9

Galois Representations

This book has explained the idea that all elliptic curves over $\mathbf{Q}$ arise from modular forms. Chapters 1 and 2 introduced elliptic curves and modular curves as Riemann surfaces, and Chapter 1 described elliptic curves as algebraic curves over $\mathbf{C}$. As a general principle, information about mathematical objects can be obtained from related algebraic structures. Elliptic curves already form Abelian groups. Modular curves do not, but Chapter 3 showed that the complex vector space of weight 2 cusp forms associated to a modular curve has dimension equal to the genus of the curve, Chapter 5 defined the Hecke operators, linear operators that act on the vector space, and Chapter 6 showed that integral homology is a lattice in the dual space and is stable under the Hecke action.

As number theorists we are interested in equations over number fields, in particular elliptic curves over $\mathbf{Q}$. Chapter 7 showed that modular curves are defined over $\mathbf{Q}$ as well. As another general principle, information about equations can be obtained by reducing them modulo primes p. Chapter 8 reduced the equations of elliptic curves and modular curves to obtain similar relations for the two kinds of curve: for an elliptic curve E over $\mathbf{Q}$,

$$a_p(E) = \sigma_{p,*} + \sigma_p^* \qquad \text{as an endomorphism of } \mathrm{Pic}^0(\widetilde{E}),$$

while for the modular curve $X_0(N)$ the Eichler–Shimura Relation is

$$T_p = \sigma_{p,*} + \sigma_p^* \qquad \text{as an endomorphism of } \mathrm{Pic}^0(\widetilde{X}_0(N)).$$

These relations hold for all but finitely many p, and each involves different geometric objects as p varies.

Using more algebraic structure, this last chapter lifts the two relations from characteristic p to characteristic 0. For any prime ℓ the ℓ-power torsion groups of an elliptic curve give rise to a vector space $V_\ell(E)$ over the *ℓ-adic number field* $\mathbf{Q}_\ell$. Similarly, the ℓ-power torsion groups of the Picard group of a modular curve give an ℓ-adic vector space $V_\ell(X)$. The vector spaces $V_\ell(E)$

and $V_\ell(X)$ are acted on by the *absolute Galois group* of $\mathbf{Q}$, the group $G_{\mathbf{Q}}$ of automorphisms of the algebraic closure $\overline{\mathbf{Q}}$. This group subsumes the Galois groups of all number fields, and it contains *absolute Frobenius elements* $\mathrm{Frob}_{\mathfrak{p}}$ for maximal ideals $\mathfrak{p}$ of $\overline{\mathbf{Z}}$ lying over rational primes p. The vector spaces $V_\ell(X)$ are also acted on by the Hecke algebra. The two relations in the previous paragraph lead to the relations

$$\mathrm{Frob}_{\mathfrak{p}}^2 - a_p(E)\mathrm{Frob}_{\mathfrak{p}} + p = 0 \qquad \text{as an endomorphism of } V_\ell(E)$$

and

$$\mathrm{Frob}_{\mathfrak{p}}^2 - T_p\,\mathrm{Frob}_{\mathfrak{p}} + p = 0 \qquad \text{as an endomorphism of } V_\ell(X_0(N)).$$

These hold for a dense set of elements $\mathrm{Frob}_{\mathfrak{p}}$ in $G_{\mathbf{Q}}$, but now each involves a single vector space as $\mathrm{Frob}_{\mathfrak{p}}$ varies. The second relation connects the Hecke action and the Galois action on the vector spaces associated to modular curves.

The vector spaces V_ℓ are *Galois representations* of the group $G_{\mathbf{Q}}$. The Galois representation associated to a modular curve decomposes into pieces associated to modular forms. The Modularity Theorem in this context is that the Galois representation associated to any elliptic curve over $\mathbf{Q}$ arises from such a piece. This fits into a larger problem, to show that Galois representations from algebraic geometry arise from modular forms.

This chapter provides less background than the rest of the book. It quotes results from algebraic number theory and it uses techniques from algebra, especially tensors, without comment. Related reading: Chapter 15 of [Hus04], Chapter III.7 of [Sil86], Section 7.4 of [Shi73]. The volumes [Mur95] and [CSS97] contain lectures on the proof of Fermat's Last Theorem, and [DDT94] is a survey article. Henri Darmon's article in [Mur95] discusses the conjecture of Serre mentioned at the end of the chapter.

