MOD 4 GALOIS REPRESENTATIONS AND ELLIPTIC CURVES

CHRISTOPHER HOLDEN

(Communicated by Ken Ono)

Abstract. Galois representations $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/n)$ with cyclotomic determinant all arise from the $n$-torsion of elliptic curves for $n = 2, 3, 5$. For $n = 4$, we show the existence of more than a million such representations which are surjective and do not arise from any elliptic curve.

1. Introduction

Given an elliptic curve $E$ defined over $\mathbb{Q}$, its $n$-torsion subgroup $E[n]$ is isomorphic to $(\mathbb{Z}/n)^2$ as an abstract group. The Galois group of $\mathbb{Q}(E[n])$ over $\mathbb{Q}$ embeds into $GL_2(\mathbb{Z}/n)$. We then have a continuous Galois representation

$$\overline{\rho}_{E,n} : G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(E[n]) \hookrightarrow GL_2(\mathbb{Z}/n).$$

The composition of $\overline{\rho}_{E,n}$ with the determinant map is the mod $n$ cyclotomic character. Thus $\overline{\rho}_{E,n}$ is odd, that is, $\det(\overline{\rho}_{E,n}(\text{complex conjugation})) = -1$. In this way, a continuous mod $n$ Galois representation with cyclotomic determinant is created from the elliptic curve. Naturally, one asks if every such representation corresponds to the $n$-torsion of some elliptic curve.

For $n = 2$, there is an elementary verification of this question (see below), and for $n = 3, 5$, an affirmative answer is given in [7] and [8]. For all primes $n \geq 7$ it has been shown that there exist continuous, irreducible mod $n$ Galois representations with cyclotomic determinant that do not come from the $n$-torsion of any elliptic curve. See [2] and [5].

When $n$ is not prime, less is known. [7] gives a mod 4 representation with image isomorphic to $\mathbb{Z}/2$ which does not correspond to any elliptic curve’s 4-torsion, but the approach does not carry over to representations having larger images. In this paper, we show the existence of many surjective mod 4 representations with cyclotomic determinant which do not arise from the 4-torsion of any elliptic curve.

Theorem 1. There exist continuous, surjective mod 4 Galois representations having cyclotomic determinant which do not arise from the 4-torsion of any elliptic curve.

Equivalently, we prove the existence of a Galois extension $W/\mathbb{Q}$ such that

1. $\text{Gal}(W/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/4)$;
2. $\mathbb{Q}(i) \subset W$ is the fixed field of $\text{SL}_2(\mathbb{Z}/4)$;
3. There is no elliptic curve $E$ such that $W = \mathbb{Q}(E[4])$.

Received by the editors May 12, 2006 and, in revised form, September 1, 2006.

2000 Mathematics Subject Classification. Primary 14H52.
Let $\rho : G_\mathbb{Q} \rightarrow GL_2(\mathbb{Z}/4)$ be a continuous and surjective homomorphism having cyclotomic determinant. The fixed field of the kernel of $\rho$ is a finite extension $W/\mathbb{Q}$ such that $\text{Im}(\rho) \simeq \text{Gal}(W/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/4)$. Likewise, such an extension determines a mapping of $G_\mathbb{Q}$ into $GL_2(\mathbb{Z}/4)$. (1) guarantees that $\rho$ is surjective and continuous, whilst (2) is equivalent to $\rho$ having cyclotomic determinant.

In the following sections we describe $G \cdot GL_2(\mathbb{Z}/4)$ using two of its normal subgroups $M$ and $N$ where $M \cap N = 1$ and $[G : MN] = 2$ (see Theorem 2). Then a field $W/\mathbb{Q}$ satisfying (1) is the product of two quartic subfields $M$ and $N$ where $\text{Gal}(M/\mathbb{Q}) \simeq G/M$ and $\text{Gal}(N/\mathbb{Q}) \simeq G/N$. A criterion developed by Cremona in [4] allows us to find fields $M/\mathbb{Q}$ which do not come from the 4-torsion of any elliptic curve. It is then a simple matter to construct $N$ so that $W = MN$ satisfies (2) and (3). In fact, we are able to find 1,628,554 such counterexamples. We expect, but are unable to show, that there are infinitely many.

