TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 352, Number 10, Pages 4533–4555
S 0002-9947(00)02368-0
Article electronically published on June 8, 2000

# EXAMPLES OF TORSION POINTS ON GENUS TWO CURVES

JOHN BOXALL AND DAVID GRANT

Abstract. We describe a method that sometimes determines all the torsion points lying on a curve of genus two defined over a number field and embedded in its Jacobian using a Weierstrass point as base point. We then apply this to the examples $y^2 = x^5 + x$, $y^2 = x^5 + 5\,x^3 + x$, and $y^2 - y = x^5$.

## Introduction

Let $C$ be a complete nonsingular curve of genus $g \geq 2$ defined over a field $k$ and let $J$ be the Jacobian variety of $C$. When $k$ is of characteristic zero, Manin and Mumford conjectured that for any embedding of $C$ in $J$, the set of torsion points lying on the image of $C$ is finite. This was proved by Raynaud [R1] in 1983. Later, new proofs and generalizations were given by Raynaud [R2], Coleman [C3], Hindry [H] and, in 1996, separately by David and Philippon [DaPh] and by Ullmo [U], following previous work of Szpiro and Zhang on Bogomolov's small point conjecture. Given a fixed embedding of $C$ in $J$, it is natural to ask whether one can determine explicitly the finite set in question. The first cases where this was possible were studied by Coleman [C1], [C2]. In [C1] he obtained a bound on the cardinality in the case where $C$ is defined over a number field $k$ and $J$ has complex multiplication. Let $J_{\mathrm{tors}}$ denote the torsion points of $J$ defined over an algebraic closure $\overline{k}$ of $k$.

**(0.1) Theorem (Coleman).** *Let $k$ be a number field, and let $C$ be a complete non-singular curve of genus $g \geq 2$ defined over $k$. Let $J$ be the Jacobian of $C$, and identify $C$ with its image in $J$ under a fixed embedding. Suppose that $J$ has complex multiplication and that $v$ is an unramified prime of $k$ at which $C$ has good ordinary reduction. Suppose that the rational prime $p$ below $v$ is at least 5. Then*

$$\#\big(C(\overline{k}) \cap J_{\mathrm{tors}}\big) \leq pg.$$

In a recent paper, Buium [B] obtains a weaker bound without the hypothesis of complex multiplication. He shows that, if $p \geq 2g + 1$, $J$ is arbitrary, and the other hypotheses are as in (0.1) except that the good reduction at $v$ need not be ordinary, then

$$\#\big(C(\overline{k}) \cap J_{\mathrm{tors}}\big) \leq p^{3g}\, 3^g\, g!\, \big(p(2g-2) + 6g\big).$$

Received by the editors October 6, 1997 and, in revised form, April 18, 1998.
2000 *Mathematics Subject Classification.* Primary 11G30, 14H25.
*Key words and phrases.* Curves of genus two, elliptic curves, torsion, Galois representations.
The first author was enjoying the hospitality of the University of Colorado at Boulder while the paper was completed. The second author was supported by NSF DMS–930322 and was enjoying the hospitality of the University of Caen while conducting part of this research.

(Buium has $p^{4g}$ in place of our $p^{3g}$, but one can obtain the improvement by noting that, in the notation of page 356 of [B], one in fact has $\#(\Gamma/p\Gamma) \leq p^g$ and not just $\#(\Gamma/p\Gamma) \leq p^{2g}$, because of the Weil pairing.)

One can use Coleman's ideas to prove the following.

**(0.2) Theorem.** *Let $C$ be the genus two curve over $\mathbb{Q}$ with affine model $y^2 - y = x^5$, and let $\Theta$ be the Albanese embedding of $C$ in $J$ whose base point is the point $\infty$ at infinity. Then $\Theta(\overline{\mathbb{Q}}) \cap J_{\text{tors}}$ consists of the eighteen points which are images of the points $\infty$, $(\alpha, 1/2)$ with $\alpha^5 = -1/4$, the points $(0,0)$ and $(0,1)$, together with the points $(\zeta^i, (1+\sqrt{5})/2)$ and $(\zeta^i, (1-\sqrt{5})/2)$, where $\zeta$ is a primitive fifth root of unity and $1 \leq i \leq 5$.*

Recall that if $C$ is a complete non-singular curve of genus $g \geq 1$ over $k$, and $J$ its Jacobian variety, then $J(\overline{k})$ is naturally isomorphic to the group $\text{Pic}_0(C)$ of divisors of degree zero on $C$ modulo principal divisors. If $P_0$ is a point on $C$, the Albanese embedding of $C$ in $J$ with base point $P_0$ is the embedding corresponding to the map that sends $P$ to the class of the divisor $P - P_0$. For more details in the case we are interested in, see the discussion after (1.4).

The result (0.2) is explicitly stated at the end of [C2], and it can also be deduced from (0.1) (see the remark at the end of §5). The points $(\alpha, 1/2)$ are of order two while $(0,0)$, $(0,1)$, and those of the form $(\zeta^i, (1 \pm \sqrt{5})/2)$ are of order five. Some further properties and applications of the points of order five are to be found in [G1] and [G2]. Note that $y^2 - y = x^5$ is a quotient of the Fermat curve $X^5 + Y^5 = 1$. Very recently, Coleman, Tamagawa and Tzermias [CTT] have determined, for all $N \geq 5$, the torsion on the image of the Fermat curve $X^N + Y^N = 1$ in its Jacobian under the Albanese embedding with $(1,0)$ as base point. They did so by studying the torsion on non-hyperelliptic images of Fermat curves embedded in their Jacobians. Similar results for hyperelliptic images have recently been obtained by Shaulis [Sha]. See the work of Coleman, Kaskel, and Ribet [CKR] for progress on modular curves. A model theoretic approach to these questions is discussed in [P].

The purpose of this paper is to explain a method that sometimes permits one to determine all the torsion lying on the image of a genus two curve, defined over a number field $K$, embedded in its Jacobian using a Weierstrass point as base point. Unlike Coleman's method, which depends on his theory of $p$-adic integration developed in [C1], our method depends only on having a good knowledge of the Galois groups over $K$ of the fields generated by torsion points of the Jacobian. The first person to establish a relation between the Manin-Mumford conjecture and these Galois groups was Lang [L]. His ideas were later taken up by Hindry [H], and in [CTT]. Thus, our paper can be viewed as an explicit working out of these ideas in the simplest case. In the same vein, we have tried to keep the paper as elementary and self-contained as possible. In particular, it is independent of the results of Coleman and Buium.

To describe the paper in greater detail, let $C$ be a complete nonsingular curve of genus 2 defined over $K$. We assume that $C$ has a Weierstrass point defined over $K$, so that $C$ has an affine model of the form $y^2 + q(x)y = p(x)$, where $p$, $q$ are polynomials with coefficients in $K$ with $p$ of degree five and $q$ of degree at most two. The Weierstrass point can then be taken to be the point at infinity, which we denote by $\infty$. As in (0.2), let $\Theta$ be the image of $C$ in $J$ via the Albanese embedding with base point $\infty$. Let $O_J$ be the origin of $J$ and, for any natural number $N$, write $J_N$ for the group of $N$-torsion points of $J$ defined over $\overline{K}$.

In §1 we recall some basic properties of $C$ and $J$. We use these in (1.6) and (1.7) to deduce explicit results about $J_{\text{tors}} \cap \Theta(\overline{K})$ from the action of the Galois group of $\overline{K}$ over $K$ on $J_{\text{tors}}$. In our computation, we reduce the study of $J_{\text{tors}} \cap \Theta(\overline{K})$ to that of $J_N \cap \Theta(\overline{K})$ for some fixed $N$, and we discuss in §2 how one can compute the latter intersection.

We illustrate the method by proving the following results in §§3 and 4.

**(0.3) Theorem.** *Let $C$ be the curve over $\mathbb{Q}$ with affine model $y^2 = x^5 + x$. Then $\Theta(\overline{\mathbb{Q}}) \cap J_{\text{tors}}$ consists of the twenty-two points which are the images of $\infty$ together with the images of the points whose $x$-coordinate is a root of $x^5 + x$, or $x^4 + 4\,x^2 + 1$, or $x^4 - 4\,x^2 + 1$.*

In this case the Weierstrass points are $\infty$ together with the points whose $x$-coordinate is a root of $x^5 + x$. The images of the remaining points are of order six. This can also be deduced from Coleman's results (see the remark at the end of §3). In the following, however, the Jacobian does not have complex multiplication.

**(0.4) Theorem.** *Let $C$ be the curve with affine model $y^2 = x^5 + 5\,x^3 + x$. Then $\Theta(\overline{\mathbb{Q}}) \cap J_{\text{tors}}$ consists of the images of the Weierstrass points, that is, $O_J$ and the images of the points whose $x$-coordinate is a root of $x^5 + 5\,x^3 + x$.*

This does not seem to follow readily from Buium's bound given above, in which one can take $p = 5$ and $g = 2$.

In the final §5 we shall show that our method can be applied to give a new proof of (0.2).

As Coleman observes in [C1], page 155, the genus 2 modular curve $X_1(13)$ has at least twenty-two torsion points on its image in its Jacobian via an Albanese embedding with base point one of its cusps. At present, no genus two curve seems to be known having more than twenty-two torsion points when embedding in its Jacobian, so that $X_1(13)$ and the curve (0.3) would seem to hold the record for the moment. At the other end of the spectrum, $\Theta$ always contains the six elements of $J_2$ which are the images of the Weierstrass points. Yet, (0.4) seems to be the first known explicit example of such a genus two curve over $\mathbb{Q}$.

*Notation.* We let $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ denote the natural numbers, the integers, and the rational numbers. For every $N \in \mathbb{N}$ we let $\mathbb{Z}_N = \varprojlim \mathbb{Z}/N^n\mathbb{Z}$. If $R$ is a commutative ring with identity, we denote the group of units of $R$ by $R^*$. We let $O_A$ denote the origin of an Abelian variety $A$. We write $A_{\text{tors}}$ for the group of torsion points over an algebraic closure of the field over which $A$ is defined. For an integer $N$, we let $A_N$ denote the points of order $N$ in $A_{\text{tors}}$, and set $A_{N^\infty} = \bigcup_{n \geq 0} A_{N^n}$. We define the Tate module by $T_N = T_N(A) = \varprojlim A_{N^n}$.

## 1. The action of the Galois group

Let $k$ be a field, let $\overline{k}$ be an algebraic closure of $k$, and denote by $G_k$ the Galois group of $\overline{k}$ over $k$. Let $C$ be a complete nonsingular curve of genus two defined over $k$. We assume that there is a Weierstrass point of $C$ defined over $k$. Then $C$ has an affine model

$$y^2 + q(x)y = p(x), \tag{1.1}$$

where $p(x)$, $q(x) \in k[x]$, with $p$ of degree five and $q$ of degree at most two. Furthermore, one can suppose $p$ to be monic. When the characteristic of $k$ is different from

two, (1.1) defines a genus two curve if and only if $p(x) + q(x)^2/4$ has no repeated root. See [I] for more details.

Let $\infty$ denote the point at infinity on this model of $C$. Every point of $C(\overline{k})$ other than $\infty$ is represented by a point on the affine curve (1.1). The hyperelliptic involution $\iota$ fixes $\infty$ and sends the point $(x, y)$ on (1.1) to $(x, -y - q(x))$. Every effective canonical divisor on $C$ is of the form $\xi + \iota(\xi)$ for some point $\xi$ on $C$. In what follows, one should keep in mind that the Weierstrass points of $C$ are the set of points stable under $\iota$, that is, they are the set of points $\xi \in C(\overline{k})$ such that $2\,\xi$ is a canonical divisor.

Let $J$ be the Jacobian variety of $C$. Recall that $\mathrm{Pic}_0(C)$ is the group of divisors on $C$ over $\overline{k}$ of degree zero modulo linear equivalence. Then $J$ is an Abelian surface defined over $k$ whose group of points $J(\overline{k})$ defined over $\overline{k}$ is canonically $G_k$-isomorphic to the group $\mathrm{Pic}_0(C)$. Let $D^{(2)}$ be the set of effective divisors of degree two on $C$ that are defined over $\overline{k}$. We henceforth identify $\mathrm{Pic}_0(C)$ and $J(\overline{k})$ via this isomorphism, and define a map $\pi : D^{(2)} \to J(\overline{k})$ by

$$\pi(\xi + \eta) = \mathrm{cl}\,(\xi + \eta - \kappa), \tag{1.2}$$

where cl is the class of the divisor modulo linear equivalence, and $\kappa$ is a canonical divisor. We write $O_J$ for the origin of $J$. The following result is a statement of the Abel-Jacobi theorem for genus two curves.

**(1.3) Theorem.** *Let $\tilde{D}$ be the set of canonical divisors in $D^{(2)}$. Then the map $\pi$ is surjective, $G_k$-equivariant, and induces a bijection from the complement of $\tilde{D}$ in $D^{(2)}$ onto $J(\overline{k})\backslash\{O_J\}$. We have $\pi(\tilde{D}) = O_J$.*

It follows from (1.3) that if $P$ is any non-zero point of $J(\overline{k})$, there exists a unique pair $\{\xi_P, \eta_P\}$ of points of $C(\overline{k})$ such that $\pi(\xi_P + \eta_P) = P$. Since $\pi$ is $G_k$-equivariant we deduce that $P$ is defined over the field of definition $k(\xi_P, \eta_P)$ of $\xi_P$ and $\eta_P$. We also have the following.

