Mathematical Research Letters **4**, 123–130 (1997)

REALIZATION OF SOME GALOIS REPRESENTATIONS OF LOW DEGREE IN MORDELL-WEIL GROUPS

David E. Rohrlich

Let $M \subset L \subset K$ be number fields, with K Galois over M, and put $G = \mathrm{Gal}(K/M)$ and $H = \mathrm{Gal}(K/L)$. We consider the representation ρ of G determined up to isomorphism by the formula

$$\mathrm{ind}_H^G 1_H \cong 1_G \oplus \rho,$$

where 1_H and 1_G denote the trivial representation of H and G respectively, ind_H^G is the induction functor from representations of H to representations of G, and the field of scalars of all representations at issue is taken to be $\mathbb{Q}$. We shall prove:

Theorem. *If $[L : M] \leqslant 9$ then there exists an elliptic curve E over M such that the natural representation of G on $\mathbb{Q} \otimes_{\mathbb{Z}} E(K)$ contains a subrepresentation isomorphic to ρ.*

For example, suppose that $G \cong S_9$ and $H \cong S_8$, where S_n denotes the symmetric group on n letters. Then ρ is one of the two irreducible representations of G of dimension 8, and according to our theorem there exists an elliptic curve E over M such that ρ occurs in $\mathbb{Q} \otimes E(K)$. The other irreducible representation of G of dimension 8 is $\rho \otimes \epsilon$, where ϵ is the "sign" character of G, and it too can be realized in a Mordell-Weil group: in fact a straightforward argument shows that if ρ occurs in $\mathbb{Q} \otimes E(K)$ then $\rho \otimes \epsilon$ occurs in $\mathbb{Q} \otimes E^\epsilon(K)$, where E^ϵ denotes the quadratic twist of E by ϵ.

The case $G \cong S_9$, $H \cong S_8$ just mentioned is actually the maximal instance of the theorem, in two respects: first, for any choice of G and H the dimension of ρ will be $\leqslant 8$, and second, if we assume without loss of generality that K is the normal closure of L over M then G is always isomorphic to a subgroup of S_9. It follows in particular that G is not isomorphic to one of the Weyl groups $W(E_6)$, $W(E_7)$, or $W(E_8)$, because these groups do not have embeddings in S_9. Thus we do not recover the "biggest" examples of Shioda ([8], [9], [10]), whose work on Mordell-Weil lattices of elliptic surfaces yields examples of type E_6, E_7, and E_8 by specialization. Here for a root system X the phrase "example of type X" means a Galois extension of number fields K/M together with an elliptic

Received June 13, 1996.
Research partially supported by NSF grant DMS-9396090

curve E over M and an identification of $G = \mathrm{Gal}(K/M)$ with $W(X)$ such that the representation of G on $\mathbb{Q} \otimes E(K)$ has a subrepresentation isomorphic to the representation of $W(X)$ on the rational span of X. In addition to examples of type E_6, E_7, and E_8, Shioda's theory also produces examples of type A_2 and D_4, and the latter cases fall within the framework of our theorem. One point to note in this connection is that in Shioda's examples the Galois extension of number fields K/M is obtained by specializing a Galois extension $\mathcal{K}/\mathcal{M}$, where $\mathcal{M}$ is a rational function field over $\mathbb{Q}$ in several variables. A natural question is whether every extension K/M with $\mathrm{Gal}(K/M) \cong W(X)$ can be obtained in this way. While there have been some positive results on this general type of question (cf. Beckmann [1], Black [2], Saltman [6]), I do not know of any theorem which would permit an affirmative answer in all of the cases at issue here.

We turn now to the proof of the theorem. Put

$$d = [G : H] = [L : M].$$

If $d = 1$ then the space of ρ is $\{0\}$ and there is nothing to prove. Henceforth we assume that $d \geqslant 2$. Fix representatives $\sigma_1, \sigma_2, \ldots, \sigma_d \in G$ for the distinct left cosets of H in G, with $\sigma_1 \in H$. Given an elliptic curve E over M, a prime ideal $\mathfrak{p}$ of K, and points $P, P' \in E(K)$, we write $P \equiv P' \pmod{\mathfrak{p}}$ to indicate that P and P' have the same image under reduction modulo $\mathfrak{p}$, the image being a point on the reduced curve if E/K has good reduction at $\mathfrak{p}$ and a point on the special fiber of the Néron minimal model in general.

