MATHEMATICS OF COMPUTATION
Volume 78, Number 267, July 2009, Pages 1825–1836
S 0025-5718(09)02218-2
Article electronically published on January 22, 2009

A COMPUTATIONAL APPROACH TO THE 2-TORSION STRUCTURE OF ABELIAN THREEFOLDS

JOHN CULLINAN

ABSTRACT. Let A be a three-dimensional abelian variety defined over a number field K. Using techniques of group theory and explicit computations with MAGMA, we show that if A has an even number of $\mathbf{F}_\mathfrak{p}$-rational points for almost all primes $\mathfrak{p}$ of K, then there exists a K-isogenous A' which has an even number of K-rational torsion points. We also show that there exist abelian varieties A of all dimensions ≥ 4 such that $\#A_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ is even for almost all primes $\mathfrak{p}$ of K, but there does not exist a K-isogenous A' such that $\#A'(K)_{tors}$ is even.

1. INTRODUCTION

Given an abelian variety A defined over a number field K, the Mordell-Weil theorem asserts that $A(K)$ is a finitely-generated abelian group. Moreover, we can estimate the size of the torsion subgroup $A(K)_{tor}$ by using the fact that there exists an injective homomorphism $A(K)[m] \hookrightarrow A_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$, where $A(K)[m]$ is the K-rational kernel of the multiplication-by-m isogeny, and $\mathfrak{p}$ is a prime of good reduction such that $\mathfrak{p} \nmid m$. This provides us with the basic divisibility property $\#A(K)[m] \equiv 0 \pmod{\#A_\mathfrak{p}(\mathbf{F}_\mathfrak{p})}$, relating the torsion subgroup of $A(K)$ and the $\mathbf{F}_\mathfrak{p}$-points of $A_\mathfrak{p}$ for almost all primes $\mathfrak{p}$ of $\mathcal{O}_K$. On the other hand, it is not clear whether the converse holds. The relevant question, originally posed by Lang and investigated by Katz in [7], is the following:

Question 1. Let $m \geq 2$ be an integer and S a set of good primes for A of density 1. If $\#A_\mathfrak{p}(\mathbf{F}_\mathfrak{p}) \equiv 0(m)$ for all $p \in S$, does there exist a K-isogenous A' such that $\#A'(K)_{tor} \equiv 0(m)$?

In [7], Katz showed that Lang's question has a positive answer when A is an elliptic curve, and in the special case $m = \ell$ is prime, for two-dimensional abelian varieties. However, he constructs explicit counterexamples for all odd primes ℓ in all dimensions greater than 2. In this paper, we revisit Question 1 for the prime $\ell = 2$ when A is three-dimensional (the first case where the answer is unknown) and obtain the following result:

Theorem 1. *Let A be a three-dimensional abelian variety defined over a number field K. If $\#A_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ is even for almost all primes $\mathfrak{p}$ of K, then there exists a K-isogenous A' such that $\#A'(K)_{tors}$ is even.*

Received by the editor February 26, 2007 and, in revised form, August 2, 2008.
2000 *Mathematics Subject Classification.* Primary 11G10.
Key words and phrases. Abelian variety, torsion points.

It is natural to ask whether Theorem 1 can be extended to abelian varieties of dimension greater than 3. It turns out that such a generalization is not possible; Serre constructed a counterexample in dimension 4, and we have generalized this to all dimensions greater than 4. In particular, we show in Section 6 that there exist abelian varieties A of all dimensions ≥ 4 such that $\#A_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})$ is even for almost all primes $\mathfrak{p}$ of K, but there does not exist a K-isogenous A' such that $\#A'(K)_{tors}$ is even,

2. Background and setup

The proof of Theorem 1 amounts to determining whether the subgroups of the finite simple group $\mathrm{S}_6(2)$ satisfy certain representation-theoretic properties. In this section we collect the relevant information about $\mathrm{S}_6(2)$ which will be used in this paper, and outline the proof of Theorem 1.