**(1.4) Corollary.** *Let $P$ be a non-zero point of $J(\overline{k})$. Then the extension of fields $k(\xi_P, \eta_P)/k(P)$ is of degree at most two. When it is of degree two, the points $\xi_P$ and $\eta_P$ are conjugate over $k(P)$.*

We now let $\Theta$ be the image of $C$ in $J$ by the map $\epsilon$ that sends the point $\xi$ to the class of the divisor $\xi - \infty$. This map is an embedding defined over $k$. In terms of $\pi$ we have $\epsilon(\xi) = \pi(\xi + \infty)$. We need the following proposition.

**(1.5) Proposition.** *Let $P \in J(\overline{k})$. Then:*
*(a) The origin $O_J \in \Theta(\overline{k})$.*
*(b) If $P \in \Theta(\overline{k})$, then $-P \in \Theta(\overline{k})$.*
*(c) If $P \in \Theta(\overline{k})$, then $2P$ and $-2P$ do not belong to $\Theta(\overline{k})$ except when $2P = O_J$.*
*(d) If $P \in \Theta(\overline{k})$, then $3P$ and $-3P$ do not belong to $\Theta(\overline{k})$ except when $2P = O_J$.*

*Proof.* (a) This is clear since $O_J = \epsilon(\infty)$.

(b) If $P = \epsilon(\xi)$, then $-P = \epsilon(\iota(\xi))$ since $\xi + \iota(\xi) - 2\infty$ is the divisor of the function $x - x(\xi)$.

(c) It suffices to treat the case of $2P$, since the assertion for $-2P$ will then follow from (b). Write $P = \epsilon(\xi)$ with $\xi \in C(\overline{k})$. If $2P \in \Theta(\overline{k})$, then $2P = \epsilon(\eta)$ for some $\eta \in C(\overline{k})$, and $2\,\xi - 2\infty$ and $\eta - \infty$ are linearly equivalent. Hence $2\xi$ and $\eta + \infty$ are linearly equivalent. By (1.3) we get that $\xi = \iota(\xi)$, so $2P = O_J$.

($d$) This is similar to ($c$). Again it suffices to treat the case of $3P$, and we write $P = \epsilon(\xi)$ with $\xi \in C(\overline{k})$. If $3P \in \Theta(\overline{k})$, then we can write $3P = \epsilon(\eta)$ with $\eta \in C(\overline{k})$, and the divisors $2\xi$ and $\eta + \iota(\xi)$ are linearly equivalent. By (1.3) we again get that $\xi = \iota(\xi)$, so $2P = O_J$. □

As an abstract group, $J_N$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^4$ when $N$ is prime to the characteristic of $k$, and since this is the only case we need, we make this hypothesis from now on. We shall be interested in $J_N$ as a $G_k$-module. The reason for this will be clear from the following two corollaries, which are the starting point of our study of torsion points lying on $\Theta$.

**(1.6) Corollary.** ($a$) *Let $N$ be an odd integer. If there exists $\sigma \in G_k$ such that $\sigma(P) = 2P$ for all $P \in J_N$ (or $\sigma(P) = -2P$ for all $P \in J_N$), then $\Theta(\overline{k}) \cap J_N = \{O_J\}$.*

($b$) *Let $N$ be an integer that is not divisible by three. If there exists $\sigma \in G_k$ such that $\sigma(P) = 3P$ for all $P \in J_N$ (or $\sigma(P) = -3P$ for all $P \in J_N$), then $\Theta(\overline{k}) \cap J_N \subseteq J_2$.*

This follows at once from (1.5$c$) and (1.5$d$).

**(1.7) Corollary.** *Let $P \in \Theta(\overline{k})$. For all $\sigma \in G_k$ such that $\sigma(P) \neq P$, the field extension $k(P, \sigma(P))/k(\sigma(P) - P)$ is of degree at most two.*

This is a consequence of (1.4).

We can now summarize the general strategy for our determination of $\Theta(\overline{k}) \cap J_{\text{tors}}$, assuming a good knowledge of the action of $G_k$ on $J_{\text{tors}}$. From the assumption of a point of order $N$ lying on $\Theta(\overline{k})$, we try to show that there are homotheties for the action of $G_k$ on $J_{\text{tors}}$ that will provide geometric contradictions coming from (1.6), or arithmetic contradictions coming from (1.7). In order to do this, it will be crucial to show that there is an extension $k'$ of $k$, over which $k'(J_N)$ and $k'(J_M)$ are linearly disjoint for $M$ and $N$ coprime.

We end this section with a result describing some properties of fields generated by torsion points of general Abelian varieties. This will help to simplify some of the calculations in §§3, 4 and 5. Clearly $k(A_{MN}) = k(A_M)k(A_N)$ when $M$ and $N$ are coprime. If $\phi : A \to B$ is an isogeny of Abelian varieties, then $k(A_N) \neq k(B_N)$ in general, but these fields are the same if $N$ is coprime to the degree of $\phi$, in which case the representations of $G_k$ on $A_N$ and $B_N$ are isomorphic. We denote by $\text{Hty}(A, k, N)$ the subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ defined as the residues (mod $N$) of those $a \in \mathbb{Z}$ for which there exists $\sigma \in G_k$ such that $\sigma(P) = aP$ for all $P \in A_N$. (Here Hty stands for homothety.) Similarly, $G_k$ acts on $k(A_{N^\infty})$ and on the Tate module $T_N(A)$. We write $\text{Hty}(A, k, N^\infty)$ for the group of $a \in \mathbb{Z}_N^*$ for which there exists $\sigma \in G_k$ such that $\sigma(P) = aP$ for all $P \in A_{N^\infty}$ (or for all $P \in T_N(A)$, the two definitions being equivalent).

**(1.8) Proposition.** *Let $A$ be an Abelian variety over $k$. Then:*

($a$) *Let $N \in \mathbb{N}$. Then the field $k(A_{N^\infty})$ depends only on the $k$-isogeny class of $A$.*

($b$) *Let $M$, $N \in \mathbb{N}$ be coprime. Then the property that $k(A_{M^\infty})$ and $k(A_{N^\infty})$ are linearly disjoint over $k$ depends only on the $k$-isogeny class of $A$ (the assertion makes sense because of ($a$)).*

(*c*) *Let $M$, $N \in \mathbb{N}$ be coprime and such that $k(A_M)$ and $k(A_N)$ are linearly disjoint over $k$. If $a \in \mathbb{Z}$ is prime to $MN$, $a \in \mathrm{Hty}(A,k,M)$ and $a \in \mathrm{Hty}(A,k,N)$, then $a \in \mathrm{Hty}(A,k,MN)$.*

(*d*) *Suppose that $k'$ is a subfield of $\overline{k}$ containing $k$ and that $N$ is such that $k'$ and $k(A_N)$ are linearly disjoint over $k$. Then $\mathrm{Hty}(A,k,N) = \mathrm{Hty}(A,k',N)$.*

(*e*) *For fixed $N \in \mathbb{Z}$, the group $\mathrm{Hty}(A,k,N^\infty)$ depends only on the isogeny class of $A$ over $k$.*

*Proof.* (*a*) This is clear when the degree of the isogeny is prime to $N$. Consider the case of a $k$-isogeny $\phi : A \to B$ of prime-power degree $\ell^n$. There exists a $k$-isogeny $\phi' : B \to A$, the dual isogeny, of degree a power of $\ell$, such that $\phi' \circ \phi$ is multiplication by $\ell^n$ on $A$. This implies $k(A_{\ell^\infty}) = k(B_{\ell^\infty})$. The general case follows because every $k$-isogeny is a composite of $k$-isogenies of prime-power degree.

(*b*) is now a consequence of (*a*).

(*c*) This follows from the fact that every $P \in A_{MN}$ can be written in a unique way as $P_M + P_N$ with $P_M \in A_M$ and $P_N \in A_N$.

(*d*) is similar to (*c*).

(*e*) Let $\phi : A \to B$ be a $k$-isogeny. Then, if $a \in \mathrm{Hty}(A,k,N^\infty)$ and $\sigma \in G_k$ is such that $\sigma(P) = aP$ for all $P \in A_{N^\infty}$, then $\sigma(P) = aP$ for all $P \in B_{N^\infty}$, since both the action of $G_k$ and multiplication by $a$ commute with $\phi$. Thus $a \in \mathrm{Hty}(B,k,N^\infty)$. To obtain the opposite inclusion, use dual isogenies $\phi'$ as in (*a*). □

## 2. Determining $\Theta(\overline{k}) \cap J_N$ with $N$ fixed

In this section we discuss the computation of $\Theta(\overline{k}) \cap J_N$ for fixed $N$. We keep the notation and hypotheses of the previous section and fix an affine model $y^2 + q(x)y = p(x)$ of $C$ as in (1.1). Recall that when discussing points of $J_N$ it is always assumed that the characteristic of $k$ does not divide $N$. We first recall the situation for $N = 2$, 3 and 4. In the following proposition (*a*) is classical, and (*b*) and (*c*) are similar to some results in [G3], but we repeat them here in order to keep the present paper as self-contained as possible.

**(2.1) Proposition.** *Let $C$ be as above.*

(*a*) *$\Theta(\overline{k}) \cap J_2$ consists of the six points $O_J$ and $\epsilon((\alpha, -q(\alpha)/2))$, where $\alpha$ is a root of $p(x)+q(x)^2/4$. Every point of $J_2$ not on $\Theta(\overline{k})$ can be written as $\pi((\alpha,-q(\alpha)/2)+(\beta,-q(\beta)/2))$, where $\alpha$ and $\beta$ are distinct roots of $p(x)+q(x)^2/4$.*

(*b*) *We have $\Theta(\overline{k}) \cap J_3 = \{O_J\}$.*

(*c*) *We have $\Theta(\overline{k}) \cap J_4 = \Theta(\overline{k}) \cap J_2$.*

*Proof.* (*a*) One checks that if $\alpha$ is a root of $p(x) + q(x)^2/4$, then the function $x - \alpha$ on $C$ has divisor $2((\alpha, -q(\alpha)/2) - \infty)$. Thus, if $P_\alpha = \epsilon((\alpha, -q(\alpha)/2))$, then $P_\alpha$ is of order two. Let $\beta$ be a second root of $p(x) + q(x)^2/4$. Since the divisor $(\alpha, -q(\alpha)/2) - (\beta, -q(\beta)/2)$ cannot be principal, $P_\beta \neq P_\alpha$. Conversely if $P \in \Theta(\overline{k}) \cap J_2$, then $P = \epsilon(\xi)$ for some $\xi \in C(\overline{k}) \setminus \{\infty\}$ such that the divisor $2\,\xi - 2\infty$ is principal. By the Riemann-Roch theorem $2\xi$ must be a canonical divisor, and hence $\xi$ is fixed by $\iota$. This implies that $\xi = (\alpha, -q(\alpha)/2)$ with $\alpha$ a root of $p(x) + q(x)^2/4$. There are sixteen points in $J_2$, of which $\Theta(\overline{k}) \cap J_2$ account for six. The points of the form $\pi((\alpha, -q(\alpha)/2) + (\beta, -q(\beta)/2))$ are certainly in $J_2$, and are distinct by (1.3), which also shows they cannot lie on $\Theta$. There are ten of them, so they must be the ten remaining points.

(*b*) This follows from (1.5*d*).

($c$) Let $P \in \Theta(\overline{k}) \cap J_4$. Then $-P = 3P$, and so $3P \in \Theta(\overline{k})$ by (1.5$b$). The assertion now follows from (1.5$d$). □

We henceforth assume that $N \geq 5$. The following follows from the Riemann-Roch theorem, and has figured in the work of Flynn and Leprévost in the search for large rational torsion of Jacobians of curves of genus 2 (see, e.g., [CasFl]).

**(2.2) Proposition.** *Assume that $C$ is given by a model* (1.1) *with $q(x) = 0$. Let $N \geq 5$ be an integer and let $P \in \Theta(\overline{k})$ be a point of order $N$. Write $P = \epsilon(\xi)$ with $\xi \in C(\overline{k}) \setminus \{\infty\}$, and let $v = x(\xi)$. Then there exist coprime polynomials $f$, $g \in \overline{k}[x]$ satisfying*

$$f(x)^2 - p(x)g(x)^2 = (-1)^N(x - v)^N \tag{2.3}$$

*where, if $N$ is even, $f$ is monic of degree $N/2$ and $g$ is of degree at most $(N-6)/2$, while if $N$ is odd, $g$ is monic of degree $(N-5)/2$ and $f$ is of degree at most $(N-1)/2$. Conversely, let $v \in \overline{k}$ and suppose one can find a pair of coprime polynomials $f$, $g \in k[x]$ satisfying all these properties. Then the two points $P = \epsilon(\xi)$ with $x(\xi) = v$ are of order dividing $N$.*

**Example.** Take $N = 6$. Then $f(x) = x^3 + Ax^2 + Bx + C$ and $g(x) = D$, where $A$, $B$, $C$, $D \in \overline{k}$ with $D \neq 0$. Consider the genus two curve $y^2 = x^5 + tx^3 + x$ ($t \in k$, $t \neq \pm 2$), which will be studied at the beginning of the next section. If $v$ is the $x$-coordinate of a point of order six, then (2.3) becomes

$$(x^3 + Ax^2 + Bx + C)^2 - s(x^5 + tx^3 + x) = (x - v)^6,$$

where $s = D^2$. We can successively eliminate $A$, $B$ and $C$ by comparing coefficients of $x^5$, $x^4$ and $x^3$. The coefficients of $x^2$, $x$ and 1 then give

$$5\,s^3 - 120\,s^2v + 32\,st + 720\,sv^2 - 192\,vt - 640\,v^3 = 0,$$
$$-s^4 + 30\,s^3v - 8\,s^2t - 240\,s^2v^2 + 96\,vst + 160\,sv^3 - 64 + 960\,v^4 + 192\,v^2t = 0,$$
$$(8\,st + s^3 - 18\,s^2v + 48\,sv^2 - 32\,v^3)(8\,t + s^2 - 18\,sv + 48\,v^2) = 0.$$

One can eliminate $s$ by taking resultants. When $t = 0$, this leads to

$$(v^4 + 4v^2 + 1)(v^4 - 4v^2 + 1) = 0.$$

For each of these eight values of $v$, one verifies there is a unique corresponding value of $s$, and hence of $D$, up to sign. The corresponding values of $C$, $B$ and $A$ are then determined from the coefficients of $x^3$, $x^4$ and $x^5$. This shows that when $C$ is the curve (0.3), there are sixteen points of order six on $\Theta$.

