Finite Monodromy and Artin Representations

Emma Lien
Louisiana State University

Follow this and additional works at: https://repository.lsu.edu/gradschool_dissertations

Part of the Number Theory Commons

Recommended Citation
Lien, Emma, "Finite Monodromy and Artin Representations" (2024). LSU Doctoral Dissertations. 6456. https://repository.lsu.edu/gradschool_dissertations/6456

This Dissertation is brought to you for free and open access by the Graduate School at LSU Scholarly Repository. It has been accepted for inclusion in LSU Doctoral Dissertations by an authorized graduate school editor of LSU Scholarly Repository. For more information, please contact gradetd@lsu.edu.
FINITE MONODROMY AND ARTIN REPRESENTATIONS

A Dissertation
Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Emma Lien
B.S., University of Central Florida, 2018
May 2024
This thesis is dedicated to my advisor Dr. Ling Long, whose guidance and encouragement made this dissertation possible.
Table of Contents

List of Tables ................................................................. v

Nomenclature, Symbols, Acronyms ........................................ vi

Abstract ................................................................. vii

Chapter 1. Introduction ................................................ 1

Chapter 2. Preliminaries ................................................ 4
  2.1. Modular Forms .................................................. 4
  2.2. Class Field Theory ................................................. 10
  2.3. Multiplicative Characters of Finite Fields ....................... 14
  2.4. Hypergeometric Functions ....................................... 17

Chapter 3. Weight 1 Eta-Quotients ..................................... 25
  3.1. Eta-Quotients .................................................. 25
  3.2. Reciprocity laws for weight 1 eta-quotients and the first main result . 26
  3.3. The Serre-Deligne Theorem ..................................... 31
  3.4. Main Results .................................................. 36
  3.5. Weight 1 eta-quotients ......................................... 41

Chapter 4. Finite Monodromy ............................................. 46
  4.1. Decompositions and Balanced Datum ............................... 46
  4.2. Applications .................................................. 49
  4.3. Future directions .............................................. 56

Bibliography ................................................................. 57

Vita ................................................................. 60
List of Tables

3.1. Reciprocity laws for non-cusp eta-quotients ........................................ 29
3.2. Reciprocity laws for cusp form eta-quotients .......................................... 30
Nomenclature, Symbols, Acronyms

As is standard, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ denote the set of integers, rational numbers, real numbers, and complex numbers respectively. For a complex number $z$, $\Re(z)$ and $\Im(z)$ denote the real and imaginary parts. For a field $F$, we denote a fixed algebraic closure by $\overline{F}$. Additionally, we use $\zeta_n := e^{\frac{2\pi i}{n}}$ for a primitive $n$th root of unity and $\mu_n(F)$ denotes the group of roots of unity in $F$.

For $L/K$ a Galois extension of number fields, we denote the corresponding Galois group $\text{Gal}(L/K)$ and for any unramified prime $p$ of the ring of integers $\mathcal{O}_L$ lying over $\mathfrak{p} := p \cap K$ we denote $\text{Frob}_p$ for the unique element of $\text{Gal}(L/K)$ such that $\text{Frob}_p(\alpha) \equiv \alpha^q \pmod{p}$ with $q = |\mathcal{O}_K/\mathfrak{p}|$.

For a ring $R$, $\text{GL}_n(R)$ (resp. $\text{SL}_n(R)$) denote the group of matrices with entries in $R$ with nonzero determinant (resp. determinant 1) and in the special case of $n = 1$, we use $R^\times$ in place of $\text{GL}_1(R)$. $I_n$ denotes the $n \times n$ identity matrix.

We abbreviate complex multiplication by CM which for an elliptic curve, means it has a larger than normal endomorphism ring and for modular forms, it means that the Fourier coefficients of the form are invariant when twisting by a specific nontrivial quadratic character.
Abstract

Artin representations, which are complex representations of finite Galois groups, appear in many contexts in number theory. The Langlands program predicts that Galois representations like these should arise from automorphic representations and many examples of this correspondence have been found such as in the proof of Fermat’s Last Theorem. This dissertation aims to make an analysis of explicitly computable examples of Artin representations from both sides of this correspondence. On the automorphic side, certain weight 1 modular forms have been shown to be related to Artin representations and an explicit analysis of their Fourier coefficients allows us to identify the exact representation. On the Galois side, certain character sums related to hypergeometric functions have been shown to be related to infinite families of Artin representations, and through the manipulation of these sums we can relate certain cases to known automorphic representations.
Chapter 1. Introduction

For a degree $n$ polynomial $f(x)$ with integer coefficients, an interesting problem is to determine the finite fields, $\mathbb{F}_p$ for $p$ a prime, where $f(x)$ has $n$ distinct roots; in which case we say that $f$ “splits” over $\mathbb{F}_p$. Conditions for describing these primes are sometimes called “reciprocity laws.” See [28] for a more detailed discussion of this. We can reduce this problem to only dealing with $f$ monic and irreducible over the rationals. For simplicity, we will only deal with the finite fields $\mathbb{F}_p$ for $p$ a prime, but the situation is not much harder for finite extensions of these fields. For quadratic polynomials, say $f(x) = x^2 + bx + c$, the solution is well known. For $p \neq 2$, we can apply the quadratic formula and reduce the problem to whether or not the discriminant, $b^2 - 4c$, is a square in $\mathbb{F}_p$. This is then solved by Gauss’s Law of Quadratic Reciprocity. See [2], [22], or [13] for more details.

Theorem 1 (Quadratic Reciprocity). For $p$ an odd prime, define a $p$-periodic arithmetic function, called the Legendre symbol

$$\left( \frac{\cdot}{p} \right) : \mathbb{Z} \to \{0, \pm 1\},$$

$$\left( \frac{a}{p} \right) = \begin{cases} 
0 & \text{if } p \text{ divides } a, \\
-1 & \text{if } a \text{ is not a square modulo } p, \\
1 & \text{if } a \in \mathbb{F}_p^\times \text{ is a square modulo } p.
\end{cases}$$

If $\ell$ is an odd prime with $\ell \neq p$, then

$$\left( \frac{\ell}{p} \right) = (-1)^{\frac{p-1}{2} \frac{\ell-1}{2}} \left( \frac{p}{\ell} \right).$$

For example, let $f(x) = x^2 + x - 1$. To determine the primes where $f$ splits, by which we mean it factorizes completely in $\mathbb{F}_p[x]$, we must determine the finite fields for
which the discriminant, \(1^2 + 4 = 5\), is a square. By Quadratic Reciprocity, \(\left( \frac{5}{p} \right) = \left( \frac{p}{5} \right)\), so 5 is a square modulo \(p\) if and only if \(p\) is a square modulo 5, which is true if and only if \(p \equiv \pm 1 \pmod{5}\).

Moving to cubic polynomials vastly complicates things. For some cubic polynomials, like \(x^3 + x^2 - 2x - 1\), we can form a similar description of the finite fields in which it splits. In fact, this polynomial splits in \(\mathbb{F}_p\) if and only \(p \equiv \pm 1 \pmod{7}\). But for other cubic polynomials, like \(x^3 - 2\), the situation is much different. In fact, \(x^3 - 2\) splits in \(\mathbb{F}_p\) if and only if \(p \equiv 1 \pmod{3}\) and there exist \(a, b \in \mathbb{Z}\) such that \(p = a^2 + 27b^2\). While this condition may seem quite different from the previous congruence conditions, this actually is in fact a kind of congruence condition itself, in particular we can describe this as \(p = a^2 + 3b^2\) with \(b \equiv 0 \pmod{3}\). The difference is that the congruence condition is for the number ring \(\mathbb{Z}[\zeta_3]\) rather than \(\mathbb{Z}\), where \(\zeta_3\) is a primitive third root of unity. So the congruence is imposed on the prime ideals of \(\mathbb{Z}[\zeta_3]\) lying above \(p\). Unlike with \(\mathbb{Z}\) however, congruences over arbitrary number rings are much harder to identify since they typically cannot be translated into congruence conditions over \(\mathbb{Z}\). When the number ring is an order in an imaginary quadratic extension, these congruences can be described quite well using positive definite quadratic forms, as in the case of \(x^3 - 2\), and in turn, these can be related to modular forms (specifically theta series), to obtain information of a more analytic nature. This dissertation takes this motivation in two very different, but related contexts. We will first discuss modular forms and how their Fourier coefficients give us information about how polynomials split over finite fields. In particular, we deal with the problem of finding a polynomial for which a specified modular form gives a reciprocity law.
Then, we will discuss hypergeometric character sums, which can be directly related to the number of roots of a one-parameter family $f_\lambda$ of polynomials with integer coefficients. In this setting, we take the opposite approach of examining a family of polynomials and trying to find modular forms which give a corresponding reciprocity law. The Langland’s program suggests a connection between these two sides and in this dissertation, we will attempt to look at a few explicitly computable examples from both sides.
Chapter 2. Preliminaries

2.1. Modular Forms

We summarize a few basic facts we will need for this dissertation, but for a more thorough treatment, see [6] or [15].

The upper half-plane \( \mathbb{H} := \{ z \in \mathbb{C} | \Im(z) > 0 \} \) admits an action of the matrix group \( SL_2(\mathbb{Z}) \) of integer matrices with determinant one as follows;

\[
\gamma \cdot z := \frac{az + b}{cz + d},
\]

for \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \]

Every point \( z \in \mathbb{H} \) is in the orbit of a point in the fundamental domain

\[
\left\{ z \in \mathbb{H} : |\Re(z)| \leq \frac{1}{2}, \text{ and } |z| \geq 1 \right\}.
\]

The geometry of the compactification of the orbit space, denoted \( X(1) \), has surprising connections in number theory, and, along with their related functions called modular forms, have been of great interest to number theorists in the last century. These modular forms possess many symmetries and were used in showing the Riemann zeta function had a meromorphic continuation to the whole plane.

A weight \( k \) modular form \( f : \mathbb{H} \to \mathbb{C} \) on \( SL_2(\mathbb{Z}) \) is a complex-valued holomorphic function such that for

\[
\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \quad f(\gamma \cdot z) = (cz + d)^k f(z).
\]

Additionally, we require that \( f \) has “moderate growth” at the cusps \( \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{ \infty \} \) which means that \( f(z) \) is bounded as \( z \) approaches any cusp in \( \mathbb{P}^1(\mathbb{Q}) \). If this condition is not necessarily satisfied, we will say that \( f \) is weakly modular and a modular form if it is.
If we point out that $\text{SL}_2(\mathbb{Z})$ is generated by the matrices
\[
\begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix}
\text{ and }
\begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix}
\]
then (2.1) is equivalent to having
\[f(z + 1) = f(z) \text{ and } f(-1/z) = z^k f(z).
\]
In particular, the first of these equations guarantees that $f$ has a Fourier expansion, typically referred to as the $q$-expansion
\[f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \text{ with } q = e^{2\pi i z}.
\]
It is these coefficients $a_n(f)$ that are of significant interest in number theory. They can sometimes appear as the exponential generating function for partition numbers, point counts of varieties over finite fields, and counting points of lattices. One of the simplest examples is given by the weight $k$ Eisenstein series
\[G_k(z) := \sum_{(n,m) \in \mathbb{Z} \setminus \{(0,0)\}} \frac{1}{(mz + n)^k}.
\]
This series is absolutely convergent for $k > 2$ and when $k$ is odd, using condition 2.1 with the negative identity matrix, $G_k(z) = (-1)^k G_k(z)$ implying that no nonzero odd weight forms exist for $\text{SL}_2(\mathbb{Z})$. The normalized Eisenstein series $E_k(z) = \frac{1}{2\zeta(k)} G_k(z)$, with $\zeta(s)$ the Riemann zeta function, has the expansion
\[E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \tag{2.2}
\]
where $B_k$ denotes the $k$th Bernoulli number and
\[\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}.
\]
The importance of Eisenstein series is made clear due to the fact that any modular form of \( \text{SL}_2(\mathbb{Z}) \) can be expressed with polynomials in \( E_4 \) and \( E_6 \). In fact, the graded algebra of modular forms of \( \text{SL}_2(\mathbb{Z}) \) is isomorphic to \( \mathbb{C}[E_4, E_6] \). One of the most famous examples is given by the weight 12 modular discriminant function

\[
\Delta(z) := q \prod_{n=0}^{\infty} (1 - q^n)^{24} = \sum_{k=0}^{\infty} \tau(k)q^k = \frac{(2\pi)^{12}}{1728} (E_4(z)^3 - E_6(z)^2)
\]

with the coefficients \( \tau(k) \) called the Ramanujan tau function. It was conjectured by Ramanujan and later proven that \( \tau \) is multiplicative, namely \( \tau(mn) = \tau(m) \tau(n) \) for \( \gcd(m, n) = 1 \), and for a prime \( p \), we have the Hasse bound \( |\tau(p)| \leq 2p^{11/2} \). Additionally, the \( p \)th power coefficients satisfy the three term recurrence relation,

\[
\tau(p) \tau(p^n) = \tau(p^{n+1}) + p^{11} \tau(p^{n-1}).
\]

The first property and the \( p \)-power recurrence relation follow from the theory of Hecke operators, while the second property is more subtle and involves relating \( \tau(p) \) to the trace of an associated Galois representation as shown by Deligne when he established a proof of one of the famous Weil conjectures in [7]. In fact, Deligne applied this process of associating the Fourier coefficients of modular forms to traces of Galois representations to a much broader class of modular forms than those on \( \text{SL}_2(\mathbb{Z}) \). By relaxing (2.1) to only hold for a finite-index subgroup \( \Gamma \leq \text{SL}_2(\mathbb{Z}) \), we can greatly increase our library of modular forms.

The most well-known of these being the congruence subgroups.

For each positive integer \( N \), we can define the congruence subgroups

\[
\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},
\]
\[
\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & \ast \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},
\]

\[
\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} \ast & \ast \\ 0 & \ast \end{pmatrix} \pmod{N} \right\},
\]

with \(\ast\) denoting the absence of any congruence condition. These form a chain of subgroups \(\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq \text{SL}_2(\mathbb{Z})\), with \(\Gamma(N)\) normal in each one. We say that a finite index subgroup \(\Gamma \leq \text{SL}_2(\mathbb{Z})\) has level \(N\) if \(\Gamma(N) \subset \Gamma\).