For an abelian variety A of dimension n over a perfect field K, the ℓ-adic Tate module $T_\ell(A) = \mathrm{Hom}(\mathbf{Q}_\ell/\mathbf{Z}_\ell, A(\overline{K}))$ is a free $\mathbf{Z}_\ell$-module of rank $2n$, where $\overline{K}$ is a fixed algebraic closure of K. The *mod ℓ representation* $\overline{\rho_\ell} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(T_\ell(A)\otimes\mathbf{F}_\ell) \simeq \mathrm{GL}_{2n}(\mathbf{F}_\ell)$ is the representation-theoretic formulation of the natural action of $\mathrm{Gal}(\overline{K}/K)$ on the $\overline{K}$-valued points of A of order ℓ. The vector space $T_\ell(A) \otimes \mathbf{F}_\ell$ is equipped with a non-degenerate, skew-symmetric, Galois-invariant pairing (the *Weil pairing*) [5, p. 133], hence $\mathrm{im}\,\overline{\rho_\ell} \leq \mathrm{Sp}_{2n}(\mathbf{F}_\ell)$. Our approach uses a reformulation of Question 1, when m is a prime number ℓ, due to Katz in [7, p. 483]:

Question 2 ($\mathrm{mod}\ \ell$ version of Question 1)**.** If for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we have $\det(I - \overline{\rho_\ell}(\sigma)) = 0$ in $\mathbf{F}_\ell$, does the semisimplification of $T_\ell(A) \otimes \mathbf{F}_\ell$ contain the trivial representation?

We now take K to be a number field and the dimension of A to be 3. Set $\ell = 2$, so that $\mathrm{im}\,\overline{\rho_2} \leq \mathrm{Sp}_6(\mathbf{F}_2)$. It is known that [8, p. 25] $\mathrm{Sp}_6(\mathbf{F}_2)$ is isomorphic to the finite simple group $\mathrm{S}_6(2)$. Let $G \leq \mathrm{S}_6(2)$ denote the image of the mod 2 representation. In Question 2, the condition on G is that each of its elements have 1 as an eigenvalue in its (natural) degree-6, $\mathbf{F}_2$-representation. We call such subgroups *fixed-point subgroups* of $\mathrm{S}_6(2)$. The proof of Theorem 1 comes down to the fact that for every fixed-point subgroup G of $\mathrm{S}_6(2)$, the module $\mathbf{F}_2[G]$ has a trivial Jordan-Hölder factor, hence our strategy is composed of two basic steps:

Step 1: Identify the fixed-point subgroups of $\mathrm{S}_6(2)$.

Step 2: Compute the Jordan-Hölder series $\mathbf{F}_2[G]$.

Any element of $\mathrm{S}_6(2)$ lying in a 2-power conjugacy class necessarily has all of its eigenvalues equal to 1, hence we are interested only in the eigenvalues of the odd-order conjugacy classes. For those, we refer to the Brauer character table of $\mathrm{S}_6(2)$ in characteristic 2 [6, p. 110]:

		1451520	160	648	108	30	7	9	15
	ind	$1A$	$3A$	$3B$	$3C$	$5A$	$7A$	$9A$	$15A$
ϕ_1	+	1	1	1	1	1	1	1	1
ϕ_2	−	6	3	-3	0	1	-1	0	-2
ϕ_3	+	8	-4	-1	2	-2	1	-1	1
ϕ_4	+	14	2	5	-1	-1	0	-1	2
ϕ_5	+	48	-12	3	0	-2	-1	0	-2
ϕ_6	+	64	4	-8	-2	-1	1	1	-1
ϕ_7	+	112	-8	-5	-2	2	0	1	2
ϕ_8	+	512	-16	8	-4	2	1	-1	-1

The splitting field of $S_6(2)$ is $\mathbf{F}_2$, hence the characteristic polynomials of the odd-order conjugacy classes of $S_6(2)$ in its natural $\mathbf{F}_2$-representation are simply the reductions modulo 2 of the lifted $\mathbf{C}$-valued polynomials, which are obtained as in the case of ordinary representation theory. By expressing the elementary symmetric polynomials in terms of the power-sum polynomials [9, p. 15], and then reducing modulo 2, we obtain the characteristic polynomials of the odd-order classes:

Class	Characteristic Polynomial
$1A$	$(x-1)^6$
$3A$	$x^6+x^5+x^4+x^2+x+1$
$3B$	$x^6+x^4+x^3+x^2+1$
$3C$	x^6+1
$5A$	x^6+x^5+x+1
$7A$	$x^6+x^5+x^4+x^3+x^2+x+1$
$9A$	x^6+x^3+1
$15A$	$x^6+x^4+x^3+x^2+1$

It is now easy to check that the conjugacy classes $3B$, $7A$, $9A$, and $15A$ do not afford 1 as an eigenvalue. Therefore, any fixed-point subgroup G of $S_6(2)$ must be a *proper* subgroup of $S_6(2)$ with odd-order classes of type $1A$, $3A$, $3C$, or $5A$.

