5-TORSION POINTS ON CURVES OF GENUS 2

JOHN BOXALL, DAVID GRANT AND FRANCK LEPRÉVOST

To Irwin Fischer, in memoriam

Introduction

Let C be a smooth proper curve of genus 2 over an algebraically closed field k. Fix a Weierstrass point ∞ in $C(k)$ and identify C with its image in its Jacobian J under the Albanese embedding that uses ∞ as base point. For any integer $N \geqslant 1$, we write J_N for the group of points in $J(k)$ of order dividing N and J_N^* for the subset of J_N of points of order N. It follows from the Riemann–Roch theorem that $C(k) \cap J_2$ consists of the Weierstrass points of C and that $C(k) \cap J_3^*$ and $C(k) \cap J_4^*$ are empty (see [**3**]). The purpose of this paper is to study curves C with $C(k) \cap J_5^*$ non-empty.

While the question is geometric in nature, the original motivation for this work is an attempt to associate units in algebraic number fields to torsion points on Abelian varieties in a manner analogous to elliptic units built up from elliptic curves. This has been done successfully for 3- and 4-torsion on the Jacobians of genus 2 curves [**2**, **8**]. (For other results on this see [**1**, **5**, **7**, **9**, **13**].)

We now describe the contents of the paper. Throughout, k denotes an algebraically closed field. In Section 1, we recall some general properties of genus 2 curves and show that $\#(C(k) \cap J_5^*) \leqslant 12$ in every characteristic $\neq 2$ and that, when C is the curve given by $y^2 + y = x^5$ and ∞ is the point at infinity, then $\#(C(k) \cap J_5^*) = 12$ in characteristic $\neq 2$ and $\#(C(k) \cap J_5^*) = 32$ in characteristic 2. In Section 2 we discuss families of curves having points of order 5. If F is any field, every triple (C, ∞, P) over F with C of genus 2, $\infty \in C(F)$ a Weierstrass point, and $P \in C(F) \cap J_5^*$ is F-isomorphic to a triple $(y^2 + (ax^2 + bx + c)\, y = x^5, \infty, (0,0))$ with $a, b, c \in F$ and $c \neq 0$, two triples (C, ∞, P) and (C', ∞', P') being F-isomorphic if there exists an F-isomorphism from C to C' that takes ∞ to ∞' and P to P'. We also sketch a construction of the coarse moduli space of isomorphism classes of triples. In Section 3 we discuss isomorphism classes of quadruples (C, ∞, P_1, P_2), with $P_1, P_2 \in C(F) \cap J_5^*$, $P_2 \neq P_1, \iota(P_1)$, where ι is the hyperelliptic involution. Each class contains a quadruple $(y^2 + (ax^2 + bx + c)\, y = x^5, \infty, (0,0), P)$. We find that in characteristic $\neq 5$, the isomorphism classes of quadruples are parametrised by the union of three rational curves (in characteristic 5, one finds that $\#(C(k) \cap J_5^*) \leqslant 2$). In Section 4, we study curves having three or more pairs of 5-torsion points. We describe, in every characteristic, the finitely many isomorphism classes of pairs (C, ∞) such that $\#(C(k) \cap J_5^*) \geqslant 6$.

1. *Preliminary results and notations*

Recall that throughout the paper k denotes an algebraically closed field. We first recall some basic properties of genus 2 curves over k (see [**10**] or [**3**, §1 and §2]). If

Received 5 July 1999; final revision 20 September 2000.

2000 *Mathematics Subject Classification* 14H45, 14H40.

J. London Math. Soc. (2) 64 (2001) 29–43.

C is such a curve, the canonical morphism $C \longrightarrow \mathbb{P}^1_k$ is separable of degree 2, so that C has an induced involution ι. If we choose the canonical morphism to be ramified over the point at infinity of $\mathbb{P}^1_k$, the Riemann–Roch theorem shows that C has an affine model $y^2+g(x)\,y=f(x)$, where g is of degree at most 2 and f is monic of degree 5. When $\operatorname{char} k \neq 2$, we can always take $g=0$. Then ι takes the point (x, y) to the point $(x, -y-g(x))$. The Weierstrass points of C other than ∞ are the points P where $2y+g(x)$ vanishes. That is, they are precisely the fixed points of the involution. When $\operatorname{char} k \neq 2$, there are six Weierstrass points. When $\operatorname{char} k = 2$, there are either one, two or three Weierstrass points. In what follows, ∞ will always denote the lone point at infinity for this model. Let J be the Jacobian of C. We will identify points of C with their image in J under the Albanese map with base point ∞. Under this identification, $\iota(P) = -P$ in the group law of J. Let $\delta(C)$ be the discriminant of C, as given in [**15**]. Recall that if $F=\sum_{i=0}^{5} F_i x^i$ and $G=\sum_{i=0}^{2} G_i x^i$ are polynomials in $\mathbb{Z}[F_i, G_j, x]$ and if δ is 2^8 times the discriminant with respect to x of $F+\frac{1}{4}G^2$, then δ lies in $\mathbb{Z}[F_i, G_j]$. Then $\delta(C)$ is the image of δ when the coefficients of F and G are specialised to those of f and g. The model $y^2+g(x)\,y=f(x)$ represents a non-singular curve of genus 2 if and only if $\delta(C)\neq 0$.

In the same spirit as [**3**, Proposition 2.2] (see also [**4**] and [**14**]), we obtain the following more general result.

PROPOSITION 1.1. *Assume that C is given by a model $y^2+g(x)\,y=f(x)$ with f, g as above. Let $P\in C(k)$ be a point of order $N\geqslant 5$ and write $x_0=x(P)$. Then there exist coprime polynomials Φ, $\Psi\in k[x]$ satisfying*

$$\Phi(x)^2-\Phi(x)\,\Psi(x)\,g(x)-f(x)\,\Psi(x)^2=(-1)^N\,(x-x_0)^N,$$

where, if N is even, Φ is monic of degree $N/2$ and Ψ is of degree at most $(N-6)/2$, while if N is odd, Ψ is monic of degree $(N-5)/2$ and Φ is of degree at most $(N-1)/2$. Conversely, let $x_0\in k$ and suppose one can find a pair of coprime polynomials $\Phi, \Psi\in k[x]$ satisfying all these properties. Then the two points P with $x(P)=x_0$ are of order dividing N.

As discussed in [**3**, §2], one can use this to find all the points of $C(k)\cap J_N$ when C and N are given with N small.

EXAMPLE 1.2. Let C be the curve $y^2+y=x^5$ over a field k of characteristic $\neq 5$. Take $N=5$, so that $\Psi(x)=1$ and $\Phi(x)=px^2+qx+r$ is of degree at most 2.

(i) Suppose that $\operatorname{char} k\neq 2$. As is well known (see for example [**3**]) one finds that $C(k)\cap J_5^*$ consists of the 12 points P with $x(P)^6=x(P)$.

(ii) Suppose now that $\operatorname{char} k=2$. Then the points P with $x(P)=x_0$ are of order 5 if and only if we can find p, q and $r\in k$ such that

$$p^2x^4+(q^2+p)\,x^2+qx+(r^2+r)=x_0\,x^4+x_0^4\,x+x_0^5.$$

Comparing coefficients and eliminating p, q and r shows that there are solutions if and only if $x_0^{16}=x_0$. We conclude that, in characteristic 2, $C(k)\cap J_5^*$ consists of the 32 points P satisfying $x(P)^{16}=x(P)$. However, as pointed out by Igusa (see the final pages of [**10**]), the automorphism group of C is generated, modulo ι, by

transformations of the form $(x,y)\longmapsto(\zeta x,y)$ and $(x,y)\longmapsto(x+\alpha,y+\alpha^8x^2+\alpha^4x+\beta)$, where $\zeta^5=1$, $\alpha^{16}=\alpha$ and $\beta^2+\beta=\alpha^5$. We deduce from this that $C(k)\cap J_5^*$ is a single orbit under the automorphism group of C.

