Mathematical Research Letters **10**, 205–217 (2003)

ICOSAHEDRAL $\mathbb{Q}$-CURVE EXTENSIONS

Edray Herber Goins

Abstract. We consider elliptic curves defined over $\mathbb{Q}(\sqrt{5})$ which are either 2- or 3-isogenous to their Galois conjugate and which have an absolutely irreducible mod 5 representation. Using Klein's classical formulas which associate an icosahedral Galois extension $K/\mathbb{Q}$ with the 5-torsion of an elliptic curve, we prove that there is an association of such extensions generated by quintics $x^5 + A\,x^2 + B\,x + C$ satisfying $A\,B = 0$ with the aforementioned elliptic curves.

1. Introduction

Let ρ be a continuous two-dimensional complex Galois representation, and consider the composition

$$\widetilde{\rho}: \quad G_{\mathbb{Q}} \xrightarrow{\ \rho\ } GL_2(\mathbb{C}) \longrightarrow PGL_2(\mathbb{C}) \tag{1}$$

As ρ is continuous, there exists a finite extension K which is the field fixed by the kernel of $\widetilde{\rho}$; we consider only the icosahedral Galois extensions i.e. $\mathrm{Gal}(K/\mathbb{Q}) \simeq A_5$. Klein [8], motivated by the isomorphism $A_5 \simeq PSL_2(\mathbb{F}_5)$, showed in 1884 that any icosahedral Galois extension $K/\mathbb{Q}$ is contained in the extension $\mathbb{Q}(E[5]_x)$ generated by the x-coordinates of the 5-torsion from a suitable elliptic curve E defined over some quadratic extension of $\mathbb{Q}(\sqrt{5})$. Conversely, Shih [13] observed in 1978 that for any elliptic curve E defined over $\mathbb{Q}(\sqrt{5})$ which possesses a p-isogeny $\lambda : E \to E^\sigma$ with its Galois conjugate for a prime $p \equiv 2, 3 \mod 5$ such that $\lambda\,(E[p]) = (\ker \lambda)^\sigma$ is rational over $\mathbb{Q}(\sqrt{5})$ and $\mathrm{Gal}\,(\mathbb{Q}(E[5]_x)/\mathbb{Q}(\zeta_5)) \simeq A_5$, there is indeed such an icosahedral Galois extension $K \subset \mathbb{Q}(E[5]_x)$. (Shih's result is stronger than stated, but this will suffice for the exposition at hand.)

In this exposition, I present an explicit characterization of Shih's result when $p = 2$, 3. My main result is the following.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}(\sqrt{5})$ which is either 2- or 3-isogenous to its Galois conjugate, and which has an absolutely irreducible mod 5 representation. Then there exists an icosahedral Galois extension $K/\mathbb{Q}$ contained in the field $\mathbb{Q}(E[5]_x)$ generated by the x-coordinates of the 5-torsion of E. Explicitly, $K(\zeta_5) = \mathbb{Q}(E[5]_x)$, and K is the splitting field of a quintic $x^5 + A\,x^2 + B\,x + C$ with $A\,B = 0$.*

Received November 13, 2002.

Key words and phrases. Galois representations, icosahedral representations, $\mathbb{Q}$-curves.

This research was sponsored in part by the National Physical Science Consortium (NPSC), and by the Max Planck Institute for Mathematics in Bonn, Germany.

Conversely, if $K/\mathbb{Q}$ is an icosahedral Galois extension that is the splitting field of a quintic $x^5 + A\,x^2 + B\,x + C$ with $A\,B = 0$, then $K(\zeta_5) = \mathbb{Q}(E[5]_x)$ for some elliptic curve E over $\mathbb{Q}(\sqrt{5})$ that is isogenous to its Galois conjugate.

Following the terminology in Ribet [10], an elliptic curve defined over a number field which is isogenous to its Galois conjugates is called a $\mathbb{Q}$-curve; we call an elliptic curve as in the proposition an icosahedral $\mathbb{Q}$-curve, and in turn call such extensions K icosahedral $\mathbb{Q}$-curve extensions with E its associated curve. In particular, any quintic in Bring-Jerrard form $x^5 - x + C$ which generates an icosahedral Galois extension actually generates an icosahedral $\mathbb{Q}$-curve extension associated 2-isogenous $\mathbb{Q}$ curve.

As the ultimate goal is to understand icosahedral Galois representations ρ, I also prove the following.

Proposition 1.2. *Let $K/\mathbb{Q}$ be an icosahedral $\mathbb{Q}$-curve extension. There exist Galois representations $\rho_0 : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ and $\rho_5 : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_5)$ such that*

1. *ρ_0 and ρ_5 are odd and continuous.*
2. *K is the field fixed by the kernel of $\widetilde{\rho}_0$.*
3. *ρ_5 has nebentype $\det \rho_0 \cdot \omega_5^{-1}$, where $\det \rho_0$ is either $(-1/*)$ or $(-3/*)$ and ω_5 is a primitive Dirichlet character mod 5.*
4. *$\rho_0 \equiv \rho_5 \mod \lambda_5$ for some prime above 5.*
5. *The residual representation $\overline{\rho} = \rho_0 \mod \lambda_5$ has image $Z(\mathbb{F}_5) \cdot SL_2(\mathbb{F}_5)$ consisting of those matrices in $GL_2(\mathbb{F}_5)$ with square determinant.*

Conversely, let ρ be a icosahedral Galois representation, and denote K as the field fixed by the kernel of its projectivization. If $K/\mathbb{Q}$ is an icosahedral $\mathbb{Q}$-curve extension, then ρ is a twist (of a conjugate) of ρ_0.

The main results above are general enough for me to prove the following.

Corollary 1.3. *Let ρ be an icosahedral Galois representation which is unramified outside of $\{2, 5, \infty\}$. Then ρ is residually modular.*

For example, the icosahedral Galois representation considered by Buhler [1] in 1978 may be realized on the 5-torsion of a modular $\mathbb{Q}$-curve because it can be associated to the splitting field $5\,x^5 + 20\,x + 16$, a fact which seems to have never been exploited in the literature. Explicitly, an associated $\mathbb{Q}$-curve is

$$y^2 = x^3 + \left(5 - \sqrt{5}\right) x^2 + \sqrt{5}\,x. \tag{2}$$

My interest in stating such a result is to give a partial converse to Buzzard, Dickinson, Shepherd-Barron, and Taylor [3] where they work with complex Galois representations which are unramified at $\{2, 5\}$. This result says that if an odd representation is ramified precisely at $\{2, 5\}$ then it is residually modular.

