ON THE ROOTS OF POLYNOMIALS MODULO PRIMES

BY JOHN T. BRYK

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Mathematics

Written under the direction of

Jerrold B. Tunnell

and approved by

____

____

____

____

New Brunswick, New Jersey

May, 2012

ABSTRACT OF THE DISSERTATION

On the roots of polynomials modulo primes

by John T. Bryk

Dissertation Director: Jerrold B. Tunnell

We study the problem of counting the number of roots of an irreducible polynomial $f(X) \in \mathbb{Z}[X]$ modulo rational primes. We consider the family of polynomials $f_n(X) = X^n - X - 1$, which have Galois groups isomorphic to S_n. The approach we take is to attach Galois representations to the counting problem and then to relate these to automorphic forms. In particular, we attempt to attach the representations to holomorphic forms on GL_2. We show this only works when $n \leq 5$, and we present the solutions to the problem in the $n = 4$ and 5 cases, following methods due to Serre, Crespo, and Buhler for explicitly constructing Galois representations. The solution to the $n = 5$ case is novel, requiring Hilbert modular forms. In solving the problem, we produce the first example of an icosahedral Hilbert form that is not the base change of a classical form.

Acknowledgements

I express deep thanks to Jerrold Tunnell for his suggestion of the problem, his guidance in the development of its solution, and his hard work in hammering out a finished product. I also thank Stephen D. Miller, Ariel Pacetti, and Chuck Weibel for comments and suggestions regarding key details of the argument. A great debt of gratitude is owed to the Magma group for their superior product and, in particular, Steve Donnelly for invaluable, countless hours of technical support. This thesis would not have been possible without the moral and emotional support of John and Linda Bryk, Samuel Coskey, Paul Ellis, and especially my loving wife, Emily Bryk.

Dedication

This thesis is dedicated to my family, Emily and Samuel Bryk. For you, everything.

Table of Contents

Chapter 1

Introduction

A classical question in number theory is that of counting the number of solutions to polynomial equations modulo primes, the simplest case concerning the roots of a univariate polynomial. Initial studies focused on counting nth roots modulo primes, with the first result being the Law of Quadratic Reciprocity, formulated by Euler and proved by Gauss. Although the explicit statement of the theorem gives a relationship between the Legendre symbols of two primes, we interpret it in a different fashion. Fixing an integer d and letting p vary over all primes, the Legendre symbol gives a formula for the number of square roots of squarefree d modulo p, namely:

$$\#\{x \pmod{p} : x^2 \equiv d \pmod{p}\} = 1 + \left(\frac{d}{p}\right)$$

Quadratic Reciprocity then implies that the Kronecker symbol $\left(\frac{d}{\cdot}\right)$ is the quadratic character modulo the absolute value of the discriminant $D = |d|$ or $|4d|$ of $\mathbb{Q}\left(\sqrt{d}\right)$, and computation of $\left(\frac{d}{\cdot}\right)$ is reduced to a congruence condition. Higher degree reciprocity theorems followed: the Laws of Biquadratic and Cubic Reciprocity and Eisenstein and Kummer's general laws for prime-power roots. (It is worth noting that these higher degree laws require passing to the Gaussian integers, Eisenstein integers, and rings of integers over other cyclotomic fields.)

The true breakthrough in formulating reciprocity laws was Artin Reciprocity, which allows representations of Galois groups of abelian extensions of number fields to be expressed as characters on ideal class groups. If K is a number field and $f(X) \in \mathfrak{o}_K[X]$ defines an abelian extension L of K, then the number of roots of f modulo almost all primes $\mathfrak{p}$ is given by a sum over characters of $G = G(L|K)$:

$$\sum_{\chi \in \widehat{G}} \chi(\sigma_{\mathfrak{p}})$$

where $\sigma_{\mathfrak{p}}$ is the Frobenius element at $\mathfrak{p}$. Artin Reciprocity then represents $G(L|K)$ as a class group C, and the character sum becomes one over $\widehat{C}$, reducing the computation to determining the structure of C and the class of $\mathfrak{p}$ in C.[1]

The sum of characters given above can be derived by looking at the complex representation $\rho : G(L|K) \to GL_n(\mathbb{C})$, $n = \deg(f)$, obtained by looking at the action of $G(L|K)$ on $L \otimes_K \mathbb{C} \simeq \mathbb{C}^n$. Indeed, ρ can be interpreted as the *permutation representation* of $G(L|K)$ acting on the roots of f. It is clear that $\chi_\rho(\sigma_{\mathfrak{p}})$ is equal to the number of points fixed by $\sigma_{\mathfrak{p}}$, and this is precisely the number of roots of f modulo $\mathfrak{p}$. As ρ is also just the regular representation of $G(L|K)$, the irreducible character decomposition $\rho = \bigoplus_{\chi \in \widehat{G}} \chi$ then gives the character sum.

This generalizes to case that $G(L|K)$ is nonabelian. We now let ρ be the permutation representation of $G(L|K)$ acting on the $\mathbb{C}$-vector space formally spanned by the roots $\{x_1, \ldots, x_n\}$ of f in L. To proceed in the above fashion, we need a nonabelian version of Artin Reciprocity and class field theory. This is part of the Langlands program for number fields, the veracity of which would imply, in small part, that all finite-dimensional complex Galois representations can be attached to automorphic representations.

Examples of attaching automorphic representations to the problem of counting the number of roots of polynomials modulo primes are given by Serre ([31]), in which Serre also considers the density of primes with a given number of roots by applying the Chebotarev Density Theorem. The family of polynomials $f_n(X) = X^n - X - 1$ is studied, in part because the Galois group of f_n is well-known to be isomorphic to S_n and, hence, all possibilities for the factorization a degree n polynomial are realized. The cases $n = 2, 3$, and 4 are worked out explicitly.

The case $n = 2$ reduces to Quadratic Reciprocity. However, irreducible representations of degree at least 2 do arise when decomposing the permutation representation ρ for $n \geq 3$. For $n = 3$ and 4, Serre shows that the permutation representation ρ can be decomposed into representations of degree 1 and odd[2] representations of degree 2

[1] This is needlessly complex in this scenario–the character sum is 0 unless $\mathfrak{p}$ is in the trivial class of C, in which case it is equal to the degree of $|C| = [L : K]$.

[2] A degree 2 representation is *odd* if its determinant at complex conjugation is -1.

on $G_{\mathbb{Q}}$. Due to results of Hecke, Langlands ([20]), and Tunnell ([37]), the degree 2 representations are known to correspond to classical modular forms, with the trace at σ_p of each representation equal to the pth Fourier coefficient of the corresponding form. Furthermore, in the $n = 3$ case, Serre gives an explicit expression for the modular form in terms of theta series of quadratic forms.

In this thesis, we extend the results of Serre to the $n = 5$ case, with one of the main results (Proposition 6.3.5) being a formula for the number of roots of $f_5(X) = X^5 - X - 1$ modulo primes in terms of modular forms on GL_2. However, in order to work with degree 2 Galois representations, we must pass to Galois representations over a real quadratic extension of K, over which f_5 has Galois group equal to the icosahedral group, A_5. Thus, the representations correspond to *Hilbert* modular forms over K. In particular, our second main result (Corollary 6.3.4) is showing the existence of icosahedral Hilbert modular forms that do not arise from base change by constructing such forms. To our knowledge, these are the first explicit examples of such.

We proceed as follows:

Chapter 2. We discuss expressing representations in terms of tensor products of smaller degree representations, in particular showing that we cannot express the permutation representation ρ in terms of degree 1 and 2 Galois representations when $n \geq 6$. We then introduce the theory developed by Serre ([32, Ch. 9]) and Crespo ([9]) necessary to show the existence of certain degree 2 Galois representations in the $n = 4$ and 5 cases.

Chapter 3. As a motivating example for the $n = 5$ case, we work through the $n = 4$ case in detail. We introduce machinery developed by Crespo ([6]) for explicitly constructing Galois representations, and we develop some tools for computing the ramification for the fixed fields of these representations. We also give an explicit expression for the square of the form we construct in terms of theta series of quadratic forms associated to a quaternion algebra.

Chapter 4. We begin the $n = 5$ case, representing the permutation representation ρ in terms of representations of degree at most 2 on an index 2 subgroup of $G_{\mathbb{Q}}$ and using Crespo's theory to show the existence of said representations. The formula for the number of roots of f_5 modulo primes is derived.

Chapter 5. The representations from Chapter 4 are explicitly constructed using Crespo's formulas ([7]) and methods used by Buhler ([4, Ch. 1,4]); the latter were used in showing the existence of an icosahedral modular form over $\mathbb{Q}$. The relative merits of using Crespo's methods versus Buhler's are discussed.

Chapter 6. The basic theory of Hilbert modular forms is introduced following [12], [14], [34], and [39]. We develop a trick for constructing a weight 1 form with specified Hecke eigenvalues, and then we use discriminant bounds due to Poitou ([24, 25]) to show that there is only one such form. It immediately follows that this form corresponds to the representations constructed in Chapter 5. The main results are stated in Corollary 6.3.4 and Proposition 6.3.5, with the latter giving the formula for the number of roots of f_5 modulo primes in terms of icosahedral Hilbert modular forms.

We conclude with appendices containing proofs and alternate techniques for some aspects Chapter 6.

Chapter 2

Galois Embedding Problems and Lifting Representations

2.1 Introduction

The study of the number of roots of a polynomial modulo primes naturally leads to linear Galois representations, while our desire to connect the problem to classical or Hilbert modular forms necessitates expressing linear representations in terms of odd, degree 2 projective representations. We discuss the problems that force us to work with projective representations, and then we introduce the theory that allows us to lift projective representations to actual Galois representations.

2.2 The Augmentation Representation

We let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree n, and we consider the permutation representation:

$$\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{C})$$

obtained by letting $G_{\mathbb{Q}}$ act on the n-dimensional vector space formally spanned by the roots of $f(X)$. If u_i are the roots of $f(X)$, then the vector $\sum_{i=1}^{n} u_i$ is fixed, and the identity representation is a summand of ρ.

Definition 2.2.1. The *augmentation representation* α is the degree $n-1$ representation $\alpha = \rho - \mathbf{1}$.

We study a specific family of polynomials, namely $f_n(X) = X^n - X - 1$, $n \geq 2$. These are irreducible for all n, and the Galois group of each f_n is the full symmetric group S_n (see, e.g., [30, p. 144]). Augmentation is always irreducible. For $n = 2$, α is a Dirichlet character, while for $n = 3$, α is an odd dihedral representation with determinant $\chi = \chi_{\mathbb{Q}(\sqrt{-23})}$, so it corresponds to a newform f in $S_1(23,\chi)$. In the $n = 2$ case, periodicity allows the values of the Dirichlet character to be given by the coefficients in the Taylor series of a rational function, while in the $n = 3$ case, Serre ([31, p. 434]) gives an expression for the modular form as the difference of two theta series coming from the quadratic forms associated to two of the ideal classes of $\mathbb{Q}(\sqrt{-23})$:

$$f = \frac{1}{2}\left(\sum_{x,y\in\mathbb{Z}} q^{x^2+xy+6y^2} - \sum_{x,y,\in\mathbb{Z}} q^{2x^2+xy+3y^2}\right)$$

For $n \geq 4$, however, we cannot immediately attach Dirichlet characters or modular forms to augmentation using the representations of the Galois group of f_n. A naive strategy for doing so might use *virtual characters* of the group S_n.

Definition 2.2.2. Let G be a profinite group. The *ring of virtual characters* $R(G)$ is the $\mathbb{Z}$-linear span of the irreducible continuous characters on G. For any $k \geq 1$, $R^{(k)}(G)$ denotes the subring generated by characters of degree at most k.

If the character χ_α is in $R^{(2)}(S_n)$, then we can immediately associate the degree 1 representations with Dirichlet characters, while if we also assume the degree 2 characters are odd, we can associate them with modular forms, giving the desired expression for χ_α. However, this is not possible. Indeed, for $n \geq 5$, there are no degree 2 characters, and $R^{(2)}(S_n)$ is the $\mathbb{Z}$-linear span of the identity and sign characters. For $n = 4$, there *is* a character χ of degree 2, but $\chi^2 = \mathbf{1} + \mathrm{sgn} + \chi$, so $R^{(2)}(S_4)$ is the $\mathbb{Z}$-linear span of χ and the two degree 1 characters.

A slightly more sophisticated strategy is to extend the virtual characters under consideration to those on $G_{\mathbb{Q}}$. In the case of $n = 4$, this works: we have $\chi_\alpha \in R^{(2)}(G_{\mathbb{Q}})$, and the degree 2 characters in the expression for χ_α do correspond to modular forms. We discuss this in the Chapter 3. However, this strategy fails in general.

Theorem 2.2.1. *Let L be a Galois extension of K with $G(L|K) \simeq S_n$, $n \geq 5$, and let α be the augmentation representation on S_n. Then $\chi_\alpha \notin R^{(2)}(G_K)$.*

Proof. Suppose $\chi_\alpha \in R^{(2)}(G_K)$, so that there are $n_i \in \mathbb{Z}$ and degree 1 and 2 characters

$\chi_{i,j}$ on G_K such that:

$$\chi_\alpha = \sum_i n_i \prod_j \chi_{i,j}$$

Adding those terms on the right with $n_i < 0$ to the left and noting that α is irreducible, we see that χ_α must occur in the irreducible character decomposition of one of the products $\prod_j \chi_{i,j}$ on the right. We drop the index i, and we let θ_j be the representation corresponding to χ_j, F_j be the fixed field of the kernel of θ_j, and $F = \prod_j F_j$.

Since F is the fixed field of the intersection of the kernels of the θ_j, $\Theta = \bigotimes_j \theta_j$ is a representation of $G(F|K)$, as is α, being a summand of Θ. And since α is a summand of Θ, $L \subset F$, giving a surjection $G(F|K) \twoheadrightarrow G(L|K) \simeq S_n$. Additionally, we have injections:

$$G(F|K) \hookrightarrow \prod_j G(F_j|K) \hookrightarrow \prod_j GL_2(\mathbb{C})$$

The proof then reduces to showing that if G is a finite subgroup of $\prod GL_2(\mathbb{C})$, G does not surject onto S_n.

Let $f : G \twoheadrightarrow S_n$ be a surjective homomorphism. Since S_n has trivial center, the center of G is in the kernel of f, and so we may assume that G actually embeds in $X = G_1 \times \ldots \times G_m$, where:

$$G_i \simeq PGL_2(\mathbb{C})$$

Let H_i be the projection of G into G_i. Let D be the final term in the derived series of G; note that $f(D) = A_n$. D embeds into the direct product of the final terms D_i of the derived series of the H_i. By inspection of the finite subgroups of $PGL_2(\mathbb{C})$, it follows that $D_i = 1$ or $D_i \simeq A_5$. The result immediately follows for $n > 5$.

For $n = 5$, note that if $D_i \simeq A_5$, then $H_i = D_i$, as A_5 is a maximal finite subgroup of $PGL_2(\mathbb{C})$. In particular, we have that $N_X(D)$ induces an inner automorphism on D, whence $N_X(D) = DC_X(D)$, whence $N_G(D) = DC_G(D)$. The same is true in $f(G)$, but this fails for A_5 in S_5, whence the result. □

The author thanks J. Buhler and R. Guralnick for help with the proof.

The proof suggests that we may be able to work something out in the case $n = 5$– indeed, it appears that if we restrict augmentation to A_5, we may be able to express χ_α in terms of degree 1 and 2 characters. Indeed, this is the case, as we see in Chapter 4, although it will necessitate passing to the absolute Galois group of K, the quadratic subextension of $L|\mathbb{Q}$ corresponding to the sign representation on S_5. At the same time, the proof suggests this approach is fruitless for $n \geq 6$: the proof does not depend on the ground field being $\mathbb{Q}$ and shows that χ_α restricted to A_n is not in $R^{(2)}(G_K)$.

Despite this dead end for studying the polynomials f_n, $n \geq 6$, using this idea, some interesting questions do arise. For a profinite group G and a whole number k:

- Is there a nice characterization of the elements of $R^{(k)}(G)$?
- What is the minimum value k, if any, such that $R^{(k)}(G) = R(G)$?
- If G is the absolute Galois group over a field K, what happens when we add extra conditions? For example, if K is totally real and $k = 2$, we can stipulate that the generators be odd. In general, we can add conditions regarding, say, the conductors of the generators.

Returning to the problem of representing augmentation in terms of degree 1 and 2 representations for f_4 and f_5, it is easy enough to find *projective* representations of S_4 or A_5 that allows us to "factor" augmentation into degree 1 and 2 representations, but we must be able to lift these to actual linear representations on $G_\mathbb{Q}$ or G_K. Furthermore, to find the modular forms to which the degree 2 representations correspond, we must be able to explicitly construct these linear representations, which requires studying the fixed fields of the kernels of these representations. We now introduce the theory required to address the problem of lifting representations.

2.3 Galois Embedding Problems

Let K be any number field, L a finite Galois extension of K. In lifting projective representations of $G(L|K)$ to G_K, we will be concerned with the existence of a superextension $M|K$ of $L|K$ such that $G(M|K)$ has a particular group structure. This is an example of a Galois embedding problem.

Definition 2.3.1. Let:

- L and K be as above;
- $G = G(L|K)$, with $\pi : G_K \to G$ the natural projection; and
- G' a finite group with a homorphism $\phi : G' \to G$.

The corresponding *Galois embedding problem* is the question of determining the existence of a continuous homomorphism $\psi : G_K \to G'$ such that $\phi \circ \psi = \pi$. If such a ψ exists, it is a *solution* to the problem.

In our case, we want to find M such that $G' = G(M|K)$; thus, we assume that ϕ is surjective and require that ψ also be surjective. Our intuition is that G corresponds to a projective representation and G' gives a lifting of this to a linear representation. This implies that the kernel of the surjection $G' \twoheadrightarrow G$ is contained in the center of G'.

Definition 2.3.2. Let A be an abelian group, and suppose we have the exact sequence:

$$1 \to A \to G' \to G \to 1$$

where the image of A is in the center of G'. Then G' is a *central extension of* G *by* A.

Equipping A with the trivial G-action, we have that isomorphism classes of central extensions of G by A are in one-to-one correspondence with the cohomology group $H^2(G, A)$. In particular, note that a central extension corresponding to a coboundary is isomorphic to the direct product $G \times A$.

There is a natural map $\pi^* \colon H^2(G, A) \to H^2(G_K, A)$ given by:

$$\pi^*(x)(\sigma, \tau) = x(\pi(\sigma), \pi(\tau))$$

for all $\sigma, \tau \in G_K$. Let c be the cocycle corresponding to the extension G'. Then we have:

Lemma 2.3.1. *Let K, G, G', ϕ, G_K, and c be as above. Then the Galois embedding problem is solvable if and only if the image $\pi^*(c)$ of c in $H^2(G_K, A)$ is trivial.*

This is standard in the literature and is generally stated without proof. Artin and Tate give one in the cohomology section of [2], while we give our own proof in Appendix B.1.

2.3.1 Lifting Projective Galois Representations

We now explicitly describe the problem of lifting projective Galois representations to linear representations in terms of the framework of Galois embedding problems. Let $\bar{\rho} : G_K \to PGL_n(\mathbb{C})$ be a projective representation, and let $G = \mathbf{Im}(\bar{\rho})$. We want to answer two questions:

1. Under what circumstances does $\bar{\rho}$ lift to a linear representation $\rho : G_K \to GL_n(\mathbb{C})$?

2. What are the possibilities for the structure of the group $G' = \mathbf{Im}(\rho)$?

The first question has a surprisingly simple answer: all projective Galois representations lift to linear representations. This is an immediate consequence of the following result due to Tate ([28, Thm. 4, p. 232]).

Proposition 2.3.2. *Let K be a number field. Then $H^2(G_K, \mathbb{C}^\times) = 1$.*

This result implies the existence of the following commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{C}^\times \arrow[r] \arrow[d] & G_K \times \mathbb{C}^\times \arrow[r] \arrow[d] & G_K \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{C}^\times \arrow[r] & GL(n, \mathbb{C}) \arrow[r] & PGL(n, \mathbb{C}) \arrow[r] & 1
\end{tikzcd}$$

and we obtain $\rho : G_K \to GL(n, \mathbb{C})$ via the vertical arrow in the center.

With regard to the second question, note that the projection $GL_n(\mathbb{C}) \to PGL_n(\mathbb{C})$ induces a surjection $\phi : G' \to G$, and $A = \mathbf{ker}(\phi)$ is a cyclic group contained in the center of G'. So G' is a solution to the Galois embedding problem for G and A. We can then more or less determine the possibilities for G' by determining all central cyclic extensions of G and by explicitly describing the map $\pi^* : H^2(G, A) \to H^2(G_K, A)$. The former problem was studied extensively in Schur's work on projective representations, and the theory is known for the groups S_n and A_n, among others. The latter problem is addressed by Serre ([32, Ch. 9]) and Crespo ([9]), and Crespo develops explicit constructions in certain cases where the Galois embedding problem is solvable.

2.4 Solvability of Galois Embedding Problems with $G = S_n$ or A_n

2.4.1 Double Covers

Let K be a number field, L a finite extension, and $G = G(L|K)$. We are first interested in solving Galois embedding problems of the form:

$$1 \to C_2 \to G' \to G \to 1$$

where C_2 is the cyclic group of order 2, meaning G' is a double cover of G. When $G = S_4$ or A_5, there are well-known nontrivial solutions: $GL_2(\mathbb{F}_3)$ is a double cover of S_4, while $SL_2(\mathbb{F}_5)$ is a double cover of A_5. We show that augmentation can be represented in terms of degree 1 and 2 representations on these groups in the following chapter.

Consider a quadratic form f of rank n over K. We may assume that f is of the form:

$$f = \sum_{i=1}^{n} a_i X_i^2$$

as any form is K-equivalent to such a form. We form the cup-product in the cohomology ring $H^\bullet(G_K, C_2)$:

$$\bigcup_{i=1}^{n}(1 + (a_i)) = 1 + \sum_{j=1}^{n} w_i$$

where $w_i \in H^i(G_K, C_2)$. Here (a) is the class of $a \in K^\times$ under the isomorphism $K^\times/{K^\times}^2 \simeq H^1(G_K, C_2)$ provided by Kummer theory.

Definition 2.4.1. The ith graded term w_i is the *ith Stiefel-Whitney class* of f.

The Stiefel-Whitney classes are invariants of the form f. Furthermore, f is characterized up to K-equivalence by its rank, signature, and the first two Stiefel-Whitney classes $w_1 = (\mathrm{disc}(f))$ and w_2.

Now let E be an extension of K of degree n, and let $\rho : G_K \to S_n$ be the permutation representation of G_K acting on the roots of a degree n polynomial defining E over K. Let L be the Galois closure of E, so that we have an injection $G(L|K) \to S_n$. The map $E \to K$ given by $x \mapsto \mathrm{Tr}_{E|K}(x^2)$ is a nondegenerate form Q_E of rank n over K.

For $n \geq 4$, we have ([32, p. 97]):

$$\begin{aligned} H^1(S_n, C_2) &\simeq C_2 \\ H^2(S_n, C_2) &\simeq C_2 \oplus C_2 \end{aligned}$$

Since C_2 is a trivial S_n-module, $H^1(S_n, C_2) \simeq \mathrm{Hom}(S_n, C_2)$, the nontrivial element of which is the sign character sgn. Then $H^2(S_n, C_2)$, viewed as a vector space over $\mathbb{F}_2$ of dimension 2, has basis $\{\mathrm{sgn} \cup \mathrm{sgn}, s_n\}$, where s_n corresponds to the double cover $\tilde{S}_n$ of S_n characterized by the property that 2-cycles lift to elements of order 2 and products of two disjoint 2-cycles lift to elements of order 4. For the alternating groups, we have:

$$\begin{aligned} H^1(A_n, C_2) &\simeq 1 \\ H^2(A_n, C_2) &\simeq C_2 \end{aligned}$$

where the first group is trivial due to simplicity of A_n, and the second group has unique nontrivial element $a_n = \mathrm{Res}(s_n)$, the restriction of s_n to A_n.

Let $G = G(L|K)$ and let $\tilde{G}$ be the preimage of G in $\tilde{S}_n$. The central extension:

$$1 \to C_2 \to \tilde{G} \to G \to 1$$

then corresponds to $\mathrm{Res}(s_n) \in H^2(G, C_2)$. To determine whether the related Galois embedding problem is solvable, we must check whether the image $e^*(s_n)$ of $\mathrm{Res}(s_n)$ in $H^2(G_K, C_2)$ is trivial. To do this, we use:

Theorem 2.4.1 (Serre, [32, 9.2.2])**.** *Let K, E, n, and $e : G_K \to S_n$ be as above, Q_E be the trace form of E over K, and let d be the discriminant of Q_E. Then:*

1. $w_1(Q_E) = e^*\mathrm{sgn}$
2. $w_2(Q_E) = e^*s_n + (2) \cup (d)$

Combining this with Lemma 2.3.1, we have:

Corollary 2.4.2. *Let G be as above. Then the Galois embedding problem:*

$$1 \to C_2 \to \tilde{G} \to G \to 1$$

is solvable if and only if $w_2(Q_E) = (2) \cup (d)$ in $H^2(G_K, C_2)$.

