VISIBILITY OF TATE-SHAFAREVICH GROUPS

TOM FISHER

Abstract. These are the notes for a short course given at the University of Warwick on 29th and 30th April 2008.

1. Weil-Châtelet groups

Let A be an abelian variety over a field K of characteristic 0. Let $\overline{K}$ be the algebraic closure of K, and let L/K be any field extension.

Definition 1.1. A torsor (V, μ) under A is a variety V together with a morphism $\mu : A \times V \to V$ (all defined over K) that induces a simply transitive action of $A(\overline{K})$ on $V(\overline{K})$.

We often write V for (V, μ).

Definition 1.2. Torsors (V_1, μ_1) and (V_2, μ_2) are isomorphic over L if there is an isomorphism $\varphi : V_1 \to V_2$ defined over L such that

$$\begin{tikzcd}
A \times V_1 \arrow[r, "\mu_1"] \arrow[d, "1\times\varphi"'] & V_1 \arrow[d, "\varphi"] \\
A \times V_2 \arrow[r, "\mu_2"] & V_2
\end{tikzcd}$$

commutes.

The trivial torsor is $(A, +)$ where $+ : A \times A \to A$ is the group law.

Lemma 1.3. *Let (V, μ) be a torsor under A. Then $V(L) \neq \emptyset$ if and only if $(V, \mu) \cong (A, +)$ over L.*

Proof: "$\Leftarrow$" We have $0 \in A(K)$. "$\Rightarrow$" Let $P_0 \in V(L)$. Then the required isomorphism is $\varphi : A \to V\,;\ P \mapsto \mu(P, P_0)$. □

Hence all torsors are trivial over $\overline{K}$. We note that $\mathrm{Aut}(V, \mu) = A$ for any torsor (V, μ). In particular this applies to $(A, +)$. So if $\varphi : V \cong A$ is an isomorphism of torsors over $\overline{K}$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$ then

$$\sigma(\varphi) \circ \varphi^{-1} = (P \mapsto P + \xi_\sigma) \tag{1}$$

for some $\xi_\sigma \in A(\overline{K})$. One easily checks that $\sigma \mapsto \xi_\sigma$ is a (continuous) cocycle, and that changing φ changes it by a coboundary.

Date: 6th May 2008.

Lemma 1.4. *The map*

$$\begin{array}{rcl}\{\textit{torsors under } A\}/\cong & \to & H^1(K,A)\\ (V,\mu) & \mapsto & \textit{class of } (\xi_\sigma)\end{array}$$

is a bijection.

Proof: Suppose V_1 and V_2 are trivialised by $\varphi_1 : V_1 \cong A$ and $\varphi_2 : V_2 \cong A$, with corresponding cocycles

$$\sigma(\phi_1) \circ \phi_1^{-1} = (P \mapsto P + \xi_\sigma) \text{ and } \sigma(\phi_2) \circ \phi_2^{-1} = (P \mapsto P + \eta_\sigma).$$

If $\xi_\sigma - \eta_\sigma = \sigma(Q) - Q$ for some $Q \in A(\overline{K})$ then

$$\varphi_2^{-1} \circ (P \mapsto P - Q) \circ \varphi_1 : V_1 \to V_2$$

is an isomorphism of torsors defined over K. This proves injectivity.

The proof of surjectivity takes more work. It uses the conditions worked out by Weil for recognising when a variety defined over $\overline{K}$ comes from one defined over K (variously known as "Galois descent" or "Weil descent"). □

Definition 1.5. $H^1(K,A)$ is called the Weil-Châtelet group.

We write V_ξ for the torsor determined by $\xi \in H^1(K,A)$.

Since $H^1(K,A)$ is a group (by adding cocycles), Lemma 1.4 shows that the set of isomorphism classes of torsors also has a group structure. Here are some alternative (partial) descriptions of the group law.

- (V,μ) has inverse (V,μ') where $\mu'(P,X) = \mu(-P,X)$.
- Let A act anti-diagonally on $V_1 \times V_2$. Then the sum of V_1 and V_2 is $(V_1 \times V_2)/A$.
- If $\dim(A) = 1$ then $n[V] = [\operatorname{Pic}^n V]$ for all $n \in \mathbb{Z}$. This includes (as the case $n = 0$) the fact that A is the Jacobian of V. (If $\dim(A) > 1$ then one should use Albanese varieties.)

2. The period-index problem

For $K \subset L \subset \overline{K}$ there is a restriction map of Galois cohomology $\operatorname{res}_{L/K} : H^1(K,A) \to H^1(L,A)$. Let $\xi \in H^1(K,A)$. Then $\operatorname{res}(\xi) = 0$ if and only if $V_\xi(L) \neq \emptyset$, in which case we say that "L splits ξ".

Definition 2.1. The *period* of ξ is its order in $H^1(K,A)$. The *index* of ξ is the greatest common divisor of the degrees of the field extensions L/K that split ξ. (Equivalently, it is the least positive degree of a K-rational zero cycle on V_ξ.)

Lemma 2.2. *If* $\dim(A) = 1$ *and* $\xi \in H^1(K,A)$ *has index* n *then*

(1) *There is a field extension L/K of degree n that splits ξ (i.e. "the index is attained").*
(2) *If K is a number field then there are infinitely many such extensions L/K.*

Proof: (i) By Riemann-Roch, every K-rational divisor D on V_ξ of positive degree is linearly equivalent to an effective divisor.
(ii) Exercise. (See [6] for the case $n = 2$). □

Remark 2.3. It is noted in both [11] and [18] that Lemma 2.2(i) is open for $\dim A > 1$.

The first part of the following theorem shows that the Weil-Châtelet group is a torsion group, *i.e.* every element has finite order.

Theorem 2.4 (Lang and Tate [18])**.** *The period divides the index and they have the same prime factors.*

Proof: (i) Suppose V is trivialised by $\varphi : V \cong A$, and let ξ be given by (1). Let $D = \sum_{i=1}^n P_i$ be a 0-cycle on V of degree n. Then

$$\sigma(\sum_{i=1}^n P_i) = \sum_{i=1}^n \varphi(\sigma P_i) + n\xi_\sigma$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. It follows that if D is K-rational then $n\xi$ is a coboundary, and hence trivial in $H^1(K, A)$.

Alternatively, we recall there is a corestriction homomorphism

$$\mathrm{cores} : H^1(L, A) \to H^1(K, A)$$

with the property that $\mathrm{cores} \circ \mathrm{res}$ is multiplication by $[L : K]$.