2. Lectures on the Icosahedron

We begin by showing the explicit relationship between a certain class of quintics and elliptic curves. Most of the exposition that follows in this section is motivated by both Klein [8] and Klute [9].

The group A_5 may be realized as the group of rotations of the icosahedron. This Platonic Solid has 12 vertices which may be inscribed on the unit sphere, so that after projecting to the extended complex plane we have a natural group action on the complex numbers

$$\left(\zeta_5 + {\zeta_5}^4\right) {\zeta_5}^\nu, \quad \left({\zeta_5}^2 + {\zeta_5}^3\right) {\zeta_5}^\nu \quad \text{for } \nu \in \mathbb{F}_5; \qquad \infty; \quad \text{and} \quad 0; \tag{3}$$

generated by the three fractional linear transformations

$$S\,z = \zeta_5\,z, \qquad T\,z = \frac{\varepsilon\,z+1}{z-\varepsilon}, \qquad \text{and} \qquad U\,z = -\frac{1}{z}; \tag{4}$$

where ζ_5 is a primitive fifth root of unity and $\varepsilon = \zeta_5 + {\zeta_5}^4$ is a fundamental unit. By considering a homogeneous polynomial which vanishes at the vertices, we find three polynomials which are "invariant" under $A_5 \simeq \langle S,\, T,\, U\rangle$:

$$\begin{aligned} c_4(z) &= \left(z^{20}+1\right) - 228\left(z^{15}-z^5\right) + 494\,z^{10} \\ c_6(z) &= \left(z^{30}+1\right) + 522\left(z^{25}-z^5\right) - 10005\left(z^{20}+z^{10}\right) \\ \Delta(z) &= \left[-z\,\left(z^{10}+11\,z^5-1\right)\right]^5 \end{aligned} \tag{5}$$

related by $c_4^3 - c_6^2 = 1728\,\Delta$. ($\Delta$ vanishes at the vertices, c_4 at the midpoints of the faces, and c_6 at the midpoints of the edges. Consult Klein [8] and Klute [9] for more details.) Since polynomials are not actually "invariant" under action by fractional linear transformations we consider instead homogeneous rational functions. Define

$$\begin{aligned} \lambda(z) &= \frac{\left[z^2+1\right]^2\,\left[z^2-2\,\varepsilon\,z-1\right]^2\,\left[z^2+2\,\varepsilon^{-1}\,z-1\right]^2}{-z\,\left(z^{10}+11\,z^5-1\right)} \\ \mu(z) &= \frac{-125\,z^5}{z^{10}+11\,z^5-1} \end{aligned} \tag{6}$$

(The numerator of $\lambda(z)$ vanishes at the fixed points of $\langle T,\, U\rangle \simeq V_4$ – the Klein Viergruppe – while the numerator of $\mu(z)$ vanishes at one of the vertices.) $\lambda(z)$ has nontrivial action by S so that we may associate a polynomial of degree 5, while $\mu(z)$ has trivial action by S so that we may associate a polynomial of degree 6.

Lemma 2.1. *Define $c_4(z)$, $c_6(z)$, $\Delta(z)$, $\lambda(z)$ and $\mu(z)$ as in* (5) *and* (6).

1. *We have the identities*

$$j := \frac{c_4^3}{\Delta} = 1728\,\frac{c_4^3}{c_4^3-c_6^2} = (\lambda+3)^3\,(\lambda^2+11\,\lambda+64) = \frac{(\mu^2+10\,\mu+5)^3}{\mu} \tag{7}$$

2. *For each m, $n \in \overline{\mathbb{Q}}$, the five resolvents*

$$x_\nu = \frac{m}{\lambda(\zeta_5{}^\nu z) + 3} + \frac{n}{[\lambda(\zeta_5{}^\nu z) + 3]\ [\lambda(\zeta_5{}^\nu z)^2 + 10\,\lambda(\zeta_5{}^\nu z) + 45]} \tag{8}$$

are roots of the quintic $x^5 + A_{m,n,j}\,x^2 + B_{m,n,j}\,x + C_{m,n,j}$ where

$$\begin{aligned} A_{m,n,j} &= -\frac{20}{j}\ \left[\left(2\,m^3 + 3\,m^2\,n\right) + 432\,\frac{6\,m\,n^2 + n^3}{1728 - j}\right] \\ B_{m,n,j} &= -\frac{5}{j}\ \left[m^4 - 864\,\frac{3\,m^2\,n^2 + 2\,m\,n^3}{1728 - j} + 559872\,\frac{n^4}{(1728 - j)^2}\right] \\ C_{m,n,j} &= -\frac{1}{j}\ \left[m^5 - 1440\,\frac{m^3\,n^2}{1728 - j} + 62208\,\frac{15\,m\,n^4 + 4\,n^5}{(1728 - j)^2}\right] \end{aligned} \tag{9}$$

3. *Conversely, given a quintic $q(x) = x^5 + A\,x^2 + B\,x + C$ over $\mathbb{Q}$ such that $A^4 - 5B^3 + 25\,A\,B\,C$ is nonzero, there exist m, n, $j \in \mathbb{Q}(\sqrt{5 \cdot \mathrm{Disc}(q)})$ such that $A = A_{m,n,j}$, $B = B_{m,n,j}$ and $C = C_{m,n,j}$.*

Remark. The discriminant of $q(x) = x^5 + A\,x^2 + B\,x + C$ is

$$\begin{aligned} \mathrm{Disc}(q) = &-27\,A^4\,B^2 + 256\,B^5 \\ &+ 108\,A^5\,C - 1600\,A\,B^3\,C + 2250\,A^2\,B\,C^2 + 3125\,C^4 \end{aligned} \tag{10}$$

Proof. The identities stated are easily verified using a symbolic calculator. Conversely, by eliminating m and n in (9), we find that j is a root of the equation

$$\delta^5\,j^2 - 1728\,\left(\gamma_4^3 - \gamma_6^2 + \delta^5\right)\,j + 1728^2\,\gamma_4^3 = 0 \tag{11}$$

where

$$\begin{aligned} 5^4 \cdot \delta &= A^4 - 5B^3 + 25\,A\,B\,C \\ 12^2\,5^5 \cdot \gamma_4 &= 128\,A^4\,B^2 - 144\,B^5 - 192\,A^5\,C - 600\,A\,B^3\,C \\ &\quad + 1000\,A^2\,B\,C^2 + 3125\,C^4 \\ 12^3\,5^{10} \cdot \gamma_6 &= 1728\,A^{10} + 10400\,A^6\,B^3 + 405000\,A^2\,B^6 \\ &\quad - 180000\,A^7\,B\,C - 1170000\,A^3\,B^4\,C + 1725000\,A^4\,B^2\,C^2 \\ &\quad - 2025000\,B^5\,C^2 - 1800000\,A^5\,C^3 + 2812500\,A\,B^3\,C^3 \\ &\quad - 4687500\,A^2\,B\,C^4 - 9765625\,C^6 \end{aligned} \tag{12}$$