As seen in most introductory texts, like [6], the set of modular forms of weight \(k\) for \(\Gamma \leq \text{SL}_2(\mathbb{Z})\), denoted by \(M_k(\Gamma)\), forms a finite-dimensional \(\mathbb{C}\) vector space. For example, the spaces \(M_4(\text{SL}_2(\mathbb{Z}))\) and \(M_6(\text{SL}_2(\mathbb{Z}))\) are both one-dimensional spaces, spanned by their respective Eisenstein series. The spaces \(M_k(\Gamma)\) consist of subspaces \(S_k(\Gamma)\), of cusp forms which vanish at the cusps \(\mathbb{P}^1(\mathbb{Q})\) (as a consequence these always have a constant coefficient of 0), and the Eisenstein subspace \(E_k(\Gamma)\). These spaces are orthogonal with respect to the Petersson inner product and come equipped with an action by the Hecke operators \(T_n\). The Hecke operators can be defined as a sort of average over the orbits of \(\Gamma\) acting on the matrices of determinant \(n\), denoted \(M_n\)

\[T_n f(z) = n^{k-1} \sum_{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \backslash M_n} (cz + d)^{-k} f \left( \frac{az + b}{cz + d} \right).\]

The Hecke operators commute with one another and when \(\gcd(n,m) = 1\), we have that \(T_n T_m = T_{nm}\). Furthermore, the Hecke operators satisfy the \(p\)-power recursion

\[T_p T_{p^{\nu}} = T_{p^{\nu+1}} + p^{k-1} T_{p^{\nu-1}}. \quad (2.3)\]

From this and properties of the Petersson inner product, we get two important facts.
Spectral theory guarantees that there exists an orthonormal basis of simultaneous eigenforms for $M_k(\Gamma)$ and $S_k(\Gamma)$; and any normalized eigenform has Fourier coefficients which are multiplicative and satisfy the aforementioned $p$-power recursion. The proof that the Ramanujan tau function is multiplicative and satisfies the Hecke recursion follows from a simple computation that $S_{12}(\text{SL}_2(\mathbb{Z}))$ is one dimensional, making $\Delta(z)$ a Hecke eigenform.

For the Eisenstein series, it is clear that the Fourier coefficients $\sigma_k(n)$ are multiplicative, and we can further show $\sigma_k(p)\sigma_k(p^n) = \sigma_k(p^{n+1}) + p^k\sigma_k(p^{n-1})$ which implies these forms are Hecke eigenforms, but their associated Galois representations are reducible as opposed to the cuspidal case.

Beyond introducing congruence subgroups, it is also important to mention that for a group homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ we can augment our condition 2.1 to instead require

$$
\begin{pmatrix}
    a & b \\
    c & d 
\end{pmatrix} \in \Gamma, \quad f \begin{pmatrix}
    az + b \\
    cz + d 
\end{pmatrix} = \chi(d)(cz + d)^kf(z).
\quad (2.4)
$$

and we obtain the space $M_k(\Gamma, \chi)$ (or $S_k(\Gamma, \chi)$) of weight $k$ forms with nebypytupus $\chi$.

Following the work of Eichler and Shimura, Deligne was able to construct a family of two dimensional Galois representation for the absolute Galois group $G_\mathbb{Q} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, namely,

**Theorem 2** (Deligne). Let $f \in M_k(\Gamma, \chi)$ be a normalized weight $k$ Hecke eigenform of level $N$ with eigenvalues $a_n(f)$ and $k \geq 2$. Additionally, suppose $\chi(-1) = -1$. Then for each prime $\ell$, there exists

$$
\rho_{f,\ell} : G_\mathbb{Q} \to \text{GL}_2(\mathbb{Q}_\ell)
$$
such that for any prime $p \neq \ell$ not dividing $N$, we have the characteristic polynomial

$$\det(\rho_{f,\ell}(\text{Frob}_p) - x I_2) = x^2 - a_p(f)x + \chi(p)p^{k-1}.$$ 

The proof of this for $k = 1$ proved much trickier as weight 1 forms typically do not possess a nice geometric analog that exists in higher weights, but with the help of Serre, they proved

**Theorem 3** (Serre, Deligne [8]). Let $N$ be an integer $\geq 1$, $\chi(\cdot)$ a Dirichlet character (mod $N$) such that $\chi(-1) = -1$, and $f$ a modular form of type $(1, \chi)$ for $\Gamma_0(N)$, not identically zero. Suppose that $f$ is a normalized eigenform by which we mean its coefficient of $q$ being 1 with respect to the Hecke operators $T_p$, $p \nmid N$, with eigenvalues $a_p$. Then there exists a continuous linear representation

$$\rho_f : G_\mathbb{Q} \to \text{GL}_2(\mathbb{C}), \quad \text{where } G_\mathbb{Q} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}),$$

which is unramified outside $N$ and

$$\text{Tr}(\rho_f(\text{Frob}_p)) = a_p \quad \text{and} \quad \det(\rho_f(\text{Frob}_p)) = \chi(p) \quad \text{for } p \nmid N.$$

This representation is irreducible if and only if $f$ is a cusp form.

The weight 1 case is the first main topic of this dissertation and the structural properties of the associated Galois representation are related to the $L$-functions of Artin representations. In this case, the image of the representation is finite. As we shall see later in §3.3.2 when $a_n(f) \in \mathbb{Z}$, the image is either isomorphic to a Dihedral group when $\rho$ is irreducible or a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ when $\rho$ is reducible.
2.2. Class Field Theory

We will give a brief review of class field theory, but for a more thorough treatment and proofs of these results, see [5] or [21]. Let $f(x)$ be a monic polynomial with integer coefficients, and $K/Q$ its splitting field with ring of integers $O_K$ and Galois group $\text{Gal}(K/Q)$. For a prime $p$ and a prime ideal $\mathfrak{P}$ lying over $p\mathbb{Z}$, the Galois group acts transitively on the prime ideals $\mathfrak{P} \subset pO_K$ we can define the decomposition group $D_\mathfrak{P} := \{\sigma \in \text{Gal}(K/Q) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$. For different $\mathfrak{P}$ lying over the same $p\mathbb{Z}$, the corresponding decomposition groups are conjugate to one another, so they are always the same if $\text{Gal}(K/Q)$ is abelian, in which case we denote it $D_p$. We also have a homomorphism $D_\mathfrak{P} \to \text{Gal}(O_K/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})$ which is surjective, and it is injective whenever $p$ is unramified in $K$. We also know that $\text{Gal}((O_K/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z}))$ is cyclic and generated by the Frobenius automorphism, $\sigma_p(\alpha) = \alpha^p$. If $\text{Gal}(K/Q)$ is abelian and $p$ is unramified in $K$, we have a unique element $\text{Frob}_p \in D_p$ which satisfies $\text{Frob}_p(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$ for all $\mathfrak{P}$ lying over $p\mathbb{Z}$.

We can then describe the condition “$f(x)$ splits into linear factors modulo $p$” using $\text{Frob}_p$. In fact, if $\text{Frob}_p$ is the identity, this implies that $O_K/\mathfrak{P} \cong \mathbb{Z}/p\mathbb{Z}$, but since $K$ is the splitting field of $f$, we must have that $f(x)$ splits in $O_K/\mathfrak{P}$ and consequently $\mathbb{Z}/p\mathbb{Z}$. Conversely, if $\text{Frob}_p$ is not the identity, then this implies that the decomposition group must be nontrivial and $O_K/\mathfrak{P}$ must be a nontrivial extension of $\mathbb{Z}/p\mathbb{Z}$, which implies $f$ cannot split modulo $p$.

When $K/Q$ is an abelian extension, the Kronecker-Weber theorem states that $K$ must be contained in some cyclotomic extension $\mathbb{Q}(\zeta_n)$ for some $n$. We can then treat the
Frobenius as a map

\[ \text{Frob} : (\mathbb{Z}/n\mathbb{Z})^\times \to \text{Gal}(K/\mathbb{Q}), \]

with \( \text{Frob}_a := \text{Frob}_p \) for \( p \) a prime with \( a \equiv p \pmod{n} \). Then, for a 1-dimensional representation

\[ \rho : \text{Gal}(K/\mathbb{Q}) \to \mathbb{C}^* \]

we can identify the composition \( \rho \circ \text{Frob} \) with a Dirichlet character. Since \( \text{Gal}(K/\mathbb{Q}) \) is abelian, its representations are all direct sums of its 1-dimensional representations. Thus, we can describe the splitting behavior of \( f(x) \) entirely with Dirichlet characters!

For example, let \( f(x) = x^3 + x^2 - 2x - 1 \). We can show that its splitting field is \( K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \) and thus, contained in \( \mathbb{Q}(\zeta_7) \). We can then identify \( K \) with any cubic Dirichlet character with modulus 7. Regardless of the choice, we can conclude that \( f(x) \) splits modulo \( p \) for \( p \neq 7 \), if and only if \( p \equiv \pm1 \pmod{7} \).

This identification of 1-dimensional representations with Dirichlet characters can further be generalized to classify abelian extensions of an arbitrary number field \( F \). The role of \( (\mathbb{Z}/n\mathbb{Z})^\times \) is then played by the ray class group \( \mathcal{R}_{F,m}^+ := \mathcal{I}_F(\mathfrak{m})/\mathcal{P}_{F,m}^+ \), where \( \mathfrak{m} \) is a nonzero ideal of \( \mathcal{O}_F \), \( \mathcal{I}_F(\mathfrak{m}) \) is the group of fractional ideals coprime to \( \mathfrak{m} \), and \( \mathcal{P}_{F,m}^+ \) is the subgroup of principal fractional ideals generated by a totally positive\(^1 \) element \( \alpha \) which is \( 1 \pmod{\mathfrak{m}} \). The role of Dirichlet characters will then be replaced by Hecke characters

\[ \chi_{F,m} : \mathcal{R}_{F,m}^+ \to \mathbb{C}^* \]

(sometimes referred to as Grössencharacters). We then have the following theorem of Artin as stated in [5].

\(^1\)Positive under every real embedding of \( F \), but this condition can be ignored when \( F \) is an imaginary quadratic extension.
Theorem 4 (Artin Reciprocity). Let $K/F$ be a finite abelian extension of number fields, with $m$ an ideal of $\mathcal{O}_F$ divisible by all ramifying primes. Then the Artin map $\phi$ sending an ideal to its corresponding Frobenius element satisfies:

1. $\phi : \mathcal{I}_F(m) \to \text{Gal}(K/F)$ is surjective,

2. the ideal $m$ can be chosen so $\mathcal{P}_{F,m}^+ \subset \ker(\phi)$ giving a surjection

$$\tilde{\phi} : \mathcal{I}_F(m)/\mathcal{P}_{F,m}^+ \to \text{Gal}(K/F),$$

3. and $\ker(\tilde{\phi}) = \mathcal{N}_{K/F}(m)$, the subgroup of fractional ideals coprime to $m$ which are the norm of an ideal in $\mathcal{O}_K$.

We can then obtain the following correspondence between abelian extensions of $F$ and ray class groups:

Theorem 5. Let $K/F$ be a finite abelian extension, then there exists a maximal choice of ideal $f \subset \mathcal{O}_F$, called the conductor, and a group $\mathcal{H}$ with $\mathcal{P}_{F,f}^+ \leq \mathcal{H} \leq \mathcal{I}_F(f)$ such that

$$\tilde{\phi} : \mathcal{R}_{F,f}^+/\mathcal{H} \to \text{Gal}(K/F)$$

is an isomorphism, so $\text{Frob}_\mathfrak{p}$ is the identity if and only if $\mathfrak{p} \in \mathcal{H}$. Similarly, for every $f \subset \mathcal{O}_F$ and $\mathcal{H}$ with $\mathcal{P}_{F,f}^+ \leq \mathcal{H} \leq \mathcal{I}_F(f)$, there exists a unique finite abelian extension $K/F$ where the above map is again an isomorphism.

In modern literature, one would typically consider the set of all places of $F$ and use the adelic formulation where $\mathcal{R}_{F,m}^+$ is replaced with the idèle class group, allowing one to work with infinite abelian extensions, but as this chapter deals only with finite extensions, we’ll continue using the more classical language for simplicity.

For nonabelian extensions, such as $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ which is the splitting field of $x^3 - 2$, and others we will consider in this chapter, we can no longer describe its splitting behavior with only Dirichlet (or Hecke) characters, since we have an irreducible two-dimensional
representation
\[ \rho : \text{Gal}(Q(\sqrt[3]{2}, \zeta_3)/Q) \hookrightarrow \text{GL}_2(\mathbb{C}). \]

However, we can observe in this case, that the representation of the quotient
\[ \text{Gal}(Q(\sqrt[3]{2}, \zeta_3)/Q(\zeta_3)) \]
splits into a direct sum of two 1-dimensional representations. We can leverage this information by looking at these representations as Hecke characters for \( Q(\zeta_3) \) and piecing them together using a CM modular form to obtain information about the overall extension.

In order to see this connection between modular forms and Galois representations, we will need to move our discussion into the world of L-functions. L-functions are analogous to the Riemann zeta function \( \zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \). They include a broad class of functions including Dirichlet L-functions, \( L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} \) for \( \chi \) a Dirichlet character. As with the Riemann zeta function, \( L(\chi, s) \) has an analytic continuation to the whole plane except when \( \chi \) is trivial, then it is equal to the Riemann zeta function and has a simple pole at \( s = 1 \). Additionally, \( L(\chi, s) \) has an Euler product, like \( \zeta(s) \), so for \( \Re(s) > 1 \)
\[ L(\chi, s) = \prod_{p \text{ prime}} (1 - p^{-s} \chi(p))^{-1} \tag{2.5} \]
with the term \( 1/(1 - \chi(p)p^{-s}) \) being known as an Euler \( p \)-factor. For our purposes now in particular, given an \( n \)-dimensional complex Galois representation
\[ \rho : \text{Gal}(L/K) \to \text{GL}_n(\mathbb{C}) \]
we define the Artin L-function
\[ L(\rho, s) = \prod_{\substack{p \in \mathcal{O}_K \text{ unramified} \atop p \text{ prime}}} \det(I_n - N(p)^{-s} \rho(Frob_p))^{-1}. \]
Note that each term in the product is the reciprocal of the characteristic polynomial of \( \rho(\text{Frob}_p) \) evaluated at \( N(p)^{-s} \). In the case of \( n = 1 \) and the extension \( \mathbb{Q}(\zeta_m)/\mathbb{Q} \), this product expansion is identical to (2.5). This is well-defined even when \( \text{Frob}_p \) is defined up to a conjugacy class as similar matrices have equal characteristic polynomials.