When $t = 5$, we find that there are no solutions. Hence the curve (0.4) has no points of order six.

A similar strategy gives the points of order five on $y^2 - y = x^5$ (using the model $y^2 = x^5 + 1/4$ obtained by replacing $y$ by $y + 1/2$).

For $N$ large, one would want to search for $N$-torsion on $\Theta$ using Cantor's techniques [Ca].

## 3. The curve $y^2 = x^5 + x$

In the rest of this paper, we shall be interested in applying the methods of the first two sections to the numerical examples (0.2), (0.3) and (0.4). In this section we shall prove Theorem (0.3). We begin by explicitly describing an isogeny between

the Jacobian of the curve $y^2 = x^5 + tx^3 + x$ and a product of two elliptic curves. The case $t = 5$ of this will then be used in the next section.

Let $k$ be a field of characteristic not equal to two and let $t \in k$ be such that there is a complete nonsingular curve $C_t$ of genus two with affine model $y^2 = x^5 + tx^3 + x$. This is equivalent to $t \neq \pm 2$. Let $\alpha$ be the involution of $C_t$ that sends the point $(x, y)$ to the point $(1/x, y/x^3)$, and define $\beta$ as the involution sending $(x, y)$ to $(1/x, -y/x^3)$. Let $E_t$ and $F_t$ be the quotient curves $C_t/\langle\alpha\rangle$ and $C_t/\langle\beta\rangle$, so that the induced projections $\phi : C_t \to E_t$ and $\psi : C_t \to F_t$ are of degree two. The general theory of varieties obtained by taking quotients by finite groups of automorphisms tells us that $E_t$ and $F_t$ are complete nonsingular curves. We define the elements $u$, $v$ and $w$ of the function field $k(C_t)$ of $C_t$ by

$$u = x + \frac{1}{x}, \quad v = y\Big(\frac{1}{x} + \frac{1}{x^2}\Big), \quad w = y\Big(\frac{1}{x} - \frac{1}{x^2}\Big).$$

We write $\alpha^*$ for the automorphism of $k(C_t)$ induced by $\alpha$, and define $\beta^*$ similarly. It is clear that $\alpha^*$ fixes $u$ and $v$ while $\beta^*$ fixes $u$ and $w$.

**(3.1) Lemma.** (*a*) *We have* $k(E_t) = k(u, v)$ *and* $k(F_t) = k(u, w)$. *Affine equations for* $E_t$ *and* $F_t$ *are then given respectively by*

$$v^2 = (u + 2)(u^2 - 2 + t) \qquad \text{and} \qquad w^2 = (u - 2)(u^2 - 2 + t).$$

(*b*) *When we write* $i$ *for a root of* $X^2 + 1$ *in* $\overline{k}$, $E_t$ *and* $F_t$ *become isomorphic over* $k(i)$.

*Proof.* (*a*) We argue for $E_t$, the case of $F_t$ being similar. The relation $v^2 = (u + 2)(u^2 - 2 + t)$ is easily verified: it shows that $k(u, v)$ is a quadratic extension of $k(u)$. By hypothesis, $k(E_t)$ is the subfield of $k(C_t)$ fixed by $\alpha^*$, and $k(C_t)/k(E_t)$ is of degree two. Since $k(u, v) \subseteq k(E_t)$, to prove equality it suffices to check that $k(C_t)/k(u, v)$ is an extension of degree two. But $k(C_t) \supseteq k(x) \supseteq k(u)$ and $k(u, v) \supseteq k(u)$, with each extension being quadratic. This proves (*a*).

(*b*) It suffices to send the point $(u, v)$ of $E_t$ to the point $(-u, iv)$ of $F_t$. □

Since $t \neq \pm 2$, we see that $E_t$ and $F_t$ are elliptic curves. As usual, we take their origins to be the points at infinity, which we denote respectively by $O_{E_t}$ and $O_{F_t}$.

Let $J_t$ be the Jacobian variety of $C_t$. Viewing $J_t$ as the Picard variety of $C_t$, and identifying $E_t$ with its Picard variety, we see that the covering $\phi : C_t \to E_t$ induces a homomorphism of Abelian varieties $\phi^* : E_t \to J_t$. Indeed, if $P \in E_t(\overline{k})$, then $\phi^*(P)$ is the point of $J_t(\overline{k})$ represented by the divisor $\xi + \eta - (0, 0) - \infty$, where $\xi$ and $\eta$ are the two points of $C_t(\overline{k})$ whose image under $\phi$ is $P$. For $O_{E_t}$ these points are $(0, 0)$ and $\infty$. We obtain similarly a homomorphism $\psi^* : F_t \to J_t$ and then a homomorphism $\phi^* + \psi^* : E_t \times F_t \to J_t$ defined by $(P, Q) \mapsto \phi^*(P) + \psi^*(Q)$.

On the other hand, we can view $J_t$ as the Albanese variety of $C_t$. Using the embedding $\epsilon : C_t \to J_t$ as defined in §1, we see that $\phi$ extends to a morphism $J_t \to E_t$, which we denote also by $\phi$. Explicitly, if $P$ is a point of $J_t(\overline{k})$ and $\xi_P$, $\eta_P$ are points of $C_t(\overline{k})$ such that $\pi(\xi_P + \eta_P) = P$ as in §1, then $\phi(P) = \phi(\xi_P) + \phi(\eta_P)$. Note that this is a homomorphism of Abelian varieties, since if $P = O_{J_t}$ then we may suppose $\xi = \eta = \infty$ and so $\phi(O_{J_t}) = 2\phi(\infty) = O_{E_t}$. We extend $\psi$ to a homomorphism $\psi : J_t \to F_t$ in a similar manner, and then consider the homomorphism $(\phi, \psi) : J_t \to E_t \times F_t$ which sends $P \in J_t(\overline{k})$ to $(\phi(P), \psi(P))$.

**(3.2) Lemma.** *The composite endomorphism* $(\phi, \psi) \circ (\phi^* + \psi^*)$ *of* $E_t \times F_t$ *is multiplication by 2.*

*Proof.* This follows from results in [FK], or [Ku], but can be done explicitly as follows. Taking $P \in E_t(\overline{k})$ and $Q \in F_t(\overline{k})$, let $\xi_1$, $\eta_1$ be the two points of $C_t(\overline{k})$ whose images under $\phi$ are $P$, and let $\xi_2$, $\eta_2$ be the two points whose images under $\psi$ are $Q$. Thus $(\phi^* + \psi^*)(P, Q) = \pi(\xi_1 + \eta_1) + \pi(\xi_2 + \eta_2)$. Thus,

$$\begin{aligned}(\phi, \psi) \circ (\phi^* + \psi^*)(P, Q) &= (\phi(\xi_1), \psi(\xi_1)) + (\phi(\eta_1), \psi(\eta_1)) \\ &\quad + (\phi(\xi_2), \psi(\xi_2)) + (\phi(\eta_2), \psi(\eta_2)) \\ &= (2P + \phi(\xi_2) + \phi(\eta_2), 2Q + \psi(\xi_1) + \psi(\eta_1)).\end{aligned}$$

Let us show that $\psi(\xi_1) + \psi(\eta_1) = O_{F_t}$. Now from the definition of $\phi$ we have $\eta_1 = \alpha(\xi_1)$. Since $\alpha = \iota \circ \beta$ and for any $\xi \in C_t(\overline{k})$, $\psi(\iota(\xi)) = -\psi(\xi)$, we find that $\psi(\xi_1) + \psi(\eta_1) = \psi(\xi_1) + \psi(\iota \circ \beta(\xi_1)) = \psi(\xi_1) - \psi(\beta(\xi_1)) = O_{F_t}$, as asserted. Similarly, $\phi(\xi_2) + \phi(\eta_2) = O_{E_t}$, and this proves the lemma. □

We specialize now to the case $t = 0$ with a view to proving (0.3). Until the end of the section, we write $E$, $F$ and $J$ for $E_0$, $F_0$ and $J_0$. The curves $E$ and $F$ have models $v^2 = (u + 2)(u^2 - 2)$ and $w^2 = (u - 2)(u^2 - 2)$ and are the curves numbered 256D1 and 256A1 in Cremona's tables [Cr]. Their $j$-invariants are 8000, which means that they have complex multiplication by the ring of integers $\mathfrak{O}_L$ of the field $L = \mathbb{Q}(\sqrt{-2})$. They have good reduction over $\mathbb{Q}$ at all primes except 2, and the same holds over $L$.

The classical theory of complex multiplication describes the action of $G_L$ on $E_{\text{tors}}$ and $F_{\text{tors}}$, and we describe this for $E_{\text{tors}}$ below. We know also from (3.1*b*) that $E$ and $F$ become isomorphic over $\mathbb{Q}(i)$ and thus also over $K = L(i)$. Thus we shall prove (0.3) by studying the action of $G_K$ on $J_{\text{tors}}$, or rather, using (1.8), its action on $(E^2)_{\text{tors}}$. In fact, we shall make no future use of the curve $F$.

Recall that $\mathfrak{O}_L$ is a principal ideal domain and that its group of units is $\{\pm 1\}$. If $\nu \in \mathfrak{O}_L$, we write $(\nu)$ for the ideal generated by $\nu$. We fix an isomorphism $\mathfrak{O}_L \cong \text{End}_{\overline{L}} E$, so that the pullback of a holomorphic differential on $E$ by the endomorphism corresponding to $\alpha \in \mathfrak{O}_L$ is given by multiplication by $\alpha$. In what follows, we consider $E_{\text{tors}}$ as an $\mathfrak{O}_L$-module. When $\nu \in \mathfrak{O}_L$ we write $E_\nu$ for the group of elements of $E(\overline{L})$ that are in the kernel of the endomorphism $\nu$ of $E$. As an $\mathfrak{O}_L$-module, $E_\nu$ is isomorphic to $\mathfrak{O}_L/\nu\mathfrak{O}_L$, and so, since endomorphisms commute with the action of $G_L$, the representation of $G_L$ in $\text{Aut}_{\mathbb{Z}}(E_\nu)$ actually takes values in $\text{Aut}_{\mathfrak{O}_L}(E_\nu)$, which is isomorphic to $(\mathfrak{O}_L/\nu\mathfrak{O}_L)^*$. In particular, $L(E_\nu)/L$ is an Abelian extension. If $P \in E_{\text{tors}}$, the annihilator of $P$ can be viewed as an ideal of $\mathfrak{O}_L$: we call this ideal the order of $P$.

Let $\theta$ be a fixed square root of $-2$ in $L$ and let $I(\theta)$ be the group of fractional ideals of $L$ that are prime to $\theta$. Classical complex multiplication theory then shows the existence of a homomorphism $\lambda : I(\theta) \to L^*$ enjoying the following properties:

(*i*) For all ideals $\mathfrak{a}$ in $I(\theta)$, $\lambda(\mathfrak{a})$ is a generator of $\mathfrak{a}$. Furthermore, since $E$ has good reduction outside $\theta$, there exists an integer $k \geq 3$ with the following property: if $\mathfrak{a}$ has a generator $\alpha$ such that $\alpha \equiv 1 \pmod{\theta^k \mathfrak{O}_L}$, then $\lambda(\mathfrak{a}) = \alpha$.

(*ii*) For all $\nu \in \mathfrak{O}_L$, for all primes $\mathfrak{p}$ of $\mathfrak{O}_L$ prime to $\theta\nu$ and for all $P \in E_\nu$, we have

$$(\mathfrak{p}, L(E_\nu)/L))P = \lambda(\mathfrak{p})P,$$

where $(\mathfrak{p}, L(E_\nu)/L))$ is the (arithmetic) Frobenius symbol.

(*iii*) For every prime $\mathfrak{p}$ of $\mathfrak{O}_L$ prime to to $\theta\mathfrak{O}_L$, $\lambda(\mathfrak{p})$ can be viewed as an endomorphism of the reduction $\tilde{E}_{(\mathfrak{p})}$ of $E$ at $\mathfrak{p}$. As such, it coincides with the (geometric) Frobenius endomorphism of $\tilde{E}_{(\mathfrak{p})}$ over $\mathfrak{O}_L/\mathfrak{p}$.

Note that the second assertion of (*i*) makes sense, since if $\mathfrak{a}$ has a generator $\equiv 1 \pmod{\theta^k\mathfrak{O}_L}$, it is unique because of the condition $k \geq 3$.

