International Journal of Number Theory

Finding Galois representations corresponding to certain Hecke eigenclasses

Meghan De Witt

Department of Mathematics
University of Wisconsin,
Madison, WI 53706
dewitt@math.wisc.edu

Darrin Doud*

Department of Mathematics
Brigham Young University
Provo, UT 84602
doud@math.byu.edu

Received (Day Month Year)
Accepted (Day Month Year)

Communicated by xxx

In 1992, Avner Ash and Mark McConnell presented computational evidence of a connection between three-dimensional Galois representations and certain arithmetic cohomology classes. For some examples they were unable to determine the attached representation. For several Hecke eigenclasses (including one for which Ash and McConnell did not find the Galois representation), we find a Galois representation which appears to be attached and show strong evidence for the uniqueness of this representation. The techniques that we use to find defining polynomials for the Galois representations include a targeted Hunter search, class field theory, and elliptic curves.

Keywords: Galois representation; Hecke eigenclass; modularity conjectures.

Mathematics Subject Classification 2000: 11F80, 11F75

1. Introduction

In [2], Avner Ash and Mark McConnell provided computational evidence of a connection between three-dimensional Galois representations and certain arithmetic cohomology classes. Their evidence was obtained by computing simultaneous eigenclasses of Hecke operators acting on certain arithmetic cohomology groups, and then

*Doud's work was supported by NSA grant H98230-05-1-0244. This manuscript is submitted for publication with the understanding that the United States Government is authorized to reproduce and distribute reprints.

attempting to compute Galois representations attached to these eigenclasses. For many of the eigenclasses that they obtained, they were able to compute a Galois representation which seemed to be attached, but for some of their examples they were unable to determine such a representation. In this paper, we examine one of these examples and find the Galois representation. The Hecke eigenvalues arising from the cohomology computation allow us to predict the orders of Frobenius elements under the Galois representation, and we will find a Galois representation with the correct orders of Frobenius to correspond to the eigenclass for all primes ℓ less than 50. We will show that under certain assumptions on the Galois representations, the representations that we find are unique, and explain why these assumptions are reasonable.

2. Attached eigenvectors

Let $\Gamma_0(N)$ be the set of matrices in $\mathrm{GL}_3(\mathbb{Z})$ whose first row is congruent to $(*, 0, 0)$ modulo N, and let Σ_N be the subsemigroup of integral matrices in $\mathrm{GL}_3(\mathbb{Q})$ satisfying the same congruence condition. For a fixed prime p, let $\mathcal{H}(N)$ be the $\bar{\mathbb{F}}_p$-algebra of double cosets $\Gamma_0(N)\backslash\Sigma_N/\Gamma_0(N)$. Then for any $\mathbb{F}_p[\Sigma_N]$-module V and any $q \geq 0$, $H^q(\Gamma_0(N), V)$ is an $\mathcal{H}(N)$-module. We call the elements of $\mathcal{H}(N)$ Hecke operators, and single out the elements corresponding to double cosets of the form $\Gamma_0(N)D(\ell, k)\Gamma_0(N)$, where $\ell \nmid N$ is prime, $0 \leq k \leq 3$, and $D(\ell, k)$ is a 3×3 diagonal matrix with the first $3 - k$ entries equal to 1 and the remaining k entries equal to ℓ. We write $T(\ell, k)$ for the double coset corresponding to $D(\ell, k)$.

Definition 2.1. *Let V be a $\mathcal{H}(pN)$ module, and suppose that $v \in V$ is a simultaneous eigenvector of all $T(\ell, k)$ for all primes $\ell \nmid pN$ and $0 \leq k \leq 3$, so that $T(\ell, k)v = a(\ell, k)v$ for some $a(\ell, k) \in \bar{\mathbb{F}}_p$. If*

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\bar{\mathbb{F}}_p)$$

is a Galois representation unramified outside pN, such that

$$\sum_{k=0}^{3} (-1)^k \ell^{k(k-1)/2} a(\ell, k) X^k = \det(I - \rho(\mathrm{Fr}_\ell)X)$$

for all $\ell \neq pN$, then we say that ρ is attached to v.

