2005-11-02

Totally Real Galois Representations in Characteristic 2 and Arithmetic Cohomology

Heather Aurora Florence de Melo
Brigham Young University - Provo

TOTALLY REAL GALOIS REPRESENTATIONS IN CHARACTERISTIC 2 AND ARITHMETIC COHOMOLOGY

by

Heather Aurora Florence de Melo

A thesis submitted to the faculty of

Brigham Young University

in partial fulfillment of the requirements for the degree of

Master of Science

Department of Mathematics

Brigham Young University

December 2005

BRIGHAM YOUNG UNIVERSITY

GRADUATE COMMITTEE APPROVAL

of a thesis submitted by

Heather Aurora Florence de Melo

This thesis has been read by each member of the following graduate committee and by majority vote has been found to be satisfactory.

Date	Darrin Doud, Chair
Date	David Cardon
Date	Denise Halverson

BRIGHAM YOUNG UNIVERSITY

As chair of the candidate's graduate committee, I have read the thesis of Heather Aurora Florence de Melo in its final form and have found that (1) its format, citations, and bibliographical style are consistent and acceptable and fulfill university and department style requirements; (2) its illustrative materials including figures, tables, and charts are in place; and (3) the final manuscript is satisfactory to the graduate committee and is ready for submission to the university library.

Date

Darrin Doud
Chair, Graduate Committee

Accepted for the Department

Tyler Jarvis
Graduate Coordinator

Accepted for the College

G. Rex Bryce, Associate Dean
Physical and Mathematical Sciences

ABSTRACT

TOTALLY REAL GALOIS REPRESENTATIONS IN CHARACTERISTIC 2 AND ARITHMETIC COHOMOLOGY

Heather Aurora Florence de Melo

Department of Mathematics

Master of Science

The purpose of this paper is to provide new examples supporting a conjecture of Ash, Doud, and Pollack. This conjecture involves Galois representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\overline{\mathbb{F}}_2)$, and our examples are where complex conjugation is mapped to the identity. Since this case has not yet been examined, the results of this paper are quite significant.

Table of Contents

1 Introduction and Acknowledgements

1.1 Introduction

The purpose of this paper is to provide new examples supporting the main conjecture of Ash, Doud, and Pollack [2], which gives details as to where to look for Hecke eigenclasses corresponding to Galois representations. Much work has been done since the 1970's towards finding and elaborating upon the correspondence between Hecke eigenclasses and Galois representations. Serre helped increase interest in this correspondence with his conjecture [14] published in 1987. In [4] and [3] published in 1991 and 1992, Ash, Pinch, Taylor, and McConnell were the first to give indications that a conjecture as in [2] might be true. They found a few examples supporting a correspondence between Hecke eigenclasses and Galois representations, although they did not make a specific prediction about where to look for eigenclasses. Then in 1998, Allison, Ash, and Conrad developed a technique to compute cohomology classes using Mathematica [1] and found more examples. Doud and Pollack [2] then refined the computational technique and programmed it in C and C++. All of this prepared the way and finally led up to the conjecture of Ash, Doud, and Pollack which not only stated where to look for such Hecke eigenclasses and Galois representations, but also explicitly provided hundreds of examples discovered by using their results.

In 2004, Ash, Pollack, and Soares published a paper [5] providing more examples of the conjecture in characteristic 2. All of these examples involved Galois representations which map complex conjugation to a non-scalar matrix. This brings up the question: would the conjecture still hold true for characteristic 2 Galois representations mapping complex conjugation to the identity? The answer most likely had to be yes, but such examples had never been provided. In this paper, we will provide examples of this type of representation and show that such representations do indeed support the conjecture of Ash, Doud, and Pollack.

1.2 Acknowledgements

All of the computations for this research were performed using GP/PARI [16] and Magma [7]. We'd also like to thank the BYU Fulton Supercomputing Laboratory for much needed resources.

2 Conjecture of Ash, Doud, and Pollack

2.1 Hecke operators

Before stating the conjecture, we make some necessary definitions. We will follow very closely some of the definitions and statements made in [5]. Let $\Gamma_0(N)$ be the subgroup of matrices in $SL_3(\mathbb{Z})$ whose first row is congruent to $(*, 0, 0)$ modulo N. Define S_N to be the subsemigroup of integral matrices in $\mathrm{GL}_3(\mathbb{Q})$ satisfying the same congruence condition and having positive determinant relatively prime to N. Let $\mathcal{H}(N)$ be the $\overline{\mathbb{F}}_2$-algebra generated by the double cosets $\Gamma_0(N)\backslash S_N/\Gamma_0(N)$. These double cosets act on the cohomology and homology of $\Gamma_0(N)$ as described in [6], and we call them Hecke operators when they act in this manner. Let

$$D(\ell, 0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, D(\ell, 1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \ell \end{pmatrix},$$

$$D(\ell,2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \ell & 0 \\ 0 & 0 & \ell \end{pmatrix}, \text{and} \quad D(\ell,3) = \begin{pmatrix} \ell & 0 & 0 \\ 0 & \ell & 0 \\ 0 & 0 & \ell \end{pmatrix}.$$

Clearly, $\mathcal{H}(N)$ contains all double cosets of the form $\Gamma_0(N)D(\ell,k)\Gamma_0(N)$, where ℓ is a prime not dividing N and $0 \leq k \leq 3$. When we consider the double coset of $D(\ell,k)$ as a Hecke operator, we call it $T(\ell,k)$.

2.2 Attached eigenvectors

Definition 2.1. Let V be an $\mathcal{H}(2N)$-module, and suppose that $v \in V$ is a simultaneous eigenvector for all $T(\ell,k)$ and that $T(\ell,k)v = a(\ell,k)v$ with $a(\ell,k) \in \overline{\mathbb{F}}_2$ for all $\ell \nmid 2N$ prime and all $0 \leq k \leq 3$. If

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\overline{\mathbb{F}}_2)$$

is a representation unramified outside $2N$, and

$$\sum_{k=0}^{n} a(\ell,k)X^k = \det(I - \rho(Fr_\ell)X)$$

for all $\ell \nmid 2N$, then we say that ρ is attached to v (or that v corresponds to ρ).

Now let

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_3(\overline{\mathbb{F}}_2)$$

be a continuous representation. We will define a level associated to ρ exactly as Serre does in [14].

2.3 Level

For each prime $\ell \neq 2$ fix an embedding of $G_{\mathbb{Q}_\ell}$ into $G_{\mathbb{Q}}$ as the decomposition group of a prime above ℓ and, for $i \geq 0$, let $g_i = |\rho(G_{\ell,i})|$, where the $G_{\ell,i}$ are the ramification subgroups of $G_{\mathbb{Q}_\ell}$

Let M be an n-dimensional $\overline{\mathbb{F}}_2$-vector space and $M^{\rho(G_{\ell,i})}$ be the elements of M fixed by $\rho(G_{\ell,i})$. Choose a basis of M so that $G_{\mathbb{Q}}$ acts on M via ρ in the natural way. Define

$$n_\ell = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \dim M/M^{\rho(G_{\ell,i})}.$$

The sum defining n_ℓ is actually a finite sum, since eventually the $\rho(G_{\ell,i})$ are trivial.

Definition 2.2. With ρ as above, define the level

$$N(\rho) = \prod_{\ell \neq 2} \ell^{n_\ell}.$$

Note that this product is actually finite, since ρ is ramified at only finitely many primes and n_ℓ is 0 at primes where ρ is unramified.

2.4 Statement of the conjecture

Conjecture 2.3. *Let $\rho : G_{\mathbb{Q}} \to GL_3(\overline{\mathbb{F}}_2)$ be a continuous Galois representation. Further, let $N = N(\rho)$ be the level of ρ. Then for at least one irreducible representation V of $GL_3(\overline{\mathbb{F}}_2)$, ρ is attached to a cohomology eigenclass in $H^*(\Gamma_0(N), V)$.*

Remark 2.4. We will test the result of this conjecture using the trivial representation, V.

Definition 2.5. Given a 3×3 matrix, M, with eigenvalues λ_1, λ_2, and λ_3,

$$\mathrm{T}_2 = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3.$$

We call T_2 the cotrace of M.

