ARTICLE IN PRESS

Available online at www.sciencedirect.com
SCIENCE DIRECT®

ELSEVIER

Journal of Number Theory ▮▮▮ (▮▮▮▮) ▮▮▮–▮▮▮

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

A_6-extensions of $\mathbb{Q}$ and the mod p cohomology of $GL_3(\mathbb{Z})$☆

A. Ash[a,1], D. Pollack[b], W. Sinnott[c,*]

[a] *Department of Mathematics, Boston College, USA*
[b] *Department of Mathematics and Computer Science, Wesleyan University, USA*
[c] *Department of Mathematics, Ohio State University, USA*

Received 1 December 2004

Communicated by D. Goss

Abstract

We present six examples of 3-dimensional mod p Galois representations of projective type A_6 for which we were able to obtain computational evidence for the generalization of Serre's Conjecture proposed by Ash, Doud, Pollack, and Sinnott (Duke Math. J. 112 (2002) 521). Five of these examples arise from A_6 extensions of $\mathbb{Q}$; one of them arises from a $3.A_6$ extension of $\mathbb{Q}$. We also propose a further refinement of the conjecture corresponding to the "peu vs. très ramifiée" distinction of Serre.

Keywords: Galois representations; Serre's Conjecture; A_6 extensions of $\mathbb{Q}$; Cohomology of arithmetic groups

0. Introduction

In this paper we give additional computational evidence for the generalization of Serre's Conjecture [Serre 87] proposed in [Ash-Sinnott 00] and extended in

☆ This manuscript is submitted for publication with the understanding that the United States government is authorized to reproduce and distribute reprints.

* Corresponding author.
E-mail addresses: ashav@bc.edu (A. Ash), dpollack@wesleyan.edu (D. Pollack), sinnott@math.ohio-state.edu (W. Sinnott).

[1] Partially supported by NSA Grant MDA 904-00-1-0046 and NSF Grant DMS-0139287.

0022-314X/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2004.12.007

[Ash-Doud-Pollack 02]. We also propose a further refinement—corresponding precisely to the "peu ramifiée–très ramifiée" distinction in Serre—which removes an ambiguity in the prediction of the earlier conjecture.

The conjecture sets out a precise relationship between mod p Galois representations and the mod p cohomology of congruence subgroups of $SL_n(\mathbb{Z})$: see below for the statement in the case of three-dimensional irreducible representations, and see [Ash-Doud-Pollack 02] for the general situation of n-dimensional, possibly reducible, representations.

Let p be a prime number, and let $\bar{\mathbb{F}}_p$ be an algebraic closure of the finite field $\mathbb{F}_p$ with p elements. We fix an algebraic closure $\bar{\mathbb{Q}}$ of the rational numbers $\mathbb{Q}$, and let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be its Galois group. We consider in this paper three-dimensional representations of $G_{\mathbb{Q}}$ over $\bar{\mathbb{F}}_p$ of "type A_6": continuous irreducible Galois representations $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_p)$ whose image in $PGL_3(\bar{\mathbb{F}}_p)$ is isomorphic to A_6. The image of ρ has larger order in these examples than any on which our conjecture been tested so far.

We looked at twelve A_6 extensions of $\mathbb{Q}$, taken from the tables of Jones (*Tables of Number Fields with Prescribed Ramification: Sextics* [Jones 98]). These are in fact all A_6 extensions ramified at most two primes $\leqslant 19$. We found six of these on which it was feasible to check the conjecture. In all of these cases, the conjecture appears to be true, in the sense that a Hecke eigenclass exists in the predicted cohomology group satisfying the equality of its Hecke polynomial at ℓ with the characteristic polynomial of Frobenius at ℓ for all unramified $\ell \leqslant 47$.

Part of the task of checking our conjecture requires studying the local behavior of these fields: determining local Galois groups and higher ramification. These computations were initially being done entirely with PARI/GP [GP], but while we were investigating these examples, the *Database of Local Fields* created by Jones and Roberts [Jones-Roberts 03] (with its enormously useful local fields calculator) came online. It allowed us to double-check the local field calculations we had made, and it made the remaining calculations much easier to complete. The other part of checking our conjecture requires determining the action of the Hecke algebra on the cohomology of certain congruence subgroups of $SL_3(\mathbb{Z})$ with mod p coefficients. For this the programs developed for [Ash-Doud-Pollack 02] (which have now been extended to allow $p = 2$) were used.

We would like to thank Koichiro Harada, Ron Solomon, John Swallow, and David Roberts for helpful conversations and information.

1. The conjecture

In this section we review and slightly refine the conjecture on mod p Galois representations found in Section 3 of [Ash-Doud-Pollack 02]. However, we only state the conjecture for irreducible, three-dimensional representations. The refinement consists of resolving the ambiguity inherent in the "prime" notation for the weight, using the concept of peu vs. très ramifiée. We simply copy Serre in his original conjecture for $GL(2)$ in this regard.

We choose for each prime q a Frobenius element Frob_q in $G_{\mathbb{Q}}$ and we fix a decomposition group G_q of q with its filtration by its ramification subgroups $G_{q,i}$ for $i \geqslant 0$, numbered so that $G_{q,0}$ is the full inertia group of q in G_q. We sometimes denote $G_{q,0}$ by I_q. The quotient $I_q/G_{q,1}$ is called the *tame inertia group* of q. We also fix a complex conjugation $\mathrm{Frob}_\infty \in G_{\mathbb{Q}}$.

Start with a continuous irreducible representation $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_p)$. We will define three invariants associated to ρ: a level, a nebentype character, and a collection of weights.

Level: For any prime $q \neq p$ set

$$n_q = \sum_{i=0}^{\infty} (|G_i|/|G_0|)\ \dim M/M^{G_i}, \tag{1}$$

where G_i denotes the image under ρ of the ith higher ramification subgroup at q and M denotes the vector space $\bar{\mathbb{F}}_p^3$ on which ρ acts. We define the level of ρ to be $N = \prod_{q \neq p} q^{n_q}$.

Nebentype: Factor $\det\rho = \varepsilon\omega^k$, where ω is the cyclotomic character modulo p and ε is a character of $G_{\mathbb{Q}}$ unramified at p. The conductor of ε divides N, so we can consider it as a Dirichlet character $(\mathbb{Z}/N\mathbb{Z})^\times \to \bar{\mathbb{F}}_p^\times$. This is the nebentype character of ρ.

Weight: This is a triple of integers (a, b, c) satisfying $0 \leqslant a - b, b - c \leqslant p - 1$ and $0 \leqslant c \leqslant p-2$. We call such a triple "p-restricted". Given such a triple, there is associated an irreducible $\mathbb{F}_p[GL_3(\mathbb{Z}/p\mathbb{Z})]$-module, which is denoted by $F(a, b, c)$. See Section 2.3 of [Ash-Doud-Pollack 02]. Associated to ρ there is a collection of weights, determined as follows:

Consider ρ restricted to I_p, the inertia subgroup of $G_{\mathbb{Q}}$ at p. This can be upper-triangularized over $\bar{\mathbb{F}}_p$, and we obtain three characters down the diagonal. There are three cases, which we refer to by the term "niveau". Recall that a character of I_p into $\bar{\mathbb{F}}_p^\times$ factors through the tame inertia group $I_p/G_{p,1}$ and is called "niveau k" if its image lies in $\mathbb{F}_{p^k}^\times$ but in no $\mathbb{F}_{p^r}^\times$ for $r < k$.

Niveau 1: In this case all three characters are niveau 1, i.e. powers of ω. Let those powers be A, B, C read from the upper left corner to the bottom right corner. Let (a, b, c) be the p-restricted triple congruent to $(A - 2, B - 1, C)$ modulo $p - 1$. (We sometimes use the "prime" notation, and write $(a, b, c) = (A - 2, B - 1, C)'$.) We say that (a, b, c) is one of the weights associated to ρ. Doing this for all different ways of upper-triangularizing $\rho|I_p$, we obtain the set of weights associated to ρ.

Niveau 2: Let ψ be the fundamental character of niveau 2. In this case, one of the characters is niveau 2, say ψ^m, another of the characters is ψ^{pm}, and the third character is niveau 1, say ω^k. Write $m = r + sp$ with $0 \leqslant r - s \leqslant p - 1$ (if possible). Let (A, B, C) be either (k, r, s), (r, k, s) or (r, s, k). Let (a, b, c) be the p-restricted triple congruent to $(A - 2, B - 1, C)$ modulo $p - 1$. We say that (a, b, c) is one of the weights associated to ρ. Doing this for all possible choices, we obtain the set of weights associated to ρ.

