AN EXPLICIT GALOIS REPRESENTATION ON THE MOD-3 HECKE ALGEBRA

ANNA MEDVEDOVSKY

Abstract. We describe in detail the structure of the space of modular forms modulo 3 of level one and all weights, and its Hecke algebra, including the compatible $(\mathbb{Z}/3\mathbb{Z})^\times$-grading on both spaces. We construct the associated Galois representations on the Hecke algebra and study the localizations of these representations modulo prime ideals. Finally we give an explicit matrix realization of this representation.

1. Modular forms mod 3 and their Hecke algebra

We use the French convention that $\mathbb{N}$ is the set of nonnegative integers $\{0, 1, 2, \dots, \}$.

1.1. **The space of forms.** For $k \geq 0$ even, let $M_k(1, \mathbb{Z})$ be the space of modular forms of weight k and level 1 with coefficients in $\mathbb{Z}$, and $M_k = M_k(1, \mathbb{F}_3) \subset \mathbb{F}_3[\![q]\!]$ the image of $M_k(1, \mathbb{Z}_3)$ under the map "form q-expansions and reduce them modulo 3":

$$M_k := \operatorname{im}\left(M_k(1, \mathbb{Z}) \xrightarrow{q\text{-exp}} \mathbb{Z}[\![q]\!] \to \mathbb{F}_3[\![q]\!]\right) \subset \mathbb{F}_3[\![q]\!].$$

Since the Eisenstein series E_4 and E_6 both have image 1 in M_4 and M_6, respectively, we know that M_k sits inside both M_{k+4} and M_{k+6}. To circumvent this inconvenience, let $M := \sum_k M_k \subset \mathbb{F}_3[\![q]\!]$ be the algebra of *all* modular forms mod 3 of level one. Swinnerton-Dyer observed in [19] that $M = \mathbb{F}_3[\Delta]$, where $\Delta = q\prod(1 - q^n)^{24} \in \mathbb{F}_3[\![q]\!]$ is the image of the normalized weight-12 cuspform.

In fact, dimension formulas imply that $\{1, \Delta, \dots, \Delta^{\lfloor k/12 \rfloor}\}$ is an $\mathbb{F}_3$-basis for M_k, unless $k \equiv 2 \bmod 12$, in which case we lose $\Delta^{\lfloor k/12 \rfloor}$. To eliminate this minor nuisance, we switch notation slightly and replace M_k by $M_{\leq k} := \sum_{k' \leq k} M_k \subset \mathbb{F}_3[\![q]\!]$. In other words, for $k \equiv 2 \bmod 12$ we replace M_k by M_{k-2}; the M_k for $k \not\equiv 2 \bmod 12$ are unchanged.

With this adjustment, the standard notion of *weight filtration* on M is now trivially equivalent to the Δ-degree filtration, which we will use instead.

Date: December 23, 2016.

1.2. **Hecke operators.** The Hecke operators act on f in M in the usual way on q-expansions. Since the weight k is always even, we have that $\ell^{k-1} \equiv \ell \bmod 3$ for all ℓ prime. A priori this is only true as soon as $\ell \neq 3$ or $k > 1$, but because the M_k nest inside M Hecke-compatibly, we actually have that for any ℓ prime and $f = \sum_{n \geq 0} a_n(f) q^n \in M$,

$$a_n(T_\ell f) = \begin{cases} a_{\ell n}(f) + \ell a_{n/\ell}(f) & \text{if } \ell \,|\, n \\ a_{\ell n}(f) & \text{otherwise.} \end{cases}$$

The operator T_3 coincides modulo 3 with the Atkin-Lehner U_3 operator, which we will write here as U. The notation T_ℓ will be reserved for the Hecke operator at a prime $\ell \neq 3$. As in the theory of p-adic modular forms (for example, [9]), U is also a left inverse (retraction) of the Frobenius operator $F : f(q) \mapsto f(q^3)$, which here modulo 3 coincides with the cubing operator $f \mapsto f^3$.

Let $K \subset M$ be the kernel of U, and $K_k := U \cap M_k$. These are Hecke-invariant subspaces of M.

1.3. **The Hecke algebra on M and K.** We introduce the so-called *shallow* Hecke algebra on M_k and on M, generated by the action of the prime-to-3 Hecke operators. For k even, let $A_k \subset \mathrm{End}(M_k)$ be the commutative subalgebra of $\mathbb{F}_3$-linear endomorphisms of M_k generated by the action of the Hecke operators T_n with n prime to 3: this is the Hecke algebra on M_k.

Since $M_k \subset M_{k+2}$, we have surjections $A_{k+2} \twoheadrightarrow A_k$. Set $A := \varprojlim_k A_k \subset \mathrm{End}(M)$: this is the Hecke algebra on M, topologically generated by the action of the prime-to-3 Hecke operators, a profinite $\mathbb{F}_3$-algebra. It is not difficult to show that, with the compact-open topology[(*)] on $\mathrm{End}(M)$ induced from the discrete topology on M, the algebra A is the closed algebra topologically generated inside $\mathrm{End}(M)$ by the action of the prime-to-3 Hecke operators.

In fact, A is also the Hecke algebra on $K = \ker U$, and moreover A and K are topological A-linear duals of each other:

Proposition 1. *(1) K is a faithful A-module.*

(2) Under this restriction, A is the closed subalgebra of $\mathrm{End}(K)$ topologically generated by the action of the prime-to-3 Hecke operators.

(3) The pairing $A \times K \to \mathbb{F}_3$ defined by $(T, f) \mapsto a_1(Tf)$ is continuous and nondegenerate on both sides.

(4) It induces isomorphisms of A-modules $A \xrightarrow{\sim} \mathrm{Hom}(K, \mathbb{F}_3)$ and $K \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(A, \mathbb{F}_3)$.

The proofs are not difficult. See [10, Theorem 6.3], [4, appendix], and [15, section 5] for closely related statements in the literature, or [12, Proposition 2.32] for full details.

[(*)] Under the compact-open topology on $\mathrm{End}(M)$, a system of open neighborhoods around $0 \in \mathrm{End}(M)$ is given by annihilators of an exhaustive sequence of finite-dimensional subspaces, such as the M_k.

1.4. **A is a complete local noetherian $\mathbb{F}_3$-algebra.** The Hecke algebra A is a semilocal ring and factors as a product of localizations at its maximal ideals, which correspond to $\mathrm{Gal}(\overline{\mathbb{F}}_3/\mathbb{F}_3)$-orbits of A-eigenforms appearing in K. Hecke eigeforms appearing in K, in turn, correspond to semisimple odd Galois representations $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ unramified outside $\{3, \infty\}$ so that we have a correspondence between maximal ideals of A and modular Galois representations.[(†)] The following observation of Serre establishes that A is a local ring:

Theorem (Serre [17], following Tate [20])**.**
The only semisimple odd $\overline{\mathbb{F}}_3$-representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ unramfied outside $\{3, \infty\}$ is $1 \oplus \omega$, where ω is the mod-3 cyclotomic character.

