Comment. Math. Helv. 78 (2003) 486–493
0010-2571/03/030486-8
DOI 10.1007/s00014-003-0768-7

Commentarii Mathematici Helvetici

The effective surjectivity of mod l Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring

Takashi Kawamura

Abstract. Mod l Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring are surjective for sufficiently large prime l as Serre proved. But he did not give an effective lower bound of l_0 such that they are surjective for $l > l_0$. We supply an effective evaluation of l_0 by an "elementary" proof of the surjectivity. The proof uses the Masser–Wüstholz theorem and Kleidman and Liebeck's classification of the maximal subgroups of $GL_2(\mathbf{F}_l)$ and $GSp_4(\mathbf{F}_l)$.

Mathematics Subject Classification (2000). Primary 11J89.

Keywords. Abelian variety, mod l Galois representation and effective surjectivity.

1. Introduction and main results

Let A be a principally polarized abelian variety of dimension n over an algebraic number field K. For a prime l let A_l be the group of l-division points of A, which is a vector space of dimension $2n$ over $\mathbf{F}_l$. Let μ_l be the group of l-th roots of unity in the algebraic closure $\bar{K}$ of K, and let $\varepsilon_l :\ G_K := \mathrm{Gal}(\bar{K}/K) \to \mathbf{F}_l{}^* \cong \mathrm{Aut}(\mu_l)$ be the cyclotomic character. As A is principally polarized, the Weil pairing $W :\ A_l \times A_l \to \mu_l$, written additively, defines a symplectic form with $2n$ variables, satisfying $W(\sigma(P),\ \sigma(Q)) = \varepsilon_l(\sigma)W(P,\ Q)$ for $(P,\ Q) \in A_l \times A_l$ and $\sigma \in G_K$. Hence a Galois representation $\rho_l :\ G_K \to GSp_{2n}(\mathbf{F}_l)$ is obtained, where $GSp_{2n}(\mathbf{F}_l)$ is the group of symplectic similitudes of dimension $2n$ with entries in $\mathbf{F}_l$.

Serre [11] proved that when $n = 2$, 6 or odd, and $\mathrm{End}_{\bar{K}}(A) = \mathbf{Z}$, ρ_l is surjective for sufficiently large l. The proof uses Faltings' theorem and standard theorems of algebraic groups. Though the result is general, it does not give an effective lower bound of l_0 such that ρ_l is surjective for $l > l_0$.

Masser and Wüstholz [5] give an effective estimate of l_0 when $n = 1$ using their isogeny estimates [4].

Le Duff [3] gives a sufficient condition for the surjectivity of ρ_l when $n = 2$ under some assumption on the reduction of abelian varieties. He also suggested that the explicit calculation of the constants in the refinement of Faltings' theorem by Masser and Wüstholz [8] should enable one to evaluate l_0 effectively. But no details are given.

The purpose of this paper is to supply an "elementary" proof of the surjectivity for $n = 1$ or 2, which also gives an effective evaluation of l_0. The proof uses the Masser–Wüstholz theorem [8] and Kleidman and Liebeck's [2] detailed results about the classification of the maximal subgroups of the finite classical groups, especially of $GSp_2(\mathbf{F}_l) \cong GL_2(\mathbf{F}_l)$ and $GSp_4(\mathbf{F}_l)$.

Let $D(K)$ be the discriminant of K, and let $h(A)$ be the Faltings height of A, which is invariant under field extensions.

Main Theorem 1. *Let $A = E$ be an elliptic curve over an algebraic number field K of degree d with $\mathrm{End}_{\bar{K}}(E) = \boldsymbol{Z}$. If $l > \max(|D(K)|,\ C(1)[\max\{48d,\ h(E)\}]^{\tau(1)})$, then $\rho_l(G_K) = GL_2(\boldsymbol{F}_l)$, where $C(1)$ is a constant $C(n)$ in Theorem 3 of Section 3 when $n = 1$, and $\tau(1)$ is the constant τ given in Theorem 1 of Masser and Wüstholz [8] when $n = 1$. Explicitly $\tau(1) = 2^{285} \cdot 3^4 \cdot 5^2 \cdot 136! \times (2^{276} \cdot 3^3 \cdot 5 \cdot 136! + 1)^7 + 2^{1073} \cdot 3 \cdot 17 \cdot 31^2 \cdot 41 \cdot 528! \times (2^{1061} \cdot 17 \cdot 31 \cdot 528! + 1)^{15} < 10^{25000}$.*

