Artin's L-functions: A Historical Approach

Noah Snyder
nsnyder@fas.harvard.edu
(617)493–3454

Supervised by Professor Benedict H. Gross

A thesis presented to the Department of Mathematics
in partial fulfillment of the requirements
for the degree of Bachelor of Arts with Honors

Harvard University
Cambridge, Massachusetts
April 1, 2002

I would like to thank my advisor, Professor Benedict Gross, for all of his advice and suggestions. Thanks also to Jared Weinstein, Paul Pollack, and Professor Keith Conrad for their answers to various questions which I stumbled upon along the way. I would like to thank Professors Arnold Ross and Daniel Shapiro, who instilled in me a love for number theory. Furthermore, I am very grateful to my parents who not only taught me for twelve years, but also were kind enough to help me with editing this thesis. I would like to thank Altavista whose Babel Fish program let me read German. Lastly, I would like to thank Emil Artin and all the other mathematicians whose work I have come to know and love while writing this thesis.

Contents

0.1 Introduction . . . 5

1 ζ and L-functions before Artin **7**

1.1 Euler and Euler Factorization . . . 8
1.1.1 Introduction . . . 8
1.1.2 Some Elementary Results on the Distribution of Primes . . . 8
1.1.3 Euler Factorization . . . 9
1.1.4 General Principles of Analytic Number Theory . . . 14
1.1.5 Euler and the Functional Equation of the Zeta Function . . . 14
1.2 Dirichlet and his L-series . . . 17
1.2.1 Introduction . . . 17
1.2.2 Elementary Results on Primes in Arithmetic Progressions . . . 17
1.2.3 A Special Case of Dirichlet's Theorem . . . 17
1.2.4 Some General Results on Dirichlet Series . . . 18
1.2.5 Dirichlet's L-series . . . 20
1.2.6 Reducing Dirichlet's Theorem to an Analytic Theorem . . . 21
1.2.7 A Full Proof of $L\left(1, \left(\frac{\cdot}{p}\right)\right) \neq 0$ for p Prime . . . 23
1.3 Riemann and the Functional Equation . . . 26
1.3.1 Introduction . . . 26
1.3.2 Analytically Continuing the Zeta Function . . . 26
1.3.3 Proving Euler's Special Values . . . 28
1.3.4 Riemann's Second Proof of the Functional Equation . . . 28
1.4 Dedekind ζ-functions and Hecke L-series . . . 30
1.4.1 Introduction . . . 30
1.4.2 Unique Factorization and Rings of Integers . . . 30
1.4.3 The Norm and the Trace . . . 32
1.4.4 The Dedekind Zeta Function . . . 33
1.4.5 Hecke's Größencharakters . . . 33
1.4.6 Characters of $(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$ . . . 34
1.4.7 Hecke L-Functions . . . 35
1.4.8 Discriminants . . . 35
1.4.9 The Gamma Factor . . . 35
1.4.10 The Functional Equation of the Hecke L-function . . . 36
1.5 Frobenius, the Frobenius Automorphism, and Group Representation Theory . . . 37
1.5.1 Introduction . . . 37
1.5.2 Factoring Primes in Extensions . . . 37
1.5.3 The Decomposition and Inertia Groups, and the Frobenius Automorphism . . . 38
1.5.4 The Frobenius Density Theorem . . . 40
1.5.5 Group Representation Theory . . . 42
1.6 Class Field Theory Before Artin . . . 46
1.6.1 Introduction . . . 46
1.6.2 Kronecker and the First Dreams of Class Field Theory . . . 46
1.6.3 An Application of the Frobenius Density Theorem . . . 47

1.6.4 Weber and the First Results of Class Field Theory . . . 47
1.6.5 Generalized Dirichlet L-series . . . 50
1.6.6 A proof of the First Fundamental Inequality . . . 51
1.6.7 Hilbert, Furtwangler, and Takagi . . . 52

2 Artin L-functions **55**
2.1 Artin L-functions, Their Definition, and Their Most Basic Properties . . . 56
2.1.1 Introduction . . . 56
2.1.2 Factoring the ζ-function of an Abelian Extension . . . 56
2.1.3 Defining the Artin L-function . . . 57
2.1.4 Additivity and the Artin L-function of a (Generalized) Character . . . 58
2.1.5 The L-series Attached to the Pullback . . . 59
2.2 The Artin L-function of an Induced Representation . . . 60
2.2.1 Hecke's Formula in Terms of Artin L-functions . . . 60
2.2.2 A Proof of the Induction Formula . . . 60
2.3 Artin Reciprocity . . . 62
2.3.1 Statement of Artin Reciprocity . . . 62
2.3.2 Why is This a Reciprocity Theorem? . . . 62
2.3.3 Chebotarev's Density Theorem . . . 64
2.4 Artin's Theorem and Generalizing from the Abelian Case . . . 65
2.4.1 Artin's Theorem . . . 65
2.4.2 Analytic Continuation and the Completed Artin L-series . . . 66
2.4.3 Conditions for Extending Functions on Cyclic Subgroups . . . 67
2.4.4 Our Program for Constructing the Completed Artin L-function . . . 69
2.5 The Local Factors for Ramified Primes . . . 70
2.5.1 Introduction . . . 70
2.5.2 Definition . . . 70
2.5.3 The Basic Properties of the Local Factors for Ramified Primes . . . 71
2.5.4 An Application to ζ-function Formulas . . . 73
2.6 The Local Factors for Infinite Primes . . . 75
2.6.1 Introduction . . . 75
2.6.2 Definition and Basic Properties . . . 75
2.7 Background for the Artin Conductor: Local Class Field Theory and the Theory of Higher Ramification Groups . . . 77
2.7.1 Introduction . . . 77
2.7.2 Valuations and Discrete Valuation Rings . . . 77
2.7.3 Extensions of $\mathfrak{p}$-adic Fields . . . 78
2.7.4 Computing Ramification Degrees . . . 80
2.7.5 Higher Ramification Groups . . . 80
2.7.6 Local Class Field Theory . . . 82
2.7.7 The Reciprocity Map and Filtrations . . . 82
2.8 The Artin Conductor . . . 84
2.8.1 Introduction . . . 84
2.8.2 Reformulating the Abelian Conductor . . . 85
2.8.3 Generalizing the New Formula to Higher Dimensional Representations . . . 85
2.8.4 The Global Artin Conductor . . . 88
2.9 The Functional Equation of the Artin L-function . . . 90

3 Computing the Completed Artin L-functions for the Splitting Field of $x^3 - n$ over $\mathbb{Q}$ **91**
3.1 The Splitting Field of $x^3 - n$ . . . 92
3.1.1 Introduction . . . 92
3.1.2 Representations of G and its Subgroups . . . 92
3.1.3 Factoring the Ramified Primes . . . 92
3.1.4 Decomposition and Inertia Groups . . . 93

3.2 Computing the Local Factors for the Finite Primes . . . 94
3.2.1 Introduction . . . 94
3.2.2 Computing $L_{\mathfrak{p}}(s, V_0)$ and $L_{\mathfrak{p}}(s, V_1)$ . . . 94
3.2.3 Computing $L_{\mathfrak{p}}(s, V_2)$ . . . 94
3.2.4 Checking the Product Formula for $\zeta_K(s)$. . . . 96
3.3 Computing the Local Factors for the Infinite Primes . . . 97
3.4 Computing the Artin Conductor and Exponential Factors . . . 98
3.4.1 Introduction . . . 98
3.5 The Local Conductor for Primes Other Than 3 . . . 98
3.6 The Local Conductor for 3 . . . 98
3.6.1 The Führerdiskriminantenproduktformel . . . 101
3.6.2 Using Machinery to find the Artin Conductors Without Extensive Computation . 101
3.6.3 Some Calculations Cited Earlier . . . 102
3.7 The Completed L-series for the Splitting Field of $x^3 - n$. . . . 104

A Artin's Paper, Über eine neue Art von L-Reihen **105**
A.1 . . . 106
A.2 . . . 107
A.3 . . . 108
A.4 . . . 110
A.5 . . . 111
A.6 . . . 114
A.7 . . . 116
A.8 . . . 116
A.9 . . . 117

0.1 Introduction

In 1923 Emil Artin published a paper in which he defined a new kind of L-function which now bears his name. This remarkably short paper was instrumental in the direction of research in number theory for much of this century. The goal of this thesis is to give Artin's definitions and to prove the results which he proved in his paper *Über eine neue Art von L-Reihen* [**Ar**, p. 105], while putting these ideas within a larger historical framework. To that end, in the first chapter we discuss the historical development of the ideas on which Artin's work depended. We will consider the ζ and L-functions defined by Euler, Dirichlet, Riemann, Dedekind, and Hecke, and get a flavor of their properties. The goal here is not to simply reproduce the historical arguments, but rather to give a flavor of the historical chain of ideas. Thus, when it is appropriate, we will eschew the original proof of a result for a cleaner one along similar lines. However, when it is possible, we do include the original language or a reference to the original paper, and we try at all costs to avoid using a modern argument or definition when a reasonable classical alternative is available.

Why, you might ask, such an emphasis on the historical progression of ideas? After all, a quick glance at some of the works which we quote shows that they often lack the rigor of modern mathematics and are almost quaint in their lack of sophistication. One reason to deal with the originals is that they give a very natural motivation for the introduction of these concepts. The sterile presentation of definitions that seem to come from nowhere is frustrating at best and, at worst, terribly misleading. If one wants to understand the way mathematics is done and learn to invent or discover new mathematics, then it is important not only to understand the ideas as they are thought about now, but also to understand why some actual person sitting somewhere with a pen and paper would ever have thought of writing down a certain definition or argument. The history of mathematical ideas is not simply a collection of enjoyable stories about various personalities, but is actually quite fundamental part of doing mathematics. Another reason for taking a historical approach is that the mathematicians whose work we will be studying are absolute giants of the field. By seeing their results in their original forms we get a glimpse of how the minds of these brilliant mathematicians worked and perhaps let some of their patterns of thought teach us how to think about mathematics. I would hope that the reader of this paper might be inspired to dig up old rarely read papers by the original masters and get a glimpse of the beauty that is the process of mathematics. Finally, if we are to stand on the shoulders of giants, we owe it to them to actually look at what they have done.

On the other hand, one can certainly go too far in following mathematics from a historical point of view. There are many dead ends and vestigial organs in mathematics. Often the progression of ideas is disorganized and tumbles out of order. Thus, while keeping history in mind, we will not be enslaved to it. In the second half of the first chapter, the ideas are arranged not chronologically but by themes. Furthermore, whenever it is necessary to omit a proof, I include whenever possible both a modern and a classical source for the proof. Most importantly, if the original sources lacked rigor, it is crucial that we fill in these gaps.

Chapter 1 provides background for the rest of the thesis, and is mostly of historical interest. Thus someone who is well acquainted with the definitions and basic properties of the Riemann ζ-function, Dirichlet L-functions, Hecke L-functions, and algebraic number theory up through basic class field theory can easily skip the first chapter or skim it to find sections of particular interest. (For example, Euler's investigations into the functional equation of the ζ-function and Dirichlet's original proof of the non-vanishing of $L(1, \chi)$ in the prime case are probably unfamiliar to most number theorists.)

In Chapter 2, we will begin by giving the basic definitions and outline what Artin accomplishes in his paper. In the next few sections, we will prove the basic results which Artin proves in this paper. The rest of the chapter will be devoted to answering some of the important questions which Artin raised in his paper and which were answered over the next decade or so. In particular in the second chapter we prove the basic functorial properties of the local factors of the Artin L-function for unramified primes. Then we discuss the connection between 1-dimensional Artin L-functions and Hecke's abelian L-functions given by Artin reciprocity. We use this connection and Artin's theorem in representation theory to give a program for generalizing all of the parts of the completed L-function from the abelian case to the non-abelian case. This program will be carried out for the ramified primes, the infinite primes, and the Artin conductor. Once we have nice definitions of all these factors, we will end Chapter 2 with the

functional equation of the Artin L-function (ignoring completely the problem of determining the root number). Here we continue to make an effort to show these ideas in their historical context. However, more than in the first chapter, we use modern ideas when they simplify the presentation. In particular, in the section on the Artin conductor we use notions from local fields and local class field theory which are crucial to our modern understanding of this theory but would have been completely foreign to Artin when he defined the Artin conductor.

Chapter 3 is an in-depth explanation of what these definitions mean for the particular example of the splitting field of $x^3 - n$ over $\mathbb{Q}$. This section is computational in nature. Rather than using the powerful theorems which we have developed in the previous sections, we favor direct computation as a means of verifying these results. Working through examples directly in this way is important since many of these results could not have been observed without getting one's hands dirty in the first place. Furthermore only by actually going through a computation does it become apparent how useful certain theorems can be. Once we have verified these theorems by hand we will also note how the computations can be simplified using more machinery.

Lastly we include an appendix with an English translation of Artin's paper *Über eine neue Art von L-Reihen*, since it is a little silly to extol the virtues of experiencing original mathematics and then bury the references in the bibliography, expecting the reader to learn to read German and dig up the article in a library. Since there are no published English translations of this paper, I was forced to translate it myself. This is slightly problematic since I do not actually read German. I was, however, able to complete a translation with the assistance of Altavista's Babel Fish and a German-English math dictionary. I am sure there are many translation errors, but hopefully no terribly egregious ones.

Chapter 1

ζ and L-functions before Artin

1.1 Euler and Euler Factorization

1.1.1 Introduction

Leonhard Euler was a Swiss mathematician who lived from 1707 to 1783. During this time, he wrote a majority of the papers published during the 18th century. As his complete works fill an entire bookshelf, it would be futile to attempt any sort of catalog of his important contributions. As an 18th century mathematician, his arguments often lack the rigor which we now expect. Guided by a brilliant intuition and amazing computational ability (he was so adept at mental calculations that half of his work was published after he became blind), however, he was able to make striking conclusions with rarely a misstep despite his lack of rigor. Although many of his methods have been for the most part discarded over the years, the process of justifying his manipulations provided a road-map for much of 19th century analysis. Of all his great works, the ones which will interest us in this paper are his results concerning a particular series one of whose generalizations is our eventual subject.

1.1.2 Some Elementary Results on the Distribution of Primes

Euler's investigations began with one of the oldest and most important questions in number theory: "How many primes are there?" For example, on average how many primes are in a given interval of the integers? How far can this distribution vary from the average? How random is this distribution?

A few of these questions can be answered with completely elementary methods. For example, it is easy to see that sequences of the form $(n!+2, n!+3, n!+4, ..., n!+n)$ show that there are arbitrarily long gaps between prime numbers. In contrast is the following result due to Euclid:

Theorem 1.1.1 (Euclid). *There are infinitely many primes.*

Proof. Suppose there were finitely many primes, $p_1, p_2, \dots p_n$. Then consider the number

$$Q = p_1 \cdots p_n + 1.$$

Clearly this number is not divisible by any prime. But it is also bigger than 1 and so (by descent) must be divisible by some prime. This is a contradiction, therefore there must be infinitely many primes. □

Although this method is certainly adequate to show that there are infinitely many primes, it does not seem to show that there are very many primes, because Q is a relatively large number compared to p_n. To quantify such questions of how the primes distributed, we introduce the following functions:

Definition 1.1.2. *Let $\pi(x)$ be the number of positive primes less than or equal to x. Let p_n be the nth positive prime.*

Euclid's result, therefore, says that $\lim_{x\to\infty} \pi(x) = \infty$, or, alternately, that p_n is actually defined for all positive n. On the other hand, the result on composites mentioned above says that $\limsup_{n\to\infty} p_n - p_{n-1} = \infty$, or, alternately, that for any n, $\pi(x+n) = \pi(x)$ for infinitely many x.

A closer look at Euclid's result allows us to get slightly stronger information on the growth of $\pi(x)$ and p_n.

Proposition 1.1.3. *$p_n < e^{e^n}$. Hence, $\pi(x) > \log\log x$.*

Proof. This theorem is obvious if $n = 1$. If $n > 1$, Euclid's construction actually says that

$$p_n \le p_1 \cdot p_2 \cdots p_{n-1} + 1 \le k p_1 \cdot p_2 \cdots p_{n-1}$$

for any $\frac{7}{6} < k$. Combining the first n such equations, we see that:

$$p_n \le k p_1 \cdot p_2 \cdots p_{n-1} \le k^2 (p_1 \cdots p_{n-2})^2 \le k^4 (p_1 \cdots p_{n-3})^4 \le \ldots \le (2k)^{(2^n)}.$$

Clearly we can pick k such that $2k < e$. □

This result shows that, for example, there are at least 2 primes smaller than 100 or that there are at least 3 primes less than 10,000. This is clearly a horrible underestimate as $\pi(100) = 25$ and $\pi(10,000) = 1,229$.

There are other classical proofs of the infinitude of primes based on similar constructive methods which give similar bounds. For example, consider Goldbach's proof of Proposition 1.1.3:

Consider the Fermat numbers, $F_n = 2^{2^n} + 1$. Fermat claimed that these were all prime, but Euler found a counterexample. However, they can still be used to prove the infinitude of primes because of the following lemma:

Lemma 1.1.4. $\gcd(F_n, F_m) = 1$ *so long as* n *and* m *are distinct.*

Proof. Without loss of generality, take $n < m$. Suppose some prime p divides both F_n and F_m. Then $-1 \equiv 2^{2^n} \pmod{p}$ and $-1 \equiv 2^{2^m} \pmod{p}$. Squaring the first equation $m - n$ times shows that $1 \equiv 2^{2^m} \pmod{p}$, which contradicts the second equation (clearly p must be odd since all the Fermat numbers are odd). Therefore, all the Fermat numbers are pairwise relatively prime. □

Now we can conclude another proof of Proposition 1.1.3 using this lemma. If all the Fermat numbers were relatively prime, then each must be divisible by a different prime from all the others. So, $p_n \leq F_n = 2^{2^n} + 1$. Thus, we have $\pi(x) > \log\log x$.

1.1.3 Euler Factorization

Obviously we would like to find a much better lower bound for $\pi(x)$ than $\log\log x$. The first proof of the infinitude of primes which allows us a substantively better bound is Euler's proof which can be found in his book *Introduction to Analysis of the Infinite*, [**Eu1**, Chapter XV]. Here he actually shows that $\sum_{p \text{ prime}} 1/p$ diverges.

Since $\sum_{n=1}^{\infty} e^{-e^n}$ clearly converges extremely rapidly, Euler's result will give us a substantively better estimate on the growth of $\pi(x)$. Furthermore, the argument itself is exceptional because it does not use constructive algebraic arguments like Euclid's and Goldbach's, but rather an argument based on the properties of a certain analytic function. Euler argued as follows:

"Let us consider the expression

$$\frac{1}{(1-\alpha z)(1-\beta z)(1-\gamma z)\cdots}.$$

"When the division is carried out, we obtain the series $1 + Az + Bz^2 + Cz^3 + \ldots$. It is clear that the coefficients A, B, C, etc. depend on the numbers α, β, γ, etc. in the following way: A is the sum of the sum of the numbers taken singly; B is the sum of the products taken two at a time; C is the sum of the products taken three at a time, etc., where we do not exclude products of the same factor.

"If for α, β, γ, etc. we substitute the reciprocals of some power of all the primes and let

$$P = \frac{1}{\left(1-\frac{1}{2^n}\right)\left(1-\frac{1}{3^n}\right)\left(1-\frac{1}{5^n}\right)\cdots},$$

then $P = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \ldots$, where all natural numbers occur with no exception.

"Because we can express the sum of the series $P = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \ldots$ as a product of factors, it is convenient to use logarithms. We have

$$\log P = -\log\left(1-\frac{1}{2^n}\right) - \log\left(1-\frac{1}{3^n}\right) - \log\left(1-\frac{1}{5^n}\right) - \ldots.$$

"If we use natural logarithms, then

$$\log P = 1\left(\frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{5^n} + \ldots\right) + \frac{1}{2}\left(\frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{5^{2n}} + \ldots\right)\ldots$$

"If $n = 1$, then $P = 1 + \frac{1}{2} + \frac{1}{3} + \ldots = \log(\frac{1}{1-1}) = \log(\infty)$. Then

$$\log\log\infty = 1\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots\right) + \frac{1}{2}\left(\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \ldots\right) + \ldots$$

"But these series, except for the first ones, not only have finite sums, but the sum of all of them taken together is still finite, and reasonably small. It follows that the first series $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \ldots$ has an infinite sum."[**Eu1**, Chapter XV]

As is to be expected, Euler's argument lacks rigor at a few points, but in this case the questionable steps are easy to identify and deal with. First we need to place the series which he discusses on a firmer foundation.

Proposition 1.1.5. *The series*

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

converges uniformly on the interval $[c, \infty)$ *for any* $c > 1$.

Proof. Since n^{-s} is monotonically decreasing for positive s, for any N and M and any $s \geq c > 1$,

$$\sum_{n=N}^{M} n^{-s} \leq \int_N^{\infty} x^{-s}dx = \frac{N^{1-s}}{s-1} < \frac{1}{c-1},$$

which shows uniform convergence. □

The key step in Euler's proof is the following fact known as the Euler factorization of the zeta function.

Proposition 1.1.6. *The product* $\prod_p \frac{1}{1-p^{-s}}$ *converges uniformly on the interval* $[c, \infty)$ *for any* $c > 1$. *(Here as always we use the notation* $\prod_p$ *(resp.* $\sum_p$*) to denote a product (resp. sum) over all positive primes.) Furthermore for* $s > 1$,

$$\prod_p \frac{1}{1-p^{-s}} = \zeta(s).$$

Proof. The important points are that $\frac{1}{1-p^{-s}} = \sum_{k=0}^{\infty} p^{-ks}$ and that every positive integer factors uniquely as a product of prime powers. We consider the finite product,

$$\prod_{p<N} \sum_{k=0}^{\infty} p^{-ks} = \sum_{n \in S_N} n^{-s},$$

where S_N is the set of all integers which are products of primes less than N. But clearly $[1, N) \subseteq S_N$. Therefore,

$$\left| \prod_{p<N} \sum_{k=0}^{\infty} p^{-ks} - \sum_{n<N} n^{-s} \right| = \varepsilon(N, s) < \sum_{n>N} n^{-s} < sN^{1-s}. \tag{1.1.1}$$

Since the right hand side goes to zero as N gets large, uniformly on the interval $[c, \infty)$ for any $c > 1$, our theorem is proved. □

These two results combine to give us the key formula in the middle of Euler's argument:

$$\log\zeta(s) = \sum_p -\log\left(1 - \frac{1}{p^s}\right). \tag{1.1.2}$$

Using the Taylor expansion for log is legitimate here because $0 < 1 - \frac{1}{p^s} < 1$, and we can exchange the order of summation because all the series involved converge uniformly and absolutely. Therefore, we find that

$$\log \zeta(s) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^n s} = \sum_{n=1}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s}$$
$$= \sum_p \frac{1}{p^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s}. \tag{1.1.3}$$

Thus far we have simply been rephrasing Euler's arguments in the language of modern analysis. The point where we need to do extra work is at the end. Essentially, we want to take the limit as $s \to 1$. Then the left hand side blows up, while the right hand side consists of the series we're interested in plus some finite part. But, unlike Euler, we can not say the left hand side is $\log\log\infty$.

We can, however, still conclude that

$$\lim_{s\to 1^+} \sum_p \frac{1}{p^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s}$$

cannot be finite.

First, we want to show that the terms with $k > 1$ on the right hand side of Equation 1.1.3 are small under the same limit. This is just another simple integral test:

$$\sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^{ns}} < \int_2^{\infty} \int_2^{\infty} x^{-1} y^{-sx} dy dx = \int_2^{\infty} s^{-1} x^{-2} 2^{-sx} dx$$
$$< \frac{1}{4s} \int_2^{\infty} 2^{-sx} dx = \frac{1}{8s^2} 2^{-2s} < \frac{1}{32}.$$

So clearly the sum of the rest of the series converges in the limiting case, just as Euler claimed. This implies that $\lim_{s\to 1^+} \sum_p \frac{1}{p^s}$ cannot be finite.

Theorem 1.1.7 (Euler). $\sum_p \frac{1}{p}$ *diverges.*

Proof. For the sake of contradiction, suppose that $\lim_{N\to\infty} \sum_{p<N} p^{-1}$ were actually finite. Then $\sum_{p>N} p^{-1}$ would give a uniform bound on the term $\sum_{p>N} \frac{1}{p^{-s}}$. Hence, $\sum_p \frac{1}{p^{-s}}$ would converge uniformly for all $s \geq 1$.

Thus the interchange of limits would be valid, and

$$\lim_{N\to\infty} \sum_{p<N} \frac{1}{p^{-1}} = \lim_{N\to\infty} \lim_{s\to 1^+} \sum_{p<N} \frac{1}{p^{-s}} = \lim_{s\to 1^+} \lim_{N\to\infty} \sum_{p<N} \frac{1}{p^{-s}} = \lim_{s\to 1^+} \sum_p \frac{1}{p^s}$$

would also be finite. This is clearly a contradiction. □

This proves the theorem which Euler set out to prove. Already this result shows powerful things like, p_n grows faster on average than n^r does for any $r > 1$. However, Euler claimed something stronger. Not only did he say that $\sum_p \frac{1}{p}$ diverged, he claimed that it was $\log\log\infty$. By this expression Euler seems to mean, in modern notation, that

$$\sum_{p<N} \frac{1}{p} = \log\log N + O(1).$$

In order to prove this result using Euler's methods, we would simply have to show that the Euler factorization was approximately valid for a finite sum and $s = 1$, i.e.

$$\left| \prod_{p<N} \frac{1}{1-p^{-1}} - \sum_{n<N} n^{-1} \right| < \varepsilon(N, 1)$$

for some nice error function. Alas, a little computation shows that this claim is not true at all. Our computation in Theorem 1.1.6 shows that the error function $\varepsilon(N,s)$ does not behave well as $s \to 1$.

In order to prove this result we will need a bit more information about the $\zeta(s)$ near $s = 1$. For many of Euler's papers in which he considers the Euler factorization and functions like his ζ-function, rather than considering the series, $\zeta(s) = \sum_n n^{-s}$, he instead looks at an alternating series:

Definition 1.1.8. $\tilde{\zeta}(s) = \sum_n (-1)^{n+1} n^{-s}$.

This new series has the distinct advantage of converging (conditionally) for all $s > 0$ by the alternating series test. If we group terms in pairs, then the series actually converges absolutely for all $s > 0$.

This new function also has an Euler factorization:

$$\begin{aligned}\tilde{\zeta}(s) &= \sum_n (-1)^n n^{-s} = (1 - 2^{-s} - 4^{-s} - \ldots)(1 + 3^{-s} + 9^{-s} - \ldots)(1 + 5^{-s} + 25^{-s} - \ldots)\ldots \\ &= \left(2 - \frac{1}{1-2^{-s}}\right) \prod_{p \neq 3} \left(\frac{1}{1-p^{-s}}\right). \end{aligned} \tag{1.1.4}$$

This factorization is very similar to that of the old ζ-function. In fact, we have the formula

$$\zeta(s) = \frac{\frac{1}{1-2^{-s}}}{2 - \frac{1}{1-2^{-s}}} \tilde{\zeta}(s) = \frac{1}{2 - 2^{1-s} - 1} \tilde{\zeta}(s) = \frac{1}{1 - 2^{1-s}} \tilde{\zeta}(s).$$

This new expression for $\zeta(s)$ now makes sense for any $s > 0$ except for $s = 1$ where it clearly blows up. This lets us get a much firmer grasp on the behavior of ζ near 1.

Theorem 1.1.9. *cf. [**J**, pp. 144-145]*

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

Proof. If we write

$$(s-1)\zeta(s) = \frac{s-1}{1-2^{1-s}} \tilde{\zeta}(s),$$

the limit as $s \to 1$ actually makes sense. By a standard result from analysis, $\lim_{s \to 1} \tilde{\zeta}(s) = \log 2$. By L'hôpital's rule,

$$\lim_{s \to 1} \frac{s-1}{1-2^{1-s}} = \frac{1}{\log 2}.$$

Thus, $\lim_{s \to 1}(s-1)\zeta(s) = 1$. □

Therefore, by Theorem 1.1.9, if we consider the series

$$(1-s)\zeta(s) = \sum_n \frac{1-s}{n^s},$$

it will converge uniformly in s for $s \in [1, \infty)$. Hence the error term $(1-s)\varepsilon(N,s)$ actually does remain bounded as $s \to 1$. Thus we have shown,

Lemma 1.1.10.

$$\lim_{s \to 1}(1-s) \left| \prod_{p<N} \frac{1}{1-p^{-1}} - \sum_{n<N} n^{-s} \right| < \lim_{s \to 1} \varepsilon(N,s) < \varepsilon(N),$$

for some error function $\varepsilon(N)$ which goes to zero as N gets large.

□

Theorem 1.1.11.

$$\sum_{p<N} \frac{1}{p} = \log\log N + O(1).$$

Proof. By the lemma for all N and $s > 1$,

$$(s-1)\prod_{p<N}\frac{1}{1-p^{-1}} = (s-1)\sum_{n<N} n^{-s} + O(1),$$

where by $O(1)$ we mean the error is bounded as $N \to \infty$ and as $s \to 1^+$. If we take logs of both sides and use an earlier lemma,

$$\log(s-1) + \sum_{p<N} p^{-s} = \log(s-1) + \log\sum_{n<N} n^{-s} + O(1).$$

Now we can cancel the $\log(1-s)$ terms and the terms we are left with are all bounded as $\lim_{s\to 1}$. Thus,

$$\sum_{p<N}\frac{1}{p} = \log\sum_{n<N} n^{-1} + O(1) = \log\log N + O(1).$$

□

Clearly it follows that there are infinitely many primes. In fact, we can extract from this theorem a very good idea of how fast $\pi(x)$ and p_n grow.

We will extend p_n to some monotonic real valued function p_x to get

$$\int_1^X \frac{1}{p_x}dx = \log\log X + O(1). \tag{1.1.5}$$

We would really like to "differentiate" this equation to get something like

$$\frac{1}{p_x} \approx \frac{d}{dx}\log\log x = \frac{1}{\log x}\frac{1}{x}.$$

This would imply that $p_x \approx x\log x$. However, although integrating preserves estimates, differentiating clearly does not. (For example, consider the fact that $x\sin x = O(x)$, but $\sin x + x\cos x = \frac{d}{dx}x\sin x \neq O(1)$.)

What this does tell us though is that p_n can not grow *significantly faster* than $n\log n$. Similarly, we can see that $\pi(x)$ can not grow significantly slower than $\frac{x}{\log x}$.

This phrase "significantly faster" (resp. slower) can mean any of a number of things, for example,

Proposition 1.1.12. *For any constant $k > 1$ and N, there exists some $n > N$, $p_n \geq kn\log n$.*

Proof. Suppose to the contrary that for some constants $k < 1$ and N, $p_n < kn\log n$ for all $n > N$. Thus, if $n > N$,

$$\frac{1}{p_n} < \frac{1}{k}\frac{1}{n\log n}.$$

Integrating yields

$$\sum_{N<n<x} p_n < \frac{1}{k}(\log\log x - \log\log N)$$

for all $x > N$. But by Equation 1.1.5, this means that for some constant c,

$$\log\log x < c - \frac{1}{k}(\log\log N) + \frac{1}{k}(\log\log x).$$

Since $k > 1$, this last equation is clearly false for large enough x. □

To show a more concrete result, like $p_n \sim n\log n$, one would need to prove something stronger about the smoothness of p_n.

It is worth noting that simply showing that there are infinitely many primes does not require any of the above arguments. We can simply note that if there were finitely many primes, then, by looking at the supposed finite Euler factorization, $\lim_{s\to 1}\zeta(s)$ would be finite.

1.1.4 General Principles of Analytic Number Theory

Euler's argument lays the foundations for the field of analytic number theory which is based on the following principles:

Principle 1. *Important number theoretic information can be encoded into analytic functions*

The Euler factorization provides the main tool for encoding information about prime numbers into analytic functions. However, there are many other analytic functions which encode number theoretic information for completely different reasons.

Principle 2. *Increased knowledge of the analytic properties of these functions translates into increased knowledge about the number theoretic information*

As we saw above, to show that there are infinitely many primes we only needed to know that $\zeta(s)$ blows up at 1. On the other hand, to get better results on how quickly the number of primes grew on average we needed to know how quickly $\zeta(s)$ blows up at one.

These two principles suggest the following types of progress in analytic number theory:

Type 1. *Finding new analytic functions with number theoretic importance*

Type 2. *Extending the domain where these functions make sense*

Type 3. *Finding new analytic properties of these functions.*

Type 4. *Translating these analytic properties (either proved or conjectured) into theorems in number theory.*

We will be focusing on the first two types of progress: firstly, generalizing the notion of a ζ-function and Euler factorization to similar functions which tell us about the distribution of certain kinds of primes in various number fields, and secondly, trying to find as large as possible a domain of definition for these functions. When important, we will note related results of types 3 and 4; but for the most part we will take for granted the fact that increased knowledge of the functions which we deal with will give important number theoretic information.

1.1.5 Euler and the Functional Equation of the Zeta Function

Although we have already seen all four types of progress in Euler's work, there is one further example of progress of types 2 and 3 which will interest us. In a later paper, Euler attempted to discuss values of $\zeta(s)$ for negative integers. Although his methods are not particularly of interest to us since they are completely un-rigorous, his answers were important to motivate the work of later mathematicians.

Before we can state Euler's claims, we need the following definition:

Definition 1.1.13. *We define the Bernoulli numbers B_k by the kth term in the Taylor expansion:*

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

One important fact about these numbers is that they vanish for any odd $k > 1$. To see this, notice that $\frac{x}{e^x-1} + \frac{x}{2}$ is an even function.

Euler claimed that these Bernoulli numbers are related to special values of the ζ series:

Claim 1.1.14. *If n is a positive even integer, then*

$$\zeta(n) = \frac{2^{n-1}\pi^n}{n!}|B_n|.$$

Proof. Euler got this formula by considering the function $f(x) = \frac{\sinh x}{x}$. Euler reasoned (in [**Eu1**, Chapters IX and X]) that

$$f(x) = \prod_{n=1}^{\infty} \left(1 + \frac{x^2}{n^2\pi^2}\right). \tag{1.1.6}$$

Essentially his argument comes down to the facts that the roots of $\sinh x$ are $\pm i\pi n$ for all integers n and that the two equations agree at 0. Clearly this is not enough to establish the equality in Equation 1.1.6 since, for example, $e^x \frac{\sinh x}{x}$ also has exactly the same roots. Nonetheless, it was proved in the late 19th century by Hadamard [**Ha**, Vol. 1, pp. 103-147] that such factorizations can be justified with some additional growth constraints (see [**Da**, Chapter 11]). For Euler, however, it was enough to describe a method and to note that this expression actually gave the correct answer if multiplied out by hand.

Once he had Equation 1.1.6, Euler could expand the left hand side as a Taylor series and multiply out the right hand side (again this is un-rigorous) to find:

$$1 + \frac{x^2}{3!} + \frac{x^4}{5!} + \ldots = 1 + \left(\sum_{n=1}^{\infty} n^{-2}\right)\left(\frac{x}{\pi}\right)^2 + \left(\sum_{n<m} n^{-2}m^{-2}\right)\left(\frac{x}{\pi}\right)^4 + \ldots \tag{1.1.7}$$

Equating the coefficients tells us that $\zeta(2) = \frac{\pi^2}{3!}$, that $\zeta(2)^2 - \zeta(4) = \frac{\pi^4}{5!}$, etc. Using these equations, Euler's claim is reduced to an exercise in combinatorics. □

In his paper *Remarques Sur Un Beau Rapport Entre Les Series Des Puissances Tant Directes Que Reciproques* [**Eu2**, Vol. 15, pp. 70-90], Euler contrasts this formula with another context in which Bernoulli numbers appeared.

Euler considered series of the form $s_k(x) = \sum_{n=0}^{\infty} n^k x^n$. Notice that $\frac{d}{dx} s_k(x) = s_{k+1}(x)$. Furthermore so long as $|x| < 1$, $s_1(x) = \frac{1}{1+x}$. These last two equations give us a recursive formula for $s_k(x)$ for any positive k and any $|x| < 1$.

Furthermore, although our original expression for s_k does not converge at $x = -1$, our recursive formula does. This enabled Euler to recursively "compute" the (divergent) series $\sum_{n=0}^{\infty}(-1)^n n^k = -\tilde{\zeta}(-k)$, for k a positive integer. Finally with some combinatorial computations, Euler managed to prove that the recursive formula actually yields

$$s_k(-1) = \frac{1}{1 - 2^{1-s}} \frac{B_n}{n+1}.$$

Thus, using our formula relating ζ and $\tilde{\zeta}$, Euler determined that

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}. \tag{1.1.8}$$

Combining Equation 1.1.8 with Claim 1.1.14, Euler deduced the startling result:

Claim 1.1.15. *For any positive integer n,*

$$\frac{\zeta(1-n)}{\zeta(n)} = \frac{2^{1-n}\cos(\frac{n\pi}{2})n!}{\pi^n}.$$

We should pause for a moment to recall that none of this actually makes sense. We have yet to give a good formula which will make sense for real values less than 0. Nonetheless, Euler was not one to be bothered with such trifles. In the remainder of this article, Euler proceeded to argue that Claim 1.1.15 actually holds for all real numbers!

Although he did not give a particularly good definition of what he meant by the ζ-function for negative values, Euler did have a nice definition of $n!$ for n a general real number.

Definition 1.1.16. *For any $s > 0$, we define*

$$\Gamma(s) = \int_0^{\infty} x^{s-1}e^{-x}dx.$$

Proposition 1.1.17. *If n is a nonnegative integer, then $\Gamma(n+1) = n!$.*

Proof. Clearly

$$\Gamma(1) = \int_0^\infty e^{-x} dx = 1 = 0!.$$

By induction, it is enough to show that $\Gamma(n+1) = n\Gamma(n)$. Recall from the definition that $\Gamma(n+1) = \int_0^\infty x^n e^{-x} dx$. Let $u = x^n$ and $dv = e^{-x} dx$. By integration by parts,

$$\Gamma(n+1) = [-x^n e^{-x}]_0^\infty + n \int_0^\infty x^n e^{-x} dx = n\Gamma(n).$$

□

Thus Euler makes the following conjecture, which is now known as the functional equation of the ζ-function.

Conjecture 1.1.18. *For any positive real number s,*

$$\frac{\zeta(1-s)}{\zeta(s)} = \frac{2^{1-s} \cos(\frac{s\pi}{2}) \Gamma(s+1)}{\pi^s}.$$

If we believe Euler's earlier argument, we already know that this is true for integers. For $s = 1/2$, the result comes down to the classical Gaussian integral $\Gamma\left(\frac{1}{2}\right) = \sqrt{\frac{\pi}{2}}$. For other half-integers, Euler attempts to give further evidence of this claim by "estimating" the values of the ζ series at these points. Unfortunately since none of these series actually converge we should be a bit skeptical of his estimations.

Nonetheless (as shocking as it may be since we have given such scant evidence so far) in a few chapters we shall find that we can give a definition of the ζ function which makes sense for all *complex* numbers (other than $s = 1$) and we shall be able to prove Conjecture 1.1.18 as well as Claim 1.1.14 using completely rigorous methods!

Although one might be tempted to dismiss Euler's mathematics as we have presented it, it is important to realize that his insights into the relation between number theory and this analytic function underpin all the great and more rigorous progress which has taken place after him. Perhaps we can even let this remind us that, although nothing is a substitute for a real proof, an interesting and perhaps correct argument which actually yields the correct answer often is just as important an insight as providing the rigorous framework.

1.2 Dirichlet and his L-series

1.2.1 Introduction

Nearly a century passed before our next important moment in history. Meanwhile, the state of mathematics had changed significantly and number theory in particular had been advanced remarkably by Gauss. During the century after Euler, very little was done to add to his picture of the ζ-function. Then, in the 1840's, Dirichlet gave a proof of a result in number theory which depended heavily on the use of certain generalizations of Euler's function. Dirichlet used the letter L to denote these functions and ever since they have been called L-functions. Dirichlet lived from 1805-1859. Not only did he make outstanding contributions to Number Theory and Fourier Analysis, he also was one of the great expositors of mathematics in the 19th century. His *Lectures in Number Theory* [**Di1**] (which, thankfully, has been translated recently into English) brought Gauss's great work in *Disquitiones Arithmeticae* to a larger audience by giving a tighter and improved exposition. Even today this book makes an excellent introduction to the elementary theory of numbers. We will be roughly following Dirichlet's proof as found in [**Di1**, Supplement VI] and [**Di2**, pp. 313-342].

1.2.2 Elementary Results on Primes in Arithmetic Progressions

Dirichlet considered a question very similar to the one which inspired Euler's introduction of the ζ-function: namely, how the primes are distributed modulo m. The simplest question of this type is whether are there infinitely many primes congruent to a modulo m. Obviously there can only be infinitely many primes of this form if a and m are relatively prime. Unfortunately, this problem turned out to be much more difficult than proving that there are infinitely many primes. Elementary results along the lines of Euclid's proof only sufficed to show very special cases. For example,

Proposition 1.2.1. *There are infinitely many primes $p \equiv 3 \pmod 4$.*

Proof. Suppose there were only finitely many such primes, $p_1, p_2, \ldots, p_n$. Consider the number

$$Q = 4p_1p_2 \ldots p_n - 1.$$

Clearly this number is not divisible by any of the primes which are 3 modulo 4. Thus, $Q \equiv 3 \pmod 4$ is a product of primes all of which are 1 modulo 4. This is clearly a contradiction. □

Proposition 1.2.2. *There are infinitely many primes $p \equiv 1 \pmod 4$.*

Proof. Here we use the fact from basic number theory that -1 is a square modulo p exactly when $p \equiv 1 \pmod 4$. Again, suppose there were only finitely many primes $p_1, p_2, \ldots, p_n \equiv 1 \pmod 4$. Let

$$Q = (2p_1p_2 \ldots p_n)^2 + 1.$$

Clearly Q is not divisible by any of the primes which are 1 modulo 4. Since $-1 \equiv (p_1p_2 \ldots p_n)^2 \pmod Q$, any prime which divides Q must be 1 modulo 4. Again, this is a contradiction. □

Although similar methods will work for $m = 3$ or $m = 6$, they are doomed to failure in general. Rather than trying to use these sorts of elementary proofs, Dirichlet instead tried to adapt Euler's analytic methods to this situation.

1.2.3 A Special Case of Dirichlet's Theorem

In particular, Dirichlet wanted to prove

Theorem 1.2.3. *For any relatively prime positive integers a and m, the series*

$$\sum_{p \equiv a \pmod m} \frac{1}{p}$$

diverges.

Let us first consider the particular case $m = 4$. Since we will consider things more rigorously in the general case, here we shall be a bit lax.

The most obvious attempt at modifying Euler's method is to consider the function

$$f_1(s) = \prod_{p \equiv 1 \pmod 4} \frac{1}{1 - p^{-s}}.$$

By the same arguments as used the last section we can conclude that

$$\sum_{p \equiv 1 \pmod 4} p^{-s} = \log f_1(s) + O(1).$$

Unfortunately, $f_1(1)$ does not obviously diverge. If we multiply out the Euler product, we see that

$$f_1(s) = \sum_{n \in S} n^{-s},$$

where S is the set of all numbers which are products of primes which are 1 modulo 4. This is entirely unhelpful. We need to find some functions whose Euler factorizations depend only on what the prime is modulo 4, and where the terms in the series do not depend on the prime factorization of n.

Dirichlet's insight was to look at the functions

$$L_1(s) = \sum_{n \text{ odd}} (-1)^{\frac{n-1}{2}} n^{-s} = \prod_{p \equiv 1 \pmod 4} \frac{1}{1 - p^{-s}} \prod_{p \equiv 3 \pmod 4} \frac{1}{1 + p^{-s}}$$

$$L_0(s) = \sum_{n \text{ odd}} n^{-s} = \prod_{p \equiv 1 \pmod 4} \frac{1}{1 - p^{-s}} \prod_{p \equiv 3 \pmod 4} \frac{1}{1 - p^{-s}} = (1 - 2^{-s})\zeta(s).$$

Just as in the last section, we can take logarithms and use the Taylor series expansion. As in the last section the contribution from quadratic and higher terms in the Taylor series are bounded. Thus,

$$\log L_1(s) = \sum_{p \equiv 1 \pmod 4} p^{-s} - \sum_{p \equiv 3 \pmod 4} p^{-s} + O(1)$$

$$\log L_0(s) = \sum_{p \equiv 1 \pmod 4} p^{-s} + \sum_{p \equiv 3 \pmod 4} p^{-s} + O(1)$$

Therefore,

$$\frac{1}{2}(\log L_0(s) + \log L_1(s)) = \sum_{p \equiv 1 \pmod 4} p^{-s} + O(1)$$

$$\frac{1}{2}(\log L_0(s) - \log L_1(s)) = \sum_{p \equiv 1 \pmod 4} p^{-s} + O(1)$$

Thus in order to prove this special case of Theorem 1.2.3, we need only show that $\log L_0(s) + \log L_1(s)$ and $\log L_0(s) - \log L_1(s)$ are both unbounded as $s \to 1^+$. Obviously $(1 - 2^{-s})\zeta(s)$ blows up at $s = 1$. Hence we've reduced this problem to showing that $\log L_1(1)$ is finite.

But, $L_1(s)$ is an alternating series; thus, we can bound it by the first two partial sums, i.e. $\frac{2}{3}3^{-s} < L_1(s) < 1$. Thus $\log \frac{2}{3} < \log L_1(1) < 0$, so we have proved Theorem 1.2.3 for the case of $m = 4$.

1.2.4 Some General Results on Dirichlet Series

Before we attack the general proof of Theorem 1.2.3, it will be useful to have a few technical definitions and results.

Definition 1.2.4. *A Dirichlet series is a series of the form,*

$$f(s, a_n) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where a_n is some sequence of complex numbers.

We will want to know when a Dirichlet series actually converges. In order to prove this, we will need the following theorem which is the analog for sums of integration by parts.

Theorem 1.2.5 (Abel Summation Formula). *Suppose (a_n) and (b_n) are two sequences. Let $(A_{\ell,N}) = \sum_{n=\ell}^{N} a_n$. Then $\sum_{n=\ell}^{N} a_n b_n = A_{\ell,N} b_N - \sum_{n=\ell}^{N} A_{\ell,n}(b_{p+1} - b_p)$.*

Proof. To verify this theorem, we simply plug in the definition of A_n and check that each term $a_i b_j$ occurs with the same multiplicity on both sides. □

Proposition 1.2.6. *cf. [**Se3**, pp. 3-4] If $\sum a_n n^{-s_0}$ converges, then the Dirichlet series $f(s, a_n)$ converges for all complex numbers s with $Re(s) > s_0$. In fact, this convergence is uniform in any wedge to the right of the point s_0: $\{s : \ Re(s) > Re(s_0)$ and $0 < \frac{|s-s_0|}{Re(s-s_0)} < M\}$, where M is an arbitrary positive constant. (Since this convergence is uniform, $f(s, a_n)$ is analytic on that region.)*

Proof. Letting M grow arbitrarily shows that the second assertion implies the first. Without loss of generality, we can assume $s_0 = 0$ (since we can look at the Dirichlet series $\sum_n (a_n n^{-s_0}) n^{-s}$). Also, without loss of generality, we can subtract off the first term a_1 and so assume $a_1 = 0$.

Since we are assuming that $\sum_n a_n$ converges for any $\varepsilon > 0$, there exists an integer N such that for any $\ell, m > N$, $|A_{\ell,m}| < \epsilon$.

We want to get a good bound on $|\sum_{n=\ell}^{m} a_n n^{-s}|$. By Abel's summation formula,

$$\left|\sum_{n=\ell}^{m} a_n n^{-s}\right| = \left|A_{\ell,m} b_m - \sum_{n=\ell}^{m} A_{\ell,m}((n+1)^{-s} - n^{-s})\right| < \epsilon \left(1 + \sum_{n=\ell}^{m} \left|e^{-s\log n} - e^{-s\log(n+1)}\right|\right).$$

To get a bound on that last term, we notice that for any $\alpha > \beta \geq 0$,

$$e^{-\alpha z} - e^{-\beta z} = z \int_{\alpha}^{\beta} e^{-tz} dt.$$

Therefore,

$$\left|e^{-\alpha z} - e^{-\beta z}\right| \leq |z| \int_{\alpha}^{\beta} e^{-t\mathrm{Re}(z)} dt = \frac{|z|}{\mathrm{Re}(z)} \left(e^{-\alpha \mathrm{Re}(z)} - e^{-\beta \mathrm{Re}(z)}\right).$$

Applying this to our particular case, we see that

$$\begin{aligned}\left|\sum_{n=\ell}^{m} a_n n^{-s}\right| &< \epsilon \left(1 + M \sum_{n=\ell}^{m} e^{-\mathrm{Re}(s)\log n} - e^{-\mathrm{Re}(s)\log(n+1)}\right) \\ &= \epsilon \left|1 + M(e^{-\mathrm{Re}(s)\log \ell}) - e^{-\mathrm{Re}(s)\log(m)}\right| < \epsilon(1+M).\end{aligned}$$

Thus for large enough N, this goes to zero independently of s, so the series converges uniformly in this region. □

It turns out that if a function can be written as a Dirichlet series then it can be done so in only one way.

Proposition 1.2.7. *cf. [**Ap**, Thm. 11.4] Suppose that $\sum_n \frac{a_n}{n^s} = 0$ on some right halfplane $Re(s) > \sigma_0$. Then, $a_n = 0$ for all n. Therefore, if we have two Dirichlet series with $\sum_n \frac{b_n}{n^s} = \sum_n \frac{c_n}{n^s}$ for all $Re(s) > \sigma_0$, then $b_n = c_n$ for all n.*

Proof. Without loss of generality, by considering $a_n n^{-\sigma_0}$ we can assume that $\sigma_0 = 0$. Thus, in order to have $\sum_n \frac{a_n}{n^s}$ converge near $s = 0$, we must have $a_n = O(1)$. Now suppose that a_N is the first non-zero term. Then

$$0 = a_N N^{-s} \left(1 + \sum_{n \geq N} \frac{a_n}{a_N} \left(\frac{n}{N} \right)^{-s} \right).$$

Multiplying by N^s we get

$$0 = a_N \left(1 + \sum_{n \geq N} \frac{a_n}{a_N} \left(\frac{n}{N} \right)^{-s} \right).$$

Now send $s \to +\infty + 0i$. Each of the terms in the sum dies exponentially. Therefore, since the coefficients are bounded, the whole sum dies. Therefore, $0 = a_N$. This is a contradiction; therefore, $a_n = 0$ for all n.