(ii) Suppose $\xi \in H^1(K, A)[n]$ and p is a prime not dividing n. Let L/K be a finite extension that splits ξ. Enlarging L if necessary we may assume L/K is Galois. Let F be the fixed field for a Sylow-p-subgroup of $\mathrm{Gal}(L/K)$. Then $\mathrm{res}_{F/K}(\xi) \in H^1(F, A)$ has period dividing n and index a power of p. Since p does not divide n it follows by (i) that $\mathrm{res}_{F/K}(\xi) = 0$, *i.e.* F splits ξ. But F/K is an extension of degree prime to p. So p does not divide the index of ξ. □

As observed by Clark [11], the statement and proof of Theorem 2.4 carry over verbatim to Galois cohomology groups in general. Indeed as Lang and Tate point out, their theorem is the analogue of some previously known results for Brauer groups, cf. $\mathrm{Br}(K) = H^2(K, \mathbb{G}_m)$.

Next we give a bound for the index in terms of the period.

Lemma 2.5. *Let $\xi \in H^1(K, A)[n]$. Then*
(i) ξ is split by a field extension of degree at most $n^{2 \dim A}$, and
(ii) the index of ξ divides $n^{2 \dim A}$.

PROOF: (i) Taking the long exact of Galois cohomology for the short exact sequence

$$0 \to A[n] \to A \to A$$

gives the Kummer exact sequence. In particular there is a surjection $H^1(K, A[n]) \to H^1(K, A)[n]$. The first of these groups parametrises the $A[n]$-torsors, and it is clear that any $A[n]$-torsor is split by a field extension of degree at most $\# A[n] = n^{2 \dim A}$. This gives the bound on the index.

(ii) If n is a power of a prime p, then by Theorem 2.4 the index is also a power of p. So we are done by (i). In general one looks at the primary decomposition of $H^1(K, A)[n]$. We leave the details as an exercise. □

The Tate-Shafarevich group is a subgroup of the Weil-Châtelet group.

Definition 2.6. If K is a number field then

$$\begin{aligned} \text{Ш}(A/K) &= \ker \left(H^1(K, A) \to \textstyle\prod_v H^1(K_v, A) \right) \\ &= \{ \xi \in H^1(K, A) \mid V_\xi(K_v) \neq \emptyset \text{ for all places } v \}. \end{aligned}$$

(For the definition as a kernel we must fix embeddings $\overline{K} \subset \overline{K}_v$, but the definition is independent of these choices.)

Theorem 2.7 (Cassels [8], Lichtenbaum [19])**.** *Let $\xi \in H^1(K, A)$ with $\dim(A) = 1$. Assume*

(i) $\text{Br}(K) = 0$, *or*
(ii) *K is a number field and $\xi \in \text{Ш}(A/K)$, or*
(iii) *K is a $\mathfrak{p}$-adic field.*

Then the period of ξ is equal to the index of ξ.

PROOF: (Sketch.) Let $G = \text{Gal}(\overline{K}/K)$. For any smooth projective variety V over K there is an exact sequence

$$0 \longrightarrow \text{Pic}_K V \longrightarrow (\text{Pic}_{\overline{K}} V)^G \longrightarrow \text{Br}(K).$$

If V is a torsor under A, then the index, respectively period, of V is the least positive degree of a divisor class in $\text{Pic}_K V$, respectively $(\text{Pic}_{\overline{K}} V)^G$. (This gives yet another proof that the period divides the index.) Moreover if $V(K) \neq \emptyset$ then $\text{Pic}_K V = (\text{Pic}_{\overline{K}} V)^G$.

(i) If $\text{Br}(K) = 0$ then $\text{Pic}_K V = (\text{Pic}_{\overline{K}} V)^G$, so the result is clear.

(ii) Let $[D]$ be any divisor class in $(\text{Pic}_{\overline{K}} V)^G$. Since $V_\xi(K_v) \neq 0$ for all v, the image of $[D]$ in $\text{Br}(K)$ is everywhere locally trivial. But by class field theory, the natural map

$$\text{Br}(K) \to \oplus_v \text{Br}(K_v)$$

is injective. Hence $[D]$ comes from $\text{Pic}_K V$.

(iii) For each $\xi \in H^1(K, A)[n]$ there is a map $(\operatorname{Pic}_{\overline{K}} V)^G \to \operatorname{Br}(K)$. Restricting to $(\operatorname{Pic}^0_{\overline{K}} V)^G = A(K)$ defines a pairing

$$A(K)/nA(K) \times H^1(K, A)[n] \to \operatorname{Br}(K) = \mathbb{Q}/\mathbb{Z}.$$

Lichtenbaum identifies this as the Tate pairing, which is known (by local class field theory) to be non-degenerate. One then checks that the image of $[D] \in (\operatorname{Pic}^n_{\overline{K}} V)^G$ in $\operatorname{Br}(K)$ is n-torsion. So this image can be made trivial by adding to $[D]$ a suitable divisor class of degree 0. □

Remark 2.8. Recent work of Clark [11] gives bounds for the index in terms of the period in the case $\dim(A) > 1$.

3. Visibility

Let $A \hookrightarrow B$ be an inclusion[1] of abelian varieties over K.

Definition 3.1. (Mazur [13],[20]) The subgroup of $H^1(K, A)$ of elements visible in B is

$$\operatorname{Vis}_B H^1(K, A) = \ker\big(H^1(K, A) \to H^1(K, B)\big)$$

This definition depends not just on A and B, but also on the map between them. Since this map is usually clear from the context, it is safe to omit it from our notation.

The quotient of B by A is again an abelian variety, C say. This gives a short exact sequence

$$0 \to A \to B \to C \to 0$$

with associated long exact sequence

$$\ldots \to B(K) \to C(K) \to H^1(K, A) \to H^1(K, B) \to \ldots \tag{2}$$

Let $x \in C(K)$ map to $\xi \in H^1(K, A)$. Then $\pi^{-1}(x)$ is a coset of A in B, and so a torsor under A. It represents ξ. One obvious appeal of visibility, is that we can specify elements of $H^1(K, A)$ by writing down (co-ordinates of) rational points on C, instead of equations for torsors under A.

A more geometric version of Definition 3.1 is the following.

Lemma 3.2. *Let (V, μ) be a torsor under A. Then (V, μ) is visible in $\iota_A : A \hookrightarrow B$ if and only if there is an inclusion of varieties $\iota_V : V \hookrightarrow B$ such that*

$$\begin{tikzcd}
A \times V \arrow[r, "\mu"] \arrow[d, "\iota_A \times \iota_V"] & V \arrow[d, "\iota_V"] \\
B \times B \arrow[r, "+"] & B
\end{tikzcd}$$

[1] This means both a morphism of group varieties, and a closed immersion.

commutes.

