Jacobians of Genus One Curves*

Sang Yook An

E-mail: sang@math.arizona.edu

and

Seog Young Kim

The University of Arizona
E-mail: seog@math.arizona.edu

and

David C. Marshall

McMaster University
E-mail: marshall@math.mcmaster.ca

and

Susan H. Marshall

The University of Arizona
E-mail: susan@math.arizona.edu

and

William G. McCallum

The University of Arizona
E-mail: wmc@math.arizona.edu

and

Alexander R. Perlis

The University of Arizona
E-mail: aprl@math.arizona.edu

Consider a curve of genus one over a field K in one of three explicit forms: a double cover of $\mathbf{P}^1$, a plane cubic, or a space quartic. For each form, a certain syzygy from classical invariant theory gives the curve's jacobian in Weierstrass form and the covering map to its jacobian induced by the K-rational divisor at infinity. We give a unified account of all three cases.

1. INTRODUCTION

Let C be a complete, non-singular curve of genus one over a field K. Let n be the smallest positive integer such that C has a K-rational divisor D of degree n. By the Riemann–Roch theorem, the linear system associated with D gives a map $\phi_D \colon C \to \mathbf{P}_K^{n-1}$ which embeds C as a curve of degree n if $n \geq 3$, and is a map to $\mathbf{P}_K^1$ of degree 2 if $n = 2$.

The case $n = 1$ is distinguished, since in that case C has a rational point, and may be given the structure of an elliptic curve. An elliptic curve over K is a pair (E, O) , where E is a curve over K of genus one and $O \in E(K)$. Such a curve has a Weierstrass equation, which, if the characteristic of K is not 2 or 3, may be written in the form

$$\zeta^2 = 4\xi^3 - g_2\xi - g_3. \tag{1}$$

Given a curve C of genus one, there is an associated elliptic curve (E, O), where E is the jacobian of C, $\mathrm{Jac}(C)$, and O is the point on E corresponding to the trivial divisor class.

In general, we can define a K-rational map of degree n^2

$$\begin{aligned} j_D \colon C &\to \mathrm{Jac}(C) \\ Q &\mapsto \text{class of } nQ - D. \end{aligned}$$

Explicit equations for the map j_D are useful in performing explicit n-descents on elliptic curves ([3], [9]) and in studying the Sharafevich–Tate group ([10], [7], [4], [8]).

In this paper we will show how formulas from classical invariant theory give explicit Weierstrass equations for the jacobian of C and for the map j_D in the cases $n = 2, 3, 4$. Partial results along these lines already exist in the literature; however, we know of no comprehensive reference with proofs for all cases, particularly for the case $n = 4$. Moreover, it seems useful for computational purposes to gather all the formulas in one place.

* Supported by an NSF GIG grant DMS9709662

Mathematica versions of these formulas may be obtained from the website `www.math.arizona.edu/~wmc`. Rodriguez-Villegas and Tate [11] have developed formulas in the cubic case that work in characteristic 2 and 3. Recently, there has been some progress on the cases $n > 4$: [5] contains useful models for genus one curves of degree 5, and [1] gives an entirely different approach, using fermionic Fock space, which gives explicit formulas for arbitrary n in terms of Wronskian determinants. The connection between this work and the classical invariant theory is not entirely clear.

2. STANDARD FORMS FOR C

From now on we assume $\mathrm{char}(K) \neq 2, 3$. Let C, n, and D be as in the previous section. A general reference for linear systems and the associated embeddings is [6, pp. 294–296].

If $n = 1$, any effective rational divisor linearly equivalent to D (they exist because $|D|$ is nonempty) is a rational point O. Then (C, O) is an elliptic curve, and can be given in Weierstrass form. (In fact, the Weierstrass form can be obtained by considering the embedding given by $|6O|$.)

If $n = 2$, the map ϕ_D is a degree 2 map $C \to \mathbf{P}^1_K$, tamely ramified at four points by the Hurwitz formula [6, p. 301]. Thus we can represent C as a singular curve in $\mathbf{P}^2_K$ with projective equation

$$C\colon Z^2Y^2 = U(X, Y), \qquad (U \text{ a binary quartic form}). \tag{2}$$

For $n \geq 3$, the divisor D is very ample [6, Corollary 3.2, p. 308], and thus the map ϕ_D embeds C as a degree n curve in $\mathbf{P}^{n-1}_K$. We repeatedly use the following fact: if C and C' are projective curves of the same degree (possibly reducible), and if $C \subset C'$, then $C = C'$. Indeed, $C' = C \cup C''$ for some projective curve C'' not contained in C, and the intersection number between C'' and a hyperplane must be 0, hence $C'' = \emptyset$.