The lemma follows since (11) has discriminant $5 \cdot \mathrm{Disc}(q)$ and m and n may be expressed in terms of j. □

Lemma 2.2. *Let $q(x) = x^5 + A\,x^2 + B\,x + C$ be a quintic over $\mathbb{Q}$ such that $A^4 - 5B^3 + 25\,A\,B\,C$ is nonzero, and denote K as its splitting field. There exists an elliptic curve E over $\mathbb{Q}(\sqrt{5 \cdot \mathrm{Disc}(q)})$ such that $K(\sqrt{5 \cdot \mathrm{Disc}(q)})$ is the field generated by sum $x_P + x_{2P}$ of x-coordinates of the 5-torsion of E. We say that such an E is associated to $q(x)$.*

Klein [8] never explicitly makes the assumption $A^4 - 5\,B^3 + 25\,A\,B\,C \neq 0$; indeed, it may be possible to prove this result even in its abscence. The field generated by the x-coordinates x_P of the 5-torsion is the splitting field of the 5-division polynomial $\psi_5(x)$, while the field generated by the sum of x-coordinates is the splitting field of the resolvent $\psi_5^*(x) = \prod_{\sigma \in A_5/D_5} \left(x - [x_{\sigma(P)} + x_{\sigma\,(2P)}]\right)$ as considered in Klute [9].

Proof. Choose $j_0 \in \mathbb{Q}(\sqrt{5 \cdot \mathrm{Disc}(q)})$ as in 2.1 so that $K(\sqrt{5 \cdot \mathrm{Disc}(q)})$ is the splitting field of $q_1(\mu) = (\mu^2 + 10\,\mu + 5)^3 - j_0\,\mu$, and let E be denote the elliptic curve $y^2 = x^3 + 3\,j_0/(1728 - j_0)\,x + 2\,j_0/(1728 - j_0)$ with invariant j_0. Given a 5-torsion point P on E,

$$x_P + x_{2P} = -2\,\frac{\mu^2 + 10\,\mu + 5}{\mu^2 + 4\,\mu - 1} \quad \text{for some root of } q_1(\mu) \tag{13}$$

so that $K(\sqrt{5 \cdot \mathrm{Disc}(q)})$ contains the field generated by the sum of the x-coordinates of the 5-torsion, and conversely, given a root of $q_1(\mu)$,

$$\mu = \frac{31104\,x^3}{(x-2)^5\,j_0 - 1728\,x^3\,(x^2 - 10\,x + 34)} \qquad \text{where } x = x_P + x_{2P} \tag{14}$$

for some 5-torsion P on E. Hence $K(\sqrt{5 \cdot \mathrm{Disc}(q)})$ is generated as claimed. □

We mention in passing that all of the previous results may be stated in the language of modular curves. Indeed, the variable z may be thought of as a hauptmodul on the moduli space $X(5)$ of genus 0 classifying elliptic curves with two points of order 5, where the twelve vertices in (3) correspond the cusps. The function μ may be thought of as a hauptmodul on the moduli space $X_0(5)$ classifying elliptic curves with a subgroup of order 5, while the function j may be thought of as a hauptmodul on the trivial moduli space $X(1)$. Recall that the quotient $X(5)/X(1)$ has degree 60 with automorphism group A_5. The quotient $X(5)/X_0(5)$ has degree 10, which explains why μ is a rational function in z of degree 10 as in (6); and the quotient $X_0(5)/X(1)$ has degree 6 which explains why j is a rational function in μ of degree 6 as in (7).

3. A_5-Extensions and $\mathbb{Q}$-Curves

A $\mathbb{Q}$-curve is an elliptic curve without complex multiplication which is isogenous to each of its Galois conjugates. Such curves were first considered by Ribet [10]. We now exhibit a family of $\mathbb{Q}$-curves associated to a subfamily of the quintics considered in the previous section.

Theorem 3.1. *For $t \in \mathbb{Q}$, define the quintics*

$$q_{p,t}(x) = \begin{cases} x^5 - 5\left(5\,t^2 - 1\right)x - 4\left(5\,t^2 - 1\right) & \text{for } p = 2, \\ x^5 - 20\left(5\,t^2 - 1\right)^2 x^2 - 48\left(5\,t^2 - 1\right)^3 & \text{for } p = 3; \end{cases} \tag{15}$$

and define the curves

$$E_{p,t}: \quad \begin{cases} y^2 = x^3 + 2\,x^2 + \frac{1}{2}(1+\sqrt{5}\,t)\,x & \text{for } p = 2, \\ y^2 + 3\,x\,y + \frac{1}{2}(1+\sqrt{5}\,t)\,y = x^3 & \text{for } p = 3. \end{cases} \tag{16}$$

We have the following.

1. *$q_{p,t}(x)$ has Galois group contained in A_5.*
2. *$E_{p,t}$ is a p-isogenous $\mathbb{Q}$-curve defined over $\mathbb{Q}(\sqrt{5})$.*
3. *$E_{p,t}$ is associated to $q_{p,t}(x)$.*
4. *Given $q(x) = x^5 + A\,x^2 + B\,x + C$ a quintic over $\mathbb{Q}$ with Galois group A_5 where $A\,B = 0$, set $t = \sqrt{\mathrm{Disc}(q)}/(125\,C^2)$ and $p = 2$ if $A = 0$ or $p = 3$ if $B = 0$. Then $E_{p,t}$ is associated to $q(x)$.*

Proof. The discriminant of $q_{p,t}(x)$ is a square, so its Galois group is contained in A_5. Any elliptic curve over $\mathbb{Q}(\sqrt{5})$ with j-invariant different from 0 or 1728 possessing a p-isogeny for $p = 2$, 3 must be a twist of either $y^2 = x^3 + 2\,x^2 + r\,x$ or $y^2 + 3\,x\,y + r\,y = x^3$ for some $r \in \mathbb{Q}(\sqrt{5})$ because, up to twist, an elliptic curve with such an isogeny has a rational point of order p. Using the equations in Roberts [11, Thm 1, Thm 2], [12], it follows that every p-isogenous $\mathbb{Q}$-curve over $\mathbb{Q}(\sqrt{5})$ is a twist of $E_{p,t}$ for $t = (2\,r-1)/\sqrt{5}$. The curve $E_{p,t}$ is singular only if $t = \pm\frac{1}{\sqrt{5}}$ which never happens when $t \in \mathbb{Q}$ so $E_{p,t}$ is indeed a p-isogenous $\mathbb{Q}$-curve. The fact that $E_{p,t}$ is associated to $q_{p,t}(x)$ comes from checking the formulas in 2.1.

