(\alpha)|^2$ is the square of the usual $\mathbb{C}$-absolute value of the v-embedding of α.

We are concerned with the behavior of primes in extensions K/k. If $\mathfrak{p}$ is a finite prime of k, then $\mathfrak{p}\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ which we may factor

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_g^{e_g}$$

into primes of K. We say that $\mathfrak{P}_i$ divides $\mathfrak{p}$, and write $\mathfrak{P}_i|\mathfrak{p}$. Furthermore we have the *inertial degree*, which is the natural number $f_i = f_{\mathfrak{P}_i|\mathfrak{p}}$ such that

$$N_{K/k}\mathfrak{P}_i = \mathfrak{p}^{f_i},$$

where $N_{K/k}$ denotes the norm map. It is not too difficult to show that

$$e_1 f_1 + e_2 f_2 + \dots + e_g f_g = [K : k]. \tag{2.1}$$

If v is an infinite prime of k and w is an infinite prime of K, then we say w divides v if

$$\iota_w|_k = \iota_v.$$

As above we write $w|v$. If w is complex and v is real, then we say v has *complexified* in K. For a discussion of whether this corresponds to ramification, see Section 2.6.

When K/k is Galois, $e_1 = e_2 = \dots = e_g$, and we shall denote this quantity by $e = e_{\mathfrak{p}}(K/k)$ and call it the *ramification index* of $\mathfrak{p}$ in K/k, and $f_1 = f_2 = \dots = f_g$ which we shall denote by $f = f_{\mathfrak{p}}(K/k)$ (and call it the inertial degree). Formula (2.1) reduces to $efg = |G|$. If $g = |G|$, we say $\mathfrak{p}$ *splits completely in* K/k and call $\mathfrak{p}$ a *splitting prime*. When $e > 1$ we say that $\mathfrak{p}$ *ramifies* in K/k. Only finitely many primes (namely those dividing the discriminant ideal $\mathfrak{d}_{K/k}$) ramify in any finite extension K/k.

Suppose from now on that K/k is Galois, with Galois group G. Let $\mathfrak{p}$ be a finite prime of k, and $\mathfrak{P}$ a prime of K dividing $\mathfrak{p}$. The group G acts transitively on the set of primes dividing $\mathfrak{p}$. We define the *decomposition group* of $\mathfrak{P}$ to be the stabilizer of $\mathfrak{P}$ under this action:

$$G_{\mathfrak{P}} = \{\sigma \in G \mid \mathfrak{P}^\sigma = \mathfrak{P}\}.$$

Because G acts transitively, the decompostion group has cardinality ef.

We may consider the residue fields $\mathbb{F}_q = \mathcal{O}_k/\mathfrak{p}$ and $\mathbb{F}_{q^f} = \mathcal{O}_K/\mathfrak{P}$. These are finite fields of order $N\mathfrak{p} = q$ and $N\mathfrak{P} = q^f$, respectively. Each $\sigma \in G_{\mathfrak{P}}$ induces an automorphism on $\mathcal{O}_K/\mathfrak{P}$ via $\alpha + \mathfrak{P} \mapsto \alpha^\sigma + \mathfrak{P}$. Such an induced automorphism fixes $\mathcal{O}_k/\mathfrak{p}$ (considered in the natural way as a subfield of $\mathcal{O}_K/\mathfrak{P}$). One discovers that all such automorphisms are achieved, and we get an exact sequence:

$$0 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \xrightarrow{\varphi} G(\mathbb{F}_{q^f}/\mathbb{F}_q) \longrightarrow 0. \tag{2.2}$$

The kernel $I_{\mathfrak{P}}$ is called the *inertial group*. The final Galois group $G(\mathbb{F}_{q^f}/\mathbb{F}_q)$ in the exact sequence (2.2) is cyclic of order f with a canonical generator, called the Frobenius, $F : a \mapsto a^q$. It follows that the cardinality of $I_{\mathfrak{P}}$ is e.

Hence when $\mathfrak{p}$ is unramified, $I_{\mathfrak{P}}$ is trivial and φ in (2.2) is an isomorphism. Therefore we may pull back

$$\sigma_{\mathfrak{P}} = \varphi^{-1}(F)$$

to arrive at the Frobenius automorphism $\sigma_{\mathfrak{P}}$, which generates the decomposition group. Equivalently, the Frobenius automorphism is the automorphism $\sigma_{\mathfrak{P}}$ such that

$$x^{\sigma_{\mathfrak{P}}} \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}}$$

for all $x \in \mathcal{O}_K$. When specifying the fields is necessary we shall either use the notation $\sigma_{\mathfrak{P}}(K/k)$ or $\left(\frac{K/k}{\mathfrak{P}}\right)$.

The next lemma lists the functoriality properties of Frobenius automorphisms under change of field and change of top prime.

Lemma 2.2.1. *(i) If τ is any automorphism in G, $\left(\frac{K/k}{\mathfrak{P}^\tau}\right) = \tau^{-1}\left(\frac{K/k}{\mathfrak{P}}\right)\tau$.*
(ii) If M is a field intermediate to K and k, with prime $\wp$ lying below $\mathfrak{P}$ then $\left(\frac{M/k}{\wp}\right) = \left(\frac{K/k}{\mathfrak{P}}\right)\Big|_M$ and $\left(\frac{K/M}{\mathfrak{P}}\right) = \left(\frac{K/k}{\mathfrak{P}}\right)^{f_{\wp|\mathfrak{p}}}$.

As a corollary of Lemma 2.2.1*(i)*, if G is abelian, then the Frobenius depends not on $\mathfrak{P}$ but merely on $\mathfrak{p}$. Hence in this situation (which is the situation in the sequel), we write $\sigma_\mathfrak{p}$ instead of $\sigma_\mathfrak{P}$. Note that $\mathfrak{p}$ splits completely in K/k if and only if $\mathfrak{p}$ is unramified and $\sigma_\mathfrak{p} = 1$.

The unit group of k consists of the invertible elements in $\mathcal{O}_k$, $U_k = \mathcal{O}_k^\times$. If S is a finite set of places of k, we let $\mathcal{O}_{k,S}$ denote the ring $\mathcal{O}_k$ localized at S, and the S-unit group be $U_{k,S} = \mathcal{O}_{k,S}^\times$.

2.3 Group rings, r-coverings, and regulators

If G is a finite abelian group, all representations of G are 1-dimensional (equal to their characters). The set of characters of G forms a group under multiplication

$$\widehat{G} = \{\chi : G \longrightarrow \mathbb{C}^\times \mid \chi \text{ is a group homomorphism}\}.$$

The *trivial character* is the character that takes every group element to $1 \in \mathbb{C}^\times$; we denote the trivial character by $\mathbf{1}_G$.

We may form the group rings $\mathbb{Z}[G]$ and $\mathbb{C}[G]$. By standard representation theory, the second ring decomposes

$$\mathbb{C}[G] = \bigoplus_{\chi \in \widehat{G}} \mathbb{C}\mathbf{e}_\chi, \tag{2.3}$$

where

$$\mathbf{e}_\chi := \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma.$$

Lemma 2.3.1. *The $\mathbf{e}_\chi$'s have the following properties:*

(i) They are idempotents: $\mathbf{e}_\chi^2 = \mathbf{e}_\chi$.

(ii) They are orthogonal: if $\chi \neq \psi$, $\mathbf{e}_\chi \mathbf{e}_\psi = 0$.

(iii) They act as χ-evaluators: if $\sigma \in G$, $\sigma \cdot \mathbf{e}_\chi = \chi(\sigma)\mathbf{e}_\chi$.

This lemma proves the decomposition of $\mathbb{C}[G]$. Moreover, it follows that if $\mathcal{M}$ is any $\mathbb{C}[G]$-module, then $\mathcal{M}$ also decomposes as a $\mathbb{C}[G]$-module into χ-components:

$$\mathcal{M} = \bigoplus_{\chi \in \widehat{G}} (\mathbf{e}_\chi \mathcal{M}).$$

On the component $(\mathbf{e}_\chi \mathcal{M})$, each $\sigma \in G$ acts simply as multiplication by $\chi(\sigma)$.

Definition 2.3.2. *Let $\mathcal{S}$ be a set of primes of k and $\chi \in \widehat{G}$, χ not the trivial character. We put*

$$r_{\mathcal{S}}(\chi) := \#\{v \in \mathcal{S} : \chi|_{G_v} = \mathbf{1}_{G_v}\}.$$

For the trivial character, $\mathbf{1}_G$, we set

$$r_{\mathcal{S}}(\mathbf{1}_G) := |\mathcal{S}| - 1.$$

If G is the Galois group of K/k, we call

$$r_{\mathcal{S}}(K/k) := \min_{\chi \in \widehat{G}} r_{\mathcal{S}}(\chi)$$

the minimal order of vanishing for $\mathcal{S}$ with respect to K/k.

Finally, for any integer j we define $(\widehat{G})_{j,\mathcal{S}} = \{\chi \in \widehat{G} : r_{\mathcal{S}}(\chi) = j\}$.

Remarks:

(1) If $\chi \in \widehat{G}$ is not the trivial character, there are exactly $r_{\mathcal{S}}(\chi)$ primes in $\mathcal{S}$ which split completely in the extension $K^{\ker \chi}/k$. Indeed a prime v splits completely in any subextension M of K containing k if and only if $G_v \subseteq G(K/M)$.

(2) The reason for the terminology 'minimal order of vanishing' is that if $\mathcal{S}$ contains all the infinite and ramified primes, then $r_{\mathcal{S}}(\chi)$ is nothing more than the order of vanishing at $s = 0$ of the $\mathcal{S}$-incomplete L-function $L_{\mathcal{S}}(s, \chi)$. See [Tat84, Proposition 3.4] for details.

Definition 2.3.3. *If $\mathcal{G}$ is any subset of $\widehat{G}$, we say that a set $\mathcal{S}$ is an r-*cover *for $\mathcal{G}$ if $r_{\mathcal{S}}(\chi) \geq r$ for all $\chi \in \mathcal{G}$.*

Lemma 2.3.4. *If $S_1, S_2 \subseteq S$ are r-covers for $(\widehat{G})_{r,S}$, then $S_1 \cap S_2$ is as well.*

Proof. Suppose S_1 and S_2 are r-covers for $(\widehat{G})_{r,S}$. Take $\chi \in (\widehat{G})_{r,S}$, χ not the trivial character. Then there must be exactly r distinct primes $v_1, ..., v_r$ in S with the property that $\chi|_{G_v} = \mathbf{1}_{G_v}$. These primes must be in S_1 and S_2 by the definition of r-cover. Hence they are in $S_1 \cap S_2$. Therefore $r_{S_1 \cap S_2}(\chi) = r$.

On the other hand, if $\chi \in (\widehat{G})_{r,S}$ *is* the trivial character, then it follows that $|S| = r+1$. In this situation, for S_1 and S_2 to be r-covers for $(\widehat{G})_{r,S}$ they also must contain at least $r+1$ primes, so must in fact be S. □

Corollary 2.3.5. *Let $r = r_S(K/k)$. The set*

$$S_{\min} = \bigcap S',$$

where the intersection is over all $S' \subseteq S$ that are r-covers for $(\widehat{G})_{r,S}$, is the minimal r-cover for $(\widehat{G})_{r,S}$.

Definition 2.3.6. *Let S be a set of places of k, and K a finite extension of k. Define*

$$S_K = \{w \mid w \text{ is a prime of } K \text{ which divides } v \text{ for some } v \in S\}.$$

Let Y_S be the free abelian group on S_K. There is a natural homomorphism, called the augmentation map,

$$Y_S \xrightarrow{aug} \mathbb{Z} \longrightarrow 0$$

sending an element $\sum_{w \in S_K} n_w \cdot w$ to $\sum_{w \in S_K} n_w$. We define X_S to be the kernel of aug.

We define, for any $\mathbb{Q}[G]$-module $\mathcal{M}$,

$$(\mathcal{M})_{r,S} = \{m \in \mathcal{M} : \mathbf{e}_\chi \cdot m = 0 \text{ in } \mathbb{C}\mathcal{M} \text{ for all } \chi \in \widehat{G} \text{ such that } r(\chi) \neq r\}.$$

(Often we will extend scalars of any $\mathbb{Z}[G]$-modules to at least $\mathbb{Q}[G]$.) We consider $(\cdot)_{r,S}$ as a functor from the category of $\mathbb{Q}[G]$-modules to itself. If we have a $\mathbb{Q}[G]$-module homomorphism $\mathcal{M}_1 \xrightarrow{\phi} \mathcal{M}_2$, then we put $(\phi)_{r,S} := \phi|_{(\mathcal{M}_1)_{r,S}}$. Note that this is well-defined; if $m \in (\mathcal{M}_1)_{r,S}$ then $\phi(m) \in (\mathcal{M}_2)_{r,S}$.

It will be useful to introduce more group-ring idempotents. In particular, for any natural number j we may form the idempotent

$$\mathbf{e}_j = \sum_{\substack{\chi \in \widehat{G} \\ r_S(\chi) = j}} \mathbf{e}_\chi.$$

Lemma 2.3.7. *Each* $\mathbf{e}_j$ *is an element of* $\mathbb{Q}[G]$.

Proof. This is obvious if there are no $\chi \in \widehat{G}$ with $r_{\mathcal{S}}(\chi) = j$. Otherwise this follows from the fact that if α is an automorphism of $\mathbb{C}$, then $r_{\mathcal{S}}(\chi \circ \alpha) = r_{\mathcal{S}}(\chi)$. (Because χ and $\chi \circ \alpha$ have the same kernel. Indeed for any two characters χ and ψ in $\widehat{G}$, there exists a $\mathbb{C}$-automorphism α with $\psi = \chi \circ \alpha$ if and only if $\ker \psi = \ker \chi$.) Hence we may group our characters by their kernels, and notice that if we take (for some ψ), $H = \ker \psi$, then

$$\sum_{\substack{\chi \in \widehat{G} \\ \ker(\chi) = H}} \mathbf{e}_\chi = \frac{1}{|G|} \left(\Phi(n) \sum_{\sigma \in H} \sigma + \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) \sum_{\sigma \notin H} \sigma \right) \in \mathbb{Q}[G].$$

where we let $n = \frac{|G|}{|H|}$, $\Phi(\cdot)$ is Euler's totient function, ζ_n is a primitive nth root of unity and Tr denotes the trace. (Notice that $\Phi(n)$ is nothing more than $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1)$.) □

Remark: If we throw in more of the $\mathbf{e}_\chi$'s we arrive at an even nicer formula: For *any* subgroup $H \subseteq G$,

$$\sum_{\substack{\chi \in \widehat{G} \\ H \subseteq \ker \chi}} \mathbf{e}_\chi = \frac{1}{|H|} N_H, \tag{2.4}$$

where

$$N_H = \sum_{h \in H} h \in \mathbb{Z}[G] \tag{2.5}$$

is the *algebraic norm* attached to the subgroup H. This can be proved by applying each $\psi \in \widehat{G}$ to both sides of the equation. If $H \subseteq \ker \psi$ we get $1 = 1$, and otherwise, $0 = 0$. By the direct sum decomposition of $\mathbb{C}[G]$, equation (2.3), we are done.

Lemma 2.3.8. *The functor $(\cdot)_{r,S}$ from the category of $\mathbb{Q}[G]$-modules to itself has the following properties*

(i) It is exact.

(ii) It commutes with taking exterior product over $\mathbb{Q}[G]$.

Proof. *(i)* Suppose $0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\phi} C \longrightarrow 0$ is a short exact sequence of $\mathbb{Q}[G]$-modules. Being merely a restriction, $(\iota)_{r,S}$ is still injective. If $c \in (C)_{r,S}$, Let $b \in B$ be such that $\phi(b) = c$. Put $b' = \sum_{r(\chi)=r} \mathbf{e}_\chi \cdot b = \mathbf{e}_r \cdot b$. Then $b' \in (B)_{r,S}$, and

$$\phi(b') = \mathbf{e}_r \cdot c = \sum_{\chi \in \widehat{G}} \mathbf{e}_\chi \cdot c = c.$$

Hence $(\phi)_{r,S}$ is onto $(C)_{r,S}$.

Exactness in the middle is an equally easy exercise.

(ii) Let $\mathcal{M}$ be a $\mathbb{Q}[G]$-module, and n a positive integer. We wish to prove that $\left(\bigwedge_{\mathbb{Q}[G]}^n \mathcal{M}\right)_{r,S} = \bigwedge_{\mathbb{Q}[G]}^n (\mathcal{M})_{r,S}$. The inclusion $(\supseteq)$ is immediate. On the other hand, if $m = m_1 \wedge \ldots \wedge m_n \in \left(\bigwedge_{\mathbb{Q}[G]}^n \mathcal{M}\right)_{r,S}$, then

$$m = \mathbf{e}_r \cdot m = \mathbf{e}_r^n \cdot m = (\mathbf{e}_r \cdot m_1) \wedge \ldots \wedge (\mathbf{e}_r \cdot m_n) \in \bigwedge_{\mathbb{Q}[G]}^n (\mathcal{M})_{r,S}.$$

The proof concludes by the linearity of multiplication by $\mathbf{e}_r$. □

Lemma 2.3.9. *If $|S| > r+1$, $(\mathbb{C}\bigwedge^r X_S)_{r,S} = (\mathbb{C}\bigwedge^r Y_S)_{r,S}$.*

Proof. Tensoring the exact sequence $0 \longrightarrow X_S \longrightarrow Y_S \longrightarrow \mathbb{Z} \longrightarrow 0$ with the flat $\mathbb{Z}$-module $\mathbb{C}$ yields an exact sequence $0 \longrightarrow \mathbb{C}X_S \longrightarrow \mathbb{C}Y_S \longrightarrow \mathbb{C}\mathbf{e}_1 \longrightarrow 0$, where we write $\mathbb{C}\mathbf{e}_1$ to emphasize the trivial G-action. Now apply the functor $(\cdot)_{r,S}$, noting that the functor annilihates $\mathbb{C}\mathbf{e}_1$ if and only if $|S| > r+1$. Now use both *(i)* and *(ii)* of Lemma 2.3.8. □

For each $v \in S$, arbitrarily fix a single $w \in S_K$ with $w|v$. We define a regulator map

$$\mathbb{C}U_{K,S} \xrightarrow{R_S} \mathbb{C}X_S$$

via $R_S(u) = \sum_{v \in S} l_w(u) \cdot w$, where

$$l_w(u) = \frac{1}{|G_v|} \sum_{\sigma \in G} \log |u^{\sigma^{-1}}|_w \cdot \sigma.$$

Proposition 2.3.10. *The map R_S is a $\mathbb{C}[G]$-isomorphism.*

Proof. That the map is a $\mathbb{C}[G]$-homomorphism is easily checked. Suppose $u \in U_{K,S}$ and $R_S(u) = 0$. Then u has trivial valuation at every single prime of K, and hence is a root of unity. But the image of such an element in $\mathbb{C}U_{K,S}$ is trivial. It follows that as a map of $\mathbb{C}$-vector spaces, R_S is injective. Since $\mathbb{C}U_{K,S}$ and $\mathbb{C}X_S$ have the same dimension over $\mathbb{C}$ (see Lemma 2.5.1 in the following unit group section), the proposition follows. □

From this isomorphism we get an isomorphism of exterior algebras

$$\mathbb{C}\bigwedge^r U_{K,S} \xrightarrow{\bigwedge^r R_S} \mathbb{C}\bigwedge^r X_S.$$

Recall that for any set $S = \{v_1, ..., v_{|S|}\}$, of places of the base field k we have arbitrarily fixed a prime w_i of K dividing v_i. We also fix an arbitrary order on S, so that if we pick a subset $I = \{v_{i_1}, ..., v_{i_r}\}$ of S with exactly r elements, we may put $w_I = w_{i_1} \wedge ... \wedge w_{i_r}$ and there is no ambiguity about the sign. If $S' \subseteq S$ has more than r elements we put

$$w_{S'} = \sum w_I,$$

where the summation runs over all subsets I of S' of cardinality exactly r. (Each distinct subset gives rise to only one summand; we always order the subscripts in increasing order.) We introduce the notation $\mathcal{P}(S)$ for the power set of S, and $\mathcal{P}_r(S)$ for the set of all subsets of S of cardinality exactly r. Thus we could write $w_{S'} = \sum_{I \in \mathcal{P}_r(S)} w_I$.

Proposition 2.3.11. *Assume S is an r-cover for $\widehat{G}$. Then $S' \subseteq S$ is an r-cover for $(\widehat{G})_{r,S}$ if and only if $(\mathbb{C}\bigwedge^r Y_S)_{r,S}$ is a free $(\mathbb{C}[G])_{r,S}$-module of rank 1 and basis $w_{S'}$.*

Proof. For this proof we refer the reader to [Pop06]. □

Let $\rho_{S_{\min}}$ be the map that sends an element $\lambda \cdot w_{S_{\min}}$ in $(\mathbb{C}\bigwedge^r Y_S)_{r,S}$ to $\lambda \in \mathbb{C}[G]$. This map is well defined by the previous proposition. In the following sequence (with our standing assumption that $|S| > r+1$), each map is an isomorphism of $\mathbb{C}[G]$-modules

$$\left(\mathbb{C}\bigwedge^r U_{K,S}\right)_{r,S} \xrightarrow{\bigwedge^r R_S} \left(\mathbb{C}\bigwedge^r X_S\right)_{r,S} \longrightarrow \left(\mathbb{C}\bigwedge^r Y_S\right)_{r,S} \xrightarrow{\rho_{S_{\min}}} \mathbb{C}[G]_{r,S}.$$

We call the composite of these maps the $S_{\min}$-regulator attached to the extension K/k, and denote it $\mathcal{R}_{K/k,S}$. At times, in the interest of succinct typography, we may suppress either or both of the subscripts.

Thus far, the regulators we have been discussing do not resemble the standard regulators of algebraic number theory, namely determinants of logarithms. However, we make that connection next. For the field extension K/k, with primes $w_1, \ldots, w_r$ we define yet another regulator map. Let $W = w_1 \wedge \ldots \wedge w_r \in \bigwedge^r_{\mathbb{Z}[G]} Y_K$, and for $u_1, \ldots, u_r \in U_{K,S}$ put

$$R_W(u_1 \wedge \ldots \wedge u_r) = \det_{1 \le i,j \le r} \left(l_{w_j}(u_i) \right) \in \mathbb{C}[G],$$

and then extend this map to all of $\mathbb{C}\bigwedge_{\mathbb{Z}[G]}^r U_{K,S}$ via linearity. These are the regulators that will be used when stating the so-called *standard* conjectures in the next chapter. It is not surprising, perhaps, that they have a link with the regulator $\mathcal{R}_{K/k,S}$ which we have already defined. For the proof of the next theorem, see [Pop06].

Theorem 2.3.12.

$$\mathcal{R}_{K/k} = R_{w_{S_{\min}}} = \sum_{I \in \mathcal{P}_r(S_{\min})} R_{w_I}.$$

Suppose H is a subgroup of G. Put $M = K^H$, and $\Gamma = G/H = G(M/k)$. There is a natural projection $\pi = \pi_{K/M} : G \to \Gamma$, which may be extended to a map $\mathbb{C}[G] \to \mathbb{C}[\Gamma]$. By abuse of notation we use π to denote both.