Lemma. *Suppose that E is an elliptic curve over M and $P \in E(L)$ is an L-rational point on E satisfying the following conditions:*

(i) *There exists a prime ideal $\mathfrak{p}$ of K such that for $1 \leqslant i \leqslant d$,*

$$\sigma_i(P) \not\equiv P \pmod{\mathfrak{p}} \iff i = d.$$

(ii) *There exists an unramified prime ideal $\mathfrak{q}$ of K of odd residue characteristic such that for $1 \leqslant i \leqslant d$,*

$$\sigma_i(P) \equiv P \pmod{\mathfrak{q}}.$$

Then the representation of G on the subspace of $\mathbb{Q} \otimes E(K)$ spanned by the vectors

$$v_i = 1 \otimes (P - \sigma_i(P)) \qquad (2 \leqslant i \leqslant d)$$

is isomorphic to ρ.

Proof. The span of the vectors v_i is in fact stable under G because it coincides with the subspace

$$\left\{ \sum_{i=1}^{d} r_i \otimes \sigma_i(P) \in \mathbb{Q} \otimes E(K) : \sum_{i=1}^{d} r_i = 0 \right\}.$$

To prove the lemma we must show that the vectors v_i are linearly independent. Suppose on the contrary that there is a nontrivial linear relation

$$\sum_{i=2}^{d} r_i v_i = 0. \tag{1}$$

After multiplying by an element of $\mathbb{Q}^\times$ we may assume that the r_i are integers with no common prime factor. Let n be the order of the reduction of $P - \sigma_d(P)$ modulo $\mathfrak{p}$. Then $n > 1$ by (i). We shall prove that each r_i is divisible by n, and this contradiction will prove the lemma.

According to (1), the point $\sum_{i=2}^{d} r_i(P - \sigma_i(P))$ has finite order on E. On the other hand, by (ii) this point reduces to 0 modulo $\mathfrak{q}$. Now the kernel of reduction modulo $\mathfrak{q}$ on $E(K)$ can be viewed as a subgroup of $\hat{E}(\mathfrak{m})$, where $\hat{E}$ is the formal group of E over the completion of K at $\mathfrak{q}$ and $\mathfrak{m}$ is the maximal ideal of the completion. Since $\mathfrak{q}$ is unramified and of odd residue characteristic, $\hat{E}(\mathfrak{m})$ has no nonzero elements of finite order, and we conclude that

$$\sum_{i=2}^{d} r_i(P - \sigma_i(P)) = 0. \tag{2}$$

Fix an integer j such that $2 \leqslant j \leqslant d$; we will show that n divides r_j. Putting $\sigma = \sigma_d \sigma_j^{-1}$, we have $\sigma H \neq \sigma_d H$ since $j \neq 1$, and consequently $\sigma(P) \equiv P \pmod{\mathfrak{p}}$ by (i). Now apply σ to both sides of (2) and reduce modulo $\mathfrak{p}$. Since

$$\sum_{i=2}^{d} r_i(\sigma(P) - \sigma\sigma_i(P)) = \sum_{i=2}^{d} r_i(P - \sigma\sigma_i(P)) - \sum_{i=2}^{d} r_i(P - \sigma(P)),$$

we obtain

$$\sum_{i=2}^{d} r_i(P - \sigma\sigma_i(P)) \equiv 0 \pmod{\mathfrak{p}}.$$

But $\sigma\sigma_i H = \sigma_d H$ if and only if $i = j$. Thus $r_j(P - \sigma_d(P)) \equiv 0 \pmod{\mathfrak{p}}$ and n divides r_j.