It is easy to check that $j(E_{p,t})$ is a solution to (11) for p and t as given in the last part of the theorem, so $E_{p,t}$ is indeed an elliptic curve over $\mathbb{Q}(\sqrt{5})$ which is associated to $q(x)$. □

Now that we have this result for quintic polynomials, we state the corresponding result for Galois extensions.

Proposition 3.2. *Let $K/\mathbb{Q}$ be an icosahedral Galois extension. The following are equivalent.*

1. *$K(\sqrt{5})$ is the field generated by sum $x_P + x_{2P}$ of x-coordinates of the 5-torsion of a $\mathbb{Q}$-curve E defined over $\mathbb{Q}(\sqrt{5})$ which is either 2- or 3-isogenous.*
2. *K is the splitting field of a quintic over $\mathbb{Q}$ in the form $x^5 + A\,x^2 + B\,x + C$ with either $A = 0$ or $B = 0$.*
3. *If K_1 is a subfield of K of degree 5, there exists an element $x \in K_1$ such that $\mathrm{tr}\,x = \mathrm{tr}\,x^2 = \mathrm{tr}\,x^{p+1} = 0$ for either $p = 2$ or $p = 3$.*

Proof. ($1 \implies 2.$) E is a twist of some $E_{q,t}$ as defined in 3.1, so K is the splitting field of some $q_{p,t}(x)$. ($2 \implies 1.$) This is a restatement of 3.1. ($2 \implies 3.$) Choose a root x of $x^5 + A\,x^2 + B\,x + C$ and let $K_1 = \mathbb{Q}(x)$. Then

$$\mathrm{tr}\,x = \mathrm{tr}\,x^2 = 0, \qquad \mathrm{tr}\,x^3 = -3\,A, \qquad \mathrm{tr}\,x^4 = -4\,B, \qquad \mathrm{tr}\,x^5 = -5\,C. \tag{17}$$

Hence $\operatorname{tr} x^{p+1} = 0$ where $p = 2$ if $A = 0$ and $p = 3$ if $B = 0$. ($3 \implies 2$.) Choose such an $x \in K_1$ with $\operatorname{tr} x = \operatorname{tr} x^2 = \operatorname{tr} x^{p+1} = 0$ and let $x^5 + A\,x^2 + B\,x + C$ be its minimal polynomial. Then either $A = 0$ or $B = 0$, and K must be its splitting field since $K/\mathbb{Q}$ has simple Galois group. □

In lieu of this result, we make the following definitions.

Definition 3.3. Any icosahedral Galois extension $K/\mathbb{Q}$ satisfying the equivalent conditions of 3.2 is said to be an icosahedral $\mathbb{Q}$-curve extension. If E is a $\mathbb{Q}$-curve as in 3.2, then we say that E is associated to K.

Definition 3.4. Any $\mathbb{Q}$-curve E over $\mathbb{Q}(\sqrt{5})$ which is either 2- or 3-isogenous to its conjugate and which has an absolutely irreducible mod 5 representation is said to be an icosahedral $\mathbb{Q}$-curve. A root $t \in \mathbb{Q}$ satisfying

$$j(E) = \begin{cases} 64\,(3\,r-4)^3 \,/\, \left(r^3 - r^2\right) & \text{if 2-isogenous,} \\ 27\,(8\,r-9)^3 \,/\, \left(r^4 - r^3\right) & \text{if 3-isogenous;} \end{cases} \qquad t = \frac{2\,r-1}{\sqrt{5}}; \tag{18}$$

is called a parameter for E.

If E is an icosahedral $\mathbb{Q}$-curve with parameter t, then E is isomorphic to $E_{p,t}$ as in 3.1. Since E has an absolutely irreducible mod 5 representation, the quintic $q_{p,t}(x)$ must generate an icosahedral Galois extension K, and so by 2.2 we have $K(\zeta_5) = \mathbb{Q}(E[5]_x)$ as the field generated by the x-coordinates of the 5-torsion on E. A $\mathbb{Q}$-curve associated to an icosahedral $\mathbb{Q}$-curve extension is also an icosahedral $\mathbb{Q}$-curve.

We may reduce the verification of icosahedral $\mathbb{Q}$-curve extensions to finding rational points on a projective curve.

Corollary 3.5. *Let $K/\mathbb{Q}$ be an icosahedral Galois extension which is the splitting field of a quintic $q(x) = \prod_\nu (x - x_\nu)$. For n a positive integer, denote the homogeneous polynomial of degree n*

$$\sigma_n(z_1,\, z_2,\, z_3,\, z_4,\, z_5) = \sum_{k_1,\ldots,k_n} \sigma^{(k_1+\cdots+k_n)}\, z_{k_1} \cdots z_{k_n} \tag{19}$$

in terms of $\sigma^{(k)} = \sum_\nu {x_\nu}^k \in \mathbb{Q}$, and define the projective curve

$$C_p(q) = \left\{\, z \in \mathbb{P}^4(\overline{\mathbb{Q}}) \mid \sigma_1(z) = \sigma_2(z) = \sigma_{p+1}(z) = 0 \,\right\}. \tag{20}$$

Then $K/\mathbb{Q}$ is an icosahedral $\mathbb{Q}$-curve extension if and only if $C_p(q)$ has a rational point for either $p = 2$ or 3.