2. 2-TORSION AND $S_3$-EXTENSIONS

When $\rho$ is a surjective and continuous mod 2 representation (det($\rho$) is necessarily trivial), it has image $GL_2(\mathbb{Z}/2) \simeq S_3$, the symmetric group on 3 letters. Given a finite Galois extension $L/\mathbb{Q}$ with Galois group isomorphic to $S_3$, there exists an irreducible cubic polynomial $f \in \mathbb{Q}[x]$ such that $L$ is the splitting field of $f$. Then the nontrivial 2-torsion points of the elliptic curve $E : y^2 = f$ are $(\phi_i, 0)$, where the $\phi_i$ are the roots of $f$.

Thus $L = \mathbb{Q}(E[2])$ and $E[2] \simeq V_\rho$, the Galois module corresponding to $\rho$. Any other irreducible cubic polynomial $g$ with coefficients in $\mathbb{Q}$ and roots generating $L$ gives an elliptic curve $E' : y^2 = g$ for which $E'[2] \simeq E[2] \simeq V_\rho$. Furthermore, every elliptic curve having this property arises in this manner.

In addition to supplying concrete motivation for the other cases, this is directly relevant to the present discussion since $E[2] \subset E[4]$ for any elliptic curve $E$ defined over $\mathbb{Q}$. As with the above case, we aim to understand surjective mod 4 representations by considering extensions with Galois group $GL_2(\mathbb{Z}/4)$.

3. $GL_2(\mathbb{Z}/4)$ AS A GALOIS GROUP

Let $S_4$ be the symmetric group on 4 letters, $A_4$ its alternating subgroup; let $D_4$ denote the dihedral group of order 8 and let $V_4$ denote the Klein four-group.

**Theorem 2.** $G = GL_2(\mathbb{Z}/4)$ has unique normal subgroups $M$ and $N$ so that

1. $M \simeq V_4$ and $G/M \simeq S_4$;
2. $N \simeq A_4$ and $G/N \simeq D_4$;
3. $M \cap N$ is trivial;

Also, $G$ is the only group (up to isomorphism) satisfying all of the above properties.
Proof. This follows from a more general set of theorems concerning the structure of $GL_2(\mathbb{Z}/n)$ as well as basic group theory. See [1, section 5.1]. We discovered these facts via MAGMA by constructing this group, looking for relations among normal subgroups and inspecting other groups of the same order. □

Remark. While $MN$ and $SL_2(\mathbb{Z}/4)$ are both index-2 subgroups of $G$, it is not true in general that $MN \not\cong SL_2(\mathbb{Z}/4)$.

An immediate consequence of this theorem is an analogous statement concerning field extensions (see also Figure 1):

Corollary 3. Let $K$ be a field. Any extension $W/K$ with Galois group $\mathcal{G}$ has 2 unique normal subextensions, $M/K$ and $N/K$, such that

1. $\text{Gal}(W/M) = M$ and $\text{Gal}(M/K) \cong S_4$;
2. $\text{Gal}(W/N) = N$ and $\text{Gal}(N/K) \cong D_4$;
3. $MN = W$;
4. $[M \cap N : K] = 2$.