In the same way, continuing to assume that $\operatorname{char}k=2$, we find that the curve $y^2+y=x^5+\mu x^3$ has no 5-torsion unless $\mu=0$. It follows from results of Igusa [**10**] that every genus 2 curve in characteristic 2 having a unique Weierstrass point is isomorphic to a curve of the form $y^2+y=x^5+\mu x^3$.

PROPOSITION 1.3. *Let C be a curve of genus 2 defined over a field k of characteristic $\neq 2$, given by $y^2=f(x)$, for f a monic quintic. Then $P\neq\infty$ is of order 5 if and only if $x(P)$ is a repeated root of the degree 12 polynomial*

$$t=f'^3-2f''f'f+4(\tfrac{1}{3}f''')f^2.$$

In particular, $\#(C(k)\cap J_5^*)\leqslant 12$.

Proof. First assume that $\operatorname{char}k\geqslant 5$. If $5P\sim 5\infty$, there must be a function F of the form $y+\Phi(x)$ with $\Phi(x)=px^2+qx+r$ whose divisor is $5P-5\infty$. Since P is not a Weierstrass point, the function $x_P=x-x(P)$ is a local parameter at P. Thus if we expand F in the local ring at P as $F=\sum_{i\geqslant 0}a_ix_P^i$, then $a_i=0$ for $0\leqslant i<5$. Hence at P, $y'''=F'''$ and $y''''=F''''$ must simultaneously vanish (where a prime denotes the derivation of the function field of C extending the derivation d/dx of $k(x)$). Now $t=\frac{8}{3}y^5y'''$, so must have a repeated root at P. Conversely, if t has a repeated root at P, then p, q and r can be chosen so that $a_i=0$ for $0\leqslant i<5$, so F has a zero of order 5 at P. Since the polar divisor of F is 5∞, the divisor of F is $5P-5\infty$, and $5P\sim 5\infty$. A similar argument works when $\operatorname{char}k=3$, provided that we understand $\frac{1}{3}f'''$ to be calculated by lifting to characteristic 0. □

REMARK 1.4. If $\operatorname{char}k\neq 2,3,5$, there is a similar result for points of order 6: there is a polynomial in the derivatives of f which is of degree 16 in x whose multiple roots are just the x-coordinates of elements of $C(k)\cap J_6^*$. Thus $\#(C(k)\cap J_6^*)\leqslant 16$ in these characteristics. This bound is best possible since it is attained by the curve $y^2=x^5+x$ (see [**3**]).

2. *Curves having a 5-torsion point*

Let F be any field. By a *triple* over F, we mean a triple (C,∞,P) consisting of a genus 2 curve C over F, a Weierstrass point $\infty\in C(F)$ and a point $P\in C(F)\cap J_5^*$. Two triples (C,∞,P) and (C',∞',P') over F are F-isomorphic if there exists an isomorphism $C\longrightarrow C'$ sending ∞ to ∞' and P to P'. Although our goal is to describe the moduli space of isomorphism classes of triples over an algebraically closed field, we begin with two lemmas which hold over an arbitrary base field that will be useful in Section 4.

LEMMA 2.1. (i) *Every triple (C,∞,P) over F is F-isomorphic to a triple of the form $(y^2+(ax^2+bx+c)y=x^5,\infty,(0,0))$ with $a,b,c\in F$ and $c\neq 0$.*

(ii) *Conversely, if $(a,b,c)\in F^3$ with $c\neq 0$ is such that $C:y^2+(ax^2+bx+c)y=x^5$ is of genus 2, then $(C,\infty,(0,0))$ is a triple.*

(iii) *When F is algebraically closed, we can take $c=1$ in* (i).

Proof. (i) Any triple (C, ∞, P) has a model $(y^2+g(x)y=f(x), \infty, P)$ with $P=(x_0, y_0)$. By Proposition 1.1 we must have

$$f(x) = (x-x_0)^5 - g(x)\Phi(x) + \Phi(x)^2. \tag{1}$$

If we substitute $y-\Phi(x)$ for y in $y^2+g(x)y=f(x)$ with f given by (1), we find

$$y^2+\beta(x)y = (x-x_0)^5,$$

where $\beta(x)=g(x)-2\Phi(x)$, and P becomes the point $(x_0, 0)$ in the new (x, y)-coordinates. We can replace x by $x+x_0$. Then, replacing Φ by $g-\Phi$ if necessary, we can assume that $P=(0,0)$. Since C is non-singular at P, we deduce that $\beta(0)\neq 0$.

(ii) The function y has a unique pole at ∞ which is of order 5. Since y only vanishes at $(0,0)$, the order of the zero there must also be 5.

(iii) It suffices to replace x by $c^{2/5}x$ and y by cy. □

If $(a, b, c)\in F^3$ with $c\neq 0$ is such that $C: y^2+(ax^2+bx+c)y=x^5$ is a genus 2 curve, we define

$$\mu(C, \infty, (0,0)) = \left(\frac{a^2b}{c}, \frac{ab^3}{c^2}, \frac{a^5}{c}, \frac{b^5}{c^3}\right). \tag{2}$$

More generally, if (C, ∞, P) is any triple, we define $\mu(C, \infty, P)$ as being the right member of (2) for any triple $(y^2+(ax^2+bx+c)y=x^5, \infty, (0,0))$ which is F-isomorphic to (C, ∞, P). That this is well-defined follows from Lemma 2.1 as well as the following lemma.

LEMMA 2.2. *Let $(a', b', c')\in F^3$, $c'\neq 0$, be such that the curve $C': y^2+(a'x^2+b'x+c')y=x^5$ is of genus* 2.

(i) *If $(C, \infty, (0,0))$ and $(C', \infty, (0,0))$ are F-isomorphic, then $\mu(C, \infty, (0,0)) = \mu(C', \infty, (0,0))$.*

(ii) *If $\mu(C, \infty, (0,0)) = \mu(C', \infty, (0,0))$, then $(C, \infty, (0,0))$ and $(C', \infty, (0,0))$ are F-isomorphic unless $a=b=a'=b'=0$ in which case they become isomorphic over any extension of F containing a fifth root of c'/c.*

(iii) *A triple (C, ∞, P) has a non-trivial automorphism over F if and only if it is F-isomorphic to $(y^2+y=x^5, \infty, (0,0))$ and F contains a primitive fifth root of unity.*

Proof. (i) Let $\alpha: (C, \infty, (0,0)) \longrightarrow (C', \infty, (0,0))$ be an isomorphism over F. Since α preserves the points at infinity we can write $\alpha(x, y) = (r^2x+s, r^5y+tx^2+ux+v)$ for some $r\in F^*$, $(s, t, u, v)\in F^4$. Since $\alpha(0,0)=(0,0)$, we must have $s=v=0$. Hence $(r^5y+tx^2+ux)^2+(a'r^4x^2+b'r^2x+c')(r^5y+tx^2+ux) = r^{10}x^5$. Comparing coefficients of x and x^2 in this relation and the relation $r^{10}(y^2+(ax^2+bx+c)y) = r^{10}x^5$ shows that $u=t=0$. Since $r\neq 0$, comparing coefficients of x^2y, xy and y shows that $ar=a'$, $br^3=b'$ and $cr^5=c'$. This is easily seen to imply that $\mu(C, \infty, (0,0)) = \mu(C', \infty, (0,0))$.

(ii) Conversely, if this condition holds, we can find $r\neq 0$ in some extension field of F such that $ar=a'$, $br^3=b'$ and $cr^5=c'$. The map $(C, \infty, (0,0)) \longrightarrow (C', \infty, (0,0))$ that sends (x, y) to (r^2x, r^5y) is an isomorphism. If one of a, b, a', b' is non-zero, we find that $r\in F$. Otherwise, we can only conclude that $cr^5=c'$.

(iii) It is clear that if $\zeta\in F$ is a primitive fifth root of unity, then $\alpha(x, y) = (\zeta x, y)$ is a non-trivial F-automorphism of $(y^2+y=x^5, \infty, (0,0))$. Conversely, if (C, ∞, P) has an automorphism α, then arguing as in (i) and (ii) with $a'=a$ and $b'=b$ we find that $s=t=u=v=0$ and that $r=1$ unless $a=b=0$, in which case $r^5=1$. □

From now on we restrict attention to curves over the algebraically closed field k. If $(a,b)\in k^2$ we write $C_{a,b}$ for the curve $y^2+(ax^2+bx+1)y=x^5$ (always tacitly supposed to be of genus 2) and $\mathscr{T}_{a,b}$ for the triple $(C_{a,b},\infty,(0,0))$.

