Galois Properties of Division Fields of Elliptic Curves

GALOIS PROPERTIES OF DIVISION FIELDS OF ELLIPTIC CURVES

D. W. MASSER AND G. WÜSTHOLZ

1. *Introduction*

Let k be a number field, let $\bar{k}$ be an algebraic closure, and write $G = \mathrm{Gal}(\bar{k}/k)$ for the relative Galois group. If E is an elliptic curve defined over k, then G acts on the group $E(\bar{k})$ of points of E defined over $\bar{k}$. In particular, for any positive integer n it acts on the group E_n of points of E with finite order dividing n. From now on, suppose $n = l$ is prime. We can regard E_l as a vector space (of dimension 2) over the finite field $\mathbb{F}_l$ with l elements, and so there is a natural homomorphism ϕ_l from G to the corresponding general linear group $\mathrm{GL}(E_l)$. A fundamental result of Serre ([**16**, **17**]) says that if E has no complex multiplication over $\bar{k}$, then $\phi_l(G) = \mathrm{GL}(E_l)$ for all sufficiently large l. In other words, there exists l_0, depending only on k and E, such that $\phi_l(G) = \mathrm{GL}(E_l)$ for all $l > l_0$.

Up to now it seems that no general estimate for l_0 has been written down. Serre gives a number of results for special classes of elliptic curves. For example, Corollaire 1 of [**17**, p. 308] yields a simple estimate when $k = \mathbb{Q}$ and E is semistable. In his later paper [**18**] he was able to eliminate the semistability condition by assuming the Generalized Riemann Hypothesis (see Théorème 22 and Lemme 15, p. 196). But in a talk at the D.-P.-P. Séminaire in April 1988, he did announce an effective estimate in the general case.

In this note we give a general upper bound for l_0. As Serre himself pointed out during a conference at Schloss Ringberg in July 1988, such a result is a relatively simple deduction from some isogeny estimates proved by us. Indeed, our exposition in Sections 3 and 4 follows closely a talk he gave there on this subject. After recording the necessary isogeny estimates in Section 2, we apply these in Section 3 to rule out some particular possibilities for $\phi_l(G)$. Then in Section 4 we prove our main result by appealing to the group-theoretical analysis of [**17**].

We also prove two further results of a similar type. In Section 5 we generalize to several elliptic curves, and in Section 6 we consider the corresponding problem for several points of infinite order on a single elliptic curve.

To state our main result we define the Weil height of the elliptic curve E as the (absolute logarithmic) Weil height of its j-invariant.

THEOREM. *There are absolute constants c, γ with the following properties. Suppose E is an elliptic curve of Weil height h defined over a number field k of degree d, and assume E has no complex multiplication over $\bar{k}$.*

(a) *If $l > c(\max\{d, h\})^{\gamma}$, then $\phi_l(G)$ contains the special linear group $\mathrm{SL}(E_l)$.*

(b) *If, further, l does not divide the discriminant of k, then $\phi_l(G) = \mathrm{GL}(E_l)$.*

Received 21 January 1992.

1991 *Mathematics Subject Classification* 11G05.

Our exponent γ is completely effective, but rather large at the moment. There is little doubt that it could be substantially reduced without any new ideas. It is rather more difficult to estimate the constant c, and it would be an interesting project to attempt.

Generally, throughout this paper we use $c, c_1, c_2, \ldots$ (but not $C, C_1, C_2, \ldots$) for sufficiently large positive absolute constants.

It is a pleasure to thank Serre for valuable correspondence on these topics. The first author was supported in part by the National Science Foundation, and the paper was written while he was enjoying the hospitality of the University of Konstanz and supported by the Alexander von Humboldt Foundation.