9.1 Galois number fields

Recall from Section 6.4 that a number field is a field $\mathbf{F} \subset \overline{\mathbf{Q}}$ such that the degree $[\mathbf{F} : \mathbf{Q}]$ is finite, and each number field has its ring of algebraic integers $\mathcal{O}_{\mathbf{F}}$. This chapter will work with number fields $\mathbf{F}$ such that the extension $\mathbf{F}/\mathbf{Q}$ is Galois. These fields are notated $\mathbf{F}$ rather than $\mathbf{K}$ to emphasize that they play a different role from other number fields earlier in the book, but the reader is cautioned that $\mathbf{F}_q$ continues to denote a finite field. The purpose of this section is to illustrate some results from algebraic number theory in the Galois case by giving specific examples, without proof, to convey a concrete sense of the ideas before we start using them. The reader without background in algebraic number theory is strongly encouraged to refer to a text on the subject.

Let $\mathbf{F}$ be a Galois number field and let $p \in \mathbf{Z}$ be prime. There are positive integers e, f, and g that describe the ideal $p\mathcal{O}_\mathbf{F}$ as a product of maximal ideals of $\mathcal{O}_\mathbf{F}$,

$$p\mathcal{O}_\mathbf{F} = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e, \qquad \mathcal{O}_\mathbf{F}/\mathfrak{p}_i \cong \mathbf{F}_{p^f} \text{ for } i = 1, \ldots, g, \qquad efg = [\mathbf{F} : \mathbf{Q}].$$

The first formula is (8.22) specialized to the Galois case. The *ramification degree* e says how many times each maximal ideal $\mathfrak{p}$ of $\mathcal{O}_\mathbf{F}$ that lies over p repeats as a factor of $p\mathcal{O}_\mathbf{F}$. There are only finitely many p such that $e > 1$, the primes that *ramify in* $\mathbf{F}$. The *residue degree* f is the dimension of the *residue field* $\mathbf{f}_\mathfrak{p} = \mathcal{O}_\mathbf{F}/\mathfrak{p}$ (a finite field) as a vector space over $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ for any $\mathfrak{p}$ over p. The *decomposition index* g is the number of distinct $\mathfrak{p}$ over p. The condition $efg = [\mathbf{F} : \mathbf{Q}]$ says that the net measure of ramification degree, residue degree, and decomposition index associated to each rational prime p is the field extension degree. Equivalently, $efg = |\mathrm{Gal}(\mathbf{F}/\mathbf{Q})|$.

The simplest Galois number fields are the quadratic fields. Let

$$\mathbf{F} = \mathbf{Q}(\sqrt{d}), \quad d \in \mathbf{Z} \text{ squarefree.}$$

Then $[\mathbf{F} : \mathbf{Q}] = 2$ and the extension $\mathbf{F}/\mathbf{Q}$ is Galois with its group generated by the automorphism taking $\sqrt{d}$ to $-\sqrt{d}$. The *discriminant* of the field is

$$\Delta_\mathbf{F} = \begin{cases} 4d & \text{if } d \not\equiv 1 \pmod 4, \\ d & \text{if } d \equiv 1 \pmod 4, \end{cases}$$

and the ring of algebraic integers in this field is

$$\mathcal{O}_\mathbf{F} = \mathbf{Z}\left[\frac{\Delta_\mathbf{F} + \sqrt{\Delta_\mathbf{F}}}{2}\right] = \left\{a + b\frac{\Delta_\mathbf{F} + \sqrt{\Delta_\mathbf{F}}}{2} : a, b \in \mathbf{Z}\right\}.$$

This says that $\mathcal{O}_\mathbf{F} = \mathbf{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$ while $\mathcal{O}_\mathbf{F} = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \pmod 4$, but phrasing results in terms of $\Delta_\mathbf{F}$ and thus making no more direct reference to cases is tidier. The Legendre symbol from elementary number theory, (a/p) where $a \in \mathbf{Z}$ and p is an odd prime, extends to incorporate the *Kronecker symbol*, defined only for $a \equiv 0, 1 \pmod 4$,