For the second conclusion, we simply consider the Dirichlet series $\sum_n \frac{b_n - c_n}{n^s} = 0$, from which it follows that $b_n - c_n = 0$ and thus $b_n = c_n$ for all n. □

Definition 1.2.8. *A sequence a_n is called multiplicative if $a_n a_m = a_{nm}$ for all relatively prime positive integers n and m. Similarly, a sequence a_n is called strongly multiplicative if $a_n a_m = a_{nm}$ for all pairs of positive integers.*

Theorem 1.2.9. *If a_n is multiplicative then the Dirichlet series $f(s, a_n)$ has the Euler factorization:*

$$f(s, a_n) = \prod_p \sum_{\ell=1}^{\infty} \frac{a_{p^k}}{p^{sk}}.$$

Furthermore if a_n is strongly multiplicative, summing this geometric series we see that

$$f(s, a_n) = \prod_p \frac{1}{1 - \frac{a_p}{p^s}}.$$

Proof. The proof here is identical to the proof of Theorem 1.1.1. □

1.2.5 Dirichlet's L-series

In order to generalize Dirichlet's argument from the case of $m = 4$ to a general m, we should look at all Dirichlet series with particularly nice Euler factorizations in which a_p depends only on what n is modulo m and vanishes when $p|m$. From our results above, it is clear that we should be looking at the series corresponding to sequences of the following form:

Definition 1.2.10. *Let a Dirichlet character modulo m be any function from $\chi : \mathbb{Z} \to \mathbb{C}$ with the properties:*

1. *If n and m are not relatively prime, then $\chi(n) = 0$.*
2. *If n and m are relatively prime, then $|\chi(n)| = 1$.*
3. *If n_1 and n_2 are any two positive integers, then $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$.*

If we restrict a Dirichlet character to $(\mathbb{Z}/m\mathbb{Z})^\times$ we get a homomorphism. (By abuse of notation, we will also call it $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.) Furthermore, if one considers any homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ it will be a Dirichlet character modulo k for any $m|k$. If χ is an injective homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \hookrightarrow \mathbb{C}^\times$, then we say that the corresponding Dirichlet character is a primitive character modulo m. The homomorphism sending everything to 1 and the corresponding Dirichlet character will both be called trivial.

The above notion of homomorphisms $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ generalizes to the more general notion of an abelian group character, which is a homomorphism $\chi : G \to \mathbb{C}^\times$ where G is an abelian group.

As far as I can tell, the linguistic history of this term *character* is quite the opposite of what one might expect. The notion of a Dirichlet character came before the notion of a general character, and the name *character* seems to come from the fact that it is a generalization of the *quadratic character* that is the quadratic nature of a number modulo m.

Definition 1.2.11. *If χ is a Dirichlet character modulo m, then define the Dirichlet L-series*

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = \prod_{p} \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

If χ_0 is the trivial character modulo m, then obviously

$$L(s,\chi_0) = \prod_{p|m} \left(1 - \frac{\chi(p)}{p^s}\right) \zeta(s)$$

converges for any $\mathrm{Re}(s) > 1$.

For a nontrivial character, we certainly could get the same region of convergence since $\sum_n \chi(n)n^{-s} < \sum_n |\chi(n)|n^{-s}$. However, we might hope to find some cancellation and be able to find a larger region of convergence.

Lemma 1.2.12 (Dirichlet). *If G is an abelian group, and χ is a nontrivial character of that group, then*

$$\sum_{g \in G} \chi(g) = 0.$$

Proof. For any $h \in G$, notice that

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

But, as g runs over all of G, so does hg. Hence,

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

Therefore, either $\chi(h) = 1$ or $\sum_{g \in G} \chi(g) = 0$. Since χ is nontrivial, we can choose h so that the former condition is not true. Thus the lemma is proved. □

Corollary 1.2.13. *If χ is a nontrivial Dirichlet character modulo m, then $L(s,\chi)$ converges for $Re(s) > 0$.*

Proof. By Lemma 1.2.12, we know that $\sum_n \chi(n)$ is bounded. Thus, $\sum_n \chi(n)n^{-s}$ converges for any positive s, which by Proposition 1.2.6 is enough. □

1.2.6 Reducing Dirichlet's Theorem to an Analytic Theorem

Now that we have proved enough technical results, we can return to Dirichlet's original question. Following Euler, we notice that

$$\log L(s,\chi) = \sum_{p} \log \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Again the Taylor series expansion is valid, and our estimate on the terms still holds:

$$\left| \sum_{n=2}^{\infty} \frac{1}{n} \sum_{p} \frac{\chi(p)}{p^{ns}} \right| < \int_2^{\infty} \int_2^{\infty} x^{-1} y^{-sx} dy dx < \frac{1}{32}.$$

Therefore,

$$\log L(s,\chi) = \sum_{p} \chi(p) p^{-s} + O(1).$$

To get Dirichlet's result, we need to write $f_a(s) = \sum_{p \equiv a \pmod m} p^{-s}$ as a sum of $\log L(s,\chi)$ for various χ. We know that

$$\log L(s,\chi) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) f_a(s) + O(1).$$

In order to get this result, Dirichlet noticed and proved a finite analog of Fourier inversion called the orthogonality of characters.

Theorem 1.2.14 (Dirichlet). *If χ_1 and χ_2 are distinct characters of a finite abelian group G, then*

$$\sum_{g \in G} \chi_1(g)\chi_2(g)^{-1} = 0.$$

Furthermore, if we let G^* denote the dual group of characters of G, then, if $g \neq h$,

$$\sum_{\chi \in G^*} \chi(gh^{-1}) = 0.$$

Proof. The first assertion follows immediately from applying Lemma 1.2.12 to the character $\chi_1\chi_2^{-1}$. Together with the obvious fact that $\sum_{g \in G} \chi(g)\chi(g)^{-1} = |G|$, this implies that the matrix $(\frac{\chi(g)}{|G|})_{\chi,g}$ has orthogonal rows. By the structure theorem for finite abelian groups, it is easy to see that $|G| = |G^*|$ (since it is obvious for cyclic groups). Thus this matrix is a square matrix. By standard linear algebra we know that having orthogonal columns is the same as having orthogonal rows and the second half of the result follows. □

Thus by Theorem 1.2.14, we see that the characters χ are all linearly independent and thus form a basis of the space of all complex valued functions on G. In particular,

$$\frac{1}{|G|} \sum_{\chi \in G^*} \chi(h^{-1})\chi(g) = \begin{cases} 1 & \text{if g=h} \\ 0 & \text{otherwise} \end{cases}.$$

Therefore, if we let $G = (\mathbb{Z}/m\mathbb{Z})^\times$,

$$f_a(s) = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(h^{-1}) \log L(s,\chi) + O(1).$$

Since $\log L(1,\chi_0)$ blows up, and $\log L(1,\chi) < \infty$ for all nontrivial characters, all that remains is to show that $\log L(1,\chi) > -\infty$. That is to say, we have shown that Theorem 1.2.3 is equivalent to the following theorem:

Theorem 1.2.15 (Dirichlet). *If χ is a nontrivial Dirichlet character, then $L(1,\chi) \neq 0$.*

Proof. First we claim that for every m there is at worst one χ with $L(1,\chi) = 0$. Notice that

$$\sum_{\chi \in G^*} \log L(s,\chi) = \varphi(m) \sum_{k=1}^{\infty} \frac{1}{k} \sum_{p:\ p^k \equiv 1 \pmod m} p^{-ks} > 0.$$

Now we already know that $\lim_{s \to 1^+} (s-1)L(s,\chi_0)$ is finite. Hence, $\log L(s,\chi_0) = \log \frac{1}{s-1} + O(1)$. But we know by Theorem 1.2.6 that for all the other $\chi \neq \chi_0$, $L(s,\chi)$ are analytic near 1. Therefore, for all of these, $\log L(s,\chi)$ either goes to $-\infty$ or is bounded.

Suppose one of these series, for instance $L(s,\tau)$, had a zero at 1. Since it is analytic, by considering the Taylor expansion, $\frac{L(s,\tau)}{s-1}$ is analytic and bounded at 1. Hence, $\log L(s,\tau) = -\log(s-1) + O(1)$. So, if we had $L(1,\tau_1) = L(1,\tau_2) = 0$, then

$$\sum_{\chi \in G^*} \log L(s,\chi) = \log(s-1) - 2\log(s-1) + \varepsilon(s),$$

where $\varepsilon(s)$ is either bounded or goes to $-\infty$ as $s \to 1^+$. Thus, the right hand side would be negative for small enough s, and we've reached a contradiction.

Notice that this proves the theorem for every character whose image is not contained in the reals. In this case there is a distinct character $\bar{\chi}(n) = \overline{\chi(n)}$ with $L(1,\chi) = 0 \iff L(1,\bar{\chi}) = 0$.

Furthermore, this shows that there is at worst 1 primitive Dirichlet character with $L(s,\chi) = 0$. If there were two, say one primitive modulo m_1 and the other primitive modulo m_2, then we could consider both of them as Dirichlet characters modulo $m_1 m_2$. Thus their L-series modulo $m_1 m_2$ would differ from the originals by only finitely many terms. Thus there would be two different Dirichlet L-series modulo $m_1 m_2$ with $L(1,\chi) = 0$, which is a contradiction.

So we have proven this theorem for all but one primitive character which must be real. Any real primitive character modulo m must have, for g a generator of $\mathbb{Z}/m\mathbb{Z}$, $\chi(g^k) = (-1)^k$. Clearly, this means $\chi(a)$ is 1 or -1 exactly when a is a square or a non-square respective. Thus, $\chi(a) = \left(\frac{a}{m}\right)$.

Dirichlet spent several years trying to prove that $L(1, \left(\frac{\cdot}{m}\right)) \neq 0$. Eventually he was able to prove this using his famous class number formula. (See [**Di1**, Chapter 5] or [**Di2**, pp.411-496] for Dirichlet's original proof of the class number formula. See [**Da**, Chapter 6] for a very readable version of Dirichlet's methods. For a more modern treatment of the class number formula see [**J**, pp.145-153]. Alternately for a much more quick proof of this theorem without using the class number formula see [**Da**, Chapter 4].) □

Although the general case of this last formula was beyond the scope of this paper, Dirichlet was, however, able to give a much simpler proof in the case of m a prime number (in [**Di2**, pp. 320-329]).

1.2.7 A Full Proof of $L\left(1, \left(\frac{\cdot}{p}\right)\right) \neq 0$ for p Prime

Theorem 1.2.16 (Dirichlet). *If p is a prime, then $L\left(1, \left(\frac{\cdot}{p}\right)\right) \neq 0$.*

Proof. Dirichlet began with the fact that $\Gamma(s) = n^s x^{n-1} \int_0^1 (\log(\frac{1}{x}))^{s-1} dx$, which can be gotten from our original definition by a simple change of variables $x \mapsto n\log(\frac{1}{x})$. Therefore,

$$n^{-s} = \frac{1}{\Gamma(s)} \int_0^1 x^{n-1} \left(\log\left(\frac{1}{x}\right)\right)^{s-1} dx. \tag{1.2.1}$$

Plugging this into the definition, we see that (interchanging sums and integrals is valid since the sum converges uniformly),

$$L\left(s, \left(\frac{\cdot}{p}\right)\right)\Gamma(s) = \int_0^1 \sum_n \left(\frac{n}{p}\right) x^{n-1} \left(\log\left(\frac{1}{x}\right)\right)^{s-1} dx.$$

Notice that

$$\sum_n \left(\frac{n}{p}\right) x^{n-1} = \frac{1}{1-x^p} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^{a-1} = -\frac{f(x)}{x^p - 1}$$

for the polynomial $f(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^{a-1}$.

Now we want to split $\frac{f(x)}{x^p-1}$ into partial fractions. Let $\zeta_p = e^{\frac{2\pi i}{p}}$ be a primitive pth root of unity, and thus a zero of the denominator. For a particular denominator $(x - \zeta_p^a)$, the numerator will be

$$\begin{aligned}\left(\frac{f}{\frac{x^p-1}{x-\zeta_p^a}}\right)(\zeta_p^a) &= \frac{f(\zeta_p^a)}{\prod_{k\neq m}(\zeta_p^a - \zeta_p^k)} = \frac{f(\zeta_p^a)}{\zeta_p^{a(p-1)} \prod_{k=1}^{p-1}(1-\zeta_p^k)} \\ &= \frac{f(\zeta_p^a)}{\zeta_p^{-a}(1^{p-1} + \ldots + 1)} = \zeta_p^a \frac{f(\zeta_p^a)}{p}.\end{aligned}$$

Therefore,

$$L\left(s,\left(\frac{\cdot}{p}\right)\right)\Gamma(s) = -\frac{1}{p}\sum_{a=0}^{p-1}\zeta_p^a f(\zeta_p^a)\int_0^1 \frac{(\log(\frac{1}{x}))^{s-1}}{x-\zeta_p^a}dx.$$

In particular, at $s=1$,

$$L\left(1,\left(\frac{\cdot}{p}\right)\right) = -\frac{1}{p}\sum_{a=0}^{p-1}\zeta_p^a f(\zeta_p^a)\int_0^1 \frac{dx}{x-\zeta_p^a}.$$

This integral can be done by using ordinary calculus:

$$\int_0^1 \frac{dx}{x-\zeta_p^a} = \log\left(2\sin\frac{m\pi}{p}\right) + \frac{i\pi}{2}\left(1-\frac{2m}{p}\right).$$

Hence,

$$L\left(1,\left(\frac{\cdot}{p}\right)\right) = -\frac{1}{p}\sum_{a=0}^{p-1}\zeta_p^a f(\zeta_p^a)\left(\log\left(2\sin\frac{a\pi}{p}\right) + \frac{i\pi}{2}\left(1-\frac{2a}{p}\right)\right).$$

$$\zeta_p^a f(\zeta_p^a) = \sum_{m=1}^{p-1}\left(\frac{m}{p}\right)\zeta_p^{am}$$

is called the Gauss sum, g_a. There are several important facts about Gauss sums that can be found in [**Da**, Chapter 2], namely $g_a = \left(\frac{a}{p}\right)g_1$; and $g_1^2 = \left(\frac{-1}{p}\right)p$. In particular $g_1 \neq 0$.

Hence, we can simplify our formula even further to

$$\begin{aligned} L\left(1,\left(\frac{\cdot}{p}\right)\right) &= -\frac{g_1}{p}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\log\left(2\sin\frac{a\pi}{p}\right) + \frac{i\pi}{2}\left(1-\frac{2a}{p}\right)\right) \\ &= -\frac{g_1}{p}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\log\left(2\sin\frac{a\pi}{p}\right) + \frac{\pi a i}{p}\right), \end{aligned}$$

where for the last equation we used the fact from Lemma 1.2.12 that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$.

Now we must split into cases depending on whether $p \equiv 1$ or $3 \pmod 4$.

Case 1. $p \equiv 3 \pmod 4$

In the case, $\left(\frac{a}{p}\right) = -\left(\frac{p-a}{p}\right)$, and $\sin\frac{m\pi}{p} = \sin\frac{(p-m)\pi}{p}$. Hence, we get

$$L\left(1,\left(\frac{\cdot}{p}\right)\right) = -\frac{g_1\pi}{p^2}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)a.$$

Now, $\sum_{a=1}^{p-1} a$ is odd and $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)a$ is odd and hence non-zero. Thus our theorem is proved.

Case 2. $p \equiv 1 \pmod 4$

Now we have $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$ and $\sin\frac{m\pi}{p} = -\sin\frac{(p-m)\pi}{p}$. Therefore,

$$L\left(1,\left(\frac{\cdot}{p}\right)\right) = -\frac{g_1}{p}\log\frac{\prod_{a=\square}\sin\frac{a\pi}{p}}{\prod_{a\neq\square}\sin\frac{a\pi}{p}}.$$

Notice that

$$\begin{aligned} \prod_{a=\square}\sin\frac{a\pi}{p} &= \prod_{a=\square}\frac{e^{\frac{a\pi i}{p}} - e^{\frac{-a\pi i}{p}}}{2i} = \left(\frac{1}{2i}\right)^{\frac{p-1}{2}}\prod_{a=\square}e^{\frac{a\pi i}{p}}(1-e^{\frac{-2a\pi i}{p}}) \\ &= \left(\frac{1}{2i}\right)^{\frac{p-1}{2}}e^{\frac{\pi i}{p}\sum_{a=\square}a}\prod_{a=\square}(1-e^{\frac{-2a\pi i}{p}}) = \left(\frac{1}{2i}\right)^{\frac{p-1}{2}}e^{\frac{\pi i}{p}\sum_{a=\square}a}\prod_{a=\square}(1-\zeta_p^a). \end{aligned}$$

We can make an identical calculation to show that

$$\prod_{a\neq\square} \sin\frac{a\pi}{p} = \left(\frac{1}{2i}\right)^{\frac{p-1}{2}} e^{\frac{\pi i}{p}\sum_{a\neq\square} a} \prod_{a\neq\square}(1-\zeta_p^a).$$

Since -1 is a square, $\sum_{a=\square} a = \sum_{a\neq\square} a = \frac{p-1}{2}\cdot p$.
Thus combining our last two equations we see that

$$\frac{\prod_{a=\square}\sin\frac{a\pi}{p}}{\prod_{a\neq\square}\sin\frac{a\pi}{p}} = \frac{\prod_{a=\square}(1-\zeta_p^a)}{\prod_{a\neq\square}(1-\zeta_p^a)} = \frac{A}{B}.$$

Notice that A and B live in the field $\mathbb{Q}(\zeta_p)$. The Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is just $(\mathbb{Z}/p\mathbb{Z})^\times$ where a means the map sending $\zeta_p \mapsto \zeta_p^a$. The subgroup of squares in $(\mathbb{Z}/p\mathbb{Z})^\times$ is the unique subgroup of index 2 and thus fixes the only field with degree 2 over $\mathbb{Q}$. In fact, since Gauss proved that $g_1^2 = \left(\frac{-1}{p}\right)p$ in the case $p \equiv 1 \pmod 4$, this quadratic subfield is none other than $\mathbb{Q}(\sqrt{p})$. A and B are clearly fixed by this subgroup. Furthermore they are taken to each other under any non-square automorphism. Therefore, we must have $A = x + y\sqrt{p}$ and $B = x - y\sqrt{p}$ with x, y rational. Notice that since $AB = p$, $x^2 - py^2 = p$. Clearly this implies that $y \neq 0$. (Notice that, although Dirichlet did not know Galois theory, Gauss had constructively worked out the complete Galois theory for cyclotomic extensions $\mathbb{Q}(\zeta_p)$.)

In conclusion, because $x + y\sqrt{p} \neq x - y\sqrt{p}$, we have shown that

$$L\left(1, \left(\frac{\cdot}{p}\right)\right) = -\frac{g_1}{p}\log\frac{A}{B} = -\frac{g_1}{p}\log\frac{x+y\sqrt{p}}{x-y\sqrt{p}} \neq 0.$$

□

1.3 Riemann and the Functional Equation

1.3.1 Introduction

Euler published shelves and shelves of papers about number theory; Dirichlet is remembered most for his extensive work in number theory; Riemann, on the other hand, published only a single number theory paper (*On the Number of Primes Less Than a Given Magnitude*, which was a mere 7 pages) in his entire life (which lasted from 1826 to 1866). This paper is packed full of little jewels with hardly a wasted word. Apart from this paper Riemann was best known for his work in geometry (Riemannian metrics, for example) and complex analysis (such as the Cauchy-Riemann equations). In fact, it was Riemann's outsider's perspective as a complex analyst which enabled him to have some amazing new insights into the behavior of primes and of the Zeta function which now bears his name.

1.3.2 Analytically Continuing the Zeta Function

Riemann's paper has been translated into English by H.M. Edwards and appears as an appendix to [**Ed**]. Riemann begins his paper by saying,

"In this investigation I take as my starting point the observation of Euler that the product

$$\prod \frac{1}{1-\frac{1}{p^s}} = \sum \frac{1}{n^s}$$

where p ranges over all prime numbers and n over all whole numbers. The function of a complex variable s which these two expressions define when they converge I denote by $\zeta(s)$. They converge only when the real part of s is greater than 1; however, it is easy to find an expression of the function which always is valid."[**Ed**, p.299]

The important thing to realize is that, unlike Euler in his attempts to extend the zeta function to negative integers, Riemann had a well-defined notion of what it meant to "find an expression of the function which always is valid." From complex analysis we know that, if two functions are complex analytic and agree on some nice region (one that contains one of its limit points), then they must agree everywhere that both are defined. Thus, for Riemann, if he can give a complex analytic function which agrees with ζ on the right half-plane $\mathrm{Re}(s) > 1$, then this is the *only* way that this function can be defined there. Thus we can manipulate the formula for $\zeta(s)$ where it converges and, if at some point we get a formula which makes sense for more values, we can take this to be the definition of the ζ-function without any ambiguity.

For an example of the notion of analytic continuation, see a proof in [**L2**, Chapter XV §2] of the analytic continuation of the Γ-function, a result which we will assume in this paper along with the following additional facts about the Γ-function.

Proposition 1.3.1. *The Γ-function can be analytically continued to the entire plane with simple poles at the negative integers and no zeroes. It satisfies the following properties:*

$$\Gamma(s+1) = s\Gamma(s) \tag{1.3.1}$$

$$\frac{\pi}{\Gamma(s)\Gamma(1-s)} = \sin \pi s \tag{1.3.2}$$

$$\Gamma(s) = 2^s \pi^{-\frac{1}{2}} \Gamma\left(1+\frac{s}{2}\right) \Gamma\left(\frac{s-1}{2}\right) \tag{1.3.3}$$

Riemann begins with a slight variant of Dirichlet's formula that

$$L(s,\chi) = -\frac{1}{\Gamma(s)} \int_0^1 \frac{f(x)}{x^p - 1} \left(\log\left(\frac{1}{x}\right)\right)^{s-1} dx,$$

where $f(x) = \sum_{a=1}^{m-1} \chi(a) x^{a-1}$.

Notice that making the change of variables $x \mapsto nx$ in Definition 1.1.16, we get

$$\Gamma(s) n^{-s} = \int_0^\infty e^{-nx} x^{s-1} dx.$$

Summing both sides and interchanging summation and integration (which can be easily justified since the integral converges uniformly in n), we get

$$\Gamma(s)\zeta(s) = \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx.$$

Riemann turns to evaluating this integral by cleverly choosing a complex contour around which to integrate the function. So, consider the integral

$$\int_{\gamma_{\delta,\epsilon}} \frac{(-z)^s}{e^z - 1} \frac{dz}{z},$$

where γ is a contour which begins at $+\infty$ and at a distance ϵ above the real line continues until it gets to real part δ, where it makes a positively oriented circle of radius δ, stopping just below the real line at $-\epsilon$ and continuing back to $+\infty$. By $(-z)^s$, Riemann means $e^{s\log(-z)}$ where we take the principal branch of the logarithm. Thus, this is not defined on the positive real axis which is why Riemann's contour must avoid it. By $\int_\gamma$, we will mean the limit of the integrals $\int_{\gamma_{\delta,\epsilon}}$ as ϵ and δ go to 0.

This integral can be pictured better by considering the Riemann surface which looks like a spiral parking lot and which is the codomain of the many valued function $\log(-x)$. Then we can ignore ϵ and consider γ_δ to be the contour which goes from $+\infty$ to δ away from 0 on the first floor above the origin, then takes a circle of radius δ about the origin ending up on the first floor below the origin and finally returning to $+\infty$ on this lower floor.

At this point Riemann simply states the value of this new integral assuming that his reader can make the derivation independently. I, however, do not find this integral entirely trivial. Riemann's skill at estimating integrals occasionally got him into trouble when he claimed that some integral could be bounded and after his death the method of evaluating them was lost.

So, following [**Ed**, p. 10], if we take ϵ to be very small with respect to δ, then the integral is extremely close to,

$$\int_{+\infty+\epsilon i}^{\delta+\epsilon i} \frac{(-z)^s}{e^z - 1} \frac{dz}{z} + \int_{|z|=\delta} \frac{(-z)^s}{e^z - 1} \frac{dz}{z} + \int_{\delta-\epsilon i}^{+\infty-\epsilon i} \frac{(-z)^s}{e^z - 1} \frac{dz}{z}.$$

First we consider the middle integral. Notice that, if we let the angle θ parameterize the circle (i.e. $z = \delta e^{i\theta}$), then $\frac{dz}{z} = id\theta$. Now define g such that $\frac{(-z)^s}{e^z-1} = g(\theta)$. Thus, the middle integral is just $\int_0^{2\pi} g(\theta) i d\theta$. But, so long as $s > 1$, $\frac{(-z)^s}{e^z-1}$ stays bounded as $z \to 0$. Therefore, if we take δ arbitrarily small, $g(\theta)$ approaches a single value. Therefore, this middle integral vanishes as δ goes to 0.

The remaining two integrals are over two different branches of the logarithm. Hence, on the first branch $(-z)^s = e^{i\pi s} z^s$, while on the other $(-z)^s = e^{-i\pi s} z^s$. Therefore, the whole integral becomes

$$\int_\gamma \frac{(-z)^s}{e^z - 1} \frac{dz}{z} = (e^{i\pi s} - e^{-i\pi s}) \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx.$$

Combining this with our old formula for $\zeta(s)$, we see that for $\mathrm{Re}(s) > 1$,

$$\zeta(s) = \frac{1}{2i \sin(\pi s)\Gamma(s)} \int_\gamma \frac{(-z)^s}{e^z - 1} \frac{dz}{z}.$$

Thus, by Equation 1.3.2,

$$\zeta(s) = \frac{\Gamma(-s)}{2\pi i} \Gamma(s) \int_\gamma \frac{(-z)^s}{e^z - 1} \frac{dz}{z}.$$

But the right hand side of that last formula actually gives an analytic function which makes sense for all complex numbers s with the exception of the pole at 1! To see this, notice that the integral part is clearly finite because of the rapid growth of e^z. Thus, the formula makes sense with the possible exceptions of s a positive integer where $\Gamma(-s)$ has poles. We already know that ζ is happily defined for all positive integers other than 1 and that it has a simple pole of order 1 at 1. Hence the ζ-function of Euler can be uniquely extended to the Riemann ζ-function, which is a function of a complex variable and is analytic on the whole complex plane except for the pole at $s = 1$.

1.3.3 Proving Euler's Special Values

Now that we have a definition of the ζ-function which makes sense for negative values, we can attempt to verify Euler's $\zeta(-n) = -\frac{B_{n+1}}{n+1}$. Although Riemann's notes show that he was aware that his methods allowed him to answer this question, he omitted this computation from his paper (considering it too far afield from his immediate goals). (Here we follow [**Ed**, p. 12].)

By definition,

$$\zeta(-n) = \frac{\Gamma(n+1)}{2\pi i}\int_\gamma \frac{(-z)^{-n}}{e^z-1}\frac{dz}{z}.$$

But, since n is an integer, a glance back at our old formula shows that the two branch terms exactly cancel each other out. Furthermore, from Definition 1.1.13, we get

$$\begin{aligned}\zeta(-n) &= \frac{n!}{2\pi i}\int_{|z|=\delta}\left(\sum_{k=0}^{\infty} B_k\frac{z^k}{k!}\right)(-z)^{-n}\frac{dz}{z^2}\\ &= (-1)^n\frac{n!}{2\pi}\left(\sum_{k=0}^{\infty}\frac{B_k}{k!}\right)\int_{|z|=\delta}(z)^{m-n-1}d\theta\\ &= (-1)^n n!\frac{B_{n+1}}{(n+1)!} = (-1)^n\frac{B_{n+1}}{n+1}.\end{aligned}$$

Thus, we have proved Euler's result on the negative special values. To get the positive even special values we need to prove the functional equation. Using a few Gamma function identities, we can change this functional equation from Euler's form to

Theorem 1.3.2 (Functional Equation, Statement 1).

$$\zeta(s) = \Gamma(1-s)(2\pi)^{s-1}2\sin(\frac{s\pi}{2})\zeta(1-s).$$

The methods which we have used above give a quick proof of this fact. In Riemann's own words,

"When the real part of s is negative, the integral can be taken, instead of in the positive sense around the boundary of the given domain, in the negative sense around the complement of this domain because in that case (when $\mathrm{Re}(s) < 0$) the integral over values with infinitely large modulus is infinitely small. But inside this complementary domain the only singularities of the integrand are at the integer multiples of $2\pi i$, and the integral is therefore equal to the sum of the integrals taken around these singularities in the negative sense." [**Ed**, p. 300]

A short calculation, which will be left as an exercise to the reader, shows that this residue sum yields exactly the functional equation. Instead of dwelling on this, we shall move on to Riemann's much more important second proof of the functional equation.

1.3.4 Riemann's Second Proof of the Functional Equation

Before addressing this theorem, we need a classical lemma. Let $\theta(z) = \sum_{n\in\mathbb{Z}} e^{-\pi i n^2 z}$ be Jacobi's theta function.

Theorem 1.3.3 (Functional Equation of the Theta Function).

$$\theta\left(-\frac{1}{z}\right) = \sqrt{-iz}\,\theta(z).$$

Proof. Let $f_z(x) = e^{-\pi i x^2 z}$. A simple calculation shows that $\hat{f}_z(y) = \frac{1}{\sqrt{-iz}}e^{-i\pi y^2/z}$. The theorem follows immediately from the Poussin summation formula. □

Riemann noticed that the functional equation of the zeta function could be written in a much more symmetric form using some Γ function identities. Namely, by Equation 1.3.2 and Equation 1.3.3,

$$\begin{aligned}\zeta(s) &= \Gamma(1-s)(2\pi)^{s-1}2\sin\left(\frac{s\pi}{2}\right)\zeta(1-s)\\ &= \pi^{-\frac{1}{2}}2^{-s}\Gamma\left(1-\frac{s}{2}\right)\Gamma\left(\frac{s-1}{2}\right)2^s\pi^{s-1}\frac{\pi s}{2}\Gamma\left(1+\frac{s}{2}\right)\Gamma\left(1-\frac{s}{2}\right)\zeta\left(1-s\right).\end{aligned}$$

Rearranging terms and replacing s with $2s$, this is equivalent to

Theorem 1.3.4 (Functional Equation of the ζ-function, Statement 2).

$$\Gamma(s)\pi^{-s}\zeta(2s) = \Gamma\left(\frac{1}{2}-s\right)\pi^{-\frac{1}{2}+s}\zeta(1-2s).$$

Proof. (Riemann's original proof appears in [**Ed**, pp. 300-301].) This time we take the definition of the Gamma function and make the change of variables $x \to n^2\pi x$ to get

$$n^{-2s}\pi^{-s}\Gamma(s) = \int_0^\infty e^{-n^2\pi x}x^s\frac{dx}{x}.$$

Again we sum over all n and use uniform convergence to interchange sum and integral to get

$$\zeta(2s)\pi^{-s}\Gamma(s) = \int_0^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x}.$$

Now we can apply the lemma to the right hand side:

$$\begin{aligned}\zeta(2s)\pi^{-s}\Gamma(s) &= \int_0^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x} = \int_0^1 \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x} + \int_1^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x}\\ &= \int_1^\infty \frac{1}{2}(\theta(-1/ix)-1)x^{-s}\frac{dx}{x} + \int_1^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x}\\ &= \int_1^\infty \frac{1}{2}(x^{\frac{1}{2}}\theta(ix)-1)x^{-s}\frac{dx}{x} + \int_1^\infty \frac{1}{2}(\theta(ix)-1)x^s\frac{dx}{x}\\ &= \int_1^\infty \frac{1}{2}(\theta(ix)-1)(x^{\frac{1}{2}-s}+x^s)\frac{dx}{x} + \int_1^\infty \frac{1}{2}(-x^{\frac{1}{2}-s}-x^{-s})\frac{dx}{x}\\ &= -\frac{1}{2(\frac{1}{2}-s)} - \frac{1}{2s} + \int_1^\infty \frac{1}{2}(\theta(ix)-1)(x^{\frac{1}{2}-s}+x^s)\frac{dx}{x}.\end{aligned}$$

Notice that the right hand side is defined and analytic for all of $\mathbb{C}$ except for simple poles at $s=0$ and $s=\frac{1}{2}$. Thus we have given another analytic continuation of ζ to the complex plane except for $s=1$ (the pole at 0 coming from the Γ factor). But more importantly, this formula is clearly symmetric under the change of variables $s \to \frac{1}{2}-s$ and our theorem is proved. Making the change of variables back from $2s \to s$, we see that the completed ζ-function $\pi^{-s/2}\Gamma(s/2)\zeta(s)$ is symmetric about the line $\mathrm{Re}(s)=1/2$ and only has poles at $s=0$ and $s=1$. □

At this point, we have gotten through about two and a half pages of Riemann's paper. In the rest of the paper, he outlines a program for proving the prime number theorem, $\pi(x) \sim \frac{x}{\log x}$, by rewriting $\pi(x)$ in terms of ζ. In particular, his argument suggests that the prime number theorem is equivalent to the claim that the ζ-function has no zeroes on the line $\mathrm{Re}(s)=1$. However, all of these results and wonderful ideas are well beyond the scope of this paper. Hence we shall leave Riemann having just taken his functional equation. For more details see [**Ed**] or [**Da**, Chapters 8-13].

One last gem from this paper: on the bottom of the third page, Riemann makes his famous conjecture (that the zeros of the completed ζ-function lie on the line of symmetry $\mathrm{Re}(s)=1/2$) with the following remark:

"One would of course like to have a rigorous proof of this, but I have put aside the search for such a proof after some fleeting vain attempts because it is not necessary for the immediate objective of my investigation." [**Ed**, p. 301]

I suppose we should be thankful that he put these vain attempts aside or perhaps the rest of his paper would never have seen the light of day.

1.4 Dedekind ζ-functions and Hecke L-series

1.4.1 Introduction

During the course of the 19th century, the focus of number theory broadened from the study of the integers to the study of other rings which had properties reminiscent of the integers. In particular, when studying biquadratic reciprocity, Gauss introduced the notion of the Gaussian integers $\mathbb{Z}[i] = \{a + bi : a,\ b \in \mathbb{Z}\}$. He proved that this ring shares many important properties with the integers. Over the course of the century, this idea was further generalized to the notion of a "ring of integers."

Definition 1.4.1. *A number field is a finite algebraic extension of* $\mathbb{Q}$.

Definition 1.4.2. *If K is a number field, we say that one of its elements is an algebraic integer if it is a root of a monic polynomial with integer coefficients. The set of algebraic integers in K will be denoted $\mathcal{O}_K$ and will be called a "ring of integers." (To see that this is a ring see [**J**, pp. 4-5]). Henceforth, we shall refer to algebraic integers as simply "integers" and use the term "rational integers" to denote elements of $\mathbb{Z}$.*

Dedekind realized that one could define an analogue of the ζ-function for each of these rings of integers. Dedekind lived from 1831-1916. He was Gauss's last Ph.D. students, and a friend of our previous heroes Dirichlet and Riemann. He is perhaps best remembered for rephrasing Kummer's theory of ideals in its modern form.

Years later, in 1917, Hecke (1887-1947) proved that Dedekind's ζ-function could be analytic continued to a meromorphic function on the whole plane except for $s = 1$ and $s = 0$ and that the completed ζ-functions had a functional much like Riemann's functional equation for his ζ-function. In his attempt to further generalize his ideas, he defined Hecke's L-functions, which are a common generalization of Dedekind's ζ-functions and Dirichlet's L-functions. Hecke was also able to give an analytic continuation and functional equation for these L-functions. Although we have neither the time nor the space to repeat Hecke's proof, we will at least state his key results.

1.4.2 Unique Factorization and Rings of Integers

The key fact about the Riemann ζ-function which gives it a connection to number theory is the existence of an Euler Factorization. This, in turn, depends on unique factorization in $\mathbb{Z}$. Thus, before we can give a definition of the ζ-function for a ring of integers $\mathcal{O}_K$, we must first explore whether such rings have unique factorization into primes.

First, let us consider the special case $\mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(i)}$. We say that an element π of $\mathbb{Z}[i]$ is irreducible if whenever $\pi = \alpha\beta$ either α or β is a unit. In order to show that every element $\alpha \in \mathbb{Z}[i]$ can in fact be written as a product of irreducibles we would like to use descent, but this requires some notion of size. Therefore, we define the norm $N(a + bi) = a^2 + b^2 = (a + bi)(a - bi)$. This norm is multiplicative and $N\alpha \geq 0$ with equality if and only if $\alpha = 0$. Furthermore, since it is multiplicative, we can easily see that if u is a unit iff $Nu = 1$.

Proposition 1.4.3. *Every nonzero Gaussian integer can be written as a product of irreducibles (where units are considered an empty product of irreducibles).*

Proof. If this statement were false, we could take α with minimal norm under the condition that it is not a product of irreducibles. But then $\alpha = \beta\gamma$ with $N\beta,\ N\gamma > 1$. Hence, since $N\alpha = N\beta N\gamma$ we have $N\alpha > N\beta,\ N\gamma$. Therefore, by assumption, β and γ are products of irreducibles, this is clearly a contradiction. □

Uniqueness of this factorization follows from the following version of the division algorithm,

Proposition 1.4.4 (Gauss). *For any Gaussian integers α and $\beta \neq 0$, there exists q and r in $\mathbb{Z}[i]$ such that*

$$\alpha = \beta q + r \qquad \text{where } Nr < N\beta.$$

Proof. Consider $\frac{\alpha}{\beta} \in \mathbb{Q}(i)$. Clearly, this must lie in some lattice square in the complex plane. Thus, it must be within $\frac{\sqrt{2}}{2}$ of a lattice point. If that lattice point is the gaussian integer q, then we can multiply by β to get $\alpha = \beta q + r$ with $Nr \leq \left(\frac{\sqrt{2}}{2}\right)^2 N\beta < N\beta$. A priori, $r \in \mathbb{Q}(i)$, but, since $r = \alpha - \beta q$, it is actually in $\mathbb{Z}[i]$. □

Thus, by a standard argument (see [**B-S**, Section 3.2.2] for example), the existence of a division algorithm implies:

Theorem 1.4.5 (Gauss). *Any non-zero Gaussian integer can be written as a product of irreducibles uniquely up to order and unit multiples.*

Thus, we can attempt a definition of a ζ-function for the Gaussian integers. First, we notice that in the integer case we only summed over the positive integers. Thus, in the case of the Gaussian integers, we should remember to keep in mind that each non-zero Gaussian integer has four different unit multiples.

Definition 1.4.6. *For $Re(s) > 1$, let*

$$\zeta_{\mathbb{Z}[i]}(s) = \frac{1}{4} \sum_{\alpha \in \mathbb{Z}[i] - \{0\}} N(\alpha)^{-s} = \prod_{\pi} \frac{1}{1 - \frac{1}{N\pi^s}},$$

where $\prod_\pi$ means a product over all irreducibles but counting each set of unit multiples only once. (To see that this sum converges for $Re(s) > 1$, simply write $\alpha = a + bi$ and bound the partial sums by a double integral.)

A similar argument proves unique factorization for $\mathbb{Z}[\sqrt{-2}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-2})}$, or $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-3}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$. However, if we tried to use the same argument for $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ this argument would fail miserably because the space between elements of $\mathbb{Z}[\sqrt{-5}]$ is simply too large. In fact, unique factorization fails in this ring of integers. For example, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ has two factorizations as a product of irreducibles. (To see this, notice that $2 = \alpha\beta$ implies $N\alpha|4$ which is impossible, and similar for the factors.)

In order to fix this problem of non-unique factorization Kummer (a number theorist who lived from 1810-1893) proposed adding to our usual irreducibles additional "ideal primes" which would restore unique factorization. In the above example, 6 would be a product of four ideal primes which could be grouped differently to give the two expressions above. Kummer noticed that the an irreducible a would have to factor further when $\mathcal{O}/a$ contains a zero divisor b. In this case there must be a composite homomorphism from $\mathcal{O} \to \mathcal{O}/a \to (\mathcal{O}/a)/b$. Thus Kummer proposed that there be an ideal prime corresponding to every homomorphism from $\mathcal{O}$ to a finite field. (For Kummer's original ideas see his letter [**Ku**, Vol. 1, p. 64-68] and the article [**Ku**, Vol. 1, pp. 211-367].) Dedekind, in his paper *Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines enlichen Körpers.* [**De**, Vol 1, p. 105], rephrased Kummer's notions in terms of the much more convenient modern notion of an ideal. Kummer's plan is justified by the following remarkable theorem,

Theorem 1.4.7 (Kummer). *If $\mathcal{O}_K$ is a ring of integers, then each of its non-zero ideals $\mathfrak{a}$ can be written uniquely as a product of prime ideals.*

(For a 19th century proof of this theorem see [**Hi**, §5], for a modern proof see [**J**, Chapter I, Theorem 3.14].)

Sometimes we would like to make the set of all non-zero ideals into a group. To do this, we define a fractional ideal as an abstract quotient of two ideals. This gives a group (which we denote I_K) which is free abelian generated by the prime ideals. It will also be useful to be able to write all ideals in terms of the principal one. To this end we make the following definition.

Definition 1.4.8. *Let P_K denote the principal fractional ideals, that is to say fractional ideals which are abstract quotients of principal ideals. The ideal class group of K is $Cl_K = I_K/P_K$.*

Theorem 1.4.9. *Cl_K is a finite abelian group.*

Proof. See [**J**, Chapter I, Theorem 13.8] or [**Hi**, Theorem 50]. □

The size of the ideal class group is called the class number.

1.4.3 The Norm and the Trace

In order to generalize our definition of the ζ-function we need to generalize the norm to elements of a general ring of integers, and to the norm of an ideal of a ring of integers.

Definition 1.4.10. *Consider K a number field and $\alpha \in K$. Let L be the Galois closure of K. Let $G = Gal(L/\mathbb{Q})$ and $H = Gal(L/K)$. The cosets G/H correspond to the embeddings of K into L which fix $\mathbb{Q}$. We define*

$$N\alpha = \prod_{\sigma \in G/H} \sigma(\alpha).$$

Since the norm is clearly fixed by $\mathrm{Gal}(L/Q)$, the norm must be rational. Furthermore, if $\alpha \in \mathcal{O}_K$, then $N\alpha$ is an algebraic integer (and thus a rational integer).

Definition 1.4.11. *If $\mathfrak{a}$ is a non-zero ideal in a ring of integers $\mathcal{O}_K$, then define*

$$N\mathfrak{a} = \prod_{\sigma \in G/H} \sigma(\mathfrak{a}).$$

Both of these definitions clearly define multiplicative functions. Furthermore, if (a) is a principal ideal, then $N(a) = (Na)$.

Both of these notions can be generalized further to the notion of a relative norm. Suppose L/K is an extension of number fields. Let M be the Galois closure of L. Again, we take $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. Thus, G/H is identified with the embeddings of L into M which preserve K.

Definition 1.4.12.

$$N_{L/K}\alpha = \prod_{\sigma \in G/H} \sigma(\alpha).$$

Again we see that $N\alpha \in K$ and sends integers to integers. Similarly, if $\mathfrak{a}$ is an ideal we define

$$N_{L/K}\mathfrak{a} = \prod_{\sigma \in G/H} \sigma(\mathfrak{a}).$$

Lastly, we will occasionally require the related notion of the trace.

Definition 1.4.13.

$$Tr_{L/K}\alpha = \sum_{\sigma \in G/H} \sigma(\alpha).$$

Again we see that $Tr\alpha \in K$ and sends integers to integers. Similarly, if $\mathfrak{a}$ is an ideal we define

$$Tr_{L/K}\mathfrak{a} = \sum_{\sigma \in G/H} \sigma(\alpha).$$

The norm is obviously multiplicative while the trace is additive. Furthermore, both the norm and trace behave well in towers. By this we mean that if one has a tower of field extensions $L/M/K$, then $N_{L/K} = N_{M/K}N_{L/M}$ and $\mathrm{Tr}_{L/K} = \mathrm{Tr}_{M/K}\mathrm{Tr}_{L/M}$.

It is worth noting that the trace and norm of an element can also be defined as the trace and determinant respectively of the K-linear transformation A_α from $L \to L$ given by multiplication by α. To see this, look at terms in the characteristic polynomial of an element corresponding to the determinant and the trace (cf. [**J**, Chapter I, Theorem 5.3]).

Proposition 1.4.14. *If $\alpha \in \mathcal{O}_K$, then $|N\alpha| = |\mathcal{O}_K/\alpha\mathcal{O}_K|$. If $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$ then $|N\mathfrak{a}| = |\mathcal{O}_K/\mathfrak{a}|$.*

Proof. Since $\alpha\mathcal{O}_K$ is a lattice in $\mathcal{O}_K$, the number of elements in the quotient space is just the volume of the fundamental parallelepiped. That is to say, $|\mathcal{O}_K/\alpha\mathcal{O}_K| = |\det(A_\alpha)| = |N\alpha|$. For an ideal the proof is more difficult, cf. [**J**, Chapter I, Proposition 8.4]. □

1.4.4 The Dedekind Zeta Function

The results from the last section allow us to give Dedekind's definition of the ζ-function associated to a number field. Dedekind first gave this definition in [**De**, P. 118].

Proposition 1.4.15. *If K is a number field then the series*

$$\zeta_K(s) = \sum_{\mathfrak{a}} N\mathfrak{a}^{-s}$$

(where $\mathfrak{a}$ here as always ranges over all nonzero ideals of $\mathcal{O}_K$) converges for all $Re(s) > 1$. Furthermore in that domain,

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}}$$

(here as always $\mathfrak{p}$ ranges over all nonzero prime ideals of $\mathcal{O}_K$).

Proof. We go about this proof backwards, first showing that the product converges and using that to show that the sum converges.

First, we claim that if $n = [K : \mathbb{Q}]$, then there are at most n prime ideals of $\mathcal{O}_K$ dividing a rational prime p. From the definition, $Np = p^n$. But, (p) factors uniquely as a product of prime ideals $p = \mathfrak{p}_1 \dots \mathfrak{p}_\ell$. Thus, k is the number of primes sitting above p. Since $N\mathfrak{p}_1 | p^n$ and is bigger than 1, we must have $N\mathfrak{p}_i \geq p$. Therefore, $p^n = Np = N\mathfrak{p}_1 \dots N\mathfrak{p}_\ell \geq p^k$.

Therefore,

$$\prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}} < \left(\frac{1}{1 - p^{-s}} \right)^n.$$

Therefore, since we already know that the Euler product for the ζ-function converges in this right half-plane, we get the same result for this new Euler product.

Now we notice that, by unique factorization into ideals,

$$\sum_{\mathfrak{a}:\ N\mathfrak{a}<n} N\mathfrak{a}^{-s} < \prod_{\mathfrak{p}:\ N\mathfrak{p}<n} \frac{1}{1 - N\mathfrak{p}^{-s}}.$$

Therefore, since the product converges, the sum must too, and they converge to the same value. □

Lastly, before moving on, we should note that Dedekind's ζ-function tells us about the distribution of prime ideals in $\mathcal{O}_K$ in much the same way as Riemann's ζ-function told us about the distribution of primes in $\mathbb{Z}$.

1.4.5 Hecke's Größencharakters

Now we turn our attention to generalizing Dirichlet's L-series. The major hurdle in doing this is that, in order to get Euler factorization, these characters should be functions of ideals not elements. Even in $\mathbb{Z}$ this presents a problem. If χ is an odd Dirichlet character modulo m (that is to say $\chi(-1) = -1$), then χ is not a well-defined function of an ideal because $(-a) = (a)$ but $\chi(-a) \neq \chi(a)$. In this case, we can easily fix this problem by telling the function to take into account the sign of the number. That is to say, if $\chi(-1) = (-1)^p$, we have the function on ideals given by,

$$\chi((a)) = \chi(a) \left(\frac{a}{|a|} \right)^p.$$

In order to generalize this notion, suppose $\mathfrak{m}$ is an ideal of $\mathcal{O}_K$, and we have a character χ_f of the abelian group $(\mathcal{O}_K/\mathfrak{m})^\times$. Let $I_K^{\mathfrak{m}}$ be the set of all fractional ideals which are relatively prime to $\mathfrak{m}$. We would like to find characters $I_K^{\mathfrak{m}} \to S^1$ which agree with χ_f in a manner similar to the correspondence in the last paragraph for $\mathbb{Z}$.

Suppose $K = \mathbb{Q}(\sqrt{2})$. Here the problem is that we have an infinite number of units. It is a relatively simple exercise to show that all of the units are of the form $\pm(1 + \sqrt{2})^n$ for some integer n. So we need

to take χ_f and twist it by some factor which cancels out the contribution of the units. Furthermore, we would like this factor to look vaguely like that $\left(\frac{a}{|a|}\right)$ sign factor which we found for the $\mathbb{Z}$ case.

In $\mathbb{Q}(\sqrt{2})$ since we cannot algebraically distinguish $\sqrt{2}$ from $-\sqrt{2}$ we could define the sign of an element in two different ways. For example, although $1+\sqrt{2}$ is positive, if we had chosen the other value, then we would have found that $1-\sqrt{2}$ is negative. So, we have two absolute values $|\cdot|_1$ and $|\cdot|_2$ and for each of them we get a possible sign. This suggest an additional factor of the form,

$$\left(\frac{a}{|a|_1}\right)^{p_1}\left(\frac{a}{|a|_2}\right)^{p_2}.$$

In fact, since -1 is negative in both embeddings and $1+\sqrt{2}$ is positive in one embedding and negative in the other, it is easy to see that for some choice of p_1, p_2 we can get this twisting factor to cancel out the annoying contributions from the units.

In general, a number field K can be embedded into the complex numbers in $n = [K:\mathbb{Q}]$ different ways. Some of the images of these embeddings are contained in the reals and will be called *real embeddings*. Others cannot be, and since complex conjugation is an automorphism of $\mathbb{C}$ these embeddings will come in pairs of distinct conjugate *complex embeddings*. Suppose that K has r_1 real embeddings and r_2 pairs of complex embeddings (thus $r_1+2r_2 = n$), then we can define an embedding from $K^\times \to (\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2} = \mathcal{G}$. Since $\mathcal{O}_K^\times \hookrightarrow \mathcal{G}$, any character of the units will come from a character of $\mathcal{G}$. Thus our above examples both fit into the following definition.