Notice that in characteristic 2, the conjecture predicts that

$$\sum_{k=0}^{n} a(\ell,k)X^k = \det(I - \rho(Fr_\ell)X)$$

$$= 1 - (\lambda_1 + \lambda_2 + \lambda_3)x + (\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3)x^2 - \det(\rho(Fr_\ell))x^3,$$

so that $a(\ell,1) = \mathrm{Tr}(\rho(Fr_\ell))$ and $a(\ell,2) = \mathrm{T}_2(\rho(Fr_\ell))$.

Since we are manually checking the equality $T(\ell,k)v = a(\ell,k)v$, where v is a simultaneous eigenvector for all primes, ℓ, we can only check this equality up to some bound. We will set this upper bound so that $\ell \leq 47$ and accept this amount of confirmation as evidence to support the conjecture.

3 Producing Galois Representations

The first step in providing evidence for the conjecture is to identify representations, $\rho : G_{\mathbb{Q}} \to GL_3(\overline{\mathbb{F}}_2)$. Since much evidence has already been provided for representations mapping complex conjugation to a nonidentity matrix, we will be searching for representations that map complex conjugation to the identity. In this section, we will explain how we found irreducible 2 and 3 dimensional representations using splitting fields of irreducible third, fifth, and seventh degree polynomials. Notice that if we analyzed polynomials with complex roots, their splitting fields would not be contained in $\mathbb{R}$, and hence complex conjugation would not be trivial. Since we are only interested in examples where complex conjugation is taken to the identity, we wish to limit our search to polynomials with all real roots.

3^{rd} **degree polynomials**	**discriminant**	**value of** n	**level:** p^n
$x^3 - 9x - 6$	$2^3 3^5$	5	3^5=243
$x^3 + x^2 - 19x - 15$	$2^3 29^2$	2	841
$x^3 - 4x - 2$	$2^2 37$	1	37
$x^3 - 10x + 8$	$2^3 71$	1	71
$x^3 - 7x - 2$	$2^2 79$	1	79
$x^3 - 32x - 32$	$2^2 101$	1	101
$x^3 - 14x - 16$	$2^3 127$	1	127
$x^3 - 11x - 2$	$2^3 163$	1	163
$x^3 - 19x - 14$	$2^3 173$	1	173
$x^3 - 20x - 34$	$2^2 197$	1	197
$x^3 - 10x - 4$	$2^2 223$	1	223
$x^3 - 16x - 8$	229	1	229
$x^3 - 20x - 24$	257	1	257
$x^3 - 8x + 6$	$2^2 269$	1	269
$x^3 - 16x + 20$	$2^2 349$	1	349
$x^3 - 11x + 12$	$2^2 359$	1	359
$x^3 + x^2 - 9x + 5$	$2^2 373$	1	373
$x^3 + x^2 - 9x - 11$	$2^2 389$	1	389
$x^3 + x^2 - 15x - 11$	$2^3 421$	1	421
$x^3 - 14x + 12$	$2^2 443$	1	443

Table 1: Cubic Polynomials

3^{rd} **degree polynomials**	**discriminant**	**value of** n	**level:** p^n
$x^3 - 19x + 22$	$2^3 449$	1	449
$x^3 - 22x - 32$	$2^3 467$	1	467
$x^3 - 14x + 18$	$2^2 557$	1	557
$x^3 - 14x - 4$	$2^2 659$	1	659
$x^3 - 20x + 28$	$2^2 677$	1	677
$x^3 - 26x - 50$	$2^2 701$	1	701
$x^3 + x^2 - 9x - 7$	$2^2 709$	1	709
$x^3 + x^2 - 10x + 4$	$2^2 733$	1	733
$x^3 + x^2 - 14x + 10$	$2^3 739$	1	739
$x^3 - 10x + 6$	$2^2 757$	1	757
$x^3 - 13x + 10$	$2^3 761$	1	761
$x^3 - x^2 - 6x - 1$	761	1	761
$x^3 - 19x + 10$	$2^3 773$	1	773
$x^3 - 17x - 22$	$2^3 823$	1	823
$x^3 - 19x - 6$	$2^3 827$	1	827
$x^3 - 16x - 22$	$2^2 829$	1	829
$x^3 + x^2 - 15x + 1$	$2^2 839$	1	839
$x^3 + x^2 - 19x + 1$	$2^3 857$	1	857
$x^3 + x^2 - 11x - 13$	$2^2 877$	1	877
$x^3 + x^2 - 24x - 40$	$2^3 941$	1	941
$x^3 - 13x - 6$	$2^3 977$	1	977
$x^3 - 16x - 4$	$2^2 997$	1	997

Table 2: Cubic Polynomials

3.1 Third degree polynomials

If f is an irreducible cubic polynomial with non-square discriminant, then $Gal(f) = S_3 \cong GL_2(\mathbb{F}_2)$. Let K be the splitting field of f. Then $K/\mathbb{Q}$ is a Galois extension contained in $\overline{\mathbb{Q}}$ and we can define the map σ as follows:

$$\sigma : G_{\mathbb{Q}} \xrightarrow{\pi} Gal(K/\mathbb{Q}) \xrightarrow{\phi} GL_2(\mathbb{F}_2),$$

where π is the canonical projection (given by $\tau \mapsto \tau|_K$) and ϕ is a 2-dimensional mod 2 representation of S_3:

$$S_3 \xrightarrow{\phi} GL_2(\mathbb{F}_2)$$

$$\phi : (12) \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\phi : (123) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Notice that ϕ is easily checked to be an isomorphism. Finally, setting $\rho = \sigma \oplus 1$, we can see that $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_2) \to GL_3(\overline{\mathbb{F}}_2)$. As mentioned previously, since we want our representations to take complex conjugation to I, complex conjugation should fix the roots of f. In other words, f should have real roots. We identify cubics with real roots by the fact that they have positive discriminant. Finally, using Magma, we examined cubic polynomials with three parameters:

$$x^3 + ax^2 + bx + c, \quad 0 \leq a \leq 1, \ \ -50 \leq b \leq 50, \ \ -50 \leq c \leq 50$$

, eliminating those defining fields with too many remified primes, and found those with positive discriminant (see Appendix 2 for Magma code of the "Cubic Polynomial Search" and discriminant calculations- “Test”). The results of our search are in Table 1. After eliminating polynomials defining fields with too many ramified primes, two polynomials remained. These polynomials, together with the corresponding level of ρ and $\rho^\vee$, are listed in Table 4.

3.2 Fifth degree polynomials

If f is an irreducible quintic polynomial with square discriminant and all real roots, then $Gal(f)$ is either $A_5, \mathbb{Z}/5\mathbb{Z}, D_5$, or F_5. Using Magma, we found that $GL_2(\mathbb{F}_4)$ has one subgroup of order 60, call it H, such that $H \cong A_5$. This relationship between A_5 and $GL_2(\mathbb{F}_4)$ gave us an idea of where to look for our quintic polynomials. By restricting our search to quintics with square discriminant, all real roots, and Galois group A_5, we knew we would also be able to find representations corresponding to these quintics which supported Conjecture 2.3.