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 8, \\ -1 & \text{if } a \equiv 5 \pmod 8, \\ 0 & \text{if } a \equiv 0 \pmod 4. \end{cases}$$

This makes the behavior of a rational prime p in $\mathcal{O}_\mathbf{F}$ easy to notate,

$$p\mathcal{O}_\mathbf{F} = \begin{cases} \mathfrak{p}\mathfrak{q} & \text{if } (\Delta_\mathbf{F}/p) = \ \ 1, \\ \mathfrak{p} & \text{if } (\Delta_\mathbf{F}/p) = -1, \\ \mathfrak{p}^2 & \text{if } (\Delta_\mathbf{F}/p) = \ \ 0. \end{cases}$$

The content of this formula is that the odd primes p such that d is a quadratic residue modulo p decompose in $\mathcal{O}_{\mathbf{F}}$, the odd primes such that d is a nonresidue remain inert, and the odd primes dividing d ramify, while 2 decomposes if $d \equiv 1 \pmod 8$, remains inert if $d \equiv 5 \pmod 8$, and ramifies if $d \not\equiv 1 \pmod 4$.

Another family of simple Galois number fields is the cyclotomic fields. Let N be a positive integer and let

$$\mathbf{F} = \mathbf{Q}(\mu_N), \quad \mu_N = e^{2\pi i/N}.$$

Then $[\mathbf{F} : \mathbf{Q}] = \phi(N)$ (Euler totient) and the extension $\mathbf{F}/\mathbf{Q}$ is Galois with group isomorphic to $(\mathbf{Z}/N\mathbf{Z})^*$,

$$\mathrm{Gal}(\mathbf{F}/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/N\mathbf{Z})^*, \qquad (\mu_N \mapsto \mu_N^a) \longmapsto a \pmod N. \tag{9.1}$$

The cyclotomic integers are

$$\mathcal{O}_{\mathbf{F}} = \mathbf{Z}[\mu_N] = \{a_0 + a_1\mu_N + \cdots + a_{N-1}\mu_N^{N-1} : a_0, \ldots, a_{N-1} \in \mathbf{Z}\}.$$

Each rational prime not dividing N is unramified in $\mathbf{F}$,

$$p\mathcal{O}_{\mathbf{F}} = \mathfrak{p}_1 \cdots \mathfrak{p}_g, \quad p \nmid N,$$

and its residue degree f is the order of $p \pmod N$ in $(\mathbf{Z}/N\mathbf{Z})^*$. The primes dividing N ramify in $\mathbf{Q}(\mu_N)$. We do not need a precise description of their behavior since we will focus on the unramified primes.

For the simplest non-Abelian Galois group, let $d > 1$ be a cubefree integer, let $d^{1/3}$ denote the real cube root of d, and let

$$\mathbf{F} = \mathbf{Q}(d^{1/3}, \mu_3).$$

In this case $[\mathbf{F} : \mathbf{Q}] = 6$ and $\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ is isomorphic to S_3, the symmetric group on three letters. The Galois group is generated by

$$\sigma : \begin{pmatrix} d^{1/3} \mapsto \mu_3 d^{1/3} \\ \mu_3 \mapsto \mu_3 \end{pmatrix}, \qquad \tau : \begin{pmatrix} d^{1/3} \mapsto d^{1/3} \\ \mu_3 \mapsto \mu_3^2 \end{pmatrix},$$

and the isomorphism (noncanonical) is

$$\mathrm{Gal}(\mathbf{F}/\mathbf{Q}) \xrightarrow{\sim} S_3, \qquad \sigma \mapsto (1\,2\,3),\ \tau \mapsto (2\,3).$$

The rational primes not dividing $3d$ are unramified in $\mathbf{F}$, and their behavior is (Exercise 9.1.1)

$$p\mathcal{O}_{\mathbf{F}} = \begin{cases} \mathfrak{p}_1 \cdots \mathfrak{p}_6 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is a cube modulo } p, \\ \mathfrak{p}_1\mathfrak{p}_2 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p, \\ \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 & \text{if } p \equiv 2 \pmod 3. \end{cases} \tag{9.2}$$