Definition 1.4.16. *If $\mathcal{O}_K$ is a ring of integers in which every ideal is principal, then $\chi : I_K^{\mathfrak{m}} \to S^1$ is a Hecke Größencharakter modulo $\mathfrak{m}$ if it can be written in the form $\chi((a)) = \chi_f(a)\chi_\infty(a)$ where $\chi_f(a)$ is a character of $(\mathcal{O}_K/\mathfrak{m})^\times$, and χ_∞ is a character of $\mathcal{G}$.*

Now suppose $\mathcal{O}_K$ is a ring of integers in which not every ideal is principal. In order to define a Größencharakter in this context we need to add another factor which extends the above definition to non-principal ideals. This is where the notion of the ideal class group is helpful. To define a character on the whole ideal group, we just need to know what it is on the ideal class group together with what it is on the principal part.

Definition 1.4.17. *Consider $\mathcal{O}_K$ is a ring of integers, with class group $I_K/P_K = \{a_1, \dots a_n\}$. Then, $\chi : I_K^{\mathfrak{m}} \to S^1$ is a Hecke Größencharakter modulo $\mathfrak{m}$ if it can be written in the form $\chi(a_i(a)) = \chi_{cl}(a_i)\chi_f(a)\chi_\infty(a)$ where χ_{cl} is a character of $Cl(K)$, $\chi_f(a)$ is a character of $(\mathcal{O}_K/\mathfrak{m})^\times$, and χ_∞ is a character of $\mathcal{G}$.*

1.4.6 Characters of $(\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2}$

During the rest of this section we roughly follow [**N**, §6 and §8]. Before turning our attention to the L-series associated to these Größencharakter, we first take a slight detour to find an explicit description of the characters of $\mathcal{G}$. This will give us a very good handle on the Größencharakter since the other two components are simply characters of finite abelian groups.

Proposition 1.4.18. *If χ_∞ is a character of $\mathcal{G}$, then*

$$\chi(x_1,\dots,x_{r_1},z_1,\dots,z_{r_2}) = \prod_{\ell=1}^{r_1}\left(\frac{x_\ell}{|x_\ell|}\right)^{p_\ell}|x_\ell|^{iq_\ell}\prod_{j=1}^{r_2}\left(\frac{z_j}{|z_j|}\right)^{p_j'}|z_j|^{iq_j'},$$

where the p_ℓ's are either 0 or 1, the p_j''s are integers and the q's are all real numbers.

Proof. First, notice that since $x = \frac{x}{|x|}|x|$, we can split up $\mathbb{R} = \{\pm 1\}\times\mathbb{R}^+$ and $\mathbb{C} = S^1\times\mathbb{R}^+$. So, we can reduce the problem to finding all characters of $\{\pm1\}$, S^1, and $\mathbb{R}^+$.

The characters of $\{\pm1\}$ are clearly given by either raising to the zeroth or first power. Also the characters of S^1 are well known to be given by raising to integer powers.

This only leaves showing that the characters of $\mathbb{R}^+$ are given by raising to a purely imaginary power. To see this, notice that the logarithm gives an isomorphism between $\mathbb{R}^+$ under multiplication and $\mathbb{R}$ under addition. The characters of the latter are given by $e^{iy\cdot}$ for some real y. Hence, the characters of the former are in the form $e^{iy\log\cdot} = \cdot^{iy}$. □

1.4.7 Hecke L-Functions

Now we can finally give a definition of a Hecke L-function.

Definition 1.4.19. *If χ is a primitive Größencharakter (that is to say χ_f does not factor through $\mathcal{O}_K/\mathfrak{d}$ for any $\mathfrak{d}|\mathfrak{n}$), then we define, for $Re(s) > 1$,*

$$L(s,\chi) = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) N\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} \frac{1}{1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}}.$$

(Here convergence is obvious from the convergence of the Dedekind ζ-function. If χ is non-trivial it actually converges conditionally in a larger halfplane.)

The crucial fact about these L-functions is that they have an analytic continuation and functional equation. Hecke's proof of this fact is a generalization of Riemann's second proof. Hecke defined much more complicated θ-functions and showed that their Mellin transforms were Hecke L-series times a factor involving the Gamma function.

In order to state this function equation we will need to define the discriminant of a number field and we will need to write down the appropriate Γ-factor.

1.4.8 Discriminants

Consider an extension of number fields L/K, with $n = [L : K]$. Suppose that $(\alpha_1, \ldots, \alpha_n)$ is a basis for L as a K-vector space, and that $\{\sigma_1 \ldots \sigma_n\}$ are all the embeddings of L into $\mathbb{C}$ which agree with some fixed embedding of K (if L/K is Galois, this set is identified with the Galois group).

Definition 1.4.20. *The discriminant $\mathfrak{d}(\alpha_1, \ldots, \alpha_n)$ is the determinant of the matrix $(\sigma_i\alpha_j)_{ij}$.*

The important properties of the discriminant are summarized in the following proposition.

Proposition 1.4.21.

1. $$\mathfrak{d}_{L/K}(\alpha_1, \ldots, \alpha_n) = \det((Tr_{L/K}(\alpha_i\alpha_j))_{ij}).$$
2. *If A is some linear transformation of L as a K vector space, and $(\beta_1, \ldots, \beta_n)^t = A(\alpha_1, \ldots, \alpha_n)^t$, then*
$$\mathfrak{d}_{L/K}(\beta_1, \ldots, \beta_n) = (\det A)^2 \mathfrak{d}_{L/K}(\alpha_1, \ldots, \alpha_n).$$

Proof. The second of these claims is clear. For the first, see [**N**, p. 11]. □

By part 2 of Proposition 1.4.21, we see that if $(\alpha_1\mathbb{Z} + \ldots + \alpha_n\mathbb{Z}) = \mathcal{O}_L$ then the discriminant does not depend on this choice of basis. Therefore, we can define the discriminant $\mathfrak{d}_{L/K}$ to be the discriminant of any $\mathbb{Z}$-basis for the ring of integers. Furthermore, since the trace of an integer in L is an integer in K, by part 2 of Proposition 1.4.21, we see that the discriminant $\mathfrak{d}_{L/K} \in \mathcal{O}_K$. This discriminant has the following important property:

Proposition 1.4.22.

$$\mathfrak{d}_{L/K} = (\mathfrak{d}_{M/K})^{[L:M]} N_{M/K}(\mathfrak{d}_{L/M})$$

Proof. For a proof see [**N**, Corrollary 2.10] or [**Hi**, §15]. □

1.4.9 The Gamma Factor

Definition 1.4.23. *Using the same notation as Proposition 1.4.18, if χ is a Hecke Größencharakter, then Hecke defined the Γ-factor corresponding to this character to be,*

$$L_\infty(\chi, s) = \prod_{\ell=1}^{r_1} \pi^{-\frac{(s+p_\ell - iq_\ell)}{2}} \Gamma\left(\frac{(s+p_\ell - iq_\ell)}{2}\right) \prod_{j=1}^{r_2} 2(2\pi)^{-(s+p'_j - iq'_j)} \Gamma(s + p'_j - iq'_j).$$

1.4.10 The Functional Equation of the Hecke L-function

We need one last notion before we can state Hecke's functional equation and that is the notion of a conductor. Consider χ a Größencharakter modulo $\mathfrak{m}$ with finite part χ_f. χ_f need not be a primitive character of $(\mathcal{O}_K/\mathfrak{m})^\times$. If it were not primitive then it would factor through $(\mathcal{O}_K/\mathfrak{a})^\times$ for some $\mathfrak{a}|\mathfrak{m}$. If it factors through $(\mathcal{O}_K/\mathfrak{a}_1)^\times$ and $(\mathcal{O}_K/\mathfrak{a}_2)^\times$, then it would have to factor through $(\mathcal{O}_K/\gcd(\mathfrak{a}_1,\mathfrak{a}_2))^\times$ So, we can define the conductor $\mathfrak{f}(\chi)$ to be the smallest of these $\mathfrak{a}$.

For example, if $K=\mathbb{Q}$ and $\mathfrak{m}=8$, then we are looking at characters of the group $(\mathbb{Z}/8\mathbb{Z})^\times$. Such a character is defined by where it sends 3 and where it sends 5. So, let $\chi_{i,j}$ be the function which sends 3 to i and 5 to j (i and j are both either ± 1). $\chi_{1,1}$ is clearly trivial. Thus its conductor is 1. $\chi_{1,-1}$ and $\chi_{-1,-1}$ do not factor through $(\mathbb{Z}/4\mathbb{Z})^\times$ since 5 is not in their kernels, and thus their conductor is 8. In the remaining case, $\chi_{-1,1}$ it is easy to see that it factors through $(\mathbb{Z}/4\mathbb{Z})^\times$ but not $(\mathbb{Z}/2\mathbb{Z})^\times$. Therefore, it has conductor 4.

Any Größencharakter modulo $\mathfrak{m}$ corresponds to a unique Größencharakter modulo $\mathfrak{f}(\chi)$. However, the Euler factorization of their L-functions will differ by finitely many terms. In the case of the integers we already saw this when we noticed that the Dirichlet L-series of the trivial character modulo m differed by a finite number of Euler factors from the Riemann ζ-function. To fix this problem, for non-primitive Größencharakter we change our definition of the L-function slightly.

Definition 1.4.24. *If χ is a Größencharakter modulo $\mathfrak{m}$ then we define its Hecke L-series to be the Hecke L-series of the corresponding primitive character modulo $\mathfrak{f}(\chi)$.*

Theorem 1.4.25. *Suppose χ is a Hecke Größencharakter of K modulo $\mathfrak{m}$. Consider the extended Hecke L-function,*

$$\Lambda(\chi,s)=(|\mathfrak{d}_{K/\mathbb{Q}}|N_{K/\mathbb{Q}}\mathfrak{f}(\chi))^{\frac{s}{2}}L(\chi,s)L_\infty(\chi,s).$$

This extended function Λ has a meromorphic continuation to the entire complex plane, which is holomorphic everywhere (except for two simple poles in the case that χ_f is trivial, χ_{cl} is trivial, and all the p's and p''s are 0). Furthermore, it satisfies the functional equation

$$\Lambda(\chi,s)=\epsilon(\chi)\Lambda(\bar{\chi},1-s),$$

where $|\epsilon(\chi)|=1$ and $\bar{\chi}(\mathfrak{a})=\overline{\chi(\mathfrak{a})}$.

Proof. For the original proof of this theorem see [**He**, pp. 178-197], for another exposition along the same lines see [**N**, Chapter VII]. A completely different approach to this theorem was developed by Tate in his thesis [**C-F**, Chapter XV]. For the special case of a Dirichlet L-series see [**Da**, Chapter IX]. □

1.5 Frobenius, the Frobenius Automorphism, and Group Representation Theory

1.5.1 Introduction

In this section, we discuss two ideas which at first glance have nothing in common. Historically, however, there is a strong connection: both of these concepts first appeared in papers of Frobenius published in 1896. Surprisingly enough, as we shall see later, there is an important mathematical connection between these two concepts since the combination of these two notions will be exactly what we need to further generalize the notion of an L-function.

Frobenius lived from 1849-1917. First we shall look at the question from number theory of how a prime ideal in one ring of integers factors in some extension to another ring of integers. One of the most important concepts in understanding this question is the notion of the Frobenius automorphism which one can attach to a prime. Although the paper in which Frobenius defined this automorphism [**Frob**, Vol. II, p. 719] was not published until 1896, its contents were well known for almost two decades before that and Frobenius was simply waiting on Kummer's publication of his ideal theory. Secondly, we shall turn our attention to the subject of group representation theory which was pioneered by Frobenius [**Frob**, Vol. III, pp. 1-77] (along with Molien and Burnside, among others). Here Frobenius generalized the notion of a group character to non-abelian groups.

1.5.2 Factoring Primes in Extensions

Suppose we have an extension of number fields L/K and a prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$. Let n be the degree $[L : K]$. We know, by Theorem 1.4.7, that $\mathfrak{p}$ factors uniquely into prime ideals in $\mathcal{O}_L$. Our goal in this section is to get more information about how these primes factor. (For another exposition of this material see [**Se2**, Chapter 1 §4].)

In particular, suppose that $\mathfrak{p} = \prod_i \mathfrak{P}_i^{e_i}$. We would like to know more about the $\mathfrak{P}_i$, for example, what are their norms? Since the norm is multiplicative,

$$\mathfrak{p}^n = N_{L/K}\mathfrak{p} = \prod_i N_{L/K}\mathfrak{P}_i^{e_i}. \tag{1.5.1}$$

Therefore, by unique factorization into ideals, we must have that each of the individual norms $N_{L/K}\mathfrak{P}_i = \mathfrak{p}^{f_i}$ for some positive integer f_i.

Definition 1.5.1. *If $\mathfrak{P}$ is a prime in $\mathcal{O}_L$ dividing a prime $\mathfrak{p}$ in $\mathcal{O}_K$, then we define $e_{\mathfrak{P}/\mathfrak{p}}$ to be the highest power of $\mathfrak{P}$ which still divides $\mathfrak{p}$, and $f_{\mathfrak{P}/\mathfrak{p}}$ to be the exponent which makes $N_{L/K}\mathfrak{P} = \mathfrak{p}^{f_{\mathfrak{P}/\mathfrak{p}}}$. These numbers are called the ramification degree and the residue field degree respectively.*

As we shall often discover, the primes which ramify are much less convenient than the primes which do not ramify. Fortunately, there are only finitely many ramifying primes as we can see by the following theorem.

Theorem 1.5.2. *A prime ramifies in an extension L/K exactly when it divides the relative discriminant $\mathfrak{d}_{L/K}$.*

Proof. For a 19th century proof see [**Hi**, Theorem 31] and for a more modern proof see [**J**, Chapter I, Theorem 7.3]. □

Proposition 1.5.3. *If we have a tower of fields $M/L/K$, and $\mathfrak{P}$ a prime in M, with $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_L$, and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.*

1. $e_{\mathfrak{q}/\mathfrak{P}} e_{\mathfrak{P}/\mathfrak{p}} = e_{\mathfrak{q}/\mathfrak{p}}$.
2. $f_{\mathfrak{q}/\mathfrak{P}} f_{\mathfrak{P}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}}$.

Proof. The first of these equations is clear. The second follows immediately from the property of norms in towers. □

Furthermore, we have from Equation 1.5.1

Proposition 1.5.4.

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}} = n.$$

The numbers $f_{\mathfrak{P}/\mathfrak{p}}$ also have another interpretation which justifies the name "residue field degree." Let $\ell_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ and $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$. Since $(\mathcal{O}_K \cap \mathfrak{P})|\mathfrak{p}$, we actually must have equality. Therefore, $\ell_{\mathfrak{P}}$ is a field extension of $k_{\mathfrak{p}}$.

Proposition 1.5.5.

$$f_{\mathfrak{P}/\mathfrak{p}} = [\ell_{\mathfrak{P}} : k_{\mathfrak{p}}].$$

Proof. By definition, $N_{L/K}\mathfrak{P} = \mathfrak{p}^{f_{\mathfrak{P}/\mathfrak{p}}}$. Now take, $N_{K/\mathbb{Q}}$ of both sides,

$$|\ell_{\mathfrak{P}}| = N_{L/\mathbb{Q}}\mathfrak{P} = N_{K/\mathbb{Q}}\mathfrak{p}^{f_{\mathfrak{P}/\mathfrak{p}}} = |k_{\mathfrak{p}}|^{f_{\mathfrak{P}/\mathfrak{p}}}.$$

Therefore,

$$[\ell_{\mathfrak{P}} : k_{\mathfrak{p}}] = \log_{|k_{\mathfrak{p}}|} |\ell_{\mathfrak{P}}| = f_{\mathfrak{P}/\mathfrak{p}}.$$

□

Now we turn our attention to the special case of L/K a Galois extension with $G = \mathrm{Gal}(L/K)$. Notice that since G fixes the base field, G acts on the set of primes $\mathfrak{P}_i$ sitting over a given prime $\mathfrak{p}$. Clearly e and f should be well-defined on each orbit of this action.

Proposition 1.5.6. *G acts transitively on the set of $\mathfrak{P}_i$.*

Proof. $N\mathfrak{P}_1 = \mathfrak{p}^{f_1}$. So, for any i, $\mathfrak{P}_i$ divides $\mathfrak{p}$ which in turn divides $N\mathfrak{P}_1$. But the norm is the product over all the conjugates. So by unique factorization into prime ideals we must have that $\mathfrak{P}_i$ is one of the Galois conjugates of $N\mathfrak{P}_1$ and so Galois group acts transitively. □

Since the Galois groups acts transitively we see that we actually have a well-defined $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$. Therefore, Proposition 1.5.4 becomes,

Theorem 1.5.7. *If $g_{\mathfrak{p}}$ is the number of distinct primes dividing $\mathfrak{p}$ in $\mathcal{O}_L$, then*

$$e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}} = n.$$

□

Since all the other parts of the efg-equation are multiplicative in towers, we also must have that g is multiplicative in towers.

One method of finding the way which a prime factors in an extension was given by Kummer.

Theorem 1.5.8 (Kummer's Theorem). *Suppose we have an extension of number fields L/K with $L = K(\alpha)$, where α is an integer with minimal polynomial $f(x)$. Suppose that $\mathfrak{p}$ is a prime in L which factors as $\mathfrak{p} = \prod_{i=1}^{k} \mathfrak{P}_i^{e_i}$ where $\mathfrak{P}_i$ has residue field degree f_i, then we also must have that $f(x) \equiv \prod_{i=1}^{k} g_i(x)^{e_i} \pmod{\mathfrak{p}}$ where $g_i(x)$ is an irreducible polynomial modulo $\mathfrak{p}$ of degree f_i.*

Proof. See [**J**, Chapter I, Theorem 7.4]. □

1.5.3 The Decomposition and Inertia Groups, and the Frobenius Automorphism

Now we get to the point where the important idea of Frobenius comes into play. With L/K still Galois, we fix some particular prime $\mathfrak{P}$ sitting over $\mathfrak{p}$. Recall from the last section that we have the residue field extension $\ell_{\mathfrak{P}}/k_{\mathfrak{p}}$ of degree $f_{\mathfrak{P}/\mathfrak{p}}$.

Definition 1.5.9. *Let $G_{\mathfrak{P}}$ be the subgroup of G which fixes the prime ideal $\mathfrak{P}$. This is called the decomposition group of $\mathfrak{P}$.*

Since the Galois group acts transitively on the primes there are g different primes, $|G_{\mathfrak{P}}| = \frac{n}{g} = ef$. Clearly we have a map from $G_{\mathfrak{P}} \to \mathrm{Gal}(\ell_{\mathfrak{P}}/k_{\mathfrak{p}})$. The kernel of this map is called the inertia group. We wish to show that this map is actually surjective. In order to do this we need to find the structure of $\mathrm{Gal}(\ell/k)$.

Lemma 1.5.10. *Suppose $\mathbb{F}_q$ is a finite field with $q = p^m$ elements. Then $Gal(\mathbb{F}_q/\mathbb{F}_p)$ is generated by the Frobenius automorphism φ defined by $\varphi(x) = x^p$.*

Proof. That φ actually is an automorphism follows from the binomial theorem. By Fermat's little theorem it fixes $\mathbb{F}_p$. To see that φ generates the entire group, we need to show that it has order m which is the size of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Suppose φ has order k. Then the polynomial $x^{p^k} - x$ has p^m solutions in F_q. Therefore $m \leq k$. Hence φ must have order m. □

Proposition 1.5.11. *$Gal(\ell_{\mathfrak{P}}/k_{\mathfrak{p}})$ is a cyclic group generated by the Frobenius automorphism attached to the prime $\mathfrak{P}$ $\varphi_{\mathfrak{P}/\mathfrak{p}}(x) = x^{N\mathfrak{p}}$.*

Proof. Since we know that $\mathrm{Gal}(\ell_{\mathfrak{P}}/\mathbb{F}_p)$ (where $p = \mathfrak{P} \cap \mathbb{Z}$) is cyclic and generated by $\varphi(x) = x^p$, $\mathrm{Gal}(\ell/k)$ has no choice but to be the unique subgroup with $[\ell_{\mathfrak{P}} : k_{\mathfrak{p}}]$ elements, generated by $\phi^{[k_{\mathfrak{p}}:F_p]}$. Since the norm is the same as the number of elements in the quotient ring, this generator is clearly the map which sends $x \mapsto x^{N\mathfrak{P}}$. □

Proposition 1.5.12. *There exists an element of the decomposition group which maps to $\varphi_{\mathfrak{P}/\mathfrak{p}}$. By abuse of notation, this element of the quotient group $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ will also be called the Frobenius automorphism attached to $\mathfrak{P}$ and be still be notated $\varphi_{\mathfrak{P}/\mathfrak{p}}$. By Proposition 1.5.11 this implies that the map $G_{\mathfrak{P}} \to Gal(\ell_{\mathfrak{P}}/k_{\mathfrak{p}})$ is surjective.*

Proof. (We follow Hilbert's proof [**Hi**, Theorem 69]. For Frobenius's original proof see [**Frob**, Vol. 2, pp. 719-733]. Unfortunately this simple proof seems to have been lost and most proofs in modern texts, e.g. [**J**, Chapter III], are much more complicated.) By the Chinese Remainder Theorem and the fact that the multiplicative group of a finite field is cyclic, we can choose a to be a generator of the unit group $\mathcal{O}_L/\mathfrak{P}$ which is divisible by all the Galois conjugates of $\mathfrak{P}$. Let

$$F(x) = \prod_{\sigma \in G} (x - \sigma a).$$

Clearly $F(a) \equiv 0 \pmod{\mathfrak{P}}$. But then, because raising to the $N\mathfrak{p}$ is an isomorphism of the quotient ring,

$$F(a^{N\mathfrak{p}}) \equiv F(a)^{N\mathfrak{p}} \equiv 0 \pmod{\mathfrak{P}}.$$

Hence, we must have for some $\sigma \in G$, $\sigma a = a^{N\mathfrak{p}}$. Suppose σ were not in the decomposition group. Then we have $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$, so by the choice of a, $a \equiv 0 \pmod{\sigma^{-1}\mathfrak{P}}$. This would imply, $\sigma a = 0 \pmod{\mathfrak{P}}$ which is a contradiction. Therefore this automorphism lies in the decomposition group. Therefore, its behavior in the whole ring of integers is determined by its behavior on the quotient field, and since a is a generator we actually get that $\sigma b = b^{N\mathfrak{p}} \pmod{\mathfrak{P}}$ for all b. □

Therefore, we have an isomorphism, $G_{\mathfrak{P}}/I_{\mathfrak{P}} \to \mathrm{Gal}(\ell_{\mathfrak{P}}/k_{\mathfrak{p}})$. Comparing sides, we see that $\frac{ef}{|I_{\mathfrak{P}}|} = f$. Therefore the size of the inertia group gives you the ramification degree. In particular if $\mathfrak{P}/\mathfrak{p}$ is unramified (that is to say $e = 1$), then the Frobenius automorphism corresponding to $\mathfrak{P}$ can be thought of as an element of the Galois group.

Proposition 1.5.13. *If $\mathfrak{P}/\mathfrak{p}$ is unramified in the extension L/K, then the Frobenius automorphism attached to $\mathfrak{P}$ has order f in the Galois group G.*

Proof. This follows immediately from the fact that the size of the decomposition group is $ef = f$. □

In particular, a prime splits completely (that is $e = 1$, $f = 1$, $g = n$) exactly when its Frobenius is trivial.

Lastly we summarize a few more properties of the Frobenius and the decomposition group.

Proposition 1.5.14. *1. If $\sigma\mathfrak{P}\sigma^{-1} = \mathfrak{P}'$ are two primes sitting above $\mathfrak{p}$, then $G_{\mathfrak{P}'} = \sigma G_{\mathfrak{P}}\sigma^{-1}$, and $\varphi_{\mathfrak{P}'} = \sigma\varphi_{\mathfrak{P}}\sigma^{-1}$. In particular if G is abelian, then the Frobenius does not depend on the choice of $\mathfrak{P}|\mathfrak{p}$.*

2. *Suppose M is an intermediate field so that $K \subset M \subset L$, and $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M$. Then, $\varphi_{\mathfrak{P}/\mathfrak{q}} = \varphi_{\mathfrak{P}/\mathfrak{p}}^{f_{\mathfrak{q}/\mathfrak{p}}}$.*

3. *Again we take an intermediate field M, this time with M/K Galois. Then $\varphi_{\mathfrak{P}/\mathfrak{p}}$ restricts to an element of $Gal(M/K)$ by forgetting its action on L. This restriction is $\varphi_{\mathfrak{q}/\mathfrak{p}}$.*

4. *Suppose L and M are both Galois over K, and furthermore there composite ML is also Galois over K. Then we have a map $Gal(ML/K) \to Gal(M/K) \times Gal(L/K)$ given by restriction in each component. This map sends the Frobenius of some prime $\mathfrak{P}$ in $\mathcal{O}_{ML}$ to the Frobenius in each component of the prime we get by intersecting with the appropriate ring of integers.*

Proof. All of these are straightforward applications of the definition. For a proof see [**J**, Chapter III] □

1.5.4 The Frobenius Density Theorem

Just as we asked before whether there were infinitely many primes which were 1 modulo m, another logical question to ask is whether there are infinitely primes in $\mathcal{O}_K$ which have some particular e, f, and g in the Galois extension L/K. Frobenius realized that his automorphism gave him the tools he needed to attack this question. Before stating his result we need the notion of Dirichlet density.

Definition 1.5.15. *Suppose S is a set of primes in a number field K. Then the Dirichlet density is defined to be (if it exists)*

$$\delta(S) = lim_{s\to 1}\frac{(\sum_{\mathfrak{P}\in S} N(\mathfrak{P})^{-s})}{(\sum_{\mathfrak{P}} N(\mathfrak{P})^{-s})}.$$

Obviously, the Dirichlet density of the set of all primes in the ring of integers is 1, and the Dirichlet density of any finite set is 0. Furthermore we notice that up to a bounded error term the denominator in the definition of Dirichlet density is the logarithm of the Dedekind ζ-function. We showed in Section 2 that $\log\zeta_{\mathbb{Q}}(s) = -\log(s-1) + O(1)$ because $\lim_{s\to 1^+}(s-1)\zeta_{\mathbb{Q}}(s) = 1$. It turns out that a similar result is true for a general Dedekind ζ-function.

Proposition 1.5.16. *If K is any number field, there exists some constant c*

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

Proof. In fact c has a nice formula in terms of the class number and some other invariants of the number field. Unfortunately the proof of this fact is beyond the scope of this paper. For a proof see [**J**, Chapter IV, Theorem 2.12]. □

Therefore, by the usual argument,

$$\sum_{\mathfrak{P}} N(\mathfrak{P})^{-s} = \log\prod_{\mathfrak{P}}\frac{1}{1-N\mathfrak{P}^{-s}} + O(1) = -\log(s-1) + O(1).$$

So we can conclude that the Dirichlet density of S is $\delta(S)$ iff

$$lim_{s\to 1}\sum_{\mathfrak{P}\in S} N(\mathfrak{P})^{-s} = -\delta(S)\log(s-1) + O(1).$$

Furthermore, it is true that if the usual density of a set of primes exists, then so does the Dirichlet density and they are equal. The converse, however, is not true.

Frobenius conjectured that the primes would be no more likely to have one Frobenius automorphism than any other one. We should pause for a moment to make sure this makes any sense. For one thing ramified primes do not have a well-defined Frobenius automorphism in the Galois group. But since

there are only finitely many such primes the set of ramified primes has density zero. Furthermore the Frobenius attached to a prime in the base field is only determined up to conjugacy in the Galois group since we could choose a different prime sitting above it. Keeping these two facts in mind, Frobenius made the following conjecture:

Conjecture 1.5.17 (Chebotarev's Density Theorem). *Consider the conjugacy class $[\sigma] \in G = Gal(K/k)$. Let S be the set of primes in k with primes sitting over whose Frobenius automorphism is σ. Then, $\delta(S) = \frac{|[\sigma]|}{|G|}$.*

Although Frobenius was not able to prove this general result, he was able to give a proof of a weaker result which says something much more awkward about the distribution of primes among certain subsets of G. Since Chebotarev eventually proved this conjecture of Frobenius, Frobenius's weaker theorem has been largely forgotten. This is unfortunate since the Frobenius Density Theorem is just as useful as Chebotarev's Theorem in many cases and is far easier to prove.

Definition 1.5.18. *Let σ be an element of order m in a group G. The division of σ is the collection of all elements in G which are conjugate to some σ^k with k and m relatively prime.*

Being in the same division is clearly an equivalence relation and so we can partition any group into its divisions.

Theorem 1.5.19 (Frobenius Density Theorem). *Let D be a division of $G = Gal(K/k)$, and let S be the set of primes in k with primes sitting over them with Frobenius automorphism in D. Then $\delta(S) = |D|/|G|$.*

Proof. (This proof is taken largely from [**J**, Chapter IV, Theorem 5.2][5] and is also copied verbatim from [**Sn**] by the current author.)

First we note an elementary lemma from group theory. If σ is an element of order m in G then the number of elements in the division of σ is $\varphi(m)[G : N_G(\langle\sigma\rangle)]$ (where φ is Euler's totient function and $N_G(H)$ is the normalizer of a subgroup G). For a proof of this fact see [**J**, Chapter IV, Prop. 5.2].

Now we proceed by induction on m the order of σ. The base case is relatively easy, which is remarkable considering that for most of the applications this is the only part of the theorem which we will use. (Again, it is worth remembering that we have used some non-trivial results about the Dedekind ζ-function and so this is not quite as easy as I've made it out to be.)

For $m = 1$ we have that $\sigma = 1$, so S is the set of primes of k which split completely in K. Consider S^* the set of all primes in K sitting over S. For each prime $\mathfrak{p} \in S$ there are exactly $(K : k) = |G|$ distinct primes in S^* with norm $\mathfrak{p}$. So,

$$\sum_{\mathfrak{P} \in S^*} N_{K/\mathbb{Q}}(\mathfrak{P})^{-s} = \sum_{\mathfrak{P} \in S^*} N_{k/\mathbb{Q}} N_{K/k}(\mathfrak{P})^{-s} = |G| \sum_{\mathfrak{p} \in S} N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}.$$

Now the set S has density 1, since the sum over primes with residue field degree more than 1 looks essentially like $\log \zeta(2s)$ which is finite at 1. So this equation tells us that the Dirichlet density of S must be $1/|G|$, which is exactly our base case.

The induction step is mostly a bunch of group theory combined with some elementary facts about the Frobenius automorphism. So assume that the order of σ is $m > 1$. For each $d|m$ let t_d denote the number of elements in the division of σ^d. Let S_d be the set of primes of k with Frobenius automorphism belonging to the division of σ^d (notice $S = S_1$). By induction we know that for $d \neq 1$ the Dirichlet density of S_d is $t_d/|G|$.

Let $L = K^{\langle\sigma\rangle}$. Now, by an elementary result, the primes $\mathfrak{p}$ of k which have at least one prime factor in L having residue field degree one are precisely those $\mathfrak{p}$ divisible by a prime $\mathfrak{P}$ of K such that the Frobenius automorphism of $\mathfrak{P}$ has a cycle of length one on the cosets of $\langle\sigma\rangle$. This occurs precisely when the Frobenius automorphism of $\mathfrak{P}$ is conjugate to some element of $\langle\sigma\rangle$, or in other words, $\mathfrak{p} \in S_d$ for some $d|m$.

Now let S_L be the set of primes of L having residue field degree one over k. For $\mathfrak{p} \in S_d$ let $n(p)$ be the number of primes of L which divide $\mathfrak{p}$ and have residue field degree one over k. Alternately, each

$\mathfrak{p} \in S_d$ is the norm of $n(\mathfrak{p})$ distinct primes in S_L. The Dirichlet density of S_L is obviously one. So we get the following relation:

$$-\log(s-1) \sim \sum_{\mathfrak{P} \in S_L} N_{k/\mathbb{Q}} N_{L/k}(\mathfrak{P})^{-s} = \sum_{d|m} \sum_{\mathfrak{p} \in S_d} n(\mathfrak{p}) N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}.$$

Now we need to find a formula for $n(\mathfrak{p})$. But by an elementary argument this is just the number of distinct cosets $\langle\sigma\rangle\sigma_i$ such that $\langle\sigma\rangle\sigma_i\sigma^d = H\sigma_i$, or alternately exactly when $\sigma_i \in N_G(\langle\sigma^d\rangle)$. So we have the formula, $n(\mathfrak{p}) = [N_G(\langle\sigma^d\rangle) : \langle\sigma\rangle]$.

With this formula and the formula for the sum above, we've reduced the problem to a relatively trivial exercise in elementary number theory.

$$\begin{aligned} -\log(s-1) \sim -\log(s-1) \left(\left(\sum_{d|m} \left[N_G(\langle\sigma^d\rangle) : \langle\sigma\rangle \right] \frac{t_d}{|G|} \right) - \left[N_G(\langle\sigma\rangle) : \langle\sigma\rangle \right] \frac{t_1}{|G|} \right) \\ + \left[N_G(\langle\sigma\rangle) : \langle\sigma\rangle \right] \sum_{\mathfrak{p} \in S_1} N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}. \end{aligned}$$

Applying the group theory lemma, and arranging all the $\log(s-1)$ terms on the same side we get:

$$\left[N_G(\langle\sigma\rangle) : \langle\sigma\rangle \right] \sum_{\mathfrak{p} \in S_1} N_{k/\mathbb{Q}}(\mathfrak{p})^{-s} \sim \log(s-1) \left(-1 - \frac{\varphi(m)}{m} + \frac{1}{m} \sum_{d|m} \varphi\left(\frac{m}{d}\right) \right).$$

But by elementary number theory that last sum is just n, and so we get that,

$$\left[N_G(\langle\sigma\rangle) : \langle\sigma\rangle \right] \sum_{\mathfrak{p} \in S_1} N_{k/\mathbb{Q}}(\mathfrak{p})^{-s} \sim -\left(\frac{\varphi(m)}{m} \right) \log(s-1).$$

So, by definition,

$$\delta(S_1) = -\frac{\varphi(n)}{n[N_G(\langle\sigma\rangle) : \langle\sigma\rangle]} = \frac{t}{|G|}$$

by the lemma. This concludes the induction step. □ □

In the next section we will see some remarkable applications of this theorem.

1.5.5 Group Representation Theory

Now we turn our attention to a completely different subject. In trying to factor the group determinant Frobenius was led to generalize the notion of a character to a general non-abelian group. For a the history of this problem and Frobenius's solution, see [**C1**]. Over the next few years through the work of Frobenius and Molien these non-abelian group characters found a more natural definition in the context of what is now known as group representation theory. This section summarizes the important results which we will need. Proofs of all of these results can be found in [**Se1**], and instead of trying to give any proofs, I will simply cite the appropriate result in that text.

If G is a group, then we define a representation of G to be a vector space V over some field k, together with a homomorphism $\rho : G \to \mathrm{GL}(V)$. That is to say, a representation is a vector space together with a linear action of the group on the vector space. When we wish to shorten notation we will refer to the representation V and leave ρ implied. We will only be interested in representations where G is finite, V is finite dimensional, and $k = \mathbb{C}$.

Example of representations abound, in fact when you imagine a group you probably imagine some particular representation of it. For example, if S_n is the group of permutations on n objects there is an obvious n-dimensional representation where the action is given by permuting the standard basis vectors. Alternately D_{2n}, the dihedral group with $2n$ elements, has a two-dimensional representation given by its action on a polygon in the plane.

First a few definitions,

Definition 1.5.20. *Suppose we have two representations (ρ_1, V_1) and (ρ_2, V_2), and a linear map $f : V_1 \to V_2$. We call this map a G-map if it commutes with the action of G. That is to say, if $\rho_2 f = f\rho_1$. Furthermore if f is a vector space isomorphism and a G-map, then we call it an isomorphism of representations, and say that V_1 and V_2 are isomorphic.*

One can easily show that isomorphism is an equivalence relation on representations of a given group G. The space of all G-maps from V_1 to V_2 will be denoted $\mathrm{Hom}_G(V_1, V_2)$.

Definition 1.5.21. *A sub-representation $W \subset V$ is a subspace of V which is preserved by the action of G.*

Definition 1.5.22. *If a representation V has no proper sub-representations, then we call V irreducible.*

Definition 1.5.23. *If (V_1, ρ_1) and (V_2, ρ_2) are two representations of G, then we can define their direct sum to be the representation $(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$, where $\rho_1 \oplus \rho_2(v_1, v_2) = \rho_1(v_1) + \rho_2(v_2)$.*

Theorem 1.5.24. *Any representation can be written as the direct sum of irreducible representations.*

Proof. [**Se1**, Theorem 2, page 7] □

Theorem 1.5.25 (Schur's Lemma). *If V_1 and V_2 are irreducible representations, any G-map between them is either trivial or an isomorphism. In particular, any G-map from V_1 to itself is a scalar map.*

Proof. [**Se1**, Proposition 4, page 13]. □

Theorem 1.5.26. *The decomposition of a representation into a direct sum of irreducible representations is unique up to order.*

Proof. This follows immediately from Schur's lemma. □

Definition 1.5.27. *If (V, ρ) is a representation then we define its character to be $\chi_V : G \to \mathbb{C}$, defined by $g \mapsto Tr\rho(V)$.*

Notice that since the trace is the same on conjugates, we actually get that χ_V is a "class function", that is to say a function not of elements but of conjugacy classes. The set of all class functions from G to $\mathbb{C}$ will be denoted $R_{\mathbb{C}}[G]$.

In particular if V is a one dimensional representation then these characters agree with the abelian group characters of $G/\ker\rho$ as defined in Section 3. Furthermore we have a remarkable generalization of Theorem 1.2.14.

Theorem 1.5.28. *Let $V_1, V_2, \ldots, V_n$ be the irreducible representations of G with corresponding characters $\chi_1, \ldots, \chi_n$. Then these characters are a basis for the vector space $R_{\mathbb{C}}[G]$. Furthermore under the inner product*

$$(\chi, \psi)_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g)^{-1},$$

this basis $\chi_1, \ldots, \chi_n$ is orthonormal. It follows that for any two $g, h \in G$, $\sum_{i=1}^{n} \chi_i(gh^{-1})$ is 0 unless $g = h$ in which case it is $\frac{|G|}{|C_g|}$, where C_g is the conjugacy class of g.

Proof. [**Se1**, §2.3-5]. □

Thus all the information about the representations of a group can be written in a "character table" whose rows are indexed by the irreducible representations and whose columns are indexed by the conjugacy classes and whose entries are the values of the characters on those classes.

The free $\mathbb{Z}$-module generated by the irreducible characters is denoted $R[G]$ and is called the Grothendieck group of G. Its elements are called generalized characters. Clearly a generalized character corresponds to an actual one exactly when all the coefficients are non-negative. We have $R[G] \otimes \mathbb{C} = R_{\mathbb{C}}[G]$, and at times we will want to consider $R_{\mathbb{Q}}[G] = R[G] \otimes \mathbb{Q}$, the $\mathbb{Q}$-vector space generated by the irreducible characters.

Suppose we have $H \subset G$. Then we have an obvious restriction map sending representations of G to representations of H, by simply forgetting the G structure. This map is called Res^G_H. By abuse of notation we will refer to $\mathrm{Res}^G_H \chi$ where χ is a character or even a class function, it should be obvious that all of these notions coincide.

We would like to be able to go the other way and build up representations of G from representations of H.

Definition 1.5.29. *Suppose $H \subset G$ and W is a representation of H. Take some $g \in G$. We define a representation gW on gHg^{-1} by the vector space W together with the action $ghg^{-1}(w) = hw$.*

Definition 1.5.30. *Choose σ_i to be representatives of the cosets G/H. Consider the vector space $Ind_H^G W = \bigoplus_{\sigma_i} \sigma_i W$. We can define a G action on this vector space. We need to define $g(\sigma_i W)$. But, for some permutation $'$ and some map $h_{(\cdot)} : G \to H$, we get that $g\sigma i = \sigma_{i'} h_g$. So we can define $g(\sigma_i w) = \sigma_{i'}(h_g w)$. If we extend this action by linearity we get a representation $Ind_H^G W$.*

(This definition is not the same a Serre's, however they do define the same representation.)

Notice that if we choose some particular basis for W, then the matrix of the action of g on $Ind_H^G W$ is given by some block permutation matrix each of whose blocks is the matrix corresponding to the action of some h.

As one might expect we also define the induction map for characters and by extension for class functions.

Theorem 1.5.31.

$$Ind_H^G \chi(g) = \frac{1}{|H|} \sum_{s \in G} \chi(s^{-1} g s),$$

where we take χ to be zero when its argument does not lie in H.

Now suppose we have χ a character of H and ψ a character of G. We could define the inner product of these two characters in two different sensible ways, namely either restricting ψ to H or inducing χ to all of G. Frobenius proved the following remarkable fact,

Theorem 1.5.32 (Frobenius Reciprocity).

$$(Ind_H^G \chi, \psi)_G = (\chi, Res_H^G \psi)_H.$$

Proof. [**Se1**, Theorem 13, page 56] □

Frobenius reciprocity is actually a special case of a more general theorem which has another special case which we will shall also have occasion to use.

Theorem 1.5.33 (Frobenius Reciprocity, part 2). *If $H \lhd G$, then we can take any representation of G/H and consider it as a representation of G. Similarly we have a map in the other direction. If χ is a character of G, then we let $\chi^\natural$ be the character of G/H given by the average of the values of χ on the preimages. If χ is a character of G and ψ is a character of G/H, then*

$$(\chi, \psi)_G = (\chi^\natural, \psi)_{G/H}.$$

Proof. [**Se1**, Serre's Exercise 7.1(b), page 57]. The proof is immediate upon plugging in the definitions. □

The character $\chi_V^\natural$ on G/H actually comes from a natural representation of G/H.

Proposition 1.5.34. *If V is a representation of G and H is a normal subgroup of G, then*

$$V^H = \{v \in V : \ hv = v \ \forall \ h \in H\}$$

is a representation of G/H with character $\chi_{V^H} = \chi_H^\natural$.

Proof. Since h acts trivially the action of G is well-defined on cosets, therefore V^H is actually a representation of G/H. Now we turn to actually computing its character. Notice that $P : V \to V$ given by

$$P(v) = \frac{1}{|H|} \sum_{h \in H} hv,$$

is a G-map (since left H-cosets are the same as right H-cosets) and a projection onto V^H. Therefore,

$$\chi_{V^H}(g) = \mathrm{Tr}(\rho_V(g)P) = \mathrm{Tr}(P\rho_V(g)) = \mathrm{Tr}\left(\frac{1}{|H|} \sum_{h \in H} hgv\right) = \chi_V^\natural(g).$$

□

Proposition 1.5.35. *If H is a subgroup of G and N is a normal subgroup of G and W is a representation of H, then*

$$(Ind_H^G W)^N \cong Ind_{H/H\cap N}^{G/N} W^{H\cap N}.$$

Proof. This can be directly verified by checking that the characters of both sides are equal. On the other hand, a natural isomorphism is given in [**N**, p. 524] using a slightly different definition of the induced representation. □

Definition 1.5.36. *If (V, ρ) is a representation of a group G, then we define the dual representation (V^*, ρ^*) to be the dual vector space V together with the map $(\rho^*(f))(v) = f(\rho(v))$.*

Proposition 1.5.37. $\chi_{V^*}(g) = \overline{\chi_V(g)}$

Proof. By basic linear algebra, if we pick a basis, then $\rho^*(g)$ with respect to the dual basis is the inverse transpose of $\rho(g)$. Thus the eigenvalues of $\rho^*(g)$ are the inverses of the eigenvalues of $\rho(g)$. Since these eigenvalues must be $|G|$th roots of unity, the result follows. □

The following are a few special cases of representations which will be useful later.

Examples 1.

1. *V_0 denotes the trivial representation, it is one-dimensional and every element of G acts trivially.*
2. *The regular representation of G is $r_G = Ind_1^G V_0$ where V_0 denotes the trivial representation of the trivial subgroup 1. By Frobenius reciprocity, $r_G = \bigoplus_V V^{\dim V}$, where the sum is over all irreducible representations.*
3. *The regular representation always has one copy of the trivial representation, therefore we can write $r_G = V_0 \oplus a_G$ where a_G is the augmentation representation.*

The last result which we will need was proved much later.

Theorem 1.5.38 (Mackey's Theorem). *Suppose G is a group with subgroups H and K. Let $H^s = sHs^{-1}$. Recall from Definition 1.5.29 that we have a representation sW of H^s. Then*

$$Res_K^G Ind_H^G W = \bigoplus_{s \in K\backslash G/H} Ind_{H^s\cap K}^K Res_{H^s\cap K}^{H^s} sW.$$

Proof. [**Se1**, Proposition 22, page 58]. □

1.6 Class Field Theory Before Artin

1.6.1 Introduction

Class field theory was the crowning achievement of late 19th century and early 20th century number theory. Rather than a single result, it is a whole system of theorems which allows one to describe, given a fixed number field K, all its abelian extensions (that is to say the Galois extensions L/K such that $\mathrm{Gal}(L/K)$ is abelian) in terms of the internal structure of K. The theory is sufficiently complex that the mathematicians who proved the later results were not even born when these results were first conjectured. This section summarizes the progress in class field theory up until Artin published his paper *Über eine neue Art von L-Reihen*.

Much of the material in this section is taken from [**Sn**] by the present author. Most of the historical information is taken from Hasse's article in [**C-F**, Chapter XI] and Katsuya's article in [**C-M-D**]. For a relatively classical exposition of class field theory see [**J**, Chapters IV and V]. For a more modern exposition see [**N**, Chapters IV-VI] or [**L1**, Part II].

1.6.2 Kronecker and the First Dreams of Class Field Theory

Both Hasse and Katsuya trace the first baby steps towards class field theory to the work of Kronecker (1823-1891). He got a lucky early boost in his mathematics education when his teacher at the Liegnitz Gymnasium (the German equivalent of high school), was Kummer. He did important work in number theory, the theory of elliptic functions, and algebra. During the later parts of the 19th century Kronecker became very powerful in the University of Berlin and used his power somewhat subjectively to advance those who agreed with his somewhat quirky philosophical views on mathematics illustrated by his famous statement that "God Himself made the whole numbers – everything else is the work of men."

Kronecker made the first conjecture attempting to classify extensions of a number field. This is now known as the Kronecker-Weber Theorem [**Kr**, Vol. IV, pp. 1-11].

Theorem 1.6.1 (Kronecker-Weber). *Any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

Furthermore Kronecker's investigations into elliptic functions lead to his "liebster Jugendtraum" or "dearest dream of his youth" in 1880 [**Kr**, Vol. II, pp. 85-93]. At its root this is an attempt to generalize the Kronecker-Weber Theorem to fields other than $\mathbb{Q}$. That is to describe all abelian extensions of any given number field. Class field theory eventually gave the answer to this question in the abstract, but Kronecker had something more concrete in mind. If we let $f(z) = e^{2\pi iz}$. The Kronecker-Weber theorem can be restated:

Theorem 1.6.2. *The function $f(z)$ has the following properties:*

1. *The special values $f(\frac{1}{n})$ are all algebraic numbers.*
2. *The field extension $\mathbb{Q}(f(\frac{1}{n}))/\mathbb{Q}$ is abelian.*
3. *Every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(f(\frac{1}{n}))$ for some n.*

Kronecker's Jugendtraum was to generalize this form of Kronecker-Weber. That is to find specific holomorphic or meromorphic functions whose special values described all abelian extensions of a given number field. In particular he thought that the quadratic imaginary case could be done using certain elliptic functions. (See the last chapter of [**S-T**] for a nice elementary introduction to this case and a excellent description of Kronecker's Jugendtraum.)

Although this concrete method of class field theory has never proceeded beyond this quadratic imaginary case, this question raised by Kronecker was essential in raising the questions that class field theory would try to answer.

1.6.3 An Application of the Frobenius Density Theorem

Although Kronecker raised several crucial questions, he provided little in the way of tools with which to answer these questions. The first tool for classifying extensions of a number field was given by Frobenius's density theorem which we proved in the last section. For example, one can use this theorem to show that the extensions of a given number field are entirely determined by the sets of primes which split completely.

Proposition 1.6.3. *Suppose that K_1 and K_2 are normal extensions of k and let S_1 and S_2 denote the sets of primes of k which split completely in K_1 and K_2 respectively. Then $S_1 \subset S_2$ (except possibly for a set of Dirichlet density 0) if and only if $K_2 \subset K_1$.*

Proof. [**J**, Chapter IV, cor. 5.5] One direction is obvious, since if a prime splits completely in some number field it must split completely in any subfield.

The other direction uses the Frobenius density theorem. Suppose $S_1 \subset S_2$ (except for a set of density 0) and define $K = K_1 \cdot K_2$ the composite field. From the fact that the Frobenius automorphism is multiplicative for composites, a prime splits completely in the composite of two fields exactly when it splits completely in each of the fields. Therefore, the only primes which split completely in K are those in S_1. Now we use the Frobenius density theorem to compute the density of S_1 in two different ways and get, $(K : k)^{-1} = (K_1 : k)^{-1}$. This can only happen when $K_1 = K$, and so $K_2 \subset K_1$. □

This theorem reduces the question of classifying Galois extensions of a number field to classifying certain purely internal objects, namely the set of primes which splits in that extension. It is the description of what these sets of primes are for abelian extensions that the rest of class field theory deals with.

1.6.4 Weber and the First Results of Class Field Theory

After Kronecker raised the right questions, and Frobenius provided some important tools, it was Weber (1842-1913) who put these together and began the study of class field theory as we know it. Weber made important contributions to analysis and applications to mathematical physics, as well as the number theory which interests us here. During the 1890's he published several papers in number theory which laid the basis for class field theory. He also gave the first proof of Kronecker-Weber theorem in 1887 [**W1**].