Main Theorem 2. *Let A be a two-dimensional principally polarized abelian variety over an algebraic number field K of degree d with $\mathrm{End}_{\bar{K}}(A) = \boldsymbol{Z}$. If $l > \max(|D(K)|,\ C(2)[\max\{3840d,\ h(A)\}]^{\tau(2)})$, then $\rho_l(G_K) = GSp_4(\boldsymbol{F}_l)$, where $C(2)$ is a constant $C(n)$ in Theorem 3 of Section 3 when $n = 2$, and $\tau(2)$ is the constant τ given in Theorem 1 of Masser and Wüstholz [8] when $n = 2$. Explicitly $\tau(2) = 2^{1074} \cdot 17 \cdot 31^2 \cdot 528! \times (2^{1061} \cdot 17 \cdot 31 \cdot 528! + 1)^{15} + 2^{4183} \cdot 3^6 \cdot 7^3 \cdot 11 \cdot 23 \cdot 2080! \times (2^{4166} \cdot 3^3 \cdot 7 \cdot 11 \cdot 2080! + 1)^{31} < 10^{240000}$.*

2. Enumeration of maximal subgroups of $GSp_4(\mathbf{F}_l)$

We enumerate maximal subgroups of $GSp_4(\mathbf{F}_l)$ in this section.

Classically, Mitchell determined the maximal subgroups of $Sp_4(\mathbf{F}_l)$ whose orders are prime to l [9], and then all the maximal subgroups of $Sp_4(\mathbf{F}_l)$ [10]. But he gave only their orders and geometric properties, and did not give their structure.

More recently, Aschbacher [1] obtained the classification theorem of the maximal subgroups of the finite classical groups as follows.

Theorem 1. *Let G be a finite almost simple classical group over a finite field F with its socle G_0, and let H be a subgroup of G not containing G_0. Then either H is contained in a member of $C(G) = \cup_{i=1}^{8} C_i(G)$ or $H \in S(G)$, where $C_i(G)$ is the collection of subgroups of G which stabilize something and $S(G)$ is that satisfying the irreducibility conditions. $C_1(G)$ are the stabilizers of totally singular* *or non-singular subspaces of V, which is the vector space over F associated with G. $C_2(G)$ are the stabilizers of direct sum decomposition of V into subspaces of the same dimension. $C_3(G)$ are the stabilizers of extension fields of F. $C_4(G)$ are the stabilizers of tensor product decompositions of V into two subspaces. $C_5(G)$ are the stabilizers of subfields of F. $C_6(G)$ are the normalizers of symplectic-type r-groups in absolutely irreducible representations. $C_7(G)$ are the stabilizers of tensor product decompositions of V into multiple subspaces of the same dimension. $C_8(G)$ are classical subgroups. The subgroup H of G lies in $S(G)$ if and only if the following hold.*

(a) *The socle S of H is a non-abelian simple group.*

(b) *If L is the full covering group of S, and if $\rho: L \longrightarrow GL(V)$ is a representation of L such that $\rho(L) \equiv S$ (mod scalars), then ρ is absolutely irreducible.*

(c) *$\rho(L)$ can not be realized over a proper subfield of F.*

(d) *If $\rho(L)$ fixes a non-degenerate quadratic form on V, then $G_0 = P\Omega_n(F)$.*

(e) *If $\rho(L)$ fixes a non-degenerate symplectic form on V, but no non-degenerate quadratic form, then $G_0 = PSp_n(F)$.*

(f) *If $\rho(L)$ fixes a non-degenerate unitary form on V, then $G_0 = PSU_n(F)$.*

(g) *If $\rho(L)$ does not satisfy the conditions in* (d), (e) *or* (f), *then $G_0 = PSL_n(F)$.*

Kleidman and Liebeck [2, p. 57, Main Theorem] decided the structure of the members of $C(G)$, their maximality conditions, and their overgroups in $C(G) \cup S(G)$.

By applying Theorem 1 and [2, Main Theorem] to $GL_2(\mathbf{F}_l)$ and $GSp_4(\mathbf{F}_l)$, we enumerate their maximal subgroups.