THEOREM 2.3. *Let*

$$\mathscr{V}=\operatorname{Spec} k\left[X,Y,Z,W,\frac{1}{\Delta}\right]/I,$$

where $\Delta=3125+16Z-500X-8X^2+225Y+XY-27W$ *and* I *is the ideal generated by* X^3-YZ, X^2Y-ZW *and* Y^2-XW. *We view* $\mathscr{V}$ *as a subscheme of affine* 4*-space* $\operatorname{Spec} k[X,Y,Z,W]$.

(i) *The mapping* $\mathscr{T}_{a,b}\longmapsto\mu(\mathscr{T}_{a,b})$ *induces a bijection between the set of* k*-isomorphism classes of triples over* k *and* $\mathscr{V}(k)$.

(ii) $\mathscr{V}$ *is the coarse moduli space of isomorphism classes over* k *of triples* (C,∞,P).

REMARK 2.4. Let F be a subfield of k and let $M=(\mu_1,\mu_2,\mu_3,\mu_4)\in\mathscr{V}(k)$. If $M\in F^4$, then we can actually find a triple (C,∞,P) over F with $\mu(C,\infty,P)=M$. To see this, it suffices to find $(a,b,c)\in F^3$ with $c\neq 0$ such that $\mu(y^2+(ax^2+bx+c)y=x^5,\infty,(0,0))=M$. For example, if $\mu_4\neq 0$ we can take $a=\mu_2$, $b=\mu_4^2$ and $c=\mu_4^3$, while if $\mu_4=0$ and $\mu_3\neq 0$, we can take $a=\mu_3$, $b=0$, $c=\mu_3^4$. If $\mu_4=\mu_3=0$, we take $a=b=0$ and $c\neq 0$ arbitrary. If $F=k$ then, by Lemma 2.1(iii), we can suppose that $c=1$.

Proof of Theorem 2.3. (i) Recall from Section 1 that $\delta(C)$ denotes the discriminant of the genus 2 curve C in the sense of [**15**]. A computation gives

$$\delta(C_{a,b})=3125+16a^5-500a^2b-8b^2a^4+225b^3a+b^4a^3-27b^5 \tag{3}$$

so the non-vanishing of $\delta(C_{a,b})$ is equivalent to the non-vanishing of Δ. It is clear that (a^2b,ab^3,a^5,b^5) is a point of $\mathscr{V}(k)$. Conversely, if $M\in\mathscr{V}(k)$, then by Remark 2.4 we can find a triple $\mathscr{T}_{a,b}$ such that $\mu(\mathscr{T}_{a,b})=M$. This proves the surjectivity. The injectivity follows from Lemmas 2.1 and 2.2.

(ii) We will only sketch the proof, which is inspired by the arguments of [**16**, §3] (see also [**11**, (2.2.10)]). Let $p:C\longrightarrow S$ be a smooth proper morphism of varieties over k, such that each geometric fibre is a non-singular curve of genus 2. If $i:S\longrightarrow C$ is a section, then i determines an effective Cartier divisor A on C/S (see [**11**, (1.2.2)]). We write $I(A)$ for the corresponding invertible sheaf. We say that (C,A) is a Weierstrass pointed family of curves of genus 2 over S if $I(A)^{\otimes 2}$ is isomorphic to the sheaf of relative differentials $\Omega_{C/S}$. Assume that there is also a section $\ell:S\longrightarrow C$ such that if B is the corresponding Cartier divisor, then $I(B)^{\otimes 5}\simeq I(A)^{\otimes 5}$ and A and B are distinct on every fibre. We call (C,A,B) a *triple* over S. One can check that every geometric fibre of (C,A,B) is a triple over k as defined above. We can cover S by affine varieties $\operatorname{Spec} R$, R a k-algebra of finite type, such that the triple (C,A,B) can be given over $\operatorname{Spec} R$ as the smooth closed subscheme D of $\mathbb{P}^3_R$ defined by

$$wy^2+y(az+bx+cw)w=xz^2,\quad zw=x^2,\ (a,b,c)\in R^3.$$

Note that since every fibre is smooth, c is not zero on any fibre and is therefore invertible in R. Thus we can define a morphism $\phi(C/S):S\longrightarrow\mathscr{V}$ by gluing together

morphisms $\phi(D/\operatorname{Spec} R):\operatorname{Spec} R \longrightarrow \mathscr{V}$ given by $(X, Y, Z, W) \longmapsto (ab^2/c, a^3b/c^2, a^5/c, b^5/c^3)$. Now $\mathscr{V}$ is isomorphic to an open set in the spectrum of the ring of invariants of the polynomial ring $R[u, v]$ under the action $u \longrightarrow \zeta^2 u$ and $v \longrightarrow \zeta v$. This shows that $\mathscr{V}$ is normal. Using (i) and applying Zariski's Main Theorem as in [**16**] allows one to conclude the proof. □

3. *Curves with two pairs of* 5*-torsion points*

In this section, by *quadruple over* k we always mean a quadruple of the form (C, ∞, P_1, P_2) with C of genus 2 over k, $\infty \in C(k)$ a Weierstrass point and $P_1, P_2 \in C(k) \cap J_5^*$ with $P_2 \neq \pm P_1$. We say two quadruples (C, ∞, P_1, P_2) and $(C', \infty', P_1', P_2')$ are isomorphic if there is an isomorphism C to C' taking ∞ to ∞', P_1 to P_1' and P_2 to P_2'. We wish to describe isomorphism classes of such quadruples. Forgetting the point P_2, we know from the previous section that (C, ∞, P_1) is isomorphic to some triple $\mathscr{T}_{a,b}$, so we want to describe the values of a, b for which there exists such a $P_2 = (x_0, y_0)$ with $x_0 \neq 0$.

We first dispose of the situation in characteristic 5.

LEMMA 3.1. *If* $\operatorname{char} k = 5$*, then there are no quadruples over* k.

Proof. As just explained, it suffices to consider quadruples of the form

$$(y^2 + (ax^2 + bx + 1)\, y = x^5, \infty, (0, 0), (x_0, y_0))$$

with $x_0 \neq 0$. Following the same lines as in the proof of Lemma 2.1, there exist $p, q, r \in k$ such that

$$(px^2 + qx + r)((a-p)\, x^2 + (b-q)\, x + (1-r)) = (x - x_0)^5 - x^5 = -x_0^5.$$

Hence $px^2 + qx + r$ and $(a-p)\, x^2 + (b-q)\, x + (1-r)$ are constant and $a = b = 0$. However the curve $y^2 + y = x^5$ is singular in characteristic 5. □

For the rest of the paper we suppose that $\operatorname{char} k \neq 5$. If $P_1, P_2 \in C(k) \cap J_5^*$, we denote by $e(P_1, P_2)$ the Weil pairing of P_1 and P_2. (The definition of e will be recalled during the proof of Lemma 3.5.) We fix once and for all a primitive fifth root of unity ζ in k and write $\epsilon = -(\zeta^2 + \zeta^3)$, a root of $T^2 - T - 1$. Our aim is to prove the following theorem.

THEOREM 3.2. (i) *Let* $\mathscr{V}$ *be as in Theorem* 2.3*, viewed as a subscheme of affine* 4*-space* $\operatorname{Spec} k[X, Y, Z, W]$. *Let*

$$H_0 : 5Z + XY - 5X^2 + 5W = 0, \tag{4}$$

$$H_1 : XY - (400 - 100\epsilon)\, X - (7 - \epsilon)\, X^2 + (13 - 3\epsilon)\, Z + (190 - 30\epsilon)\, Y - 25W + 2400 - 800\epsilon = 0,$$

$$H_2 : XY - (300 + 100\epsilon)\, X - (6 + \epsilon)\, X^2 + (10 + 3\epsilon)\, Z + (160 + 30\epsilon)\, Y - 25W + 1600 + 800\epsilon = 0. \tag{5}$$

Let $i \in \{0, 1, 2\}$. *Then a necessary and sufficient condition for a triple* (C, ∞, P_1) *to extend to a quadruple* (C, ∞, P_1, P_2) *with* $e(P_1, P_2) = \zeta^{\pm i}$ *is that* $\mu(C, \infty, P_1) \in H_i(k)$.