First let us take a look at Kronecker-Weber theorem. Most modern books view this as a corollary of class field theory, but as with the Frobenius density theorem, this can be a dangerous view to take because the 19th century result is significantly easier to prove then the 20th century theorems of which it is an "easy corollary." The early proofs of Kronecker-Weber theorem were all elementary and mostly based on Hilbert's ramification theory (which we shall discuss briefly in Chapter 2). Unfortunately, all these results were published in German, and there is an unfortunate tendency in the literature to cite a German paper by Speiser from 1919 [**Sp**]. Fortunately in the past few years two elementary proofs of the Kronecker-Weber theorem have been published in English. One appears in [**M**, 9, section 4.4] and the other appears in the recent translation of Hilbert's Zahlbericht [**Hi**, Theorem 131]. Both proofs use Hilbert's notion of ramification fields which was not available to Weber.

Weber's other contribution was giving the first statements of the main results of class field theory. Weber introduced the notion of a "class field" attached to certain "class groups". Although he only treated special cases, Weber's definition works generally and agrees with the modern definition (with only one defect, since he was dealing with purely imaginary special cases he did not treat the primes at infinity).

In order to define these notions we first take a closer look at the Kronecker-Weber theorem. As we saw above an extension is completely determined by which primes split completely, that is to say those primes with trivial Frobenius automorphisms. In the case of a cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, the Galois group G is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$ where we act by raising ζ_m to a power. It is easy to see that the Frobenius attached to a prime above p is simply raising to the pth power. Thus the only primes which factor completely are those which are 1 modulo m. Now suppose $K \subset \mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m)/K = H$. By the result on the behavior of the Frobenius in towers, the primes which split completely in K are those which

are trivial in G/H, that is those which are elements of H. Hence, we can restate the Kronecker-Weber theorem as follows:

Corollary 1.6.4. *If $K/\mathbb{Q}$ is an Abelian extension then the set of primes which factor in $K/\mathbb{Q}$ is exactly the set of primes lying in some particular subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ for some m.*

Furthermore we can get a result in the reverse direction. For each subgroup H of $(\mathbb{Z}/m\mathbb{Z})^\times$ we get an abelian extension given by the subfield of $\mathbb{Q}(\zeta_m)$ fixed by H. As stated this correspondence is not unique, since we can realize essentially the same subset of $\mathbb{Z}$ as a subgroup of different $(\mathbb{Z}/m\mathbb{Z})^\times$. That is to say, if $d|m$ then we have a map $(\mathbb{Z}/m\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/d\mathbb{Z})^\times$ and the field corresponding to a subgroup H of $(\mathbb{Z}/d\mathbb{Z})^\times$ is the same as that corresponding to its pre-image in $(\mathbb{Z}/d\mathbb{Z})^\times$. Thus we make the following definition,

Definition 1.6.5. *A primitive class group modulo m for the field $\mathbb{Q}$ is a quotient group of the form $(\mathbb{Z}/m\mathbb{Z})^\times/H$ such that for any $d|m$, H is not the pre-image of a subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$.*

Definition 1.6.6. *If H is a primitive class group modulo m, then we say that K is a class field for H if the primes which ramify all divide m, and (with at most finitely many exceptions) the primes which split completely in $K/\mathbb{Q}$ are those in H.*

Then the Kronecker-Weber theorem actually tells us the following results:

1. Every abelian extension of $\mathbb{Q}$ is a class field for some class group.
2. For every class group there exists exactly one class field.
3. The Galois group of the class field is isomorphic to the class group.
4. An inclusion of class groups (by which we mean a that if we write each class group as equivalent to another one which is a quotient of $\mathbb{Z}/m\mathbb{Z}$ for some m then the groups we are taking the quotient by are contained in each other) corresponds to an inclusion of the corresponding class fields but reversing direction.

Kronecker generalized this notion of a class group and a class field beyond the case of the rationals. In order to do this we must rephrase these definitions in terms of ideals instead of elements. As with the case of defining Größencharakters this presents certain problems, since several different integers can generate the same ideal, but yet be different modulo m.

Let $\mathbb{Q}^{(m)}$ be the set of all fractional ideals in $\mathbb{Q}$ relatively prime to m (by relatively prime we mean that for each prime dividing (m) is 0). We want to mod out by something to get the group $(\mathbb{Z}/m\mathbb{Z})^\times$. The obvious candidate for this is to mod out by all fractional ideals of the form (a) where $a \equiv 1 \pmod{m}$. Unfortunately, since $(a) = (-a)$ this quotient is actually $(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$. We need some way of distinguishing between the positive and negative elements.

This is where the notion of infinite primes as developed by Takagi (who we shall meet a little later) comes in handy. An infinite prime of a field K is either a real embedding or a pair of complex embeddings. At first glance calling these embeddings "primes" seems ridiculous, but they can be thought of as generalizations of finite primes.

Definition 1.6.7. *If K is a field, we define an absolute value $|\cdot|$ on K to be a map from K to the nonnegative real numbers with the following properties:*

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$

Clearly each real embedding gives an absolute value by pulling back the real absolute value. Also each complex embedding gives an absolute value by pulling back the complex absolute value. But furthermore, if K is a number field for each prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ we get the so-called $\mathfrak{P}$-adic absolute value.

Definition 1.6.8. *Suppose $\mathfrak{P}$ is a prime ideal in $\mathcal{O}_K$. If a is in $\mathcal{O}_K$, we define $ord_{\mathfrak{P}}(a)$ to be the highest power of $\mathfrak{P}$ dividing a. Then we define the $\mathfrak{P}$-adic absolute value of an algebraic integer to be $|(a)|_{\mathfrak{P}} = N\mathfrak{P}^{-ord_{\mathfrak{P}}(a)}$. This can be extended to all of K by taking quotients. One can check that this is in fact an absolute value.*

In fact the only absolute values on K are the ones coming from the infinite primes or the finite primes. If we have an extension L/K, we say that an infinite prime of L lies over an infinite prime of K when they agree on K. Furthermore we can define the decomposition and inertia group of an extensions of infinite primes to be trivial unless we are looking at a complex prime sitting over a real prime in which case we take the subgroup of the Galois group generated by this complex conjugation.

For $\mathbb{Q}$ there is only one infinite prime. But this infinite prime will let us distinguish between positive numbers and negative numbers.

Definition 1.6.9. *If ρ is an infinite prime, then we say that $a \equiv 1 \pmod{\rho}$ if $\rho(a)$ is positive and ρ is real, or if ρ is complex.*

Now if we let ∞ be the infinite prime of $\mathbb{Q}$ and let $P^{m\infty}$ be the set of all ideals generated by elements which are congruent to 1 modulo m and modulo ∞, then $\mathbb{Q}^{(m)}/P^{m\infty}$ is actually $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

Definition 1.6.10. *A modulus $\mathfrak{m}$ is an abstract product of primes both infinite and finite of K, but where the real infinite primes only have multiplicity 0 or 1 and the complex infinite primes have multiplicity 0. Let $\mathfrak{m}_0$ denote the finite part, which is an ideal, and $\mathfrak{m}_\infty$ denote the infinite part. If a and b are non-zero elements of $\mathcal{O}_K$, then we say $a \equiv b \pmod{m}$ if $\frac{a}{b} \equiv 1 \pmod{\mathfrak{m}_0}$ and $\frac{a}{b} \equiv 1 \pmod{\rho}_\infty$ for each infinite prime dividing $\mathfrak{m}_\infty$.*

Definition 1.6.11. *If $\mathfrak{m}$ is a modulus of K, then we let $I_K^{\mathfrak{m}}$ be the group of all fractional ideals relatively prime to $\mathfrak{m}_0$. $I_K = I_K^{(1)}$ is the group of all fractional ideals.*

Definition 1.6.12. *If $\mathfrak{m}$ is a modulus for some field K, then we define the ray class $P_K^{\mathfrak{m}}$ to be set of all fractional principal ideals which are generated by elements congruent to 1 modulo $\mathfrak{m}$.*

Definition 1.6.13. *A class group for a modulo $\mathfrak{m}$ is a quotient of the form $(I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}})/H$. Two class groups modulo different $\mathfrak{m}$ are said to be equivalent if the sets of primes ideals in the pre-image in I_K of the respective subgroups H agree with only finitely many exceptions.*

Notice that if $m = (1)$ then the class groups are precisely the subgroups of the ideal class group.

Proposition 1.6.14. *The ray class group $(I_K^{\mathfrak{m}}/P_K)$ is finite.*

Proof. For a proof see [**J**, Chapter IV, Cor. 1.6]. □

Definition 1.6.15. *If $(I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}})/H$ is a class group, then we say that L is a class field for this group if all of the primes which ramify in L are contained in $\mathfrak{m}$ and (with at most finitely many exceptions) the primes which split completely are exactly those in $HP_K^{\mathfrak{m}}$.*

Weber stated the following main results of class field theory (in the special cases of cyclotomic fields and quadratic imaginary fields, he did not know that all of them held generally, and several of these he did not state so precisely):

Conjecture 1.6.16.

1. *The completeness theorem: Every abelian extension is a class field.*
2. *The existence theorem: For every class group there exists some class field.*
3. *The uniqueness theorem: The class field given in (2) is unique up to equivalence.*
4. *The "first" (or second depending on what approach you are using) fundamental inequality of class field theory. If we have some field extension L/K and any modulus $\mathfrak{m}$ of K then we have the following inequality, then*

$$[I_K^{\mathfrak{m}} : N_{K/k}(I_L^{\mathfrak{m}})P_K^{\mathfrak{m}}] = h \leq n = (L : K).$$

5. *The fundamental equality: If $\mathfrak{m}$ contains all the primes which ramify in L/K, then equality actually holds in (4).*

6. *The isomorphy theorem: The Galois group of a class field is isomorphic to the class group.*

7. *The ordering theorem: The correspondence between class groups and class fields preserves order in the sense that if $\mathfrak{m}'|\mathfrak{m}$ and if H is a subset of H' (consider as subsets of I_K), then the class field of $(I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}})/H$ contains the class field of $(I_K^{\mathfrak{m}'}/P_K^{\mathfrak{m}'})/H'$.*

First we should pause for a moment to notice how remarkable the completeness theorem actually is. As we noted above in the integer case the units can make the class groups smaller than we might expect them to be. The addition of primes at infinity was enough to eliminate this problem in the integers, but since we have no condition involving the infinite primes if we are in a purely imaginary field, thus the units will actually make the class group much smaller than we might expect.

In particular consider $K = \mathbb{Q}(i)$. As we have seen before its ring of integers is $\mathbb{Z}[i]$ which is a principal ideal domain. The units are ± 1 and $\pm i$. Now consider the prime $(1+2i)$. $(\mathbb{Z}[i]/(1+2i))^\times$ is a cyclic group with four elements, the equivalence classes of ± 1 and $\pm i$. But since the class group is defined in terms of ideals $I_K^{(1+2i)}/P_K^{(1+2i)}$ kills not only the ideals generated by things congruent to 1 modulo $(1+2i)$ it also kills those things who have a unit multiple congruent to 1 modulo $(1+2i)$. Therefore this class group is actually trivial!

By the completeness theorem this means that there are no non-trivial abelian extensions L/K which ramify only at the prime $(1+2i)$. In fact if we sit down and try to construct such a field we will inevitably run into problems. For example if we look at $K(\sqrt{1+2i})$ this will ramify at $1+2i$. However, as we will show in Proposition 2.7.19, the prime $(1+i)$ also ramifies in this extension.

Weber proved Conjecture 1.6.16 parts 3, 4, and 7 by using analytic methods drawn from Dirichlet's proof about primes in arithmetic progressions and the Frobenius density theorem. We'll illustrate how this is done in the most difficult of these cases, namely the first fundamental inequality of class field theory. To see the meaning of this result notice that the left hand side is what the class group would be if L were the class field of something (to show it actually is the corresponding class field we also need that all of the primes in $P_K^{\mathfrak{m}}$ are actually in $N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})$), and the right hand side is the size of the Galois group that we hope this class group is isomorphic to.

1.6.5 Generalized Dirichlet L-series

Before giving a proof of the first fundamental inequality we need to define some new L-functions.

Definition 1.6.17. *A generalized Dirichlet character modulo a modulus $\mathfrak{m}$ is a function on I_K which agrees with an abelian group character of a ray class group $I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ (and which is 0 exactly on things not relatively prime to $\mathfrak{m}$).*

It is easy to see that such characters are exactly the Hecke Größencharakter which have all the q_ℓ and q_j' zero, the p_j' all 0 (remember these are the components corresponding to complex primes), and the p_ℓ zero for the real primes which do not divide $\mathfrak{m}$. (It should be noted that Hecke defined his Größencharakter after the definition of class fields, so historically we should think of Hecke's definition as a generalization of this notion of a Dirichlet character and not that the Dirichlet characters are special cases.) Furthermore, one can see that these are the Hecke Größencharakter of finite order. Thus for each of these generalized Dirichlet characters we have a Hecke L-series. From our theorem on Hecke L-functions these are all analytically continuable and satisfy a functional equation. Before stating this special case of Hecke's functional equation we need a few definitions.

Definition 1.6.18. *If χ is a generalized Dirichlet character modulo some modulus $\mathfrak{m}$ for some field K, then we define its conductor $\mathfrak{f}(\chi)$ to be the smallest modulus such that χ factors through $I_K^{\mathfrak{f}}/P_K^{\mathfrak{f}}$.*

The fact that such a conductor exists again comes from constructing it as the greatest common divisor of all possibilities. Notice that here the conductor is a modulus, this agrees with our former definition in the sense that the finite part $\mathfrak{f}_0$ agrees with our old definition of a conductor.

At times it will be useful to think of the conductor in a different way.

Definition 1.6.19. *If L/K is class field, then its conductor $\mathfrak{f}_{L/K}$ is the greatest common divisor of all modulii $\mathfrak{m}$ such that L/K is a class field for some class group modulo $\mathfrak{m}$. That is to say, the conductor is the smallest modulus such that every prime congruent to one modulo $\mathfrak{f}$ splits completely in L.*

If χ is a primitive character of a class field L/K it is easy to see that its conductor is the same as the conductor of the field extension. Furthermore if χ is not a primitive character and has kernel $N \subset G$ (G being the class group for L/K, then if N is the class group for some extension M/K the conductor of χ is the conductor of M/K.

Definition 1.6.20. *Suppose χ is generalized Dirichlet character with conductor $\mathfrak{f}$ and ρ is an infinite prime of a field K. Then we define the local factor of the L-series at ρ, written $L_\rho(s,\chi)$, as follows.*

$$L_\rho(s,\chi) = \begin{cases} \Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) & \text{If } \rho \text{ is a real prime not dividing } \mathfrak{f} \\ \Gamma_{\mathbb{R}}(s+1) = \pi^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right) & \text{If } \rho \text{ is a real prime dividing } \mathfrak{f} \\ \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s) & \text{If } \rho \text{ is a complex prime} \end{cases}.$$

Now Theorem 1.4.25 can be rephrased as follows:

Theorem 1.6.21. *If χ is a generalized Dirichlet character modulo $\mathfrak{m}$ for a field K, then the completed abelian L-function,*

$$\Lambda(\chi,s) = (|\mathfrak{d}_{K/\mathbb{Q}}|N_{K/\mathbb{Q}}\mathfrak{f}(\chi)_0)^{\frac{s}{2}} \prod_\rho L_\rho(s,\chi) \prod_{\mathfrak{p}\nmid\mathfrak{f}} \frac{1}{1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}},$$

(where ρ ranges over all infinite primes) can be analytically completed to a holomorphic function (unless χ is trivial in which case it is meromorphic with poles at 1 and 0) with the functional equation $\Lambda(\chi,s) = \epsilon(\chi)\Lambda(\bar{\chi}, 1-s)$ where $|\epsilon(\chi)| = 1$.

Proof. We have simply restated Theorem 1.4.25 in this special case. □

1.6.6 A proof of the First Fundamental Inequality

Theorem 1.6.22 (The "first" fundamental inequality of class field theory). *If we have some field extension K/k and any modulus $\mathfrak{m}$ then we have the following inequality, then*

$$[I_k^{\mathfrak{m}} : N_{K/k}(I_K^{\mathfrak{m}})i(k_{\mathfrak{m},1})] = h \leq n = (K:k).$$

Proof. (Following [**J**, Chapter IV, Thms. 5.6. and 4.7.])

We compute the Dirichlet densities of $S = N_{K/k}(\mathbf{I}_K^{\mathfrak{m}})$ and $S' = N_{K/k}(\mathbf{I}_K^{\mathfrak{m}})P_K^{\mathfrak{m}}$. Clearly $\delta(S) \leq \delta(S')$. Except for a set of density 0, S is the set of primes which split completely in K, so by the Frobenius Density Theorem (again just the easy base case), $\delta(S) = 1/|G| = 1/(K:k)$.

Next we consider $\delta(S')$. Let χ be a generalized Dirichlet character of $I_k^{\mathfrak{m}}/N_{K/k}(I_K^{\mathfrak{m}})P_K^{\mathfrak{m}}$, that is to say a generalized Dirichlet character modulo $\mathfrak{m}$ which is trivial on $N_{K/k}(I_K^{\mathfrak{m}})$. By Euler factorization,

$$\log L(s,\chi) = \sum_{\mathfrak{p}\in\mathbf{I}^{\mathfrak{m}}} \chi(\mathfrak{p})N(\mathfrak{p})^{-s} + O(1).$$

By the orthogonality relations for abelian group characters, for any $\mathfrak{p}$, $\sum_\chi \chi(\mathfrak{p}) = 0$ unless $\mathfrak{p} \in S'$ in which case it is h. Therefore, we can sum the above expression for $\log L(s,\chi)$ over all χ to get,

$$\sum_{\mathfrak{p}\in S'} hN\mathfrak{p}^{-s} = \left(\sum_{\chi\neq\chi_0} \log L(s,\chi)\right) - \log(s-1) + O(1),$$

where to get the second term we used the fact that the set of primes relatively prime to $\mathfrak{m}$ obviously has density 1.

By definition, $\sum_{\mathfrak{p}\in S'} N(\mathfrak{p}^{-s}) = -\delta(S')\log(s-1) + O(1)$, so we can arrange terms in the above expression to get,

$$0 = -(1 - h\delta(S'))\log(s-1) + \sum_{\chi\neq\chi_0} \log L(s,\chi) + O(1).$$

Now, if $L(1,\chi) \neq 0$ the terms in the sum are all bounded as s goes to 1, otherwise they all go to negative infinity. In either case we get that, $0 \leq 1 - h\delta(S')$, so $\delta(S') \leq 1/h$. (Notice that equality holds here exactly when all the nonprincipal $L(1,\chi) \neq 0$.)

Combining these two computations, we get, $1/(K:k) = \delta(S) \leq \delta(S') \leq 1/h$. Therefore, $h \leq (k:k)$. □

(As an interesting side note, notice that by the Kronecker-Weber theorem we have $\delta(S') = 1/h$ in the above theorem. Therefore, we can conclude that the ordinary Dirichlet L-series have $L(1,\chi) \neq 0$.)

1.6.7 Hilbert, Furtwangler, and Takagi

David Hilbert lived from 1862 until 1943 and was the dominant mathematical figure at the turn of the century. He did important work in algebraic forms, algebraic number theory, foundations of geometry, analysis, theoretical physics and the foundations of mathematics. He is perhaps most famous for his 23 questions which he proposed before the Second International Congress of Mathematicians at Paris in 1900. Two of these questions were related to class field theory:

Hilbert's Problem 9: "Proof of the most general law of reciprocity in any number field."

Hilbert's Problem 12: "Extension of Kronecker's theorem on Abelian fields to any algebraic realm of rationality."

Problem 12 is essentially the question which class field theory was invented to answer. Hilbert made several contributions to this theory. He gave a new proof of Kronecker-Weber theorem which lead him to suggest the following program for generalizing this to other fields: first describe the maximal unramified abelian extension of any number field, and second, find a good collection of abelian extensions which can add in all the ramified parts. This lead him to begin studying the Hilbert class field, or the maximal unramified extension, which is also the class field of the full ideal class group. He proved the existence of the Hilbert class field in the special case of degree 2 extensions with class number 2. The methods that he used for this were eventually modified to give more general existence theorems. He also conjectured that all ideals become principal in the Hilbert class field.

Problem 9 on the surface bears no relation to class field theory, but Hilbert's other great contribution to class field theory was to realize the connection between class field theory and reciprocity laws. The connection between quadratic reciprocity and certain abelian extensions goes all the way back to Gauss's 6th proof using Gauss sums and hence the embedding of the quadratic field into a cyclotomic field. The following proof makes this connection even more apparent:

Theorem 1.6.23 (Quadratic Reciprocity). *If p and q are two positive primes and $q^* = \left(\frac{-1}{q}\right) q$, then*

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right).$$

Proof. Consider two distinct odd primes p and q. By Kronecker-Weber theorem and a calculation of discriminants (or by Gauss sums), we see that $\mathbb{Q} \subset \mathbb{Q}(\sqrt{q^*}) \subset \mathbb{Q}(\zeta_q)$ where $q^* = \left(\frac{-1}{q}\right) q$. Now look at the Frobenius substitution of p in each of those fields. In the quadratic field it is obviously $\left(\frac{q^*}{p}\right)$ and in the cyclotomic field it is obviously the map that sends $\zeta_q \mapsto \zeta_q^p$. When we restrict this second map to the quadratic field we notice that the map on Galois groups is the only non-trivial map from $(\mathbb{Z}/q\mathbb{Z})^\times \to \{\pm 1\}$ namely the one that takes squares to 1 and non-squares to -1. So the restriction of the Frobenius substitution of p is $\left(\frac{p}{q}\right)$. The fact that the Frobenius substitution behaves well in extensions implies that $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$. □

Thus we have seen that quadratic reciprocity can be realized as a corollary of Kronecker-Weber theorem, which in turn is equivalent to class field theory for $\mathbb{Q}$. Hilbert took this connection further and defined the Hilbert norm residue symbol and proved a reciprocity law for that symbol.

Furtwangler generalized Hilbert's approach to the general power reciprocity law which he proved in varying generality between 1902 and 1928. Not only did he prove the general reciprocity law, he also gave a general proof of the existence of Hilbert class fields which was the first general result in class field theory since Weber's proof of the first fundamental inequality. His existence proof provided many of the tools which would later be applied to the general existence theorem.

In 1920, a full 30 years since Weber first discussed the main results of class field theory, there was still very little in the way of proofs. The existence theorem had only been proven for the case of Hilbert class fields and other than in a few very special cases there was no progress on the completeness theorem, and outside of the Hilbert class field case there was no progress on the isomorphy theorem. Then in 1920 Takagi proved them all.

At this point we take a slight historical tangent since the appearance of Takagi is remarkably interesting. Teiji Takagi was born in 1875 near Gifu, Japan and died in 1960 (additional biographical information taken from *On the Life and Works of Teiji Takagi* [**T**, Appendix]). Takagi was the first Japanese mathematician of note. Modern mathematics was introduced to Japan via military science, in particular the use of European textbooks in Nagasaki Naval Academy. The adoption of European methods was hastened by the existence of an abstract Japanese form of mathematics called wasan (unlike the more practical computational mathematics which dominated China) and the strong push in Meiji Japan to match the military prowess of the European powers. In 1877 the University of Tokyo and the Tokyo Mathematical Society were founded, events which heralded the beginning of a strong modern mathematical tradition in Japan. The University had 5 professors in the Department of Mathematics-Physics-Astronomy, four of whom were foreigners and one was Japanese but educated in England (it is this professor, Dairoku Kikuchi who was the only Professor of Mathematics).

In the first few years the University of Tokyo was based on the English model, but in 1887 Rikitaro Fujisawa a former student at the University of Tokyo returned from graduate studies in Germany and became the second professor of mathematics at the University of Tokyo. He brought with him the more rigorous research based approach of the German University system. Fujisawa had studied under Kronecker, Weierstrass, and Kummer and thus had a much stronger understanding of modern mathematics than any prior Japanese mathematician. Although Fujisawa was the first modern mathematician in Japan, it was his student Takagi who was the first to make a significant contribution. His thesis proving Kronecker's Jugendtraum in the special case of $\mathbb{Q}(i)$ (see [**S-T**] for a proof of this case) published in 1903 was the first major result proved by a Japanese mathematician. The progression from the opening of Japan in 1853 until Takagi in 1903 is shockingly rapid. (Although perhaps this development is a bit less shocking if we remember that in this same amount of time Japan went from having no navy whatsoever to sinking the entire Russian fleet. On the other hand it is still worth noting because naval prowess does not always correspond to mathematical ability, for example, the Viking's were not famous for their number theorists.) For more information of mathematics in Meiji Japan see Sasaki's article in [**C-M-D**].

Takagi worked on the main results of class field theory in Japan during the war in seclusion from his German colleagues and was so shocked by the generality of his results that he doubted there validity for quite some time.

Takagi's proofs of the main theorems are obviously beyond the scope of this paper. His methods for proving the fundamental equality have been described both as a complicated generalization of Gauss's genus theory and as an early form of cohomology. The basic method that Takagi used in proving the main results of class field theory was to restrict to the cyclic case where one could prove things just by counting, and then gluing these results together to get the general results.

After Takagi there were three remaining open questions in class field theory, Hilbert's principal ideal theorem, Frobenius's conjecture concerning the density of primes with a certain Frobenius automorphism, and generalizing the reciprocity theorems to general abelian extensions.

Although Takagi had already published his important class field theory paper in 1920, his results were not yet well known partly because of disruptions caused by the war. In particular Takagi presented his main papers in 1920 in Strasborg which changed hands after the war, and so the German mathematicians were not allowed to attend. It was only when Siegel persuaded Artin to read these papers in 1922 that

Takagi's results became generally known. The results of Artin's investigations prompted by his reading of Takagi's paper is the subject of the second chapter and so the rest of the story of class field theory will have to wait until then.

Chapter 2

Artin L-functions

2.1 Artin L-functions, Their Definition, and Their Most Basic Properties

2.1.1 Introduction

At long last, we have reached the point in our story where our lead actor takes the stage. Emil Artin was born in 1898 in Vienna and died in 1962. His university studies were interrupted when he was called into military service from 1916 to 1919. Fortunately for mathematics, he survived. After the war he studied under Herglotz and received his doctorate in 1921. Artin became famous, not only for his early work in class field theory, but also for his important conjectures concerning the Riemann hypothesis for algebraic curves, his involvement in later developments in class field theory and analytic number theory, and his work in abstract algebra.

His paper *Über eine neue Art von L-Reihen* [**Ar**, p. 105] was published in 1923, and was only the second paper he had published. At the time, Artin was trying to generalize the results of Hecke and Weber's that showed if L/K is a class field, then $\frac{\zeta_L}{\zeta_K}$ is a holomorphic function. This says something rather remarkable about the distribution of the zeroes of these ζ-functions. Weber had given a decomposition of the ζ-function of the larger field into a product of L-functions of characters of the class group. By Hecke's results these L-functions could be holomorphically continued to the entire complex plane. Since Artin was aware of Takagi's results, he knew that all abelian extensions were class fields. Thus Weber's result holds for all Abelian extensions. Artin wanted to generalize this result to non-abelian extensions. In order to do this, he needed to define a completely new kind of L-function which made sense for non-abelian extensions. In his investigations, he not only proved many important basic results about L-functions, he also conjectured Artin Reciprocity (a result which subsumed all the previous reciprocity theorems and gave class field theory a much nicer formulation), and he laid out a program for generalizing facts about abelian L-functions to his new Artin L-functions. In this section, we concentrate on the definition and most basic properties of these Artin L-functions.

2.1.2 Factoring the ζ-function of an Abelian Extension

Before we can understand Artin's definitions, it is important to understand the result of Weber's which he was trying to generalize.

Theorem 2.1.1 (Weber). *Suppose L/K is a class field for the class group $G = (I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}})/H$. Let G^* denote the group of abelian characters of G. Then,*

$$\zeta_L(s) = \prod_{\chi \in G^*} L(s,\chi) = \zeta_K(s) \prod_{\chi \neq \chi_0} L(s,\chi),$$

(where χ_0 is the trivial character). In particular, by Theorem 1.6.21, we have that $\frac{\zeta_L(s)}{\zeta_K(s)}$ is a holomorphic function on the entire complex plane.

Proof. This theorem was first proved by Weber in [**W2**, Vol. 3 §163]. We check this equality prime by prime in the Euler factorization. Suppose $\mathfrak{p}$ is unramified. If $\mathfrak{p}$ is a prime of K, then we want to show:

$$\prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1 - N\mathfrak{P}} = \prod_{\chi} \frac{1}{1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s}}. \tag{2.1.1}$$

Since $N\mathfrak{P} = N\mathfrak{p}^{f_\mathfrak{p}}$, the left hand side of Equation 2.1.1 is

$$\left(\frac{1}{1 - N\mathfrak{p}^{f_\mathfrak{p}}}\right)^{g_\mathfrak{p}} = \left(\frac{1}{\prod_{\ell=1}^{f_\mathfrak{p}} (1 - \zeta_{f_\mathfrak{p}}^{\ell} N\mathfrak{p})}\right)^{g_\mathfrak{p}}.$$

On the other hand, if $\mathfrak{p}$ has order j in the class group, then it is easy to see that the different characters will send it to j-th roots of unity. Furthermore each j-th root of unity will appear equally

often. (To prove these claims, decompose G into a product of cyclic groups, and classify the characters of a cyclic group.) Therefore, if $n = |G|$, then the right hand side of Equation 2.1.1 is

$$\left(\frac{1}{\prod_{\ell=1}^{j} (1 - \zeta_j^{\ell} N\mathfrak{p})} \right)^{\frac{n}{j}}.$$

Thus we have reduced this result to showing that the order of $\mathfrak{p}$ in the class group equals $f_{\mathfrak{p}}$. But, both of these numbers are the smallest power of $\mathfrak{p}$ which can be written as a norm down from L. Therefore, they must be equal.

If $\mathfrak{p}$ is ramified, then this takes a bit more work. The point is that now we are trying to show,

$$\prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1 - N\mathfrak{P}} = \prod_{\chi} \frac{1}{1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s}}, \tag{2.1.2}$$

where χ does not range over all characters of the class group G, but rather over all characters of the group $G' = (I_K^{\mathfrak{d}}/P_K^{\mathfrak{d}})/H'$ (where $\mathfrak{d}$ is the part of $\mathfrak{m}$ relatively prime to $\mathfrak{p}$). This group is the class group for some field M sitting between L and K. We can then use the above result for unramified primes applied to the extension M/K to get the needed result. □

Furthermore, Hecke showed (in the simpler case that K is purely imaginary) that this equality actually held for the completed L-functions [**He**, pp. 172-177].

Theorem 2.1.2 (Hecke). *Suppose L/K is a class field for the class group $G = (I_K^{\mathfrak{m}}/P_K^{\mathfrak{m}})/H$. Let G^* denote the group of abelian characters of G. Then, for Hecke's extended L-functions and ζ-functions, we still have*

$$\zeta_L(s) = \prod_{\chi \in G^*} L(s, \chi) = \zeta_K(s) \prod_{\chi \neq \chi_0} L(s, \chi),$$

(where χ_0 is the trivial character).

Proof. First we check this formula for the infinite primes. We have three different cases, either ρ is a real prime of K and all the primes over it in L are also real, ρ is a complex prime of K (and hence extends to complex primes in L), or ρ is a real prime of K which extends to a complex primes of L. The first two cases are trivial since on the left hand side we get n copies of $\Gamma_{\mathbb{R}}(s)$ or $\Gamma_{\mathbb{C}}(s)$ respectively (one for each prime sitting above ρ), and, on the right-hand side, since the prime never divides the conductor of any of the characters, we also get n copies of $\Gamma_{\mathbb{R}}(s)$ or $\Gamma_{\mathbb{C}}(s)$ respectively (one for each character).

The remaining case is more difficult. If ρ is a real prime but the primes sitting over it are complex, then ρ divides the conductor of the extension. It will not, however, divide the conductor of each of the characters. In fact, if $\mathfrak{m}'\rho = \mathfrak{m}$, then $(I_K^{\mathfrak{m}'}/P_K^{\mathfrak{m}'})/H)$ is a subgroup of G of index 2. Thus, exactly half of the characters will not have ρ in their conductor. Therefore, the right hand side is $(\Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1))^{\frac{n}{2}}$, while the left hand side is $\Gamma_{\mathbb{C}}(s)^{\frac{n}{2}}$ (because conjugate embeddings only count as one prime). Thus, we have reduced to showing that $\Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = \Gamma_{\mathbb{C}}(s)$. This is just Equation 1.3.3.

Now we know that the formula holds for the local factors for the finite and infinite primes. For the exponential factor, we can actually pull equality out of thin air. Notice that both sides of the equation with the infinite prime factors included have a unique analytic continuation to the entire plane. Furthermore, by the functional equation, the ratio of the values of each side at 1 and their value at 0 tells you, up to a factor of size 1, the exponential factor. Therefore, by the uniqueness of analytic continuation, the exponential factors must be equal up to a factor of size 1. However, for real s, the exponential factor on both sides is strictly positive. Therefore, the exponential factors must be genuinely equal. □

2.1.3 Defining the Artin L-function

Artin was fascinated by these L-function relationships and his first paper [**Ar**, pp. 95-104] explored other more complicated relationships between L-functions. For example, he proved that if $\mathrm{Gal}(L/K) = S_3$,

and k is the subfield fixed by one of the subgroups of size 2 and F is the subfield fixed by the normal subgroup A_3, then

$$\zeta_L \zeta_K^2 = \zeta_F \zeta_k^2.$$

This formula implies that $\frac{\zeta_L}{\zeta_K}$ is a product of abelian L-functions and is therefore holomorphic. Although Artin managed to prove by hand a lot of very surprising relationships like this one, he was unable to find a general explanation for the origin of these relationships. Artin surmised that generalizing Weber's result to non-abelian extensions would allow him to classify these formulas relating ζ-functions and L-functions.

To have any hope of being able to define non-abelian L-functions, Artin needed to translate the characters of a class group into some other form which did not have to do with the class group at all. After reading Takagi, Artin realized that Takagi's proof of the isomorphy theorem gave him exactly the tool he needed. Since the class group is isomorphic to the Galois group, one should be able to attach the L-series to characters of the Galois group. This reformulation would allow him to generalize the notion of L-series to the non-abelian case.

Suppose χ is the character of some representation V of a (non-abelian) Galois group G. We want to define an L-series as a product of Euler factors for each prime. In order to do so, we need some way of identifying to every prime an element of the Galois group. In the unramified case, this is exactly what the Frobenius does. This suggested to Artin the following definition:

Definition 2.1.3. *Suppose K/L is a Galois extension of number fields with Galois group G, and suppose (V, ρ) is a representation of G, then we define the Artin L-function to be:*

$$L(s, V; L/K) = \prod_{\mathfrak{p}} \det(Id - N\mathfrak{p}^{-s} \rho(\varphi_{\mathfrak{P}/\mathfrak{p}}))^{-1},$$

where the product is taken over all unramified primes in K, and where $\mathfrak{P}$ is any prime over $\mathfrak{p}$. Notice that this definition actually makes sense, because choosing a different prime $\mathfrak{P}$ over $\mathfrak{p}$ changes the Frobenius by conjugation which does not change the determinant. (Later we will change this definition by adding terms corresponding to the ramified primes.)

For other sources on the definition of the Artin L-function and its basic properties, see Artin's article in the appendix, Martinet's article [**Fröh**, pp. 1-87], and [**N**, Chapter VII, §10].

Since conjugating $\rho(\varphi_{\mathfrak{P}/\mathfrak{p}})$ by another matrix in the above definition does not change the value of the L-function (because the determinant does not depend on choice of basis), the above definition only depends on V up to isomorphism, as we would hope. Furthermore, the above product converges so long as $s > 1$ because it is bounded by $\zeta_K^{\dim V}$. Lastly, we notice that if we multiply out the right hand side of this definition, the Artin L-series is a Dirichlet series.

As we saw in the last section, it is often useful to consider the L-function term by term. Thus, we define the local factor at a prime $\mathfrak{p}$ of the L-series to be

Definition 2.1.4. *If $\mathfrak{p}$ is unramified, let*

$$L_{\mathfrak{p}}(s, V) = \det(Id - N\mathfrak{p}^{-s} \rho(\varphi_{\mathfrak{P}/\mathfrak{p}}))^{-1}.$$

2.1.4 Additivity and the Artin L-function of a (Generalized) Character

Since the Artin L-function only depends on V up to isomorphism, it only depends on the character χ_V. Artin's first goal was to find an expression for the L-function in terms of the character. In order to do this, Artin took the logarithm of the L-function and expanded each term using the Taylor expansion.

That is to say,

$$\log L(s, V; L/K) = \sum_{\mathfrak{p}} - \log \det(\mathrm{Id} - N\mathfrak{p}^{-s} \rho(\varphi_{\mathfrak{p}})).$$

Now for each term in this sum we can diagonalize $\rho(\varphi_{\mathfrak{p}})$, say it has eigenvalues $\lambda_1, \ldots, \lambda_n$. Therefore,

$$\log \det(\mathrm{Id} - N\mathfrak{p}^{-s} \rho(\varphi_{\mathfrak{p}})) = \log \prod_{i=1}^{n} (1 - N\mathfrak{p}^{-s} \lambda_i) = \sum_{i=1}^{n} \log(1 - N\mathfrak{p}^{-s} \lambda_i).$$

By the Taylor expansion of the logarithm and switching the order of summation (which is legitimate because one of the sums is finite),

$$\sum_{i=1}^{n} \log(1 - N\mathfrak{p}^{-s}\lambda_i) = \sum_{i=1}^{n} \sum_{\ell=1}^{\infty} \frac{\lambda_i^\ell}{\ell} N\mathfrak{p}^{-s\ell} = \sum_{\ell=1}^{\infty} \frac{\chi_V(\varphi_\mathfrak{p}^\ell)}{\ell} N\mathfrak{p}^{-s\ell}.$$

Plugging this result into the formula for $\log L(s, V; L/K)$, we get

$$\log L(s, V; L/K) = -\sum_{\mathfrak{p}} \sum_{\ell=1}^{\infty} \frac{\chi_V(\varphi_\mathfrak{p}^\ell)}{\ell} N\mathfrak{p}^{-s\ell}.$$

Thus the original definition of the Artin L-function attached to a representation agrees with the following definition of the Artin L-function attached to a class function.

Definition 2.1.5. *Suppose L/K is Galois extension with Galois group G, and ψ is a class function of G. Then, let*

$$L(s, \psi; L/K) = \exp\left(-\sum_{\mathfrak{p}} \sum_{\ell=1}^{\infty} \frac{\psi(\varphi_\mathfrak{p}^\ell)}{\ell} N\mathfrak{p}^{-s\ell} \right).$$

Theorem 2.1.6 (Artin).

$$L(s, \psi_1 + \psi_2; L/K) = L(s, \psi_1; L/K) L(s, \psi_2; L/K).$$

Proof. This follows immediately from our definition, since the logarithm of the L-series is clearly additive. □

In particular, since the characters of irreducible representations are a basis for the space of all class functions, the Artin L-series attached to any class function ψ, can be written in the from

$$L(s, \psi; L/K) = \prod_{\chi} L(s, \chi; L/K)^{r_i},$$

for some complex numbers r_i (where the sum is over all characters of irreducible representations).

2.1.5 The L-series Attached to the Pullback

Suppose ψ is a class function on G which has some nontrivial kernel N. Then, ψ is also a class function on the group G/N (which is the Galois group of M/K for $M = L^N$). In this case, we can consider two different L-functions assigned to ψ, namely $L(s, \psi; L/K)$ and $L(s, \psi; M/K)$. One would hope that these two functions would be equal. In fact, if we look at our definition it is clear that these definitions do agree with one small problem: in the one case we are summing over all primes which are unramified in L/K, while in the other case we are summing over all primes which are unramified in M/K. Thus, these two answers differ by finitely many Euler factors.

This is reminiscent of a similar problem for abelian L-functions. Namely, if we had a non-primitive character the obvious definition differed from the definition which we got by considering the associated primitive character modulo the conductor by finitely many factors.

Although we shall later see that we can add Euler factors for the ramified primes into our definition in such a way that this problem disappears, for the time being we will use the symbol $\equiv$ when applied to Artin L-series to mean "equal up to finitely many primes."

2.2 The Artin L-function of an Induced Representation

2.2.1 Hecke's Formula in Terms of Artin L-functions

As we recall, Artin's original goal in introducing these L-functions is to generalize Hecke's formula for $\frac{\zeta_L}{\zeta_K}$. Both of these ζ-functions are Artin L-series; $\zeta_L = L(s, \chi_0, L/L)$ and $\zeta_K(s, \chi_0, L/K)$, where χ_0 is the trivial character. In order to write ζ_L as a product of Artin L-series, we need to rewrite $L(s, \chi_0, L/L)$ as an L-function for L/K. This is a special case of the more general problem of taking the L-function of a character of a subgroup and rewriting it as the L-function of a character of the whole group. There is really only one logical way to build up such a character, namely, by induction. Thus, Artin's next step was to prove, if we have number fields $K \subset M \subset L$ with $\mathrm{Gal}(L/K) = G$ and $\mathrm{Gal}(L/M) = H$ (H can be identified with subgroup of G), then, for χ is any character of H,

$$L(s, \chi; L/M) \equiv L(s, \mathrm{Ind}_H^G \chi; L/K).$$

In particular, we apply this theorem to $M = L$ and $\chi = \chi_0$. By Frobenius reciprocity, $\mathrm{Ind}_H^G \chi_0 = \sum_\chi \chi(0)\chi$, where the sum is over all irreducible characters. Thus,

$$\frac{\zeta_K(s)}{\zeta_k(s)} \equiv \prod_{\chi \neq \chi_0} L(s, \chi; L/K).$$

2.2.2 A Proof of the Induction Formula

Artin proved this induction formula by direct computation. The reader is encouraged to look at this proof in the appendix (Theorem A.3.1). It is remarkable how many questions are first resolved by brute force long before they're conquered in a clever way (Gauss's first proof of quadratic reciprocity by induction is a particularly shocking example). However, much of Artin's calculations are only a special case of Mackey's Theorem. Thus, rather than repeating his proof, we will rephrase it in terms of Mackey's Theorem to elucidate what is actually going on behind Artin's proof.

Theorem 2.2.1 (Artin). *Suppose we have number fields $K \subset M \subset L$ with $Gal(L/K) = G$ and $Gal(L/M) = H$. H can be identified with subgroup of G. Then, if χ is any class function on H, then*

$$L(s, \chi; L/M) \equiv L(s, Ind_H^G \chi; L/K).$$

Proof. By additivity it is enough to show this formula for characters. So consider some representation W of H with character χ.

In order to simplify notation if (V, ρ) is any representation then we will use the notation $\det(1 - gt; V)$ to denote $\det(1 - \rho(g)t)$.

As one might expect, considering we only have equality up to finitely many primes, we will prove this equality prime by prime. To write down the local factors, we must first choose some notation. Fix $\mathfrak{p}$ some unramified finite prime of K. In M this will factor as $\mathfrak{p} = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_g$. For each i, choose some $\mathfrak{P}_i \in L$ sitting over $\mathfrak{q}_i$. Let G_i denote the decomposition group of $\mathfrak{P}_i/\mathfrak{p}$. Now take $\varphi \in G_1$ the Frobenius of $\mathfrak{P}_1/\mathfrak{p}$. Thus, by definition, the local factor at $\mathfrak{p}$ is

$$L_\mathfrak{p}(s, \mathrm{Ind}_H^G W; L/K) = \det\left(1 - \varphi N\mathfrak{p}^{-s}; \mathrm{Ind}_H^G W\right)^{-1}.$$

We would like to rewrite this local factor so that it will look like a product of the local factors at the $\mathfrak{q}_i$. First, we notice that the Frobenius actually lives in G_1. Therefore, in general we can replace $\mathrm{Ind}_H^G W$ with $\mathrm{Res}_{G_1}^G \mathrm{Ind}_H^G W$. In this case, this lets us rewrite our local factor as

$$L_\mathfrak{p}(s, \mathrm{Ind}_H^G W, L/K) = \det\left(1 - \varphi N\mathfrak{p}; \mathrm{Res}_{G_1}^G \mathrm{Ind}_H^G W\right)^{-1}.$$

At first glance, this seems to make the situation more complicated. However, Mackey's theorem is precisely what we need to simplify such a situation.

To apply this theorem we need a concrete description of $G_1\backslash G/H$. Recall that G acts transitively on the set of primes in L sitting over $\mathfrak{p}$. Thus, the cosets $G_i\backslash G$ are determined by the image of the right action $g^{-1}\mathfrak{P}_1$. But, the left action of H acts transitively on the primes in L over $\mathfrak{q}_1$. Therefore, the cosets $G_i\backslash G/H$ are determined by the image of $g^{-1}\mathfrak{q}_i$. Stated more concretely, suppose we take $\tau_i \in G$ such that $\tau_i^{-1}\mathfrak{q}_1 = \mathfrak{q}_i$, then $\{\tau_i\}$ is a set of representatives for the double cosets $G_i\backslash G/H$. (Here as always i ranges between 1 and g.) Furthermore, since the $\mathfrak{P}_i$ were chosen arbitrarily (as divisors of $\mathfrak{q}_i$), we can choose them so that $\tau_i^{-1}\mathfrak{P}_1 = \mathfrak{P}_i$.

Hence we can rewrite our local factor as

$$\begin{aligned} L_{\mathfrak{p}}(s, \mathrm{Ind}_H^G W, L/K) &= \det\left(1 - \varphi N\mathfrak{p}; \bigoplus_{i=1}^{g} \mathrm{Ind}_{G_1 \cap \tau_i H \tau_i^{-1}}^{G_1} \tau_i W\right)^{-1} \\ &= \prod_{i=1}^{g} \det\left(1 - \varphi N\mathfrak{p}; \mathrm{Ind}_{K \cap \tau_i H \tau_i^{-1}}^{G_1} \tau_i W\right)^{-1} \end{aligned}$$

Conjugating each term individually by τ_i^{-1} yields

$$\begin{aligned} L_{\mathfrak{p}}(s, \mathrm{Ind}_H^G W, L/K) &= \prod_{i=1}^{g} \det\left(1 - \tau_i^{-1}\varphi\tau_i N\mathfrak{p}; \mathrm{Ind}_{\tau_i^{-1} G_1 \tau_i \cap H}^{\tau_i^{-1} G_1 \tau_i} W\right)^{-1} \\ &= \prod_{i=1}^{g} \det\left(1 - \varphi_i N\mathfrak{p}; (\mathrm{Ind}_{H_i}^{G_i} W)\right)^{-1}. \end{aligned} \tag{2.2.1}$$

Thus we have reduced our general problem to verifying the equation

$$\det\left(1 - \varphi_i^{f_i} N\mathfrak{p}^{f_i}; W\right) = \det\left(1 - \varphi_i N\mathfrak{p}; \mathrm{Ind}_{H_i}^{G_i} W\right)$$

But, this is exactly the equality of local factors in the special case of the extension of decomposition fields $L^{G_i} \subseteq L^{H_i} \subseteq L$ (in this case $g = 1$). (It is important to note here that the Frobenii for this field extension are exactly the same as those at the same prime in the original field extension.)

Now we take $\mathfrak{P}_i$ is prime in L^{G_i} and is completely inert in the extension L/L^{G_i}. Therefore, the Frobenius generates the full Galois group G_i. This allows us to simply compute the right hand side of the equation. Choose some basis for W, and let A be the matrix for φ^{f_i} with respect to that basis. Then, since φ generates G_i, we have $\mathrm{Ind}_{H_i}^{G_i} W = W \oplus \varphi W \oplus \varphi^2 W \oplus \ldots \oplus \varphi^{n-1} W$. Therefore, φ^i times each element of our basis for W gives us a basis for $\mathrm{Ind}_H^G W$. With respect to this basis the matrix for φ is (taking I to be the appropriate identity matrix):

$$\begin{pmatrix} 0 & I & 0 & \ldots & 0 \\ 0 & 0 & I & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & I \\ A & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Now we know that the righthand side, $\det\left(1 - \varphi N\mathfrak{p}; \mathrm{Ind}_{H_i}^{G_i} W\right)$, becomes

$$\begin{vmatrix} I & -N\mathfrak{p}I & 0 & \ldots & 0 \\ 0 & I & -N\mathfrak{p}I & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -N\mathfrak{p}I \\ -A & 0 & 0 & \ldots & I \end{vmatrix} = \det(1 - \varphi^n N\mathfrak{p}^n; W).$$

To get the last equality take the first column multiply by $N\mathfrak{p}$ and add it to the second column, then multiply the second column by $N\mathfrak{p}$ and add to the third, etc.

This completes the proof of the special case, and hence the proof of the full theorem.

□

2.3 Artin Reciprocity

2.3.1 Statement of Artin Reciprocity

Thus far, we have skirted around the crucial issue of whether Artin's L-functions are actually generalizations of abelian L-functions or not? After all, Artin's goal was to explain the origin of certain relations between abelian L-functions. Suppose that χ is the character of a one-dimensional representation of an abelian group $G = \mathrm{Gal}(L/K)$, then the Artin L-series is

$$L(s,\chi) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\varphi_{\mathfrak{p}})}{N\mathfrak{p}^s}}.$$

The right hand side looks like the definition of an abelian L-function, so long as $\chi(\varphi_{\mathfrak{p}})$ agrees with some character of the class group. Suppose that all these characters of G actually agreed with some character of the class group. This would give us a concrete identification of elements of G with elements of the class group. In particular, Artin realized that we would have the following explicit form of the isomorphy theorem.

Definition 2.3.1. *If L/K is an abelian extension with conductor $\mathfrak{f}$ (here we are including the infinite part of the conductor), then we define the Artin map to be $\varphi_{L/K} : I_K^{\mathfrak{f}} \to Gal(L/K)$ given by $\varphi_{L/K}(\mathfrak{p}) = \varphi_{\mathfrak{p}}$ and extended by multiplicativity.*

Notice that the kernel of the reciprocity map contains precisely those prime ideals which are norms down from L.