4. Restriction of scalars

Let L/K be a finite extension of fields. The idea of restriction of scalars is conveyed by the following example.

Example 4.1. Let $L = K(\sqrt{d})$ for some $d \in K$, and let $X \subset \mathbb{A}^n$ be the hypersurface defined by $f \in L[x_1, \ldots, x_n]$. We can then write

$$f(u_1 + \sqrt{d}v_1, \ldots, u_n + \sqrt{d}v_n) = g + \sqrt{d}h$$

for some polynomials $f, g \in K[u_1, \ldots, u_n, v_1, \ldots, v_n]$. The restriction of scalars of X is $\mathrm{Res}_{L/K}(X) = \{g = h = 0\} \subset \mathbb{A}^{2n}$. By construction we have $X(L) = \mathrm{Res}_{L/K}(X)(K)$.

For S a scheme over K we write $S_L = S \times_K L$.

Definition 4.2. Let X be a variety over L. The restriction of scalars $\mathrm{Res}_{L/K}(X)$ is a variety defined over K representing the functor

$$\begin{array}{rcl} \text{Schemes}\,/K & \rightarrow & \text{Sets} \\ S & \mapsto & X(S_L) = \mathrm{Hom}_L(S_L, X) \end{array}$$

See [4, §7.6]. We note that $\mathrm{Res}_{L/K}(A_L)$ is an abelian variety of dimension $[L : K] \dim(A)$. (We are following the treatment in [1].)

Theorem 4.3. *Let $\xi \in H^1(K, A)$. Then ξ is split by L if and only if it is visible in $A \hookrightarrow \mathrm{Res}_{L/K}(A_L)$.*

Proof: (Sketch.) We recall that $\overline{K} \otimes_K L \cong \prod_\sigma \overline{K}$ where σ runs over all K-embeddings $L \hookrightarrow \overline{K}$. Taking points on A with co-ordinates in this ring we obtain

$$\mathrm{Res}_{L/K}(A)(\overline{K}) \cong \prod_\sigma A(\overline{K}).$$

Keeping track of the action of $\mathrm{Gal}(\overline{K}/K)$, it turns out we are precisely in the situation where Shapiro's lemma applies. This shows that the vertical map in the following diagram is an isomorphism.

$$\begin{tikzcd} H^1(K, A) \arrow[r] \arrow[dr] & H^1(K, \mathrm{Res}_{L/K}(A_L)) \arrow[d, "\cong"] \\ & H^1(L, A). \end{tikzcd}$$

The proof is completed by checking this diagram commutes. □

Remark 4.4. An more geometric proof of the first implication of Theorem 4.3 is the following. Let $V = V_\xi$ and suppose L splits ξ. Then $V_L \cong A_L$. Let ι_V be the composite $V \hookrightarrow \mathrm{Res}_{L/K}(V_L) \cong \mathrm{Res}_{L/K}(A_L)$. One then checks that the hypotheses of Lemma 3.2 are satisfied for $\iota_A : A \hookrightarrow \mathrm{Res}_{L/K}(A_L)$.

Definition 4.5. The *visibility dimension* of $\xi \in H^1(K, A)$ is the least dimension of an abelian variety B such that ξ is visible in $A \hookrightarrow B$.

Theorem 4.3 not only shows that every element of $H^1(K, A)$ is visible in some abelian variety, but also, when combined with the results of §2 gives bounds for the visibility dimension. For example, by Lemma 2.5(i), the visibility dimension of $\xi \in H^1(K, A)[n]$ is at most $(\dim A)n^{2 \dim A}$. Moreover if $\dim(A) = 1$ then by Lemma 2.2(i), the visibility dimension is at most the index.

Lemma 4.6. *Suppose K is a number field, and let $S \subset H^1(K, A)$ be any subgroup. Then every element of S can be visualised inside the same abelian variety B if and only if S is finite.*

Proof: "$\Rightarrow$" We pick a finite extension L_ξ/K splitting each $\xi \in S$. Let L be the composite of these fields. Since S is finite, this is a finite extension of K. We put $B = \mathrm{Res}_{L/K}(A)$ and use Theorem 4.3.
"$\Leftarrow$" By (2) we see that $\mathrm{Vis}_B\, H^1(K, A)$ is both a quotient of $C(K)$, hence finitely generated by the Mordell-Weil theorem, and a subgroup of $H^1(K, A)$, hence torsion by Theorem 2.4. Hence $\mathrm{Vis}_B\, H^1(K, A)$ is finite. □

Lemma 4.6 gives an equivalent formulation of the conjecture that the Tate-Shafarevich group is finite.

Remark 4.7. The following analogy (discussed at the end of [15]) is worth some consideration. Let K be a number field and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be a collection of ideals in $\mathcal{O}_K$ generating the class group. The capitulation problem is to find a finite extension L/K so that each of the ideals $\mathfrak{a}_1\mathcal{O}_L, \ldots, \mathfrak{a}_n\mathcal{O}_L$ is principal. This problem is easily solved, and the solution is far from unique. However there is a unique solution, namely the Hilbert class field of K, if one imposes some additional conditions on L. Might there be corresponding additional conditions that could be used to make the abelian variety B in Lemma 4.6 unique?

5. Some diagram chasing

Let J be an abelian variety of K. (In some of the examples J will be the Jacobian of a curve, but we do not need to assume this now.) It is well known (see [22]) that every abelian subvariety $A \subset J$ has a complementary abelian subvariety B such that $\Delta = A \cap B$ is finite and $A + B = J$. (There is no claim that B is unique.) Let $B' = J/A$ and $A' = J/B$. This gives two exact sequences. We combine them in a commutative diagram

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & B \arrow[d] \arrow[dr, "\psi"] & & \\
0 \arrow[r] & A \arrow[r] \arrow[dr, "\phi"'] & J \arrow[r] \arrow[d] & B' \arrow[r] & 0 \\
 & & A' \arrow[d] & & \\
 & & 0 & &
\end{tikzcd}$$

where the diagonal maps ϕ and ψ are isogenies with kernel Δ.

Alternatively, we may arrive at the same set-up, by taking abelian varieties A and B with common finite sub-K-group scheme Δ, and then putting $J = (A \times B)/\Delta$.