Niveau 3: Let θ be the fundamental character of niveau 3. In this case, one of the characters is niveau 3, say θ^m, another of the characters is θ^{pm}, and the third character is θ^{p^2m}. Write $m = r+sp+tp^2$ with $0 \leqslant r-t, s-t \leqslant p-1$ (if possible). Let (A, B, C) be the rearrangement of (r, s, t) into descending order. (Note that conditions on r, s, and t imply that $C = t$, but r and s may not be in descending order.) Let (a, b, c) be the p-restricted triple congruent to $(A-2, B-1, C)$ modulo $p-1$. We say that (a, b, c) is one of the weights associated to ρ. Doing this for all possible choices, we obtain the set of weights associated to ρ.

If $A-B-1$ or $B-C-1$ or both are divisible by $p-1$ there is an ambiguity in our definition of (a, b, c). In niveau 1 we resolve it as follows: suppose first that $A-B-1$ is divisible by $p-1$. We view the upper left 2×2 block as a representation of $\rho|I_p$ into $GL(2, \bar{\mathbb{F}}_p)$. This representation is either peu or très ramifiée, in the sense of Section 2.4 (ii) of [Serre 87]. If it is peu ramifiée, we allow both $a = b$ and $a = b + p - 1$. If it is très ramifiée, we set $a = b + p - 1$. We resolve the ambiguity if $B - C - 1$ is divisible by $p - 1$ in a similar way.

In the niveaux 2 and 3 we expect that any ambiguity should be resolved by allowing both possibilities, i.e., if $A-B-1$ is divisible by $p-1$ we should allow both $a = b$ and $a = b+p-1$, and if $B-C-1$ is divisible by $p-1$ we should allow both $b = c$ and $b = c+p-1$. See the upcoming paper of Ash, Pollack and Soares [Ash-Pollack-Soares] for examples of this behavior when $p = 2$.

Before we state the conjecture we briefly review the cohomology of certain subgroups of $GL_3(\mathbb{Z})$ as Hecke modules.

For any level N prime to p, set $\Gamma_0(N)$ to be the subgroup of $SL_3(\mathbb{Z})$ consisting of matrices whose first row is congruent to $(*, 0, 0)$ modulo N. If $\varepsilon : \mathbb{Z}/N\mathbb{Z} \to \bar{\mathbb{F}}_p^{\times}$ is a character, we pull it back to a character of $\Gamma_0(N)$. If V is any $\bar{\mathbb{F}}_p[SL_3(\mathbb{Z}/p\mathbb{Z})]$-module, pull it back to a $\Gamma_0(N)$-module V^*. We denote by V_ε the $\Gamma_0(N)$-module $V^* \otimes \varepsilon$.

The Hecke algebra H acts on $H^*(\Gamma_0(N), V_\varepsilon)$. Let x be a Hecke eigenclass and ℓ a prime not dividing pN. Write $T_{\ell,k}x = a_{\ell,k}x$ where $T_{\ell,k}$ is the Hecke operator corresponding to the double coset $\Gamma_0(N)\mathrm{diag}(1, \ldots, \ell)\Gamma_0(N)$ with k ℓ's, and $a_{\ell,k} \in \bar{\mathbb{F}}_p^{\times}$.

If $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_p)$ is a continuous irreducible representation unramified outside pN, we say that ρ is attached to x if

$$\sum_{k=0}^{3} (-1)^k \ell^{k(k-1)/2} a_{\ell,k} t^k = \det(I - \rho(\mathrm{Frob}_\ell)t) \tag{2}$$

for all ℓ not dividing pN.

We are ready to state the conjecture.

Conjecture. *Let $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_p)$ be a continuous irreducible representation. If $p > 2$, we assume that $\rho(\mathrm{Frob}_\infty)$ has eigenvalues $1, 1, -1$ or $1, -1, -1$. Let N be the level and ε the nebentype character associated to ρ. Then for any weight (a, b, c) associated to ρ, there exists a Hecke eigenclass x in $H^3(\Gamma_0(N), F(a, b, c)_\varepsilon)$ with ρ attached.*

2. Fields with Galois group A_6 ramified at two small primes

We used the tables of Jones [Jones 98] to obtain a complete list of all sextic extensions of $\mathbb{Q}$ which are at most ramified at two primes $\leqslant 19$ and whose Galois closure has Galois group A_6. There are 24 such fields in these tables, each ramified at two primes $\leqslant 19$ (and at infinity). However, A_6 has two conjugacy classes of subgroups of index 6: one is represented by the "natural" subgroups isomorphic to A_5, i.e. the stabilizers of the elements $1, \ldots, 6$ under the natural permutation representation of A_6, and the two classes are interchanged by an outer automorphism of S_6. Hence sextic fields whose Galois closure has group A_6 will occur in pairs with the same Galois closure.

We can determine the pairing as follows. Since an outer automorphism of S_6 switches the two conjugacy classes of elements of order 3 (the 3-cycles and the double 3-cycles) and preserves the other S_6-conjugacy classes in A_6, we can identify sextic fields with the same Galois closure by examining the cycle structure of the Frobenius automorphism Frob_q for various primes q. In more detail: let $K/\mathbb{Q}$ be a Galois extension of $\mathbb{Q}$ with Galois group $G \simeq A_6$, let H and H' be representatives of the two conjugacy classes of subgroups of G of index 6. Then K^H and $K^{H'}$ will be nonconjugate sextic extensions of $\mathbb{Q}$ whose Galois closure is K. If we let G act on the cosets of H and H', we obtain two homomorphisms $\phi, \phi' : G \to S_6$ (depending on a numbering of the cosets): both homomorphisms give an isomorphism of G with A_6, and we have $\phi' = \alpha \circ \phi$, for some outer automorphism α of S_6. If $\mathrm{Frob}_q \in G$ is a Frobenius for q, then the cycle structures of $\phi(\mathrm{Frob}_q)$ and $\phi'(\mathrm{Frob}_q)$ are the same unless Frob_q has order 3 (α switches the 3-cycles and the double 3-cycles, but preserves the other S_6-conjugacy classes in A_6).

Thus there are twelve Galois extensions with Galois group A_6 arising from Jones's tables. These extensions are listed in Table 1. Since Jones's tables are complete, this is a *complete* list of all A_6 extensions of $\mathbb{Q}$ at most ramified at two primes $\leqslant 19$.

Under "location" we have indicated where in Jones's tables each A_6 extension can be found; e.g. "2,3:#55 or #56" means that entries #55 and #56 in the table *New sextic fields ramifying above* {2,3} are nonconjugate sextic fields with the same A_6 extension as their normal closure. The polynomial listed in each case generates the first field of the pair. Henceforth, we refer to these A_6 extensions by the first sextic in each pair.

We used this table to find representations of type A_6 on which we could test our conjecture. Let K be the splitting field of one of these polynomials. Then $\mathrm{Gal}(K/\mathbb{Q}) \simeq A_6$. If $p \neq 3$, A_6 has no irreducible 3-dimensional representations over $\bar{\mathbb{F}}_p$, but its triple cover $3.A_6$ does, so when $p \neq 3$ we have to determine whether K is contained in a $3.A_6$ extension $\tilde{K}/\mathbb{Q}$. If such an extension $\tilde{K}$ exists, we obtain from it a representation $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_p)$ (via $G_{\mathbb{Q}} \to \mathrm{Gal}(\tilde{K}/\mathbb{Q}) \to GL_3(\bar{\mathbb{F}}_p)$). On the other hand, if we take $p = 3$, A_6 does have representations into $GL_3(\bar{\mathbb{F}}_3)$, so we can use K directly to obtain a representation $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_3)$. (We discuss the group $3.A_6$ and its representations more fully in the next section.) Since our conjecture is stable under twisting by Dirichlet characters, we can suppose without loss of generality that (when $p \neq 3$) $\tilde{K}$ is ramified at the same primes as K. This can be seen as follows, using