2. *Isogeny estimates*

The following result is a preliminary version of what we shall need. For an abelian variety A defined over a number field k, we denote by $h(A)$ the (absolute logarithmic) Faltings height of A, obtained by passing to any field extension over which A has semistable reduction (see, for example, p. 248 of Chai's article in [**4**]). For an elliptic curve E, this is known to have the same order of magnitude as the Weil height h (see, for example, Proposition 2.1 on p. 258 of Silverman's article in [**4**]). In particular, $h(E) \leqslant c \max\{1, h\}$ and so it suffices to prove our Theorem for the Faltings height in place of the Weil height.

LEMMA 2.1. *Given a positive integer n, there are constants C_1, λ_1, depending only on n, with the following property. Suppose that A, A^* are abelian varieties of dimension n defined over a number field k of degree d, and that they are isogenous over $\bar{k}$. Assume further that A, A^* are principally polarized. Then there is an isogeny from A^* to A, defined over $\bar{k}$, of degree at most $C_1(\max\{d, h(A)\})^{\lambda_1}$.*

Proof. In the Theorem of [**13**] we proved a result of this kind with C_1 depending on d as well as on n; but in Section 6 of the paper we computed the dependence on d. From the formulae given there, in particular equation (6.2), the present lemma follows at once.

Note that for elliptic curves, a result of this form, with C_1 depending also on d, was proved in [**11**] with $\lambda_1 = 4$. So small exponents can be achieved in this game. The result was then used in [**10**] to give some effective estimates like our Theorem when the j-invariant of E is not an algebraic integer.

In fact, we shall need a modified version of Lemma 2.1 in which the polarization hypothesis on A^* is removed at the expense of an extra condition on A.

LEMMA 2.2. *Given a positive integer n, there are constants C, λ, depending only on n, with the following property. Suppose that A, A^* are abelian varieties of dimension n defined over a number field k of degree d, and that they are isogenous over $\bar{k}$. Assume further that A is principally polarized and factorizes as $A_1^{e_1} \times \ldots \times A_r^{e_r}$, where $e_1, \ldots, e_r$ are positive integers and $A_1, \ldots, A_r$ are abelian varieties, pairwise non-isogenous over $\bar{k}$, with trivial endomorphism rings over $\bar{k}$. Then there is an isogeny from A^* to A, defined over $\bar{k}$, of degree at most $C(\max\{d, h(A)\})^{\lambda}$.*

Proof. We define $Z = (A \times \hat{A})^4$, where $\hat{A}$ is the dual of A, and we define Z^* analogously for A^*. Then Z, Z^* are defined over k and isogenous over $\bar{k}$. Moreover, since A is principally polarized, Z is isomorphic over $\bar{k}$ to A^8; and a well-known observation of Zarhin (see, for example, [**19**, p. 314]) shows that Z^* is principally polarized. Therefore by Lemma 2.1 there is an isogeny from Z^* to A^8 of degree $b \leqslant C_2(\max\{d, h(A^8)\})^\lambda$, where C_2 and λ are the values of C_1 and λ_1 with n replaced by $8n$. Choose any embedding of A^* into Z^*, and compose this with the above isogeny to obtain a homomorphism ε from A^* to A^8. This is surjective onto its image $B = \varepsilon(A^*)$, and it is easy to see that ε is an isogeny from A^* to B of degree at most b.

Thus B is an abelian subvariety of A^8 which is isogenous to A (that is, it is 'stably isogenous' to A in the sense of [**19**]). Now it follows from our factorization assumptions about A that in fact B must be isomorphic to A. One way of seeing this is to use the concept of 'disjointness' introduced in [**9**, p. 235]. Each of $A_1, \ldots, A_r$ is simple, and any two are non-isogenous, so by Lemma 7(i) of [**9**, p. 262], any two are disjoint. It follows from Lemma 7(iii) that $A_1, \ldots, A_r$ are disjoint. Hence, by repeated use of Lemma 7(ii), we see that the factors $A_1^{8e_1}, \ldots, A_r^{8e_r}$ of A^8 are also disjoint. In other words, B in A^8 must factorize as $B_1 \times \ldots \times B_r$ for B_i in $A_i^{8e_i}$ $(1 \leqslant i \leqslant r)$. But since A_i has trivial endomorphism ring, B_i must be isomorphic to some power $A_i^{f_i}$ $(1 \leqslant i \leqslant r)$. Now 'uniqueness of factorization up to isogeny' shows that $f_i = e_i$ $(1 \leqslant i \leqslant r)$; hence the desired conclusion.