Proposition 2.3.13. *For any* $z \in \mathbb{C}\bigwedge^r U_{K,S}$*,*

$$\pi_{K/M}\mathcal{R}_{K/k}(z) = \mathcal{R}_{M/k}(N_{M/K}^{(r)}z).$$

Proof. By the linearity of all operators considered, it suffices to assume z is a simple tensor, $z = u_1 \wedge \ldots \wedge u_r$. Let $v_1, ..., v_r$ be any r primes of k, and fix $w_i | \text{Ш}_i | v_i$ primes of $K/M/k$, respectively.

Recalling the way we normalize our absolute values, and that for decomposition groups, $|H_{\rm II}|/|G_v| = 1/|\Gamma_v|$, we have

$$\begin{aligned}
\pi l_w(u) &= \frac{1}{|G_v|}\sum_{\sigma\in G}\log|u^{\sigma^{-1}}|_w\cdot\sigma H \\
&= \frac{1}{|G_v|}\sum_{\substack{\sigma H \text{ rep.}\\ G/H}}\left(\sum_{h\in H}\log|u^{h^{-1}\sigma^{-1}}|_w\right)\cdot\sigma H \\
&= \frac{1}{|G_v|}\sum_{\substack{\sigma H \text{ rep.}\\ G/H}}\log|N_{K/M}(u^{\sigma^{-1}})|_w\cdot\sigma H \\
&= \frac{1}{|G_v|}\sum_{\substack{\sigma H \text{ rep.}\\ G/H}}\log|(N_{K/M}u)^{\sigma^{-1}H}|_{\rm II}^{|H_{\rm II}|}\cdot\sigma H \\
&= l_{\rm II}(N_{K/M}u)
\end{aligned}$$

for any $u \in U_{K,S}$.

Let $\mathrm{II} = \mathrm{II}_1 \wedge \ldots \wedge \mathrm{II}_r$ and $W = w_1 \wedge \ldots \wedge w_r$. Then

$$\pi R_W(z) = \pi \det_{1\le i,j\le r}(l_{w_i}(u_j)) = \det_{1\le i,j\le r}(l_{\mathrm{II}_i}(N_{K/M}u_j)) = R_{\rm II}(N^{(r)}_{K/M}z).$$

Hence, we are done by Theorem 2.3.12. □

Finally we need to construct a map that is a one-sided inverse of $\pi_{K/M}$. We define

$$\begin{aligned}
\Psi_{K/M}: \quad & \mathbb{C}[\Gamma] \longrightarrow \mathbb{C}[G] \\
& \textstyle\sum_{\tau H\in\Gamma} n_{\tau H}\cdot\tau H \longmapsto \frac{1}{|H|}\sum_{\sigma\in G} n_{\sigma H}\cdot\sigma
\end{aligned}$$

Lemma 2.3.14. *The map $\Psi_{K/M}$ has the following properties:*

(i) $\pi_{K/M}\circ\Psi_{K/M} = \mathrm{id}_{\mathbb{C}[\Gamma]}$

(ii) $\Psi_{K/M}\circ\pi_{K/M} =$ *(multiplication by* $\frac{1}{|H|}N_H$ *in* $\mathbb{C}[G]$*)*

(iii) For $\chi \in \widehat{\Gamma}$ *any character,* $\Psi_{K/M}(\mathbf{e}_\chi) = \mathbf{e}_{\chi\circ\pi_{K/M}}$.

Proof. These are all straight-forward computations. As an example, we perform the computation for *(iii)*:

$$\begin{aligned}\Psi(\mathbf{e}_\chi) &= \Psi\left(\frac{1}{|\Gamma|}\sum_{\sigma H\in\Gamma}\chi((\sigma H)^{-1})\sigma H\right)\\ &= \frac{1}{|\Gamma||H|}\sum_{\sigma\in G}\chi(\sigma^{-1}H)\cdot\sigma\\ &= \frac{1}{|G|}\sum_{\sigma\in G}(\chi\circ\pi)(\sigma^{-1})\cdot\sigma\\ &= \mathbf{e}_{\chi\circ\pi}.\end{aligned}$$

□

2.4 Artin L-functions

Let S be a finite set of primes of k. As a standing assumption, S contains all the Archimedean primes, and those ramifying in K/k. Define, originally for $\Re e(s) > 1$, a so-called G-equivariant (S,T)-modified L-function

$$\Theta_{K/k,S,T}(s) : \mathbb{C} \to \mathbb{C}[G]$$

by

$$\Theta_{K/k,S,T}(s) = \prod_{v\notin S}(1-\sigma_v^{-1}Nv^{-s})^{-1}\prod_{v\in T}(1-\sigma_v^{-1}Nv^{1-s}) \tag{2.6}$$

The product converges absolutely and uniformly on compact subsets of $\Re e(s) > 1$. The function given by the product may be uniquely analytically continued to a entire function on $\mathbb{C}\setminus\{1\}$ with a simple pole at $s = 1$, thereby defining Θ. The individual term $(1-\sigma_v^{-1}Nv^{-s})^{-1}$ is called the *Euler factor* associated to v. The terms appearing rightmost are called the *smoothing factors* associated to T.

There is an alternate way to write $\Theta_{K/k,S,T}(s)$:

$$\Theta_{K/k,S,T}(s) = \sum_{\chi \in \widehat{G}} L_{K/k,S,T}(s, \chi^{-1})\mathbf{e}_{\chi}, \tag{2.7}$$

where $L_{K/k,S,T}(s,\chi)$ is the (S,T)-modified Artin L-function attached to χ. Specifically the L-functions are given by the formula:

$$L_{S,T}(s,\chi) = \prod_{v \notin S}(1 - \chi(\sigma_v)Nv^{-s})^{-1} \prod_{v \in T}(1 - \chi(\sigma_v)Nv^{1-s}).$$

Because we are assuming K/k is abelian, all representations are 1-dimensional and we do not need to consider the determinant of the action as is done in general (see [Neu99, VII§12]). Further, because S contains all infinite and ramifying primes, we avoid defining Euler factors for these "bad" primes.

If one multiplies out the Euler factors, one obtains (for simplicity taking $T = \emptyset$)

$$L_S(s,\chi) = \sum \frac{\chi(\sigma_{\mathfrak{a}})}{(N\mathfrak{a})^s},$$

where the sum is over all (integral) ideals $\mathfrak{a}$ of k relatively prime to S. The automorphism $\sigma_{\mathfrak{a}}$ is defined by

$$\sigma_{\mathfrak{a}} = \sigma_{\mathfrak{p}_1}\sigma_{\mathfrak{p}_2}\ldots\sigma_{\mathfrak{p}_t}$$

where $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_t$ is the prime factorization of $\mathfrak{a}$.

When G is abelian, these functions may be extended to analytic functions of the entire complex plane for $\chi \neq \mathbf{1}$ and $L_{K/k,S,T}(s,\mathbf{1}) = \zeta_{k,S,T}(s)$ is analytically continued to the whole plane except for a simple pole at $s = 1$.

As in the previous section, we take $H \subseteq G$ a subgroup and put $M = K^H$, and $\Gamma = G/H = G(M/k)$. We denote the natural projection $\mathbb{C}[G] \to \mathbb{C}[\Gamma]$ by π. In this situation, Artin L-functions satisfy some well-known functoriality properties, which are summarized in the next proposition.

Proposition 2.4.1. *(i) (Inflation) If* $\psi : G(M/k) \to \mathbb{C}^\times$ *is any character, then* $\psi \circ \pi$ *is a character of* $G(K/k)$ *and*

$$L_{K/k}(s, \psi \circ \pi) = L_{M/k}(s, \psi).$$

(ii) (Restriction) If $\widetilde{\chi} : G(K/M) \to \mathbb{C}^\times$ *is a character of* $G(K/M)$*, then*

$$L_{K/M}(s, \widetilde{\chi}) = \prod_{\substack{\chi \in \widehat{G(K/k)} \\ \chi|_{G(K/M)} = \widetilde{\chi}}} L_{K/k}(s, \chi).$$

Proof. The proof is based on looking one-at-a-time at each Euler factor coming from a prime in the base field. See for example [Neu99, Proposition VII.10.4]. ☐

Remarks: (1) Notice that in part *(ii)* if we take $M = K$, and $\widetilde{\chi}$ to be (by necessity) the trivial character, then we recover the important formula

$$\zeta_K(s) = \prod_{\chi \in \widehat{G}} L_{K/k}(s, \chi).$$

(2) Also, because of these properties, we could suppress the notation of which fields we are working with from the L-functions, however we will mainly only do this when the fields are fixed.

(3) All stated properties also hold for S- and (S, T)-modified L-functions.

Let us push the idea in Remark (1) a bit further and prove an amusing lemma which relates the total splitting of the primes of $\mathcal{S}$ in K/k to their splitting in each cyclic subextension of K/k.

Lemma 2.4.2. *For any set of primes $\mathcal{S}$ of the base field k, we have the following equality*

$$\sum_{\substack{\chi\in\widehat{G}\\ \chi\neq\mathbf{1}_G}} r_{\mathcal{S}}(\chi) = \sum_{v\in\mathcal{S}}(g_v - 1), \tag{2.8}$$

where $g_v = \frac{|G|}{|G_v|}$ is the number of primes of K lying above v.

Proof. By Remark (1) above, we may conclude (by dividing the zeta function of k across) that

$$\mathrm{ord}_{s=0}(\zeta_{K,\mathcal{S}}(s)) - \mathrm{ord}_{s=0}(\zeta_{k,\mathcal{S}}(s)) = \sum_{\substack{\chi\in\widehat{G}\\ \chi\neq\mathbf{1}_G}} \mathrm{ord}_{s=0}(L_{K/k,\mathcal{S}}(s,\chi)).$$

The right hand side is exactly $\sum_{\substack{\chi\in\widehat{G}\\ \chi\neq\mathbf{1}_G}} r_{\mathcal{S}}(\chi)$, while the left hand side is $(|\mathcal{S}_K| - 1) - (|\mathcal{S}| - 1)$. But $|\mathcal{S}_K| = \sum_{v\in\mathcal{S}} g_v$. □

2.5 Unit groups

At the heart of the theory lies the (S,T)-modified unit group $U_{K,S,T}$, defined by

$$U_{K,S,T} = \left\{u \in K^\times :\ |u|_w = 1\ (\forall w \notin S_K),\ u \equiv 1 \pmod{\mathfrak{P}}\ \ (\forall \mathfrak{P} \in T_K)\right\}.$$

In this section, we collect several (slightly disjointed) lemmas that will help us when working with these groups. Let us describe their structure as $\mathbb{Z}$- and $\mathbb{Z}[G]$-modules. The first is not far to seek; the following lemma describes the $\mathbb{Z}$-structure completely.

Lemma 2.5.1. *As abelian groups,* $U_{K,S} \cong \mu_K \times \mathbb{Z}^{|S_K|-1}$*, and* $U_{K,S,T} \cong \mu_{K,T} \times \mathbb{Z}^{|S_K|-1}$ *where* μ_K *(respectively* $\mu_{K,T}$*) is the group of roots of unity of* K *(respectively roots of unity of* K *congruent to 1 modulo every prime in* T_K*).*

Proof. The first is the well-known Dirichlet Theorem for S-units (see e.g. [Gra03] or [Neu99]). For the second, suppose that $u_1, \ldots, u_n$ $(n = |S_K| - 1)$ is a basis for $U_{K,S}/\mu_K$. Then by Fermat's Little Theorem, if we raise each u_i to a high enough power ν, we will have $u_i^\nu \equiv 1 \pmod{\mathfrak{M}_T}$ where $\mathfrak{M}_T$ is the product of all the primes in T_K. Hence the $\mathbb{Z}$-rank of $U_{K,S,T}$ is at least that of $U_{K,S}$, but as the former is contained in the latter, the ranks must be equal. The reduction from μ_K to $\mu_{K,T}$ is immediate. □

The structure of $U_{K,S,T}$ (or $U_{K,S}$) as a $\mathbb{Z}[G]$-module is not well understood. Indeed, coming to understand this structure is one of the key hopes of pursuing Stark-type conjectures.

When we deal with (S,T)-modified objects in the conjectures that are to follow, we will be making the requirement that $U_{K,S,T}$ is $\mathbb{Z}$-torsion free, or equivalently, that $\mu_{K,T} = \{1\}$. This is not at all hard to achieve, as evidenced by the following lemma.

Lemma 2.5.2. *The condition that* $U_{K,S,T}$ *is* $\mathbb{Z}$*-torsion-free is satisfied if* T *contains at least one prime* $\mathfrak{p}$ *that does not divide* $w_K\mathcal{O}_K$ *(where* w_K *denotes the number of roots of unity in* K*).*

Proof. Consider the function $f(x) = x^{w_K} - 1$, which is a (reducible) defining equation for the roots of unity in $\mathcal{O}_K$. Let $\mathfrak{P}$ be a prime of K lying above $\mathfrak{p}$. The fact that $f'(x) = w_K x^{w_K - 1}$ is trivial $\pmod{\mathfrak{P}}$ only at $x \equiv 0 \pmod{\mathfrak{P}}$ tells us that the roots of f are distinct $\pmod{\mathfrak{P}}$. Hence for $\zeta \in \mu_K$,

$$\zeta \neq 1 \Rightarrow \zeta \not\equiv 1 \pmod{\mathfrak{P}} \Rightarrow \zeta \notin U_{K,S,T}.$$

□

In the coming sections, when we define certain lattices inside $\mathbb{C}\bigwedge^r U_{K,S}$ we will be working not only with the unit groups, but also with their $\mathbb{Z}[G]$-duals. As usual we need to understand their behavior under change of field.

Lemma 2.5.3. *For any $\mathbb{Z}[G]$-module $\mathcal{M}$ there is an isomorphism of abelian groups*

$$\mathrm{Hom}_{\mathbb{Z}}(\mathcal{M}, \mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathcal{M}, \mathbb{Z}[G]).$$

Proof. An isomorphism is given by the map $\varphi \longmapsto (m \mapsto \sum_{\sigma \in G} \varphi(m^\sigma) \cdot \sigma^{-1})$, with inverse map $\phi \longmapsto (m \mapsto (\text{coefficient of } id_G \text{ in } \phi(m)))$. See [Rub96]. □

Definition 2.5.4. *We follow [Pop04, Section 4], in defining a map*

$$N^*_{K/M} : \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G]) \to \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_{M,S,T}, \mathbb{Z}[\Gamma])$$

via

$$(N^*_{K/M}\varphi)(u) = \frac{1}{[K:M]} \pi_{K/M} \circ \varphi \circ \iota_{K/M}(u). \tag{2.9}$$

Lemma 2.5.5. *If $\widehat{\mathrm{H}}^1(G(K/M), \mu_{K,T}) = 1$, then the map $N^*_{K/M}$ is surjective.*

Proof. The sequence $1 \to U_{M,S,T} \to U_{K,S,T} \to U_{K,S,T}/U_{M,S,T} \to 1$ leads to a long exact sequence

$$1 \to \mathrm{Hom}_{\mathbb{Z}}(U_{K,S,T}/U_{M,S,T}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(U_{K,S,T}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(U_{M,S,T}, \mathbb{Z}) \xrightarrow{\delta}$$
$$\mathrm{Ext}^1_{\mathbb{Z}}(U_{K,S,T}/U_{M,S,T}, \mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(U_{K,S,T}, \mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(U_{M,S,T}, \mathbb{Z}) \to 1.$$

The final term is 1 because, for any abelian group A, $\mathrm{Ext}^i_{\mathbb{Z}}(A,\mathbb{Z})$ is trivial if $i \geq 2$ (see [DF91, Section 17.1]). Further, $\#\mathrm{Ext}^1_{\mathbb{Z}}(A,\mathbb{Z})$ is equal to the order of the torsion subgroup of A, if it is finite.

Let us show, by counting cardinalities, that the long exact sequence above splits into two short exact sequences at δ. Pick a u in the torsion subgroup $\mathcal{Z}$ of $U_{K,S,T}/U_{M,S,T}$, so that $u^n \in U_{M,S,T}$ for some $n \geq 1$. Consider the map $H \to \mu_{K,T}$, $\sigma \mapsto u^{\sigma-1}$. Let's justify that $\mu_{K,T}$ is indeed the target of this map. For each $h \in H := G(K/M)$, we then have $(u^{h-1})^n = (u^n)^{h-1} = 1$, so that $u^{h-1} = \zeta_h$ is some n^{th} root of unity in $U_{K,S,T}$. One checks that this map is a 1-cocycle. (Indeed, $u^{\tau\sigma-1} = u^{\tau\sigma-\tau+\tau-1} = u^{\tau-1}u^{\tau(\sigma-1)}$.) Thus, by modding out coboundaries, this map induces one

$$1 \to \ker\varphi \to \mathcal{Z} \xrightarrow{\varphi} \widehat{\mathrm{H}}^1(H, \mu_{K,T}),$$

where $\ker\varphi = \mu_{K,T}U_{M,S,T}/U_{M,S,T} \cong \mu_{K,T}/\mu_{M,T}$. By assumption, the cohomology group $\widehat{\mathrm{H}}^1(H,\mu_{K,T})$ is trivial, and hence $\mathcal{Z} \cong \ker\varphi$. We conclude that $\#\mathcal{Z} = \frac{w_{K,T}}{w_{M,T}}$ and hence by looking at cardinalities,

$$1 \to \mathrm{Ext}^1_{\mathbb{Z}}(U_{K,S,T}/U_{M,S,T},\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(U_{K,S,T},\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(U_{M,S,T},\mathbb{Z}) \to 1$$

is exact, so that

$$1 \to \mathrm{Hom}_{\mathbb{Z}}(U_{K,S,T}/U_{M,S,T},\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(U_{K,S,T},\mathbb{Z}) \xrightarrow{\mathrm{res}_{K/M}} \mathrm{Hom}_{\mathbb{Z}}(U_{M,S,T},\mathbb{Z}) \to 1$$

is an exact sequence.

Next, one checks that the diagram

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(U_{K,S,T},\mathbb{Z}) & \xrightarrow{\mathrm{res}_{K/M}} & \mathrm{Hom}_{\mathbb{Z}}(U_{M,S,T},\mathbb{Z}) \\ \downarrow \cong & & \downarrow \cong \\ \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T},\mathbb{Z}[G]) & \xrightarrow{N^*_{K/M}} & \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_{M,S,T},\mathbb{Z}[\Gamma]) \end{array}$$

is commutative. We have just seen that the top map in the above commutative diagram is surjective. Since the vertical maps are isomorphisms (by Lemma 2.5.3), it follows that the bottom map is also surjective. □

Note of course that if, as we often assume, $\mu_{K,T} = \{1\}$ then $\widehat{\mathrm{H}}^1(H, \mu_{K,T})$ is obviously trivial.

It will be important to know how the map N^* interacts with the natural projection and elements of the dual group of $U_{K,S,T}$. The answer lies in the following

Lemma 2.5.6. *If $z \in \mathbb{Q}\bigwedge^r_{\mathbb{Z}[G]} U_{K,S,T}$ and $\phi_1, \ldots, \phi_r \in U^*_{K,S,T}$, we have*

$$\pi_{K/M}(\phi_1 \wedge \ldots \wedge \phi_r)(z) = ((N^*_{K/M}\phi_1) \wedge \ldots \wedge (N^*_{K/M}\phi_r))(N^{(r)}_{K/M}z).$$

Proof. By linearity, it suffices to assume $z = u_1 \wedge \ldots \wedge u_r$. Then

$$\begin{aligned} \pi_{K/M}(\phi_1 \wedge \ldots \wedge \phi_r)(u_1 \wedge \ldots \wedge u_r) &= \pi_{K/M} \det(\phi_i(u_j)) \\ &= \det(\pi_{K/M}\phi_i(u_j)) \\ &= \det\left(\pi_{K/M}\frac{N_{K/M}}{[K:M]}\phi_i(u_j)\right) \\ &= \det\left(\frac{1}{[K:M]}\pi_{K/M}\phi_i(N_{K/M}u_j)\right) \\ &= \det\big((N^*_{K/M}\phi_i)(N_{K/M}u_j)\big) \\ &= ((N^*_{K/M}\phi_1) \wedge \ldots \wedge (N^*_{K/M}\phi_r))(N^{(r)}_{K/M}z) \end{aligned}$$

as desired. □

Finally we round out this section by proving that the evaluators we will be examining in the rest of this dissertation are supported only at certain primes.

Lemma 2.5.7. *Suppose that S contains exactly r primes that split completely in the extension K/k and $u \in (U_{K,S})_{r,S}$. Then $|u|_w = 1$ for all primes w not dividing the split primes in S.*

Proof. Fix such a w and call v the prime below it in k. If $v \notin S$ then $|u|_w = 1$ by the definition of $U_{K,S}$. So suppose $v \in S$, in which case we are assuming v does not split completely in K/k, so the decomposition group G_v is nontrivial.

We work with the element $\lambda = |G|\mathbf{e}_r \in \mathbb{Z}[G]$. As $u \in (U_{K,S})_{r,S}$, $\mathbf{e}_r \cdot u = u$ in $\mathbb{C}U_{K,S}$, which means that $u^\lambda = \zeta \cdot u^{|G|}$ for some root of unity ζ. By applying the absolute values,

$$\begin{aligned}
|u|_w^{|G|} &= \prod_{\sigma \in G} \left| u^{\sum_{\chi \in \widehat{G}_{r,S}} \chi(\sigma^{-1})\sigma} \right|_w \\
&= \prod_{\sigma \in G} \left| u^{\sum_{\chi \in \widehat{G}_{r,S}} \chi(\sigma)} \right|_{w^\sigma} \\
&= \prod_{\sigma \in G/G_v} \left| u^{\sum_{\chi \in \widehat{G}_{r,S}} \chi(\sigma) \sum_{\tau \in G_v} \chi(\tau)} \right|_{w^\sigma} \\
&= 1.
\end{aligned}$$

The last equality holds because in general $\sum_{\tau \in G_v} \chi(\tau)$ is either $|G_v|$ or 0 based on whether $G_v \subseteq \ker \chi$ or not—however $\chi \in \widehat{G}_{r,S}$ means that for primes in S, *only* the r split ones have $G_v \subseteq \ker \chi$.

Since $|u|_w$ is a nonnegative real number, $|u|_w = 1$. ∎

2.6 Class field theory

Class field theory has intimate connections with Stark's conjectures, which is apparent from the h_K figuring so prominently in the seminal formula

$$\zeta_K(s) = -\frac{h_K R_K}{w_K} s^d + O(s^{d+1}).$$

In the higher order conjectures, the behaviors of the primes in S must be known. Do they ramify in K/k? How many of them split in each subextension? This is one of the two uses we will have for class field theory: it governs these behaviors. When we turn to studying extensions of exponent two (Chapter 4), we need to understand the 2-rank of certain ideal class groups. In this section we introduce these groups and begin to discuss relationships between their ranks.