For $n = 3$, the linear system $|3D|$ has dimension 9 by Riemann–Roch, yet the space of cubic forms on $\mathbf{P}^2_K$ has dimension 10, and thus there is a non-zero cubic form that vanishes on C. Hence C is contained in the zero locus of this form, and since they both have the same degree, namely 3, they must be equal. Thus C has equation:

$$C\colon U(X, Y, Z) = 0, \qquad (U \text{ an ternary cubic form}). \tag{3}$$

For $n = 4$, the linear system $|2D|$ has dimension 4 by Riemann–Roch, yet the space of quadratic forms on $\mathbf{P}^3_K$ has dimension 6, and thus there are two linearly independent quadratic forms that vanish on C. Hence C is contained in the intersection of two quadric hypersurfaces, and since it has the same degree as the intersection, namely 4, it must be the equal to it. So C has equations:

$$C\colon U(X,Y,Z,W) = V(X,Y,Z,W) = 0, \qquad (U,V \text{ quaternary quadratic forms}). \tag{4}$$

From now on, we suppose C to be given in one of the forms (2), (3), or (4), and we let D be the intersection of C with the hyperplane at infinity. Our problem now is to determine formulas for the coefficients g_2 and g_3 of a Weierstrass model for J_C, and to determine equations for the map $\phi_D\colon C \to J_C$.

3. STATEMENT OF MAIN THEOREM

We recall some basic terminology from classical invariant theory. Consider the vector space V composed of k-tuples of homogeneous forms of degree d in n variables $X_1, \ldots, X_n$. Then $\mathrm{GL}_n(\overline{K})$ acts on V: for $F = (F_1, F_2, \ldots, F_k) \in V$, $g \in \mathrm{GL}_n(\overline{K})$, we define gF by

$$(gF)(X) = F(gX), \quad X = (X_1, X_2, \ldots, X_n).$$

If I is a polynomial on V (that is, a polynomial in the coefficients of the forms $F_1, \ldots, F_k$), we define g^*I by $g^*I(F) = I(gF)$, $F \in V$. An **invariant** is such a polynomial satisfying

$$g^*I = \det(g)^p I$$

for some non-negative integer p. It is necessarily homogeneous in the coefficients of F. A **covariant** is a homogeneous form $U(X)$ whose coefficients are homogeneous polynomials in the coefficients of F such that

$$(g^*U)(X) = \det(g)^p U(gX).$$

Here g^*U denotes the form whose coefficients are transformed by g^*. In particular, the forms $F_1, \ldots, F_k$ are themselves covariants.

A program of classical invariant theory was to determine a set of generators (fundamental covariants) and relations (syzygies) for the algebra of covariants for a given n, k, and d. We quote results from the nineteenth century literature giving the fundamental covariants and syzygies for the three cases relevant to our problem: binary quartic forms, ternary cubic forms, and pairs of quaternary quadratic forms. In each case we show how the syzygy gives a map from our curve C to an elliptic curve E in Weierstrass form. In what follows, we denote partial derivatives of a form $U(X,Y,Z)$ by U_X, U_{XY}, etc.

3.1. Case $n = 2$

Our curve C is assumed to be given as in (2). There are three fundamental covariants of binary quartic forms U:

$$\begin{aligned}
U(X,Y) &= a_0X^4 + 4a_1X^3Y + 6a_2X^2Y^2 + 4a_3XY^3 + a_4Y^4, \\
g(X,Y) &= \frac{1}{144}\left(U_{XY}^2 - U_{XX}U_{YY}\right), \\
h(X,Y) &= \frac{1}{8}\begin{vmatrix} U_X & U_Y \\ g_X & g_Y \end{vmatrix},
\end{aligned}$$

and two invariants:

$$\begin{aligned}
i &= a_0a_4 - 4a_1a_3 + 3{a_2}^2, \\
j &= a_0a_2a_4 + 2a_1a_2a_3 - a_0{a_3}^2 - a_4{a_1}^2 - {a_2}^3.
\end{aligned}$$