Table 1
A_6 Sextics

Location	Polynomial
2,3: #55 or #56	$x^6+3x^5+3x^4+2x^3-3x^2-3x-1$
2,3: #57 or #60	$x^6+8x^3+9x^2-6$
2,3: #58 or #61	$x^6+6x^4-4x^3-3x^2-12x-12$
2,3: #59 or #62	$x^6-12x^3+21x^2+12x-34$
2,5: #17 or #18	$x^6-2x^5+15x^4+50x^2-4x-82$
3,5: #7 or #10	$x^6-5x^3+45x^2-99x-15$
3,5: #8 or #9	$x^6+3x^5+15x^4+25x^3+45x+60$
3,7: #3 or #4	$x^6+3x^5+3x^4-9x^3-18x^2+9x+18$
3,13: #9 or #10	$x^6+3x^5+3x^4+2x^3+3$
3,19: #3 or #4	$x^6-3x^5-3x^4+14x^3-12x+9$
5,17: #1 or #2	$x^6-2x^5+5x^2-11x-13$
13,19: #1 or #2	$x^6-4x^4-15x^3-15x^2-8x+4$

a technique due to Tate [Serre 77, §6]. Suppose that ℓ is a rational prime which is ramified in $\tilde{K}$ but not in K. Then $\rho(I_\ell)$ equals the center Z of $SL_3(\bar{\mathbb{F}}_p)$. Let G_ℓ be a decomposition group of ℓ in $G_{\mathbb{Q}}$: since $\rho(G_\ell)/Z$ is isomorphic to the decomposition group of ℓ in $\mathrm{Gal}(K/\mathbb{Q})$, it is cyclic, and therefore $\rho(G_\ell)$ is abelian. Therefore the commutator subgroup G'_ℓ of G_ℓ is contained in $\ker\rho$, and $G'_\ell \subseteq I_\ell$; hence $\rho|I_\ell$ factors through I_ℓ/G'_ℓ. Now I_ℓ/G'_ℓ may be identified with $\mathrm{Gal}(\mathbb{Q}_\ell(\mu_{\ell^\infty})/\mathbb{Q}_\ell)$, which in turn can be identified with $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q})$. (Here μ_{ℓ^∞} is the group of roots of unity of order a power of ℓ.) Hence there is a cubic character χ_ℓ of $G_{\mathbb{Q}}$, unramified outside ℓ, such that

$$\rho(\tau) = \chi_\ell(\tau) I \qquad \text{for } \tau \in I_\ell.$$

Here I is the 3×3 identity matrix. So $(\prod_\ell \chi_\ell)^{-1}\cdot\rho$ is only ramified at the primes that ramify in K. (Here ℓ runs over rational primes that ramify in $\tilde{K}$ but not in K.) Thus we may assume that the level N of ρ is divisible only by the primes (other than p) which ramify in K. Note that ρ still has determinant 1, so it has trivial nebentype, and still has image $3.A_6$ in $SL_3(\bar{\mathbb{F}}_p)$. Sometimes the level N can be lowered further by twisting by a suitable Dirichlet character ramified at a prime ($\neq p$) that does ramify in K; this can change the nebentype.

There are two aspects to testing our conjecture:

- We have to study the field $\tilde{K}$ (or just K, when $p=3$), to determine the level N and weights (a,b,c) attached to ρ; and we need to determine the characteristic polynomials of $\rho(\mathrm{Frob}_\ell)$ for $\ell \nmid pN$. The main difficulty here is the analysis of the ramification groups, which is required to determine the level and the weight. We give examples of these calculations below.
- Once the level N, nebentype ε, and weights (a,b,c) have been found, we have to look for eigenclasses x for the action of the Hecke algebra on $H^3(\Gamma_0(N), F(a,b,c)_\varepsilon)$

which appear correspond to ρ. This means checking that the equation (2) holds for primes $\ell \nmid pN$, $\ell \leqslant 47$. For these calculations, we use the programs developed for [Ash-Doud-Pollack 02] (which have now been extended to allow $p = 2$); for a description of these programs, see [Ash-Doud-Pollack 02]. The main difficulties that arise here are limitations on the feasibility of the computations if the level N or the weight are too large. For this reason, we have always taken p to be one of the primes that ramify in K, since this substantially reduces the level.

3. Modular representations of $3.A_6$

The Schur multiplier of A_6 has order 6, so the universal central extension of A_6 is a six-fold cover of A_6, denoted by $6.A_6$, and the quotient of $6.A_6$ by its central subgroup of order 2 is a triple cover of A_6 denoted by $3.A_6$. $3.A_6$ has faithful three-dimensional complex representations; explicit generators for the image of one of these representations can be found in [Crespo-Hajto].

If $p \neq 3$, A_6 has no three-dimensional linear representations over $\bar{\mathbb{F}}_p$, but it does have representations into $PGL_3(\bar{\mathbb{F}}_p)$. The map $SL_3(\bar{\mathbb{F}}_p) \to PGL_3(\bar{\mathbb{F}}_p)$ is surjective, and its kernel has order 3, and therefore any representation of A_6 into $PGL_3(\bar{\mathbb{F}}_p)$ can be lifted uniquely to a representation of $3.A_6$ into $SL_3(\bar{\mathbb{F}}_p)$. On the other hand, A_6 does have three-dimensional linear representations over $\bar{\mathbb{F}}_3$.

All of these representations can be obtained by reduction mod p from the three-dimensional complex representations of $3.A_6$. There are 4 such representations, which can be realized over $F = \mathbb{Q}(\zeta_3, \sqrt{5})$. In fact, the whole character table of $3.A_6$ lies in F, and all the representations of $3.A_6$ can be realized over F: for any finite group G, the Schur indices of $F[G]$ divide the order of the center of G, and also divide $\phi(m)$, where m is the exponent of G (see for example Serre [Serre 71, p. 109]). Since the center of $3.A_6$ has order 3 and the exponent of $3.A_6$ is 60 (and $\phi(60) = 16$), the Schur indices of $F[3.A_6]$ are all 1. So all the complex representations of $3.A_6$ can be realized over F. The 4 three-dimensional representations of $3.A_6$ are conjugate over $\mathbb{Q}$.

Let p be a rational prime, let $\mathfrak{p}$ be a prime of F lying above p, let $\tilde{\rho} : 3.A_6 \to GL_3(\mathfrak{o}_\mathfrak{p})$ be a realization of one of the three-dimensional representations of $3.A_6$ over the integers $\mathfrak{o}_\mathfrak{p}$ of $F_\mathfrak{p}$, and let ρ be the reduction of $\tilde{\rho}$ mod $\mathfrak{p}$. All the three-dimensional modular representations of $3.A_6$ (up to similarity) arise in this way; this can be seen from the decomposition matrices of $3.A_6$, which are available from [GAP], for example.

We can summarize three-dimensional modular representations of $3.A_6$ as follows:

- $p > 5$, $p \equiv 1, 4 \bmod 15$: There are 4 irreducible three-dimensional representations of $3.A_6$, each defined over $\mathbb{F}_p$.
- $p > 5$, $p \not\equiv 1, 4 \bmod 15$: There are 4 irreducible three-dimensional representations of $3.A_6$, each defined over $\mathbb{F}_{p^2}$. They are conjugate in pairs over $\mathbb{F}_p$.
- $p = 5$: There are 2 irreducible three-dimensional representations of $3.A_6$, each defined over $\mathbb{F}_{25}$. They are conjugate over $\mathbb{F}_5$.
- $p = 3$: There are 2 irreducible three-dimensional representations of $3.A_6$, each defined

over $\mathbb{F}_9$. They are conjugate over $\mathbb{F}_3$.

- $p = 2$: There are 4 irreducible three-dimensional representations of $3.A_6$, each defined over $\mathbb{F}_4$. They are conjugate in pairs over $\mathbb{F}_2$.

All these representations are faithful except the mod 3 representations, for which the center lies in the kernel: these are three-dimensional representations of A_6 in $GL_3(\mathbb{F}_9)$.

4. Mod p Galois representations of type A_6

In this section we describe the mod p Galois representations of type A_6 that arise from the twelve A_6-extensions listed in Table 1, and give examples of the computation of the level N and the associated weights, and the characteristic polynomials of Frobenius. As explained in §2, we always assume that p is one of the ramified primes. We discuss the cases with $p = 3$ separately since we don't need to worry about the existence of a triple cover in those cases.

4.1. Mod 3 *Galois representations of type* A_6

Let K be one of the nine A_6 fields in Table 1 that are ramified at 3. We take $p = 3$ and let ρ be a representation of $G_{\mathbb{Q}}$ into $GL_3(\bar{\mathbb{F}}_3)$ which cuts out K, i.e. $K = \bar{\mathbb{Q}}^{\ker \rho}$. As discussed above, there are two such representations: we may assume that the image of ρ lies in $GL_3(\mathbb{F}_9)$, and the other possible choice for ρ is ρ^{ϕ}, where ϕ is the nontrivial element of $\mathrm{Gal}(\mathbb{F}_9/\mathbb{F}_3)$. ρ has trivial nebentype.