We organize our search for the fixed-point subgroups G as follows. Since $G \leq S_6(2)$ is proper, it must be contained in some maximal subgroup of $S_6(2)$. We will show that no maximal subgroup of $S_6(2)$ is a fixed-point subgroup, whence G must lie in (at least) a "level-2" maximal subgroup of $S_6(2)$. We iterate this process until all fixed-point subgroups are found.

3. The subgroup structure of $S_6(2)$

Since our proof relies heavily on the subgroup structure of $S_6(2)$, we use this section to record its maximal subgroups, as well as some basic results which will be used throughout the paper. We use Atlas notation, e.g., $U_n(q)$ for $PSU_n(\mathbf{F}_{q^2})$, and $L_n(q)$ for $PSL_n(\mathbf{F}_q)$.

Maximal Subgroups of $S_6(2)$	**Index**
$U_4(2)$:2	28
S_8	36
$U_3(3)$:2	120
2^6:$L_3(2)$	135
$(2^{1+4} \times 2^2)$:$(S_3 \times S_3)$	315
$S_3 \times S_6$	336
$L_2(8)$:3	960

Definition 1. Any fixed-point subgroup of $S_6(2)$ whose semisimplification does not contain the trivial representation will be called an *obstruction*.

Lemma 1. *A cyclic fixed-point subgroup of* $\mathrm{S}_6(2)$ *cannot be an obstruction.*

Proof. If $G = \langle g \rangle$ is a fixed-point subgroup, then there exists $v \in \mathbf{F}_2^6$ such that $g \cdot v = v$. Since G is cyclic, this means all of G acts trivially on the line spanned by v, corresponding to a trivial Jordan-Hölder factor in the semisimplification of $\mathbf{F}_2[G]$. □

Lemma 2. *A fixed-point subgroup of* $\mathrm{S}_6(2)$ *must have index divisible by* 7*.*

Proof. The characteristic polynomial of the class $7A$ of $\mathrm{S}_6(2)$ does not vanish at 1, hence no element of order 7 in $\mathrm{S}_6(2)$ can have 1 as an eigenvalue. □

Definition 2. The *semisimplification type* of a representation V of a finite group G is the vector whose entries are the dimensions of the Jordan-Hölder factors of V.

Since there are no non-trivial irreducible representations of a p-group in characteristic p, it follows that the semisimplification type of a 2-subgroup of $\mathrm{S}_6(2)$ is $(1, 1, 1, 1, 1, 1)$. We therefore have the following lemma.

Lemma 3. *Every* 2*-subgroup of* $\mathrm{S}_6(2)$ *is a fixed-point subgroup, but not an obstruction.*

4. The role of magma

A polynomial over a field k has 1 as a root if and only if its coefficients sum to 0 in k. Therefore, G is a fixed-point subgroup of $\mathrm{S}_6(2)$ if and only if the characteristic polynomial of each conjugacy class has an even number of terms. We use the computer program MAGMA to determine the fixed-point subgroups as follows:

Step 1

```
C:=ConjugacyClasses(G);
for i:=1 to #C do
print CharacteristicPolynomial(C[i][3]);
end for;
```

Now suppose G is a fixed-point subgroup of $\mathrm{S}_6(2)$ with generators $a, b, \ldots c$. The following code will determine the composition factors of G:

Step 2

```
A:=MatrixAlgebra<GF(2), 6 | a,b,...,c>;
M:=RModule(A);
B:=CompositionFactors(B);
B;
```

Remark. Since any one-dimensional composition factor over $\mathbf{F}_2$ is automatically trivial, it suffices to show that the semisimplification of every fixed-point subgroup of $\mathrm{S}_6(2)$ contains a one-dimensional factor.

Our approach is iterative, hence we require a compact, easy-to-read notational scheme to present our results. Given a subgroup G of $\mathrm{S}_6(2)$ which is not a fixed-point subgroup, we look to its maximal subgroups for fixed-point subgroups. Whenever one is found, the MAGMA code of Section 4 will show that the semisimplification type has a "1".