Proof. By 3.2, $K = \mathbb{Q}(x_1, \ldots, x_5)$ is an icosahedral $\mathbb{Q}$-curve extension if and only if it is the splitting field of some $X^5 + A\,X^2 + B\,X + C$ for $A\,B = 0$. The idea is to exhibit a transformation which will map $q(x) \mapsto X^5 + A\,X^2 + B\,X + C$. To this end, choose $z_1, \ldots, z_5 \in \mathbb{Q}$ to be determined, and set $X_\nu = \sum_k z_k\, {x_\nu}^k \in K$. We wish to find z_k such that $\sum_\nu X_\nu = \sum_\nu {X_\nu}^2 = \sum_\nu {X_\nu}^{p+1} = 0$ for either $p = 2$ or 3. We have $\sum_\nu {X_\nu}^n = \sum_\nu \sum_{k_1,\ldots,k_n} x_\nu^{k_1+\cdots+k_n}\, z_{k_1} \cdots z_{k_n} = \sigma_n(z_1, \ldots, z_5)$ so we seek rational points on $C_p(q)$ i.e. if $C_p(q)$ has a rational point $z = (z_1 : \ldots z_5)$

then $K/\mathbb{Q}$ is an icosahedral $\mathbb{Q}$-curve extension. Conversely, if $K/\mathbb{Q}$ is indeed an icosahedral $\mathbb{Q}$-curve extension then $(1:0:0:0:0) \in C_p(q)$ is a rational point. □

We present two examples of this result. Consider the splitting field of the quintic $q_1(x) = x^5 + 10\,x^3 - 10\,x^2 + 35\,x - 18$ as in [1]; this is an icosahedral Galois extension. The curve $C_2(q_1)$ has the rational point $(568:91:152:9:8)$ which corresponds to the principal quintic $5\,x^5 + 20\,x + 16$. Hence this splitting field is an icosahedral $\mathbb{Q}$-curve extension. On the other hand, consider the splitting field of the principal quintic $q_2(x) = x^5 + 20\,x - 16$; this is also an icosahedral Galois extension. Then the curve $C_2(q_2)$ has *two* rational points, namely $(1:0:0:0:0)$ and $(20:-2:0:1:1)$, which correspond to the quintics $x^5 + 20\,x - 16$ and $4\,x^5 - 25\,x + 50$. Hence this icosahedral $\mathbb{Q}$-curve extension has *two* associated elliptic curves. These examples lead to the following.

Proposition 3.6. *Let $K/\mathbb{Q}$ be an icosahedral Galois extension which is unramified outside of $\{2, 5, \infty\}$. Then $K/\mathbb{Q}$ is an icosahedral $\mathbb{Q}$-curve extension with an associated modular curve.*

Proof. By Jones [7], there are only five such A_5-extensions of $\mathbb{Q}$, so it is a computational exercise to show that the splitting fields actually come from principal quintics:

(21)

Original Quintic	Principal Quintic
$x^5 + 20\,x - 16$	$4\,x^5 - 25\,x + 50$
$x^5 + 10\,x^3 - 10\,x^2 + 35\,x - 18$	$5\,x^5 + 20\,x + 16$
$x^5 - 10\,x^3 + 20\,x^2 + 110\,x - 116$	$5\,x^5 - 20\,x + 16$
$x^5 + 10\,x^3 - 40\,x^2 + 60\,x - 32$	$5\,x^5 - 5\,x + 4$
$x^5 - 10\,x^3 - 20\,x^2 + 10\,x + 216$	$5\,x^5 + 5\,x + 8$

The associated $\mathbb{Q}$-curves can now be found via 3.1:

(22)

Quintic $q(x)$	$\mathbb{Q}$-curve $E_{q,t}$	Parameter t
$x^5 + 20\,x - 16$	$y^2 = x^3 + 2\,x^2 - \varepsilon\,x$	1
$4\,x^5 - 25\,x + 50$	$y^2 = x^3 + 10\,x^2 + \sqrt{5}\,\varepsilon^5\,x$	$11/25$
$5\,x^5 + 20\,x + 16$	$y^2 = x^3 + 2\,\sqrt{5}\,x^2 - \sqrt{5}\,\varepsilon^2\,x$	$3/5$
$5\,x^5 - 20\,x + 16$	$y^2 = x^3 + 2\,\sqrt{5}\,x^2 + \sqrt{5}\,\varepsilon\,x$	$1/5$
$5\,x^5 - 5\,x + 4$	$y^2 = x^3 + 4\,\sqrt{5}\,x^2 + 2\,\sqrt{5}\,\varepsilon^3\,x$	$2/5$
$5\,x^5 + 5\,x + 8$	$y^2 = x^3 + 8\,\sqrt{5}\,x^2 - 2\,\sqrt{5}\,\varepsilon^6\,x$	$9/20$

where $\varepsilon = \zeta_5 + {\zeta_5}^4$. These $\mathbb{Q}$-curves are modular by Ellenberg and Skinner [4] since they are not ramified at the prime above 3. □

We would like to make the same claim for the six A_5-extensions which are unramified outside of $\{3, 5, \infty\}$ but we seem to be missing a few principal polynomials. By Jones [7], there are only six such quintics, so we have the following

incomplete table which show the fields actually come from principal quintics:

(23)

Original Quintic	Principal Quintic
$x^5 + 15\,x^3 - 5\,x^2 + 60\,x - 96$	?
$x^5 + 15\,x^3 - 25\,x^2 + 15\,x - 3$	$3\,x^5 - 5\,x^2 + 3$
$x^5 + 25\,x^2 - 75$	$x^5 + 25\,x^2 - 75$
$x^5 - 25\,x^2 - 75$	$x^5 - 25\,x^2 - 75$
$x^5 + 15\,x^3 - 20\,x^2 + 60\,x - 24$	?
$x^5 - 15\,x^3 - 15\,x^2 + 135\,x + 63$	?

with associated $\mathbb{Q}$-curves

(24)

Quintic $q(x)$	$\mathbb{Q}$-curve $E_{q,t}$	Parameter t
$3\,x^5 - 5\,x^2 + 3$	$y^2 + 9\,\varepsilon\,x\,y + 9\,\varepsilon\,y = x^3$	$1/3$
$x^5 + 25\,x^2 - 75$	$y^2 + 3\,\sqrt{5}\,\varepsilon\,x\,y + 5\,\varepsilon^2\,y = x^3$	$1/5$
$x^5 - 25\,x^2 - 75$	$y^2 + 3\,\sqrt{5}\,\varepsilon\,x\,y + 5\,\varepsilon\,y = x^3$	$3/5$

However, finding the remaining three principal quintics seems unlikely, since in general the projective curves $C_2(q)$ and $C_3(q)$ have genus 4 and 9, respectively.

We mention in passing that all of the previous results may again be stated in the language of modular curves. One considers twists of the moduli spaces $X(5,p)$ obtained as fiber products of $X_0(5)$ and $X(p)$. We refer the reader to [5] for details.