A number of facts follow:

(1) The only cuspidal eigenform in M is Δ, and $a_\ell(\Delta) = 1 + \ell$ for all primes ℓ prime to 3.
(2) Write T'_ℓ for the *modified Hecke operator* $T_\ell - a_\ell(\Delta) = \begin{cases} 1 + T_\ell & \text{if } \ell \equiv 1 \bmod 3 \\ T_\ell & \text{if } \ell \equiv 2 \bmod 3. \end{cases}$
Then T'_ℓ acts locally nilpotently on M, so that $\deg_\Delta(Tf) < \deg_\Delta f$ for any $f \in M$.
(3) A is a complete local noetherian ring whose maximal ideal $\mathfrak{m}$ is generated by the modified Hecke operators T'_ℓ.

In particular (3) relies on constructions from deformation theory of pseudocharacters [16] to establish that A is noetherian, which implies that the profinite topology coincides with the local topology [12, Proposition 2.9].

1.5. **The grading on the space of forms.** For $n \in (\mathbb{Z}/3\mathbb{Z})^\times$, let $M^i := \mathbb{F}_3\langle\, \Delta^n : n \equiv i \bmod 3 \,\rangle$, so that $M = M^0 \oplus M^1 \oplus M^2$ is a $\mathbb{Z}/3\mathbb{Z}$-graded $\mathbb{F}_3$-algebra.

Proposition 2.
(1) $M^i = \{f \in M : a_n(f) \neq 0 \implies n \equiv i \bmod 3\}$.
(2) For $\ell \neq 3$ prime, the Hecke operator T_ℓ acts compatibly with the grading: $T_\ell M^i \subset M^{\ell i}$.

Proof. To prove (1) for Δ, use the fact that Δ is an eigenform with $a_3(\Delta) = 0$ and $a_\ell(\Delta) = 1 + \ell$ for $\ell \neq 3$ prime, as well as the algebraic relationships between Hecke eigenvalues. The general case follows formally: if $f = \sum a_n(f)q^n$ and $g = \sum a_n(g)q^n$ have the property that $a_n(f)$ is nonzero only

[(†)] See [1, Chapter I] for the eigenalgebra construction. The construction of $\bar{\rho}$ is due to Deligne via the Deligne-Serre lifting lemma. Serre Reciprocity implies that there correspondence is between maximal ideals of A and *all* $\mathrm{Gal}(\overline{\mathbb{F}}_3/\mathbb{F}_3)$-orbits of semisimple odd Galois representations unramified outside $\{3, \infty\}$, but it is not strictly necessary here.

for n is some congruence class i_f modulo some N, and similarly $a_n(g) \neq 0$ only if $n \equiv i_g \bmod N$, then fg has the property that $a_n(f+g) = \sum_{r+s=n} a_r(f)a_s(g)$ is nonzero only if $n \equiv i_f + i_g \bmod N$.

For (2), use (1), the action of a Hecke operator on q-expansions, and the happy accident that $\ell \equiv \ell^{-1} \bmod 3$. (A similar happy accident gives us a mod-8 grading on the space of modular forms of level one mod 2: see [14].) □

The proposition above implies that $K = \mathbb{F}_3\langle \Delta^n : (n,3) = 1\rangle = M^1 \oplus M^2$ is a $(\mathbb{Z}/3\mathbb{Z})^\times$-graded Hecke-invariant submodule of M. For $i \in (\mathbb{Z}/3\mathbb{Z})^\times$, let $K^i := M^i$.

The elements of $K^1 \cup K^2$ (that is, the homogeneous elements of K) will be called *graded*.

1.6. **The structure of A.** Refining [4, appendix] very slightly, define four disjoint sets of primes prime to 3:

$$\mathcal{P}_x = \{\ell : \ell \equiv 2 \bmod 9\}; \quad \mathcal{P}_{-x} = \{\ell : \ell \equiv 5 \bmod 9\};$$
$$\mathcal{P}_y = \{\ell : \ell \equiv 1 \bmod 3 \text{ but } 3 \text{ is not a cube mod } \ell\};$$
$$\mathcal{P}_0 = \{\ell : \ell \neq 3 \text{ and } \ell \text{ is not in } \mathcal{P}_x \cup \mathcal{P}_{-x} \cup \mathcal{P}_y\}.$$

Note that

$$\mathcal{P}_{\pm x} := P_x \cup \mathcal{P}_{-x} = \{\ell : \mathrm{Frob}_\ell \text{ generates } \mathrm{Gal}\left(\mathbb{Q}(\mu_9)/\mathbb{Q}\right)\}$$
$$\mathcal{P}_y = \{\ell : \mathrm{Frob}_\ell \text{ generates } \mathrm{Gal}\left(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q}(\mu_3)\right)\}.$$

Theorem 3. *The map $\mathbb{F}_3[\![x,y]\!] \to A$ sending x to $T_2' = T_2$ and y to $T_7' = 1 + T_7$ is an isomorphism of topological $\mathbb{F}_3$-algebras. Under this isomorphism, for $\alpha \in \{x, -x, y, 0\}$ we have $T_\ell' \equiv \alpha \mod \mathfrak{m}^2$ if and only if $\ell \in \mathcal{P}_\alpha$.*

Surjectivity follows from deformation theory for reducible pseudocharacters as developed in [2]; see [4, appendix] for the short version or [12, Chapter 7] for details. For injectivity, it suffices to prove that the Krull dimension of A is at least 2. This theorem is stated in [4, appendix] by Bellaïche; the proof is completed by the main theorem of [13]. See also [12, Chapter 8].

From now on, we will write x for T_2 and y for T_7', so that $A = \mathbb{F}_3[\![x,y]\!]$.

1.7. **The grading on A.** Endow $A \cong \mathbb{F}_3[\![x,y]\!]$ with a $(\mathbb{Z}/3\mathbb{Z})^\times$-grading as follows: x is weighed 2 and y weighted 1, and the grading is extended to monomials multiplicatively. In other words, $A^1 = \mathbb{F}_3[\![x^2, y]\!]$ and $A^2 = xA^1$, so that $A = A^1 \oplus A^2$.

Proposition 4. *(1) K is a graded A-module.*

(2) For $i \in (\mathbb{Z}/3\mathbb{Z})^\times$, we have $A^i = \{T \in A : T(K^1) \subset K^i \text{ and } T(K^2) \subset K^{2i}\}$.

(3) For $\ell \neq 3$ prime, both T_ℓ and T'_ℓ are in A^ℓ.

Proof. (1) We have established that $T^\ell(K^i) \subset K^{\ell i}$ in Proposition 2. In particular, x^2 and y preserve the graded components of K, and x maps K^1 into K^2 and vice versa. Therefore $A^iK^j \subset K^{ij}$, so that K is a graded A-module.

(2) This a formal statement about faithful graded modules. Let $B^i := \{T \in A : T(K^j) \subset K^{ij} \text{ for } j = \pm 1\}$. From (1) we know that $A^i \subset B^i$, and seek the other inclusion. Suppose $T \in B^1$. Using the decomposition $A = A^1 \oplus A^2$, write $T = T^1 + T^2$ with $T^i \in A^i$. For $i = (\mathbb{Z}/3\mathbb{Z})^\times$, we know that, on one hand, $T^2 = T - T^1$ maps K^i into K^i by assumption on T and by (1) for T^1. On the other hand, T^2 maps K^i into K^{2i} by (1) for T^2. Since $K^i \cap K^{2i} = \{0\}$, we have $T^2(K^i) = 0$. But since A acts faithfully on K, we actually have $T^2 = 0$, so that $T = T^1$. Therefore $B^1 \subset A^1$. The other case is completely analogous.