We further note that if $e(G_K) \subset A_n$, the discriminant d is a square in K, and so $(d) = (1)$ in $H^1(G_K, C_2)$. This implies that $w_2(Q_E) = e^* s_n$, and we have:

Corollary 2.4.3 (Serre, [32, 9.2.3]). *If $G \subset A_n$, then the Galois embedding problem:*

$$1 \to C_2 \to \tilde{G} \to G(L|K) \to 1$$

is solvable if and only if $w_2(Q_E) = 1$ in $H^2(G_K, C_2)$.

Corollary 2.4.2 will show that we can lift the projective representations for the $n = 4$ case, namely that we can realize $GL_2(\mathbb{F}_3)$ as the Galois group of a central extension of $L|\mathbb{Q}$. However, Corollary 2.4.3 will show that $SL_2(\mathbb{F}_5)$ *cannot* be realized as the Galois group of a central extension of $L|K$, and we need to consider central extensions by larger cyclic groups.

2.4.2 Higher Order Covers of A_n

Since A_5 has an inclusion in $PGL_2(\mathbb{C})$, Tate's result implies that there must exist some central extension:

$$1 \to A \to G' \to A_5 \to 1$$

with A cyclic such that the corresponding Galois problem with $A_5 = G(L|K)$ is solvable. *A priori*, we do not know what A or G' are, so we describe *all* cyclic central extensions of A_n for any n.

For positive integers m, n, we have that:

$$H^2(A_n, C_m) = \begin{cases} 1 & \text{if } m \text{ is odd} \\ C_2 & \text{if } m \text{ is even} \end{cases}$$

Note that this implies all extensions with kernel of odd order are isomorphic to the direct product $A_n \times C_m$.

For even values of m, let mA_n denote the unique nontrivial extension of A_n with cyclic central kernel of order m. Writing $m = 2^r m'$, m' odd, we have an isomorphism:

$$mA_n \simeq 2^r A_n \times C_{m'}$$

Thus we can restrict our attention to extensions with kernel of order a power of 2. We note that for $r \leq s$, there is an embedding $2^r A_n \to 2^s A_n$.

The following result due to Crespo completely characterizes the solvability of the embedding problem $2^r A_n \to A_n$.

Proposition 2.4.4 (Crespo, [9, p. 71])**.** *Let $L|K$ be a Galois extension of number fields with $G(L|K) \simeq A_n$, $n \geq 4$. Then the embedding problem:*

$$1 \to C_{2^r} \to 2^r A_n \to G(L|K) \to 1 \quad (1)$$

is solvable if and only if there exists a Galois extension $K_1|K$ with $G(K_1|K) \simeq C_{2^{r-1}}$, $K_1 \cap L = K$, and such that the cocyles corresponding to the extensions:

$$1 \to C_2 \to C_{2^r} \to G(K_1|K) \to 1 \quad (2)$$

and:

$$1 \to C_2 \to 2A_n \to G(L|K) \to 1 \quad (3)$$

agree in $H^2(G_K, C_2)$.

The key to the proof of the proposition is to consider, instead of (1), the embedding problem:

$$1 \to C_2 \to 2^r A_n \to G(LK_1|K) \to 1 \quad (4)$$

Noting that $G(LK_1|K) \simeq A_n \times C_{2^{r-1}}$, (4) is solvable precisely when (1) is. The cocycle corresponding to (4) is simply the product of the cocycles corresponding to (2) and (3), so (4) is solvable if and only if the product of the cocycles is trivial in $H^2(G_K, C_2)$. Since this group has exponent 2, this is the same as the cocycles having the same image.

Chapter 3

The Quartic Case

3.1 Introduction

We study the roots of the polynomial $f(X) = f_4(X) = X^4 - X - 1$ modulo primes. We show that the augmentation representation α can be written in terms of characters of degree 1 and odd, degree 2 representations of $G_{\mathbb{Q}}$, and we attach modular forms to the latter. We use the results of Serre and Crespo from Chapter 2 to show the existence of the representations, while we follow methods due to Crespo ([6]) and Quer (unpublished but communicated in [9]) to explicitly construct the representations. The long-established modularity of octahedral representations immediately gives us the desired modular form, but we go a step further and answer a question of Serre's in [31] by giving an explicit formula for this form in terms of theta series of quaternion algebras.

We note that the suite of methods used by Crespo and Quer is only one of a few different approaches. We discuss and apply methods due to Buhler ([4]) in Chapter 5; these avoid explicit global constructions of the fixed field of the kernel of a linear representation. We also refer the reader to results by Jehanne ([16]), in which the fixed field of the kernel of a linear representation is explicitly constructed by producing a defining polynomial.

3.2 Notation

Letting f be the polynomial above, we let:

- E be a root field of f over $\mathbb{Q}$;

- L be the splitting field of f over $\mathbb{Q}$; and

- $K = \mathbb{Q}(\sqrt{-283})$, where -283 is the discriminant of f.

We note that:

- $G(L|\mathbb{Q}) \simeq S_4$;
- K is the fixed field of the image of A_4 in $G(L|\mathbb{Q})$; and
- L is unramified over K.[1]

3.3 Factoring Augmentation

There is a well-known double cover $GL_2(\mathbb{F}_3) \twoheadrightarrow S_4$. This can be realized explicitly by considering the transitive action of $GL_2(\mathbb{F}_3)$ on the projective line $\mathbb{P}^1(\mathbb{F}_3) = \{[1:0], [1:1], [1:2], [0:1]\}$. Thus, we can consider augmentation α and the sign character sgn as representations on $GL_2(\mathbb{F}_3)$. We note that sgn corresponds to the determinant ϵ on $GL_2(\mathbb{F}_3)$.

S_4 has five conjugacy classes, each corresponding to the disjoint cyclic decomposition of a permutation. Three can be determined by order alone–the classes of order 1, 3, and 4. There are also two classes of order 2, one containing the 2-cycles and the other consisting of the disjoint products of 2-cycles. We refer to these classes as **1** (1 element), **3** (8 elements), **4** (6 elements), **2A** (6 elements), and **2B** (3 elements), respectively.

$GL_2(\mathbb{F}_3)$ has 8 conjugacy classes. Letting:

$$z = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad a = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \quad b = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \quad c = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad d = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

then the conjugacy classes have representatives 1 (1 element, order 1), z (1 element, order 2), a (12 elements, order 2), b (6 elements, order 4), c (8 elements, order 3), zc (8 elements, order 6), d (6 elements, order 8), and zd (6 elements, order 8). Under the surjection $GL_2(\mathbf{F}_3) \twoheadrightarrow S_4$, 1 and z map to **1**; a to **2A**; b to **2B**; c and zc to **3**; and d and zd to **4**.

[1] More generally, we have that if $X^n - aX - b \in \mathbb{Z}[X]$ has discriminant D, and $(n-1)a$ are nb are relatively prime, then its splitting field is unramified over $\mathbb{Q}[\sqrt{D}]$ ([38]). This provides a more general but still relatively easy to work with family of polynomials to study than simply taking $a = b = 1$.

Although the theory of the representations of the general linear groups over finite fields is well-known and can be worked out by hand for small fields, we use MAGMA ([3]) to compute the irreducible character table of $GL_2(\mathbb{F}_3)$. We list the values of three characters–augmentation α, determinant ϵ, and a degree 2 irreducible representation θ–in the table below. (We exclude the classes zc and zd as the values can be readily by the values at z, c, and d.)

	1	z	a	b	c	d
α	3	3	1	-1	0	-1
ϵ	1	1	-1	1	1	-1
θ	2	-2	0	0	-1	$\sqrt{-2}$

It is clear from the table that $\alpha \oplus \epsilon \simeq \theta \otimes \theta$, which can be expressed by the equality of virtual characters:

$$\chi_\alpha = \chi_\theta^2 - \epsilon$$

If we can realize $GL_2(\mathbb{F}_3)$ as the Galois group of a Galois superextension M of $L|\mathbb{Q}$, then we have the desired factorization of α into degree 1 and odd degree 2 representations. Indeed, that θ is odd follows from the fact that, since $X^4 - X - 1$ has two real roots, complex conjugation in $G(L|\mathbb{Q})$ corresponds to **2A** in S_5. This, in turn, corresponds to the class of a in $GL_2(\mathbb{F}_3)$. As $\theta(a)$ has order 2 and trace 0, its characteristic polynomial must be $1 - t^2$, implying $\det(\theta(a)) = -1$. (Indeed, this shows that a degree 2 Galois representation is odd so long as complex conjugation does not map to ± 1.)

3.4 Lifting $\bar{\theta}$

The representation θ of $GL_2(\mathbb{F}_3)$ gives a projective Galois representation $\bar{\theta}$, and Tate's result that $H^2(G_{\mathbb{Q}}, \mathbb{C}^\times) = 1$ implies that some lifting exists. We would like to construct this explicitly. The existence of the desired lifting comes from the results of Serre and Crespo, while the explicit construction comes from techniques due to Crespo and Quer.

We first note that, since 2-cycles in S_4 lift to elements of order 2 and products of disjoint 2-cycles to elements of order 4 in $GL_2(\mathbb{F}_3)$, the central extension:

$$1 \to C_2 \to GL_2(\mathbb{F}_3) \to S_4 \to 1$$

corresponds to the cocycle $s_4 \in H^2(S_4, C_2)$. Thus, to determine whether $GL_2(\mathbb{F}_3)$ can be realized as the Galois group of a super extension of $L|\mathbb{Q}$, Corollary 2.4.2 states that we must check that $w(Q_E) = (2) \cup (d)$ in $H^2(G_{\mathbb{Q}}, C_2)$, where Q_E is the trace form of $E|\mathbb{Q}$ and d is its discriminant.

Letting u be a root of f in E, and using the basis $\{1, u, u^2, u^3\}$, the trace form has matrix:

$$\begin{bmatrix} 4 & 0 & 0 & 3 \\ 0 & 0 & 3 & 4 \\ 0 & 3 & 4 & 0 \\ 3 & 4 & 0 & 3 \end{bmatrix}$$

As $\{1, u, u^2, u^3\}$ forms an integral basis for $\mathfrak{o}_E$, the determinant of this matrix is the discriminant of E, so the discriminant of Q_E is $d = -283$. Q_E is equivalent over $\mathbb{Q}$ to the form corresponding to the diagonal matrix with entries $\{1, 1, -1, 283\}$, whence $w(Q_E) = (-1) \cup (283)$.

To determine whether $(-1) \cup (283) = (2) \cup (-283)$, we use the correspondence between $H^2(G_{\mathbb{Q}}, C_2)$ and quaternion algebras over $\mathbb{Q}$. Computations in MAGMA show that both of $(-1, 283)$ and $(2, -283)$ are ramified only 2 and 283, whence the desired identity of cocycles is verified. Thus, there is a quadratic extension M of L, Galois over $\mathbb{Q}$, such that $G(M|\mathbb{Q}) \simeq GL_2(\mathbb{F}_3)$. As such, we can view θ as a representation on $G_{\mathbb{Q}}$, and we obtain the desired expression of augmentation. Noting that the determinant character ϵ corresponds to the quadratic character χ_{-283} of discriminant -283, we have:

$$\alpha = \theta^2 - \chi_{-283}$$

Furthermore, we can compute χ_{-283} at Frobenius using the Kronecker symbol, $\chi_{-283}(\sigma_p) = (\frac{-283}{p})$. Thus, we have:

$$\chi_\alpha(\sigma_p) = \chi_\theta(\sigma_p)^2 - \left(\frac{-283}{p}\right)$$

This implies:

Proposition 3.4.1. *There exists an odd octahedral representation on $G_{\mathbb{Q}}$ of conductor* 283 *such that for any prime p, the number of roots of $X^4 - X - 1$ modulo p is equal to:*

$$\chi_\theta(\sigma_p)^2 - \left(\frac{-283}{p}\right) + 1$$

3.5 Explicit Construction of M and θ

A natural method for obtaining an explicit construction of θ is to find an element $\gamma \in L$ such that $M = L(\sqrt{\gamma})$ is a solution to the above embedding problem. Intuitively, we should be able to determine the trace of Frobenius at p by determining whether or not γ is a square modulo p.

3.5.1 Crespo's Formula

Until otherwise noted, we repurpose the notation developed above: K is a number field, $f(X) \in K[X]$ is a polynomial of degree n, E is a root field of f over K, L is the splitting field of f over K. In the case that $G(L|K) \simeq A_n$ and the Galois embedding problem for the double cover of A_n is soluble, Crespo develops formulas for constructing γ. This can then be modified suitably when A_n is replaced with S_n or when considering higher order covers of A_n.

To develop some intuition for Crespo's formula, we first state:

Proposition 3.5.1. *Let $\gamma \in L$ be such that $M = L(\sqrt{\gamma})$ is a solution to the Galois embedding problem $1 \to C_2 \to \tilde{A}_n \to A_n \to 1$.*

i. For any $\sigma \in G(L|K)$, there exists $b_\sigma \in L^\times$ such that $\gamma^{\sigma-1} = b_\sigma^2$, and the cocycle corresponding to the embedding problem is $c(\sigma, \tau) = b_\sigma^\tau b_\tau b_{\sigma\tau}^{-1}$.

ii. All solutions to the embedding problem are given by $k\ell^2\gamma$, $k \in K^\times$ and $\ell \in L^\times$.

These facts are stated without proof throughout the literature (e.g., [6, p. 453]), but we provide a proof in Appendix B.2.

We give a brief overview of the derivation of the formula in [6]. The formula is developed by considering Clifford algebras corresponding to various quadratic forms.

Definition 3.5.1. Let Q be a quadratic form on K^n. The *Clifford algebra $C(Q)$* is the free algebra generated over K^n subject to the relations:

$$\begin{aligned} v^2 &= Q(v) \\ vw + wv &= 2\langle v, w\rangle \end{aligned}$$

$\langle \cdot, \cdot \rangle$ being the bilinear form correspond to Q.

We note that $C(Q)$ is a central algebra over K.

The intuition is that we want to construct elements of a particular Clifford algebra that are analogs of the field elements b_σ and γ. The analogs of the b_σ are easy to construct due to a standard embedding of $\tilde{A}_n$, the double cover of A_n, in a group of units in a Clifford algebra, while Crespo constructs the analog of γ in the course of deriving the formula for γ.

$C(Q)$ is equipped with an automorphism α that is the extension of the map $v \mapsto -v$ on the quadratic space (K^n, Q). $C(Q)$ then decomposes into positive (even) and negative (odd) eigenspaces for α, $C(Q) = C^+(Q) \oplus C^-(Q)$, giving $C(Q)$ the structure of a $\mathbb{Z}/2\mathbb{Z}$-graded algebra. There also exists a unique antiautomorphism β such that the restriction of β to K^n is trivial. We then define the *spin norm* of $c \in C(Q)$ by $N(x) = \beta(x)x$.

We now let Q_1 be the standard quadratic form on K^n, and let Q_E be the quadratic form given by $x \mapsto Tr_{E|K}(x^2)$. Clearly, the $n \times n$ identity matrix I is the matrix corresponding to the bilinear form associated to Q_1. If:

$$M = [u_i^{(j)}], \quad 1 \leq i, j \leq n$$

where the u_i form a basis of E over K and $u_i^{(j)}$ are the embeddings of the u_i in L, then:

$$T = M^t M = [Tr_{E|K}(u_i u_j)], \quad 1 \leq i, j \leq n$$

is a matrix for the bilinear form corresponding to Q_E.

$\tilde{A}_n$ has an embedding in a group of units, the *spin group*:

$$\mathrm{Spin}_n(K) = \{a \in C^+(Q)^\times | a(K^n)a^{-1} \subset K^n, N(a) = 1\}$$

as described in [29, 2.3]. Letting x_σ, $\sigma \in A_n$, be a section, we have that for the standard basis e_i of K^n:

$$x_\sigma e_i x_\sigma^{-1} = e_{\sigma(i)}$$

Furthermore, we have the equality of cocycles:

$$c(\sigma, \tau) = x_\sigma x_\tau x_{\sigma\tau}^{-1}$$

where c is the cocycle corresponding to the embedding problem.

The matrix M^{-1} gives an isomorphism of quadratic spaces $f : L^n \to E \otimes_K L$, and this extends to an isomorphism $f : C_L(Q_1) \to C_L(Q_E)$, where $C_L(Q) = C(Q) \otimes_K L$. We then have:

$$f^{-1}f^{\sigma}(e_i) = e_{\sigma(i)}, \quad f^{\sigma}(x) = [f(x^{\sigma^{-1}})]^{\sigma}$$

Crespo proves that, if the embedding problem is solvable, then we also have an isomorphism $g : C(Q_1) \to C(Q_E)$ of $\mathbb{Z}/2\mathbb{Z}$-graded algebras.

Letting $v_i = f(e_i)$ and $w_i = g(e_i)$, we construct an element of $C_L^+(Q_E)$:

$$z = \sum_{\epsilon_i=0,1} v_1^{\epsilon_1} v_2^{\epsilon_2} \cdots v_n^{\epsilon_n} w_n^{\epsilon_n} \cdots w_2^{\epsilon_2} w_1^{\epsilon_1}$$

z satisfies the identities:

$$v_i z = z w_i$$

and, letting $y_\sigma = f(x_\sigma)$:

$$y_\sigma v_i y_\sigma^{-1} z^\sigma = v_{\sigma(i)} z^\sigma = z^\sigma w_i$$

Solvability of the embedding problem and the Skolem-Nöther theorem imply that z is invertible, so we can define:

$$b_\sigma = y_\sigma^{-1} z^\sigma z^{-1}$$

The two identities above imply that b_σ is a central element of $C_L(Q_E)$ and, hence, is in L. Furthermore, b_σ gives the same cocycle as y_σ^{-1}, i.e. the cocycle c corresponding to the embedding problem. Since since $N(y_\sigma) = 1$, we finally have ([6, Prop. 2]):

$$N(z)^\sigma = b_\sigma^s N(z)$$

We then let γ be a nonzero coordinate of $N(z)$ in terms of the basis $\{w_1^{\epsilon_1} \cdots w_n^{\epsilon_n}\}$ of $C_L(Q_E)$.

The simplest case of computing a coordinate of $N(z)$ occurs when Q_E and Q_1 are K-equivalent, as we can take g to be the extension of this equivalence:

Theorem 3.5.2 (Crespo, [6, Thm. 4])**.** *Suppose Q_E is K-equivalent to Q_1. Then there exists $P \in GL_n(K)$ such that:*

$$P^t T P = I, \quad \gamma = \det(MP + I) \neq 0$$

and $L(\sqrt{\gamma})$ is a solution to the embedding problem.

3.5.2 Ramification

We now study the ramification of the extension $M|L$. We begin with an obvious lemma:

Lemma 3.5.3. *Suppose that $L|K$ is a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K, M be a quadratic extension of L Galois over K, and P be a prime of L over $\mathfrak{p}$. Then P ramifies in M if and only if all primes in L lying over $\mathfrak{p}$ ramify.*

Proof. This follows immediately from the transitivity of the action of Galois on primes of M and L lying over a given prime in K. □

We can apply this lemma in a variety of ways. For example:

Corollary 3.5.4. *Let L, K, $\mathfrak{p}$, and M be as in the previous lemma. Suppose $L|K$ is unramified at $\mathfrak{p}$ and that $\mathfrak{p}$ does not divide 2. Furthermore, let $\gamma \in L$ be an integer such that $M = L(\sqrt{\gamma})$, and let $n = [L : K]$. If $N_{L|\mathbb{Q}}(\gamma)$ is not divisible by $N(\mathfrak{p})^n$, then $\mathfrak{p}$ is unramified in M.*

Proof. Suppose that $\mathfrak{p}$ is ramified in M. Then there exists a prime P of L lying over $\mathfrak{p}$ that ramifies in M, and hence all such P ramify in M. The discriminant of the order $\mathfrak{o}_L + \sqrt{\gamma}\mathfrak{o}_L$ of M is 4γ and is divisible by the $d_{M|L}$, and so γ must be divisible by all primes P lying over $\mathfrak{p}$. This implies that $N_{L|\mathbb{Q}}$ is divisible by:

$$\prod_{P|\mathfrak{p}} N(P) = N(\mathfrak{p})^{fr} = N(\mathfrak{p})^n$$

where r is the number of primes P lying over $\mathfrak{p}$ and f is the residue degree of P over $\mathfrak{p}$, and $n = fr$ due to the fact that $P|\mathfrak{p}$ is unramified. □

The situation at primes over 2 is similar to the classical case of quadratic fields over the rationals: even if the norm of γ is odd, ramification may still occur. The criterion for ramification at 2 in this case is essentially the same:

Lemma 3.5.5. *Let M, L, and γ be as above, and assume that 2 is unramified in L. Let P be a prime of L lying over 2 not dividing γ. Then P is unramified in M if and only if γ is a quadratic residue modulo P^2.*

Proof. Let P be a prime of L dividing 2, and suppose that $a+b\sqrt{\gamma} \in \mathfrak{o}_M$, $a, b \in L$. We first show a relationship between the valuations of a and b at P. We have $\mathrm{Tr}_{M|L_1} = 2a$, and so $2a \in \mathfrak{o}_L$ and $v_P(a) \geq -1$. Let Q be a prime lying over P in M. The ramification index e of Q over P is either 1 or 2; in any case, $v_Q(a) \geq -e$. This implies $v_Q(b\sqrt{\gamma}) \geq -e$, with equality holding if and only if $v_Q(a) = -e$. Furthermore, since P does not divide γ, this implies $v_Q(b) \geq -e$ with equality holding if and only if $v_Q(a) = -e$. Thus $v_P(a), v_P(b) \geq -1$, and equality in one case holds if and only if it holds in the other.

Next we show that P is unramified in M if and only if there exists some integer $a + b\sqrt{\gamma}$ with $v_P(a) = v_P(b) = -1$. Suppose some such integer exists. Then the discriminant of the order $\mathfrak{o}_L + (a+b\sqrt{\gamma})\mathfrak{o}_L$ is $4b^2\gamma$. Since 2 is unramified in L, $v_P(2) = 1$, and so $v_P(4b^2\gamma) = 2 \cdot v_P(2) + 2 \cdot v_P(b) = 0$, whence P is unramified in $M|L$.

Conversely, if P is unramified in $M|L$, then since the discriminant of $M|L$ is generated by the discriminants of free $\mathfrak{o}_L$-modules contained in $\mathfrak{o}_M$, there exist two integers $a + b\sqrt{\gamma}, c + d\sqrt{\gamma} \in \mathfrak{o}_M$ such that P does not divide:

$$\mathrm{disc}(\{a + b\sqrt{\gamma}, c + d\sqrt{\gamma}\}) = 4\gamma(ad - bc)^2$$

Since $v_P(\gamma) = 0$ and $v_P(4) = 2$, we must have $v_P(ad - bc) = -1$. This implies that some $x \in \{a, b, c, d\}$ satisfies $v_P(x) < 0$, which implies $v_P(x) = -1$. Without loss of generality, let $x = a$ or b. Then $v_P(a) = v_P(b) = -1$.

Finally, we show that γ is a quadratic residue modulo P^2 if and only if there exists an integer $a + b\sqrt{\gamma}$ with $v_P(a) = v_P(b) = -1$. Suppose γ satisfying the latter condition exists. Then $v_Q(ab^{-1} + \sqrt{\gamma}) = v_Q(ab^{-1} - \sqrt{\gamma}) \geq 1$ for each prime Q lying over P in M, and so:

$$v_P(a^2b^{-2} - \gamma) = v_P(N_{M|L}(ab^{-1} + \sqrt{\gamma})) \geq 2$$

Noting that $v_P(ab^{-1}) = 0$, this inequality implies that γ is a square modulo P^2.

Conversely, suppose there exists $x \in \mathfrak{o}_L$ such that $x^2 \equiv \gamma \pmod{P^2}$. Let Q be a prime of M lying over P. Then $v_Q(x - \sqrt{\gamma}) \geq 1$. For any $y \in P^{-1} \setminus P$, we have $v_Q(xy - y\sqrt{\gamma}) \geq 0$, $xy - y\sqrt{\gamma} \in \mathfrak{o}_M$, and $v_P(xy) = v_P(y) = -1$. □

3.5.3 Constructing M

We return to the case that $f(X) = X^4 - X - 1$, and we let $K = \mathbb{Q}(\sqrt{-283})$, E, and L be as before. We cannot immediately apply Crespo's formula to our case, as $G(L|\mathbb{Q}) \simeq S_4$. However, we can pass to the subextension $L|K$, as $G(L|K) \simeq A_4$. We can then find a solution $\gamma \in L$ to the embedding problem $\tilde{A_4} \twoheadrightarrow G(L|K)$. If this γ does not give a solution to the problem $\tilde{S_4} \twoheadrightarrow G(L|\mathbb{Q})$, we must be able to find an element $k \in K^\times$ such that $k\gamma$ does.