So we end up with our required isogeny from A^* to A; and because $h(A^8) = 8h(A)$, its degree satisfies the required bound with $C = 8^\lambda C_2$. This proves the lemma.

3. *Isogeny arguments*

Throughout this and the next section we let E be an elliptic curve of Faltings height h defined over a number field k of degree d, with no complex multiplication over $\bar{k}$; and for a prime l we define E_l and ϕ_l as in Section 1. We write, for brevity,

$$M = \max\{d, h\},$$

and we denote by $\lambda = \lambda(n)$ the exponent in Lemma 2.2.

LEMMA 3.1. *Suppose $l > c_1 M^{\lambda(1)}$. Then $\phi_l(G)$ does not fix any one-dimensional subspace of E_l.*

Proof. This is in [**10**], but for completeness we reproduce the argument. Suppose, to the contrary, that $\phi_l(G)$ fixes some one-dimensional subspace Γ of E_l. Then Γ is defined over k. So the abelian varieties $A = E$ and $A^* = E/\Gamma$ are defined over k and isogenous over k. Hence by Lemma 2.2 (or Lemma 2.1) there is an isogeny from E/Γ to E of degree $b \leqslant c_1 M^{\lambda(1)}$. Composing this with the natural isogeny from E to E/Γ of degree l, we end up with an endomorphism of E, which by hypothesis must be multiplication by some integer p. Comparing degrees, we obtain $p^2 = bl$. So l divides p, and therefore l must also divide b. In particular, $l \leqslant b$. This is a contradiction, and the lemma is proved.

The next result uses a two-dimensional version of the same argument.

LEMMA 3.2. *Suppose $l > c_2 M^{\lambda(2)/2}$. Then if $\phi_l(G)$ is commutative, it is contained in the group $\mathbb{F}_l^*$ of scalars in* $\mathrm{GL}(E_l)$.

Proof. Suppose, to the contrary, that $\phi_l(G)$ is commutative but not contained in $\mathbb{F}_l^*$. Choose any f in $\phi_l(G)$ not in $\mathbb{F}_l^*$, and define Γ in $E \times E$ as the group of elements (x, fx) as x runs over E_l. Then Γ is defined over k, since an arbitrary g in G acts on (x, fx) to give $(\phi_l(g)x, \phi_l(g)fx)$, which is (y, fy) for $y = \phi_l(g)x$ by commutativity. Hence $A = E \times E$ and $A^* = A/\Gamma$ are both defined over k and isogenous over k.

We can now apply Lemma 2.2 to obtain an isogeny of degree $b \leqslant c_3 M^{\lambda(2)}$ from A^* to A; note that $h(A) = 2h$. Composing this with the natural isogeny from A to A/Γ of degree l^2, we obtain an endomorphism ε of A. This can be represented by an integral matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ acting on elements (x, x') of $E \times E$. Since it annihilates Γ, we obtain

$$px + rfx = qx + sfx = 0$$

for all x in E_l. On the other hand, since f is not in $\mathbb{F}_l^*$ there is no integer a such that $fx = ax$, and we deduce easily that p, q, r, s are all divisible by l. So l^4 divides the degree $(ps - qr)^2$ of ε. But this is bl^2; hence l^2 divides b and $l \leqslant b^{1/2}$. This contradiction completes the proof of the lemma.