(ii) *For* $i \in \{0, 1, 2\}$ *let* $\mathscr{W}_i$ *be the reduced closed subscheme of* $\mathscr{V}$ *which is the intersection of* $\mathscr{V}$ *with* H_i. *Then each* $\mathscr{W}_i$ *is a rational curve.*

REMARK 3.3. We shall find explicit parametrisations of the $\mathscr{W}_i$ in the course of the proof.

REMARK 3.4. Note that $\mathscr{W} := \bigcup_{i=0}^{2} \mathscr{W}_i$ is not the moduli space of isomorphism classes of quadruples over k since both (C, ∞, P_1, P_2) and $(C, \infty, P_1, -P_2)$ correspond to the same point on $\mu(C, \infty, P_1) \in \mathscr{W}(k)$. Furthermore, since $e(P_1, -P_2) = e(P_1, P_2)^{-1}$, we obtain only three components $\mathscr{W}_0$, $\mathscr{W}_1$ and $\mathscr{W}_2$ corresponding to the three cases $e(P_1, P_2) = 1$, $\zeta^{\pm 1}$ and $\zeta^{\pm 2}$.

Proof of Theorem 3.2. We now begin the proof of the theorem. Take a triple $\mathscr{T}_{a,b} = (y^2 + (ax^2 + bx + 1)\, y = x^5, \infty, (0,0))$ and suppose there is a point $P = (x_0, y_0)$ of order 5 with $x_0 \neq 0$. As before, there is a function $\Phi(x) = px^2 + qx + r$ such that $y + \Phi(x)$ has a zero of order 5 at P and we have, as in (1)

$$y^2 + y(ax^2 + bx + 1) + (ax^2 + bx + 1)\,\Phi(x) - \Phi(x)^2 = (x - x_0)^5 = x^5 + (ax^2 + bx + 1)\,\Phi(x) - \Phi(x)^2. \quad (6)$$

Note that (6) implies that

$$r^2 - r = x_0^5. \quad (7)$$

We require the following lemma.

LEMMA 3.5. *With the notation that has just been introduced, we have*

$$e((0,0), P) = -\frac{y_0}{r}.$$

Proof. Recall (see [**12**, VI §4]), that, if momentarily C denotes a curve of genus $g \geqslant 1$ over k and J is the Jacobian of C, and if $N \in \mathbb{N}^*$ is prime to the characteristic of k, then the Weil pairing e_N is a non-degenerate alternating pairing from $J_N \times J_N$ to the Nth roots of unity and can be calculated as follows. Let $P_1, P_2 \in J_N$ and choose disjoint degree 0 divisors α and β on C representing P_1 and P_2. Then the divisors $N\alpha$ and $N\beta$ are principal, say the divisors of functions f_α and f_β in $k(C)$. Then

$$e(P_1, P_2) = \frac{f_\alpha(\beta)}{f_\beta(\alpha)}$$

where, if $\beta = \sum n_Q Q$, then $f_\alpha(\beta)$ denotes $\prod f_\alpha(Q)^{n_Q}$, and similarly for $f_\beta(\alpha)$.

We return to the case in hand, writing e for e_5. Since $(0, -1) = [-1](0,0)$ and e is alternating, we have $e((0,0), P) = e((0,0), P + (0,0)) = e((0,0) - \infty, P - (0, -1))$ and the divisors $(0,0) - \infty$ and $P - (0, -1)$ are disjoint. Since y has divisor $5(0,0) - 5\infty$ and $(y + \Phi(x))/(y + ax^2 + bx + 1)$ has divisor $5P - 5(0, -1)$, the lemma follows. □

Returning to the proof of the theorem we find, using (6), that

$$-x_0 \prod_{\ell=1}^{4} ((1 - \zeta^\ell)\, x - x_0) = (x - x_0)^5 - x^5 = \Phi(x)\,(ax^2 + bx + 1 - \Phi(x)). \quad (8)$$

We now write the left-hand side of (8) as a product of two quadratics as follows. Replacing P by $-P$ if necessary, there exists a unique $i \in \{2, 3, 4\}$ such that the product of the two terms in the product with $\ell = 1$ and $\ell = i$ is a constant multiple of $\Phi(x)$

and the product of the remaining two terms is a constant multiple of $ax^2+bx+1-\Phi(x)$. Then, adjusting constant terms and writing j and k for the integers in $\{2,3,4\}$ different from i, we have

$$\left(\frac{r}{x_0^2}\right)(x^2(1-\zeta)(1-\zeta^i)-x_0x(2-\zeta-\zeta^i)+x_0^2)=px^2+qx+r \tag{9}$$

and

$$\left(\frac{1-r}{x_0^2}\right)(x^2(1-\zeta^j)(1-\zeta^k)-x_0x(2-\zeta^j-\zeta^k)+x_0^2)=(a-p)x^2+(b-q)x+1-r.$$

Comparing coefficients of powers of x shows that

$$\begin{aligned} a&=\frac{1}{x_0^2}(1-\zeta^j-\zeta^k+\zeta^{j+k}+r(\zeta^{1+i}-\zeta^{j+k}+\zeta^j+\zeta^k-\zeta-\zeta^i)),\\ b&=\frac{1}{x_0}(\zeta^j+\zeta^k-2+r(\zeta+\zeta^i-\zeta^j-\zeta^k)),\\ p&=\frac{r}{x_0^2}(1-\zeta-\zeta^i+\zeta^{1+i}),\quad q=\frac{r}{x_0}(\zeta+\zeta^i-2), \end{aligned} \tag{10}$$

from which we deduce that

$$y_0=-\Phi(x_0)=-r\zeta^{i+1}. \tag{11}$$

Also, substituting $x=x_0$ in (9) and using Lemma 3.5 and (7) shows that

$$e((0,0),P)=\zeta^{i+1}. \tag{12}$$

REMARK 3.6. Since $i\in\{2,3,4\}$, we have apparently excluded the possibilities $e((0,0),P)=\zeta$ or ζ^2. These are just the cases where we have to replace P by $-P$. Thus the restriction on $e((0,0),P)$ is consistent with Remark 3.4.

We first consider the case $e(P_1,P_2)=1$.

LEMMA 3.7. *Let $c(S)$ be the polynomial $(S^2-S-1)(2S-1)(S^2+4S-1)$. There is a morphism $\alpha_0:\operatorname{Spec}k[S,1/c(S)]\longrightarrow\mathscr{V}$ (which will be defined during the course of the proof) with the following properties.*

(a) *α_0 is injective and its image is $\mathscr{W}_0$.*

(b) *For any $s\in k$ with $c(s)\neq 0$, there is a unique pair of isomorphism classes of quadruples $(C,\infty,P_1,\pm P_2)$ satisfying $e(P_1,P_2)=1$ such that $\mu(C,\infty,P_1)=\alpha_0(s)$. Conversely, for every pair of isomorphism classes $(C,\infty,P_1,\pm P_2)$ satisfying $e(P_1,P_2)=1$, there is a unique $s\in k$ with $c(s)\neq 0$ such that $\mu(C,\infty,P_1)=\alpha_0(s)$.*

(c) *Let η_0 be the involution of $\operatorname{Spec}k[S,1/c(S)]$ defined by $\eta_0(S)=(S+2)/(2S-1)$. Then, if (C,∞,P_1,P_2) is any quadruple with $e(P_1,P_2)=1$, we have $\mu(C,\infty,P_1)=\alpha_0(s)$ if and only if $\mu(C,\infty,P_2)=\alpha_0(\eta_0(s))$.*