4. Icosahedral Galois Representations

Let ρ be a two-dimensional complex Galois representation with finite image, denote $\widetilde{\rho}$ as the composition

$$\widetilde{\rho}: \qquad \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\ \rho\ } GL_2(\mathbb{C}) \longrightarrow PGL_2(\mathbb{C}) \tag{25}$$

and let K be the field fixed by the kernel of this map. The only nonsolvable image of $\widetilde{\rho}$ is A_5; hence we consider only representations ρ such that $K/\mathbb{Q}$ is an A_5-extension. We call such a representation ρ an icosahedral Galois representation, and $\widetilde{\rho}$ its projectivization. We will show rather explicitly that every icosahedral $\mathbb{Q}$-curve extension $K/\mathbb{Q}$ has a complex Galois representation by constructing the representation. The idea is as follows: Such an extension has an associated curve E, so the composition

$$G_{\mathbb{Q}(\sqrt{5})} \xrightarrow{\ \overline{\rho}_{E,5}\ } Z(\mathbb{F}_5)\cdot SL_2(\mathbb{F}_5) \xrightarrow{\ \pi_0\ } GL_2(\mathbb{C}) \tag{26}$$

yields a complex representation over $\mathbb{Q}(\sqrt{5})$ for some group homomorphism π_0. ($Z(\mathbb{F}_5)$ is the center of $GL_2(\mathbb{F}_5)$.) We will exploit the properties of E to show that a twist of such a representation can actually be defined over $\mathbb{Q}$.

Lemma 4.1. *Let ω_5 be a primitive Dirichlet character modulo 5, $Z(\mathbb{F}_5)$ be the center of $GL_2(\mathbb{F}_5)$, and $\varpi = (\omega_5(2)\cdot\varepsilon^{-1} - 1) \in \mathbb{Q}(\sqrt{-1},\sqrt{5})$ in terms of the fundamental unit $\varepsilon = \zeta_5 + {\zeta_5}^4$. Define the map $\pi_0 : Z(\mathbb{F}_5)\cdot SL_2(\mathbb{F}_5) \to GL_2(\mathbb{C})$ by*

$$\begin{pmatrix}1 & 1\\ & 1\end{pmatrix}, \begin{pmatrix} & -1\\ 1 & \end{pmatrix}, \begin{pmatrix}a & \\ & d\end{pmatrix} \mapsto \tag{27}$$
$$\frac{1}{2}\begin{pmatrix}\varepsilon & \varpi+2\\ \varpi & \varepsilon\end{pmatrix}, \begin{pmatrix} & -1\\ 1 & \end{pmatrix}, \begin{pmatrix}\omega_5(a) & \\ & \omega_5(d)\end{pmatrix}.$$

Then π_0 is an irreducible representation, and $\pi_0 \equiv 1 \mod (\varpi)$.

Proof. We take for granted that $Z(\mathbb{F}_5)\cdot SL_2(\mathbb{F}_5)$ is generated by the three matrices above, so it suffices to check π on these generators. We follow the exposition in [2, page 405]. It is a rather straightforward exercise to show that the orders of each generator match correctly, so it suffices to consider the commutation relations among the image of these generators. Denote the images

$$S = \pi_0\begin{pmatrix}1 & 1\\ & 1\end{pmatrix}, \qquad T = \pi_0\begin{pmatrix} & -1\\ 1 & \end{pmatrix}, \qquad U(a,d) = \pi_0\begin{pmatrix}a & \\ & d\end{pmatrix}. \tag{28}$$

The relations which must be verified are

1. $T\cdot U(a,d)\cdot T^{-1} = U(d,a)$,
2. $U(a,d)\cdot S\cdot U(a,d)^{-1} = S^n$ where $n \equiv a\,d^{-1}$ (5),
3. $T\,S^d\,T^{-1} = U(a,d)\;S^{-d}\,T^{-1}\,S^{-a}$ where $a\,d \equiv 1$ (5).

(Condition 2 is *not* satisfied if $n \equiv \pm 2$ (5); this explains why we must restrict to $Z\cdot SL_2(\mathbb{F}_5)$ where $n \equiv \pm 1$.) It is a straightforward to verify these relations; consult [6]. The irreducibility of π_0 follows from the fact that the image is not abelian. Since $\omega_5(2)^2 + 1 = \varepsilon^2 + \varepsilon - 1 = 0$, $\mathbb{F}_5^\times = \langle 2\rangle$, and the following are all contained in the ideal $(\varpi) \subset \mathbb{Q}(\sqrt{-1}, \sqrt{5})$:

$$2 - \varepsilon = \varepsilon^2\,\varpi\,\varpi^\sigma, \qquad 2 - \omega_5(2) = \varepsilon\,\varpi\,(\varepsilon\,\varpi^\sigma - 1), \qquad \pm\sqrt{5} = \varepsilon\,\varpi\,\varpi^\sigma; \tag{29}$$

(with σ being complex conjugation) the congruence $\pi_0 \equiv 1$ follows. □

Lemma 4.2. *Let E be an icosahedral $\mathbb{Q}$-curve. Denote $\rho_{E,5}$, $\overline{\rho}_{E,5}$ as its 5-adic and mod 5 representations respectively, χ_5 as the 5-adic cyclotomic character, and ω_5, π_0, ϖ as in 4.1. There exists a Hecke character χ_E such that*

1. *$\varrho_{E,5} = \chi_E \otimes \rho_{E,5}$ is an irreducible 5-adic representation which can be defined over $\mathbb{Q}$, where $\det \varrho_{E,5} = {\chi_E}^2\cdot(\chi_5 \circ \mathbb{N})$ is the composition with the norm map.*
2. *$\varrho_E = \chi_E \otimes (\pi_0 \circ \overline{\rho}_{E,5})$ is an irredicuble complex representation which can be defined over $\mathbb{Q}$, where $\det \varrho_E = {\chi_E}^2\cdot(\omega_5 \circ \mathbb{N})$.*
3. *$\varrho_{E,5} \equiv \varrho_E \mod (\varpi)$ and $\det \varrho_{E,5} = \det \varrho_E \cdot (\chi_5/\omega_5 \circ \mathbb{N})$.*

A similar result is true for all $\mathbb{Q}$-curves; see Ellenberg and Skinner [4] for a proof using cohomology. We will present instead a more constructive proof.