The choices for the matrices M and P, in addition to MAGMA code computing γ, can be found at `http://math.rutgers.edu/~jbryk/`. We obtain:

$$\begin{aligned}\gamma \quad = \quad & -\frac{376288}{283}wu_1^3u_2^2 - \frac{420195}{283}wu_1^3u_2 + \frac{607296}{283}wu_1^3 - \frac{420195}{566}wu_1^2u_2^2 + \frac{280130}{283}wu_1^2u_2 \\ & -\frac{376288}{283}wu_1^2 + \frac{186058}{283}wu_1u_2^2 - \frac{188144}{283}wu_1u_2 - \frac{1029577}{566}wu_1 + \frac{188144}{283}wu_2^2 \\ & -\frac{36320}{283}wu_2 - \frac{702411}{566}w - u_1^3u_2 - \frac{1}{2}u_1^2u_2^2 - 2u_1^2u_2 - 2u_1u_2^2 - \frac{1}{2}u_1 + u_2 - \frac{9}{2}\end{aligned}$$

This choice of γ is integral. Letting $\sigma \in G(L|\mathbb{Q}) \setminus G(L|K)$ be the automorphism corresponding to the odd permutation (34), we have that g^σ is obtained by replacing w with $-w$, and we verify through MAGMA that $g^{\sigma-1}$ is a square in L. Thus, γ actually gives a solution to the embedding problem over $\mathbb{Q}$, and we take $M = L(\sqrt{\gamma})$.

To determine the ramification of $M|L$, we first compute the norm of γ:

$$N_{L|\mathbb{Q}}(\gamma) = 298{,}240{,}394{,}342{,}618{,}798{,}292{,}560{,}073{,}938{,}406{,}494{,}450{,}235{,}324{,}398{,}960{,}851^2$$

(That the norm is a square is no surprise; since $\gamma^{\sigma-1}$ is a square, the product of any two–and hence any even number–of conjugates of γ is a square.) Corollary 3.5.4 states that if an odd prime $p \neq 283$ ramifies in $M|\mathbb{Q}$, then p^{24} divides $N_{L|\mathbb{Q}}(\gamma)$, which implies that:

$$p \leq (N_{L|\mathbb{Q}}(\gamma))^{1/24} < 28{,}590$$

It is trivial to check that no primes less than 28,590 divide the norm of γ and, hence, $M|L$ is unramified outside of primes over 2 (including 283).

A prime P over 2 is given by an embedding of L into F, the degree 4 unramified extension of $\mathbb{Q}_2$. Since the Galois group of $L|\mathbb{Q}$ is S_4, any identification of $u_1, \ldots, u_4$

with the roots of f in F gives a valid embedding. Noting that our choice of the matrix M gives $\det(M) = -w$, the image of w is then determined as the negative of the determinant of the image of the matrix M in $\mathrm{Mat}_4(F)$.

We let u denote the image of u_1 in F. To get rid of 2 in the denominator in the expression of γ to make computations easier, we let $w = 2w_0 + 1$. We define a prime P by the embedding (modulo 4):

$$\begin{aligned} u_2 &\mapsto 2u^2 + u + 1 \\ u_3 &\mapsto u^2 + 2u \\ u_4 &\mapsto u^2 - 1 \\ w_0 &\mapsto 2u^3 + u^2 + u - 1 \end{aligned}$$

Then $\gamma \mapsto u^3 + 2u^2 - u \equiv (u^3 + u^2 + u - 1)^2 \pmod{P^2}$, whence Lemma 3.5.5 implies that $M|L$ is unramified.

3.5.4 Constructing θ

To construct θ–that is to say, to find the local factors of the Artin L-function of θ–we need to find the determinant and trace at Frobenius. It is obvious that $\det(\theta)$ is the quadratic character χ_{-283}, and, again, we can compute $\theta(\sigma_p) = (\frac{-283}{p})$. Alternately, we can view the character as the sign character on $S_4 = G(L|\mathbb{Q})$, so we can compute it by considering the disjoint cyclic decomposition of σ_p in this group.

To determine the trace at Frobenius, we first factor $X^4 - X - 1$ modulo p.[2] This gives the class in $G(L|\mathbb{Q})$, as the degrees of the irreducible factors correspond to the lengths of cycles in the disjoint cyclic decomposition of σ_p. This immediately determines the local factors when σ_p is in **2A** or **2B**, as there is only one class in $G(M|\mathbb{Q})$ lying above each of these classes.

[2] This may seem to defeat the purpose of introducing representation theory. Indeed, our original problem is to count the number of roots of a polynomial modulo primes, while computing the trace at Frobenius requires we go beyond this and completely factor the polynomial. However, we need only do this for sufficiently many primes to identify the modular form that corresponds to the representation. Once this is accomplished, methods of computing coefficients of modular forms can then be applied to compute traces at Frobenius.

If σ_p is in **1** or **3**, then σ_p is in one of two classes in $G(M|\mathbb{Q})$. One class has the same order as the class in $G(L|\mathbb{Q})$, while the other has twice the order. The former occurs when γ is a square modulo a prime P of L lying over p, while the latter occurs otherwise.

The same analysis cannot be used in the case that σ_p is in **4**, as both of the corresponding classes in $G(M|\mathbb{Q})$ have order 8. Instead, we have to explicitly determine the action of σ_p on $\sqrt{\gamma}$–namely, determining which sign holds in the equality $b_{\sigma_p} = \pm(\sqrt{\gamma})^{\sigma_p - 1}$. Checking this modulo a prime P of L lying over odd p amounts to checking the congruence:

$$b_{\sigma_p} \equiv \pm\gamma^{\frac{p-1}{2}} \pmod{P}$$

Letting $\tau = (123) \in S_4$, an explicit computation in the Clifford algebra gives the equality ([9, p. 79]):

$$b_{\sigma_p} = -\frac{1}{2} + \frac{\gamma^{\tau^{-1}} - \gamma^{\tau}}{2\gamma}$$

The last difficulty in computing the trace at Frobenius is at the prime 2, over which $X^4 - X - 1$ is irreducible and, hence, σ_2 is in **4**. However, since we know θ is modular, we can consider both possibilities for the local factor at 2 and then determine which is correct by seeing which candidate actually corresponds to a modular form.

Finally, we compute the conductor of θ using the formula in Appendix A. We compute using MAGMA that, for a prime Q in M lying over 283, I_Q is generated by a 2-cycle, while $G_{Q,s}$ is trivial for $s \geq 1$. Furthermore, if V underlying vector space for θ, V^{I_Q} has dimension 1, as a 2-cycle maps to a matrix with minimal polynomial $X^2 - 1$; and, clearly, $V^{G_{Q,s}} = 0$ for $s \geq 1$. Thus the formula gives $f_Q(\chi_\theta) = 1$ and $\mathfrak{f}(\chi_\theta) = 283$.

3.6 Modular Forms

As ρ is an odd octahedral representation of conductor 283 and character χ_{-283}, it corresponds to a newform $f_{-283} \in S_1(283, \chi_{-283})$. Thus, if:

$$f = \sum_{n=1}^{\infty} a_n q^n$$

we have:

$$\chi_\theta(\sigma_p) = a_p$$

And so we immediately obtain.

Corollary 3.6.1. *There exists a newform $f_{-283} \in S_1(283, \chi_{-283})$ with Fourier coefficients $a_n \in \mathbb{Z}[\sqrt{-2}]$ such that for any prime p, the number of roots of $X^4 - X - 1$ modulo p is equal to:*

$$a_p^2 - \left(\frac{-283}{p}\right) + 1$$

Serre gives an explicit expression for f_{-283} modulo 283 ([31, pp. 438–439]); we go one step further and obtain a closed formula. We consider form $f_{-283}^2 \in M_2(283)$, which has dimension 24 and is spanned by theta series coming from the quaternion algebra $(-1, -283)$ according to the Jacquet-Langlands correspondence. Using algorithms developed by Pizer and implemented in Pari-GP ([36]) by Rodriguez-Villegas and Pacetti ([40]), we find a maximal order B such that the theta series of the quadratic forms corresponding to the 24 left ideal classes of B are linear independent. We can take B to have $\mathbb{Z}$-basis $\{1, 3i, \frac{1}{2} + \frac{1}{6}i + \frac{1}{6}j + \frac{1}{6}k, \frac{1}{2}i - \frac{1}{2}k\}$. We only need 19 of the ideal classes, with representatives given by the $\mathbb{Z}$-bases:

1. $\{-3, -\frac{17}{6}i + \frac{1}{6}j + \frac{1}{6}ij + \frac{1}{2}, -\frac{2}{3}i - \frac{1}{6}j + \frac{1}{3}ij + \frac{3}{2}, \frac{37}{6}i + \frac{1}{6}j + \frac{1}{6}ij + \frac{1}{2}\}$
2. $\{\frac{17}{6}i - \frac{1}{6}j - \frac{1}{6}ij - \frac{7}{2}, \frac{17}{6}i - \frac{1}{6}j - \frac{1}{6}ij + \frac{11}{2}, -\frac{41}{6}i - \frac{1}{3}j + \frac{1}{6}ij - 2, -\frac{23}{3}i + \frac{1}{3}j - \frac{2}{3}ij - 3\}$
3. $\{-2, \frac{1}{6}i + \frac{1}{6}j + \frac{1}{6}ij - \frac{1}{2}, -\frac{2}{3}i - \frac{1}{6}j + \frac{1}{3}ij - \frac{1}{2}, 6i\}$
4. $\{3, -\frac{1}{6}i - \frac{1}{6}j - \frac{1}{6}ij - \frac{3}{2}, \frac{13}{6}i - \frac{1}{3}j + \frac{1}{6}ij - 1, -\frac{20}{3}i - \frac{1}{6}j + \frac{1}{3}ij + \frac{1}{2}\}$
5. $\{-4, \frac{5}{6}i + \frac{1}{3}j - \frac{1}{6}ij + 2, \frac{35}{6}i - \frac{1}{6}j - \frac{1}{6}ij - \frac{3}{2}, \frac{37}{6}i + \frac{1}{6}j + \frac{1}{6}ij + \frac{3}{2}\}$
6. $\{-5, \frac{17}{6}i - \frac{1}{6}j - \frac{1}{6}ij + \frac{5}{2}, \frac{7}{3}i - \frac{1}{6}j + \frac{1}{3}ij + \frac{1}{2}, -7i - \frac{1}{2}j + \frac{1}{2}\}$
7. $\{-\frac{31}{6}i + \frac{1}{3}j - \frac{1}{6}ij + 2, -\frac{1}{2}i + \frac{1}{2}ij + 3, 10, -7i - \frac{1}{2}j + \frac{1}{2}\}$
8. $\{-6, 6i, -\frac{1}{2}i + \frac{1}{2}ij + 1, -i - \frac{1}{2}j + \frac{5}{2}\}$
9. $\{-\frac{5}{6}i - \frac{1}{3}j + \frac{1}{6}ij - 3, -7, \frac{37}{6}i + \frac{1}{6}j + \frac{1}{6}ij + \frac{3}{2}, \frac{10}{3}i - \frac{1}{6}j - \frac{2}{3}ij - \frac{3}{2}\}$
10. $\{-\frac{31}{6}i + \frac{1}{3}j - \frac{1}{6}ij, -\frac{7}{2}i + \frac{1}{2}ij + 4, -11, 7i + \frac{1}{2}j - \frac{7}{2}\}$
11. $\{-3, \frac{17}{6}i - \frac{1}{6}j - \frac{1}{6}ij + \frac{1}{2}, \frac{7}{3}i - \frac{1}{6}j + \frac{1}{3}ij - \frac{1}{2}, -\frac{37}{6}i - \frac{1}{6}j - \frac{1}{6}ij + \frac{1}{2}\}$

12. $\{-\frac{1}{6}i - \frac{1}{6}j - \frac{1}{6}ij + \frac{1}{2}, 4, -\frac{2}{3}i - \frac{1}{6}j + \frac{1}{3}ij - \frac{1}{2}, 12i\}$

13. $\{-6, -\frac{2}{3}i - \frac{1}{6}j + \frac{1}{3}ij + \frac{3}{2}, \frac{37}{6}i + \frac{1}{6}j + \frac{1}{6}ij - \frac{5}{2}, -\frac{17}{3}i + \frac{1}{3}j + \frac{1}{3}ij + 1\}$

14. $\{-\frac{2}{3}i - \frac{1}{6}j + \frac{1}{3}ij - \frac{9}{2}, \frac{2}{3}i + \frac{1}{6}j - \frac{1}{3}ij - \frac{15}{2}, \frac{7}{6}i + \frac{2}{3}j + \frac{1}{6}ij + 3, \frac{71}{6}i - \frac{1}{6}j - \frac{1}{6}ij - \frac{7}{2}\}$

15. $\{-\frac{10}{3}i - \frac{1}{3}j - \frac{1}{3}ij - 1, -\frac{29}{3}i - \frac{1}{6}j + \frac{1}{3}ij + \frac{3}{2}, -\frac{3}{2}i + \frac{1}{2}j - \frac{1}{2}ij - \frac{5}{2}, 15\}$

16. $\{-\frac{20}{3}i - \frac{1}{6}j + \frac{1}{3}ij - \frac{1}{2}, \frac{19}{3}i + \frac{1}{3}j + \frac{1}{3}ij + 3, -\frac{9}{2}i + \frac{1}{2}j - \frac{1}{2}ij + \frac{5}{2}, 14\}$

17. $\{\frac{17}{6}i - \frac{1}{6}j - \frac{1}{6}ij - \frac{3}{2}, \frac{17}{6}i - \frac{1}{6}j - \frac{1}{6}ij + \frac{23}{2}, -\frac{5}{3}i + \frac{1}{3}j - \frac{2}{3}ij + 3, -13i - \frac{1}{2}j - \frac{9}{2}\}$

18. $\{6i + 6, -5i + \frac{1}{2}j + \frac{7}{2}, 7i + \frac{1}{2}j - \frac{5}{2}, -\frac{3}{2}i + \frac{3}{2}ij + 3\}$

19. $\{-i - \frac{1}{2}j + \frac{1}{2}, \frac{1}{2}i - \frac{1}{2}ij + 1, 24, -\frac{139}{6}i + \frac{1}{3}j - \frac{1}{6}ij\}$

Then f_{-283}^2 is represented in terms of the corresponding theta series by the vector $[-\frac{3}{2}+i\sqrt{2}, -\frac{3}{2}-i\sqrt{2}, -\frac{3}{2}, 4, \frac{3}{2}, -\frac{1}{2}, 1+i\sqrt{2}, -1, \frac{3}{2}, 1-i\sqrt{2}, -\frac{1}{2}, -\frac{3}{2}, -\frac{1}{2}, -\frac{1}{2}, 2, -5, 2, 2, -1]$. This data can also be found at `http://math.rutgers.edu/~jbryk/4theta.txt`.

Serre also asks what the coefficient of q^{283} is in f_{-283}. Using the above representation, we find q^{283} has coefficient 1.

Chapter 4

The Quintic Case: Factoring Augmentation

4.1 Introduction

We now consider the problem of finding the number of roots of the polynomial $f(X) = f_5(X) = X^5 - X - 1$ modulo primes. We follow the same general strategy as in the quartic case:

1. We "factor" augmentation α into projective representations of a Galois group.
2. We lift these to linear representations.
3. We explicitly construct the fixed field of the kernel of these representations to compute traces at Frobenius.
4. We find the modular forms attached to these representations.

Although we have already stated in the exposition that the Galois group we will consider is $G(L|K) \simeq A_5$, where L is the splitting field of f over $\mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2869})$ is the quadratic subextension of $L|\mathbb{Q}$, and, as such, we will attach the representations to Hilbert modular forms, it is worth considering what other strategies we could have taken. The main alternative to factoring augmentation to work with degree 2 representations and Hilbert modular forms is to use Siegel modular forms. The augmentation representation α may correspond to a Siegel modular form of degree 2. However, algorithms for computing Siegel forms are not as well-developed as those for Hilbert forms. For example, MAGMA has a whole suite of commands related to Hilbert forms but nothing devoted to Siegel forms.

4.2 Notation and Basic Facts

Letting f be as above, we let:

- E be a root field of f over $\mathbb{Q}$;
- L be the splitting field of $f(X)$ over $\mathbb{Q}$; and
- $K = \mathbb{Q}(\sqrt{2869})$, where $2869 = 19 \cdot 151$ is the discriminant of f;
- K has class number $h = 1$ and narrow class number $h^+ = 2$ (or, equivalently, there exists a totally positive fundamental unit of K); and
- L is unramified over K.

We note that:

- $G(L|\mathbb{Q}) \simeq S_5$;
- K is the fixed field of the image of A_5 in $G(L|\mathbb{Q})$.

4.3 Factoring Augmentation

As we cannot factor augmentation as a representation on $G_{\mathbb{Q}}$, we instead attempt to factor it over G_K. We start with the well-known double cover $SL_2(\mathbb{F}_5) \twoheadrightarrow A_5$. The simplest realization of such seems to be the action of $SL_2(\mathbb{F}_5)$ on the conjugacy class of its 2-Sylow subgroups, which are isomorphic to the quaternion group Q_8. Indeed, the matrices:

$$i = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}, \quad j = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}, \quad k = ij$$

satisfy the usual quaternion identities and, thus, generate such a subgroup. As such, we can consider augmentation to be a representation on $SL_2(\mathbb{F}_5)$.

A_5 has five conjugacy classes. Three are determined by the disjoint cyclic decomposition of a permutation–the identity, the disjoint products of 2-cycles, and the 3-cycles. There are also two classes of 5-cycles. We denote these classes as **1** (1 element), **2** (15 elements), **3** (20 elements), and **5A** and **5B** (12 elements each).

There are 9 conjugacy classes in $SL_2(\mathbb{F}_5)$. Letting:

$$z = \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}, \quad a = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}, \quad b = \begin{bmatrix} 1 & 4 \\ 1 & 0 \end{bmatrix}, \quad c = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

then the conjugacy classes have representatives: 1 (1 elements, order 1); z (1 element, order 2); a (30 elements, order 4); b (20 elements, order 6); b^2 (20 elements, order 3); c and c^2 (12 elements each, order 5); and zc and zc^2 (12 elements each, order 10). Under the surjection $SL_2(\mathbb{F}_5) \twoheadrightarrow A_5$: 1 and z map to **1**; a to **2**; b and b^2 to **3**; c and zc to **5A**; and c^2 and zc^2 to **5B**.

Again, the representation theory of special linear groups of finite fields is well-known, but we refer to MAGMA to find the character table for $SL_2(\mathbb{F}_5)$. We list the value of three characters–augmentation α and two degree 2 irreducible representations η_i–in the following table.

	1	z	a	b^m	c	c^2
α	4	4	0	1	-1	-1
η_1	2	-2	0	$(-1)^{m+1}$	$\frac{1}{2}(-1+\sqrt{5})$	$\frac{1}{2}(-1-\sqrt{5})$
η_2	2	-2	0	$(-1)^{m+1}$	$\frac{1}{2}(-1-\sqrt{5})$	$\frac{1}{2}(-1+\sqrt{5})$

From the above table, it is immediate that $\alpha \simeq \eta_1 \otimes \eta_2$. This is the desired factorization of α into projective representations. Due to Tate's result, we immediately know that there are linear representations θ_i on G_K such that $\bar{\theta}_i = \bar{\eta}_i$ as representations on $G(L|K)$. $\theta_1 \otimes \theta_2$ gives the same projective representation as α, and so $\theta_1 \otimes \theta_2 = \alpha \otimes \chi$ for some character χ on G_K. Replacing θ_1 by $\theta_1 \otimes \bar{\chi}$, we see that there exist θ_i such that $\theta_1 \otimes \theta_2 = \alpha$.

4.4 Lifting $\bar{\theta}_i$

We follow the same approach as in the quartic case, and we first consider whether there exists a quadratic extension $M|L$ Galois over K such that $G(M|K) \simeq SL_2(\mathbb{F}_5)$. We note that $SL_2(\mathbb{F}_5)$ has no nontrivial degree 1 representations. Thus the determinant of the representation η_i must be identically 1. In particular, this implies that if η_i is a Galois representation, it is not odd. Furthermore, the parity of any two liftings of a projective representation of G_K must be the same. Thus, if we find a number field M as above, we cannot express the trace at Frobenius of α in terms of holomorphic Hilbert modular forms.

To determine whether such an M exists, we use Serre's results on the solvability of the Galois extension problem:

$$1 \to C_2 \to \tilde{A}_5 \to G(L|K) \to 1$$

In the alternating case, Corollary 2.4.3 states we must determine whether $w(Q_E)$ is trivial, where Q_E is the trace form of $E|K$. Letting x be a root of f in E and using the basis $\{1, x, x^2, x^3, x^4\}$, the matrix associated to the trace form Q_E is:

$$\begin{bmatrix} 5 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 4 & 5 \\ 0 & 0 & 4 & 5 & 0 \\ 0 & 4 & 5 & 0 & 0 \\ 4 & 5 & 0 & 0 & 4 \end{bmatrix}$$

We can diagonalize the form to have the diagonal matrix with entries $\{1, 1, 1, -1, -1\}$, whence $w(Q_E) = (-1) \cup (-1)$. This corresponds to the quaternion algebra $(-1, -1)$ over K. Since K is totally real, $(-1, -1) \otimes_K \mathbb{R} = \mathbb{H}$, the Hamiltonian quaternions, and so $(-1, -1)$ is ramified at the infinite places and is, in particular, nontrivial in $H^2(G_K, C_2)$. (We note that, since $(-1, -1)$ ramifies at an even number of places, and since 2 is inert in K, we must have that $(-1, -1)$ as an algebra over K is split at 2, i.e. it is only ramified at the real places.) This implies that the Galois extension problem:

$$1 \to C_2 \to \tilde{A}_5 \to G(L|K) \to 1$$

is not solvable.

We now apply Proposition 2.4.4, which deals with higher order covers of A_n. We would like to find a Galois extension $K_1|K$ such that $K_1 \cap L = K$, $G(K_1|K)$ is cyclic of order 2^k for some k, and the cocycle c corresponding to the extension $C_{2^{k+1}} \to G(K_1|K)$ is equal to $(-1, -1)$ in $H^2(G_K, C_2)$. (The condition $K_1 \cap L = K$ is automatic, since $K_1 \cap L|K$ is a strict Galois subextension of $L|K$, while simplicity of $A_5 \simeq G(L|K)$

implies that there are no Galois extension of K lying properly between K and L.) It suffices to let $k = 2$.

The following lemma is well-known, but we give a shorter proof than we have found in the literature (e.g., [7, pp. 625–626]).

Lemma 4.4.1. *Let K be a number field, and let $K_1 = K(\sqrt{a})$ for some $a \in K^\times \setminus K^{\times 2}$. Let $c \in H^2(G(K_1|K), C_2)$ correspond to the extension $C_4 \to G(K_1|K)$. Then the image of c in $H^2(G_K, C_2)$ is $(-1, a)$.*

Proof. Let x be the image of c in $H^2(G_K, C_2)$. Then $x(\sigma, \tau) \neq 1$ iff $\sigma, \tau \notin G_{K_1}$. Since $(a) \in H^1(G_K, C_2)$ can be represented by the projection $G_K \to G(K_1|K) \simeq C_2$, it is clear that $(a, a) = (a) \cup (a) = x$. Since $(-a, a) = 1$, we have:

$$x = (a, a) = (a, a) \cdot (-a, a) = (-a^2, a) = (-1, a)$$

□

Taking $a = -1$, the Lemma 4.4.1 and Proposition 2.4.4 immediately imply that the Galois embedding problem is solvable for $k = 2$. However, we will not use the field $K_1 = K(\sqrt{-1})$ for our calculations. We wish to make the conductors of the liftings θ_i as small as possible. We are already in good shape due to the fact that $L|K$ is unramified, but this choice of K_1 introduces ramification at 2.

We consider another choice. K has a totally positive fundamental unit ϵ. Explicitly, we have:

$$\epsilon = 191619922383199 + 3577464936120\sqrt{2869}$$

Note that $\epsilon \equiv 3 \pmod 4$. Thus if we take $K_1 = K(\sqrt{-\epsilon})$, i.e. we adjoin the square root of the *totally negative* fundamental unit $-\epsilon$, we have $K_1|K$ is unramified at all finite primes due to Lemma 3.5.5 and to the fact that $-\epsilon$ is a square modulo 4. It is also clear that K_1 has no real embeddings. This information, combined with the fact that $h_K^+ = 2$, implies that K_1 is the narrow Hilbert class field of K. It is sometimes useful in our computations to note that $K_1 = K(\sqrt{-19}) = K(\sqrt{-151})$: the latter two fields are clearly equal, and so they must be unramified at all finite places, since they can be generated by roots of monic integral polynomials with relatively prime discriminants. Thus they must be contained in K_1 and, due to degree considerations, must be equal.