(3) Proposition 2 and (2).

□

1.8. **The dual basis on K.** By the duality between K and A (Proposition 1), given any isomorphism $\mathbb{F}_3[\![x, y]\!] \xrightarrow{\sim} A$ (equivalently, a choice of two parameters x and y whose images in the cotangent space $\mathfrak{m}/\mathfrak{m}^2$ are an $\mathbb{F}_3$-basis), there exists a unique basis $\{m(a, b) : a, b \in \mathbb{N}\}$ of K *adapted to* the pair of generators (x, y) satisfying

(1) If $a > 0$, then $x \cdot m(a, b) = m(a - 1, b)$, and $x \cdot m(0, b) = 0$.
(2) If $b > 0$, then $y \cdot m(a, b) = m(a, b - 1)$, and $y \cdot m(a, 0) = 0$.
(3) $m(0, 0) = \Delta$ and $a_1(m(a, b)) = 0$ unless $(a, b) = (0, 0)$.

Given the compatible grading on K and A, we want to restrict ourselves to parameters compatible with the grading. Call parameters (X, Y) of A *graded parameters* if $X \in A^2 \cap (\mathfrak{m} - \mathfrak{m}^2)$ and $Y \in A^1 \cap (\mathfrak{m} - \mathfrak{m}^2)$.

Proposition 5. *Suppose that (X, Y) are graded parameters of A. Then:*

(1) $X \equiv \pm x \bmod \mathfrak{m}^2$ and $Y \equiv \pm y \bmod \mathfrak{m}^2$;
(2) x and X generate the same ideal of A;
(3) $A^1 = \mathbb{F}_3[\![X^2, Y]\!]$ and $A^2 = XA^1$;
(4) the element $m(a, b)$ of the basis adapted to (X, Y) is graded, and namely in K^{2^a}.

Moreover,

(5) if $\ell_x \in \mathcal{P}_{\pm x}$ and $\ell_y \in \mathcal{P}_y$ are any two primes, then $(T_{\ell_x}, 1 + T_{\ell_y})$ is a pair of graded parameters for A.

Proof. Item (1) is clear by considering bases of $\mathfrak{m}/\mathfrak{m}^2$. For (2), since X is in both $A^2 = x\mathbb{F}_3[\![x^2, y]\!]$ and in $\pm x + \mathfrak{m}^2$, it's clear that $X = x\,u$ for some $u \in (A^1)^\times$. This also establishes the last part of (3). Further, since Y is in both $A^1 = \mathbb{F}_3[\![x^2, y]\!]$ and in $\pm y + \mathfrak{m}^2$, we must have $Y = yu' + f$ for some unit $u \in (A^1)^\times$ and some power series $f \in x^2\mathbb{F}_3[\![x^2]\!]$. Therefore $X^2 = x^2u^2$ and Y are parameters for A^1 (that is, their images give a basis of the cotangent space of A^1), which establishes the first part of (3). Item (4) follows by induction from the definition of an adapted basis and a formal description of K^i similar to the formal description of A^i in Proposition 4(2). Finally, (5) follows from Theorem 3 and Proposition 4(3). □

With a little linear algebra, we can compute elements of the basis $m(a, b)$ adapted to $(x, y) = (T_2, 1+T_7)$:

$$m(0,0) = \Delta \qquad m(1,1) = \Delta^{11} + 2\Delta^8 + 2\Delta^5$$
$$m(0,1) = 2\Delta^{10} + \Delta^7 \qquad m(2,0) = \Delta^{10} + 2\Delta^7 + \Delta^4$$
$$m(1,0) = \Delta^2 \qquad m(0,3) = 2\Delta^{82} + \Delta^{55} + \Delta^{34} + \Delta^{31} + \Delta^{25} + \Delta^{22} + 2\Delta^{19}$$
$$m(0,2) = \Delta^{28} + \Delta^{19} + 2\Delta^{16} + \Delta^{13} \qquad m(1,2) = 2\Delta^{29} + 2\Delta^{17} + 2\Delta^{14} + \Delta^8 + \Delta^5$$
$$m(2,1) = \Delta^{28} + \Delta^{19} + 2\Delta^{16} + 2\Delta^{10} \qquad m(3,0) = 2\Delta^{11} + \Delta^8$$

A list of forms $m(a, b)$ adapted to $(T_2, 1 + T_7)$ for $a + b \leq 17$, computed using `SAGE`, is available at `http://math.brown.edu/~medved/Data/mab3upto17.txt`.

2. The Galois group associated to A

In this section, we study the Galois group through which the Galois pseudocharacter carried by the Hecke algebra factors. The starting-off point is the theorem of Deligne that associates, to a level-one Hecke eigenform f of weight k a Galois representation $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ factoring through $G_{\mathbb{Q},p}$, the maximal extension of $\mathbb{Q}$ unramified outside $\{p, \infty\}$ and satisfying $\mathrm{tr}\,\rho_f(\mathrm{Frob}_\ell) = a_\ell(f)$ for any prime $\ell \neq p$.

2.1. **The Galois group associated to a residually reducible level-one ρ.** As above, we begin with a continuous representation $\rho_f : G_{\mathbb{Q},p} \to \mathrm{GL}_2(L)$ defined over some finite extension L over $\overline{\mathbb{Q}}_p$ associated to a level-one Hecke eigenform of some weight k with coefficients in L. Choosing a Galois-stable integral lattice of L and reducing modulo the maximal ideal, we get a mod-p representation $\bar{\rho}_f : G_{\mathbb{Q},p} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, well defined up to semisimplifcation. If $\bar{\rho}$ is reducible, then $\mathrm{tr}\,\bar{\rho}_f = \omega^a + \omega^b$, where $\omega : G_{\mathbb{Q},p} \to {\mathbb{F}_p}^\times$ is the mod-p cyclotomic character, and we can deduce that ρ_f itself factors through a quotient of $G_{\mathbb{Q},p}$.

More precisely, let E_p be the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p. Let $G_p = \mathrm{Gal}(E_p/\mathbb{Q})$, so that G_p is a quotient of $G_{\mathbb{Q},p}$; and let $H_p = \mathrm{Gal}\left(E_p/\mathbb{Q}(\mu_p)\right)$ so that we have an exact sequence

$$1 \to H_p \to G_p \to \mathrm{Gal}\left(\mathbb{Q}(\mu_p)/\mathbb{Q}\right) \to 1.$$

We claim that any residually reducible modular representation ρ_f attached to a level-1 form over $\overline{\mathbb{Q}}_p$ will factor through G_p. We state this in a slightly more general context: suppose $\mathcal{O}$ is any local pro-p ring (such as $\mathcal{O} = \mathbb{Z}_p$ or $\mathcal{O} = \mathbb{F}_{p^2}[\![x, y, z]\!]$), $\mathfrak{m}_\mathcal{O}$ the maximal ideal of $\mathcal{O}$, and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O})$ a representation unramified outside p.

Proposition 6. *If the trace* $\mathrm{tr}\,\rho$ *modulo* $\mathfrak{m}_\mathcal{O}$ *is a sum of powers of the mod-p cyclotomic character, then* ρ *factors through* $\mathrm{Gal}(E_p/\mathbb{Q})$.