Let $G_1, \ldots, G_n$ be the maximal subgroups of G, ordered so that $G_1, \ldots, G_k$ are fixed-point subgroups, and $G_{k+1}, \ldots, G_n$ are not; let ss_i denote the semisimplification type of G_i We illustrate this in the following table:

Maximal Subgroup	Fixed-Point	Semisimplification Type
$G_1, \ldots, G_k$	Y	$ss_1, \ldots ss_k$
G_{k+1}	N	-
G_{k+2}	N	-

Maximal Subgroup	Fixed-Point	Semisimplification Type
$G_{(k+1)_1}, \ldots, G_{(k+1)_k}$	Y	$ss_{(k+1)_1}, \ldots, ss_{(k+1)_k}$
$G_{(k+1)_{k+1}}$	N	-

The table is iterative in the sense that for each maximal subgroup which is not a fixed-point subgroup, we present its subgroup data in its entry in the table. Owing to the amount of data involved, we only present our results for two of the maximal subgroups of $\mathrm{S}_6(2)$, namely $\mathrm{L}_2(8)$:3 and S_8. The rest of the data can be found at the website `http://math.bard.edu/cullinan/groupdata.pdf`. Moreover, the data presented is only for conjugacy classes of subgroups, since conjugate subgroups have the same semisimplification types.

Remark. If a subgroup H of $\mathrm{S}_6(2)$ is not a fixed-point subgroup, and has the property that all of its subgroups are either cyclic or 2-groups, then we do not investigate its maximal subgroup structure since it cannot contain an obstruction.

In the following section we provide some examples of the output of the computer search.

5. Examples

5.1. **Subgroups of $\mathrm{L}_2(8)$:3.** The group $\mathrm{L}_2(8)$ has three Brauer Characters of degree 2 which fuse to form the single degree-6 Brauer Character of $\mathrm{L}_2(8)$:3. The order of $\mathrm{L}_2(8)$:3 is divisible by 7, hence it cannot be an obstruction. The maximal subgroup structure of $\mathrm{L}_2(8)$:3, along with its semisimplification data, is displayed in the following table:

Maximal Subgroup of $\mathbf{L_2(8)}$:3	**F-P**	**Type**
7:6	N	-
9:6	N	-
2^3:7:3	N	-

7:6		
$\mathbf{Z}/6$	Y	(1,1,1,1,2)
$\mathbf{Z}/7$, D_7	N	-

9:6		
$A_3 \wr S_2$	N	-
D_9	N	-
9:3	N	-

$A_3 \wr S_2$		
$\mathbf{Z}/6$	Y	(1,1,1,1,2)
$\mathbf{Z}/6$, $\mathbf{Z}/3$	N	-

D_9		
S_3, $\mathbf{Z}/9$	N	-

9:3		
$\mathbf{Z}/9$, $\mathbf{Z}/9$, $\mathbf{Z}/9$, $\mathbf{Z}/3 \times \mathbf{Z}/3$	N	-

2^3:7:3		
2^3:3	Y	$(1,1,2,2)$
7:3	N	-
2^3:7	N	-

2^3:7		
$\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$	Y	(1,1,1,1,1,1)
$\mathbf{Z}/7$	N	-

There are no novel subgroups of $\mathrm{L}_2(8)$:3 (in the sense of [3, p. xix]), whence the omission of $\mathrm{L}_2(8)$ from the table above.

5.2. **Subgroups of S_8.** The order of S_8 is divisible by 7, so S_8 is not a fixed-point subgroup of $S_6(2)$. The maximal subgroups [3, p. 22] of S_8, along with their semisimplification data, are as follows:

Maximal Subgroup of S_8	**F-P**	**Type**
$2^4{:}S_4$, $S_6 \times S_2$, $S_4 \wr S_2$	Y	(1, 1, 2, 2), (1,1,4), (1,1,4)
A_8, S_7, $\mathrm{L}_2(7){:}2$, $2^3{:}\mathrm{L}_2(7)$, $S_5 \times S_3$	N	-

We now provide a case-by-case description of the non-fixed-point groups, starting with S_7. The alternating group A_7 is a maximal subgroup of S_7, but we only include data for its subgroups isomorphic to $\mathrm{L}_2(7)$ since they fuse in S_7 to form the novel subgroup 7:6. All other subgroups of A_7 are ordinary and are therefore subsumed by the maximal subgroups of S_7.