Returning to the general situation, again let $\mathbf{F}$ be a Galois number field and let p be a rational prime. For each maximal ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{F}}$ lying over p

the *decomposition group of* $\mathfrak{p}$ is the subgroup of the Galois group that fixes $\mathfrak{p}$ as a set,

$$D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(\mathbf{F}/\mathbf{Q}) : \mathfrak{p}^\sigma = \mathfrak{p}\}.$$

The decomposition group has order ef, so its index in $\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ is indeed the decomposition index g. By its definition it acts on the residue field $\mathbf{f}_{\mathfrak{p}} = \mathcal{O}_{\mathbf{F}}/\mathfrak{p}$,

$$(x + \mathfrak{p})^\sigma = x^\sigma + \mathfrak{p}, \quad x \in \mathcal{O}_{\mathbf{F}},\ \sigma \in D_{\mathfrak{p}}.$$

The *inertia group of* $\mathfrak{p}$ is the kernel of the action,

$$I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : x^\sigma \equiv x \pmod{\mathfrak{p}} \text{ for all } x \in \mathcal{O}_{\mathbf{F}}\}.$$

The inertia group has order e, so it is trivial for all $\mathfrak{p}$ lying over any unramified p. Recall the Frobenius automorphism $\sigma_p : x \mapsto x^p$ in characteristic p from Chapter 8. If we view $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ as a subfield of $\mathbf{f}_{\mathfrak{p}} = \mathcal{O}_{\mathbf{F}}/\mathfrak{p} \cong \mathbf{F}_{p^f}$ then there is an injection

$$D_{\mathfrak{p}}/I_{\mathfrak{p}} \longrightarrow \mathrm{Gal}(\mathbf{f}_{\mathfrak{p}}/\mathbf{F}_p) = \langle \sigma_p \rangle.$$

Since both groups have order f, the injection is an isomorphism and the quotient $D_{\mathfrak{p}}/I_{\mathfrak{p}}$ has a generator that maps to σ_p. Any representative of this generator in $D_{\mathfrak{p}}$ is called a *Frobenius element* of $\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ and denoted $\mathrm{Frob}_{\mathfrak{p}}$. That is, $\mathrm{Frob}_{\mathfrak{p}}$ is any element of a particular coset $\sigma I_{\mathfrak{p}}$ in the subgroup $D_{\mathfrak{p}}$ of $\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$. Its action on $\mathbf{F}$, restricted to $\mathcal{O}_{\mathbf{F}}$, descends to the residue field $\mathbf{f}_{\mathfrak{p}} = \mathcal{O}_{\mathbf{F}}/\mathfrak{p}$, where it is the action of σ_p. When p is unramified, making the inertia group $I_{\mathfrak{p}}$ trivial, $\mathrm{Frob}_{\mathfrak{p}}$ is unique. To summarize,

Definition 9.1.1. *Let* $\mathbf{F}/\mathbf{Q}$ *be a Galois extension. Let* p *be a rational prime and let* $\mathfrak{p}$ *be a maximal ideal of* $\mathcal{O}_{\mathbf{F}}$ *lying over* p*. A* ***Frobenius element*** *of* $\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ *is any element* $\mathrm{Frob}_{\mathfrak{p}}$ *satisfying the condition*

$$x^{\mathrm{Frob}_{\mathfrak{p}}} \equiv x^p \pmod{\mathfrak{p}} \quad \textit{for all } x \in \mathcal{O}_{\mathbf{F}}.$$

Thus $\mathrm{Frob}_{\mathfrak{p}}$ *acts on the residue field* $\mathbf{f}_{\mathfrak{p}}$ *as the Frobenius automorphism* σ_p*.*