Proposition 1. *When $l \geq 5$, a maximal subgroup of $GL_2(\boldsymbol{F}_l)$ is conjugate to one of the following five subgroups.*

(1) *$SL_2(\boldsymbol{F}_l) \rtimes$ (maximal subgroup of $\langle\delta_1\rangle$),*

(2) *Borel subgroup,*

(3) *normalizer of the split Cartan subgroup $\cong (\boldsymbol{F}_l{}^* \times \boldsymbol{F}_l{}^*) \rtimes S_2$,*

(4) *normalizer of the nonsplit Cartan subgroup $\cong \boldsymbol{F}_{l^2}{}^* \bullet \boldsymbol{Z}_2$, and*

(5) *$Q_8 \bullet D_6 \rtimes \langle\delta_1\rangle \cong GL_2(\boldsymbol{F}_3) \rtimes \langle\delta_1\rangle$,*

where δ_1 is the element expressed as $\mathrm{diag}(\mu,\ 1)$ *with respect to a basis of $\boldsymbol{F}_l{}^2$, μ being a generator of $\boldsymbol{F}_l{}^*$. For groups G and H, $G \bullet H$ denotes the extension of G by H. $\boldsymbol{Z}_2$ is the cyclic group of order 2, Q_8 is the quaternion group, and D_n is the dihedral group of order n.*

Proposition 2. *When $l \geq 3$, a maximal subgroup of $GSp_4(\boldsymbol{F}_l)$ is conjugate to one of the following seven subgroups.*

(1) *$Sp_4(\boldsymbol{F}_l) \rtimes$ (maximal subgroup of $\langle\delta_2\rangle$),*

(2) *maximal parabolic subgroup,*

(3) *$(SL_2(\boldsymbol{F}_l) \times SL_2(\boldsymbol{F}_l)) \rtimes S_2 \rtimes \langle\delta_2\rangle$,*

(4) *$GL_2(\boldsymbol{F}_l) \bullet \boldsymbol{Z}_2 \rtimes \langle\delta_2\rangle$,*

(5) $SL_2(\boldsymbol{F}_{l^2}) \rtimes \langle\delta_2\rangle$,
(6) $GU_2(\boldsymbol{F}_{l^2}) \rtimes \langle\delta_2\rangle$, *and*
(7) $D_8 \circ Q_8 \bullet O_4^{-}(\boldsymbol{F}_2) \rtimes \langle\delta_2\rangle$,

where δ_2 *is the element expressed as* $diag(\mu,\ \mu,\ 1,\ 1)$ *with respect to a symplectic basis of* $\boldsymbol{F}_l{}^4$. $\circ$ *denotes the central product, and* $O_4{}^{-}$ *is the* 4*-dimensional orthogonal group with Witt defect* 1.

Proof. Proposition 1 is well-known, so we prove only Proposition 2. The socle G_0 of $G = GSp_4(\mathbf{F}_l)$ is $Sp_4(\mathbf{F}_l)$. Therefore the maximal subgroup containing G_0 is given by (1). If $G_0 \not\subset H$, then $G_0 \cap H$ is contained in a subgroup on the table [2, p. 72, Table 3.5.C] of Kleidman and Liebeck.

By applying Theorem 1 and [2, Main Theorem] to $Sp_4(\mathbf{F}_l)$, we see from [2, Table 3.5.C] that the set $S(Sp_4(\mathbf{F}_l))$ is empty, and $C_i(Sp_4(\mathbf{F}_l))$ ($i = 4,\ 5,\ 7,\ 8$) are also empty. The same table shows that a maximal subgroup of $Sp_4(\mathbf{F}_l)$ is conjugate to a maximal parabolic subgroup in $C_1(Sp_4(\mathbf{F}_l))$, $(SL_2(\mathbf{F}_l)\times SL_2(\mathbf{F}_l))\rtimes S_2$ and $GL_2(\mathbf{F}_l)\bullet \mathbf{Z}_2$ in $C_2(Sp_4(\mathbf{F}_l))$, $SL_2(\mathbf{F}_{l^2})$ and $GU_2(\mathbf{F}_{l^2})$ in $C_3(Sp_4(\mathbf{F}_l))$, or $D_8 \circ Q_8 \bullet O_4{}^{-}(\mathbf{F}_2)$ in $C_6(Sp_4(\mathbf{F}_l))$.