There is a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \Delta \arrow[r] \arrow[d] & B \arrow[r, "\psi"] \arrow[d] & B' \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & A \arrow[r] & J \arrow[r] & B' \arrow[r] & 0.
\end{tikzcd}$$

Taking the long exact sequence of Galois cohomology gives

$$\begin{tikzcd}
 & B(K) \arrow[r, "\psi"] \arrow[d] & B'(K) \arrow[r] \arrow[d, equal] & H^1(K,\Delta) \arrow[r, "\iota_B"] \arrow[d, "\iota_A"] & H^1(K,B) \arrow[d] \\
A(K) \arrow[r] & J(K) \arrow[r] & B'(K) \arrow[r] & H^1(K,A) \arrow[r] & H^1(K,J).
\end{tikzcd} \tag{3}$$

Theorem 5.1. (i) *Let $\xi \in H^1(K,A)$. Then ξ is visible in $A \hookrightarrow J$ if and only if there exists $\eta \in H^1(K,\Delta)$ such that $\iota_A(\eta) = \xi$ and $\iota_B(\eta) = 0$.*

(ii) *There are exact sequences*

$$0 \to \frac{J(K)}{A(K)+B(K)} \to \frac{B'(K)}{\psi B(K)} \to \mathrm{Vis}_J\, H^1(K,A) \to 0$$

and (swapping the roles of A and B)

$$0 \to \frac{J(K)}{A(K)+B(K)} \to \frac{A'(K)}{\phi A(K)} \to \mathrm{Vis}_J\, H^1(K,B) \to 0.$$

Proof: Both parts are proved from (3) by a diagram chase. □

Remark 5.2. Theorem 5.1(i) shows that $\xi \in H^1(K,A)$ is visible in $J = (A \times B)/\Delta$ if and only if it comes from $B'(K)$ in the diagram

$$\begin{tikzcd}
0 \arrow[r] & A'(K)/\phi A(K) \arrow[r] & H^1(K,\Delta) \arrow[r] \arrow[d, equal] & H^1(K,A)[\phi] \arrow[r] & 0 \\
0 \arrow[r] & B'(K)/\psi B(K) \arrow[r] & H^1(K,\Delta) \arrow[r] & H^1(K,B)[\psi] \arrow[r] & 0.
\end{tikzcd}$$

6. Visibility in abelian surfaces

Theorem 6.1 (Klenke [17], Mazur [20]). *Let E/K be an elliptic curve and let $\xi \in H^1(K,E)$.*

(i) *(Klenke) If ξ has period 2 then it is visible in an abelian surface.*
(ii) *(Mazur) If ξ has index 3 then it is visible in an abelian surface.*

The following lemma prepares for the proof of Theorem 6.1(i).

Lemma 6.2. (i) *Any $\xi \in H^1(K,E)$ of period 2 is represented by*

$$C = \left\{ \begin{array}{l} q_1(x_1,x_2,x_3) = 0 \\ q_2(x_1,x_2,x_3) = x_4^2 \end{array} \right\} \subset \mathbb{P}^3$$

for some quadrics $q_1, q_2 \in K[x_1,x_2,x_3]$.

(ii) *Let $\Phi = \{q_1 = q_2 = 0\} \subset \mathbb{P}^2$. Then Φ is an $E[2]$-torsor and the natural map $H^1(K,E[2]) \to H^1(K,E)$ sends the class of Φ to the class of C.*

(iii) *The image of $E[2] \subset \mathrm{Aut}(\Phi) \cong S_4$ is the Klein 4-group.*

Proof: (i) Our claim is that C embeds in $\mathbb{P}^3$ as an intersection of quadrics, and that at least one of the four singular fibres in the pencil of quadrics (defining C) is defined over K.

This statement will be clear to anyone familiar with 2-descent on elliptic curves (as described in [9]). Since ξ has period 2, it lifts to

$$H^1(K,E[2]) \cong \ker(L^\times/(L^\times)^2 \overset{N_{L/K}}{\to} K^\times/(K^\times)^2)$$

where L is the étale algebra of $E[2] - \{0\}$. If E has Weierstrass equation $y^2 = f(x)$ then $L = K[\theta] = K[x]/(f(x))$. To decide whether the class of $\alpha \in L^\times$ comes from $E(K)$ in the Kummer exact sequence, one must solve the equation

$$x - \theta = \xi(u_0 + u_1\theta + u_2\theta^2)^2$$

for $(x,y) \in E(K)$ and $u_0,u_1,u_2 \in K$. Taking coefficients of θ^i for $i = 1,2$ gives two quadratic equations in u_0, u_1, u_2. These homogenise to give equations for $C \subset \mathbb{P}^3$ of the required form.

A more direct alternative would be to start from a 2-covering $\pi : C \to E$ and embed $C \subset \mathbb{P}^3$ by the divisor $\pi^*(0)$. Let A and B the 4 by 4 symmetric matrices corresponding to the quadrics defining C. There are classical formulae (reproduced in [3], [21]) defining a morphism $\nu : C \to C_1 = \{y^2 = g(x,z)\}$ where $g(x,z) = \det(Ax + Bz)$. It may be checked that ν takes the quotient of C by $E[2]$, and that if P is a ramification point for $C_1 \to \mathbb{P}^1$ then $\nu^*(P)$ is a hyperplane section on $C \subset \mathbb{P}^3$. Thus $C_1 \cong E$ and with this identification, the ramification points of $C_1 \to \mathbb{P}^1$ map to the 2-torsion points of E. It follows that $g(x,z)$ has a linear factor defined over K, as required.

(ii) Notice that C is a double cover of the conic $\Gamma = \{q_1 = 0\} \subset \mathbb{P}^2$, ramified above the four points Φ. We must check that the action of E on C restricts to an action of $E[2]$ on Φ. It suffices to prove this claim over an algebraically closed field, in which case we need nothing more than the statement that $E[2]$ acts on the set of ramification points for the double cover $E \to \mathbb{P}^1$ given by the x-co-ordinate of a Weierstrass equation.

(iii) This is the only transitive subgroup of S_4 of order 4. □

Proof of Theorem 6.1(i): Let ξ be represented by $C \subset \mathbb{P}^3$ with equations as in Lemma 6.2(i). Since C is smooth, there are exactly 4 rank 3 quadrics in the pencil defining C. So the pencil of conics in $\mathbb{P}^2$ spanned by q_1 and q_2 has exactly 3 singular fibres. Each singular fibre is a pair of lines, and together they make up the 6 lines of the complete quadrilateral through the 4 points Φ.

Let $P \in \mathbb{P}^2(K)$ be any rational point, not on one of the 6 lines. We pick a new basis q_1', q_2' for the space of quadrics spanned by q_1 and q_2 so that $q_1'(P) = 0$. We then define

$$C' = \left\{ \begin{array}{l} q_1'(x_1,x_2,x_3) = 0 \\ q_2'(x_1,x_2,x_3) = dx_4^2 \end{array} \right\} \subset \mathbb{P}^3$$

where $d \in K$ is chosen so that C' has a K-rational point above P. Our choice of P (avoiding the 6 lines) guarantees that C' is a smooth curve of genus one. So its Jacobian is an elliptic curve, F say. Lemma 6.2(iii) shows that $E[2]$ and $F[2]$ are isomorphic as Galois modules, equal to Δ say. We apply Theorem 5.1(i) with $A = E$, $B = F$ and η the class of Φ in $H^1(K,\Delta)$. By Lemma 6.2(ii) this element η maps to the classes of C and C' in $H^1(K,E)$ and $H^1(K,F)$ respectively. The first of these is ξ, and second is zero since $C'(K) \neq \emptyset$. □

The proof of Theorem 6.1(ii) has exactly the same format.