Proof. Write $\mathbb{F}_\mathcal{O} = \mathcal{O}/\mathfrak{m}_\mathcal{O}$ for the residue field of $\mathcal{O}$. From the assumptions, the restriction of the residual representation $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\mathcal{O})$ to $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)\right)$ is unipotent. Since both the kernel $1 + M_2(\mathfrak{m}_\mathcal{O})$ of the reduction map $\mathrm{GL}_2(\mathcal{O}) \to \mathrm{GL}_2(\mathbb{F}_\mathcal{O})$ and any unipotent subgroup of $\mathrm{GL}_2(\mathbb{F}_\mathcal{O})$ are pro-p, the claim follows. □

The next theorem of Shafarevich completely determines the structure of H_p in the case that $p > 2$[‡] is a regular prime.

Theorem (Shafarevich, [18], p. 82, example after Theorem 5)**.**
If $p > 2$ is a regular prime, then H_p is a free pro-p group on $\frac{p+1}{2}$ generators.

2.2. **Generators for the Galois group of a reducible level-one ρ.** We continue the notation from the previous section. Moreover, let K_p be $\mathbb{Q}(\mu_p)$ and $\Delta_p = \mathrm{Gal}(K/\mathbb{Q})$, and let $h_p = \frac{p+1}{2}$ Recall that we have an exact sequence of Galois groups

$$1 \to H_p \to G_p \to \Delta_p \to 1,$$

and if $p > 2$ is a regular prime then Theorem 2.1 (Shafarevich) implies that H_p is a free pro-p group on h_p generators.

Theorem 7. *If $p > 2$ is a regular prime, and $\bar{\rho} = \omega_p^a + \omega_p^b$, then G_p is topologically generated by two elements, σ and γ, where*

(1) the image of σ in Δ_p generates;
(2) γ is in H_p, and the h_p elements γ, $\sigma\gamma\sigma^{-1}$, …, $\sigma^{h_p-1}\gamma\sigma^{-h_p+1}$ are free prop-p generators of H_p.

[‡]For the case $p = 2$, see Markshaitis [11]: $H_2 = G_2$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by a free pro-2 group on 2 generators.

Proof. We drop the p subscript and write H, G, Δ, ω, K, h.

Recall that a set of elements generates a pro-p group if and only if their images generate its p-Frattini (that is, maximal abelian exponent-p) quotient. Let $\widetilde{H}$ be the p-Frattini quotient of H, and let $\widetilde{K}$ be its fixed field. From Shafarevich's theorem, we know that $\widetilde{H}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^h$. From the exact sequence $1 \to \widetilde{H} \to \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \to \Delta \to 1$, we further know that Δ acts on $\widetilde{H}$ by conjugation. This is an action of a group of $p-1$ elements on a finite $\mathbb{F}_p$-vector space, so it breaks up into a sum of characters of $\Delta \to {\mathbb{F}_p}^\times$. These characters are all powers of ω, so that

$$\widetilde{H} = \bigoplus_{0 \le k < p-1} \widetilde{H}[\omega^k].$$

Each $\widetilde{H}[\omega^k]$ is still an abelian exponent-p group, so a direct sum of elementary p-groups. In fact, we can use Kummer theory, the Dirichlet Unit Theorem, and the reflection principle to understand $\widetilde{H}[\omega^k]$ quite precisely.

Lemma 8.

$$\dim_{\mathbb{F}_p} \widetilde{H}[\omega^k] = \begin{cases} 1 & \textit{if } k = 0 \textit{ or } k \textit{ is odd} \\ 0 & \textit{otherwise.} \end{cases}$$

Indeed, by Kummer theory, any elementary p-extension of K is given by adjoining a p^{th} roots of some element α of $K^\times$; the extension is then unramified outside p if and only if α is a unit except possibly at the prime above p. Letting $\mathcal{O}_p^\times$ be the away-from-p units of $K^\times$, we see that the different size-p-subextensions of E will be given by various α in $\widetilde{\mathcal{O}}_p := \mathcal{O}_p^\times/(\mathcal{O}_p^\times)^p$. A refinement of the Dirichlet Unit Thoerem tells us that this is also an abelian group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^h$, and that its action by Δ similarly breaks up into ω^k-eigenspaces

$$\widetilde{\mathcal{O}}_p = \bigoplus_{0 \le k < p-1} \widetilde{\mathcal{O}}_p[\omega^k];$$

further the ω^k-eigenspace has dimension 1 if $k = 1$ or is even, and zero otherwise. Finally, the reflection principle tells us that, for $\alpha_k \in \widetilde{\mathcal{O}}_p[\omega^k]$, we have

$$\mathrm{Gal}\left(K(\alpha_k^{\frac{1}{p}})/K\right) = \widetilde{H}[\omega^{1-k}].$$

(It is not difficult to see that $\widetilde{H}[\omega^0] = \mathrm{Gal}\left(\mathbb{Q}(\mu_{p^2})/K\right)$, that $\widetilde{H}[\omega^1] = \mathrm{Gal}(K(p^{\frac{1}{p}})/K)$, and if $p = 1 \bmod 4$ then $\widetilde{H}[\omega^{\frac{p+1}{2}}] = \mathrm{Gal}(K(u^{\frac{1}{p}})/K)$ where u is a fundamental unit of $\mathbb{Q}(\sqrt{p}) \subset K$.)

With Lemma 8 dispatched, we return to the main argument. Choose a generator g of $\mathbb{F}_p^\times$, and let σ be any element of G that satisfies $\omega(\sigma) = g$. For $k = 0$ or $1 \le k < p-1$ odd, let γ_k be an element of H mapping to a generator of $\widetilde{H}[\omega^k]$, and set $\gamma := \prod_k \gamma_k$. I claim that the image $\bar{\gamma}$ in $\widetilde{H}$ generates a basis for $\widetilde{H}$ under the conjugation action of σ.

Indeed, the defining property of $\bar{\gamma}_k$ (the bar denotes image in $\widetilde{H}$) is that

$$\sigma \cdot \overline{\gamma}_k = \overline{\sigma \gamma_k \sigma^{-1}} = \overline{\gamma}_k^{\omega(\sigma)^k} = \overline{\gamma}_k^{g^k}$$

so that $\sigma^2 \cdot \overline{\gamma}_k = \left(\overline{\gamma}_k^{g^k}\right)^{g^k} = \overline{\gamma}_k^{g^{2k}}$ and more generally $\sigma^i \cdot \overline{\gamma}_k = \overline{\gamma}_k^{g^{ik}}$. To see that $\overline{\gamma}, \sigma \cdot \overline{\gamma}, \ldots, \sigma^{h-1} \cdot \overline{\gamma}$ is a basis for $\widetilde{H}$, we start with the known basis

$$\overline{\gamma}_0, \overline{\gamma}_1, \overline{\gamma}_3, \ldots, \overline{\gamma}_{p-2}$$

and verify that the change-of-basis matrix is invertible. The i^{th} column of the change-of-basis matrix corresponds to

$$\sigma^i \cdot \overline{\gamma} = \overline{\gamma}_0^{g^{0i}} \overline{\gamma}_1^{g^{1i}} \overline{\gamma}_3^{g^{3i}} \cdots \overline{\gamma}_{p-2}^{g^{(p-2)i}}$$

so that the change-of-basis matrix (note that we've been using multiplicative notation) is

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ g & g^2 & g^3 & \cdots & g^{h-1} \\ g^3 & g^6 & g^9 & \cdots & g^{3(h-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g^{p-2} & g^{(p-2)2} & g^{(p-2)3} & \ldots & g^{(p-2)(h-1)} \end{pmatrix}.$$

This is a Vandermonde matrix with determinant

$$\prod_{\substack{k,k' \in \{0,1,3,\ldots,p-2\} \\ k<k'}} (g^k - g^{k'})^2,$$

visibly nonzero since g is a generator of $\mathbb{F}_p^\times$.