*Remark.* We can also calculate $\lambda(\mathfrak{p})$ as follows, using (*iii*) and the well-known formula of Hasse concerning points on curves over finite fields,

$$\#(\tilde{E}_{(\mathfrak{p})}) = 1 + N\mathfrak{p} - \mathrm{tr}(\lambda(\mathfrak{p})), \tag{3.3}$$

where $N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$ and tr the trace from $L$ to $\mathbb{Q}$. Since the only units in $\mathfrak{O}_L$ are $\pm 1$, and since a generator of $\mathfrak{p}$ necessarily has non-zero trace, (3.3) together with (*i*) determine $\lambda(\mathfrak{p})$ completely . This method is useful when $\mathfrak{p}$ is of degree one: when it is of degree two, so that $\mathfrak{p} = p\mathfrak{O}_L$ for some rational prime $p > 0$, then it is well-known that

$$\lambda(\mathfrak{p}) = -p. \tag{3.4}$$

Doing such calculations, using the traces of Frobenius as given in [Cr], we see that $\lambda(1+\theta) = 1+\theta$, whereas $\lambda(-3+\theta) = 3-\theta$. Since $1+\theta \equiv -3+\theta \pmod{\theta^4}$, we conclude that $k \geq 5$. In fact, that $k = 5$ follows from a formula of Deuring [D].

We are now ready to compute the Galois group of $L(E_\nu)$ over $L$.

**(3.5) Proposition.** (*a*) *For all $\nu \in \mathfrak{O}_L$ prime to $\theta$, the representation of $G_L$ in $(\mathfrak{O}_L/\nu\mathfrak{O}_L)^*$ is surjective.*

(*b*) *For all $j \geq 5$, the image of the representation of $G_L$ in $(\mathfrak{O}_L/\theta^j\mathfrak{O}_L)^*$ is of index 2.*

(*c*) *For all $\nu \in \mathfrak{O}_L$ prime to $\theta$, $L(E_{\theta^\infty}) \cap L(E_\nu) = L$.*

(*d*) *When $\mu$, $\nu$ are two coprime elements of $\mathfrak{O}_L$, the fields $L(E_\mu)$ and $L(E_\nu)$ are disjoint over $L$.*

(*e*) *When $\mu$, $\nu$ are two coprime elements of $\mathfrak{O}_L$, the fields $K(E_\mu)$ and $K(E_\nu)$ are disjoint over $K$.*

*Proof.* (*a*) This follows since any element of $(\mathfrak{O}_L/\nu\mathfrak{O}_L)^*$ can be represented by some $\alpha \in \mathfrak{O}_L$ such that $\alpha \equiv 1 \pmod{\theta^k}$.

(*b*) By standard results of the theory of complex multiplication, if $F$ is the field generated over $L$ by the $u$-coordinates of all points of $E_{\theta^j}$, then $F$ is the ray class field of $L$ of conductor $\theta^j$. Since $j > 2$, $[F : L] = \#((\mathfrak{O}_L/\theta^j\mathfrak{O}_L)^*/\pm 1) = 2^{j-2}$. Since $F \subseteq L(E_{\theta^j})$ and we have an injection of $\mathrm{Gal}(L(E_{\theta^j})/L)$ into $\mathrm{Aut}(E_{\theta^j}) = (\mathfrak{O}_L/\theta^j\mathfrak{O}_L)^*$, it suffices to show that there is a residue class in $(\mathfrak{O}_L/\theta^j\mathfrak{O}_L)^*$ which is not $\lambda(\mathfrak{a})$ for any fractional ideal $\mathfrak{a}$. Note that if $\lambda(\mathfrak{a}) \equiv 5 \pmod{\theta^5}$, then $\mathfrak{a}$ has a generator which is 5 (mod $\theta^5$), hence another which is 3 (mod $\theta^5$). By (*i*) and the remark, it suffices therefore to show that $\lambda(3)$ and $\lambda(5)$ are not congruent to 5 (mod $\theta^5$). By the remark, $\lambda(3) = \lambda(1+\theta)\lambda(1-\theta) = (1+\theta)(1-\theta) = 3$, and $\lambda(5) = -5$, so we are done.

(*c*) Take $\nu \in \mathfrak{O}_L$ prime to $\theta$, and let $L(E_{\theta^\infty}) \cap L(E_\nu) = L'$. Then since $L$ has class number 1, $L'$ is totally ramified over $L$ at $\theta$. On the other hand, by (*a*), $L(E_\nu)$ is a quadratic extension of the ray class field of $L$ of conductor $\nu$, so $L'/L$ is at most a quadratic extension. If $L' = L$ we are done. Assume not. Then, via (3.5*a*), the projection of $\mathrm{Gal}(L(E_\nu)/L)$ onto $\mathrm{Gal}(L'/L)$ gives us a surjective homomorphism $\rho : (\mathfrak{O}_L/\nu\mathfrak{O}_L)^* \to \mathbb{Z}/2\mathbb{Z}$. Let $(\nu) = \prod_{i=1}^n (\pi_i)^{e_i}$, where the $(\pi_i)$ are

prime ideals in $\mathfrak{O}_L$, and $\nu' = \prod_{i=1}^n \pi_i$. Since the kernel of the natural projection $(\mathfrak{O}_L/\nu\mathfrak{O}_L)^* \to (\mathfrak{O}_L/\nu'\mathfrak{O}_L)^*$ has odd order, $\rho$ factors through $(\mathfrak{O}_L/\nu'\mathfrak{O}_L)^*$. By the Chinese remainder theorem, $(\mathfrak{O}_L/\nu'\mathfrak{O}_L)^* \cong \prod_{i=1}^n (\mathfrak{O}_L/\pi_i\mathfrak{O}_L)^*$, and $(\mathfrak{O}_L/\pi_i\mathfrak{O}_L)^*$ is cyclic. Therefore $\rho$ factors through $\prod_{i=1}^n (\mathfrak{O}_L/\pi_i\mathfrak{O}_L)^*/((\mathfrak{O}_L/\pi_i\mathfrak{O}_L)^*)^2 \cong (\mathbb{Z}/2\mathbb{Z})^n$. This corresponds to $L'$ being contained in the compositum $\prod_{i=1}^n H_i$, where $H_i$ is the unique quadratic extension of $L$ contained in $L(E_{\pi_i})$. It is well known, see for example [St], that $L(E_{\pi_i})/L$ is totally ramified over $\pi_i$. Hence $H_i$ is totally ramified over $L$ at $\pi_i$ and at no other primes outside $\theta$. By Kummer theory, the only extension of $L$ contained in $\prod_{i=1}^n H_i$ unramified outside $\theta$ is $L$ itself. So $L' = L$.

(*d*) Let $\mu$, $\nu$ be two coprime elements of $\mathfrak{O}_L$. If they are both prime to $\theta$, then this follows from (*a*). Suppose then that $\mu = \theta^j \mu'$, where $\mu'$ is prime to $\theta$. By (*c*),

$$[L(E_{\theta^j\mu'}) : L] = [L(E_{\theta^j}) : L][L(E_{\mu'}) : L]$$

and

$$[L(E_{\theta^j\mu'\nu}) : L] = [L(E_{\theta^j}) : L][L(E_{\mu'\nu}) : L].$$

But by (*a*),

$$[L(E_{\mu'\nu}) : L] = [L(E_{\mu'}) : L][L(E_\nu) : L],$$

so we get

$$[L(E_{\theta^j\mu'\nu}) : L] = [L(E_{\theta^j\mu'}) : L][L(E_\nu) : L],$$

and we are done.

(*e*) From the equation of the curve we have that $K = L(E_{\theta^2})$. The statement now follows easily from (*d*). □

We can now begin the proof of (0.3). As indicated above, we shall in fact work over the field $K = L(i)$. We think of $K$ as a subfield of $\overline{L}$ and identify $G_K$ with a subgroup of $G_L$. The field $K = L(i)$ is the field of eighth roots of unity, and $J$ has complex multiplication by the ring of integers $\mathfrak{O}_K$ of $K$. (This is induced by the automorphism $(x, y) \mapsto (ix, \rho y)$ of $C$, where $\rho^2 = i$.) Hence $\mathfrak{O}_L \subseteq \mathrm{End}(J)$, and we will measure the order of an element of $J_{\mathrm{tors}}$ as an ideal in $\mathfrak{O}_L$.

Step I: As a preliminary, let $\nu$ be coprime to $\theta$, and let $N$ be an odd rational integer divisible by $\nu$. We want to prove that $2 \in \mathrm{Hty}(J, K, N)$ (using the notation introduced just before (1.8)). For this, it suffices to show that $2 \in \mathrm{Hty}(J, K, N^\infty)$ or, using (1.8*e*), that $2 \in \mathrm{Hty}(E^2, K, N^\infty)$ and this is equivalent to $2 \in \mathrm{Hty}(E, K, N^\infty)$. But since $K = L(E_2)$, $K$ and $L(E_{N^r})$ are linearly disjoint for all $r$, so this is equivalent to $2 \in \mathrm{Hty}(E, L, N^\infty)$ by (1.8*d*). But since $2 \in \mathrm{Hty}(E, L, N^r)$ for all $r$ by (3.5*a*), this is clear.

Recall from (3.2) that there are $K$-isogenies $\phi : E^2 \to J$, $\phi' : J \to E^2$ such that $\phi' \circ \phi$ is multiplication by 2. Hence if $P$ is of order $\nu$, then $K(P) = K(2P) = K(\phi' \circ \phi(P)) \subseteq K(\phi(P)) \subseteq K(P)$, so $K(P) = K(\phi(P))$. Moreover, since $E^2$ and $J$ are $K$-isogenous, they have the same Hecke character over $K$, so if $P \in J_{\mathrm{tors}}$, $\sigma \in G_K$, and $\sigma(P) = \alpha P$, then $\sigma(\phi(P)) = \alpha\phi(P)$.

Step II: We next show that, if $\nu \in \mathfrak{O}_L$ is not divisible by a prime over 3, then $\Theta(\overline{L}) \cap J_\nu \subseteq J_2$. To use (1.6*b*), by an argument similar to one given in Step I, we need to show that $3 \in \mathrm{Hty}(E, K, N^\infty)$, $N$ being a rational integer not divisible by 3. If $N$ is odd this is clear. To deal with the general case it suffices to suppose $N = 2$. In the proof of (3.5*b*), we showed that $3 \in \mathrm{Hty}(E, L, 2^\infty)$. Since $3 \equiv 1 \pmod{\theta^2}$, and $K = L(E_{\theta^2})$, we find that $3 \in \mathrm{Hty}(E, K, 2^\infty)$.

For the rest of the proof, we take a point $P \in \Theta(\overline{L}) \cap J_{\mathrm{tors}}$ whose order is $(\nu)$, where $\nu = \theta^n(1+\theta)^a(1-\theta)^b\mu$ with $n \geq 0$, $a+b \geq 1$ and $\mu$ prime to 6. Our purpose is to show that $(\mu) = \mathfrak{O}_L$, $n \leq 2$ and $a+b=1$. This will show that the order of $P$ as an element of the $\mathbb{Z}$-module $J_{\mathrm{tors}}$ is six and so we are left with checking the existence of points of order dividing 6 as described in §2. We write $P$ as a sum of points $P_\theta + P_{1+\theta} + P_{1-\theta} + Q$ with $P_\theta$ of order $(\theta^n)$, $P_{1+\theta}$ of order $(1+\theta)^a$, $P_{1-\theta}$ of order $(1-\theta)^b$, and $Q$ of order $(\mu)$.

Step III. We will show that $a \leq 1$. The proof that $b \leq 1$ is similar. Suppose that $a > 1$. By (3.5) and Step I, there is a Galois element so that $\sigma(P_{1+\theta}) = P_{1+\theta} + R$, with $R \neq O_J$ and $R \in J_{1+\theta}$. By linear disjointness we can assume that $\sigma$ fixes $P - P_{1+\theta}$. Then $\sigma(P) = P + R$, so $P \in \Theta \cap \Theta_{-R}$, where for $W \in J$, $\Theta_W$ is the image of $\Theta$ under the translation-by-$W$ map. Note that $R$ is defined over a quadratic extension of $K$, so by (1.4), $P$ is defined over a quartic extension of $K$. By (3.5$a$) and (3.5$c$), we have that $P_{1+\theta}$ has $2 \cdot 3^{a-1}$ conjugates over $K$, so $a \leq 1$.

Step IV. Suppose now that $n > 2$. Write $P_3 = P_{1+\theta} + P_{1-\theta}$. We have seen in Step II that $3 \in \mathrm{Hty}(J, K, 2^\infty)$. Using linear disjointness (3.5$e$), we can choose $\sigma \in G_K$ such that $\sigma(P_\theta) = 3P_\theta \neq P_\theta$, $\sigma(P_3) = P_3$ and $\sigma(Q) = Q$. Then $\sigma(P) - P = \sigma(P_\theta) - P_\theta = 2P_\theta$, and so, by (1.7), we must have $[K(\sigma(P), P) : K(2P_\theta)] \leq 2$. Furthermore, $P_\theta$ is a multiple of $P$, so that $\sigma(P) = P + 2P_\theta$ also is, and $K(\sigma(P), P) = K(P)$. Similarly $P_3$ and $Q$ are multiples of $P$, so that that are defined over $K(P)$ and $K(P)$ is generated over $K$ by the three subfields $K(P_\theta)$, $K(P_3)$ and $K(Q)$, which are pairwise linearly disjoint over $K$. Letting $K' = K(2P_\theta)$, we deduce that each of the extension degrees

$$[K(P_\theta) : K'],\ [K(P_3) : K] = [K'(P_3) : K'],\ [K(Q) : K] = [K'(Q) : K'] \tag{3.6}$$

is at most two, with equality occurring at most once. Since $a$ or $b$ is positive, we get that $[K(P_3) : K]=2$, so $[K(P_\theta) : K'] = 1$.