For three of the nine fields K, we can lower the level by twisting by a suitable quadratic Dirichlet character ε; for the remaining fields, we let $\varepsilon = 1$. Then for all nine cases the representation is $\rho\varepsilon$ and the nebentype is ε. In Table 2 below, we list the nine fields which are ramified at 3, the level N of the representation $\rho\varepsilon$, and the nebentype ε. (We omit the nebentype ε when it is trivial.) ω_4 denotes the Dirichlet character corresponding to $\mathbb{Q}(i)$ and ψ_8 the Dirichlet character corresponding to $\mathbb{Q}(\sqrt{2})$, considered as taking values in $\mathbb{F}_3$.

We illustrate the computation of the level for the first field above (2,3:#55). Let K be the splitting field of $T(x) = x^6+3x^5+3x^4+2x^3-3x^2-3x-1$, $G = \mathrm{Gal}(K/\mathbb{Q}) \simeq A_6$. We need to find the images of the ramification groups $G_{2,i}$ of 2 in G. To this end we let L be the splitting field of T over $\mathbb{Q}_2$, and let $D = \mathrm{Gal}(L/\mathbb{Q}_2)$; D may be identified with a decomposition group of 2 in G. Let $G_i = \rho(G_{2,i})$; the G_i's may be identified with the ramification groups of $L/\mathbb{Q}_2$.

The following computations are easily done in PARI/GP. If we factor T over $\mathbb{Q}_2$ we find that $T = H \cdot Q$, where H is an irreducible quartic and Q is an irreducible quadratic. Using the results of the Appendix, we find that $g(x) = x^4+4x^3-14x^2+3$ generates the same extension of $\mathbb{Q}_2$ as H, and $q(x) = x^2+x+1$ generates the same extension of $\mathbb{Q}_2$ as Q. Note that g and q are both irreducible over $\mathbb{Q}_2$: $g(x-1) = x^4-20x^2+36x-14$ is an Eisenstein polynomial, and q is irreducible mod 2.

Let $g_1(x) = g(x-1) = x^4 - 20x^2 + 36x - 14$, and let h_1 be the resolvent cubic of g_1: $h_1 = x^3 + 20x^2 + 56x - 176$. Then $h_2(x) = h_1(2x)/8 = x^3 + 10x^2 + 14x - 22$ is Eisenstein, so h_1 is irreducible; the discriminant of h_1 has the form $2^8 \cdot u$, where

Table 2
Levels of mod 3 representations

K	N, ε
2,3: #55	2^8
2,3: #57	2^7, ψ_8
2,3: #58	2^7, $\omega_4\psi_8$
2,3: #59	2^8, ω_4
3,5: #7	5^4
3,5: #8	5^4
3,7: #3	7^2
3,13: #9	13^2
3,19: #3	19^2

$u \equiv 5 \bmod 8$—which is not a square, so the Galois group (over $\mathbb{Q}_2$) of h_1 is S_3, and the Galois group (over $\mathbb{Q}_2$) of g_1 is S_4.

The splitting field of $g_1(x)$ over $\mathbb{Q}_2$ contains the discriminant field of g_1, namely $\mathbb{Q}_2(\sqrt{5})$, which is the unramified quadratic extension of $\mathbb{Q}_2$, and is also the splitting field of q. Hence the splitting field of g_1 is also the splitting field L of $T(x)$ over $\mathbb{Q}_2$. Thus $D \simeq S_4$. In what follows we will identify D with S_4.

The ramification index of $L/\mathbb{Q}_2$ is divisible by 4 (from g_1) and 3 (from h_2), so equals 12 or 24. But it cannot be 24, since $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified. So $G_0 = A_4$ and $G_1 = V_4$ (since G_1 is the Sylow 2-subgroup of G_0). Since S_4 has no normal subgroups between V_4 and 1, we have $G_1 = G_2 = \cdots = G_r$ and $G_{r+1} = 1$ for some $r \geqslant 1$; we need to determine r.

To study the higher ramification, let α be a root of $g_1(x)$ in L, β a root of $h_2(x)$, and let $\pi = \beta/\alpha$: then $\mathrm{ord}_2(\pi) = \frac{1}{3} - \frac{1}{4} = \frac{1}{12}$, so π is a local parameter in L (here ord_2 is normalized so that $\mathrm{ord}_2(2) = 1$). Let ord_L be the valuation on L, normalized so that $\mathrm{ord}_L(\pi) = 1$. Let $\sigma \in V_4$. Then $\sigma\beta = \beta$ (because β has degree 3 over $\mathbb{Q}_2$) so that we have

$$\begin{aligned}\mathrm{ord}_L(\sigma\pi - \pi) &= \mathrm{ord}_L\left(\beta\,\frac{\alpha - \sigma\alpha}{\alpha\,\sigma\alpha}\right)\\ &= 4 - 3 - 3 + \mathrm{ord}_L(\alpha - \sigma\alpha)\\ &= \mathrm{ord}_L(\alpha - \sigma\alpha) - 2.\end{aligned}$$

Let $v = \mathrm{ord}_L(\sigma\pi - \pi)$ for $\sigma \neq 1, \sigma \in V_4$; v does not depend on σ because there are no ramification groups between V_4 and 1. Since $g_1'(\alpha) = \prod_{\sigma\in V_4, \sigma\neq 1}(\alpha - \sigma\alpha)$ and $\mathbf{N}_{L/\mathbb{Q}_2}(g_1'(\alpha)) = \mathrm{disc}(g_1)^6$, we get

$$\begin{aligned}\mathrm{ord}_L\mathbf{N}_{L/\mathbb{Q}_2}(g_1'(\alpha)) &= \mathrm{ord}_L(\mathrm{disc}(g_1)^6)\\ 24 \cdot 3 \cdot (v+2) &= 6 \cdot 8 \cdot 12;\end{aligned}$$

so $v = 6$, and so $r = 5$.

It follows that $G_i = \rho(G_{2,i})$ contains a subgroup of $GL_3(\mathbb{F}_9)$ isomorphic to V_4 for $i = 0 \ldots 5$. We can diagonalize this subgroup and assume that G_i (for $i = 0 \ldots 5$) contains the subgroup of diagonal matrices of the form $\mathrm{diag}(\pm 1, \pm 1, \pm 1)$ (with determinant 1). It follows that $M^{G_i} = 0$ for such i. So the power of 2 in the level of ρ is 8, as can be computed from definition (1) in §2. So $N(\rho) = 2^8$.

To compute the weight(s) attached to ρ, we find the possible upper-triangularizations of $\rho(I_p)$ (with $p = 3$). Let S be the splitting field of T over $\mathbb{Q}_3$: we need to determine the inertia group of $S/\mathbb{Q}_3$ (which may be identified with $\rho(I_3)$). For this we can use the "local field calculator" attached to the local field database of Jones and Roberts [Jones-Roberts 03], which identifies the field S as an extension of $\mathbb{Q}_3$ with inertia group $C_3 \times C_3$. Hence the elements of $\rho(I_3)$ are unipotent in $GL_3(\bar{\mathbb{F}}_3)$. It follows that there is just one weight attached to ρ by our conjecture, namely $(-2, -1, 0)' = (2, 1, 0)$.

The difficulties in computing $N(\rho)$ in this example arise from the fact that 2 is wildly ramified in K. For the examples ramified at 3 and q with $q \neq 2, 5$, the ramification will be tame, and $N(\rho)$ is easier to determine. For example, consider the field ramified at 3 and 13 (3–13 #9). The polynomial is $T(x) = x^6+3x^5+3x^4+2x^3+3$, which factors over $\mathbb{Q}_{13}$ into two cubics g_1 and g_2, both of which have square discriminants (in $\mathbb{Q}_{13}$) and therefore cyclic Galois groups. $g_1(x-5)$ is Eisenstein, while g_2 is irreducible mod 13. So the splitting field of T over $\mathbb{Q}_{13}$ has Galois group $D \simeq C_3 \times C_3$; the inertia group G_0 has order 3, and we have $G_1 = 1$, since the ramification is tame.

We now need to know the dimension M^{G_0}: since G_0 is generated by a 3-cycle τ in A_6 (in terms of its action on the roots of T), and since a 3-cycle in A_6 normalizes a V_4 (i.e., we may view the 3-cycle as an element of $A_4 \subseteq A_6$) it follows that we may suppose that $\rho(\tau)$ is a permutation matrix of order 3 in $GL_3(\mathbb{F}_9)$, which fixes a one-dimensional subspace of M. From this it is easy to see from definition (1) that the level of ρ is 13^2.