Proof. By (12), for $e(P_1,P_2)=1$, we need to take $i=4$ and $\{j,k\}=\{2,3\}$ in (10). We find, on writing $s=\epsilon+(1-2\epsilon)r$, that

$$a=\frac{1}{x_0^2}(2+s),\quad b=-\frac{1}{x_0}(2+s), \tag{13}$$

and we let C_s denote $C_{a,b}$ with these values of a and b. A calculation shows that C_s is of genus 2 if and only if $c(s)\neq 0$. Given s with $c(s)\neq 0$, we find using (7) that

$s^2-s-1=5x_0^5$ so that there are five possibilities for C_s corresponding to the five possibilities for x_0. Given x_0 and writing $y_0=(s-\epsilon)/(2\epsilon-1)$ using (11), we find that $(C_s,\infty,(0,0),(x_0,y_0))$ is a quadruple with $e((0,0),(x_0,y_0))=1$. However Lemma 2.2 shows that resulting quadruples $(C_s,\infty,(0,0),(x_0,y_0))$ are all isomorphic. Therefore if we define α_0 by

$$\alpha_0(S)=\left(\frac{-5(S+2)^3}{(S^2-S-1)},\frac{-5(S+2)^4}{(S^2-S-1)},\frac{25(S+2)^5}{(S^2-S-1)^2},\frac{-5(S+2)^5}{(S^2-S-1)}\right), \tag{14}$$

we find that $\mu(C_s,\infty,(0,0))=\alpha_0(s)$.

Since $c(s)\neq 0$, we have $s^2-s-1\neq 0$ and a calculation now shows that the image of α_0 is $\mathscr{W}_0^{\wedge}$. Furthermore, since the ratio of the first two coordinates of the right-hand side of (14) is $S+2$, we see that α_0 is an isomorphism outside $S=-2$. On the other hand, -2 is the only value of s for which $\alpha_0(s)=(0,0,0,0)$. This proves (a). Then (b) follows from Theorem 2.3.

To prove (c), we need to calculate $\mu(C_s,\infty,P_2)$. To shift P_2 so that $x(P_2)=y(P_2)=0$, we transform $x-x_0\longrightarrow\lambda^2x$ and $y+\Phi\longrightarrow\lambda^5y$ in (6) with $\lambda\in k^*$. Recall that $\epsilon=-(\zeta^2+\zeta^3)$. Using

$$p=\frac{s-\epsilon}{x_0^2}(1-\epsilon),\quad q=-\frac{s-\epsilon}{x_0}(1-\epsilon),$$

as follows from (10), we obtain the curve $C'\colon y^2+(a'x^2+b'x+1)\,y=x^5$, where

$$a'=\frac{a-2p}{\lambda}=\frac{(2\epsilon-1)\,s}{\lambda x_0^2},\quad b'=\frac{b-2q+2x_0(a-2p)}{\lambda^3}=\frac{(2\epsilon-1)\,s}{\lambda^3x_0}, \tag{15}$$

with

$$\lambda^5=x_0^2(a-2p)+x_0(b-2q)+1-2r=\frac{(2\epsilon-1)}{5}(2s-1).$$

Now C' corresponds to a choice s' of the parameter s and the point $(0,0)$ on $C_{a,b}$ is transformed to one with x-coordinate $x_0'=-x_0/\lambda^2$ in $C'(k)$. Using (13), we find that

$$\frac{s'+2}{x_0'^2}=a'=\frac{(2\epsilon-1)\,s}{\lambda x_0^2}$$

from which it follows that $s'=(s+2)/(2s-1)$. □

We next consider the case $e(P_1,P_2)\neq 1$. We only discuss the case $e(P_1,P_2)=\zeta^{\pm 2}$ in detail, giving the result for the case $e(P_1,P_2)=\zeta^{\pm 1}$ at the end of this section.

LEMMA 3.8. *Let $d(T)$ be the polynomial $(T^2-\epsilon T+1)(T+2-2\epsilon)(2T^2+(55-37\epsilon)T+182-110\epsilon)$. There is a morphism $\alpha_2\colon \operatorname{Spec} k[T,1/d(T)]\longrightarrow\mathscr{V}^{\wedge}$ with the following properties.*

(a) *The image of α_2 is $\mathscr{W}_2^{\wedge}$. Furthermore, α_2 is injective, except that the roots of $T^2+4(1-\epsilon)T+15-8\epsilon$ are both mapped to the point $Q_1=(40,80,800,160)$ and (except when k is of characteristic 11 and $\epsilon=4$) the roots of $T^2+(8-6\epsilon)T+11-6\epsilon$ are both mapped to the point*

$$Q_2=(40(2+\epsilon),80(3+2\epsilon),\frac{4000(8+9\epsilon)}{(10+3\epsilon)},4(184+152\epsilon)).$$

(b) *For any $t \in k$ with $d(t) \neq 0$, and $\alpha_2(t) \neq Q_1, Q_2$, there is a unique isomorphism class of quadruples (C, ∞, P_1, P_2) satisfying $e(P_1, P_2) = \zeta^{-2}$ such that $\mu(C, \infty, P_1) = \alpha_2(t)$. If $\alpha_2(t) = Q_1$ or Q_2, there are two such classes. Likewise, $(C, \infty, P_1, -P_2)$ gives the corresponding isomorphism classes such that $e(P_1, -P_2) = \zeta^2$ and such that $\mu(C, \infty, P_1) = \alpha_2(t)$. Conversely, given a pair of isomorphism classes (C, ∞, P_1, P_2) and $(C, \infty, P_1, -P_2)$ such that $e(P_1, P_2) = \zeta^{\pm 2}$, there is a unique $t \in k$ with $d(t) \neq 0$ such that $\mu(C, \infty, P_1) = \alpha_2(t)$.*

(c) *Let η_2 be the involution of* $\operatorname{Spec} k[T, 1/d(T)]$ *defined by $\eta_2(T) = (2T - \epsilon)/(\epsilon T - 2)$. Then if (C, ∞, P_1, P_2) is any quadruple with $e(P_1, P_2) = \zeta^{\pm 2}$, we have $\mu(C, \infty, P_1) = \alpha_2(t)$ if and only if $\mu(C, \infty, P_2) = \alpha_2(\eta_2(t))$.*

REMARK 3.9. (1) In (b) there are two pairs of isomorphism classes of quadruples mapping to Q_1 and Q_2 because they project to the same isomorphism class of triples.

(2) In (b), the characteristic 11, $\epsilon = 4$ case has been excluded because in this case $T^2 + 2T(4 - 3\epsilon) + 11 - 6\epsilon$ divides $d(T)$, so that α_2 is not defined at the roots of this polynomial.

Proof of Lemma 3.8. By (12), for $e(P_1, P_2) = \zeta^{-2}$, we need to take $i = 2$ in (10). We write $t = (\zeta^2 - \zeta^3) r - \zeta^2$. From (10) we obtain

$$\begin{aligned} a &= \frac{1}{x_0^2}((2+\epsilon)(1-t)), \qquad b = \frac{1}{x_0}((1+\epsilon)t - 3 - \epsilon), \\ p &= \frac{1}{x_0^2}((\zeta^3 - 1)t + 1 - \zeta^2), \quad q = \frac{1}{x_0}((-2\zeta^3 - \zeta^4)t - 2 - \zeta), \end{aligned} \tag{16}$$

since $x_0^5 = r^2 - r = (t^2 - \varepsilon t + 1)/(\varepsilon - 3)$. We let D_t denote the curve $C_{a,b}$ with these values of a and b. As with the curves C_s, this leads in general to five curves D_t but the resulting quadruples $(D_t, \infty, (0,0), (x_0, y_0))$ are again isomorphic. Define α_2 by

$$\begin{aligned} \alpha_2(T) = \Bigg(& \frac{-(15+20\epsilon)(T-1)^2(T-5+2\epsilon)}{T^2 - \epsilon T + 1}, \frac{(25+40\epsilon)(T-1)(T-5+2\epsilon)^3}{T^2 - \epsilon T + 1}, \\ & \frac{(-375-500\epsilon)(T-1)^5}{(T^2 - \epsilon T + 1)^2}, \frac{-(47+76\epsilon)(T-5+2\epsilon)^5}{T^2 - \epsilon T + 1} \Bigg). \end{aligned} \tag{17}$$

Then $\mu(D_t, \infty, P_1) = \alpha_2(t)$. The case $t^2 - \epsilon t + 1 = (t + \zeta^2)(t + \zeta^3) = 0$ never occurs since $r \neq 0, 1$, because we took $x_0 \neq 0$.