It remains to construct an elliptic curve over M with a point satisfying the hypotheses of the lemma. The construction depends on the choice of an element ξ of L together with a polynomial

$$f(u) = \sum_{i=0}^{9} a_i u^i$$

such that $a_9 = 1$, $a_8 = 0$, $a_0 \neq 0$, $a_i \in M$ for $0 \leqslant i \leqslant 9$, and $f(\xi) = 0$. Given such ξ and f, we consider the projective plane curve E with affine equation

$$a_9 + a_7 x + a_6 y + a_5 x^2 + a_4 xy + (a_3 - b)y^2 + bx^3 + a_2 x^2 y + a_1 xy^2 + a_0 y^3 = 0, \tag{3}$$

where

$$b = -a_5 - a_7 - a_9. \tag{4}$$

On multiplying the equation for E by ξ^9 and substituting the values $x = \xi^{-2}$, $y = \xi^{-3}$, we see that $E(L)$ contains the point

$$P = (\xi^{-2}, \xi^{-3}).$$

The choice of b ensures that E also has an M-rational point, namely the point

$$O = (1, 0).$$

Now $a_0 \neq 0$ by assumption, so that E is a plane cubic. We shall choose ξ in such a way that E is a *smooth* plane cubic – hence an elliptic curve over M with origin O – and P satisfies the hypotheses of the lemma.

We begin with a small detail. Consider the equation

$$1 - 36x + 168y - 378x^2 + 504xy - 833y^2 + 413x^3 + 216x^2y - 63xy^2 + 8y^3 = 0. \tag{5}$$

Its relevance to our problem will become apparent only later, but if we reduce this equation modulo 7 we obtain

$$1 - x - x^2y + y^3 = 0. \tag{6}$$

A straightforward calculation shows that the projective plane curve over $\mathbb{F}_7$ with affine equation (6) is smooth, whence the projective plane curve over $\mathbb{Q}$ with affine equation (5) is also smooth. It follows that all but finitely many primes p have the property that the reduction of (5) modulo p is the affine equation of a smooth projective cubic curve over $\mathbb{F}_p$. We fix a positive integer e such that this property holds for all p not dividing e.

Next choose a prime number p not dividing $3de$ which splits completely in K, and let $\mathfrak{p}$ be a prime ideal of K lying over p. Pick a prime number q not dividing $6pd$ which is unramified in K, and let $\mathfrak{q}$ be a prime ideal of K lying over q. Finally, select $r \in \mathbb{Z}$ so that

$$\begin{cases} r \equiv 1 \pmod{p} \\ r \equiv 0 \pmod{q}. \end{cases} \tag{7}$$

Let us agree that if $\mathfrak{l}$ is a prime ideal of a number field F and α and β are elements of F integral at $\mathfrak{l}$ then $\alpha \equiv \beta \pmod{\mathfrak{l}}$ means $\alpha \equiv \beta \pmod{^*\mathfrak{l}}$, in other words, α and β are congruent modulo the maximal ideal of the localization at $\mathfrak{l}$ of the ring of integers of F. We claim that there is an element ξ of L, integral at p and q, satisfying the system of congruences

$$\begin{cases} \xi \equiv 1 \pmod{\sigma_i^{-1}(\mathfrak{p}) \cap L} & (1 \leqslant i \leqslant d-1) \\ \xi \equiv -8 \pmod{\sigma_d^{-1}(\mathfrak{p}) \cap L} & \\ \xi \equiv 0 \pmod{\sigma_i^{-1}(\mathfrak{q}) \cap L} & (1 \leqslant i \leqslant d) \end{cases} \tag{8}$$

as well as the trace condition

$$\text{tr}_{L/M}(\xi) + (9-d)r = 0. \tag{9}$$

To see this, observe that since p splits completely in K the prime ideals $\sigma_1^{-1}(\mathfrak{p}) \cap L, \ldots, \sigma_d^{-1}(\mathfrak{p}) \cap L$ of L are distinct. Of course all of these ideals are distinct from the ideals $\sigma_i^{-1}(\mathfrak{q}) \cap L$, because $p \neq q$. Consequently there exists an integer ξ' of L such that (8) holds with ξ replaced by ξ'. On writing $\text{tr}_{L/M}(\xi') = \sigma_1(\xi') + \sigma_2(\xi') + \cdots + \sigma_d(\xi')$ we deduce that

$$\begin{cases} \text{tr}_{L/M}(\xi') \equiv d - 9 \pmod{\mathfrak{p} \cap M} \\ \text{tr}_{L/M}(\xi') \equiv 0 \pmod{\mathfrak{q} \cap M}. \end{cases} \tag{10}$$

Now put

$$\xi = \xi' - \frac{\text{tr}_{L/M}(\xi') - (d-9)r}{d}.$$

Then (9) holds, while (7) and (10) together imply that ξ is congruent to ξ' modulo any prime ideal of L lying over $\mathfrak{p} \cap M$ or $\mathfrak{q} \cap M$. Therefore (8) holds also. Define

$$f(u) = (u-r)^{9-d} \prod_{i=1}^{d} (u - \sigma_i(\xi)),$$

and write $f(u) = \sum_{i=0}^{9} a_i u^i$ as before. It is immediate that $a_9 = 1$, that $a_i \in M$ for all i, and that $f(\xi) = 0$. Also (9) implies that $a_8 = 0$, and the congruences (7) and (8) imply that $r\xi \neq 0$, so that $a_0 \neq 0$. It remains to check that E is smooth and that P satisfies conditions (i) and (ii) of the lemma.