Note that in this paper, the $\mathcal{H}(pN)$-module V will be taken to be $H^3(\Gamma_0(N), \mathbb{F}_p)$. Also note that the definition of attached merely indicates a coincidence of the Hecke polynomial at ℓ with the characteristic polynomial of $\rho(\mathrm{Fr}_\ell)$ for all ℓ. Given an eigenvector v, the problem of finding an attached ρ (if one exists) can be very difficult. In this paper, we will content ourselves with the following: given v, we will compute the Hecke polynomial. Under the assumption that this is the characteristic polynomial of a 3×3 matrix, we will predict the order of that matrix. We will then find a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\bar{\mathbb{F}}_p)$ such that for each $\ell < 50$, the order of $\rho(\mathrm{Fr}_\ell)$ matches this prediction. Note that for any set of eigenvalues appearing with trivial coefficients, $a_i(\ell, 0) = a_i(\ell, 3) = 1$.

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$a_1(\ell,1)$	4	4	$*$	1	0	3	4	0	0	2	0	1	4	1	0
$a_1(\ell,2)$	1	1	$*$	0	0	3	1	2	4	0	0	0	4	2	3
$a_2(\ell,1)$	1	1	$*$	0	0	3	1	2	4	0	0	0	4	2	3
$a_2(\ell,2)$	4	4	$*$	1	0	3	4	0	0	2	0	1	4	1	0
$a_3(\ell,1)$	2	2	$*$	1	2	3	4	4	3	4	2	0	2	1	0
$a_3(\ell,2)$	2	0	$*$	0	2	3	1	3	3	3	2	3	2	2	3
$a_4(\ell,1)$	2	0	$*$	0	2	3	1	3	3	3	2	3	2	2	3
$a_4(\ell,2)$	2	2	$*$	1	2	3	4	4	3	4	2	0	2	1	0
$a_5(\ell,1)$	3	2	$*$	2	0	3	2	0	2	2	1	0	2	3	0
$a_5(\ell,2)$	4	0	$*$	2	0	3	2	2	0	0	1	3	2	3	3
$a_6(\ell,1)$	4	0	$*$	2	0	3	2	2	0	0	1	3	2	3	3
$a_6(\ell,2)$	3	2	$*$	2	0	3	2	0	2	2	1	0	2	3	0

Table 1. Six sets of eigenvalues in $H^3(\Gamma_0(163),\mathbb{F}_5)$.

3. Systems of Hecke eigenvalues

We begin by describing the Hecke eigenclasses in which we are interested. In [2], Ash and McConnell remark that there is a quasicuspidal eigenclass in $H^3(\Gamma_0(163),\mathbb{F}_5)$ and indicate that it has eigenvalues defined over $\mathbb{F}_5$. Using software developed for [1], we have computed the space $H^3(\Gamma_0(163),\mathbb{F}_5)$, and found that it has six one-dimensional eigenspaces with eigenvalues defined over $\mathbb{F}_5$. We list the eigenvalues $a_i(\ell,1)$ and $a_i(\ell,2)$ with $1\le i\le 6$ for these eigenclasses in Table 1. Each of these sets of eigenvalues should have a three-dimensional Galois representation ρ_i attached.