4. 4-Torsion and $GL_2(\mathbb{Z}/4)$

Let $W/Q$ have Galois group $GL_2(\mathbb{Z}/4)$ and subextensions $M/Q$ and $N/Q$ as above. If $W = Q(E[4])$ for some elliptic curve $E$, then $N = Q(i, \sqrt{\Delta})$ and $M \cap N = Q(\sqrt{\Delta})$, where $\Delta$ is the discriminant of $E$. See pages 80, 81 in [1]. Also, if $W = Q(E[4])$, then $Q(i)$ is the subfield of $W$ fixed by $SL_2(\mathbb{Z}/4)$ ($MN \not\cong SL_2(\mathbb{Z}/4)$). See pages 69, 72 in [1]. To find a $W/Q$ that does not come from an elliptic curve, it suffices then to construct an appropriate $S_4$-extension $M/Q$:

Lemma 4. Let $M/Q$ have Galois group $S_4$ and let $\Delta$ be the discriminant of $M$ such that $Q(\sqrt{\Delta})$, the quadratic normal subfield of $M$, is not $Q(i)$. If $M \not\subset Q(E[4])$ for any elliptic curve $E$, then $W = M\mathbb{Q}(i, \sqrt{\Delta})$ satisfies the three properties following Theorem 1.

Proof. This is clear because $W$ has the correct Galois group over $Q$, $Q(i) \subset W$ is the fixed field of $SL_2(\mathbb{Z}/4)$, and $W$ is uniquely determined by its subfields $M$ and $N$. □
Given an elliptic curve $E$, we can determine the polynomial which generates the $S_4$-extension contained within $\mathbb{Q}(E[4])$.

**Theorem 5.** Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve defined over $\mathbb{Q}$ with discriminant $\Delta$ such that $\text{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{Z}/4)$. Then the unique $S_4$-subextension of $\mathbb{Q}(E[4])$ is the splitting field of the following quartic:

$$B_E(x) = x^4 - 4\Delta x - 12a_4\Delta.$$

**Proof.** See page 83 in [1] and page 9 in [4] (slightly different form).

Every $S_4$-extension $M$ contains a unique $S_3$-subextension $L$. If $M$ were to come from the 4-torsion of an elliptic curve $E$, then $L = \mathbb{Q}(E[2])$ as in Section 2. Also, $\mathbb{Q}(\sqrt{\Delta}) = M \cap N \subset L \subset M$.

If we replace $E$ with another curve $E'$ such that $E'[2] \cong E[2]$ (as Galois modules), then $\Delta$ and $a_4$ may both change. In this case, $B_{E'} \neq B_{E}$, and the two polynomials may determine distinct $S_4$-extensions of $\mathbb{Q}$. However, the $S_3$-field $L = \mathbb{Q}(E[2]) = \mathbb{Q}(E'[2])$ remains constant. Therefore, in order to construct an $S_4$-extension that does not come from an elliptic curve, we need to understand better the connection between $S_4$-extensions of $\mathbb{Q}$ that share a common $S_3$-subfield and the quartic polynomials that generate them.

5. $S_4$-EXTENSIONS AND SEMI-INVARIANTS

In [4], invariants and semi-invariants of binary quartic forms are used to develop a better 2-descent for elliptic curves. Here we use them to show that the class of $S_4$-extensions properly contains those that come from the 4-torsion point fields of elliptic curves.

5.1. **Definitions.** Suppose $K$ is a field, not having characteristic 2 or 3. To a quartic polynomial

$$g = ax^4 + bx^3 + cx^2 + dx + e \in K[x]$$

we associate a binary form $g(x, y) = ax^4 + bx^3y + cx^2y^2 + dx^2y^3 + ey^4$. $\text{GL}_2(K)$ acts on the set of these forms by

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : g(x, y) \mapsto g(\alpha x + \beta y, \gamma x + \delta y).$$

Two quartics $g$ and $h$ are considered equivalent under this action if they lie in the same $\text{GL}_2(K)$ orbit. In this case we write $g \sim h$.

We define the two basic invariants of $g$: $I = 12ae - 3bd + c^2$ and $J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$.