They satisfy the syzygy given in [16], which for $Z^2Y^2 = U(X,Y)$ may be written

$$h(X,Y)^2 = 4g(X,Y)^3 - ig(X,Y)Z^4Y^4 - jZ^6Y^6. \tag{5}$$

Note that $g(X,Y)$ and $h(X,Y)$ are forms of degree 4 and 6, so that (5) is homogeneous of degree 12. Divide by Z^6Y^6 to obtain

$$E : \left(\frac{h(X,Y)}{Z^3Y^3}\right)^2 = 4\left(\frac{g(X,Y)}{Z^2Y^2}\right)^3 - i\left(\frac{g(X,Y)}{Z^2Y^2}\right) - j. \tag{6}$$

Thus we have obtained the Weierstrass equation (1) with $g_2 = i$ and $g_3 = j$. Furthermore, we have the following rational map $\psi\colon C \to E$:

$$\psi\colon [X,Y,Z] \longmapsto \left(\frac{g(X,Y)}{(ZY)^2}, \frac{h(X,Y)}{(ZY)^3}\right). \tag{7}$$

3.2. Case $n = 3$

Our curve C is assumed to be given as in (3). The ternary cubic form

$$\begin{aligned}
U = aX^3 + bY^3 + cZ^3 + 3a_2X^2Y + 3a_3X^2Z + 3b_1Y^2X + 3b_3Y^2Z + \\
3c_1Z^2X + 3c_2Z^2Y + 6mXYZ
\end{aligned}$$

has four covariants, U, H, Θ, J and two invariants S, T. Here H is the Hessian

$$H = \frac{1}{216}\begin{vmatrix} U_{XX} & U_{XY} & U_{XZ} \\ U_{YX} & U_{YY} & U_{YZ} \\ U_{ZX} & U_{ZY} & U_{ZZ} \end{vmatrix}.$$

Note that H is also a cubic form.

To define the covariant Θ we recall some more terminology from classical analytical geometry. The **polar conic** of a cubic form W with respect to a fixed point $[X' : Y' : Z']$ is given by the equation

$$X'W_X + Y'W_Y + Z'W_Z = 0.$$

A conic can by written in the form $(X,Y,Z)A(X,Y,Z)^t = 0$ for some symmetric matrix A; the **dual conic** is obtained by replacing A by its adjoint $\mathrm{adj}(A)$. Finally, given two conics corresponding to the matrices

$$\begin{bmatrix} a & h & g \\ h & b & f \\ g & f & c \end{bmatrix}, \quad \begin{bmatrix} a' & h' & g' \\ h' & b' & f' \\ g' & f' & c' \end{bmatrix}$$

there is a conic covariant to the two with matrix

$$\begin{bmatrix} b'c + bc' - 2ff' & f'g + fg' - c'h - ch' & h'f + hf' - b'g - bg' \\ f'g + fg' - c'h - ch' & c'a + ca' - 2gg' & g'h + gh' - a'f - af' \\ h'f + hf' - b'g - bg' & g'h + gh' - a'f - af' & a'b + ab' - 2hh' \end{bmatrix}$$

To construct Θ, take the polar conics to U and H with respect to a fixed point $[X' : Y' : Z']$, construct the conic which is covariant to their duals, set $(X', Y', Z') = (X, Y, Z)$, then multiply the result by $1/9$. The resulting covariant of degree 6 has 6952 terms.

Finally, we have a covariant of degree 9,

$$J = -\frac{1}{9}\left|\frac{\partial(U, H, \Theta)}{\partial(X, Y, Z)}\right|.$$

The formulas for the two invariants, S and T, are monuments to the algebraic skills of our forebears:

$$\begin{aligned} S = abcm &- (bca_2a_3 + cab_1b_3 + abc_1c_2) - m(ab_3c_2 + bc_1a_3 + ca_2b_1) + \\ &(ab_1c_2^2 + ac_1b_3^2 + ba_2c_1^2 + bc_2a_3^2 + cb_3a_2^2 + ca_3b_1^2) - m^4 + \\ &2m^2(b_1c_1 + c_2a_2 + a_3b_3) - 3m(a_2b_3c_1 + a_3b_1c_2) - \\ &(b_1^2c_1^2 + c_2^2a_2^2 + a_3^2b_3^2) + (c_2a_2a_3b_3 + a_3b_3b_1c_1 + b_1c_1c_2a_2) \end{aligned} \tag{8}$$