Now we show that $(-1,-\epsilon) = (-1,-1)$. We can use MAGMA to do the computations, but they are easy enough to do by hand that we proceed in this direction. Recall from above that $(-1,-1)$ is ramified only at the infinite place. We show the same holds true for $(-1,-\epsilon)$. That $(-1,-\epsilon)$ is ramified at the real places is immediate because $-\epsilon$ is totally negative and because an quaternion algebra (a,b) over the real numbers is isomorphic to $\mathbb{H}$ precisely when a and b are both negative. To determine which other primes can ramify, we construct an order in $(-1,-\epsilon)$ and compute its discriminant. Let $1, i, j, ij$ be a basis for $(-1,-\epsilon)$ such that $i^2 = -1$, $j^2 = -\epsilon$, and $ij = -ji$. Then $B = \mathbb{Z}+i\mathbb{Z}+j\mathbb{Z}+ij\mathbb{Z}$ is an order in $(-1,-\epsilon)$. The discriminant d of B can be calculated as the ideal generated by the determinant of the matrix of traces of products of basis elements for B. We have $d = -16\epsilon^3\mathfrak{o}_K = 16\mathfrak{o}_K$, and so the only finite prime at which $(-1,-\epsilon)$ can ramify is 2. As before, the parity condition implies that 2 is unramified, so $(-1,-\epsilon) = (-1,-1)$.

We summarize our findings:

Proposition 4.4.2. *Let $K = \mathbb{Q}(\sqrt{2869})$, $K_1 = K(\sqrt{-19})$ be its narrow Hilbert class field, and L the splitting field of the polynomial $f(X) = X^5 - X - 1$ over K. Then $L \cap K_1 = K$, and there exists a Galois extension M of K such that:*

1. *$G(M|K) \simeq 4A_5$; and*

2. *$L_1 = L \cdot K_1$ is the fixed field of $C_2 \subset 4A_5$ and is unramified over K.*

We find it useful to have a picture of the lattice of Galois subextensions of $M|K$:

$$\begin{tikzcd}
 & M & \\
 & L_1 \arrow[u, dash] \arrow[dr, dash] \arrow[ddl, dash] & \\
 & & L \\
K_1 & & \\
 & K \arrow[ul, dash] \arrow[uur, dash] &
\end{tikzcd}$$

4.5 Formula for the Number of Roots of $f(X)$ Modulo Primes

The irreducible representations of $2^r A_n$ can be readily deduced from those of $2A_n = \tilde{A}_n$.

Lemma 4.5.1. *There is a one-to-one correspondence between the irreducible representations ρ of $2^r A_n$ and the pairs (ρ', χ) of representations ρ' of $2A_n$ and characters χ on C_{2^r} satisfying $\rho'(z) = \chi(z) I_2$, where I_2 is the 2×2 identity matrix.*

This statement is fairly obvious; we give a proof in Appendix B.3.

Notes. 1. For any irreducible representation ρ' of $2A_5$, there are 2^{r-1} irreducible representations of $2^r A_5$ that restrict down to ρ'.

2. The projective representation attached to an irreducible representation ρ of $2^r A_n$ is determined by the restriction ρ' to $2A_n$: any two representations restricting down to ρ' differ by a character of $2^r A_n$ (necessarily trivial on $2A_n$). In fact, the image of $\bar{\rho}$ in $PGL(m, \mathbb{C})$ is the same as that of $\bar{\rho'}$.

3. In the case of $n = 5$, there is a nice description of $2^r A_5$ in terms of matrices. We now let ζ denote a 2^r-th root of unity in $\overline{\mathbb{F}}_5^{\times}$. We can then realize $2^r A_5$ as the subgroup of $GL_2(\overline{\mathbb{F}}_5)$ generated by the scalar matrix ζI_2 and $SL_2(\mathbb{F}_5)$.

We now apply this to our case. The representations $\eta_i : SL_2(\mathbb{F}_5) \simeq 2A_5 \to GL_2(\mathbb{C})$ both satisfy $\eta_i(z) = -I_2$. The characters $\chi : C_4 \to \mathbb{C}^{\times}$ satisfying $\chi(z) = -1$ must satisfy $\chi(\zeta) = \pm i$. Let χ_1 satisfy $\chi_1(\zeta) = i$ and χ_2 satisfy $\chi_2(\zeta) = -i$, and let θ_i be the irreducible representation of $4A_5$ determined by η_i and χ_i. It is then clear that $\theta_1 \otimes \theta_2 \simeq \alpha$. We note that this gives us two choices for the θ_i, and so there are four representations θ on $4A_5$ that restrict down to one of the η_i. Furthermore, given that the η_i are conjugate over $\mathbb{Q}(\sqrt{5})$, the four representations θ are conjugate over $\mathbb{Q}(\sqrt{5}, \sqrt{-1})$.

To determine the parity of the θ_i, we note that $G(M|K_1)$ corresponds to the subgroup $2A_5$ in $4A_5$. Thus ζ is a representative of complex conjugation. Since $\det(\theta_i(\zeta)) = \chi_i(\zeta)^2 = -1$, the θ_i are odd.

If we were trying to count the number of roots of $f(X)$ modulo primes in K, we would have our formula: given our discussions and calculations so far, we have the number of roots of $f(X)$ modulo a prime π of K is equal to:

$$\chi_{\theta_1}(\sigma_\pi)\chi_{\theta_2}(\sigma_\pi) + 1 \quad (*)$$

However, we are interested in what happens over $\mathbb{Q}$. The rule giving the number of roots modulo a prime p depends on whether p is inert or splits in K. One case is simple: if p splits in K as $\pi \cdot \pi'$, then $\mathbb{Z}/(p) \simeq \mathfrak{o}_K/(\pi)$, so the number of roots is given by $(*)$. Note that $\sigma_p = \sigma_\pi$ in this case.

However, if p is inert in K, then $\mathfrak{o}_k/(p)$ is a degree 2 extension of $\mathbb{Z}/(p)$. Let σ_p be the Frobenius at p as a prime in $\mathbb{Q}$ and σ'_p be the Frobenius at p as a prime in K. Then $\sigma'_p = \sigma_p^2$. Since p is inert, σ_p is not in the kernel of the quadratic character modulo 2869 associated to $K|\mathbb{Q}$. As K is the fixed field of the sign character on $S_5 \simeq G(L|\mathbb{Q})$, σ_p is an odd permutation viewed as an element of S_5. We further break things down and consider a few cases:

1. If σ_p is a 2-cycle, then $f(X)$ has 3 roots modulo p and $\sigma'_p = 1$.
2. If σ_p is the disjoint product of a 2-cycle and a 3-cycle, then $f(X)$ has no roots modulo p and σ'_p is a 3-cycle.
3. If σ_p is a 4-cycle, then $f(X)$ has one root modulo p and σ'_p is the product of two disjoint 2-cycles.

Analyzing this information, we note that $(*)$ overcounts the number of roots for cases σ'_p in **1** and **2** while giving the correct value for σ'_p in **3**. If instead we modify the formula to:

$$\chi_{\theta_1}(\sigma_\pi)\chi_{\theta_2}(\sigma_\pi) + \left(\frac{2869}{p}\right) \quad (**)$$

where π is a prime of K lying over p, then $(**)$ gives the correct value for all cases except for the third case when p is inert. In this case, the formula gives -1 while the correct number of roots is 1. This is easy to surmount:

Proposition 4.5.2. *Let f, K, and M be as in the previous proposition. There exist two degree 2, odd representations θ_i of $G(M|K)$ such that for any prime number p and any prime π of K lying over p:*

$$(\#\{x\ (mod\ p) : f(x) \equiv 0\ (mod\ p)\})^2 = \left(\chi_{\theta_1}(\sigma_\pi)\chi_{\theta_2}(\sigma_\pi) + \left(\frac{2869}{p}\right)\right)^2$$

Chapter 5

The Quintic Case: Explicit Constructions

The methods we used in the quartic case to explicitly construct a representation and the fixed field of its kernel readily extend to the quintic case. Crespo again provides us with a method of explicitly computing an element (retaining the same notation as used in the previous chapter) $\gamma \in L_1$ such that $L_1(\sqrt{\gamma}) = M$ ([7]). As before, we will then be able to determine the trace at Frobenius for many primes by determining whether γ is a square at those primes. However, when we study the conjugacy classes of $4A_5$, we will find that we run into the same problem as in the quartic case: there exist two pairs of classes of the same order that map to the same class in $G(L_1|K) \simeq A_5 \times C_2$. Distinguishing these class again requires that the 1-cocycle b_σ be explicitly constructed. However, this is much more difficult in the quintic case than in the quartic. We note that Quer uses this approach in a computation of a twist of Buhler's original icosahedral. The results of the computation are given in [9], but the steps and, in particular, the formula for b_σ are unpublished.

On the other hand, Buhler ([4]) does not use an explicit global construction of the fixed field of the kernel of the icosahedral representation corresponding to his form. Instead, he develops techniques to determine the minimal conductor of a lifting of a projective representation. This information combined with explicit local constructions at the ramified primes gives enough information to determine the *centric character* of the lifting, i.e. the restriction of the representation to the projective kernel. In the case of icosahedral representations, the centric character is then enough to determine the conjugacy class of Frobenius at any prime.

We take ideas from both of these approaches. We use Crespo's formula to derive an explicit construction of the field $M = L_1(\sqrt{\gamma})$, $\gamma \in L_1$, and we use this to determine the conductor of the θ_i. As $L_1|K$ is unramified, the possible structure of the localizations of M are very simple to determine. Computing the centric character is then much more straightforward than computing b_σ.

It is worth noting that, in general, Crespo's approach is superior, as it requires a single formula for b_σ that is independent of the fields in question. Buhler's approach, on the other hand, requires generating relations between idèles to compute the centric character, and this process grows more difficult depending on the ramification of the centric character and the class numbers of subextensions of $L_1|K$.

5.1 Conjugacy Classes

5.1.1 Classes in $G(L_1|K)$

Let p be a rational prime. K has class number 1, so for a rational prime $p \neq 19, 151$, either p is prime in K or $p = \pi\pi'$, where π, π' are prime elements of $\mathfrak{o}_K$ of norm $\pm p$. In general, for any prime $\pi \in K$, and we let p be the rational prime over which π lies, so that either $\pi = p$ or $N_{K|\mathbb{Q}}(\pi) = \pm p$. We let σ_π (resp. σ_p) denote the Frobenius element at π (resp. p) in whichever Galois group over K (resp. $\mathbb{Q}$) we are considering at the time.

If π is irrational, then to find the $G(L|K)$ class of σ_π, we factor $f(X)$ modulo p, and the degrees of the factors correspond to the lengths of the cycles in the disjoint cyclic decomposition of σ_π.

The only ambiguity is that there are two classes of 5-cycles. To distinguish between the two, we fix a root x of $f(X)$, and we compute:

$$\prod_{0 \leq i < j \leq 4} (x^{\sigma_\pi{}^i} - x^{\sigma_\pi{}^j}) = \pm\sqrt{2869}$$

One class corresponds to the positive sign, one to the negative. Explicitly, if y is a root of $g(X) = X^2 - X - 717$, then $\mathfrak{o}_K = \mathbb{Z}[y]$, and we choose $2y - 1$ to be the "positive" square root of 2869. Then if $\pi = a + by$, we have $y = -a/b$ and $2y - 1 = -2a/b - 1$ (modulo π). So σ_π is in, say, **5A** if the above product is $-2a/b - 1$ and is in **5B** if the product is $2a/b + 1$.

If π is rational, then to find the $G(L|K)$ class of σ_π, we factor $f(X)$ modulo p, and σ_π is the *square* of the permutation that corresponds to the factorization of $f(X)$ modulo p. So if:

- $f(X)$ splits into one quadratic factor and three linear factors, then σ_π is in **1**;
- $f(X)$ splits into one quartic factor one linear factor, then σ_π is in **2**;
- $f(X)$ splits into one cubic factor and one quadratic factor, then σ_π is in **3**.

Determining the class of σ_π in $G(K_1|K)$ is simple.

Definition 5.1.1. $\xi \in K^\times$ is *definite* if ξ is *totally positive* (i.e., both embeddings of ξ in $\mathbb{R}$ are positive) or *totally negative.* Equivalently, ξ is definite if $N_{K|\mathbb{Q}}(\pi) > 0$. Otherwise, ξ is *indefinite.*

A prime π splits in K_1 if and only if it is definite. (Note that this implies all rational primes p inert in K split in K_1.) Indeed, let $\mu : C_K \to \mathbb{C}^\times$ be the idèle class character corresponding to $K_1|K$. μ is unramified at all finite places of K, and so it must be nontrivial for at least one of the real places. Evaluating μ at the principal idèle -1, we see it must be nontrivial at both real places. Let μ_i be the real components of μ, $i = 1, 2$. Then for $x \in K^\times$:

$$\mu_1(x)\mu_2(x) = \operatorname{sgn}(N_{K|\mathbb{Q}}(x))$$

It follows that for a prime π, $\mu_\pi(\pi) = \operatorname{sgn}(N_{K|\mathbb{Q}}(\pi))$. Together with the above analysis, this determines the conjugacy class of σ_π in $G(L_1|K)$.

5.1.2 Classes in $G(M|K)$

We now determine the conjugacy classes in $G(M|K) \simeq 4A_5$. We find it useful to represent $4A_5$ as the subgroup $2SL_2(\mathbb{F}_5)$ of $GL_2(\mathbb{F}_5)$ generated by $SL_2(\mathbb{F}_5)$ and:

$$\zeta = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

If we let $C = \{1, z, a, b, b^2, c, c^2, zc, zc^2\}$ be the representatives of the classes of $SL_2(\mathbb{F}_5)$, then a set of representatives of the classes of $2SL_2(\mathbb{F}_5)$ is given by $\{x, \zeta x : x \in C\}$.

Clearly, the size of the class of ζx is the size of the class of x. The order of the elements is given by (writing $\zeta z = \zeta^3$):

class representative	ζ	ζ^3	ζa	ζb	ζb^2	ζc	ζc^2	$\zeta^3 c$	$\zeta^3 c^2$
order of members	4	4	2	12	12	20	20	20	20

In the surjection $2SL(2, \mathbb{F}_5) \to A_5$, ζx maps to the same class as x. The necessity in explicitly constructing b_σ in Crespo's method is now immediate: we cannot distinguish the pairs of classes $\{\zeta, \zeta^3\}$, $\{\zeta b, \zeta b^2\}$, $\{\zeta c, \zeta^3 c\}$, and $\{\zeta c^2, \zeta^3 c^2\}$, as each pair has the same image in $G(L_1|K)$ and has the same order in $G(M|K)$.

However, Buhler provides us with a simpler way of accomplishing this. If P is a prime of L lying over π, then σ_P is the smallest power of σ_π lying in $G(M|L)$; this gives a map from classes in $G(M|K)$ to elements of $G(M|L)$. No two distinct classes in $G(M|K)$ lying over the same element in $G(L|K)$ map to the same element of $G(M|L)$. Thus, determining σ_P determines the class of $\sigma_\pi \in G(M|K)$. As $G(M|L)$ is cyclic, we can use class field theory to determine σ_P.

5.2 Explicit Construction of M

We now find $\gamma \in L_1$ such that $M = L_1(\sqrt{\gamma})$ provides a solution to the embedding problem $4A_5 \twoheadrightarrow G(L|K)$. The following proposition describes all of the possibilities for γ. For the moment, we let K, E, and L represent arbitrary fields:

Proposition 5.2.1 (Crespo, [7, Thm. 2]). *Let K be a number field, E an extension of K of degree $n \geq 4$, and L the Galois closure of K of E. Suppose that $G(L|K) \simeq A_n$ and, furthermore, that the Galois embedding problem $4A_n \twoheadrightarrow G(L|K)$ is solvable. For each $a \in K^\times \setminus (L^\times)^2$ such that $w(Q_E) = (-1, a)$, define the quadratic form:*

$$\hat{Q}_a = \mathrm{Tr}_{E|K}(X^2) \perp \mathrm{Tr}_{K(\sqrt{a})|K}(X^2) \perp \mathrm{Tr}_{K(\sqrt{a})|K}(X^2)$$

Letting u_j be a K-basis for E and s_i be the n distinct embeddings of E in L:

$$\begin{aligned}
M_a &= \begin{bmatrix} M_E & 0 & 0 \\ 0 & M'_a & 0 \\ 0 & 0 & M'_a \end{bmatrix} \\
M_E &= [u_j^{s_i}]_{1\leq i,j\leq n} \\
M'_a &= \begin{bmatrix} 1 & \sqrt{a} \\ 1 & -\sqrt{a} \end{bmatrix}
\end{aligned}$$

Suppose that $\hat{Q}_a$ is equivalent over K to the form:

$$Q_q = -(X_1^2 + \cdots + X_q^2) + X_{q+1}^2 + \cdots + X_{n+4}^2$$

where $q \equiv 0 \pmod 4$. Let $[\hat{Q}_a]$ and $[Q_q]$ be the symmetric matrices corresponding to the forms $\hat{Q}_a$ and Q_q, and let $P \in GL(n+4, K)$ be such that $P^t[\hat{Q}_a]P = [Q_q]$. Then there is an element $\gamma_a \in L(\sqrt{a})$ given as a function of the minors of M_aP such that the fields $L(\sqrt{a}, \sqrt{k\gamma_a})$, $k \in K^\times$, are the solutions to the embedding problem.

We apply the theorem with our usual choices of K and L. We will work with $a = -19$.

For an $n \times n$ matrix A and indices $1 \leq i_1 < \cdots < i_k \leq n$, $1 \leq j_1 < \cdots < j_k \leq n$, we let:

$$A\begin{bmatrix} i_1 & \ldots & i_k \\ j_1 & \ldots & j_k \end{bmatrix}$$

denote the minor of A omitting the i_ℓth rows and j_ℓth columns. Then letting $A = M_aP + J$, where:

$$J = \begin{bmatrix} 0 & 0 \\ 0 & I_5 \end{bmatrix}$$

Crespo gives the formula ([8]):

$$\begin{aligned}
\gamma_a \;=\; & A\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} - A\begin{bmatrix} 1 & 2 & 4 \\ 1 & 2 & 4 \end{bmatrix} + A\begin{bmatrix} 1 & 3 & 4 \\ 1 & 3 & 4 \end{bmatrix} - A\begin{bmatrix} 2 & 3 & 4 \\ 2 & 3 & 4 \end{bmatrix} \\
& -A\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} - A\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} - A\begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix} - A\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} - A\begin{bmatrix} 2 & 4 \\ 1 & 3 \end{bmatrix} \\
& -A\begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix} + A\begin{bmatrix} 1 \\ 1 \end{bmatrix} - A\begin{bmatrix} 2 \\ 2 \end{bmatrix} + A\begin{bmatrix} 3 \\ 3 \end{bmatrix} - A\begin{bmatrix} 4 \\ 4 \end{bmatrix}
\end{aligned}$$

Applying this formula gives gives us an element γ. As in the quartic case, we multiply γ by an element of K so as to make it integral and as an initial step in getting rid of ramification. We give M, P, γ, and $n = N_{L_1|\mathbb{Q}}(\gamma)$, in addition to MAGMA code computing γ, at `http://math.rutgers.edu/~jbryk/`.

5.3 Ramification

We now determine the ramification of $M|L_1$. Using two methods, we will find that $M|L_1$ is either unramified or ramified at the primes lying a single K-prime. Although we cannot specify where the ramification occurs using these methods, we can still go through the motions of computing the θ_i for each case, one of which must give the correct values.

5.3.1 Following the Quartic Case

We first use the tools developed in Chapter 3 to determine the ramification of $M|L_1$. Applying Lemma 3.5.5, we run into a problem when trying to determine $N_{L_1|\mathbb{Q}}(\gamma)$ is divisible by $N(\pi)^{120}$, $120 = [L_1 : K]$, for any prime $\pi \neq 2$ of K. This would require checking whether the norm is divisible by any rational primes $p < \lceil N_{L_1|\mathbb{Q}}(\gamma)^{1/120} \rceil =$ 4,330,586,521,668,727,367,001, which is simply infeasible.

However, it is possible to check the condition for, say, $p < \lceil N_{L_1|\mathbb{Q}}(\gamma)^{1/240} \rceil =$ 65,807,192,021. We find that the norm is divisible by only 2, 17, 1,973, and 79,193, and with the valuation of the norm at these primes being 72, 6, 2, and 2, respectively. Thus, $M|L_1$ is unramified outside of primes lying over 2 and rational primes p less than 65,807,192,021. Now if $M|L_1$ is ramified at some prime of L_1 lying over a rational prime p greater than $N_{L_1|\mathbb{Q}}(\gamma)^{1/240}$, then $p^{120} > N_{L_1|\mathbb{Q}}(\gamma)^{1/2}$ divides $N_{L_1|\mathbb{Q}}(\gamma)$, whence $N_{L_1|\mathbb{Q}}(\gamma)^{1/240}$ cannot be divisible by the 120th power of any other prime. Furthermore, p must split in K, as otherwise p^{240} would divide the norm. The same argument indicates that if $p = \pi_1 \cdot \pi_2$ in K, then ramification can only occur at primes lying over one the π_i. Thus, $M|L_1$ is unramified outside of primes lying over 2 and possibly one other prime of K.

Since 2^{72} exactly divides the norm of γ, the only way ramification can occur at 2 is if γ is not a square modulo primes P of L_1 lying over 2. We construct a prime P of L_1 lying over 2 by letting w be a root of $X^2 + X - 717$, which has discriminant 2869. If z is the root of $X^2 + X + 5$, which has discriminant -19, then we take $z \mapsto w + 2$ modulo 4. We find that, modulo 4:

$$X^5 - X - 1 \equiv (X - w)(X + w)(X^3 + 3X^2 + 2X + 1)$$

Thus, if u_i are the roots of $X^5 - X - 1$ in L_1, and if u is a root of the irreducible cubic factor of $X^5 - X - 1$ over K_2, we let:

$$\begin{aligned} u_1 &\mapsto w \\ u_2 &\mapsto -w \\ u_3 &\mapsto u \\ u_4 &\mapsto -u^2 + 2 \\ u_5 &\mapsto u^2 - u - 1 \end{aligned}$$

Then the image of γ in L_1 modulo P^2 is:

$$\gamma \mapsto wu^2 + 2u^2 + 2wy + w + 2 \equiv (2wu^2 + 2u^2 + wu + u - w + 1)^2 \pmod{P^2}$$

Thus, $M|L_1$ is unramified at all primes P lying over 2, and we conclude $M|L_1$ is ramified at primes lying over at most one prime of K.

Finally, we note that we can move all ramification to the primes lying over 2. Indeed, if P in L_1 ramifies in M, and if P lies over a prime $\pi \in K$, then M is ramified at all primes of L_1 lying over π. Since all primes P over π divide γ, then π itself must divide γ. Replacing γ with γ/π^k, where k is the minimum of the valuations of γ at the primes P of L_1 lying over π, we remove the ramification at primes over π. We note that k must be odd; thus, if P_2 is a prime lying over 2 and π is not a square modulo P_2^2, our new γ will not be a square modulo P_2^2. This introduces ramification at 2. We may try multiplying by units in K, but since the totally negative fundamental unit is a square modulo 4, the only possibility is to replace γ by $-\gamma$, which is not guaranteed to give a square modulo 4.

5.3.2 Twisting by Characters

Let $\phi : G_K \to GL_n(\mathbb{C})$ be an Artin representation, and let $\chi : G_K \to \mathbb{C}^\times$ be a character. Then the representations ϕ and $\chi \otimes \phi$ induce the same projective representation on G_K. This gives us considerable latitude in choosing a linear representation that gives a particular projective representation. In particular, we can choose χ so as to make the conductor of $\chi \otimes \phi$ as small as possible (e.g., so that few primes divide the conductor or so that the norm of the conductor is small).

For a prime π of K, choose an embedding $G_\pi = G_{K_\pi} \hookrightarrow G_K$. Let I_π be the image of the inertia group under this embedding. Let ϕ_π be the restriction of ϕ to G_π. We note that I_π is in the kernel of ϕ_π for almost all primes. At the primes where this is not true, we can find a character χ_π on G_π such that $\chi_\pi \otimes \phi_\pi$ has minimal local conductor. If we can find a character χ on G_K such that the local component of χ at π agrees with χ_π on I_π, then $\chi \otimes \phi$ has minimal global conductor. However, this is not always possible, as seen in the following result inspired by Theorem 5 in [4]:

Theorem 5.3.1. *Let $\chi_\pi : I_\pi \to \mathbb{C}^\times$ be characters such that χ_π is trivial for almost all primes π of K, and let ϵ be the totally positive fundamental unit of K. Then there exists a character $\chi : G_K \to \mathbb{C}^\times$ such that the restriction of χ to I_π is equal to χ_π for each π if and only if:*

$$\prod_\pi \chi_\pi(\epsilon) = 1$$

Furthermore, χ is unique up to multiplication by the nontrivial character of $G(K_1|K)$.