$I$ and $J$ are invariants under the subgroup of matrices $A$ such that $\det A = \pm 1$ (not all of $\text{GL}_2(K)$). They are thus invariant up to multiplication by fourth and sixth powers of $\det A$, respectively. We then think of $I$ and $J$ as being defined up to multiplication by fourth and sixth powers in $K$ and note that two equivalent quartics have the same $I$ and $J$. We will also follow [4] and define two semi-invariants of $g$:

$$p = 3b^2 - 8ac \quad r = b^3 + 8a^2d - 4abc,$$
which are invariant under action by a Borel subgroup in $GL_2(K)$, i.e., the subgroup of upper triangular matrices. Using $I$ and $J$, we then define the resolvent polynomial

$$F(x) = x^3 - 3Ix + J.$$ 

This definition of $F$ does not become problematic due to our notion that $I$ and $J$ are only defined up to multiplication by fourth and sixth powers, respectively. Suppose $F'(x) = x^3 + 3\alpha^4 Ix + \alpha^6 J$, where $\alpha$ lies in $K$. Then $F'(\alpha^2 x) = \alpha^6 F(x)$. The splitting field of $F$ is thus invariant under $GL_2(K)$. Finally, let $\phi$ be any root of $F$. This gives us a third semi-invariant of $g$,

$$z = \frac{4\alpha \phi - p}{3}.$$ 

5.2. Classification. These invariants and semi-invariants then allow us to describe the field extensions associated with quartic polynomials. Suppose a quartic $g \in K[x]$ is irreducible with splitting field $M/K$ and $\text{Gal}(M/K) \cong S_4$. The splitting field of $F$, $L$, is the unique $S_3$-extension contained within $M$. By choosing $\phi$ to be any root of $F$, we also define a cubic extension $K(\phi)/K$. Additionally, $M$ is the Galois closure of $K(\sqrt{z})$ and $N_{K(\phi)/K}(z) = r^2$.

Conversely, if we have any $v$ in $K(\phi) - K$ with square norm over $K(\phi)$, then the Galois closure of $K(\sqrt{v})$ is an $S_3$-extension containing $L$. Ostensibly, $v = \lambda_2 \phi^2 + \lambda_1 \phi + \lambda_0$ ($\lambda_i \in \mathbb{Q}$), but if $v$ is linear in $\phi$, then the quartic generating this extension has the same $I$ and $J$ invariants as $g$.

In section 3 of [4] it is shown that the set of $S_4$-extensions $M/K$ containing a given $S_3$-extension $L$ is in one-to-one correspondence with nontrivial elements of $H^1(G_K, V_4)$, where $G_K$ acts via the quotient $\text{Gal}(L/K)$ on $V_4$ as an automorphism group. This bijection is given by identifying $H^1(G_K, V_4)$ with $H = \ker(\text{Norm} : (K(\phi)^\times/(K(\phi)^\times)^2 \to K^\times/(K^\times)^2))$ in a way that is explicitly compatible with the construction of $M$ via $z$. One then obtains, as a subset, a one-to-one correspondence between quartics $g$ with invariants $I$ and $J$ up to $GL_2(K)$-equivalence and nonzero elements $z$ of $K(\phi)$ that are linear in $\phi$ and have square norm, up to equivalence mod $(K(\phi)^\times)^2$.

**Theorem 6.** Let $g$ and $h$ be two quartics defined over $K$ whose splitting fields, $M_g$ and $M_h$, are $S_4$-extensions of $K$. Then,

$$M_g = M_h \iff g \sim h.$$ 

**Proof.** Suppose $g \sim h$. Then they share the same $I$ and $J$ and we have $L$, the splitting field of $F = x^3 - 3Ix + J$, contained in both $M_g$ and $M_h$. Under the
correspondences above, \( g \) and \( h \) then generate the same \( V_4 \)-extension of \( L \); thus \( M_g = M_h \).

Now suppose \( M_g = M_h = M \). \( M \) contains a unique field \( L \) with Galois group \( S_3 \) over \( K \). Clearly, if \( g \) and \( h \) share the same \( I \) and \( J \), then the above correspondences indicate that they would generate the same extension only if they were equivalent. So suppose \( g \) and \( h \) have distinct \( I \)- and \( J \)-invariants. Then they correspond to different elements of \( H \) and thus distinct \( V_4 \)-extensions of \( L \). But this cannot be. Hence \( g \sim h \).