Maximal Subgroup of S_7	**F-P**	**Type**
S_6, $S_5 \times S_2$, $S_4 \times S_3$	Y	(1,1,4), (1,1,4), (1,1,2,2)
7:6	N	-
Z/6 | Y | (1,1,1,1,2)		
Z/7, D_7 | N | -		
$\mathrm{L}_2(7)$	N	-
S_4, S_4 | Y | (1,1,2,2), (1,1,2,2)		
7:3 | N | -		
$\mathrm{L}_2(7)$	N	-
S_4, S_4 | Y | (1,1,2,2), (1,1,2,2)		
7:3 | N | -		

Next, we consider the subgroup $\mathrm{L}_2(7){:}2$ of S_8. The two maximal subgroups of $\mathrm{L}_2(7)$ isomorphic to S_4 fuse to form the novel maximal subgroups D_8 and D_6 of $\mathrm{L}_2(7){:}2$. The semisimplification data for $\mathrm{L}_2(7){:}2$ is given by the following:

Maximal Subgroups of $\mathrm{L}_2(7){:}2$	**F-P**	**Type**
D_8, D_6	Y	(1,1,1,1,1,1), (1,1,2,2)
7:6	N	-
Z/6 | Y | (1,1,1,1,2)		
Z/7, D_7 | N | -		
S_4, S_4	Y	(1,1,2,2), (1,1,2,2)

The maximal subgroup $S_5 \times S_3$ of S_8 intersects the conjugacy class $15A$ of $\mathrm{S}_6(2)$, hence is not a fixed-point subgroup. The subgroup data is as follows:

Maximal Subgroups of $S_3 \times S_5$			**F-P**	**Type**
$A_3 \times S_5$			N	-
$A_3 \times D_6$, $A_3 \times S_4$, S_5	Y	(1,1,2,2), (1,1,2,2),(1,1,4)		
$A_3 \times F_{20}$	N	-		
$\mathbf{Z}/12$, F_{20}	Y	(1,1,1,1,1,2), (1,1,4)		
$A_3 \times D_5$	N	-		
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,1,2) (1,1,4)		
$\mathbf{Z}/15$	N	-		
$A_3 \times A_5$	N	-		
$A_3 \times S_3$, $A_3 \times A_4$, A_5	Y	(1,1,2,2), (1,1,2,2),(1,1,4)		
$A_3 \times D_5$	N	-		
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,1,2), (1,1,4)		
$\mathbf{Z}/15$	N	-		
$S_3 \times A_5$			N	-
$S_3 \times S_3$, $S_3 \times A_4$, $S_2 \times A_5$	Y	(1,1,2,2), (1,1,2,2),(1,1,4)		
$S_3 \times D_5$	N	-		
D_6, $S_2 \times S_5$	Y	(1,1,1,1,1,2), (1,1,4)		
$A_3 \times D_5$	N	-		
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,1,2), (1,1,4)		
$\mathbf{Z}/15$	N	-		
$S_3 \times \mathbf{Z}/15$	N	-		
$S_3, \mathbf{Z}/10$	Y	(1,1,1,1,1,2), (1,1,4)		
$\mathbf{Z}/15$	N	-		
D_{15}	N			
S_3, D_5	Y	(1,1,1,1,1,2), (1,1,4)		
$\mathbf{Z}/15$	N			
$A_3 \times A_5$	N	-		
$A_3 \times S_3$, $A_3 \times A_4$, A_5	Y	(1,1,2,2), (1,1,2,2),(1,1,4)		
$A_3 \times D_5$	N	-		
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,1,2), (1,1,4)		
$\mathbf{Z}/15$	N	-		
$3.S_5$			N	-
$S_3 \times S_3$, $A_4{:}S_3$, S_5	Y	(1,1,2,2), (1,1,2,2),(1,1,4)		
$(\mathbf{Z}/15){:}(\mathbf{Z}/4)$	N	-		
$\mathbf{Z}/3 \rtimes \mathbf{Z}/4$, $\mathbf{Z}/5 \rtimes \mathbf{Z}/4$	Y	(1,1,1,1,1,2), (1,1,4)		
$D_5 \times A_3$	N	-		
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,1,2) (1,1,4)		
$\mathbf{Z}/15$	N	-		
$A_3 \times A_5$	N	-		
$A_3 \wr S_3$, $A_3 \times A_4$, A_5	Y	(1,1,2,2), (1,1,2,2),(1,1,4)		
$D_5 \times A_3$	N	-		
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,1,2), (1,1,4)		
$\mathbf{Z}/15$	N	-		