When \( \rho \) is a 1-dimensional representation, we can use Artin Reciprocity to associate \( \rho \) with a Hecke character, \( \chi_{F,m} \). Using these characters, Hecke constructed a generalization of Dirichlet L-functions, Hecke L-functions

\[
L(\chi_K, m, s) = \sum_{I \in \mathcal{O}_K / (I, m) = 1} \chi_K(I) N(I)^{-s},
\]

so that \( L(\rho, s) = L(\chi_K, m, s) \). He showed that each of these L-functions satisfies a functional equation, which gives an analytic continuation to the whole plane. Thus, from class field theory, the associated Artin L-functions \( L(\rho, s) \) do as well! Whether Artin L-functions have an analytic continuation in general is known as the Artin conjecture.

2.3. Multiplicative Characters of Finite Fields

We will now turn our attention to character theory and give a brief summary of the results we will need from it. For a more thorough treatment, see [13] or [24].

Let \( q = p^f \) be a prime power. The finite field \( \mathbb{F}_q \) with \( q \) elements, is a degree \( f \) Galois extension of the finite field \( \mathbb{F}_p \) with \( p \) elements. We have the following trace map

\[
\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p, \quad \text{Tr}(\alpha) := \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{f-1}}
\]

which is a group homomorphism between their respective additive groups. The multiplicative group of the finite field of order \( q \), denoted \( \mathbb{F}_q^\times \), has the structure of a cyclic group of
order $q - 1$. This group is isomorphic to its character group

$$\hat{\mathbb{F}_q^\times} := \{\text{group homomorphisms } \chi : \mathbb{F}_q^\times \to \mathbb{C}^\times\}.$$ 

For a character $\chi \in \hat{\mathbb{F}_q^\times}$, its inverse is given by $\chi^{-1}(s) := \overline{\chi(s)}$ coinciding with the standard complex conjugation. One such character is the order two Legendre character $\left(\frac{\cdot}{p}\right)$ for $p$ an odd prime, as discussed in §2.2, and the trivial character $\varepsilon(s) := 1$ when $s \neq 0$.

Due to the isomorphism between $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and $(\mathbb{Z}/m\mathbb{Z})^\times$ we can often think of these characters as 1-dimensional Galois representations and treat our finite fields as residue fields coming from some larger extension. Denote $\eta_N$ for a fixed choice of a mod $q$ character with exact order $N$ and for $d|N$, take $\eta_d = \eta_N^{N/d}$ which amounts to a fixed choice of a prime ideal $p$ over $p\mathbb{Z}[\zeta_N]$. For $c/N \in \mathbb{Q}$ take $\iota_p(c/N) = \eta_N^c$. We will occasionally conflate $\eta_N$ with the $N$th power residue symbol as both take value 1 when evaluated on $N$th powers. The characters of $\mathbb{F}_p$ can be extended to Dirichlet characters using the natural projection from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ and the convention that $\chi(0) = 0$ for all characters (including the trivial character).

For a character $\chi \in \hat{\mathbb{F}_q^\times}$, we define the standard Gauss Sum

$$g_c(\chi) := \sum_{s \in \mathbb{F}_q} \chi(s) \zeta_p^{c \text{Tr}(s)}$$

for $c \in \mathbb{F}_p^\times$. The various Gauss sums are related by the relation

$$g_c(\chi) = \chi^{-1}(c)g_1(\chi),$$

and so we define

$$g(\chi) := g_1(\chi).$$
The main tools to manipulate the character sums are the Reflection (or Norm) principle and the Hasse-Davenport relation (sometimes called the multiplication formula) which are analogous to the reflection and multiplication formulas for the Gamma function in §2.4. Additionally, we adopt the following notation for the indicator function

\[
\delta(t) := \begin{cases} 
1, & \text{if } t = 0, \\
0, & \text{otherwise},
\end{cases}
\quad \delta(\chi) := \begin{cases} 
1, & \text{if } \chi = \varepsilon, \\
0, & \text{otherwise}.
\end{cases}
\]

**Theorem 6** (Reflection). For \( \chi \in \mathbb{F}_q^\times \) we have

\[
g(\chi)g(\overline{\chi}) = \chi(-1)q - (q - 1)\delta(\chi)
\]

\[
\frac{1}{g(\chi)g(\overline{\chi})} = \frac{\chi(-1)}{q} + \frac{q - 1}{q}\delta(\chi).
\]

We can use this to deduce that \( |g(\chi)| = \sqrt{q} \) for \( \chi \neq \varepsilon \).

**Theorem 7** (Hasse-Davenport). For \( q \) a prime power and \( n \) a positive integer with \( q \equiv 1 \pmod{n} \), we have that for every \( \psi \in \mathbb{F}_q^\times \),

\[
\prod_{\chi \in \mathbb{F}_q^\times, \chi^n = \varepsilon} g(\psi\chi) = -g(\psi^n)\psi(n^n) \prod_{\chi \in \mathbb{F}_q^\times, \chi^n = \varepsilon} g(\chi)
\]

Their importance is made clear with the following conjecture of Hasse, which was proven by Yamamoto in [29].

**Theorem 8** (Yamamoto). The only multiplicative relationships between the ideals generated by Gauss sums of \( n \)th power residue symbols are the reflection principle and Hasse-Davenport relation.

For characters \( A, B \in \mathbb{F}_q^\times \) we define the Jacobi sum

\[
J(A, B) := \sum_{\substack{a, b \in \mathbb{F}_q \\
a + b = 1}} A(a)B(b)
\]
and note the following relationship to Gauss sums, analogous to the relationship between
the Beta and Gamma functions,

\[ J(A, B) = \frac{g(A)g(B)}{g(AB)} + (q - 1)B(-1)\delta(AB). \tag{2.7} \]

and similarly to the Gauss sum, we have \(|J(A, B)| = \sqrt{q}\) for \(AB \neq \varepsilon\).

We also have the following orthogonality properties

\[ \sum_{\chi \in \overline{F}_q} \chi(a) = (q - 1)\delta(a - 1) \tag{2.8} \]

which is 0 when \(a \neq 1\) and

\[ \sum_{s \in \overline{F}_q} \chi(s) = (q - 1)\delta(\chi). \tag{2.9} \]

### 2.4. Hypergeometric Functions

#### 2.4.1. Classical Hypergeometric Functions

**Definition 1.** Let \(a, b, c \in \mathbb{Q}\) and \(z \in \mathbb{C}\). The classical hypergeometric function with data\n\[ HD = \{\alpha, \beta\} = \{\{a, b\}, \{1, c\}\} \]

is a special function which can be defined via the power series

\[ _2F_1(HD; z) := \sum_{k=0}^{\infty} \frac{(a)_k(b)_k}{(c)_k} \frac{z^k}{k!} \]

with \((x)_k = x(x + 1) \cdots (x + k - 1)\) denoting the Pochhammer symbol.

It is a direct generalization of the standard geometric series and in fact

\[ _2F_1(\{1, 1\} ; \{1, 1\} ; z) = \sum_{k=0}^{\infty} z^k. \]

It satisfies the 2nd order hypergeometric differential equation

\[ z(1 - z)y'' + [c - (a + b + 1)z]y' - aby = 0. \]
Equivalently, this equation has 3 regular singularities at 0, 1, and \( \infty \) with the singularity at 1 being a “pseudo-reflection”. It was originally studied by Euler, who had the idea that one could study solutions to differential equations by only looking at their behavior around the singularities. While solutions to differential equations are not solely determined by their behavior at singularities in general (a property now known as rigidity), Euler was lucky in that the hypergeometric equation is in fact rigid due to the special property of the singularity at 1. Their importance to number theory can be seen when we take our hypergeometric data to consist of rational numbers. One of the most well known examples occurs when taking \( HD = \{\{1/2,1/2\},\{1,1\}\} \). Then

**Theorem 9** (Koike).

\[
2F1(HD; \lambda) = \frac{1}{\pi} \int_0^1 \frac{dx}{y}
\]

where \( dx/y \) is the unique holomorphic differential on the Legendre elliptic curve

\[
E_\lambda : \quad y^2 = x(1-x)(1-\lambda x).
\]

For \( \lambda \neq 0, 1, \infty \), it is the double cover of the complex projective sphere parameterized by \( x \) which ramifies at 0, 1, 1/\( \lambda \) and \( \infty \) respectively. When \( \lambda \in \mathbb{Q} - \{0, 1\} \), \( E_\lambda \) is an elliptic curve defined over \( \mathbb{Q} \). Hence the modularity theorem says its L-function coincides with the L-function of a weight-2 cuspidal Hecke eigenform. For example when \( \lambda = -1 \), the elliptic admits CM and the corresponding modular form is \( f_{32.2.a.a} \), which also admits CM.
While typically transcendental functions, there are many examples of hypergeometric datum for which \( {}_2F_1(HD; \lambda) \) is an algebraic function, such as an example of \([26]\)

**Theorem 10.**

\[
{}_2F_1 \left( \begin{array}{cc} \frac{1}{3} & -\frac{1}{3} \\ \frac{1}{2} & \lambda \end{array} \right) = \frac{1}{2} \left( 1 - \frac{\lambda}{\lambda - 1} \right)^{\frac{1}{3}} \left( 1 + \sqrt[3]{\frac{\lambda}{\lambda - 1}} \right)^{-\frac{2}{3}} + \left( 1 - \sqrt[3]{\frac{\lambda}{\lambda - 1}} \right)^{-\frac{2}{3}}
\]

Hypergeometric functions have many relationships with the Gamma function

**Definition 2.** For \( \Re(z) > 0 \),

\[
\Gamma(z) := \int_0^\infty t^z e^{-t} dt
\]

which is a generalization of the factorial and one can show that it satisfies the functional equation

\[
\Gamma(z + 1) = z\Gamma(z),
\]

which also gives us the following relationship with the Pochhammer symbol

\[
(a)_n = \frac{\Gamma(a + n)}{\Gamma(n)}.
\]

As with the Gauss sum in §2.3 we have Euler’s Reflection Formula

**Theorem 11** (Theorem 1.2.1 in [1]).

\[
\Gamma(z)\Gamma(1 - z) = \frac{\pi}{\sin(\pi z)}, \quad (2.11)
\]

which is analogous the reflection principle 6 and Gauss’ multiplication formula
Theorem 12 (Theorem 1.5.2 in [1]). For $n \in \mathbb{Z}_{>0}$ and $z \in \mathbb{C}$

$$
\Gamma(nz)(2\pi)^{(n-1)/2} = n^{nz-1/2}\Gamma(z)\Gamma\left(z + \frac{1}{n}\right) \cdots \Gamma\left(z + \frac{n-1}{n}\right). \tag{2.12}
$$

We also have the Beta function

**Definition 3.** For $\Re(z_1) > 0$ and $\Re(z_2) > 0$

$$
B(z_1, z_2) = \int_0^1 t^{z_1-1}(1-t)^{z_2-1}dt
$$

It is important to note that we can drop the condition on the real part of $z_1$ and $z_2$ by taking a carefully chosen contour integral, and we have the following relationship between the Gamma and Beta functions

$$
B(z_1, z_2) = \frac{\Gamma(z_1)\Gamma(z_2)}{\Gamma(z_1 + z_2)}
$$

which is analogous to the relationship (2.7) between the Gauss and Jacobi sums.

From rigidity, we also get a wide breadth of identities for hypergeometric functions.

For example, we have one of Kummer’s 24 relations

**Theorem 13 (Kummer).**

$$
\begin{align*}
\binom{ab}{c} z = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)} \binom{a}{a+b+1-c} \binom{b}{1-z} \\
+ \frac{\Gamma(c)\Gamma(a+b-c)}{\Gamma(a)\Gamma(b)} \binom{c-a}{1+c-a-b} \binom{c-b}{1-z},
\end{align*}
$$

as well as the Pfaff transformation
Theorem 14 (Pfaff).

\[
2\, _2F_1\left(a \quad b \quad ; \quad z \quad \right) = (1 - z)^{-a} \, _2F_1\left(a \quad c - b \quad z \quad ; \quad \frac{z}{z - 1} \quad \right)
\]

\[
= (1 - z)^{-b} \, _2F_1\left(c - a \quad b \quad ; \quad z \quad ; \quad \frac{z}{z - 1} \quad \right)
\]

(2.14)

These functions can be generalized to allow for \( \alpha \) and \( \beta \) sets of larger length. If we take \( \alpha = \{a_1, \ldots, a_n\} \) and \( \beta = \{b_1, \ldots, b_n\} \), we can define the generalized hypergeometric function

\[
_nF_{n-1}\left(\begin{array}{c}
a_1 & \cdots & a_n \\
b_1 & \cdots & b_n
\end{array} ; z \right) = \sum_{k=0}^{\infty} \left( \prod_{i=1}^{n} \frac{a_i}{(b_i)_k} \right) z^k.
\]

Typically, we assume that \( b_1 = 1 \) and omit it from notation. Like in the \( _2F_1 \) case, the generalized \( _nF_{n-1} \) functions satisfy an \( n \)th order ordinary differential equation, so for

\[
\mathcal{L}_{\alpha,\beta; z} := \prod_{i=1}^{n} (\theta_z + b_i - 1) - z \prod_{i=1}^{n} (\theta_z + a_i)
\]

with \( \theta_z = z \frac{d}{dz} \), we have that

\[
\mathcal{L}_{\alpha,\beta; z}(nF_{n-1}(\alpha, \beta; z)) = 0.
\]

The generalized hypergeometric differential equation has the same properties as in the “length 2” case, with regular singularities at 0, 1, \( \infty \) and the singularity at 1 being a “pseudo-reflection”. As such, it is also rigid, producing a rich array of interesting identities. The \( _nF_{n-1} \) function lies in an \( n \)-dimensional locally defined solutions at \( z = 0 \) to this differential equation and the other solutions can be expressed in terms of other generalized hypergeometric functions possibly with logarithmic terms.
2.4.2. Hypergeometric Functions over Finite Fields

In the classical setting, the hypergeometric functions can be related to periods of algebraic varieties over \( \mathbb{Q} \), but these varieties also have reductions to finite fields with point counts being analogous to periods, so mathematicians sought to formulate a version of hypergeometric functions that included the finite field setting. Greene, in [11], was the first to give a definition of hypergeometric functions over finite fields as a way to give point counts of the reductions of varieties in the classical setting. Many others have given alternative definitions of hypergeometric character sums (such as in the papers of McCarthy [20], Katz [14]), and Beukers-Cohen-Mellit [3]). In this chapter, we will primarily use the definition given by McCarthy.