Now, letting K be the splitting field of f, $K/\mathbb{Q}$ is a Galois extension contained in $\overline{\mathbb{Q}}$ and we can define the map σ as described in Section 3.1:

$$\sigma : G_{\mathbb{Q}} \xrightarrow{\pi} Gal(K/\mathbb{Q}) \xrightarrow{\phi} GL_2(\mathbb{F}_4),$$

where π is the canonical projection (given by $\tau \mapsto \tau|_K$) and ϕ is an injective 2-dimensional representation of A_5 defined over $\mathbb{F}_4$ [15, pg. 157]. We define

$$\phi : A_5 \to GL_2(\mathbb{F}_4) \text{by}$$

$$\phi : (12)(34) \mapsto \begin{pmatrix} a^2 & a^2 \\ 1 & a^2 \end{pmatrix} \qquad \phi : (123) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\phi : (12345) \mapsto \begin{pmatrix} 0 & a \\ a^2 & a \end{pmatrix} \qquad \phi : (13524) \mapsto \begin{pmatrix} 1 & a^2 \\ 1 & a \end{pmatrix},$$

where $a \in \mathbb{F}_4$ is of order 3. We used Magma to explicitly find the matrices in $H < GL_2(\mathbb{F}_4)$ shown in the map ϕ above. Notice that ϕ is an injective homomorphism. Similar to the cubic case, we define $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_4) \to GL_3(\overline{\mathbb{F}}_2)$ by

5^{th} **degree polynomials**	**discriminant**	**value of** n	**level:** p^n
$x^5 + x^4 - 11x^3 - x^2 + 12x + 4$	$2^2 881^2$	2	881^2=776161
$x^5 - 10x^3 - 2x^2 + 19x + 6$	$2^6 887^2$	1	887

Table 3: Quintic Polynomials

$\rho = \sigma \oplus 1$. Additionally, for every representation, ρ, we automatically find a second representation, ρ^*, by composing ρ with conjugation of $\mathbb{F}_4$, say θ: $\rho^* = \theta \circ \rho$. In order to find irreducible quintic polynomials with all real roots, we used an algorithm by Sturm resulting from the following theorem [8, pg. 153], proved in [11, pg. 369-377].

Theorem 3.1. *Let T be a squarefree polynomial with real coefficients. Assume that $A_0 = T, A_1 = T'$, and that A_i is a polynomial remainder sequence such that for all i with $a \leq i \leq k$:*

$$e_i A_{i-1} = Q_i A_i - f_i A_{i+1},$$

where the e_i and f_i are real and positive, and A_{k+1} is a constant polynomial (non-zero since T is squarefree). Set $\ell_i = \ell(A_i)$, and $d_i = \deg(A_i)$. Then, if s is the number of sign changes in the sequence $\ell_0, \ell_1, ..., \ell_{k+1}$, and if t is the number of sign changes in the sequence $(-1)^{d_0}\ell_0, (-1)^{d_1}\ell_1, ..., (-1)^{d_{k+1}}\ell_{k+1}$, the number of real roots of T is equal to $t - s$.

Since Sturm's Algorithm outputs the number of real roots of any irreducible polynomial, it was very helpful in searching for quintic polynomials with 5 parameters:

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e,$$

$$0 \leq a \leq 2, \quad -50 \leq b \leq 50, \quad -50 \leq c \leq 50, \quad -50 \leq d \leq 50, \quad -50 \leq e \leq 50$$

(see Appendix 2 for Magma code of the "Quintic Polynomial Search" and discriminant calculations- "Test"). We also eliminated polynomials defining fields with too many ramified primes. Our search resulted in two quintic polynomials, only one of which had discriminant small enough to perform the cohomology calculations. These polynomials, together with the corresponding level of ρ and ρ^* (the Galois conjugate of ρ), are listed in Table 3.

3.3 Seventh degree polynomials

Finally, we want to find irreducible seventh degree polynomials with all real roots such that $Gal(f) \cong GL_3(\mathbb{F}_2)$. Letting K be the splitting field of f, $K/\mathbb{Q}$ is a Galois extension contained in $\overline{\mathbb{Q}}$. In this case we can directly define

$$\rho : G_{\mathbb{Q}} \xrightarrow{\pi} Gal(K/\mathbb{Q}) = GL_3(\mathbb{F}_2) \xrightarrow{i} GL_3(\overline{\mathbb{F}}_2),$$

where π is the canonical projection given by $\tau \mapsto \tau|_K$ and i is inclusion. Next define $\rho^\vee$ to be the contragredient of ρ, i.e. the composition of ρ with the unique outer automorphism of $GL_3(\mathbb{F}_2)$, which takes a matrix to its transpose inverse.

The task of identifying irreducible, seventh degree polynomials with the correct Galois group, $\mathrm{GL}_3(\mathbb{F}_2)$, was a little bit more tricky than the fifth degree case. Since maybe one in a million or even a billion seventh degree polynomials has the correct Galois group, a direct search using seven parameters would have taken much too long, even with the help of Sturm's Algorithm. Thus, we looked to an article by Gunter Malle for help [12]. In this paper, Malle identifies two three-parameter families of polynomials with Galois group $\mathrm{GL}_3(\mathbb{F}_2)$.

7^{th} **degree polynomials**	**discriminant**	**value of** n	**level:** p^n
$x^7 - 8x^5 + 2x^4 + 16x^3 - 6x^2 - 6x + 2$	$2^6 73^4$	2	73^2=5329
$x^7 - 8x^5 + 2x^4 + 15x^3 - 4x^2 - 6x + 2$	$2^{10} 809^2$	1	809

Table 4: Seventh degree polynomials

Theorem 3.2. *The polynomials*

$$\begin{aligned} f_1(a,b,t,x) =& (x^4 + 2ax^3 + 2(a^2 + ab - 1)x^2 + 4bx + 2b^2) \\ & \cdot (x^3 - (a + b + 3)x^2 + 2(b + a + 1)x + b) + tx^3(x - 2) \quad \textit{and} \\ f_2(a,b,t,x) =& (x^4 - 2(b + 2)x^2 + 4bx - a) \\ & \cdot (x^3 + 2(b - 1)x^2 + (a + b^2 - 4b)x - 2a) + tx^2(x - 2). \end{aligned}$$

have Galois group $GL_3(\mathbb{F}_2)$ over $\mathbb{Q}(a, b, t)$.

Since the Galois group of each polynomial over $\mathbb{Q}(a, b, t)$ is $\mathrm{GL}_3(\mathbb{F}_2)$, specializing a, b, t to rational numbers yields a polynomials over $\mathbb{Q}$ with Galois group $\mathrm{GL}_3(\mathbb{F}_2)$.

We then ran a search on Magma for each of these three-parameter families with $-20 \le a \le 20, -10 \le b \le 10$, and $-10 \le t \le 10$, together with Sturm's Algorithm to find our seventh degree candidates (see Appendix 2 for Magma code of the "Seventh Degree Polynomial Search" and discriminant calculations- "Test"). After eliminating polynomials defining fields with too many ramified primes, two polynomials remained, only one of which had discriminant small enough to perform the cohomology calculations. These polynomials, together with the corresponding level of ρ and $\rho^\vee$ (the contragredient of ρ), are listed in Table 4.

3.4 Narrowing our list of polynomials

At this point we had long lists of possible candidates. The next condition the polynomials had to meet was a reasonable level so that the calculations of the cohomology classes would also be feasible. We set our limit at 1000. In order to calculate the level corresponding to each polynomial, we needed to look at the discriminants. Since the conjecture works with cohomology classes in characteristic 2, for discriminants in the form $2^m p^n$ where p is a prime, only the prime p contributes to the level, while the power of 2 contributes to the weight. The formula for calculating the level is p^n, where p is this prime and

$$n = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \dim(M/M^{G_i}),$$

where M is the n-dimensional vector space over $\overline{\mathbb{F}}_2$ acted on by $GL_n(\overline{\mathbb{F}}_2)$, where n is 2 or 3, G_i is the i^{th} ramification group at p, and $g_i = o(G_i)$. Therefore we were able to narrow our list of polynomials by searching only for those with discriminant in the form $2^m p^n$ where p is a prime and $p \leq 1000$. We excluded polynomials with level $p^n > 1000$ since our methods of computing the cohomology classes were only capable up to level $p^n \leq 1000$.

Since many polynomials of the same degree can have the same splitting field, we also only included in our list one polynomial representing each splitting field. Tables 1-4 list the polynomials we found, together with the levels of the resulting representations ρ, ρ^*, and $\rho^\vee$.

4 Cohomology Calculations

For a given ρ, our goal is to compare the characteristic polynomial of $\rho(Fr_\ell)$ with the Hecke eigenvalues $T(\ell,1)$ and $T(\ell,2)$. Having obtained the polynomials defining ρ we will be able to compute the characteristic polynomials of Frobenius elements using techniques described below. In order to compute the Hecke eigenvalues we used the techniques of [2]. Using the software developed in [2], we computed the matrices of $T(\ell,1)$ and $T(\ell,2)$ on $H^3(\Gamma_0(N),V)$ for $2 \leq \ell \leq 47$. We then use Magma and GP/PARI to find simultaneous eigenvectors for these matrices. The eigenvalues thus obtained are the eigenvalues we compare to the characteristic polynomial of Frobenius.