Proof. Let $\mathfrak{o}_\pi$ be the ring of integers of the completion K_π of K at π, let C_K be the idèle class group of K, and let ∞_i, $i = 1, 2$ be the real places of K. If χ exists satisfying the above conditions, then we may view χ as a character on the C_K, and we may view the local components χ_π as characters on the unit groups $\mathfrak{o}_\pi^\times$. Since ϵ is totally positive, if χ_{∞_i} is the local component at ∞_i, then $\chi_{\infty_i}(\epsilon) = 1$. Thus, since $\chi(\epsilon) = 1$, we have:

$$1 = \chi(\epsilon) = \prod_\pi \chi_\pi(\epsilon)$$

Now suppose that the χ_π satisfy:

$$\prod_\pi \chi_\pi(\epsilon) = 1$$

Consider the idèle group:

$$J_K^\infty = \prod_{i=1}^{2} K_{\infty_i}^\times \times \prod_\pi \mathfrak{o}_\pi^\times$$

Since K has class number 1, we have:

$$C_K = J_K^\infty / \mathfrak{o}_K^\infty$$

If:

$$\prod_\pi \chi_\pi(-1) = -1$$

then let χ_{∞_1} be the sign character on $K_{\infty_1}^\times$, and let χ_{∞_2} be trivial. Then, letting v run over all places of K, we have:

$$\prod_v \chi_v(-1) = \prod_v \chi_v(\epsilon) = 1$$

which implies that for all $u \in \mathfrak{o}_K^\times$:

$$\prod_v \chi_v(u) = 1$$

Let $\chi = \prod_v \chi_v$. This defines a character of J_K^∞ trivial on $\mathfrak{o}_K^\times$ and hence gives a character on C_K. Identifying C_K with G_K^{ab} and $\mathfrak{o}_\pi^\times$ with I_π^{ab} as above, we have that $\chi : G_K \to \mathbb{C}^\times$ satisfies the desired properties.

The uniqueness statement follows from the fact that the ratio of two characters on G_K satisfying the above conditions is unramified at all finite places and hence factors through $G(K_1|K)$. □

We apply the theorem to our scenario. Let $\theta = \theta_i$ be one of the representations we are constructing. Since $L_1|K$ is unramified, the image of I_π in $G(M|K) = 2SL_2(\mathbb{F}_5)$ is contained in $\{\pm 1\}$ for all π. Thus, there is a real-valued character χ_π on I_π such that $\theta_\pi(\sigma) = \chi_\pi(\sigma) I_2$ for all $\sigma \in I_\pi$. If:

$$\prod_\pi \chi_\pi(\epsilon) = 1$$

then we apply the theorem to find χ with local components χ_π. Clearly, the local restrictions of $\chi \otimes \theta$ are all trivial, and so we can take θ to be unramified at all primes.

On the other hand, if:

$$\prod_{\pi} \chi_\pi(\epsilon) = -1$$

then there exists some π_0 such that $\chi_{\pi_0}(\epsilon) = -1$. Thus:

$$\prod_{\pi \neq \pi_0} \chi_\pi(\epsilon) = 1$$

and we can find χ with local components χ_π at all $\pi \neq \pi_0$ and trivial at π_0. The local restrictions of $\chi \otimes \theta$ are all trivial except at π_0, so θ is ramified at exactly one prime.[1]

Note. We will only work through the unramified case, as this happens to be the correct one. In Chapter 6, we succeed in constructing an icosahedral form of full level and with a few specified eigenvalues. The only possible fixed field of the projective kernel for the corresponding representation θ' is L. The fixed field of the kernel of the determinant must be an unramified cyclic extension of K, i.e. either K or K_1. It cannot be K since $2A_5 \twoheadrightarrow G(L|K)$ is not solvable, so it must be K_1. If M is the fixed field of the kernel of θ', then we must have $G(M|K) \simeq 4A_5$. Our construction below assumes the existence of such an M, and the representations we construct are uniquely determined up to conjugation over $\mathbb{Q}(\sqrt{5}, \sqrt{-1})$. Thus, θ' must be one of the representations we construct.

If the argument seems circular, we remind the reader that the representations we construct are only used to give us the Fourier coefficients of an object which is conjectured to be a modular form. Once we construct the object with these coefficients, the existence of the representations we construct is irrelevant.

5.4 The Centric Character

For the moment, let K, L, and M represent arbitrary fields. Consider an Artin representation $\phi : G(M|K) \to GL_n(\mathbb{C})$, and let L be the fixed field of the projective kernel

[1] We note that, since there is a quadratic character χ_4 modulo 4 such that $\chi_4(\epsilon) = -1$, we can shift the ramification to 2 by further twisting by a character with trivial local components except at 2 and π_0, where we take χ_4 and χ_{π_0} to be the local components.

of ϕ. The elements of $G(M|L)$ act by scalars under ϕ, and so there is a character $\chi : G(M|L) \to \mathbb{C}^\times$ such that $\phi(\sigma) = \chi(\sigma)I_n$ for all $\sigma \in G(M|L)$.

Definition 5.4.1. The character χ on $G(M|L)$ such that $\phi(\sigma) = \chi(\sigma)I$ is the *centric character* of ϕ.

We identify χ with the corresponding character on C_L.

Notes.

- Let $\bar{\phi} : G(L|K) \to PGL_n(\mathbb{C})$ be a projective Galois representation. We say that χ is *centric* for $\bar{\phi}$ if there exists a lifting ϕ of $\bar{\phi}$ such that χ is the centric character of ϕ.

- Since any two liftings of $\bar{\phi}$ differ by a character on G_K, the ratio of any two centric characters lifts to a character on G_K.

- If ϕ is an Artin representation with centric character χ, then χ is $G(L|K)$ invariant in the sense that for all $x \in C_L$ and all $\sigma \in G(L|K)$, $\chi(x^\sigma) = \chi(x)$.

We return to our specific scenario. Let π be a prime of K and P a prime of L lying over K. We use the centric character as a means of determining $\sigma_P \in G(M|L)$. As we have noted, if we know the class of σ_π as an element of $G(L|K)$, then knowing what σ_P is in $G(M|L)$ immediately gives us the class of σ_π in $G(M|K)$, whence we can compute $\chi_{\theta_i}(\sigma_\pi)$.

5.4.1 The Centric Characters of θ_i

Let χ_i be the centric character of θ_i, $i = 1, 2$. Note that, since $\theta_1 \otimes \theta_2$ is a real-valued character, we must have $\chi_1 = \bar{\chi}_2$. Thus we let $\chi = \chi_1$, and determining χ then determines both characters. Let P be a prime of L, and, by abuse of notation, let $\chi(P)$ be the value of χ at an idèle which is 1 at all places except at P, where it is a uniformizing element at P. Equivalently, $\chi(P)$ is the value of the local component χ_P at a uniformizing element at P.

We note that our explicit construction of γ allows us to compute centric character at primes P lying over definite primes π. Let π be such a prime of K, P a prime of

L lying over π, and Q a prime of M lying over P. Then π splits in K_1, and hence P splits in L_1. Letting Q be a prime of M lying over P, we then have $[M_Q : L_P] = 1$ or 2, with the former holding when $\chi(P) = 1$ and the latter when $\chi(P) = -1$. This implies that $\chi(P) = 1$ if and only if γ is a square modulo P or, equivalently, if and only if σ_π in $G(M|K)$ has twice the order of the image of σ_π in $G(L|K)$. We thus have:

- $\chi(P) = 1$ for σ_π in the class of 1, b^2, c, c^2, or ζa;

- $\chi(P) = -1$ for σ_π in the class of z, b, zc, zc^2, or a.

If π is indefinite, let $f = 1, 3, 5$ be the residue index of P over π. Then $\sigma_P = \sigma_\pi^f$ as elements of $G(M|K)$, and have that $\sigma_P = \zeta$ or ζ^3. We choose $\chi(\zeta) = i$. We obtain:

- $\chi(P) = i$ for σ_π in the class of ζ, ζb, ζc, or ζc^2;

- $\chi(P) = -i$ for σ_π in the class of ζ^3 ζb^2, $\zeta^3 c$, or $\zeta^3 c^2$.

However, the order of σ_π in $G(M|K)$ is always twice the order of σ_π in $G(L|K)$, and so γ is not a square modulo P. This is where the explicit construction of the 1-cocycle b_σ, where $\gamma^{\sigma-1} = b_\sigma^2$, or computation of the centric character becomes necessary.

On the surface, it seems that computing χ requires working with idèles in C_L, a degree 60 extension of K. To make the computation more manageable, we use Buhler's method of relating χ to an idèle character over a degree 6 extension of K:

Theorem 5.4.1 (Buhler, [4, Thm. 2])**.** *Let K be a number field, and let $\bar{\phi} : G_K \to PGL_n(\mathbb{C})$ be a projective Galois representation with kernel G_L. Let c be the cohomology class in $H^2(G(L|K), \mathbb{C}^\times)$ determined*[2] *by $\bar{\phi}$, and let E' be an intermediate extension. Then there exists a quasicharacter $\psi : C_{E'} \to \mathbb{C}^\times$ such that $\psi \circ N_{L|E'}$ is a centric character for a lifting of $\bar{\phi}$ if and only if:*

$$\mathrm{Res}_{G(L|E')}^{G(L|K)} c = 0$$

Using the facts that A_5 contains subgroups isomorphic to the dihedral group D_5 and that $H^2(D_5, \mathbb{C}^\times) = 1$, we have:

[2] *The exact sequence $1 \to \mathbb{C}^\times \to GL_n(\mathbb{C}) \to PGL_n(\mathbb{C}) \to 1$ corresponds to a cocycle in $H^2(PGL_n(\mathbb{C}), \mathbb{C}^\times)$; c is the pullback of this class under $\bar{\phi}$.*

Corollary 5.4.2 (Buhler [4, p. 55]). *Using the notation of the theorem, suppose $G(L|K) \simeq A_5$. Let χ be centric for $\bar{\rho} : G(L|K) \hookrightarrow PGL_2(\mathbb{C})$, and let E' be the fixed field of an embedding of $D_5 \hookrightarrow G(L|K)$. Then there exists $\psi : C_{E'} \to \mathbb{C}^\times$ such that $\chi = \psi \circ N_{L|E'}$.*

We apply this corollary to our scenario. Let $u_1, \ldots, u_5$ be the roots of $f(X)$, and consider the element of L:

$$v = (u_1u_2 + u_2u_3 + u_3u_4 + u_4u_5 + u_5u_1) - (u_1u_3 + u_3u_5 + u_5u_2 + u_2u_4 + u_4u_1)$$

Then v has degree 12 over $\mathbb{Q}$. Its minimal polynomial over $\mathbb{Q}$ factors into two sextic polynomials over K:

$$\begin{aligned} g(X) &= X^{12} + 10X^{10} + 55X^8 + 140X^6 + 175X^4 - 3019X^2 + 25 \\ &= (X^6 + 5X^4 + 15X^2 + \sqrt{2869}X - 5)(X^6 + 5X^4 + 15X^2 - \sqrt{2869}X - 5) \end{aligned}$$

Let $E' = K(v)$. Then it is immediate that $G(L|E') \simeq D_5$, since $[L : E'] = 10$ and D_5 is the unique (up to conjugation) subgroup of A_5 of order 10. Thus, there exists an idèle class character $\psi : C_{E'} \to \mathbb{C}^\times$ such that $\chi = \psi \circ N_{L|E'}$.

Let π be a prime of K, and let $\mathfrak{p}$ be a prime of E' lying over π. Following the same abuse of notation as above, we want to find the value of $\psi(\mathfrak{p})$. Letting P be a prime of L lying over $\mathfrak{p}$ and f be the residue index of P over $\mathfrak{p}$, we then have $\chi(P) = \psi(\mathfrak{p})^f$.

Let ψ and ψ' be two distinct characters on $C_{E'}$ such that $\chi = \psi \circ N_{L|E'} = \psi' \circ N_{L|E'}$. Then the ratio $\psi\psi'^{-1}$ is trivial on $N_{L|E'}C_L$. The maximal abelian quotient of $G(L|E')$ is $G(E''|E')$, where E'' is the quadratic extension of E' fixed by the subgroup of $G(L|E')$ of order 5. Thus $N_{L|E'}C_L = N_{E''|E'}C_{E''}$, and $\psi\psi'^{-1}$ is character on $C_{E'}/N_{E''|E'}C_{E'} \simeq G(E''|E')$. Letting Θ be the nontrivial character on this group, we have $\psi' = \Theta\psi$.

Note that since $[L : E''] = 5$ and L is totally complex, E'' has only complex embeddings. Thus all real places of E' split in E'', and Θ must have nontrivial components at all real places of E'.

5.4.2 Evaluating ψ

We first study ψ the real places of E'. Each ∞_i, $i = 1, 2$, splits into two real paces and two complex places. Let the real places above ∞_1 be v_1 and v_2, and let the real places above ∞_2 be v_3 and v_4, and for each v_i, let sgn_i denote the sign character on $K_{v_i}^{\times}$.

We evaluate ψ at the principal idèle -1. Since ψ is unramified at finite places, we have that:

$$\prod_{i=1}^{4} \psi_{v_i}(-1) = 1$$

This implies that $\psi_{v_i} = \mathrm{sgn}_i$ for an even number of i and is trivial for the other values of i.

Now let π be a prime of K such that σ_π is in the class of ζb in $G(M|K)$. Then $\mu(\pi) = -1$, so that π is indefinite. Without loss of generality, π is negative at ∞_1 and positive at ∞_2. $\pi\mathfrak{o}_K$ factors as $\mathfrak{p}_1\mathfrak{p}_2$ for two primes $\mathfrak{p}_i$ in E. Let P_i be primes of L lying over $\mathfrak{p}_i$. Then for each i, since the residue degree of P_i over $\mathfrak{p}_i$ is 1:

$$\psi(\mathfrak{p}_i) = \chi(P_i) = \sqrt{-1}$$

Thus:

$$1 = \psi(\pi) = \psi_{v_1}(\pi)\psi_{v_2}(\pi)\psi_{\mathfrak{p}_1}(\pi)\psi_{\mathfrak{p}_1}(\pi)$$

And so:

$$\psi_{v_1}(\pi)\psi_{v_2}(\pi) = -1$$

Thus $\psi_{v_i} = \mathrm{sgn}_i$ for precisely one of $i = 1, 2$. Since this identity holds for an even number $i = 1, 2, 3, 4$, $\psi_{v_i} = \mathrm{sgn}_i$ for precisely one of $i = 3, 4$. Without loss of generality, assume that the identity holds for $i = 1, 3$. This determines the components of ψ at the real places up to multiplication by Θ.[3]

To compute $\psi(\mathfrak{p})$, we note that E' has class number 2. If $\mathfrak{p} = \Pi\mathfrak{o}_{E'}$ is principal, then we have:

$$1 = \psi(\Pi) = \mathrm{sgn}_1(\Pi)\mathrm{sgn}_3(\Pi)\psi(\mathfrak{p}) \quad \Rightarrow \quad \psi(\mathfrak{p}) = \mathrm{sgn}_1(\Pi)\mathrm{sgn}_3(\Pi)$$

If $\mathfrak{p}$ is not principal, then let $\mathfrak{q}$ be a representative of the nontrivial ideal class, e.g. a prime dividing 3. Then $\mathfrak{p}\mathfrak{q} = \Pi\mathfrak{o}_{E'}$, and:

$$1 = \psi(\Pi) = \mathrm{sgn}_1(\Pi)\mathrm{sgn}_3(\Pi)\psi(\mathfrak{p})\psi(\mathfrak{q}) \quad \Rightarrow \quad \psi(\mathfrak{p}) = \mathrm{sgn}_1(\Pi)\mathrm{sgn}_3(\Pi)\bar{\psi}(\mathfrak{q})$$

[3] In computations, we instead determine which real places have nontrivial components by looking at the signs of the embeddings of an indefinite fundamental unit.

For any prime Q of L lying over $\mathfrak{q}$, we have $\chi(Q) = \pm i$, so that $\psi(\mathfrak{q}) = \pm i$. We choose $\psi(\mathfrak{q}) = i$, so that:

$$\psi(\mathfrak{p}) = -i\,\mathrm{sgn}_1(\Pi)\mathrm{sgn}_3(\Pi)$$

We give code for computing $\chi_{\theta_i}(\sigma_\pi)$ and the results thereof at `http://math.rutgers.edu/~jbryk/`.

Chapter 6

Hilbert Modular Forms

6.1 Introduction

In this chapter, we consider any of the four representations θ constructed in chapter 4, and then we construct a Hilbert modular form $\mathbf{f}$ to which it corresponds. Conjecturally, there is a one-to-one correspondence between Hilbert eigenforms of parallel weight 1 over a totally real number field K and odd, degree 2 Galois representations of G_K. The Fourier coefficients of the form correspond to the traces at Frobenius of the representation. Furthermore, the level of the form is the conductor of the representation, and the nebentypus of the form is given by the determinant of the representation. One direction of this correspondence is known: for any cuspidal eigenform of positive integral weight, there exists a system of compatible Galois representations, with parallel weight 1 forms corresponding to complex representations. Jarvis ([15]) relates the sequence of results leading to this general fact; of specific interest to us are the results for parallel weight 1 by Rogawski-Tunnell ([26]) and Ohta ([23]).

The converse is known for most cases: for any nonicosahdedral representation $\phi : G_K \to GL_2(\mathbb{C})$, there exists an Hilbert eigenform corresponding to ϕ. The cyclic and dihedral cases are due to Hecke, while Langlands ([20]) and Tunnell ([37]) showed the tetrahedral and octahedral cases, respectively.

The icosahedral case has been more elusive. Buhler ([4]) was the first to show the existence of an icosahedral classical modular form, while Taylor improved upon this by constructing infinite families of such forms in [35] and in joint work with Buzzard, Dickinson, and Shepherd-Barron ([5]). The full conjecture over $\mathbb{Q}$ was recently obtained as a corollary of Serre's conjecture for modular representations of $G_{\mathbb{Q}}$, which was proved by Khare-Wintenberger in 2009 ([17], [18]). Given these results, icosahedral Hilbert modular forms can be trivially constructed over totally real fields via base change. However, our search through the literature indicates that the existence of icosahedral forms not thus obtained is unknown. To our knowledge, we provide the first example of such in constructing the form $\mathbf{f}$.

We let $\mathbf{f}_\theta$ be the formal series whose coefficients are obtained from the Artin L-function of θ. (We describe what sort of series we are considering in the sequel.) The basic idea for showing that $\mathbf{f}_\theta$ is a weight 1 form is to:

1. compute "enough" coefficients of $\mathbf{f}_\theta$;
2. find a basis of an "appropriate" space of modular forms;
3. using this basis, construct a weight 1 form $\mathbf{f}$ that agrees with $\mathbf{f}_\theta$ for the coefficients we have computed; and
4. verify that $\mathbf{f}_\theta = \mathbf{f}$ by showing the existence of a Hecke eigenvalue that must come from an icosahedral form.

What makes this task nontrivial is that there are not effective methods for finding bases for spaces of forms of weight 1. This necessitates working with spaces of forms of weight at least 2, for which we do have effective algorithms. However, the dimensions of these spaces become large fairly quickly, as do the degrees of the number fields over which the coefficients of their Hecke eigenbases are defined. These factors present computational challenges which require the careful application of theory and the development of efficient algorithms.

6.2 Hilbert Modular Forms

We discuss the basic theory of Hilbert modular form from two perspectives. First, we introduce the classical theory–that is, we will interpret Hilbert modular forms to be functions on products of upper-half planes invariant under the action of discrete groups of isometries. We favor this point of view, as it eases certain aspects of our computation. However, we will tie the classical theory to the adèlic perspective, which provides a more natural setting in which to introduce Hecke operators, eigenforms, and

L-series. We largely follow the presentation given in [34], but we also use [12] and [39] as references.

Let K be a totally real number field of degree n and let $\mathfrak{o}$ be its ring of integers. There are n distinct embeddings $K \hookrightarrow \mathbb{R}$, $\alpha \mapsto \alpha^{(i)}$, $1 \leq i \leq n$.

Definition 6.2.1. $\alpha \in K$ is *totally positive* if $\alpha^{(i)} > 0$ for all i. We denote this by $\alpha \gg 0$.

The notation introduced above is extended to all $\alpha, \beta \in K$ by defining $\alpha \gg \beta$ if and only if $\alpha - \beta \gg 0$.

The n embeddings $K \hookrightarrow \mathbb{R}$ give an embedding:

$$GL_2^+(K) \hookrightarrow \prod_{i=1}^{n} GL_2^+(\mathbb{R})$$

where the superscript $+$ indicates matrices of totally positive determinant. The action of $GL_2^+(\mathbb{R})$ on the upper half plane $\mathfrak{H}$ by linear fractional transformations gives an action of $GL_2^+(K)$ on the n-fold product $\mathfrak{H}^n$.

Let $\mathbf{k} \in \mathbb{Z}^n$ and $\gamma \in GL_2^+(K)$. For functions $f : \mathfrak{H}^n \to \mathbb{C}$, we introduce the slash operator:

$$(f|\gamma)(z) = \left(\prod_{i=1}^{n} (\det(\gamma^{(i)}))^{k_i/2} (c^{(i)} z_i + d^{(i)})^{-k_i} \right) f(\gamma z), \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Let $\mathfrak{d}$ be the different of K over $\mathbb{Q}$. The maximal orders of $M_2(K)$ are given by:

$$\begin{pmatrix} \mathfrak{o} & (\mathfrak{a}\mathfrak{d})^{-1} \\ \mathfrak{a}\mathfrak{d} & \mathfrak{o} \end{pmatrix}$$

where $\mathfrak{a}$ ranges over the fractional ideals of K. We define the group $\Gamma = \Gamma(\mathfrak{a})$ to be the subset of matrices of determinant in $\mathfrak{o}_+^\times$, the group of totally positive units of $\mathfrak{o}$. Two such groups $\Gamma(\mathfrak{a})$ and $\Gamma(\mathfrak{b})$ are conjugate in $GL_2^+(K)$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ lie in the same narrow ideal class–i.e., if $\mathfrak{a}\mathfrak{b}^{-1}$ is principally generated by a totally positive element. Thus, the number of such groups up to conjugation is h^+, the narrow class number of K.

Note that the groups Γ are *not congruence subgroups* but, rather, *a system of groups of full level.* We can define congruence subgroups for each Γ in analogy to the classical theory of modular forms, but as our representation is of trivial conductor, we opt not to introduce this additional bit of structure.

We can now define Hilbert modular forms:

Definition 6.2.2. Let $n > 1$, and let $\mathbf{k}$ and Γ be as above. A holomorphic function $f : \mathfrak{H}^n \to \mathbb{C}$ is a *Hilbert modular form* of weight $\mathbf{k}$ on Γ if $f|\gamma = f$ for all $\gamma \in \Gamma$.

We let $M_{\mathbf{k}}(\Gamma)$ denote the vector space of Hilbert modular forms of weight $\mathbf{k}$ on Γ. If $\mathbf{k}$ is of *parallel weight* k–i.e., $\mathbf{k} = (k, \ldots, k)$, we denote this space by $M_k(\Gamma)$.

For any $\epsilon \in \mathfrak{o}^\times$, consider the scalar matrix $\gamma = \epsilon\mathbf{1} \in \Gamma$. For any $f \in M_{\mathbf{k}}(\Gamma)$, we have:

$$f(z) = f|\gamma(z) = \prod_{i=1}^{n} \left(\frac{|\epsilon^{(i)}|}{\epsilon^{(i)}} \right)^{k_i} f(z) = \prod_{i=1}^{n} \operatorname{sgn}\left(\epsilon^{(i)}\right)^{\mathbf{k_i}} f(z)$$

Thus, $M_k(\Gamma) = 0$ unless for all $\epsilon \in \mathfrak{o}^\times$:

$$\operatorname{sgn}(\epsilon)^{\mathbf{k}} := \prod_{i=1}^{n} \operatorname{sgn}\left(\epsilon^{(i)}\right) = 1$$

As such, we assume this condition is always true.

Given a Hilbert modular form f on $\Gamma(\mathfrak{a})$, f is invariant under the translations $z \mapsto z + \alpha$ for precisely $\alpha \in (\mathfrak{a}\mathfrak{d})^{-1}$, and so it has a Fourier series indexed by $\mathfrak{a}$, the dual module to $(\mathfrak{a}\mathfrak{d})^{-1}$ with respect to the trace form:

$$f(z) = \sum_{\nu \in \mathfrak{a}} a_\nu \exp(2\pi i \operatorname{Tr}(\nu z)), \quad \operatorname{Tr}(\nu z) = \sum_{i=1}^{n} \nu^{(i)} z_i$$

Note that the definition of Hilbert modular forms given above does not stipulate a holomorphy condition for the cusps. This is due to the *Gotzky principle* ([13]), which essentially states that holomorphy at the cusps is guaranteed. More specifically, for $n > 1$ and any function satisfying the conditions of Definition 6.2.2, $a_\nu = 0$ unless $\nu = 0$ or $\nu \gg 0$. If the class number h of K is equal to 1, then a Hilbert modular form f is a *cusp form* if $a_0 = 0$; we denote the space of such forms by $S_{\mathbf{k}}(\Gamma)$. For $h > 1$, the definition of cusp form is more restrictive, as there are h cusps, and Fourier expansions at each of these must be considered.