Let \( \alpha \) and \( \beta \) be multisets of rational functions as before and \( t \in \mathbb{Q} - \{0,1\} \). Let \( N \) be the least common multiple of the denominators (or \( \text{lcd} \) to abbreviate) of the \( a_i \) and \( b_i \).

Let \( q = p^f \) for \( p \) an odd prime such that \( \text{ord}_p(t) \geq 0 \), and \( q \equiv 1 \pmod{N} \). Denote \( \phi \) for the unique quadratic character modulo \( q \) and \( \varepsilon \) the trivial character as in §2.3. Denote \( \eta_N \) as defined in §2.3. We also have a map

Definition 4. We call the set \( \{\alpha, \beta, t\} \) the hypergeometric datum (dropping the parameter \( t \) when treated as arbitrary), and we define

\[
H_q(\alpha, \beta; t) := \frac{1}{1 - q} \sum_{\chi \in \hat{\mathbb{F}}_q^*} \left( \prod_{i=1}^{n} \frac{g(t_p(a_i)\chi)g(t_p(b_i)\overline{\chi})}{g(t_p(a_i))g(t_p(b_i))} \right) \chi((-1)^nt)
\]

where \( g \) denotes the Gauss sum.

Additionally, if for all \( i, j \), we have that \( a_i - b_j \not\in \mathbb{Z} \), we call the datum \( \{\alpha, \beta\} \) primitive.

In the classical setting, the previously mentioned point counts can be related to the
trace of certain Galois representation, so in the case of the Legendre elliptic curve $E_\lambda$ as (2.10) we have a representation for each prime $\ell$

$$\rho_{\lambda,\ell} : G_\mathbb{Q} \rightarrow \text{GL}_2(\mathbb{Q}_\ell),$$

with the point counts being related by

$$\#E_\lambda(\mathbb{F}_p) = p + 1 - \text{Tr}(\rho_{\lambda,\ell}(\text{Frob}_p)),$$

moreover

$$\text{Tr}(\rho_{\lambda,\ell}(\text{Frob}_p)) = H_p \left( \left\{ \frac{1}{2}, \frac{1}{2} \right\}, \{1, 1\}; \lambda \right)$$

for any prime $p \neq \ell$ and not dividing the conductor of $E_\lambda$. With this picture in mind, it was shown by Katz in [14] (see Theorem 1 in [16]), that these character sums do in fact correspond to traces of Galois representations for $G_{\mathbb{Q}(\zeta_N)}$ and it is natural to ask when this representation can be extended to $G_{\mathbb{Q}}$, motivating our next definition

**Definition 5.** We say that the datum $HD = \{\{a_1, \ldots, a_n\}, \{b_1, \ldots, b_n\}\}$ is defined over $\mathbb{Q}$, if the polynomials

$$\prod_{k=1}^n (x - e^{2\pi ia_k}) \text{ and } \prod_{k=1}^n (x - e^{2\pi ib_k})$$

have integer coefficients.

McCarthy gave one possible extension using the Reflection principle and Hasse-Davenport relation to define the character sums for $q \not\equiv 0 \pmod{N}$ and it was shown by Beukers-Cohen-Mellit in [3] that for datum defined over $\mathbb{Q}$, there exists an algebraic variety $V/\mathbb{Q}$ and the point counts for these varieties over finite fields can be given by McCarthy’s $H_q$ function.
We will stick to the definition for \( q \equiv 1 \pmod{N} \) but know that we can relate these to other \( q \) in the same way as McCarthy as long as we are careful when handling certain normalization factors when applying the Hasse-Davenport relation.

We can also obtain finite field analogues of many identities in the classical setting such as the Kummer relation

**Theorem 15** ([11]). For \( a, b, c \in \mathbb{Q} \), denote \( A := \iota_p(a), B := \iota_p(b), \) and \( C := \iota_p(c) \)

\[
H_q \begin{pmatrix} A & B \\ C \end{pmatrix} ; \lambda = B(-1)H_q \begin{pmatrix} A & B \\ C & ABC \end{pmatrix} ; 1 - \lambda .
\] (2.15)
Chapter 3. Weight 1 Eta-Quotients

Among the many modular forms we can now properly discuss, we will begin with
the weight 1/2 Dedekind eta function

\[ \eta(z) = q^{1/24} \prod_{n=0}^{\infty} (1 - q^n) \]

which is a 24th root of the modular discriminant \( \Delta(z) \) from §2.1. The existence of a product expansion for \( \eta(z) \) is exceptional and greatly simplifies computations. For this reason, taking products and quotients of the Dedekind eta-function in various levels allows us to produce explicitly computable examples of modular forms and provides a nice testing ground for conjectures involving them.

3.1. Eta-Quotients

Let \( N \) be a positive integer and for each divisor \( d \mid N \) we associate an integer \( r_d \), which is not necessarily positive. We then can take an eta-quotient as being a function of the form

\[ \prod_{d \mid N} \eta(dz)^{r_d}. \]

We then have the following result

**Theorem 16.** Let \( N \) be a positive integer and \( f(z) = \prod_{d \mid N} \eta^{r_d}(dz) \) be an eta-quotient with \( k = \frac{1}{2} \sum_{d \mid N} r_d \in \mathbb{Z} \). Then \( f \) is weakly modular of weight \( k \) for some \( \Gamma_0(M, \chi) \) if and only if \( \sum_{d \mid N} d r_d \equiv 0 \pmod{24} \) and \( \sum_{d \mid N} (N/d) r_d \equiv 0 \pmod{24} \). Explicitly, we can take \( M \) to be the least common multiple of the \( d \) with \( r_d \) nonzero and the denominator of \( \sum_{d \mid N} r_d/(24d) \), and

\[ \chi(d) = \left( \frac{-1)^k P}{d} \right), \text{ where } P = \prod_{d \mid N} d^{r_d}. \]

Checking holomorphicity can then be done with the following result
Theorem 17. Let $a/c \in \mathbb{P}^1(\mathbb{Q})$ be a cusp with $\gcd(a,c) = 1$ and $c > 0$. If $f(z) = \prod_{d|N} \eta^{r_d}(d\tau)$ is an eta-quotient, then the order of $f$ at the cusp $a/c$ is given by

$$v_{a/c}(f) = \frac{1}{24} \sum_{d|N} \frac{\gcd(d,c)^2 r_d}{d}.$$ 

In particular, $f$ is holomorphic at $a/c$ if and only if $v_{a/c}(f) \geq 0$ and vanishes if $v_{a/c}(f) > 0$.

Example 1. Take $f(z) = \eta(4z)\eta(20z)$, we have that $lcm(4, 20) = 20$ and $1/(24 \cdot 4) + 1/(24 \cdot 20) = 1/80$ so we can take the level to be 80. Since $P = 80$, we have that $\chi = \left(\frac{-80}{.}\right)$.

The product expansion for eta-quotients is very useful for studying the analytic properties of an eta-quotient, but to obtain direct information about the Fourier coefficients, we will use the following classical result of Euler,

Theorem 18 (Euler’s Pentagonal Number Theorem).

$$\prod_{k=1}^{\infty} (1 - q^k) = \sum_{l \in \mathbb{Z}} (-1)^l q^{(3l+1)/2}, |q| < 1.$$ 

3.2. Reciprocity laws for weight 1 eta-quotients and the first main result

In [12], Hiramatsu gives conditions for which the eta-product $\eta(n\tau)\eta(m\tau)$, where $m, n$ are positive integers, (which can be identified with a theta series gives a weight 1 modular form, and proves the following

Theorem 19 (Hiramatsu). The polynomial $x^3 - x^2 - x - 1$ splits modulo a prime $p$ if and only if $c(p) = 2$, where $c(n)$ is defined so

$$\eta(2\tau)\eta(22\tau) = \sum_{u,v \in \mathbb{Z}} (-1)^{u+v} q^{((6u+1)^2 + 11(6v+1)^2)/12} = \sum_{n=0}^{\infty} c(n) q^n.$$

He goes on to give similar reciprocity laws using the Fourier coefficients of $\eta(\tau)\eta(23\tau)$, $\eta(8\tau)\eta(16\tau)$, and $\eta(12\tau)^2$. 

26
Eta-quotients have the added benefit of being able to express them as theta series, which allows us to easily describe their Fourier coefficients at any prime and to give reciprocity laws for higher degree polynomials. Not all weight 1 eta-quotients can be used to give reciprocity laws, as we specifically need a Hecke eigenform. It was shown in [18], by Martin, that there are only finitely many eta-quotients which are Hecke eigenforms and he gave a complete list. As such, the first main topic in this dissertation was to determine reciprocity laws for all the weight 1 eta-quotients where applicable. While most (if not all) of these results are known\(^1\), the goal was a concrete methodology for proving results like this. Thus, we prove the following:

**Theorem 20.** The following tables gives all multiplicative weight one eta-quotients \( g = \prod_i r_i^{t_i} := \prod_i \eta(r_i \tau)^{t_i} \), with the following data:

- \( N \): the level of the eta-quotient
- \( \chi(\cdot) = (\frac{-N}{\cdot}) \)
- \( F = \mathbb{Q}(\sqrt{-N}) \): the fixed field of the kernel of \( \chi \) as a character of \( G_{\mathbb{Q}} \)
- \( h_N \): the class number of \( F \)
- \( f \): a non-unique polynomial with the property that \( f \) splits modulo a prime \( p \) if and only if the \( p \)th Fourier coefficient of \( g \) is 2
- \( G := \text{Gal}(K/\mathbb{Q}) \), the Galois group of the splitting field \( K \) of \( f \) up to isomorphism
- \( \mathcal{f} \): the conductor for the ray class character \( \mathcal{R}_{F,f} \rightarrow \mathbb{C}^\times \) (defined in §2.2) of \( K/F \) which gives a congruence condition over \( F \) as described above

Table 1 gives the reciprocity laws for eta-quotients which give Eisenstein series, with \( V := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). Table 2 gives the reciprocity laws for eta-quotients which give

---

\(^1\)All cusp form examples can be found on the LMFDB.
cusp forms, with $D_n$ the dihedral group of order $n$,

$$\eta(\tau) = q^{1/24} \sum_{n \in \mathbb{Z}} (-1)^n q^{3n^2 + n} = \frac{1}{2} \sum_{n \in \mathbb{Z}} \left( \frac{12}{n} \right) q^{n^2/24},$$

(3.1)

$$\mu(\tau) = \frac{\eta^3(2\tau)}{\eta(\tau)\eta(4\tau)} = \frac{1}{2} \sum_{n \in \mathbb{Z}} \left( \frac{24}{n} \right) q^{n^2/24},$$

(3.2)

$$\theta_2(\tau) = 2 \frac{\eta^2(2\tau)}{\eta(\tau)} = \sum_{n \in \mathbb{Z}} \left( \frac{4}{n} \right) q^{n^2/8} = \sum_{n \in \mathbb{Z}} q^{(n+1/2)^2},$$

(3.3)

and

$$\theta_4(\tau) = \frac{\eta^2(\tau)}{\eta(2\tau)} = \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2}.$$
Table 3.1. Reciprocity laws for non-cusp eta-quotients

<table>
<thead>
<tr>
<th>$g$</th>
<th>$N$</th>
<th>$h_N$</th>
<th>$f$</th>
<th>$G$</th>
<th>$\ell$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{10}{1^4}$</td>
<td>4</td>
<td>1</td>
<td>$x^2 + 4$</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>4</td>
</tr>
<tr>
<td>$\frac{1^2}{1^8}$</td>
<td>8</td>
<td>1</td>
<td>$x^2 + 8$</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>8</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>15</td>
<td>2</td>
<td>$x^2 + 15$</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>15</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>15</td>
<td>2</td>
<td>$x^4 - 4x^2 + 64$</td>
<td>$V$</td>
<td>15</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>20</td>
<td>2</td>
<td>$x^2 + 20$</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>20</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>20</td>
<td>2</td>
<td>$x^4 - 8x^2 + 36$</td>
<td>$V$</td>
<td>20</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>24</td>
<td>2</td>
<td>$x^2 + 24$</td>
<td>$\mathbb{Z}/2\mathbb{Z}$</td>
<td>24</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>24</td>
<td>2</td>
<td>$x^4 - 8x^2 + 36$</td>
<td>$V$</td>
<td>24</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>32</td>
<td>1</td>
<td>$x^4 - 8x^2 + 144$</td>
<td>$V$</td>
<td>8</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>36</td>
<td>1</td>
<td>$x^4 - 18x^2 + 225$</td>
<td>$V$</td>
<td>4</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>48</td>
<td>1</td>
<td>$x^4 - 16x^2 + 256$</td>
<td>$V$</td>
<td>3</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>64</td>
<td>1</td>
<td>$x^4 + 256$</td>
<td>$V$</td>
<td>4</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>96</td>
<td>2</td>
<td>$x^4 - 40x^2 + 784$</td>
<td>$V$</td>
<td>24</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>96</td>
<td>2</td>
<td>$x^4 - 8x^2 + 400$</td>
<td>$V$</td>
<td>24</td>
</tr>
<tr>
<td>$\frac{1^2}{1^2}$</td>
<td>576</td>
<td>1</td>
<td>$x^4 + 2304$</td>
<td>$V$</td>
<td>4</td>
</tr>
</tbody>
</table>
Table 3.2. Reciprocity laws for cusp form eta-quotients