When $\mathbf{F}/\mathbf{Q}$ is Galois the Galois group acts transitively on the maximal ideals lying over p, i.e., given any two such ideals $\mathfrak{p}$ and $\mathfrak{p}'$ there is an automorphism $\sigma \in \mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ such that

$$\mathfrak{p}^\sigma = \mathfrak{p}'.$$

(We made reference to this fact, and to the earlier-mentioned fact that $D_{\mathfrak{p}}$ surjects to $\mathrm{Gal}(\mathbf{f}_{\mathfrak{p}}/\mathbf{F}_p)$, in the proof of Theorem 8.5.4.) The associated decomposition and inertia groups satisfy

$$D_{\mathfrak{p}^\sigma} = \sigma^{-1} D_{\mathfrak{p}} \sigma, \qquad I_{\mathfrak{p}^\sigma} = \sigma^{-1} I_{\mathfrak{p}} \sigma,$$

and the relation between corresponding Frobenius elements is

$$\mathrm{Frob}_{\mathfrak{p}^\sigma} = \sigma^{-1}\mathrm{Frob}_{\mathfrak{p}}\,\sigma.$$

If p is ramified then this means that the conjugate of a Frobenius is a Frobenius of the conjugate. The relation shows that if the Galois group is Abelian then $\mathrm{Frob}_{\mathfrak{p}}$ for any $\mathfrak{p}$ lying over p can be denoted Frob_p.

To compute the Frobenius element in the quadratic field case, again let $\mathbf{F} = \mathbf{Q}(\sqrt{d})$ where $d \in \mathbf{Z}$ is squarefree. The Galois group $\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ consists of the identity and the map taking $\sqrt{\Delta_{\mathbf{F}}}$ to $-\sqrt{\Delta_{\mathbf{F}}}$. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_{\mathbf{F}}$ lying over an odd prime p. Each $a + b(\Delta_{\mathbf{F}} + \sqrt{\Delta_{\mathbf{F}}})/2 \in \mathcal{O}_{\mathbf{F}}$ reduces to the residue field $\mathbf{f}_{\mathfrak{p}}$, with a, b, and $\Delta_{\mathbf{F}}$ reducing to its subfield $\mathbf{F}_p$ and with 2 reducing to $\mathbf{F}_p^*$. Using the same symbols for the reductions, compute in the residue field that

$$\left(a + b\,\frac{\Delta_{\mathbf{F}} + \sqrt{\Delta_{\mathbf{F}}}}{2}\right)^p = a + b\,\frac{\Delta_{\mathbf{F}} + \Delta_{\mathbf{F}}^{(p-1)/2}\sqrt{\Delta_{\mathbf{F}}}}{2}.$$

This shows that the Frobenius element is the Legendre symbol in that $\mathrm{Frob}_{\mathfrak{p}}$ multiplies $\sqrt{\Delta_{\mathbf{F}}}$ by $\Delta_{\mathbf{F}}^{(p-1)/2} = (\Delta_{\mathbf{F}}/p)$ for odd primes p. There are infinitely many such p such that $(\Delta_{\mathbf{F}}/p) = 1$, and similarly for $(\Delta_{\mathbf{F}}/p) = -1$. Therefore every element of the Galois group of $\mathbf{F}$ takes the form Frob_p for infinitely many p, and there is an isomorphism

$$\mathrm{Gal}(\mathbf{F}/\mathbf{Q}) \xrightarrow{\sim} \{\pm 1\}, \qquad \mathrm{Frob}_p \mapsto (\Delta_{\mathbf{F}}/p) \text{ for odd } p \nmid \Delta_{\mathbf{F}}.$$

The Frobenius automorphism has a natural description in the cyclotomic case $\mathbf{F} = \mathbf{Q}(\mu_N)$ as well. For any prime $p \nmid N$ let $\mathfrak{p}$ lie over p and note that in the residue field $\mathbf{f}_{\mathfrak{p}} = \mathbf{F}_p[\mu_N]$, again using the same symbols to denote reductions,

$$\left(\sum_m a_m \mu_N^m\right)^p = \sum_m a_m \mu_N^{pm}.$$

This shows that Frob_p is the element of $\mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q})$ that takes μ_N to μ_N^p, and thus the isomorphism (9.1) takes Frob_p to $p \pmod N$. By Dirichlet's Theorem on Arithmetic Progressions, for each $a \in (\mathbf{Z}/N\mathbf{Z})^*$ there are infinitely many p such that $p \equiv a \pmod N$. Therefore every element of the Galois group of $\mathbf{F}$ again takes the form Frob_p for infinitely many p, and the isomorphism (9.1) is

$$\mathrm{Gal}(\mathbf{F}/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/N\mathbf{Z})^*, \qquad \mathrm{Frob}_p \mapsto p \pmod N \text{ for } p \nmid N. \tag{9.3}$$