4.2. Mod p Galois representations of type A_6, $p \neq 3$

Let K be a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to A_6, and let $p \neq 3$. There is always a projective representation $\tilde{\rho} : G_{\mathbb{Q}} \to PGL_3(\bar{\mathbb{F}}_p)$ which cuts out K, and we need to examine the question of whether $\tilde{\rho}$ lifts to a special linear representation $\rho : G_{\mathbb{Q}} \to SL_3(\bar{\mathbb{F}}_p)$. (Note that $PSL_3(\bar{\mathbb{F}}_p) = PGL_3(\bar{\mathbb{F}}_p)$.) Now, a theorem of Neukirch (see [Neukirch 73, Satz 2.2]) says that such a ρ exists precisely if the "local lifting problem" can be solved for each place v on $\mathbb{Q}$. This means that for each place v of $\mathbb{Q}$, we have to find a lifting

$$\rho_v : G_v \to SL_3(\bar{\mathbb{F}}_p)$$

of $\tilde{\rho}|G_v : G_v \to PGL_3(\bar{\mathbb{F}}_p)$. Here G_v denotes the decomposition group at v. Also, the local lifting problem at v is always solvable if the order of $\tilde{\rho}(G_v)$ is not divisible by 9. This is an observation of Feit's (see [Feit 89, §6]). Indeed, let $Y = \tilde{\rho}(G_v)$, and suppose that Y does not have order divisible by 9. Let H be the inverse image of Y in $SL_3(\bar{\mathbb{F}}_p)$. Then H contains the center $Z \simeq C_3$ of $SL_3(\bar{\mathbb{F}}_p)$. Let W be the

Table 3
$3.A_6$ extensions

A_6 field	$3.A_6$?
2,3: #55	Yes
2,3: #57	Yes
2,3: #58	Yes
2,3: #59	Yes
2,5: #17	Yes
3,5: #7	Yes
3,5: #8	Yes
3,7: #3	Yes
3,13: #9	No
3,19: #3	Yes
5,17: #1	Yes
13,19: #1	No

Sylow 3-subgroup of Y, and X the Sylow 3-subgroup of H. Then either $W = 1$ and $X = Z$ or $W \simeq C_3$ and $X \simeq Z \times C_3$ (since $3.A_6$ has no elements of order 9). So the class of X in $H^2(W, Z)$ is trivial, and therefore the class of H in $H^2(Y, Z)$ is trivial ($\mathrm{res}^Y_W : H^2(Y, Z) \to H^2(W, Z)$ is injective). Therefore H splits as $Z \times Y$. So the local lifting problem is solvable. The theorem of Neukirch and the observation of Feit were pointed out to us by John Swallow.

Suppose that $v = q$ is unramified in K: if $g \in SL_3(\bar{\mathbb{F}}_p)$ is any lifting of $\tilde{\rho}(\mathrm{Frob}_q)$, we can define a lifting ρ_q by setting $\rho_q(\mathrm{Frob}_q) = g$ and $\rho_q(I_q) = 1$ (the point being that $G_q/I_q \simeq \hat{\mathbb{Z}}$). If $v = \infty$, then 9 does not divide the order of $\tilde{\rho}(G_\infty)$. Hence the possibly delicate cases occur when v is a finite prime which ramifies in K.

Table 3 below sets out what we have been able to find out about the question of whether the fields in Table 1 embed in a $3.A_6$ extension. We would like to thank David Roberts for resolving for us the harder cases (2,3#55, 3,5#8, and 3,7#7). Roberts also finds eighteenth degree polynomials whose splitting fields give the $3.A_6$ extensions when they exist. For a discussion of these questions, see his upcoming paper [Roberts].

4.3. An example: the A_6 extension ramified at 5 and 17

We discuss this example in some detail. (The calculations were done with PARI/GP, v. 2.1.4.) Let K be the splitting field of $T(x) = x^6 - 2x^5 + 5x^2 - 11x - 13$. This polynomial is 5,17:#1 from Table 1. The discriminant of the sextic field generated by a root of T is $5^8 17^2$, and $\mathrm{Gal}(K/\mathbb{Q}) \simeq A_6$.

First we show that K is contained in a $3.A_6$ extension $\tilde{K}$ of $\mathbb{Q}$. Let $\tilde{\rho} : G_{\mathbb{Q}} \to PGL_3(\bar{\mathbb{F}}_p)$ be the projective representation that cuts out K, where p is any prime except 3 (later we will take $p = 5$).

- Over $\mathbb{Q}_5$, T factors into a linear factor and a totally ramified quintic. So the Galois group of T over $\mathbb{Q}_5$ is a subgroup of A_5, hence does not have order divisible by 9.

- Over $\mathbb{Q}_{17}$, T factors into three quadratics, one unramified, one equal to $\mathbb{Q}_{17}(\sqrt{17})$; the third lies in the compositum of the other two. So the Galois group of T over $\mathbb{Q}_{17}$ is a four-group, and 4 is not divisible by 9.

Hence the local lifting problems are all solvable, so there is a representation $\rho : G_{\mathbb{Q}} \to SL_3(\bar{\mathbb{F}}_p)$. The kernel of the map $SL_3(\bar{\mathbb{F}}_p) \to PGL_3(\bar{\mathbb{F}}_p)$ is the center of $SL_3(\bar{\mathbb{F}}_p)$, and has order 3: so the fixed field of the kernel of ρ is a $3.A_6$-extension $\tilde{K}$ of $\mathbb{Q}$ containing K. Let $\tilde{G} = \mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq 3.A_6$; then $Z = \mathrm{Gal}(\tilde{K}/K)$ is the center of $\tilde{G}$.

Next we show that we can twist ρ by Dirichlet characters so that $\tilde{K}/K$ becomes an unramified extension. As noted in §2 above, we may assume that $\tilde{K}/K$ is unramified outside 5 and 17. Let k be the sixth degree extension of $\mathbb{Q}$ obtained from a root of T. Then $\mathrm{Gal}(\tilde{K}/k)$ is a triple cover of A_5; but since the Schur multiplier of A_5 is 2, $\mathrm{Gal}(\tilde{K}/k) \simeq C_3 \times A_5$. Hence there is a cyclic cubic extension $\tilde{k}/k$ which gives $\tilde{K}$, i.e. $\tilde{K} = \tilde{k}K$. Since we can and have assumed that $\tilde{K}/K$ is unramified outside 5 and 17, the conductor of $\tilde{k}/k$ must divide $5 \cdot 17$ (since the ramification over 5 and 17 in $\tilde{k}/k$ is must be tame).

According to PARI/GP (`bnrinit(bnfinit(T),5*17).clgp` gives us the order and the structure of the ray class group of conductor $5 \cdot 17$) the ray class group with conductor $5 \cdot 17$ has a unique quotient of order 3, which is in fact the ideal class group of k. So $\tilde{k}/k$ is the Hilbert class field of k, and so $\tilde{K}/K$ is unramified, too.

We now take $p = 5$, and find the level of $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_5)$. Let I_{17} be an inertia group of 17 in $G_{\mathbb{Q}}$; then the image I of I_{17} in $\tilde{G}$ has order 2. Let s be an element of I_{17} which maps to the nontrivial element of I; then we may assume that $\rho(s) = \mathrm{diag}(1, -1, -1)$ (since $\rho(s)$ has order 2 and $\det \rho = 1$). Hence M^{G_0} is one-dimensional. (Recall that $G_0 = \rho(I_{17}) \simeq I$.) On the other hand $G_1 = 1$, so the power of 17 in the level of ρ is 2, according to (1). Thus the level of ρ is 17^2.

We can in fact lower this by twisting by the quadratic character ε_{17} of conductor 17. Let $\rho' = \varepsilon_{17}\rho$. Then $\rho'(I_{17})$ still has order 2, since tame ramification is cyclic. Since $\varepsilon_{17}(s) = -1$ (this is because ε_{17} corresponds to the local extension $\mathbb{Q}_{17}(\sqrt{17})$, and s restricts to the nontrivial automorphism of $\mathbb{Q}_{17}(\sqrt{17})$), $\rho'(s) = \mathrm{diag}(-1, 1, 1)$, so M^{G_0} is two-dimensional for the twisted action. So ρ' has level 17 and nebentype ε_{17}.