<table>
<thead>
<tr>
<th>g</th>
<th>N</th>
<th>h_N</th>
<th>f</th>
<th>G</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>\eta(\tau)\eta(23\tau)</td>
<td>23</td>
<td>3</td>
<td>x^3 - x - 1</td>
<td>D_6</td>
<td>1</td>
</tr>
<tr>
<td>\eta(2\tau)\eta(22\tau)</td>
<td>44</td>
<td>1</td>
<td>x^3 - x^2 - x - 1</td>
<td>D_6</td>
<td>2</td>
</tr>
<tr>
<td>\eta(3\tau)\eta(21\tau)</td>
<td>63</td>
<td>1</td>
<td>x^4 - x^3 + 2x + 1</td>
<td>D_8</td>
<td>3</td>
</tr>
<tr>
<td>\eta(4\tau)\eta(20\tau)</td>
<td>80</td>
<td>2</td>
<td>x^4 + x^2 - 1</td>
<td>D_8</td>
<td>2</td>
</tr>
<tr>
<td>\eta(6\tau)\eta(18\tau)</td>
<td>108</td>
<td>1</td>
<td>x^3 - 2</td>
<td>D_6</td>
<td>6</td>
</tr>
<tr>
<td>\eta(8\tau)\eta(16\tau)</td>
<td>128</td>
<td>1</td>
<td>x^4 - 2x^2 + 2</td>
<td>D_8</td>
<td>4</td>
</tr>
<tr>
<td>\eta^2(12\tau)</td>
<td>144</td>
<td>1</td>
<td>x^4 - 12</td>
<td>D_8</td>
<td>6</td>
</tr>
<tr>
<td>\mu(2\tau)\mu(22\tau)</td>
<td>176</td>
<td>1</td>
<td>x^6 - 2x^5 + 2x^4 - 2x^3 + 4x^2 - 4x + 2</td>
<td>D_{12}</td>
<td>4</td>
</tr>
<tr>
<td>\frac{1}{2}\theta_2(8\tau)\theta_4(16\tau)</td>
<td>256</td>
<td>1</td>
<td>x^4 + 2</td>
<td>D_8</td>
<td>8</td>
</tr>
<tr>
<td>\mu(4\tau)\mu(20\tau)</td>
<td>320</td>
<td>2</td>
<td>x^4 - 4x^2 + 5</td>
<td>D_8</td>
<td>4</td>
</tr>
<tr>
<td>\mu(6\tau)\mu(18\tau)</td>
<td>432</td>
<td>1</td>
<td>x^6 - 2x^3 + 2</td>
<td>D_{12}</td>
<td>12</td>
</tr>
<tr>
<td>\mu^2(12\tau)</td>
<td>576</td>
<td>1</td>
<td>x^4 - 6x^2 + 12</td>
<td>D_8</td>
<td>12</td>
</tr>
</tbody>
</table>

It is important to point out the difference between how the Eisenstein series eta-quotients and cusp form eta-quotients are named. For the cusp forms, they can all be expressed as the product of two multiplicative weight 1/2 eta-quotients which provides us with an auxiliary quadratic form which gives us a fairly straightforward analysis of the Fourier coefficients and we can use this with the level and character to narrow down the possible number fields associated to it. For the Eisenstein series, it does not appear that every form can be expressed as a product of this form. While some of them can be ex-
pressed in this way, such as

$$\frac{\eta^{10}(2\tau)}{\eta^{4}(\tau)\eta^{4}(4\tau)} = \theta_{3}^{2}(\tau)$$

or

$$\frac{\eta^{2}(4\tau)\eta^{2}(16\tau)}{\eta^{2}(8\tau)} = \frac{1}{2} \theta_{1}(4\tau)\theta_{2}(8\tau),$$

this is not needed as the Fourier coefficients in these cases are determined up to a finite modulus dividing the level.

### 3.3. The Serre-Deligne Theorem

The main tool in obtaining a polynomial related to a modular form is the aforementioned theorem by Serre and Deligne, as stated as Theorem 3.

Since $G_{\mathbb{Q}}$ has the profinite topology, which is incompatible with the topology on $\text{GL}_{2}(\mathbb{C})$, $\rho$ necessarily has finite image. Thus, $\rho$ factors through a representation of the finite group $G := G_{\mathbb{Q}}/\ker(\rho)$. The group $G$ corresponds to a Galois group $\text{Gal}(K/\mathbb{Q})$ with $K$ a finite Galois extension. Then by the primitive element theorem, $K = \mathbb{Q}(\alpha)$ with $\alpha$ having a minimal polynomial $f(x) := \text{minpoly}_{\mathbb{Q}}(\alpha)$, and $K$ is the splitting field of $f(x)$. This polynomial is precisely what we are looking for!

All that is required, is for $f$ to be a Hecke eigenform. We can then assume without loss of generality that $f$ is normalized so the eigenvalue $a_{p}$ is just its $p$th Fourier coefficient. There is a concrete condition we can check using the Fourier coefficients of $f$. If $f(\tau) = \sum_{n=0}^{\infty} a_{n}q^{n}$ is the Fourier expansion of a weight $k$ modular form, then $f$ is a Hecke eigenform if and only if $a_{n}a_{m} = a_{nm}$ when $(n, m) = 1$ and $a_{p}a_{p^{\alpha}} = a_{p^{\alpha+1}} + \chi(p)p^{k-1}a_{p^{\alpha-1}}$ for all $p \nmid N$. We must first determine when this occurs. In particular, it has been shown in [25] by Serre that the only weight-one eta products which are Hecke eigenforms are the
ones given in Table 2.

However, it is not too difficult to show these forms are Hecke eigenforms and there is a useful connection between these forms and theta series twisted by Hecke characters that makes the proof much simpler. As we will discuss in the proof of the main result, we can deduce the class group from the coefficients by looking for congruences via the quadratic form obtained from writing these forms as theta series. From there, we can use a database to brute force the polynomial, use the structural information to explicitly construct it, or use the theory of CM elliptic curves to directly compute it. Another more mysterious method of finding these extensions is through “special values” of an $L$-function attached to the form, as done by Stark in [27], where he showed that $L'(\eta(\tau)\eta(23\tau), 0) = 3 \log(\epsilon)$, where $\epsilon$ is the unique real root of $x^3 - x - 1$.

The corresponding polynomials for $\eta(\tau)\eta(23\tau)$, $\eta(2\tau)\eta(22\tau)$, $\eta(8\tau)\eta(16\tau)$, and $\eta(12\tau)^2$ are given as examples in [12] so we will focus on the remaining 3 eta-products, $\eta(3\tau)\eta(21\tau)$, $\eta(4\tau)\eta(20\tau)$, and $\eta(6\tau)\eta(18\tau)$.

Rather than tediously work through each eta-quotient one by one, we elect to give a few representative examples to show how these reciprocity laws can be found using very concrete methods.

3.3.1. Coefficients of the modular forms

By examining the coefficients of the modular forms, we can find information on the associated polynomials. Many of the properties of the Fourier coefficients of modular forms in general have much simpler statements in the weight 1 case and even simpler for weight 1 eta-quotients. For eta-quotients at any prime $p$, we have that $a_p, \chi(p) \in \mathbb{Z}$.  

32
Since the representation, as in Theorem 3, has finite image in $\text{GL}_2(\mathbb{C})$, $a_p$ is the trace of a finite order matrix, so it can be expressed as the sum of two roots of unity. Thus, we have $|a_p| \leq 2$, which is a much simpler case of the Hasse bound, $|a_p| \leq 2p^{(k-1)/2}$, for weight $k$ modular forms in general. Since the representation is semisimple, as it complex with finite image, the order of any element can be completely determined by its trace. In particular, the only possibilities for integer coefficient forms are:

- If $a_p = -2$, this forces the characteristic polynomial to be $x^2 + 2x + 1$ so the element has order 2.

- If $a_p = -1$, this forces the characteristic polynomial to be $x^2 + x + 1$ so the element has order 3.

- If $a_p = 0$, this forces the characteristic polynomial to be $x^2 \pm 1$ so the element has order 2 or 4, depending on whether $\chi(p) = 1$ or $\chi(p) = -1$ respectively. One can circumvent looking at the determinant since the $p$-power recurrence gives us that $a_{p^2} = -\chi(p)$ in this case.

- If $a_p = 1$, this forces the characteristic polynomial to be $x^2 - x + 1$ so the element has order 6.

- If $a_p = 2$, this forces the characteristic polynomial to be $x^2 - 2x + 1$ so the element has order 1.

Observe that among the these cases, the only characteristic polynomial with constant term $\chi(p) = -1$ occurs only when $a_p = 0$. One can even determine some information on the intermediate extensions. For our case, the character $\chi(\cdot)$ of $f(\tau)$, is just the Jacobi symbol $(\frac{-N}{\cdot})$, where $N$ is the level of $f$. This gives us that for an unramified prime $p$, if $\chi(p) = 1$ (resp. $-1$), then the ideal $(p)$ splits (resp. remains inert) in the ring of integers of $\mathbb{Q}(\sqrt{-N})$.

Furthermore, for an unramified prime $p$, the trace $a_p$ then determines how the unknown polynomial factors modulo $p$. In particular, the target polynomial splits modulo $p$.
if and only if $a_p = 2$. So if we can determine all $p$ for which $a_p = 2$, this will uniquely characterize the desired number field. As we can write each eta-quotient as a theta series, this amounts to showing $a_p = 2$ if and only if a certain congruence condition holds for the $p$ that can be represented by the quadratic form associated to the theta series. After finding a potential candidate for the polynomial, we can use Theorem 5 from class field theory to show that the splitting field $K/F$ (which must be abelian) has a conductor that gives the same congruence condition for prime ideals of $F$ as the one obtained from the coefficients of the modular form and thus must be our desired number field.

3.3.2. Galois Representations

One particularly important fact about the Galois representations associated to these eta-products is the following

**Theorem 21.** If $f$ is a weight one modular cuspidal eigenform form with integer coefficients and

$$\rho_f : G_\mathbb{Q} \to \text{GL}_2(\mathbb{C})$$

is the associated Galois representation via Serre-Deligne, then $G := G_\mathbb{Q}/\ker \rho_f$ is isomorphic to a dihedral group of order 6, 8, or 12.

**Proof.** Let $\rho : G \to \text{GL}_2(\mathbb{C})$ be the corresponding irreducible faithful representation. Let $p$ be a prime such that $\chi(p) = -1$, then we must have $a_p = 0$ which implies $s := \text{Frob}_p \in G$ has trace 0 in the image of $\rho_f$. Then the characteristic polynomial of $\rho_f(s)$ is $x^2 - 1$ and this forces $s$ to have order 2 in $G$.

Let $r \in G$ such that $\det(\rho_f(r)) = 1$. Then $\det(\rho_f(sr)) = -1$, which implies $sr$ has order 2 and $srs = r^{-1}$.
Let $H \leq G$ be the subgroup generated by elements of determinant 1. Note that, \[
\text{Ind}_H^G(\rho|_H) \simeq \rho \oplus (\rho \otimes \text{det}). \]
This follows from the fact that, by Frobenius reciprocity,
\[
\text{Ind}_H^G(\rho|_H) \simeq \text{Ind}_H^G(1_H \otimes \rho|_H) \\
\simeq \text{Ind}_H^G(1_H) \otimes \rho \\
\simeq \rho \oplus (\rho \otimes \text{det}),
\]
where $1_H$ is the trivial representation of $H$. Since having determinant $-1$ implies the trace vanishes, we have that $\rho \otimes \text{det} \simeq \rho$. We then have
\[
\langle \rho|_H, \rho|_H \rangle = \langle \text{Ind}_H^G(\rho|_H), \rho \rangle = 2.
\]
This implies, from degree considerations, $\rho|_H$ decomposes into a direct sum of two one-dimensional representations; say $\rho|_H \simeq \chi_1 \oplus \chi_2$.

Now, $\chi_1$ and $\chi_2$ are distinct, since otherwise,
\[
\langle \text{Ind}_H^G(\chi_1), \rho \rangle = \langle \chi_1, \rho|_H \rangle = 2,
\]
but this is impossible since $\rho$ is irreducible and $\rho$ and $\text{Ind}_H^G(\chi_1)$ have degree 2. Thus, $\langle \text{Ind}_H^G(\chi_1), \rho \rangle = 1$ and so $\rho \simeq \text{Ind}_H^G(\chi_1)$. Since $\rho$ is faithful, so is $\chi_1$, so we must have that $H$ is cyclic. Since $r$ can be taken to be arbitrary in $H$, we can assume $r$ generates $H$. It then follows that $r$ and $s$ must generate $G$ since $H$ has index 2 in $G$. Thus, $G$ is a Dihedral group. From the previous section, the only possible orders are 6, 8, or 12 under the integer coefficients assumption.
3.4. Main Results

We will use the following lemmas to simplify each of the cases

**Lemma 1.** Let \( f(\tau) := \eta(n\tau)\eta(m\tau) \) be an eta-product with \( n + m = 24 \) (note that this assumption is necessary for \( f \) to be an eigenform in \( q \)). then

\[
f(\tau) = \sum_{u,v\in\mathbb{Z}} (-1)^{u+v} q^{(n(6u+1)^2+m(6v+1)^2)/24}.
\]