Throughout this section we will follow the notational conventions found in Gras [Gra03]. We fix a number field k and take S and T to be a finite disjoint sets of places of k. Let $\mathcal{I}_k$ denote the group of fractional ideals of k, and Pl_0 denote the set of finite places of k. Similarly Pl_∞, Pl_∞^{r}, and Pl_∞^{c} denote the infinite places, and the real and complex subsets of them, respectively. Finally, for a rational prime number $p \in \mathbb{Z}$, Pl_p denotes the primes of k that divide p. For any set of places $\mathcal{T}$ we denote $\mathcal{T}_0 = \mathcal{T} \cap Pl_0$. We can form the ideal

$$\mathfrak{M}_{\mathcal{T}} = \prod_{\mathfrak{p} \in \mathcal{T}_0} \mathfrak{p}.$$

We consider subgroups of fractional ideals—first those relatively prime to $\mathcal{T}$:

$$\mathcal{I}_{k,\mathcal{T}} = \{\mathfrak{a} \in \mathcal{I}_k \mid (\mathfrak{a}, \mathfrak{M}_{\mathcal{T}}) = 1\}.$$

Now for any ideal $\mathfrak{M}$ and any subset $\Delta \subseteq Pl^{\mathrm{r}}_{\infty}$, we form the principal ray class

$$P_{k,\mathfrak{M},\Delta} = \{(a) \in \mathcal{I}_{k,\mathrm{supp}(\mathfrak{M})} \mid a \in k^{\times},\ a \equiv 1 \pmod{\mathfrak{M}},\ \iota_v(a) > 0\ \ \forall v \in \Delta\}.$$

Definition 2.6.1. *Given a finite sets S of places of k, and an ideal $\mathfrak{M}$ with* $\mathrm{supp}(\mathfrak{M}) \cap S = \emptyset$*, we define the S-ray class group modulo $\mathfrak{M}$ to be the quotient*

$$Cl_{k,S,\mathfrak{M}} = \mathcal{I}_{k,\mathrm{supp}(\mathfrak{M})}/P_{k,\mathfrak{M},S^{\mathrm{r}}_{\infty}}\langle S_0\rangle.$$

The class groups of interest to us generally have a *tame modulus* with support equal to T, so we give these a special name:

Definition 2.6.2. *The (S,T)-modified class group of k is*

$$A_{k,S,T} = Cl_{k,S,\mathfrak{M}_T}.$$

If T is the empty set, we often abbreviate $A_{k,S} := A_{k,S,\emptyset}$.

The fundamental theorems of class field theory (applied to these circumstances) now combine to give:

Theorem 2.6.3. *There exists a field $H_{k,S,T}$ which is a finite Galois extension of k, coupled with a group isomorphism, called the Artin map, $A_{k,S,T} \xrightarrow{\cong} G(H_{k,S,T}/k)$. Moreover $H_{k,S,T}$ is the maximal abelian extension of k, which is unramified outside T, at most tamely ramified in T, and in which all primes in S split completely.*

Remark: Unlike many other sources, we follow Gras [Gra03] and Neukirch [Neu99] (in particular, see the discussion after Proposition III.3.13 in Neukirch) in calling a complexifying infinite prime "inert" as opposed to "ramifying." One then places any infinite prime one does not want "to ramify", i.e., one wishes to split, into S. Thus by not including any infinite primes in S one gets a *narrow* class field, and by including all of them one gets an *ordinary* class field.

Definition 2.6.4. *The cardinality of $A_{k,S,T}$, or equivalently of $G(H_{k,S,T}/k)$, is denoted $h_{k,S,T}$; we refer to it as the (S,T)-modified class number.*

As mentioned before, in Chapter 4 we study multiquadratic extensions, and the prime 2 is of utmost importance. Therefore we give primes that divide 2, i.e., those in Pl_2, a special name, and call them *dyadic* primes.

Theorem 2.6.5. *Suppose S contains the set of Archimedean places Pl_∞, and that T contains no dyadic primes and is disjoint from S. Then*

$$\mathrm{rk}_2(Cl_{k,S,\mathfrak{M}_T}) - \mathrm{rk}_2(Cl_{k,T,\mathfrak{M}^*}) = |T| - |S|,$$

where

$$\mathfrak{M}^* = \prod_{\mathfrak{p}\in S_0\setminus S_2} \mathfrak{p} \prod_{\mathfrak{p}\in S_2} \mathfrak{p}^{2e_\mathfrak{p}(k/\mathbb{Q})+1} \prod_{\mathfrak{p}\in Pl_2\setminus S_2} \mathfrak{p}^{2e_\mathfrak{p}(k/\mathbb{Q})}.$$

Proof. If we apply [Gra03, Theorem I.4.6(ii)] to this situation, we obtain

$$\mathrm{rk}_2(Cl_{k,S,T}) - \mathrm{rk}_2(Cl_{k,T,\mathfrak{M}^*}) = |T| - |S|,$$

where $Cl_{k,S,T} = \varprojlim Cl_{k,S,\mathfrak{N}}$ with the projective limit taken over all $\mathfrak{N}$ with support in T. It remains to show $\mathrm{rk}_2(Cl_{k,S,T}) = \mathrm{rk}_2(Cl_{k,S,\mathfrak{M}_T})$, which is achieved by the following argument. Let $\mathfrak{N} = \prod_{\mathfrak{p}\in T} \mathfrak{p}^{n_\mathfrak{p}}$ be any ideal with $n_\mathfrak{p} > 0$ for all $\mathfrak{p} \in T$ (i.e. $\mathfrak{M}_T|\mathfrak{N}$). According to Corollary I.4.5.4 in [Gra03],

$$0 \le \mathrm{rk}_2(Cl_{k,S,\mathfrak{N}}) - \mathrm{rk}_2(Cl_{k,S,\mathfrak{M}_T}) \le \sum_{\mathfrak{p}\in T} \mathrm{rk}_2((U_\mathfrak{p})^2 U_\mathfrak{p}^{(1)}/(U_\mathfrak{p})^2 U_\mathfrak{p}^{(n_\mathfrak{p})}),$$

where $U_{\mathfrak{p}}$ is the group of local units in the completion $k_{\mathfrak{p}}$, and $U_{\mathfrak{p}}^{(i)}$ is the subgroup of local units congruent to 1 modulo $\pi_{\mathfrak{p}}^i$ for a uniformizer $\pi_{\mathfrak{p}}$. But

$$(U_{\mathfrak{p}})^2 U_{\mathfrak{p}}^{(1)}/(U_{\mathfrak{p}})^2 U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \cong U_{\mathfrak{p}}^{(1)}/((U_{\mathfrak{p}})^2 U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \cap U_{\mathfrak{p}}^{(1)}).$$

But the group on the right is a quotient of $U_{\mathfrak{p}}^{(1)}/U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$, which has cardinality $(N\mathfrak{p})^{n_{\mathfrak{p}}-1}$. Since $\mathfrak{p}$ is non-dyadic, this cardinality is odd, so the 2-rank is zero. □

Next we turn to studying so-called *governing fields* as explicated in [Gra03]. For the moment M denotes any field intermediate between K and k, and $\Gamma = G(M/k)$.

Definition 2.6.6. *Let*

$$\mathcal{Y}_M^S = \{x \in M^\times \mid (x) = \mathfrak{a}^2 \mathfrak{a}_{S_0}, \mathfrak{a} \in \mathcal{I}_M, \mathfrak{a}_{S_0} \in \langle S_{M,0} \rangle\},$$

and

$$\mathcal{Q}_M = M(\sqrt{\mathcal{Y}_M^S}).$$

The field $\mathcal{Q}_M$ is called the $S-$governing field associated to M.

Note that $\mathcal{Y}_M^S$ is a $\mathbb{Z}[\Gamma]$-module, so by Lemma A.1.3 (found in Appendix A), the extension $\mathcal{Q}_M/k$ is Galois.

For each $w \in T_M$, let $\left(\frac{\mathcal{Q}_M/M}{w}\right)$ denote the Frobenius of w in $G(\mathcal{Q}_M/M)$.

Lemma 2.6.7. *If $T \neq \emptyset$ and T contains no dyadic primes, then there exists a T-totally ramified S-split relative quadratic extension of M if and only if*

$$\prod_{w \in T_M} \left(\frac{\mathcal{Q}_M/M}{w}\right) = 1.$$

Proof. This lemma is merely the specification to $p = 2$ of [Gra03, Corollary V.2.4.2]. □

2.7 Evaluators and lattices

When Stark examined the first derivatives of the L-functions, he expected their values to arise from a regulator map applied to an element $\varepsilon_{K/k}$ in $U_{K,S}$. When $r = r_S(K/k) > 1$, we want to examine the higher derivatives of the L-functions, and it becomes natural to ask not that the values come from a single unit, but rather from an r^{th} exterior product of $U_{K,S}$. We may need denominators, and indeed we shall first define the evaluator

$$\varepsilon_{K/k,S,T} \in \mathbb{C} \bigwedge_{\mathbb{Z}[G]}^{r} U_{K,S,T}.$$

More technically, the evaluator will be in the minimal order of vanishing $(\cdot)_{j,S}$ submodule of the exterior product. Indeed

Lemma 2.7.1. *If j denotes the number of primes which split completely in K/k then*

$$\frac{1}{j!}\Theta^{(j)}_{K/k,S,T}(0) \in (\mathbb{C}[G])_{j,S}. \tag{2.10}$$

Proof. By differentiating equation (2.7) j times, substituting $s = 0$ and dividing by $j!$, we see that the $\mathbf{e}_\chi$-component of $\frac{1}{j!}\Theta^{(j)}_{K/k,S,T}(0)$ is $\frac{1}{j!}L^{(j)}_{K/k,S,T}(0,\chi^{-1})$. For every character $\chi \in \widehat{G}$, $r_S(\chi) \geq j$, because of the j splitting primes and the remarks following Definition 2.3.2. On the other hand, if $r_S(\chi) > j$ we have $r_S(\chi^{-1}) > j$ and therefore these L-functions vanishing to order higher than j at $s = 0$, so its j^{th} derivative evaluates to 0. Therefore this element of $\mathbb{C}[G]$ is only supported on $\mathbf{e}_\chi$-components with $r_S(\chi) = j$. □

The evaluators we fix *will* depend on our choice of primes w sitting above primes $v \in S$ that we use to define the regulators. However, this dependence is well-understood and does not affect the truth of the conjectures. For details, see Remark 2 in Section 2.1 of [Pop04]. Also note that we will be using the notation $f^{(r)}(s)$ to denote the usual r^{th} derivative of $f(s)$, as opposed to the r^{th} derivative divided by $r!$ as is done in some of the literature on Stark-type conjectures.

Definition 2.7.2. *(*THE STANDARD RUBIN-STARK EVALUATOR*) Let S^+ denote the primes in S that split completely in K/k. Let j be a nonnegative integer.*
(i) If $j = |S^+|$ we put $W = w_{S^+}$ in the sense of Section 2.3, and define

$$\varepsilon_{K/k,S,T,j} \quad = \quad R_W^{-1}\left(\frac{1}{j!}\Theta^{(j)}_{K/k,S,T}(0)\right)$$

—the inverse image under the isomorphism

$$\left(\mathbb{C}\bigwedge^{j} U_{K,S,T}\right)_{j,S} \xrightarrow{R_W} (\mathbb{C}[G])_{j,S}$$

of the special value of the j-th derivative of the equivariant L-function.
(ii) If $j < |S^+|$ we put $\varepsilon_{K/k,S,T,j} = 0$.
(iii) If $j \geq |S|-1$ or $j > |S^+|$ we do not define $\varepsilon_{K/k,S,T,j}$. (This case will be avoided in the sequel.)

These epsilons are called the standard Rubin-Stark evaluators for the data K/k, S, and T. They are the elements that appear in the standard conjectures, which we will meet in the next chapter. Note that although $\varepsilon_{K,S,T,j}$ is an element of the (j,S)-submodule of the exterior product, we often regard it as an element of $\mathbb{C}\bigwedge^r_{\mathbb{Z}[G]} U_{K,S,T}$ itself.

Definition 2.7.3. *(*THE EXTENDED RUBIN-STARK EVALUATOR*) On the other hand, we introduce for this dissertation a more general evaluator, $\epsilon_{K/k,S,T}$, as fol-*

lows:

$$\epsilon_{K/k,S,T} = \mathcal{R}_{K/k,S}^{-1}\left(\frac{1}{r!}\Theta_{K/k,S,T}^{(r)}(0)\right),$$

where $r = \min_{\chi\in\widehat{G}} r_S(\chi)$ *is the minimal order of vanishing.*

As defined, these evaluators always exist. The conjectures we formulate will therefore not stipulate their existence, but rather predict where exactly they lie. *A priori*, they are elements of a $\mathbb{C}$-vector space. We will first conjecture them to lie in a rational ("$\mathbb{Q}$") component of it, and then in an integral ("$\mathbb{Z}$") lattice inside that component.

Finally we turn to defining lattices inside of exterior products. Let D be a commutative ring and $\mathcal{M}$ be any D-module. Let $\mathcal{M}^* := \mathrm{Hom}_D(\mathcal{M}, D)$ be the dual in the category of D-modules. As described by Rubin (in [Rub96, Section 1.2]), for any $0 \le j \le r$, there is a canonical map

$$\bigwedge_D^j \mathcal{M}^* \to \mathrm{Hom}_D\left(\bigwedge_D^r \mathcal{M},\ \bigwedge_D^{r-j}\mathcal{M}\right).$$

This is achieved by iterating the map that a single ϕ defines from $\bigwedge^r \mathcal{M}$ to $\bigwedge^{r-1}\mathcal{M}$:

$$m_1 \wedge \ldots \wedge m_r \mapsto \sum_{i=1}^r (-1)^{i+1}\phi(m_i) m_1 \wedge \ldots \wedge m_{i-1} \wedge m_{i+1} \wedge \ldots \wedge m_r.$$

When $j = r$, the induced map is $(\phi_1 \wedge \ldots \wedge \phi_r)(m_1 \wedge \ldots \wedge m_r) = \det(\phi_i(m_j))$.

In order to define a lattice we are going to implement these ideas with $D = \mathbb{Z}[G]$, $\mathcal{M} = U_{K,S,T}$ and $j = r$ or $j = r - 1$.

We define the Rubin-conjectured lattice $\Lambda_{K/k,S,T,r}$ to be

$$\left\{\lambda \in \left(\mathbb{Q}\bigwedge_{\mathbb{Z}[G]}^r U_{K,S,T}\right)_{r,S} \middle|\ \phi_1 \wedge \ldots \wedge \phi_{r-1}(\lambda) \in U_{K,S,T},\ \forall\ \phi_1, \ldots, \phi_{r-1} \in U_{K,S,T}^*\right\}.$$

Equivalently, we could require, as Rubin does, the condition that

$$\phi_1 \wedge \ldots \wedge \phi_r(\lambda) \in \mathbb{Z}[G]$$

for all $\phi_1, ..., \phi_r \in U^*_{K,S,T}$. However, the first definition is an important way of looking at the Rubin-conjectured lattice, as we also define a slightly larger lattice, called the Popescu-conjectured lattice, $\Lambda'_{K/k,S,T,r}$ via

$$\left\{ \lambda \in \left(\mathbb{Q} \bigwedge_{\mathbb{Z}[G]}^{r} U_{K,S,T} \right)_{r,S} \middle| \ \phi_1 \wedge \ldots \wedge \phi_{r-1}(\lambda) \in U_{K,S,T}, \ \forall \ \phi_1, \ldots, \phi_{r-1} \in U^*_{K,S} \right\}.$$

As usual, we will suppress many of the subscripts when then are not relevant. If no T is indicated, then $T = \emptyset$.

Lemma 2.7.4. *(i)* $\mathbb{C}\Lambda_{S,T} = \mathbb{C}\Lambda'_{S,T} = \left(\mathbb{C} \bigwedge^r_{\mathbb{Z}[G]} U_{K,S}\right)_{r,S}$

Proof. This is immediate, as all the unit groups considered are of finite index in $U_{K,S}$, and all are supported on the same χ-eigenspaces. $\square$

Chapter 3

The conjectures

As in the previous chapter, K/k is an abelian extension of number fields.

Definition 3.0.5. *We call a set S* appropriate *for the extension K/k if it is a non-empty finite set of places of k which*

(i) contains all infinite places of k, and

(ii) contains all places ramifying in K/k.

Further we call a pair of sets (S, T) appropriate *for the extension K/k if S is appropriate for K/k, T and S are disjoint, and $U_{K,S,T}$ is $\mathbb{Z}$-torsion-free.*

We remind the reader that the last condition is not at all hard to satisfy; recall Lemma 2.5.2.

The philosophy of the conjectures we shall be investigating is summarized in the following diagram. We have two objects, which are isomorphic as $\mathbb{C}[G]$-modules:

$$\begin{array}{ccc} \left(\mathbb{C} \bigwedge_{\mathbb{Z}[G]}^{r} U_{K,S,T}\right)_{r,S} & \xrightarrow{\cong} & (\mathbb{C}[G])_{r,S} \\ \epsilon_{K/k,S,T} & \leftrightsquigarrow & \frac{1}{r!}\Theta_{S,T}^{(r)}(0). \end{array}$$

On the right-hand side we have a natural analytically-defined object $\Theta_{S,T}(s)$. We pull a special value of this object back through the regulator map to arrive at an object which is of an arithmetic flavor, the Rubin-Stark evaluator $\epsilon_{S,T}$. One then asks that this evaluator have good arithmetic properties, which we force by asking it to be in some $\mathbb{Z}[G]$-sublattice. The same idea is used for both the *standard* and the *extended* conjectures, the main difference is that (as we saw in the previous chapter) the regulator has a simpler description under the presence of enough splitting primes.

3.1 Statements of the conjectures

There are five conjectures we will mention. The first is Stark's Main Conjecture for minimal order of vanishing; following the literature we call this conjecture A. Next is the standard Rubin conjecture, B and the standard Popescu conjecture, C. Finally comes the *extended* conjecture $\widetilde{B}$ with Rubin's lattice, and that with Popescu's lattice, $\widetilde{C}$. Consult the introductory chapter for the history of these conjectures.

CONJECTURE $A(K/k, S, r)$ (STARK'S RATIONALITY CONJECTURE):

Suppose S is appropriate for K/k. Then $\varepsilon_{K/k,S,r}$, which a priori *is only an element* *of* $\mathbb{C}\Lambda_S$*, is actually an element of* $\mathbb{Q}\Lambda_S$*.*

CONJECTURE $B(K/k, S, T, r)$ (The standard Rubin conjecture):

Suppose (S, T) *is appropriate for* K/k*,* S *contains at least* r *primes which split completely in* K/k *and* $|S| \geq r+1$*. Then*

$$\varepsilon_{K/k,S,T,r} \in \Lambda_{S,T}.$$

CONJECTURE $C(K/k, S, r)$: (The standard Popescu conjecture):

Suppose S *is appropriate for* K/k*,* S *contains at least* r *primes which split completely in* K/k *and* $|S| \geq r+1$*. Then for all sets* T *such that* (S, T) *is appropriate,*

$$\varepsilon_{K/k,S,T,r} \in \Lambda'_{S,T}.$$

CONJECTURE $\widetilde{B}(K/k, S, T)$ (The extended conjecture, Rubin's lattice):

Let $r = \min_{\chi \in \widehat{G}} r_S(\chi)$*. Suppose* (S, T) *is appropriate for* K/k*,* $|S| \geq r+2$*, and* $S \neq S_{\min}$*. Then*

$$\epsilon_{K/k,S,T} \in \Lambda_{S,T}.$$

CONJECTURE $\widetilde{C}(K/k, S)$ (The extended conjecture, Popescu's lattice):

Let $r = \min_{\chi \in \widehat{G}} r_S(\chi)$*. Suppose* S *is appropriate for* K/k*,* $|S| \geq r+2$*, and* $S \neq S_{\min}$*. Then for all sets* T *such that* (S, T) *is appropriate,*

$$\epsilon_{K/k,S,T} \in \Lambda'_{S,T}.$$

Throughout this dissertation we usually focus on the relationship between B and $\widetilde{B}$, and content ourselves to make passing reference to $\widetilde{C}$, primarily when it differs from $\widetilde{B}$. The phrase *extended conjecture* refers to $\widetilde{B}$. Many results proven for $\widetilde{B}$ can be directly exported to $\widetilde{C}$.

One may wonder about the slightly artificial-seeming hypothesis in $\widetilde{B}$ and $\widetilde{C}$ that $|S| \geq r+2$. In the previous chapter, we used this convention to make sure that the trivial character vanished to order greater than r and to thereby define the regulator $\mathcal{R}$. In truth, the restriction on the size of S need not be there at the price of introducing a more complicated regulator. However, we do not really gain anything from its removal. This is shown by the following

Lemma 3.1.1. *If S is an r-cover for $\widehat{G}$ and $|S| = r+1$, then S contains at least r primes that split completely in K/k.*

Proof. We begin with the formula from Lemma 2.4.2, and the fact that $r \leq r_S(\chi)$ for all χ to get

$$r(|G|-1) \leq \sum_{v \in S} (g_v - 1).$$

Now suppose, for the sake of contradiction, that S contained two primes v_1, v_2 which did not split completely in K/k. That is to say $g_{v_1}, g_{v_2} < |G|$ (where g_v represents the number of primes of K dividing v), and hence (as g_v divides $|G|$), $\frac{g_{v_i}-1}{|G|-1} < \frac{1}{2}$ for $i = 1, 2$. Then we have

$$r \leq \sum_{v \in S} \frac{g_v - 1}{|G|-1} < \frac{1}{2} + \frac{1}{2} + (r-1) = r,$$

a contradiction. Therefore such v_1 and v_2 do not exist, and at least r primes of S split in K/k. □

This lemma says that if $|S| = r+1$ we satisfy the hypothesis of the standard

Rubin conjecture, and so need not do any extra work to specify an extended conjecture in this case.

On the other hand, the condition $S \neq S_{\min}$ is completely nontrivial. Indeed there are computational examples of number field extensions K/k and sets S and T such that all hypotheses of $\widetilde{B}(K/k,S,T)$ are satisfied except $S \neq S_{\min}$, but $\epsilon_{K/k,S,T} \notin \Lambda_{S,T}$. These examples, due to Dummit and Hayes, occur even in the first order case, $r_S(K/k) = 1$ (see [Eri05, Section 4.2] for an exposition). We shall discuss this situation further in Section 5.4.

When considering $\widetilde{B}(K/k,S,T)$ as distinct from $B(K/k,S,T,r)$, one assumes K/k to be a non-cyclic extension. The is because of the

Lemma 3.1.2. *If K/k is cyclic, then $\widetilde{B}(K/k,S,T)$ is equivalent to $B(K/k,S,T,r)$ where $r = r_S(K/k)$.*

Proof. Suppose K/k is cyclic. We must show that if S is an r-cover for K/k then S contains at least r primes which split completely. So suppose S is an r-cover for K/k. Let χ be a faithful character (which exists because G is cyclic). We know at least r primes split in $K^{\ker\chi}/k$. But $K^{\ker\chi} = K$. The next section will show that $\epsilon_{K/k,S,T} = \varepsilon_{K/k,S,T,r}$ in this situation. □

Corollary 3.1.3. *For any number field k, the conjecture $\widetilde{B}(k/k,S,T)$ is true.*

Proof. Since $B(k/k,S,T,r)$ is known, this is immediate, as k/k is cylic! □

3.2 Relationships between evaluators

One relationship for the standard evaluators is detailed in the following proposition.

Proposition 3.2.1. *For any tower of extensions $K/M/k$, appropriate sets (S,T) and integer j,*

$$\varepsilon_{M/k,S,T,j} = N^{(r)}_{K/M}\varepsilon_{K/k,S,T,j}.$$

This result, though a simple consequence of the behaviour of the regulator maps under change of fields, is important in the construction of Euler systems from the conjectures. For details, see [Rub96] or [Pop04]. It will also prove invaluable when proving relationships among the extended evaluators.