Next by applying Theorem 1 and [2, Main Theorem] to $GSp_4(\mathbf{F}_l)$, we find that a maximal subgroup of $GSp_4(\mathbf{F}_l)$ other than (1) is conjugate to a maximal parabolic subgroup of $GSp_4(\mathbf{F}_l)$ or (a maximal subgroup of $Sp_4(\mathbf{F}_l)$) $\rtimes \langle\delta_2\rangle$, that is, (3), (4), (5), (6) and (7). $\square$

Remark. Explicit realization of these subgroups in $GSp_4(\mathbf{F}_l) = \{g^tJg = \varepsilon_l(g)J \mid g \in GL_4(\mathbf{F}_l),\ \varepsilon_l(g) \in \mathbf{F}_l{}^*\}$ is as follows. Here

$$J = \begin{pmatrix} O_2 & -E_2 \\ E_2 & O_2 \end{pmatrix},$$

where O_2 is the 2×2 zero matrix and E_2 is the 2×2 identity matrix.

(3)
$$\left\{\begin{pmatrix} A & O_2 \\ O_2 & B \end{pmatrix} \middle| A,\ B \in SL_2(\mathbf{F}_l)\right\} \rtimes \left\langle \begin{pmatrix} O_2 & E_2 \\ E_2 & O_2 \end{pmatrix} \right\rangle \rtimes \langle\delta_2\rangle.$$

(4)
$$\left\{\begin{pmatrix} A & O_2 \\ O_2 & (A^t)^{-1} \end{pmatrix} \middle| A \in GL_2(\mathbf{F}_l)\right\} \bullet \left\langle \begin{pmatrix} O_2 & E_2 \\ E_2 & O_2 \end{pmatrix} \right\rangle \rtimes \langle\delta_2\rangle.$$

(5)
$$\left\{\begin{pmatrix} a_1 & a_2 & b_1 & b_2\lambda^2 \\ a_2\lambda^2 & a_1 & b_2\lambda^2 & b_1\lambda^2 \\ c_1 & c_2 & d_1 & d_2\lambda^2 \\ c_2 & c_1\lambda^{-2} & d_2 & d_1 \end{pmatrix}\right\} \rtimes \langle\delta_2\rangle,$$

where a_i, b_i, c_i and $d_i \in \mathbf{F}_l$ for $i = 1$ and 2 such that $(a_1 + a_2\lambda)(d_1 + d_2\lambda) - (b_1 + b_2\lambda)(c_1 + c_2\lambda) = 1$, and $\lambda \in \mathbf{F}_{l^2}{}^*$ such that $\lambda + \lambda^l = 0$.

(6)

$$\left\{\begin{pmatrix} A & B \\ \lambda^2 B & A \end{pmatrix}\right\} \rtimes \langle \delta_2 \rangle,$$

where A and $B \in M_2(\mathbf{F}_l)$, $A^tA - \lambda^2 B^tB = E_2$ and $A^tB - B^tA = O_2$.

(7)

$$\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \otimes \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \right\rangle \bullet O_4{}^{-}(\mathbf{F}_2) \rtimes \langle \delta_2 \rangle,$$

where a and b in $\mathbf{F}_l$ are chosen such that $a^2+b^2 = -1$, and $\otimes$ denotes the Kronecker product.

Remark. The necessary properties of the subgroups are as follows.

(a) It stabilizes a positive-dimensional subspace of $V_n := \mathbf{F}_l{}^{2n}$.

(b) It has a subgroup satisfying (a) whose index is bounded independently of l.

(c) Its commutant is larger than $\mathbf{F}_l$.

(d) It has a subgroup satisfying (c) whose index is bounded independently of l.

(2) satisfies (a), (3) and (4) satisfy (b), (5) and (6) satisfy (c), and (7) satisfies (d).

3. Proof of Main Theorems

Masser and Wüstholz [7, Theorem II] (see also the note at the end of [7]) estimated the degree of an isogeny between abelian varieties over a number field effectively.

Theorem 2. *Given positive integers n and d, there are constants $\kappa(n)$ and $C(n)$ depending only on n with the following property. Let A and A' be abelian varieties of dimension n defined over a number field K of degree d. Then if they are isogenous over K, there is an isogeny over K from A to A' of degree at most $C(n)[\max\{d,\ h(A)\}]^{\kappa(n)}$.*

Using Theorem 2, they [8, Theorem 1] (see also the note at the end of [8]) refined Faltings' theorem in the following effective way.