Theorem 2.3.2 (Artin Reciprocity). *The Artin map, $\varphi_{L/K} : I_K^{\mathfrak{f}} \to Gal(L/K)$, is surjective and its kernel contains $P_K^{\mathfrak{f}}$. Thus, the Artin map gives an explicit isomorphism between the class group $(I_K^{\mathfrak{f}}/P_K^{\mathfrak{f}})/\ker\varphi_{L/K}$ and the Galois group $Gal(L/K)$.*

It may seem amazing to us in retrospect that in the decades between the conjecture of the isomorphy theorem and Artin's statement of his reciprocity theorem, no one had bothered to ask the question, "what exactly is this isomorphism." Takagi gave a proof of the result simply by reducing to the cyclic case and counting. The modern student of mathematics are conditioned to ask immediately when presented an isomorphism, "is it canonical?" But in the 19th century this was not yet considered a crucial question.

A proof of Artin reciprocity is well beyond the scope of this paper (see [**J**, Chapter V §5] or [**N**, Chapters VI §7]), however we can give a short proof of the first half of the claim (that the Artin map is surjective) using the Frobenius density theorem.

Proof. (Following [**J**, Chapter IV, Cor. 5.3] and taken directly from [**Sn**].) Given an element $\sigma \in \mathrm{Gal}(L/K)$, the division of σ consists of exactly those elements which generate $\langle\sigma\rangle$. So, by the Frobenius density theorem, there exist infinitely many primes not in $\mathfrak{m}$ whose Frobenius substitution generates $\langle\sigma\rangle$. So, there exists some $\mathfrak{P}$ sitting over $\mathfrak{p}$ with $\varphi_{L/K}(\mathfrak{P})$ a generator of $\langle\sigma\rangle$. Therefore, the image of the map contains every cyclic subgroup, and must be the entire group. □

2.3.2 Why is This a Reciprocity Theorem?

Certainly Artin reciprocity is enough to show that all the Artin L-series of irreducible characters for an abelian extension correspond (up to finitely many factors) to some abelian L-function. However, this theorem is important of its own right. In Artin's words, "In the case of a cyclic extension our theorem becomes the general reciprocity law (if k contains the appropriate root of unity), this agreement means that we must understand Theorem 2 as the formulation of the general reciprocity law in any field (also without unit root), even if the wording seems somewhat strange to us at first sight. " [Appendix, page 111.]

What exactly does Artin mean by this? Certainly at first site the wording of this looks nothing like a reciprocity law. However, this theorem can be rephrased as "The way a prime factors in an abelian extension is given by some modularity condition," where by "the way a prime factors" we mean what

its Frobenius is, and by "a modularity condition" we mean which coset of a particular subgroup of the ray class group modulo $\mathfrak{f}$.

In this guise the connection to reciprocity laws becomes apparent. By Kummer's theorem, whether p is a square modulo q is the same as asking how p factors in $\mathbb{Q}(\sqrt{q})$. Thus Quadratic reciprocity tells us exactly that the way a prime (p) factors in $Q(\sqrt{d})$ is given by a modularity condition on p modulo $4d\infty$. Thus quadratic reciprocity proves Artin reciprocity in the case of quadratic extensions of the rationals.

Similarly all of the other reciprocity laws prove special cases of Artin reciprocity. Thus, with the results of Hilbert and Furtwangler, Artin was able to prove his reciprocity law for all extensions that were composites of extensions of prime degree. He was not, however, able to prove the remaining case of prime power degree extensions.

It is not clear immediately, nor does Artin attempt to show, that one can actually derive all of the classical reciprocity results from his new reciprocity law. The classical reciprocity laws actually explicitly give a modularity condition rather than simply claiming that one exists. In order to find such explicit formulations, one needs to be able to find the conductors of the extensions in question. For certain simple cases this is possible.

Theorem 2.3.3 (Quadratic Reciprocity). *Suppose that p and q are odd primes in $\mathbb{Z}$. Then $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$, where $p^* = \left(\frac{-1}{p}\right)p$.*

Proof. Consider the extension L/K where $L = \mathbb{Q}(\sqrt{q})$ and $K = \mathbb{Q}$. Since a quadratic algebraic number is an integer exactly when its norm and trace are integers, $\mathcal{O}_L = \mathbb{Z}[\alpha]$ where $\alpha = \sqrt{d}$ unless $q \equiv 1 \pmod 4$ in which case $\alpha = \frac{1}{2} + \frac{\sqrt{q}}{2}$. Thus we can compute the discriminant in these cases, getting $(4q)$ and (q) respectively. As we shall see later (Proposition 3.6.7), the finite part of the conductor of a quadratic extension is the same as its discriminant. Thus the finite part of the conductor of L/K is $(4q)$ or (q) respectively. To find the infinite part, we need only find out whether the infinite prime of $\mathbb{Q}$ stays real in L. Obviously, this happens exactly when q is positive, and so the infinite prime appears in the conductor exactly when q is negative.

By Kummer's theorem, the value of $\left(\frac{q}{p}\right)$ is given by whether or not (p) splits completely in K. This in turn is determined by whether $\varphi_{(p)}$ is trivial. Now, by Artin reciprocity, the value of $\varphi_{(p)}$ is given by some modularity condition modulo $\mathfrak{f}$. Regardless of what $\mathfrak{f}$ is, this means that the value of $\varphi_{(p)}$ is given by some modularity condition modulo $(4q)\infty$. Since $(p) = (p^*)$, we can look at p^* instead, which has the advantage of being $1 \pmod 4$. Thus, whether $\varphi_{(p)}$ is 1 is given by whether p^* lies in some subgroup of index 2 in $I_K^{(4q)\infty}/P_K^{(4q)\infty} = (\mathbb{Z}/4q\mathbb{Z})^\times = (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$. The only such subgroup is the squares. Since p^* is automatically a square modulo 4, we get that the way that (p) factors in L is given by whether p^* is a square modulo q. Therefore, we get $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. □

The same sort of argument works for more difficult reciprocity laws.

Definition 2.3.4. *Let $K = \mathbb{Q}(\zeta_3)$. Suppose π is a prime in $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$. Then we define the cubic residue symbol, for any $a \in \mathcal{O}_K$ relatively prime to π, $\left(\frac{a}{\pi}\right)_3 = a^{\frac{N\pi-1}{3}}$.*

This definition makes sense because $N\pi \equiv 1 \pmod 3$. In order to see this notice that $K = \mathbb{Q}(\sqrt{-3})$ and so by quadratic reciprocity $\pi \cap \mathbb{Z}$ splits exactly when it is $1 \pmod 3$. Hence if $\pi \cap \mathbb{Z}$ is $2 \pmod 3$ then it has residue field degree 2, and so its norm is congruent to $1 \equiv 2^2 \pmod 3$.

Just as with the Legendre symbol, one can argue that the cubic residue symbol is 1 exactly when a is a cube modulo π.

Now if we consider the Galois extension L/K where $L = K(\sqrt[3]{\pi_1})$, then by Kummer's theorem, the way that some other prime π_2 factors in L is given by the cubic residue symbol.

Theorem 2.3.5 (Cubic Reciprocity). *Suppose that π_1 and π_2 are distinct primes in $\mathcal{O}_K$ relatively prime to 3. Then there exists a unique π_2^* which is a unit multiple of π_2 and with $\pi_2^* \equiv 1 \pmod 3$. Furthermore we have*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2^*}{\pi_1}\right)_3.$$

Proof. First we show that for any prime π there exists a unique π^* which is a unit multiple of π and with $\pi^* \equiv 1 \pmod 3$. A prime which is $1 \pmod 3$ is called primary. First notice that the only units are $\pm 1,\ \pm\zeta_3, \pm\zeta_3^2$. To see this, notice that $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2} + \frac{\sqrt{-3}}{2}]$ and recall that the only units are those things with norm 1. Thus each prime has 6 unit multiples. Furthermore $(\mathcal{O}_K/(3))^\times$ has exactly $3^2 - 3 = 6$ elements. So all we need to do is check that all the units are distinct modulo (3). This is an elementary computation so we will leave it as an exercise to the reader.

As one might expect the rest of the proof proceeds by considering Artin reciprocity for the extension L/K. As in the quadratic case the first thing we need to do is find the conductor. As we shall see in Proposition 3.6.7, one can show that the finite part of the conductor divides $(3\pi_1)$. Since K is complex, there are no real primes and so a priori no ramified primes. Thus the conductor genuinely divides $(3\pi_1)$.

Thus we can go through the same argument as for quadratic reciprocity. The value of φ_{π_2} (and thus of the cubic residue symbol) is given by a congruence condition modulo $(3\pi_1)$. We need to write the class group $I_K^{(3\pi_1)}/P_K^{(3\pi_1)}$ in a more manageable form. Notice that every element of $I_K^{(3\pi)}$ can be written uniquely as a product of principal prime ideals generated by primary primes. In this form, the things we are modding out by are solely those principal prime ideals generated by a primary prime congruent to one modulo π. Thus the class group can be identified with $(\mathcal{O}_K/(\pi_1))^\times)$, where to each prime ideal we associate the primary prime which generates it.

Thus, Artin reciprocity says that $\varphi_{(\pi_2)}$ is given by the image of π_2^* in the quotient of $(\mathcal{O}_K/(\pi_1))^\times)$ by some subgroup of index 3. Since this group is cyclic, the only such subgroup is the subgroup of cubes. Therefore, we get that

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2^*}{\pi_1}\right)_3.$$

□

2.3.3 Chebotarev's Density Theorem

One interesting consequence of Artin reciprocity is that it allows one to prove Frobenius's conjecture on the even distribution of primes with a given Frobenius automorphism. There is a clever trick which allows one to reduce to the case of an abelian extension. For any $\sigma \in \mathrm{Gal}(L/K)$ we can show that Frobenius's conjecture holds for σ and L/K exactly when it holds for σ and L/L^σ by a counting argument done in [**L1**, VII.4, Thm 10].

Now by Artin reciprocity, the set of primes with a given Frobenius in an abelian extension is the same (up to finitely many terms) as the set of primes in some particular coset of the ray class of some modulus. Thus we have reduced the general conjecture of Frobenius to a simple generalization of Dirichlet's theorem on primes in arithmetic progressions. The exact same proof which Dirichlet used will give this result, provided that we can show that $L(1, \chi) \neq 0$ for any non-trivial character of the class group of L/K. As we commented in our proof of the first fundamental inequality, this non-vanishing follows from L/K being a class group.

Unfortunately since Artin was unable to prove his reciprocity theorem, he was unable to give a proof of Frobenius's conjecture. But in 1923, Chebotarev proved Frobenius's conjecture without using any of Artin's methods. From this point on it has been referred to as "the Chebotarev density theorem." Nikolai Chebotarev was born in 1894 (after Frobenius conjectured the result that now bears Chebotarev's name) in Kamenets-Podolsk in Russia and died in 1947.

Chebotarev's method's are beyond the scope of this paper, but there is a nice outline in [**S-L**]. He used a clever method to reduce to the case of a cyclotomic extension where he could prove the result by hand. Chebotarev's methods were a crucial step forward in completing class field theory, however, for a few years Chebotarev was not aware of the developments in class field theory and the German class field theorists were not aware of Chebotarev's results. Although Chebotarev published his paper in 1923, he did not publish a German version until 1925, and he did not study class field theory until 1927. Chebotarev's methods were exactly what was needed to prove Artin reciprocity and this became clear to Artin in 1925 and Chebotarev in 1927. Thus Artin was able to complete the proof of his reciprocity law first in July 1927 using the methods of Chebotarev.

2.4 Artin's Theorem and Generalizing from the Abelian Case

2.4.1 Artin's Theorem

Artin's next goal was to show that his new L-series had the same properties as the abelian L-series. For example, we would like to show that they can be analytically continued to a meromorphic or holomorphic function on the whole plain, that they have a certain functional equation, that they do not vanish at 1, etc.

Before attempting to concoct a whole new proof of these results it is worth pausing for a moment to notice in which situations we have already proven them. In particular, let's consider the fact that the L-series do not vanish on the line $\mathrm{Re}(s) = 1$ (this fact is needed for certain theorems on the distribution of primes). We might hope that the same result holds for all Artin L-series.

Suppose V is any 1-dimensional representation V of a group $G = \mathrm{Gal}(L/K)$,then this representation has some kernel N and $G/N \hookrightarrow \mathbb{C}^\times$ is abelian. Thus V is the pull-back of a character of an abelian group, and its L-series agrees (up to finitely many Euler factors) with the L-series of some class group. Therefore, our fact is true for all 1-dimensional representations.

Furthermore, by the induction property, if V is a 1-dimensional representation of a subgroup $H \subset G$, then $L(s, \mathrm{Ind}_H^G V) \equiv L(s, V)$ also is non-vanishing on the line $\mathrm{Re}(s) = 1$. Lastly, notice that if this property holds for two representations of G, V_1 and V_2, then it clearly holds for $L(s, V_1 + V_2) = L(s, V_1)L(s, V_2)$.

We can even squeeze a bit more information out of the abelian case, since the above argument actually works for arbitrary class functions. That is to say, we have already shown that $L(1+it, f) \neq 0$ for any class function f that can be written as a $\mathbb{Q}$-linear combination of representations induced from 1-dimensional representations. (Henceforth, representations which are induced from 1-dimensional representations will be called monomial representations and their characters will also be called monomial.)

This seems to be of little use since we do not a priori know which representations can be written as a $\mathbb{Q}$-linear combination of monomial representations. However, we have the following theorem due to Artin.

Theorem 2.4.1 (Artin). *Let H_i index the cyclic subgroups of a group G. For each H_i, we have the induction function on the space of class functions sending $R_{\mathbb{C}}(H_i) \to R_{\mathbb{C}}(G)$. This gives us a composite map*

$$\mathit{Ind}: \quad \bigoplus_i R_{\mathbb{C}}(H_i) \to R_{\mathbb{C}}(G).$$

This map is surjective.

Proof. Any linear map of vector spaces gives an adjoint linear map in the opposite direction of their dual spaces. Since we have a canonical inner product on all of these spaces, the dual spaces are canonically identified with the spaces themselves. Frobenius reciprocity tells us precisely that the adjoint map to induction is restriction. Thus in our case, the adjoint map on dual spaces is

$$\mathrm{Res}: \quad R_{\mathbb{C}}(G) \to \bigoplus_i R_{\mathbb{C}}(H_i).$$

By basic linear algebra, if we choose a basis, then the dual map is the conjugate transpose of the original map. Therefore, showing that the induction map is surjective is the same as proving this restriction map is injective. But, $R_{\mathbb{C}}(G)$ is simply the space of complex valued class functions. Since every element of G is contained in one of the H_i, no non-trivial class function can be mapped to 0 under restriction. □

Corollary 2.4.2 (Artin's Theorem).

$$\mathit{Ind}: \quad \bigoplus_i R_{\mathbb{Q}}(H_i) \twoheadrightarrow R_{\mathbb{Q}}(G).$$

Proof. Here we simply note that by the formula for induction, if we pick a basis, all the matrix element of Ind are rational numbers. Therefore, the rank of this map has the same dimension as the rank of the map in Theorem 2.4.1. □

This lets one prove many results about Artin L-functions immediately from the abelian case.

Proposition 2.4.3. *For any character χ of $Gal(L/K)$, $L(1+it, \chi; L/K) \neq 0$.*

Proof. By Artin's theorem, we can write χ as a linear combination of monomial representations. But as commented above, this is enough to prove this result. □

By some standard arguments from analytic number theory (cf. [**C-F**, Theorem 4, p. 214]), it follows that

Corollary 2.4.4. *If x is a positive integer and C is a conjugacy class of $G = Gal(K/\mathbb{Q})$, let $\pi(x, C)$ be the number of distinct prime ideals with norm less than x in some field K which have Frobenius lying in C.*

$$\pi(x, C) \sim \frac{|C|}{|G|}$$

(where $\sim$ denotes asymptotic equality, that is their ratio approaches 1).

2.4.2 Analytic Continuation and the Completed Artin L-series

Similarly, one can use Artin's theorem to get a functional equation for Artin L-series. We can decompose any character of G into $\mathbb{Q}$-linear combination of monomial characters, say

$$\chi = \sum_i a_i \mathrm{Ind}_{H_i}^{G_i} \psi_i.$$

Each of the terms on the right hand side has an associated abelian L-function each of which can be extended to a meromorphic function on the entire plain which has a functional equation. Furthermore, this functional equation relates the value of each of these L-functions of monomial characters to the value of its conjugate character. Since the conjugate of a linear combination is the same as the linear combinations of the conjugates we get that this functional equation relates the value of the L-function at s to the value of the conjugate Artin L-function at $1 - s$.

There are several problems with this picture. Firstly, since the Artin L-series is a $\mathbb{Q}$-linear combination of the abelian L-functions, its analytic continuation is not meromorphic, because it may have several branches. We only get that some power of the Artin L-function is meromorphic. Secondly, since we don't have an explicit decomposition of χ into a linear combination of monomial characters, we do not have an explicit form of this functional equation.

To fix the first problem, Artin suggested that in fact every character is a $\mathbb{Z}$-linear combination of monomial characters.

Definition 2.4.5. *A subgroup of G is p-elementary if it is the direct product of a cyclic group of order prime to p with a p-group. A subgroup is elementary if it is p-elementary for some p.*

Theorem 2.4.6 (Brauer's Theorem). *Every character of an elementary subgroup is 1-dimensional. Furthermore, if G is any group and χ is any character of G, then we can write $\chi = \sum_i a_i Ind_{H_i}^G \psi_i$ where H_i indexes the elementary subgroups, a_i is an integer, and ψ_i is character of H_i (which is therefore 1-dimensional).*

Proof. This result was finally proved by Richard Brauer in 1946. For the original article see [**B**, pp. 539-551] for another proof see [**Se1**, Chapter 10]. With this result we get that every Artin L-series can be analytically continued to a meromorphic function on the whole plane. Although we do not have time to give the proof of this result, it will occasionally be necessary to use it. □

As Artin nonchalantly notes, "However, it will require completely new methods to show that the L-series are associated to entire functions (aside from the principal character)." This claim is one of several which bears the name "Artin's Conjecture." It is still an open problem and a subject of very active research. For a survey of the methods which are being applied to this problem in the simplest case of two-dimensional representations, see Serre's article in [**Fröh**, pp. 193-268].

In order to give an explicit formulation of the functional equation for the Artin L-function, we would like to define the notion of a completed Artin L-series. Artin's theorem suggests a program for accomplishing this, namely, we decompose our L-function as a product of powers of abelian L-functions and define the completed Artin L-function to the product of the corresponding completed abelian L-functions. This definition has a significant problem in that it is conceivable that several different decompositions could yield different completed abelian L-functions.

2.4.3 Conditions for Extending Functions on Cyclic Subgroups

In order to fix this problem and find a well-defined completed Artin L-function, we need to know when a function on characters of abelian subgroups of a group defines a unique function of characters of the whole group by extending by additivity and induction. In other words, suppose we have a group G, and for each element of g we have the cyclic subgroup H_g generated by g, and for each H_g we have some function f_g on the set of characters of H_g, when does this define a unique class function on G given by $f(\sum_i a_i \mathrm{Ind}_{H_{g_i}}^G \chi_i) = \sum_i a_i f_g(\chi_i)$, where χ_i are characters of dimension 1?

The methods which we used to prove Artin's theorem are precisely what we need to answer this question. Since we have a canonical inner product on class functions, each $f_g(\chi)$ must be given by (χ, ψ_g) for some class function ψ_g. Furthermore, if ψ is a class function on G we have a restriction map

$$\mathrm{Res}: \ R_{\mathbb{C}}[G] \to \bigoplus_{g \in G} R_{\mathbb{C}}[H_g].$$

Since restriction is the dual of induction, a collection of ψ_g will define a class function on the whole group precisely when it is in the image of this restriction map.

Proposition 2.4.7. *cf. [**Se1**, Exercise 9.6] A collection of $\psi_g \in R_{\mathbb{C}}[H_g]$ for all $g \in G$ defines a class function in $R_{\mathbb{C}}[G]$ by extending by additivity and induction exactly when, for all integers k,*

$$Res_{H_{g^k}}^{H_g} \psi_g = \psi_{g^k},$$

and for any $g' \in H_g$ and any $s \in G$,

$$\psi_g(g') = \psi_{sgs^{-1}}(sg's^{-1}).$$

Proof. As we have already argued, it is enough to show that these are the image of

$$\mathrm{Res}: \ R_{\mathbb{C}}[G] \to \bigoplus_{g \in G} R_{\mathbb{C}}[H_g].$$

Consider the function on G given by $\psi(g) = \psi_g(g)$. By the second condition, this is a class function. By the first condition $\mathrm{Res}_{H_g}^G \psi(g) = \psi_g$. □

Thus, if we want to determine whether we can extend a function defined on abelian characters to a function defined on characters of non-abelian Galois groups by induction and additivity, then it is enough to check that it satisfies the two conditions of Proposition 2.4.7.

In particular, let us check that the unramified part of the abelian L-functions extends in this way. We already know that it does, because we have proved that the Artin L-function has this property, but we can check this with our new condition without actually constructing the Artin L-function. First notice that the L-function is not actually additive in characters, but $\log L$ is.

Definition 2.4.8. *Fix some Galois extension L/K, take $g \in Gal(L/K)$, and let H_g be the subgroup generated by g. If χ is a (class) function on $Gal(L/L^{H_g})$, then we define*

$$\hat{L}(s, \chi) = \log \prod_{\mathfrak{p} \ unram.} \frac{1}{1 - \chi(\varphi_{\mathfrak{p}}) N\mathfrak{p}^{-s}} = \sum_{\mathfrak{p} \ unram.} \sum_{\ell=1}^{\infty} \chi(\varphi_{\mathfrak{p}}^{\ell}) \ell^{-1} N\mathfrak{p}^{-s\ell},$$

where the product (resp. sum) is taken over all finite primes of L^{H_g} which do not divide primes in K which ramify in L/K.

We want to show that this function gives us a unique function on characters of L/K by extending by additivity and induction. In order to apply Proposition 2.4.7, we need to write $\hat{L}(s,\chi)$ in the form (χ,ψ_g) for some class function ψ_g on H_g.

Lemma 2.4.9. *$\hat{L}(s,\chi)=(\chi,\psi_g)$ where,*

$$\psi_g = |H_g| \sum_{\substack{\mathfrak{p},\ \ell \text{ s.t.} \\ \varphi_{\mathfrak{p}}^{\ell}=h}} \ell^{-1} N\mathfrak{p}^{-\bar{s}\ell},$$

where ℓ goes from 1 to ∞ and $\mathfrak{p}$ ranges over all finite primes of L^{H_g} which do not divide primes in K which ramify in L/K.

Proof.

$$\sum_{\mathfrak{p}\ \text{unram.}} \sum_{\ell=1}^{\infty} \chi(\varphi_{\mathfrak{p}}^{\ell})\ell^{-1}N\mathfrak{p}^{-s\ell} = \frac{1}{|H_g|}\sum_{h\in H_g}\chi(h)\overline{|H_g| \sum_{\substack{\mathfrak{p},\ \ell \text{ s.t.} \\ \varphi_{\mathfrak{p}}^{\ell}=h}} \ell^{-1}N\mathfrak{p}^{-\bar{s}\ell}}.$$

□

Theorem 2.4.10. *The functions ψ_g extend to a unique class function ψ of G by induction and additivity. Thus we can define $L(s,\chi;L/K)$ for any character χ of $Gal(L/K)$. (By uniqueness, this is just the Artin L-function.)*

Proof. By Proposition 2.4.7, we only need to check that ψ_g has those two properties. For the first property, we notice that

$$\psi_{g^k}(h) = |H_{g^k}| \sum_{\substack{\mathfrak{q},\ m \text{ s.t.} \\ \varphi_{\mathfrak{q}}^{\ell}=h}} m^{-1}N\mathfrak{q}^{-\bar{s}m},$$

where $\mathfrak{q}$ ranges over all primes in $L^{H_{g^k}}$ which divide unramified primes in L/K. On the other hand, by Proposition 1.5.14, $\varphi_{\mathfrak{q}}=\varphi_{\mathfrak{p}}^{f_{\mathfrak{q}}}$ where $\mathfrak{p}$ is the prime in L^{H_g} under $\mathfrak{q}$. Also, $N\mathfrak{p}=N\mathfrak{q}^{\frac{1}{f_{\mathfrak{q}}}}$. Therefore, since there are $g_{\mathfrak{q}}$ different primes dividing $\mathfrak{p}$ we get,

$$\mathrm{Res}^{H_g}_{H_{g^k}}\psi_g(h) = |H_g| \sum_{\substack{\mathfrak{q},\ \ell \text{ s.t.} \\ \varphi_{\mathfrak{p}}^{\ell}=h^{f_{\mathfrak{q}}}}} g_{\mathfrak{q}}^{-1}\ell^{-1}(N\mathfrak{q}^{\frac{1}{f_{\mathfrak{q}}}})^{-\bar{s}\ell}.$$

Now, because $f_{\mathfrak{q}}$ divides $|H_g|$, $\varphi_{\mathfrak{p}}^{\ell}=h^{f_{\mathfrak{q}}}$ exactly when $\ell=mf_{\mathfrak{q}}$ for some integer m. Therefore, we can make a change of variables $\ell=f_{\mathfrak{q}}m$ to get

$$\mathrm{Res}^{H_g}_{H_{g^k}}\psi_g(h) = |H_g| \sum_{\substack{\mathfrak{q},\ m \text{ s.t.} \\ \varphi_{\mathfrak{p}}^{m}=h}} g_{\mathfrak{q}}^{-1}f_{\mathfrak{q}}^{-1}m^{-1}N\mathfrak{q}^{-\bar{s}m}.$$

But, since $g_{\mathfrak{q}}f_{\mathfrak{q}}=[H_g:H_{g^k}]$, we get $\mathrm{Res}^{H_g}_{H_{g^k}}\psi_g(h)=\psi_{g^k}(h)$ and we have checked condition 1.

Now we turn to the second condition. If $\mathfrak{p}$ runs over all primes in L^{H_g} which divide unramified primes in L/K, then $s\mathfrak{p}s^{-1}$ runs over all primes in $L^{H_{sgs^{-1}}}$ which divide unramified primes in L/K. Also, by Proposition 1.5.14, $\varphi_{s\mathfrak{p}s^{-1}}=s\varphi_{\mathfrak{p}}s^{-1}$. Therefore,

$$\psi_{sgs^{-1}}(h) = |H_g| \sum_{\substack{\mathfrak{p},\ \ell \text{ s.t.} \\ \varphi_{s\mathfrak{p}s^{-1}}^{\ell}=h}} \ell^{-1}N(s\mathfrak{p}s^{-1})^{-\bar{s}\ell} = \psi_g(h),$$

because the norm of conjugate primes are equal. □

2.4.4 Our Program for Constructing the Completed Artin L-function

One of the most important problems which Artin has left unanswered in his paper is showing that one can actually construct a well-defined completed Artin L-function. To do this, we need to show that we can extend the terms for ramified primes, the terms for infinite primes, and the exponential term just as we were able to extend the unramified terms. Although we could attempt nonconstructive proofs like the one in the last section, we will actually be able to explicitly construct functions that behave well under sums and induction and that agree with the abelian case. The bulk of the rest of this chapter will be devoted to extending each of these parts of the abelian L-function to the non-abelian case so that in the end we will be able to explicitly write down a completed L-function with a functional equation.

2.5 The Local Factors for Ramified Primes

2.5.1 Introduction

Our first step in completing the Artin L-function is to give a definition of the local factors for the ramified primes. Recall that, for the unramified primes the local factors, if $L/M/K$ is a tower of extension with L and M both Galois over K and if ψ is a class function on $\mathrm{Gal}(M/K)$, then $L_{\mathfrak{p}}(s,\psi;L/K) = L_{\mathfrak{p}}(s,\psi;M/K)$. We would hope that the same is true of the ramified primes. This will be our key tool for motivating Artin's definition which he gave in his paper *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren* [**Ar**, pp. 165-179]. Once we have this definition, we can verify that this definition satisfies the basic properties concerning the sum of characters, the pullback of characters, and induced characters.

2.5.2 Definition

Recall that, for $\mathfrak{p}$ unramified,

$$\log L_{\mathfrak{p}}(s,\chi;L/K) = \sum_{\ell=1}^{\infty} \frac{\chi(\varphi_{\mathfrak{p}}^{\ell})}{\ell N\mathfrak{p}^{\ell s}} = (\chi,\psi_{\mathfrak{p}}),$$

where

$$\psi(g) = |G| \sum_{\varphi_{\mathfrak{p}}^{\ell}=g} \frac{1}{\ell N\mathfrak{p}^{s\ell}}.$$

Suppose that χ is trivial on some normal subgroup H. By the second version of Frobenius reciprocity, we have $(\chi,\psi)_G = (\chi,\psi^{\natural})_{G/H}$. Thus, if χ is trivial on a normal subgroup H, we have

$$\log L_{\mathfrak{p}}(s,\chi;K^H/K) = \sum_{\ell=1}^{\infty} \frac{1}{\ell N\mathfrak{p}^{\ell s}} \frac{1}{|H|} \sum_{g\in\varphi_{\mathfrak{p}}^{\ell}H} \chi(g).$$

In particular, suppose that χ is trivial on the inertia group $I_{\mathfrak{p}}$. Then, the prime $\mathfrak{p}$ is unramified in the extension $L^{I_{\mathfrak{p}}}/K$. Hence, in the expression above, the left hand side makes sense and suggests that we use the right hand side as the definition of the local factor in the general case.

Definition 2.5.1. *If $\mathfrak{p}$ is any finite prime of K (possibly ramified), $\mathfrak{P}$ is any prime sitting over $\mathfrak{p}$ in L, and χ is a character of L/K, then we define the local factor*

$$L_{\mathfrak{p}}(s,\chi;L/K) = \exp\left(\sum_{\ell=1}^{\infty} \frac{1}{\ell N\mathfrak{p}^{\ell s}} \frac{1}{e_{\mathfrak{P}}} \sum_{g\in\varphi_{\mathfrak{P}}^{\ell}I_{\mathfrak{P}}} \chi(g)\right) = \exp\left(\sum_{\ell=1}^{\infty} \frac{1}{\ell N\mathfrak{p}^{\ell s}} \chi^{\natural}(\varphi_{\mathfrak{P}}^{\ell})\right).$$

It is clear that this definition agrees with the definition in the unramified case. Furthermore, we can rewrite this formula in a way which is more reminiscent of our original formula.

Proposition 2.5.2. *If $\mathfrak{p}$ is a prime in K, $\mathfrak{P}$ is some prime sitting over it in L, and V is a representation of $Gal(L/K)$, then*

$$L_{\mathfrak{p}}(s,\chi;L/K) = \det\left(Id - N\mathfrak{p}^{-s}\varphi_{\mathfrak{P}};V^{I_{\mathfrak{P}}}\right)^{-1}.$$

Proof. Suppose that $\lambda_1,\ldots,\lambda_n$ are the eigenvalues of $\varphi_{\mathfrak{P}}$ acting on $V^{I_{\mathfrak{P}}}$, then

$$\log\det\left(\mathrm{Id} - N\mathfrak{p}^{-s}\varphi_{\mathfrak{P}};V^{I_{\mathfrak{P}}}\right)^{-1} = -\log\prod_{i=1}^{n}(1-N\mathfrak{p}^{-s}\lambda_i) = -\sum_{i=1}^{n}\log(1-N\mathfrak{p}^{-s}\lambda_i).$$

Now we can take the Taylor expansion to get,

$$\log\det\left(\mathrm{Id} - N\mathfrak{p}^{-s}\varphi_{\mathfrak{P}};V^{I_{\mathfrak{P}}}\right)^{-1} = -\sum_{i=1}^{n}\sum_{\ell=1}^{\infty}\frac{1}{\ell N\mathfrak{p}^{\ell s}}\lambda_i^{\ell}.$$

Interchanging sums and using the fact that $\sum_{i=1}^{n} \lambda_i^\ell = \chi_{V^{I_\mathfrak{P}}}(\varphi_\mathfrak{P}^\ell)$, we see that

$$\log\det\left(\mathrm{Id} - N\mathfrak{p}^{-s}\varphi_\mathfrak{P}; V^{I_\mathfrak{P}}\right)^{-1} = \sum_{\ell=1}^{\infty} \frac{1}{\ell N\mathfrak{p}^{\ell s}} \chi_{V^{I_\mathfrak{P}}}(\varphi_\mathfrak{P}^\ell).$$

Thus, our claim follows from Proposition 1.5.34. □

2.5.3 The Basic Properties of the Local Factors for Ramified Primes

Now that we have a definition of the local factor for the ramified primes which agrees with our old definition, we need to check that it has all of the nice properties which the unramified factors had.

Proposition 2.5.3 (Artin).

$$L_\mathfrak{p}(s, \chi_1 + \chi_2; L/K) = L_\mathfrak{p}(s, \chi_1; L/K) L_\mathfrak{p}(s, \chi_2; L/K).$$

Proof. The formula for the logarithm of the local factor is clearly additive, thus exponentiating gives our result. □

Proposition 2.5.4 (Artin). *If $Gal(L/K) = G$ has a normal subgroup H and χ is a character of G/H, then*

$$L_\mathfrak{p}(s, \chi; L^H/K) = L_\mathfrak{p}(s, \chi; L/K).$$

Proof. Take $\mathfrak{q}$ a prime above $\mathfrak{p}$ in L^H, and $\mathfrak{P}$ a prime above $\mathfrak{q}$ in L. By Proposition 1.5.14 $\varphi_\mathfrak{q}$ is $\varphi_\mathfrak{P} H$. Furthermore, $I_\mathfrak{P} = I_\mathfrak{q} H$. Thus $\rho_{V^{I_\mathfrak{P}}}(\varphi_\mathfrak{P}) = \rho_{V^{I_\mathfrak{q}}}(\varphi_\mathfrak{q})$, and the proposition follows from Proposition 2.5.2. □

Proposition 2.5.5 (Artin). *If $Gal(L/K)$ is an abelian group, then $L_\mathfrak{p}(s, \chi; L/K)$ equals the local factor of the abelian L-function of the corresponding character of the class group given by Artin reciprocity.*

Proof. Recall that the definition of the abelian L-function is given by taking the character and looking at it as a primitive character of a quotient of the class group by the kernel of the character. By Artin reciprocity, this corresponds to considering $L_\mathfrak{p}(s, \chi; L^H/K)$ where H be the kernel of χ. By Proposition 2.5.4, $L_\mathfrak{p}(s, \chi; L/K) = L_\mathfrak{p}(s, \chi; L^H/K)$, which is exactly what we wanted to show. □

Lastly we need to prove that the Artin L-function attached to an induced representation is the same as that attached to the original representation. In order to prove this in general, we will need a slightly stronger version of Mackey's theorem.

Theorem 2.5.6 (Mackey's Theorem, stronger version). *If H and G' are subgroups of G, W a representation of H, and N is a normal subgroup of G', then*

$$(Res_{G'} Ind_H^G W)^N \cong \bigoplus_{s \in G' \backslash G / H} (Ind_{K \cap sHs^{-1}}^{G'} sW)^{N \cap sHs^{-1}}.$$

(Where (ρ_s, sW) is a representation of sHs^{-1} given by $\rho_s(x) = \rho(s^{-1}xs)$.)

Proof. The proof of the special case of $N = 1$ [**Se1**, Proposition 22, page 58] actually works for any N if one simply follows through what the N-invariance means in each step of the proof. Since it is purely a representation theoretic result, we will not repeat this proof here. □

Proposition 2.5.7 (Artin). *Suppose we have number fields $K \subset M \subset L$ with $Gal(L/K) = G$ and $Gal(L/M) = H$. H can be identified with subgroup of G. Fix $\mathfrak{p}$ some prime of K. If χ is any character of H, then*

$$\prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}(s, \chi; L/M) = L_\mathfrak{p}(s, Ind_H^G \chi; L/K).$$

Proof. Take χ to be the character of some representation W.

Following our notation and argument in Theorem 2.2.1, we have that in M $\mathfrak{p}$ factors as $\mathfrak{p} = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_g$. For each i, choose some $\mathfrak{P}_i \in L$ sitting over $\mathfrak{q}_i$. Let G_i and I_i denote the decomposition and inertia groups of $\mathfrak{P}_i/\mathfrak{p}$ respectively. Now take $\varphi \in G_1$ which reduces to the Frobenius in G_1/I_1. Thus, by definition, the local factor is

$$L_{\mathfrak{p}}(s, V, L/K) = \det\left(1 - \varphi N\mathfrak{p}; V^{I_1}\right)^{-1}.$$

Since the Frobenius lives in G_1 not G, we can replace V with $\mathrm{Res}_{G_1}V$. In this case this lets us rewrite our local factor as:

$$L_{\mathfrak{p}}(s, V, L/K) = \det\left(1 - \varphi N\mathfrak{p}; (\mathrm{Res}_{G_1}\mathrm{Ind}_H^G W)^{I_1}\right)^{-1}.$$

Just as before we want to apply Mackey's theorem. Recall that, if we take $\tau_i \in G$ such that $\tau_i^{-1}\mathfrak{q}_1 = \mathfrak{q}_i$, then $\{\tau_i\}$ is a set of representatives for the double cosets $G_i\backslash G/H$ (here as always i ranges between 1 and g). Furthermore, since the $\mathfrak{P}_i$ were arbitrarily, we can choose them so that $\tau_i^{-1}\mathfrak{P}_1 = \mathfrak{P}_i$.

Therefore, by the stronger version of Mackey's theorem, we can rewrite our local factor as:

$$\begin{aligned} L_{\mathfrak{p}}(s, V, L/K) &= \det\left(1 - \varphi N\mathfrak{p}; \bigoplus_{i=1}^{g} (\mathrm{Ind}_{G_1\cap\tau_i H\tau_i^{-1}}^{G_1}\tau_i W)^{I_1\cap\tau H\tau^{-1}}\right)^{-1} \\ &= \prod_{i=1}^{g}\det\left(1 - \varphi N\mathfrak{p}; (\mathrm{Ind}_{K\cap\tau_i H\tau_i^{-1}}^{G_1}\tau_i W)^{I_1\cap\tau_i H\tau_i^{-1}}\right)^{-1} \end{aligned}$$

Conjugate each term individually by τ_i^{-1} to find

$$L_{\mathfrak{p}}(s, V, L/K) = \prod_{i=1}^{g}\det\left(1 - \tau_i^{-1}\varphi\tau_i N\mathfrak{p}; (\mathrm{Ind}_{\tau_i^{-1}G_1\tau_i\cap H}^{\tau_i^{-1}G_1\tau_i} W)^{\tau_i^{-1}I_1\tau_i\cap H}\right)^{-1} \tag{2.5.1}$$

But, clearly, from the definition of τ_i, $G_i = \tau_i^{-1}G_1\tau_i$ and $I_i = \tau_i^{-1}I_1\tau_i$ are (respectively) the decomposition and inertia groups for $\mathfrak{P}_i/\mathfrak{p}$. Furthermore, by Proposition 1.5.14, $\varphi_i = \tau_i^{-1}\varphi\tau_i$ reduces to the Frobenius in G_i/I_i.

Notice that $G_i \cap H = H_i$ and $I_i \cap H = I_i'$ are (respectively) the decomposition and inertia groups for $\mathfrak{P}_i/\mathfrak{q}_i$.

Now this expression is beginning to look like the product of the local factors for each $\mathfrak{q}_i$. By Proposition 1.5.14 if f_i is the relative degree of $\mathfrak{P}_i/\mathfrak{q}_i$, then $\varphi_i^{f_i}$ is the Frobenius for $\mathfrak{P}_i/\mathfrak{q}_i$. Thus,

$$\prod_{i=1}^{g} L_{\mathfrak{q}_i}(s, W, L/M) = \prod_{i=1}^{g}\det\left(1 - \varphi_i^{f_i}N\mathfrak{p}^{f_i}; W^{I_i'}\right)^{-1}.$$

Therefore we have reduced our general problem to verifying the equation

$$\det\left(1 - \varphi_i^{f_i}N\mathfrak{p}^{f_i}; W^{I_i'}\right) = \det\left(1 - \varphi_i N\mathfrak{p}; (\mathrm{Ind}_{H_i}^{G_i}W)^{I_i'}\right)$$

But, this is exactly the equality of local factors in the special case of the extension of decomposition fields, $L^{G_i} \subseteq L^{H_i} \subseteq L$ (in this case $g = 1$). (It is important to note here that the Frobenii for this field extension are exactly the same as those at the same prime in the original field extension.)

Now that we are in this special case we can reduce even further to get rid of the ramification. By Proposition 1.5.35 $(\mathrm{Ind}_H^G W)^I \cong Ind_{H/H\cap I}^{G/I} W^{I\cap H}$. Applying this to equation Equation 2.5.1 reduces us to proving the equality of local factors for the tower of extensions $L^{G_i} \subseteq L^{H_i} \subseteq L^{I_i}$, where now our prime above $\mathfrak{p}$ in L^{G_i} is completely unramified. Thus we have reduced to the calculation which we already made in the end of Theorem 2.2.1. □

In particular, since the logarithm of $L_{\mathfrak{p}}(s, \chi; L/K)$ is additive and preserved under induction, by Artin's theorem, it is the unique function which extends the abelian definition to characters of non-abelian groups by additivity and induction.

Since we now have a definition for the ramified primes we change our original definition of the Artin L-function.

Definition 2.5.8.

$$L(s, \chi; L/K) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, \chi; L/K).$$

Clearly we have that with this new definition the Artin L-series has actual equality in the following formulas:

Theorem 2.5.9 (Artin).

1. *If $Gal(L/K)$ is abelian, then $L(s, \chi; L/K)$ equals the abelian L-function associated to the character $\chi \circ \varphi_{L/K}$ of the class group of L/K (where $\varphi_{L/K}$ is the Artin map).*
2. $$L(s, \chi_1 + \chi_2; L/K) = L(s, \chi_1; L/K)L(s, \chi_2; L/K).$$
3. *If $Gal(L/K) = G$ has a normal subgroup H and χ is a character of G/H, then*
$$L(s, \chi; L^H/K) = L(s, \chi; L/K).$$
4. *Suppose we have number fields $K \subset M \subset L$ with $Gal(L/K) = G$ and $Gal(L/M) = H$. H can be identified with subgroup of G. If χ is any character of H, then*
$$L(s, \chi; L/M) = L(s, Ind_H^G \chi; L/K).$$

Proof. We have already shown these equalities prime by prime. □

2.5.4 An Application to ζ-function Formulas

We now have a definition of the Artin L-function which is genuinely equal to the abelian L-function in the abelian case and where we have genuine equality in the induction formula. This gives us a means of finding relations between abelian L-functions. In particular,

Theorem 2.5.10 (Artin). *If L/K is a Galois extension of number fields, then*

$$\zeta_L(s) = \prod_{\chi} L(s, \chi)^{\chi(1)},$$

where the product is taken over all irreducible characters.

Proof. By Theorem 2.5.9 property 1, we know that $\zeta_L(s) = L(s, \chi_0; L/L)$ where χ_0 is the trivial character. By the induction formula (property 4), we see that,

$$\zeta_L(s) = L(s, \mathrm{Ind}_{\{1\}}^G \chi_0; L/K).$$

By Frobenius reciprocity,

$$\mathrm{Ind}_{\{1\}}^G \chi_0 = r_G = \sum_{\chi} \chi(0)\chi.$$

Therefore, by the additivity property (property 2),

$$\zeta_L(s) = \prod_{\chi} L(s, \chi)^{\chi(1)}.$$

□

This formula gives us our required generalization of Weber's formula. In particular, if we knew Artin's conjecture we would be able to conclude that $\frac{\zeta_L(s)}{\zeta_K(s)}$ is a holomorphic function. However, even without this conjecture, this formula explains the origins of the mysterious ζ-function formulas which Artin had found. For each intermediate field M we can write the $\zeta_M(s)$ as a product of Artin L-functions, hence by finding relations between these combinations of L-functions we get ζ-function formulas. Moreover, at least when $K = \mathbb{Q}$, there are no non-trivial relations between the Artin L-functions.

Proposition 2.5.11 (Artin). *If L is a number field Galois over $\mathbb{Q}$ with $Gal(L/\mathbb{Q}) = G$ and ψ is a class function of G, then $L(s, \psi; L/\mathbb{Q}) = 1$ if and only if ψ is trivial.*

Proof. Suppose that $\psi = \sum_\chi a_\chi \chi$, where the sum is taken over all irreducible representations of G. Using the formula for the logarithm of the L-series, if $\mathfrak{P}$ is a prime over p, then

$$\sum_{p^\ell} \left(\sum_\chi a_\chi \chi^\natural(\varphi_p^\ell) \right) \frac{1}{\ell p^{\ell s}} = 0.$$

We can rewrite this sum as a Dirichlet series,

$$\sum_{p^\ell} \frac{\left(\frac{\sum_\chi a_\chi \chi^\natural(\varphi_p^\ell)}{\ell} \right)}{p^{\ell s}} = 0.$$

Now, by Proposition 1.2.7, this implies that $\sum_\chi a_\chi(g) = 0$ for every $g \in G$ which can be written as the Frobenius of some prime. By Corollary 2.4.4, there are infinitely many primes with each Frobenius, in particular there must be at least one. Therefore, for all $g \in G$, $\sum_\chi a_\chi \chi(g) = 0$. By the orthogonality of characters $a_\chi = 0$. □

This proposition does not apply to general base field K, because we can have several distinct primes in K which have the same norm and thus we could get some additional cancellation within a particular term of the Dirichlet series. In fact, one can find many examples of such additional L-series relations. For example, see Equation 3.2.1.

Proposition 2.5.4 does give us a method for determining all relations between ζ-functions or L-functions of any extensions of number fields. Simply take L to be a sufficiently large Galois extension of $\mathbb{Q}$ which contains all the fields used in the definitions of the functions. By pulling back and inducing, all of these L-functions can be written in terms of the L-functions of $L/\mathbb{Q}$. Then using gives us all the relations between them.

In particular in the next chapter we will use this to prove some interesting relations between the L-functions of an S_3 extension of $\mathbb{Q}$ and confirming Artin's previous formula that (taking $\mathrm{Gal}(L/K) = S_3$, and k is the subfield fixed by one of the subgroups of size 2 and F is the subfield fixed by the normal subgroup A_3)

$$\zeta_L \zeta_K^2 = \zeta_F \zeta_k^2.$$

For another example of using Proposition 2.5.4 to find relations between ζ-functions and L-functions see the last page of the appendix, where Artin applies this theorem to an A_5 extension of $\mathbb{Q}$.

2.6 The Local Factors for Infinite Primes

2.6.1 Introduction

Now we turn our attention to generalizing the Γ-factors to the non-abelian case. In this section, we define the local factors at infinity for the completed Artin L-series and prove that this definition still behaves well under addition, pull-backs, and induction. Like the ramified case, these definitions and results first appeared in Artin's paper *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren*[**Ar**, pp. 165-179].

2.6.2 Definition and Basic Properties

From the abelian case (see Definition 1.6.20) we recall the following definitions. Let

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right);$$
$$\Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = 2(2\pi)^{-s}\Gamma(s).$$

Now suppose that we have some extension L/K and a one-dimensional character χ of $\mathrm{Gal}(L/K)$ and some infinite prime v in K divisible by a prime w in L. We recall the definition of the decomposition group, G_w, for infinite primes. If w and v are both real or both complex, then G_w is trivial. If w is real and v is complex, then G_w consists of two elements: the identity and complex conjugation. Clearly, $\mathrm{Res}_{G_w}\chi$ is either trivial or the sign representation.

We recall from the abelian case (Definition 1.6.20) that the local factor at v is:

$$L_v(s,\chi) = \begin{cases} \Gamma_{\mathbb{C}}(s) & \text{if } v \text{ is complex} \\ \Gamma_{\mathbb{R}}(s) & \text{if } v \text{ is real and } \mathrm{Res}_{G_w}\chi \text{ is trivial} \\ \Gamma_{\mathbb{R}}(s+1) & \text{if } v \text{ is real and } \mathrm{Res}_{G_w}\chi \text{ is non-trivial} \end{cases}$$

As usual we want to extend this definition to the non-abelian case in such a way that it will be additive and preserved under induction. So suppose that we have an extension L/K, any representation (ρ, V), and infinite primes $w|v$ as above. From the abelian case and from the finite prime case, we would expect that this definition should be local in the sense that it only depends on $\mathrm{Res}_{G_w}V$. As mentioned before, G_w only has one or two elements. Therefore, $V = n_+(w)\chi_+ + n_-(w)\chi_-$ where χ_+ is the trivial representation and χ_- is the non-trivial representation. Clearly, $n_+(w) = \dim V^{G_w}$ and $n_-(w) = \mathrm{codim}\ V^{G_w}$. Thus if we assume additivity and our locality condition then there is really only one sensible definition of the local factors, namely:

Definition 2.6.1. *If v is an infinite prime, then we define the local factor of the Artin L-series at that prime to be*

$$L_v(s,V) = \begin{cases} \Gamma_{\mathbb{R}}(s)^{(\dim V^{G_w})}\Gamma_{\mathbb{R}}(s+1)^{(codim\ V^{G_w})} & \text{if } v \text{ is real} \\ \Gamma_{\mathbb{C}}(s)^{\chi(1)} & \text{if } v \text{ is complex} \end{cases}$$

This definition makes $L_v(s, V+W) = L_v(s,V)L_v(s,W)$, because dimension and codimension are clearly additive. Furthermore, since it only depends on the value the character takes on the Frobenius element, it is clearly preserved under the pull-back. Thus, all we have left to prove is that the local factors at the infinite primes behave well under induction.

Theorem 2.6.2 (Artin). *Suppose we have number fields $K \subset M \subset L$ with $Gal(L/K) = G$ and $Gal(L/M) = H$. H can be identified with subgroup of G. Then if χ is any character of H, and v is any infinite prime,*

$$L_v(s,\chi; L/M) = L_v(s, Ind_H^G\chi; L/K).$$

Proof. To do this we emulate the proof in the case of the finite primes. Just as before we consider the tower of fields $L/M/K$ with $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(L/M)$, and W a representation of H with $V = \mathrm{Ind}_H^G W$. Fix v some infinite prime of K. In M this will factor as $v = w_1 w_2 \cdots w_g$. For each i choose some $u_i \in L$ sitting over w_i. Let G_i denote the decomposition group of u_i/v. Just as before

we take coset representatives $\tau_i \in G$ of $G_v \backslash G / H$ such that $\tau_i^{-1} u_1 = u_i$. Again $G_i = \tau_i^{-1} G_1 \tau_i$ is the decomposition and group for u_i/v. Also $H_i = G_i \cap H$ is the decomposition group for u_i/w_i.