We can now contradict the assumption that $n > 2$. Since $J$ and $E^2$ have the same Hecke character over $K$, $K(J_{\theta^n}) = K(E_{\theta^n})$ for all $n$. We know that $L = L(E_\theta)$ and that $K = L(E_{\theta^2}) = K(E_{\theta^2})$. Since $\lambda((1+\theta)^2) = (1+\theta)^2 \equiv 1 + \theta^2 + \theta^3 \pmod{\theta^4}$, we get that $K(E_{\theta^3})$ is a quadratic extension of $K$. Then (3.5$b$) shows that $K(E_{\theta^5})$ is a quadratic extension of $K(E_{\theta^3})$, and that, for all $j \geq 5$, $K(E_{\theta^{j+1}})$ is a quadratic extension of $K(E_{\theta^j})$. Since $[K(P_\theta) : K(2P_\theta)] = 1$, and $(2) = (\theta^2)$, we get that $n \leq 2$.

Step V: We now have that $n \leq 2$ and $a$, $b \leq 1$. In particular, $P_\theta \in J_2$ and is defined over $K$. It only remains to show that $(\mu) = \mathfrak{O}_L$, or equivalently that $Q = O_J$. Write $P_{\mathrm{odd}} = Q + P_3$, so we have to show that $P_{\mathrm{odd}}$ is a point of order dividing 3. By Step I, there is a Galois element $\sigma$ fixing $P_\theta$ such that $\sigma(P_{\mathrm{odd}}) = 2P_{\mathrm{odd}}$, and similarly, an element $\tau$ such that $\tau(P_{\mathrm{odd}}) = -P_{\mathrm{odd}}$ that fixes $P_2$. Hence $3P_{\mathrm{odd}} = \sigma(P) - \tau(P)$. On the other hand, it is also easy to see that $3P_{\mathrm{odd}} = \sigma^2(P) + \tau(P)$. By (1.3), if $3P_{\mathrm{odd}} \neq O_J$, then $\tau(P) = -\tau(P)$, in which case $P_{\mathrm{odd}} = O_J$, or $\tau(P) = \sigma(P)$, in which case $3P_{\mathrm{odd}} = O_J$. In any case, $3P_{\mathrm{odd}} = O_J$, so we are done.

*Remark.* Since $C$ has good ordinary reduction at 11, Coleman's bound shows that there are at most 22 torsion points on $\Theta$. Since we have described 22 such, they must be all the torsion points on $\Theta$.

## 4. The curve $y^2 = x^5 + 5\,x^3 + x$

We next turn our attention to the fiber at $t = 5$ of the curve denoted by $C_t$ in §3. In this section we denote it by $C$, and write $J$ for its Jacobian and $E$ and $F$ for the corresponding fibers of $E_t$ and $F_t$. Thus $C$ has affine model $y^2 = x^5 + 5\,x^3 + x$, and the models of $E$ and $F$ are respectively $v^2 = (u+2)(u^2+3)$ and $w^2 = (u-2)(u^2+3)$. Using (3.1), we know that $J$ is isogenous to $E^2$ over $\mathbb{Q}(i)$, and, as in the example of $y^2 = x^5 + x$, our first task is to study the action of $G_{\mathbb{Q}}$ on $E_{\text{tors}}$.

The elliptic curve $E$ is that labeled 672A1 in Cremona's tables [Cr]. Its discriminant is $-2^6 \cdot 3 \cdot 7^2$ and its $j$-invariant is $2^6 \cdot 5^3/3 \cdot 7^2$. Thus, there is multiplicative reduction at 3 and, in particular, $E$ does not have complex multiplication. We are therefore in the situation of Serre [S2], the main theorem of which tells us that, for all sufficiently large prime $\ell$, the representation of $G_{\mathbb{Q}}$ on $\mathrm{Aut}_{\mathbb{Z}}(E_\ell)$ is surjective. In fact, we shall see in a moment that it is surjective for all $\ell \geq 3$. However, we need to study the representation on $\mathrm{Aut}_{\mathbb{Z}}(E_N)$ for all $N$.

For any $N$, recall that the Tate module $T_N$ is a free $\mathbb{Z}_N$-module of rank 2. The action of $G_{\mathbb{Q}}$ on $T_N$ gives us a homomorphism $G_{\mathbb{Q}} \to \mathrm{Aut}(T_N)$, the image of which we denote by $\Gamma_{N^\infty}$. If $L$ is a number field, we write $\Gamma_{N^\infty}^L$ for the image of the subgroup $G_L$. We let $\Gamma_{N^n}$ and $\Gamma_{N^n}^L$ denote the images of $G_{\mathbb{Q}}$ and $G_L$ under the induced homomorphism into the automorphisms of $E_{N^n} = T_N/N^n T_N$.

If for every prime $\ell$ we pick a basis $P_{\ell^\infty}, Q_{\ell^\infty}$ for $T_\ell$, we get a representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. We will let $P_{\ell^n}$ and $Q_{\ell^n}$ denote the projections of $P_{\ell^\infty}$ and $Q_{\ell^\infty}$ in $E_{\ell^n}$. The actions of $\Gamma_{\ell^n}$ and $\Gamma_{\ell^n}^L$ on $P_{\ell^\infty}$ and $Q_{\ell^\infty}$ give us representations into $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. These choices of bases for $T_\ell$ give us a base for any $T_N$, so we similarly get representations of $\Gamma_{N^\infty}$, $\Gamma_{N^\infty}^L$, $\Gamma_N$, and $\Gamma_N^L$ in $\mathrm{GL}_2(\mathbb{Z}_N)$ and $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Let us now recall some facts and establish some notation. The number $c_6$ attached to $E$ (see for example [Cr], page 45) is equal to $2^7 \cdot 31$. As remarked in [S2], page 276, the fact that $-c_6$ is a square of $\mathbb{Q}_3$ shows that $E_{\mathbb{Q}_3}$ is a "Tate elliptic curve" over $\mathbb{Q}_3$, with parameter $q \in \mathbb{Q}_3$. The 3-adic order of $q$ is the same as that of $1/j$, which is 1. Hence by [S1], IV-20, Lemma 1, for every prime $\ell$, $\Gamma_\ell$ contains a transvection. That is, there is a choice of $P_\ell$ and $Q_\ell$ so that the transvection is represented in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ as $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

We denote by $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ the subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ consisting of those matrices that have determinant one. If $k$ is a field and $N \in \mathbb{N}$, then $k^{(N)}$ denotes the subfield of $\overline{k}$ obtained from $k$ by adjoining all $N$-th roots of unity.

We recall the following well-known fact, which follows from the non-degeneracy of the Weil pairing.

**(4.1) Lemma.** *For all $N \in \mathbb{N}$, $\mathbb{Q}(E_N)$ contains $\mathbb{Q}^{(N)}$ and the action of $g \in G_{\mathbb{Q}}$ on the $N$-th roots of unity is given by raising to the power of the determinant of the image of $g$ in $\Gamma_N$. In particular, $\Gamma_N^{\mathbb{Q}^{(N)}} = \Gamma_N \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Since the cyclotomic polynomial of order $N$ is irreducible over $\mathbb{Q}$, the restriction to $\Gamma_N$ of the determinant map $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^*$ is surjective. Similarly $\Gamma_{N^\infty}^{\mathbb{Q}^{(N^\infty)}} = \Gamma_{N^\infty} \cap \mathrm{SL}_2(\mathbb{Z}_N)$ and the restriction to $\Gamma_{N^\infty}$ of the determinant map $\mathrm{GL}_2(\mathbb{Z}_N) \to \mathbb{Z}_N^*$ is surjective.*

We also need the following lemma, which is a mild generalization of [S1], IV-23, Lemma 3, and enjoys a virtually identical proof.

**(4.2) Lemma.** *Let $\ell$ be a prime, and $m = 1$ for $\ell \geq 5$, $m = 2$ for $\ell = 3$, and $m = 3$ for $\ell = 2$. For $n \geq k$, let $\pi_n^k : \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ be the natural projection. Let $C_1 \subseteq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be a subgroup, and $C_n = (\pi_n^1)^{-1}(C_1)$, $C_\infty =$*

$\varprojlim C_n = (\pi_\infty^1)^{-1}(C_1)$, *where* $\pi_\infty^n : \mathrm{SL}_2(\mathbb{Z}_\ell) \to \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ *is the natural projection. Suppose further that for all* $n \geq m$, *the kernel of* $\pi_{n+1}^n$ *is contained in* $C_{n+1}$. *If* $X$ *is a closed subgroup of* $C_\infty$ *such that* $\pi_\infty^m(X) = C_m$, *then* $X = C_\infty$.

We are now ready to prove the following.

**(4.3) Lemma.** *Let* $\ell$ *be an odd prime.*
(*a*) $\Gamma_\ell = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.
(*b*) $\Gamma_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

*Proof.* (*a*). Table I in [Cr] shows that all curves in the $\mathbb{Q}$-isogeny class of $E$ are linked by isogenies of 2-power order. Thus the $G_\mathbb{Q}$-module $E_\ell$ is irreducible. (One can also give a theoretical argument avoiding the reference to table I in [Cr] by using the methods of [S2], §5.6.) Since the determinant on $\Gamma_\ell$ is surjective, $\Gamma_\ell$ contains a transvection, and $E_\ell$ is irreducible, an argument of Serre [S1], pages IV-18 to IV-22, gives (*a*).

(*b*) When $\ell \geq 5$, the second assertion now follows from (*a*) using the surjectivity of the determinant on $\Gamma_{\ell^\infty}$, (4.1), and (4.2). This argument will also suffice for $\ell = 3$, if we can show that $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \subseteq \Gamma_9$. By (*a*), it suffices to show that the kernel $\Upsilon$ of the natural projection $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is in $\Gamma_9$. Note that $\Upsilon$ is a $\mathbb{Z}/3\mathbb{Z}$-vector space of dimension 3 generated by $\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}$, $\begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix}$, and $\begin{pmatrix}7 & 0\\ 0 & 4\end{pmatrix}$. The first two are in $\Gamma_9$ for free. Let $\alpha \in \Gamma_9$ be such that $\alpha \equiv \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \pmod 3$. Then $\alpha^3 = \begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}$. Similarly, $\begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix} \in \Gamma_9$. Now Cremona's tables show that the action of the Frobenius $\mathrm{Fr}_{73}$ at 73 acts on $T_3$ with trace $-2$ and determinant 73. So the eigenvalues of $\mathrm{Fr}_{73}$ are $-1 \pm 6\sqrt{-2} \in \mathbb{Z}_3$. Hence there is a basis of $T_3$ so that $\mathrm{Fr}_{73}$ is represented as $\begin{pmatrix}-1+6\sqrt{-2} & 0\\ 0 & -1-6\sqrt{-2}\end{pmatrix}$, where we let $\sqrt{-2}$ be the square root of $-2$ congruent to 4 (mod 9). The square of this matrix is congruent (mod 9) to $\begin{pmatrix}7 & 0\\ 0 & 4\end{pmatrix}$, as desired. □

The situation at points of order a power of two is more complicated. For the rest of this section, we denote by $K$ the field $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt{7})$.

**(4.4) Proposition.** (*a*) *We have* $\mathbb{Q}(E_2) = \mathbb{Q}(\sqrt{-3})$.

(*b*) *Let the ordered basis* $Q_{2^\infty}$, $P_{2^\infty}$ *of* $T_2$ *be chosen so that* $P_2 = (-2, 0)$. *The field* $\mathbb{Q}(E_4)$ *contains* $K$, *and the point* $P_4$ *is defined over a quadratic extension of* $K$ *but not over* $K$.

(*c*) *The relative Galois group of* $\mathbb{Q}(E_4)$ *over* $\mathbb{Q}(E_2)$ *is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^4$, *and*

$$\Gamma_4 = \left\{ \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \mid c \in 2\mathbb{Z}/4\mathbb{Z} \right\}.$$

(*d*) *We have*

$$\Gamma_4^K = \left\{ \begin{pmatrix}a & b\\ 0 & d\end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \mid ad \equiv 1 \pmod 4,\ b \in 2\mathbb{Z}/4\mathbb{Z} \right\}.$$

(*e*) *We have*

$$\Gamma_{2^\infty} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_2) \mid c \in 2\mathbb{Z}_2 \right\}.$$

*Proof.* (*a*) It is clear that $\mathbb{Q}(E_2) = \mathbb{Q}(\sqrt{-3})$.