Finally, since the σ^i conjugates of $\overline{\gamma}$ generate $\widetilde{H}$, the σ^i conjugates of γ generate H, as claimed.

□

Note that, for $p > 3$, Theorem 7 will not give a proper presentation of G as a topological group — we do not a priori know anything about $\sigma \in G$. The exception is the case $p = 3$, in which the exact sequence $1 \to H \to G \to \Delta \to 1$ splits by a choice of complex conjugation. (Something similar happens for $p = 2$; see [11] and unpublished work of Serre.)

2.3. **The Galois group of interest in the case $p = 3$.**

We want to apply Theorem 7 to the case $p = 3$ and study the structure of $G = G_3$. Set $H = H_3$. The exact sequence $1 \to H \to G \to \mathrm{Gal}\left(\mathbb{Q}(\mu_3)/\mathbb{Q}\right) \to 1$ splits by any choice of complex conjugation c lifting that of $\mathrm{Gal}\left(\mathbb{Q}(\mu_3)/\mathbb{Q}\right)$. Shafarevich's theorem implies that G is a semidirect product $H \rtimes \{1, c\}$, where H is a free pro-3 group on 2 generators. We begin with an abstract study of this type of group.

Definition (after Serre, unpublished)**.** A group Γ will be called an *M_3-group* if Γ is profinite, and topologically generated by two elements g and c with $c^2 = 1$ satisfying the following:

the closed subgroup $\Gamma^1 := \overline{\langle g, cgc\rangle}$ topologically generated by g and cgc is a free pro-3 group.

In other words Γ is an M_3-group if it is a split extension of $\mathbb{Z}/2\mathbb{Z}$ by a free pro-3 group generated by two elements a and b where the action of $\mathbb{Z}/2\mathbb{Z}$ exchanges a and b.

If Γ is an M_3-group, we will call any pair (g, c) satisfying the definition above a *pinning* of Γ. Let $\Phi \subset \Gamma^1$ be its 3-Frattini subgroup, generated by the cubes of elements of Γ^1. (Recall that a pro-3 group is generated by any set that generates its 3-Frattini quotient.) Since Γ^1 is free pro-3 of rank 2, we have $\Gamma^1/\Phi \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, generated by $\bar{g}$ and $\overline{cgc}$. (Here for any element $\gamma \in \Gamma^1$, we write $\overline{\gamma}$ for its image in Γ^1/Φ.)

Proposition 9. *(1) Γ^1 is the set of squares of elements in Γ.*

(2) Γ^1 does not depend on the pinning.

(3) If (g, c) is a pinning of Γ, and $n \in \mathbb{Z}$ prime to 3, then (g^n, c) and (cg^n, c) are also pinnings of Γ.

Proof. On one hand, the square of any element in Γ certainly lies in Γ^1 since the quotient $\Gamma/\Gamma^1 = \{1, c\}$ has order 2. On the other hand, any $\gamma \in \Gamma^1$ is a square. Indeed, the closed group generated by γ is the free cyclic pro-3 group, isomorphic to $\mathbb{Z}_3$. Therefore $\gamma^{\frac{1}{2}} = \lim_{n\to\infty} \gamma^{-(1+3+\cdots+3^n)}$ is a square root of γ. So Γ^1 is indeed the set of squares of elements of Γ, and hence independent of the pinning. Similarly, for n prime to 3, the elements g and g^n generate the same closed subgroup, as do cgc and $cg^nc = (cgc)^n$. Therefore (g^n, c) and (cg^nc, c) are also pinnings. More generally, for $\gamma \in \Gamma^1 - \Phi$, the pair (γ, c) is a pinning of Γ if and only if $\overline{c\gamma c} \notin \{\overline{\gamma}, \overline{\gamma}^{-1}\}$. □

Question. We will identify the Galois group G_3 as M_3-group, so it is natural to ask if it is true that any order-2 element of Γ is conjugate to c? (Serre has shown that this is true in G_2, but that group is pro-2 so the same methods do not apply.) Similarly, what is the centralizer of c in an M_3-group Γ?

Following unpublished work of Bellaïche, we define two subgroups of an M_3-group Γ with pinning (g, c). Let $\mathrm{Ab}(\Gamma) := [\Gamma, \Gamma]$ be the derived subgroup, the closed normal subgroup generated by $cgcg^{-1}$, and $\mathrm{Di}(\Gamma)$ be the closed normal subgroup generated by $cgcg$.

A group G will be called *dihedral* (or *G^1-dihedral*) if G contains an abelian index-2 subgroup G^1 and an order-2 element c so that $c\gamma c = \gamma^{-1}$ for every $\gamma \in G^1$. In other words, G is a split extension of the form $1 \to G^1 \to G \to \{1, c\} \to 1$ where c acts on G^1 by inversion.

Proposition 10. *Let Γ be an M_3-group with pinning (g, c).*

(1) $\Gamma/\operatorname{Ab}(\Gamma)$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_3^\times$, topologically generated by the image of gc.
(2) $\Gamma/\operatorname{Di}(\Gamma)$ is a $\mathbb{Z}_3$-dihedral group, with the index-2 subgroup generated by g.

Let G be a topological group, and $\varphi : \Gamma \to G$ a continuous surjective homomorphism. Then

(3) G is an abelian group if and only if $\operatorname{Ab}(\Gamma) \subset \ker(\varphi)$
(4) G is a dihedral group if and only if $\operatorname{Di}(\Gamma) \subset \ker(\varphi) \subsetneq \Gamma$.
(5) $\operatorname{Ab}(\Gamma)$ and $\operatorname{Di}(\Gamma)$ do not depend on the pinning.
(6) $\operatorname{Ab}(\Gamma)$ and $\operatorname{Di}(\Gamma)$ are contained in Γ^1 and contain its derived subgroup $[\Gamma^1, \Gamma^1]$.
(7) Both $\operatorname{Ab}(\Gamma)/[\Gamma^1, \Gamma^1]$ and $\operatorname{Di}(\Gamma)/[\Gamma^1, \Gamma^1]$ are free pro-3 cyclic groups, generated by the images of g.