The remaining verifications depend on further deductions from the congruences (7) and (8). Observe first of all that since the coefficients of (3) are integral at p and q we can speak of the reduction of (3) modulo $\mathfrak{p} \cap M$ or $\mathfrak{q} \cap M$. Taking account of (4), and noting that $a_9 = 1$ while all other coefficients of f are congruent to 0 modulo $\mathfrak{q} \cap M$, we see that the reduction of (3) modulo $\mathfrak{q} \cap M$ is

$$1 + y^2 - x^3 = 0. \tag{11}$$

Since $q \nmid 6$ this is the affine equation of a smooth projective curve over $\mathbb{F}_q$. It follows in particular that E itself is smooth and that (3) is an equation of good reduction for E/K at $\mathfrak{q}$. Hence we can compute the reduction of points on $E(K)$ modulo $\mathfrak{q}$ by naively reducing homogeneous coordinates relative to (3), where the coordinates are chosen to be $\mathfrak{q}$-integral and not all 0 modulo $\mathfrak{q}$. In the case of the points $\sigma_i(P)$ we have

$$\sigma_i(P) = [\sigma_i(\xi)^{-2} : \sigma_i(\xi)^{-3} : 1] = [\sigma_i(\xi) : 1 : \sigma_i(\xi)^3], \tag{12}$$

and all of these points reduce to the same point $[0:1:0]$ on (11). Therefore condition (ii) of the lemma is satisfied. To verify (i), observe that (7) and (8) give $a_0 \equiv 8 \pmod{\mathfrak{p} \cap M}$ and

$$(-1)^{i+1} a_i \equiv \binom{8}{i-1} - 8\binom{8}{i} \pmod{\mathfrak{p} \cap M}$$

for $1 \leqslant i \leqslant 7$. Therefore equation (3) reduces modulo $\mathfrak{p} \cap M$ to equation (5). Since $p \nmid e$ it follows that (3) is an equation of good reduction for E at $\mathfrak{p}$ and that we may compute the reduction of $\sigma_i(P)$ modulo $\mathfrak{p}$ by reducing homogeneous coordinates relative to (3), as before. Referring to (12), we see that for $1 \leqslant i \leqslant d-1$ the point $\sigma_i(P)$ reduces modulo $\mathfrak{p}$ to $[1:1:1]$ while $\sigma_d(P)$ reduces modulo $\mathfrak{p}$ to $[-8:1:-512]$. As $p \neq 3$ the points $[1:1:1]$ and $[-8:1:-512]$ are distinct modulo p and condition (i) of the lemma follows.

Example. Take $M = \mathbb{Q}$, $L = \mathbb{Q}(\xi_1)$, and $K = \mathbb{Q}(\xi_1, \xi_2, \ldots, \xi_7)$, where $\xi_1, \xi_2, \ldots$ are the roots of the equation $x^7 - 7x + 3 = 0$. Then $d = 7$ and $G \cong \mathrm{PSL}(2, \mathbb{F}_7)$, a result of Trinks (see LaMacchia [3], p. 990, or Matzat [4], p. 212). Up to isomorphism, ρ is the unique absolutely irreducible representation of G of dimension 6, and according to our theorem there exists an elliptic curve E over $\mathbb{Q}$ such that ρ occurs in $\mathbb{Q} \otimes E(K)$. On the other hand, if one grants the "generalized Birch-Swinnerton-Dyer conjecture" then for *any* elliptic curve E over $\mathbb{Q}$ the multiplicity of ρ in $\mathbb{Q} \otimes E(K)$ is even ([5], p. 345), hence $\geqslant 2$ if ρ occurs in $\mathbb{Q} \otimes E(K)$. Taking E to be the curve