Theorem 3. *Given positive integers n and d, there are constants $\tau(n)$ and $C(n)$ depending only on n with the following property. Let A be an abelian variety of dimension n defined over a number field K of degree d. Then there is a positive integer $M \leq C(n)[\max\{d,\ h(A)\}]^{\tau(n)}$ such that for any prime l the natural map $\mathrm{End}_K(A) \to \mathrm{End}_{G_K}(A_l)$ has cokernel killed by M.*

Corollary. *Suppose M as in Theorem 3. Then for any prime l not dividing M the natural map $\mathrm{End}_K(A) \otimes_{\mathbf{Z}} \mathbf{F}_l \to \mathrm{End}_{G_K}(A_l)$ is an isomorphism.*

Explicitly $\tau(n) = n^2\{\lambda(8n) + 3\kappa(2n)\}$ *by* [8, *Section 6*], *where*

$$\lambda(n) = 16n^3(2n-1)k(n)\{2nk(n)+1\}^{n-1}$$

by [6, *Section 5*], $k(n)$ *being* $(2n^2+n-1)4^{n(2n+1)}\{n(2n+1)\}!$, *and* $\kappa(n) = 10n^3\lambda(8n) + 32n^2\mu(8n)$ *by* [7, *Section 7*], $\mu(n)$ *being* $\lambda(n)/(4n)$ *by* [6, *Section 6*].

Let ζ_l be a primitive l-th root of unity. If $K \cap \mathbf{Q}(\zeta_l) = \mathbf{Q}$, then ε_l is surjective. The condition on l is given by the following Lemma.

Lemma. *If* $l > |D(K)|$, *then* $K \cap \boldsymbol{Q}(\zeta_l) = \boldsymbol{Q}$.

Proof. The discriminant of $\mathbf{Q}(\zeta_l)$, $D(\mathbf{Q}(\zeta_l))$, is l^{l-2} when $l = 2$ or $\equiv 1 \pmod 4$, and $-l^{l-2}$ when $l \equiv 3 \pmod 4$. The discriminant of $K \cap \mathbf{Q}(\zeta_l)$ divides the greatest common divisor of $D(K)$ and $D(\mathbf{Q}(\zeta_l))$, which is 1 if $l > |D(K)|$. By Minkowski's theorem $K \cap \mathbf{Q}(\zeta_l) = \mathbf{Q}$. □

Proof of Main Theorem 1. We prove that $G_l := \rho_l(G_K)$ is not contained in any maximal subgroups of $GL_2(\mathbf{F}_l)$ in Proposition 1.

As $l > |D(K)|$, ε_l is surjective by Lemma, so that

$$G_l \not\subset SL_2(\mathbf{F}_l) \rtimes (\text{maximal subgroup of } \langle\delta_1\rangle).$$

The Borel subgroup stabilizes a one-dimensional subspace W of V_1. If G_l is contained in it, then there is a K-isogeny $f : E/W \to E/V_1 \cong E$ the degree of which is l. By Theorem 2 there is a K-isogeny $g : E \to E/W$ the degree of which, say d_0, is at most $C(1)[\max\{d, h(E)\}]^{\kappa(1)}$. The degree of the composition K-isogeny $g \circ f$ is $d_0 l$. On the other hand, as $\mathrm{End}_{\bar{K}}(E) = \mathbf{Z}$, $\mathrm{End}_K(E/W) = \mathbf{Z}$. Thus $d_0 l$ is the square of an integer, say m. So l divides m, and l divides d_0, contradicting the inequality $l > d_0$.

Next if $G_l \subset (\mathbf{F}_l{}^* \times \mathbf{F}_l{}^*) \rtimes S_2$, then there exists a homomorphism φ_1 from G_l to S_2. Let L_1 be $\bar{K}^{\ker(\varphi_1 \circ \rho_l)}$, then $[L_1 : K] \leq 2$, and $\rho_l(G_{L_1} := \mathrm{Gal}(\bar{K}/L_1)) \subset \mathbf{F}_l{}^* \rtimes \langle\delta_1\rangle$. Thus $\mathrm{End}_{G_{L_1}}(E_l) \supset \mathbf{F}_l{}^2$. On the other hand, as $l > C(1)[\max\{2d, h(E)\}]^{\tau(1)}$, $\mathrm{End}_{G_{L_1}}(E_l) \cong \mathrm{End}_{L_1}(E) \otimes_{\mathbf{Z}} \mathbf{F}_l \cong \mathbf{F}_l$ by Corollary. This is a contradiction.