In fact, we make our job a bit easier by using the fact that we know what eigenvalues we are looking for. Since we know the desired eigenvalue $a(\ell,1)$ for $T(\ell,1)$, we compute the eigenspace of $T(\ell,1)$ with eigenvalue $a(\ell,1)$. If this space is empty, we would have a counterexample to the conjecture. We then proceed to compute the eigenspace of $T(\ell,2)$ with eigenvalue $a(\ell,2)$, and intersect this with the space we already have. The intersection consists of simultaneous eigenvectors of $T(\ell,1)$ and $T(\ell,2)$ with the correct eigenvalues to correspond to ρ. We continue computing eigenspaces and intersecting for all primes ℓ from 3 to 47. When we are finished we have a subvspace (often one-dimensional) of $H^3(\Gamma_0(N),V)$ consisting of simultaneous eigenvectors for all $T(\ell,k)$ with $3 \leq \ell \leq 47$ with the correct eigenvalues to have ρ attached.

5 Computing the trace and cotrace

5.1 Cubic examples

5.1.1 A theorem of Dedekind

For the cubic polynomials, we used a theorem of Dedekind to find the order of the Frobenius element for each prime $\ell \leq 47$.

Theorem 5.1. *Given a monic irreducible degree n polynomial $g(x) \in \mathbb{Z}[x]$ with splitting field K, the cycle structure of Fr_ℓ in the symmetric group S_n of permutations of the n roots of $g(x)$ for a prime ℓ not dividing the discriminant of $g(x)$ is given by the factorization of $g(x) \mod \ell$. In other words, if*

$$g(x) = \prod_{i=1}^{k} g_i(x) \pmod{\ell},$$

then $Fr_\ell = \prod_{i=1}^{k}(d_i - cycles)$, where, for each i, d_i is the degree of $g_i(x)$.

See [10] for proof. This theorem says that $Fr_\ell \in S_3$ has cycle structure equivalent to the structure of the polynomial factored mod ℓ, for each prime $\ell \nmid \text{disc}(f)$. For example, $x^3 - 9x - 6$ factors into $(x+6)(x^2+x+6) \mod 7$, and thus the Frobenius at 7 is a 2-cycle. For the primes dividing the discriminant, one can simply analyze how these primes split. We used Magma to do this. For unramified primes, the sum of the inertial degrees equals the degree of the polynomial [13], and the Frobenius element will have cycle structure corresponding to these inertial degrees. We can then easily find the order of (Fr_ℓ) by finding the least common multiple of the lengths of each cycle in Fr_ℓ.

5.1.2 Level 3^5

In order to calculate the level of the cubic polynomial $f(x) = x^3 - 9x - 6$ with discriminant $2^3 3^5$, since $p = 3$ is wildly ramified in this case, dim $M/M^{\rho(G_{\ell,i})} > 0$ for some $i \geq 1$ in the equation

$$n_p = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \dim M/M^{\rho(G_{p,i})}.$$

We thus called on a theorem by Doud in [9] to help us calculate the level.

Theorem 5.2. *Let L/K be a degree p extension of number fields, and let $\mathfrak{p}$ be a prime of K lying over $p \in \mathbb{Q}$. Suppose that $\mathfrak{p}$ is wildly ramified in L/K. Let $n = v_p(\Delta_{L/K})$. Then there are integers d and t such that*

$$|G_{i,\mathfrak{p}}| = \begin{cases} pt & \text{if } i=0, \\ p & \text{if } 0 < i \leq d, \\ 1 & \text{if } i > d \end{cases} \tag{1}$$

with $n = (p-1)(1 + d/t)$, and $(d,t) = 1$.

Since $v_p(\Delta_{L/K}) = 5 = (3-1)(1+3/2)$, we have $d = 3$ and $t = 2$. We can now apply the theorem to find $|G_{i,\mathfrak{p}}|$ for each i:

$$|\rho(G_{i,\mathfrak{p}})| = \begin{cases} 6 & \text{if i=0}, \\ 3 & \text{if } 0 < i \leq 3, \\ 1 & \text{if } i > 3. \end{cases} \tag{2}$$

Since $\rho(G_{i,\mathfrak{p}}) \leq GL_2(\mathbb{F}_2) \times I$ for each i and $|GL_2(\mathbb{F}_2)|$=6, we have (up to conjugacy)

$$\rho(G_{i,\mathfrak{p}}) = \begin{cases} GL_2(\mathbb{F}_2) \times I & \text{if i=0,} \\ \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle & \text{if } 0 < i \leq 3, \\ I & \text{if } i > 3. \end{cases} \tag{3}$$

In order to calculate n_3, we must find $M^{\rho(G_{i,\mathfrak{p}})}$, which is the set of elements contained in M, a 2-dimensional $\overline{\mathbb{F}}_2$-vector space, and fixed by $\rho(G_{i,\mathfrak{p}})$. It is easy to see that

$$\dim(M^{\rho(G_{i,\mathfrak{p}})}) = \begin{cases} 1 & \text{if i=0} \\ 1 & \text{if } 0 < i \leq 3 \\ 3 & \text{if } i > 3 \end{cases}, \tag{4}$$

so that

$$\dim(M/M^{\rho(G_{i,\mathfrak{p}})}) = \begin{cases} 2 & \text{if i=0} \\ 2 & \text{if } 0 < i \leq 3 \\ 0 & \text{if } i > 3 \end{cases}, \tag{5}$$

and hence

$$n_3 = \dim(M/M^{\rho(G_{0,\mathfrak{p}})}) + \frac{3}{6}\dim(M/M^{\rho(G_{1,\mathfrak{p}})}) + \frac{3}{6}\dim(M/M^{\rho(G_{2,\mathfrak{p}})}) + \frac{3}{6}\dim(M/M^{\rho(G_{3,\mathfrak{p}})})$$

$= 2 + 1 + 1 + 1 = 5$. (Notice that $\dim M/M$=0) The level is thus $3^5 = 243$.

For the polynomial $f = x^3 - 9x - 6$, since $Gal(f) \cong S_3$, and since S_3 has only three conjugacy classes, Fr_ℓ is contained in either the identity class, the class of 2-cycles, or the class of 3-cycles. Also, since $S_3 \cong \mathrm{GL}_2(\mathbb{F}_2)$, we can represent these conjugacy classes by any 2×2 matrices in $\mathrm{GL}_2(\mathbb{F}_2)$ of order 1, 2, or 3, respectively.

Remember that $|Fr_\ell|$ is determined using either Theorem 5.1 for primes $\ell \nmid p$ or analyzing the splitting of the primes ℓ using Magma. These conjugacy classes in A_5, the matrices representing them in $\mathrm{GL}_2(\mathbb{F}_2)$, and the images under the mapping ρ can be listed as follows:

1. order 1- the identity class, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

2. order 2- transpositions, $M_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, M_2' = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$,

3. order 3- 3-cycles, $M_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, M_2' = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

When $|Fr_\ell| = 1$, trivially $Tr(\rho(Fr_\ell)) = T_2(\rho(Fr_\ell)) = 1$.

When $|Fr_\ell| = 2$, we can easily see that $Tr(\rho(Fr_\ell)) = 1$. In order to find the cotrace, let 1, λ, and μ be the eigenvalues of M_2', where λ and μ are the eigenvalues of M_2. Now we can see that

$$T_2(\rho(Fr_\ell)) = T_2(M_2') = \lambda \cdot 1 + \mu \cdot 1 + \lambda \cdot \mu = Tr(M_2) + \det M_2 = 1$$

.

When $|Fr_\ell| = 3$, we can similarly find that $Tr(\rho(Fr_\ell)) = T_2(\rho(Fr_\ell)) = 0$.