4.3.1. Weights

To determine the weights predicted by the conjecture, we need to know how 5 ramifies in $\tilde{K}$. As noted above, T factors over $\mathbb{Q}_5$ into a linear factor and a totally ramified quintic $g(x)$. The polynomial $g(x + 1)$ is Eisenstein, and applying Proposition A.1 *bis* of the Appendix, we see that the polynomial $g_1(x) = x^5 - 5x^4 - 5$ generates the same extension of $\mathbb{Q}_5$. The Galois group of g_1 is either C_5 or D_{10} or M_{20}. M_{20} is ruled out because the discriminant of g_1 is a square. We can use the PARI/GP routine `polcompositum` to find a polynomial h (of degree 20) for an extension of $\mathbb{Q}$ containing two roots of $x^5 - 5x^4 - 5$. h factors over $\mathbb{Q}_5$ into two tenth degree polynomials; we take either of these, apply `polred`, and factor the resulting polynomials mod 5: some of these factor as $q^5 \bmod 5$, where q is an unramified quadratic. This means that the Galois group of g_1 is D_{10}, and that the splitting field of g_1 over $\mathbb{Q}_5$ is a

cyclic totally ramified fifth degree extension of the unramified quadratic extension of $\mathbb{Q}_5$. Thus the inertia group of 5 in $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order 5, and since $\tilde{K}/K$ is unramified at 5, we can say that the inertia group of 5 in $\tilde{G}$ is also cyclic of order 5. Hence the image $\rho'(I_5)$ of inertia in $GL_3(\bar{\mathbb{F}}_5)$ is unipotent, so the unique weight predicted by our conjecture is $(-2,-1,0)'(\varepsilon_{17}) = (6,3,0)(\varepsilon_{17})$.

4.3.2. Characteristic polynomials of Frobenius

We used the symbolic algebra system GAP [GAP] for information about the conjugacy classes and the characters of A_6 and $3.A_6$, and we use the notations of that system (in particular, the labeling of conjugacy classes) in what follows. Let X be the character of the representation ρ; then X is the reduction of the character of a three-dimensional representation of $3.A_6$ modulo a suitable prime above 5. The character values of X are as follows:

$$\begin{array}{rcccccccccccc}
A6: & 1a & 1a & 1a & 2a & 2a & 2a & 3ab & 4a & 4a & 4a & 5ab & 5ab & 5ab \\
3.A_6: & 1a & 3a & 3b & 2a & 6a & 6b & 3cd & 4a & 12a & 12b & 5ab & 15ac & 15bd \\
X: & 3 & 3z & 3z' & -1 & -z & -z' & 0 & 1 & z & z' & -2 & -2z & -2z'
\end{array}$$

Here z is a cube root of unity in $\mathbb{F}_{25}$, $z' = z^5$ its conjugate. Recall that there are 2 three-dimensional representations of $3.A_6$ over $\bar{\mathbb{F}}_5$; the other one is obtained by switching z and z'. We have collapsed the table according to the values of X: thus we have written $3cd$ for the union of the two conjugacy classes $3c$ and $3d$, on which X takes the common value 0. We call these collapsed classes ($3cd$, $5ab$, etc.) "coarse" conjugacy classes; we only need to know in which coarse conjugacy class an element of $3.A_6$ lies to determine the value of X on that element. Above each conjugacy class of $3.A_6$ we have listed its image in A_6.

For each prime $\ell \neq 5, 17$, we need to determine the characteristic polynomial $\det(1 - \rho'(\mathrm{Frob}_\ell)t)$ that appears in (2). For this it is enough to determine the coarse class of Frob_ℓ in $3.A_6$, since

$$\det(1 - \rho'(\mathrm{Frob}_\ell)t) = 1 - \varepsilon_{17}(\ell)X(\mathrm{Frob}_\ell)t + X(\mathrm{Frob}_\ell^{-1})t^2 - \varepsilon_{17}(\ell)t^3.$$

From the factorization of $T \bmod \ell$, we determine the cycle structure of Frob_ℓ as an element of A_6, which determines the coarse conjugacy class of Frob_ℓ in A_6 (the usual problem of distinguishing $5a$ and $5b$ thus disappears here).

Let Z be the center of $3.A_6$, and fix a generator c of Z. In the calculation that follows, we assume that $X(c) = 3z$, i.e. that c belongs to class $3a$. (If $X(c) = 3z'$, the calculation would be similar and the result would be the same.) Suppose that g is an element of A_6 of order prime to 3: then there is a *unique* element g' of $3.A_6$ of the same order which maps to g; and the other elements of $3.A_6$ which map to g are cg' and c^2g'.

Let ℓ be a prime other than 5 or 17, and let $s = \mathrm{Frob}_\ell|\tilde{K}$ be a Frobenius for ℓ in $\tilde{G}$. We distinguish two cases.

Case 1: $g = s|K$ has order prime to 3; then $s = c^i g'$ for some i, and we would like to determine i. We do this as follows:

Let $\mathfrak{P}$ be a prime above ℓ in K, and let $\tilde{\mathfrak{P}}$ be a prime above $\mathfrak{P}$ in $\tilde{K}$; we may assume that s is the Frobenius associated to $\tilde{\mathfrak{P}}/\ell$. Suppose that f is the residue degree of $\mathfrak{P}/\ell$: then

$$s^f = \text{the Frobenius associated to } \tilde{\mathfrak{P}}/\mathfrak{P} = (\mathfrak{P}, \tilde{K}/K),$$

so

$$c^{if} = (\mathfrak{P}, \tilde{K}/K),$$

since f is the order of g and g'. So $c^i = (\mathfrak{P}, \tilde{K}/K)^f$ (f is its own inverse mod 3), and thus

$$s = g'(\mathfrak{P}, \tilde{K}/K)^f.$$

We can ask PARI/GP to calculate $(\mathfrak{P}, \tilde{K}/K)$ by calculating the class of $\mathbf{N}_{K/k}\mathfrak{P}$ in the ideal class group of k: we have

$$(\mathbf{N}_{K/k}\mathfrak{P}, \tilde{k}/k) = (\mathfrak{P}, \tilde{K}/K)|\tilde{k}.$$

Finally, we need to find the coarse class of s. The class of $g = \mathrm{Frob}_\ell|K$ is determined by the cycle decomposition, and g' then lies in the unique class in $3.A_6$ with the same order. $(\mathfrak{P}, \tilde{K}/K)^f$ lies in $1a$, $3a$, or $3b$, according to whether it equals 1, c, or c^2. The class of $s = \mathrm{Frob}_\ell|\tilde{K}$ is then found by the rules $3a.5ab = 15ac$, etc. These relations can be read off from the character values of X.

Case 2: $g = s|K$ has order 3. There is only one coarse conjugacy class whose elements have order 3 in A_6, namely $3ab$, and it lifts to a unique coarse conjugacy class in $3.A_6$, namely $3cd$. So the coarse class of $s = \mathrm{Frob}_\ell|\tilde{K}$ is $3cd$ in this case.

We illustrate this calculation with an example. Suppose that $\ell = 2$, which has residue degree 5 in K; if $\mathfrak{P}$ is a prime above 2 in K, then we claim that $(\mathfrak{P}, \tilde{K}/K) = c$.

We first calculate the decomposition of 2 in k:

```
? T=x^6-2*x^5+5*x^2-11*x-13;
? k=nfinit(T);
? idealprimedec(k,2)
% = [[2, [1, 1, 0, 0, 0, 0]~, 1, 1, [0, 1, 0, 0, 1, 1]~],
     [2, [2, -1, 6, -10, -7, 23]~, 1, 5, [1, 1, 0, 0, 0, 0]~]]
```

So there are two primes above 2 in k, call them $\mathfrak{p}_1$ and $\mathfrak{p}_2$; $\mathfrak{p}_2$ has residue degree 5, so that if we choose a prime $\mathfrak{P}$ of K above $\mathfrak{p}_2$, we will have $f(\mathfrak{P}/\mathfrak{p}_2) = 1$ and $\mathfrak{p}_2 = \mathbf{N}_{K/k}(\mathfrak{P})$. So $\mathfrak{p}_2$ can be used directly to find $(\mathfrak{P}, \tilde{K}/K)$:

```
? bnfisprincipal(k,\%[2] )
% = [[1]~, [-3/5, 3/10, 2/5, -6/5, -9/10, 23/10]~, 344]
```

This says that $\mathfrak{p}_2$ lies in the ideal class of the generator that PARI/GP has chosen for the ideal class group of k: so $(\mathfrak{P}, \tilde{K}/K) = c$, as claimed, since we are identifying $\mathrm{Gal}(\tilde{K}/K)$ with $\mathrm{Gal}(\tilde{k}/k)$.