Maximal Subgroups of $S_3 \times S_5$ (cont'd)	**F-P**	**Type**
$S_3 \times D_6$, $S_3 \times S_4$, $S_2 \times S_5$	Y	(1,1,1,1,2), (1,1,2,2),(1,1,4)
$S_3 \times F_{20}$	N	-
$S_3 \times \mathbf{Z}/4$, $S_2 \times F_{20}$	Y	(1,1,1,1,2), (1,1,4)
$(\mathbf{Z}/15)$:$(\mathbf{Z}/4)$	N	-
$\mathbf{Z}/3 \rtimes \mathbf{Z}/4$, F_{20}	Y	(1,1,1,1,2), (1,1,4)
$A_3 \times D_5$	N	-
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,2), (1,1,4)
$\mathbf{Z}/15$	N	-
$A_3 \times F_{20}$	N	-
$\mathbf{Z}/12$, F_{20}	Y	(1,1,1,1,2), (1,1,4)
$A_3 \times D_5$	N	-
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,2), (1,1,4)
$\mathbf{Z}/15$	N	-
$S_3 \times D_5$	N	-
D_6, $S_2 \times D_5$	Y	(1,1,1,1,2), (1,1,4)
$A_3 \times D_5$	N	-
$\mathbf{Z}/6$, D_5	Y	(1,1,1,1,2), (1,1,4)
$\mathbf{Z}/15$	N	-
$S_3 \times \mathbf{Z}/15$	N	-
$S_3, \mathbf{Z}/10$	Y	(1,1,1,1,2), (1,1,4)
$\mathbf{Z}/15$	N	-
D_{15}	N	
S_3, D_5	Y	(1,1,1,1,2), (1,1,4)
$\mathbf{Z}/15$	N	

We end with the subgroups of A_8 which give rise to the novel subgroups 2^4:S_4 and $\mathrm{L}_2(7)$:2 of S_8, namely the two subgroups isomorphic to 2^3:$\mathrm{L}_2(7)$. The data for each group is identical, so we only present it once.

Maximal Subgroups of 2^3:$\mathbf{L_3(2)}$	**F-P**	**Type**
2^3:S_4, 2^3:S_4	Y	(1,1,2,2) (1,1,2,2)
$\mathrm{L}_2(7)$	N	-
S_4, S_4	Y	(1,1,2,2) (1,1,2,2)
7:3	N	-
$\mathrm{L}_2(7)$	N	-
S_4, S_4	Y	(1,1,2,2) (1,1,2,2)
7:3	N	-
2^3:3:7	N	-
2^3:3	Y	(1, 1, 2, 2)
7:3	N	-
2^3:7	N	-
$\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$	Y	(1,1,1,1,1,1)
$\mathbf{Z}/7$	N	-

6. Higher-dimensional abelian varieties

Recall that Question 1 has a positive answer when A has dimension 1, that Question 2 has a positive answer when A has dimension 2, and that counter-examples to Question 2 (and therefore Question 1) exist in all dimensions greater than 2, provided $\ell \neq 2$.

The natural question is whether or not Theorem 1 is valid for abelian varieties of arbitrary dimension. The answer is no: Serre has provided the following example of an eight-dimensional mod-2 representation for which every element has a fixed-point, but whose Jordan-Hölder series does not contain the trivial representation [10].

The simple group $\mathrm{SL}_3(\mathbf{F}_2)$ has an irreducible eight-dimensional symplectic representation (the Steinberg representation). The characteristic polynomials of the odd-order classes of $\mathrm{SL}_3(\mathbf{F}_2)$ are as follows:

Class	Characteristic Polynomial
$3A$	$x^8 + x^7 + x^6 + x^2 + x + 1$
$7A$	$x^8 + x^7 + x + 1$
$7B$	$x^8 + x^7 + x + 1$

Each polynomial clearly has 1 as a root and the Steinberg representation is irreducible, hence the semisimplification does not contain the trivial representation.

To see there exists an abelian variety with the prescribed mod 2 representation, start with a 4-dimensional abelian variety A over $\mathbf{Q}$ such that $\operatorname{im}\overline{\rho_{\ell,A}} = \mathrm{Sp}_8(\mathbf{F}_2)$. Extend the base-field $\mathbf{Q}$ to the fixed-field K of $\mathrm{SL}_3(\mathbf{F}_2)$. By Galois theory, the image of the mod 2 representation is $\mathrm{SL}_3(\mathbf{F}_2)$. Thus Serre's example produces a counterexample to Question 1.