Lemma 6.3. (i) *Any $\xi \in H^1(K, E)$ of index 3 is represented by a plane cubic $C \subset \mathbb{P}^2$.*

(ii) *Let $\Phi \subset \mathbb{P}^2$ be the set of points of inflection on C. Then Φ is an $E[3]$-torsor and the natural map $H^1(K, E[3]) \to H^1(K, E)$ sends the class of Φ to the class of C.*

(iii) *The image of $E[3] \hookrightarrow \mathrm{Aut}(\Phi) \cong S_9$ depends on Φ, but not on C or E.*

Proof: (i) By Lemma 2.2(i) there is a K-rational divisor of degree 3 on C, and we use this to embed $C \subset \mathbb{P}^2$ as a plane cubic.

(ii) We must show that the action of E on C restricts to an action of $E[3]$ on Φ. It suffices to check this over $\overline{K}$, in which case we need nothing more than the statement that the points of inflection on an elliptic curve in Weierstrass form are the 3-torsion points.

(iii) It suffices to check this for C in Hesse normal form:

$$a(x^3 + y^3 + z^3) + bxyz = 0.$$

Each non-singular member of the Hesse pencil has the same set of points of inflection, namely $\Phi = \{x^3 + y^3 + z^3 = xyz = 0\}$. Conversely every plane cubic containing Φ belongs to the Hesse pencil. Moreover, for each non-singular member of the Hesse pencil, the action of the 3-torsion of its Jacobian is generated by

$$\begin{pmatrix} 1 & & \\ & \zeta_3 & \\ & & \zeta_3^2 \end{pmatrix} \text{ and } \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & \end{pmatrix}.$$

□

Proof of of Theorem 6.1(ii): By Lemma 6.3(i) we can represent ξ by a plane cubic $C \subset \mathbb{P}^2$. There are 4 singular fibres in the pencil of plane cubics spanned by C and its Hessian. Each of these singular fibres in the union of 3 lines. Let $P \in \mathbb{P}^2(K)$ be any rational point, not on one of the 12 lines. Let C' be the member of the Hesse pencil with $P \in C'(K)$. Our choice of P (avoiding the 12 lines) guarantees that C' is a smooth curve of genus one. So its Jacobian is an elliptic curve, F say. Lemma 6.3(iii) shows that $E[3]$ and $F[3]$ are isomorphic as Galois modules, equal to Δ say. We apply Theorem 5.1(i) with $A = E$, $B = F$ and η the class of Φ in $H^1(K, \Delta)$. By Lemma 6.3(ii) this element η maps to the classes of C and C' in $H^1(K, E)$ and $H^1(K, F)$ respectively. The first of these is ξ, and second is zero since $C'(K) \neq \emptyset$. □

If K is a number field, the results of Klenke and Mazur show that every element of $Ш(E/K)$ of order $p = 2$ or 3 is visible in an abelian surface. (In fact the first of these is already clear by restriction of scalars.) So it is natural to ask the following questions.

- Let $p = 2$ or 3. Can all of $Ш(E/K)[p]$ be visualised in the same abelian surface?
- Are all elements $\xi \in H^1(K, E)$ of index $n = 4$ or 5 visible in an abelian surface? If not, is it true for $\xi \in Ш(E/K)$?
- Is every element of $H^1(K, E)$ of period 3 visible in an abelian surface?

The original papers of Mazur and Klenke phrase the proof of Theorem 6.1 in terms of finding rational points on certain twists of the total space for the family of elliptic curves above $X(n)$ for $n = 2, 3$. In fact they show that all relevant surfaces are birational (over K) to $\mathbb{P}^2$. The surfaces for $n = 4$ or 5 have more interesting geometry.

In preparing these notes, I realised how to construct a counterexample to the third of these questions. The basic idea is that the obstruction map $\mathrm{Ob}_3 : H^1(K, E[3]) \to \mathrm{Br}(K)$, defined in [24], depends only on the structure of $E[3]$ as a Galois module equipped with the Weil pairing, and not on E itself.

7. Using visibility to construct elements of Ш

The results in this section are due to Agashé and Stein [1]. From now on we take K a number field. (In all the examples $K = \mathbb{Q}$.)

As in §5 we let A and B be complementary abelian subvarieties of an abelian variety J. We also put $B' = J/A$ and $A' = J/B$.

Proposition 7.1. *Let $n \geq 2$ be an integer. Suppose*

(i) $B[n] \subset A \cap B$ *and* $\gcd(n, \#B(K)_{\mathrm{tors}}) = 1$, *and*
(ii) $\operatorname{rank} A(K) = 0$ *and* $\gcd(n, \#A'(K)_{\mathrm{tors}}) = 1$.

Then

$$B(K)/nB(K) \hookrightarrow \mathrm{Vis}_J \, H^1(K, A).$$

Proof: The first hypothesis shows that the isogeny $\psi : B \to B'$ factors through multiplication-by-n as $\psi = \tau \circ [n]$. Then τ induces a map $B(K)/nB(K) \to B'(K)/\psi B(K)$. Our assumption on the torsion of $B(K)$ shows that this map is injective. The second hypothesis shows that $A'(K)/\phi A(K)$ is a finite group of order coprime to n. We are done by Theorem 5.1(ii). □

Proposition 7.2. *Suppose in addition to the above hypotheses that*

(i) *all the Tamagawa numbers of A and B are coprime to n.*
(ii) *J has good reduction at all places $v \,|\, n$.*
(iii) $e(K_v/\mathbb{Q}_p) < p - 1$ *for all places $v \,|\, n$.*

Then

$$B(K)/nB(K) \hookrightarrow \mathrm{Vis}_J\,\text{Ш}(A/K).$$

Proof: (Sketch.) We recall that a cohomology class in $H^i(K_v, M)$ is unramified if it is in the kernel of the restriction map to $H^i(K_v^{\mathrm{nr}}, M)$, where K_v^{nr} is the maximal unramified extension of K_v. We write $A^0(K_v)$ for the subgroup of $A(K_v)$ consisting of points whose reduction mod v belong to the identity component of the special fibre of the Néron model.