Using Magma and a simple program to run through the primes between 3 and 47 (see "Trace" in Appendix 2), we were able to calculate Table 5, listing the traces and cotraces for the cubic polynomial, $x^3 - 9x - 6$.

prime	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	*	0	1	1	1	1	0	0	0	1	1	1	1	0
$T_2(\rho(Fr_\ell))$	*	0	1	1	1	1	0	0	0	1	1	1	1	0

Table 5: Trace and Cotrace chart for $x^3 - 9x - 6, p = 3^5 = 243$

prime	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	0	1	1	0	1	0	*	0	1	1	1	0
$T_2(\rho(Fr_\ell))$	1	1	0	1	1	0	1	0	*	0	1	1	1	0

Table 6: Trace and Cotrace chart for $x^3 + x^2 - 19x - 15, p = 29$

Then, using the techniques described in Section 4, we computed the cohomology in level $3^5 = 243$ and trivial weight and found that there is a nontrivial eigenspace with the correct eigenvalues to correspond to ρ. This provides evidence supporting Conjecture 2.3.

5.1.3 Level 29^2

For the cubic polynomial $f(x) = x^3+x^2-19x-15$ with discriminant $2^3 29^2$, the prime $p = 29$ is tamely ramified and $M^{\rho(G_i)} = M$ for all $i > 0$. Hence $n_{29} = \dim M/M^{\rho(G_0)}$. Since the inertia group, G_0 is of order 3, as shown in Section 5.1.2, $M^{\rho(G_0)} = \{0\}$ and $n_{29} = \dim M/M^{\rho(G_0)} = 2$. Thus the level is $p^{n_{29}} = 29^2 = 841$.

The calculations for the trace and cotrace for this polynomial are similar to the previous case, and are given in Table 6. Computations in the cohomology group in level 841 yield an eigenspace with the correct eigenvalues to correspond to ρ, providing evidence for the conjecture.

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	1	1	1	0	1	1	0	1	0	0	1	0
$T_2(\rho(Fr_\ell))$	1	0	1	1	1	0	1	1	0	1	0	0	1	0

Table 7: Trace and Cotrace chart for $x^3 - x^2 - 6x - 1, p = 761$

5.1.4 Level 761

For the cubic polynomial $x^3 - x^2 - 6x - 1$ with discriminant $2^3 761$, the prime $p = 761$ is tamely ramified and $M^{\rho(G_i)} = M$ for all $i > 0$. Hence $n_{761} = \dim M/M^{\rho(G_0)}$. Since the inertia group, G_0 is of order 2, $\rho(G_0) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $M^{\rho(G_0)}$ is 1-dimensional. Hence $n_{761} = \dim M/M^{\rho(G_0)} = 1$. We can conclude that the level is $p^{n_{761}} = 761$.

The calculations for the trace and cotrace for this polynomial are similar to the previous case, and are given in Table 7.

5.1.5 Other cubic polynomials

We followed the same steps as in Section 5.1.4 for the rest of the cubic polynomials in Table 1. Tables listing their traces and cotraces are included in Appendix 1, with the Magma code for computing the traces and cotraces under "Trace" in Appendix 2. And once again, after computing the cohomology classes for these cubic polynomials, we found nontrivial eigenspaces with the correct eigenvalues to correspond to the respective representations ρ. Thus we obtain many more examples supporting Conjecture 2.3 for representations which take complex conjugation to the identity matrix.

5.2 Quintic example

For the quintic polynomial $f = x^5 - 10x^3 - 2x^2 + 19x + 6$ with discriminant $2^6 887^2$, let K be the splitting field of f and $\mathcal{O}_K$ be the number field above K. Since the prime $p = 887$ is tamely ramified, $M^{\rho(G_i)} = M$ for all $i > 0$. Hence $n_{887} = \dim M/M^{\rho(G_0)}$. The inertia group G_0 is of order 2, since 2 is the least common multiple of the ramification indices of the prime 887 split in $\mathcal{O}_K$. Since $\mathrm{GL}_3(\mathbb{F}_4)$ has a unique conjugacy class of order 2, we can thus represent $\rho(G_0)$ by any matrix of order 2 in $\mathrm{GL}_3(\mathbb{F}_4)$, say $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. The fixed space of this matrix is 2-dimensional, and since M is a 3-dimensional vector space, $n_{887} = \dim M/M^{\rho(G_0)} = 1$. Thus the level for this polynomial is $p^{n_{887}} = 887^1 = 887$.

In order to calculate the trace and cotrace, remember that $Gal(f) = A_5 < \mathrm{GL}_2(\mathbb{F}_4)$. Also recall that A_5 has five conjugacy classes, represented, up to conjugacy class, by matrices in $GL_2(\mathbb{F}_4)$:

1. order 1- the identity class, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

2. order 2- pairs of transpositions, $M_2 = \begin{pmatrix} a^2 & a^2 \\ 1 & a^2 \end{pmatrix}$,

3. order 3- 3-cycles, $M_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$,

4. order 5- 5-cycles, $M_5 = \begin{pmatrix} 0 & a \\ a^2 & a \end{pmatrix}$,

5. order 5- 5-cycles, $M_5' = \begin{pmatrix} 1 & a^2 \\ 1 & a \end{pmatrix}$.

Because there are two conjugacy classes of order five, we are able to find two different representations supporting the conjecture from our single quintic example (we will explain this shortly).

Given a prime, ℓ, between 3 and 47, since $Gal(f) = A_5$, ℓ can split into one of five different prime decompositions:

1. $P_1P_2P_3P_4P_5$- five primes of inertial degree 1, corresponding to the conjugacy class of order one,

2. $P_1P_2P_3$- two primes of inertial degree 2 and one of degree 1, corresponding to the conjugacy class of order two,

3. $P_1P_2P_3$- one prime or inertial degree 3 and two of degree 1, corresponding to the conjugacy class of order three,

4. P- one prime of inertial degree 5, corresponding to one of the conjugacy classes of order five,

5. P- also one prime of inertial degree 5, correspdonding to the other conjugacy class of order five.

Since the Galois group is A_5, Fr_ℓ must be an even permutation, so these are the only possible ways unramified primes can split.

As in the cubic case, by either using Dedekind's Theorem or simply analyzing the structure of the prime decomposition, we can find matrices representing $\rho(Fr_\ell)$ for each prime and use these matrices to calculate the traces and cotraces.

The only tricky part about this case was distinguishing between the two conjugacy classes of order five.

Theorem 5.3. *Let C_1 and C_2 be the two conjugacy classes of A_5 of order 5. Given an irreducible, fifth degree polynomial f with Galois group A_5 and discriminant Δ^2, for primes $\ell \leq 47$ such that $o(Fr_\ell)$=5,*

1. *if $\Delta \equiv \prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \pmod{\ell}$, then $Fr_\ell \in C_1$ and*

2. *if $-\Delta \equiv \prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \pmod{\ell}$, then $Fr_\ell \in C_2$.*

Proof. Suppose that the function f has roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$. Letting $Fr_\ell = \sigma = (12345)$, where σ permutes the roots of f,

$$D = \Delta^2 = [\prod_{i<j}(\sigma^i(\alpha_1) - \sigma^j(\alpha_1))]^2 = [\prod_{i<j}(\alpha_1^{\ell^i} - \alpha_1^{\ell^j})]^2,$$

where D is the discriminant of f. Note that Δ^2 is a square in $\mathbb{Z}$. Now let $\vartheta_K = \mathbb{Z}[\alpha_1]$ and let P be the prime lying above p in ϑ_K, so that $\vartheta_K/P = \mathbb{Z}[\alpha_1]/P \cong \mathbb{Z}_\ell[x]/f(x)$. Since $\Delta = \prod_{i<j}(\sigma^i(\alpha_1) - \sigma^j(\alpha_1)) \in \mathbb{Z}$, $\prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \in \mathbb{Z}_\ell$. If σ is in the same conjugacy class as Fr_ℓ, then $\Delta \equiv \prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \pmod{\ell}$, and if not, then $-\Delta \equiv \prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \pmod{\ell}$. We can thus distinguish between the two conjugacy classes of order five. ◻

In order to actually apply this theorem to distinguishing between the conjugacy classes of order 5, we first used the Magma code "$f \pmod{p}$ degree 5" given in