and

$$\begin{aligned}T = {} & 8a_3^3b_3^3 + 4a_3^3b^2c - 12a_2a_3^2bb_3c + 24a_3^2b_1^2b_3c + 24a_2^2a_3b_3^2c- \\ & 12aa_3b_1b_3^2c + 4a^2b_3^3c + 4a_2^3bc^2 + a^2b^2c^2 - 6aa_2bb_1c^2- \\ & 3a_2^2b_1^2c^2 + 4ab_1^3c^2 - 12a_3^2b_1b_3^2c_1 - 12aa_3b_3^3c_1 - 6aa_3b^2cc_1+ \\ & 18a_2a_3bb_1cc_1 - 12a_3b_1^3cc_1 + 6aa_2bb_3cc_1 + 6a_2^2b_1b_3cc_1 - 12ab_1^2b_3cc_1- \\ & 3a_3^2b^2c_1^2 + 6a_2a_3bb_3c_1^2 - 12a_3b_1^2b_3c_1^2 - 27a_2^2b_3^2c_1^2 + 24ab_1b_3^2c_1^2+ \\ & 4ab^2c_1^3 - 12a_2bb_1c_1^3 + 8b_1^3c_1^3 - 12a_3^3bb_3c_2 - 12a_2a_3^2b_3^2c_2- \\ & 12a_2^2a_3bcc_2 + 6aa_3bb_1cc_2 + 6a_2a_3b_1^2cc_2 - 12a_2^3b_3cc_2 - 6a^2bb_3cc_2+ \\ & 18aa_2b_1b_3cc_2 + 6a_3^2bb_1c_1c_2 + 18aa_3bb_3c_1c_2 - 6a_2a_3b_1b_3c_1c_2 + 6aa_2b_3^2c_1c_2+ \\ & 24a_2^2bc_1^2c_2 - 12abb_1c_1^2c_2 - 12a_2b_1^2c_1^2c_2 + 24a_2a_3^2bc_2^2 - 27a_3^2b_1^2c_2^2- \\ & 12a_2^2a_3b_3c_2^2 + 6aa_3b_1b_3c_2^2 - 3a^2b_3^2c_2^2 - 12aa_2bc_1c_2^2 - 12a_2^2b_1c_1c_2^2+ \\ & 24ab_1^2c_1c_2^2 + 8a_2^3c_2^3 + 4a^2bc_2^3 - 12aa_2b_1c_2^3 - 24a_3^2bb_1cm+ \\ & 12aa_3bb_3cm - 60a_2a_3b_1b_3cm - 24aa_2b_3^2cm + 12a_3^2bb_3c_1m + 36a_2a_3b_3^2c_1m- \\ & 24a_2^2bcc_1m + 12abb_1cc_1m + 12a_2b_1^2cc_1m + 12a_3bb_1c_1^2m - 24abb_3c_1^2m+ \\ & 36a_2b_1b_3c_1^2m + 36a_3^2b_1b_3c_2m + 12aa_3b_3^2c_2m + 12aa_2bcc_2m + 12a_2^2b_1cc_2m- \\ & 24ab_1^2cc_2m - 60a_2a_3bc_1c_2m + 36a_3b_1^2c_1c_2m + 36a_2^2b_3c_1c_2m - 60ab_1b_3c_1c_2m- \\ & 24aa_3bc_2^2m + 36a_2a_3b_1c_2^2m + 12aa_2b_3c_2^2m - 24a_3^2b_3^2m^2 + 36a_2a_3bcm^2+ \\ & 12a_3b_1^2cm^2 + 12a_2^2b_3cm^2 + 36ab_1b_3cm^2 - 12a_3b_1b_3c_1m^2 + 12ab_3^2c_1m^2+ \\ & 12a_2bc_1^2m^2 - 24b_1^2c_1^2m^2 + 12a_3^2bc_2m^2 - 12a_2a_3b_3c_2m^2 + 36abc_1c_2m^2- \\ & 12a_2b_1c_1c_2m^2 - 24a_2^2c_2^2m^2 + 12ab_1c_2^2m^2 - 20abcm^3 - 12a_2b_1cm^3- \\ & 12a_3bc_1m^3 - 36a_2b_3c_1m^3 - 36a_3b_1c_2m^3 - 12ab_3c_2m^3 + 24a_3b_3m^4+ \\ & 24b_1c_1m^4 + 24a_2c_2m^4 - 8m^6. \end{aligned} \tag{9}$$