The following three facts are established in [1].

(1) The unramified subgroup of $H^1(K_v, A)$ has order equal to the Tamagawa number $c_v(A) = [A(K_v) : A^0(K_v)]$.

(2) If $v \nmid n$ then $B^0(K_v^{\mathrm{nr}}) \xrightarrow{\times n} B^0(K_v^{\mathrm{nr}})$ is surjective.

(3) If J has good reduction at v and $e(K_v/\mathbb{Q}_p) < p - 1$ then $J(K_v^{\mathrm{nr}}) \to B'(K_v^{\mathrm{nr}})$ is surjective.

Assuming these facts, we complete the proof of the proposition. It suffices to show that for each place v of K, the map π in the diagram

$$\begin{tikzcd}
B(K_v) \arrow[r, "\times n"] \arrow[d] & B(K_v) \arrow[r] \arrow[d, "\tau"'] \arrow[dr, "\pi"] & H^1(K_v, B[n]) \arrow[d] \\
J(K_v) \arrow[r] & B'(K_v) \arrow[r] & H^1(K_v, A)
\end{tikzcd}$$

is the zero map. It is clear that the image of π is killed by multiplication by n. So by (1) and our hypothesis on the Tamagawa numbers of A, it suffices to show that every ξ in the image of π is unramified. This follows by (2) if $v \nmid n$ and by (3) if $v \mid n$. This is seen by a diagram chase that takes place in the above diagram and its analogue with K_v replaced by K_v^{nr}.

Finally we note that by hypothesis (iii), n is odd. So there is nothing to check at the infinite places. □

8. Examples

We end with a demonstration using Magma [5].

Example 1. (This is the first example in Table 1 of [13].) We start by computing the space of modular forms of weight 2 for $\Gamma_0(681)$. This is done using *modular symbols*, as described in [12], [26].

```
>M := ModularSymbols(681);
>N := NewSubspace(CuspidalSubspace(M));
>D := SortDecomposition(NewformDecomposition(N));
```

The new part of the modular Jacobian $J = J_0(681)$ determines abelian varieties of the following dimensions.

```
> [Dimension(x)/2:  x in D];
[ 1, 1, 1, 1, 1, 6, 6, 10, 10 ]
```

Each conjugacy class of newforms determines both a subvariety and a quotient of J. (These are dual abelian varieties, so equal in the case of an elliptic curve.) We always work with the subvarieties.

```
> [CremonaReference(EllipticCurve(D[i])):i in [1..5]];
[ 681a1, 681b1, 681c1, 681d1, 681e1 ]
> CD := CremonaDatabase();
> E := EllipticCurve(CD,"681b1");E;
Elliptic Curve defined by $y^2 + xy = x^3 + x^2 - 1154x -$
15345 over Rational Field
> F := EllipticCurve(CD,"681c1");F;
Elliptic Curve defined by $y^2 + y = x^3 - x^2 + 2$ over
Rational Field
```

The intersection of E and F inside $J_0(681)$ can be computed using modular symbols, as described in [2].

```
> IntersectionGroup(D[2],D[3]);
Abelian Group isomorphic to Z/3 + Z/3
Defined on 2 generators
Relations:
  3*$.1 = 0
  3*$.2 = 0
```

So $E[3]$ and $F[3]$ are isomorphic as Galois modules. (We say that E and F are 3-congruent.)

```
> AnalyticRank(E);
0 1.8448
> AnalyticRank(F);
2 1.0263
> MW,MWmap := MordellWeilGroup(F);MW;
Abelian Group isomorphic to Z + Z
Defined on 2 generators (free)
> [#TorsionSubgroup(A) : A in IsogenousCurves(E)];
[ 2, 4, 4, 2 ]
> [#TorsionSubgroup(A) : A in IsogenousCurves(F)];
[ 1 ]
```

We can now apply Proposition 7.1 with $A = E$, $B = F$ and $n = 3$. It follows that $F(\mathbb{Q})/3F(\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$ injects into $H^1(\mathbb{Q}, E)$. It is natural to ask whether these might be elements of the Tate-Shafarevich group. The value of $\#\text{Ш}(E/\mathbb{Q}). \operatorname{Reg}(E(\mathbb{Q}))$ predicted by the Birch–Swinnerton-Dyer conjecture is

```
> ConjecturalRegulator(E);
9.00000000000000000000000000000 0
```

Since E has rank 0, the regulator is 1. So there certainly should be a copy of $(\mathbb{Z}/3\mathbb{Z})^2$ inside $\text{Ш}(E/\mathbb{Q})$. But we still have to check local solubility before we can be certain this is the subgroup we found. The Tamagawa numbers of an elliptic curve are computed by Tate's algorithm.

```
> BadPrimes(E);
[ 3, 227 ]
> TamagawaNumbers(E);
[ 2, 2 ]
> TamagawaNumbers(F);
[ 2, 1 ]
```

So by Proposition 7.2 (or rather its proof) local solubility is guaranteed at all primes, except possibly for $p = 3$.

We check local solubility at $p = 3$ by using Lemma 6.3 to write the visible elements of $H^1(\mathbb{Q}, E)$ as plane cubics. First we compute the Hesse pencil of F (embedded as a plane cubic in $\mathbb{P}^2$ via $|3.0|$).

```
> P<t> := PolynomialRing(Rationals());
> U := GenusOneModel(3,F);U;
Genus one model of degree 3 defined over Rational Field
given by $-x^3 + x^2z + y^2z + yz^2 - 2z^3$
> H := Hessian(U);H;
Genus one model of degree 3 defined over Rational Field
given by $4x^2z-12xy^2-12xyz-84xz^2+4y^2z+4yz^2+28z^3$
> vecU := Vector(P,Eltseq(U));
> vecH := Vector(P,Eltseq(H));
> HessePencil := GenusOneModel(3,Eltseq(t*vecU+vecH));
> HessePencil;
Genus one model of degree 3 defined over Univariate
Polynomial Ring in t over Rational Field given by
$-tx^3 + (t + 4)x^2z - 12xy^2 - 12xyz - 84xz^2 + (t + 4)y^2z$
$+ (t + 4)yz^2 + (-2t + 28)z^3$
```

Classical invariant theory give a formula (see [3]) for the Jacobian of a plane cubic. Since the above family has a section we are really only using this formula to re-write this family in the Weierstrass form $y^2 = x^3 - 27c_4x - 54c_6$.

```
> c4,c6,Delta := Invariants(HessePencil);
> c4;
$16t^4 - 7520t^3 + 1536t^2 - 120320t + 14125312$
> c6;
$-1880t^6 + 1536t^5 - 451200t^4 + 70688000t^3 - 7219200t^2 -$
$677425152t + 53088071680$
```