ℓ	5	11	13	17	29	37	43	47
$\Delta = 7096 \pmod{\ell}$	4	10	2	7	20	8	1	46
$\prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \pmod{\ell}$	-4	-10	-2	7	20	-8	1	46
conjugacy class	C_2	C_2	C_2	C_1	C_1	C_2	C_1	C_1

Table 8: Distinguishing between conjugacy classes of order 5

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$o(Fr_\ell)$	3	5	3	5	5	5	2	3	5	2	5	3	5	5
$Tr(\rho(Fr_\ell))$	0	a	0	a	a	a^2	1	0	a^2	1	a	0	a^2	a^2
$T_2(\rho(Fr_\ell))$	0	a	0	a	a	a^2	1	0	a^2	1	a	0	a^2	a^2
$T_2(\rho^*(Fr_\ell))$	0	a^2	0	a^2	a^2	a	1	0	a	1	a^2	0	a	a
$T_2(\rho^*(Fr_\ell))$	0	a^2	0	a^2	a^2	a	1	0	a	1	a^2	0	a	a

Table 9: Trace and Cotrace chart for $x^5 - 10x^3 - 2x^2 + 19x + 6, p = 887$

Appendix 2 to find whether $\Delta \equiv \prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \pmod{\ell}$ or $-\Delta \equiv \prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \pmod{\ell}$ for each prime $\ell \leq 47$ such that $o(Fr_\ell)$=5. Since $D = 50353216$ for this polynomial, $\Delta = 7096$. We thus calculated $7096 \pmod{\ell}$ and compared this number to Δ for each of these primes. The results of this process can be seen in Table 8 and the lists of computed traces and cotraces in Table 9.

Using the techniques described in Section 4, we computed the cohomology in level 887 and trivial weight for both representations ρ and ρ^* and found that there are nontrivial eigenspaces with the correct eigenvalues corresponding to ρ and ρ^*, respectively, thus providing two more examples supporting Conjecture 2.3.

5.3 Seventh degree example

For the seventh degree polynomial $f = x^7 - 8x^5 + 2x^4 + 15x^3 - 4x^2 - 6x + 2$ with discriminant $2^{10}809^2$, let K be the splitting field of f and $\mathcal{O}_K$ be the number field above K. Since the prime $p = 809$ is tamely ramified, $M^{\rho(G_i)} = M$ for all $i > 0$. Hence $n_{809} = \dim M/M^{\rho(G_0)}$. The inertia group G_0 is of order 2, since 2 is the least common multiple of the ramification indices of the prime 809 split in $\mathcal{O}_K$. We can thus represent $\rho(G_0)$ by a matrix of order 3 in $\mathrm{GL}_3(\mathbb{F}_2)$, say $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. The fixed space of this matrix is 2-dimensional, and since M is a 3-dimensional vector space, $n_{887} = \dim M/M^{\rho(G_0)} = 1$. Thus the level for this polynomial is $p^{n_{809}} = 809^1 = 809$.

In order to compute the trace and cotrace, recall that $Gal(f) \cong GL_3(\mathbb{F}_2)$. The primes ℓ of $\mathbb{Q}$ can split in one of the following six manners, followed by matrices representing the conjugacy classes in $GL_3(\mathbb{F}_2)$:

1. $P_1P_2P_3P_4P_5P_6P_7$ all with inertial degree 1; $M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

   $, of order 1,$

2. $P_1P_2P_3P_4$ with inertial degrees 2, 2, 2, and 1; $M_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

   $of order 2,$

3. $P_1P_2P_3$ with inertial degrees 3, 3, and 1; $M_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$

ℓ	3	5	7	13	17	41
$\Delta = -25888 \pmod{\ell}$	2	2	2	8	14	17
$\prod_{i<j}(x^{\ell^i} - x^{\ell^j}) \pmod{\ell}$	2	2	-2	8	-14	-17
conjugacy class	C_1	C_1	C_2	C_1	C_2	C_2

Table 10: Distinguishing between conjugacy classes of order 7

of order 3,

4. $P_1P_2P_3$ with inertial degrees 4, 2, and 1; $M_4 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$, of order 4,

5. P with inertia degree 7; $M_7 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, of order 7, or

6. P with inertia degree 7; $M_7' = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$, also of order 7.

These matrices can be found using the different possibilities for matrices in $GL_3(\mathbb{F}_2)$ written in rational canonical form. Since every $n \times n$ matrix can be written in rational canonical form, it is simple to find representatives for the various conjugacy classes of this group.

Similar to the fifth degree example, $GL_3(\mathbb{F}_2)$ has two conjugacy classes of order 7. So when a prime ℓ does not split, there are two different possibilities for the conjugacy class of order 7, giving rise to two distinct representations for this polyno-

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\mathrm{o}(Fr_\ell)$	7	7	7	3	7	7	3	4	4	3	3	7	3	3
$Tr(\rho(Fr_\ell))$	1	1	0	0	1	0	0	1	1	0	0	0	0	0
$T_2(\rho(Fr_\ell))$	0	0	1	0	0	1	0	1	1	0	0	1	0	0
$T_2(\rho^\vee(Fr_\ell))$	0	0	1	0	0	1	0	1	1	0	0	1	0	0
$T_2(\rho^\vee(Fr_\ell))$	1	1	0	0	1	0	0	1	1	0	0	0	0	0

Table 11: Trace and Cotrace chart for $x^7-8x^5+2x^4+15x^3-4x^2-6x+2, p=809$

mial. In order to distinguish between these two conjugacy classes, we used a similar method to the one we used in the fifth degree example. First of all, recall that any Galois group of a polynomial can be written as a permutation group on the roots of the polynomial. Magma has a special command to identify this permutation group. In the seventh degree example, Magma specifically identifies two elements of S_7 as the generators of the permutation group corresponding to $Gal(f)$, c_2c_2' and c_7, a double transposition and a 7-cycle. Since not all 7-cycles are in this permutation group, the ordering of the roots of f matters. The ordering we specifically used was $\{0.3622,\ 0.6479,\ 2.0510,\ 1.5781,\ -1.3391, -2.5199, -0.7802\}$, the 7-cycle was $c_7 = (1234567)$, and the double transposition $c_2c_2' = (12)(36)$. Letting $\sigma = c_7$ and proceeding in a similar manner as before, we can compare Δ with $\prod_{i<j}(x^{\ell^i} - x^{\ell^j})$ (mod ℓ) to find what conjugacy class Fr_ℓ is in for each prime ℓ which does not split (Magma code found under "f (mod p) degree 7" in Appendix 2). See Table 10 for results of the conjugacy classes of order 7 and Table 11 for lists of traces and cotraces.

Using the techniques described in Section 4, we computed the cohomology in level 809 and trivial weight for both representations ρ and $\rho^\vee$ and found that there are nontrivial eigenspaces with the correct eigenvalues corresponding to ρ and $\rho^\vee$, respectively, thus providing two more examples supporting Conjecture 2.3.