We find that D_t is of genus 2 if and only if $d(t) \neq 0$ and again a calculation shows that the image of α_2 is $\mathscr{W}_2$.

On $\mathscr{W}_2(k)$, we can write $t = N_2/M_2$ where

$$\begin{aligned} N_2 &= (200\epsilon - 325)\mu_4 + (380\epsilon - 620)\mu_1 + (32\epsilon - 52)\mu_1^2 \\ &\quad + (-910\epsilon + 1480)\mu_2 + (13 - 8\epsilon)\mu_1\mu_2, \\ M_2 &= (200\epsilon - 325)\mu_4 + (11\epsilon - 18)\mu_1^2 + (540 - 330\epsilon)\mu_2 \\ &\quad + (60\epsilon - 100)\mu_1 + (13 - 8\epsilon)\mu_1\mu_2, \end{aligned} \tag{18}$$

where $\mu(D_t, \infty, (0,0)) = (\mu_1, \mu_2, \mu_3, \mu_4)$. Thus t is uniquely determined by $\mu(D_t, \infty, (0,0))$ at every point where M_2 does not vanish. Now M_2 vanishes at three points. The first is the point with $\mu_1 = \mu_2 = \mu_4 = 0$, so that $\mu_3 = (-800\epsilon - 1600)/(10 + 3\epsilon)$ (unless

$\operatorname{char} k = 11$ and $\epsilon = 4$, in which case this point does not exist). One verifies that $t = 5-2\epsilon$ is the unique value giving this point. The other two points correspond to the roots of the two quadratics given in the statement of the lemma and a calculation shows that both roots of each quadratic map to the same point. This proves (a). Assertions (b) and (c) then follow as in the proof of Lemma 3.7. □

For the case $e(P_1, P_2) = \zeta^{\pm 1}$, one takes $i = 3$ in (6). The consequence of this is to replace ϵ by the second root $1-\epsilon$ of T^2-T-1 throughout the argument. A natural choice of parameter for $\mathscr{W}_1$ is now $t' = (\zeta-\zeta^4)r-\zeta$. We can then define $\alpha_1, \eta_1, H_1, Q_4$ and $D_{t'}$ analogously to $\alpha_2, \eta_2, H_2, Q_2$ and D_t.

This completes the proof of Theorem 3.2. □

4. *Curves with three or more pairs of* 5*-torsion points*

We can now begin to study those curves for which $\#(C(k) \cap J_5^*) \geqslant 6$. We continue to suppose that $\operatorname{char} k \neq 5$. We define quintuples $(C, \infty, P_1, P_2, P_3)$ and their isomorphism in a manner analogous to quadruples, so $P_1, P_2, P_3 \in C(k) \cap J_5^*$, and $P_i \neq \pm P_j$ for $i \neq j$.

We define the points $Q_i \in k^4$ for $0 \leqslant i \leqslant 5$ by

$$
\begin{aligned}
Q_0 &= (0, 0, 0, 0),\\
Q_1 &= (40, 80, 800, 160),\\
Q_2 &= \left(40(2+\epsilon), 80(3+2\epsilon), \frac{4000(8+9\epsilon)}{(10+3\epsilon)}, 32(23+19\epsilon)\right),\\
Q_3 &= (5(12+\theta), 5(28+5\theta), 125(12+\theta), 315+93\theta),\\
Q_4 &= \left(40(3-\epsilon), 80(5-2\epsilon), \frac{4000(17-9\epsilon)}{(13-3\epsilon)}, 32(42-19\epsilon)\right),\\
Q_5 &= (5(13-\theta), 5(33-5\theta), 125(13-\theta), 409-93\theta),
\end{aligned}
$$

whenever this makes sense. Here, θ is a root of T^2-T+4 in k and ϵ is a root of T^2-T-1 in k as before. Note that Q_4 and Q_5 are the points obtained from Q_2 and Q_3, respectively, by replacing ϵ by $1-\epsilon$ and θ by $1-\theta$. One verifies that all the Q_i make sense in all characteristics, except that in characteristic 11 we find that Q_2 is not defined when $\epsilon = 4$ and Q_4 is not defined when $\epsilon = -3$. We write $\mathscr{Q}_k$ for the set of Q_i that lie in $\mathscr{V}(k)$.

LEMMA 4.1. *Let $(C, \infty, P_1, P_2, P_3)$ be a quintuple. Up to permutation of the P_i, one of the following* (a) *to* (d) *must hold.*

(a) *We have $e(P_1, P_2) = e(P_1, P_3) = 1$. Then $\mu(C, \infty, P_1) = Q_0$ and therefore (C, ∞, P_1) is isomorphic to $(y^2+y = x^5, \infty, (0, 0))$.*

(b) *We have $e(P_1, P_2) = e(P_1, P_3)^{\pm 1} = \zeta^{\pm 2}$. Then $\mu(C, \infty, P_1)$ is either Q_1 or Q_2, the latter case not occurring in characteristic* 11 *when $\epsilon = 4$.*

(c) *We have $e(P_1, P_2) = e(P_1, P_3)^{\pm 1} = \zeta^{\pm 1}$. Then $\mu(C, \infty, P_1)$ is either Q_1 or Q_4, the latter case not occurring in characteristic* 11 *when $\epsilon = -3$.*

(d) *If $e(P_1, P_2) \neq e(P_1, P_3)^{\pm 1}$, then $\mu(C, \infty, P_1) \in \mathscr{W}_\ell \cap \mathscr{W}_m(k)$ for some $\ell \neq m$. In particular, if for no $j \neq k$ does $e(P_i, P_j) = e(P_i, P_k)^{\pm 1}$, then for some i, $\mu(C, \infty, P_i) \in \mathscr{W}_1(k) \cap \mathscr{W}_2(k)$.*

Proof. (a) The hypothesis implies that (C, ∞, P_1) is isomorphic to some $(C_s, \infty, (0,0))$, so by Lemma 3.7 the quadruple (C, ∞, P_1, P_3) is isomorphic to (C, ∞, P_1, P_2) or $(C, \infty, P_1, -P_2)$. Lemma 2.2(iii) implies that $(C_s, \infty, (0,0))$ is $(y^2+y = x^5, \infty, (0,0))$.

(b) Either (C, ∞, P_1, P_2) is isomorphic to (C, ∞, P_1, P_3) or $(C, \infty, P_1, -P_3)$, or it is isomorphic to neither. In the former case, we have $\mu(C, \infty, P_1) = Q_0$ by Lemma 2.2(iii) and so $Q_0 \in \mathscr{W}_2(k)$. This only happens if $\operatorname{char} k = 2$ when $Q_1 = Q_0$. In the latter case, the hypothesis and Lemma 3.8 imply that $\mu(C, \infty, P_1) = Q_1$ or Q_2, the last possibility not occurring in characteristic 11 when $\epsilon = 4$.

(c) This is similar to (b).

(d) The first assertion follows from Theorem 3.2. If no pair of the pairs $\{P_i, P_j\}, \{P_i, P_k\}$ have the same or reciprocal Weil pairings, there must be a pair $\{P_i, P_j\}$ with $e(P_i, P_j) = \zeta^{\pm 1}$ and another pair $\{P_i, P_k\}$ with $e(P_i, P_k) = \zeta^{\pm 2}$, so $\mu(C, \infty, P_i) \in \mathscr{W}_1(k) \cap \mathscr{W}_2(k)$. □

The following two lemmas are proved by computation.

LEMMA 4.2. *We have* $(\mathscr{W}_1 \cap \mathscr{W}_2)(k) = \{Q_1, Q_3, Q_5\}$, *except in characteristics* 2 *and* 3 *where the intersection is* $\{Q_1\}$.