We find that the coarse class of $\mathrm{Frob}_2|\tilde{K}$ in $3.A_6$ is $(5ab)c^i$, where $c^i = (\mathfrak{P}, \tilde{K}/K)^f = c^5 = c^2$; so the coarse class of $\mathrm{Frob}_2|\tilde{K}$ is $15bd$.

5. Summary of calculations

We summarize here the calculations we have been able to complete. There are six cases in all for which we were able to test the conjecture. In the other cases, we determined that the level and weights were too big for computation at present.

In this table ε_{17} denotes the quadratic character with conductor 17, ω_4 the quadratic character with conductor 4, and ψ_8 the real quadratic character of conductor 8. We have omitted the nebentype if it is 1.

Recall that when $p = 5$ or 3 there are 2 irreducible three-dimensional representations of $3.A_6$ or A_6, respectively, each defined over $\mathbb{F}_{p^2}$ and conjugate over $\mathbb{F}_{p^2}$. Therefore, in each of the examples displayed in Table 4 the conjecture predicts 2 distinct Hecke eigenclasses, with eigenvalues in $\mathbb{F}_{p^2}$ and conjugate over $\mathbb{F}_{p^2}$, to which the corresponding Galois representations appear to be attached, in the sense explained in the introduction. This is indeed what we found. Of course, since the action of the Hecke algebra on cohomology is defined over $\mathbb{F}_p$, if we do find a Hecke eigenclass that appears to be attached to one of the two Galois representations, the conjugate eigenclass will appear to be attached to the other.

Note that verifying the $p = 3$ examples requires determining which of the Frobenii of order 5 are conjugate in A_6. We were able to do this in all cases except for Frob_2 in the level 13^2 example. In that case all we could determine is that Frob_2 has order 5. In this case, therefore, we could not check the equality (2), though our results do show that the left- and right-hand sides of (2) are either equal or conjugate over $\mathbb{F}_3$.

The first five of these examples take $p = 3$, and so use a representation $\rho : G_{\mathbb{Q}} \to GL_3(\bar{\mathbb{F}}_3)$ which cuts outs K; we don't need to know whether K embeds in a $3.A_6$ extension of $\mathbb{Q}$. But the case $3, 13 : \#9$, $p = 3$ is interesting because there is in fact no $3.A_6$ extension: so the representation ρ does not arise by reduction from a complex Galois representation.

In the second through fifth examples both the upper and the lower 2×2 block of $\rho|I_3$ are "très ramifiée," in the sense of Section 2.4 (ii) of [Serre 87]. In accordance with the conjecture, we predict and find in each case an appropriate Hecke eigenclass in weight (5,3,1). But we have also checked that there are no such eigenclasses in weights $(3, 3, 1)$, $(3, 1, 1)$, or $(1, 1, 1)$, which are the other possible ways of resolving the ambiguity in the procedure used to determine the weights.

The sixth example has $p = 5$, and therefore requires that K can be extended to a $3.A_6$ extension of $\mathbb{Q}$. This example was discussed in more detail in the previous section.

Table 4
Completed cases

A_6 field	$3.A_6$?	p	N, ε	Predicted weights
2,3: #55	Yes	3	2^8	(2,1,0)
2,3: #57	Yes	3	2^7, ψ_8	(5,3,1)
2,3: #58	Yes	3	2^7, $\omega_4\psi_8$	(5,3,1)
3,7: #3	Yes	3	7^2	(5,3,1)
3,13: #9	No	3	13^2	(5,3,1)
5,17: #1	Yes	5	17, ε_{17}	(6,3,0)

Remark. The isomorphism $A_6 \simeq PSL(2, \mathbb{F}_9)$ gives rise to a two-dimensional linear representation $\sigma : 2.A_6 \xrightarrow{\sim} SL(2, \mathbb{F}_9)$ of the double cover $2.A_6$. The symmetric square of this representation is trivial on the center of $2.A_6$, and in this way one can obtain the three-dimensional representations of A_6 underlying the $p = 3$ examples above. This raises the question of whether the representations $\rho : G_{\mathbb{Q}} \to SL_3(\bar{\mathbb{F}}_9)$ in the first five examples in Table 4 are symmetric squares of representations $\tau : G_{\mathbb{Q}} \to SL(2, \bar{\mathbb{F}}_9)$. If this were the case, then at least a weak form of our conjecture for these representations ρ could be deduced from Serre's Conjecture ([Serre 87]; see also the discussion in [Ash-Sinnott 00, §3(i)]).

However, this would require that the A_6 extensions in these examples embed in $2.A_6$ extensions. It is easy to see that they do not. All the 12 A_6 fields considered here are totally complex. If K is a totally complex A_6 extension of $\mathbb{Q}$, and $\hat{K}$ is a quadratic extension of K such that $\mathrm{Gal}(\hat{K}/\mathbb{Q}) \simeq 2.A_6$, let c be a complex conjugation in $\mathrm{Gal}(\hat{K}/\mathbb{Q})$. Since the only element of $2.A_6$ of order 2 lies in the center, it follows that c fixes K, which contradicts the fact that K is totally complex.

Appendix A. Polynomials and extensions of $\mathbb{Q}_p$

The aim of this appendix is to find useful estimates for how accurately one needs to know the coefficients of an irreducible polynomial over a local field in order to have determined (up to isomorphism) the field extension obtained by adjoining a root. When factoring polynomials over $\mathbb{Q}_p$, we need these estimates in order to determine the accuracy required in the factorization.

The arguments are taken from the paper of Pauli and Roblot [Pauli-Roblot], adapted very slightly for our different purpose.

We work over $\mathbb{Q}_p$, but the case of a general local field of characteristic 0 is no different. $|\cdot|$ denotes throughout the p-adic absolute value, normalized as usual by $|p| = 1/p$.

Suppose that $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}_p[x]$ is an irreducible polynomial, and let $\alpha_1, \ldots, \alpha_n$ be the roots of f (in $\bar{\mathbb{Q}}_p$). Let

$$\delta_f = \min_{i \neq j} |\alpha_i - \alpha_j|.$$

We can calculate δ_f by finding the largest finite slope λ in the Newton polygon of $f(x+\alpha_1)$. Then $\delta_f = |p|^{\lambda}$. A convenient way to calculate the Newton polygon of $f(x+\alpha_1)$ in PARI/GP is to work instead with $\tilde{f}(x) = \mathbb{N}_{\mathbb{Q}_p(\alpha_1)/\mathbb{Q}_p}(f(x+\alpha_1))$; then $\tilde{f}$ lies in $\mathbb{Z}_p[x]$ and has the same set of slopes as does f (the *multiplicities* of these slopes, however, will have been multiplied by n).

We may also use the following lower bound for δ_f:

Lemma A.1. *Let* $D_f = |\mathrm{disc}(f)|$: *then*

$$\delta_f \geqslant \left(\frac{D_f}{|a_n|^{n-2}}\right)^{1/n}.$$

Proof. We suppose that the roots of f have been numbered so that $\delta_f = |\alpha_1 - \alpha_2|$. Then we have

$$\begin{aligned} |f'(\alpha_1)| &= \prod_{i=2}^{n} |\alpha_1 - \alpha_i| \\ &= \delta_f \prod_{i=3}^{n} |\alpha_1 - \alpha_i| \\ &\leqslant \delta_f \prod_{i=3}^{n} \max(|\alpha_1|, |\alpha_i|) \\ &\leqslant \delta_f |a_n|^{(n-2)/n}. \end{aligned}$$

Since $D_f = |f'(\alpha_1)|^n$, the above inequality may be written

$$\delta_f \geqslant D_f^{1/n}/|a_n|^{(n-2)/n} \qquad \square$$

Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ and $g(x) = x^n + b_1 x^{n-1} + \cdots + b_n$ be irreducible polynomials in $\mathbb{Z}_p[x]$; let $\alpha_1, \ldots, \alpha_n$ be the roots of f and $\beta_1, \ldots, \beta_n$ be the roots of g. We consider the valuation of the resultant of f and g:

$$|R(f,g)| = \prod_{i,j=1}^{n} |\alpha_i - \beta_j| = \prod_{i=1}^{n} |g(\alpha_i)| = \prod_{j=1}^{n} |f(\beta_j)|.$$