4. *Group theory*

We can now prove part (a) of our Theorem. Suppose first that l divides the order of $\phi_l(G)$. By Proposition 15 (p. 280) of [17], either $\phi_l(G)$ contains $\mathrm{SL}(E_l)$ as desired, or $\phi_l(G)$ is contained in a Borel subgroup. By definition, the latter fixes some one-dimensional subspace of E_l, so we can use Lemma 3.1 to eliminate this possibility if

$$l > c_1 M^{\lambda(1)}. \tag{4.1}$$

So henceforth we may assume that l does not divide the order of $\phi_l(G)$. Let H be the image of $\phi_l(G)$ under the canonical map from $\mathrm{GL}(E_l)$ to the projective group $\mathrm{PGL}(E_l)$. By Section 2.6 (p. 282) of [17] we have the following three possibilities:

(i) $\phi_l(G)$ is contained in a Cartan subgroup C;

(ii) $\phi_l(G)$ is contained in the normalizer N of a Cartan subgroup C;

(iii) H has order at most 60.

We proceed to eliminate each of these in turn.

In case (i) we may suppose $\phi_l(G)$ is not contained in $\mathbb{F}_l^*$ by assuming (4.1) and using once again Lemma 3.1. Now every Cartan subgroup is commutative, and so we can use Lemma 3.2 to eliminate this case completely if

$$l > c_2 M^{\lambda(2)/2}. \tag{4.2}$$

Next, in case (ii) it is known that C has index 2 in N if $l > 2$ (see p. 279 of [17]). Thus $K = C \cap \phi_l(G)$ has index at most 2 in $\phi_l(G)$. Hence it corresponds to an extension k_0 of k with

$$[k_0 : k] \leqslant 2, \quad \phi_l(G_0) = K \subseteq C$$

for $G_0 = \mathrm{Gal}(\bar{k}_0/k_0)$. So over k_0 we are back in case (i). Thus to eliminate this it suffices to replace d by $2d$, and therefore it is enough to assume (4.1) and (4.2) with M replaced by $2M$.

Finally, in case (iii) the group $K = \mathbb{F}_l^* \cap \phi_l(G)$ has index at most 60 in $\phi_l(G)$, and we obtain an extension k_0 of k with

$$[k_0 : k] \leqslant 60, \quad \phi_l(G_0) = K \subseteq \mathbb{F}_l^*.$$

So over k_0 we are back in a special case of (i), and to eliminate this it suffices to replace M by $60M$ in (4.1) and (4.2).

This completes the proof of part (a) of the Theorem. From (4.1) and (4.2) we see that we can take

$$\gamma = \max\{\lambda(1), \lambda(2)/2\}. \tag{4.3}$$

To prove part (b), we introduce the number

$$e = e(k, l) = d[k(\mu_l): \mathbb{Q}(\mu_l)]^{-1} = (l-1)\,[k(\mu_l): k]^{-1},$$

where $\mu_l = e^{2\pi i/l}$. This is an integer since $\mathrm{Gal}\,(k(\mu_l)/k)$ is a subgroup of $\mathbb{F}_l^*$ and so its order divides $l-1$. Now an arbitrary g in G sends μ_l to μ_l^m, where m is the determinant $\det \phi_l(g)$ in $\mathbb{F}_l^*$. It follows easily from part (a) that if $l > cM^\gamma$, then $\phi_l(G)$ is the subgroup of $\mathrm{GL}\,(E_l)$ consisting of all elements whose determinant is an eth power in $\mathbb{F}_l^*$. So $\phi_l(G) = \mathrm{GL}\,(E_l)$ if and only if $e = 1$. But this last condition is certainly satisfied when l does not divide the discriminant of k. For then l does not ramify in k, and the Eisenstein criterion shows that the minimal polynomial for μ_l over $\mathbb{Q}$ remains irreducible over k; hence $[k(\mu_l): k] = l-1$. This proves part (b), and thereby completes the proof of the Theorem.