LEMMA 4.3. *The set* $\mathscr{Q}_k$ *is given as follows.*

(i) *In characteristic* 2, *we have* $Q_0 = Q_1 = Q_2 = Q_4$ *and* $\mathscr{Q}_k = \{Q_0\}$.

(ii) *In characteristic* 3, $\mathscr{Q}_k = \{Q_0, Q_1\}$, *these points being distinct.*

(iii) *In characteristic* 11, Q_i *belongs to* $\mathscr{Q}_k$ *for* $i \in \{0,1,3,4,5\}$ *when* $\epsilon = 4$ *and for* $i \in \{0,1,2,3,5\}$ *when* $\epsilon = -3$. *In each case, the listed points are distinct.*

(iv) *In all other characteristics all the points* Q_i $(0 \leqslant i \leqslant 5)$ *belong to* $\mathscr{Q}_k$ *and are distinct.*

PROPOSITION 4.4. (i) *All quintuples* $(C, \infty, P_1, P_2, P_3)$ *have* $\mu(C, \infty, P_i) \in \mathscr{Q}_k$ *for some* i.

(ii) *Let* (C, ∞, P_1) *be a triple such that* $\mu(C, \infty, P_1) \in \mathscr{Q}_k$, *then* $\#(C(k) \cap J_5^*) \geqslant 6$.

(iii) *Up to isomorphism, the numbers of isomorphism classes of pairs* (C, ∞) *which extend to quintuples are one in characteristics* 2 *and* 3, *four in characteristic* 11, *two in characteristic* 19 *and five in every other characteristic.*

Proof. (i) This follows from Lemmas 4.1 and 4.2.

(ii) We divide the proof into three cases: case 1: $\mu(C, \infty, P_1) = Q_0$ or Q_1, case 2: $\mu(C, \infty, P_1) = Q_2$ or Q_4, case 3: $\mu(C, \infty, P_1) = Q_3$ or Q_5.

Case 1: Let $C_{0,0}$ be the curve $y^2+y = x^5$. Then $\mu(C_{0,0}, \infty, (0,0)) = Q_0$. Note by Lemma 3.5 that if $P = (\zeta^r, -\epsilon)$, then $P \in C_{0,0}(k) \cap J_5^*$ and $e((0,0), P) = 1$. Hence $Q_0 \in \mathscr{W}_0(k)$ and therefore $\mu(C_{0,0}, \infty, P) = \alpha_0(\eta_0(-2))$ since -2 is the only value of s with $\alpha_0(s) = Q_0$. However $\alpha_0(\eta_0(-2)) = Q_1$, and hence $\mu(C_{0,0}, \infty, P) = Q_1$. Now let P' be any point $C_{0,0}(k) \cap J_5^*$. Then, since by Lemma 4.2, $Q_1 \in (\mathscr{W}_0 \cap \mathscr{W}_1 \cap \mathscr{W}_2)(k)$, $\mu(C_{0,0}, \infty, P')$ is an involute of Q_1 on one of the $\mathscr{W}_i$. Let t_1 and t_1' be the values of the t-parameter on $\mathscr{W}_1$ such that $\alpha_1(t_1) = \alpha_1(t_1') = Q_1$. Then t_1 and t_1' are interchanged by η_1 so, abusing terminology, we find that Q_1 is fixed by η_1. In the same way, it is fixed by η_2. As a result, $\mu(C_{0,0}, \infty, P') \in \{Q_0, Q_1\}$ and $(C_{0,0}, \infty)$ is the only pair which extends to a triple whose image under μ is Q_0 or Q_1. Example 1.2 showed that $\#(C_{0,0}(k) \cap J_5^*) \geqslant 12$.

Case 2: Take a triple (C, ∞, P_1) with $\mu(C, \infty, P_1) = Q_2$. Assume that $\operatorname{char} k \neq 2$ or 3 since in the former case, $Q_2 = Q_0$ and in the latter $Q_2 \notin \mathscr{Q}_k$. Then, by case 1, no $\mu(C, \infty, P_i)$ is Q_0 or Q_1. Since there are two values t_2 and t_3 with $\alpha_2(t_2) = \alpha_2(t_3) = Q_2$ there are corresponding points P_2 and P_3 such that the pairs of isomorphism classes $(C, \infty, P_1, \pm P_2)$ and $(C, \infty, P_1, \pm P_3)$ are not isomorphic. Therefore $P_3 \neq \pm P_2$ and $(C, \infty, P_1, P_2, P_3)$ is a quintuple. Similarly for Q_4.

Case 3: Now take the triple (C, ∞, P_1) with $\mu(C, \infty, P_1) = Q_3$. Since $Q_3 \in W_1(k)$, there exists P_2 such that (C, ∞, P_1, P_2) is a quadruple with $e(P_1, P_2) = \zeta^{\pm 1}$. Since $Q_3 \in W_2(k)$, there exists P_3 such that (C, ∞, P_1, P_3) is a quadruple with $e(P_1, P_3) = \zeta^{\pm 2}$. In particular $P_3 \neq \pm P_2$ and so we get a quintuple, and similarly for Q_5.

(iii) If (C, ∞) extends to a quintuple, $(C, \infty, P_1, P_2, P_3)$, then we have shown that $\mu(C, \infty, P_i) \in \mathscr{Q}_k$ for some i. When $\operatorname{char} k = 2$ or 3, (iii) follows from Lemma 4.3 and (i) and (ii). Suppose from now on that $\operatorname{char} k \neq 2, 3$. We have seen in (i) that $(C_{0,0}, \infty)$ extends to triples whose μ-value is Q_0 or Q_1, and no other Q_i. For $i \in \{2, 3, 4, 5\}$ take triples (C_i, ∞, P_i) such that $\mu(C_i, \infty, P_i) = Q_i$. Suppose there is an isomorphism $\phi : (C_i, \infty) \longrightarrow (C_j, \infty)$ for some $j \neq i$. Since the Q_i are distinct, ϕ does not extend to an isomorphism from (C_i, ∞, P_i) to (C_j, ∞, P_j). Hence $(C_i, \infty, P_i, \phi^{-1}(P_j))$ and $(C_j, \infty, P_j, \phi(P_i))$ are quadruples and must lie on the same $\mathscr{W}_\ell$ and Q_i and Q_j are involute to each other on $\mathscr{W}_\ell$.

However, a calculation shows that if t_2, t_2' are the values of the t-parameter on $\mathscr{W}_2$ with $\alpha_2(t) = Q_2$, then $\alpha_2(\eta_2(t_2))$ and $\alpha_2(\eta_2(t_2'))$ are neither Q_2, nor Q_3 nor Q_5 except when $\operatorname{char} k = 19$ and $\epsilon = 5$ and $\theta = 9$, in which case for some ordering of t_2 and t_2' we have $\alpha_2(\eta_2(t_2)) = Q_2$ and $\alpha_2(\eta_2(t_2')) = Q_3$. A similar statement holds for Q_4. Likewise, one can check that if t_3 is the unique value of the t-parameter on $\mathscr{W}_2$ such that $\alpha_2(t) = Q_3$ and if u_3 is the unique value of the t-parameter on $\mathscr{W}_1$ such that $\alpha_1(u) = Q_3$ then $\alpha_2(\eta_2(t_3))$ and $\alpha_1(\eta_1(u_3))$ are not Q_5. Finally, a calculation shows that $Q_i \notin \mathscr{W}_0(k)$ when $i \in \{2, 3, 4, 5\}$ and $\operatorname{char} k \neq 19$.

Hence if $\operatorname{char} k \neq 19$, no Q_i is involute to a Q_j when $j \neq i$ when $i, j \in \{2, 3, 4, 5\}$, so the number of non-isomorphic pairs (C, ∞) which extend to quintuples is $\#(\mathscr{Q}_k) - 1$, which is four in characteristic 11 and five in any other characteristic. Finally, in characteristic 19, a calculation shows that there are precisely two such curves. □

Finally we treat sextuples and complete the study of the situation in characteristic 19.