Again we can use Mackey's theorem.

$$\mathrm{Res}_{G_1} V \cong \bigoplus_{i=1}^{g} (\mathrm{Ind}_{G_1 \cap \tau_i H \tau_i^{-1}}^{G_1} \tau_i W).$$

We know the dimension of the trivial component is not going to affected by conjugation. Therefore, $L_v(s, V, L/K) = \prod_{i=1}^{g} L_v(s, \mathrm{Ind}_{H_i}^{G_i} W, L/L^{G_1})$. So we have reduced to the situation $g = 1$.

In this case we now have a tower of primes $u/w/v$. We need to split into cases on whether they are complex or real primes. If v and w are both complex or both real, then the induction from $H = G$ and the induction is trivial. So the only remaining case is when v is real w is complex, and thus u is also complex.

Now W is some multiple of the trivial representation of the trivial group H. Thus, $V = \mathrm{Ind}_H^G W = \dim(W) \mathrm{Ind}_H^G \chi_0$ where χ_0 is the trivial representation. Hence, the induced representation of a trivial representation on the trivial subgroup is the regular representation. So, $V = \dim(W)\chi_+ + \dim(W)\chi_-$. By definition $L_w(H, s) = \Gamma_{\mathbb{C}}^{\dim(W)}$. Therefore,

$$\begin{aligned} L_v(G, s) &= \Gamma_{\mathbb{R}}(s)^{n_+(u)} \Gamma_{\mathbb{R}}(s+1)^{n_-(u)} = \Gamma_{\mathbb{R}}(s)^{\dim(W)} \Gamma_{\mathbb{R}}(s+1)^{\dim(W)} \\ &= \Gamma_{\mathbb{C}}^{\dim(W)} = L_w(H, s). \end{aligned}$$

Therefore, in the special case of $g = 1$, the local factors at infinite primes are preserved under induction. Hence for any g the local factors at infinity are preserved under induction. □

2.7 Background for the Artin Conductor: Local Class Field Theory and the Theory of Higher Ramification Groups

2.7.1 Introduction

Thus far, we have followed out our program for completing the Artin L-function to give a formula for both the local factors at the ramified finite primes and the infinite primes. The only remaining part of the completed L-function is the exponential factor. In order to generalize the exponential factor to the non-abelian situation, we need to have a definition of the conductor of a character of a (possibly non-abelian) Galois group. This turns out to be significantly more difficult than the previous parts. In this section, we introduce the theory of higher ramification groups which will be necessary to define the Artin conductor. Although it is not strictly necessary, the language of local fields and the corresponding local class field theory will be very helpful in defining the Artin conductor. Since these results are rather difficult we will simply summarize them, for a more thorough treatment of these ideas see Serre's *Local Fields* [**Se2**].

2.7.2 Valuations and Discrete Valuation Rings

Recall from Definition 1.6.7 that we define an absolute value on a field by

Definition 2.7.1. *If K is a field, we define an absolute value $|\cdot|$ on K to be a map from K to the nonnegative real numbers with the following properties:*

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$

Aside from the obvious absolute values given by the real and complex embeddings, we also had the $\mathfrak{p}$-adic absolute values.

Definition 2.7.2. *Suppose $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$. If a is in $\mathcal{O}_K$, we define $ord_{\mathfrak{p}}(a)$ to be the highest power of $\mathfrak{p}$ dividing a. Then we define the $\mathfrak{p}$-adic absolute value of an algebraic integer to be $|(a)|_{\mathfrak{p}} = N\mathfrak{p}^{-ord_{\mathfrak{p}}(a)}$. This can be extended to all of K by taking quotients.*

The $\mathfrak{p}$-adic absolute value gives us a metric on K and thus we can take its completion with respect to this metric. This new ring is called the $\mathfrak{p}$-adic numbers and will be denoted $K_{\mathfrak{p}}$. The crucial fact about these rings is that they are principal ideal domains with a unique non-zero prime ideal. Thus, by replacing K by $K_{\mathfrak{p}}$ we can restrict our attention to a single prime of K and not have to worry about the others. To see this, we generalize the $\mathfrak{p}$-adic absolute value.

Definition 2.7.3. *A discrete valuation of a field K is a homomorphism $v : K^{\times} \to \mathbb{Z}$ which is surjective and has $v(x + y) \geq \min(v(x), v(y))$.*

Obviously $\text{ord}_{\mathfrak{p}}$ gives a discrete valuation on K. Furthermore, if v is a discrete valuation then for any real number r between 0 and 1, $|x| = r^{v(x)}$ is an absolute value.

Definition 2.7.4. *If K is a field with a valuation v, then we call its ring of v-integers $A_v = \{k \in K : v(k) \geq 0\}$ which is called a discrete valuation ring.*

Proposition 2.7.5. *cf. [**Se2**, Chapter 1, Prop. 1] A is a discrete valuation ring if and only if it is a principal ideal domain that has a unique non-zero prime ideal (π).*

Proof. Firstly, suppose we have an A which is a principal ideal domain with a unique non-zero prime ideal π. Let K be the field of fractions of A. By assumption, every element of A can be written in the form $a = u\pi^k$, where u is a unit and k is a non-negative integer. Then, we define the π-adic valuation

of an element of A to be $v(u\pi^k) = k$ and extend this to all of K by multiplicativity. Since $v(\pi^k) = k$, this is surjective. To see the second condition, notice that if $a \geq b$,

$$u_1\pi^a + u_2\pi^b = (u_1\pi^{a-b} + u_2)\pi^b.$$

$(u_1\pi^{a-b} + u_2)$ is in A. Therefore, it can be written in the form $u\pi^k$ for $k \geq 0$. Therefore, $u_1\pi^a + u_2\pi^b = u\pi^k\pi^b$. Hence,

$$v(u_1\pi^a + u_2\pi^b) = v(u\pi^k\pi^b) \geq b = \max(v(u_1\pi^a), v(u_2\pi^b)).$$

On the other hand, suppose we have some K with a valuation v. Let π be any element such that $v(\pi) = 1$. Every $x \in A_K$ can be written in the form $x = \pi^n u$ with $n = v(x)$ and $v(u) = 0$. Therefore, $v(u^{-1}) = -0 = 0$, hence $u^{-1} \in \mathcal{O}_K$. Hence, every ideal of A_K can be written in the form $\pi^k A_K$ which shows that $\mathcal{O}_K$ is a principal ideal domain with a unique non-zero prime ideal π. □

Definition 2.7.6. *An element π of a discrete valuation ring A is called a uniformizer if it generates the unique non-zero prime ideal.*

So suppose A is some discrete valuation ring with valuation v, uniformizer π, and field of fractions K (notice that here K is not a number field). Any valuation gives us an absolute value and every absolute value gives a topology on K. Thus, we can take the completion of K with respect to this topology. The valuation v extends to this completion in the obvious way (the valuation of a cauchy sequence is the limit of the valuations). This completion will be denoted $\hat{K}$, and the closure of A in this ring will be denoted $\hat{A}$. The ideals of the form $(\pi)^n$ form a base for the neighborhoods of zero in K, therefore they also form a base for neighborhoods of zero in A.

Proposition 2.7.7. *cf. [**Se2**, p. 27]*

$$\hat{A} = \varprojlim A/\pi^n A,$$

where here by equality we mean that there is a natural map from one to the other is an isomorphism as topological groups where on the latter space we take the limit of the discrete topology in each component.

Proof. We have a natural homomorphism $f : A \to \varprojlim A/\pi^n A$. If we have some Cauchy sequence (a_n) in A, then for some subsequence of (a_n), call it (b_n), we have for all $i, j \geq n$ $\pi^k | (b_i - b_j)$. Thus $f(b_n)$ is a sequence of elements if A which is constant in the $A/\pi^m A$ component for all $m > n$. Therefore, this sequence converges in $\varprojlim A/\pi^n A$, and we have a natural map $f : \hat{A} \to \varprojlim A/\pi^n A$. To see that this is surjective, suppose we have some element a in $\varprojlim A/\pi^n A$ whose nth component is a_n. We can take some element $b_n \in A$ such that $a_n = f(b_n)$. Furthermore, for $i, j > n$ we have $a_i \cong a_j \pmod{\pi^n}$, and thus b_n is a cauchy sequence in A, and its limit in $\hat{A}$ is a preimage of a. Therefore, the map f is also surjective. □

Our key example will be the field of $\mathfrak{p}$-adic numbers, $K_\mathfrak{p}$.

Definition 2.7.8. *Suppose that K is a number field. Then we have the $\mathfrak{p}$-adic valuation on K defined above. The completion of K with respect to this valuation is denoted $K_\mathfrak{p}$, and the closure of $\mathcal{O}_K$ will be called the $\mathfrak{p}$-adic integers and written $\mathcal{O}_\mathfrak{p}$ (K is left implied since it will be specified by giving $\mathfrak{p}$).*

2.7.3 Extensions of $\mathfrak{p}$-adic Fields

Most of the concepts which we introduced for number fields can be redefined in the context of the $\mathfrak{p}$-adic fields. Suppose that $L_\mathfrak{P}/K_\mathfrak{p}$ is some extension of $\mathfrak{p}$-adic fields.

Proposition 2.7.9. *If L/K is Galois with $Gal(L/K) = G$, then $Gal(L_\mathfrak{P}/K_\mathfrak{p}) = G_\mathfrak{P}$ the decomposition group of $\mathfrak{P}$.*

Proof. Since $L \subset L_\mathfrak{P}$ we get a map $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$ by restriction. Furthermore, this map is an injection since any automorphism which is trivial on L must, by continuity, be trivial on all of $L_\mathfrak{P}$. Lastly we need to show that the image of this map is $G_\mathfrak{P}$. That is to say, we must show that every element of $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ fixes $\mathfrak{P}$. But for any $\sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ we must have $\sigma\mathfrak{P}$ is a prime ideal in $L_\mathfrak{P}$, which leaves only one choice $\sigma\mathfrak{P} = \mathfrak{P}$, exactly as we had hoped. □

Definition 2.7.10. *Suppose $L_\mathfrak{P}/K_\mathfrak{p}$ is an extension of $\mathfrak{p}$-adic fields. Let $M_\mathfrak{q}$ be the Galois closure of $L_\mathfrak{p}$. Take $G = Gal(M_\mathfrak{q}/K_\mathfrak{p})$ and $H = Gal(M_\mathfrak{q}/L_\mathfrak{P})$. Thus G/H is identified with the embeddings of $L_\mathfrak{P}$ into $M_\mathfrak{q}$ which preserve $K_\mathfrak{p}$. Let,*

$$N_{L_\mathfrak{P}/K_\mathfrak{p}}\alpha = \prod_{\sigma \in G/H} \sigma(\alpha).$$

Definition 2.7.11.

$$Tr_{L_\mathfrak{P}/K_\mathfrak{p}}\alpha = \sum_{\sigma \in G/H} \sigma(\alpha).$$

Just as in the number field case, we get that the norm and trace preserve integers, that they behave well in extensions, and that the $N_{K_\mathfrak{p}/\mathbb{Q}_p}(a) = K_\mathfrak{p}/(a)$. Notice that since all ideals in a $\mathfrak{p}$-adic field are principal there is no need to go through the same definitions for ideals.

Definition 2.7.12. *If $L_\mathfrak{P}/K_\mathfrak{p}$ is an extension of $\mathfrak{p}$-adic fields, let $e_\mathfrak{P} = v_\mathfrak{P}(\mathfrak{p}\mathcal{O}_\mathfrak{P})$, and let $f_\mathfrak{P} = [\mathcal{O}_\mathfrak{P}/\mathfrak{P} : \mathcal{O}_\mathfrak{p}/\mathfrak{p}]$.*

These agree with the definition of the ramification degree and the local field degree in the number field case. Thus, in the Galois case, we have $e_\mathfrak{P} f_\mathfrak{P} = |G_\mathfrak{P}| = [L_\mathfrak{P} : K_\mathfrak{p}]$. Since e, f, and the degree of the extension all behave well in towers, by applying this theorem to $M_\mathfrak{q}/L_\mathfrak{P}$ and $M_\mathfrak{q}/K_\mathfrak{p}$ where $M_\mathfrak{q}$ is the Galois closure, we get that $e_\mathfrak{P} f_\mathfrak{P} = [L_\mathfrak{P} : K_\mathfrak{p}]$ in the non-Galois case as well.

Definition 2.7.13. *If $L_\mathfrak{P}/K_\mathfrak{p}$ is an extension of $\mathfrak{p}$-adic fields, then we define the relative discriminant of a basis $e_1, \ldots, e_n$ of $L_\mathfrak{P}/K_\mathfrak{p}$ to be*

$$\mathfrak{d}(e_1, \ldots, e_n) = (\det(\sigma(e_i))^2$$

(where σ ranges over all cosets of the Galois group of the Galois closure as in the last few definitions).

Just as before we get that $\mathfrak{d}(e_1, \ldots, e_n) = \det(\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(e_i e_j))$. Furthermore, we also have the same change of basis formula and so the discriminant of the ring of integers is well-defined and we will call it $\mathfrak{d}_{L_\mathfrak{P}/K_\mathfrak{p}}$.

Notice that the discriminant $\mathfrak{d}_{L_\mathfrak{P}/K_\mathfrak{p}}$ is an ideal of $K_\mathfrak{p}$ and thus of the form $\mathfrak{p}^k$ for some non-negative integer k.

Proposition 2.7.14. *Suppose that $\mathfrak{d}_{L_\mathfrak{P}/K_\mathfrak{p}} = \mathfrak{p}^{k_\mathfrak{P}}$, then*

$$\mathfrak{d}_{L/K} = \prod_\mathfrak{P} \mathfrak{p}^{k_\mathfrak{P}}$$

where the product is taken over all primes of L and $\mathfrak{p} = \mathfrak{P} \cap K$.

Proof. [**N**, Chapter III, 2.11]. □

Just like the global discriminant, the local discriminant has a formula for its behavior in towers of extensions.

Proposition 2.7.15. *If we have a tower of extensions $L_\mathfrak{P}/M_\mathfrak{q}/K_\mathfrak{p}$, then*

$$\mathfrak{d}_{L_\mathfrak{P}/K_\mathfrak{p}} = (\mathfrak{d}_{M_\mathfrak{q}/K_\mathfrak{p}})^{[L_\mathfrak{P}:M_\mathfrak{q}]} N_{M_\mathfrak{q}/K_\mathfrak{p}}(\mathfrak{d}_{L_\mathfrak{P}/M_\mathfrak{q}})$$

Proof. For a proof see [**Se2**, Prop. 8, p. 51]. □

2.7.4 Computing Ramification Degrees

We shall need several tools for finding which primes ramify in some extension and computing their degrees of ramification. Before doing so, let us change notation. Now we will let L and K denote $\mathfrak{p}$-adic fields with primes $\mathfrak{P}$ and $\mathfrak{p}$ respectively, and completely ignore any number field from which they might have come. $\mathfrak{p}$-adic fields will be called local, while the number fields will be called global.

Proposition 2.7.16. *L/K is ramified if and only if $\mathfrak{d}_{L/K} \neq \mathcal{O}_K$.*

Proof. See [**Se2**, Chapter III §5]. □

Definition 2.7.17. *A monic polynomial f with coefficients in $\mathcal{O}_K$ is Eisenstein (for the prime $\mathfrak{p}$) if all of the non-leading coefficients are divisible by $\mathfrak{p}$ but the constant coefficient is not divisible by $\mathfrak{p}^2$.*

It was known classically that Eisenstein polynomials are irreducible, but they also have another importance.

Proposition 2.7.18. *Suppose we have an extension of local fields L/K with $L = K(\alpha)$ for some integer α. Let f be the minimal polynomial of α over $\mathcal{O}_K$. If $f(x)$ is an Eisenstein polynomial (for the prime $\mathfrak{p}$), then the extension is totally ramified.*

Proof. See [**Se2**, Chapter I §6] . □

For example, this theorem allows us to verify our earlier claim that the prime $(i+1)$ ramifies in the extension $\mathbb{Q}(i, \sqrt{1+2i})/\mathbb{Q}(i)$.

Proposition 2.7.19. *The prime $(i+1)$ ramifies in the extension $\mathbb{Q}(i, \sqrt{1+2i})/\mathbb{Q}(i)$.*

Proof. Let $\mathfrak{p} = (1+i)$ and $\mathfrak{P}$ be some prime dividing $\mathfrak{p}$ in $\mathbb{Q}(i, \sqrt{1+2i})$. Let $K = Q(i)_{\mathfrak{p}}$ and $L = \mathbb{Q}(i, \sqrt{1+2i})_{\mathfrak{P}}$. Since $i(1+2i) = -2+i$, $L = K(\sqrt{1+2i}) = K(\sqrt{-2+i}) = K(i+\sqrt{-2+i})$. Since the minimal polynomial of $\sqrt{-2+i}$ is x^2+2-i, the minimal polynomial of $i+\sqrt{-2+i}$ is $x^2-2ix+(1-i)$. But since $-2i = (1+i)(-1-i)$ and $(1-i) = -i(1+i)$, $x^2-2ix+(1-i)$ is Eisenstein for $\mathfrak{p} = 1+i$. Therefore, $1+i$ totally ramifies in the extension $\mathbb{Q}(i, \sqrt{1+2i})/\mathbb{Q}(i)$. □

Proposition 2.7.20. *If L/K is a extension of local fields, $a \in \mathcal{O}_K$ generates the residue field extension $(L/\mathfrak{P})/(K/\mathfrak{p})$, and π is any uniformizer of L, then $\mathcal{O}_L = \mathcal{O}_K[a]$ or $\mathcal{O}_L = \mathcal{O}_K(a+\pi)$.*

Proof. [**L1**, Prop. 3, p. 59]. □

In particular, we see that we can always find $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Furthermore, if L/K is totally ramified, then $(L/\mathfrak{P})/(K/\mathfrak{p})$ is trivial and $\mathcal{O}_L = \mathcal{O}_K[\pi]$.

2.7.5 Higher Ramification Groups

In order to better understand the way in which primes ramified, Hilbert introduced the notion of a higher ramification group. These generalize the notion of an inertia group. Suppose L/K is a Galois extension of local fields with Galois group G (recall this is the decomposition group of the corresponding global extension) and primes $\mathfrak{P}$ and $\mathfrak{p}$ respectively.

Definition 2.7.21. *Let the ith ramification group G_i be the subgroup of G which acts trivially on $\mathcal{O}_L/\mathfrak{P}^{i+1}$.*

By convention we will let $G_{-1} = G$ the decomposition group. Notice that G_0 is the inertia group. Also, since $\mathcal{O}_L = \varprojlim \mathcal{O}_L/\mathfrak{P}^{i+1}$, for i sufficiently large we must have that $G_i = 1$. Thus, the G_i give a filtration of the decomposition group G.

Definition 2.7.22. *Suppose that we have some $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$. Let $i_G(g) = v_L(g(\alpha)-\alpha)$. If g is not equal to 1, then this is a positive integer. If $g = 1$ then $i_G(1) = +\infty$.*

Proposition 2.7.23. *The function i_G has the following properties:*

1. $i_G(g) \geq i+1$ *if and only if* $g \in G_i$
2. $i_G(tst^{-1}) = i_G(s)$
3. $i_G(st) = \min(i_G(s), i_G(t)$

Proof. [**Se2**, p. 62]. □

These ramification groups behave well with respect to subgroups.

Proposition 2.7.24. *If H is a subgroup of G, then it corresponds to some intermediate extension L/M. $G_i \cap H = H_i$ and $i_H(h) = i_G(h)$ for all $h \in H$.*

Proof. The first claim is obvious. The second claim follows from Proposition 2.7.23. □

We would like to have an analogous result for quotients. There is a nice formula relating i_G to $i_{G/H}$.

Proposition 2.7.25. *Suppose that H is a normal subgroup of G, then for each $\sigma \in G/H$,*

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K}} \sum_{g \in \sigma H} i_G(g).$$

Proof. [**Se2**, p. 63]. □

Translating this result into a result concerning the higher ramification groups, however, takes a bit more work. To this end Herbrand defined the following functions:

Definition 2.7.26. *If $m \geq -1$ is an integer, then let $\phi_{L/K}(m) = \sum_{i=1}^{m} |G_i|$. Extend $\phi_{L/K}$ to a function on all real numbers by linearly interpolating. Let $\psi_{L/K}$ be its inverse map (which exists since $\phi_{L/K}$ is strictly increasing).*

Theorem 2.7.27 (Herbrand's Theorem).

$$G_u H/H = (G/H)_{\phi_{L/K}(u)}.$$

Proof. [**Se2**, p. 75]. □

Definition 2.7.28. *Define the upper numbering of the ramification groups to be $G^v = G_{\psi(v)}$.*

Notice that, $G^{\phi(u)} = G_u$.
By Herbrand's theorem, we have

Corollary 2.7.29 (Herbrand).

$$(G/H)^v = G^v H/H.$$

Notice that the upper numbered ramification groups G^v might have jumps at non-integer points. For example, if we have L/K with $\mathrm{Gal}(L/K)$ the quaternion group, then there is a jump at $v = \frac{3}{2}$. However, in the abelian case this never happens.

Theorem 2.7.30 (Hasse-Arf). *If G is an abelian group and if v is a jump in the filtration G^v, then v is an integer. That is to say, if $G_i \neq G_{i+1}$, then $\phi(i)$ is an integer.*

Proof. [**Se2**, Chapter V §7], [**Se2**, Thm. 1, p. 227], or [**N**, Chapter V, Prop. 6.3]. □

i_G has one more property which we will require.

Proposition 2.7.31. *cf. [**Se2**, Prop 3, p. 63]*

$$f_{L/K} \sum_{s \neq 1} i_G(s) = v_K(\mathfrak{d}_{L/K})$$

Proof. By Proposition 2.7.20, we can choose α such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Thus, the discriminant is $\mathfrak{d}_{L/K} = (\det(\sigma(\alpha^k))^2$. This is just the Vandermonde determinant. Thus,

$$\mathfrak{d}_{L/K} = \prod_{g_1 \neq g_2 \in G} (g_1(\alpha) - g_2(\alpha)).$$

Now, $(g_1(\alpha) - g_2(\alpha)) = g_1(\alpha - g_1^{-1}g_2(\alpha))$. Therefore, taking $g = g_1$ and $s = g_1^{-1}g_2$,

$$\mathfrak{d}_{L/K} = \prod_{g \in G} g\left(\prod_{s \neq 1}(\alpha - s(\alpha))\right) = N_{L/K}\prod_{s \neq 1}(\alpha - s(\alpha)).$$

Thus, taking v_k of both sides,

$$v_K(\mathfrak{d}_{L/K}) = v_K N_{L/K}\prod_{s \neq 1}(\alpha - s(\alpha)) = f_{L/K}\sum_{s \in G} v_L(\alpha - s(\alpha)) = f_{L/K}\sum_{s \neq 1} i_G(s).$$

□

2.7.6 Local Class Field Theory

Just as in the global case there is a description of all abelian extensions of a local field K in terms of purely internal objects which is explicitly given by a reciprocity law. In all that follows, L/K is an abelian extension of $\mathfrak{p}$-adic fields.

Theorem 2.7.32. *$NL^\times$ is a closed subgroup of finite index of $K^\times$. Furthermore, no two abelian extensions have the same norm group $NL^\times$.*

Theorem 2.7.33. *If C is any closed subgroup of $K^\times$, then there exists some abelian extension L/K with $NL^\times = C$.*

Theorem 2.7.34. *If L/K is an abelian extension with Galois group G, then there exists a natural reciprocity homomorphism $\omega_{L/K} : K^\times \to G$ which is surjective and has kernel $NL^\times$. This map is natural in the sense that if M is an intermediate field with $Gal(L/M) = H$, then $\omega_{L/K} \to G \to G/H$ agrees with $\omega_{M/K}$. Furthermore, this map agrees with the global reciprocity map in sense that if L/K is unramified, then $\omega_{L/K}(x) = \varphi_{\mathfrak{P}/\mathfrak{p}}^{v_K(x)}$.*

For the construction of this map see, [**Se2**, Chapter XIII], [**N**, Chapter V], or Serre's article [**C-F**, Chapter VI].

There is a much deeper connection between local class field theory and global class field theory which was discovered by Chevalley who introduced the notion of idèles. This allowed him to derive global class field theory from local class field theory. For more on this connection see [**N**, Chapter VI].

2.7.7 The Reciprocity Map and Filtrations

Notice that, if K is a local field with uniformizer π, then every element of $K^\times$ can be written uniquely in the form $u\pi^k$ for k an integer and $u \in \mathcal{O}_K^\times$. Thus, $K^\times \cong \mathcal{O}_K^\times \oplus \mathbb{Z}$. Further suppose that we have an abelian field extension L/K. We have the norm map $N : L \to K$. Take π_L and π_K uniformizers of the respective fields. Then, if we choose π_K properly, the norm map can be decomposed into a map $N : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ and $N : \mathbb{Z} \to \mathbb{Z}$. By the definition of the residue field degree, the latter map is just multiplication by f. So in order to understand the norm map it is enough to understand what it does to units. In order to do this, we study a natural filtration of the group of units.

Definition 2.7.35. *Let $U_K = U_K^0$ be the units $\mathcal{O}_K^\times$ and let $U_K^i = 1 + \mathfrak{p}^k$.*

Notice that, since $U_K = \varprojlim(\mathcal{O}_K/\pi^k\mathcal{O}_K)^\times$, $U_K/U_K^1 = (\mathcal{O}_K/\mathfrak{p})^\times$ and $U_K^i/U_K^{i+1} = \mathcal{O}_K/\mathfrak{p}$ for $i \geq 1$.

This filtration of U_K gives us a filtration of U_K/NU_L:

$$\ldots \hookrightarrow U_K^n/(NL^\times \cap U_K^n) \hookrightarrow \ldots \hookrightarrow U_K^2/(NL^\times \cap U_K^2) \hookrightarrow U_K^1/(NL^\times \cap U_K^1) \hookrightarrow K^\times/NL^\times. \tag{2.7.1}$$

Definition 2.7.36. *If i is the smallest integer such that $U_K^i/(U_K^i \cap NU_L) = 1$, then we define $\mathfrak{f}_\mathfrak{p} = \mathfrak{p}^i$ the local conductor of L/K.*

Just as before we can define the conductor of a character of the class group to be the character of the subextension for which it is primitive.

Proposition 2.7.37. *The finite part of the Global conductor is $\mathfrak{f}_{L'/K'}$ is $\prod_\mathfrak{p} \mathfrak{f}_\mathfrak{p}$.*

Proof. One direction is easy: if every $a \equiv 1 \pmod{\mathfrak{f}}$ is a norm down from L', then if we localize at $\mathfrak{p}$, $u \equiv 1 \pmod{\mathfrak{a}}$ implies that $u \in NU_{L_\mathfrak{P}}$.

To prove the other direction takes a bit more work. Essentially it depends on the deep connection between the local reciprocity symbol and the global one. Since the principal part of the kernel of the global reciprocity map is exactly those things which are 1 modulo the conductor and since the global reciprocity map can be built up from the local ones, this result follows. cf. [**Se2**, Appendix, pp. 221-222]. □

The reciprocity map gives us an isomorphism $K^\times/NL^\times \to G$, but we would like to be able to restrict our attention to the units.

Proposition 2.7.38. *The reciprocity map $\omega_{L/K}$ sends U_K onto the inertia group G_0.*

Proof. [**Se2**, p. 198]. □

By the reciprocity isomorphism, we would expect the filtration of U_K/NU_L to correspond with some filtration of the inertia group G_0. We have two natural candidates for such a filtration: G_i and G^i. Recall that the major difference between these two filtrations is that the former is well-behaved under subgroups while the latter is well-behaved under quotients. Notice that the filtration in Equation 2.7.1 is well behaved with respect to quotient groups, because it is indexed by the filtration of $K^\times$, not by the filtration of $L^\times$. Hence, one might conjecture that the filtration in Equation 2.7.1 corresponds under the reciprocity isomorphism to the filtration given by upper numbering.

Theorem 2.7.39. *We have the following canonical isomorphism of filtrations given by the reciprocity isomorphism:*

$$\begin{array}{ccccccccccc}
1 & \hookrightarrow & U_K^n/U_L^{\psi(n)} & \hookrightarrow & \dots & \hookrightarrow & U_K^2/U_L^{\psi(2)} & \hookrightarrow & U_K^1/U_L^{\psi(1)} & \hookrightarrow & K^\times/NL^\times \\
= & & = & & & & = & & = & & = \\
1 & \hookrightarrow & U_K^n/(NL^\times \cap U_K^n) & \hookrightarrow & \dots & \hookrightarrow & U_K^2/(NL^\times \cap U_K^2) & \hookrightarrow & U_K^1/(NL^\times \cap U_K^1) & \hookrightarrow & K^\times/NL^\times \\
\downarrow \omega & & \downarrow \omega & & & & \downarrow \omega & & \downarrow \omega & & \downarrow \omega \\
1 & \hookrightarrow & G^n & \hookrightarrow & \dots & \hookrightarrow & G^1 & \hookrightarrow & G^0 & \hookrightarrow & G^{-1} \\
= & & = & & & & = & & = & & = \\
1 & \hookrightarrow & G_{\psi(n)} & \hookrightarrow & \dots & \hookrightarrow & G_{\psi(1)} & \hookrightarrow & G_{\psi(0)} & \hookrightarrow & G_{\psi(-1)}
\end{array}$$

Proof. [**Se2**, Chapter XV §2]. □

2.8 The Artin Conductor

2.8.1 Introduction

Recall from Hecke's work that the completed abelian L-functions have three parts: the Euler factors at the finite primes, the Euler factors at the infinite primes, and an exponential factor involving the conductor. In previous sections we have generalized the first two parts to non-abelian groups. In this section we generalize the third part. Furthermore, in the abelian case, the conductor factors as a product of local conductors each of which correspond to one of the primes that ramify. In this section, we will describe how the concept of the conductor of an abelian character generalizes to the Artin conductor of a Galois representation, and show how this gives us a convenient formula for the exponential factor of an Artin L-series. Our treatment is roughly based on [**Se2**, Chapter VI].

In analogy with the generalization we have already made, we want a new factor which depends on some local extension L/K and a representation of its Galois group G, and which has the following properties:

1. The new factor in the completed L-function should agree with our old definition for representations of abelian groups.
2. If V is trivial on some normal subgroup $H \lhd G$, then the new factor in our L-function should be unchanged if we consider V as a representation of G/H the Galois group of the extension L/K^H.
3. The new term for the sum of two representations should be the product of the terms for each of the representations.
4. Each of these terms should be unchanged if we replace a representation by its induced representation to some larger Galois group.

The old exponential factor was $(|\mathfrak{d}_{K/\mathbb{Q}}|N(\mathfrak{f}(\chi;L/K))^{s/2}$. By looking at representations which are sums of one-dimensional representations it is clear that this should generalize to something of the form $(|\mathfrak{d}_{K/\mathbb{Q}}|^{\dim V}N(\mathfrak{f}(V;L/K))^{s/2}$. So, our objective is to show the following theorem:

Theorem 2.8.1. *There exists a natural number valued function $f_{\mathfrak{p}}(V;L/K)$ (where L/K is a ramified Galois extension of local fields and V is a representation of the Galois group $G = Gal(L/K)$, and $\mathfrak{p}$ is the prime in K) with the following properties:*

1. *If L/K is an abelian extension, then*

$$\mathfrak{p}^{f_{\mathfrak{p}}(V;L/K)} = \mathfrak{f}_{\mathfrak{p}}(\chi;L/K),$$

   where χ is the Dirichlet character corresponding to V under the isomorphism given by class field theory and $\mathfrak{f}_{\mathfrak{p}}$ is the abelian conductor.

2. *If V is trivial on some normal subgroup $H \lhd G$, then $f_{\mathfrak{p}}(V;L/K) = f_{\mathfrak{p}}(V;L^H/K)$.*
3. *If V_1 and V_2 are two representations of G, then $f_{\mathfrak{p}}(V_1+V_2;L/K) = f_{\mathfrak{p}}(V_1;L/K) + f_{\mathfrak{p}}(V_2;L/K)$.*
4. *Consider a tower of fields $L/M/K$ with $G = Gal(L/K)$, $H = Gal(L/M)$, and W a representation of H with $V = Ind_H^G W$. Then,*

$$f_{\mathfrak{p}}(V) = v_K(\mathfrak{d}_{M/K})\dim W + f_{M/K}f_{\mathfrak{q}}(W),$$

   where $\mathfrak{q}|\mathfrak{p}$ is a prime in M, v_K is the local valuation, $\mathfrak{d}_{M/K}$ is the discriminant, and $f_{M/K}$ has nothing to do with our function f but denotes the degree of the residue field extension. (This complicated formula comes from the formula relating discriminants in towers.)

2.8.2 Reformulating the Abelian Conductor

The conductor in the abelian case was defined in terms of the Dirichlet character, not in terms of the a representation of the Galois group. So to generalize this notion to the non-abelian case we first need to find a new definition of the conductor in the abelian case in terms of the Galois group. Since the abelian conductor is the product of the local conductors we will look at the local case. So consider L/K a ramified extension of local fields with prime ideals $\mathfrak{P}$ and $\mathfrak{p}$ respectively.

Recall that if $\mathfrak{p}$ is a prime in K dividing $\mathfrak{P}$ a prime in L, then the local conductor is the smallest power $\mathfrak{p}^k$ such that χ acts trivially on $U_K^k/(NL^\times \cap U_K^k)$. Equivalently, the conductor is the number of terms in the filtration

$$1 \hookrightarrow U_K^n/(NL^\times \cap U_K^n) \hookrightarrow \ldots \hookrightarrow U_K^2/(NL^\times \cap U_K^2) \hookrightarrow U_K^1/(NL^\times \cap U_K^1) \hookrightarrow K^\times/NL^\times, \tag{2.8.1}$$

on which χ acts nontrivially. Recall that the reciprocity isomorphism from local class field theory transforms this filtration of $K^\times/NL^\times$ into a filtration of G_{-1} the decomposition group. By, Theorem 2.7.39

$$\begin{array}{ccccccccccc} 1 & \hookrightarrow & U_K^n/U_L^{\psi(n)} & \hookrightarrow & \ldots & \hookrightarrow & U_K^2/U_L^{\psi(2)} & \hookrightarrow & U_K^1/U_L^{\psi(1)} & \hookrightarrow & K^\times/NL^\times \\ \downarrow \omega & & \downarrow \omega & & & & \downarrow \omega & & \downarrow \omega & & \downarrow \omega \\ 1 & \hookrightarrow & G_{\psi(n)} & \hookrightarrow & \ldots & \hookrightarrow & G_{\psi(1)} & \hookrightarrow & G_{\psi(0)} & \hookrightarrow & G_{\psi(-1)} \end{array}$$

This allows us to restate the definition of the abelian conductor in terms of the ramification groups instead of the class groups.

Theorem 2.8.2. *If c is the largest integer such that V acts nontrivially on G_c, then $\mathfrak{p}^{\phi(c)+1} = \mathfrak{f}_\mathfrak{p}(\chi)$*

Proof: By the Hasse-Arf theorem (Theorem 2.7.30), since $G_c \neq G_{c+1}$, $\phi(c) \in \mathbb{Z}$. By the correspondence in Theorem 2.7.39, the non-trivial action of V on $G_c = G^{\phi(c)}$ corresponds to a non-trivial action of χ on $U_K^{\phi(c)}/(NL^\times \cap U_K^{\phi(c)})$. Similarly since V acts trivially on $G^{\phi(c)+1}$, by Theorem 2.7.39, χ acts trivially on $U_K^{\phi(c)+1}/(NL^\times \cap U_K^{\phi(c)+1})$. Hence by the definition of the abelian conductor, $\mathfrak{p}^{\phi(c)+1} = \mathfrak{f}_\mathfrak{p}(V)$. □

Corollary 2.8.3. *If V is a representation of the Galois group of dimension one corresponding to the Dirichlet character χ, $g_i = |G_i|$, and $h_i(V)$ is 1 iff V is a nontrivial representation of G_i, then*

$$\mathfrak{f}_\mathfrak{p}(\chi) = \mathfrak{p}^{\sum_{i=0}^\infty \frac{g_i}{g_0} h_i(V)}.$$

Proof: Here we have simply substituted the formula for ϕ. □

2.8.3 Generalizing the New Formula to Higher Dimensional Representations

Now that we have a formula for the conductor in the abelian case in terms of the Galois group, we can ask how this might generalize to higher dimensional representations. Since the formula for f should be additive, if V is a representation which is the direct sum of one-dimensional representatives, then we should have

$$f_\mathfrak{p}(V) = \sum_{i=0}^\infty \frac{g_i}{g_0} h_i(V),$$

where now $h_i(V)$ gives the number of nontrivial components of V as a representation of G_i. Notice that $h_i(V) = \operatorname{codim} V^{G_i} = \dim V - \dim V^{G_i}$. This gives us a definition which we can apply to any representation.

Definition 2.8.4. *Let*

$$f_\mathfrak{p}(V, L/K) = \sum_{i=0}^\infty \frac{g_i}{g_0} \operatorname{codim} V^{G_i}.$$

(At various times when it is convenient we will abuse notation by dropping the field extension or by replacing the representation by its character.)

In order to prove Theorem 2.8.1, we must prove that $f_{\mathfrak{p}}$ is natural number valued and satisfies conditions 1-4. In the last section we proved condition 1. Condition 2 is obvious since codim is additive. Conditions 3 and 4 take a bit more work.

The additivity condition and the induction condition suggest that $f_{\mathfrak{p}}$ might take the form of an inner product (a_G, χ), where a_G is some class function and χ is the character of V. (Notice that this usage of χ differs from the last section where we were only dealing with one-dimensional characters and used χ to denote the corresponding Dirichlet character.)

To this end notice that if 1_i, r_i, and u_i are the characters of the trivial representation, the regular representation, and the augmentation representation (respectively) of G_i, then

$$\begin{aligned}(1_i, \mathrm{Res}_{G_i}\chi) &= \dim V^{G_i} \\ (r_i, \mathrm{Res}_{G_i}\chi) &= \dim \mathrm{Res}_{G_i} V = \dim V \\ (u_i, \mathrm{Res}_{G_i}\chi) &= \mathrm{codim}\ V^{G_i}.\end{aligned}$$

Now we can apply Frobenius reciprocity to show,

$$(\mathrm{Ind}_{G_i}^{G} u_i, \chi) = \mathrm{codim}\ V^{G_i}.$$

Definition 2.8.5. *Let a_G be the class function*

$$a_G = \sum_{i=0}^{\infty} \frac{g_i}{g_0} Ind_{G_i}^{G} u_i.$$

Thus we have shown,

Theorem 2.8.6. $f_{\mathfrak{p}}(\chi) = (a_G, \chi)$

Before we can prove conditions 3 and 4 we will need one last characterization of the function f. Recall that $f_{L/K}$ is the degree of the residue field extension. We can rephrase the definition of a_G in terms of the function i_G (see Definition 2.7.22).

Theorem 2.8.7.

$$a_G(g) = \begin{cases} f_{L/K} \sum_{s \neq 1} i_G(s) & \text{if } g = 1 \\ -f_{L/K} i_G(g) & \text{if } g \neq 1 \end{cases}.$$

Proof: If $g \notin G_i$, then $\mathrm{Ind}_{G_i}^{G} u_i(g) = 0$. If $g \in G_i$, but $g \neq 1$, then

$$\mathrm{Ind}_{G_i}^{G} u_i(g) = -\frac{|G|}{g_i} = -f_{L/K}\frac{g_0}{g_i}.$$

Therefore, if $i_G(g) = k$ (i.e. for $g \in G_{k-1} - G_k$), then we have

$$a_G(g) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \mathrm{Ind}_{G_i}^{G} u_i = -\sum_{i=0}^{k} \frac{g_i}{g_0} f_{L/K} \frac{g_0}{g_i} = -k f_{L/K} = -i_G(g) f_{L/K}.$$

Hence we have proved this theorem for any $g \neq 1$. However, both $a_G(g)$ and the new formula are clearly class functions which are orthogonal to the trivial character. Therefore, since they are equal for all but one class, they must actually be equal everywhere. □

This gives us enough to prove properties 3 and 4.

Theorem 2.8.8. *If V is trivial on some normal subgroup $H \lhd G$, then $f_{\mathfrak{p}}(V; L/K) = f_{\mathfrak{p}}(V; L^H/K)$.*

Proof: Here we want to show that $(a_{G/H}, \chi)_{G/H} = (a_G, \chi)_G$. We know from Frobenius reciprocity that $(a_G, \chi)_G = (a_G^{\natural}, \chi)_{G/H}$. Hence we need only show that $a_{G/H} = a_G^{\natural}$. Since both of these class functions are clearly orthogonal to the trivial representation, it is enough to show that $a_{G/H}(g) = a_G^{\natural}(g)$ for all $g \in G/H - \{1\}$. By Theorem 2.8.7, this in turn is reduced to showing that $i_{G/H}(g) = i_G^{\natural}(g)$. This is just Proposition 2.7.25. □

Before proving property 4 we need the following lemma:

Lemma 2.8.9. *Suppose H is a subgroup of G with $L^H = M$. Let v_K be the local valuation, $\mathfrak{d}_{M/K}$ be the discriminant, r_H the character of the regular representation, and $f_{M/K}$ the degree of the residue field extension.*

$$Res_H a_G = v_K(\mathfrak{d}_{M/K}) r_H + f_{M/K} a_H$$

Proof: Suppose $s \neq 1$ is an element of H, then $a_G(s) = -f_{L/K} i_G(s) = -f_{L/M} f_{M/K} i_G(s)$. Also,

$$v_K(\mathfrak{d}_{M/K}) r_H(s) + f_{M/K} a_H(s) = 0 - f_{M/K} f_{L/M} i_H(s).$$

But, since $i_G(s) = i_H(s)$, we can conclude

$$a_G(s) = v_K(\mathfrak{d}_{M/K}) r_H(s) + f_{M/K} a_H(s).$$

Consider the remaining case, $s = 1$. By Proposition 2.7.31,

$$a_G(1) = f_{L/K} \sum_{s \neq 1} i_G(s) = v_k(\mathfrak{d}_{L/K}).$$

Similarly, $a_H(1) = v_M(\mathfrak{d}_{L/M})$. But, by Proposition 2.7.15,

$$\mathfrak{d}_{L/K} = (\mathfrak{d}_{M/K})^{[L:M]} N_{M/K}(\mathfrak{d}_{L/M}).$$

Taking v_K of both sides yields

$$a_G(1) = v_K(\mathfrak{d}_{L/K}) = [L : M] v_k(\mathfrak{d}_{M/K}) + f_{M/K} v_M(\mathfrak{d}_{L/M}) = v_K(\mathfrak{d}_{M/K}) r_H(1) + f_{M/K} a_H(1).$$

□

Theorem 2.8.10. *Consider a tower of fields $L/M/K$ with $G = Gal(L/K)$, $H = Gal(L/M)$, and W a representation of H with $V = Ind_H^G W$. Then,*

$$f_{\mathfrak{p}}(V) = v_K(\mathfrak{d}_{M/K}) \dim W + f_{M/K} f_{\mathfrak{q}}(W),$$

where $\mathfrak{q}|\mathfrak{p}$ is a prime in M.

Proof: Let χ denote the character of V and ψ the character of W. By Theorem 2.8.6 and Frobenius reciprocity, $f_{\mathfrak{p}}(\chi) = (a_G, \mathrm{Ind}_H^G \psi) = (\mathrm{Res}_H a_G, \psi)$. By Lemma 2.7.25, we get

$$f_{\mathfrak{p}}(\chi) = v_K(\mathfrak{d}_{M/K})(\psi, r_H) + f_{M/K}(\psi, a_H) = v_K(\mathfrak{d}_{M/K}) \dim W + f_{M/K} f_{\mathfrak{q}}(W).$$

□

Thus we have shown all four properties, all that remains to show is that the function $f_{\mathfrak{p}}$ is actually natural number valued.

Theorem 2.8.11. *$f_{\mathfrak{p}}(V; L/K)$ is a nonnegative integer.*

Proof: From the original definition it is clear that $f_{\mathfrak{p}}(V; L/K)$ is a positive rational number. By Brauer's theorem we can write $V = \sum_i c_i \mathrm{Ind}_{H_i}^G W_i$ for some subgroups H_i, integers c_i, and one dimensional representations W_i. By Theorem 2.8.10 and the fact that $f_{\mathfrak{p}}$ is additive we get,

$$\begin{aligned} f_{\mathfrak{p}}\left(\sum_i c_i \mathrm{Ind}_{H_i}^G W_i; L/K\right) &= \sum_i c_i f_{\mathfrak{p}}(\mathrm{Ind}_{H_i}^G W_i; L/K) \\ &= \sum_i c_i \left(v_K(\mathfrak{d}_{L^{w_i}/K}) \dim W_i + f_{L^{w_i}/K} f_{\mathfrak{q}_i}(W_i)\right). \end{aligned}$$

However, since W_i is one dimensional, we know that $f_{\mathfrak{q}_i}(W_i)$ is just the exponent in the local abelian conductor for some quotient extension, and hence must be an integer. Since $f_{\mathfrak{p}}(V; L/K)$ is both a nonnegative rational and an integer, the theorem follows. □

Thus, we have completed a proof of Theorem 2.8.1. Furthermore, we have the following corollary,

Corollary 2.8.12. *a_G is the character of a representation.*

Proof: a_G must be some linear combination of characters of irreducible representations. The coefficients can be recovered by considering (a_G, χ). Thus, Theorem 2.8.11 shows that a_G is a nonnegative integer linear combination of characters of irreducible representations. Hence a_G must be the character of some representation. □

Definition 2.8.13. *The local Artin representation is the representation whose character is the class function a_G.*

This only defines the Artin representation up to isomorphism. One can give the Artin representation a natural definition as a representation, however, to do so is far beyond the scope of this thesis.

2.8.4 The Global Artin Conductor

Now suppose that L/K is an extension of global fields with Galois group G. For $\mathfrak{P}$ any prime in L (sitting over some prime $\mathfrak{p} \in K$), we have a local extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ with Galois group $G_{\mathfrak{P}}$. Let $a_{\mathfrak{P}}$ be the local Artin representation for this local extension. Let $a_{\mathfrak{p}} = \mathrm{Ind}_{G_{\mathfrak{p}}}^{G} a_{\mathfrak{P}}$. This notation is justified since $a_{\mathfrak{p}}$ does not depend on the choice of $\mathfrak{P}$ over $\mathfrak{p}$. To see this, simply notice that G acts transitively by conjugation on the set of such $\mathfrak{P}$. If χ is a character of a representation of G, let $f(\chi, \mathfrak{p}) = (\chi, a_{\mathfrak{p}}) = f(Res_{D_{\mathfrak{P}}}\chi)$.

Definition 2.8.14. *Let*

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{f(\chi,\mathfrak{p})},$$

this function is called the global Artin conductor.

Theorem 2.8.15.

1. *$\mathfrak{f}(\chi + \chi') = f(\chi)f(\chi')$ and $\mathfrak{f}(1) = (1)$.*
2. *If M/K is a subextension with Galois group $H \subset G$, and if ψ is a character of H,*

$$\mathfrak{f}(Ind_H^G \psi, L/K) = \mathfrak{d}_{M/K}^{\psi(1)} N_{M/K}(\mathfrak{f}(\psi, L/M)).$$

3. *If H is a normal subgroup of G and χ is a character of G/H, then*

$$\mathfrak{f}(\chi, L/K) = \mathfrak{f}(\chi, L^H/K).$$

Proof: All of these follow immediately from Theorem 2.8.1. □

As an immediate corollary we get the famous Führerdiskriminantenproduktformel of Artin and Hasse.

Corollary 2.8.16 (Artin-Hasse).

$$\mathfrak{d}_{L/K} = \prod_{\chi \ irred.} \mathfrak{f}(\chi)^{\chi(1)}.$$

Proof: By Theorem 16, part 2, we find

$$\mathfrak{f}(r_G, L/K) = \mathfrak{f}(\mathrm{Ind}_1^G 1, L/K) = \mathfrak{d}_{L/K}.$$

But $r_G = \sum_{\chi \text{ irred.}} \chi(1)\chi$. Hence by the first part of Theorem 2.8.15,

$$\mathfrak{d}_{L/K} = \mathfrak{f}(r_G, L/K) = \prod_{\chi \text{ irred.}} \mathfrak{f}(\chi)^{\chi(1)}.$$

□

At long last, let us conclude with the formula for the exponential factor and give the formulas they satisfies. All of these claims follow quickly from Theorem 2.8.15.

Theorem 2.8.17. *Let $c(\chi, L/K)$ be the positive generator of the ideal*

$$\mathfrak{d}_{K/\mathbb{Q}}^{\chi(1)} N_{K/\mathbb{Q}}(\mathfrak{f}(\chi, L/K).$$

$c(\chi, L/K)^{s/2}$ is the exponential factor which appears in the extended Artin L-series given by Artin's theorem, and it has the following expected properties:

1. *$c(\chi + \chi'; L/K) = c(\chi; L/K)c(\chi'; L/K)$ and $c(1; L/K) = |\mathfrak{d}_{K/\mathbb{Q}}$.*
2. *$c(Ind_H^G \psi; L/K) = c(\psi; L/M))$.*
3. *$c(\chi; L/K) = c(\chi; M/K)$.*

Proof. This follows from the properties of the discriminant and the Artin conductor which we have already proven. □

2.9 The Functional Equation of the Artin L-function

Combining the results of this chapter we see that,

Definition 2.9.1. *For $\mathfrak{p}$ a finite prime we defined,*

$$L_{\mathfrak{p}}(s,\chi;L/K)=\det\left(Id-N\mathfrak{p}^{-s}\varphi_{\mathfrak{P}};V^{I_{\mathfrak{P}}}\right)^{-1}.$$

For $\mathfrak{p}$ an infinite prime we defined

$$L_v(s,V)=\begin{cases}\Gamma_{\mathbb{R}}(s)^{(\dim V^{G_w})}\Gamma_{\mathbb{R}}(s+1)^{(codim\ V^{G_w})} & \text{if } v \text{ is real}\\ \Gamma_{\mathbb{C}}(s)^{\chi(1)} & \text{if } v \text{ is complex}\end{cases}$$

Lastly, we defined the exponential factor to be $c(V;L/K)^{s/2}$, where $c(V;L/K)$ to be the positive generator of the ideal

$$\mathfrak{d}_{K/\mathbb{Q}}^{\dim V}N_{K/\mathbb{Q}}(\mathfrak{f}(V,L/K).$$

With these definitions, we have the completed Artin L-function

$$\Lambda(s,V;L/K)=c(V;L/K)^{s/2}\prod_{\mathfrak{p}}L_{\mathfrak{p}}(s,V;L/K),$$

where the product is taken over all primes both infinite and finite.