Ash and McConnell indicate that the representation potentially associated to their cohomology eigenclass seems to be reducible as a sum of a two-dimensional representation and a one-dimensional representation. To see this, we let $\sigma : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_5)$ be an ordinary Galois representation of Serre weight 2 [12], with determinant the cyclotomic character modulo 5 (denoted ω). According to the main conjecture of [1], there are two ways to obtain a three-dimensional Galois representation with trivial predicted weight from σ: we may take the direct sum $\theta = \omega^2 \oplus \sigma$, or we may take the direct sum $\theta' = \omega\sigma \oplus 1$. If we denote the trace of $\sigma(\mathrm{Fr}_\ell)$ by $b(\ell)$, we see that $\det(I - \sigma(\mathrm{Fr}_\ell)X) = 1 - b(\ell)X + \ell X^2$,

$$\det(I-\theta(\mathrm{Fr}_\ell)) = (1-b(\ell)X+\ell X^2)(1-\ell^2X) = 1-(b(\ell)+\ell^2)X+(\ell+\ell^2 b(\ell))X^2-\ell^3X^3$$

and

$$\det(I-\theta'(\mathrm{Fr}_\ell)) = (1-\ell b(\ell)X+\ell^3X^2)(1-X) = 1-(\ell b(\ell)+1)X+(\ell^3+\ell b(\ell))X^2-\ell^3X^3.$$

If we can find a single set of $b(\ell)$, so that some $a_i(\ell,1) = b(\ell)+\ell^2$, $a_i(\ell,2) = 1+\ell b(\ell)$, $a_j(\ell,1) = \ell b(\ell)+1$, and $a_j(\ell,2) = \ell^2 + b(\ell)$, then we can begin to search for a two-dimensional Galois representation with $\mathrm{Tr}(\sigma(\mathrm{Fr}_\ell)) = b(\ell)$.

In fact, there are three possible sets of traces indicated in Table 2. If we de-

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$b_1(\ell)$	0	0	*	2	4	4	0	4	1	1	4	2	3	2	1
$b_2(\ell)$	3	3	*	2	1	4	0	3	4	3	1	1	1	2	1
$b_3(\ell)$	4	3	*	3	4	4	3	4	3	1	0	1	1	4	1

Table 2. Traces of Frobenius under conjectured two-dimensional representations.

note by σ_i the (conjectured) two-dimensional Galois representation associated to the $b_i(\ell)$, and by θ_i, θ_i' the two direct sums derived from σ_i, we see that ρ_{2i-1} and θ_i have the same characteristic polynomials, and that ρ_{2i} and θ_i' have the same characteristic polynomials. Therefore, we will concentrate on finding the two-dimensional representations σ_1, σ_2, and σ_3.

4. Number Fields from Galois representations

A Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$ is a continuous homomorphism from $G_{\mathbb{Q}}$ (the absolute Galois group of $\mathbb{Q}$, or the Galois group of $\bar{\mathbb{Q}}/\mathbb{Q}$) to a matrix group over the algebraic closure of a finite field. Continuity here is with respect to the standard profinite (or Krull) topology on $G_{\mathbb{Q}}$, and the discrete topology on $\mathrm{GL}_n(\mathbb{F}_p)$. The continuity of the homomorphism implies that it has finite image. This in turn implies that its kernel is an open normal subgroup of finite index. Then the fixed field of the kernel is a finite Galois extension $K/\mathbb{Q}$, and we can factor ρ as a composition $\rho = \eta \circ \pi$, where $\pi : G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q})$ is the canonical projection, and $\eta : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{F}_p)$ is a representation of the finite group $\mathrm{Gal}(K/\mathbb{Q})$. We call K the number field cut out by ρ. Note that given the number field K and a homomorphism $\eta : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$, we immediately obtain a Galois representation ρ. Note that when we speak of $\rho(\mathrm{Fr}_\ell)$, with Fr_ℓ in $G_{\mathbb{Q}}$, we may actually work with $\eta(\mathrm{Fr}_\ell)$ with $\mathrm{Fr}_\ell \in \mathrm{Gal}(K/\mathbb{Q})$, since the canonical projection takes Frobenius elements to Frobenius elements. Note also that η is injective, so that to find the order of $\rho(\mathrm{Fr}_\ell)$, it suffices to find the order of a Frobenius at ℓ in $\mathrm{Gal}(K/\mathbb{Q})$. Our goal in this paper is to find polynomials with splitting fields $K/\mathbb{Q}$, such that the order of Frobenius at each prime ℓ matches the predicted order of Frobenius from the Hecke eigenvalues described above. Given the Hecke eigenvalues, we know the trace and determinant of $\sigma_i(\mathrm{Fr}_\ell)$, and from this can easily compute the characteristic polynomial and eigenvalues. If $\sigma_i(\mathrm{Fr}_\ell)$ has two distinct eigenvalues, we know that $\sigma_i(\mathrm{Fr}_\ell)$ is diagonalizable, and its order is the least common multiple of the orders of the eigenvalues. If $\sigma_i(\mathrm{Fr}_\ell)$ has a repeated eigenvalue, then $\sigma_i(\mathrm{Fr}_\ell)$ is either diagonalizable (in which case it has the same order as the eigenvalue) or has an upper triangular Jordan canonical form (in which case it has order 5 times the order of the eigenvalue). Note that knowing only the characteristic polynomial does not allow us to distinguish these latter two possibilities.