Proof. We prove (4); the other statements are variation on similar themes. We make use of a simple lemma:

Lemma 11. *Every nontrivial quotient of a dihedral group is dihedral.*

Proof of Lemma. Let G be G^1-dihedral, and suppose that $H \subset G$ is a normal subgroup. If $H \subset G^1$, then G/H is a (G^1/H)-dihedral group. Otherwise, H contains an element c of $G - G^1$; I claim that in this case, H also contains the subgroup $2G^1 \subset G^1$ consisting of squares of elements in G^1. Indeed, for $g \in G^1$, we have $gcg^{-1} = (gc)c(gc)^{-1} = g^2c$, so that the conjugacy class of c is exactly $(2G^1)c$. On the other hand, since H contains c and $(2G^1)c$, it also contains $2G^1$. So H contains $(2G^1) \cup (2G^1)c$. More precisely, letting $H^1 := H \cap G^1$ we must have $G^1 \supset H^1 \supset 2G^1$, and G/H is (G^1/H^1)-dihedral. (Note that $G^1/2G^1$, and hence G^1/H^1, is a 2-torsion group. If V is 2-torsion, then a V-dihedral group is abelian, isomorphic to $V \times \mathbb{Z}/2\mathbb{Z}$.) □

And now if $\ker\varphi$ contains $\operatorname{Di}(\Gamma)$, then by (2), G is a quotient of a $\mathbb{Z}_3$-dihedral group, hence dihedral if nontrivial. Conversely, if G is a G^1-dihedral group, and $\Gamma \to G$ is surjective, I claim that $\varphi(\Gamma^1) = G^1$. Indeed, we know that $\varphi(\Gamma^1) = \varphi(2\Gamma) \subset 2G \subset G^1$. Therefore, $\varphi(\Gamma - \Gamma^1) \subset G - G^1$, and since φ is surjective all the containments are in fact equalities. But now $\varphi(g)^{-1} = \varphi(c)\varphi(g)\varphi(c)$, so that $cgcg \in \ker\varphi$.

□

Finally we return to the Galois setting for forms mod 3 and the notation of Section 2.1.

Theorem 12. *The Galois group $G = G_3 = \mathrm{Gal}(E_3/\mathbb{Q})$ is an M_3-group. A pinning is given by (g, c) where c is any complex conjugation, and g is an element of $G^1 = H_3 = \mathrm{Gal}(E_3/\mathbb{Q}(\mu_3))$ whose images generate both $\mathrm{Gal}\left(\mathbb{Q}(\mu_9)/\mathbb{Q}(\mu_3)\right)$ and $\mathrm{Gal}\left(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q}(\mu_3)\right)$.*

In particular, if $c \in G$ be any complex conjugation, and $\ell \equiv 4$ or $7 \bmod 9$ is a prime with 3 is not a cube modulo ℓ, then (Frob_ℓ, c) is a pinning of G. This includes $\ell = 7, 13, 31, 43, 79, 97$.

Proof. Shafarevich's theorem (Section 2.1) is the starting-off point. To understand the generators: the 3-Frattini quotient of G^1 is $\mathrm{Gal}\left(\mathbb{Q}(\mu_9, \sqrt[3]{3})/\mathbb{Q}(\mu_3)\right)$, the compositum of the first steps in the cyclotomic and the anticyclotomic extensions of $\mathbb{Q}(\mu_3)$. Let $a \in G^1/\Phi$ be any element that generates $\mathrm{Gal}(\mathbb{Q}(\mu_9)/\mathbb{Q}(\mu_3))$ but fixes $\sqrt[3]{3}$, so that a and c together generate $\mathrm{Gal}(\mathbb{Q}(\mu_9)/\mathbb{Q}) \cong (\mathbb{Z}/9)^\times$. Let $b \in G^1/\Phi$ fix μ_9 but generate $\mathrm{Gal}(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q}(\mu_3))$, so that b and c together generate $\mathrm{Gal}(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q}) \cong \mathbb{S}_3$. Then the two elements together ab and ab^{-1} generate G^1/Φ), and c permutes them by conjugation. See Theorem 7 for a more conceptual approach.

Finally, let $g \in G^1$ be any lift of ab. Then cgc is a lift of ab^{-1}, so that g and cgc are generators of the free pro-3 group G^1. Another description of any such g is that it move both $\sqrt[3]{3}$ and μ_9 over μ_3.

□

3. The Galois representation carried by A

This subsection and the next loosely follow Bellaïche's treatment in [3] of the case $p = 2$.

As in section 2, let E_3 is the maximal pro-3 extension of $\mathbb{Q}(\mu_3)$ unramified outside 3, $G = \mathrm{Gal}(E_3/\mathbb{Q})$, and $G^1 = \mathrm{Gal}(E_3/\mathbb{Q}(\mu_3))$. Let $G^2 = G - H$. As in section 1, let $A = \mathbb{F}_3[\![x, y]\!]$ be the completed Hecke algebra acting on M, with graded parameters (x, y) and grading $A^1 = \mathbb{F}_3[\![x^2, y]\!]$ and $A^2 = x\mathbb{F}_3[\![x^2, y]\!]$. Let F be the field of fractions of A.

In general, a *continuous pseudocharacter of dimension* 2 of a group Γ to a topological ring $B \ni \frac{1}{2}$ is a continuous map $t : \Gamma \to B$ designed to mimick the algebraic behavior of the trace of a two-dimensional representation of Γ over B. Specifically, for all $g, h \in \Gamma$, we have $t(gh) = t(hg)$ — that is, t is *central* — and

$$t(gh) + d(g)t(g^{-1}h) = t(g)t(h),$$

where $d = \det t : \Gamma \to B^\times$ is the map $d(g) = \frac{t(g)^2 - t(g^2)}{2}$.

Pseudocharacters have been studied by Rouquier in [16] and Chenevier in [6], where they are called *determinants*. We use Chenevier's definitions but Rouquier's terminology.

Theorem 13.

(1) *There is a unique continuous pseudocharacter* $t : G \to A$ *satisfying* $t(\mathrm{Frob}_\ell) = T_\ell$ *for* $\ell \neq 3$ *prime. Its determinant is* $\det(t) = \omega$. *Moreover:*
   (a) t *is* **universal** *in the following sense: if* B *is a noetherian local* $\mathbb{F}_3$*-algebra, and* $\tau : G \to B$ *is a continuous pseudocharacter with* $\tau \equiv 1 + \omega$ *modulo* $\mathfrak{m}_B$ *and* $\det \tau = \omega$, *then* τ *factors through* t.
   (b) t *is* **graded**: *For* $i \in (\mathbb{Z}/3)^\times$, *we have* $t(G^i) \subset A^i$.
   (c) *If* (g, c) *is a pinning of* G, *then* $\big(t(cg), 1 + t(g)\big)$ *is graded pair of parameters for* A.
(2) *There exists a unique representation* $r : G \to \mathrm{GL}_2(F)$ *satisfying* $\operatorname{tr} r(\mathrm{Frob}_\ell) = T_\ell$ *for* $\ell \neq 3$ *prime. Its determinant is* ω. *It is absolutely irreducible.*

The construction of t is a standard one; see, for example, [3]. The universality follows from the isomorphism $\mathcal{R} \cong A$, where R is the universal ring parametrizing deformations of $1 + \omega$ as a pseudocharacter to profinite local $\mathbb{F}_3$-algebras. The compatibility of t with the grading follows from the Chebotarev density theorem since we already know that $T_\ell \in A^\ell$. The existence of r over $\bar{F}$ follows from the theory of pseudocharacters. This representation descends to F because it is odd. It is absolutely irreducible because A is the universal deformation ring of $\bar{t} = 1 + \omega$, and, for example, Bellaïche gives an irreducible deformation of $\bar{t}$ to $\mathbb{F}_3[\varepsilon]$ factoring through $\mathrm{Gal}(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q})$ in [4, appendix].