Theorem 2.9.2. *The complete Artin L-function has a meromorphic continuation to the entire complex plane which satisfies the functional equation*

$$\Lambda(s,V;L/K)=\varepsilon(V)\Lambda(1-s,V^*;L/K),$$

where V^* is the dual representation (see Definition 1.5.36 and Proposition 1.5.37), and $\varepsilon(V)$ is a constant with absolute value 1. In terms of the characters of these representations, we get

$$\Lambda(s,\chi;L/K)=\varepsilon(\chi)\Lambda(1-s,\bar{\chi};L/K).$$

Proof. By the results earlier in this chapter, $\log\Lambda$ is additive and preserved under induction. Furthermore, in the 1-dimensional case, this theorem follows from Hecke's result on abelian L-functions. Thus this result follows from Brauer's theorem. □

Chapter 3

Computing the Completed Artin L-functions for the Splitting Field of $x^3 - n$ over $\mathbb{Q}$

3.1 The Splitting Field of $x^3 - n$

3.1.1 Introduction

Let K be the splitting field of $x^3 - n$ over $\mathbb{Q}$ and let G the corresponding Galois group. In this chapter we calculate the Artin L-function for each character of G. Inspiration for many of these calculations comes from [**C2**], [**F-T**, Chapter VIII. §7.], and the end of Heilbronn's article [**C-F**, Chapter VIII].

In this section we make some general computations which will be useful in computing all of the parts of the L-function.

3.1.2 Representations of G and its Subgroups

Notice that $K = \mathbb{Q}(\sqrt[3]{n}, \omega)$ where $\omega = (-1 + \sqrt{-3})/2$ is a primitive cube root of unity.

Proposition 3.1.1. *The Galois group of K is $G \cong S_3$.*

Proof. In order to define an element of the Galois group it is enough to give its action on ω and $\sqrt[3]{n}$. Let x be the automorphism which sends $\omega \mapsto \omega^2$ and fixes $\sqrt[3]{n}$. Let y be the automorphism which sends $\sqrt[3]{n} \mapsto \omega\sqrt[3]{n}$ and leaves ω fixed. Clearly $x^2 = y^3 = 1$ and $xyx^{-1} = y^2$ which is enough to show that $G \cong S_3$. □

Thus the subfields of K correspond to the subgroups of S_3. S_3 has one normal subgroup $N = A_3 = \langle(123)\rangle$ and three conjugate subgroups with two elements, for example $H = \langle(12)$. Therefore, the subfields of K are, $k = \mathbb{Q}(\sqrt[3]{n})$, the two conjugates of k, and $F = \mathbb{Q}(\omega)$ (which correspond Galois groups $N = \mathrm{Gal}(K/F) \cong C_3$ and $H = \mathrm{Gal}(K/k) \cong C_2$).

Now let us compute the character table for S_3. By general principles or direct computation, the conjugacy classes of S_3 are determined by cycle structure. Thus we have three conjugacy classes $[\varepsilon]$, $[(12)]$ and $[(123)]$. Since N is normal and S_3/N is abelian, we get two 1-dimensional representations, V_0 the trivial representation, and V_1 the sign representation. Furthermore, since $S_3 \cong D_6$ we have the defining 2-dimensional representation of D_6 given by rigid motions of a triangle. A simple computation shows that this yields the character table,

S_3	ε	(12)	(123)
χ_0	1	1	1
χ_1	1	-1	1
χ_2	2	0	-1

For the characters of subgroups and quotient groups of G we fix the following notation. For a character of a cyclic group with a fixed generator (namely (12) or (123)) we will let χ_z be the representation sending that generator to the root of unity z, hence χ_1 will denote the trivial representation, and χ_{-1} the sign representation, etc.

3.1.3 Factoring the Ramified Primes

We need to know which primes ramify in $K/\mathbb{Q}$ and how they factor in order to compute the Artin L-function. Suppose a prime p ramifies in the extension $K/\mathbb{Q}$. Since the ramification degree is multiplicative in towers and 2 and 3 are relatively prime, $e_p(K/\mathbb{Q}) = e_p(k/\mathbb{Q})e_p(F/\mathbb{Q})$. Since 2 and 3 are prime, computing $e_p(k/\mathbb{Q})$ and $e_p(F/\mathbb{Q})$ reduces to simply finding which primes divide the discriminants of each of these subextensions.

Lemma 3.1.2. *The only primes which ramify in $k/\mathbb{Q}$ are 3 and those primes dividing n.*

Proof. The discriminant of the extension $k/\mathbb{Q}$ is at worst the discriminant of

$$\mathbb{Z}[\sqrt[3]{n}] = -4 \cdot 0^3 - 27n^2 = -27n^2.$$

In fact, since the discriminant of the whole ring of integers differs from $-27n^2$ by a square, clearly 3 divides the discriminant and thus ramifies.

On the other hand, $x^3 - n$ is Eisenstein in any prime dividing n, thus all of these primes totally ramify. □

The discriminant of the extension $F/\mathbb{Q}$ is -3, thus the prime 3 obviously ramifies (with index 2) in the extension $F/\mathbb{Q}$. Therefore, we have $(e, f, g)_3 = (6, 1, 1)$.

If $p|n$, then we need to look at how p factors in $F/\mathbb{Q}$. By Kummer's theorem this is determined by the Legendre symbol $\left(\frac{-3}{p}\right)$. Thus, by quadratic reciprocity, p splits in F iff $p \equiv 1 \mod 3$. In conclusion, we summarize can summarize all the information about the primes which ramify (that is $p|3n$).

Proposition 3.1.3.

$$(e, f, g)_p = \begin{cases} (6, 1, 1) & \text{if } p \equiv 0 \mod 3 \\ (3, 1, 2) & \text{if } p \equiv 1 \mod 3 \\ (3, 2, 1) & \text{if } p \equiv 2 \mod 3 \end{cases}.$$

□

3.1.4 Decomposition and Inertia Groups

Next we turn to computing the decomposition groups and inertia groups for a general prime p. The main tools here will be the fact that G_p/I_p is a cyclic group generated by the Frobenius, has order f_p the relative degree of a prime sitting over p, and the order of I_p is e the ramification index.

Definition 3.1.4. *Let S_i be the sets of primes which have $(e, f, g)_p = (1, i, 6/i)$. Let R_i be the sets of prime which ramify and are congruent to i modulo 3.*

Proposition 3.1.5. *S_6 is empty. For the remaining primes we have,*

$$G_p = \begin{cases} G & \text{if } p \in R_0 \\ N & \text{if } p \in R_1 \\ G & \text{if } p \in R_2 \\ 1 & \text{if } p \in S_1 \\ H & \text{if } p \in S_2 \\ N & \text{if } p \in S_3 \end{cases}.$$

$$G_p = \begin{cases} G & \text{if } p \in R_0 \\ N & \text{if } p \in R_1 \\ G & \text{if } p \in R_2 \\ 1 & \text{if } p \in S_i \end{cases}.$$

Proof. First suppose p ramifies. If $p|n$ and $p \cong 1 \mod 3$, then we know from above that $(e, f, g)_p = (3, 1, 2)$. Therefore, $\#I_p = 3$ and $\#G_p = 3$. Obviously, the only choices for these groups are $I_p = N$ and $G_p = N$. If $p|n$ and $p \cong 2 \mod 3$, then we know from above that $(e, f, g)_p = (3, 2, 1)$. Therefore $\#I_p = 3$ and $\#G_p = 6$. Obviously, the only choices for these groups are $I_p = N$ and $G_p = G$. If $p = 3$, the situation is even simpler, because I_p already must be all of G. Hence, G_p is squeezed between I_p and G. Therefore G_p must also be G.

Suppose p is an unramified prime. Therefore, I_p is trivial. Hence, G_p must be a cyclic subgroup of S_3 of order f_p. For $f_p = 6$, this is impossible. Hence there can be no primes with $f_p = 6$. For $f_p = 3$, we can only pick $G_p = N$. If $f_p = 2$ then $G_p = H$ or any of its conjugates, we cannot be sure which, but it won't ultimately matter since the representation doesn't care up to conjugation. Finally if $f_p = 1$ then clearly G_p is trivial.

Rather than depending on the properties of the inertia and decomposition groups, we'd like to independently verify the fact that $f_p = 6$ is impossible. Notice that, since f is multiplicative in extensions, $f_p(K/\mathbb{Q}) = 6$ if and only if $f_p(k/\mathbb{Q}) = 3$ and $f_p(F/\mathbb{Q}) = 2$. But these are easy to compute. In fact, $f_p(k/\mathbb{Q}) = 3$ exactly when n is not a cube mod p, and $f_p(H/\mathbb{Q}) = 2$ exactly when -3 is not a square mod p. Now, by quadratic reciprocity, this means we must have that $p \equiv 2 \mod 3$. But when $p \equiv 2 \mod 3$, *every* number is a perfect cube. Therefore, $f_p(K/\mathbb{Q}) = 6$ is clearly impossible even without resorting to the notion of decomposition groups. □

3.2 Computing the Local Factors for the Finite Primes

3.2.1 Introduction

Now that we know the irreducible representations and the decomposition and inertia groups for each prime, we can find the local factors of L-series corresponding to the finite primes for the various representations. In the course of making these computations we will confirm the basic results from chapter two for each of these particular cases. We will use results from the last section without quoting them because it would get cumbersome.

3.2.2 Computing $L_{\mathfrak{p}}(s, V_0)$ and $L_{\mathfrak{p}}(s, V_1)$

First we consider the trivial representation V_0. For any subgroup $G' \subset G$, we have that $V_0^{G'} = V_0$, and clearly whatever the Frobenius is, it must act trivially. Therefore, the Artin L-series is:

$$\begin{aligned} L(s, V_0) &= \prod_p \det(1 - \sigma_{\mathfrak{P}} p^{-s} | V^{I_p})^{-1} \\ &= \prod_p |1 - p^{-s}|^{-1} = \prod_p \frac{1}{1 - p^{-s}} = \zeta_{\mathbb{Q}}(s). \end{aligned}$$

The equality $L(s, V_0) = \zeta_{\mathbb{Q}}(s)$ is exactly what we expect, because V_0 is the pullback of the trivial representation on the trivial quotient group G/G. That is to say, we already knew

$$\zeta_{\mathbb{Q}}(s) = L(s, \chi_1, \mathbb{Q}/\mathbb{Q}) = L(s, \text{Infl } \chi_1, K/\mathbb{Q}) = L(s, V_0, K/\mathbb{Q}).$$

Now we turn to the sign representation V_1. For $p \in R_1$, $V_1^{I_p} = V_1^N = V_1$. The group G_p/I_p is trivial. Therefore, the Frobenius is the trivial element of the Galois group. Thus, we get the local factor $\frac{1}{1-2^{-s}}$.

For $p \in R_2$, $V_1^{I_p} = V_1^N = V_1$. The group G_p/I_p has order 2. Therefore, the Frobenius is clearly any nontrivial element, so (12) will do. (12) acts by -1. Therefore, we get the local factor $\frac{1}{1+2^{-s}}$.

For the prime 3, $V_1^{I_3} = V_1^G$ is trivial. Therefore there is no local factor for 3.

For the remaining non-ramifying primes the Frobenius is determined by the way the prime factors. For $p \in S_1$ the Frobenius is ε; for $p \in S_2$ the Frobenius is conjugate to (12); for $p \in S_3$ the Frobenius is conjugate to (123). Therefore, the finite part of the Artin L-series is:

$$L(s, V_1) = \prod_{p \in R_1} \frac{1}{1 - p^{-s}} \prod_{p \in R_2} \frac{1}{1 + p^{-s}} \prod_{p \in S_1} \frac{1}{1 - p^{-s}} \prod_{p \in S_2} \frac{1}{1 + p^{-s}} \prod_{p \in S_3} \frac{1}{1 - p^{-s}}$$

We want to simplify this into a form where we can conclude that it is equal to the appropriate abelian L-series. So, we want to find a better way to classify the different primes. We notice that p is in S_1 or S_3 exactly when f_p is relatively prime to 2, therefore, by the multiplicativity of f in extensions, p is in S_1 or S_3 exactly when $f_p(F/\mathbb{Q}) = 1$. By quadratic reciprocity, this happens exactly when $p \equiv 1 \mod 3$. Therefore, we find that

$$L(s, V_1) = \prod_{p \equiv 1 \mod 3} \frac{1}{1 - p^{-s}} \prod_{p \equiv 2 \mod 3} \frac{1}{1 + p^{-s}} = \frac{\zeta_F(s)}{\zeta_{\mathbb{Q}}(s)},$$

which is of course the Abelian L-series for the nontrivial character modulo 3. Again this is exactly what we expect from the fact about the L-function of the pullback of a representation.

3.2.3 Computing $L_{\mathfrak{p}}(s, V_2)$

Finally, consider the two dimensional representation V_2. First we look at the ramified primes. In any of the cases $N \subset I_p$, and V_2^N is already trivial (because the eigenvalues of the action of (123) are the primitive cube roots of unity, not 1). Therefore, none of the ramified primes appear in the L-series.

Second, we turn our attention to the unramified case. For $p \in S_1$ the Frobenius is ε; for $p \in S_2$ the Frobenius is conjugate to (12); for $p \in S_3$ the Frobenius is conjugate to (123). The actual actions of the elements in diagonal form (obviously they cannot be simultaneously diagonalized, but the local factors are the same in any basis, so we can pick a diagonal basis for each local factor separately) are $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $\begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$.

In conclusion,

Theorem 3.2.1. *The Artin L-series is:*

$$\begin{aligned} L(s, V_2) &= \prod_{p \in S_1} \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} p^{-s} \right)^{-1} \prod_{p \in S_2} \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} p^{-s} \right)^{-1} \\ &\quad \prod_{p \in S_3} \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix} p^{-s} \right)^{-1} \\ &= \prod_{p \in S_1} \begin{vmatrix} 1-p^{-s} & 0 \\ 0 & 1-p^{-s} \end{vmatrix}^{-1} \prod_{p \in S_2} \begin{vmatrix} 1-p^{-s} & 0 \\ 0 & 1+p^{-s} \end{vmatrix}^{-1} \prod_{p \in S_3} \begin{vmatrix} 1-\omega p^{-s} & 0 \\ 0 & 1-\bar{\omega} p^{-s} \end{vmatrix}^{-1} \\ &= \prod_{p \in S_1} \frac{1}{1 - 2p^{-s} + p^{-2s}} \prod_{p \in S_2} \frac{1}{1 - p^{-2s}} \prod_{p \in S_3} \frac{1}{1 + p^{-s} + p^{-2s}} \end{aligned}$$

Now, by Brauer's theorem, we should be able to write this L-series in terms of abelian L-series. To do this, we need to find what the induced representations from various cyclic subgroups are. By using Frobenius Reciprocity early and often we find:

Proposition 3.2.2.

$$\begin{aligned} Ind_{\varepsilon}^{G}(\chi_1) &= V_0 + V_1 + 2V_2 \\ Ind_{H}^{G}(\chi_1) &= V_0 + V_2 \\ Ind_{H}^{G}(\chi_{-1}) &= V_1 + V_2 \\ Ind_{N}^{G}(\chi_1) &= V_0 + V_1 \\ Ind_{N}^{G}(\chi_\omega) &= V_2 \\ Ind_{N}^{G}(\chi_{\bar{\omega}}) &= V_2. \end{aligned}$$

Therefore, we have

$$L(s, V_2, K/\mathbb{Q}) = L(s, \mathrm{Ind}_N^G(\chi_\omega); K/\mathbb{Q}) = L(s, \chi_\omega; K/F).$$

Clearly this implies Artin's conjecture for this particular extension (which we expect to be easy since G is solvable).

Also notice that since $\mathrm{Ind}_N^G(\chi_{\bar{\omega}}) = V_2$, we have

$$L(s, \chi_\omega; K/F) = L(s, \chi_{\bar{\omega}}; K/F) \tag{3.2.1}$$

However, we would like to verify the identity $L(s, V_2, K/\mathbb{Q}) = L(s, \chi_\omega, K/F)$ by hand without resorting to the general theorem. A quick glance at the formula:

$$L(s, V_2) = \prod_{p \in S_1} \frac{1}{1 - 2p^{-s} + p^{-2s}} \prod_{p \in S_2} \frac{1}{1 - p^{-2s}} \prod_{p \in S_3} \frac{1}{1 + p^{-s} + p^{-2s}}$$

shows us that we need to show the following facts:

1) $p \in S_1$ means that p factors in F as $p = q_1 q_2$ with $\chi_\omega(q_1) = \chi_\omega(q_2) = 1$
2) $p \in S_2$ means that p stays prime in F
3) $p \in S_3$ means that $p = q_1 q_2$ with $\chi(q_1)$ and $\chi(q_2)$ are conjugate 3rd roots of unity.
4) 3 and any divisors of n ramify in the extension K/F.

Fact 4) we already know. 2) follows immediately from the fact that $f_p(K/\mathbb{Q})$ is divisible by 2. 1) and 3) are slightly more difficult. We know that since in these cases $f_p(K/\mathbb{Q})$ is relatively prime to 2, in both cases p is a product of distinct primes. To distinguish whether $\chi(q_1)$ is 1 or not, we need to know if the Frobenius of q_1 in the extension K/F is trivial or not. That is to say, whether the decomposition group for that extension and that prime is trivial or not. This in term is simply a question of whether $f_p(K/F)$ is 1 or not. Clearly this just depends on whether $f_p(K/\mathbb{Q})$ is divisible by 3 or not. Therefore 1) and 3) are also solved. Therefore, we have the result which we wanted.

3.2.4 Checking the Product Formula for $\zeta_K(s)$.

One final result to check is the fact that $\zeta_K(s) = L(s, V_0)L(s, V_1)L(s, V_2)^2$. From the above formulas:

$$\begin{aligned}
L(s, V_0)L(s, V_1)L(s, V_2)^2 &= \frac{1}{1-2^{-s}} \cdot \frac{1}{1+2^{-s}} \cdot \frac{1}{1-3^{-s}} \\
&\quad \prod_{p \in S_1} \frac{1}{1-p^{-s}} \cdot \frac{1}{1-p^{-s}} \cdot \left(\frac{1}{1-2p^{-s}+p^{-2s}}\right)^2 \\
&\quad \prod_{p \in S_2} \frac{1}{1-p^{-s}} \cdot \frac{1}{1+p^{-s}} \cdot \left(\frac{1}{1-p^{-2s}}\right)^2 \\
&\quad \prod_{p \in S_3} \frac{1}{1-p^{-s}} \cdot \frac{1}{1-p^{-s}} \cdot \left(\frac{1}{1+p^{-s}+p^{-2s}}\right)^2 \\
&= \frac{1}{1-2^{-2s}} \cdot \frac{1}{1-3^{-s}} \prod_{p \in S_1} \left(\frac{1}{1-p^{-s}}\right)^6 \\
&\quad \prod_{p \in S_2} \left(\frac{1}{1-p^{-2s}}\right)^3 \prod_{p \in S_3} \left(\frac{1}{1-p^{-3s}}\right)^2 \\
&= \prod_p \left(\frac{1}{1-p^{-f_p s}}\right)^{g_p} = \prod_{\mathfrak{P} \in K} \frac{1}{1-N\mathfrak{P}^{-s}} \\
&= \zeta_K(s).
\end{aligned}$$

Thus we have checked all the basic identities for the finite part of the Artin L-series for the specific case of $K/\mathbb{Q}$.

3.3 Computing the Local Factors for the Infinite Primes

Next let us compute these infinite factors $L_v(s, \chi)$.

We recall the character table for S_3:

S_3	ε	(12)	(123)
χ_0	1	1	1
χ_1	1	-1	1
χ_2	2	0	-1

There is only one infinite prime for the rationals and it is real. The prime sitting over this in K is complex. Therefore, the decomposition group is made up of the identity and one of the elements of order 2. Thus, $\mathrm{Res}_{G_v}\chi_0 = \chi_+$, $\mathrm{Res}_{G_v}\chi_1 = \chi_-$, and $\mathrm{Res}_{G_v}\chi_2 = \chi_+ + \chi_-$. Therefore, the infinite factors are:

$$L_v(\chi_0, s) = \Gamma_{\mathbb{R}}(s)$$
$$L_v(\chi_1, s) = \Gamma_{\mathbb{R}}(s+1)$$
$$L_v(\chi_2, s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = \Gamma_{\mathbb{C}}(s).$$

3.4 Computing the Artin Conductor and Exponential Factors

3.4.1 Introduction

In this section, we use our formula for the Artin conductor to compute the conductors of all the characters for the splitting field of $x^3 - n$ over $\mathbb{Q}$. This gives us the exponential factor for the Artin L-series, and thus completes our program of computing the full completed L-functions for these extensions.

Recall from prior sections that the only primes which ramify in $K/\mathbb{Q}$ are 3 and those primes dividing n. 3 has inertia group G, while the other primes dividing n have inertia group N.

3.5 The Local Conductor for Primes Other Than 3

Let us first consider p a ramifying primes other than 3.

Before we can compute the local conductors we need to find the higher ramification groups for this prime.

Proposition 3.5.1. *If $3 \nmid p$ is a prime which ramifies in $K/\mathbb{Q}$, then the ramification groups for this prime are $G_0 = N$ and $G_i = 1$ if $i > 0$*

Proof. Since the inertia group is N and the ramification groups behave well under subgroups, it is enough to find the ramification groups for a prime over p in the extension K/F.

Fix $\mathfrak{P}$ a prime in K dividing $\mathfrak{p}$ a prime in F dividing p. Since p does not ramify in $F/\mathbb{Q}$, the polynomial $x^3 - n$ is Eisenstein for $\mathfrak{p}$ in F. Therefore, n completely ramifies in K/F, and locally $\mathcal{O}_{K_\mathfrak{P}} = \mathcal{O}_{F_\mathfrak{p}}[\sqrt[3]{n}]$. Take σ a generator of N (say the automorphism sending $\sqrt[3]{n}$ to $\omega\sqrt[3]{n}$). For $\sigma \in G_i$ is the same as saying

$$v_{K_\mathfrak{P}}(\sigma(x) - x) = i_G(\sigma) \geq i + 1,$$

where x is any generator of $K_\mathfrak{P}/F_\mathfrak{p}$, for example $x = \sqrt[3]{n}$. Thus, we are reduced to computing $v_{K_\mathfrak{P}}(\sigma(\sqrt[3]{n}) - \sqrt[3]{n})$.

Clearly,

$$\sigma(\sqrt[3]{n}) - \sqrt[3]{n}\mathcal{O}_{K_\mathfrak{P}} = (1-\omega)\sqrt[3]{n}\mathcal{O}_{K_\mathfrak{P}} = \sqrt{-3}\omega^2\sqrt[3]{n}\mathcal{O}_{K_\mathfrak{P}} = \sqrt[3]{n}\mathcal{O}_{K_\mathfrak{P}},$$

because $\sqrt{-3}\omega^2$ is a unit. Therefore,

$$v_{K_\mathfrak{P}}(\sigma(\sqrt[3]{n}) - \sqrt[3]{n}) = v_{K_\mathfrak{P}}(\sqrt[3]{n}) = 1.$$

Therefore, $G_0 = N$ and $G_i = 1$ if $i > 0$. □

(One can prove Proposition 3.5.1 very quickly using a bit more machinery. One can prove in general that $|G_0/G_1|$ is relatively prime to p, while G_1 is a p-group. Since $G_0 = N$ has order relatively prime to p clearly G_1 must be trivial.)

Now we can compute the local Artin conductors for each of the representations of G.

Proposition 3.5.2. *If $3 \nmid p$ is a prime which ramifies in $K/\mathbb{Q}$, then $\mathfrak{f}_p(V_0) = 1$, $\mathfrak{f}_p(V_1) = 1$, and $\mathfrak{f}_p(V_2) = p^2$*

Proof. For V_0, we notice codim V^N is 0, and so $f_p(V_0) = 0$. This is, of course, what we expect.

For V_1, codim $V_1^N = 0$. Hence $f_p(V_1) = 0$. This is also exactly what we would expect if we considered V_1 as an abelian character for the extension $F/\mathbb{Q}$.

For V_2, codim $V_2^N = 2$. Hence, $f_p(V_2) = \frac{1}{3}(3 \cdot 2) = 2$. □

3.6 The Local Conductor for 3

Now we will turn our attention to the more difficult prime 3. Again we begin by computing the higher ramification groups for this prime.

Proposition 3.6.1. *If $3|n$, then $G_0 = G$, $G_1 = G_2 = G_3 = N$ and $G_i = 1$ for $i > 3$. On the other hand, if $3 \nmid n$, then $G_0 = G$, $G_1 = N$ and $G_i = 1$ for $i > 1$.*

Proof. In order to do this we first compute the ramification groups for the subextensions K/F and $F/\mathbb{Q}$.

For $F/\mathbb{Q}$ the Galois group, G/N, has two elements, call them 1 and σ. In this case, $\sqrt{-3}$ is obviously the prime lying over 3. Again we need to find the highest power of $\sqrt{-3}$ dividing $\omega - \sigma(\omega)$, since ω generates the ring of integers in K_3.

$$(\omega - \sigma(\omega))\mathcal{O}_{K_3} = (\omega - \omega^2)\mathcal{O}_{K_3} = \sqrt{-3}\mathcal{O}_{K-3}.$$

Therefore, only $\sqrt{-3}$ to the first power will divide $x - \sigma(x)$ for all x.

Therefore, $(G/N)_0 = \{1, \sigma\}$ and $(G/N)_i = 1$ if $i > 0$. Rephrasing this in terms of the upper numbering we see $(G/N)^0 = G_0 = \{1, \sigma\}$ and $(G/N)^i = 1$ if $i > 0$.

Since upper numbering is preserved under quotients, we must have that for the whole extension $K/\mathbb{Q}$, $G^0 = G$, but $G^i \subset N$ if $i > 0$. If G_1 were all of G, then $G^1 = G_1 = G$ which is a contradiction. Thus, we actually get that $G_0 = G$ and $G_i \subset N$ if $i > 0$.

(Again we could have seen this more quickly using the result that G_0/G_1 has order prime to 3 while G_1 has order a power of p.)

Thus, since all the $G_i \subset N$ for $i > 0$ and ramification groups are preserved under subgroups, it is enough to compute N_i for the extension K/F and the prime $\sqrt{-3}$ lying above 3.

Here we will be forced to take cases based on what n is modulo 9.

For K/F the Galois group N is cyclic and so to check whether the group acts trivially it is enough to check whether its generator, call it τ acts trivially. Choose $\mathfrak{P}$ a prime ideal sitting over $\mathfrak{p} = (\sqrt{-3}) = \mathfrak{P}^3$ which in turn sits over $(3) = \mathfrak{P}^6$ and $\mathfrak{q} = \mathfrak{P}^2$ a prime sitting over (3) in k. (By abuse of notation we will also use these same symbols to refer to the ideals in the corresponding local fields.) We need to actually find $\mathfrak{P}$ concretely. Notice, however, that $\mathfrak{P} = \frac{\mathfrak{P}^3}{\mathfrak{P}^2} = \frac{\mathfrak{p}}{\mathfrak{q}}$. Thus, it is enough to find $\mathfrak{q}$.

Here we need to take cases on what n is modulo 9. Since n is square-free, clearly $n \not\equiv 0 \mod 9$.

Case 3.

$$n \equiv 3 \text{ or } 6 \mod 9.$$

In this case $x^3 - n$ is already Eisenstein, and so $\mathfrak{q} = \sqrt[3]{n}\mathcal{O}_{k_\mathfrak{q}}$.

Case 4.

$$n \equiv 4 \text{ or } 7 \mod 9.$$

Now $(x+1)^3 - n = x^3 + 3x^2 + 3x + (1-n)$ is Eisenstein. Thus, $\mathfrak{q} = (-1 + \sqrt[3]{n})\mathcal{O}_{k_\mathfrak{q}}$.

Case 5.

$$n \equiv 4 \text{ or } 7 \mod 9.$$

Here $(x-1)^3 - n$ is Eisenstein, thus $\mathfrak{q} = (1 + \sqrt[3]{n})\mathcal{O}_{k_\mathfrak{q}}$.

Case 6.

$$n \equiv 1 \mod 9.$$

Here no simple linear change of variables will work. In order to guess a prime over 3, we compute the norm form

$$N_{k/\mathbb{Q}}(a + b\sqrt[3]{n} + c\sqrt[3]{n^2}) = a^3 + nb^3 + n^2c^3 - 3nabc.$$

To get the this norm to be divisible by 3 but not 9, we take $(a, b, c) = (1, 1, 1)$. Thus our candidate for $\mathfrak{q}$ is $(1 + \sqrt[3]{n} + \sqrt[3]{n^2})\mathcal{O}_{k_\mathfrak{q}}$. A simple computation shows that the minimal polynomial for this element is in fact Eisenstein in 3.

Case 7.

$$n \equiv 8 \mod 9.$$

This case is similar to the above case, only now we must take $(a,b,c) = (1,-1,1)$ to get that the uniformizer is $(1 - \sqrt[3]{n} + \sqrt[3]{n^2})\mathcal{O}_{k_\mathfrak{q}}$.

Now we have enough information to compute the ramification groups.

In Case 1,

$$\mathfrak{P} = \frac{\sqrt{-3}}{\sqrt[3]{n}}\mathcal{O}_{K_\mathfrak{P}} = \frac{\sqrt{-3}\sqrt[3]{n^2}}{n}\mathcal{O}_{K_\mathfrak{P}} = \frac{\sqrt{-3}\sqrt[3]{n^2}}{3}\mathcal{O}_{K_\mathfrak{P}}.$$

Hence we need to compute $\sigma(x) - x$ where x is $\frac{\sqrt{-3}\sqrt[3]{n^2}}{3}$.

$$(\sigma(x) - x)\mathcal{O}_{K_\mathfrak{P}} = (1-\omega^2)\frac{\sqrt{-3}\sqrt[3]{n^2}}{3}\mathcal{O}_{K_\mathfrak{P}} = (1-\omega)(1+\omega)\mathfrak{P}^{(3+2\cdot 2-6)} = \omega\sqrt{-3}\mathfrak{P} = \mathfrak{P}^4.$$

Thus, we see that $N_i = N$ if $i \leq 3$ and $N_i = 1$ if $i > 3$.

Combined with our old information this tells us that $G_0 = G$, $G_1 = G_2 = G_3 = N$, and $G_i = 1$ if $i > 3$.

The remaining cases all yield the same answers as each other using the same methods. So, for simplicity, I will only deal with Case 2. Here

$$\mathfrak{P} = \frac{\sqrt{-3}}{-1+\sqrt[3]{n}} = \frac{\sqrt{-3}(-1+\omega\sqrt[3]{n})(-1+\omega^2\sqrt[3]{n})}{n-1}\mathcal{O}_{K_\mathfrak{P}} = (1+\sqrt[3]{n}+\sqrt[3]{n^2})\frac{\sqrt{-3}}{n-1}.$$

Now we consider $\sigma(x) - x$, where $x = (1+\sqrt[3]{n}+\sqrt[3]{n^2})\frac{\sqrt{-3}}{n-1}$. We have,

$$\begin{aligned}(\sigma(x) - x)\mathcal{O}_{K_\mathfrak{P}} &= (1-\omega)\sqrt[3]{n}\left(1 + (1+\omega)\sqrt[3]{n}\right)\frac{\sqrt{-3}}{n-1}\mathcal{O}_{K_\mathfrak{P}} \\ &= \mathfrak{P}^3\mathfrak{P}^2(1-\omega^2\sqrt[3]{n})\mathfrak{P}^3\mathfrak{P}^{-6} = \mathfrak{P}^2,\end{aligned}$$

since $(1-\omega^2\sqrt[3]{n}) \equiv 1 \mod \mathfrak{P}$ is a unit.

Hence, in this case, $N_0 = N_1 = N$ and $N_i = 1$ for $i > 1$. Therefore, for the whole extension, $G_0 = G$, $G_1 = N$ and $G_i = 1$ for $i > 1$. □

Notice that in the middle of that proof, by finding the uniformizer in $k_\mathfrak{q}$ for each case, we actually showed the following result.

Corollary 3.6.2.

$$\mathcal{O}_{\mathbb{Q}_3(\sqrt[3]{n})} = \mathbb{Z}_3[\sqrt[3]{n}].$$

□

Now that we have finished computing the ramification groups we can compute the Artin conductors.

Proposition 3.6.3. *If $3|n$, then the local Artin conductors for each character are, $\mathfrak{f}_3(V_0) = 1$, $\mathfrak{f}_3(V_0) = 3$, and $\mathfrak{f}_3(V_0) = 3^5$. On the other hand, if $3 \nmid n$, then $\mathfrak{f}_3(V_0) = 1$, $\mathfrak{f}_3(V_0) = 3$, and $\mathfrak{f}_3(V_0) = 3^5$.*

In either case, the global Artin conductor is, $\mathfrak{f}(V_0) = 1$, $\mathfrak{f}(V_0) = 3$, and $\mathfrak{f}_3 = 27n^2$.

Proof. First consider the case $3|n$.

For V_0 we notice codim V^G is already 0, and so $f_3(V_0) = 0$. This is, of course, what we expect.

For V_1, codim $V^G = 1$, while codim $V_1^N = 0$. Hence,

$$f_3(V_1) = \frac{1}{6}\left(6\cdot 1 + 3\cdot 0 + 3\cdot 0 + 3\cdot 0\right) = 1.$$

This is also exactly what we would expect if we considered V_1 as an abelian character for the extension $F/\mathbb{Q}$.

For V_2, codim $V_2^G =$ codim $V_2^N = 2$. Hence,

$$f_3(V_2) = \frac{1}{6}\left(6\cdot 2 + 3\cdot 2 + 3\cdot 2 + 3\cdot 2\right) = 5.$$

Therefore, in this case, we see that the global Artin conductors are:

$$\begin{aligned}\mathfrak{f}(V_0) &= 1\\ \mathfrak{f}(V_1) &= 3\\ \mathfrak{f}(V_2) &= 3^5\left(\frac{n}{3}\right)^2 = 3^3n^2.\end{aligned}$$

If $3 \nmid n$:
$f_3(V_0) = 0$ as expected; $f_3(V_1) = \frac{1}{6}(6\cdot 1 + 3\cdot 0) = 1$ also as expected; finally,

$$f_3(V_2) = \frac{1}{6}(6\cdot 2 + 3\cdot 2) = 3.$$

Thus, the global Artin conductor for V_0 is 1, for V_1 is 3, and for V_2 is 3^3n^2.

Notice that, as if by miracle (a better explanation will be given later), these two formulas agree. □

Since the base field is the rationals, the $c(V)$ of the completed Artin L-series is simply the Artin conductor.

3.6.1 The Führerdiskriminantenproduktformel

By the Führerdiskriminantenproduktformel we would hope that the discriminant of $K/\mathbb{Q}$ is 3^7n^4. So let's compute the discriminants and check this.

We will compute the discriminant locally for the prime 3 and for any other ramifying prime p by computing it first for the subextensions K/F and $F/\mathbb{Q}$ and then using the formula for discriminants in towers.

For primes other than 3, the local extension $F_\mathfrak{p}/F_p$ is unramified and so has trivial discriminant. On the other hand we have shown earlier that, $\mathcal{O}_{K_\mathfrak{P}} = \mathcal{O}_{F_\mathfrak{p}}[\sqrt[3]{n}]$. Therefore, the local discriminant $\mathfrak{d}_{K_\mathfrak{P}/F_\mathfrak{p}}$ is $(-27n^2)$. Since we only care about the p component, the local discriminant is (p^2). Using the formula for discriminants in towers,

$$\mathfrak{d}_{K_\mathfrak{P}/\mathbb{Z}_p} = N_{F_\mathfrak{p}/Z_p}(\mathfrak{d}_{K_\mathfrak{P}/F_\mathfrak{p}})\mathfrak{d}^3_{F_\mathfrak{p}/Z_p} = (p^4),$$

which agrees with the Führerdiskriminantenproduktformel.

For the prime 3 we would again be forced to split into different cases based on what n is modulo 9. We have already computed generators of the extension $\mathcal{O}_{K_\mathfrak{P}}/\mathcal{O}_{F_\mathfrak{p}}$. In fact we have found a generator for the entire extension $\mathcal{O}_{K_\mathfrak{P}}/\mathbb{Z}_3$. Thus, computing the discriminant is reduced to 4 different tedious calculations. This seems a waste of time, since the method is completely analogous to the one above and all of the conceptually difficult calculations have already been done. So, suffice it to say that these computations do in fact agree with the Führerdiskriminantenproduktformel.

3.6.2 Using Machinery to find the Artin Conductors Without Extensive Computation

Although the amount of calculations required to actually compute the Artin conductors by hand in this simple case is daunting, the theory of these conductors does allow one to compute the discriminants and the conductors with much more ease.

By Brauer's Theorem, we expect that each of these Artin conductors can be written in terms of abelian conductors which may be more easy to compute. To that end, we begin by recalling from Proposition 3.2.2,

$$\begin{aligned}\mathrm{Ind}_\varepsilon^G(\chi_1) &= V_0 + V_1 + 2V_2\\ \mathrm{Ind}_H^G(\chi_1) &= V_0 + V_2\\ \mathrm{Ind}4_H^G(\chi_{-1}) &= V_1 + V_2\\ \mathrm{Ind}_N^G(\chi_1) &= V_0 + V_1\\ \mathrm{Ind}_N^G(\chi_\omega) &= V_2\\ \mathrm{Ind}_N^G(\chi_{\bar\omega}) &= V_2.\end{aligned}$$

In particular, by part 2 of Theorem 2.8.1,

$$\begin{array}{lllllll} \mathfrak{d}_{K/\mathbb{Q}} & = & \mathfrak{f}(\mathrm{Ind}_{\varepsilon}^{G}(\chi_1)) & = & \mathfrak{f}(V_0)\mathfrak{f}(V_1)\mathfrak{f}(V_2)^2 & = & \mathfrak{f}(V_1)\mathfrak{f}(V_2)^2 \\ \mathfrak{d}_{k/\mathbb{Q}} & = & \mathfrak{f}(\mathrm{Ind}_{H}^{G}(\chi_1)) & = & \mathfrak{f}(V_0)\mathfrak{f}(V_2) & = & \mathfrak{f}(V_2) \\ \mathfrak{d}_{F/\mathbb{Q}} & = & \mathfrak{f}(\mathrm{Ind}_{N}^{G}(\chi_1)) & = & \mathfrak{f}(V_0)\mathfrak{f}(V_1) & = & \mathfrak{f}(V_1). \end{array}$$

Thus we have reduced the question of computing Artin conductors to simply computing discriminants. As we saw above, this can be difficult. However, given the above formulas they can actually be computed much more quickly. The value $\mathfrak{f}(V_1) = 3$ we get immediately. For V_2 this takes a bit more work.

One way to do this is to actually compute the ring of integers in k.

Theorem 3.6.4.

$$\mathcal{O}_k = \mathbb{Z}[\sqrt[3]{n}].$$

Proof. Consider a general element of k, $x = a + b\sqrt[3]{n} + c\sqrt[3]{n^2}$ with rational coefficients a, b, c. If this is an integer, then all of $\mathrm{Tr}_{k/\mathbb{Q}}x$, $\mathrm{Tr}_{k/\mathbb{Q}}\sqrt[3]{n}x$, $\mathrm{Tr}_{k/\mathbb{Q}}\sqrt[3]{n^2}x$ are also integers. Thus the denominators of a, b, and c can only be divisible by the prime 3 or by primes dividing n. Therefore, it is enough to compute the ring of integers locally in $\mathbb{Q}_3(\sqrt[3]{n})$ and $\mathbb{Q}_p(\sqrt[3]{n})$ for all primes dividing n.

In Corollary 3.6.2 we showed that $\mathcal{O}_{\mathbb{Q}_3(\sqrt[3]{n})} = \mathbb{Z}_3[\sqrt[3]{n}]$. Since $x^3 - n$ is Eisenstein for any prime dividing n, by Proposition 2.7.20, $\mathcal{O}_{\mathbb{Q}_p(\sqrt[3]{n})} = \mathbb{Z}_p[\sqrt[3]{n}]$. Thus, the theorem follows. □

Corollary 3.6.5.

$$\mathfrak{d}_{k/\mathbb{Q}} = (-27n^2).$$

□

Therefore, $\mathfrak{f}(V_2) = 27n^2$. This completes an alternate proof of Theorems 2 and 4 in less about a page, a significant improvement on the 5 pages which it took to calculate this by hand.

Lastly we notice that the above equations give us a formula relating the various discriminants of the number fields. (Essentially this formula is a special case of the Führerdiskriminantenproduktformel.)

Theorem 3.6.6. $\mathfrak{d}_{F/\mathbb{Q}}\mathfrak{d}_{k/\mathbb{Q}}^2 = \mathfrak{d}_{K/\mathbb{Q}}$.

(The proof is immediate, but it should be noted that this formula does not depend on the base field being $\mathbb{Q}$. It is in fact valid for any S_3 extension of number fields. Furthermore an identical formula holds for the completed Artin L-functions. [**F-T**] as well as [**C2**] use this to give a class number formula.) □

Therefore, we can conclude $\mathfrak{d}_{K/\mathbb{Q}} = 3 \cdot (3^3n^2)^2 = 3^7n^4$, again with a minimal amount of actual computation.

3.6.3 Some Calculations Cited Earlier

Now that we better understand how to compute conductors we can return to several computations which we cited in the section on Artin reciprocity.

Proposition 3.6.7. *If $M/\mathbb{Q}$ is a quadratic extension, then the finite part of its conductor is the same as its discriminant. Take $F = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. Pick any prime $\pi \in F$ lying over p in $\mathbb{Q}$ relatively prime to 3. Let $K = F(\sqrt[3]{\pi})$. The finite part of the conductor $\mathfrak{f}(K/F)$ divides 3π.*

Proof. The first of these claims follows immediately from the Führerdiskriminantenproduktformel, because the conductor of the nontrivial character is the conductor of the extension and the conductor of the trivial character is just 1.

The second claim takes a bit more work. If π has residue field degree 2 and then K is the splitting field of $x^3 - p$ over $\mathbb{Q}$ and we can use our above computations. Thus, since $\mathrm{Ind}_N^G\chi_\omega = V_2$ we get that the conductor of K/F is just the conductor of V_2, which we showed earlier is $3p$.

However, if π has residue field degree 1 then we must go about this question differently. By the Führerdiskriminantenproduktformel, $\mathfrak{f}(\chi_1)\mathfrak{f}(\chi_\omega)\mathfrak{f}(\chi_{\omega^2}) = \mathfrak{d}_{K/F}$. Therefore, $\mathfrak{f}(K/F)^2 = \mathfrak{d}_{K/F}$. So, we need only show that $\mathfrak{d}_{K/F}$ divides $9\pi^2$.

The obvious sublattice of $\mathcal{O}_K$ is $\mathcal{O}_F[\sqrt[3]{\pi}]$. This has discriminant $27\pi^2$. This must differ from the actual discriminant by a perfect square (of an element of $\mathcal{O}_F$). Thus, since $(\sqrt{-3}^2) = (3)$, the only way that $\mathfrak{d}_{K/F}$ could not divide $9\pi^2$ is if the discriminant is actually all of $27\pi^2$. Hence, it is enough to show that $\mathcal{O}_K \neq \mathcal{O}_F[\sqrt[3]{\pi}]$.

Since π is relatively prime to 3, we must have $\pi \equiv \pm 1 \pmod{\sqrt{-3}}$. A direct computation shows that

$$\sqrt{-3} | N_{K/F}(1 \pm \sqrt[3]{\pi} \pm \sqrt[3]{\pi^2}).$$

Therefore, by unique factorization into ideals,

$$\frac{(1 \pm \sqrt[3]{\pi} \pm \sqrt[3]{\pi^2})}{\sqrt{-3}} \in \mathcal{O}_K,$$

but it clearly is not in $\mathcal{O}_F[\sqrt[3]{\pi}]$. $\square$

3.7 The Completed L-series for the Splitting Field of $x^3 - n$.

Thus, combining the results from the rest of this chapter, the completed L-functions for the field extension $K/\mathbb{Q}$ are:

$$\Gamma(s, V_0) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\prod_{p}\frac{1}{1-p^{-s}}$$

$$\Gamma(s, V_1) = 3^{\frac{s}{2}}\cdot\pi^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right)\prod_{p\equiv 1 \mod 3}\frac{1}{1-p^{-s}}\prod_{p\equiv 2 \mod 3}\frac{1}{1+p^{-s}}$$

$$\Gamma(s, V_2) = (27n^2)^{\frac{s}{2}}\cdot 2(2\pi)^{-s}\Gamma(s)\prod_{p\in S_1}\frac{1}{1-2p^{-s}+p^{-2s}}\prod_{p\in S_2}\frac{1}{1-p^{-2s}}\prod_{p\in S_3}\frac{1}{1+p^{-s}+p^{-2s}}.$$

Appendix A

Artin's Paper, Über eine neue Art von L-Reihen

Concerning a New Kind of L-series
By Emil Artin

A.1

For a more general discussion including non-abelian algebraic number fields, we need a new analytic function built out of the Frobenius group characters that reduces to the usual L-function in the abelian case. The following pages are dedicated to the investigation of this function.

For the comfort of the reader, we include the basic results from the theory of group characters [1]

Let $\mathfrak{G}$ be a finite group of order n. This can be partitioned into $\mathbf{x}$ classes $\mathfrak{C}_i$ equivalent under conjugation, with h_i elements in $\mathfrak{C}_i$.

Furthermore, let Γ be a representation of the group $\mathfrak{G}$ by matrices with non-vanishing determinant. Every such representation Γ gives rise to a character $\chi(\sigma)$ given by the trace of the matrix corresponding to σ. There are $\mathbf{x}$ irreducible representations Γ_i $(i = 1, ...\mathbf{x})$ with corresponding characters $\chi^i(\sigma)$ which are called the irreducible characters of $\mathfrak{G}$. Every character is a linear combination of irreducible characters:

$$\chi(\sigma) = \sum_{i=1}^{\mathbf{x}} r_i \chi^i(\sigma), \tag{A.1.1}$$

where the r_i are all nonnegative and the indexed over the irreducible characters Γ.

For the irreducible characters, we have the following formulas:

$$\sum_{\sigma} \chi^i(\sigma)\chi^k(\sigma^{-1}) = n\delta_{ik}, \tag{A.1.2}$$

$$\sum_{i=1}^{\mathbf{x}} \chi^i(\sigma)\chi^i(\tau^{-1}) = \begin{cases} 0 & \text{if } \sigma \text{ and } \tau \text{ are not conjugates,} \\ n/h_r & \text{if } \sigma \text{ and } \tau \text{ are in the class } \mathfrak{C}_r. \end{cases} \tag{A.1.3}$$

Let $\mathfrak{g}$ be a subgroup and

$$\mathfrak{G} = \sum_{i=1}^{s} \mathfrak{g} S_i \tag{A.1.4}$$

be the decomposition of $\mathfrak{G}$ into cosets.

Let Δ be a representation of $\mathfrak{g}$. Now we generally understand A_σ to be the matrix in Δ corresponding to the element σ if s is an element of $\mathfrak{g}$, and otherwise $A_\sigma = 0$ if σ is not in $\mathfrak{g}$. Then, we can build the matrices:

$$B_\sigma = (A_{S_i \sigma S_k^{-1}}), \tag{A.1.5}$$

which give a representation of $\mathfrak{G}$, which is induced by the representation Δ of $\mathfrak{g}$ [2].

Let ψ be the character of the representation Δ, thus we call the character of the representation given in Equation A.1.5 χ_ψ the character induced by χ.

Let ψ_i $(i = 1 \dots n)$ be the irreducible characters of $\mathfrak{g}$, and for every τ in $\mathfrak{g}$ write:

$$\chi^i(\tau) = \sum_{\nu=1}^{\lambda} r_{\nu i} \psi_\nu(\tau) \tag{A.1.6}$$

where $(i = 1 \dots \mathbf{x})$, in the other direction, for any element of $\mathfrak{G}$ we have:

$$\chi_{\psi_i}(\tau) = \sum_{\nu=1}^{\mathbf{x}} r_{i\nu} \chi^r(\tau) \tag{A.1.7}$$

$(i = 1 \dots \lambda)$.

[1] Compare with J. Schur: Neue Begründung der Theorie der Gruppencharaktere, Sitzungsberichte, Berlin 1905, S.406. Furthermore see A. Speiser: Theorie der Gruppetti von enricher Ordering. Chapters 10-12.

[2] Speiser: Gastroenteric §52, from which one can derive Equation A.1.5 easily. Frobenius: Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen, Sitzungsberichte Berlin 1898.

A.2

Now let k be an algebraic number field, K a Galois extension of k and $\mathfrak{G}$ the Galois group of K/k. Take $\mathfrak{p}$ a prime ideal of k that does not divide the relative discriminant of K/k, and $\mathfrak{P}$ a prime factor of $\mathfrak{p}$ in K.

We now take a substitution σ in $\mathfrak{G}$ such that for any A in K we have:

$$\sigma A \equiv A^{N\mathfrak{p}} \mod \mathfrak{P}, \tag{A.2.1}$$

with $N\mathfrak{p}$ understood to mean the norm of $\mathfrak{p}$ in k. The existence of such a substitution can be found in Weber, Algebra II, zweite Auflage, §178.

σ is uniquely determined by $\mathfrak{P}$. If σ_1 shared this characteristic with σ, then

$$\sigma^{-1}\sigma_1 A \equiv A \mod \mathfrak{P},$$

thus $\sigma^{-1}\sigma_1$ belongs to the inertia group, and by our condition on $\mathfrak{P}$ it must be the identity of $\mathfrak{G}$.