(*b*) It is shown in [Si], p. 293, that if $R = (x_0, y_0)$ is a point on the elliptic curve $y^2 = x^3 + ax^2 + bx$, then the $x$-coordinate of $R$ plus the 2-torsion point $(0,0)$ is $b/x_0$. We apply this now to our curve $E$ given by $v^2 = w^3 - 4w^2 + 7w$, obtained by letting $w = u + 2$, which transforms $P_2$ to $(0,0)$. Since $P_4 + P_2 = -P_4$, and $w(-P_4) = w(P_4)$, we see that $w(P_4) = 7/w(P_4)$, so $w(P_4) = \sqrt{7}$, for some choice of square root of 7. Hence $v(P_4)^2 = -28 + 14\sqrt{7}$. Let $\alpha$ be a square root of $-28 + 14\sqrt{7}$, and $\beta$ a square root of its conjugate $-28 - 14\sqrt{7}$. Then $(\alpha + \beta)^2$ is $-56 \pm 28\sqrt{-3}$. So $\mathbb{Q}(P_4)/\mathbb{Q}(P_2)$ has Abelian Galois group of type $(2,2)$, corresponding via Kummer theory to the group generated by representatives $\{-2 + \sqrt{-3}, -2 - \sqrt{-3}\}$ in $\mathbb{Q}(\sqrt{-3})^*/(\mathbb{Q}(\sqrt{-3})^*)^2$. Since $K/\mathbb{Q}(\sqrt{-3})$ is also an Abelian extension of type $(2,2)$ corresponding to the group generated by $\{7, -1\}$, we see that $K(P_4)/K$ is a quadratic extension. Lastly, $\sqrt{-1} \in \mathbb{Q}(E_4)$ by the Weil pairing, so $K \subseteq \mathbb{Q}(E_4)$.

(*c*) The Galois group of $\mathbb{Q}(E_4)$ over $\mathbb{Q}(E_2)$ embeds in the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. It is therefore isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some $r \leq 4$. By (*b*), $r \geq 3$. As in (*b*), letting $w = u - \sqrt{-3}$, which transforms $(\sqrt{-3}, 0)$ to the point $(0,0)$, we find that $\mathbb{Q}(\sqrt{-3})(u(Q_4)) = \mathbb{Q}(\sqrt{2\sqrt{-3}(2 + \sqrt{-3})})$. Since $\mathbb{Q}(E_4)/\mathbb{Q}$ is a Galois extension, we find that $\mathbb{Q}(E_4)/\mathbb{Q}(\sqrt{-3})$ is an Abelian extension of type $(2,2,2,2)$, corresponding via Kummer theory to the subgroup of $\mathbb{Q}(\sqrt{-3})^*/(\mathbb{Q}(\sqrt{-3})^*)^2$ generated by $\{-2 + \sqrt{-3}, -2 - \sqrt{-3}, 2\sqrt{-3}, -1\}$, which is of order 16. Thus $r = 4$. Since the reduction map $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ must induce a surjection $\Gamma_4 \to \Gamma_2$, and $P_2$ is defined over $\mathbb{Q}$, the description of $\Gamma_4$ now follows easily.

(*d*) The condition $ad \equiv 1 \pmod 4$ follows from the fact that $K$ contains $\mathbb{Q}(\sqrt{-1})$. Since $K$ contains $\mathbb{Q}(E_2)$, the image of $\Gamma_4^K$ in $\Gamma_2$ is trivial, so in particular $b \in 2\mathbb{Z}/4\mathbb{Z}$. Finally, it follows from (*b*) and the proof of (*c*) that $\pm P_4$ are the only conjugates of $P_4$ over $K$, and this implies that $c = 0$.

(*e*) From the surjectivity of the determinant (4.1), and (4.2), it suffices to prove that

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z}) \mid c \in 2\mathbb{Z}/8\mathbb{Z} \right\} \subset \Gamma_8.$$

By (c), it suffices to prove that the kernel $\Omega$ of the natural projection $\mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ is in $\Gamma_8$. Note that $\Omega$ is a 3-dimensional $\mathbb{Z}/2\mathbb{Z}$-vector space, generated by $\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$, and $\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$. An argument similar to one in the proof of (4.3*b*) shows that these first two matrices are automatically contained in $\Omega$. As for the last matrix, Cremona's tables show that $\mathrm{Fr}_{59}$ is represented in $\mathrm{GL}_2(\mathbb{Z}_2)$ as a matrix with trace 0 and determinant 59. Therefore the square of this matrix is represented as $-59$ times the identity. Since $-59 \equiv 5 \pmod 8$, we are done. □

The final step before beginning the proof of (0.4) is to show that a suitable linear disjointness property holds over the field $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$.

**(4.5) Theorem.** (*a*) *For any two coprime integers $M$ and $N$, we have $L(E_{M^\infty}) \cap L(E_{N^\infty}) = L$.*

(*b*) *For any two coprime integers $M$ and $N$, we have $K(E_{M^\infty}) \cap K(E_{N^\infty}) = K$.*

(*c*) *Let $\ell$ be a prime number. Then*

$$\Gamma_{2^\infty}^K = \left\{ \begin{pmatrix} a & 2b' \\ 4c' & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_2) \mid ad \equiv 1 \pmod 4,\ b',\ c' \in \mathbb{Z}_2 \right\},$$

$$\Gamma_{3^\infty}^K = \{\gamma \in \mathrm{GL}_2(\mathbb{Z}_3) \mid \det \gamma \equiv 1 \pmod 3\},$$

$$\Gamma_{7^\infty}^K = \{\gamma \in \mathrm{GL}_2(\mathbb{Z}_7) \mid \det \gamma \textit{ is a square}\},$$

$$\Gamma_{\ell^\infty}^K = \mathrm{GL}_2(\mathbb{Z}_\ell) \quad \textit{for all other } \ell.$$

In order to prove this, we recall some facts about groups of invertible two-by-two matrices. In what follows, $\ell$ always denotes an odd prime number.

Recall that the projective special linear group $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is defined by the exact sequence

$$1 \to \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \to \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to 1.$$

**(4.6) Lemma.** *Let $\ell$ be a prime with $\ell \geq 3$.*

(*a*) *The groups $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ are pairwise non-isomorphic; they are simple and non-Abelian for $\ell \geq 5$. Furthermore, when $\ell \geq 5$, $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ does not contain any subgroup isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

(*b*) *Let $\ell \geq 5$. Every homomorphism from $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to a solvable group factors through the determinant homomorphism $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to (\mathbb{Z}/\ell\mathbb{Z})^*$.*

(*c*) *Every homomorphism from $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ to a two-group factors through the determinant homomorphism $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \to (\mathbb{Z}/3\mathbb{Z})^*$.*

(*d*) *Every homomorphism from $\mathrm{GL}_2(\mathbb{Z}_\ell)$ onto a group of order $\ell$ is trivial on $\mathrm{SL}_2(\mathbb{Z}_\ell)$.*

*Proof.* (*a*) is well-known. (*b*) follows from (*a*) and the Jordan-Hölder theorem, which show that the kernel must contain $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. (*c*) The kernel must contain every element of order 3. This includes $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, which generate $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. To prove (*d*), suppose for a contradiction that there is such a homomorphism, and let $G$ be its kernel. Since $G$ is of finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$, it is open and hence closed. Since $\ell$ is odd, $G$ contains every element of order two in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Now notice that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ topologically generate $\mathrm{SL}_2(\mathbb{Z}_\ell)$, and are respectively $\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. □

*Proof of* (4.5*a*). We first prove that $\mathbb{Q}(E_{2^\infty}) \cap \mathbb{Q}(E_{3^\infty}) = \mathbb{Q}(\sqrt{-3})$. Write $F = \mathbb{Q}(E_{2^\infty}) \cap \mathbb{Q}(E_{3^\infty})$. Then $F$ is a Galois extension of $\mathbb{Q}$. By the main result of [S2], the index of $\Gamma_N$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ in bounded independently of $N$, so $F$ is a finite extension of $\mathbb{Q}$. By (4.4) we know that $\mathbb{Q}(E_{2^\infty})$ is a pro-2-extension of $\mathbb{Q}$; it follows that $F$ is a 2-extension of $\mathbb{Q}$. On the other hand, $\mathbb{Q}(E_{3^\infty})$ is a pro-3-extension of $\mathbb{Q}(E_3)$; therefore $F \subseteq \mathbb{Q}(E_3)$. By (4.3) we see that its Galois group is a quotient of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, and by (4.6*c*) and (4.1), we deduce that $F = \mathbb{Q}(\sqrt{-3})$.

Next we show that $\mathbb{Q}(E_{6^\infty}) \cap \mathbb{Q}(E_{7^\infty}) = \mathbb{Q}(\sqrt{-7})$. Again, write $F = \mathbb{Q}(E_{6^\infty}) \cap \mathbb{Q}(E_{7^\infty})$, so that $F$ is a finite Galois extension of $\mathbb{Q}$. Since $\mathbb{Q}(E_{6^\infty})$ is a pro-$\{2,3\}$

extension of $\mathbb{Q}$, $F$ is a $\{2,3\}$-group, hence solvable by Burnside's theorem. Since $\mathbb{Q}(E_{7^\infty})$ is a pro-7 extension of $\mathbb{Q}(E_7)$, $F$ is contained in $\mathbb{Q}(E_7)$. We deduce from (4.6*b*) and (4.1) that $F$ is an Abelian extension of $\mathbb{Q}$ contained in $\mathbb{Q}^{(7)}$. If 3 divided $[F:\mathbb{Q}]$, then $\mathbb{Q}(E_{6^\infty})$ would contain a cyclic extension of $\mathbb{Q}$ of degree 3, but since $\mathbb{Q}(E_{3^\infty})$ and $\mathbb{Q}(E_{2^\infty})$ are linearly disjoint over a quadratic extension, $F \cap \mathbb{Q}(E_{3^\infty})$ would contain a cyclic extension of $\mathbb{Q}$ of degree 3. From (4.6*d*) and (4.1), we find that it would be contained in a field of three-power roots of unity, and hence cannot be contained in $\mathbb{Q}^{(7)}$. Therefore $F = \mathbb{Q}(\sqrt{-7})$, as asserted.

To conclude the proof of (4.5*a*), since $L \subseteq \mathbb{Q}(E_{42^\infty})$, it suffices to show that if $S$ is a finite set of primes containing $\{2,3,7\}$ and $N$ the product of the primes in $S$, then

$$\Gamma_{N^\infty} = \Gamma_{42^\infty} \times \prod_{\substack{\ell' \in S \\ \ell' \neq 2,3,7}} \mathrm{GL}_2(\mathbb{Z}_{\ell'}). \tag{4.7}$$

We do this by induction on the cardinality of $S$, the case $S = \{2,3,7\}$ being trivial. We thus assume $S$ satisfies (4.7) and show that if $\ell$ is a prime not in $S$, then $\mathbb{Q}(E_{N^\infty}) \cap \mathbb{Q}(E_{\ell^\infty}) = \mathbb{Q}$. This implies that (4.7) holds with $S$ replaced by $S \cup \{\ell\}$. We can assume that $\ell$ is greater than all $\ell' \in S - \{2,3,7\}$. Again, write $F$ for $\mathbb{Q}(E_{N^\infty}) \cap \mathbb{Q}(E_{\ell^\infty})$. Again $F$ is a finite Galois extension of $\mathbb{Q}$, so we can pick $n$ sufficiently large that $F \subseteq \mathbb{Q}(E_{N^n}) \cap \mathbb{Q}(E_{\ell^n})$. If $G = \mathrm{Gal}(F/\mathbb{Q})$, then since $F \subseteq \mathbb{Q}(E_{N^n})$, $\#G$ is prime to $\ell$. This is automatic if $\ell > 5$, since $\ell$ does not divide $\ell'$ nor $\#\mathrm{GL}_2(\mathbb{Z}/\ell'\mathbb{Z}) = (\ell'-1)(\ell'^3-\ell')$ for any $\ell' < \ell$. If $\ell = 5$, then it follows since 5 does not divide $\#\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) = 2^5 \cdot 3^2 \cdot 7$. Hence $F \subseteq \mathbb{Q}(E_\ell)$. Thus there is a surjection from $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ to $G$, and so, by the Jordan-Hölder theorem, the composition series for $G$ is a subset of the composition series for $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which consists of Abelian simple groups and $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Since also the composition series of $G$ is a subset of that of $\Gamma_{N^n}$, it cannot contain $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ by (4.6*a*). Therefore $G$ is solvable, and so, by (4.6*b*), $F \subseteq \mathbb{Q}^{(\ell)}$, so is ramified only at $\ell$. Since $E$ has good reduction at $\ell$, and $F \subseteq \mathbb{Q}(E_{N^n})$, $F$ is unramified at $\ell$. We deduce that $F$ is everywhere unramified and therefore equal to $\mathbb{Q}$.

(*b*) Since $K = L(i)$ and $i \in \mathbb{Q}(E_4)$, this follows from the proof of (*a*).

(*c*) now follows easily from (*b*). Suppose $\ell \neq 2$. Since $\mathrm{Gal}(K/\mathbb{Q})$ is a two-group, $K \cap \mathbb{Q}(E_{\ell^\infty}) \subseteq \mathbb{Q}(E_\ell)$. Then we have a surjection from $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{Gal}(\mathbb{Q}(E_\ell) \cap K/\mathbb{Q})$. Since $K$ is an Abelian extension, by (4.6*b*) and (4.6*c*), this map factors through the determinant, so $\mathbb{Q}(E_\ell) \cap K \subseteq \mathbb{Q}^{(\ell)}$. When $\ell > 7$, this means $K$ is linearly disjoint from $\mathbb{Q}(E_{\ell^\infty})$, and so $\Gamma^K_{\ell^\infty} = \mathrm{GL}_2(\mathbb{Z}_\ell)$ by (4.3). Similarly, $K \cap \mathbb{Q}(E_{7^\infty}) = \mathbb{Q}(\sqrt{-7})$, and this gives the condition that the determinant of an element of $\Gamma^K_{7^\infty}$ is a square. The same argument works for $\Gamma^K_{3^\infty}$. The description of $\Gamma^K_{2^\infty}$ then follows from (4.4*d*) and (4.4*e*) together with the surjectivity of $\Gamma^K_{2^\infty} \to \Gamma^K_4$. □

*Proof of* (0.4). Let $N \geq 2$ be an integer, and let $P \in \Theta(\overline{K})$ be of order $N$. Write $N$ as $2^a M$ with $M$ odd, and write $P = P_2 + P_M$, with $P_2$ of order $2^a$ and $P_M$ of order $M$. Suppose first that $a \leq 1$. Then, as in Step V in the proof of (0.3), we conclude that $M$ divides 3. But in §2, we saw that the only points of $J_6$ contained in $\Theta$ are in $J_2$.