5. *Several elliptic curves*

For an integer $n \geqslant 2$ let $E^{(1)}, \ldots, E^{(n)}$ be elliptic curves defined over a number field k, with l-torsion groups $E_l^{(1)}, \ldots, E_l^{(n)}$ respectively. These provide homomorphisms $\phi_l^{(i)}$ from $G = \mathrm{Gal}\,(\bar{k}/k)$ to $\mathrm{GL}\,(E_l^{(i)})$ $(1 \leqslant i \leqslant n)$ and so a homomorphism $\Phi_l = (\phi_l^{(1)}, \ldots, \phi_l^{(n)})$ from G to the product $\mathrm{GL}\,(E_l^{(1)}) \times \ldots \times \mathrm{GL}\,(E_l^{(n)})$. Let $\Delta = \Delta(E_l^{(1)}, \ldots, E_l^{(n)})$ be the subgroup of this product consisting of all $(f^{(1)}, \ldots, f^{(n)})$ with

$$\det f^{(1)} = \ldots = \det f^{(n)}$$

in $\mathbb{F}_l^*$. When $n = 2$, Serre proved in [**17**, p. 327] that $\Phi_l(G) = \Delta$ for all sufficiently large l, provided $E^{(1)}, E^{(2)}$ have no complex multiplication over $\bar{k}$ and the associated l-adic representations are not isomorphic over $\bar{k}$. By Faltings [**7**], this latter condition is equivalent to $E^{(1)}, E^{(2)}$ being non-isogenous over $\bar{k}$. We shall prove the following more precise version for arbitrary n; when $n = 1$ it reduces to our Theorem already proved.

PROPOSITION 1. *There are absolute constants c, γ with the following property. Suppose $E^{(1)}, \ldots, E^{(n)}$ are elliptic curves defined over a number field k of degree d, with Weil heights at most h. Assume that $E^{(1)}, \ldots, E^{(n)}$ have no complex multiplication over $\bar{k}$ and that they are pairwise non-isogenous over $\bar{k}$.*

(a) *If $l > c(\max\{d, h\})^\gamma$, then $\Phi_l(G)$ contains $\mathrm{SL}\,(E_l^{(1)}) \times \ldots \times \mathrm{SL}\,(E_l^{(n)})$.*

(b) *If, further, l does not divide the discriminant of k, then $\Phi_l(G) = \Delta(E_l^{(1)}, \ldots, E_l^{(n)})$.*

For the proof we shall need the following result, which slightly generalizes the arguments of Lemma 8 of [**17**, p. 326].

LEMMA 5.1. *For a prime $l \geqslant 5$, let e be a divisor of $l-1$, let V, V' be vector spaces of dimension 2 over $\mathbb{F}_l$, and let B, B' be the subgroups of $\mathrm{GL}(V)$ and $\mathrm{GL}(V')$ respectively consisting of all elements whose determinants are eth powers. Let D be the*

subgroup of $B \times B'$ consisting of all (b, b') with $\det b = \det b'$, and suppose H is a subgroup of D in $B \times B'$ whose projections to each factor are surjective. Then if $H \neq D$ there is an isomorphism f from V to V' and a character χ of H with $\chi^2 = 1$ such that

$$b' = \chi(h) f b f^{-1}$$

for all $h = (b, b')$ in H.

Proof. As in [**17**], we let N, N' be the kernels defined by

$$N \times \{1\} = H \cap (B \times \{1\}), \quad \{1\} \times N' = H \cap (\{1\} \times B');$$

then the image of H in $B/N \times B'/N'$ is the graph of an isomorphism α from B/N to B'/N'. Since $H \subseteq D$ we have $N \subseteq \mathrm{SL}(V)$. If $N = \mathrm{SL}(V)$, it is easily seen that $H = D$; thus since N is a normal subgroup and $l \geqslant 5$, it follows that $N = \{1\}$ or $\{1, -1\}$. Similarly for N'. Let Z, Z' be the centres of B, B' respectively; then $Z/N, Z'/N'$ are the centres of $B/N, B'/N'$ respectively, so α induces an isomorphism between these. So it also induces an isomorphism $\tilde{\alpha}$ from B/Z to B'/Z'.