We can easily extend Serre's construction to produce counterexamples in *all* dimensions ≥ 4. For every even integer $n \geq 2$, there is an embedding of classical groups

$$\mathrm{Sp}_{(n-m)} \times \mathrm{Sp}_m \hookrightarrow \mathrm{Sp}_n$$

whenever m is even and $2 \leq m < n/2$ [8, Prop. 4.1.3]. Writing $n = 8 + 2 \cdot (n-8)/2$, we see that the embedding

$$\mathrm{SL}_3(\mathbf{F}_2) \times \underbrace{\mathrm{Sp}_2(\mathbf{F}_2) \times \cdots \times \mathrm{Sp}_2(\mathbf{F}_2)}_{(n-8)/2} \leq \mathrm{Sp}_8(\mathbf{F}_2) \times [\mathrm{Sp}_2(\mathbf{F}_2)]^{(n-8)/2} \leq \mathrm{Sp}_n(\mathbf{F}_2)$$

clearly gives rise to a fixed-point subgroup of $\mathrm{Sp}_n(\mathbf{F}_2)$ without a trivial Jordan-Hölder factor. As stated in the Introduction, this shows that there exist abelian varieties A of all dimensions ≥ 4 such that $\#A_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})$ is even for almost all primes $\mathfrak{p}$ of K, but there does not exist a K-isogenous A' such that $\#A'(K)_{tors}$ is even.

Appendix A. A group-theoretic proof

Our basic strategy for the proof was first to use theoretical considerations to reduce the original problem to a finite computation, and then to demonstrate how a computer algebra package can be used to perform this computation. This technique was employed in several instances by the author in [4]. Upon submission of the paper, the referee suggested an alternative argument that replaces the computer

algebra portion of the finite calculation with arguments from group theory and geometric algebra. We would like to take this opportunity to thank the referee and to present a sketch of his argument.

We start by recalling some facts from finite group theory; see [1] for details. Given a finite group $\mathcal{G}$ with order divisible by p, let $O^p(\mathcal{G})$ be the smallest normal subgroup of $\mathcal{G}$ such that $\mathcal{G}/O^p(\mathcal{G})$ is a p-group, and let $O_p(\mathcal{G})$ be the largest normal p-subgroup of $\mathcal{G}$. The *Fitting Subgroup* $F(\mathcal{G})$ of $\mathcal{G}$ is the largest nilpotent normal subgroup of $\mathcal{G}$, and is isomorphic to the direct products of all the $O_p(\mathcal{G})$. Now let $V = \mathbf{F}_2^6$, and let $H \leq S_6(2)$ be an obstruction of minimal order.

Lemma 4. *The group H cannot have a 2-group as a quotient, so that $H = O^2(H)$.*

Proof. A 2-group acts unipotently on V, hence it's Jordan-Hölder series has trivial factors. Since H is an obstruction, this is impossible. □

A Sylow-3 subgroup S of $S_6(2)$ has order 81 and is isomorphic to $\mathbf{Z}/3 \wr \mathbf{Z}/3 \simeq (\mathbf{Z}/3 \times \mathbf{Z}/3 \times \mathbf{Z}/3) \rtimes \mathbf{Z}/3$. Let T be a Sylow-3 subgroup of H.

Lemma 5. *The group T is elementary abelian of order dividing 9, and is a proper subgroup of H.*

Proof. Any central element of S lies in its elementary abelian subgroup $(\mathbf{Z}/3)^3$ and has no fixed points, hence T is a proper subgroup of S. Moreover, if T contains any element of S outside $(\mathbf{Z}/3)^3$, plus *any* nontrivial element of $(\mathbf{Z}/3)^3$, then T contains a central element of S and cannot be an obstruction. Hence $\#T$ divides 9. It is easy to check that H has no elements of order 9, so T must be elementary abelian. It is clear that no elementary abelian subgroup of $S_6(2)$ of order 3 or 9 is an obstruction, hence T is a proper subgroup of H. □

Lemma 6. *The group H has even order.*

Proof. Otherwise, $\#H$ divides $3^4 \cdot 5$, so either has a normal 3-subgroup or 5-subgroup. Since H does not meet the conjugacy class $15A$ of $S_6(2)$, it must be the case that H is a 3-group or cyclic of order 5. By the preceding argument, H cannot be a 3-group, and by Lemma 1, H cannot be cyclic. □

Since T is elementary abelian of order dividing 9, its Jordan-Hölder factors have dimension either 1 or 2. Moreover, since T is not an obstruction it must be the case that T fixes a subspace of V of even dimension. This observation will be used in the following lemma.

Lemma 7. *If N is a normal solvable subgroup of H, then N is a 2-group.*

Proof. Suppose N is a minimal normal solvable subgroup of H which is not a 2-group. Then $N = O_2(N)P$, where P is an elementary abelian p-group. By the Frattini argument, $H = NN_H(P) = O_2(N)N_H(P)$. Since the Jordan-Hölder factors of $O_2(N)$ are all trivial, H and $N_H(P)$ have isomorphic factors, hence we can assume $H = N_H(P)$.