**Proof.** We can use Euler’s pentagonal number theorem,

\[
\prod_{k=1}^{\infty} (1 - q^k) = \sum_{l\in\mathbb{Z}} (-1)^l q^{l(l+1)/2}, |q| < 1,
\]

to get the Fourier expansion. Indeed,

\[
\eta(n\tau)\eta(m\tau) = \left( q^{n/24} \prod_{k=1}^{\infty} (1 - q^{nk}) \right) \left( q^{m/24} \prod_{k=1}^{\infty} (1 - q^{mk}) \right),
\]

\[
= \left( q^{n/24} \sum_{u\in\mathbb{Z}} (-1)^u q^{nu(3u+1)/2} \right) \left( q^{m/24} \sum_{v\in\mathbb{Z}} (-1)^v q^{mv(3v+1)/2} \right),
\]

\[
= q \sum_{u,v\in\mathbb{Z}} (-1)^{u+v} q^{12(3nu^2+nu+3mv^2+mv)/24},
\]

\[
= q \sum_{u,v\in\mathbb{Z}} (-1)^{u+v} q^{36nu^2+12nu+36mv^2+12mv)/24},
\]

\[
= \sum_{u,v\in\mathbb{Z}} (-1)^{u+v} q^{(n(6u+1)^2+m(6v+1)^2)/24},
\]

\[
= \sum_{u,v\in\mathbb{Z}} (-1)^{u+v} q^{(n(6u+1)^2+m(6v+1)^2)/24}.
\]

\[\square\]
Lemma 2. For all \( u, v \in \mathbb{Z} \)

\[ 6u + 1 \equiv 6v + 1 \pmod{4} \iff u \equiv v \pmod{2}. \]

3.4.1. Proof of Theorem 20

Proof of Theorem 20 for the mentioned eta-products. For the first case, our first lemma gives

\[ \eta(3\tau)\eta(21\tau) = \sum_{u,v \in \mathbb{Z}} (-1)^{u+v} q^{((6u+1)^2 + 7(6v+1)^2)/8} := \sum_{n=0}^{\infty} a_n q^n, \]

Let \( p \neq 2, 3, 7 \) be a prime with \( a_p = 2 \), then \( \left( \frac{-7}{p} \right) = 1 \). Note that \( \mathbb{Q} (\sqrt{-7}) \) has class number 1, so there exist \( a', b' \in \mathbb{Z} \) such that \( p = (a')^2 + a'b' + 2(b')^2 \). For \( p \neq 2 \), we necessarily have \( a' \) odd and \( b' \) even, so we have \( p = a^2 + 7b^2 \) with \( a = a' + b' / 2 \) and \( b = b' / 2 \). Since \( \mathbb{Z} [\frac{1+\sqrt{-7}}{2}] \) is a UFD, the only solutions (up to a sign) to \( 8p = x^2 + 7y^2 \) are \( 8p = (a - 7b)^2 + 7(a + b)^2 \) and \( 8p = (a + 7b)^2 + 7(a - b)^2 \). Since \( p \) is odd, we must have \( a \not\equiv b \pmod{2} \). If \( p \equiv 2 \pmod{3} \), then we must have neither \( a \) nor \( b \) divisible by 3. Then either \( a - 7b \equiv a - b \equiv 0 \pmod{3} \) or \( a + 7b \equiv a + b \equiv 0 \pmod{3} \), but this would imply \( a_p = 0 \). As such, we can assume \( p \equiv 1 \pmod{3} \) so either \( 3|a \) or \( 3|b \). If \( 3|a \), then \( a - 7b \not\equiv a + b \pmod{3} \), \( a + 7b \not\equiv a - b \pmod{3} \), and we need to adjust the sign of exactly one of \( x = a \pm 7b \) or \( y = a \mp b \) to satisfy the \( 1 \pmod{6} \) restriction. Without loss of generality, assume \( a - 7b \equiv -a - b \equiv 1 \pmod{3} \). Since \( a_p = 2 \), Lemma 2 implies \( a - 7b \equiv -a - b \pmod{4} \). But then, \( 2(a - 3b) \equiv 0 \pmod{4} \). Thus, \( a \equiv b \pmod{2} \), a contradiction, so we must have \( 3|b \).
Thus,

\[ a_p = 0 \iff \left( \frac{-7}{p} \right) = -1 \text{ or } \left( \frac{-3}{p} \right) = -1 \]

\[ a_p = -2 \iff p = a^2 + 7b^2 \text{ with } a \text{ divisible by 3} \]

\[ a_p = 2 \iff p = a^2 + 7b^2 \text{ with } b \text{ divisible by 3}. \]

So the desired extension must be a cyclic extension of degree 4 over \( \mathbb{Q}(\sqrt{-7}) \) corresponding to the\(^2\) character

\[ \chi : \mathcal{R}^+_{F,3} \cong ((\mathbb{Z}[\omega]/(3))^\times)/\{\pm 1\} \xrightarrow{\sim} \mu_4 \]

and is ramified at 3, 7, and possibly 2 and \( \omega = -1/2 + \sqrt{-7}/2 \).

Now let \( K \) be the splitting field of \( x^4 - x^3 + 2x + 1 \). Since this is ramified only at 3 over \( \mathbb{Q}(\sqrt{-7}) \) which is coprime to the order of \( \text{Gal}(K/\mathbb{Q}(\sqrt{-7})) \cong \mathbb{Z}/4\mathbb{Z} \), we have that the conductor must be (3). Thus, the corresponding Hecke character must be

\[ \chi : \mathcal{R}^+_{F,3} \xrightarrow{\sim} \mu_4 \]

as desired, where \( \mu_n \) denotes the cyclic multiplicative group of \( n \) elements.

Alternatively on the coefficients side, we can use the series expansion

\[ \eta(\tau) = \frac{1}{2} \sum_{n \in \mathbb{Z}} \left( \frac{12}{n} \right) q^{n^2/24} \quad (3.5) \]

to get

\[ \eta(3\tau)\eta(21\tau) = \frac{1}{4} \sum_{u,v \in \mathbb{Z}} \left( \frac{12}{uv} \right) q^{(u^2+7v^2)/8}. \]

Since \( \left( \frac{12}{n} \right) = \left( \frac{12}{m} \right) \), the sign of \( u \) and \( v \) can be ignored and we can assume \( u, v \geq 0 \) without loss of generality. If \( a_p = 2 \), then as before, we have \( p = a^2 + 7b^2 \) for some \( a, b \in \mathbb{Z} \) and the

\(^2\)Characters with the same kernel necessarily correspond to the same extension.
only two solutions to $8p = u^2 + 7v^2$ are $(u, v) = (a \pm 7b, a \mp b)$ and so $uv = a^2 - 7b^2 \pm 6ab$. Since $a \not\equiv b \pmod{2}$, we have $uv \equiv a^2 - 7b^2 \pm 6ab \equiv (a + b)^2 \equiv 1 \pmod{4}$. As $a_p = 2$ we must have $uv \equiv (a + b)(a - b) \equiv 1 \pmod{3}$ as otherwise $(\frac{12}{uv}) \neq 1$. Thus, $a + b \equiv a - b \pmod{3}$ which implies $3 | b$ as desired.

As in the previous case, we obtain the Fourier expansion of $\eta(4\tau)\eta(20\tau)$ as

$$\eta(4\tau)\eta(20\tau) = \sum_{u,v \in \mathbb{Z}} (-1)^{u+v} q^{((6u+1)^2 + 5(6v+1)^2)/6} := \sum_{n=0}^{\infty} b_n q^n.$$ 

As well, for a prime $p$ not dividing the level, we have that if $(-5/p) = -1$, then of course, $b_p = 0$. If $(-5/p) = 1$, we have that the ideal $(p)$ splits into either two principal ideals (in which case $p = a^2 + 5b^2$ for some $a, b \in \mathbb{Z}$), or two non-principal ideals (so $2p = a^2 + 5b^2$ for some $a, b \in \mathbb{Z}$ as $\mathcal{O}_F$ has class number 2 and the ideal $2\mathcal{O}_F$ splits into the square of a non-principal ideal). In the latter case, we must have $b_p = 0$, since $3\mathcal{O}_F$ also splits into non-principal ideals which implies there are no solutions to $6p = x^2 + 5y^2$. So suppose $p = a^2 + 5b^2$, which is equivalent to saying $p\mathcal{O}_F$ splits into two principal ideals, and with consideration to the class number, the only two solutions (up to signs) of $6p = x^2 + 5y^2$ are $6p = (a - 5b)^2 + 5(a + b)^2$ and $6p = (a + 5b)^2 + 5(a - b)^2$. Since

$$p = a^2 + 5b^2 \equiv a^2 - b^2 \pmod{6} \equiv (a + b)(a - b) \pmod{6}$$

and

$$p \equiv \pm 1 \pmod{6}$$

we must have that $a - 5b \equiv a + b \equiv \pm 1 \pmod{6}$ and $a + 5b \equiv a - b \equiv \pm 1 \pmod{6}$. So there are exactly two solutions to $6p = (6u+1)^2 + 5(6v+1)^2$ after an appropriate choice of
sign. Finally, we note that

\[ a - 5b \equiv a - b \equiv a + b \pmod{4} \iff b \equiv 0 \pmod{2}. \]

Thus, we have

\[ b_p = 0 \iff \left( \frac{-5}{p} \right) = -1, \text{ or } \left( \frac{-5}{p} \right) = 1 \text{ and } \left( \frac{-1}{p} \right) = -1, \]

\[ b_p = -2 \iff p = a^2 + 5b^2 \text{ with } b \text{ odd}, \]

\[ b_p = 2 \iff p = a^2 + 5b^2 \text{ with } b \text{ even}. \]

So our desired extension must be a quadratic extension of the Hilbert Class field of \( \mathbb{Q}(\sqrt{-5}) \), which we know to be \( H := \mathbb{Q}(\sqrt{-5}, \sqrt{-1}) \), corresponding to the character

\[ \chi : \mathcal{R}_{F,2}^+ \to \mu_4. \]

If \( K \) is the splitting field of \( f(x) = x^4 + x^2 - 1 \) then \( H \subset K \) as expected and \( \text{disc}_{K/\mathbb{Q}(\sqrt{-5})} = (4) \) which gives an upper bound on the conductor. By checking how \( f \) splits at a carefully chosen prime based on its equivalence class in \( \mathcal{R}_{F,4}^+ \), we can verify that the conductor is 2.

Indeed, taking \( P = (3 + 4\sqrt{-5})|(89) \), we have that \( P \equiv 3 \pmod{4} \) and

\[ x^4 + x^2 - 1 \equiv (x + 3)(x + 41)(x + 48)(x + 86) \pmod{89}. \]

This implies \( \chi(I) = 1 \) for all \( I = P \in \mathcal{I}_{F,4}/\mathcal{P}_{F,4}^+ \) and consequently, that the conductor of \( K/\mathbb{Q}(\sqrt{-5}) \) is 2 as desired.

For the last case, using Euler’s pentagonal number theorem to write

\[ \eta(6\tau)\eta(18\tau) = \sum_{u,v \in \mathbb{Z}} (-1)^{u+v} q^{((6u+1)^2+3(6v+1)^2)/4} := \sum_{n=0}^{\infty} c_n q^n. \]
If \( p = a^2 + 3b^2 \) for some \( a, b \in \mathbb{Z} \) and \( p \neq 2, 3 \), we have that by unique factorization in \( \mathcal{O}_F \)
\[
4p = (a - 3b)^2 + 3(a + b)^2 = (a + 3b)^2 + 3(a - b)^2 = (2a)^2 + 3(2b)^2
\]
are the only solutions to \( 4p = x^2 + 3y^2 \) (up to sign) with the last solution being safe to ignore since it does not contribute to \( c_p \) given the restriction that \( x \) and \( y \) are \( 1 \) (mod \( 6 \)).

Since \( p \equiv 1, 5 \) (mod \( 6 \)), we have that
\[
a^2 + 3b^2 \equiv (a + 3b)(a - 3b) \equiv 1, 5 \pmod{6},
\]
so \( a - 3b \equiv a + 3b \equiv \pm 1 \) (mod \( 6 \)). If 3 divides \( b \), we can take appropriate signs such that
\[
a - 3b \equiv a + 3b \equiv a - b \equiv a + b \equiv 1 \pmod{6}.
\]
If 3 does not divide \( b \), exactly one of \( a - b, a + b \) must be 0 (mod \( 3 \)) since \( p \neq 3 \) implies \( a \equiv \pm 1 \) (mod \( 3 \)), and we only have one solution capable of satisfying the 1 (mod \( 6 \)) restriction.

The sign of the coefficient is then determined by Lemma 2 and noticing that \( a - 3b \equiv a + b \) (mod \( 4 \)) and \( a + 3b \equiv a - b \) (mod \( 4 \)).

So we have that \( c_p = 2 \) if and only if \( p = a^2 + 3b^2 \) with \( b \) a multiple of 3. But this is a well known case of cubic reciprocity, see [13] for example, and these are precisely the primes in which \( x^3 - 2 \) splits modulo \( p \) and so this must be the desired polynomial.

3.5. Weight 1 eta-quotients

While the eigenforms examined are limited to the eta products in [12], we can expand our reasoning to any weight one eta-quotients. In [18], Martin gave a list of all eta-quotients that are Hecke eigenforms by showing that there are only finitely many eigenform eta-quotients \( f \) such that \( W_N f \) is also an eigenform, where \( W_N \) is the Fricke involution and \( N \) is the level of \( f \). In particular, he showed that the order of zero at any cusp
is bounded for eta-quotients satisfying this property, putting restrictions on the level and weight, and gave a complete list. Of the multiplicative eta quotients listed, 27 of them are of weight one. Of these 27, 12 are cusp forms and 15 correspond to Eisenstein series.

### 3.5.1. Eisenstein series

For the Eisenstein series, the structure of their Galois representations can be deduced similarly to the cusp form case.

**Corollary 1.** Let $f$ be a weight one noncusp eigenform with integer coefficients and $K$ be the corresponding Galois extension as discussed in previous sections. Then $K$ is either a quadratic or biquadratic extension.

**Proof.** Similarly to the cusp form case, if $r, s \in G$ (as in §3.3.2) with the image of $r$ and $s$ having determinant $+1$ and $-1$ respectively, then $s$ has order 2 and $srs = r^{-1}$. Since $f$ is a noncusp form, its corresponding Galois representation is reducible, which implies $G$ is abelian. Thus, $r$ has order at most 2 and $G$ must be a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Since we can associate a weight 1 Eisenstein series of level $N$ to a triplet $\{\phi_1, \phi_2\}$, where the $\phi_i$ are Dirichlet characters mod $N$ with conductors $n_1$ and $n_2$ respectively such that $\phi_1\phi_2(-1) = -1$ (see [9]), our previous corollary implies that the of Dirichlet characters are either quadratic or trivial. Additionally, the reducibility gives us

$$\text{Tr}(\rho(\text{Frob}_p)) = \phi_1(p) + \phi_2(p).$$

For explicitly determining $\phi_1$ and $\phi_2$ from a given eta-quotient, the restrictions on the conductors imply that it is sufficient to only look at the Fourier coefficients $a_{\psi(1)}, \ldots, a_{\psi(N-1)}$ where $\psi(i)$ is a prime $p_i \equiv i \pmod{N}$, and comparing the coefficients to the finitely many
possible characters. Each quadratic character uniquely determines a quadratic extension and the corresponding polynomials follow easily and are given in Theorem 20.