We can link the standard evaluators and the extended evaluators. Suppose S is an r-cover for the extension K/k (and that $|S| > r+1$). The idea is that although there may not be r primes that split in the full extension K/k, if one picks a character $\chi \in \widehat{G}$ then there are at least r primes that split in a certain canonical subextension associated to χ. Specifically:

Definition 3.2.2. *For any $\chi \in \widehat{G}$, let*

$$K_\chi := K^{\ker\chi},$$

$$G_\chi := \ker\chi$$

and

$$\Gamma_\chi := G/G_\chi \cong G(K_\chi/k).$$

We put $r = \min_{\chi\in\widehat{G}} r_S(\chi)$. In the (cyclic) extension K_χ/k there are exactly $r_S(\chi) \geq r$ primes of S that split completely (see the remark after Definition 2.3.2). If there are strictly more than r, the Rubin-Stark evaluator $\varepsilon_\chi = \varepsilon_{K_\chi/k,S,T,r}$ is trivial, otherwise it is a nontrivial element of $\mathbb{C}\bigwedge^r_{\mathbb{Z}[\Gamma_\chi]} U_{K_\chi,S,T}$.

Theorem 3.2.3. *Suppose* $|S| > r+1$. *Let*

$$\epsilon_{K/k} = \sum_{\chi\in\widehat{G}} \frac{1}{|G_\chi|^r}\mathbf{e}_\chi\varepsilon_\chi. \tag{3.1}$$

Then $\epsilon_{K/k}$ *is the* extended *Rubin-Stark evaluator for the extension* K/k.

Proof. We need to show that $\mathcal{R}_{K/k,S}(\epsilon_{K/k}) = \frac{1}{r!}\Theta^{(r)}_{K/k,S,T}(0)$. We do this one character at a time.

Indeed,

$$\begin{aligned}
\mathcal{R}_{K/k,S}(\epsilon_{K/k})\mathbf{e}_\chi &= \sum_{I\in\mathcal{P}_r(S_{\min})} R_{w_I}(\epsilon_{K/k})\mathbf{e}_\chi && \text{(Theorem 2.3.12)}\\
&= \sum_{I\in\mathcal{P}_r(S_{\min})} \frac{1}{|G_\chi|^r} R_{w_I}(\varepsilon_{K_\chi/k,S,T,r})\mathbf{e}_\chi && \text{(Linearity of regulator)}
\end{aligned}$$

Now if $\chi \in \widehat{G}$ is such that $r_S(\chi) > r$ then

$$\varepsilon_{K_\chi/k,S,T,r} = 0 = \frac{1}{r!}\Theta^{(r)}_{K/k,S,T}(0)\mathbf{e}_\chi.$$

So hereafter suppose that $r_S(\chi) = r$. In the summation above, there are two cases. If I does not consist of exactly the r primes that split in K_χ/k then let $v_1 \in I$ be one such prime with the decomposition group $D = (\Gamma_\chi)_{v_1} \neq \{1\}$, and $v_2, ..., v_r$ be the other primes in I, and fix primes of K_χ, $\text{II}_i|v_i$. We are going to show that the piece of the regulator corresponding to I is zero, by a standard method when dealing with characters. We provide the details so one can see how the various objects are linked at the levels of the different fields. By the definition of Γ_χ, there is a character $\widetilde{\chi} \in \widehat{\Gamma_\chi}$ with trivial kernel in Γ_χ such that $\chi = \widetilde{\chi} \circ \pi$. Then

$$\begin{aligned}
R_{\mathrm{II}}(\varepsilon_\chi)\mathbf{e}_{\widetilde{\chi}} &= R_{\mathrm{II}_1 \wedge \ldots \wedge \mathrm{II}_r}(\varepsilon_\chi)\mathbf{e}_{\widetilde{\chi}} \\
&= \frac{1}{|\Gamma_\chi|} \sum_{\gamma \in \Gamma_\chi} \widetilde{\chi}(\gamma^{-1}) R_{\mathrm{II}_1^\gamma \wedge \ldots \wedge \mathrm{II}_r}(\varepsilon_\chi) \\
&= \frac{1}{|\Gamma_\chi|} \sum_{\overline{\gamma} \in \Gamma_\chi / D} \left(\sum_{\beta \in D} \widetilde{\chi}(\beta) \right) R_{\mathrm{II}_1^{\overline{\gamma}} \wedge \ldots \wedge \mathrm{II}_r}(\varepsilon_\chi) \\
&= 0.
\end{aligned}$$

The last equality holds because $\widetilde{\chi}$ has trivial kernel, while D is nontrivial. However

$$R_{w_I}(\varepsilon_\chi)\mathbf{e}_\chi = \Psi_{K/K_\chi}(R_{\mathrm{II}}(\varepsilon_\chi)\mathbf{e}_{\widetilde{\chi}}) = 0$$

where Ψ is the map whose properties were outlined in Lemma 2.3.14.

It follows that only the set I consisting of the primes splitting in K_χ/k survives, and

$$\mathcal{R}_{K/k,S}(\epsilon_{K/k})\mathbf{e}_\chi = \tfrac{1}{|G_\chi|^r} R_{w_1^\chi \wedge \ldots \wedge w_r^\chi}(\varepsilon_\chi)\mathbf{e}_\chi, \tag{3.2}$$

where $W = w_1^\chi \wedge \ldots \wedge w_r^\chi$ consists of arbitrarily chosen primes of K above the r primes of k that split in K_χ/k.

However, according to the proof of Proposition 2.3.13, if π is the natural projection,

$$\pi_{K/K_\chi} R_{w_1^\chi \wedge \ldots \wedge w_r^\chi}(\varepsilon_\chi) = R_{\mathrm{II}_1^\chi \wedge \ldots \wedge \mathrm{II}_r^\chi}(N^{(r)}_{K/K_\chi} \varepsilon_\chi) = |G_\chi|^r R_{\mathrm{II}_1^\chi \wedge \ldots \wedge \mathrm{II}_r^\chi}(\varepsilon_\chi). \tag{3.3}$$

(Here $\amalg_i^\chi$ is the prime of M that lies below w_i^χ.) We need the map $\Psi = \Psi_{K/K_\chi}$ whose properties were introduced in Lemma 2.3.14. We compute—

$$\begin{aligned}
\mathcal{R}_{K/k,S}(\epsilon_{K/k})\mathbf{e}_\chi &= \frac{1}{|G_\chi|^r} R_W(\varepsilon_\chi)\mathbf{e}_\chi \\
&= \frac{1}{|G_\chi|^r}\Psi \circ \pi(R_W(\varepsilon_\chi))\mathbf{e}_\chi \\
&= \frac{1}{|G_\chi|^r}\Psi(|G_\chi|^r R_{\amalg_1^\chi \wedge \ldots \wedge \amalg_r^\chi}(\varepsilon_\chi))\mathbf{e}_\chi \\
&= \Psi\left(\frac{1}{r!}\Theta^{(r)}_{K_\chi/k}(0)\right)\mathbf{e}_\chi \\
&= \frac{1}{r!}\left(\sum_{\psi\in\widehat{\Gamma}} L^{(r)}_{K_\chi/k,S,T}(0,\psi^{-1})\mathbf{e}_{\psi\circ\pi}\right)\mathbf{e}_\chi \\
&= \frac{1}{r!}L^{(r)}_{K/k,S,T}(0,\chi^{-1})\mathbf{e}_\chi \\
&= \frac{1}{r!}\Theta^{(r)}_{K/k,S,T}(0)\mathbf{e}_\chi
\end{aligned}$$

The first equality is equation (3.2), the second holds because $R_W(\varepsilon_\chi)$ is fixed by G_χ, the third is equation (3.3), the fourth is the evaluation property of ε_χ, the fifth is the definition of $\Theta_{K_\chi/k}$ and Lemma 2.3.14*(iii)*, the sixth is the Inflation Property of Artin L-functions combined with the fact that $\mathbf{e}_\chi$ is an idempotent, and the seventh is the definition of $\Theta_{K/k}$.

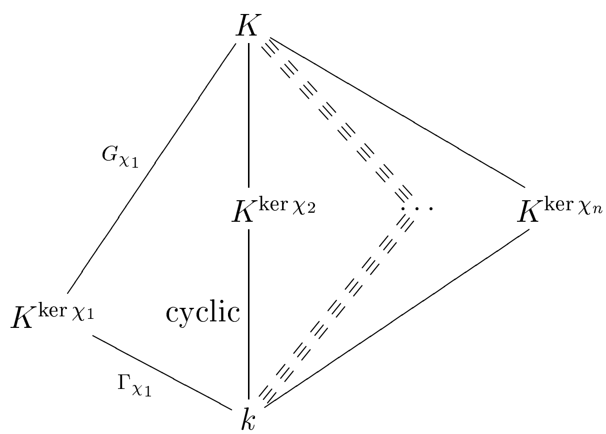
Since we have shown the two values we wish are equal on every $\mathbf{e}_\chi$-component of $\mathbb{C}[G]$, they must be equal. □

Remark: Throughout this dissertation, we are using the fact that, for $M = K^H$ we have an embedding of $\mathbb{C}[G]$-modules

$$\mathbb{C}\bigwedge_{\mathbb{Z}[\Gamma]}^{r} U_{M,S,T} \hookrightarrow \mathbb{C}\bigwedge_{\mathbb{Z}[G]}^{r} U_{K,S,T}$$

to consider the module on the left as a submodule of that on the right and are suppressing any cumbersome notation that might be used such as $\wedge^r \iota_{K/M}$.

The meat of formula (3.1) is that it allows us to realize the evaluator for the full extension K/k as a $\mathbb{C}[G]$-linear combination of evaluators coming from cyclic subextensions:



Note that not all of the fields are distinct because for each subgroup $H \subseteq G$ with G/H cyclic of order c, there are exactly $\Phi(c)$ characters with $\ker \chi = H$ where $\Phi(c)$ denotes Euler's totient function.

The above description of $\epsilon_{K/k}$ is certainly very useful and does have the advantage of allowing us to reduce all calculations of Stark evaluators to the level of *cyclic* extensions of the base field k. The spirit of the Stark Conjectures, however, is to work at least "over $\mathbb{Q}$" whenever possible; i.e., we would prefer to build $\epsilon_{K/k}$ out of a $\mathbb{Q}[G]$-linear combination of evaluators arising in subextensions. The fact that we are really working "over $\mathbb{Q}$" is apparent after considering the proof of Lemma 2.3.7, and that ε_χ depends not on χ but on $\ker \chi$. The following theorem will give another formula for $\epsilon_{K/k}$ even more in the spirit of working "over $\mathbb{Q}$."

Recall $\mathcal{P}_r(S_{\min})$ consists of those subsets of $S_{\min}$ of cardinality exactly r. For each $I \in \mathcal{P}_r(S_{\min})$, we set up the following notation.

Definition 3.2.4. *First*

$$D_I = \langle G_v \mid v \in I \rangle,$$

is the subgroup of G generated by the decomposition groups of the primes in I. Put

$$M_I = K^{D_I}.$$

Let ε_I be the Rubin-Stark evaluator corresponding to the standard Rubin conjecture $B(M_I/k, S, T, r)$. (Notice that ε_I may be zero if yet more primes of S split in M_I/k; and M_I is the largest subextension of K/k in which all the primes in I split completely.)

Theorem 3.2.5. *The extended Rubin-Stark evaluator for K/k is*

$$\epsilon_{K/k} = \sum_{I \in \mathcal{P}_r(S_{\min})} \frac{1}{|D_I|^r} \varepsilon_I$$

Proof. For any I, we compute

$$\begin{aligned} \tfrac{1}{|D_I|^r}\varepsilon_I &= \frac{1}{|D_I|^r}\frac{N_{D_I}}{|D_I|}\varepsilon_I \\ &= \frac{1}{|D_I|^r} \sum_{\substack{\chi \in \widehat{G} \\ D_I \subseteq \ker\chi}} \mathbf{e}_\chi \varepsilon_I \\ &= \frac{1}{|D_I|^r} \sum_{\substack{\chi \in \widehat{G} \\ D_I \subseteq \ker\chi}} \mathbf{e}_\chi \frac{N^{(r)}_{M_I/K_\chi}}{(\ker\chi : D_I)^r} \varepsilon_I \\ &= \sum_{\substack{\chi \in \widehat{G} \\ D_I \subseteq \ker\chi}} \frac{1}{|\ker\chi|^r} \mathbf{e}_\chi \varepsilon_\chi \end{aligned}$$

where the first equality holds because elements of D_I fix ε_I, the second is equation (2.4), the third holds because $\chi(N_{M_I/K_\chi}) = (\ker\chi : D_I)$ for those χ which contain D_I in their kernel, and the last is Proposition 3.2.1.

Therefore

$$\sum_{I\in\mathcal{P}_r(S_{\min})} \frac{1}{|D_I|^r}\varepsilon_I = \sum_{\chi\in\widehat{G}} \frac{n_\chi}{|\ker\chi|^r}\mathbf{e}_\chi\varepsilon_\chi$$

where

$$\begin{aligned} n_\chi &= \#\{I\in\mathcal{P}_r(S_{\min}) | D_I \subseteq \ker\chi\} \\ &= \#\{I\in\mathcal{P}_r(S_{\min}) \text{ and for all } v\in I, v \text{ splits in } K_\chi\} \\ &\begin{cases} = 1 & \text{if } \chi \text{ is relevant,} \\ > 1 & \text{otherwise.} \end{cases} \end{aligned}$$

However, when $n_\chi > 1$ we have more than r primes which split in K_χ/k and $\varepsilon_\chi = 0$ by definition. The proof concludes by Theorem 3.2.3. □

3.3 Varying S and T in the conjectures

Suppose we know $\widetilde{B}(K/k,S,T)$ is true and we wish to increase the set T to some $T' \supseteq T$. What can be said?

The first thing to notice is that for either the standard or extended conjecture,

$$\epsilon_{K/k,S,T\cup\{v\}} = (1-\sigma_v^{-1}Nv)\cdot\epsilon_{K/k,S,T}$$

which follows from differentiating the equation

$$\Theta_{K/k,S,T\cup\{v\}}(s) = (1-\sigma_v^{-1}Nv^{1-s})\cdot\Theta_{K/k,S,T}(s).$$

r times, dividing by $r!$, and evaluating at $s = 0$. For this reason we introduce the notation (for any finite set of unramified places $\mathcal{T}$)

$$\delta_{\mathcal{T}} = \prod_{v \in \mathcal{T}} (1 - \sigma_v^{-1} Nv).$$

The following proposition is proven for conjecture B instead of $\widetilde{B}$ in [Pop02, Proposition 5.3.1]. However, as the statement really only concerns the lattices Λ_T and $\Lambda_{T'}$ and the fact that $\epsilon_{S,T'} = \delta_{T' \setminus T} \cdot \epsilon_{S,T}$, the identical proof also works for the extended conjecture.

Proposition 3.3.1. *If $T \subseteq T'$, then $\widetilde{B}(K/k, S, T) \Rightarrow \widetilde{B}(K/k, S, T')$.*

This is all that can be said of functoriality in T, as the opposite implication is currently not known and indeed will likely never be proven directly but will only follow from already knowing the truth of $\widetilde{B}(K/k, S, T)$. (The $\delta_{\mathcal{T}}$'s, though invertible in $\mathbb{Q}[G]$, pick up large denominators upon inversion, anathema to knowing that the new epsilon lies in any given lattice.)

The situation of functoriality of $\widetilde{B}$ in S is much more subtle than that of functoriality in T. Indeed it is even more subtle than the functoriality of the standard conjecture B in S. In the standard conjecture, one breaks the situation into four cases: adding/subtracting a totally split/non-totally split prime from S. However, upon considering the extended conjecture, one sees that the cases are really about whether the minimal order of vanishing r decreases, stays the same, or increases.

First we review the functoriality in S of the standard conjectures. The easiest case is when one is adding a prime to S which does not split completely in the extension K/k.

Proposition 3.3.2. *If $v \notin S \cup T$ is a prime of k that* does not *split completely in K/k, then $B(K/k, S, T, r) \Rightarrow B(K/k, S \cup \{v\}, T, r)$ and*

$$\varepsilon_{K/k,S\cup\{v\},T,r} = (1 - \sigma_v^{-1})\varepsilon_{K/k,S,T,r}.$$

Proof. The second fact is all we need to prove, as the first will then follow immediately. But the second is a consequence of the equation

$$\Theta_{K/k,S\cup\{v\},T}(s) = (1 - \sigma_v^{-1} Nv^{-s})\Theta_{K/k,S,T}(s).$$

As above, one differentiates r times, divides by $r!$, and evaluates at $s = 0$ (using the fact that $\Theta^{(j)}_{K/k,S,T}(0) = 0$ for $j < r$). Of course the Frobenius σ_v exists because S may be assumed to be appropriate and therefore contains all the unramified primes. □

On the other hand, when removing a prime from S that does not split completely to get $S' = S \setminus \{v_0\}$, the truth of the conjecture with S *does not* imply the truth of the conjecture with S'. (Of course if v_0 is an infinite or ramifying prime the hypotheses of the conjecture are not even satisfied anymore.)

What about splitting primes? It turns out one can always *remove* a split prime and the truth of the conjecture will stay the same.

Proposition 3.3.3. *If $r > 0$ and $v_1 \in S$ is a prime that splits completely in K/k then*

$$B(K/k, S, T, r) \Longrightarrow B(K/k, S \setminus \{v_1\}, T, r - 1).$$

The following gives a partial answer to the question of *adding* a split prime. The condition that the evaluator be in a certain Fitting ideal times $\Lambda_{S,T}$ is stronger than $B(K/k, S, T, r)$, which only requires that the evaluator be in $\Lambda_{S,T}$ itself.

Proposition 3.3.4. *If $v \notin S \cup T$ is a prime that splits completely in K/k, and $\varepsilon_{K/k,S,T,r} \in \mathrm{Fitt}_{\mathbb{Z}[G]}(\langle [v]_{K,S,T} \rangle)\Lambda_{S,T}$ then $B(K/k, S \cup \{v\}, T, r+1)$ is true.*

Proof. See [Rub96, Theorem 5.3(iii)]. □

There are extra complications when it comes to the extended conjecture $\widetilde{B}$. The difficulty is that if one adds a prime $S' = S \cup \{v\}$, the minimal order of vanishing may increase even if v does not split completely. In this case the leading terms of more L-functions may enter the picture, as the following example illustrates.

Example 3.3.5. *Let $K = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and $k = \mathbb{Q}$. Suppose $S = \{\infty, 2, 3, 17\}$. If the character group $\widehat{G}$ consists of $\chi_0, \chi_1, \chi_2, \chi_3$ with fixed fields $\mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ respectively, then the orders of vanishing are*

$$\begin{aligned} r_S(\chi_0) &= 3 \\ r_S(\chi_1) &= 1 \\ r_S(\chi_2) &= 2 \\ r_S(\chi_3) &= 2. \end{aligned}$$

But if we put $S' = S \cup \{p\}$ where p is any rational prime congruent to $5 \pmod 8$, then p will split in $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ (and $\mathbb{Q}/\mathbb{Q}$) but remain inert in the other two fixed *fields. The new orders of vanishing would be*

$$\begin{aligned} r_{S'}(\chi_0) &= 4 \\ r_{S'}(\chi_1) &= 2 \\ r_{S'}(\chi_2) &= 2 \\ r_{S'}(\chi_3) &= 2, \end{aligned}$$

and hence the minimal order of vanishing jumps from $r_S(K/k) = 1$ *to* $r_{S'}(K/k) = 2$. *Moreover, while* $\Theta_S^{(1)}(0)$ *encodes information only about the L-function attached to* χ_1, $\Theta_{S'}^{(2)}(0)$ *encodes information about the three L-functions attached to the nontrivial characters* χ_1, χ_2 *and* χ_3. *Hence we cannot express* $\epsilon_{K/k,S'}$ *merely in terms of* $\epsilon_{K/k,S}$.

The author is currently working on a theory in which the leading terms of all L-functions (not just those of minimal order of vanishing) are encoded into an evaluator. Upon adding a prime into S, this new evaluator behaves in a well-understood manner, which gives hope for proving an analogue of Proposition 3.3.4 in this situation.

3.4 Main investigation of this dissertation

The extended conjectures seem perhaps more natural in that the vanishing of the L-functions is not forced by adding split primes, but rather just arises "like a mist off the ocean." The standard conjectures do not predict anything nontrivial with many arbitrarily chosen extentions K/k and sets S. What will often happen is that S will contain some number j of split primes, while all the L-functions vanish to order greater than j due to the other primes in S. The extended conjectures, however, are always nontrivial.

It is natural to ask what the link between the standard and extended conjectures is. Are they "equivalent" in some sense? And if so, in what sense precisely? Already we have seen some links between the evaluator $\epsilon_{K/k}$ that arises in the extended conjecture and standard evaluators that arise in certain subextensions of K/k (c.f. Theorems 3.2.3 and 3.2.5).

In this section we will present a theorem, which partially answers the questions.

Theorem 3.4.1. *If $\widetilde{B}(K/k, S, T)$ is true and r is the associated minimal order of vanishing, then for any field M such that $K \supseteq M \supseteq k$ the standard conjecture $B(M/k, S, T, r)$ is true.*

Proof. Fix such an M and put $H = G(K/M)$. If less than r primes split in M/k then $B(M/k, S, T, r)$ is vacuously true: the hypotheses are not satisfied. If $|S| = r+1$, conjectures $\widetilde{B}(K/k, S, T)$ and $B(K/k, S, T, r)$ are equivalent by Lemma 3.1.1, and the theorem follows from the natural behavior of conjecture B under change of top field. So we may assume $|S| \geq r+2$. If more than r primes of S split completely in M/k then $B(M/k, S, T, r)$ is trivially true with $\varepsilon_{M/k,S,T,r} = 0$, since $|S| \geq r+2$. So assume that exactly r primes of S split completely in M/k.

Let $\epsilon_{K/k}$ be the extended Rubin-Stark evaluator for K/k. We calculate

$$\begin{aligned} N_H^{(r)}\epsilon_{K/k} &= N_H^{(r)} \sum_{\chi\in\widehat{G}} \frac{1}{|\ker\chi|^r}\mathbf{e}_\chi \varepsilon_\chi \\ &= \sum_{\substack{\chi\in\widehat{G} \\ H\subseteq\ker\chi}} \frac{|H|^r}{|\ker\chi|^r}\mathbf{e}_\chi N_{M/K_\chi}^{(r)} \varepsilon_{M/k} \\ &= \frac{N_H}{|H|}\varepsilon_{M/k} \\ &= \varepsilon_{M/k}. \end{aligned}$$

The first equality is Theorem 3.2.3, the second is the fact that in the group ring $\mathbb{C}[G]$,

$$N_H \mathbf{e}_\chi = \begin{cases} |H|\mathbf{e}_\chi & \text{if } H\subseteq \ker\chi \\ 0 & \text{otherwise} \end{cases}$$

and $\varepsilon_\chi = N_{M/K_\chi}^{(r)}\varepsilon_{M/k}$ (see Proposition 3.2.1), the third is equation (2.4), and finally the fourth is simply that every element of H acts trivially on $\varepsilon_{M/k}$.

Now take $\varphi_1, \ldots, \varphi_r \in U_{M,S,T}^*$. Pick $\phi_1, \ldots, \phi_r \in U_{K,S,T}^*$ such that $N_{K/M}^*\phi_i = \varphi_i$ (we can do this by Lemma 2.5.5 because we are working under the hypothesis that $\mu_{K,T} = \{1\}$).