If $G_l \subset \mathbf{F}_{l^2}{}^* \bullet \mathbf{Z}_2$, then there exists a quadratic extension L_2 of K such that $\rho_l(G_{L_2} := \mathrm{Gal}(\bar{K}/L_2)) \subset \mathbf{F}_{l^2}{}^*$. Thus $\mathrm{End}_{G_{L_2}}(E_l) \supset \mathbf{F}_{l^2}$. On the other hand, as $l > C(1)[\max\{2d, h(E)\}]^{\tau(1)}$, $\mathrm{End}_{G_{L_2}}(E_l) \cong \mathrm{End}_{L_2}(E) \otimes_{\mathbf{Z}} \mathbf{F}_l \cong \mathbf{F}_l$ by Corollary. Hence a contradiction.

Lastly assume that $G_l \subset GL_2(\mathbf{F}_3) \rtimes \langle\delta_1\rangle$. As ε_l is surjective by Lemma, $G_l \supset \langle\delta_1\rangle$. Let L_3 be $\bar{K}^{(\rho_l)^{-1}(\langle\delta_1\rangle)}$, then $[L_3 : K] \leq |GL_2(\mathbf{F}_3)| = 48$, and $\rho_l(G_{L_3} := \mathrm{Gal}(\bar{K}/L_3)) = \langle\delta_1\rangle$. Thus $\mathrm{End}_{G_{L_3}}(E_l) \supset \mathbf{F}_l{}^4$. On the other hand, as $l > C(1)[\max\{48d,\ h(E)\}]^{\tau(1)}$, $\mathrm{End}_{G_{L_3}}(E_l) \cong \mathrm{End}_{L_3}(E) \otimes_{\mathbf{Z}} \mathbf{F}_l \cong \mathbf{F}_l$ by Corollary. This is a contradiction.

Proof of Main Theorem 2. We prove that G_l is not contained in any maximal subgroups of $GSp_4(\mathbf{F}_l)$ in Proposition 2.

$G_l \not\subset Sp_4(\mathbf{F}_l) \rtimes$ (maximal subgroup of $\langle\delta_2\rangle$), for ε_l is surjective.

Maximal parabolic subgroups stabilize a one- or two-dimensional subspace of V_2. So G_l is not contained in them similarly as the case of the Borel subgroup in Main Theorem 1.

Next if $G_l \subset (SL_2(\mathbf{F}_l)\times SL_2(\mathbf{F}_l))\rtimes S_2 \rtimes \langle\delta_2\rangle$, then there exists a homomorphism φ_2 from G_l to S_2. Let L_4 be $\bar{K}^{\ker(\varphi_2\circ\rho_l)}$, then $[L_4 : K] \leq 2$, and $\rho_l(G_{L_4} := \mathrm{Gal}(\bar{K}/L_4)) \subset (SL_2(\mathbf{F}_l)\times SL_2(\mathbf{F}_l))\rtimes\langle\delta_2\rangle$. As $(SL_2(\mathbf{F}_l)\times SL_2(\mathbf{F}_l))\rtimes\langle\delta_2\rangle$ stabilizes two-dimensional subspaces of V_2, a contradiction arises similarly as the case of the Borel subgroup in Main Theorem 1.

$G_l \not\subset GL_2(\mathbf{F}_l)\bullet\mathbf{Z}_2\rtimes\langle\delta_2\rangle$ similarly as the case of $(SL_2(\mathbf{F}_l)\times SL_2(\mathbf{F}_l))\rtimes S_2\rtimes\langle\delta_2\rangle$, for $GL_2(\mathbf{F}_l)\rtimes\langle\delta_2\rangle$ stabilizes two-dimensional subspaces of V_2.

If $G_l \subset SL_2(\mathbf{F}_{l^2})\rtimes\langle\delta_2\rangle$ or $G_l \subset GU_2(\mathbf{F}_{l^2})\rtimes\langle\delta_2\rangle$, then G_l commutes with $\mathbf{F}_{l^2}$. On the other hand, as $l > C(2)[\max\{d, h(A)\}]^{\tau(2)}$, $\mathrm{End}_{G_K}(A_l) \cong \mathrm{End}_K(A)\otimes_{\mathbf{Z}}\mathbf{F}_l \cong \mathbf{F}_l$ by Corollary. Hence a contradiction.