If we choose $\mathfrak{P}'$ another prime divisor of $\mathfrak{p}$ such that $\tau\mathfrak{P} = \mathfrak{P}'$, then the corresponding substitution can be easily seen to be $\tau\sigma\tau^{-1}$.

In this way, to every prime ideal $\mathfrak{p}$ we can assign a unique conjugacy class $\mathfrak{C}$ of substitutions. The substitutions in $\mathfrak{C}$ are well known to be generators of the decomposition groups of the prime divisors of $\mathfrak{p}$. This property, however, does not determine the class $\mathfrak{C}$ since we could take appropriate powers of these substitutions and get something non-equivalent [3]. We say that the prime $\mathfrak{p}$ belongs to the class $\mathfrak{C}$ and we call this class $\mathfrak{C}_\mathfrak{p}$.

Now take Γ a representation of $\mathfrak{G}$ and $A_\mathfrak{p}$ the matrix for an element of $\mathfrak{C}$. The "characteristic function"

$$|E - tA_\mathfrak{p}|$$

(where E=the identity matrix), where the lines define the determinant as usual, also the characteristic function does not change if $A_\mathfrak{p}$ is replaced by an equivalent matrix. So this is independent of the selection of $A_\mathfrak{p}$ from $\mathfrak{C}$ and is also the same for isomorphic representations.

Let χ be the character of Γ, then let the L-series of the field k corresponding to χ by the formula

$$L(s,\chi;k) = \prod_\mathfrak{p} \frac{1}{|E - N\mathfrak{p}^{-s}A_\mathfrak{p}|}, \tag{A.2.2}$$

where the product is taken over all prime ideals not dividing the relative discriminant. It is clear that our product converges absolutely and uniformly when $\Re(s) > 1$ because the roots of the characteristic functions, which are in the denominator, are all roots of unity.

One can now rewrite Equation A.2.2 as a Dirichlet series and find the coefficients in terms of the character χ. These coefficients, however, are not given by simple formulas. We can arrive at a simple formula by looking at the logarithm of Equation A.2.2.

First we extend our consideration from the classes of prime ideals to those of powers of prime ideals. To the ideal $\mathfrak{p}^\nu$ we assign the class $\mathfrak{C}_{\mathfrak{p}^\nu}$, the νth powers of the elements in $\mathfrak{C}_\mathfrak{p}$. It is easy to see that this is actually a conjugacy class. If σ is any substitution in $\mathfrak{C}_{\mathfrak{p}^\nu}$, we write:

$$\chi(\mathfrak{p}^\nu) = \chi(\sigma). \tag{A.2.3}$$

Now let $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_f$ be the roots of the equation $|Et - A_\mathfrak{p}| = 0$, this yields

$$\chi(\mathfrak{p}^\nu) = \varepsilon_1^\nu + \varepsilon_2^\nu + \ldots + \varepsilon_f^\nu. \tag{A.2.4}$$

[3] This allocation of prime ideals to substitution classes which we explain here was done by Frobenius in the same way. See Frobenius: Über Beziehungen zwischen Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Sitzungsberichte Berlin 1896.

Thus we get that for $|t| < 1$

$$-\log|E - tA_{\mathfrak{p}}| = -\sum_{i=1}^{f}\log(1-t\varepsilon_i) = \sum_{i=1}^{f}\sum_{\nu=1}^{\infty}\frac{\varepsilon_i^{\nu}}{\nu}t^{\nu}$$
$$= \sum_{\nu=1}^{\infty}\frac{\chi(\mathfrak{p}^{\nu})}{\nu}t^{\nu}.$$

This gives us our desired formula:

$$+\log L(s,\chi;k) = \sum_{\mathfrak{p}^{\nu}}\frac{\chi(\mathfrak{p}^{\nu})}{\nu N\mathfrak{p}^{\nu s}}, \tag{A.2.5}$$

where the sum is taken over all powers of prime ideals in k relatively prime to the relative discriminant.

Either from Equation A.2.2 or from Equation A.2.5, we can check the correctness of the equation:

$$L(s,\chi+\chi') = L(s,\chi)L(s,\chi'), \tag{A.2.6}$$

for any two characters χ and χ'.

We call the L-series belonging to irreducible characters the primitive L-series. We can write any L-series in terms of the $\mathbf{x}$ primitive L-series. If Equation A.1.1 applies to χ, then we get from Equation A.2.6

$$L(s,\chi) = \prod_{i=1}^{\mathbf{x}}(L(s,\chi^i))^{r_i}. \tag{A.2.7}$$

One short remark on the dependency on K. Let Ω containing K be another Galois extension of k, $\mathfrak{H}$ its Galois group, and $\mathfrak{g}$ the subgroup corresponding to K, then $\mathfrak{G}$ is isomorphic to the factor group $\mathfrak{H}/\mathfrak{g}$.

Now if Equation A.2.1 applies to all integers in Ω, then it also applies to all integers in K. Since substitutions in $\mathfrak{g}$ leave K fixed, Equation A.2.1 is also true for all elements of the coset $\sigma\mathfrak{g}$ as long as A is an element of K. Now we need only note that every character of $\mathfrak{H}/\mathfrak{g}$ is also a character of H and that irreducible characters of $\mathfrak{H}/\mathfrak{g}$ correspond to irreducible characters of $\mathfrak{H}$ to see that our L-series for K correspond to L-series for Ω and that primitive L-series remain primitive. However, in Equation A.2.2 the L-series for K will have extra terms for the prime ideals which appear only in the relative discriminant Ω/k. But, any L-series which differ only at finitely many factors we do not want to regard as substantially different. By the way, we will be able to standardize our choice of which of the L-series to pick.

A.3

Now let $\mathfrak{g}$ be a subgroup of $\mathfrak{G}$, and Ω be the subfield of K corresponding to $\mathfrak{g}$. Then $\mathfrak{g}$ is the Galois group of K/Ω.

Let Δ be a representation of $\mathfrak{g}$, Γ_{Δ} the representation of $\mathfrak{G}$ induced by Δ, ψ and χ_{ψ} the corresponding characters of Δ and Γ_{Δ}. Now if we let all the L-series be those where the products only include the primes relatively prime to the relative discriminant K/k then we have the following fundamental theorem:

Theorem A.3.1. *With the just described convention we have*

$$L(s,\psi;\Omega) = L(s,\chi_{\psi};k). \tag{A.3.1}$$

Proof: In Ω let $\mathfrak{p} = \mathfrak{q}_1\mathfrak{q}_2\ldots\mathfrak{q}_r$, where $\mathfrak{p}$ does not divide the relative discriminant of K/k. $\mathfrak{q}_i$ has relative degree l_i over k. Let $\mathfrak{P}_i$ be a prime divisor of $\mathfrak{q}_i$ in Ω with $\mathfrak{P}_i = \tau_i\mathfrak{P}_1$. For every A in K apply

$$\sigma A \equiv A^{N\mathfrak{p}} \mod \mathfrak{P}_1.$$

We set

$$\sigma_i = \tau_i\sigma\tau_i^{-1},$$

so for every A in K we have the equation

$$\sigma_i A \equiv A^{N\mathfrak{p}} \mod \mathfrak{P}_i. \tag{A.3.2}$$

Let $\mathbf{N}$ be the norm in Ω, we find that:

$$\sigma_i^{l_i} A \equiv A^{N\mathfrak{p}^{l_i}} \equiv A^{\mathbf{N}\mathfrak{q}_i} \mod \mathfrak{P}_i. \tag{A.3.3}$$

The substitution $\sigma_i^{l_i}$ is the lowest power of σ_i which belongs to $\mathfrak{g}$. On the one hand, applying Equation A.3.3 to the integer $A = \alpha$ in Ω, by Fermat's little theorem:

$$\sigma_i^{l_i} \alpha \equiv \alpha \mod \mathfrak{P}_i,$$

by our assumption about $\mathfrak{p}$, $\sigma_i^{l_i}\alpha = \alpha$. On the other hand for any α in Ω:

$$\sigma_i^{l_i} \alpha = \alpha \equiv \alpha^{N\mathfrak{p}^{\nu}} \mod \mathfrak{P}_i,$$

it thus follows from Equation A.3.2 that $N\mathfrak{p}^{\nu} \geq \mathbf{N}\mathfrak{q}_i$ and $\nu \geq l_i$.

In Ω to the prime ideal $\mathfrak{q}_i$ we assign the substitution $\sigma_i^{l_i}$.

We now state:

Two cosets $\mathfrak{g}\sigma_\nu^a\tau_\nu$ and $\mathfrak{g}\sigma_\mu^b\tau_\mu$ are equal only when $\nu = \mu$ and $a \equiv b \mod l_\nu$.

Indeed, then $\sigma_\nu^a\tau_\nu$ would have the form:

$$\sigma_\nu^a\tau_\nu = \tau_0\sigma_\mu^b\tau_\mu,$$

where τ_0 is in $\mathfrak{g}$. By the definitions of σ_ν and σ_μ we get that for τ_0:

$$\tau_0 = \sigma_\nu^a\tau_\nu\tau_\mu^{-1}\sigma_\mu^{-b} = \tau_\nu\sigma^{a-b}\tau_\nu^{-1}.$$

So when $\tau_\mu\mathfrak{P}_i = \mathfrak{P}_\mu$ one finds $\sigma\mathfrak{P}_1 = \mathfrak{P}_1$ and [4]:

$$\tau_0\mathfrak{P}_\mu = \tau_\nu\mathfrak{P}_1 = \mathfrak{P}_\nu.$$

Thus the substitution τ_0 sends the prime $\mathfrak{P}_\mu$ dividing $\mathfrak{q}_\mu$ to the prime $\mathfrak{P}_\nu$ dividing $\mathfrak{q}_\nu$. However, since τ_0 is an element of $\mathfrak{g}$, thus $\tau_0\mathfrak{q}_\nu = \mathfrak{q}_\nu$, so $\mathfrak{P}_\nu$ is a prime divisor of $\mathfrak{q}_\mu$. This is only true for $\mu = \nu$. Then, since $\mathfrak{g}\sigma_\nu^a - \mathfrak{g}\sigma_\nu^b$, we also have $a \equiv b \mod l_\nu$.

The coset $\mathfrak{g}\sigma_\nu^a\tau_\nu$ can also be written $\mathfrak{g}\tau_\nu\sigma^a$. There are $l_1 + l_2 \ldots l_r$ different cosets of this form. The sum of the relative degrees is the degree of the extension Ω/k, this is also the index of $\mathfrak{g}$ in $\mathfrak{G}$. So we can partition $\mathfrak{G}$ into cosets of $\mathfrak{g}$ with, using the notation of Equation A.1.4, the S_i being the following:

$$\tau_1, \tau_1\sigma, \ldots \tau_1\sigma^{l_1-1}, \tau_2, \tau_2\sigma, \ldots\ldots \tau_r, \tau_r\sigma \ldots \tau_r\sigma^{l_r-1}.$$

The element σ is assigned the matrix B_σ by the representation induced by Δ given by Equation A.1.5:

$$B_\sigma = (A_{S_i\sigma S_k^{-1}}) = (A_{\tau_\nu\sigma^{a-b+1}\tau_\mu^{-1}}).$$

Now, if $\tau_\nu\sigma^{a-b+1}\tau_\mu^{-1}$ is in $\mathfrak{g}$, then $\tau_\nu\sigma^{a-b+1}$ is in $\mathfrak{g}\tau_\mu$, and so we get that this happens only when $\nu = \mu$, $a - b + 1 \equiv 0 \mod l_\nu$.

Consider the matrix B_σ, it decomposes into:

$$B_\sigma = \begin{pmatrix} C_1 & 0 & \ldots & 0 \\ 0 & C_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & C_r \end{pmatrix},$$

[4] σ belongs to the decomposition group of $\mathfrak{P}_1$.

where C_ν is of the form $(A_{\tau_\nu \sigma^{a-b+1} \tau_\nu^{-1}})$. The only terms which come into consideration are those where $a - b + 1 \equiv 0 \mod l_\nu$. For $a = 0, 1, \ldots l_\nu - 2$, $b = a + 1$, and for $a = l_\nu - 1$, $b = 0$. C_ν has the following form, where E is the appropriate identity matrix:

$$C_\nu = \begin{pmatrix} 0 & E & 0 & \ldots & 0 \\ 0 & 0 & E & 0 \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & E \\ A_{\sigma_\nu}^{l_\nu} & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Thus we find that the characteristic function is:

$$\begin{aligned} |E - tB_\sigma| = \prod_{\nu=1}^{r} |E - tC_\nu| &= \prod_{\nu=1}^{r} \begin{vmatrix} E & -tE & 0 & \ldots & 0 \\ 0 & E & -tE & 0 \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -tE \\ -tA_{\sigma_\nu}^{l_\nu} & 0 & 0 & \ldots & E \end{vmatrix} \\ &= |E - t^{l_\nu} A_{\sigma_\nu}^{l_\nu}|. \end{aligned}$$

To get the last equality take the first column multiply by t and add it to the second column, then multiply the second column by t and add to the third, etc.

In our formula we have used the choice of coset representatives, and our formula depends on this choice. However, if we change our choice Equation A.1.5 gives us an equivalent matrix, and so the characteristic function is independent of this choice.

So the contribution of the prime ideal $\mathfrak{p}$ to $L(s, \chi_\psi; k)$ is:

$$\frac{1}{|E - N\mathfrak{p}^{-s} B_\sigma|} = \prod_{\nu=1}^{r} \frac{1}{|E - N\mathfrak{p}^{-l_\nu s} A_{\sigma_\nu}^{l_\nu}|} = \prod_{\nu=1}^{r} \frac{1}{|E - \mathbf{N}\mathfrak{q}_\nu^{-s} A_{\sigma_\nu}^{l_\nu}|}.$$

Now we have already seen that $\sigma_\nu^{l_\nu}$ is assigned to the prime ideal $\mathfrak{q}_\nu$. Thus the right hand side is exactly the contribution of the prime divisors of $\mathfrak{p}$ to the function $L(s, \psi; \Omega)$. Therefore, Theorem A.3.1 is proved.

A.4

The theorem we have just proved allows us to write the zeta function of a subfield in terms of primitive L-series.

For the principal character $\chi = 1$, corresponding to the representation by the matrix (1), the L-series $L(s, \chi_1; k)$ is the zeta function of the ground field (up to finitely many factors).

Now if Ω is the Galois group of $\mathfrak{g}$ and ψ_1 the principal character of $\mathfrak{g}$, then we also have $L(s, \psi_1; \Omega) = \zeta_\Omega(s)$. The representation Π_Ω induced by ψ_1 is the representation of $\mathfrak{G}$ as group of permutations of the cosets of $\mathfrak{g}$ (if Ω coincides with the Galois extension K, then this is just the Galois group of Ω). The corresponding character $\chi_\Omega(\sigma)$ is the number of letters fixed by the permutation in Π_Ω corresponding to σ, as can be determined easily. So set:

$$\chi_\Omega(\sigma) = \sum_{i=1}^{\mathbf{x}} g_i \chi^i(\sigma),$$

because of Equation A.1.2

$$g_i = \frac{1}{n} \sum_{\sigma} \chi_\Omega(\sigma) \chi^i(\sigma^{-1}) \tag{A.4.1}$$

(n is the size of $\mathfrak{G}$, or the relative degree of K), in connection with Theorem A.3.1 and (14) this yields:

$$\zeta_\Omega(s) = \prod_{i=1}^{\mathbf{x}} (L(s, \chi^i))^{g_i}, \tag{A.4.2}$$

which is the decomposition which we wanted (up to finitely many factors).

For the field K corresponding to the regular representation in particular we get the simple formula:

$$\zeta_K(s) = \prod_{i=1}^{\mathbf{x}} (L(s, \chi^i))^{f_i}. \tag{A.4.3}$$

Formula Equation A.4.2 actually contains all relationships between the zeta functions of the subfields. One simply eliminates the $L(s, \chi^i)$ for all Ω to get the relationship between the ζ_Ω. The equations Equation A.4.2 are to be regarded in this sense as a "parametric" representation of the relations. That one really gets all the relations (if we take the base field to be the rational numbers), we will show later [5]. Thus the problem of all relations is essentially solved.

We can give another formulation of this result. One can see that the decomposition in Equation A.4.2 of $\zeta_\Omega(s)$ runs over all irreducible factors of the group determinant. So we can say:

All relations between the zeta functions of the subfields are given by relations between the group determinants of the representation of $\mathfrak{G}$ as transitive group of permutations where we replace the group determinants by the appropriate zeta functions.

The relations gotten in this way a priori only apply up to finally many factors. Because of the functional equation due to Hecke, they are actually exact relations[6].

Naturally the same considerations also apply to the relations between the L-series of the subfield.

A.5

Now we must examine whether in the abelian case, these L-series coincide with the usual L-series.

When K/k is an abelian extension, each conjugacy class of substitutions consists of only a single element, and so Equation A.2.1 gives one element σ for all the prime factors $\mathfrak{P}$ of $\mathfrak{p}$.

So here we can replace Equation A.2.1 with the condition

$$\sigma A \equiv A^{N\mathfrak{p}} \mod \mathfrak{p}. \tag{A.5.1}$$

The irreducible representations of the group $\mathfrak{G}$ have dimension 1 and so are just the usual group characters $\chi^i(\sigma)$ of $\mathfrak{G}$. Therefore this becomes:

$$L(s, \chi^i) = \prod_p \frac{1}{1 - \frac{\chi^i(\sigma)}{N\mathfrak{p}^s}}, \tag{A.5.2}$$

where σ is the substitution corresponding to the ideal $\mathfrak{p}$.

Now let K be the class field [7] for the group of ideal classes $C_1, C_2, \ldots C_n$ of the modulus $\mathfrak{m}$ of k, the prime ideals from the principal class C_1 are exactly those who split completely in K. The equality of our L-series with the normal ones would be proved if we could show:

Theorem A.5.1 (Artin Reciprocity). *a) The substitution σ depends only on the ideal class C_i containing $\mathfrak{p}$.*

b) The correlation between ideal classes and substitutions is a bijection and gives an isomorphism between $\mathfrak{G}$ and the class group. That is, the product of two substitutions corresponds is assigned to the product of the appropriate two ideal classes.

[5] See E. Artin: Über die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann. Bd. 89, to find particular cases of these relations

[6] E. Hecke: Über eine neue Anwendung der Zetafunktionen auf die Arithmetik der Zahlkörper. Göttinger Nachrichten 1917.

[7] See Teiji Takagi: Über eine Theorie des relativ Abelschen Zahlkörpers, Journal of the College of Science, Tokyo 1920. Also in the sequel we will quote Takagi's results from this paper.

Indeed, we would then have that ever character of $\mathfrak{G}$ corresponds to a character of the class group. Therefore each of our L-series is also a normal L-series. Furthermore all the normal L-series come up this way. So we would have shown that our new definition is really a generalization of the old one.

Theorem A.5.1 is also of interest in its own right. Indeed, it gives explicitly the isomorphism between $\mathfrak{G}$ and the class group. In the case of a cyclic extension our theorem becomes the general reciprocity law (if k contains the appropriate root of unity), this agreement means that we must understand Theorem A.5.1 as the formulation of the general reciprocity law in any field (also without unit root), even if the wording seems somewhat strange to us at first sight.

Having said this, it only falls to reason that we cannot prove this theorem except in the cases where reciprocity laws have already been proven, thus for fields K of prime degree and fields composed of these. For general extensions we must postulate this result. For the rest of the paper we will treat this theorem as though it were proved and explore its consequences.

We proceed gradually through the accessible cases. At the end this proof is as general as possible, but we go through it step by step in order to make the necessary conditions more clear.

1. The principal class C_1 is the only class which corresponds to the identity substitution.

Proof: For every A in K: $A \equiv A^{N\mathfrak{p}} \mod \mathfrak{p}$, also $\mod \mathfrak{P}$, where $\mathfrak{P}$ is a prime divisor of $\mathfrak{p}$, so $\mathfrak{P}$ has relative degree 1. By Takagi's Theorem 31 $\mathfrak{p}$ is in the principal class. In reverse, if $\mathfrak{p}$ is in the principal class, then it splits completely into primes of relative degree 1 and so our congruence applies to $\sigma = 1$.

2. If we have Theorem A.5.1 for the field K/k then we have it for every subfield Ω/k of K.

Proof: Ω corresponds to the subfield $\mathfrak{g}$ of $\mathfrak{G}$ of order r and index s. $\mathfrak{G} = \sum_{i=1}^{s} \mathfrak{g}S_i$ is the decomposition into cosets. Furthermore, Ω is the class field for the group $H_1, H_2, \ldots H_s$ where

$$H_1 = C_1 + C_2 \ldots + C_r$$

is the principal class (addition here denotes union of sets). By 1., g (the principal element of the quotient group) is assigned to the class H_1 (for Ω/k).

We can write, for example, $H_i = C_i' H_1$. Now, if C_ν is a class in H_1, which corresponds to the substitution τ of K, then τ must belong to $\mathfrak{g}$. So if, in K, the class C_ν corresponds to τ_i, then $C_i C_\nu$ corresponds to $\sigma_i \tau$, so H_i corresponds to $\sigma_i \mathfrak{g}$. Since, conversely, every substitution from $\mathfrak{G}$ is assigned to a class C_i, so every coset $\sigma_i \mathfrak{g}$ corresponds to some H_i. The fact that to $H_i H_k$ corresponds the coset $\sigma_i \sigma_k \mathfrak{g}$ is clear, because we assumed the correspondence for the C_ν.

3. If this theorem is true for two fields whose intersection is k, then it is true for their compositum $K = K_1 K_2$.

Proof: Let $C_1, C_2, \ldots C_n; D_1, D_2, \ldots D_m$ be the class groups of K_1 and K_2 respectively considered as subsets of a common larger group. Let $\mathfrak{g}_1$ be the Galois group of K_1 and $\mathfrak{g}_2$ be that of K_2. The class C_i corresponds to σ_i in $\mathfrak{g}_i$, and the class D_i corresponds to τ_i in $\mathfrak{g}_2$. The Galois group of $K = K_1 K_2$ is the direct product of $\mathfrak{g}_1$ and $\mathfrak{g}_2$, if we determine σ_i to fix the numbers in K_2 and τ_i to fix the numbers in K_i. If we denote the intersection as (C_r, D_s), this is a partition which has K as its class field, and we have:

$$(C_r, D_s)(C_u, D_r) = (C_r C_u, D_s D_v).$$

Let A_1 and A_2 be generators of K_1 and K_2 and $A = \varphi(A_1, A_2)$ a integer in K, finally let $\mathfrak{p}$ be an element of (C_r, D_s), then:

$$A^{N\mathfrak{p}} \equiv \varphi(A_1^{N\mathfrak{p}}, A_2^{N\mathfrak{p}}) \equiv \varphi(\sigma_r A_1, \tau_s A_2) \equiv \sigma_r \tau_s A \mod \mathfrak{p}.$$

Thus (C_r, D_s) corresponds to $\sigma_r \tau_s$ from which everything follows.

Thus it is sufficient to prove our theorem for all cyclic extensions of prime number power degree. We will only be able to complete the proof in the case of prime degree.

4. Let $\zeta = e^{\frac{2\pi i}{m}}$ be an mth root of unity, then our theorem is true for $K = k(\zeta)$ [8].

Proof: If $\mathfrak{p}$ splits into primes of relative degree 1 in K, then we have: $\zeta^{N\mathfrak{p}} \equiv \zeta \mod \mathfrak{p}$, also when $\mathfrak{p}$ is not in m, $N\mathfrak{p} \equiv 1 \mod m$. In the other direction, for any integer $A = \alpha_0 + \alpha_1 + \ldots$ ($\alpha_0, \alpha_1 \ldots$ in k):

$$A^{N\mathfrak{p}} \equiv A \mod \mathfrak{p}.$$

[8] The proof for the class fields with complex multiplication can similar be furnished. This shows how the reciprocity laws can be proven by the transcendental production of the class fields.

$\mathfrak{p}$ must then split as a product of primes of relative degree 1. The prime ideals $\mathfrak{p}$ in the principal class are thus characterized by the congruence $N\mathfrak{p} \equiv 1$. If $\mathfrak{a}$ is an ideal in the same class modulo m as $\mathfrak{p}$, that is with $\mathfrak{a} = \alpha\mathfrak{p}$ and $\alpha \equiv 1 \mod m$ and α totally positive, then also $N\alpha \equiv 1 \mod m$ and therefore $N\mathfrak{a} \equiv 1 \mod m$.

So the class group of K over k has as its principal class all ideals with $N\mathfrak{a} \equiv 1 \mod m$. So for two ideals to be in the same class, it is necessary and sufficient that their norms be congruent mod m.

Now if $A = \alpha_0 + \alpha_1\zeta + \ldots$ is an integer in K, then

$$A^{N\mathfrak{p}} \equiv \alpha_0 + \alpha_1\zeta^{N\mathfrak{p}} + \ldots \mod \mathfrak{p}.$$

Thus the substitution σ corresponding to $\mathfrak{p}$ is also the automorphism: $\sigma = (\zeta, \zeta^N\mathfrak{p})$. By what was said above, thus σ only depends on the class to which $\mathfrak{p}$ belongs. Lastly, by the condition determining the class (congruence of the norms) multiplicativity is obvious, the substitution belonging to the product of the classes is the product of their substitutions. Thus, if two classes have the same substitution, then their quotient which corresponds to the unit ideal is the principal class. Finally, since there are just as many classes as substitution, this correspondence is a bijection.

5. If k contains the root of unity $\zeta = e^{\frac{2\pi i}{l^n}}$, then our theorem is true for any cyclic extension K of degree l^n.

Proof: Let $K = k(\sqrt[l^n]{\mu})$. For every prime ideal $\mathfrak{p}$ relatively prime to l, the existence of ζ in k means that we have the congruence: $N\mathfrak{p} \equiv 1 \mod l^n$.

Therefore,

$$(\sqrt[l^n]{\mu})^{N\mathfrak{p}} \equiv \mu^{\frac{N\mathfrak{p}-1}{l^n}} \sqrt[l^n]{\mu} \equiv \left(\frac{\mu}{\mathfrak{p}}\right) \sqrt[l^n]{\mu} \mod \mathfrak{p},$$

where $\left(\frac{\mu}{\mathfrak{p}}\right)$ is the l^n-th power symbol. Thus, the prime ideal $\mathfrak{p}$ corresponds to the automorphism:

$$\sigma = \left(\sqrt[l^n]{\mu}; \left(\frac{\mu}{\mathfrak{p}}\right) \sqrt[l^n]{\mu}\right).$$

The substance of the general reciprocity law [9] is, however, exactly that $\left(\frac{\mu}{\mathfrak{p}}\right)$ only depends on the class containing $\mathfrak{p}$ (more generally, this is true for any fractional ideal (a) relatively prime to μ). Since, conversely, we can find a $\mathfrak{p}$ such that $\left(\frac{\mu}{\mathfrak{p}}\right)$ has whatever value we like, to each σ corresponds exactly one ideal class. Finally, because of the multiplicative characteristic of $\left(\frac{\mu}{\mathfrak{p}}\right)$, the product of the substitutions corresponds to the product of two classes.

6. Take $K = k(A)$ cyclic of degree l^n, $\zeta = e^{\frac{2\pi i}{l}}$ an lth root of unity, and $\Omega = k(\zeta)$ of degree m, where since m divides $l-1$ it is relatively prime to l. Then, if our theorem holds for the extension $\Omega(A)/\Omega$, it must also hold for K/k.

Proof: Let σ and τ be generators of the Galois groups of K/k and Ω/k. K is the class field for the class group consisting of C^ν ($\sigma^{l^n} = 1$, $C^{l^n} = C_0 =$ the principal class). Ω is the class field for the class group consisting of D^μ ($\tau^m = 1$, $D^m = D_0 =$ the principal class).

Since m and l are relatively prime, the same must be true of K and Ω. From them we make the composite field K^* which is the class field for the class group consisting of (C^ν, D^μ), where this again denotes the intersection.

Now partition the ideals of Ω according to the same modulus used in k and let $\mathfrak{C}_0$ be the class be the class of ideals whose relative norm lies in C_0. We call $\mathfrak{C}_0$ the principal class. Let $\mathfrak{C}'$ be the class of ideals with norm in C^e (the norm of $\mathfrak{a}\mathfrak{C}_0$ is in $\mathbf{N}\mathfrak{a} \cdot C_0$, which lies in one of the classes C^ν), so we choose s such that $ms \equiv e \mod l^n$ and set $\mathfrak{C}' = C^s \cdot \mathfrak{C}'_0$. The norm of $\mathfrak{C}'_0$ falls in C_0, and so $\mathfrak{C}'_0 = \mathfrak{C}_0$. The class $\mathfrak{C} = C\mathfrak{C}_0$ thus generates the class group of Ω and $\mathfrak{C}^{l^n} = \mathfrak{C}_0$. Let K_1 be the class field for this group. The relative norm with respect to Ω of its ideals fall in $\mathfrak{C}_0$, those down to k thus lie in C_0. The relative norm of these ideals also fall in D_0, therefore, they are contained in (C_0, D_0). K_1 is therefore the class field for the same class group as K^*, so by Takagi $K_0 = K^*$.

[9] Teiji Takagi: Über das Reziprozitätsgesetz in beliebigen algebraischen Zahlkörpern. Journal of the College of Science, Tokyo 1922.

The Galois group of K^* consists of $\sigma^\nu\tau^\mu$ and the Galois group of Ω is the subgroup σ^ν. Since our Theorem A.5.1 was assumed for K^*/Ω, we choose this designation so that σ corresponds to the class $\mathfrak{C}$, σ^ν also corresponds to $\mathfrak{C}^\nu$.

Take $\mathfrak{p}$ a prime ideal in (C^r, D^s). Let g_s be the greatest common devisor of m and s and let $m = g_s e_s$, so by the decomposition theorem, $\mathfrak{p}$ in Ω factors as a product of e_s prime ideals $\mathfrak{q}_i$ of degree g_s. Now we have:

$$\sigma^\nu A \equiv A^{N\mathfrak{p}} \mod \mathfrak{p},$$

so $\sigma^{\nu g_s}$ corresponds to $\mathfrak{q}_i$ in Ω. Thus all the $\mathfrak{q}_i$ are in the class $\mathfrak{C}^{\nu g_s}$, their norm $\mathfrak{p}^{g_s}$ thus lies in $C^{m\nu g_s}$. g_s is a divisor of m and hence relatively prime to l, therefore $\mathfrak{p}$ is in the class $C^{m\nu}$ and thus only depends on σ^ν. Since m is relatively prime to l, $C^{m\nu}$ runs over all classes as ν varies and $C^{m(\nu+\mu)}$ corresponds to $\sigma^{\nu+\mu} = \sigma^\nu\sigma^\mu$.

Thus, by 5., our Theorem A.5.1 for extensions of prime number degrees is proved, thus it is also proven for fields composed from these (by 3.)

A.6

Now we return to the case of a general field K (having assumed Theorem A.5.1). Let σ be an element of $\mathfrak{G}$ of order $m(\sigma)$, let $\mathfrak{g}^\sigma$ the group of powers of σ, and let Ω be the subfield of K corresponding to $\mathfrak{g}^\sigma$.

Let $\psi_i^{(\sigma)}(\tau)$ be a character (hence a usual abelian group character) of $\mathfrak{g}^\sigma$ ($i = 1, 2, \ldots m(\sigma)$, where $i = 1$ is the principal character), thus we make the L-series in Ω for the extension K:

$$L(s, \psi_i^{(\sigma)}).$$

By applying Equation A.1.5 and Equation A.1.7, if we fix σ, it follows that:

$$L(s, \psi_i^{(\sigma)}) = \prod_{\nu=1}^{\mathbf{x}} (L(s, \chi^\nu))^{r_{i\nu}^{(\sigma)}} \tag{A.6.1}$$

($i = 1, 2, \ldots m(\sigma)$). Because of our assumption, the left hand side is just an Abelian L-series. Therefore, Equation A.6.1 allows us to prove the analytic continuation of our functions. First $L(s, \chi^1) = \zeta_k(s)$. Thus its analytic continuation has already been proven.

For $\nu > 1$ we want to show that $L(s, \chi^\nu)$ can be expressed as a product of rational powers of $L(s, \chi^\nu)$ for all σ, without using the principal character $\psi_1^{(\sigma)}$.

Because of Equation A.6.1 it is enough to show the $\mathbf{x}$ equations

$$\sum_{\sigma \neq 1} \sum_{i=2}^{m(\sigma)} r_{i\nu}^{(\sigma)} x_i^\sigma = \delta_{k\nu} \tag{A.6.2}$$

($\nu = 1, 2, \ldots \mathbf{x}$) can be solved for any fixed k and the series $2, 3, \ldots \mathbf{x}$.

If for $i > 1$ we set $r_{i1} = 0$ then Equation A.6.2 is still true for $\nu = 1$, so we only need to find a solution for Equation A.6.2 for $\nu > 2$. Thus this is equivalent to the matrix $(r_{i\nu}^{(0)})$ where $\sigma \neq 1$, $i = 2 \ldots m(\sigma)$, and $\nu = 2, \ldots \mathbf{x}$ (where σ and i indicate the column and ν indicates the row) having a non-vanishing $(\mathbf{x} - 1)$-th sub-determinant. This is depends on the fact that the equations

$$\sum_{\nu=2}^{\mathbf{x}} r_{i\nu}^{(\sigma)} y_\nu = 0, \tag{A.6.3}$$

for every $\sigma \neq 1, i \geq 2$ has only the solution $y_\nu = 0$.

In order to show this we multiply Equation A.6.3 by $\psi_i^{(\sigma)}(\tau)$ (understood to mean any element of $\mathfrak{g}^\sigma$, $\tau = 1$ is included) and summing over i from 2 to $m(\sigma)$. By Equation A.1.6 this gives

$$\sum_{\nu=2}^{\mathbf{x}} (\chi^\nu(\tau) - r_{1\nu}^{(\sigma)}) y_r = 0 \text{ or}$$

$$\sum_{\nu=2}^{\mathbf{x}} \chi^{\nu}(\tau) y_{\nu} = \sum_{\nu=2}^{\mathbf{x}} r_{1\nu}^{(\sigma)} y_{\nu}.$$

The left hand side has the same value for all τ in $\mathfrak{g}^{\sigma}$, because the righthand side does not depend on τ. Since $\tau = 1$ is an element of all the $\mathfrak{g}^{\sigma}$, so the left hand side has the same value for all τ in $\mathfrak{G}$, we call this common value $-y_1 = -y_1\chi^1(\tau)$. Our equations thus become:

$$\sum_{\nu=1}^{\mathbf{x}} \chi^{\nu}(\tau) y_{\nu} = 0$$

for all τ. Multiply this by $\chi^i(\nu^{-1})$ and sum over all ν, then because of Equation A.1.2 this becomes:

$$n y_i = 0$$

from which everything follows.

Therefore, since we can express $L(s, \chi^{\nu})$ in terms of Abelian L-series, they are continuable to the whole complex plane with at most a branch points of finite order. For $\nu > 1$ they are regular and non-zero at $s = 1$ and share all other properties of the usual L-series.

Now we modify the original definition of our L-series. Only finitely many factors are affected by this alteration, so that all relations derived so far remain valid for the new L-series up to finally many factors, if we define the most general L-series by formula Equation A.2.7. These new L-series, however, give us a simple functional equation in a suitable branch, since we have functional equations for the Abelian L-series. From the conclusions of Mr. Hecke, therefore all formulas derived so far apply exactly, if we use our new definition of the L-series. In the case of circling a possible branch point the L-functions multiply by root of unity. Finally we notice that our new definition is independent of which decomposition by Abelian L-series we used (again because of the functional equation).

The functional equation takes the form [10]:

$$L(1-s, \overline{\chi^i}) = a_i A^s (\Gamma(s))^{l_i^{(1)}} \left(\cos\frac{s\pi}{2}\right)^{l_1^{(2)}} \left(\sin\frac{s\pi}{2}\right)^{l_1^{(3)}} L(s, \chi^i),$$

where $\overline{\chi^i}$ is the inverse character of χ^i and a_i is a root of unity which depends on which branch of $L(s, \chi^i)$ is chosen.

To find the $l_i^{(1)}$ we plug the functional equation into Equation A.1.3. On the right hand the a power of the Γ-factor is

$$\sum_{\nu=1}^{\mathbf{x}} r_{i\nu}^{(\sigma)} l_{\nu}^{(1)},$$

on the left hand it is $m \cdot \frac{n}{m(\sigma)}$ (the degree of the field Ω), where m is degree of k. Therefore, it must be that:

$$\sum_{\nu=1}^{\mathbf{x}} r_{i\nu}^{(\sigma)} l_{\nu}^{(1)} = m\frac{n}{m(\sigma)}$$

for every i and σ. Multiply by $\psi_i^{(\sigma)}(\nu)$ and sum over i, then by Equation A.1.6:

$$\sum_{\nu=1}^{\mathbf{x}} \chi^{\nu}(\tau) l_{\nu}^{(1)} = mn \cdot \epsilon_{\tau},$$

where $\epsilon_{\tau} = 1$ or 0 depending on wither $\tau = 1$ or $\tau \neq 1$.

Multiply this by $\chi^i(\tau^{-1})$ and sum over τ, then by Equation A.1.2: $n l_i^{(1)} = mnf_i$ or $l_i^{(1)} = mf_i$.

Similarly one can find the other constants, and in summary we get:

[10] E. Landau: Über Ideale and Primideale in Idealklassen. Math Zeitschrift Volume 2, page 104, theorem LXVI

Theorem A.6.1. *The primitive L-series $L(s,\chi^i)$ can be continued to the whole complex plane with only branch points of finite order. For $i>1$, if we plug in $s=1$, the function is regular and non-zero. On the line $\Re(s)=1$ and in a region $(\log T)^{-1}$ to the left of $\Re(s)=1$ it is free of zeroes. They have a functional equation of the form:*

$$\frac{L(1-s,\overline{\chi^i})}{L(s,\chi^i)}=\epsilon_i\left(\frac{2}{(2\pi)^s}\right)^{mf_i}(\alpha_i|\Delta|^{f_i})^{s-\frac{1}{2}}\left(\cos\frac{s\pi}{2}\right)^{l_1^{(2)}}\left(\sin\frac{s\pi}{2}\right)^{l_1^{(3)}}(\Gamma(s))^{mf_i}. \tag{A.6.4}$$

In that formula Δ is the discriminant of k, α_i is a product of rational powers of rational numbers and ϵ_i is a number which depends on the branch with $|\epsilon_i|=1$.

Furthermore, $l_i^{(2)}$ and $l_i^{(3)}$ are rational numbers.

In the same way one can determine these relations with even more clarity; without much difficulty one can at least see that the order of the branches can only be products of primes factors of n.

However, it will require completely new methods to show that the L-series are associated to entire functions (aside from the principal character).

A.7

With these results because of Equation A.1.2 we can confirm a theorem of Frobenius [11].

In addition, one can strengthen this result. From Equation A.2.5 it follows from well known methods that:

$$\sum_{N\mathfrak{p}\leq x}\chi^i(\mathfrak{p})=\delta_{1i}\mathrm{Li}(x)+O(xe^{-\alpha\sqrt{\log x}}), \tag{A.7.1}$$

where $\delta_{11}=1$ and $\delta_{1i}=0$ otherwise.

Now let $\mathfrak{C}_r$ be a fixed class of substitutions and σ a substitution in $\mathfrak{C}_r$ and let $\pi(x,\mathfrak{c}_r)$ be the number of prime ideals in $\mathfrak{C}_r$ in k with $N\mathfrak{p}\leq x$.

Multiplying Equation A.7.1 by $\chi^i(\sigma^{-1})$ and sum over i, so by Equation A.1.3:

$$\frac{n}{h_r}\pi(x,\mathfrak{C}_r)=\mathrm{Li}(x)+O(x\cdot e^{-\alpha\sqrt{\log x}}).$$

Theorem A.7.1. *Let $\pi(x,\mathfrak{C}_i)$ be the number of prime ideals with $N\mathfrak{p}\leq x$, found in the class $\mathfrak{C}_i$, then:*

$$\pi(x,\mathfrak{C}_i)=\frac{h_r}{n}Li(x)+O(x\cdot e^{-\alpha\sqrt{\log x}}). \tag{A.7.2}$$

The density of these prime ideals is thus equal to the density in $\mathfrak{G}$ of the substitutions from $\mathfrak{C}_i$. In particular, there are infinitely many prime ideals belonging to each class $\mathfrak{C}$.

This theorem is a generalization of the theorem on arithmetic progressions which it (with the help of our reciprocity theorem) contains as a special case. Its true meaning still awaits clarification.

A.8

Theorem A.8.1. *With the ground field R of rational numbers there are no multiplicative relations between the primitive L-series.*

Proof: We have

$$\prod_{i=1}^{x}(L(s,\chi^i))^{x_i}=1.$$

By Equation A.2.5 it follows that:

$$\sum_{\mathfrak{p}^\nu}\left(\sum_{i=1}^{x}x_i\chi^i(p^\nu)\right)\frac{1}{\nu p^{\nu s}}=0.$$

[11] See the work quoted in footnote 3, §5 Formulas (16) and (18).

By Theorem A.7.1 in each class there are infinitely many prime numbers. Therefore, for all τ and $\mathfrak{G}$:

$$\sum_{i=1}^{x} x_i \chi^i(\tau) = 0.$$

From this it follows by well-known methods that:

$$x_i = 0.$$

The just proven theorem does not apply generally to any ground field, since then the conjugate prime ideals can destroy everything. Indeed one can easily design oneself examples in which the same L-series are assigned to conjugate characters (already in quadratic fields).

With Theorem A.8.1 we can determine all relationships between any ζ-functions or L-series. We look at a sufficiently large Galois extension which contains all the fields in which the functions of question are defined. These split into primitive L-series of R. By elimination we receive all relations, since each relation would reduce to a relation between the primitive L-series.

A.9

In the end the results we have proved may be applied to the simplest field which is not made up of abelian fields, that is an icosahedral field. We first remark that, in this case, the reciprocity laws in question are actually proven. In fact, apart from 4, only the simple prime factors 3 and 5 go into 60, and also the 4 part of the Galois group is only the Klein 4-group, since the icosahedral group has no element of order 4, rather contains only elements of order 2.

There are 5 conjugacy classes $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4, \mathfrak{C}_5$ which have $1, 15, 20, 12, 12$ elements respectively. The density of prime ideals which belong to these classes is therefore, $\frac{1}{60}, \frac{1}{4}, \frac{1}{3}, \frac{1}{5}, \frac{1}{5}$.

Furthermore we have 5 irreducible characters of degrees 1, 3, 3, 4, 5, and we call their L-series $L_3^{(1)}, L_3^{(2)}, L_4, L_5$ (the trivial character corresponds to the zeta function ζ of the ground field k).

For the ζ functions of the subfields (the index refers to the relative degree of the field) we can easily find according to our methods:

$$\begin{aligned}
\zeta_5 &= \zeta L_4 \\
\zeta_6 &= \zeta L_5 \\
\zeta_{10} &= \zeta L_4 L_5 \\
\zeta_{12} &= \zeta L_3^{(1)} L_3^{(2)} L_5 \\
\zeta_{15} &= \zeta L_4 (L_5)^2 \\
\zeta_{20} &= \zeta L_3^{(1)} L_3^{(2)} (L_4)^2 L_5 \\
\zeta_{30} &= \zeta L_3^{(1)} L_3^{(2)} (L_4)^2 (L_5)^3 \\
\zeta_{60} &= \zeta (L_3^{(1)} L_3^{(2)})^3 (L_4)^4 (L_5)^5
\end{aligned} \tag{A.9.1}$$

In the case of an icosahedral field all of the L-series are well-defined functions. From the first to formulas this follows for L_4 and L_5. Furthermore the icosahedral field is a cyclic extension of degree 5 of its subfield of degree 12. Thus four of the L-series must be situated there. From our formulas for ζ_{60} and ζ_{12} we see that the product of these L-series is:

$$(L_3^{(1)} L_3^{(2)})^2 (L_4)^4 (L_5)^4.$$

Now the number 12 must be written as a sum of 3, 4, and 5 (for each of the L-series) in such a way that the above product appears. One easily sees that the only possible allocations are $L_3^{(1)} L_4 L_5$ and $L_3^{(2)} L_4 L_5$. Two (conjugate) characters each have this L-series (here we have an example of a field with identical L-series). From this we can conclude that $L_3^{(1)}$ and $L_3^{(2)}$ are well-defined functions.

Furthermore the function L_5 is whole. Indeed the field Ω_{15} is a cyclic extension of σ_5 so there are two L-series found there. However, L_5 is clearly the only possibility. Thus the two L-series of Ω_5 collapse into the single one L_5.

Ω_{12} is a quadratic extension of Ω_6, so in Ω_6 there is one L-series, which must be $L_3^{(1)} \cdot L_3^{(2)}$ (by Equation A.9.1). Similarly Ω_{20} is a quadratic extension of Ω_{10} and its L-series is $L_3^{(1)} L_3^{(2)} L_4$. The other fields do not contribute anything substantially new. Thus the functions $L_3^{(1)} L_4 L_5$, $L_3^{(2)} L_4 L_5$, $L_3^{(1)} L_3^{(2)}$, $L_3^{(1)} L_3^{(2)} L_4$ are all whole functions.

From the formulas in Equation A.9.1 one can read off all the relationships which I described in the work quoted in footnote 5. Likewise one detects the divisibility of ζ_6, ζ_{12}, and ζ_{60} by the zeta-function ζ of the ground field.

Hamburg, Mathematics Seminar, July 1923.

Bibliography

[**Ar**] Artin, Emil. "Collected Papers," Springer-Verlag, New York, 1965.

[**Ap**] Apostol, Tom. "Introduction to Analytic Number Theory," 5th ed., Springer-Verlag, New York, 1998.

[**B**] Brauer, Richard. "Collected Papers," MIT Press, Cambridge, Mass., 1980.

[**B-S**] Borevich, Z.I. and Shafarevich, I.R. "Number Theory," Academic Press, New York, 1966.

[**C1**] Conrad, Keith. "The Origin of Representation Theory," L'Ensignement Matheématique, t. 44 (1998) p.361-392.

[**C2**] Conrad, Keith. "The Splitting Field of $X^3 - 2$ over $\mathbb{Q}$," unpublished notes.

[**C-F**] Edited by Cassels, J. and Fröhlich, A. "Algebraic Number Theory," Thompson Book Company, Washington D.C., 1967.

[**C-M-D**] Edited by Chikara, Mitsuo, and Dauben. "The Intersection of History and Mathematics," Science Networks Historical Studies, Volume 15.

[**Da**] Davenport, Harold. "Multiplicative Number Thoery," Markham, Chicago, 1967.

[**De**] Dedekind, Richard. "Gesammelte mathematische Werke," Druck un Verlag, Braunshweig, 1930.

[**Di1**] Dirichlet, Peter Gustav Lejeune. "Lectures on Number Theory," AMS, 1999.

[**Di2**] Dirichlet, Peter Gustav Lejeune. "G. Lejeune Dirichlet's Werke." Chelsea Publishing Company, New York, 1969.

[**Eu1**] Euler, Leohnard. "Introduction to Analysis of the Infinite, Book 1," Springer-Verlag, New York, 1988.

[**Eu2**] Euler, Leohnard, "Opera Omnia," Lipsiae et Berolini, 1911-.

[**Ed**] Edwards, H.M. "Riemann's Zeta Function," Academic Press, New York, 1974.

[**Frob**] Frobenius, Georg. "Gesammelte Abhandlungen," Springer-Verlag, Berlin, 1968.

[**Fröh**] Edited by Frölich, A. "Algebraic Number Fields," Academic Press, London, 1977.

[**F-T**] Frölich, A. and Taylor, M.J. "Algebraic Number Theory," Cambridge University Press, Cambridge, 1991.

[**Ha**] Hadamard, Jacques. "Oeuvres de Jacques Hadamard," Centre National de la Recherche Scientifique, Paris, 1968.

[**He**] Hecke, Erich. "Mathematische Werke," Vandernhoeck & Ruprecht, Göttingen, 1959.

[**Hi**] Hilbert, David. "The Theorey of Algebraic Number Fields (Zahlbericht)," Springer-Verlag, Berlin, 1991.

[**J**] Janusz, Gerald. "Algebraic Number Fields, Second Edition," AMS, 1996.

[**Kr**] Kronecker, Leopold. "Leopold Kronecker's Werke," New York : Chelsea Pub. Co., 1968.

[**Ku**] Kummer, Ernst. "Collected Papers," Springer-Verlag, Berlin, 1975.

[**L1**] Lang, Serge. "Algebraic Number Theory," 3rd ed., Springer-Verlag, New York, 1994.

[**L2**] Lang, Serge. "Complex Analysis," 4th ed., Springer-Verlag, New York, 1999.

[**M**] Mollin, Richard. "Algebraic Number Theory," CRC Press, Boca Raton, Fla, 1999.

[**N**] Neukirch, Jürgen. "Algebraic Number Theory," Springer-Verlag, Berlin, 1999.

[**Se1**] Serre, Jean-Pierre. "Linear Representations of Finite Groups," Springer-Verlag, New York, 1977.

[**Se2**] Serre, Jean-Pierre. "Local Fields," Springer-Verlag, New York, 1979.

[**Se3**] Serre, Jean-Pierre. "Analytic Number Theory," unpublished Harvard lecture notes, to be published by the AMS.

[**Sn**] Snyder, Noah. "A Brief History of Class Field Theory from 1880-1930," unpublished.

[**Sp**] Speiser, A. Die Zergungsgruppe. J. reine angew. Math. Vol. 149, pp. 174-188 (1919).

[**S-T**] Silverman, Joseph and Tate, John. "Rational Points on Eliptic Curves," Springer-Verlag, New York, 1992.

[**S-L**] Stevenghagen and Lenstra, "Chebotarev and his Density Theorem," The Mathematical Intelligencer Vol. 18, No. 2, pp. 26-37.

[**T**] Takagi, Teiji. "Teiji Takagi Collected Papers," 2nd ed.," Springer-Verlag Tokyo, New York, 1990.

[**W1**] Weber, Heinrich. "Theorie der Abel'schen Zahlkorper I, II," Acta math. Stock., (1886), 8, 193-263; (1897), 49, 83-100.

[**W2**] Weber, Heinrich. "Lehrbuch der Algebra," 3rd ed., Chelsea Publsihing Company, New York, [1961?].