Using this technique, we obtain the orders of Frobenius listed in Table 3, where $n_i(\ell)$ denotes the order of the image of a Frobenius at ℓ under σ_i. Note that the

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$n_1(\ell)$	24	24	*	4	3	4	4	4,20	24	4,20	4	24	6	4	24
$n_2(\ell)$	8	8	*	4	3	4	8	4,20	4	4,20	3	4	2,10	24	24
$n_3(\ell)$	4	24	*	4	6	4	8	12	4	12	6	24	6	24	24

Table 3. Orders of $\sigma_i(\mathrm{Fr}_\ell)$

systems of eigenvalues $a_i(\ell)$ all take values in $\mathbb{F}_5$ (and continue to do so for arbitrarily large ℓ, since they arise from a one-dimensional eigenspace). This implies (by [8, Lemma 6.13]) that the representations σ_i (if they exist) may also be defined over $\mathbb{F}_5$. Hence, the image of σ_i is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$. Based on [1, Conjecture 3.1], we deduce that the Serre level of σ_i is 163 and the nebentype of σ_i is trivial. These facts easily imply that the image of inertia at 163 under σ_i has order 5. Combining this with the fact that we predict that the order of some Frobenius under σ_i is 24, we see immediately that the σ_i are surjective onto $\mathrm{GL}_2(\mathbb{F}_5)$ (since Magma [3] indicates that no proper subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ of order divisible by 5 has an element of order 24). Now there is an exact sequence

$$0 \to \mathbb{F}_5^\times \to \mathrm{GL}_2(\mathbb{F}_5) \to S_5 \to 0,$$

where the injection takes $a \in \mathbb{F}_5^\times$ to aI, and we use the well known fact that $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$. Hence the fixed field of σ_i contains an S_5-extension of $\mathbb{Q}$, ramified only at 5 and at 163 (with $e = 5$). We now make the additional assumptions that $\det(\sigma_i) = \omega$, and that σ_i is ordinary, wildly ramified, and finite at 5. Then the field cut out by σ_i contains an S_5-extension in which 5 has ramification index 20 (and is *peu ramifiée* in the sense of Serre), and 163 has ramification index 5. By [10, Theorem 4.2] and [9], we see that the S_5-extension must be the Galois closure of a quintic field with discriminant $5^5 163^4$, in which both 5 and 163 have ramification index 5.

Under the assumption that σ_i exists, and has the properties described above, we will show that there is a unique $\mathrm{GL}_2(\mathbb{F}_5)$-extension of $\mathbb{Q}$ with the correct orders of Frobenius to be cut out by σ_i. In the conclusion, we will explain why these conditions on σ_i are reasonable.

5. Targeted Hunter searches

A Hunter search is designed to find a polynomial defining a number field K of degree n and discriminant D, if such a number field exists. This search is based on the use of Hunter's theorem and relations between coefficients of polynomials that bound the coefficients of the defining polynomial in question. However, the search space produced by this method is generally far too large to examine. Thus we refine the Hunter search by using the desired ramification type for a certain prime p in K. By knowing the desired ramification of p in K, we could determine congruence conditions of the defining polynomial of K. This allowed us to decrease the search

space to such an extent as to make our search feasible in a reasonable amount of time [11].