The invariants and covariants satisfy the syzygy

$$\begin{aligned}J^2 = {} & 4\Theta^3 + TU^2\Theta^2 + \Theta(-4S^3U^4 + 2STU^3H - 72S^2U^2H^2 \\ & - 18TUH^3 + 108SH^4) - 16S^4U^5H - 11S^2TU^4H^2 - 4T^2U^3H^3 \\ & + 54STU^2H^4 - 432S^2UH^5 - 27TH^6, \end{aligned} \tag{10}$$

[14, p. 196], which for $U = 0$ simplifies to

$$\begin{aligned}& J(X,Y,Z)^2 = \\ & \quad 4\Theta(X,Y,Z)^3 + 108S\Theta(X,Y,Z)H(X,Y,Z)^4 - 27TH(X,Y,Z)^6. \end{aligned} \tag{11}$$

Note that $\deg(J) = 9$, $\deg(\Theta) = 6$, and $\deg(H) = 3$, so that (11) is homogeneous of degree 18. Divide by $H(X,Y,Z)^6$ to obtain

$$E: \left(\frac{J(X,Y,Z)}{H(X,Y,Z)^3}\right)^2 = 4\left(\frac{\Theta(X,Y,Z)}{H(X,Y,Z)^2}\right)^3 + 108S\left(\frac{\Theta(X,Y,Z)}{H(X,Y,Z)^2}\right) - 27T. \tag{12}$$

Thus we have obtained the Weierstrass equation (1) with $g_2 = -108S$ and $g_3 = 27T$. Furthermore, we have the following rational map $\psi\colon C \to E$:

$$\psi\colon [X,Y,Z] \longmapsto \left(\frac{\Theta(X,Y,Z)}{H(X,Y,Z)^2}, \frac{J(X,Y,Z)}{H(X,Y,Z)^3}\right). \tag{13}$$

3.3. Case $n = 4$

Our curve C is assumed to be given as in (4). The pair of quaternary quadratic forms U and V has four covariants U, V, T, T', J and five invariants $\Delta, \Theta, \Phi, \Theta', \Delta'$. Write

$$U(X,Y,Z,W) = (X,Y,Z,W)A(X,Y,Z,W)^t$$
$$V(X,Y,Z,W) = (X,Y,Z,W)B(X,Y,Z,W)^t$$

where A and B are symmetric 4×4 matrices. The invariants are defined by

$$\det(\lambda A + B) = \Delta\lambda^4 + \Theta\lambda^3 + \Phi\lambda^2 + \Theta'\lambda + \Delta'.$$

Let $A' = \operatorname{adj}(A)$, $B' = \operatorname{adj}(B)$. Define T and T' to be the two symmetric matrices determined by

$$\operatorname{adj}(A' + \lambda B') = \Delta^2 A + \lambda\Delta T + \lambda^2\Delta' T' + \lambda^3\Delta'^2 B.$$

Denote also by T and T' the associated quadratic forms. Finally, let J be (1/16) times the jacobian determinant of U, V, T, and T' with respect to X, Y, Z, and W.

The covariants and invariants satisfy the syzygy in [13, p. 241, ex. 2], which for $U = V = 0$ simplifies to

$$C'\colon J^2 = \Delta T^4 - \Theta T^3 T' + \Phi T^2 {T'}^2 - \Theta' T {T'}^3 + \Delta' {T'}^4. \tag{14}$$

This defines a double cover of $\mathbf{P}^1$. We have the following rational map $\psi'\colon C \to C'$:

$$\psi'\colon [X,Y,Z,W] \longmapsto [TT', J, {T'}^2]. \tag{15}$$

Applying the case $n = 2$ to C', we obtain an elliptic curve E and a rational map $C' \to E$, so that composition with ψ' gives a rational map $\psi\colon C \to E$:

$$\psi\colon [X, Y, Z, W] \longmapsto [gJ, h, J^3]. \tag{16}$$

Here the covariants g, h are associated with the binary quartic form (14) in T and T'.