We compute (using Lemma 2.5.6),

$$\begin{aligned} (\varphi_1\wedge\ldots\wedge\varphi_r)(\varepsilon_{M/k}) &= (\varphi_1\wedge\ldots\wedge\varphi_r)(N_{K/M}^{(r)}\epsilon_{K/k}) \\ &= \pi_{K/M}\Big((\phi_1\wedge\ldots\wedge\phi_r)(\epsilon_{K/k})\Big) \\ &\in \pi_{K/M}\mathbb{Z}[G] = \mathbb{Z}[\Gamma] \end{aligned}$$

□

Note we can also prove the above theorem for Popescu's lattice $\Lambda'_{S,T}$ only with the triviality of $\widehat{\mathrm{H}}^1(G(K/M), \mu_{K,T})$ (which we used in applying Lemma 2.5.5).

Corollary 3.4.2. *If $S_{\min}$ contains only primes which split completely, then $\widetilde{B}$ is equivalent to B.*

Proof. Simply take $M = K$ in the previous Theorem. □

We wish to also prove results in the other direction: when does knowing the truth of the standard conjectures imply the truth of the extended conjectures? One main reason we wish for such an implication is that the standard conjectures are known in many cases, and thus we may prove the extended conjecture in this manner. However, at this time we cannot prove such an implication in general. Several special cases are taken care of in the course of the remaining chapters. (See in particular Theorem 5.1.1.) Of course, we have almost done enough work to prove the next two propositions, which are weak converses.

Proposition 3.4.3. *Let $r = r_S(K/k)$ be the minimal order of vanishing. If $B(M_I/k, S, T, r)$ is true for all $I \in \mathcal{P}_r(S_{\min})$, then*

$$\epsilon_{K/k,S,T} \in \frac{1}{|G|}\Lambda_{S,T},$$

i.e., $\widetilde{B}(K/k, S, T)$ is true up to factor of $|G| = [K : k]$.

Proof. Let $\phi = \phi_1 \wedge \ldots \wedge \phi_r \in \bigwedge^r_{\mathbb{Z}[G]} U^*_{K,S,T}$. Note that Lemma 2.5.6 combined with the fact that $\varepsilon_{M/k}$ is fixed by $H = G(K/M)$ yield

$$\begin{aligned}\phi\left(\frac{1}{[K:M]^r}\varepsilon_{M/k}\right) &= \frac{1}{[K:M]^r}\Psi_{K/M}\pi_{K/M}\phi(\varepsilon_{M/k}) \\ &= \frac{1}{[K:M]^r}\Psi_{K/M}((N^*_{K/M})^{(r)}\phi)(N^{(r)}_{K/M}\varepsilon_{K/M}) \\ &= \Psi_{K/M}((N^*_{K/M})^{(r)}\phi)(\varepsilon_{K/M}) \\ &\in \Psi_{K/M}\mathbb{Z}[\Gamma] \subseteq \frac{1}{[K:M]}\mathbb{Z}[G].\end{aligned}$$

Now we apply this computation repeatedly with $M = M_I$ for each $I \in \mathcal{P}_r(S_{\min})$ to the formula Theorem 3.2.5 to obtain the result. (Noting of course that $|D_I| = [K : M_I]$, both of which divide $|G|$.) ☐

Proposition 3.4.4. *Let $r = r_S(K/k)$ be the minimal order of vanishing. If $B(K^{\ker\chi}/k, S, T, r)$ is true for all $\chi \in \widehat{G}_{r,S}$, then*

$$\epsilon_{K/k,S,T} \in \frac{1}{|G|}\Lambda_{S,T},$$

i.e., $\widetilde{B}(K/k, S, T)$ is true up to factor of $|G| = [K : k]$.

Proof. The proof is identical to that of the previous Proposition; one simply examines the pieces of $\epsilon_{K/k}$ coming from $K^{\ker\chi}$ and uses Theorem 3.2.3 instead of Theorem 3.2.5. ☐

Finally we notice that the conjecture $\widetilde{B}$ also acts naturally under change of top field:

Proposition 3.4.5. *If M is a field intermediate between K and k and the minimal order of vanishing remains constant $r_S(M/k) = r_S(K/k)$, then*

$$N^{(r)}_{K/M}(\epsilon_{K/k}) = \epsilon_{M/k}.$$

Proof. Fix $H \subseteq G$ as the Galois group of K/M. Let ψ be a character of $\Gamma = G(M/k) = G/H$. Note that under the identification $\mathbb{Z}[\Gamma] \cong \mathbb{Z}[G]^H = N_H\mathbb{Z}[G]$,

$$\mathbf{e}_\psi = \sum \mathbf{e}_\chi, \tag{3.4}$$

where the summation runs over all $\chi \in \widehat{G}$ for which $H \subseteq \ker\chi$ and $\widetilde{\chi} = \psi$. (Here $\widetilde{\chi}$ denotes the map induced by χ after we mod out its domain by H.)

Then

$$\begin{aligned}
N^{(r)}_{K/M}\epsilon_{K/k} &= \left(|H|^r \sum_{H\subseteq \ker\chi} \mathbf{e}_\chi\right)\epsilon_{K/k} \\
&= \sum_{H\subseteq\ker\chi}\left(\frac{|H|}{|\ker\chi|}\right)^r \mathbf{e}_\chi \varepsilon_{K_\chi/k} \\
&= \sum_{\psi\in\widehat{\Gamma}}\left(\sum_{\substack{H\subseteq\ker\chi \\ \widetilde{\chi}=\psi}} \mathbf{e}_\chi\right)\frac{1}{|\ker\psi|^r}\varepsilon_{M_\psi/k} \\
&= \sum_{\psi\in\widehat{\Gamma}}\frac{1}{|\ker\psi|^r}\mathbf{e}_\psi\varepsilon_{M_\psi/k} \\
&= \epsilon_{M/k}.
\end{aligned}$$

(We have used the fact that if $\widetilde{\chi} = \psi$, then $|\ker\psi| = \frac{|\ker\chi|}{|H|}$ and $K_\chi = M_\psi$.) The hypothesis that $r_S(K/k) = r_S(M/k)$ was used in that $\varepsilon_{M_\psi/k}$ denotes $\varepsilon_{M_\psi/k,S,T,r}$ and we are raising the coefficients to the correct power to apply Theorem 3.2.3 and achieve $\epsilon_{M/k}$ in the last equality. □

Corollary 3.4.6. *If $r_S(M/k) = r_S(K/k)$, then*

$$\widetilde{B}(K/k,S,T) \Longrightarrow \widetilde{B}(M/k,S,T).$$

Proof. This result follows directly from the previous proposition, applying the computation at found at end of the proof of Theorem 3.4.1. □

Chapter 4

Multiquadratic extensions

Since we are not able to prove the equivalence of the standard and extended conjectures in the most general case, we attack subcases. One key case in which Popescu's and Rubin's conjectures, $C(K/k, S, r)$ and $B(K/k, S, T, r)$, are known is when K/k is a relative quadratic extension, i.e. an extension of relative degree two. This is due to work of Stark, Tate, and Rubin (see in particular [Tat84] Théorème IV.5.4 and [Rub96] Theorem 3.5). There has been work on extending this result to arbitrary multiquadratic extensions in [DST03, San04]. The multiquadratic *extended* conjecture in the case $r = 1$ was tackled in [Eri05].

Definition 4.0.7. *By a* multiquadratic extension *of rank m we mean an (abelian) Galois extension of number fields K/k such that $G = G(K/k) \cong (\mathbb{Z}/2\mathbb{Z})^m$.*

In this chapter we mirror much of Sands [San04] work toward proving Popescu's conjecture C in multiquadratic extensions, working instead with T-modified units, class groups, etc., and trying to get a handle on Rubin's conjecture B and the extended conjecture $\widetilde{B}$.

We note that G can be thought of as an m-dimensional vector space over the finite field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Intermediate fields are in one-to-one correspondence with subspaces of G. Intermediate relative quadratic extensions M/k are in one-to-one correspondence with $(m-1)$-dimensional subspaces $G_M := G(K/M) \subseteq G$. These subspaces occur naturally as the kernels of the character group of $\widehat{G}$ of G. So for this group we have a nice canonical isomorphism between $\widehat{G}$ and G that simply sends $\chi \in \widehat{G}$ to the nonzero element of $(\ker \chi)^{\perp}$.

Let M be such an intermediate relative quadratic extension of k. We shall denote the Galois group $G(M/k)$ as $\Gamma_M = \{1, \tau_M\}$, and omit the subscripts if M is fixed. Recall $A_{M,S,T}$ is the (S,T)-modified ideal class group: the quotient of the set of fractional ideals of M that are prime to S_M and T_M by the subgroup consisting of principal ideals that have a generator that is prime to S_M and congruent to 1 modulo all primes in T_M (and similarly for $A_{k,S,T}$). There is a well-defined map $A_{k,S,T} \xrightarrow{\iota} A_{M,S,T}$ induced by lifting an ideal in k to M. (Of course ι depends on M, but we suppress this from the notation, as the field M is usually apparent.)

Throughout this chapter, we fix $r := r_S(K/k)$ as the minimal order of vanishing for K/k.

Definition 4.0.8. *We call a quadratic extension M/k* relevant *if M is contained in K and exactly r primes of S split in M/k.*

We work under our standing assumption that $|S| > r+1$, in which case these quadratic extensions are the only ones for which $\varepsilon_{M/k,S,T} \neq 0$.

The main tool we will use in this chapter is the following theorem.

Theorem 4.0.9. *Suppose K/k is a multiquadratic extension of rank m and for every relevant quadratic extension M/k the following inequality is satisfied*

$$|S| - r + \mathrm{ord}_2|A_{M,S,T}/\iota A_{k,S,T}| \geq m + 1. \tag{4.1}$$

Then the extended conjecture, $\widetilde{B}(K/k, S, T)$, is true.

We will prove this theorem later in the chapter.

The group $A_{M,S,T}/\iota A_{k,S,T}$ can be unwieldly to work with, so we note that

Lemma 4.0.10. *When M/k is relevant,*

$$\mathrm{ord}_2|A_{M,S,T}/\iota A_{k,S,T}| \geq \mathrm{rk}_2(A_{k,S,T}).$$

Proof. We consider the map induced by the norm,

$$\begin{array}{ccc} A_{M,S,T}/\iota A_{k,S,T} & \xrightarrow{\mathcal{N}} & A_{k,S,T}/A^2_{k,S,T} \\ [\mathfrak{a}]_{M,S,T}\iota A_{k,S,T} & \longmapsto & [N_{M/k}\mathfrak{a}]_{k,S,T}A^2_{k,S,T}. \end{array}$$

The map is well-defined, as the norm acts by squaring on ideals of k. Since $|S| \geq r + 2$, in a relevant quadratic extension M/k, S must contain at least one prime that does not split completely in M/k. Thus $M \cap H_{k,S} = k$ where $H_{k,S}$ denotes the S-Hilbert class field of k. Therefore by class field theory, the norm map on the S-class group is surjective. □

By combining Lemma 4.0.10 with Theorem 4.0.9, we obtain the slightly weaker

Corollary 4.0.11. (Main Theorem for Multiquadratic Extensions) *Suppose K/k is a multiquadratic extension of rank m and for every relevant quadratic*

M/k the following inequality is satisfied

$$|S| - r + \mathrm{rk}_2(A_{k,S,T}) \geq m + 1. \tag{4.2}$$

Then the extended conjecture, $\widetilde{B}(K/k, S, T)$, is true.

Note that since $\widetilde{B}$ implies B (c.f. Theorem 3.4.1), we may also apply Corollary 4.0.11 to conclude the truth of B.

Example 4.0.12. *Let K/k be any multiquadratic extension of number fields of rank m, and (S, T) be appropriate for the extension. Fix a particular character of minimal order of vanishing $\chi_1 \in \widehat{G}_{r,S}$. Put $a = \mathrm{rk}_2(A_{k,S,T})$ and*

$$b = r + m + 1 - |S| - a.$$

By applying Corollary 4.0.11 we see that if $b \leq 0$ then $\widetilde{B}(K/k, S, T)$ is true. So assume that $b \geq 1$. Let

$$E = \{v_{|S|+1}, \ldots, v_{|S|+a+b}\}$$

be a set of $a + b$ primes disjoint from S and T and such that

$$\chi_1(\sigma_v) \neq 1 \tag{4.3}$$

for all $v \in E$. Such a set may be chosen by the Tchebotarev Density Theorem [Neu99, Theorem VII.13.4]. Let $S' = S \cup E$.

I claim that $\widetilde{B}(K/k, S', T)$ is true. First of all, (S', T) is clearly appropriate for K/k. Next, because of (4.3), no prime in E splits in K_{χ_1}/k and hence $r_{S'}(\chi_1) = r_S(\chi_1) = r$.

Since $|S'| = |S| + a + b$ *and* $\mathrm{rk}_2(A_{k,S',T}) \geq 0$*, it follows that*

$$\begin{aligned} |S'| - r + \mathrm{rk}_2(A_{k,S',T}) &\geq |S| + a + b - r \\ &= m + 1. \end{aligned}$$

Hence we may apply Corollary 4.0.11 to conclude the truth of $\widetilde{B}(K/k, S', T)$*.*

4.1 Finding an explicit formula for $\varepsilon_{M/k}$

The first step toward proving the theorem is to give an explicit formula for the evaluators arising in the relevant quadratic extensions. Let us remark briefly that under our hypotheses on T, $U_{M,S,T}/U_{k,S,T}$ is $\mathbb{Z}$-torsion-free. Indeed, suppose $u \in U_{M,S,T}$ satisfies $u^b \in U_{k,S,T}$ for some natural number b. Then $(u^{\tau_M - 1})^b = (u^b)^{\tau_M - 1} = 1$ implies $u^{\tau_M - 1}$ is a b^{th} root of unity in $U_{M,S,T}$, and hence is equal to 1. Therefore u is fixed by Γ_M and so $u \in U_{k,S,T}$.

Theorem 4.1.1. *Suppose* M/k *is a relevant quadratic extension with Galois group* $\Gamma = \{1, \tau\}$*. Let* $u_1, ..., u_r$ *constitute a* $\mathbb{Z}$*-basis for* $U_{M,S,T}/U_{k,S,T}$*. Then the Rubin-Stark evaluator is*

$$\varepsilon_{M/k} = 2^{|S|-r-2} \frac{h_{M,S,T}}{h_{k,S,T}} (1 - \tau) \cdot u_1 \wedge \ldots \wedge u_r,$$

where $h_{M,S,T} = |A_{M,S,T}|$*.*

Proof. See the proof of Theorem 3.5 in [Rub96]. □

We want to increase the coefficient in front of the exterior product of units as much as possible. We use a method employed by Sands in [San04]. To this end, we rewrite $(1-\tau) = 2^{1-r}(1-\tau)^r$, so that

$$\varepsilon_{M/k} = 2^{|S|-r-2}\frac{h_{M,S,T}}{h_{k,S,T}}2^{1-r}u_1^{1-\tau}\wedge\ldots\wedge u_r^{1-\tau}.$$

Let $U^-_{M,S,T}$ denote the set of units $u \in U_{M,S,T}$ such that $N_{M/k}u = 0$ (remember we are writing the unit groups additively!). The $\mathbb{Z}$-rank of $U^-_{M,S,T}$ is r, as it is the kernel of a map from $U_{M,S,T}$ ($\mathbb{Z}$-rank $|S|+r-1$) onto a subgroup of $U_{k,S,T}$ which contains $U^2_{k,S,T}$ ($\mathbb{Z}$-rank $|S|-1$). Therefore we can choose $z_1,\ldots,z_r$ a $\mathbb{Z}$-basis for $U^-_{M,S,T}$.

As $u_1^{1-\tau},\ldots,u_r^{1-\tau}$ is a $\mathbb{Z}$-basis for $U^{1-\tau}_{M,S,T}$, we have

$$u_1^{1-\tau}\wedge\ldots\wedge u_r^{1-\tau} = (U^-_{M,S,T} : U^{1-\tau}_{M,S,T})\cdot z_1\wedge\ldots\wedge z_r.$$

We will understand the unit group index above in terms of group cohomology.

4.2 Some cohomological lemmas

Next we prove a

Lemma 4.2.1. *For any relative quadratic extension M/k of number fields, and any finite disjoint sets S and T of primes in k such that S contains all the primes which ramify in M/k we have the following exact sequence.*

$$0 \longrightarrow \widehat{\mathrm{H}}^1(\Gamma, U_{M,S,T}) \longrightarrow A_{k,S,T} \stackrel{\iota}{\longrightarrow} A_{M,S,T} \longrightarrow A_{M,S,T}/\iota A_{k,S,T} \longrightarrow 0.$$

Proof. The following proof is a T-modified version of a result found in [Tat84].

Let $M_T^\times$ denote the elements of $M^\times$ that are congruent to 1 modulo all primes in T_M, and $P_{M,S,T}$ denote the set of principal fractional ideals of M which are relatively prime to S and have a generator that is in $M_T^\times$. We make similar definitions for $k_T^\times$ and $P_{k,S,T}$. It is readily verified that the following sequences are exact

$$0 \longrightarrow U_{k,S,T} \longrightarrow k_T^\times \longrightarrow P_{k,S,T} \longrightarrow 0 \tag{4.4}$$

$$0 \longrightarrow U_{M,S,T} \longrightarrow M_T^\times \longrightarrow P_{M,S,T} \longrightarrow 0. \tag{4.5}$$

Applying the "fixed by Γ" functor to (4.5) yields another exact sequence

$$0 \longrightarrow U_{k,S,T} \longrightarrow k_T^\times \longrightarrow P_{M,S,T}^\Gamma \longrightarrow \widehat{\mathrm{H}}^1(\Gamma, U_{M,S,T}) \longrightarrow \widehat{\mathrm{H}}^1(\Gamma, M_T^\times). \tag{4.6}$$

Lemma 4.2.3 will show that $\widehat{\mathrm{H}}^1(\Gamma, M_T^\times) = 0$ (i.e., that we have a T-modified Hilbert Theorem 90). Assuming that for now, an application of the Snake Lemma to sequences (4.4) and (4.6) yields

$$\widehat{\mathrm{H}}^1(\Gamma, U_{M,S,T}) \cong \mathrm{Coker}(P_{k,S,T} \hookrightarrow P_{M,S,T}^\Gamma).$$

Next we consider the exact sequences

$$0 \longrightarrow P_{k,S,T} \longrightarrow \mathcal{I}_{k,S\cup T} \longrightarrow A_{k,S,T} \longrightarrow 0, \tag{4.7}$$

$$0 \longrightarrow P_{M,S,T} \longrightarrow \mathcal{I}_{M,S\cup T} \longrightarrow A_{M,S,T} \longrightarrow 0, \tag{4.8}$$

where for example $\mathcal{I}_{k,S\cup T}$ denotes the group of fractional ideals of k that are relatively prime to S and T.

Applying the "fixed by Γ" functor to (4.8), and using the fact that S contains all the ramified place of M/k, gives an exact sequence

$$0 \longrightarrow P_{M,S,T}^\Gamma \longrightarrow \mathcal{I}_{k,S\cup T} \longrightarrow A_{M,S,T}^\Gamma \subseteq A_{M,S,T}. \tag{4.9}$$

Putting this all together gives the diagram

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & \ker\iota & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_{k,S,T} & \longrightarrow & \mathcal{I}_{k,S\cup T} & \longrightarrow & A_{k,S,T} & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow{\scriptstyle\iota} & & \\
0 & \longrightarrow & P^{\Gamma}_{M,S,T} & \longrightarrow & \mathcal{I}_{k,S\cup T} & \longrightarrow & A_{M,S,T} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \widehat{\mathrm{H}}^1(\Gamma, U_{M,S,T}) & & 0 & & A_{M,S,T}/\iota(A_{k,S,T}) & & .
\end{array}
$$

Another application of the Snake Lemma gives $\ker\iota \cong \widehat{\mathrm{H}}^1(\Gamma, U_{M,S,T})$, and then the last exact column is what we were trying to prove. □

At this point we note the

Corollary 4.2.2. *Under the hypotheses of the previous lemma,*

$$\frac{h_{M,S,T}}{h_{k,S,T}}|\widehat{\mathrm{H}}^1(\Gamma, U_{M,S,T})| = |A_{M,S,T}/\iota A_{k,S,T}|.$$

Remember that we needed to prove the following

Lemma 4.2.3. *If T does not contain any ramified primes,* $\widehat{\mathrm{H}}^1(\Gamma, M_T^\times) = 0$.

Proof. Let $M_{(T)}^\times$ denote the anti-units at T, namely the set of $\alpha \in M^\times$ such that $\mathrm{ord}_w(\alpha) = 0$ for all $w \in T_M$. Put $\Delta(T) = \bigoplus_{w\in T_M} M(w)^\times$, where $M(w)^\times$ denotes the the invertible elements of the residue field at w. With these notations, the following sequence is exact:

$$0 \longrightarrow M_T^\times \longrightarrow M_{(T)}^\times \longrightarrow \Delta(T) \longrightarrow 0. \qquad (4.10)$$

Write $\Delta(T) \cong \bigoplus_{v\in T}(M(w)^\times \otimes_{\mathbb{Z}[\Gamma_v]} \mathbb{Z}[\Gamma])$, where a fixed $w|v$ is chosen arbitrarily for each $v \in T$. Applying Shapiro's Lemma (c.f. [Cas67]), allows us to compute

$$\widehat{\mathrm{H}}^i(\Gamma, \Delta(T)) = \bigoplus_{v\in T} \widehat{\mathrm{H}}^i(\Gamma_v, M(w)^\times).$$

By Hilbert's Theorem 90, $\widehat{\mathrm{H}}^1(\Gamma_v, M(w)^\times) = 0$, and since Γ_v is cyclic (as $v \in T$ is unramified) we may consider the Herbrand Quotient. But because $M(w)^\times$ is finite, it has trivial Herbrand Quotient, hence $\widehat{\mathrm{H}}^i(\Gamma_v, M(w)^\times) = 0$ for all i. We conclude that $\widehat{\mathrm{H}}^i(\Gamma, \Delta(T)) = 0$.

By examining the long exact sequence of Tate cohomology associated to (4.10), it follows that $\widehat{\mathrm{H}}^i(\Gamma, M_T^\times) \cong \widehat{\mathrm{H}}^i(\Gamma, M_{(T)}^\times)$ for all i.

Next we consider the exact sequence

$$0 \longrightarrow M_{(T)}^\times \longrightarrow M^\times \xrightarrow{\bigoplus \mathrm{ord}_w} \bigoplus_{w\in T_M} \mathbb{Z} \longrightarrow 0$$

whose long exact cohomology, thanks the Hilbert's Theorem 90, looks like

$$0 \longrightarrow k_{(T)}^\times \longrightarrow k^\times \xrightarrow{\theta} \left[\bigoplus_{w\in T_M} \mathbb{Z}\right]^\Gamma \longrightarrow \widehat{\mathrm{H}}^1(\Gamma, M_{(T)}^\times) \longrightarrow 0$$

Now the approximation theorem combined with the fact that T does not contain any ramified primes, yields that the map

$$\theta = \left(\bigoplus_{w\in T_M} \mathrm{ord}_w\right)\Bigg|_{k^\times}$$

is surjective, and hence $\widehat{\mathrm{H}}^1(\Gamma, M_{(T)}^\times) = 0$, completing the lemma. □

4.3 The proof of Theorem 4.0.9

Proof. Assume the hypotheses of the theorem. That is, let K/k be a multi-quadratic extension of rank m with Galois group G, and fix S, T, and r so that the hypotheses of the extended conjecture are satisfied, and further that we have the inequality 4.1 for all relevant M/k.