One interesting observation from the Eisenstein series forms is that the eta-quotients with corresponding Galois group $\mathbb{Z}/2\mathbb{Z}$ are precisely the forms which do not vanish at the cusp $i\infty$.

### 3.5.2. Remaining cusp forms

Of the 12 cusp forms in Martin’s table, 7 of them are the aforementioned eta-products. Like with the eta-products, we can make use of quadratic forms to identify the Artin representations attached to the remaining 5 cases.

The method in which these can be proven is similar enough to the proofs for the eta-products.

We can obtain the series representations by noting that all of these forms are products of two primitive eta-quotients of weight $1/2$ and the corresponding theta series of all of these forms was given by Mersmann, which can be found in [6] with some earlier known series expansions described in [19]. From here, most of the remaining cusp forms can be dealt with very similarly to the alternative proof given for $\eta(3\tau)\eta(21\tau)$.

In fact, for a form $\mu(a\tau)\mu(b\tau)$, where $\mu$ is given as in 3.2, on the list and $d := b/a$, the relevant quadratic form is $x^2 + dy^2$. So for a prime $p$ with the $p$th Fourier coefficient $a_p = 2$, we have that $p$ is of the form $a^2 + db^2$ and $(24/a)p = (a + db)^2 + d(a \mp b)^2$. Then we can determine that $\left(\frac{24}{a^2 - db^2 \pm (d-1)ab}\right) = 1$ which puts congruence conditions on $a$ and $b$. Then just like for the case of $\eta(4\tau)\eta(20\tau)$, after making a guess for the corresponding polynomial, it is just a matter of factoring the polynomial over carefully chosen primes to
show that the corresponding Hecke character matches the congruence conditions on $a$ and $b$. We’ll list the relevant congruence conditions below for $p \nmid ab$:

\[
a_p(\mu(2\tau)\mu(22\tau)) = 2 \iff p = a^2 + 11b^2 \text{ with } 4|b
\]

\[
a_p(\mu(4\tau)\mu(20\tau)) = 2 \iff p = a^2 + 5b^2 \text{ with } 4|ab
\]

\[
a_p(\mu(6\tau)\mu(18\tau)) = 2 \iff p = a^2 + 3b^2 \text{ with } 6|b
\]

\[
a_p(\mu^2(12\tau)) = 2 \iff p = a^2 + 4b^2 \text{ with either } 6|b, \text{ or } 3|a \text{ and } 2 \nmid b.
\]

For the last form, the relevant quadratic form is $x^2 + y^2$ and the condition that $p = a^2 + 4b^2$, is just to give a simpler congruence condition.

One interesting observation, is that if we consider

\[
\mu(\tau) = \frac{1}{2} \sum_{n \in \mathbb{Z}} \left( \frac{24}{n} \right) q^{n^2/24},
\]

then the corresponding conductors for $\mu(2\tau)\mu(22\tau)$, $\mu(4\tau)\mu(20\tau)$, $\mu(6\tau)\mu(18\tau)$, and $\mu^2(12\tau)$ are exactly twice the conductors for $\eta(2\tau)\eta(22\tau)$, $\eta(4\tau)\eta(20\tau)$, $\eta(6\tau)\eta(18\tau)$, and $\eta^2(12\tau)$ respectively. In fact, compared to the alternative series representation for $\eta(\tau)$ given in equation (3.5), we can see from the coefficients that the representations for the “$\mu$ products” are the same as the eta products but tensored with the unique nontrivial representation

\[
\rho_2 : \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \to \text{GL}_2(\mathbb{C}).
\]

This is an example of a “newform twist,” so $\mu(\tau) = \eta(\tau) \otimes \left( \frac{2}{N} \right)$, where $\left( \frac{2}{N} \right)$ is a grossen-character in the sense of Weil. The forms $\mu(\tau)\mu(23\tau)$ and $\mu(3\tau)\mu(21\tau)$ are in fact multiplicative, however they are not holomorphic at all cusps. Coincidentally(?), $\eta(\tau)\eta(23\tau)$
and $\eta(3\tau)\eta(21\tau)$ are also the only eta-products in which the ideal (2) splits in the corresponding imaginary quadratic extension.

Another difference from the eta-products, is that for each eta-product, the corresponding class group is the full ray class group for the given conductor, but this is not the case for the “$\mu$ products.” This is not surprising given that the restriction of integer coefficients gives a small bound for the degree of the extension. The kernels for the Hecke characters can be determined using the congruence conditions above.

For the last cusp form, we have the series expansion

\[ \frac{1}{2} \theta_2(8\tau)\theta_4(16\tau) = \frac{1}{2} \sum_{u,v \in \mathbb{Z}} \left( \frac{4}{u} \right) (-1)^v q^{u^2+16v^2} \]

and it can easily be seen that

\[ a_p \left( \frac{1}{2} \theta_2(8\tau)\theta_4(16\tau) \right) = 2 \iff p = a^2 + b^2 \text{ with } 8|b. \]
Chapter 4. Finite Monodromy

For the next main topic of this dissertation, we recall the facts from characters of finite fields summarized in 2.3 and hypergeometric functions summarized in 2.4.

4.1. Decompositions and Balanced Datum

Assume that the polynomials \(Q_j(x - e^{2\pi ia_j})\) and \(Q_k(x - e^{2\pi ib_k})\) have integer coefficients. While working over finite fields, the character sums depend only the values of the \(a_i\) and \(b_i\) modulo \(Z\), so without loss of generality we can assume \(a_i, b_i \in (0, 1]\).

**Definition 6.** After a suitable ordering, if either

\[ a_1 < b_1 < \cdots < a_n < b_n, \quad \text{or} \quad b_1 < a_1 < \cdots < b_n < a_n, \]

then we call the datum *interlacing*.

It was shown by Beukers–Heckman in [4] that the monodromy group arising from the hypergeometric differential equation with an interlacing datum is a finite group. Classically, Schwarz gave a list of all length 2 hypergeometric data whose monodromy groups are finite and these correspond to spherical tilings. Under these assumptions it is known that the \(H_q\) functions from 2.4 with any argument \(t \in \overline{Q}\) give the trace of an Artin representation

\[ \rho_t : \text{Gal}(K_{t,N}/\mathbb{Q}) \to \text{GL}_n(\mathbb{C}) \]

with \(K_{t,N}\) a number field which contains \(\mathbb{Q}(\zeta_N)\). In particular, this corresponds to the kernel of the BCM representation defined coming from [3].
Definition 7. We’ll say that $\alpha$ and $\beta$ are balanced if

$$H_q(\alpha, \beta; t) = \frac{1}{q-1} \sum_{\chi \in \hat{\mathbb{F}}_q^\times} J(A\chi^{k_1}, B\chi^{k_2})\chi((-1)^nM(k_1, k_2)t)$$

$$= \left( \sum_{s \in \mathbb{F}_q, f_t(s) = 0} A(s)B(1-s) \right) - \kappa_t$$

where $A$ and $B$ are characters of order at most 2, $f_t \in \mathbb{Z}[x]$, and $\kappa_t$ is a constant depending only on $t$. In this case $K_{t,N}$ is at most a composite of quadratic extensions of the splitting field of $f_t$. In particular, $f_t$ and $\kappa_t$ are independent of $q$.

Example 2. Let $\alpha = \{\frac{1}{3}, \frac{2}{3}\}$ and $\beta = \{1, \frac{1}{2}\}$, $\text{lcm}(\alpha, \beta)=6$, then for $q \equiv 1 \pmod{3}$

$$H_q(\alpha, \beta; t) = \frac{1}{1-q} \sum_{\chi \in \hat{\mathbb{F}}_q^\times} \frac{g(\eta_3\chi)g(\overline{\eta_3}\chi)g(\chi\phi\chi)}{\overline{g(\eta_3)}g(\overline{\eta_3})g(\varepsilon)g(\phi)} \chi(t),$$

where $\eta_3$ denotes a primitive order 3 character in $\hat{\mathbb{F}}_q^\times$ as in §2.3. Multiplying by $\frac{g(\chi)}{g(\chi)}$, using $g(\varepsilon) = -1$, and applying the Hasse-Davenport relation (Theorem 7) we get

$$H_q(\alpha, \beta; t) = \frac{1}{q-1} \sum_{\chi \in \hat{\mathbb{F}}_q^\times} \frac{g(\chi^3\overline{\chi}(3^3)g(\chi^2)\chi(2^2)}{g(\chi)} \chi(t).$$

The right hand side expression does not require $q \equiv 1 \pmod{3}$ and hence can be extended to all finite fields whose characteristic is larger than 3 and in fact, agrees with the BCM character sum. Combining the $\chi$ terms and using the relationship between Gauss and Jacobi sums, we get
$$H_q(\alpha, \beta; t) = \frac{1}{q - 1} \sum_{\chi \in \mathbb{F}_q^\times} g(\chi^3) g(\overline{\chi}^2) \frac{g(\chi)}{g(\chi)} \chi \left( \frac{4t}{27} \right)$$

$$= \frac{1}{q - 1} \sum_{\chi \in \mathbb{F}_q^\times} (J(\chi^3, \overline{\chi}^2) - (q - 1) \delta(\chi)) \chi \left( \frac{4t}{27} \right)$$

$$= \left( \frac{1}{q - 1} \sum_{\chi \in \mathbb{F}_q^\times} J(\chi^3, \overline{\chi}^2) \chi \left( \frac{4t}{27} \right) \right) - 1.$$  

Since

$$J(\chi^3, \overline{\chi}^2) = \sum_{s \in \mathbb{F}_q} \chi^3(s) \overline{\chi}^2(1 - s)$$

$$= \sum_{s \in \mathbb{F}_q} \chi \left( \frac{s^3}{(1 - s)^2} \right),$$

by swapping sums, and collecting the $\chi$ terms we get

$$\left( \frac{1}{q - 1} \sum_{s \in \mathbb{F}_q} \sum_{\chi \in \mathbb{F}_q^\times} \chi \left( \frac{4ts^3}{27(1 - s)^2} \right) \right) - 1.$$  

Then, by orthogonality

$$\sum_{\chi \in \mathbb{F}_q^\times} \chi \left( \frac{4ts^3}{27(1 - s)^2} \right) = \begin{cases} q - 1 & \text{if } \frac{4ts^3}{27(1 - s)^2} = 1 \\ 0 & \text{otherwise.} \end{cases}$$

So if $4ts^3/(27(1 - s)^2) = 1$, then $4ts^3 - 27(1 - s)^2 = 0$. Taking $f_t(s) = 4ts^3 - 27(1 - s)^2$ we can get

$$H_q(\alpha, \beta; t) = \# \{ s \in \mathbb{F}_p \mid f_t(s) = 0 \} - 1.$$  

From the perspective of representations of finite groups, $f_t$ is irreducible for most choices of $t$ and this family of representations can be viewed as the regular representation of $S_3$ with the subtraction of $\kappa_t$ corresponding to the removal of the trivial component of this
representation. In this view, other invariants of $f_t$ can be used to classify the primes $p$ for which $H_p(\alpha, \beta; t)$ takes on a specified value. For example, if the discriminant of $f_t$ is a square modulo $p$, the corresponding permutation coming from $\text{Frob}_p$ must be even which implies $f_t$ has either 0 or 3 solutions modulo $p$ making the $H_p$ value either -1 or 2 respectively. This is similar to the analysis of Artin representations arising from weight 1 eta-quotients.

**Example 3.** Let $\alpha = \{\frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}\}$ and $\beta = \{1, \frac{1}{2}, \frac{3}{4}\}$. Similar computations can be used to show that when $q \equiv 1 \mod 4$

$$H_q(HD; t) = \left( \frac{1}{q-1} \sum_{\chi \in \mathbb{F}_q^*} J(\phi \chi^6, \chi^4) \chi\left(\frac{2^4 t}{3^6}\right) \right) - \left( \eta_4\left(\frac{t}{9}\right) + \eta_4\left(\frac{t}{9}\right) \right).$$

After reducing the sum to an expression with a single Jacobi sum, the rest of the computation follow similar to the previous example.

Given that there are only finitely many $HD$ corresponding to finite monodromy for a fixed length, it is not hard to check that all the data defined over $\mathbb{Q}$ and interlacing of length 2 and 3 are balanced. However, complications begin to arise in length 4, for example, take $\alpha = \{\frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}\}$ and $\beta = \{1, \frac{1}{2}, \frac{5}{6}\}$ does not appear to be balanced as does the data for the same $\alpha$ set and $\beta = \{1, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}\}$.

**4.2. Applications**

By writing our character sums in this way, we have another tool for decomposing hypergeometric Galois representations and hopefully produce more examples of explicitly computable potentially reducible representations. One such decomposition can be found with the data

$$HD = \{\{1/2, 1/6, 5/6, 1/2, 1/6, 5/6\}, \{1, 1/3, 2/3, 1, 1/3, 2/3\}\}$$
By using the data $HD_1 = \{\{1/2, 1/6, 5/6\}, \{1, 1/3, 2/3\}\}$, which corresponds to finite monodromy, we can decompose the representation at $t = -1$ as follows

**Theorem 22.** Let $HD$ be as above, then for any prime $p \geq 5$

$$H_p(HD; -1) = H_q \left( \begin{array}{ccc} \frac{1}{2} & \frac{1}{2} & -1 \\ \frac{1}{3} & \frac{2}{3} & 1 \\ 1 & \frac{1}{6} & \frac{5}{6} \end{array} \right) + H_q \left( \begin{array}{ccc} \frac{1}{2} & \frac{2}{3} & 1 \\ \frac{1}{3} & \frac{2}{3} & 1 \\ 1 & \frac{1}{6} & \frac{5}{6} \end{array} \right) = a_p(f_{32.2.a.a}) + a_p(f_{36.2.a.a})a_p(\eta(12\tau)^2).$$

For the proof of this theorem, we will need the following Lemma

**Lemma 3.** Let $HD_1 = \{\{1/2, 1/6, 5/6\}, \{1, 1/3, 2/3\}\}$, then,

$$H_q(HD_1; \lambda) = \begin{cases} 0 & \text{if } \lambda \text{ is not a cube modulo } q \\ \phi(1 - s) & \text{if } q \equiv 2 \pmod{3} \\ \phi(1 - s) + \phi(1 - \zeta_3 s) + \phi(1 - \zeta_3^2 s) & \text{if } q \equiv 1 \pmod{3} \end{cases}$$

Where $s^3 \equiv \lambda \pmod{q}$ when possible and $\zeta_3 \in \mathbb{F}_q^\times$ a primitive cube root of 1, and $\phi$ the unique order 2 character on $\mathbb{F}_q^\times$.