However, these latter quotients are isomorphic to either $\mathrm{PGL}_2(\mathbb{F}_l)$ or $\mathrm{PSL}_2(\mathbb{F}_l)$, according to whether e is odd or even. It is known that every automorphism of these groups is induced by an inner automorphism of $\mathrm{PGL}_2(\mathbb{F}_l)$ (see [**6**, pp. 103–104] and also [**14**, p. 795]). It follows that there is an isomorphism f from V to V' such that $\tilde{\alpha}(\tilde{b}) = f \tilde{b} f^{-1}$ for every $\tilde{b}$ in B/Z. This means that for every $h = (b, b')$ in H, we have $b' = \chi f b f^{-1}$ for some $\chi = \chi(h)$ in $\mathbb{F}_l^*$. Clearly χ defines a homomorphism, and by taking determinants we see that $\chi^2 = 1$. This proves the lemma.

We can now prove part (a) of Proposition 1 for $n = 2$; for consistency of notation, we rename $E^{(1)}, E^{(2)}, \phi_l^{(1)}, \phi_l^{(2)}$ as E, E', ϕ_l, ϕ_l' respectively. Assume first that

$$l > cM^{\gamma} \tag{5.1}$$

for c, γ as in the Theorem and $M = \max\{d, h\}$. We shall apply Lemma 5.1 to $H = \Phi_l(G)$ for $V = E_l$, $V' = E_l'$. By the Theorem and the remarks at the end of Section 4, we know that H projects surjectively onto B, B'. If $H = D$, then H contains $\mathrm{SL}(E_l) \times \mathrm{SL}(E_l')$ and we are done. Otherwise, $H \neq D$ and Lemma 5.1 gives

$$\phi_l'(g) = \chi_0(g) f \phi_l(g) f^{-1} \tag{5.2}$$

for every g in G, where χ_0 is the induced character on G, with $\chi_0^2 = 1$.

Assume for the moment that $\chi_0 = 1$ identically. We define Γ in $E \times E'$ as the group of elements (x, fx) as x runs over E_l. Then Γ is defined over k, since an arbitrary g in G acts on (x, fx) to give $(\phi_l(g)x, \phi_l'(g)fx)$, which is (y, fy) for $y = \phi_l(g)x$ by (5.2). Hence $A = E \times E'$ and $A^* = A/\Gamma$ are both defined over k and isogenous over k.

We can now apply Lemma 2.2 to obtain an isogeny of degree $b \leqslant c_4 M^{\lambda(2)}$ from A^* to A; note that $h(A) = h(E) + h(E') \leqslant 2h$. Composing this with the natural isogeny from A to A/Γ of degree l^2, we obtain an endomorphism ε of A. This can be represented by an integral matrix $\begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}$, and since it annihilates Γ we obtain $px = qfx = 0$ for all x in E_l. Because f is an isomorphism, this implies that l divides p and q. Therefore l^4 divides the degree p^2q^2 of ε. But this is bl^2; hence l^2 divides b, and $l \leqslant b^{1/2}$. So this case can be ruled out by assuming that

$$l > c_5 M^{\lambda(2)/2}. \tag{5.3}$$

It remains to consider the case when χ_0 is not identically 1 in (5.2). But then there is a quadratic extension k_0 of k such that $\chi_0 = 1$ on $G_0 = \mathrm{Gal}(\bar{k}_0/k_0)$. Now the

foregoing arguments apply over k_0, and by assuming (5.3) with M replaced by $2M$ we conclude that $\Phi_l(G_0)$ contains $\mathrm{SL}(E_l) \times \mathrm{SL}(E_l')$. Hence so does $\Phi_l(G)$. This proves part (a) of Proposition 1 for $n = 2$; from (4.3), (5.1) and (5.3) we see that a single condition

$$l > c_6 M^{\gamma} \tag{5.4}$$

suffices, where γ as in (4.3) is the exponent appearing in the statement of the Theorem. Part (b) of the proposition follows easily, as at the end of Section 4, and this completes the proof for $n = 2$.