We also limited our search space using congruence relations based upon the desired ramification of certain primes [11]. We wanted our quintic field extension to only ramify at 5 and 163, each with $e = 5$. By [11, Theorem 2], we see that a defining polynomial for the field must be congruent to a polynomial $(x-a)^5$ modulo 5 and modulo 163. This restriction on the polynomial places congruences on the coefficients, reducing the size of our search space greatly. For more information on determining the coefficient bounds and the congruence conditions, see [11].

Using these techniques, we programmed a search for a quintic polynomial using GP/Pari[14]. We ran this search (which took about 36 hours) and obtained a list of polynomials satisfying the desired condition. We then tested the polynomials to make sure that they had the desired discriminant of 5^5163^4, eliminated polynomials defining isomorphic number fields, and were left with three fields, defined by the following three quintic polynomials:

$$\begin{aligned} g_1 &= x^5 + 13040x^2 - 117360x + 307744 \\ g_2 &= x^5 + 10595x^2 - 104320x + 254932 \\ g_3 &= x^5 + 13040x^2 - 104320x - 8319520. \end{aligned}$$

Each of these polynomials defines an S_5-extension, and the order of Frobenius at ℓ in the splitting field of each g_i divides the predicted order of Frobenius under σ_i (with a quotient dividing 4, as expected).

We will find it useful to describe the splitting field of each of these quintic polynomials as the splitting field of a sextic polynomial. To do this, we use a resolvent calculation, described in [4, Algorithm 6.3.10(1)]. This resolvent calculation yields a degree six polynomial with the same splitting field as the quintic. When we perform this calculation on our quintic polynomials we obtain the following sextic polynomials:

$$\begin{aligned} f_1 &= x^6 - 3x^5 + 5x^4 + 60x^3 - 95x^2 - 118x - 91, \\ f_2 &= x^6 - 2x^5 - 25x^4 + 190x^3 - 315x^2 - 336x + 1712, \\ f_3 &= x^6 - 3x^5 - 25x^4 + 5185x^3 - 62915x^2 + 585072x + 213824. \end{aligned}$$

6. Structure of $\mathbf{GL_2(\mathbb{F}_5)}$

Using Magma [3], we note that $G = \mathrm{GL}_2(\mathbb{F}_5)$ has a single conjugacy class of subgroups of order 80. It is simple to see that a representative subgroup of this conjugacy class is of the form

$$H = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}.$$

We note that H has a normal subgroup J of order 20, where

$$J = \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\},$$

and we note that every subgroup of G of order 20 is conjugate to this one. Our conditions on σ_i force the image of inertia at 5 under σ_i to be a subgroup conjugate to J. Hence, with a proper choice of basis, we may choose this image to equal J. Let $K/\mathbb{Q}$ be the extension cut out by σ_i. Then $K^J/\mathbb{Q}$ has degree 24 and is the inertia field of a prime lying over 5. Further, K^J/K^H is Galois, with Galois group $H/J \cong \mathbb{Z}/(4\mathbb{Z})$. One checks easily that J has no subgroups which are normal in G, so that the Galois closure of K^J is equal to K. Hence, we may describe K by finding a degree 24 polynomial defining the inertia field of a prime above 5. We already have a degree 6 polynomial defining a field contained in this inertia field, namely the f_i. We will use class field theory to study the inertia field and to compute a degree 24 defining polynomial for it.

7. Class field theory

Denote K^H by F and K^J by L. Then L/F is a cyclic extension of degree 4. Since 5 and 163 are the only primes in $K/\mathbb{Q}$ that ramify, they must be the only primes that ramify in L/F. However, for 163, $e = 5$, so no primes over 163 can ramify in a degree four subextension.