Choose $\phi_1, \ldots, \phi_r$ in $\mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$. In order to prove the extended conjecture $\tilde{B}(K/k, S, T, r)$ it remains to show $\phi(\epsilon_{K/k}) = (\phi_1 \wedge \ldots \wedge \phi_r)(\epsilon_{K/k})$ is an element of $\mathbb{Z}[G]$.

From Lemma 2.5.6, we know that if π_M is the natural projection from $\mathbb{Z}[G]$ to $\mathbb{Z}[G/G_M] = \mathbb{Z}[\Gamma_M]$ that

$$\begin{aligned} \pi_M(\phi(\epsilon_{K/k})) &= (N^{*(r)}_{K/M}\phi)(N^{(r)}_{K/M}\epsilon_{K/k}) \\ &= \varphi(\varepsilon_{M/k}) \end{aligned}$$

where $\varphi = \varphi_1 \wedge \ldots \wedge \varphi_r$, and each $\varphi_i = N^{*}_{K/M}\phi_i$ is some element of $U^{*}_{M,S,T} = \mathrm{Hom}_{\mathbb{Z}[\Gamma_M]}(U_{M,S,T}, \mathbb{Z}[\Gamma_M])$. Let $z_1, ..., z_r$ be a $\mathbb{Z}$-basis for $U^{-}_{M,S,T}$ as in the earlier section. Notice that since $(1+\tau_M)\varphi_i(z_j) = \varphi_i((1+\tau_M)z_j) = \varphi_i(0) = 0$,

$$\varphi_i(z_j) \in \mathbb{Z}[\Gamma_M]^{-} = (1-\tau_M)\mathbb{Z}. \tag{4.11}$$

Fix $n_{ij} \in \mathbb{Z}$ such that $\varphi_i(z_j) = (1-\tau_M)n_{ij}$.

We compute

$$\begin{aligned}
\varphi(\varepsilon_{M/k}) &= \varphi\left(2^{|S|-r-2}\frac{h_{M,S,T}}{h_{k,S,T}}2^{1-r}u_1^{1-\tau}\wedge\ldots\wedge u_r^{1-\tau}\right)\\
&= 2^{|S|-r-2}\frac{h_{M,S,T}}{h_{k,S,T}}(U^-_{M,S,T}:U^{1-\tau}_{M,S,T})2^{1-r}\varphi(z_1\wedge\ldots\wedge z_r)\\
&= 2^{|S|-r-2}\frac{h_{M,S,T}}{h_{k,S,T}}|\widehat{\mathrm{H}}^{-1}(\Gamma_M,U_{M,S,T})|\cdot 2^{1-r}\det(\varphi_i(z_j))\\
&= 2^{|S|-r-2}\frac{h_{M,S,T}}{h_{k,S,T}}|\widehat{\mathrm{H}}^{1}(\Gamma_M,U_{M,S,T})|\cdot 2^{1-r}\det((1-\tau_M)n_{ij})\\
&= 2^{|S|-r-2}|A_{M,S,T}/\iota A_{k,S,T}|\cdot 2^{1-r}(1-\tau_M)^r\det(n_{ij})\\
&= 2^{|S|-r-2}|A_{M,S,T}/\iota A_{k,S,T}|(1-\tau_M)\det(n_{ij})
\end{aligned}$$

The first equality uses our explicit description of $\varepsilon_{M/k}$, the third the definition of $\widehat{\mathrm{H}}^{-1}$, the fourth the fact that Γ is cyclic, and the fifth is Lemma 4.2.1.

It is now evident that $\varphi(\varepsilon_{M/k})\in 2^{|S|-r+\mathrm{ord}_2(|A_{M,S,T}/\iota A_{k,S,T}|)-2}\mathbb{Z}[\Gamma_M]$. Combining this with our initial assumption that $|S|-r+\mathrm{ord}_2(|A_{M,S,T}/\iota A_{k,S,T}|)\geq m+1$, it follows that $\varphi(\varepsilon_{M/k})\in 2^{m-1}\mathbb{Z}[\Gamma_M]$. Note we get this conclusion whether M/k is relevant or not. Indeed, if M/k is not relevant, then $\varphi(\varepsilon_{M/k})=0$ because $\varepsilon_{M/k}=0$.

Hence we have an element $\lambda=\phi(\epsilon_{K/k})$ in $\mathbb{Q}[G]$ such that every projection of λ into an order 2 quotient space lands in $2^{m-1}\mathbb{Z}[\Gamma_M]$, and whose projection into $\mathbb{Z}$ via the augmentation map is zero (this is true for our λ since $|S|>r+1$). I claim that this means λ is in $\mathbb{Z}[G]$.

We prove this final claim, which completes the proof of the theorem. Write $\lambda=\sum_{\sigma\in G}q_\sigma\sigma$. We know that for every $H\subseteq G$ of index 2 ($H=G_M$ for some M),

$$\pi_M(\lambda)=(\sum_{h\in H}q_h)H+(\sum_{h\in H}q_{h\tau_M})\tau_M H\in 2^{m-1}\mathbb{Z}[\Gamma_M]. \tag{4.12}$$

In particular for any fixed σ we see $\sum_{h\in H} q_{h\sigma} \in 2^{m-1}\mathbb{Z}$. We view G as the vector space $\mathbb{F}_2^m$. Let W be the set of all subspaces $H \subseteq G$ such that $(G : H) = 2$. It is not hard to see using results on vector spaces over finite fields that the number of such subspaces is $2^m - 1$. Consider the sum $\sum_{H\in W}\sum_{h\in H} q_{h\sigma}$. We see that q_σ appears $|W|$ times, while for every $\gamma \in G$, $\gamma \neq \sigma$, q_γ appears $2^{m-1}-1$ times. Hence $(2^m - 1)q_\sigma + (2^{m-1} - 1)\sum_{\gamma\neq\sigma} q_\gamma \in 2^{m-1}\mathbb{Z}$. But we have $(2^{m-1} - 1)\sum_{g\in G} q_g = 0$. Subtracting gives $2^{m-1}q_\sigma \in 2^{m-1}\mathbb{Z}$. Therefore $q_\sigma \in \mathbb{Z}$. □

4.4 Results towards the standard conjecture

For a fixed base field k, we use the following notations: Pl is the set of places of k; Pl_2 represents the *dyadic* primes, i.e. those that divide 2; Pl_0 is the set of finite place; Pl_∞^{r}, Pl_∞^{c} is the set of real and complex places of k respectively, while finally $Pl_\infty = Pl_\infty^{\mathrm{r}} \cup Pl_\infty^{\mathrm{c}}$. For any set of places $\mathcal{S}$, we put $\mathcal{S}_0 = \mathcal{S} \cap Pl_0$, $\mathcal{S}_\infty = \mathcal{S} \cap Pl_\infty$, *etc.*

Generally we have a fixed extension K/k in mind, and for any set of places $\mathcal{S}$, we put $\mathcal{S}^+ = \{v \in \mathcal{S} |\ v \text{ splits completely in } K/k\}$ and $\mathcal{S}^- = \mathcal{S} \setminus \mathcal{S}^+$. We use the notation for ray class groups introduced in Section 2.6. For any abelian group B we put $B^{(2)} = B/B^2$, which is an elementary abelian 2-group.

Proposition 4.4.1. *If K/k is a multiquadratic extension, T consists of a single prime v_T which splits completely in K/k, and $Pl_2 \subseteq S^-$, then the standard Rubin conjecture $B(K/k, S, T, r)$ is true up to a factor of $2^{2+|S_\infty^+|}$.*

Proof. Break the set S into two pieces $S = S^+ \cup S^-$ consisting of the primes that split completely in K/k and those that do not respectively. We may assume that $|S^+| = r$, because otherwise the conjecture is trivially true.

Let $A = Cl^{(2)}_{k,\emptyset,S_0^- \cup T}$. This group corresponds to the maximal multiquadratic extension of k that is unramified outside of $S_0^- \cup T$. Let B_+ be the subgroup of A generated by the decomposition groups of the primes in S^+, and similarly B_- and B_T for the primes in S^- and T. We find that $Cl^{(2)}_{k,S^-,T} \cong A/B_-$ and $Cl^{(2)}_{k,T,S_0^-} \cong A/B_T$. Moreover, $\mathrm{rk}_2(Cl_{k,S^-,T}) - \mathrm{rk}_2(Cl_{k,S,T}) = \mathrm{rk}_2(\frac{B_+}{B_+ \cap B_-})$ and $\mathrm{rk}_2(Cl_{k,T,S_0^-}) - \mathrm{rk}_2(Cl_{k,T\cup S^+,S_0^-}) = \mathrm{rk}_2(\frac{B_+}{B_+ \cap B_T})$. Since the groups on the right sides are elementary abelian, we conclude

$$\mathrm{rk}_2(Cl_{k,S^-,T}) - \mathrm{rk}_2(Cl_{k,S,T}) - (\mathrm{rk}_2(Cl_{k,T,S_0^-}) - \mathrm{rk}_2(Cl_{k,T\cup S^+,S_0^-})) = \\ \mathrm{rk}_2(B_+ \cap B_T) - \mathrm{rk}_2(B_+ \cap B_-)$$

But B_T is generated by the decomposition group of v_T. Since v_T is tamely ramified ($v_T \notin Pl_2$), its ramification index is at most $e = 2$ and its inertial degree in the multiquadratic extension $H_{k,\emptyset,S^-\cup T}/k$ is at most $f = 2$ (because $f = |G_{v_T}/I_{v_T}|$ is a *cyclic* sub-quotient of G). Hence the decomposition group of v_T has 2-rank at most 2. We conclude that $\mathrm{rk}_2(B_+ \cap B_T) \leq 2$. Also note that $K \subseteq H^{(2)}_{k,T\cup S^+,S_0^-}$, so $m := \mathrm{rk}_2(G(K/k)) \leq \mathrm{rk}_2(Cl_{k,T\cup S^+,S_0^-})$ (Here is where we are using the hypothesis that v_T splits in K/k). Putting these facts together yields

$$\mathrm{rk}_2(Cl_{k,S^-,T}) - \mathrm{rk}_2(Cl_{k,S,T}) - \big(\mathrm{rk}_2(Cl_{k,T,S_0^-}) - m\big) \leq 2,$$

or

$$\mathrm{rk}_2(Cl_{k,S^-,T}) - \mathrm{rk}_2(Cl_{k,T,S_0^-}) \leq 2 - m + \mathrm{rk}_2(Cl_{k,S,T}).$$

Now according to the reflection formula (Theorem 2.6.5; here is where we are using the hypothesis that $Pl_2 \subseteq S^-$),

$$\begin{aligned} \mathrm{rk}_2(Cl_{k,S^-,T}) - \mathrm{rk}_2(Cl_{k,T\cup S_\infty^{\mathrm{r}+},S_0^-}) &= |T| - |Pl_\infty| - |S_0^-| + |S_\infty^{\mathrm{r}+}| \\ &= 1 - (|S| - r) - |S_\infty^{\mathrm{c}+}|. \end{aligned}$$

And by Corollary I.4.5.4 of [Gra03], $\mathrm{rk}_2(Cl_{k,T\cup S_\infty^{\mathrm{r}+},S_0^-}) - \mathrm{rk}_2(Cl_{k,T,S_0^-}) \geq -|S_\infty^{\mathrm{r}+}|$. Therefore

$$2 - m + \mathrm{rk}_2(Cl_{k,S,T}) \geq 1 - |S| + r - |S_\infty^{\mathrm{c}+}| - |S_\infty^{\mathrm{r}+}|.$$

or, with the fact that when T contains no dyadic primes, $\mathrm{rk}_2(Cl_{k,S,T}) = \mathrm{rk}_2(A_{k,S,T})$,

$$|S| + \mathrm{rk}_2(A_{k,S,T}) \geq 1 + r + m - (2 + |S_\infty^{+}|).$$

By examining Corollary 4.0.11, we see that the proof is complete. □

Corollary 4.4.2. *If k is totally real and K is totally complex, then with the hypothesis of the previous proposition, $B(K/k, S, T, r)$ is true up to a factor of 2^2.*

Example 4.4.3. *If the base field is $k = \mathbb{Q}$, then under the hypothesis of the previous proposition we have proven that $B(K/k, S, T, r)$ is true up to a factor of $2^{2+1} = 8$. However the requirements that $Pl_2 \subseteq S$ and v_T split completely are not really necessary in this case, and this result may be proved directly from Corollary 4.0.11 via other methods.*

We wrap up this section by proving the

Proposition 4.4.4. *Suppose K/k is a multiquadratic extension. If $|T^+| \geq r + 1$ and $Pl_2 \subseteq S$, then $B(K/k, S, T, r)$ is true.*

Proof. By Theorem 2.6.5,

$$\mathrm{rk}_2(Cl_{k,S,T^+}) - \mathrm{rk}_2(Cl_{k,T^+,S_0}) = |T^+| - |S|$$

Also $\mathrm{rk}_2(Cl_{k,S,T}) \geq \mathrm{rk}_2(Cl_{k,S,T^+})$, and, since $K \subseteq H_{k,T^+,S_0}$, $m \leq \mathrm{rk}_2(Cl_{k,T^+,S_0})$. Putting these inequalities together yields the necessary one to apply Theorem 4.0.9. □

Note that the condition that $Pl_2 \subseteq S$ is often fulfilled naturally because it is quite common for dyadic primes to ramify in multiquadratic extensions (as the extension is Kummer and the dyadic primes divide the exponent.)

4.5 Results towards the extended conjecture

In this section we derive further results for the extended conjecture. Of course **all results for the extended conjecture $\widetilde{B}$ also imply the corresponding results for the standard Rubin conjecture** B. (Take $M = K$ in Theorem 3.4.1.)

Proposition 4.5.1. *If K/k is a biquadratic bicyclic extension, i.e. $G(K/k) \cong (\mathbb{Z}/2\mathbb{Z})^2$, and $\mathrm{rk}_2(A_{M,S,T}) \geq 1$ for all relevant quadratic extensions M/k, then $\widetilde{B}(K/k, S, T)$ is true.*

Proof. We are also assuming, as always, that the L-function attached to the trivial character vanishes to order greater than r, i.e. $|S| \geq r + 2$. According to Theorem 4.0.9, we are done if, for each relevant quadratic extension M/k,

$$|S| + \mathrm{ord}_2(|A_{M,S,T}/\iota A_{k,S,T}|) \geq r + m + 1 = r + 3.$$

Hence we are reduced to the case where there exists a relevant extension M/k in which $\operatorname{ord}_2(|A_{M,S,T}/\iota A_{k,S,T}|) = 0$ and $|S| = r + 2$. Let M/k be such a quadratic extension and $\Gamma = G(M/k)$.

By Lemma 4.0.10 we have $\operatorname{ord}_2(|A_{M,S,T}/\iota A_{k,S,T}|) \geq \operatorname{rk}_2(A_{k,S,T})$; we conclude that $A_{k,S,T}$ also has odd cardinality. Now the long exact sequence of finite groups (see Lemma 4.2.1),

$$0 \longrightarrow \widehat{\mathrm{H}}^1(\Gamma, U_{M,S,T}) \longrightarrow A_{k,S,T} \xrightarrow{\iota} A_{M,S,T} \longrightarrow A_{M,S,T}/\iota A_{k,S,T} \longrightarrow 0$$

implies that both $|\widehat{\mathrm{H}}^1(\Gamma, U_{M,S,T})|$ and $|A_{M,S,T}|$ are odd, since their product is. However this contradicts our hypothesis that $\operatorname{rk}_2(A_{M,S,T}) \geq 1$. Therefore no such relevant extension exists and the proposition follows. □

The next theorem we shall prove applies to the extended conjecture, and thereby also to Rubin's conjecture. It is the strongest theorem known to the author regarding Rubin's conjecture in multiquadratic extensions. It says that if we are allowed to chose the set T judiciously, we may take T to be of cardinality $m - 1$ and the conjecture definitely becomes true. Moreover, if any set T of non-dyadic primes is chosen of cardinality larger than $r + m$, the conjecture will be true. (The condition that the primes in T be non-dyadic is simply to avoid trouble with wild ramification. However, if one truly wishes to put dyadic primes into T that is not a problem, one should simply replace the set T below with $T \setminus T_2$, apply the theorem, and then add the dyadic primes back into T, and conjecture $\widetilde{B}$ will remain true by Proposition 3.3.1.)

Theorem 4.5.2. *Suppose K/k is a multiquadratic extension of rank m, S is appropriate for K/k and is an r-cover for $\widehat{G}$. Then:*

(i) For any integer t with $t \geq r + m + 1 - |S| - \mathrm{rk}_2(A_{k,S})$, there exists a set T with $|T| = t$ such that $\widetilde{B}(K/k, S, T)$ is true.

(ii) If T is any *set of non-dyadic places with $|T| \geq r + m + 1$, the conjecture $\widetilde{B}(K/k, S, T)$ is true.*

Proof. We prove (ii) first. Suppose T of the indicated size is given. Let $\mathcal{P}(T)$ denote the power set of T. We make $\mathcal{P}(T)$ into a group under the operation

$$T_1 \cdot T_2 = (T_1 \cup T_2) \setminus (T_1 \cap T_2).$$

(The identity element is the empty set, and every element is its own inverse.)

Recall the construction of the S-governing field of k from Section 2.6. First we put

$$\mathcal{Y}_k^S = \{x \in k^\times \mid (x) = \mathfrak{a}^2 \mathfrak{a}_{S_0}\}.$$

Then we form the governing field

$$\mathcal{Q}_k = k(\sqrt{\mathcal{Y}_k^S}). \tag{4.13}$$

Define a homomorphism $\mathcal{P}(T) \xrightarrow{\psi} G(\mathcal{Q}_k/k)$ via the formula

$$\psi(T_1) = \prod_{v \in T_1} \left(\frac{\mathcal{Q}_k/k}{v} \right).$$

That ψ is actually a homomorphism relies simply on the fact that $G(\mathcal{Q}_k/k)$ is an elementary 2-group. According to Lemma 2.6.7, each $T_1 \in \ker(\psi)$, $T_1 \neq \emptyset$, corresponds to a relative quadratic extension of k which is T_1-totally ramified and S-split. We conclude that

$$\mathrm{rk}_2(A_{k,S,T}) - \mathrm{rk}_2(A_{k,S}) \geq \mathrm{rk}_2(\ker(\psi)). \tag{4.14}$$

Now

$$|\ker(\psi)| = \frac{|\mathcal{P}(T)|\cdot|\mathrm{Coker}(\psi)|}{|G(\mathcal{Q}_k/k)|} \geq \frac{|\mathcal{P}(T)|}{|G(\mathcal{Q}_k/k)|} = 2^{|T|-\mathrm{rk}_2(G(\mathcal{Q}_k/k))}. \tag{4.15}$$

Let $A_{k,S}[2]$ denote the 2-torsion of $A_{k,S}$, i.e., those elements annihilated by 2. The exact sequence

$$0 \longrightarrow A_{k,S}[2] \longrightarrow A_{k,S} \xrightarrow{2} A_{k,S} \longrightarrow A_{k,S}^{(2)} \longrightarrow 0 \tag{4.16}$$

implies $\#A_{k,S}[2] = \#A_{k,S}^{(2)}$, and hence, since both groups are elementary abelian, $\mathrm{rk}_2(A_{k,S}[2]) = \mathrm{rk}_2(A_{k,S}^{(2)}) = \mathrm{rk}_2(A_{k,S})$. We use the following short exact sequence to analyze the rank of the Galois group of the governing field:

$$0 \longrightarrow \frac{U_{k,S}(k^\times)^2}{(k^\times)^2} \longrightarrow \frac{\mathcal{Y}_k^S}{(k^\times)^2} \xrightarrow{\phi} A_{k,S}[2] \longrightarrow 0$$

where for $\overline{x} \in \mathcal{Y}_k^S/(k^\times)^2$ we decompose $(x) = \mathfrak{a}^2\mathfrak{a}_{S_0}$ and then set $\phi(\overline{x}) := [\mathfrak{a}]_{k,S}$. This map is clearly well defined. Now we verify the exactness. First, if $\mathbf{c} = [\mathfrak{a}]_{k,S} \in A_{k,S}[2]$, then $\mathfrak{a}^2 = (x)\mathfrak{b}_{S_0}$ with $x \in k^\times$ and $\mathfrak{b}_{S_0} \in \langle S_0\rangle$. Hence $\phi(\overline{x}) = \mathbf{c}$. Next, if $\overline{x} \in \mathcal{Y}_k^S/(k^\times)^2$ gets mapped to the identity under ϕ, then $(x) = (x_0)^2\mathfrak{a}_{S_0}$. Hence $x = \frac{x}{x_0^2}\cdot x_0^2 \in U_{k,S}(k^\times)^2$. On the other hand, it is clear that all such elements get mapped to the identity under ϕ.

Since all the groups in the exact sequence are finite elementary 2-groups, we use Kummer theory to find that

$$\mathrm{rk}_2(G(\mathcal{Q}_k/k)) = \mathrm{rk}_2(\mathcal{Y}_k^S/(k^\times)^2) = \mathrm{rk}_2(U_{k,S}(k^\times)^2/(k^\times)^2) + \mathrm{rk}_2(A_{k,S}).$$

Combining the fact that $\mathrm{rk}_2(U_{k,S}(k^\times)^2/(k^\times)^2) = \mathrm{rk}_2(U_{k,S}/U_{k,S}^2) = |S|$ with equations (4.14) and (4.15), we find that

$$\mathrm{rk}_2(A_{k,S,T}) - \mathrm{rk}_2(A_{k,S}) \geq |T| - |S| - \mathrm{rk}_2(A_{k,S}).$$

Recalling our hypothesis on $|T|$ and rearranging yields

$$|S| + \mathrm{rk}_2(A_{k,S,T}) \geq r + m + 1$$

which, in view of the Main Theorem of multiquadratic extensions (Corollary 4.0.11), finishes the proof of (ii).

For part (i), let $t \geq r + m + 1 - |S| - \mathrm{rk}_2(A_{k,S})$ be a given integer. Choose t distinct primes $v_1, ..., v_t$ of k such that

$$\left(\frac{\mathcal{Q}_k/k}{v_i}\right) = 1$$

for each $1 \leq i \leq t$, and collect them to form the set T.

Consider the map ψ as above. In this situation all of $\mathcal{P}(T)$ is in the kernel of ψ, so that equation (4.14) becomes

$$\mathrm{rk}_2(A_{k,S,T}) - \mathrm{rk}_2(A_{k,S}) \geq \mathrm{rk}_2(\mathcal{P}(T)) = t.$$

Substituting the bound on t, and rearranging yields the necessary inequality to apply the Main Theorem for multiquadratic extensions. □

Remark: Since $|S| - r - 2 \geq 0$, it follows that we may choose the t in part (i) of the above theorem to be $m - 1$. In the biquadratic case we therefore may take $t = 1$. Hence in the biquadratic bicyclic case we may always add one prime to T to make the conjecture true, namely a prime which splits completely in $\mathcal{Q}_k/k$.

4.6 Completely nontrivial r-covers

The spirit of the conjecture $\widetilde{B}$ is that we do not wish to consider only the cases where there are r primes which split completely. We may well ask what happens if we push this idea to its extreme, and supposed that S does not contain *any* prime which splits completely in the extension K/k. It turns out that in certain cases we can then say even more.