Since P is either cyclic of order 5, or an elementary abelian 3-group, it fixes a nondegenerate (hence even-dimensional) subspace of V. The normalizer stabilizes this decomposition, whence $V = A \perp B$ with A of dimension 2. Hence

$$H \leq \mathrm{Sp}_2(\mathbf{F}_2) \times \mathrm{Sp}_4(\mathbf{F}_2) \simeq S_3 \times S_6.$$

By Lemma 4, H is in fact a subgroup of $\mathbf{Z}/3 \times A_6$ and cannot be an obstruction due to the orthogonal decomposition of the representation. Indeed, if H is a direct-product subgroup of $\mathbf{Z}/3 \times A_6$, then it cannot be an obstruction since the fixed-points of H are composed of the fixed-points of the projections. Therefore, the projection Π of H onto A_6 must have $\mathbf{Z}/3$-quotient (Goursat's Lemma [2, p. 864]). An analysis of the subgroups Π of A_6 with this property reveals that no such H can be an obstruction. □

A similar argument shows that H must act irreducibly on V (this involves analyzing the stabilizers of both non-degenerate and totally singular decompositions of V). Therefore, $O_2(H)$ is trivial. Since $F(H)$ is the product of the $O_p(H)$, $p = 2, 3, 5$, it follows from the lemmas above that $F(H)$ is trivial also. Thus, the product of the minimal normal subgroups is a direct product of *simple* groups. A simple factor cannot have fixed-points, hence by minimality H must be simple.

Therefore, any obstruction H must be a simple subgroup of $\mathrm{S}_6(2)$ of index divisible by 7, possessing an elementary abelian subgroup of order dividing 9, and having an irreducible degree-6 $\mathbf{F}_2$-representation. One can check (via Magma or the Atlas [3]) that the only non-trivial, proper, simple subgroups of $\mathrm{S}_6(2)$ are A_5, $\mathrm{L}_2(7)$, A_6, $\mathrm{L}_2(8)$, A_7, $\mathrm{G}_2(2)'$, A_8, and $\mathrm{U}_4(2)$. Of these, only A_5, A_6, and $\mathrm{U}_4(2)$ have index divisible by 7 and possess an elementary abelian subgroup of order dividing 9. Out of these three groups, only $\mathrm{U}_4(2)$ has a six-dimensional, irreducible, $\mathbf{F}_2$-representation [6, p. 2, 4, 60]. The associated irreducible character takes on the value -3 on each of the classes $3A$ and $3B^{\star\star}$ [6, p. 60], hence $\mathrm{U}_4(2)$ meets the conjugacy class $3B$ of $\mathrm{S}_6(2)$. By the remark at the end of Section 2, $\mathrm{U}_4(2)$ is not a fixed-point subgroup. Therefore, $\mathrm{S}_6(2)$ contains no obstructions.

Acknowledgments

We would like to thank Serre for providing us with the counterexample in dimension 4 and helpful comments. We would also like to thank the referee for providing us with the proof in Appendix A, and Berger and Wong for useful discussions. Computations with Magma were performed at `http://magma.maths.usyd.edu.au/calc`.

References

[1] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, Cambridge, 2000. MR1777008 (2001c:20001)

[2] G. Butler and J. McKay. The transitive groups of degree up to eleven. *Comm. Algebra.* **11** (1983), 863-911 MR695893 (84f:20005)

[3] J. Conway *et al.*, *ATLAS of Finite Groups*, Oxford University Press, Cambridge, 1985. MR827219 (88g:20025)

[4] J. Cullinan. Local-global properties of torsion points on three-dimensional abelian varieties. *J. Algebra.* **311** (2007), 736-774. MR2314732 (2008b:14077)

[5] M. Hindry and J.H. Silverman, *Diophantine Geometry: An Introduction*, Springer-Verlag, New York, 2000. MR1745599 (2001e:11058)

[6] C. Jansen *et al.*, *An Atlas of Brauer Characters*, London Mathematical Society Monographs, Oxford University Press, New York, 1995. MR1367961 (96k:20016)

[7] N.M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.* **62** (1981), 481-502. MR604840 (82d:14025)

[8] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, 1990. MR1057341 (91g:20001)

[9] I.G. Macdonald, *Symmetric Functions and Hall Polynomials*, Clarendon Press, Oxford, 1979. MR553598 (84g:05003)
[10] J-P. Serre. Letter to J. Cullinan, 2006.

Department of Mathematics, Bard College, P.O. Box 5000, Annandale-on-Hudson, New York 12504
E-mail address: cullinan@bard.edu