We note that F has two primes lying over 5, one of ramification index 1 and one of ramification index 5. We will write these primes as $\mathfrak{p}_1$ and $\mathfrak{p}_2$, with $\mathfrak{p}_1$ having ramification index 1. By our choice of L as the inertia field of a prime lying over 5, we see immediately that $\mathfrak{p}_1$ cannot ramify in L/F. Hence, the only finite prime of F which ramifies in L is $\mathfrak{p}_2$. Since the ramification is tame, we see then that F lies inside the ray class field of L modulo $\mathfrak{p}_2\mathfrak{m}_\infty$ (where $\mathfrak{m}_\infty$ denotes the product of the infinite primes of F, so that we are allowing $\mathfrak{p}_2$ and any infinite primes to ramify). Note also that the narrow class number of F (for f_1 and f_2) is 1, so that L/F must be totally ramified.

Using GP/PARI to compute the ray class group of F modulo $\mathfrak{p}_2\mathfrak{m}_\infty$, we find that for f_1 and f_3, it is cyclic of order 4. Hence, L/F is in fact the ray class field. For f_2, the desired ray class group is $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the problem is more complicated, since this group has several quotients which are cyclic of order 4. We use a different technique to find the defining polynomial for σ_2. However, at this point we may examine the cyclic degree 4 extensions of F unramified outside $\mathfrak{p}_2$. There are two such extensions (since $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has two quotients isomorphic to $\mathbb{Z}/4\mathbb{Z}$), but only one of them yields the correct orders of Frobenius to correspond to the Hecke eigenvalues. We have then proved the following theorem.

Theorem 7.1. *Assume that the σ_i exist, have level 163 and determinant ω, and are ordinary, wildly ramified and finite at 5. Then there is at most one candidate* $\mathrm{GL}_2(\mathbb{F}_5)$*-extension for each σ_i.*

Proof. We have seen that such an extension must contain an S_5-extension with certain ramification at 5 and 163. A Hunter search shows that there is exactly one such S_5-extension for each σ_i. Class field theory then shows that each S_5-extension

is contained in at most one $\mathrm{GL}_2(\mathbb{F}_5)$-extension with the correct ramification and orders of Frobenius to correspond to σ_i. □

8. Kummer Theory

We require the following theorem:

Theorem 8.1. *[5, pg 114] Let $L = K(\sqrt{u})$ be a quadratic extension with $u \in \mathfrak{O}_K$, and let $\mathfrak{p}$ be prime in $\mathfrak{O}_K$.*

(i) If $2u \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in L.

(ii) If $2 \in \mathfrak{p}$, $u \notin \mathfrak{p}$ and $u = b^2 - 4c$ for some $b, c \in \mathfrak{O}_K$, then $\mathfrak{p}$ is unramified in L.

If we denote by M the unique quadratic subextension of L/F, then we see that $M = L(\sqrt{u})$ for some $u \in \mathfrak{O}_L$, and that M/L is ramified only at $\mathfrak{p}_2$. Hence, u must be an element of $\mathfrak{p}_2$, but of no other prime ideal (by 8.1). Since the class number of F is 1, we see that $\mathfrak{p}_2 = (\alpha)$ is principal. Hence, an element of $\mathfrak{O}_K$ which is contained in $\mathfrak{p}_2$ but in no other prime ideal is of the form $\alpha^m\eta$, where η is a unit in $\mathfrak{O}_K$. Adjusting this element by a square factor will not affect m, so we may take $u = \pm\alpha\eta$, where η is a product of some subset of the fundamental units of F. Note that there are only finitely many such elements. For each such element, we compute a minimal polynomial for u, and substitute x^2 for x to obtain a minimal polynomial for $\sqrt{u}$. We then check to see if the resulting polynomial yields a field which is unramified at 2. If it does, we check this polynomial to see if the orders of Frobenius in the resulting extension match those desired for σ_i.