In the non-Abelian example $\mathbf{F} = \mathbf{Q}(d^{1/3}, \mu_3)$ since the conjugacy classes in any symmetric group S_n are specified by the cycle structure of their elements, in this case of S_3 they are

$$\{1\}, \quad \{(1\,2), (2\,3), (3\,1)\}, \quad \{(1\,2\,3), (1\,3\,2)\}.$$

So the conjugacy class of an element of S_3 is determined by the element's order, and therefore this holds in $\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ as well. To determine the conjugacy class

of $\mathrm{Frob}_{\mathfrak{p}}$ it thus suffices to determine its order, the residue degree f of the prime p lying under $\mathfrak{p}$. Formula (9.2) and the formula $efg = 6$ combine to show that for any unramified rational prime p, i.e., $p \nmid 3d$, the associated conjugacy class

$$\{\mathrm{Frob}_{\mathfrak{p}} : \mathfrak{p} \text{ lies over } p\} \tag{9.4}$$

is

$$\text{the elements of order } \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is a cube modulo } p, \\ 3 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p, \\ 2 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Each conjugacy class takes the form (9.4) for infinitely many p, as with the previous two fields. This fact, as well as Dirichlet's Theorem, is a special case of

Theorem 9.1.2 (Tchebotarov Density Theorem, weak version). *Let* $\mathbf{F}$ *be a Galois number field. Then every element of* $\mathrm{Gal}(\mathbf{F}/\mathbf{Q})$ *takes the form* $\mathrm{Frob}_{\mathfrak{p}}$ *for infinitely many maximal ideals* $\mathfrak{p}$ *of* $\mathcal{O}_{\mathbf{F}}$.

We end this section with a motivating example. There is an embedding of S_3 in $\mathrm{GL}_2(\mathbf{Z})$ (Exercise 9.1.2) such that

$$(1\,2\,3) \mapsto \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \qquad (2\,3) \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{9.5}$$

Again letting $\mathbf{F} = \mathbf{Q}(d^{1/3}, \mu_3)$ this gives a representation

$$\rho : \mathrm{Gal}(\mathbf{F}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{Z}).$$

The trace of ρ is a well defined function on conjugacy classes (9.4) and therefore depends only on the underlying unramified rational primes p,

$$\mathrm{tr}\,\rho(\mathrm{Frob}_{\mathfrak{p}}) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is a cube modulo } p, \\ -1 & \text{if } p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p, \\ 0 & \text{if } p \equiv 2 \pmod 3. \end{cases} \tag{9.6}$$

Recall from Section 4.11 the theta function $\theta_\chi(\tau) \in \mathcal{M}_1(3N^2, \psi)$ where $N = 3\prod_{p|d} p$ and ψ is the quadratic character with conductor 3. Formula (9.6) for $\mathrm{tr}\,\rho(\mathrm{Frob}_{\mathfrak{p}})$ matches formula (4.51) for the Fourier coefficient $a_p(\theta_\chi)$ when $p \nmid 3d$. Similarly the determinant of ρ is defined on conjugacy classes over unramified primes,

$$\det \rho(\mathrm{Frob}_{\mathfrak{p}}) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

This is $\psi(p)$. So the Galois group representation ρ, as described by its trace and determinant on Frobenius elements, arises from the modular form θ_χ. This modular form is a normalized eigenform by Section 5.9 and a cusp form by Exercise 5.11.3. The idea of this chapter is that 2-dimensional representations of Galois groups arise from such modular forms in great generality.

http://www.springer.com/978-0-387-23229-4

A First Course in Modular Forms
Diamond, F.; Shurman, J.
2005, XVI, 450 p. 57 illus., Hardcover
ISBN: 978-0-387-23229-4