6.2.1 The Adèlic Perspective

Let $\mathbb{A}_K$ be the ring of adèles over K, and consider the topological group $GL_2(\mathbb{A}_K)$. The topology is determined by the fundamental system of open subgroups:

$$GL_2^+(\mathbb{R})^n \times \prod_{\mathfrak{p}} GL_2(\mathfrak{o}_\mathfrak{p})$$

where $\mathfrak{p}$ runs over the (finite) primes of K. Let:

$$K_\infty = \left\{ \begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix}, \dots, \begin{pmatrix} x_n & -y_n \\ y_n & x_n \end{pmatrix} \right\} \subset GL_2^+(\mathbb{R})^n$$

and:

$$K_0 = \prod_{\mathfrak{p}} GL_2(\mathfrak{o}_\mathfrak{p})$$

We can put a complex structure on $GL_2(\mathbb{R})^n/K_\infty$ by identifying it with $(\mathfrak{H} \cup \overline{\mathfrak{H}})^n$ via the mapping $g \mapsto (g_1 i, \dots, g_n i)$. This gives a complex structure on the quotient:

$$GL_2(\mathbb{A}_K)/K_\infty = (GL_2(\mathbb{R})^n/K_\infty) \times GL_2(\mathbb{A}_K^f)$$

where $\mathbb{A}_K^f$ is the ring of finite adèles. This, in turn, endows a complex structure on the quotient:

$$GL_2(K)\backslash GL_2(\mathbb{A}_K)/K_\infty K_0$$

Let $\mathfrak{a}_j$, $j = 1, \dots, h^+$, be a system of representatives of the narrow ideal classes of K, and let $\Gamma_j = \Gamma(\mathfrak{a}_j)$. We have:

Proposition 6.2.1 ([39, 7.2])**.** *There is an identification of complex manifolds:*

$$GL_2(K)\backslash GL_2(\mathbb{A}_K)/K_\infty K_0 = \bigcup_{j=1}^{h^+} \Gamma_j \backslash \mathfrak{H}^n$$

Furthermore, there are $g_j \in GL_2(\mathbb{A}_K^f)$ such that:

$$\begin{aligned} GL_2(\mathbb{A}_K) &= \bigcup_{j=1}^{h^+} GL_2(K) g_j GL_2^+(\mathbb{R})^n K_0 \\ \Gamma_j &= g_j GL_2^+(\mathbb{R})^n K_0 g_j^{-1} \cap GL_2(K) \end{aligned}$$

The proposition gives us a roundabout means of defining modular forms on $GL_2(\mathbb{A}_K)$.

Definition 6.2.3. Fix a weight $\mathbf{k}$. A function $\mathbf{f} : GL_2(\mathbb{A}_K) \to \mathbb{C}^{h^+}$ is a *modular form* of weight $\mathbf{k}$ on K_0 if there is an h^+-tuple of forms $(f_1, \ldots, f_{h^+})$, $f_j \in M_{\mathbf{k}}(\Gamma_j)$ such that for each $\gamma \in GL_2(K)$ and $g = g_\infty g_f \in GL_2^+(\mathbb{R})^n \times K_0$:

$$\mathbf{f}(\gamma g_j g) = (f_j|g_\infty)(i, \ldots, i)$$

As such, we identify $\mathbf{f}$ with $(f_1, \ldots, f_{h^+})$. $\mathbf{f}$ is a *cusp form* precisely when each of the f_j is a cusp forms. We let $M_{\mathbf{k}}(K_0)$ denote the space of modular forms, and we let $S_{\mathbf{k}}(K_0)$ denote the space of cusp forms. These spaces are identified with $\oplus_j M_{\mathbf{k}}(\Gamma_j)$ and $\oplus_j S_{\mathbf{k}}(\Gamma_j)$, respectively.

We can introduce nontrivial levels by modifying the group K_0 to include congruence subgroups at a finite number of places. Since each component of K_0 is the full group $GL_2(\mathfrak{o}_\mathfrak{p})$, we also say that Hilbert modular forms on K_0 are of *full level.*

6.2.2 Hecke Operators and L-Series

Hecke operators on Hilbert modular forms are best described in terms of adèles. For each finite prime $\mathfrak{p}$ of K, define:

$$\begin{aligned} Y_\mathfrak{p} &= \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & \mathfrak{d}_\mathfrak{p}^{-1} \\ \mathfrak{d}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix} \\ W_\mathfrak{p} &= \{y \in Y_\mathfrak{p} : \det(y) \in \mathfrak{o}_\mathfrak{p}^\times\} \end{aligned}$$

and let:

$$\begin{aligned} Y &= GL_2(\mathbb{A}_K) \bigcap \left(GL_2^+(\mathbb{R})^n \times \prod_\mathfrak{p} Y_\mathfrak{p} \right) \\ W &= GL_2^+(\mathbb{R})^n \times \prod_\mathfrak{p} W_\mathfrak{p} \end{aligned}$$

For $y \in Y$, the double coset WyW decomposes into a finite union $\bigcup_j W y_j$ with $y_j \in GL_2(\mathbb{A}_K^f)$. For $\mathbf{f} \in M_{\mathbf{k}}(K_0)$, we define the action of the double coset by:

$$(\mathbf{f}|WyW)(x) = \sum_j \mathbf{f}(x y_j^\iota)$$

where, for 2×2 matrices x, ι is the main involution:

$$x^\iota = \det(x) x^{-1}$$

In terms of the representation $M_{\mathbf{k}}(K_0) = \oplus_j M_{\mathbf{k}}(\Gamma_j)$, the action of WyW maps $M_{\mathbf{k}}(\Gamma_j)$ to $M_{\mathbf{k}}(\Gamma_i)$ if $\det(y)\mathfrak{a}_j\mathfrak{a}_i^{-1}$ is in the trivial narrow ideal class.

Definition 6.2.4. Let $\mathfrak{m}$ be an integral ideal of K. The $\mathfrak{m}$*th Hecke operator* is:

$$T(\mathfrak{m}) = \sum_{\substack{y \in Y \\ \det(y)\mathfrak{o} = \mathfrak{m}}} WyW$$

We define additional operators $S(\mathfrak{m}) = WaW$, where $a \in \mathbb{A}_K^\times$ is such that $a\mathfrak{o} = \mathfrak{m}$. The operators $T(\mathfrak{m})$ and $S(\mathfrak{m})$ permute the spaces $M_{\mathbf{k}}(\Gamma_j)$ according to the same rule as for the action by WyW, replacing $\det(y)$ with $\mathfrak{m}$ and $\mathfrak{m}^2$, respectively. The product of Hecke operators is given by:

$$T(\mathfrak{m})T(\mathfrak{n}) = \sum_{\mathfrak{m}+\mathfrak{n} \subset \mathfrak{a}} N(\mathfrak{a})S(\mathfrak{a})T(\mathfrak{a}^{-2}\mathfrak{m}\mathfrak{n})$$

and this gives the formal Euler product:

$$\sum_{\mathfrak{m}} T(\mathfrak{m})N(\mathfrak{m})^{-s} = \prod_{\mathfrak{p}} \left(1 - T(\mathfrak{p})N(\mathfrak{p})^{-s} + S(\mathfrak{p})N(\mathfrak{p})^{1-2s}\right)^{-1}$$

We can decompose the space of modular forms into common eigenspaces for the $S(\mathfrak{p})$, $\mathfrak{p}$ prime. For each such subspace there is a Hecke character of finite order ψ on $\mathbb{A}_K^\times$ so that $\mathbf{f}(vx) = \psi(v)\mathbf{f}(x)$ for each $v \in \mathbb{A}_K^\times$. Noting that we can take $(\mathbf{f}|S(\mathfrak{p}))(x) = \mathbf{f}(\pi_{\mathfrak{p}}x)$, $\pi_{\mathfrak{p}}$ a uniformizer in $\mathfrak{o}_{\mathfrak{p}}$, we have that the eigenvalue of $S(\mathfrak{p})$ is $\psi(\pi_{\mathfrak{p}})$. Each ψ must satisfy the consistency condition:

$$\psi(v) = \operatorname{sgn}(v)^{\mathbf{k}}, \quad v \in \prod_{j=1}^{n} \mathbb{R}^\times$$

and must be trivial on $\prod_{\mathfrak{p}} \mathfrak{o}_{\mathfrak{p}}^\times$. This corresponds to a character ψ^* on the narrow ideal group given by $\psi^*(\mathfrak{p}) = \psi(\pi_{\mathfrak{p}})$.

For simplicity's sake, we assume that $\mathbf{k}$ has parallel weight k. For each component f_j of a modular form $\mathbf{f}$, we have a Fourier expansion:

$$f_j(z) = \sum_{\substack{\nu \in \mathfrak{a}_j \\ \nu \gg 0 \text{ or } \nu = 0}} a_{j,\nu} \exp(2\pi i \operatorname{Tr}(\nu z))$$

Since $f_j(\epsilon z) = f_j(\epsilon z)N_{K|\mathbb{Q}}(\epsilon)^{k/2} = f_j(z)$ for all $\epsilon \in \mathfrak{o}_+^\times$, we have that the value of $a_{j,\nu} = a_{j,\nu'}$ if $\nu\mathfrak{o} = \nu'\mathfrak{o}$. Any integral ideal $\mathfrak{b}$ of K can be written $\mathfrak{b} = \nu\mathfrak{a}_j^{-1}$ for a unique

j and ideal $\nu\mathfrak{o}$. We then define:

$$C(\mathfrak{b}, \mathbf{f}) = a_{j,\nu} N(\mathfrak{a}_j)^{-k/2}$$

Renormalizing $T'(\mathfrak{m}) = N(\mathfrak{m})^{k/2-1} T(\mathfrak{m})$, we have:

$$C(\mathfrak{b}, \mathbf{f}|T'(\mathfrak{m})) = \sum_{\mathfrak{b}+\mathfrak{m}\subset\mathfrak{a}} \psi^*(\mathfrak{a}) N(\mathfrak{a})^{k-1} C(\mathfrak{a}^{-2}\mathfrak{b}\mathfrak{m}, \mathbf{f})$$

We attach an L-series to $\mathbf{f}$:

$$L(s, \mathbf{f}) = \sum_{\mathfrak{b}} C(\mathfrak{b}, \mathbf{f}) N(\mathfrak{b})^{-s}$$

This can be extended to a meromorphic function on the s-plane and is entire if $\mathbf{f}$ is a cusp form. If $\mathbf{f}$ is a common eigenform of all the Hecke operators, where $\mathbf{f}|T'(\mathfrak{m}) = \lambda(\mathfrak{m})\mathbf{f}$, then $C(\mathfrak{m}, \mathbf{f}) = \lambda(\mathfrak{m}) C(\mathfrak{o}, \mathbf{f})$. The formal Euler product for Hecke operators then translates to the Euler product:

$$\sum_{\mathfrak{b}} \lambda(\mathfrak{b}) N(\mathfrak{b})^{-s} = \prod_{\mathfrak{p}} \left(1 - \lambda(\mathfrak{p}) N(\mathfrak{p})^{-s} + \psi^*(\mathfrak{p}) N(\mathfrak{p})^{k-1-2s}\right)^{-1}$$

If $C(\mathfrak{o}, \mathbf{f}) = 1$, then $L(s, \mathbf{f})$ is equal to this Euler product, and we call $\mathbf{f}$ *normalized.*

6.2.3 Eisenstein Series

We now introduce Eisenstein series for the groups $\Gamma(\mathfrak{a})$, and we state formulas for their Fourier coefficients. The presentation and formulas are due to Gundlach ([14, §4]). For the sake of simplicity, we assume that $h = 1$. Thus, there is only one cusp, and we only have to worry about one Fourier series for each Eisenstein series. We still assume that we have parallel weight k.

There are convergence issues for Eisenstein series when $k \leq 2$, so we introduce a complex parameter s. We define:

$$G_k(z, s, \mathfrak{a}) = \sum_{\substack{(\mu_1,\mu_2)\in(\mathfrak{a}\mathfrak{d}\times\mathfrak{o})/\mathfrak{o}^\times \\ (\mu_1,\mu_2)\neq(0,0)}} N(\mu_1 z + \mu_2)^{-k} |N(\mu_1 z + \mu_2)|^{-s}, \quad k + \Re(s) > 2$$

It is immediate that this is automorphic under $\Gamma(\mathfrak{a})$. This series may be analytically continued to the s-plane, and from this we recover the correct notion of Eisenstein series for $k \leq 2$. Furthermore, we can use this to determine the Fourier coefficients of these Eisenstein series. We define:

$$G_k(z, \mathfrak{a}) = G_k(z, s, \mathfrak{a})\big|_{s=0}$$

We have that $G_k(z, \mathfrak{a}) \in M_k(\Gamma(\mathfrak{a}))$. For totally positive $\nu \in \mathfrak{a}$, $\nu \neq 0$, the Fourier coefficients of $G_k(z, \mathfrak{a})$ are given by:

$$a_k(\nu, \mathfrak{a}) = \frac{(-2\pi i)^{nk}}{(k-1)!\sqrt{|D|}}(N(\nu))^{k-1} \sum_{\mathfrak{a}\mathfrak{d}|(\mu)|\nu\mathfrak{d}} \frac{\operatorname{sgn}(N(\mu))^k}{|N(\mu)|^{k-1}}$$

where D is the discriminant of K over $\mathbb{Q}$. When $k = 1$, we have:

$$a_1(\nu, \mathfrak{a}) = \frac{(-2\pi i)^n}{\sqrt{|D|}} \sum_{\mathfrak{a}\mathfrak{d}|(\mu)|\nu\mathfrak{d}} \operatorname{sgn}(N(\mu))$$

For $\nu = 0$, there are different formulas for $k \geq 2$ and $k = 1$. We only need the expression for $k = 1$, so we present only this case. Let χ be the character on the narrow ideal class group given by $\chi(\xi\mathfrak{o}) = \operatorname{sgn}(N(\xi))$. (This character and, hence, the series exist if and only if there are no units of norm -1.) Write $\mathfrak{b} \sim \mathfrak{c}$ for integral ideals of K lying in the same ideal class, and let:

$$L(s, \mathfrak{c}, \chi) = \sum_{\mathfrak{b}\sim\mathfrak{c}} \chi(\mathfrak{b})N(\mathfrak{b})^{-s}$$

We then have:

$$a_1(0, \mathfrak{a}) = L(1, \mathfrak{o}, \chi) + \bar{\chi}(\mathfrak{a}\mathfrak{d}^2)L(1, \mathfrak{a}\mathfrak{d}^2, \chi)$$

6.3 Constructing the Weight 1 Form

We fix $K = \mathbb{Q}(\sqrt{2869})$, $\mathfrak{o} = \mathfrak{o}_K$, and $k = 1$. We have $\mathfrak{d} = \sqrt{2868}\mathfrak{o}$, $h = 1$, and $h^+ = 2$. $\mathfrak{a}_1 = \mathfrak{o}$ and $\mathfrak{a}_2 = \mathfrak{p}_3$, a prime of norm 3 principally generated by an indefinite element, are a system of representatives of the narrow ideal class group. There is a unique Hecke character ψ satisfying the conditions above, and ψ^* is then the nontrivial character, i.e. $\psi^*(\xi\mathfrak{o}) = \operatorname{sgn}(N(\xi))$. We let $\chi(\mathfrak{p}) = \chi_\theta(\sigma_\mathfrak{p})$. Then the L-function associated to θ is given by the Euler product:

$$\prod_{\mathfrak{p}} \left(1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s} + \psi^*(\mathfrak{p})N(\mathfrak{p})^{-2s}\right)^{-1} = \sum_{\mathfrak{a}} C(\mathfrak{a}, \theta)N(\mathfrak{a})^{-s}$$

From this, we compute the coefficients $a_{j,\nu}$ of a pair of Fourier series $\mathbf{f}_\theta = (f_{\theta,1}, f_{\theta,2})$:

$$a_{j,\nu} = C(\nu\mathfrak{a}_j^{-1}, \theta)N(\mathfrak{a}_j)^{1/2}$$

where $a_{j,\nu}$ are the coefficients of $f_{\theta,j}$ and ν runs over totally positive elements of $\mathfrak{a}_j$.

Consider $G_1(z, \mathfrak{a}_i)$, the weight 1 Eisenstein series associated to each narrow ideal class. A quick computation shows that $G_1(z, \mathfrak{p}_3) = 0$. Thus, to follow the strategy outlined above, we can only work with modular forms on the group $\Gamma(\mathfrak{o})$. To simplify notation, we let $\Gamma = \Gamma(\mathfrak{o})$, f_θ be the first component of $\mathbf{f}_\theta$, and $G(z) = G_1(z, \mathfrak{o})$. We are then looking to find a form $f \in M_1(\Gamma)$ that agrees with f_θ for "enough" coefficients, and we obtain $\mathbf{f}$ as $(f, \lambda^{-1} f|T'(\mathfrak{p}_3))$, where λ is an appropriate nonzero constant (which, circularly defined, is the eigenvalue of $T'(\mathfrak{p}_3)$ acting on $\mathbf{f}$). However, first we need a lemma and a proposition:

Lemma 6.3.1. *Let L be an unramified extension of K. Then:*

1. *if L is a cyclic extension of K, then $L = K_1 = K(\sqrt{-19})$, and $G(L|K) \simeq C_2$;*
2. *if L is a dihedral extension of K, then L is the Hilbert class field of K_1 and $G(L|K) \simeq D_7$; and*
3. *L is not a tetrahedral or octahedral extension of K.*

Proof. We recall that K_1 is the narrow Hilbert class field of K. This immediately proves the first statement.

Suppose L is a dihedral extension of K, with $G(L|K) \simeq D_n$, $n \geq 2$. Since C_n is a subgroup of index 2 in D_n, there is a quadratic subextension of $L|K$. Since $L|K$ is unramified, the quadratic subextension must be K_1. We have $G(L|K_1) \simeq C_n$, and so L is contained in the Hilbert class field of K_1. Since K_1 is totally complex and $h(K_1) = 7$, L must be the Hilbert class field of K_1, and $n = 7$.

Suppose L is tetrahedral or octahedral. In the former case, $G(L|K) \simeq A_4$ contains a normal subgroup of index 3, and so K must have an abelian extension of degree 3, contradicting that $h^+(K) = 2$. In the latter case, $G(L|K) \simeq S_4$ contains A_4 as a subgroup of index 2. Thus, as in the dihedral case, $K_1|K$ must be a subextension of $L|K$, with $G(L|K_1) \simeq A_4$. However, this implies that K_1 has an abelian extension of degree 3, contradicting that $h(K_1) = 7$. □

We apply the lemma when studying eigenvalues of the weight 1 form we construct. Let K_2 denote the Hilbert class field of K_1. Since $H^2(C_2, \mathbb{C}^\times)$ and $H^2(D_7, \mathbb{C}^\times)$ are trivial, any projective representation on either group lifts to a linear representation. Thus, any odd, unramified cyclic or dihedral representations of G_K are twists of odd, degree 2 representations of $G(K_1|K)$ or $G(K_2|K)$ by even, unramified characters on G_K. However, all unramified characters of G_K factor through $G(K_1|K)$, and the nontrivial character is odd. So the odd, unramified cyclic and dihedral representations of G_K are precisely the odd, degree 2 representations of $G(K_1|K)$ and $G(K_2|K)$. The possible traces of Frobenius coming from these representations are 0, 2, and the roots of the irreducible polynomial $X^3 + X^2 - 2X - 1$, which generates the cubic subextension of the cyclotomic field $\mathbb{Q}(\zeta_7)$. If we show the existence of an eigenvalue which is not listed here, it must come from an icosahedral representation.

The following result gives a simple condition to show that a representation is equal to one of the representations we constructed. We note that we originally planned to use an effective version of the Chebotarev Density Theorem ([1]), but that approach did not take advantage of the specific structure of the number fields with which we are working. As such, we would have had to compute traces at Frobenius for a very large set of primes, while the proposition states that we need only check the traces at two primes. Although we do not need the Chebotarev-inspired approach, we discuss in Appendix A some results that tailor the effective theorem to our scenario and that are interesting in their own right.

Proposition 6.3.2. *Let θ' be an icosahedral representation of G_K with trivial conductor such that $C(\mathfrak{p}, \theta') = C(\mathfrak{p}, \theta)$ for the primes $\mathfrak{p}$ of K lying over 2 and 17, where θ is one of the representations we have constructed. Then $\theta' = \theta$.*

Proof. First, suppose that the projective kernel L' of θ' is Galois over $\mathbb{Q}$. Since L' is unramified over K, it must be the splitting field of a quintic polynomial of discriminant

2869. However, tables of number fields computed by Klünews and Malle ([19]) show that, up to isomorphism, there is only one degree 5 extension of $\mathbb{Q}$ of discriminant 2869, namely a root field of $X^5 - X - 1$. Thus, $L' = L$, and so θ' must be one of the four representations we constructed.

We now assume that L' is not Galois over $\mathbb{Q}$. Let L'' be the conjugate of L' over $\mathbb{Q}$, i.e. the fixed field of the conjugate of $G_{L'}$ in $G_{\mathbb{Q}}$. $L' \cap L''$ is a Galois subextension of $L'|\mathbb{Q}$, and $G(L' \cap L''|K)$ is a quotient of $G(L'|K) \simeq A_5$. The quotient is either A_5 or 1, so either $L' \cap L'' = L'$ or K. By assumption, L' is not Galois over $\mathbb{Q}$, so $L' \cap L'' = K$. This implies that $M = L'L''$ has Galois group $G(M|K) \simeq A_5 \times A_5$.

M is Galois over $\mathbb{Q}$, and $G(M|\mathbb{Q})$ is a group of order 7,200 with normal subgroup $A_5 \times A_5$. It is immediate from the definition of M that $K|\mathbb{Q}$ is the unique proper Galois subextension of $M|\mathbb{Q}$, and this implies that $A_5 \times A_5$ is the unique nontrivial normal subgroup of $G(M|\mathbb{Q})$.

Consider the map $c : G(M|\mathbb{Q}) \to \mathrm{Aut}(G(M|K))$ given by $[c(\sigma)](\tau) = \sigma\tau\sigma^{-1}$. For $\sigma \notin G(M|K)$, we obtain $G(M|\mathbb{Q})$ as the homomorphic image of the semi direct product:

$$G(M|K) \rtimes_c \langle\sigma\rangle$$

via the map $(\tau, \sigma) \mapsto \tau\sigma$. It is clear that σ has even order, and so we can conduct a coarse search for the correct structure of $G(M|\mathbb{Q})$ by considering all semidirect products:

$$(A_5 \times A_5) \rtimes_\phi C_{2m}, \quad \phi : C_{2m} \to \mathrm{Aut}(A_5 \times A_5)$$

and finding all quotients of order 7,200. This is good enough to uniquely identify the structure of $G(M|\mathbb{Q})$, as only one such group has $A_5 \times A_5$ as its unique nontrivial normal subgroup. This can be realized by letting $m = 1$ and $[\phi(g)](\tau_1, \tau_2) = (\tau_2, \tau_1)$, where g is the generator of C_2. We let $S = (A_5 \times A_5) \rtimes_\phi C_2$, and we identify S with $G(M|\mathbb{Q})$.

S has a unique (up to conjugation) maximal subgroup S_0 of order 120 and isomorphic to $A_5 \times C_2$. Let F be the fixed field of S_0; F is a degree 60 extension of $\mathbb{Q}$. By considering the possible decomposition groups for 19 and 151 in S, namely particular subgroups of S isomorphic to $C_m \times C_2$, $m = 1, 2, 3, 5$, we find that the maximum possible absolute discriminant $|d_{F|\mathbb{Q}}|$ is 2869^{22}. A similar analysis shows that F has 4 real embeddings and, thus, 28 (pairs of conjugate) complex embeddings. Given the assumption that $\chi_{\theta'}$ agrees with χ_θ at the primes over $p = 2, 17$, we can identify the conjugacy classes of σ_p in S. This allows us to determine the splitting behavior of p:

- 2 splits into the product of 1 prime with residue degree $f = 1$, 1 prime with $f = 2$, 5 primes with $f = 3$, and 7 primes with $f = 6$; and
- 17 splits into the product of 3 primes with $f = 1$ and 19 primes with $f = 3$.

We can also show that 19 (and 151) must split in one of the following ways:

- 38 primes with $f = 1$ (22 ramified);
- 4 primes with $f = 1$ (all unramified) and 20 primes with $f = 2$ (2 ramified);
- 2 primes with $f = 1$ (one ramified) and 12 primes with $f = 3$ (7 ramified); or
- 3 primes with $f = 1$ (2 ramified) and 7 primes with $f = 5$ (4 ramified).