$G_l \not\subset D_8\circ Q_8\bullet O_4{}^-(\mathbf{F}_2)\rtimes\langle\delta_2\rangle$ similarly as the case of $GL_2(\mathbf{F}_3)\rtimes\langle\delta_1\rangle$ in Main Theorem 1, for $|D_8\circ Q_8\bullet O_4{}^-(\mathbf{F}_2)| = 3840$.

Remarks. (a) The effective dependence of $C(n)$ on the dimension n remains an interesting problem [7].

(b) When $\dim A = 3$, the classification of maximal subgroups of $GSp_6(\mathbf{F}_l)$ is also known ([1] and [2, pp. 57 and 72]). When $l \geq 5$, they are

(1) $Sp_6(\mathbf{F}_l)\rtimes$ (maximal subgroup of $\langle\delta_3\rangle$),
(2) maximal parabolic subgroup,
(3) $SL_2(\mathbf{F}_l)\times Sp_4(\mathbf{F}_l)\rtimes\langle\delta_3\rangle$,
(4) $(SL_2(\mathbf{F}_l)\times SL_2(\mathbf{F}_l)\times SL_2(\mathbf{F}_l))\rtimes S_3\rtimes\langle\delta_3\rangle$,
(5) $GL_3(\mathbf{F}_l)\bullet\mathbf{Z}_2\rtimes\langle\delta_3\rangle$,
(6) $SL_2(\mathbf{F}_{l^3})\rtimes\langle\delta_3\rangle$,
(7) $GU_3(\mathbf{F}_{l^2})\rtimes\langle\delta_3\rangle$, and
(8) $SL_2(\mathbf{F}_l)\circ O_3(\mathbf{F}_l)\rtimes\langle\delta_3\rangle$,

where δ_3 is the element expressed as $\mathrm{diag}(\mu,\mu,\mu,1,1,1)$ with respect to a symplectic basis of $\mathbf{F}_l{}^6$. Explicit realization of the subgroups are similar to the two-dimensional case. (2) and (3) satisfy the property (a) of the remark after Proposition 2, (4) and (5) satisfy (b), and (6) and (7) satisfy (c), so the first seven are handled similarly as the 2-dimensional case. Only the case (8) seems to be difficult to treat.

Acknowledgements. The author is most grateful to Professor Takayuki Oda for helpful advice. He thanks Professor Jean-Pierre Serre and Professor David W. Masser for valuable comments. He is indebted to Professor Akio Tamagawa for pointing out problems in the draft. He is grateful also to Dr. Fumio Sairaiji for reference to the paper [3]. Lastly he thanks the referees for suggesting many improvements.

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514.
[2] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series **129**, Cambridge Univ. Press, 1990.
[3] P. Le Duff, Points d'ordre l des jacobiennes de certaines courbes de genre 2, *C. R. Acad. Sci. Paris* **325**, Série I (1997), 243–246.
[4] D. W. Masser and G. Wüstholz, Isogeny estimates for abelian varieties, and finiteness theorems, *Ann. Math.* **137** (1993), 459–472.
[5] D. W. Masser and G. Wüstholz, Galois properties of division fields of elliptic curves, *Bull. London Math. Soc.* **25** (1993), 247–257.
[6] D. W. Masser and G. Wüstholz, Endomorphism estimates for abelian varieties, *Math. Z.* **215** (1994), 641–653.
[7] D. W. Masser and G. Wüstholz, Factorization estimates for abelian varieties, *Publ. Math. IHES* **82** (1995), 5–24.
[8] D. W. Masser and G. Wüstholz, Refinements of the Tate conjecture for abelian varieties, in: *Abelian Varieties* (W. Barth, K. Hulek and H. Lange, Eds.), Walter de Gruyter, 1995, 211–223.
[9] H. H. Mitchell, Determination of the finite quaternary linear groups, *Trans. Amer. Math. Soc.* **14** (1913), 123–142.
[10] H. H. Mitchell, The subgroups of the quaternary abelian linear groups, *Trans. Amer. Math. Soc.* **15** (1914), 379–396.
[11] J.-P. Serre, Résumés des cours au Collège de France, *Ann. Coll. France* (1985–86), 95–99.

Takashi Kawamura
University of Tokyo
Graduate School of Mathematical Sciences
3-8-1 Komaba Meguro-ku
Tokyo 153-8914
Japan
e-mail: nn39302@mail.ecc.u-tokyo.ac.jp

(Received: November 2, 2001)