Proof. Following Roberts [11], as E is p-isogenous for $p = 2$ or 3, the isogeny is defined over $\mathbb{Q}(\sqrt{5}, \sqrt{D_E})$ where $D_E = -p\cdot \mathbb{N}\,D$ for some $D \in \mathbb{Q}(\sqrt{5})^\times$. Equivalently, $a_E(\mathfrak{p}^\sigma) = (D_E/\mathbb{N}\,\mathfrak{p})\cdot a_E(\mathfrak{p})$ in terms of the trace of Frobenius of $\rho_{E,5}$, the Legendre symbol $(D_E/*)$, and the nontrivial Galois automorphism σ of $\mathbb{Q}(\sqrt{5})$. We seek a character χ_E such that ${\chi_E}^{\sigma-1} = (D_E/*)\circ\mathbb{N}$: Then the

twisted representations $\varrho_{E,5} := \chi_E \otimes \rho_{E,5}$ and $\varrho_E := \chi_E \otimes (\pi_0 \circ \overline{\rho}_{E,5})$ will be Galois invariant and hence defined over $\mathbb{Q}$; the compositum

$$G_{\mathbb{Q}(\sqrt{5})} \xrightarrow{\overline{\rho}_{E,5}} Z(\mathbb{F}_5) \cdot SL_2(\mathbb{F}_5) \xrightarrow{\pi_0} GL_2(\mathbb{C}) \xrightarrow{\text{twist by } \chi_E} GL_2(\mathbb{C}) \tag{30}$$

will be invariant and hence defined over $\mathbb{Q}$; and the congruence $\varrho_{E,5} \equiv \varrho_E$ will follow as a consequence of 4.1. Irreducibility is clear since the mod 5 representation is irreducible by assumption, and the relations involving the determinants are clear by 4.1. Clearly D is included because of twisting, so write $\chi_E = (D/*) \cdot \chi_p$ where ${\chi_p}^{\sigma-1} = (-p/*) \circ \mathbb{N}$. We turn to constructing χ_p.

$\mathbb{Q}(\sqrt{5})$ has class number 1 with ring of integers $\mathbb{Z}[\varepsilon]$, so we extend the Dirichlet characters of conductors (4), (8), (3), and $(\sqrt{5})$:

(31)

$$\omega_4 : \begin{Bmatrix} -1 & \mapsto & -1 \\ \varepsilon & \mapsto & \zeta_6 \end{Bmatrix}, \quad \omega_8 : \begin{Bmatrix} -1 & \mapsto & -1 \\ 1+4\,\varepsilon & \mapsto & -1 \\ \varepsilon & & \zeta_{12} \end{Bmatrix}, \quad \omega_3 : \varepsilon \mapsto \zeta_8, \quad \omega_5 : \varepsilon \mapsto \zeta_4;$$

corresponding to the extensions $\mathbb{Q}(\sqrt{5}, \zeta_4)$, $\mathbb{Q}(\sqrt{5}, \zeta_8)$, $\mathbb{Q}(\sqrt{5}, \zeta_3)$, and $\mathbb{Q}(\zeta_5)$ of $\mathbb{Q}(\sqrt{5})$, respectively. One verifies that $\chi_2 := {\omega_4}^3\,{\omega_8}^3\,\omega_5$ and $\chi_3 := {\omega_3}^2\,\omega_5$ yield the desired relations by checking on the generators -1, $1+4\,\varepsilon$, and ε; in fact ${\chi_2}^2 = \left(\omega_4 \cdot {\omega_5}^{-1}\right) \circ \mathbb{N}$ and ${\chi_3}^2 = \left(\omega_3 \cdot {\omega_5}^{-1}\right) \circ \mathbb{N}$. Hence, we have constructed the desired characters with the properties

$$\begin{aligned} {\chi_2}^{\sigma-1} &= \left(\frac{-2}{*}\right) \circ \mathbb{N}, \qquad {\chi_2}^2 = \left[\left(\frac{-1}{*}\right) \cdot {\omega_5}^{-1}\right] \circ \mathbb{N}; \\ {\chi_3}^{\sigma-1} &= \left(\frac{-3}{*}\right) \circ \mathbb{N}, \qquad {\chi_3}^2 = \left[\left(\frac{-3}{*}\right) \cdot {\omega_5}^{-1}\right] \circ \mathbb{N}; \end{aligned} \tag{32}$$

which completes the proof. □

Theorem 4.3. *Let $K/\mathbb{Q}$ be an icosahedral $\mathbb{Q}$-curve extension. There exist Galois representations $\rho_0 : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ and $\rho_5 : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_5)$ such that, with notation as in 4.1,*

1. *ρ_0 and ρ_5 are odd and continuous.*
2. *K is the field fixed by the kernel of the projectivization $\widetilde{\rho}_0$.*
3. *ρ_5 has nebentype $\det \rho_0 \cdot \omega_5^{-1}$, where $\det \rho_0$ is either $(-1/*)$ or $(-3/*)$.*
4. *$\rho_0 \equiv \rho_5 \mod \lambda_5$ for some prime above 5.*
5. *The residual representation $\overline{\rho} = \rho_0 \mod \lambda_5$ has image $Z(\mathbb{F}_5) \cdot SL_2(\mathbb{F}_5)$.*

Conversely, let ρ be a icosahedral Galois representation, and denote K as the field fixed by the kernel of its projectivization. If $K/\mathbb{Q}$ is an icosahedral $\mathbb{Q}$-curve extension, then ρ is a twist (of a conjugate) of ρ_0.

Remark. Any icosahedral Galois representation ρ we hope to associate to an icosahedral $\mathbb{Q}$-curve must necessarily be odd.

Proof. Let E be a $\mathbb{Q}$-curve associated to $K/\mathbb{Q}$. Since $K(\sqrt{5})$ is contained in the field generated by the x-coordinates, we may twist E by any element in $\mathbb{Q}(\sqrt{5})$ and find another $\mathbb{Q}$-curve associated to K. In particular, we may choose a curve such that $\chi_E = \chi_p$ as in (32) for either $p = 2$ or 3. Let ρ_5 and ρ_0 be the representations $\varrho_{E,5}$ and ϱ_E as in 4.2, respectively, assumed defined over $\mathbb{Q}$.

It is clear that ρ_5 and ρ_0 are continuous. Considering 4.2 and (32), the statements regarding determinants and congruence are clear; both representations are odd since $(-1/*)$ and $(-3/*)$ are odd quadratic characters. Denote K_0 as the field fixed by kernel of $\widetilde{\rho}_0$; we claim that $K_0 = K$. $K(\sqrt{5}) = K_0(\sqrt{5})$ is the field fixed by the projectivization of $\overline{\rho}_{E,5}$, while both $K/\mathbb{Q}$ and $K_0/\mathbb{Q}$ are icosahedral extensions. $\sqrt{5} \notin K_0$ since A_5 has no subgroups of index 2; hence $K_0 \subset K$ and similarly $K \subset K_0$ so we indeed have equality. It remains to show that $\overline{\rho} = \rho_0 \mod (\varpi)$ as in 4.1 has image $Z(\mathbb{F}_5) \cdot SL_2(\mathbb{F}_5)$, the subgroup of $GL_2(\mathbb{F}_5)$ of index 2 consisting of those matrices with square determinants. Since $\det \rho_0 \equiv \pm 1$ (5) is a quadratic character the image is contained in $Z(\mathbb{F}_5) \cdot SL_2(\mathbb{F}_5)$. The restriction $\overline{\rho}|_{\mathbb{Q}(\sqrt{5})}$ is the twist of an absolutely irreducible mod 5 representation, which has image $Z(\mathbb{F}_5) \cdot SL_2(\mathbb{F}_5)$. This gives equality.