There is also a simple criterion to determine when two quartics are equivalent.

**Theorem 7** (Prop. 3.2(2) in [4]). Let \( g \) and \( h \) be two quartics having the same invariants \( I, J \) and semi-invariants \( z_g, z_h \). Then,

\[
g \sim h \iff z_gz_h \in (K(\phi))^2.
\]

This is precisely what we need in order to prove that a particular \( S_4 \)-extension \( M/\mathbb{Q} \) cannot sit inside \( \mathbb{Q}(E[4]) \) for any \( E \).

6. The Result

**Theorem 8.** Let \( g \) be any quartic polynomial defined over \( \mathbb{Q} \) such that its splitting field \( M \) has \( \text{Gal}(M/\mathbb{Q}) \simeq S_4 \). Let \( L \) be the unique \( S_3 \)-subextension, choose \( \phi \), and let \( g \) have semi-invariants \( p \) and \( a \).

\( M \subset \mathbb{Q}(E[4]) \) for some elliptic curve \( E \implies \phi(4a\phi - p) \in (K(\phi))^2 \).

**Proof.** Let \( z_E, a_E \) and \( p_E \) be the semi-invariants associated to \( B_E \), and let \( z \) be the \( z \)-semi-invariant of \( g \). Suppose \( M \) is contained within \( \mathbb{Q}(E[4]) \) for some elliptic curve \( E \). Then \( g \sim B_E \). In particular, \( g \) and \( B_E \) share the same \( I \) and \( J \) (a more stringent criterion than \( \mathbb{Q}(E[2]) = L \)), and \( z_E \) is defined to be linear in \( \phi \). \( I \) and \( J \) determine \( F \) (i.e. \( \phi \)), and hence \( z_E = \frac{4a_E - p_E}{3} \). \( B_E \) is monic, so \( a_E = 0 \). Also \( B_E \) has no quadratic or cubic terms, so \( p_E \) is zero. Thus \( z_E = \frac{4p}{3} \).

Now we have \( z z_E = \frac{4}{9}(\phi)(4a\phi - p) \). By Theorem 7, this is a square and we are done.

Tables of quartic extensions of \( \mathbb{Q} \) have been constructed by [3], ordered by absolute value of their discriminants (and signature), up to \( 10^7 \). There are 1,635,308 \( S_4 \)-fields in these tables, each given by a defining polynomial. Of these polynomials, all but 6,755 have \( \phi(4a\phi - p) \notin (K(\phi))^2 \) and so do not come from the 4-torsion of
any elliptic curve. In Table 1, we list all 18 such extensions with discriminant less than 1000 in absolute value. Of these, only 3 could (and do) lie inside the 4-torsion of an elliptic curve.

We thus have many $S_4$-extensions of $\mathbb{Q}$ which do not arise from the 4-torsion of any elliptic curve as well as an easy computation which usually tells us whether a given quartic generates such an extension. We close with a few remarks.

7. Concluding remarks

7.1. The converse of Theorem 8 is not true; given a quartic $g$ for which $\phi(4a\phi - p)$ is a square and $\text{Gal}(M_g/\mathbb{Q}) \simeq S_4$, there is not necessarily an elliptic curve $E : y^2 = x^3 + ax + b$ whose 4-torsion field contains $M_g$.

For example, consider $g = x^4 + 3x^2 - 2x + 1$, with discriminant 1264, $I = 21$, $J = 54$ and $p = 24$. It is the quartic of smallest discriminant for which $\phi(4a\phi - p)$ is square but $p \neq 0$. Let $\alpha$ be a root of $g$, and suppose there is an $h = x^4 - 4\Delta x - 12\Delta^2$ with root $\beta = b_1\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. $\beta$ must be in the kernel of the map $\text{tr}: \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}$ given by $\alpha \mapsto \text{trace}(\alpha)$, because the $x^4$-coefficient of $h$ is $\text{tr}(\beta)$. In fact, $\ker(\text{tr}) = (c_1, c_2, c_3)$ where

$$c_1 = 2\alpha^3 + 5\alpha - 3, \quad c_2 = 2\alpha^3 + 4\alpha - 3, \quad c_3 = 21\alpha^3 - \alpha^2 + 48\alpha - 33.$$

So $\beta = uc_1 + vc_2 + wc_3$ for some rationals $u$, $v$ and $w$.