Appendix 1

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	0	0	1	1	1	1	1	1	*	0	1	0
$T_2(\rho(Fr_\ell))$	0	1	0	0	1	1	1	1	1	1	*	0	1	0

Trace and Cotrace chart for $x^3 - 4x - 2, p = 37$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	0	1	0	1	0	0	1	0	1	1	0	0
$T_2(\rho(Fr_\ell))$	0	1	0	1	0	1	0	0	1	0	1	1	0	0

Trace and Cotrace chart for $x^3 - 10x + 8, p = 71$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	0	0	1	0	1	1	1	1	1	1	1	1	0
$T_2(\rho(Fr_\ell))$	0	0	0	1	0	1	1	1	1	1	1	1	1	0

Trace and Cotrace chart for $x^3 - 7x - 2, p = 79$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	1	1	0	0	0	0	1	0	1	1	1	0
$T_2(\rho(Fr_\ell))$	1	0	1	1	0	0	0	0	1	0	1	1	1	0

Trace and Cotrace chart for $x^3 - 32x - 32, p = 101$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	0	0	1	0	0	0	1	1	1	0	1	1
$T_2(\rho(Fr_\ell))$	1	0	0	0	1	0	0	0	1	1	1	0	1	1

Trace and Cotrace chart for $x^3 - 14x - 16, p = 127$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	0	1	0	1	1	0	0	0	1	0	0	1
$T_2(\rho(Fr_\ell))$	1	0	0	1	0	1	1	0	0	0	1	0	0	1

Trace and Cotrace chart for $x^3 - 11x - 2, p = 163$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	0	1	1	1	1	0	0	1	0	1	0	1	0
$T_2(\rho(Fr_\ell))$	0	0	1	1	1	1	0	0	1	0	1	0	1	0

Trace and Cotrace chart for $x^3 - 19x - 14, p = 173$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	0	1	1	1	0	0	0	1	0	0	0	0
$T_2(\rho(Fr_\ell))$	1	1	0	1	1	1	0	0	0	1	0	0	0	0

Trace and Cotrace chart for $x^3 - 20x - 34, p = 197$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	0	1	0	1	0	0	1	0	0	1	1
$T_2(\rho(Fr_\ell))$	0	1	1	0	1	0	1	0	0	1	0	0	1	1

Trace and Cotrace chart for $x^3 - 10x - 4, p = 223$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	0	1	0	1	0	0	1	1	1	1	1	0	1
$T_2(\rho(Fr_\ell))$	0	0	1	0	1	0	0	1	1	1	1	1	0	1

Trace and Cotrace chart for $x^3 - 16x - 8, p = 229$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	1	0	0	0	1	0	0	0	1	1	1	1
$T_2(\rho(Fr_\ell))$	1	1	1	0	0	0	1	0	0	0	1	1	1	1

Trace and Cotrace chart for $x^3 - 20x - 24, p = 257$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	1	0	1	1	1	0	1	1	0	0	0	0
$T_2(\rho(Fr_\ell))$	1	0	1	0	1	1	1	0	1	1	0	0	0	0

Trace and Cotrace chart for $x^3 - 8x + 6, p = 269$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	1	1	0	0	0	0	0	0	1	1	1
$T_2(\rho(Fr_\ell))$	0	1	1	1	1	0	0	0	0	0	0	1	1	1

Trace and Cotrace chart for $x^3 - 16x + 20, p = 349$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	0	1	1	0	0	1	1	0	0	1	0	1
$T_2(\rho(Fr_\ell))$	1	0	0	1	1	0	0	1	1	0	0	1	0	1

Trace and Cotrace chart for $x^3 - 11x + 12, p = 359$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	1	0	0	1	1	1	0	0	0	1	1
$T_2(\rho(Fr_\ell))$	0	1	1	1	0	0	1	1	1	0	0	0	1	1

Trace and Cotrace chart for $x^3 + x^2 - 9x + 5, p = 373$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	0	1	0	1	0	1	1	1	1	0	1	1
$T_2(\rho(Fr_\ell))$	1	0	0	1	0	1	0	1	1	1	1	0	1	1

Trace and Cotrace chart for $x^3 + x^2 - 9x - 11, p = 389$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	0	1	0	0	0	1	1	0	0	1	0	1
$T_2(\rho(Fr_\ell))$	1	1	0	1	0	0	0	1	1	0	0	1	0	1

Trace and Cotrace chart for $x^3 + x^2 - 15x - 11, p = 421$

prime(3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	0	0	0	0	0	0	1	0	0	1	1	1
$T_2(\rho(Fr_\ell))$	1	1	0	0	0	0	0	0	1	0	0	1	1	1

Trace and Cotrace chart for $x^3 - 14x + 12, p = 443$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	0	1	1	1	0	0	1	1	0	0	0	1
$T_2(\rho(Fr_\ell))$	0	1	0	1	1	1	0	0	1	1	0	0	0	1

Trace and Cotrace chart for $x^3 - 19x + 22, p = 449$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	0	1	1	1	1	1	1	1	0	0	0	0	1
$T_2(\rho(Fr_\ell))$	0	0	1	1	1	1	1	1	1	0	0	0	0	1

Trace and Cotrace chart for $x^3 - 22x - 32, p = 467$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	0	1	1	0	1	1	0	1	1	1	0	1
$T_2(\rho(Fr_\ell))$	1	1	0	1	1	0	1	1	0	1	1	1	0	1

Trace and Cotrace chart for $x^3 - 14x + 18, p = 557$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	0	1	0	1	1	1	1	0	0	1	0	0
$T_2(\rho(Fr_\ell))$	1	0	0	1	0	1	1	1	1	0	0	1	0	0

Trace and Cotrace chart for $x^3 - 14x - 4, p = 659$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	1	1	0	1	1	1	1	1	0	0	1	1
$T_2(\rho(Fr_\ell))$	1	1	1	1	0	1	1	1	1	1	0	0	1	1

Trace and Cotrace chart for $x^3 - 20x + 28, p = 677$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	0	1	0	0	0	1	0	0	1	0	0	1
$T_2(\rho(Fr_\ell))$	1	1	0	1	0	0	0	1	0	0	1	0	0	1

Trace and Cotrace chart for $x^3 - 26x - 50, p = 701$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	0	1	0	1	1	1	1	0	1	1	1	1	0
$T_2(\rho(Fr_\ell))$	0	0	1	0	1	1	1	1	0	1	1	1	1	0

Trace and Cotrace chart for $x^3 + x^2 - 9x - 7, p = 709$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	1	1	0	0	1	1	0	0	0	1	0
$T_2(\rho(Fr_\ell))$	0	1	1	1	1	0	0	1	1	0	0	0	1	0

Trace and Cotrace chart for $x^3 + x^2 - 10x + 4, p = 733$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	0	0	0	1	1	0	0	1	1	0	1	0
$T_2(\rho(Fr_\ell))$	1	1	0	0	0	1	1	0	0	1	1	0	1	0

Trace and Cotrace chart for $x^3 + x^2 - 14x + 10, p = 739$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	1	0	0	0	0	0	1	1	1	1	1	1	1
$T_2(\rho(Fr_\ell))$	1	1	0	0	0	0	0	1	1	1	1	1	1	1

Trace and Cotrace chart for $x^3 - 10x + 6, p = 757$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	1	0	0	1	0	1	1	1	0	1	0
$T_2(\rho(Fr_\ell))$	0	1	1	1	0	0	1	0	1	1	1	0	1	0

Trace and Cotrace chart for $x^3 - 13x + 10, p = 761$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	1	0	0	0	1	0	1	1	1	0	0
$T_2(\rho(Fr_\ell))$	0	1	1	1	0	0	0	1	0	1	1	1	0	0

Trace and Cotrace chart for $x^3 - 19x + 10, p = 773$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	0	1	1	1	1	1	0	1	1	1	1	0
$T_2(\rho(Fr_\ell))$	1	0	0	1	1	1	1	1	0	1	1	1	1	0

Trace and Cotrace chart for $x^3 - 17x - 22, p = 823$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	0	0	0	1	0	1	0	1	0	1	1	1
$T_2(\rho(Fr_\ell))$	1	0	0	0	0	1	0	1	0	1	0	1	1	1

Trace and Cotrace chart for $x^3 - 19x - 6, p = 827$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	0	1	1	0	0	1	1	1	1	1	1	1	1
$T_2(\rho(Fr_\ell))$	0	0	1	1	0	0	1	1	1	1	1	1	1	1

Trace and Cotrace chart for $x^3 - 16x - 22, p = 829$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	1	0	1	1	1	1	1	0	0	1	1	1
$T_2(\rho(Fr_\ell))$	1	0	1	0	1	1	1	1	1	0	0	1	1	1

Trace and Cotrace chart for $x^3 + x^2 - 15x + 1, p = 839$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	0	1	1	0	0	1	0	0	0	1	1
$T_2(\rho(Fr_\ell))$	0	1	1	0	1	1	0	0	1	0	0	0	1	1

Trace and Cotrace chart for $x^3 + x^2 - 19x + 1, p = 857$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	0	1	1	1	1	1	1	0	0	1	0	1
$T_2(\rho(Fr_\ell))$	0	1	0	1	1	1	1	1	1	0	0	1	0	1