Suppose next that $a > 1$. Using (1.8*b*), (1.8*e*) and (4.5), we see that there exists $\sigma \in G_K$ such that $\sigma(P) = -P_2 + P_M$, and $-P_2 \neq P_2$. Then by (1.7), $K(\sigma(P), P)$ is an extension of $K(2P_2)$ of degree at most 2. Now $P_M$ is a multiple of $P$ and

therefore defined over $K(\sigma(P), P)$, so that, since $M$ is odd, linear disjointness over $K$ implies that $[K(P_M) : K] \leq 2$. We know from (3.2) and (3.1$b$) that there are $K$-isogenies $\phi : J \to E^2$ and $\phi' : E^2 \to J$ whose composite is multiplication by 2. It follows as in Step I in the proof of (0.3) that $K(P_M) = K(\phi(P_M))$. Suppose $M > 1$, and let $\ell$ be a prime dividing $M$. Then $\ell$ is odd, so by (4.5) $\Gamma_\ell^K$ contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and this group acts transitively on the set of $\ell^2 - 1$ points of $E_{\mathrm{tors}}$ of order $\ell$. Since some multiple of $\phi(P_M)$ is of order $\ell$, we deduce that $K(P_M)$ contains $K(Q)$ for some point $Q \in E_{\mathrm{tors}}$ of order $\ell$, and so $[K(P_M) : K] \geq \ell^2 - 1 \geq 3^2 - 1 = 8$, which is impossible. Therefore $M = 1$ and $P$ is of order $2^a$. But, using (1.8), we then find that $3 \in \mathrm{Hty}(J, K, 2^\infty)$, and so we conclude using (1.6$b$) that $a = 1$, a contradiction. □

## 5. The curve $y^2 - y = x^5$

Finally, we discuss the case of the curve with affine model $y^2 - y = x^5$. Throughout this section, we will denote this curve by $C$ and its Jacobian by $J$.

We first recall some properties of $C$ and $J$. Let $\zeta$ be a primitive fifth root of unity; then $C$ has an automorphism of order 5 that sends the point $(x, y)$ to the point $(\zeta x, y)$. This automorphism fixes $\infty$ and therefore induces an automorphism of $J$ that we also denote by $\zeta$. Thus, $J$ has complex multiplication by the ring of integers $\mathbb{Z}[\zeta]$ of the field $\mathbb{Q}(\zeta)$ of fifth roots of unity. As a consequence, $K(J_{\mathrm{tors}})$ is an Abelian extension of $K$. In contrast with the cases (0.3) and (0.4), $J$ is an absolutely simple Abelian variety.

We recall some standard properties of $K$. It is a cyclic extension of $\mathbb{Q}$ of degree 4. If $\alpha \in K$, we write $\alpha_i$ for the image of $\alpha$ under the automorphism $\tau_i$ of $K$ that sends $\zeta$ to $\zeta^i$.

**(5.1) Lemma.** (*a*) *The ring $\mathfrak{O}_K = \mathbb{Z}[\zeta]$ is a principal ideal domain. The extension $K/\mathbb{Q}$ is unramified outside 5, where it is totally ramified. Let $\theta = 1 - \zeta$. Then $\theta\mathfrak{O}_K$ is the unique prime ideal of $\mathfrak{O}_K$ lying above 5. We have $\theta^4\mathfrak{O}_K = 5\mathfrak{O}_K$. The rational prime $p$ splits in $K$ into four primes of degree one when $p \equiv 1 \pmod 5$, into two primes of degree two when $p \equiv -1 \pmod 5$, and remains prime in all other cases. Let $\epsilon = (-1 + \sqrt{5})/2$. Then $\epsilon$ is a unit of $\mathfrak{O}_K$, and every element of $\mathfrak{O}_K^*$ can be written uniquely as $\pm\zeta^a\epsilon^n$ with $0 \leq a \leq 4$ and $n \in \mathbb{Z}$.*

(*b*) *If $\eta \in \mathfrak{O}_K^*$ satisfies $\eta \equiv 1 \pmod{\theta^2}$, then $\eta_1\eta_3 = 1$. Every integral ideal $\mathfrak{a}$ of $K$ not divisible by $\theta\mathfrak{O}_K$ has a generator $\alpha$ satisfying $\alpha \equiv 1 \pmod{\theta^2}$.*

Here (*a*) is standard, and (*b*) follows by a simple calculation from the final assertion of (*a*).

In what follows, we write $(\alpha)$ for the ideal generated by $\alpha \in \mathfrak{O}_K$.

**(5.2) Lemma.** *The curve $C$ acquires everywhere good reduction over the field $L = K(\sqrt[5]{2}, \sqrt{\theta})$.*

This is well-known. See for instance [G3], Lemma 2, or [BoMM-B], section 4.1.

Unlike the situation in §4, this information suffices to establish linear disjointness over $K$.

**(5.3) Proposition.** *Let $M$ and $N$ be two coprime rational integers. Then $K(J_M) \cap K(J_N) = K$.*

In order to prove this, we need one further lemma.

**(5.4) Lemma.** (*a*) *There is no quadratic extension of $K$ unramified outside $\theta$.*
(*b*) *There is no Galois quintic extension of $K$ unramified outside* 2.

*Proof of* (5.4). (*a*) Indeed, such an extension would have to have conductor $\theta$. By (5.1), every prime ideal prime to $\theta$ has a generator congruent to one (mod $\theta$), so $K$ is its own ray class field of conductor $\theta$. Similarly for (*b*): such an extension would be of conductor 2, but $\#\big((\mathfrak{O}_K/2\mathfrak{O}_K)^*\big) = 15$ and the image of $\mathfrak{O}_K^*$ in $(\mathfrak{O}_K/2\mathfrak{O}_K)^*$ contains the subgroup of order 5 generated by the image of $\zeta$, and a subgroup of order 3 generated by $\epsilon$. Hence $K$ is its own ray class field of conductor 2. □

*Proof of* (5.3). Write $F = K(J_M) \cap K(J_N)$, so that $F$ is an Abelian extension of $K$. Since $J$ has good reduction over $K$ at all primes except $\theta$, $K(J_M)/K$ is ramified only at $\theta$ and at primes dividing $M$. Similarly $K(J_N)/K$ is ramified only at $\theta$ and at primes dividing $N$. It follows that $F$ is ramified only at $\theta$. Furthermore, since $K$ is of class number one and totally complex, $F/K$ is totally ramified at $\lambda$. Now let $L$ be the field defined in (5.2). Hence $L(J_M)/L$ is ramified only at primes dividing $M$ and $L(J_N)/L$ is ramified only at primes dividing $N$, and we deduce that $LF$ is an everywhere unramified extension of $L$. By (5.4*a*), $L$ is totally ramified at 2; hence $F$ and $L$ are linearly disjoint over $K$ and $F$ is the inertia field of 2 in $LF/K$. Let $I$ be the inertia field of $\theta$ in $LF$ over $K$. Since $\theta$ is totally ramified in $L$ and then unramified in $LF$, we find, comparing ramification degrees, that $IL = LF$, that $[I : K] = [LF : L] = [F : K]$, and that $[F : K]$ divides $[L : K]$. Note that $L$ is a cyclic extension of $K$ of degree ten. Suppose therefore that $F$ were not equal to $K$. Then either 2 would divide $[F : K]$, and so $F$ would contain a quadratic extension of $K$ unramified outside $\theta$, in contradiction to (5.4*a*); or 5 would divide $[F : K]$ and, since $[I : K] = [F : K]$, $I$ would contain a quintic Galois extension of $K$ unramified outside 2, in contradiction to (5.4*b*). Therefore $F = K$. □

In order to prove (0.2), we need to study the action of $G_K$ on $J_{\text{tors}}$ in more detail. We will use standard results from the theory of complex multiplication as given in [ShT] and [W]. A standard calculation shows that the action of $\zeta$ on $C$, extended to divisor classes, endows $J$ with a CM-type of $\{\tau_1, \tau_2\}$ which describes the isomorphism $\mathfrak{O}_K \simeq \text{End}_{\overline{K}} J$. Let $\nu$ be an element of $\mathfrak{O}_K$, and write $J_\nu$ for the subgroup of $J_{\text{tors}}$ killed by the endomorphism $\nu$ of $J$. Since $\mathfrak{O}_K$ is a Dedekind domain, one knows that $J_\nu \simeq \mathfrak{O}_K/\nu\mathfrak{O}_K$ as an $\mathfrak{O}_K$-module, so that the action of $G_K$ on $J_\nu$ gives rise to a homomorphism $G_K \to (\mathfrak{O}_K/\nu\mathfrak{O}_K)^*$. In particular, $K(J_\nu)$ is an Abelian extension of $K$. The following lemma gives a precise description of this action.

**(5.5) Lemma.** *Let $\nu \in \mathfrak{O}_K$. Then for every prime ideal $\mathfrak{p}$ of $K$ not dividing $\theta\nu$, and for all $P \in J_\nu$, we have*

$$(\mathfrak{p}, K(J_\nu)/K)P = \pi_1\pi_3 P,$$

*where $\pi$ is any generator of $\mathfrak{p}$ with $\pi \equiv 1 \pmod{\theta^2}$.*

For the proof, one can consult [G1], Lemma 7. Note that, by (5.1*b*), the product $\pi_1\pi_3$ is independent of the choice of a generator $\pi$.

Let $I(\theta)$ be the group of fractional ideals of $K$ prime to $\theta$. We define a homomorphism $\lambda : I(\theta) \to K^*$ by $\lambda(\mathfrak{a}) = \alpha_1\alpha_3$, $\alpha$ being any generator of $\mathfrak{a}$ with $\alpha \equiv 1 \pmod{\theta^2}$. Writing $\Gamma_\nu^K$ for the image of $G_K$ in $(\mathfrak{O}_K/\nu\mathfrak{O}_K)^*$, we conclude that $\Gamma_\nu^K$ consists of the residue classes of the form $\alpha_1\alpha_3$ for some $\alpha \equiv 1 \pmod{\theta^2}$ prime to $\theta\nu$.

**(5.6) Lemma.** *Let $N$ be a rational integer not divisible by 5. Then*

$$\mathrm{Hty}(J,K,N) = (\mathbb{Z}/N\mathbb{Z})^*.$$

*Proof.* Let $a$ be any integer relatively prime to $N$. By Dirichlet's theorem, there is a prime $p$ congruent to 1 (mod 5) and congruent to $a$ (mod $N$). Let $\pi$ by a generator of any prime of $K$ above $p$ with $\pi \equiv 1 \pmod{\theta^2}$. Let $\alpha = \pi_1\pi_4$. Then $\alpha_1\alpha_3 = \pi_1\pi_2\pi_4\pi_3 = N(\pi_1) = p$. So $p \in \mathrm{Hty}(J,K,N)$. □

Let $\mathfrak{O}_{K,\theta}$ be the completion of $\mathfrak{O}_K$ at $\theta$. Thus the action of $\mathfrak{O}_K$ on $J_{\theta^n}$ for all $n$ induces a continuous action of $\mathfrak{O}_{K,\theta}$ on $J_{\theta^\infty}$.

When $P \in J_{\mathrm{tors}}$, by the order of $P$ we mean the annihilator ideal of $P$ as an element of the $\mathfrak{O}_K$-module $J_{\mathrm{tors}}$.