Now, $\text{tr}(\beta^2) - \text{tr}(\beta^2)$ is twice the coefficient of $x^2$ in $h$. But $\text{tr}(\beta^2)$ and $\text{tr}(c_i c_j) \ (i \neq j)$ are all 0 whilst $\text{tr}(c_1^2) = -2$, $\text{tr}(c_2^2) = -4$ and $\text{tr}(c_3^2) = 158$. Hence, $h$ has zero $x^2$-coefficient if and only if

$$u^2 + 2v^2 - 79w^2 = 0.$$
However, this quadratic form does not vanish for any nontrivial rationals $u, v$ and $w$. So there is no elliptic curve $E : y^2 = x^3 + a_4 x + a_6$ whose 4-torsion field contains $M_g$. (We would like to thank the referee for suggesting this argument.)

7.2. When a quartic polynomial does correspond to an elliptic curve, it can be difficult to find the appropriate $E$. Since $\Delta$ appears in the coefficients of $B_E$ (giving us $I = -3^2\Delta a_4$ and $J = -2^43^3\Delta^2$) and the polynomials given in the tables have minimized coefficients (giving us relatively small $I$ and $J$), one cannot usually read the elliptic curve from the coefficients of the original quartic.

For example, the first extension listed, given by $x^4 - x + 1$, does not correspond to the 4-torsion field of the unique elliptic curve of conductor 229. Instead, the elliptic curve $E : y^2 = x^3 - 395712x - 90618048$ of conductor $2^2229^2$ has $B_E \sim x^4 - x + 1$. The $S_4$-extension coming from the curve of conductor 229 occurs much further down the list.

To find $E$, we employed the following method: Since $I$ and $J$ are determined only up to 4th and 6th powers respectively, we look for an $E$ defined by the minimal polynomial of a nonmaximal order of $L$ of conductor divisible by $\text{disc}(g)$ (and possibly other primes). Then $\Delta = k^2(\text{disc}(g))^3$ and the $a_4$ from $E$ often is divisible by $\text{disc}(g)$. We can hope in this way to obtain an $E$ such that $B_E$ has the correct $I$ and $J$.

This procedure was also successful for the other two quartics on the short list above, but it does not tell us whether or not such a curve exists. The order corresponding to $E$ could lie arbitrarily deep in $O_L$ or not be there at all, as is the case for the quartic in Remark 7.1.

7.3. If $g$ does come from the 4-torsion of some elliptic curve, it is never the case that $E$ is given by $y^2 = F$, the resolvent polynomial of $g$. This follows from Prop. 4.3 in [4].

7.4. The $I$ and $J$ invariants also determine isomorphism classes of 4-torsion modules. If $E$ and $E'$ are elliptic curves such that $\text{Gal}(\Q(E[4])/\Q) \simeq \text{Gal}(\Q(E'[4])/\Q) \simeq GL_2(\Z/4)$ and $B_E$ and $B_{E'}$ share $I$ and $J$ invariants, then $B_E \sim B_{E'}$ and so they generate the same $S_4$-extension. $I$ and $J$ also determine the discriminant of this extension ($D$ in Section 4) up to a twelfth power. In particular, the fourth roots of the two elliptic curves’ discriminants are the same; both curves generate the same $D_4$-extension. Thus, the two 4-torsion fields of $E$ and $E'$ are equal and they define the same mod 4 Galois representation.

References


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, 480 LINCOLN DRIVE, MADISON, WISCONSIN 53706-1388

E-mail address: holden@math.wisc.edu