We now introduce a discriminant bound developed by Poitou ([24, 25]). Let H be an extension of degree n over $\mathbb{Q}$ with r_1 real embeddings, y be a real parameter, and:

$$L(y) = -\frac{3}{20y^2} + \frac{33}{10y} + 2 + \left(\frac{3}{80y^3} + \frac{3}{4y^2}\right)\log(1+4y) - \left(\frac{3}{y} + \frac{12}{5}\right)\frac{1}{\sqrt{y}}\arctan(2\sqrt{y})$$

$$L_1(y) = \sum_{i=0}^{\infty} \frac{1}{2i+1} L\left(\frac{y}{(2i+1)^2}\right) + \frac{r_1}{n}\sum_{i=1}^{\infty}\frac{(-1)^{i+1}}{i} L\left(\frac{y}{i^2}\right)$$

$$f(x) = \left(\frac{3}{x^3}(\sin(x) - x\cos(x))\right)^2$$

Then we have a lower bound for the (log of the root) discriminant:

$$\frac{1}{n}\log|d_{H|\mathbb{Q}}| \geq \gamma + \log(4\pi) + \frac{r_1}{n} - \frac{12\pi}{5n\sqrt{y}} - L_1(y) + \frac{4}{n}\sum_{m;\ \mathfrak{p}} \frac{\log N\mathfrak{p}}{1+N\mathfrak{p}^m} f(\sqrt{y}\log N\mathfrak{p}^m)$$

where the sum is over all positive integers m and primes $\mathfrak{p}$ of H. Ignoring the sum over primes, the optimal choice of y is given by:

$$y = \left(\frac{3\pi}{2(n\lambda_3 + r_1\eta_2)}\right)^{2/3} \quad \text{for} \quad n\lambda_3 + r_1\eta_2 \geq 12\pi$$

where:

$$\lambda_3 = \frac{7}{8}\zeta(3)$$
$$\eta_2 = \frac{1}{2}\zeta(2)$$

We let $H = F$, $n = 60$, and $r_1 = 4$, and we maximize $|d_{F|\mathbb{Q}}|$ by 2869^{22}. Subtracting all terms except for the sum over primes to the left side, we have:

$$0.178879\ldots \geq \frac{4}{n}\sum_{m;\ \mathfrak{p}} \frac{\log N\mathfrak{p}}{1+N\mathfrak{p}^m} f(\sqrt{y}\log N\mathfrak{p}^m)$$

Restricting the sum on the right to the primes over 2 and 17, we have:

$$\frac{4}{n}\sum_{m;\ \mathfrak{p}|2,17} \frac{\log N\mathfrak{p}}{1+N\mathfrak{p}^m} f(\sqrt{y}\log N\mathfrak{p}^m) = 0.167052\ldots$$

while the sum over the primes dividing 19 is minimized when 19 splits into primes of residue degree 1 and 2:

$$\frac{4}{n}\sum_{m;\ \mathfrak{p}|19} \frac{\log N\mathfrak{p}}{1+N\mathfrak{p}^m} f(\sqrt{y}\log N\mathfrak{p}^m) \geq 0.014807\ldots$$

Thus:

$$\frac{4}{n}\sum_{m;\ \mathfrak{p}} \frac{\log N\mathfrak{p}}{1+N\mathfrak{p}^m} f(\sqrt{y}\log N\mathfrak{p}^m) \geq 0.181859\ldots$$

which is the desired contradiction. Thus, L' must be Galois over $\mathbb{Q}$, and $\theta' = \theta$.

□

The proof of the main result hinges on showing that two weight 4 forms on Γ constructed from the representation and the Eisenstein series are equal. The mechanics of the computation are simple: we need to be able to compute Fourier coefficients for products of forms and for the eigenbasis of weight 2 forms. However, the sheer number of coefficients that need to be computed to verify that the weight 4 forms are equal makes the process very time-intensive.

We considered two ways of determining how many coefficients needed to be checked to show equality. The first approach was the application of Sturm bounds for Hilbert modular forms developed by Gil and Pacetti (work in progress; example in [11]). Pacetti performed computations for us giving a set of indices such that two weight 4 on forms on Γ whose coefficients agree on these indices must be equal. This type of bound is useful in that Hecke operators and eigenvalues do not need to be computed in order to determine the set. However, the set contained millions of indices, presenting an infeasible computation.

The second and successful approach was to find a set of primes of K such the Hecke operators at these primes give a basis for the Hecke algebra on $M_4(K_0)$. Although this is an obvious approach, it is a time-consuming process for MAGMA to generate matrices representing the action of Hecke operators on a basis of a space of Hilbert modular forms. However, these computations are performed by considering matrices of the Hecke operators acting on a larger, auxiliary vector space, and computing these matrices is a much faster process. It then suffices to find a basis for the Hecke algebra on this space. We can then check that the two weight 4 have the same Fourier coefficients at these primes to show that they are equal. This approach required the computation of only tens of thousands of Fourier coefficients, a process which took around 50 hours.

Proposition 6.3.3. *The series $\mathbf{f}_\theta$ obtained from the representation θ is the Fourier series of a weight* 1 *Hilbert modular form of full level.*

Proof. Consider the series $f_\theta G$ and f_θ^2. $S_2(K_0)$ has dimension 319; find the Hecke eigenbasis $\{\mathbf{f}_1, \dots, \mathbf{f}_{319}\}$ and a set $\mathcal{P} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{319}\}$ of primes of K such that the matrix:

$$(C(\mathfrak{p}_j, \mathbf{f}_i))_{1 \le i,j \le 319}$$

has full rank. Both can be computed in MAGMA. Let $\mathbf{g}$ and $\mathbf{h}$ be the forms in $S_2(K_0)$ that agree with $(f_\theta G, 0)$ and $(f_\theta^2, 0)$, respectively, on $C(\mathfrak{p}, \cdot)$ for $\mathfrak{p} \in \mathcal{P}$. It is immediate that $\mathbf{g} = (g, 0)$ and $\mathbf{h} = (h, 0)$ for forms $g, h \in M_2(\Gamma)$.

Now consider the forms g^2 and hG^2 in $S_4(\Gamma)$, which has dimension 2,733. Let $\mathcal{Q}$ be a set of primes such that the Hecke operators $T'(\mathfrak{p})$, $\mathfrak{p} \in \mathcal{Q}$, on $S_4(K_0)$ that span the full Hecke algebra on $S_4(K_0)$. Then two forms on $S_4(K_0)$ are equal if and only if they agree on $C(\mathfrak{p}, \cdot)$ for all $\mathfrak{p} \in \mathcal{Q}$. Computations in MAGMA provide such a set $\mathcal{Q}$ (`http://math.rutgers.edu/~jbryk/5wt4code.txt`) and verify that $(g^2, 0) = (hG^2, 0)$ in $M_4(K_0)$. In particular, $g^2 = hG^2$ in $S_4(\Gamma)$.

Let:

$$f = \frac{g}{G}$$

We claim that $f \in S_1(\Gamma)$. That f is holomorphic on $\mathfrak{H}^2$ follows from the fact that:

$$f^2 = \frac{g^2}{G^2} = \frac{hG^2}{G^2} = h$$

is holomorphic. That f is automorphic of weight 1 on Γ and vanishes at the cusp follows from the fact that $g \in S_2(\Gamma)$ and $G \in M_1(\Gamma)$. Thus, the claim is clear.

Now we claim that $(f, 0)$ is an eigenform of $T'(\mathfrak{p}_3^2)$. This is true if for all $\mathfrak{p} \in \mathcal{P}$:

$$\sum_{\mathfrak{p}+\mathfrak{p}_3^2 \subset \mathfrak{a}} \psi^*(\mathfrak{a}) C(\mathfrak{a}^{-2}\mathfrak{p}\mathfrak{p}_3^2, (f, 0)) = C(\mathfrak{p}_3^2, (f, 0)) C(\mathfrak{p}, (f, 0))$$

This is trivially true for $\mathfrak{p}$ in the nontrivial narrow ideal class: the summands and $C(\mathfrak{p}, (f, 0))$ are equal to 0, as they are coefficients coming from the second component of $(f, 0)$. For $\mathfrak{p}$ in the trivial narrow ideal class, $\mathfrak{p} + \mathfrak{p}_3^2 = \mathfrak{o}$, so that we must show:

$$C(\mathfrak{p}\mathfrak{p}_3^2, (f, 0)) = C(\mathfrak{p}_3^2, (f, 0)) C(\mathfrak{p}, (f, 0))$$

In showing that $g^2 = hG^2$, it is also shown that:

$$C(\mathfrak{a}, (f, 0)) = C(\mathfrak{a}, \theta)$$

for all $\mathfrak{a}$ in the trivial narrow ideal class with $N(\mathfrak{a}) \leq 60{,}000$. The maximum of $N(\mathfrak{p})$ for $\mathfrak{p} \in \mathcal{P}$ is 3,467, and so $N(\mathfrak{p}\mathfrak{p}_3^2) \leq 31{,}203$ for all $\mathfrak{p} \in \mathcal{P}$. Thus, the identity we wish to show is equivalent to showing for all $\mathfrak{p} \in \mathcal{P}$:

$$C(\mathfrak{p}\mathfrak{p}_3^2, \theta) = C(\mathfrak{p}_3^2, \theta) C(\mathfrak{p}, \theta)$$

This follows immediately from the fact that these coefficients are obtained from an Euler product.

Letting $\lambda = C(\mathfrak{p}_3, \theta)$, it is immediate that from the previous paragraph that:

$$\mathbf{f} = \left(f, \lambda^{-1} f | T'(\mathfrak{p}_3)\right)$$

is an eigenform for $T'(\mathfrak{p}_3)$ with eigenvalue λ. We note that λ is a root of the irreducible polynomial $X^4 + 3X^2 + 1$, so it cannot correspond to a cyclic or dihedral representation.

Thus, it must come from an icosahedral representation, and $\mathbf{f}$ must be in a space spanned by icosahedral representations.

The same argument used to show that $(f, 0)$ is an eigenform for $T'(\mathfrak{p}_3^2)$ also shows that $\mathbf{f}$ is an eigenform for $T'(\mathfrak{p})$ for the primes $\mathfrak{p}$ lying over 2 and 17. Again, the common eigenspace for these operators (including the prime over 3) must be spanned by icosahedral representations. But Proposition 6.3.2 implies there is only one representation with these traces at Frobenius–namely, one of the representations θ we have constructed. Thus, the dimension of the space is 1, $\mathbf{f}$ is a Hecke eigenform, and it is equal to $\mathbf{f}_\theta$. □

We immediately have the two main results. Theorem 2.2.1 implies:

Corollary 6.3.4. *There is an icosahedral Hilbert modular form that does not arise from base change.*

Replacing traces at Frobenius with Hecke eigenvalues in Proposition 4.5.2 gives:

Proposition 6.3.5. *Let $f(X) = X^5 - X - 1$. There exist two Hilbert new forms $\mathbf{f}_i$ over K of weight 1 and full level and with Hecke eigenvalues $C(\nu, i) = C(\nu\mathfrak{o}_K, \mathbf{f}_i)$ such that for any rational prime p and any prime π of K dividing p:*

$$(\#\{x \ (mod\ p) : f(x) \equiv 0 \ (mod\ p)\})^2 = \left(C(\pi, 1)C(\pi, 2) + \left(\frac{2869}{p}\right)\right)^2$$

Appendix A

Bounding Degrees in Terms of Conductors

We originally considered using an effective version of the Chebotarev Density Theorem in order to show that two representations are equal–one of those that we constructed and the representation coming from the icosahedral form we produce. Although we abandoned this approach, the techniques we developed to apply the theorem to our scenario merit discussion. The effective Chebotarev theorem gives bounds depending on the degree of the fixed field of the kernels of the representation. We develop methods for bounding the degree of said field in terms of the conductors and degrees of the representations with the aim of getting bounds for the effective Chebotarev theorem that depend on the latter two pieces of information and not the former.

A.1 An Effective Chebotarev Density Theorem

Fix a number field K and an integer $n \geq 1$, and let $\rho, \rho' : G_K \to GL_n(\mathbb{C})$ be two Artin representations. The Chebotarev Density Theorem suggests a method for showing whether $\rho \simeq \rho'$. It suffices to show that the characters $\chi = \chi_\rho$ and $\chi' = \chi_{\rho'}$ are equal. Fix a field M such that both representations factor through $G(M|K)$, and let $c \subset G(M|K)$ be a conjugacy class. Then the Chebotrarev Density Theorem implies that there exists a prime $\mathfrak{p}$ of k such that $c = \mathrm{Frob}_\mathfrak{p}$. If $\chi(\mathrm{Frob}_\mathfrak{p}) = \chi'(\mathrm{Frob}_\mathfrak{p})$, where $\mathfrak{p}$ runs over a set of primes so that each conjugacy class is equal to some $\mathrm{Frob}_\mathfrak{p}$, then $\chi = \chi'$.

In our situation, we know that the conductors of ρ and ρ' divide some fixed ideal $\mathfrak{f}$ of K, and we can compute $\chi(\mathrm{Frob}_\mathfrak{p})$ and $\chi'(\mathrm{Frob}_\mathfrak{p})$ for any prime $\mathfrak{p}$ of K, perhaps lying outside some fixed finite subset of primes S. In order to make the above effective, it seems necessary to be able to find some constant $X = X(K, M, S)$ such that, for any conjugacy class $c \subset G(M|K)$, there is a prime $\mathfrak{p} \notin S$ such that $N(\mathfrak{p}) \leq X$ and $c = \mathrm{Frob}_{\mathfrak{p}}$.

Indeed, such effective versions of the Chebotarev Density Theorem do exist. Fix an integer $N \geq 1$. Let $d_{K|\mathbb{Q}}$ denote the discriminant of K over $\mathbb{Q}$ and, for a prime $\mathfrak{p}$ of K, let $p_{\mathfrak{p}}$ be the residue characteristic. Define:

$$\begin{aligned}
\Delta^*(K,S,N) &= |d_{K|\mathbb{Q}}|^N \left(N \cdot \prod_{\mathfrak{p}\in S} p_{\mathfrak{p}}^{1-1/N} \right)^{N\cdot[K:\mathbb{Q}]} \\
B_{\mathrm{LO}}(K,S,N) &= 70 \cdot (\log \Delta^*(K,S,N))^2 \\
B_{\mathrm{BS}}(K,S,N) &= (4 \log \Delta^*(K,S,N) + 2.5N \cdot [K:\mathbb{Q}] + 5)^2 \\
B_{\mathrm{GRH}}(K,S,N) &= \min\{B_{\mathrm{LO}}(K,S,N), B_{\mathrm{BS}}(K,S,N)\}
\end{aligned}$$

And, for an effective constant A given by Lagarias-Montgomery-Odlyzko, define:

$$B_{\mathrm{U}}(K,S,N) = \begin{cases} \Delta^*(K,S,N)^A & K \neq \mathbb{Q} \\ 2\Delta^*(K,S,N)^A & K = \mathbb{Q} \end{cases}$$

Then we have:

Lemma A.1.1 (Achter, [1, Lemma 1.1])**.** *Let K be a finite extension of $\mathbb{Q}$, and let S be a finite set of prime ideals of K. Let $M|K$ be a Galois extension with $[M:K] \leq N$ unramified outside S. For any class $c \subset G(M|K)$, there exists a prime $\mathfrak{p} \notin S$ of K such that $N(\mathfrak{p}) \leq B_{\mathrm{U}}(K,S,N)$ and $c = \mathrm{Frob}_{\mathfrak{p}}$. If the Generalized Riemann Hypothesis holds, we may then take $N(\mathfrak{p}) \leq B_{\mathrm{GRH}}(K,S,N)$.*

The following immediately follows by our discussion above.

Corollary A.1.2. *Let $\rho, \rho' : G_K \to GL_n(\mathbb{C})$ be two representations that factor through $G(M|K)$. If $\chi(\mathrm{Frob}_{\mathfrak{p}}) = \chi'(\mathrm{Frob}_{\mathfrak{p}})$ for all primes $\mathfrak{p} \notin S$ of K such that $N(\mathfrak{p}) \leq B_{\mathrm{U}}(K,S,N)$, then $\rho \simeq \rho'$. If the Generalized Riemann Hypothesis holds, we may then take $N(\mathfrak{p}) \leq B_{\mathrm{GRH}}(K,S,N)$.*

Our field M depends on the representations ρ and ρ'. We assume the only two conditions on these representations are that they have degree n and have conductor dividing $\mathfrak{f}$. In order to apply the above, we must be able to bound $[M:K]$ in terms of

n and $\mathfrak{f}$. We note here that if M is as small as possible, i.e. if M is the fixed field of the kernels of ρ and ρ', then M is only ramified at primes dividing $\mathfrak{f}$, so we may take S to be the set of primes dividing $\mathfrak{f}$.

A.2 Ramification Groups and Conductors

We introduce the notation for and some basic results about ramification groups and conductors of Artin representations. We follow the presentation given in [21]. Let $L|K$ be a Galois extension of number fields. Fix a prime $\mathfrak{p}$ of K and a prime $\mathfrak{P}$ of L such that $\mathfrak{P}|\mathfrak{p}$. Let e be the ramification degree of $\mathfrak{P}$ over $\mathfrak{p}$. If $v_{\mathfrak{p}}$ is the normalized valuation on the completion $K_{\mathfrak{p}}$, there is a unique extension w to the completion $L_{\mathfrak{P}}$; let $v_{\mathfrak{P}} = ew$, the associated normalized valuation on $L_{\mathfrak{P}}$.

A.2.1 Ramification Groups

Definition A.2.1. For every real number $s \geq -1$, the *s-th ramification group* of $L|K$ at $\mathfrak{P}$ is:

$$G_s = G_s(L|K) = \{\sigma \in G(L_{\mathfrak{P}}|K_{\mathfrak{p}}) : v_{\mathfrak{P}}(\sigma a - a) \geq s + 1 \text{ for all } a \in \mathcal{O}_{\mathfrak{P}}\}$$

Note. Viewing $G(L_{\mathfrak{P}}|K_{\mathfrak{p}})$ as the decomposition group $D_{\mathfrak{P}}$ in $G(L|K)$, we have $G_{-1} = G(L_{\mathfrak{P}}|K_{\mathfrak{p}}) = D_{\mathfrak{P}}$ and $G_0 = I_{\mathfrak{P}}$, the inertia group.

Now let E be an intermediate Galois extension of $L|K$, and let $\mathfrak{P}' = \mathfrak{P} \cap E$. There is a natural relationship between the groups $G_s(L|K)$ and $G_s(L|E)$.

Proposition A.2.1 (Neukirch, Ch. II §10). *For all $s \geq -1$:*

$$G_s(L|E) = G_s(L|K) \cap G(L|E)$$

The relationship between the ramification groups for $L|K$ and $E|K$ is more subtle. Although the image of a ramification group of $G(L|K)$ in $G(E|K)$ is itself a ramification group, the indices do not always match. Instead, we have an explicit formula due to Herbrand. We introduce the function $\eta_{L|K} : [-1, \infty) \to [-1, \infty)$, defined by:

$$t = \eta_{L|K}(s) = \int_0^s \frac{dx}{[G_0(L|K) : G_x(L|K)]}$$

By convention, we set $[G_0 : G_{-1}] = [G_{-1} : G_0]^{-1}$; note that $G_x = G_0$ for $-1 < x \leq 0$. If we define the quantities:

$$g_i(L|K) = |G_i(L|K)|$$

we can express the function as:

$$\eta_{L|K}(s) = \sum_{i=1}^{[s]} \frac{g_i}{g_0} + \frac{\{s\} g_{[s]+1}}{g_0}$$

where $[s]$ is the greatest integer less than or equal to s and $\{s\} = s - [s]$ is the fractional part of s.

We then have:

Theorem A.2.2 (Herbrand)**.** *Let $E|K$ be a Galois subextension of $L|K$. Then one has for $s \geq -1$ and $t = \eta_{L|E}(s)$:*

$$G_s(L|K)G(L|E)/G(L|E) = G_t(E|K)$$

Note. If we introduce the **upper numbering** for $t = \eta_{L|K}(s)$:

$$G^t(L|K) = G_s(L|K)$$

Then the above theorem can be reformulated as:

$$G^t(L|K)G(L|E)/G(L|E) = G^t(E|K)$$

A.2.2 Artin Conductors

Now we define the Artin conductor of a representation and recall some basic facts. Let $L|K$ a Galois extension of number fields, and let (ρ, V) be an Artin representation of $G(L|K)$ with character χ. For the time being, fix a prime $\mathfrak{p}$ of K and a prime $\mathfrak{P}$ of L such that $\mathfrak{P}|\mathfrak{p}$.

Define:

$$f(\chi) = \sum_{i \geq 0} \frac{g_i(L|K)}{g_0(L|K)} \operatorname{codim} V^{G_i(L|K)}$$

If χ is of degree 1, let j be the biggest integer such that $\chi|_{G_j}$ is not the trivial character (where we put $j = -1$ if χ is the trivial character). Then it can be shown that:

$$f(\chi) = \eta_{L|K}(j) + 1$$

A theorem due to Hasse and Arf implies that $\eta_{L|K}(j) \geq -1$ is an integer, and so $f(\chi) \geq 0$ is an integer. An application of Brauer's theorem then shows that, for arbitrary characters χ, $f(\chi)$ is a nonnegative integer. Thus the following definitions make sense.

Definition A.2.2. The *local Artin conductor* of χ at $\mathfrak{p}$ is the ideal:

$$\mathfrak{f}_{\mathfrak{p}}(\chi) = \mathfrak{p}^{f(\chi)}$$

The *global Artin conductor* of χ is the ideal:

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p} \text{ finite}} \mathfrak{f}_{\mathfrak{p}}(\chi)$$

Note that if ρ is a faithful representation of $G(L|K)$, then a prime $\mathfrak{p}$ divides $\mathfrak{f}(\chi)$ if and only if $\mathfrak{p}$ ramifies in L. Indeed, that $\mathfrak{p}$ does not ramify is equivalent to $G_0(L|K)$ being trivial for $\mathfrak{p}$. Since ρ is faithful, this is equivalent to $V^{G_0(L|K)} = V$. Since $V^{G_0(L|K)} \subset V^{G_i(L|K)}$ for all $i \geq 0$, we have that $V^{G_0(L|K)} = V$ if and only if $V^{G_i(L|K)} = V$ for all $i \geq 0$. The exponent $f(\chi)$ is 0 precisely when $\operatorname{codim} V^{G_i(L|K)} = 0$ for all $i \geq 0$.

We only need two facts regarding the Artin conductor. First:

Proposition A.2.3 (Neukirch, Ch. VII §11)**.** *If $E|K$ is a Galois subextension of $L|K$ and χ is a character of $G(E|K)$, then:*

$$\mathfrak{f}(L|K, \chi) = \mathfrak{f}(E|K, \chi)$$

For the second fact, we recall a few notions from class field theory. We follow the conventions of Neukirch. Let $\mathfrak{f}$ be an ideal of K, let $J^{\mathfrak{f}}$ be the group of fractional ideals of K prime to $\mathfrak{f}$, and let $P^{\mathfrak{f}}$ be the group of principal ideals of K generated by a such that $a \equiv 1 \bmod \mathfrak{f}$ and a is positive at all real places of K. Then there exists a finite abelian extension $K^{\mathfrak{f}}$ of K called the *ray class field* modulo $\mathfrak{f}$ such that:

$$J^{\mathfrak{f}}/P^{\mathfrak{f}} \simeq G(K^{\mathfrak{f}}|K)$$

where the isomorphism is given by the Artin symbol $(\frac{K^{\mathfrak{f}}|K}{\cdot})$.

For an arbitrary abelian extension L of K, we define the class field theoretic *conductor* of L to be the smallest ideal $\mathfrak{f}$ such that $L \subset K^{\mathfrak{f}}$. We then have:

Proposition A.2.4. *Let $L|K$ be a Galois extension of number fields, χ a degree 1 character of $G(L|K)$, L_χ the fixed field of $\ker(\chi)$, and $\mathfrak{f}$ the conductor of $L_\chi|K$. Then:*

$$\mathfrak{f} = \mathfrak{f}(\chi)$$

A.3 Bounds on the Degree of the Fixed Field of an Artin Representation

We fix a number field K, an integer n, an ideal $\mathfrak{n}$ of K, and a representation $\rho : G_K \to GL_n(\mathbb{C})$ of conductor dividing $\mathfrak{n}$. We will develop some general methods for bounding the degree of certain extensions of K fixed by the kernel of ρ. In the case $n = 2$, we will further show that the degree of the fixed field of the kernel of ρ is bounded in terms of K and $\mathfrak{n}$.

First, we fix notation:

- V, the vector space associated to ρ;
- $\chi = \chi_\rho$;
- $\epsilon = \det(\rho)$;
- M, the fixed field of $\ker(\rho)$;
- L, the fixed field of $\ker(\bar{\rho})$; and
- K_1, the fixed field of $\ker(\epsilon)$.

We are also interested in the field $L_1 = LK_1$, which is the fixed field of the group:

$$\ker(\bar{\rho}) \cap \ker(\epsilon) = \{\sigma \in G_k : \rho(\sigma) = \zeta I_n, \zeta^n = 1\}$$

Now we describe the general strategy to bound the degree $[M : K]$. The extensions $M|L_1$ and $K_1|K$ are abelian. The former is easily shown to have degree at most n, while we can use the conductor of ρ to bound the conductor of $F|k$ and hence the degree, too.

The most difficult part is bounding the degree of $L_1|K_1$. We note that $G(L_1|K_1)$ is a finite subgroup of $PGL_n(\mathbb{C})$. In certain cases, we have explicit descriptions of these subgroups. For example, for $n = 2$, such subgroups are either in one of two infinite families of solvable groups, or they are isomorphic to one of three "exceptional" groups (two of which are also solvable). For solvable groups, the techniques used to bound the degree of $K_1|K$ can be modified to find bounds for the degree of $L_1|K_1$, namely we break the extension up into a chain of abelian extensions and estimate the conductor of each extension using the conductor of ρ.