As for the converse, let ρ be a icosahedral Galois representation with K the field fixed by the kernel of its projectivization, and consider the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_K & \longrightarrow & G_{\mathbb{Q}} & \longrightarrow & \mathrm{Gal}\,(K/\mathbb{Q}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \chi} & & \downarrow{\scriptstyle \rho,\,\rho_0} & & \downarrow{\scriptstyle \bar{\rho},\,\bar{\rho}_0} & & \\ 1 & \longrightarrow & \mathbb{C}^\times & \longrightarrow & GL_2(\mathbb{C}) & \longrightarrow & PGL_2(\mathbb{C}) & \longrightarrow & 1 \end{array} \tag{33}$$

Both $\widetilde{\rho}$ and $\widetilde{\rho_0}$ are projective complex representations of A_5. There are only two such representations so upon choosing a different 5-cycle we have $\widetilde{\rho} \simeq \widetilde{\rho_0}$. Without loss of generality we assume equality. We must show that there exists a character χ in the leftmost column. For automorphisms σ and τ, define the symbol $\chi(\sigma)$ by $\chi(\sigma) \cdot 1_2 = \rho(\sigma) \cdot \rho_0(\sigma)^{-1}$. Then χ is actually a multiplicative character since

$$\chi(\sigma\,\tau) \cdot 1_2 = \rho(\sigma\,\tau)\,\rho_0(\sigma\,\tau)^{-1} = \rho(\sigma)\left[\rho(\tau)\,\rho_0(\tau)^{-1}\right]\rho_0(\sigma)^{-1} = \chi(\sigma)\,\chi(\tau) \cdot 1_2 \tag{34}$$

Hence, $\rho \simeq \chi \otimes \rho_0$ as claimed. □

We present an example of this theorem. Let K be the splitting field of the quintic $x^5 + 10\,x^3 - 10\,x^2 + 35\,x - 18$ as considered in [1]; we found in 3.6 that it is also the splitting field of the principal quintic $5\,x^5 + 20\,x + 16$ proving that $K/\mathbb{Q}$ is a icosahedral $\mathbb{Q}$-curve extension. Quite explicitly, K has associated curve

$$E: \quad y^2 = x^3 + \left(5 - \sqrt{5}\right)\,x^2 + \sqrt{5}\,x \tag{35}$$

It is easy to check that the 2-isogeny of E is defined over $\mathbb{Q}(\sqrt{5}, \sqrt{-2})$. If $\overline{\rho}_{E,5}$ is the mod 5 representation of this curve then $\chi_2 \otimes \left(\pi_0 \circ \overline{\rho}_{E,5}\right)$ is the restriction

to $\mathbb{Q}(\sqrt{5})$ of a complex representation ρ_0 defined over $\mathbb{Q}$ with $\det \rho_0 = (-1/*)$. This is precisely the representation constructed in [1]. This falls into the larger result of the following.

Proposition 4.4. *Let ρ be an icosahedral Galois representation which is unramified outside of $\{2, 5, \infty\}$. Then ρ is residually modular.*

Proof. Let K be the field fixed by the kernel of $G_{\mathbb{Q}} \xrightarrow{\rho} PGL_2(\mathbb{C})$; then $K/\mathbb{Q}$ is an icosahedral Galois extension which is unramified outside of $\{2, 5, \infty\}$. By 3.6, $K/\mathbb{Q}$ has an associated modular elliptic curve E, and by 4.2 and 4.3 there exists a character χ such that $\rho|_{\mathbb{Q}(\sqrt{5})} \simeq \chi \otimes \left(\pi_0 \circ \overline{\rho}_{E,5}\right)$. Hence, ρ is residually modular. □

Acknowledgements

I would like to thank Dan Bump for suggesting the original problem; and Joe Buhler, Kevin Buzzard, David Carlton, Jordan Ellenberg, Dick Gross, John Jones, Ken Ribet, Karl Rubin, Chris Skinner, William Stein and Richard Taylor for helpful conversations.

References

[1] J. Buhler, *Icosahedral Galois representations,* Lecture Notes in Mathematics, Vol. 654. Springer-Verlag, Berlin-New York, 1978.
[2] D. Bump, *Automorphic forms and representations,* Cambridge Studies in Advanced Mathematics, 55. Cambridge University Press, Cambridge, 1997.
[3] K. Buzzard, M. Dickinson, N. Shepherd-Barron, R. Taylor, *On icosahedral Artin representations,* Duke Math. J. **109** (2001), 283–318.
[4] J. Ellenberg, C. Skinner, *On the modularity of $\mathbb{Q}$-curves,* Duke Math. J. **109** (2001), 97–122.
[5] J. Fernández, *A moduli approach to quadratic $\mathbb{Q}$-curves realizing mod p projective Galois representations,* Preprint 65, 2003: `http://www.math.leidenuniv.nl/gtem/view.php`
[6] E. Goins, *Elliptic curves and icosahedral Galois representations,* PhD thesis, Stanford University, 1999.
[7] J. Jones, *Cumulative quintic tables,* preprint, 1999: `http://hobbes.la.asu.edu/NumberFields/cum-quintics.html`
[8] F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade,* Reprint of the 1884 original. Edited, with an introduction and commentary by Peter Slodowy. Birkhäuser Verlag, Basel; B. G. Teubner, Stuttgart, 1993.
[9] A. Klute, *Icosahedral Galois extensions and elliptic curves,* Manuscripta Math. **93** (1997), 301–324.
[10] K. Ribet, *Abelian varieties over $\mathbb{Q}$ and modular forms,* Algebra and topology 1992 (Taejŏn), 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.
[11] B. Roberts, *$\mathbb{Q}$-curves over quadratic fields,* PhD thesis, University of Maryland, 1999.
[12] B. Roberts, L. Washington, *The modularity of some $\mathbb{Q}$-curves,* Compositio Math. **111** (1998), 35–49.
[13] K.-Y. Shih, *p-division points on certain elliptic curves,* Compositio Math. **36** (1978), 113–129.

California Institute of Technology, Mathematics 253-37, Pasadena, CA 91125, U.S.A.
E-mail address: `goins@caltech.edu`