3.1. **The specializations of the Galois representations on** A**.** Choose a free G-stable lattice Λ of r as follows: A (not necessarily free) G-stable lattice Λ' of r exists because the trace lands in A[(§)] Since A is a regular local ring of dimension 2, a lattice will be free if and only if it is reflexive. Therefore the double dual of Λ' will be both free and G-stable.

Write r_Λ for the action of G on Λ and $r_{\Lambda,B}$ for the action of G on $\Lambda \otimes B$ for any extension $A \to B$ of rings. Write $r_{\Lambda,\mathfrak{p}}$ for $r_{\Lambda,k(\mathfrak{p})}$, where $\mathfrak{p} \subset A$ is a prime ideal and $k(\mathfrak{p})$ is its residue field, and $r_\mathfrak{p}^{\mathrm{ss}}$ for its semisimplification. Let $t_\mathfrak{p} := \operatorname{tr} r_{\Lambda,\mathfrak{p}}$. (We suppress Λ from notation whenever the relevant object does not depend on it.)

We already know that $r_{(0)} = r$ is absolutely irreducible, and that $r_\mathfrak{m}^{\mathrm{ss}} = 1 \oplus \omega$. We study $r_{\Lambda,\mathfrak{m}}$ and $r_{\Lambda,\mathfrak{p}}$ for primes $\mathfrak{p}$ of height 1, which are all principal. Let $\mathfrak{p}_0 \subset A$ be the prime ideal generated by

$$y - P_\alpha(x^2) + 2 = y - x^2 - x^{10} + x^{12} - x^{14} - x^{16} + O(x^{28}),$$

where $\alpha = \frac{\log_3 7}{\log_3 4} \in \mathbb{Z}_3$ with $\log_3$ the 3-adic logarithm, and $P_\alpha \in \mathbb{F}_3[\![u]\!]$ is the power series satisifying $P_\alpha(z + z^{-1} - 2) = z^\alpha + z^{-\alpha}$. Recall that H is the index-2 free pro-3 subgroup of G.

(§)This relies on an unpublished argument of Bellaïche. Alternatively, use [7, Proposition 1.6.1] to construct a free A-lattice directly.

Theorem 14.

(1) *The residual representation* $r_{\Lambda,\mathfrak{m}}$ *is indecomposable. Moreover,* $r_{\mathfrak{m}}|_H \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ *is a non-trivial extension in* $\mathrm{H}^1_{\mathrm{cont}}(H, \mathbb{F}_3) = \mathrm{Hom}_{\mathrm{cont}}(H, \mathbb{F}_3)$ *corresponding to* $\mathrm{Gal}(\mathbb{Q}(\mu_3, \sqrt[3]{3})/\mathbb{Q}(\mu_3))$.

(2) *If* $\mathfrak{p} \neq \mathfrak{p}_0$ *is a prime of height* 1*, then* $r_{\mathfrak{p}}$ *is absolutely irreducible. If further* $\mathfrak{p} \neq (x)$*, then* $r_{\mathfrak{p}}$ *is strongly absolutely irreducible: it stays absolutely irreducible restricted to any finite-index subgroup of* G.

(3) *The represenation* $r_{\Lambda,\mathfrak{p}_0}$ *is reducible over* $A/\mathfrak{p}_0 \subset k(\mathfrak{p}_0)$*. Its trace is* $t_{\mathfrak{p}_0} = \chi + \omega\chi^{-1}$*, where* $\chi : G^{\mathrm{ab}} = \mathbb{Z}_3^\times \to (A/\mathfrak{p}_0)^\times = \mathbb{F}_3[\![x]\!]^\times$ *is the continuous character defined by* $\chi(\mathrm{Frob}_2) = -x + \sqrt{1+x^2}$.

(4) *The image of* $r_{\Lambda,(x)}$ *is dihedral, and* $r_{\Lambda,(x)} = \mathrm{Ind}_H^G \psi$*, where* ψ *is a character of* $H/\mathrm{Di}(G)$ *defined over a quadratic extension of* $A/(x) = \mathbb{F}_3[\![y]\!]$ *and characterized by setting* $\psi(\mathrm{Frob}_7) = -y \pm \sqrt{y+y^2}$*. In particular* $r_{\Lambda,(x)}|_H = \psi + \psi^{-1}$ *is irreducible over* $k(\!(x)\!)$.

Corollary 15. *Up to* A*-isomorphism, there are exactly two* G*-representations* $r^\pm : G \to \mathrm{GL}_2(A)$ *satisfying* $\mathrm{tr}\, r^\pm(\mathrm{Frob}_\ell) = T_\ell$ *for* $\ell \neq 3$ *prime, distinguished by* $r^+_{\mathfrak{m}} \sim \begin{pmatrix} 1 & * \\ 0 & \omega \end{pmatrix}$ *and* $r^-_{\mathfrak{m}} \sim \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$*. Both are continuous and satisfy* $\mathrm{tr}(r^\pm) = t$ *and* $\det(r^\pm) = \omega$*. They are twists of each other by* ω*. They are isomorphic over* F.

Proof. Let V be the representation r_K. Any A-representation r satisfying $\mathrm{tr}\, r(\mathrm{Frob}_\ell) = T_\ell$ must become isomorphic to V when base-changed to K, so we may view any such as a free G-stable A-lattice inside V. Let Λ' and Λ be two such; since they are reflexive, they are completely determined by their localizations at height-1 primes. For all but finitely many $\mathfrak{p}$, we a priori have $\Lambda_{\mathfrak{p}} = \Lambda'_{\mathfrak{p}}$, so we may scale Λ' by an element of K to guarantee $\mathfrak{p}\Lambda \subsetneq \Lambda' \subset \Lambda$ for all $\mathfrak{p}$. But in our case, for $\mathfrak{p} \neq \mathfrak{p}_0$, we further have $r_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}/\mathfrak{p}\Lambda_{\mathfrak{p}}$ irreducible, so that $\Lambda_{\mathfrak{p}} = \Lambda'_{\mathfrak{p}}$. Finally, $\Lambda_{\mathfrak{p}_0}/\mathfrak{p}_0\Lambda_{\mathfrak{p}_0}$ is reducible but not indecomposable, so there are exactly two choices for $\Lambda'_{\mathfrak{p}_0}$: either $\Lambda'_{\mathfrak{p}_0} = \Lambda_{\mathfrak{p}_0}$, or $\Lambda'_{\mathfrak{p}_0}/\mathfrak{p}\Lambda_{\mathfrak{p}_0}$ is the G-invariant line in $r_{\Lambda,\mathfrak{p}_0}$, and the two choices will alter which mod-$\mathfrak{m}$ character appears as the invariant sub. Therefore both occur. See [5] for the theory of reflexive modules over a noetherian normal domain. □

3.2. **The Galois representation over A explicitly.** We give an explicit matrix realization of the representations analyzed in the previous section with respect to a pinning of G. The construction is inspired by an explicit unpublished construction of Serre for $p = 2$ of the representation defined by

Bellaïche in [3]. Serre credits W. Goldman's exposition of work of Fricke and Vogt for the particular matrices: see [8].