We now deduce the general case. Write $S_i = \mathrm{SL}(E_l^{(i)})$ $(1 \leqslant i \leqslant n)$, and consider the intersection H of $\Phi_l(G)$ with $S = S_1 \times \ldots \times S_n$. If (5.4) holds, then the projection of H to each product $S_i \times S_j$ $(1 \leqslant i < j \leqslant n)$ is surjective. Since $S_1, \ldots, S_n$ have no non-trivial commutative quotients for $l \geqslant 5$, Lemma 5.2.2 (p. 793) of **[14]** implies that $H = S$. This proves part (a), and again part (b) is an immediate consequence. This completes the proof of Proposition 1; once more the exponent γ is as in (4.3).

6. *Points of infinite order*

Let E be an elliptic curve defined over a number field k, and for a positive integer m let $P_1, \ldots, P_m$ be elements of the group $E(k)$ of points of E defined over k. For a prime l let ϕ_l be the homomorphism of $G = \mathrm{Gal}(\bar{k}/k)$ into $\mathrm{GL}(E_l)$ defined in Section 1, and write G_l for its kernel in G. We now define a homomorphism ψ_l from G_l into the additive group E_l^m, as follows. Pick $Q_1, \ldots, Q_m$ in $E(\bar{k})$ with $lQ_i = P_i$ $(1 \leqslant i \leqslant m)$, and for g in G_l let

$$\psi_l(g) = (gQ_1 - Q_1, \ldots, gQ_m - Q_m).$$

Since g fixes all points of order l, it is easily checked that ψ_l is independent of the choice of $Q_1, \ldots, Q_m$.

Assume now that $P_1, \ldots, P_m$ are linearly independent over the ring of endomorphisms of E over $\bar{k}$. Bashmakov **[1]** proved that $\psi_l(G_l) = E_l^m$ for all sufficiently large l. In **[2]**, Bertrand extended this result and gave an effective version when E has complex multiplication. When E has no complex multiplication, we obtained in **[10]** an effective version for $m = 1$. Our Theorem now enables this to be generalized to arbitrary m. We shall need the (absolute logarithmic) Néron–Tate height q on $E(k)$.

PROPOSITION 2. *There are absolute constants c, δ with the following property. Suppose E is an elliptic curve of Weil height h defined over a number field k of degree d. Assume E has no complex multiplication over $\bar{k}$, and $P_1, \ldots, P_m$ are points of $E(k)$ linearly independent over $\mathbb{Z}$. Then if $l > (cM^{\delta}U)^{m/2}$, we have $\psi_l(G_l) = E_l^m$, where*

$$M = \max\{d, h\}, \quad U = q(P_1) + \ldots + q(P_m).$$

For the proof we follow the proof of Theorem 3 of **[10]**. We have to check the validity of the axioms B_1, B_2, B_3, B_4 of Ribet's paper **[15**, p. 747] for E.

First, if $l > cM^{\gamma}$ for the constants c, γ of our Theorem, then $\phi_l(G)$ contains $\mathrm{SL}(E_l)$, and therefore the commutant of $\phi_l(G)$ in $\mathrm{End}\, E_l$ is contained in the commutant of $\mathrm{SL}(E_l)$ in $\mathrm{End}\, E_l$, which is well-known to be $\mathbb{F}_l$. This settles B_1.

Similarly, if $l > cM^{\gamma}$, then E_l is irreducible as a $\phi_l(G)$-module, and so by Lemma 10 of **[3**, p. 179], the cohomology group $H^1(\phi_l(G), E_l)$ vanishes. This deals with B_2 and B_3.