For f_1 and f_3, we obtain unique polynomials from this process, each of which yields the correct orders of Frobenius. Hence, there is a unique quadratic extension of L unramified outside $\mathfrak{p}_2$. This extension is the desired M.

Finally, we repeat this process to find a quadratic extension of M ramified only at the unique prime of M lying over $\mathfrak{p}_2$. Fortunately, each M encountered has class number 1, so that the above procedure can be repeated. We then obtain 2 degree 24 polynomials, one for each σ_i, as indicated in Table 4. Note that the class number of F for f_2 is 6, so that we cannot find a generator for the ideal $\mathfrak{p}_2$, and this process does not work. We could use a more complicated technique of explicit class field theory, but we choose instead to use an entirely different method to find a defining polynomial.

9. Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$. Let $E(\bar{\mathbb{Q}})_p = \{P_1, P_2, \ldots, P_k\}$ be the p-torsion points on $E(\bar{\mathbb{Q}})$. Then $E(\bar{\mathbb{Q}})_p$ is an $\mathbb{F}_p$-vector space, on which $G_{\mathbb{Q}}$ acts as linear transformations. This gives rise to a Galois representation $\tau : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$. If the conductor of E is N, then τ is unramified outside pN.

Define $P_i = (x_i, y_i)$ and

$$K = \mathbb{Q}(x_1, \ldots, x_k, y_1, \ldots, y_k)$$

Representation	Defining Polynomial
σ_1	$x^{24} - 637659x^{22} + 109056774377x^{20}$ $+1632464535273540x^{18}$ $-371651092248574570x^{16} - 2672604891733833170x^{14}$ $-5269788031324753370x^{12} + 155802031802967990x^{10}$ $-5228343306748595x^8 + 117734861534580x^6$ $+817310749930x^4 - 3278260x^2 + 5$
σ_3	$x^{24} - 368662181x^{22} - 56979878945733576x^{20}$ $-592673922344726032977377 0x^{18}$ $+2825061262048524412523252201750x^{16}$ $-4922992696508215067329496139089055 05x^{14}$ $-1307345148590597879883355731944130x^{12}$ $-2523365902992980267458964728102 5x^{10}$ $-2169037021175047052994698921 0x^8$ $-6000118929463687916632897 0x^6$ $+427960300381201917390 40x^4$ $+930599517955x^2 + 5$

Table 4. Defining polynomials for σ_1 and σ_3.

Then K is stable under the action of $G_{\mathbb{Q}}$, so $K/\mathbb{Q}$ is a Galois extension. We note that K is exactly the field cut out by τ. This implies that $\mathrm{Gal}(K/\mathbb{Q})$ is a Galois extension of $\mathbb{Q}$, with Galois group a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

We now examine the elliptic curve of conductor 163 given by the equation

$$y^2 + y = x^3 - 2x + 1$$

(obtained from [6]). The 5-torsion representation arising from this curve is ramified only at 5 and 163. From [7, Prop 2.11(c)], we see that in the fixed field K of τ, the prime 5 has ramification index 20. From [13, Theorem VII.3.4] we then see that for each torsion point, py_i is an algebraic integer, and that the Galois conjugates of the py_i are all of the form py_j. Using GP/PARI, we then compute the degree 24 polynomial

$$\prod_{y_i}(x - py_i)$$

to high enough precision to recognize the coefficients as integers, and round off to obtain the polynomial $f(x)$ in Table 5, which has splitting field contained in the fixed field K of τ. This polynomial is irreducible, and we easily compute that in the field defined by f, 19 has inertial degree 20 and 47 has inertial degree 24. Hence, the Galois group of f is a subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ containing elements of orders 20 and 24, so it must be all of $\mathrm{GL}_2(\mathbb{F}_5)$. Thus, the splitting field of f is exactly the field K cut out by τ.