**Proof of Lemma.** The proof follows the same process as in Example 2. We will continue to use $\eta_n$ to denote a primitive order $n$ character in $\mathbb{F}_q^\times$. By definition

$$H_q(HD_1; \lambda) = \frac{1}{1 - q} \sum_{\chi \in \mathbb{F}_q^\times} g(\phi \chi)g(\eta_6 \chi)g(\eta_3 \chi)g(\eta_3 \chi g(\eta_3 \chi)g(\eta_3 \chi g(\eta_3 \chi g(\eta_3 \chi g(\eta_3 \chi g(\eta_3 \chi g(\eta_3 \chi g(\eta_3 \chi g(\eta_3 \chi)) \chi(-\lambda).$$

Using the Hasse-Davenport relation (Theorem 7)

$$g(\phi \chi)g(\eta_6 \chi)g(\eta_3 \chi) = g(\phi \chi^3)\eta_6 \chi(3^3)g(\eta_3)g(\eta_3),$$

and

$$g(\chi)g(\eta_3 \chi)g(\eta_3 \chi) = g(\chi^3)\chi(3^3)g(\eta_3)g(\eta_3).$$
Along with $g(\varepsilon) = -1$, we get

$$H_q(HD_1; \lambda) = \frac{1}{q-1} \sum_{\chi \in \mathbb{F}_q^\times} \frac{g(\phi \chi^3) \eta_6 \chi(3^2) g(\eta_3) g(\overline{\eta_3}) g(\overline{\chi}^3) \chi(3^2)}{g(\phi) g(\eta_6) g(\overline{\eta_6})} \chi(-\lambda).$$

The Reflection principle gives us

$$g(\eta_3) g(\overline{\eta_3}) = \eta_3(-1)q = q$$

and

$$g(\eta_6) g(\overline{\eta_6}) = \phi(-1)q,$$

giving us

$$H_q(HD_1; \lambda) = \frac{1}{q-1} \sum_{\chi \in \mathbb{F}_q^\times} \frac{\phi(-3) g(\phi \chi^3) g(\overline{\chi}^3)}{g(\phi)} \chi(-\lambda).$$

If we note that $\overline{\eta_6}(3^2) = \phi(3)$ and collecting $\chi$ terms

$$H_q(HD_1; \lambda) = \frac{1}{q-1} \sum_{\chi \in \mathbb{F}_q^\times} \phi(-3) \frac{\phi(-3) g(\phi \chi^3) g(\overline{\chi}^3)}{g(\phi)} \chi(-\lambda).$$

By the relationship between Gauss and Jacobi sums

$$\frac{g(\phi \chi^3) g(\overline{\chi}^3)}{g(\phi)} = J(\phi \chi^3, \overline{\chi}^3)$$

$$= \sum_{s \in \mathbb{F}_q} \phi \chi^3(s) \overline{\chi^3(1-s)}$$

$$= \sum_{s \in \mathbb{F}_q} \phi(s) \chi \left( \frac{s^3}{(1-s)^3} \right).$$

After changing the order of summation, this gives us

$$H_q(HD_1; \lambda) = \frac{1}{q-1} \sum_{s \in \mathbb{F}_q} \phi(s) \sum_{\chi \in \mathbb{F}_q^\times} \chi \left( \frac{\lambda s^3}{(1-s)^3} \right).$$

Note that the $\phi(-3)$ term is dropped; this is because the extension to $G_Q$ by McCarthy [20] and Beukers-Cohen-Mellit [3] defines the character sum as the result of repeated applications the Hasse-Davenport relation, leaving out the normalizing terms we picked up.
here. By orthogonality

\[ \sum_{\chi \in \widehat{F}_q} \chi \left( \frac{\lambda s^3}{(1-s)^3} \right) = \begin{cases} 0 & \text{if } \frac{\lambda s^3}{(1-s)^3} \neq 1 \\ q - 1 & \text{otherwise.} \end{cases} \]

Taking \( f_\lambda(s) = \lambda s^3 + (1-s)^3 \), we then get our sum in the form previously described,

\[ H_q(HD_1; \lambda) = \sum_{s \in \widehat{F}_q, f_\lambda(s) = 0} \phi(s). \]

Take note that this implies \( H_q(HD_1; \lambda) = 0 \) if \( \lambda \) is not a cube. We then have that the roots of this polynomial are \( \frac{1}{1 - \sqrt[3]{\lambda}}, \frac{1}{1 - \zeta_3 \sqrt[3]{\lambda}}, \frac{1}{1 - \zeta_3^2 \sqrt[3]{\lambda}} \) and since \( \phi(1/t) = \phi(t) \), the result then follows.

\[ \Box \]

**Proof of Theorem 22.** Following an idea of Whipple, we first use orthogonality to show

\[ H_q(HD; -1) = \sum_{t \in \widehat{F}_q} H_q(HD_1; t) H_q(HD_1; -1/t). \]

On the left hand side, we have

\[ \frac{1}{1 - q} \sum_{\chi \in \widehat{F}_q} \sum_{\psi \in \widehat{F}_q^*} \frac{g(\phi \chi) g(\eta_6 \chi)^2 g(\eta_6 \chi) g(\chi) g(\eta_3 \chi) g(\eta_3 \chi)}{g(\phi) g(\eta_6 \chi) g(\eta_6 \chi) g(\eta_3 \chi) g(\eta_3 \chi)} \chi(-t), \]

and on the right hand side, we have

\[ \sum_{t \in \widehat{F}_q} \frac{1}{(1 - q)^2} \sum_{\chi \in \widehat{F}_q} \sum_{\psi \in \widehat{F}_q^*} \frac{g(\phi \psi) g(\eta_6 \psi) g(\eta_6 \psi) g(\psi) g(\eta_3 \psi) g(\eta_3 \psi)}{g(\phi) g(\eta_6 \psi) g(\eta_6 \psi) g(\psi) g(\eta_3 \psi) g(\eta_3 \psi)} \chi(-t) \psi(1/t) \]

\[ = \sum_{t \in \widehat{F}_q} \frac{1}{(1 - q)^2} \sum_{\chi \in \widehat{F}_q} \sum_{\psi \in \widehat{F}_q^*} \frac{g(\phi \psi) g(\eta_6 \psi) g(\eta_6 \psi) g(\psi) g(\eta_3 \psi) g(\eta_3 \psi)}{g(\phi) g(\eta_6 \psi) g(\eta_6 \psi) g(\psi) g(\eta_3 \psi) g(\eta_3 \psi)} \chi(-1) \psi(t). \]
Moving $\sum_{t \in \mathbb{F}_q}$ inside, we can see that

$$\sum_{t \in \mathbb{F}_q} \chi \overline{\psi}(t) = \begin{cases} 0 & \text{if } \chi \neq \psi \\ q - 1 & \text{otherwise.} \end{cases}$$

This causes the sum on the right hand side to collapse into that of the left hand side.

Using this, we use that Lemma 4.2 tells us that

$$H_q(HD_1; t) = 0$$

if $t$ is not a cube modulo $q$, so we can re-index our summation

$$H_q(HD; \lambda)$$

$$= \frac{1}{3} \sum_{t \in \mathbb{F}_q} H_q(HD_1; t^3) H_q(HD_1; (-1/t)^3)$$

$$= \frac{1}{3} \sum_{t \in \mathbb{F}_q} \left( \phi(1 - t) + \phi(1 - \zeta_3 t) + \phi(1 - \zeta_3^2 t) \right) \left( \phi \left( 1 + \frac{1}{t} \right) + \phi \left( 1 + \frac{\zeta_3}{t} \right) + \phi \left( 1 + \frac{\zeta_3^2}{t} \right) \right) .$$

We can then consider our sum over the cross terms

$$\sum_{t \in \mathbb{F}_q} \phi(1 - t) \phi(1 + 1/t)$$

Using length 1 data, we get

$$\phi(1 - t) = H_q(\{1/2\}, \{1\}; t)$$

$$= \frac{1}{q - 1} \sum_{\chi \in \mathbb{F}_q^*} g(\phi \chi) g(\overline{\chi}) \chi(-t),$$

so we get
\[
\sum_{t \in \mathbb{F}_q} \phi(1-t)\phi(1+1/t) = \sum_{t \in \mathbb{F}_q} \frac{1}{(q-1)^2} \sum_{\chi \in \mathbb{F}_q^*} \sum_{\psi \in \mathbb{F}_q^*} \frac{g(\phi\chi)g(\bar{\chi})g(\phi\psi)g(\bar{\psi})}{g(\phi)^2} \chi(-t)\psi(1/t)
\]
\[
= \frac{1}{(q-1)^2} \sum_{\chi \in \mathbb{F}_q^*} \sum_{\psi \in \mathbb{F}_q^*} \frac{g(\phi\chi)g(\bar{\chi})g(\phi\psi)g(\bar{\psi})}{g(\phi)^2} \chi(-1) \sum_{t \in \mathbb{F}_q} \chi\bar{\psi}(t).
\]

By orthogonality
\[
\sum_{t \in \mathbb{F}_q} \chi\bar{\psi}(t) = \begin{cases} 
0 & \text{if } \chi \neq \psi \\
q - 1 & \text{otherwise,}
\end{cases}
\]
and thus,
\[
\sum_{t \in \mathbb{F}_q} \phi(1-t)\phi(1+1/t) = H_q(\{1/2, 1/2\}; \{1, 1\}; -1).
\]

Examining the other cross terms gives in a similar fashion
\[
H_q(HD; -1) = H_q(\{1/2, 1/2\}; \{1, 1\}; -1)
\]
\[
+ H_q(\{1/2, 1/2\}; \{1, 1\}; -\zeta_3) + H_q(\{1/2, 1/2\}; \{1, 1\}; -\zeta_3^2).
\]

Now the first term matches our theorem and its equality to the Fourier coefficient is a known result. Now, by a Kummer transformation (2.15)
\[
H_q(\{1/2, 1/2\}; \{1, 1\}; -\zeta_3) = \phi(-1)H_q(\{1/2, 1/2\}; \{1, 1\}; -\zeta_3^2),
\]
so we have
\[
H_q(\{1/2, 1/2\}; \{1, 1\}; -\zeta_3) + H_q(\{1/2, 1/2\}; \{1, 1\}; -\zeta_3^2)
\]
\[
= H_q(\{1/2, 1/2\}; \{1, 1\}; -\zeta_3)(1 + \phi(-1)).
\]
Thus, it suffices to show

$$H_q(\{1/2, 1/2\}; \{1, 1\}; -\zeta_3)(1 + \phi(-1)) = H_q(\{1/3, 2/3\}; \{1, 1\}; 1/2)H_q(HD_1; 1).$$

The representation corresponding to $H_q(1/2, 1/2; 1, 1; -\zeta_3)$ can be viewed as the trace of a Galois representation arising from a Legendre elliptic curve over the fiber $\lambda = -\zeta_3$ and its easy to show this has $j$-invariant 0, which is the same as the elliptic curve corresponding to $H_q(\{1/3, 2/3\}; \{1, 1\}; 1/2)$. However, it is not extendable to $G_\mathbb{Q}$ since its conjugate differs by a sign for $q \equiv 7 \pmod{12}$. If we tensor by $\xi(p) = \left(\frac{2+\zeta_3}{p}\right)$, which has conjugate $\bar{\xi}(p) = \phi(-1)\xi(p)$, we can correct this sign difference and from a similar analysis to chapter 3 we have that

$$\xi(p)(1 + \phi(-1)) = a_p(\eta(12\tau)^2).$$

Then from [17], this Fourier coefficient is that of $H_q(HD_1; 1)$ completing the proof. \hfill \Box

It is important to note that the decomposition only used that -1 is a perfect cube, so this implies that the representation for $\lambda^3$ decomposes into a direct sum of a 2-dimensional representation coming from a modular form and a 4-dimensional representation which is expected to come from a Bianchi modular form.

Other possible applications arise from the computations of hypergeometric moments for data corresponding to finite monodromy. In the above example, the corresponding Galois representation is shown to be reducible when restricted to $G_{\mathbb{Q}(\sqrt{3})}$ and it should be doable to produce other examples of potentially reducible representations from similar datum.
4.3. Future directions

It is the author’s hope that this can lead to a full classification of Artin representations arising from hypergeometric functions. Efficient algorithms exist for computing these character sums and having a wide array of explicitly computable examples can help with identifying patterns and testing conjectures for these representations such as the Artin conjecture or Malle’s conjecture. The definition of balanced datum also leaves much to be desired as it is unclear as to whether all intertwining data is balanced and with more computations, the obstruction to datum being balanced will hopefully reveal itself. Certain examples have been shown to suggest that similar identities exist in the classical setting such as a result of Zagier in [30] relating the value of a hypergeometric function to a special value of an $L$-function.

There are also many lingering questions from the analysis of weight 1 modular forms such as whether examples similar to Stark’s example from 3.
Bibliography


Vita

Emma Lien is a 6th year graduate student in the mathematics department at Louisiana State University. She obtained her Bachelor’s Degree in Mathematics from University of Central Florida. Born and raised in Orlando, Florida, she became interested in mathematics as a career path after being inspired by a Calculus teacher at her high school. She anticipates graduating with her Ph.D. in mathematics in May 2024.