We begin with the simple:

Lemma A.3.1. *$[M : L_1] \leq n$.*

Proof. $G(M|L_1)$ is isomorphic to the image of $\ker(\bar{\rho}) \cap \ker(\epsilon)$ in $GL_n(\mathbb{C})$. The image is contained inside the group $\{\zeta I_n : \zeta^n = 1\}$, which has order n. □

We next bound the conductor of $K_1|K$ in terms of the conductor of $\mathfrak{f}(\chi)$. We prove a more general lemma about cyclic subextensions $E|K$ of $M|K$.

Lemma A.3.2. *Let $E|K$ be a cyclic subextension of $M|K$. Then $\mathfrak{f}(E|K)$ divides $\mathfrak{f}(M|L, \chi)$.*

Proof. Proposition A.2.4 implies that $\mathfrak{f}(E|K) = \mathfrak{f}(E|K, \psi)$, where ψ is any faithful character of $G(E|K)$. Proposition A.2.3 implies that $\mathfrak{f}(M|K, \psi) = \mathfrak{f}(E|K, \psi)$, so we need to show that $\mathfrak{f}(M|K, \psi)$ divides $\mathfrak{f}(M|K, \chi)$.

Fix a prime $\mathfrak{p}$ of K, and let $f(\psi) = v_{\mathfrak{p}}(\mathfrak{f}(M|K, \psi))$ and $f(\chi) = v_{\mathfrak{p}}(\mathfrak{f}(M|K, \chi))$. The statement of the lemma is equivalent to showing that $f(\psi) \leq f(\chi)$ for each prime $\mathfrak{p}$.

By definition:

$$f(\psi) = \sum_{i=0}^{\infty} \frac{g_i(M|K)}{g_0(M|K)} \operatorname{codim} \mathbb{C}^{G_i(M|K)}$$

If $\operatorname{codim} \mathbb{C}^{G_i(M|K)} = 1$ for some i, then $G_i(M|K)$ is not contained in the kernel of ψ, and so $G_i(M|K)$ contains more than one element. Since ρ is a faithful representation of $G(M|K)$, this implies $\operatorname{codim} V^{G_i(M|K)} \geq 1$. So:

$$f(\psi) = \sum_{i=0}^{\infty} \frac{g_i(M|K)}{g_0(M|K)} \operatorname{codim} \mathbb{C}^{G_i(M|K)} \leq \sum_{i=0}^{\infty} \frac{g_i(M|K)}{g_0(M|K)} \operatorname{codim} V^{G_i(M|K)} = f(\chi)$$

□

Corollary A.3.3. *Let $E|K$ be a cyclic subextension of $M|K$. Then $[E:K] \leq [K^{\mathfrak{f}(\chi)}:K]$.*

Proof. Since the conductor of E divides $\mathfrak{f}(\chi)$, E is contained in $K^{\mathfrak{f}(\chi)}$. □

We note that it is easier to bound $[K_1:K]$ if we have an explicit description of ϵ.

It is a more delicate matter to bound the degrees $[L_1:K_1]$ or $[L:K]$. Doing so requires having a decent understanding of the structure of $G(L|K)$, which is a finite subgroups of $PGL_n(\mathbb{C})$. When $n=2$, we know that the possibilities for $G(L|K)$ are the cyclic groups C_n, the dihedral groups D_n, and three "exceptional" groups A_4, S_4, and A_5. Thus the only trouble is bounding the order of the first two possibilities.

Corollary A.3.3 can be applied to the cyclic case. For the dihedral case (and for more general solvable groups) we need the following lemma.

Lemma A.3.4. *Let $E|K$ be a subextension of $M|K$, and view χ as a character on $G(M|E)$. Then $\mathfrak{f}(M|E,\chi)$ divides $\mathfrak{f}(M|K,\chi)$, where we view both conductors as ideals in E.*

Proof. Fix a prime $\mathfrak{p}$ of K and a prime $\mathfrak{P}$ of E dividing $\mathfrak{p}$. Let $e = e(\mathfrak{P}|\mathfrak{p})$ be the ramification degree of $\mathfrak{P}$ over $\mathfrak{p}$, and let $f_{\mathfrak{p}} = v_{\mathfrak{p}}(\mathfrak{f}(M|K,\chi))$ and $f_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{f}(M|E,\chi))$. The statement of the lemma is equivalent to showing $f_{\mathfrak{P}} \leq ef_{\mathfrak{p}}$ for each prime $\mathfrak{p}$ of K and each prime $\mathfrak{P}$ of E lying over $\mathfrak{p}$.

Let $s \geq 0$ be an integer, and let $t = \eta_{M|E}(s)$. Then Theorem A.2.2 implies:

$$G_s(M|K)G(M|E)/G(M|E) = G_t(E|K)$$

which can be restated via Proposition A.2 as:

$$G_s(M|K)/G_s(M|E) = G_t(E|K)$$

This gives the equality:

$$\frac{g_s(M|K)}{g_s(M|E)} = g_t(E|K) \tag{A.1}$$

In particular, when $s=0$, it is clear from the definition of $\eta_{L|M}$ that $t=0$, so that:

$$\frac{g_0(M|K)}{g_0(M|E)} = g_0(E|K) \tag{A.2}$$

Dividing A.2 by A.1, we have:

$$\begin{aligned}
\frac{g_0(M|K)g_s(M|E)}{g_0(M|E)g_s(M|K)} &= \frac{g_0(E|K)}{g_t(E|K)} \\
\Rightarrow \frac{g_s(M|E)}{g_0(M|E)} &= \frac{g_s(M|K)}{g_0(M|K)} \cdot \frac{g_0(E|K)}{g_t(E|K)}
\end{aligned}$$

Finally, noting that $g_0(E|K) = e$, we have:

$$\frac{g_s(M|E)}{g_0(M|E)} = \frac{g_s(M|K)}{g_0(M|K)} \cdot \frac{g_0(E|K)}{g_t(E|K)} \leq \frac{g_s(M|K)}{g_0(M|K)} \cdot e$$

We apply the above to:

$$\begin{aligned}
f_{\mathfrak{P}} &= \sum_{i\geq 0} \frac{g_i(M|E)}{g_0(M|E)} \operatorname{codim} V^{G_i(M|E)} \\
&\leq e \cdot \sum_{i\geq 0} \frac{g_i(M|K)}{g_0(M|K)} \operatorname{codim} V^{G_i(M|E)}
\end{aligned}$$

We trivially have that $\operatorname{codim} V^{G_i(M|E)} \leq \operatorname{codim} V^{G_i(M|K)}$, and so we obtain the desired inequality:

$$\begin{aligned}
f_{\mathfrak{P}} &\leq e \cdot \sum_{i\geq 0} \frac{g_i(M|K)}{g_0(M|K)} \operatorname{codim} V^{G_i(M|E)} \\
&\leq e \cdot \sum_{i\geq 0} \frac{g_i(M|K)}{g_0(M|K)} \operatorname{codim} V^{G_i(M|K)} \\
&= e f_{\mathfrak{p}}
\end{aligned}$$

□

We now restrict ourselves to the case $n = 2$. The method of proof for the dihedral case should be easy to generalize to cases where $G(M|K)$ is known to be solvable and has a composition series of some bounded length.

Proposition A.3.5. *Let:*

$$B_{\mathfrak{f}} = \max\{[E^{\mathfrak{f}} : E] : E|K \textit{ is a quadratic subextension of } K^{\mathfrak{f}}|K\}$$

Then:

$$[M : K] \leq 2\max\{B_{\mathfrak{f}}, 60\}[K^{\mathfrak{f}} : K]$$

Proof. We break our analysis into three cases depending on the structure of $G(M|K)$. We fix $\mathfrak{f} = \mathfrak{f}(M|K, \chi)$, and we recall that Lemma A.3.1 implies that $[L_1 : K_1] \leq 2$.

i. $G(L|K)$ cyclic: Lemma A.3.2 implies that $L, K_1 \subset K^{\mathfrak{f}}$, whence $[L_1 : K] \leq [K^{\mathfrak{f}} : K]$. So:

$$[M : K] \leq 2[K^{\mathfrak{f}} : K]$$

ii. $G(K|k)$ dihedral: Let $E|K$ be the subextension of $L|K$ such that $G(L|E)$ is the cyclic subgroup of index 2 in $G(L|K)$. $[E : K] = 2$ and $E \subset K^{\mathfrak{f}}$.

Lemma A.3.4 implies that $\mathfrak{f}(M|E, \chi)$ divides $\mathfrak{f}$. Since $L|E$ is cyclic, Lemma A.3.2 implies that $\mathfrak{f}(L|E)$ divides $\mathfrak{f}(M|E, \chi)$ and hence $\mathfrak{f}$. Thus $L \subset E^{\mathfrak{f}}$. Thus we have $[L : E] \leq B_{\mathfrak{f}}$.

Lemma A.3.2 also implies that $E, K_1 \subset K^{\mathfrak{f}}$, and so $[EK_1 : K] \leq [K^{\mathfrak{f}} : K]$, while $[L_1 : EL_1] \leq [L : E] \leq B_{\mathfrak{f}}$. Combined with $[M : L_1] \leq 2$, we have:

$$[M : K] \leq 2B_{\mathfrak{f}}[K^{\mathfrak{f}} : K]$$

iii. $G(L|K)$ is "exceptional": $G(L|K)$ is one of three groups of order at most 60. Thus $[L_1 : K_1] \leq [L : K] \leq 60$. Lemma A.3.2 implies $K_1 \subset K^{\mathfrak{f}}$, and so $[K_1 : K] \leq [K^{\mathfrak{f}} : K]$. We thus have:

$$[M : K] \leq 120[K^{\mathfrak{f}} : K]$$

□

If ρ, ρ' are two representations of G_K with M, M' the fixed fields of the kernels, we can apply the effective Chebotarev theorem to the extension $MM'|k$. If ρ, ρ' have conductors dividing some ideal $\mathfrak{f}$, then a crude estimate gives $[MM' : k] \leq 4\max\{B_{\mathfrak{f}}, 60\}^2[K^{\mathfrak{f}} : K]^2$. However, we can do better by mimicking the ideas of the proof of Proposition A.3.5.

Appendix B

Miscellaneous Proofs

B.1 Proof of Lemma 2.3.1

Lemma B.1.1. *The Galois embedding problem:*

$$1 \to A \to G' \to G(L|K) \to 1$$

corresponding to the cocycle $c \in H^2(G(L|K), A)$ is solvable if and only if the image $\pi^*(c)$ of c in $H^2(G_K, A)$ is trivial.

Proof. We let $G = G(L|K)$. Suppose the image of c in $H^2(G_K, A)$ is trivial. Then we have the commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d] & G_K \times A \arrow[r] \arrow[d] & G_K \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & A \arrow[r] & G' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

The natural inclusion of G_K into $G_K \times A$ composed with the map from $G_K \times A$ to G' then gives the desired map $\psi : G_K \to G'$.

Conversely, suppose that the Galois embedding problem is solvable, so that there exists $\psi : G_K \to G'$ such that $\phi \circ \psi = \pi$. Let $s : G \to G'$ be a section of ϕ, so that $\phi \circ s = \mathbf{1}_G$. We may assume that for $\sigma, \tau \in G$:

$$c(\sigma, \tau) = s(\sigma)s(\tau)s(\sigma\tau)^{-1}$$

Therefore the image of c in $H^2(G_K, A)$ is given by the map for $\sigma, \tau \in G_K$:

$$\pi^*(c) = (s \circ \pi)(\sigma)(s \circ \pi)(\tau)(s \circ \pi)(\sigma\tau)^{-1}$$

Now we compare the maps ψ and $s \circ \pi$ from G_K to G'. Note that $\phi \circ (s \circ \pi) = \pi = \phi \circ \psi$ so that, for any $\sigma \in G_K$, $s \circ \pi(\sigma) \equiv \psi(\sigma) \pmod{A}$. Define $y : G_K \to A$ by $y(\sigma) = (s \circ \pi(\sigma))\psi(\sigma)^{-1}$. Then:

$$\begin{aligned} \pi^*(c)(\sigma, \tau) &= (s \circ \pi)(\sigma)(s \circ \pi)(\tau)(s \circ \pi)(\sigma\tau)^{-1} \\ &= \psi(\sigma)y(\sigma)\psi(\tau)y(\tau)\psi(\sigma\tau)^{-1}y(\sigma\tau)^{-1} \\ &= y(\sigma)y(\tau)y(\sigma\tau)^{-1} \end{aligned}$$

Thus the $\pi^*(c)$ is a coboundary. □

B.2 Proof of Proposition 3.5.1

We prove a slightly more general fact:

Proposition B.2.1. *Let $L|K$ be a Galois extension, $G(L|K) \simeq G$ a subgroup of S_n, and $\tilde{G}$ the preimage of G in $\tilde{S}_n$. Let $\gamma \in L$ be such that $M = L(\sqrt{\gamma})$ is a solution to the Galois embedding problem $1 \to C_2 \to \tilde{G} \to G(L|K) \to 1$. Then:*

i. For any $\sigma \in G(L|K)$, there exists $b_\sigma \in L^\times$ such that $\gamma^{\sigma-1} = b_\sigma^2$, and the cocycle corresponding to the embedding problem is $c(\sigma, \tau) = b_\sigma^\tau b_\tau b_{\sigma\tau}^{-1}$.

ii. All solutions to the embedding problem are given by $k\ell^2\gamma$, $k \in K^\times$ and $\ell \in L^\times$.

Proof. We identify $G(L|K)$ with the group G and $G(M|K)$ with the group $\tilde{G}$. We first show that given γ providing a solution to the embedding problem and all $\sigma \in G$, we have $\gamma^{\sigma-1} \in (L^\times)^2$. Indeed, if σ' is a preimage of σ in $\tilde{G}$, then $(\sqrt{\gamma})^{\sigma'}$ is a square root of γ^σ. There exist $a, b \in L$ such that:

$$(\sqrt{\gamma})^{\sigma'} = a + b\sqrt{\gamma}$$

Squaring both sides, we have:

$$\gamma^\sigma = a^2 + b^2\gamma + 2ab\sqrt{\gamma}$$

which implies that $2ab = 0$. If $b = 0$, then $\gamma^\sigma = a^2$, which implies that $\gamma = (a^{\sigma^{-1}})^2$, a contradiction to $\gamma \notin (L^\times)^2$. So $a = 0$, and:

$$\gamma^{\sigma-1} = b^2$$

For each $\sigma \in G$, write:

$$\gamma^{\sigma-1} = b_\sigma^2, \quad b_\sigma \in L_1^\times$$

If we define for $\sigma, \tau \in G$:

$$c(\sigma, \tau) = b_\sigma^\tau b_\tau b_{\sigma\tau}^{-1}$$

then $c \in H^2(G, C_2)$ is a cocycle corresponding to the extension $\tilde{G} \twoheadrightarrow G$. Indeed, if $s : G \to \tilde{G}$ is the section such that:

$$(\sqrt{\gamma})^{s(\sigma)} = b_\sigma \sqrt{\gamma}$$

then by comparing $(\sqrt{\gamma})^{s(\sigma)s(\tau)}$ and $(\sqrt{\gamma})^{s(\sigma\tau)}$, it is clear that $c(\sigma, \tau) = s(\sigma)s(\tau)s(\sigma\tau)^{-1}$.

If γ' is another element such that $L(\sqrt{\gamma'})$ provides a solution to the embedding problem, and if:

$$\gamma'^{\sigma-1} = b'^2_\sigma$$

$$c'(\sigma, \tau) = b'^\tau_\sigma b'_\tau b'^{-1}_{\sigma\tau}$$

then c and c' are in the same class in $H^2(G, C_2)$, as they give the same group extension. Consider the short exact sequence:

$$1 \to C_2 \to L^\times \to (L^\times)^2 \to 1$$

The corresponding long exact sequence on cohomology gives:

$$\cdots \to H^1(G, L^\times) \to H^1(G, (L^\times)^2) \to H^2(G, C_2) \to H^2(G, L^\times) \to \cdots$$

By definition, c and c' are trivial in $H^2(G, L^\times)$, and so they are both in the image of $H^1(G, (L^\times)^2)$ in $H^2(G, C_2)$; indeed if $y(\sigma) = b_\sigma^2$, $y'(\sigma) = b'^2_\sigma \in H^1(G, (L_1^\times)^2)$, then $y \mapsto c$ and $y' \mapsto c'$. Furthermore, Hilbert's Theorem 90 implies $H^1(G, L^\times) = 1$, and so y and y' must be in the same class in $H^1(G, (L^\times)^2)$. We may deduce from the long exact sequence on cohomology corresponding to:

$$1 \to (L^\times)^2 \to L^\times \to L^\times/(L^\times)^2 \to 1$$

that:

$$\{x \in L^\times : x^{\sigma-1} \in (L^\times)^2 \text{ for all } \sigma \in G\} / \left(K^\times \cdot (L^\times)^2\right) \simeq H^1(G, (L^\times)^2)$$

where the isomorphism is explicitly given by $x \mapsto \{\sigma \mapsto x^{\sigma - 1}\}$. Thus γ maps to y and γ' maps to y'. Since y and y' are in the same class, $\gamma/\gamma' \in K^\times \cdot (L^\times)^2$.

Conversely, suppose $\gamma' = k\ell^2\gamma$, $k \in K$, $\ell \in L$. We may as well assume $\ell = 1$, as $k\ell^2\gamma$ and $k\gamma$ give the same quadratic extension. Then we have:

$$\gamma'^{\sigma - 1} = b_\sigma^2$$

Thus, γ and γ' give the same element in $H^1(G, (L_1^\times)^2)$, and they both have the same image c in $H^2(G, C_2)$. $M' = L(\sqrt{\gamma'})$ is Galois over K, since the conjugates of $\sqrt{\gamma}$ are equal to $\pm b_\sigma \sqrt{\gamma'}$ as σ runs over G. Thus $\tilde{G}' = G(M'|K)$ is a central extension of G by C_2. We obtain a section $s : G' \to \tilde{G}'$ by defining $s(\sigma)$ to be the element of G'' such that:

$$\sqrt{\gamma'}^{s'(\sigma)} = b_\sigma \sqrt{\gamma'}$$

Then it is clear that c corresponds to s' and that $\tilde{G}' \simeq \tilde{G}$. □

B.3 Proof of Lemma 4.5.1

Lemma B.3.1. *There is a one-to-one correspondence between the irreducible representations ρ of $2^r A_n$ and the pairs (ρ', χ) of representations ρ' of $2A_n$ and characters χ on C_{2^r} satisfying $\rho'(z) = \chi(z) I_2$, where I_2 is the 2×2 identity matrix.*

Proof. Let ζ be a generator of $C_{2^r} \subset 2^r A_n$. Then any element of $2^r A_n$ can be represented as $\zeta^k \cdot \sigma$ for some integer k and some $\sigma \in 2A_n$. Furthermore, this representation is unique if $0 \leq k < 2^{r-1}$.

Now let ρ be an irreducible representation of $2^r A_n$. Let ρ' be the restriction of ρ to $2A_n$. Since C_{2^r} is in the center of $2^r A_n$, it acts by scalars through ρ, and thus any invariant subspace of ρ' must be invariant for ρ. Thus ρ' must be irreducible. Since C_{2^r} acts by scalars, there is a character $\chi : C_{2^r} \to \mathbb{C}^\times$ such that the restriction of ρ to C_{2^r} is isomorphic to $\chi \oplus \chi$. Thus ρ uniquely determines an irreducible representation of $2A_n$ and a character on C_{2^r}. We note that, if $z = \zeta^{2^{r-1}}$, then z is the only nontrivial element of $2A_n \cap C_{2^r}$, and we must have that $\rho'(z)$ acts by the scalar $\chi(z)$.

Conversely, let ρ' be an irreducible representation of $2A_n$, and let χ be a character on C_{2^r} such that $\rho'(z)$ acts by the scalar $\chi(z)$. Then one can easily check that, for $0 \leq k < 2^{r-1}$ and $\sigma \in 2A_n$:

$$\rho(\zeta^k \sigma) = \chi(z)^k \rho'(\sigma)$$

defines a representation on $2^r A_n$, and it is clearly irreducible. □

References

[1] J. D. Achter, *Detecting complex multiplication*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 38–50.

[2] E. Artin and J. Tate, *Class field theory*, W. A. Benjamin, Inc., 1967.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[4] J. Buhler, *Icosahedral Galois representations*, Lecture Notes in Mathematics, no. 654, Springer-Verlag, 1978.

[5] K. Buzzard, M. Dickinson, N. Shepherd-Barron, and R. Taylor, *On icosahedral Artin representations*, Duke Math. J. **109** (2001), no. 2, 283–318.

[6] T. Crespo, *Explicit construction of $\tilde{A}_n$ type fields*, J. Algebra **127** (1989), 452–461.

[7] ______, *Extensions de A_n par C_4 comme groupes de Galois*, C. R. Acad. Sci. Paris Sér. I Math. **315** (1992), no. 6, 625–628.

[8] ______, *Erratum: "Explicit construction of $\tilde{A}_n$ type fields"*, J. Algebra **157** (1993), no. 1, 283.

[9] ______, *Galois representations, embedding problems and modular forms*, Collectanea Math. **48** (1997), 63–83.

[10] P. Deligne and J. P. Serre, *Formes modulaires de poids 1*, Ann. Scient. Éc. Norm. Sup. **7** (1974), 507–530.

[11] L. Dieulefait, A. Pacetti, and M. Schuett, *Modularity of the Consani-Scholten quintic*, 2010.

[12] E. Freitag, *Hilbert modular forms*, Springer-Verlag, 1990.

[13] F. Götzky, *Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlicher*, Math. Ann. **100** (1928), no. 1, 411–437.

[14] K. B. Gundlach, *Poincáresche und Eisensteinsche Reihen zur Hilbertschen Modulgruppe*, Math. Z. **64** (1956), 339–352.

[15] F. Jarvis, *On Galois representations associated to Hilbert modular forms*, J. Reine Angew. Math. **491** (1997), 199–216.

[16] A. Jehanne, *Realization over $\mathbb{Q}$ of the groups $\tilde{A}_5$ and $\hat{A}_5$*, J. Number Theory **89** (2001), no. 2, 340–368.

[17] C. Khare and J. P. Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504.

[18] ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586.

[19] J. Klüners and G. Malle, *A database for number fields*, `http://www.math.uni-duesseldorf.de/~klueners/minimum/minimum.html`.

[20] R. Langlands, *Base change for $GL(2)$*, Annals of Mathematical Studies, no. 96, Princeton University Press, 1980.

[21] J. Neukirch, *Algebraic number theory*, A Series of Comprehensive Studies in Mathematics, Springer, 1999.

[22] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, A Series of Comprehensive Studies in Mathematics, Springer, 2000.

[23] M. Ohta, *Hilbert modular forms of weight one and Galois representations*, Automorphic forms of several variables (Katata, 1983), Progr. Math., vol. 46, Birkhäuser Boston, Boston, MA, 1984, pp. 333–352.

[24] G. Poitou, *Minorations de discriminants (d'après A. M. Odlyzko)*, Séminaire Bourbaki, Vol. 1975/76 28ème année, Exp. No. 479, Springer, Berlin, 1977, pp. 136–153. Lecture Notes in Math., Vol. 567.

[25] ———, *Sur les petits discriminants*, Séminaire Delange-Pisot-Poitou, 18e année: (1976/77), Théorie des nombres, Fasc. 1 (French), Secrétariat Math., Paris, 1977, pp. Exp. No. 6, 18.

[26] J. D. Rogawski and J. Tunnell, *On Artin L-functions associated to Hilbert modular forms of weight one*, Inv. Math. **74** (1983), 1–42.

[27] J. P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, Springer, 1977.

[28] ———, *Modular forms of weight one and Galois representations*, Algebraic Number Fields (A. Frölich, ed.), 1977, pp. 193–268.

[29] ———, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. **59** (1984), no. 4, 651–676.

[30] ———, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[31] ———, *On a theorem of Jordan*, Bull. Amer. Math. Soc. **40** (2003), no. 4, 429–440.

[32] ———, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, A K Peters Ltd., Wellesley, MA, 2008.

[33] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[34] ———, *The special values of the zeta functions associated with Hilbert modular forms*, Duke Math. J. **45** (1978), no. 3, 637–679.

[35] R. Taylor, *On icosahedral Artin representations. II*, Amer. J. Math. **125** (2003), no. 3, 549–566.

[36] The PARI Group, Bordeaux, *PARI/GP, version* `2.5.0`, 2011, available from `http://pari.math.u-bordeaux.fr/`.

[37] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. **5** (1981), 173–175.

[38] K. Uchida, *Unramified extensions of quadratic fields, ii*, Tôhoku Math. J. **22** (1970), 220–224.

[39] G. van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 16, Springer-Verlag, Berlin, 1988.

[40] F.R. Villegas and A. Pacetti, *Computational number theory*, `http://www.ma.utexas.edu/users/villegas/cnt/cnt-no-frames.html`.