Definition 4.6.1. *For an extension K/k and integer r, we call an r-cover $\mathcal{S}$ for $\widehat{G}$* completely nontrivial *if it does not contain* any *primes that split completely in K/k.*

Proposition 4.6.2. *If K/k is a multiquadratic extension of rank m and S is a completely nontrivial r-cover with $r \geq m$, then $\widetilde{B}(K/k, S, T)$ is true.*

Proof. Recall the inequality from Lemma 2.4.2,

$$\sum_{\substack{\chi \in \widehat{G} \\ \chi \neq \mathbf{1}_G}} r_S(\chi) = \sum_{v \in S} (g_v - 1). \tag{4.17}$$

Since, by hypothesis, none of the primes in S split completely in K/k, it follows that each decomposition group is nontrivial and $g_v \leq 2^{m-1}$ for each $v \in S$. Since S is an r-cover for $\widehat{G}$, for every $\chi \in \widehat{G}$, $r_S(\chi) \geq r$. Plugging these estimates into (4.17) yields $(2^m - 1)r \leq (2^{m-1} - 1)|S|$, or $|S| \geq \frac{2^m - 1}{2^{(m-1)} - 1} r > 2r$. Since $|S|$ is an integer, $|S| \geq 2r + 1$, which, by hypothesis is at least $r + m + 1$. Again we are done by the Main Theorem regarding multiquadratic extensions (Corollary 4.0.11). □

Corollary 4.6.3. *If S is a completely nontrivial r-cover, conjecture $\widetilde{B}$ is true in biquadratic bicyclic extensions (i.e. when $G = (\mathbb{Z}/2\mathbb{Z})^2$).*

Proof. According to the previous Proposition, we are done if $r \geq 2$. The case $r = 1$ was taken care of in [Eri05]. □

4.7 A remark on the approach

Our attack on the problem of multiquadratic extensions was to write the evaluator for the full extension K/k in terms of pieces coming from each quadratic level. We have not been able to prove any conjecture in full using this method, so it is natural to ask whether it might not always work. The answer is that indeed at times it is not strong enough: some of the pieces add together to give an element in the lattice while each piece is not in the lattice. The following example demonstrates this phenomenon.

Example 4.7.1. *Let $k = \mathbb{Q}$ and $K = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$. Let $S = \{\infty, 2, 17\}$ and $T = \{3\}$. The field K has three quadratic subfields, $K_1 = \mathbb{Q}(\sqrt{-1})$, $K_2 = \mathbb{Q}(\sqrt{-2})$ and $K_3 = \mathbb{Q}(\sqrt{2})$. All five fields have class number one. One finds that the three Rubin-Stark units for the quadratic extensions $K_i/\mathbb{Q}$ are $\varepsilon_1 = \frac{8-15\sqrt{-1}}{17}$, $\varepsilon_2 = \frac{-1+12\sqrt{-2}}{17}$ and $\varepsilon_3 = 1$. Since 17 splits completely in K/k, we are in the situation of the standard Rubin conjecture, though we can consider it also from the viewpoint of the extended conjecture, as S is a 1-cover for $\widehat{G}$. From our earlier description we obtain (now written multiplicatively)*

$$\varepsilon_{K/k} = \varepsilon_1^{1/2} \varepsilon_2^{1/2} \varepsilon_3^{1/2}.$$

One can check that, for example $\varepsilon_1^{1/2} \notin K$. Indeed, in K we may decompose ε_1 into primes:

$$(\varepsilon_1)\mathcal{O}_K = \mathfrak{P}_{17}\mathfrak{P}'_{17}(\mathfrak{P}''_{17}\mathfrak{P}'''_{17})^{-1},$$

where

$$
\begin{aligned}
(17)\mathcal{O}_K &= \mathfrak{P}_{17}\mathfrak{P}'_{17}\mathfrak{P}''_{17}\mathfrak{P}'''_{17} \\
&= (2+\sqrt{-1}+\sqrt{2})(2+\sqrt{-1}-\sqrt{2})(2-\sqrt{-1}+\sqrt{2})(2-\sqrt{-1}-\sqrt{2}).
\end{aligned}
$$

Never-the-less, $\varepsilon_{K/k} \in U_{K,S,T}$. *This happens because the* $\varepsilon_1^{1/2}$ *and* $\varepsilon_2^{1/2}$ *combine to give something in the lattice. Our analysis from in the current chapter would not have detected this fact.*

Chapter 5

More general extensions

In the previous chapter we studied extensions of exponent two extensively. Here we move back to studying more general types of extensions.

5.1 Covers with finite, unramifying primes

In this section K/k is any arbitrary finite abelian extension of number fields, and the pair of sets (S, T) is appropriate for K/k. Denote the minimal order of vanishing by $r = r_S(K/k)$. Recall that $\mathcal{P}_r(S_{\min})$ is simply the set of all subsets of $S_{\min}$ with cardinality exactly r. If S contains 'enough' finite unramifying primes, the standard conjecture implies the extended conjecture. To be precise:

Theorem 5.1.1. *Suppose S is an r-cover for $\widehat{G}$ which has a subset S' which is an r-cover for $\widehat{G}$ consisting of only finite unramifying primes. If $B(M_I/k, S, T, r)$ is true for all $I \in \mathcal{P}_r(S_{\min})$ then $\widetilde{B}(K/k, S, T)$ follows.*

Proof. Note that $S_{\min} \subseteq S'$. Let $S_b = S \setminus S'$; this set is a 0-cover to which we will be adding primes to generate zeroes in the L-functions of certain subextensions of K/k. As S' contains only finite, unramifying primes, S_b still contains all infinite and ramifying primes and hence is appropriate for the extension K/k. We call S_b the base appropriate set. We may assume that $|S'| > r$ because if $|S'| = r$, then $S_{\min} = S'$ contains r primes that split completely and $M_I = K$ for $I = S_{\min}$. We are actually assuming $B(K/k, S, T, r)$ is true in this case! However in this situation B and $\widetilde{B}$ are equivalent (see Corollary 3.4.2) and we would be done. Therefore assume $|S'| > r$ and hence for any $I \in \mathcal{P}_r(S_{\min})$ we may also define

$$\eta_I = \prod_{v \in S' \setminus I} \left(1 - \sigma_v^{-1}\right)$$

(the Frobenius automorphisms exist because we are assuming the primes in S' are unramified).

We shall use the notation of Section 3.2. Temporarily fix some $I \in \mathcal{P}_r(S_{\min})$. Take $v \in I$ and $\chi \in \widehat{G}$. We claim that $\chi((\sigma_v - 1)\eta_I)$ is zero. Obviously the claim is true if $\chi(\eta_I) = 0$. But $\chi(\eta_I) \neq 0$ implies that no prime in $S' \setminus I$ splits in K_χ/k. However we know at least r primes of S' have to split in K_χ/k, as S' is an r-cover. Thus all the primes in I split in K_χ/k, so $\chi(\sigma_v) = 1$ and the claim has been shown. Since this holds for all $\chi \in \widehat{G}$ we conclude that $(\sigma_v - 1)\eta_I = 0$, that is, $\sigma_v \cdot \eta_I = \eta_I$.

In the case of unramified primes, D_I, the subgroup generated by the decomposition groups of the primes in I, is actually generated by the Frobenius automorphisms, $D_I = \langle \sigma_v \mid v \in I \rangle$. Thus, the previous paragraph has shown that η_I is fixed by D_I. But $\mathbb{Z}[G]$ is cohomologically trivial, so $\mathbb{Z}[G]^{D_I} = N_{D_I}\mathbb{Z}[G]$. Therefore $\eta_I = N_{D_I} \cdot \eta_I'$ for some $\eta_I' \in \mathbb{Z}[G]$.

Picking up this extra coefficient N_{D_I} is enough to finish the proof. Take an element $\phi = \phi_1 \wedge \ldots \wedge \phi_r \in \bigwedge^r U^*_{K,S,T}$. We need only show that $\phi(\epsilon_{K/k,S,T}) \in \mathbb{Z}[G]$, as this will imply that $\epsilon_{K/k,S,T}$ is an element of $\Lambda_{S,T}$, which is the prediction of the extended conjecture. We will show first that $\phi(\varepsilon_{M_I/k,S_b \cup I,T,r}) = N^r_{D_I}\beta^\phi_I$ for some $\beta^\phi_I \in \mathbb{Z}[G]$. According to a computation identical to the one performed in the proof of Proposition 3.4.3,

$$\phi(\varepsilon_{M_I/k,S_b \cup I,T,r}) \in |D_I|^r \Psi_{K/M_I}(\mathbb{Z}[G/D_I]) = |D_I|^{r-1} N_{D_I}\mathbb{Z}[G] = N^r_{D_I}\mathbb{Z}[G].$$

Now we use Theorem 3.2.5 to compute

$$\begin{aligned}
\phi(\epsilon_{K/k,S,T}) &= \sum_{I \in \mathcal{P}_r(S_{\min})} \frac{1}{|D_I|^r}\phi(\varepsilon_{M_I/k,S,T,r}) \\
&= \sum \frac{\eta'_I}{|D_I|^r} N_{D_I}\phi(\varepsilon_{M_I/k,S_b \cup I,T,r}) \\
&= \sum \frac{\eta'_I}{|D_I|^r} N^{r+1}_{D_I}\beta^\phi_I \\
&= \sum \eta'_I N_{D_I}\beta^\phi_I \\
&\in \mathbb{Z}[G],
\end{aligned}$$

thereby ending the proof. □

Example 5.1.2. *Over $\mathbb{Q}$, Rubin's conjecture is known for $\mathbb{Z}/l\mathbb{Z}$-extensions if l is an odd prime [Bur04]. So we may construct examples of extensions $K/\mathbb{Q}$ in which the extended conjecture $\widetilde{B}$ is known. One way to proceed is the following: By Dirichlet's Theorem on primes in progression, we know the sequence $\{1+bl\}_{b=1}^\infty$ contains infinitely many rational primes. Let $p_i = 1 + b_i l$ for $i = 1, \ldots, m$ be m of these.*

Consider the cyclotomic field $L = \mathbb{Q}(\zeta_N)$ *where* $N = p_1 \cdot \ldots \cdot p_m$*. By well known cyclotomic field theory,* $G(L/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \cong \bigoplus_{i=1}^m \mathbb{Z}/b_i l\mathbb{Z}$ *and let* H *denote the subgroup* $\bigoplus_{i=1}^m l\mathbb{Z}/b_i l\mathbb{Z}$ *of* G *under the last identification. Finally, let* $K = L^H$ *be the fixed field. Then* $G(K/\mathbb{Q})$ *is isomorphic to* $(\mathbb{Z}/l\mathbb{Z})^m$*. One can then fill out sets* S *and* T *of primes of* $\mathbb{Q}$ *for which we can prove* $\widetilde{B}(K/\mathbb{Q}, S, T)$*.*

As a general rule, any result which says "B for all such extensions implies $\widetilde{B}$" may be reproven almost verbatim for "C for all such extensions implies $\widetilde{C}$". All that is needed is to replace $\Lambda_{S,T}$ with $\Lambda'_{S,T}$. Thus we have also the following

Theorem 5.1.3. *Suppose* S *is an* r*-cover for* $\widehat{G}$ *which has a subset* S' *which is an* r*-cover for* $\widehat{G}$ *consisting of only finite unramified primes. If* $C(M_I/k, S, r)$ *is true for all* $I \in \mathcal{P}_r(S_{\min})$ *then* $\widetilde{C}(K/k, S)$ *follows.*

5.2 Extensions of prime exponent

In this section we suppose our finite abelian Galois group G has prime exponent l, that is $G = G(K/k) \cong (\mathbb{Z}/l\mathbb{Z})^m$. We do not necessarily suppose that our base field k contains the l^{th} roots of unity; the extension K/k may not be a Kummer extension. Our goal is to prove $\widetilde{B}(K/k, S, T)$ under the hypothesis that the standard Rubin conjecture is true for (cyclic) extensions of degree l. If $l > 2$ the main difference from the multiquadratic extensions considered earlier is that we currently do not have an explicit formula for the Stark-evaluators $\varepsilon_{M,S,T,j}$. Indeed, we do not know in general that the conjectures are true, as we do in the quadratic case. None-the-less we will arrive at similar (but weaker) inequalities on $|S|$ and r

which imply the truth of the conjectures. To wit:

Theorem 5.2.1. *Suppose l is a prime number, $G = G(K/k) \cong (\mathbb{Z}/l\mathbb{Z})^m$ and that $B(M/k, S', T, r)$ is true for every degree l extension M of k contained in K and appropriate $S' \subseteq S$. Let S_{ram} denote the set of finite primes of k that ramify in K/k, and Pl_∞ denote the set of infinite places of k. If*

$$|S| \geq r + |S_{\mathrm{ram}}| + |Pl_\infty| + (m-1)l \tag{5.1}$$

then $\widetilde{B}(K/k, S, T)$ is true.

Proof. Take a $\chi \in \widehat{G}_{r,S}$, and let $H = \ker \chi$. Then $M = K^H$ is a *relevant* extension of k, i.e., a $\mathbb{Z}/l\mathbb{Z}$-extension in which exactly r primes of S split. According to Theorem 3.2.3, we know that

$$\epsilon_{K/k,S,T} = \sum_{\chi \in \widehat{G}} \frac{1}{|\ker \chi|^r} \mathbf{e}_\chi \varepsilon_{K^{\ker \chi}/k,S,T,r}$$

and so if we look at the piece coming from the field M, this is (see the Remark after Lemma 2.3.7)

$$\frac{1}{|H|^r} \frac{N_H}{|H|} \varepsilon_{M/k,S,T,r} = \frac{1}{|H|^r} \varepsilon_{M/k,S,T,r}$$

(the equality because every element of H acts trivially on $\varepsilon_{M/k,S,T,r}$.)

We know further that upon application of an element $\phi \in \bigwedge^r U^*_{K,S,T}$, we will pick up a $N_H^r = |H|^{r-1} N_H$:

$$\phi\left(\frac{1}{|H|^r} \varepsilon_{M/k,S,T,r}\right) \in \frac{N_H}{|H|} \mathbb{Z}[G] = l^{1-m} N_H \mathbb{Z}[G].$$

The key is to run this same argument not with $\varepsilon_{M/k,S,T,r}$, but rather with $\varepsilon_{M/k,S_H,T,r}$ for some $S_H \subsetneq S$. In particular we take S_H to consist of the r primes of

S that split in M/k, the primes that ramify in M/k and the infinite primes of k. Thus S_H is appropriate, and we do have an $\varepsilon_{M/k,S_H,T,r}$. Notice $U^*_{K,S,T} \subseteq U^*_{K,S_H,T}$. The two epsilons are linked in the following way:

$$\varepsilon_{M/k,S,T,r} = \left[\prod_{v \in S \setminus S_H} \left(1 - \sigma_v(M/k)^{-1}\right)\right] \varepsilon_{M/k,S_H,T,r}. \tag{5.2}$$

Because of our hypothesis on $|S|$, we know $|S \setminus S_H| = |S| - |S_H| \geq (m-1)l$.

We need to study the product that appears in equation (5.2). Fix σ a generator of $\Gamma = G(M/k) \cong \mathbb{Z}/l\mathbb{Z}$. Then for any set of $n_i \in \{1, 2, ..., l-1\}$,

$$\prod_{i=1}^{l}(1 - \sigma^{n_i}) = \prod_{i=1}^{l}(1-\sigma)(1 + \sigma + ... + \sigma^{n_i - 1}) \in (1-\sigma)^l \mathbb{Z}[\Gamma].$$

If $l = 2$, $(1-\sigma)^2 = 2(1-\sigma) \in l\mathbb{Z}[\Gamma]$, while if l is an odd prime the first and last terms cancel and $(1-\sigma)^l = \sum_{j=1}^{l-1} \binom{l}{j} \sigma^j \in l\mathbb{Z}[\Gamma]$. Since we know $|S \setminus S_H| \geq (m-1)l$ and each set of l factors in the product contributes at least a factor of l we conclude that $\left[\prod_{v \in S \setminus S_H} (1 - \sigma_v(M/k)^{-1})\right] \in l^{m-1}\mathbb{Z}[\Gamma]$. We conclude that $\phi\left(\frac{1}{|H|^r}\varepsilon_{M/k,S,T,r}\right) \in \mathbb{Z}[G]$, and so by linearity $\phi(\epsilon_{K/k,S,T}) \in \mathbb{Z}[G]$, which completes the proof. □

Corollary 5.2.2. *If our data satisfy all the hypothesis of Theorem 5.2.1 except the bound on $|S|$, we may still add sufficiently many primes to S so that the extended conjecture for K/k becomes true.*

Proof. Confer Example 4.0.12. □

Corollary 5.2.3. *If $G = G(K/k) \cong (\mathbb{Z}/l\mathbb{Z})^m$, $B(M/k, S', T, r)$ is true for every degree l extension of k contained in K and appropriate $S' \subseteq S$, S is a completely* *nontrivial r-cover and*

$$r \geq \frac{1}{l-1}\Big[|S_{\mathrm{ram}}| + |Pl_\infty| + (m-1)l - 1\Big]$$

then $\widetilde{B}(K/k,S,T)$ is true.

Proof. (Compare Proposition 4.6.2). We use the inequality from Lemma 2.4.2,

$$\sum_{\substack{\chi\in\widehat{G}\\ \chi\neq\mathbf{1}_G}} r_S(\chi) = \sum_{v\in S}(g_v - 1). \tag{5.3}$$

Since, by hypothesis, none of the primes in S split completely in K/k, it follows that each decomposition group is nontrivial and $g_v \leq l^{m-1}$. Since S is an r-cover for $\widehat{G}$, for every $\chi \in \widehat{G}$, $r_S(\chi) \geq r$. Substituting these estimates into (5.3) yields $(l^m - 1)r \leq (l^{m-1}-1)|S|$, or $|S| \geq \frac{l^m-1}{l^{(m-1)}-1}r > lr$. Since $|S|$ is an integer, $|S| \geq lr+1 = r+(l-1)r+1$, which, by hypothesis is at least $r+|S_{\mathrm{ram}}|+|Pl_\infty|+(m-1)l$. We are done by the previous Theorem. □

5.3 A Stark-type conjecture of Burns

Recently David Burns has proposed a conjecture which may imply conjecture B, and related conjectures of Gross and Tate. See [Bur04].

The conjecture predicts that in the standard situation of r splitting primes in K/k, for $\phi \in \bigwedge^r_{\mathbb{Z}[G]} U^*_{K,S,T}$ we have

$$\phi(\varepsilon_{K/k,S,T,r}) \equiv \pm h_{k,S,T}\mathrm{Reg}^\phi_G \pmod{I_G^{|S|-r}}$$

where I_G (the so-called *augmentation ideal*) is the kernel of $\mathbb{Z}[G] \xrightarrow{aug} \mathbb{Z}$; and Reg^ϕ_G is a canonical Gross-type regulator taking values in $\mathbb{Z}[G]$ and defined via local reciprocity maps and the isomorphism $G \cong I_G/I_G^2$. See [Hay04] for details.

In particular, this conjecture implies that, in our situation where r primes of S split in M/k, for $\phi = \phi_1 \wedge \ldots \wedge \phi_r \in \bigwedge^r_{\mathbb{Z}[G]} U^*_{K,S,T}$,

$$((N^*_{L/M})^r \phi)(\varepsilon_{M/k}) \in I^{|S|-r-1}_{G(M/k)}. \tag{5.4}$$

Hence if $G \cong (\mathbb{Z}/l\mathbb{Z})^m$ we may play off the same ideas as Section 5.2 state the following proposition:

Proposition 5.3.1. *Suppose l is a prime number, $G = G(K/k) \cong (\mathbb{Z}/l\mathbb{Z})^m$ and that Burns' conjecture as stated above is true for every degree l extension of k contained in K and appropriate $S' \subseteq S$. If*

$$|S| \geq r + (m-1)l + 1 \tag{5.5}$$

then $\widetilde{B}(K/k, S, T)$ is true.

Proof. For a $\mathbb{Z}/l\mathbb{Z}$-extension M/k with Galois group $\Gamma = \{1, \sigma\}$, we have $I_\Gamma = (\sigma - 1)\mathbb{Z}[\Gamma]$. But then $I^l_\Gamma \subseteq l\mathbb{Z}[\Gamma]$. Hence if $|S| - r - 1 \geq (m-1)l$, by equation (5.4) we have

$$((N^*_{L/M})^r \phi)(\varepsilon_{M/k}) \in l^{m-1}\mathbb{Z}[\Gamma].$$

The proof finishes exactly as that of Theorem 5.2.1. ☐

Corollary 5.3.2. *Suppose Burns' conjecture for degree l extensions. If S is a completely nontrivial r-cover, and $G \cong (\mathbb{Z}/l\mathbb{Z})^m$ and moreover*

$$r \geq \frac{l}{l-1}(m-1)$$

then $\widetilde{B}(K/k, S, T)$ is true.

Proof. This corollary follows from the previous proposition in exactly the same manner that Corollary 5.2.3 followed from Theorem 5.2.1. □

Corollary 5.3.3. *Suppose Burns' conjecture for degree l extensions. If S is a completely nontrivial r-cover, $G \cong (\mathbb{Z}/l\mathbb{Z})^2$ and $r \geq 2$ then $\widetilde{B}(K/k, S, T)$ is true.*

5.4 Counterexamples to potential conjectures

It is safe to say that Stark's rationality conjecture is believed to hold, i.e. $\epsilon_{K/k,S,T} \in \mathbb{Q}\bigwedge_{\mathbb{Z}[G]}^r U_{K,S,T}$ (actually the submodule thereof supported on the characters of minimal order of vanishing). The search for the correct lattice inside $\mathbb{Q}\bigwedge_{\mathbb{Z}[G]}^r U_{K,S,T}$ is still in progress. Indeed, Rubin settled on the condition $(\phi_1 \wedge \ldots \wedge \phi_r)(\varepsilon) \in \mathbb{Z}[G]$ only after realizing that the more natural first guess of $\bigwedge_{\mathbb{Z}[G]}^r U_{K,S,T}$ itself was incorrect.

There is a relatively large amount of support for Rubin's lattice $\Lambda_{S,T}$ in the case of the *standard* conjecture. However we have only provided very partial support for the use of it for the extended conjectures in this dissertation. (This is perhaps more likely to be due to weaknesses in this author's methods of proof than to the lattice?) In any case, because of the result of Proposition 3.4.3, if one believes the standard Rubin conjecture, then the correct lattice is some sublattice of $\frac{1}{|G|}\Lambda_{S,T}$. Indeed by examining that proof more closely, one sees that $\frac{1}{c}\Lambda_{S,T}$ can be used where

$$c = \mathrm{lcm}_{I \in \mathcal{P}_r(S_{\min})} |D_I|.$$

We have also proven $\Lambda_{S,T}$ itself can be used when S has a sub-r-cover consisting of finite unramifying primes, or in multiquadratic extensions when T is sufficiently large.

The statement of the conjecture $\widetilde{B}$ included the hypothesis $S \neq S_{\min}$. The case $S = S_{\min}$ may be viewed as a 'boundary case,' and often a different conclusion follows in boundary cases. For example, in the introduction we only introduced Stark's First Order Abelian Conjecture under the hypothesis $|S| \geq 3$ to avoid a more complicated formulation of what happens when $|S| = 2$. For the extended conjecture, when $S = S_{\min}$ and $r = 1$ there is numerical evidence that at times $\epsilon_{K/k,S,T} \notin \Lambda_{S,T}$. See [Eri05, Section 4.2] for the explicit construction.