**(5.7) Lemma.** (*a*) *We have $\Gamma^K_{\theta^\infty} \subseteq (1+\theta^3\mathfrak{O}_{K,\theta})^\times$.*

(*b*) *Let $k \in \mathbb{Z}$ with $k \geq 3$ and $k \not\equiv 2 \pmod 4$. Then there exists $c \in \mathfrak{O}^*_{K,\theta}$ such that $1 + c\theta^k \in \Gamma^K_{\theta^\infty}$.*

(*c*) *Let $n \in \mathbb{Z}$ with $n \geq 4$. If $Q \in J_{\mathrm{tors}}$ be a point of order $(\theta^n)$, then there exist $\sigma \in G_K$ and $R \in J_{\theta^2}$ with $R \neq O_J$ and $\sigma(Q) = Q + R$.*

*Proof.* We first note that $\theta_3 = (1+\zeta+\zeta^2)\theta = (3 - 3\theta + \theta^2)\theta$. As for (*a*), every element of $(1+\theta^2\mathfrak{O}_{K,\theta})^\times$ is congruent (mod $\theta^3$) to one of the form $1 + a\theta^2$ with $a \in \mathbb{Z}$. But then

$$(1+a\theta^2)(1+a{\theta_3}^2) \equiv 1 + a(\theta^2 + {\theta_3}^2) \equiv 1 + a(1+3^2)\theta^2 \equiv 1 \pmod{\theta^3}.$$

Similarly for (*b*), $(1+\theta^k)(1+{\theta_3}^k) \equiv 1 + (1+3^k)\theta^k \pmod{\theta^{k+1}}$. Since $1+3^k$ is not divisible by 5 unless $k \equiv 2 \pmod 4$, this gives (*b*). Finally, (*c*) is a consequence of (*b*). If $n \not\equiv 3 \pmod 4$, we take $\sigma$ such that its image in $\Gamma^K_{\theta^\infty}$ is $1 + c\theta^{n-1}$, in which case $R$ is $c\theta^{n-1}Q$. If $n \equiv 3 \pmod 4$, we take $\sigma$ such that its image in $\Gamma^K_{\theta^\infty}$ is $1 + c\theta^{n-2}$, in which case $R$ is $c\theta^{n-2}Q$. In either case $R$ is a non-zero element of $J_{\theta^2}$. □

**(5.8) Lemma.** *Let $\nu$ be an element of $\mathfrak{O}_K$ such that $(\nu) \neq (\theta^n)$ with $0 \leq n \leq 3$. Then $\#(\Gamma^K_\nu) \geq 4$.*

*Proof.* Since $K(J_{\nu'})$ is contained in $K(J_\nu)$ whenever $(\nu')$ divides $(\nu)$, we reduce to the case where either $(\nu) = (\theta^4)$ or $\nu$ generates a prime ideal $\mathfrak{l} \neq (\theta)$ of $K$. Now (5.7a) shows that $\Gamma^K_{\theta^\infty}$ is a pro-5-group, so that the degree of any non-trivial finite extension of $K$ contained in $J_{\theta^\infty}$ is a power of five. But (5.7c) shows that $\Gamma^K_{\theta^\infty}$ acts non-trivially on $J_{\theta^4}$. On the other hand, if $(\nu)$ is a prime ideal $\mathfrak{l} \neq (\theta)$, let $\ell$ be the rational prime dividing $\mathfrak{l}$. Since the kernel of the map $\mathbb{Z} \to \mathfrak{O}_K \to \mathfrak{O}_K/\mathfrak{l}$ is $\ell\mathbb{Z}$, we deduce from (5.6) that for every $a \in \mathbb{Z}$ that is not a multiple of $\ell$, there exists $\sigma \in G_K$ such that $\sigma(P) = aP$ for all $P \in J_\mathfrak{l}$. The result follows immediately when $\ell \geq 7$. When $\ell = 2$ we find that if $\mathfrak{a} = (1-\theta^2)$ then $\lambda(\mathfrak{a}) \equiv \zeta^3 \pmod{2\mathfrak{O}_K}$, so that $\Gamma^K_2$ contains an element of order five. Similarly, when $\ell = 3$ we find that if $\mathfrak{a} = (1-\theta^3)$ then $\lambda(\mathfrak{a}) \equiv \zeta^2 \pmod{3\mathfrak{O}_K}$, so again $\Gamma^K_2$ contains an element of order 5. □

*Proof of* (0.2). Let $P \in \Theta(\overline{K}) \cap J_{\mathrm{tors}}$ be a point whose order is the ideal $(\nu)$. Writing $\nu = \theta^n\mu$ with $n \in \mathbb{N}$ and $\mu$ prime to $\theta$, we have a corresponding decomposition $P = P_\theta + P_\mu$ where $P_\theta$ is of order $(\theta^n)$ and $P_\mu$ of order $(\mu)$. We shall prove that

either $(\mu) = \mathfrak{O}_K$ and $n \leq 3$, or $(\mu) = (2)$ and $n = 0$. This will show that every point in $\Theta(\overline{K}) \cap J_{\text{tors}}$ is of integer order 2 or 5. This reduces the determination of $\Theta(\overline{K}) \cap J_{\text{tors}}$ to a calculation as described in §2 with $N = 5$, and this gives the points listed in (0.2).

We consider successively the other possibilities for $n$ and $\mu$, repeatedly using the linear disjointness proposition (5.3). We also need to recall that if $P$ is a point of order $(\nu)$, then $P$ generates $J_\nu$ as an $\mathfrak{O}_K$-module. Since all the endomorphisms are defined over $K$, this means that $K(P) = K(J_\nu)$. We define the maps $\pi$ and $\epsilon$ as in §1.

(*i*) $n = 0$ and (2) does not divide $(\mu)$. Choose an odd rational integer $M$ divisible by $\mu$. Using (5.6), we see that $2 \in \text{Hty}(J, K, M)$, so this case is impossible by (1.6*a*).

(*ii*) $2|\nu$, $(2) \neq (\nu)$. Say $\nu = 2^a\rho$, with $\rho$ prime to 2. Write $P_\nu = P_2 + P_\rho$, where $P_2$ is of order $2^a$ and $P_\rho$ is of order $(\rho)$. If $a > 1$, by (5.6) $1 + 2^{a-1}$ is a homothety on $J_{2^\infty}$, so there is a Galois element $\sigma$ such that $\sigma(a) = a + R$, where $R \in J_2$, $R \neq O_J$. If $a = 1$, such a $\sigma$ also exists by (5.8). In any case, we can assume that $\sigma$ fixes $P_\rho$. Then $\sigma(P) - P = R$. Let $\xi_R$ and $\eta_R$ be the two points of $C(\overline{K})$ such that $R = \pi(\xi_R + \eta_R)$ as in §1. Since $P \in \Theta(\overline{K})$ and $\Theta$ is defined over $K$, $\sigma(P) \in \Theta(\overline{K})$. Therefore, from the uniqueness in (1.3), we deduce that $\{\sigma(P), -P\} = \{\epsilon(\xi_R), \epsilon(\eta_R)\}$. But then, by (2,1a), we deduce that $P$ and $\sigma(P)$ are of order two, which is a contradiction.

(*iii*) $1 \leq n \leq 3$ and $(\mu) \neq (1)$. By (*ii*) we can assume that $(\mu) \neq (2)$. Using (5.6), we choose $\sigma$ such that $\sigma(P_\mu) = -P_\mu \neq P_\mu$. Since $J_{\theta^3}$ is defined over $K$, we have $\sigma(P) = P_\theta - P_\mu$, and so $\sigma(P) + P = 2P_\theta$. By an argument similar to (*ii*), we see that $\{\sigma(P), P\} = \{\epsilon(\xi), \epsilon(\eta)\}$, where $\xi$ and $\eta \in C(\overline{K})$ are such that $\pi(\xi + \eta) = 2P_\theta$. It follows from (1.4) that $P$ and $\sigma(P)$ are defined over a quadratic extension of $K(2P_\theta) = K$, and this contradicts (5.8).

(*iv*) $n \geq 4$. This time, we take $\sigma$ such that $\sigma(P_\theta) = P_\theta + R$ with $R \in J_{\theta^2}$; that this is possible follows from (5.7*c*). We suppose $\sigma$ acts trivially on $P_\mu$. Then $\sigma(P) - P = R$, so that $P$ is defined over an extension of $K(R) = K$ of degree at most two. But this contradicts (5.8). □

*Remark.* It follows from (5.7*a*) and (5.8) that $J_{\text{tors}}(K) = J_{\theta^3}$. That $J_{\theta^3} \subseteq J(K)$ was proved by Greenberg [Gr]. The points $(0, 0)$ and $(0, 1)$ are stable under the automorphism $\zeta$ of $C$, so that their images $P_0$ and $P_1$ in $\Theta$ are of order $(\theta)$. One can verify that the points $(\zeta^i, (1 \pm \sqrt{5})/2)$, $1 \leq i \leq 5$, are of order $(\theta^3)$. One can also deduce (0.2) directly from (0.1). Since in fact $P_1 = -P_0$ by (1.5*b*), the other two non-zero points of $J_\theta$ are $\pm 2P_0$; they cannot lie in $\Theta$ because of (1.5*c*). But the points of $J_{\text{tors}} \setminus J_\theta$ are not fixed by $\zeta$, so any point of $\Theta(\overline{K}) \cap J_{\text{tors}}$ not in $J_\theta$ would in fact give rise to an orbit of 5 such points. Hence if $\Theta(\overline{K}) \cap J_{\text{tors}}$ contained a nineteenth point, it would in fact contain at least twenty-three points. But 11 is split in $K$, so $J$ has good ordinary reduction at 11 and (0.1) therefore shows that $\#(\Theta(\overline{K}) \cap J_{\text{tors}}) \leq 22$.

## References


[BoMM-B] J.-B. Bost, J.-F. Mestre, L. Moret-Bailly, *Calculs explicite en genre 2*, Astérisque **183** (1990), 69–106. MR **92g:**14018b

[B] A. Buium, *Geometry of p-jets*, Duke Math. Jour. **82** (1996), 349–367. MR **97c:**14029

[Ca] D. Cantor, *On the analogue of the division polynomials for hyperelliptic curves*, Crelle **447** (1994), 91–145. MR **94m:**11071

[CasFl] J. W. S. Cassels, E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996. MR **97i:**11071

[C1] R. F. Coleman, *Torsion points on curves and p-adic Abelian integrals*, Annals of Math. **121** (1985), 111–168. MR **86j:**14014

[C2] R. F. Coleman, *Torsion points on Fermat curves*, Composition Math. **58** (1986), 191–208. MR **87k:**14019

[C3] R. F. Coleman, *Ramified torsion points on curves*, Duke Math. J. **54** (1987), 615–640. MR **89c:**14033

[CKR] R. F. Coleman, B. Kaskel, K. A. Ribet, *Torsion points on* $X_0(N)$, in Automorphic Forms, Automorphic Representations, and Arithmetic, Proc. Sympos. Pure Math., vol. 66, part 1, 1999, pp. 27–49. CMP 99:16

[CTT] R. F. Coleman, A. Tamagawa, P Tzermias, *The cuspidal torsion packet on the Fermat curve*, J. Reine Angew. Math. **496** (1998), 73–81. MR **99b:**11066

[Cr] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1992. MR **93m:**11053

[DaPh] S. David, P. Philippon, *Minorations des hauteurs normalisées de sous-variétés de variétés abéliennes*, Cont. Math. **210** (1998), 333-364. MR **98j:**11044

[D] M. Deuring, *Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins, I–IV*, Gott. Nach. (1953). MR **15:**779d

[FK] G. Frey, E. Kani, *Curves of genus 2 covering elliptic curves and an arithmetic application*, Prog. Math. **89** (1991), 153–175. MR **91k:**14014

[G1] D. Grant, *A proof of quintic reciprocity using the arithmetic of* $y^2 = x^5 + 1/4$, Acta Arith **LXXV.4** (1996), 321–337. MR **97b:**11083

[G2] D. Grant, *Units from* 5*-torsion on the Jacobian of* $y^2 = x^5 + 1/4$ *and the conjectures of Stark and Rubin*, J. Number Theory **77** (1999), 227–251. CMP 99:16

[G3] D. Grant, *Units from* 3*- and* 4*- torsion on Jacobians of curves of genus* 2, Compositio Math. **95** (1994), 311–320. MR **95j:**11053

[Gr] R. Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. **42** (1981), 345–359. MR **82j:**14036

[H] M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), 575–603. MR **89k:**11046

[I] J. Igusa, *Arithmetic variety of moduli for genus two*, Annals of Math. **72** (1960), 612–649. MR **22:**5637

[Ku] R. Kuhn, *Curves of genus 2 with split Jacobian*, Trans. AMS **307** (1988), 41–49. MR **89f:**14027

[L] S. Lang, *Division points on curves*, Ann. Math. Pura Appl. **LXX** (1965), 229–234. MR **32:**7560

[P] A. Pillay, *Model theory and diophantine geometry*, Bull. Amer. Math. Soc. **34** (1997), 405–422. MR **98h:**11164a

[R1] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*, Invent. Math. **71** (1983), 207–233. MR **84c:**14021

[R2] M. Raynaud, *Sous-variétés d'une variété abélienne et points de torsion*, Prog. Math. **35** (1983), 327–352. MR **85k:**14022

[S1] J.-P. Serre, *Abelian* $l$*-adic representations and elliptic curves*, Benjamin, New York, 1968. MR **41:**8422

[S2] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331. MR **52:**8126

[Sha] D. Shaulis, *Torsion points on the Jacobian of a hyperelliptic image of a Fermat curve*, PhD. Thesis, University of Colorado at Boulder (1998).

[ShT] G. Shimura, Y. Taniyama, *Complex multiplication of Abelian varieties and its applications to number theory,* Publ. Math. Soc. Japan No. 6, 1961. MR **23:**A2419

[Si] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986. MR **87g:**11070

[St] H. Stark, *The Coates-Wiles theorem revisited*, Prog. Math. **36** (1982), 349–362. MR **84c:**14039

[U] E. Ullmo, *Positivité et discrétion des points algébriques de courbes*, Annals of Math. (2) **147** (1998), 167–179. MR **99e:**14031

[W] A. Weil, *On a certain type of character of the idele class group*, Proc. Int. Symp. Algebraic Number Theory, Kyoto (1955), 1–7. MR 18,720e

CNRS, UPRESA 6081, Département de Mathématiques et de Mécanique, Université de Caen, Boulevard maréchal Juin, B.P. 5186, 14032 Caen cedex, France

*E-mail address*: boxall@math.unicaen.fr

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395

*E-mail address*: grant@boulder.colorado.edu