Alternatively, we can compute these invariants directly from F (using some formulae I contributed to Magma).

```
> DD,cc4,cc6 :=
> HessePolynomials(3,1,cInvariants(F):Variables := [t,1]);
> [c4,c6,Delta] eq [cc4,cc6,Discriminant(F)*DD∧3];
true
```

Can we find E in the Hesse pencil of F?

```
> poly := c4∧3 - jInvariant(E)*Delta;
> Roots(poly);
[]
```

Apparently not! The problem is that the isomorphism $E[3] \cong F[3]$ does not respect the Weil pairing. One solution is to use the contravariants P, Q in place of the covariants U, H. (See [14] for details.) An alternative, that works in this case, is to switch to a 2-isogenous curve.

```
> E1 := EllipticCurve(CD,"681b4");
> flag,isog := IsIsogenous(E,E1);flag,Degree(isog);
true 2
> poly := c4∧3 - jInvariant(E1)*Delta;
> rts := Roots(poly); rts;
[ <12, 1> ]
```

We have now found a member of the Hesse pencil of F isomorphic to E_1. (Although so far we have only checked they have the same j-invariant.) We pick some representatives for $F(\mathbb{Q})/3F(\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$

```
> pts := [MWmap(MW!x):x in [[1,0],[0,1],[1,1],[1,-1]]];
```

and compute their images under the map $F(\mathbb{Q})/3F(\mathbb{Q}) \to H^1(\mathbb{Q}, E)$.

```
> for pt in pts do
for> print "pt =",pt;
for> D := 2*Divisor(F!0) + Divisor(pt);
for> U := GenusOneModel(Image(DivisorMap(D)));
for> U := Reduce(Minimise(U));
for> assert cInvariants(U) eq cInvariants(F);
for> H := Hessian(U);
for> vecU := Vector(Eltseq(U));vecH := Vector(Eltseq(H));
for> V := GenusOneModel(3,Eltseq(rts[1][1]*vecU + vecH));
for> V := Reduce(Minimise(V));
for> assert IsIsomorphic(Jacobian(V),E1);
for> print Equation(V);
for> assert IsLocallySolvable(Curve(V),3);
for> end for;
pt = (-1 :  0 :  1)
```

$$x^3 - x^2z + 7xy^2 - 3xyz - 3xz^2 - y^3 - y^2z - yz^2 - 10z^3$$

```
pt = (6 :  13 :  1)
```

$x^3-4x^2y-2x^2z-4xy^2-xyz+3xz^2-3y^3-4y^2z+9yz^2-9z^3$

```
pt = (-27/49 :  -629/343 :  1)
```

$-x^3-3x^2y+x^2z+2xy^2-5xyz-3xz^2-5y^3-7y^2z-16yz^2-8z^3$

```
pt = (0 :  1 :  1)
```

$x^3-4x^2z+4xy^2-9xyz+4xz^2-3y^3-3yz^2-9z^3$

We have now checked local solubility at $p=3$. Mazur does this in a more high-brow way (using flat cohomology) as described in the appendix to [2].

Example 2. (This is the second example in Table 1 of [13].) We consider the following two elliptic curve from the Cremona database.

```
> E := EllipticCurve(CD,"1058d1");
> F := EllipticCurve(CD,"1058c1");
> AnalyticRank(E);
0 2.4854
> ConjecturalRegulator(E);
25.0000000000000000000000000000 0
```

In fact E is the first elliptic curve (by conductor) with no rational 5-isogeny that is predicted to have an element of order 5 in its Tate-Shafarevich group. Conveniently there is a rank 2 curve at the same level (namely F) that can be used to explain the 5-torsion in Ш$(E/\mathbb{Q})$. It is a mystery why accidents like this, as catalogued in [13], happen so often.

```
> MW,MWmap := MordellWeilGroup(F); MW;
Abelian Group isomorphic to Z + Z
Defined on 2 generators (free)
```

We check for a 5-congruence by using the analogue of the Hesse family in degree 5. (See [14] for details.)

```
> DD,c4,c6 :=
> HessePolynomials(5,1,cInvariants(F):Variables := [t,1]);
> poly := c4∧3 - jInvariant(E)*Discriminant(F)*DD∧5;
> rts := Roots(poly);rts;
[ <-23, 1> ]
> E1 := EllipticCurve([Evaluate(x,rts[1][1])
                              :  x in [-27*c4,-54*c6]]);
> IsIsomorphic(E,E1);
true
```

We have found E in the Hesse pencil of F. So $E[5]$ and $F[5]$ are isomorphic as Galois modules.

```
> [#TorsionSubgroup(A) : A in IsogenousCurves(E)];
[ 1 ]
> [#TorsionSubgroup(A) : A in IsogenousCurves(F)];
[ 1, 1 ]
```

```
> BadPrimes(E);
[ 2, 23 ]
> TamagawaNumbers(E);
[ 1, 1 ]
> TamagawaNumbers(F);
[ 2, 1 ]
```

So by Propositions 7.1 and 7.2 the group $F(\mathbb{Q})/5F(\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^2$ injects into Ш$(E/\mathbb{Q})$. We can also give equations for these elements of Ш exactly as in Example 1, by using my degree 5 analogue of the Hessian, as described in [14]. (However, the functions to minimise and reduce genus one models of degree 5 are not yet in Magma.)

Example 3. We start with the elliptic curves E and F where

```
> E := EllipticCurve(CD,"3364c1");E;
Elliptic Curve defined by y^2 = x^3-4062871x-3152083138
over Rational Field
> F := EllipticCurve(CD,"10092c1");F;
Elliptic Curve defined by y^2 = x^3-x^2-42330x+3568581
over Rational Field
> AnalyticRank(E);
0 5.2106
> ConjecturalRegulator(E);
49.0000000000000000000000000000 0
```

In [13] the 7-torsion of Ш$(E/\mathbb{Q})$ is listed as invisible, since E is not congruent modulo 7 to any curve of conductor ≤ 5500 (the range of Cremona's tables at that time). We show that it is explained by a rank 2 curve (namely F) with conductor 3 times that of E.

```
> MW,MWmap := MordellWeilGroup(F);MW;
Abelian Group isomorphic to Z + Z
Defined on 2 generators (free)
```

The modular forms attached to E and F are

```
> fE := ModularForm(E);SetPrecision(Parent(fE),15);fE;
q + 3q^3 + 3q^5 + 4q^7 + 6q^9 + q^11 - 3q^13 + O(q^15)
> fF := ModularForm(F);SetPrecision(Parent(fF),15);fF;
q - q^3 - 4q^5 - 3q^7 + q^9 + q^11 - 3q^13 + O(q^15)
```