Finally, the validity of B_4 is obvious, and from Proposition 1.1 **[15**, p. 747] it will suffice to make l so large that $P_1, \ldots, P_m$ remain linearly independent modulo $lE(k)$. By

the discussion in [2, pp. 85, 87], this holds if $l > (\mu^{-1}U)^{m/2}$, where μ is the minimum of $q(P)$ taken over all non-torsion P in $E(k)$. Since $U \geqslant \mu$, we deduce Proposition 2 with $\delta = \beta + 2\gamma$ as soon as we can show that $\mu^{-1} \leqslant c_7 M^{\beta}$ for some absolute constant β.

Such a bound follows from a recent result of S. David [5]. For $g = 1$, his Théorème 1.4 leads to the estimate

$$\mu^{-1} \leqslant c_8 h_1^{-1} d^6 (h_1 + \log d)^6 \leqslant c_9 M^{11},$$

with $h_1 = \max\{1, h\}$. A slightly better exponent can be obtained using the method of [8]; in this paper we did not work out the dependence on d, but it is a relatively easy matter to do so, and we find

$$\mu^{-1} \leqslant c_{10} h_1 d^4 (h_1 + \log d)^2 \leqslant c_{11} M^7$$

This completes the proof of Proposition 2.

References

1. M. BASHMAKOV, 'The cohomology of abelian varieties over a number field', *Russian Math. Surveys* 27 (1972) 25–70.
2. D. BERTRAND, 'Kummer theory on the product of an elliptic curve by the multiplicative group', *Glasgow Math. J.* 22 (1981) 83–88.
3. J. H. COATES, 'An application of the division theory of elliptic functions to diophantine approximation', *Invent. Math.* 11 (1970) 167–182.
4. G. CORNELL and J. SILVERMAN (eds), *Arithmetic geometry* (Springer, New York, 1986).
5. S. DAVID, 'Minorations de hauteurs sur les variétés abéliennes', *Bull. Soc. Math. France*, to appear.
6. J. DIEUDONNÉ, *La géometrie des groupes classiques* (Springer, Berlin, 1971).
7. G. FALTINGS, 'Endlichkeitssätze für abelsche Varietäten über Zahlkörpern', *Invent. Math.* 73 (1983) 349–366; 75 (1984) 381.
8. D. W. MASSER, 'Counting points of small height on elliptic curves', *Bull. Soc. Math. France* 117 (1989) 247–265.
9. D. W. MASSER and G. WÜSTHOLZ, 'Zero estimates on group varieties II', *Invent. Math.* 80 (1985) 233–267.
10. D. W. MASSER and G. WÜSTHOLZ, 'Some effective estimates for elliptic curves', *Arithmetic of complex manifolds*, Lecture Notes in Math. 1399 (ed. W.-P. Barth and H. Lange, Springer, New York, 1989), 103–109.
11. D. W. MASSER and G. WÜSTHOLZ, 'Estimating isogenies on elliptic curves', *Invent. Math.* 100 (1990) 1–24.
12. D. W. MASSER and G. WÜSTHOLZ, 'Periods and minimal abelian subvarieties', *Ann. of Math.*, to appear.
13. D. W. MASSER and G. WÜSTHOLZ, 'Isogeny estimates for abelian varieties, and finiteness theorems', *Ann. of Math.*, to appear.
14. K. RIBET, 'Galois action of division points of abelian varieties with real multiplication', *Amer. J. Math.* 98 (1976) 751–804.
15. K. RIBET, 'Kummer theory on extensions of abelian varieties by tori', *Duke Math. J.* 46 (1979) 745–761.
16. J-P. SERRE, *Abelian l-adic representations and elliptic curves* (Benjamin, New York, 1968).
17. J-P. SERRE, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* 15 (1972) 259–331.
18. J-P. SERRE, 'Quelques applications du théorème de densité de Chebotarev', *Publ. Math. IHES* 54 (1981) 123–201.
19. Y. ZARHIN, 'A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction', *Invent. Math.* 79 (1985) 309–321.

Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA

Departement für Mathematik
ETH-Zentrum
8092 Zürich
Switzerland