$$x^{24} + 60x^{23} + 8475x^{22} + 402875x^{21}$$
$$+13913355x^{20} + 354220875x^{19} + 8309320000x^{18}$$
$$+169517221875x^{17} + 2491765593750x^{16}$$
$$+24464219093750x^{15} + 179155477734375x^{14}$$
$$+1413835025390625x^{13} + 14279768203125000x^{12}$$
$$+132599856298828125x^{11} + 849863511181640625x^{10}$$
$$+2785809996337890625x^{9} - 3487057855224609375x^{8}$$
$$-8246535919189453125x^{7} - 4076755126953125000000x^{6}$$
$$-1095723202056884765625x^{5} - 1700718978881835937500x^{4}$$
$$-1327285671234130859375x^{3} - 1567749023437500000000x^{2}+$$
$$3595819473266601562500x + 615432262420654296875$$

Table 5. Degree 24 polynomial defining σ_2

By computing the splitting of primes in K we were able to determine that this polynomial defines a $\mathrm{GL}_2(\mathbb{F}_5)$-extension of $\mathbb{Q}$ which has the correct orders of Frobenius (for $\ell < 50$) to correspond to be the field cut out by σ_2.

Note that we can explicitly compute the trace of $\tau(\mathrm{Fr}_\ell)$ where τ is the 5-torsion representation of an elliptic curve E. This trace is the reduction mod p of $a_\ell = p + 1 - |E(\mathbb{F}_\ell)|$. When we do this, the numbers a_ℓ that we obtain are identical to the traces of σ_2, as desired.

10. Conclusion

Under the assumption that each σ_i exists, has level 163 and determinant ω, is ordinary, wildly ramified and finite at 5, we have shown that there is a single candidate for the field cut out by σ_i, and determined this field. Note that these assumptions are not unreasonable. The assumptions on the level and determinant are natural to make, based on [1, Conjecture 3.1].

If we assume that σ_i is ordinary and tamely ramified, then the ramification index at 5 would be 4, and σ_i would cut out a field containing an S_5-extension in which the ramification index at 5 is 4. If we assume that σ_i is supersingular (and hence tamely ramified), then σ_i would cut out a field containing an S_5-extension in which the ramification index at 5 is 6. In either case, the S_5-extension would be the Galois closure of a cubic field of discriminant 5^3163^4. A Hunter search shows that no such field exists.

Finally, if we assume that σ_i is ordinary, wildly ramified at 5, and not finite, the Serre weight of σ_i would be 5 rather than 2, and we would not expect $\omega^2 \oplus \sigma_i$ to be attached to an eigenclass with trivial coefficients. The field cut out by σ_i in this case would contain the Galois closure of a quintic field of discriminant 5^9163^4. A Hunter search for such a field could show that it does not exist, but would involve searching too many polynomials to be feasible.

References

[1] Avner Ash, Darrin Doud, and David Pollack. Galois representations with conjectural connections to arithmetic cohomology. *Duke Math. J.*, 112(3):521–579, 2002.

[2] Avner Ash and Mark McConnell. Experimental indications of three-dimensional Galois representations from the cohomology of $\mathrm{SL}(3, \mathbf{Z})$. *Experiment. Math.*, 1(3):209–223, 1992.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The MAGMA algebra system, I: The user language. *J. Symb. Comp.*, 24:235–265, 1997.

[4] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[5] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[6] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[7] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Current developments in mathematics, 1995 (Cambridge, MA)*, pages 1–154. Int. Press, Cambridge, MA, 1994.

[8] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530 (1975), 1974.

[9] Darrin Doud. Wild ramification in number field extensions of prime degree. *Arch. Math. (Basel)*, 81(6):646–649, 2003.

[10] Darrin Doud. Wildly ramified Galois representations and a generalization of a conjecture of Serre. *Experiment. Math.*, 14(1):119–127, 2005.

[11] Darrin Doud and Michael W. Moore. Even icosahedral Galois representations of prime conductor. *J. Number Theory*, 118(1):62–70, 2006.

[12] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[13] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[14] The PARI-Group, Bordeaux. *PARI/GP, Version 2.1.5*, 2000. available from `http://www.parigp-home.de`.