Trace and Cotrace chart for $x^3 + x^2 - 11x - 13, p = 877$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	0	0	1	1	1	1	1	1	1	1	0
$T_2(\rho(Fr_\ell))$	0	1	1	0	0	1	1	1	1	1	1	1	1	0

Trace and Cotrace chart for $x^3 + x^2 - 24x - 40, p = 941$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	1	0	0	1	0	0	0	1	1	0	0	1	1	0
$T_2(\rho(Fr_\ell))$	1	0	0	1	0	0	0	1	1	0	0	1	1	0

Trace and Cotrace chart for $x^3 - 13x - 6, p = 977$

prime (3-47)	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$Tr(\rho(Fr_\ell))$	0	1	1	1	0	1	1	0	1	1	1	1	1	1
$T_2(\rho(Fr_\ell))$	0	1	1	1	0	1	1	0	1	1	1	1	1	1

Trace and Cotrace chart for $x^3 - 16x - 4, p = 997$

Appendix 2

Sturm's Algorithm:

```
Sturm:=function(T);

    if Degree(T) eq 0 then return 0;end if;

    A:=PrimitivePart(T);

    B:=PrimitivePart(Derivative(T));

    g:=1;h:=1;s:=Sign(LeadingCoefficient(A));

    n:=Degree(A);t:=(-1)^(n-1)*s;r1:=1;R:= x;

    while Degree(R) gt 0 do

        delta:=Degree(A)-Degree(B);

        R:=(LeadingCoefficient(B)^(delta+1)*A) mod B;

        if R eq 0 then return -1; end if;

        if (LeadingCoefficient(B) gt 0) or (delta mod 2 eq 1)

           then R:= -R; end if;

        if Sign(LeadingCoefficient(R)) ne s then s:=-s; r1:= r1 -1;

           end if;

        if Sign(LeadingCoefficient(R)) ne (-1)^(Degree(R))*t

           then t:= -t; r1:= r1 +1; end if;

        if Degree(R) eq 0 then return r1; end if;

        A:=B; B:=R div (IntegerRing()!(g*h^delta));

        g:=AbsoluteValue(LeadingCoefficient(A));

        h:=(h^(1-delta)*g^delta);

    end while;

end function;
```

Cubic Polynomial Search:

```
for a:=0 to 1 do
  print "a=",a;
  for b:= -50 to 50 do
    for c:=-50 to 50 do
      f:=x^3+a*x^2+b*x+c;
      D:=Discriminant(f);
      if D gt 0 then
        if IsIrreducible(f) then
          if IsEven(D) then
            if #Factorization(D) lt 3 then
              if Factorization(D)[#Factorization(D)][1] lt 1000 then
                if Order(GaloisGroup(f)) eq 6 then
                  print f,Factorization(D);
                end if;
              end if;
            end if;
          end if;
        end if;
      end if;
    end for;
  end for;
end for;
```

Quintic Polynomial Search:

```
for a:=0 to 2 do
  print "a=",a;
  for b:=-50 to 50 do
    print "b=",b;
    for c:=-50 to 50 do
      for d:=-50 to 50 do
        for e:=-50 to 50 do
          f:=x^5+a*x^4+b*x^3+c*x^2+d*x+e;
          D:=Discriminant(f);
          if IsIrreducible(f) then
            if IsSquare(D) then
              if IsEven(D) then
                if #Factorization(D) lt 3 then
                  if Factorization(D)[#Factorization(D)][1] lt 1000
                    then
                    if Sturm(f) eq 5 then
                      if Order(GaloisGroup(f)) eq 60 then
                        print f,Factorization(D);
                      end if;
                    end if;
                  end if;
                end if;
              end if;
```

```
            end if;
          end if;
        end for;
      end for;
    end for;
  end for;
end for;
```

7th Degree Polynomial Search:

1st Algorithm:

```
for a:=-20 to -11 do
  print "a=",a;
  for b:= -10 to 10 do
    for t:=-10 to 10 do
      f:=(x^4+2*a*x^3+2*(a^2+a*b-1)
      *x^2+4*b*x+2*b^2)*(x^3-(a+b+3)*x^2+2*(b+a+1)*x+b)+t*x^3*(x-2);
      D:=Discriminant(f);
      if IsEven(D) then
        if IsSquare(D) then
          if Sturm(f) eq 7 then
            if IsIrreducible(f) then
              print f,Factorization(D);
            end if;
          end if;
        end if;
      end if;
    end for;
  end for;
end for;
```

2nd Algorithm:

```
for a:=-20 to 20 do
  print "a=",a;
  for b:= -20 to 20 do
    for t:=-20 to 20 do
      f:=(x^4-2*(b+2)*x^2+4*b*x-a)*(x^3+2*(b-1)*x^2+(a+b^2-4*b)*x-2*a)
         +t*x^2*(x-2);
      D:=Discriminant(f);
      if IsIrreducible(f) then
        if IsEven(D) then
          if IsSquare(D) then
            if #Factorization(D) lt 3 then
              if Factorization(D)[#Factorization(D)][1] lt 1000 then
                if Sturm(f) eq 7 then
                  print f,Factorization(D);
                end if;
              end if;
            end if;
          end if;
        end if;
      end if;
    end for;
  end for;
end for;
```

Other Programs:

Test:

```
Test:=function(T);
  K:=NumberField(T);
  OK:=MaximalOrder(K);
  D:=Discriminant(T);
  d:=Factorization(D)[2][1];
  print Decomposition(OK,d);
end function;
```

Trace:

```
Trace:=function(T);
  K:=NumberField(T);
  OK:=MaximalOrder(K);
  n:=3;
  while n lt 50 do
    if #Decomposition(OK,n) eq 1 then print "(",n,",0,0)";
    end if;
    if #Decomposition(OK,n) eq 2 then print "(",n,",1,1)";
    end if;
    if #Decomposition(OK,n) eq 3 then print "(",n,",1,1)";
    end if;
    n:=NextPrime(n);
  end while;
  return T;
```

```
end function;
```

<u>$f \mod p$, **degree 5:**</u>

```
f:=x^5-10x^3-2x^2+19x+6; a=Mod(Mod(1,p)*x,f); g=1;

for(i=0,3,for(j=i+1,4,g=g*a^(p^i)-a^(p^j)));g;
```

<u>$f \mod p$, **degree 7:**</u>

```
f:=x^7-8x^5+2x^4+15x^3-4x^2-6x+2; a=Mod(Mod(1,p)*x,f); g=1;

for(i=0,5,for(j=i+1,6,g=g*a^(p^i)-a^(p^j)));g;
```

References

[1] Gerald Allison, Avner Ash, and Eric Conrad. Galois representations, Hecke operators, and the mod-p cohomology of $\mathrm{GL}(3, \mathbf{Z})$ with twisted coefficients. *Experiment. Math.*, 7(4):361–390, 1998.

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

[3] 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.

[4] Avner Ash, Richard Pinch, and Richard Taylor. An $\widehat{A_4}$ extension of $\mathbf{Q}$ attached to a nonselfdual automorphic form on GL(3). *Math. Ann.*, 291(4):753–766, 1991.

[5] Avner Ash, David Pollack, and Dayna Soares. $\mathrm{SL}_3(\mathbb{F}_2)$-extensions of $\mathbb{Q}$ and arithmetic cohomology modulo 2. *Experiment. Math.*, 13(3):298–307, 2004.

[6] Avner Ash and Glenn Stevens. Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues. *J. Reine Angew. Math.*, 365:192–220, 1986.

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

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

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

[10] Brian Hansen. Explicit computations supporting a generalization of Serre's conjecture. Master's thesis, Brigham Young University, 2005.

[11] Donald E. Knuth. *The art of computer programming. Vol. 2*. Addison-Wesley Publishing Co., Reading, Mass., second edition, 1981. Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[12] Gunter Malle. Multi-parameter polynomials with given Galois group. *J. Symbolic Comput.*, 30(6):717–731, 2000. Algorithmic methods in Galois theory.

[13] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York-Berlin-Heidelberg, 1977.

[14] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[15] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

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