Let Γ be an M_3-group with pinning (g,c), and let $B = \mathbb{F}_3[\![x,y]\!]$ be an abstract power series ring with $\mathfrak{m}_B$ its maximal ideal. Let $\alpha^{\pm} \in B$ be two elements satisfying $\alpha^{-1} - \alpha = x$. Namely,

$$\alpha^{\pm} = x \pm \sqrt{1+x^2} = x \pm (1 - x^2 + x^4 + x^6 - x^8 + x^{10} + x^{18} + \cdots).$$

For $\alpha = \alpha_+, \alpha_-$, define three matrices in $\mathrm{GL}_2(B)$:

$$M_g = \begin{pmatrix} y-1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad M_h = \begin{pmatrix} 0 & \alpha^{-2} \\ -\alpha^2 & y-1 \end{pmatrix}, \qquad M_c = \begin{pmatrix} 0 & \alpha^{-1} \\ \alpha & 0 \end{pmatrix}.$$

Proposition 16. *For each choice of α, the map $\rho : \Gamma \to \mathrm{GL}_2(B)$ defined by $\rho(g) = M_g$, $\rho(cgc) = M_h$, and $\rho(c) = M_c$ defines a continuous representation. Moreover, ρ^+ and ρ^- are isomorphic over* $\operatorname{Frac} B$ *but not over B.*

Proof. Check that $M_c^2 = 1$ and $M_c M_g M_c = M_h$. And modulo $\mathfrak{m}_B$ we see that $\overline{M}_g = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ and $\overline{M}_h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ land in the same order-3 subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$, which means that M_g and M_h lie in some pro-3 subgroup of $\mathrm{SL}_2(B)$, so that ρ extends continuously to H and then to G. One can check explicitly that the matrix $X = \begin{pmatrix} \alpha^2(y-1) & -1-\alpha^2) \\ 1+\alpha^2 & -y+1 \end{pmatrix}$ intertwines ρ^+ and ρ^-, but $\det X \equiv -y \bmod \mathfrak{m}_B^2$, so that $X \notin \mathrm{GL}_2(B)$. □

One can also check explicitly the following:

(1) $\rho^+_{\mathfrak{m}_B}$ is the nonsplit extension of the nontrivial character of Γ/Γ^1 by the trivial character, and $\rho^-_{\mathfrak{m}_B}$ is the nonsplit extension of same characters in the other order.
(2) $\rho_{B/I}$ is reducible if and only if $I \supset \big(y + y^2 - x^2\big) = \big(y - 1 + \sqrt{1+x^2}\big)$.
(3) $\rho_{B/I}\big|_{\Gamma^1}$ is reducible if and only if $I \supset \big(y + y^2 - x^2\big)$ or $I \supset \big(x\big)$.

We now return to our Galois group G and our Hecke algebra H.

Corollary 17. *For any pinning (g,c) of G the two represenations $r^{\pm}$ from Corollary 15 can be realized explicitly:*

$$r^{\pm}(g) = \begin{pmatrix} t(g) & -1 \\ 1 & 0 \end{pmatrix}, \qquad r^{\pm}(cgc) = \begin{pmatrix} 0 & (\alpha^{\pm})^{-2} \\ -(\alpha^{\pm})^2 & t(g) \end{pmatrix}, \qquad r^{\pm}(c) = \begin{pmatrix} 0 & (\alpha^{\pm})^{-1} \\ \alpha^{\pm} & 0 \end{pmatrix}.$$

Here $\alpha^{\pm} = t(cg) \pm \sqrt{1 + t(cg)^2} \in A$.

Proof. A semisimple continous representation of Γ whose determinant is the nontrivial character of Γ/Γ^1 over a field K is defined uniquely by the K-triple $(\mathrm{tr}(g), \mathrm{tr}(c), \mathrm{tr}(cg))$: a consequence of the pseudocharacter identity. □

References

[1] Bellaïche, J. *Eigenvarieties, families of Galois representations, p-adic L-functions*. Unpublished course notes. Available at `http://people.brandeis.edu/~jbellaic/preprint/coursebook.pdf`.

[2] Bellaïche, J. Pseudodeformations. *Mathematische Zeitschrift 270*, 3-4 (2012), 1163–1180.

[3] Bellaïche, J. Une représentation galoisienne universelle attachée aux formes modulaires modulo 2. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[4] Bellaïche, J., and Khare, C. Level 1 Hecke algebras of modular forms modulo p. *Compositio Mathematica 151*, 3 (2015), 397–415. Older version at `http://people.brandeis.edu/~jbellaic/preprint/Heckealgebra6.pdf`.

[5] Bourbaki, N. *Algèbre Commutative*. Chapter 7, Section 4.3, Theorem 3.

[6] Chenevier, G. The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings. In *Proceedings of the LMS Durham Symposium: Automorphic forms and Galois representations* (2011). Available at `http://gaetan.chenevier.perso.math.cnrs.fr/articles/determinants.pdf`.

[7] Chenevier, G., and Bellaïche, J. *Families of Galois representations and Selmer groups*.

[8] Goldman, W. An exposition of results of Fricke and Vogt. `http://arxiv.org/pdf/math/0402103.pdf`.

[9] Gouvêa, F. *Arithmetic of p-adic modular forms*, vol. 1304 of *Lecture Notes in Mathematics*. Springer-Verlag, 1985.

[10] Jochnowitz, N. A study of the local components of the Hecke algebra mod l. *Transactions of the American Mathematical Society 270*, 1 (1982), 253–267.

[11] Markshaitis, G. On p-extensions with a single critical number. *Izvestiya akademii nauk SSSR 27* (1963), 463–466. In Russian.

[12] Medvedovsky, A. Lower bounds on dimensions of mod-p Hecke algebras: The nilpotence method. Ph.D. thesis, 2015. Available at `http://www.math.brown.edu/~medved/Mathwriting/DissertationMedvedovsky_Fall2015.pdf`.

[13] Medvedovsky, A. Nilpotence order growth of recursion operators in characteristic p. Preprint at `http://www.math.brown.edu/~medved/Mathwriting/Nilgrowth.pdf`.

[14] Nicolas, J.-L., and Serre, J.-P. Formes modulaires modulo 2 : l'ordre de nilpotence des opérateurs de Hecke modulo 2. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[15] Nicolas, J.-L., and Serre, J.-P. Formes modulaires modulo 2 : structure de l'algèbre de Hecke. *Comptes rendus mathématique. Académie des Sciences. Paris 350* (2012).

[16] Rouquier, R. Caractérisation des caractères et pseudo-caractères. *Journal of Algebra 180*, 2 (1996), 571–586.

[17] Serre, J.-P. *Œuvres. Vol. III*. Springer-Verlag, Berlin, 1986, p. 710. Note 229.2.

[18] Shafarevich, I. R. Extensions with prescribed ramification points. *Publications Mathématiques de l'IHES*, 18 (1963), 71–95.

[19] Swinnerton-Dyer, H. P. F. On l-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*. Springer, Berlin, 1973, pp. 1–55. Lecture Notes in Math., Vol. 350.

[20] Tate, J. The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2. In *Arithmetic geometry (Tempe, AZ, 1993)*, vol. 174 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1994, pp. 153–156.