Another hypothesis that might be imposed in lieu of '$S \neq S_{\min}$' is that the decomposition groups of the primes in S generate the full Galois group of K/k. This condition is equivalent to $H_{k,S} \cap K = k$, where $H_{k,S}$ is the maximal everywhere unramified abelian extension of k in which all primes of S split completely. Hence by imposing this condition, we would not gain information about a class of very interesting examples when $A_{k,S}$ is nontrivial. For example, we could not investigate examples similar to that Rubin gives to demonstrate the need for the lattice $\Lambda_{S,T}$, i.e. ones where all or most of the primes in S split in K/k.

It would be interesting to discover the 'right' lattice to capture the evaluators as closely as possible, including one that captures components arising from non-minimal order of vanishing L-functions.

Appendix

Characterizing central extensions

Throughout this appendix, K/k is an abelian extension of number fields, $G = G(K/k)$, μ_K denotes the roots of unity in K and $w_K = \#\mu_K$. In what follows, every occurance of U_K may be interepreted as $U_{K,S}$ for any set of primes S containing all Archimedean places. We arbitrarily fix a function

$$N : G \longrightarrow \mathbb{Z} \tag{A.1}$$

such that $\zeta^\sigma = \zeta^{N\sigma}$ for all $\zeta \in \mu_K$. Let $U_{K/k}^{\mathrm{ab}}$ denote the set of units of K whose w_K-th root is abelian over k. There is a (non-injective) map $U_K \to \mathbb{Q}U_K$ sending u to $\widetilde{u} = 1 \otimes u$. This map annihilates torsion (all roots of unity get sent to 1). The image of U_K under this map is denoted $\widetilde{U_K}$. As usual, k^{ab} denotes the maximal abelian extension of k.

The following characterization of when adjoining a w_K-*th* root of an S-unit to K generates an extension that is abelian over k can be found in [Tat84, Proposition IV.1.2]. It is due originally to Coates [Coa77], and we shall refer to it as 'Coates condition.'

Proposition A.0.1. *Let $\{\sigma_i\}_{i\in I}$ be a system of generators for G. For any $u \in \mathbb{Q}U_K$, the following are equivalent:*

(i) There exists an $\varepsilon \in U_{K/k}^{\text{ab}}$ such that $u^{w_K} = \widetilde{\varepsilon}$.

(ii) There exists a field $L \subseteq k^{ab}$ such that $u \in \widetilde{U_L}$.

(iii) For almost all finite places $\mathfrak{p}$ of k unramified in K, there exists $\varepsilon_{\mathfrak{p}} \in U_K$ such that $\varepsilon_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{p}\mathcal{O}_K}$ and $\widetilde{\varepsilon_{\mathfrak{p}}} = u^{\sigma_{\mathfrak{p}} - N\mathfrak{p}}$.

(iv) There exists $\varepsilon \in U_K$ and $\{\alpha_i\}_{i\in I} \subseteq U_K$ such that $u^{w_K} = \widetilde{\varepsilon}$, $\forall i, j \in I$

$$\alpha_i^{\sigma_j - N\sigma_j} = \alpha_j^{\sigma_i - N\sigma_i}$$

and $\varepsilon^{\sigma_i - N\sigma_i} = \alpha_i^{w_K}$.

A.1 An analogue of Coates' condition

The aim of this appendix is to prove a similar type of characterization of when the extension $L = K(\varepsilon^{1/w_K})$ is not necessarily abelian, but merely central over k.

Definition A.1.1. *Recall that a group extension*

$$1 \longrightarrow H \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 1 \tag{A.2}$$

is called central *if H is contained in the center of $\mathcal{G}$, i.e., any element $h \in H$ commutes with every element of $\mathcal{G}$. A series of field extensions $L/K/k$ with L/k and K/k Galois is called* central *if the corresponding exact sequence of Galois groups*

$$1 \longrightarrow G(L/K) \longrightarrow G(L/k) \longrightarrow G(K/k) \longrightarrow 1 \tag{A.3}$$

is central.

We may consider the group of roots of unity μ_K as a $\mathbb{Z}[G]$-module (any field automorphism will take a root of unity to another root of unity).

Definition A.1.2. *Let*

$$\mathcal{A}(K/k) := \mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K) \subseteq \mathbb{Z}[G]$$

be the annihilator ideal of μ_K under this action.

It can be shown (see [Tat84, Lemme IV.1.1]) that $\mathcal{A}(K/k)$ is generated over $\mathbb{Z}$ by the elements $(\sigma_{\mathfrak{p}} - N\mathfrak{p})$ as $\mathfrak{p}$ runs through the set of primes of k unramified in K/k.

We begin by studying general Kummer extensions of an abelian extension K/k. (A Kummer extension of K is any extension obtained by adjoining to K the w_K*-th* roots of elements of K.) Choose a subgroup $\Delta \subseteq K^\times/(K^\times)^{w_K}$ and $L = K(\sqrt[w_K]{\Delta})$.

Lemma A.1.3. *The extension $L = K(\sqrt[w_K]{\Delta})$ is Galois over k if and only if Δ is a $\mathbb{Z}[G]$-module.*

Proof. ($\Rightarrow$) Suppose L/k is Galois. Let $\sigma \in G$ and $\overline{\delta} \in \Delta$. Let $\widetilde{\sigma}$ be any lift of σ into $\mathcal{G} = G(L/k)$. Fix η as a w_K-th root of δ. Since $\eta^{\widetilde{\sigma}} \in L$, δ^σ is a w_K-th power of an element of L, and hence by Kummer theory $\overline{\delta}^\sigma \in \Delta$.

($\Leftarrow$) Suppose Δ is a $\mathbb{Z}[G]$-module. Let $\eta \in L$ be a fixed w_K-th root of some δ with $\overline{\delta} \in \Delta$. Let $\mathcal{L}$ be the normal closure of L/k, and $\gamma \in G(\mathcal{L}/k)$. As K/k is Galois, clearly $\gamma(K) = K$. Next we notice that $\eta^\gamma = (\delta^\gamma)^{1/w_K}$ is the w_K-th root of something which, by hypothesis, is in Δ. Therefore $\eta^\gamma \in L$. Since this hold for all generators of L/K, $\gamma(L) = L$. Therefore L/k is Galois. ☐

Lemma A.1.4. *A Kummer extension* $L = K(\sqrt[w_K]{\Delta})$ *is central over* k *if and only if* Δ *is annihilated by* $\mathcal{A}(K/k)$ *in* $K^\times/(K^\times)^{w_K}$.

Proof. ($\Rightarrow$) Suppose $L/K/k$ is a central extension. Pick $\overline{\delta} \in \Delta$, and $\sigma \in G = G(K/k)$. Fix a root, $\eta = \delta^{1/w_K}$. Let $a \in \mathcal{A}(K/k)$. Fix $h \in H = G(L/K)$. Then $\eta^{h-1} = \zeta$ is a root of unity. We compute (using centrality)

$$\eta^{a(h-1)} = \eta^{(h-1)a} = \zeta^a = 1.$$

Thus η^a is fixed by H, so $\eta^a \in K^\times$ which means $\delta^a \in (K^\times)^{w_K}$.

($\Leftarrow$) Suppose Δ is annihilated by $\mathcal{A}(K/k)$. First we prove that L/k is Galois. Let g be an element of $G = G(K/k)$. Let $\overline{\delta} \in \Delta$. Then

$$\overline{\delta^g} = \overline{\delta^{g-Ng+Ng}} = \overline{\alpha^{w_K}\delta^{Ng}} = \overline{\delta^{Ng}} \in \Delta.$$

Hence Δ is a $\mathbb{Z}[G]$-module, so by Lemma A.1.3, L/k is Galois.

Now take $h \in H = G(L/K)$. For $x \in K$ it is clear that $x^{gh} = x^{hg}$. It remains to verify that the same holds for elements of $\sqrt[w_K]{\Delta}$. Let $\eta = \delta^{1/w_K}$ be such an element, so that $\eta^h = \zeta\eta$ for a root of unity ζ. By hypothesis $\eta^{g-Ng} = \alpha$ for some $\alpha \in K$. Then

$$\begin{aligned}
\eta^{gh-hg} &= \eta^{gh-(Ng)h+(Ng)h-hg} \\
&= \eta^{(g-Ng)h}\eta^{h(Ng-g)} \\
&= \alpha^h(\zeta\eta)^{-(g-Ng)} \\
&= \alpha\alpha^{-1} \\
&= 1.
\end{aligned}$$

□

Let $\mathcal{T}$ be a finite set of non-Archimedean primes of k such that

(1) $\mathcal{T}$ does not contain any primes that ramify in K/k or that divide $w_K\mathcal{O}_k$,

(2) for every $\tau \in G$ there is a $\mathfrak{q} \in \mathcal{T}$ such that $\sigma_{\mathfrak{q}} = \tau$, and

(3) $\{\sigma_{\mathfrak{p}} - N\mathfrak{p} \mid \mathfrak{p} \in \mathcal{T}\}$ generates $\mathcal{A}(K/k)$ as a $\mathbb{Z}$-module.

Then there are sets of integers $\{b_{\mathfrak{p}}\}$ and $\{b_{i\mathfrak{p}}\}$ such that

$$w_K = \sum_{\mathfrak{p}\in\mathcal{T}} b_{\mathfrak{p}}(\sigma_{\mathfrak{p}} - N\mathfrak{p}), \tag{A.4}$$

and

$$\sigma_i - N\sigma_i = \sum_{\mathfrak{p}\in\mathcal{T}} b_{i\mathfrak{p}}(\sigma_{\mathfrak{p}} - N\mathfrak{p}). \tag{A.5}$$

Of course we may (and do) choose the $b_{\mathfrak{p}}$'s so that they are nonzero only if $\mathfrak{p}$ splits completely in K/k.

The next proposition accomplishes our goal in establishing a condition for centrality which is the analogue of Coates condition for abelianness.

Proposition A.1.5. *Let $u \in \mathbb{Q}U_K$, $\{\sigma_i\}_{i\in I}$ be a system of generators for G and $\mathcal{T}$ be as above. The following are equivalent.*

(i) There is an $\varepsilon \in U_K$ such that $u^{w_K} = \widetilde{\varepsilon}$ and $K(\varepsilon^{1/w_K})/K/k$ is central.

(ii) There exists a collection $\{\alpha_i\}_{i\in I} \subseteq U_K$ and an $\varepsilon \in U_K$ such that $\widetilde{\varepsilon} = u^{w_K}$ and for all $i \in I$, $\alpha_i^{w_K} = \varepsilon^{\sigma_i - N\sigma_i}$.

(iii) There exists a collection of units $\{\varepsilon_{\mathfrak{p}}\}_{\mathfrak{p}\in\mathcal{T}} \subseteq U_K$ such that $u^{\sigma_{\mathfrak{p}} - N\mathfrak{p}} = \widetilde{\varepsilon_{\mathfrak{p}}}$ and for all $\mathfrak{p}$ in $\mathcal{T}$ which split completely in K/k, $\varepsilon_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{p}\mathcal{O}_K}$.

Proof. $(i) \Leftrightarrow (ii)$: This is a special case of Lemma A.1.4.

$(i) \Rightarrow (iii)$: Let $L = K(\varepsilon^{1/w_K})$. Fix a root $\eta = \varepsilon^{1/w_K}$. For each $\mathfrak{p} \in \mathcal{T}$ arbitrarily choose a prime $\mathfrak{P}$ of L dividing $\mathfrak{p}$. We define $\varepsilon_{\mathfrak{p}} = \eta^{\sigma_{\mathfrak{P}} - N\mathfrak{p}}$. (Note that this *does* depend on our choice of $\mathfrak{P}$, but we suppress this from the notation). We verify that indeed $\varepsilon_{\mathfrak{p}}$ is in K. This is because if $h \in H = G(L/K)$,

$$\varepsilon_{\mathfrak{p}}^{h-1} = \eta^{(h-1)(\sigma_{\mathfrak{P}} - N\mathfrak{p})} = \zeta^{\sigma_{\mathfrak{P}} - N\mathfrak{p}} = 1.$$

If $\mathfrak{p} \in \mathcal{T}$ splits completely in K/k then under the identification $G \cong \mathcal{G}/H$, we have $\sigma_{\mathfrak{p}} = 1 \cdot H$. For any other prime $\mathfrak{q} \in \mathcal{T}$,

$$\frac{\varepsilon_{\mathfrak{p}}^{\sigma_{\mathfrak{q}} - N\mathfrak{q}}}{\varepsilon_{\mathfrak{q}}^{\sigma_{\mathfrak{p}} - N\mathfrak{p}}} = \eta^{\sigma_{\mathfrak{P}}\sigma_{\mathfrak{Q}} - \sigma_{\mathfrak{Q}}\sigma_{\mathfrak{P}}}$$

where of course $\mathfrak{Q}$ is our chosen prime of L that divides $\mathfrak{q}$. But as $\sigma_{\mathfrak{P}} \in H$, it commutes with $\sigma_{\mathfrak{Q}}$ (by assumed centrality), so the ratio is 1. Therefore

$$\varepsilon_{\mathfrak{p}}^{\sigma_{\mathfrak{q}} - N\mathfrak{q}} = \varepsilon_{\mathfrak{q}}^{\sigma_{\mathfrak{p}} - N\mathfrak{p}}. \tag{A.6}$$

Let $\wp$ be the prime of K below $\mathfrak{P}$. Because $\varepsilon_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{P}}$ and $\varepsilon_{\mathfrak{p}} \in K$, it follows $\varepsilon_{\mathfrak{p}} \equiv 1 \pmod{\wp}$. Hence also $\varepsilon_{\mathfrak{p}}^{-N\mathfrak{q}} \equiv 1 \pmod{\wp}$.

Now reduce equation (A.6) modulo $\wp$ to get $\varepsilon_{\mathfrak{p}}^{\sigma_{\mathfrak{q}}} \equiv 1 \pmod{\wp}$, or equivalently $\varepsilon_{\mathfrak{p}} \equiv 1 \pmod{\wp^{\sigma_{\mathfrak{q}}^{-1}}}$. Therefore, letting $\sigma_{\mathfrak{q}}^{-1}$ range over the Galois group G (which we may do because of condition (2) on $\mathcal{T}$), we find that $\varepsilon_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{p}\mathcal{O}_K}$.

(iii) $\Rightarrow$ *(ii)*. Suppose the collection $\{\varepsilon_{\mathfrak{p}}\}_{\mathfrak{p}\in\mathcal{T}} \subseteq U_K$ with the stated properties is given. We define

$$\varepsilon = \prod_{\mathfrak{p}\in\mathcal{T}} \varepsilon_{\mathfrak{p}}^{b_{\mathfrak{p}}},$$

and

$$\alpha_i = \prod_{\mathfrak{p}\in\mathcal{T}} \varepsilon_{\mathfrak{p}}^{b_{i\mathfrak{p}}}.$$

Remember that we have chosen the $b_{\mathfrak{p}}$ such that $b_{\mathfrak{p}} \neq 0$ implies $\mathfrak{p}$ splits completely in K/k. In this case, by hypothesis, $\varepsilon_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{p}\mathcal{O}_K}$. Suppose $\mathfrak{p}$ is such a prime and $\mathfrak{q}$ is any other prime of $\mathcal{T}$. Then as

$$\widetilde{\varepsilon_{\mathfrak{p}}^{\sigma_{\mathfrak{q}}-N\mathfrak{q}}} = \widetilde{\varepsilon_{\mathfrak{q}}^{\sigma_{\mathfrak{p}}-N\mathfrak{p}}},$$

these two elements must differ by a root of unity. But in this case the root of unity must be congruent to 1 modulo $\mathfrak{p}\mathcal{O}_K$. By our hypothesis on $\mathcal{T}$, it follows that this root of unity is actually equal to one. That is

$$\varepsilon_{\mathfrak{p}}^{\sigma_{\mathfrak{q}}-N\mathfrak{q}} = \varepsilon_{\mathfrak{q}}^{\sigma_{\mathfrak{p}}-N\mathfrak{p}}$$

when $b_{\mathfrak{p}} \neq 0$.

One computes

$$\begin{aligned} \varepsilon^{\sigma_i - N\sigma_i} &= \left[\prod_{\mathfrak{p}\in\mathcal{T}} \varepsilon_{\mathfrak{p}}^{b_{\mathfrak{p}}}\right]^{\sum_{\mathfrak{q}\in\mathcal{T}} b_{i\mathfrak{q}}(\sigma_{\mathfrak{q}}-N\mathfrak{q})} \\ &= \prod_{\mathfrak{p},\mathfrak{q}\in\mathcal{T}} \varepsilon_{\mathfrak{p}}^{b_{\mathfrak{p}} b_{i\mathfrak{q}}(\sigma_{\mathfrak{q}}-N\mathfrak{q})} \\ &= \prod_{\mathfrak{p},\mathfrak{q}\in\mathcal{T}} \varepsilon_{\mathfrak{q}}^{(\sigma_{\mathfrak{p}}-N\mathfrak{p}) b_{\mathfrak{p}} b_{i\mathfrak{q}}} \\ &= \alpha_i^{w_K} \end{aligned}$$

as needed. □

A.2 Application to Stark's conjectures

The reason Coates' condition (Proposition A.0.1) is important is that it gives a new way to formulate the statement '$K(\varepsilon^{1/w_K})/k$ is abelian' in terms of T-moditified unit groups as we let $T = \{v_T\}$ with v_T varying over a set of primes as in part (iii) of the proposition. (Here ε is of course the Stark unit arising from the First Order Integral Stark conjecture.) That is, this proposition establishes the link between Rubin's formulation and Stark's formulation of the integral conjecture when $r = 1$. Harold Stark has claimed that his original prediction or "all he needed" was that $K(\varepsilon^{1/w_K})/K/k$ be a central extension. Yet in every case of the original first order Stark conjecture, the extension was found to be abelian. None-the-less, it was of interest to see what exactly is needed to achieve a central extension.

Proposition A.0.1 is also apparent in the difference between conjectures B and C (and $\widetilde{B}$ and $\widetilde{C}$). Both B and C reduce to Stark's original formulation when $r = 1$, but each generalizes the abelian condition in a different way to higher order. Let us examine the idea in C and use this to formulate another statement where we replace 'abelianness' with 'centrality' in the higher order of vanishing situation.

An alternate formulation of conjecture $C(K/k, S, r)$ is to take $T = \emptyset$ and require that

$$\phi_1 \wedge \ldots \wedge \phi_{r-1}(\varepsilon_{K/k,S}) \in \frac{1}{w_K} U^{\mathrm{ab}}_{K/k,S}$$

for all $\phi_1, \ldots, \phi_{r-1} \in U^*_{K,S}$. It then becomes natural to ask instead that

$$\phi_1 \wedge \ldots \wedge \phi_{r-1}(\varepsilon_{K/k,S}) \in \frac{1}{w_K} U^{\mathrm{cent}}_{K/k,S}$$

for all $\phi_1, \ldots, \phi_{r-1} \in U^*_{K,S}$. Here of course $U^{\mathrm{cent}}_{K/k,S}$ denotes those S-units u for which $K(u^{1/w_K})/K/k$ is a central extension.

According to our main result in this appendix, Proposition A.1.5, this means we might formulate a conjecture weaker even that $\widetilde{C}$. In this weaker conjecture we let

$T = \{v_T\}$ run through the sets of cardinality one such that (S, T) is appropriate, and for all $\phi_1, \ldots, \phi_{r-1} \in U^*_{K,S}$, we ask that

$$\phi_1 \wedge \ldots \wedge \phi_{r-1}(\epsilon_{K/k,S,T}) \in U$$

where $U = U_{K,S,T}$ if v_T splits completely in K/k and $U = U_{K,S}$ otherwise.

Although currently we have not proven any further cases of this weakened conjecture than those implied by $\widetilde{B}$, it is quite conceivable that this may be the more natural statement, given the propensity of the results in Chapter 4 to require that T contain primes *which split completely* in K/k (see e.g. Proposition 4.4.1).

Bibliography

[Bur04] David Burns. Congruences between derivatives of abelian L-functions at $s = 0$. *Preprint*, 2004.

[Cas67] *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London, 1967.

[CH88] P. E. Conner and J. Hurrelbrink. *Class number parity*, volume 8 of *Series in Pure Mathematics*. World Scientific Publishing Co., Singapore, 1988.

[Coa77] John Coates. p-adic L-functions and Iwasawa's theory. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 269–353. Academic Press, London, 1977.

[DF91] David S. Dummit and Richard M. Foote. *Abstract algebra*. Prentice Hall Inc., Englewood Cliffs, NJ, 1991.

[dS01] Bart de Smit. Brauer-Kuroda relations for S-class numbers. *Acta Arith.*, 98(2):133–146, 2001.

[DST03] David S. Dummit, Jonathan W. Sands, and Brett Tangedal. Stark's conjecture in multi-quadratic extensions, revisited. *J. Théor. Nombres Bordeaux*, 15(1):83–97, 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[Eri05] Stefan Erickson. *New Settings of the First Order Stark Conjectures*. PhD thesis, University of California, San Diego, 2005.

[Gra03] Georges Gras. *Class field theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. From theory to practice, Translated from the French manuscript by Henri Cohen.

[Gro88] Benedict H. Gross. On the values of abelian L-functions at $s = 0$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 35(1):177–197, 1988.

[Hay04] A. Hayward. A class number formula for higher derivatives of abelian L-functions. *Compos. Math.*, 140(1):99–129, 2004.

[Ion04] Costel Ionita. *Class Groups and Norms of Units*. PhD thesis, Louisiana State University, 2004.

[Jan73] Gerald J. Janusz. *Algebraic number fields*. Academic Press [A Subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973. Pure and Applied Mathematics, Vol. 55.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Pop02] Cristian D. Popescu. Base change for Stark-type conjectures "over $\mathbb{Z}$". *J. Reine Angew. Math.*, 542:85–111, 2002.

[Pop04] Cristian D. Popescu. Rubin's integral refinement of the abelian Stark conjecture. In *Stark's conjectures: recent work and new directions*, volume 358 of *Contemp. Math.*, pages 1–35. Amer. Math. Soc., Providence, RI, 2004.

[Pop06] Cristian D. Popescu. Stark-type conjectures "over $\mathbb{Z}$". *In preparation*, 2006.

[Rei03] Michael Reid. The local Stark conjecture at a real place. *Compositio Math.*, 137(1):75–90, 2003.

[Rub96] Karl Rubin. A Stark conjecture "over $\mathbf{Z}$" for abelian L-functions with multiple zeros. *Ann. Inst. Fourier (Grenoble)*, 46(1):33–62, 1996.

[San04] Jonathan W. Sands. Popescu's conjecture in multi-quadratic extensions. In *Stark's conjectures: recent work and new directions*, volume 358 of *Contemp. Math.*, pages 127–141. Amer. Math. Soc., Providence, RI, 2004.

[Sta71] H. M. Stark. Values of L-functions at $s = 1$. I. L-functions for quadratic forms. *Advances in Math.*, 7:301–343 (1971), 1971.

[Sta75] H. M. Stark. L-functions at $s = 1$. II. Artin L-functions with rational characters. *Advances in Math.*, 17(1):60–92, 1975.

[Sta76] H. M. Stark. L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem. *Advances in Math.*, 22(1):64–84, 1976.

[Sta80] H. M. Stark. L-functions at $s = 1$. IV. First derivatives at $s = 0$. *Adv. in Math.*, 35(3):197–235, 1980.

[Tat84] John Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, volume 47 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1984. Lecture notes edited by Dominique Bernardi and Norbert Schappacher.