Since f and g are irreducible, this can be written

$$|R(f,g)| = |g(\alpha_1)|^n = |f(\beta_1)|^n$$

We have the following upper estimate for $|R(f,g)|$:

Lemma A.2.

$$|R(f,g)|^{1/n} \leqslant |a_n|^{1/n} \max_{1\leqslant i\leqslant n} |b_i - a_i|$$

Proof.

$$\begin{aligned} |R(f,g)|^{1/n} &= |g(\alpha_1)| \\ &= |g(\alpha_1) - f(\alpha_1)| \\ &= \left|\sum_{i=1}^{n} (b_i - a_i)\alpha_1^i\right| \\ &\leqslant \max_{1\leqslant i\leqslant n} |b_i - a_i||a_n|^{i/n} \\ &\leqslant |a_n|^{1/n} \max_{1\leqslant i\leqslant n} |b_i - a_i| \end{aligned}$$

(since $|\alpha_1| = |a_n|^{1/n} \leqslant 1$). □

Next we derive an additional expression for $|R(f,g)|$. We suppose that the roots of g have been numbered so that $|\alpha_1 - \beta_1|$ is as small as possible. We have

$$|R(f,g)| = |g(\alpha_1)|^n = \prod_{j=1}^{n} |\alpha_1 - \beta_j|^n.$$

Now $|\alpha_1 - \beta_j| \geqslant |\alpha_1 - \beta_1|$ by our numbering; and we notice that

- if $|\alpha_1 - \beta_j| > |\alpha_1 - \beta_1|$, then

$$|\alpha_1 - \beta_j| = |\alpha_1 - \beta_j - (\alpha_1 - \beta_1)| = |\beta_1 - \beta_j|,$$

so

$$|\alpha_1 - \beta_j| = \max(|\alpha_1 - \beta_1|, |\beta_1 - \beta_j|);$$

- if $|\alpha_1 - \beta_j| = |\alpha_1 - \beta_1|$, then

$$\begin{aligned} |\beta_1 - \beta_j| &= |\beta_1 - \alpha_1 + \alpha_1 - \beta_j| \\ &\leqslant \max(|\beta_1 - \alpha_1||, |\alpha_1 - \beta_j|) \\ &= |\alpha_1 - \beta_1|, \end{aligned}$$

so again we have

$$|\alpha_1 - \beta_j| = \max(|\alpha_1 - \beta_1|, |\beta_1 - \beta_j|);$$

Thus we have

$$|R(f,g)|^{1/n} = \prod_{j=1}^{n} \max(|\alpha_1 - \beta_1|, |\beta_1 - \beta_j|)$$

and in the same way, reversing the roles of f and g:

$$|R(f,g)|^{1/n} = \prod_{i=1}^{n} \max(|\alpha_1 - \beta_1|, |\alpha_1 - \alpha_i|).$$

We put these together to obtain a criterion for f and g to give the same extension of $\mathbb{Q}_p$, i.e. for $\mathbb{Q}_p[x]/(f(x)) \simeq \mathbb{Q}_p[x]/(g(x))$:

Proposition A.1. *If f and g are irreducible and if*

$$\max_{1 \leqslant i \leqslant n} |b_i - a_i| < \delta_f \left(\frac{D_f}{|a_n|}\right)^{1/n}$$

or if

$$\max_{1 \leqslant i \leqslant n} |b_i - a_i| < \left(\frac{D_f^2}{|a_n|^{n-1}}\right)^{1/n}$$

—then f and g give the same extension of $\mathbb{Q}_p$.

Proof. Assume that f and g give different extensions of $\mathbb{Q}_p$; then by Krasner's Lemma,

$$\delta_f \leqslant |\alpha_i - \beta_j|$$

for all i and j.

We give a lower bound on $|R(f,g)|$ based on this inequality.

$$|R(f,g)|^{1/n} = \prod_{i=1}^{n} \max(|\alpha_1 - \beta_1|, |\alpha_1 - \alpha_i|)$$

$$\begin{aligned}
&\geqslant \prod_{i=1}^{n} \max(\delta_f, |\alpha_1 - \alpha_i|) \\
&= \delta_f \prod_{i=2}^{n} \max(\delta_f, |\alpha_1 - \alpha_i|) \\
&= \delta_f \prod_{i=2}^{n} |\alpha_1 - \alpha_i| \\
&= \delta_f |f'(\alpha_1)| \\
&= \delta_f D_f^{1/n}.
\end{aligned}$$

So the first inequality in the statement of the proposition leads to a contradiction with Lemma A.2. The second inequality implies the first, by Lemma A.1, and so leads to a contradiction as well. □

Finally, we rewrite these results using the p-adic valuation ord_p. Let $d = \mathrm{ord}_p \mathrm{disc}(f)$; let $a = \mathrm{ord}_p(a_n)$; and let $\lambda = \max_{i \neq j} \mathrm{ord}_p(\alpha_i - \alpha_j)$. Then we have

Lemma A.1 bis.

$$\lambda \leqslant \frac{d - (n-2)a}{n}.$$

Proposition A.1 bis. *If k is an integer such that*

$$k > \lambda + \frac{d-a}{n}$$

or such that

$$k > \frac{2d - (n-1)a}{n},$$

Then any monic irreducible polynomial of degree n congruent to $f \bmod p^k$ gives the same extension of $\mathbb{Q}_p$ as f.

Caveat: The second polynomial *must* be irreducible for the result to apply. If we simply calculate k and find a monic polynomial $g \in \mathbb{Z}_p[x]$ such that $f \equiv g \bmod p^k$, it can happen that g is reducible and fails to give the same extension of $\mathbb{Q}_p$. For example, let $p = 2$ and let $f = x^3 - 2$; then $d = 2$, $a = 1$, so that $(2d - (n-1)a)/n = 2/3$ and we may take $k = 1$. We cannot take $g = x^3$, but the Proposition does say that any irreducible polynomial $g \equiv x^3 \bmod 2$ gives the same extension as f.

References

[Ash-Doud-Pollack 02] A. Ash, D. Doud, D. Pollack, Galois representations with conjectural connections to arithmetic cohomology, Duke Math. J. 112 (2002) 521–579.

[Ash-Pollack-Soares] A. Ash, D. Pollack, D. Soares, $SL_3(\mathbb{F}_2)$-Galois representations and arithmetic cohomology modulo 2, preprint.

[Ash-Sinnott 00] A. Ash, W. Sinnott, An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of $GL(n, \mathbb{Z})$, Duke Math. J. 105 (2000) 1–24.

[CR] C. Curtis, I. Reiner, Methods of Representation Theory, vol. 1, Wiley Interscience, New York, 1981.

[Crespo-Hajto] T. Crespo, Z. Hajto, The Valentiner group as Galois group, Proc. Amer. Math. Soc. 133 (2005) 51–56.

[Feit 89] W. Feit, Some finite groups with non-trivial centers which are Galois groups, in: K.N. Cheng, Y.K. Leong (Eds.), Group Theory, Proceedings of the Singapore Group Theory Conference 1987, Walter de Gruyter, Berlin, New York, 1989, , pp. 87–109.

[GP] PARI/GP, Version 2.1.4. The PARI Group, Bordeaux. Available: http://www.pari.math.u-bordeaux.fr.

[GAP] GAP4, Version: 4.3fix4. Available: http://www.gap-system.org.

[Jones 98] J. Jones, Tables of Number Fields with Prescribed Ramification: Sextics (September 21, 1998) [ONLINE]. Available: http://hobbes.la.asu.edu/Number_Fields/sextics.html [March 22, 2003].

[Jones-Roberts 03] J. Jones, D. Roberts, Database of Local Fields (September 9, 2003) [ONLINE]. Available: http://math.asu.edu/jj/localfields/[November 1, 2003].

[Neukirch 73] J. Neukirch, Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. Math. 21 (1973) 59–116.

[Pauli-Roblot] S. Pauli, X. Roblot, On the computation of all extensions of a p-adic field of a given degree, Math. Comp. 70 (236) (2001) 1641–1659 (electronic).

[Roberts] 3.G number fields for G a sextic or septic group, in preparation.

[Serre 71] J.-P. Serre, Représentations Linéaires des Groupes Finies, 2nd ed., Hermann, Paris, 1971.

[Serre 77] J.-P. Serre, Modular forms of weight one and Galois representations, in: A. Fröhlich (Ed.), Algebraic Number Fields (L-functions and Galois properties), Academic Press, London, 1977, .

[Serre 87] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987) 179–230.