They seem to satisfy a 7-congruence.

```
> function SturmBound(N)
function> ff := Factorization(N);
function> prod := &*[q∧r + q∧(r-1)
                  where q,r is Explode(f):  f in ff];
function> return prod/6;
function> end function;
> SturmBound(10092);
```

```
3480
> aE := TracesOfFrobenius(E,3500);
> bE := TracesOfFrobenius(F,3500);
> [i :  i in [1..#aE] | (aE[i] - bE[i]) mod 7 ne 0];
[ 2 ]
```

From these calculations it follows (specifically by checking the conditions specified in [16]) that $E[7]$ and $F[7]$ are equal in $J_0(10092)$.

```
> #IsogenousCurves(E), #IsogenousCurves(F);
1 1
> BadPrimes(E);
[ 2, 29 ]
> TamagawaNumbers(E);
[ 1, 2 ]
> TamagawaNumbers(F);
[ 1, 1, 4 ]
```

So by Propositions 7.1 and 7.2 the group $F(\mathbb{Q})/7F(\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^2$ injects into $\text{Ш}(E/\mathbb{Q})$.

Example 4. This is a higher dimensional example, taken from [25] (see also [1],[2]).

```
> M := ModularSymbols(389);
> N := NewSubspace(CuspidalSubspace(M));
> D := SortDecomposition(NewformDecomposition(N));
> [Dimension(x)/2:  x in D];
[ 1, 2, 3, 6, 20 ]
> A := D[5]; B := D[1];
```

So A and B are abelian varieties of dimensions 20 and 1 inside $J_0(389)$.

```
> WeqnB := EllipticCurve(B);WeqnB;
Elliptic Curve defined by $y^2 + y = x^3 + x^2 - 2x$ over
Rational Field
> CremonaReference(WeqnB);
389a1
> MW,MWmap := MordellWeilGroup(WeqnB);MW;
Abelian Group isomorphic to Z + Z
Defined on 2 generators (free)
```

The intersection of A and B inside $J_0(389)$ is computed using modular symbols.

```
> IntersectionGroup(A,B);
Abelian Group isomorphic to Z/20 + Z/20
Defined on 2 generators
Relations:
  20*$.1 = 0
  20*$.2 = 0
```

Reducing modulo some small primes (up to 7) gives some bounds on $\#A(\mathbb{Q})_{\rm tors}$ and $\#B(\mathbb{Q})_{\rm tors}$.

```
> TorsionBound(A,7);
97
> TorsionBound(B,7);
1
```

These bounds also apply to any abelian varieties isogenous to A or B.

```
> TamagawaNumber(A,389);
97
> TamagawaNumber(B,389);
1
```

The hypotheses of Propositions 7.1 and 7.2 are now satisfied with $n = 5$. It follows that $B(\mathbb{Q})/5B(\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^2$ injects into $\text{Ш}(A/\mathbb{Q})$. Since $\dim(A) = 20$ there is no chance of giving equations!

References

[1] A. Agashé and W. Stein, Visibility of Shafarevich-Tate groups of abelian varieties, *J. Number Theory* **97** (2002), no. 1, 171–185.

[2] A. Agashé and W. Stein, Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero, with an appendix by J. Cremona and B. Mazur, *Math. Comp.* **74** (2005), no. 249, 455–484.

[3] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis, Jacobians of genus one curves, *J. Number Theory* **90** (2001), no. 2, 304–315.

[4] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[5] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comb.* **24**, 235-265 (1997).
`http://magma.maths.usyd.edu.au/magma/`

[6] N. Bruin, Visualising $\text{Ш}[2]$ in abelian surfaces, *Math. Comp.* **73** (2004), no. 247, 1459–1476.

[7] N. Bruin and E.V. Flynn, Exhibiting $\text{Ш}[2]$ on hyperelliptic Jacobians, *J. Number Theory* **118** (2006), no. 2, 266–291.

[8] J.W.S. Cassels, Arithmetic on curves of genus 1, V. Two counterexamples, *J. London Math. Soc.* **38** 1963 244–248.

[9] J.W.S. Cassels, *Lectures on elliptic curves*, LMS Student Texts 24, Cambridge University Press, Cambridge, 1991.

[10] P.L. Clark, The period-index problem in WC-groups, I. Elliptic curves, *J. Number Theory* **114** (2005), no. 1, 193–208.

[11] P.L. Clark, *Period-index problems in WC-groups II: abelian varieties*, preprint.

[12] J.E. Cremona, Algorithms for modular elliptic curves, Second edition, Cambridge University Press, Cambridge, 1997.

[13] J.E. Cremona and B. Mazur, Visualizing elements in the Shafarevich-Tate group, *Experiment. Math.* **9** (2000), no. 1, 13–28.

[14] T.A. Fisher, *The Hessian of a genus one curve*, preprint.
`http://arxiv.org/abs/math/0610403`

[15] D.P. Jetchev, *Visibility of Shafarevich-Tate Groups.* `http://modular.math.washington.edu/projects/`

[16] D.P. Jetchev and W.A. Stein, Visibility of the Shafarevich-Tate group at higher level, *Doc. Math.* **12** (2007), 673–696.

[17] T.A. Klenke, Visualizing elements of order two in the Weil-Châtelet group, *J. Number Theory* **110** (2005), no. 2, 387–395.

[18] S. Lang and J. Tate, Principal homogeneous spaces over abelian varieties. *Amer. J. Math.* **80** 1958 659–684.

[19] S. Lichtenbaum, The period-index problem for elliptic curves. *Amer. J. Math.* **90** 1968 1209–1223.

[20] B. Mazur, Visualizing elements of order three in the Shafarevich-Tate group, *Asian J. Math.* **3** (1999), no. 1, 221–232.

[21] J.R. Merriman, S. Siksek, and N.P. Smart, Explicit 4-descents on an elliptic curve, *Acta Arith.* **77** (1996), no. 4, 385–404.

[22] J.S. Milne, Abelian varieties, in *Arithmetic geometry*, G. Cornell and J.H. Silverman (eds.), 103–150, Springer, New York, 1986.

[23] J.S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, **1**, Academic Press, Inc., Boston, MA, 1986.

[24] C. O'Neil, The period-index obstruction for elliptic curves, *J. Number Theory* **95** (2002), no. 2, 329–339.

[25] W.A. Stein, Studying the Birch and Swinnerton-Dyer conjecture for modular abelian varieties using Magma, *Discovering mathematics with Magma*, 93–116, Algorithms Comput. Math., **19**, Springer, Berlin, 2006.

[26] W.A. Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, **79**, American Mathematical Society, Providence, RI, 2007.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`