PROPOSITION 4.5. *Let (C, ∞, P_1) be part of a sextuple.*

(i) *If $\mu(C, \infty, P_1) = Q_2$, then $Q_2 \in \mathscr{W}_0(k)$, which only happens in characteristic* 19 *with $\epsilon = 5$. Similarly, if $\mu(C, \infty, P_1) = Q_4$ then $Q_4 \in \mathscr{W}_0(k)$,* $\operatorname{char} k = 19$ *and $\epsilon = -4$.*

(ii) *If $\mu(C, \infty, P_1) = Q_3$, then $Q_3 \in \mathscr{W}_0(k)$, which only happens in characteristic* 19 *when $\theta = 9$. Similarly, if $\mu(C, \infty, P_1) = Q_5$, then $Q_5 \in \mathscr{W}_0(k)$,* $\operatorname{char} k = 19$ *and $\theta = -8$.*

(iii) *Let (C, ∞) be a pair such that $\#(C(k) \cap J_5^*) > 6$. Then either* (a) *$\mu(C, \infty, P_1) = Q_0$ or Q_1, in which case (C, ∞) is isomorphic to $(y^2 + y = x^5, \infty)$ and $\#(C(k) \cap J_5^*) = 32$ or* 12 *according as to whether* $\operatorname{char} k = 2$ *or* $\neq 2$, *or* (b) $\operatorname{char} k = 19$ *and (C, ∞) is isomorphic to $(y^2 + (-2x^2 - 6x + 1)y = x^5, \infty)$, in which case $\#(C(k) \cap J_5^*) = 8$.*

Proof. (i) We retain the notation of the proof of case 2 of Proposition 4.4(ii) and continue to assume that $\operatorname{char} k \neq 2, 3$. Let P_4 be such that $(C, \infty, P_1, P_2, P_3, P_4)$ is a sextuple. We suppose that $\mu(C, \infty, P_1) = Q_2$, the other case being similar. Since by

Lemma 3.8 there are only two values of the t-parameter on $\mathscr{W}_2$ giving rise to Q_2, we must have $e(P_1, P_4) = \zeta^{\pm 1}$ or 1. The former case implies that $\mu(C, \infty, P_1) = Q_2$ is on $\mathscr{W}_1$, and so is in $(\mathscr{W}_1 \cap \mathscr{W}_2)(k) \subseteq \{Q_1, Q_3, Q_5\}$. However the Q_i are distinct, so $Q_2 \in \mathscr{W}_0(k)$ which is not the case unless $\operatorname{char} k = 19$ and $\epsilon = 5$.

(ii) We use the notation of case 3 of the proof of Proposition 4.4(ii). It suffices to treat the case $\mu(C, \infty, P_1) = Q_3$. Again, let P_4 be such that $(C, \infty, P_1, P_2, P_3, P_4)$ is a sextuple. If $e(P_1, P_4) = \zeta^{\pm 2}$, then $Q_3 \in \{Q_1, Q_2\}$ by Lemma 3.8. Likewise, if $e(P_1, P_4) = \zeta^{\pm 1}$, then $Q_3 \in \{Q_1, Q_4\}$. Since the Q_i are distinct, we have $e(P_1, P_4) = 1$. Hence $Q_3 \in \mathscr{W}_0(k)$ which only happens when $\operatorname{char} k = 19$ and $\theta = 9$.

(iii) By Example 1.2 and Lemma 4.1 we reduce to the case when $(\operatorname{char} k, \epsilon, \theta) = (19, 5, 9)$. In this case, $Q_2 = (14, 14, 6, 14)$ and $Q_3 = (10, 4, 3, 13)$. We have $Q_2, Q_3 \in \mathscr{W}_0(k)$ and a calculation using Lemma 3.7 shows that if s_2 and s_3 are the values of s such that $\alpha_0(s_2) = Q_2$ and $\alpha_0(s_3) = Q_3$, then $\eta_0(s_2) = s_3$, so Q_2 and Q_3 arise from the same pair $(C_{a,b}, \infty)$. Applying Remark 2.4 to Q_2, we find the model $(C_{-2,-6}, \infty)$ given in the statement. Likewise, Q_4 and Q_5 also give rise to $(C_{-2,-6}, \infty)$. We conclude by applying Proposition 1.3 to find that $\#(C_{-2,-6}(k) \cap J_5^*) = 8$. □

REMARK 4.6. In characteristic 19, $C_{-2,-6}$ has an automorphism group of order 8. The subgroup fixing ∞ is cyclic of order 4. It is generated by an automorphism which sends x to $-x-8$. The eight points of $C_{-2,-6}(k) \cap J_5^*$ form two orbits under this subgroup.

Acknowledgements. This paper is dedicated to the memory of Irwin Fischer who, along with Igusa, pioneered the study of moduli of genus 2 curves [**6**, **10**]. Part of this work was done while the second author was enjoying the hospitality of the University of Caen.

We would like to thank the referee for a number of helpful comments.

References

1. J. ARLEDGE, 'S-units attached to genus 3 hyperelliptic curves', *J. Number Theory* 63 (1997) 12–29.
2. J. BOXALL and E. BAVENCOFFE, 'Quelques propriétés arithmétiques des points de 3-division de la jacobienne de $y^2 = x^5 - 1$', Séminaire de Théorie des Nombres de Bordeaux 4, 1992, 113–128.
3. J. BOXALL and D. GRANT, 'Examples of torsion points on genus two curves', *Trans. Amer. Math. Soc.* 352 (2000) 4533–4555.
4. J. W. S. CASSELS and E. V. FLYNN, *Prolegomena to a middlebrow arithmetic of curves of genus two*, London Mathematical Society Lecture Notes 230 (Cambridge University Press, 1996).
5. E. DE SHALIT and E. GOREN, 'On special values of theta functions of genus two', *Ann. Inst. Fourier* 47 (1997) 775–799.
6. I. FISCHER, 'The moduli of hyperelliptic curves', *Trans. Amer. Math. Soc.* 82 (1956) 64–84.
7. T. FUKUDA and K. KOMATSU, 'On a unit group generated by special values of Siegel modular functions', *Math. Comp.* 69 (2000) 1207–1212.
8. D. GRANT, 'Units from 3- and 4-torsion on Jacobians of curves of genus 2', *Compositio Math.* 95 (1994) 311–320.
9. D. GRANT, 'Units from 5-torsion on the Jacobian of $y^2 = x^5 + \frac{1}{4}$ and the conjectures of Stark and Rubin', *J. Number Theory* 77 (1999) 227–251.
10. J. IGUSA, 'Arithmetic variety of moduli for genus two', *Ann. of Math.* 72 (1960) 612–649.
11. N. KATZ and B. MAZUR, 'Arithmetic moduli of elliptic curves', *Ann. of Math. Stud.* 108 (1985).
12. S. LANG, *Abelian varieties* (Interscience, 1959).
13. O. LECACHEUX, 'Unités de corps de nombres et courbes de genre un et deux', *Number theory*, CMS Conference Proceedings 15 (ed. Karl Dilcher, American Mathematical Society, Providence, RI, 1995) 229–243 (Fourth Conference of the Canadian Number Theory Association, Dalhousie University, Halifax, Nova Scotia, Canada, 2–8 July 1994).
14. F. LEPRÉVOST, 'Sur une conjecture sur les points de torsion rationnels des jacobiennes de courbes', *J. Reine Angew. Math.* 473 (1996) 59–68.

15. D. LOCKHART, 'On the discriminant of a hyperelliptic curve', *Trans. Amer. Math. Soc.* 342 (1994) 729–752.
16. D. MUMFORD and K. SUOMINEN, 'Introduction to the theory of moduli', *Algebraic Geometry, Oslo* 1970 (ed. F. Oort, Wolters–Noordhoff, Groningen, 1972) 171–222.

John Boxall
Département de Mathématiques et de Mécanique
CNRS – FRE 2271
Université de Caen
Esplanade de la Paix
14032 Caen Cedex
France

boxall@math.unicaen.fr

David Grant
Department of Mathematics
University of Colorado at Boulder
Boulder
CO 80309-0395
USA

grant@boulder.colorado.edu

Franck Leprévost
Université de Grenoble
Institut Fourier BP 74
F-38402 St-Martin-d'Hères Cedex
France

franck.leprevost@ujf-grenoble.fr