$$1 + 2x^3 - y^2 + x^2 y = 0 \tag{13}$$

(say with origin $O = [0:1:0]$) and putting $\xi = \xi_1$ and

$$P = (\xi^{-2}, 3\xi^{-3}) \in E(L),$$

we shall see that the representation of G on the span of the vectors

$$v_i = 1 \otimes (P - \sigma_i(P)) \in \mathbb{Q} \otimes E(K) \qquad (2 \leqslant i \leqslant 7)$$

is isomorphic to ρ. It is an open problem to exhibit a second G-stable subspace of $\mathbb{Q} \otimes E(K)$, linearly independent of the one considered here, on which the representation of G is also isomorphic to ρ.

We shall give two proofs that the space spanned by the vectors v_i is isomorphic as a representation to ρ. For the first proof, choose prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of K lying over 3 and 7 respectively. A calculation shows that that E has good reduction at 3 and 7 and in fact that (13) is an equation of good reduction at these primes. In view of the congruence

$$x^7 - 7x + 3 \equiv (x-1)^3 (x+1)^3 x \pmod{3},$$

we may assume that the ξ_i are numbered so that $\xi_1, \xi_2, \xi_3 \equiv 1 \pmod{\mathfrak{p}}$, $\xi_4, \xi_5, \xi_6 \equiv -1 \pmod{\mathfrak{p}}$, and $\xi_7 \equiv 0 \pmod{\mathfrak{p}}$. We may also choose the coset representatives $\sigma_1, \sigma_2, \ldots, \sigma_7$ so that $\sigma_i(\xi) = \xi_i$. Writing $P = [1 : 3/\xi : \xi^2]$, we find that $\sigma_i(P)$ reduces to $[1 : 0 : 1]$ modulo $\mathfrak{p}$ for $1 \leqslant i \leqslant 6$ while $\sigma_7(P)$ reduces to $[1 : 1 : 0]$ since $3/\xi_7 = -\xi_1\xi_2 \cdots \xi_6$. Hence condition (i) of the lemma is satisfied. As for (ii), the congruence

$$x^7 - 7x + 3 \equiv (x+3)^7 \pmod{7}$$

shows that $\sigma_i(P)$ reduces to $(4, -4)$ modulo $\mathfrak{q}$ for all i, but (ii) is not satisfied because $\mathfrak{q}$ is a ramified prime ideal (L ramifies precisely at 3 and 7). However, the proof of the lemma still goes through provided we know that reduction modulo $\mathfrak{q}$ is injective on the torsion subgroup of $E(K)$. In fact it suffices to show that $E(K)$ has no points of order 7, because locally at $\mathfrak{q}$ the kernel of reduction is $\hat{E}(\mathfrak{m})$ (notation as in the proof of the lemma) and $\hat{E}(\mathfrak{m})$ is a pro-7-group.

Let us prove, then, that the group $E(K)[7]$ of points on $E(K)$ of order dividing 7 is zero. If this group is nonzero then its dimension as a vector space over $\mathbb{F}_7$ is either one or two, and consequently its automorphism group is isomorphic either to $\mathbb{F}_7^\times$ or to $\mathrm{GL}(2, \mathbb{F}_7)$. The natural action of G on $E(K)[7]$ gives a map $\varphi : G \longrightarrow \mathrm{Aut}(E(K)[7])$, and since $\mathrm{PSL}(2, \mathbb{F}_7)$ is simple φ is either trivial or an embedding. But neither $\mathbb{F}_7^\times$ nor $\mathrm{GL}(2, \mathbb{F}_7)$ has a subgroup isomorphic to $\mathrm{PSL}(2, \mathbb{F}_7)$, so φ is trivial and $E(K)[7] = E(\mathbb{Q})[7]$. Thus we are reduced to showing that $E(\mathbb{Q})[7]$ is zero. Now E has good reduction at 5, and the group of points on the reduced curve over $\mathbb{F}_5$ has order 8. Hence the reduced curve has no points of order 7 over $\mathbb{F}_5$, and consequently E has no points of order 7 over $\mathbb{Q}$.

This completes the first proof. For the second we return to the general setting ($M \subset L \subset K$ are arbitrary number fields, with K Galois over M) but we place restrictions on G and ρ.

Proposition. *Assume that G is a nonabelian simple group and that ρ is irreducible as a representation over $\mathbb{Q}$. If E is an elliptic curve over M such that $E(L) \neq E(M)$ then the natural representation of G on $\mathbb{Q} \otimes E(K)$ contains a subrepresentation isomorphic to ρ.*

Proof. Choose a point $P \in E(L)$ not belonging to $E(M)$ and put $v_i = 1 \otimes (P - \sigma_i(P))$ $(2 \leqslant i \leqslant d)$ as before. Since ρ is irreducible over $\mathbb{Q}$ it suffices to show that the span of the v_i is not $\{0\}$. Suppose on the contrary that $v_i = 0$ for all i. Then $\sigma(P) - P$ is a torsion point for every $\sigma \in G$, whence the map $\sigma \mapsto \sigma(P) - P$ represents a class in $H^1(G, E(K)[n])$ for some n. We claim that $E(K)[n] = E(M)[n]$. Granting this, we deduce that $\sigma \mapsto \sigma(P) - P$ is actually a homomorphism from G to $E(M)[n]$ and is therefore identically zero since G is a nonabelian simple group and $E(M)[n]$ is abelian. It follows that $\sigma(P) = P$ for all $\sigma \in G$, whence $P \in E(M)$, a contradiction.

It remains to prove that $E(K)[n] = E(M)[n]$. It will suffice to see that $E(K)[p^\nu] = E(M)[p^\nu]$, where p is a prime and ν a positive integer. We use

induction on ν. As in the first proof, the canonical map $\varphi : G \longrightarrow \mathrm{Aut}(E(K)[p])$ is either injective or trivial; but $\mathrm{Aut}(E(K)[p])$ is isomorphic to $\{1\}$, $\mathbb{F}_p^\times$, or $\mathrm{GL}(2, \mathbb{F}_p)$, and none of these groups has a nonabelian simple subgroup (use the classification of subgroups of $\mathrm{GL}(2, \mathbb{F}_p)$ as in [7], pp. 280 – 281, together with two facts about the alternating group on five letters: (i) A_5 has no faithful 2-dimensional representations in characteristic 0, hence none in characteristics $\geqslant 7$, and (ii) A_5 is not isomorphic to a subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ for $p = 2, 3$, or 5). We conclude that φ is trivial and that $E(K)[p] = E(M)[p]$. Suppose now that $E(K)[p^\nu] = E(M)[p^\nu]$ for some $\nu \geqslant 1$. Then $pR \in E(M)$ for all $R \in E(K)[p^{\nu+1}]$. Hence the image of the canonical map $\varphi : G \longrightarrow \mathrm{Aut}(E(K)[p^{\nu+1}])$ is contained in the subgroup

$$B = \{\gamma \in \mathrm{Aut}(E(K)[p^{\nu+1}]) : \gamma(R) - R \in E(K)[p] \text{ for all } R \in E(K)[p^{\nu+1}]\}.$$

A straightforward calculation using the fact that $E(K)[p] = E(M)[p]$ shows that B is abelian, whence φ is trivial and $E(K)[p^{\nu+1}] = E(M)[p^{\nu+1}]$. This completes the proof.

References

1. S. Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering?*, J. Algebra **164** (1994), 430–451.
2. E. V. Black, *Arithmetic lifting of dihedral extensions*, J. Algebra (to appear).
3. S. E. LaMacchia, *Polynomials with Galois group PSL(2,7)*, Comm. Algebra **8** (1980), 983–992.
4. B. H. Matzat, *Konstruktive Galoistheorie*, Lect. Notes in Math. 1284, Springer-Verlag, 1987.
5. D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Comp. Math. **100** (1996), 311–349.
6. D. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250–283.
7. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
8. T. Shioda, *The Galois representation of type E_8 arising from certain Mordell-Weil groups*, Proc. Japan Acad. **65** (1989), 195–197.
9. T. Shioda, *Mordell-Weil lattices and Galois representations I, II, III*, Proc. Japan Acad. **65** (1989), 268–271, 296–299, 300–303.
10. T. Shioda, *Construction of elliptic curves with high rank via the invariants of the Weyl groups*, J. Math. Soc. Japan **43** (1991), 673–719.

Department of Mathematics, Boston University, Boston, MA 02215
E-mail address: rohrlich@math.bu.edu