THEOREM 3.1. *The maps $\psi\colon C \to E$ defined by equations (7), (13), and (16) are the maps ϕ_D from the respective curves to their jacobians, where D is the divisor at infinity on the projective model for C given by (2), (3), and (4), respectively.*

We will prove this theorem in the next two sections.

4. RECOLLECTIONS ON ELLIPTIC CURVES

Let C be a curve of genus one. If L is any field extension of K such that C has an L-rational point O, then we may regard (C, O) as an elliptic curve over L. There is an isomorphism, defined over L,

$$\begin{aligned} i_O\colon C &\simeq \mathrm{Jac}(C) \\ P &\mapsto \text{class of } P - O \end{aligned}$$

This gives C the structure of an algebraic group, with O as the identity element. Furthermore, if $\phi\colon (C, O) \to (C', O')$ is a morphism of elliptic curves, then it is a homomorphism for the group structure. In fact, if $\phi_*\colon \mathrm{Jac}(C) \to \mathrm{Jac}(C')$ is the map on jacobians induced by ϕ, then $\phi = i_{O'}^{-1} \circ \phi_* \circ i_O$.

Given an elliptic curve (E, O), defined over a field K, we consider the set $\mathrm{WC}(E)$ of isomorphism classes of pairs (C, i), where C is a genus one curve over K and i is an isomorphism of elliptic curves $\mathrm{Jac}(C) \simeq E$, defined over K. Two pairs (C, i) and (C', i') are isomorphic if there exists a map $\phi\colon C \to C'$ defined over K such that the following diagram commutes:

$$\begin{tikzcd} \mathrm{Jac}(C) \arrow[d, "i"', "\simeq"] & \mathrm{Jac}(C') \arrow[l, "\phi^*"'] \arrow[d, "i'"', "\simeq"] \\ E \arrow[r, equal] & E \end{tikzcd}$$

The set $\mathrm{WC}(E)$ contains a distinguished element, namely (E, i_O^{-1}). In fact, $\mathrm{WC}(E)$ can be given a group structure in which this element becomes the identity element; the resulting group is called the Weil–Châtelet group. One can reconcile this definition of the Weil–Châtelet group with the more traditional definition in terms of principle homogenous spaces by noting that C has a natural structure of principle homogeneous space over its jacobian.

DEFINITION 4.1. Let (C, i) and (C', i') be elements of $\mathrm{WC}(E)$. We say that a map $\phi\colon C \to C'$ defined over K is an ***n*-covering** if the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Jac}(C) & \xrightarrow{\phi_*} & \mathrm{Jac}(C') \\ i\big\downarrow\simeq & & i'\big\downarrow\simeq \\ E & \xrightarrow{n} & E \end{array}$$

The simplest example of an n-covering is the multiplication-by-n map on E itself. The kernel of this map is the group $E[n]$ of n-torsion points on E, which has n^2 points defined over $\overline{K}$ if $\mathrm{char}(K)$ does not divide n, which we assume from now on.

DEFINITION 4.2. On a curve C of genus one over K, an ***n*-torsion packet**, T_n, is a set of n^2 points on C such that given $P, Q \in T_n$, $nP - nQ$ is the divisor of a function f in $\overline{K}(C)$.

LEMMA 4.1. *Let (E, O) be an elliptic curve. If T_n is an n-torsion packet on E and if $O \in T_n$, then $T = E[n]$.*

Proof. It follows directly from the definition of the group structure on E that T_n is contained in $E[n]$, and it has the same cardinality as $E[n]$. ▮

LEMMA 4.2. *Let n be a positive integer prime to the characteristic of K. Given a morphism of elliptic curves $\phi\colon E \to E'$, defined over K, such that $\mathrm{Ker}(\phi) = E[n]$, there exists an isomorphism $E' \simeq E$ defined over K such that the following diagram commutes:*

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \big\downarrow= & & \big\downarrow\simeq \\ E & \xrightarrow{n} & E \end{array}$$

Proof. The morphism ϕ induces an injective map of function fields $K(E') \to K(E)$. Since $\ker \phi = E[n]$, the image of this map is the subfield L of of $K(E)$ fixed by $E[n]$. The multiplication-by-n map induces an isomorphism between L and $K(E)$; composing this with ϕ we get an isomorphism of function fields $K(E') \simeq K(E)$. The corresponding isomorphism of curves has the desired properties. ∎

The following key proposition was noted in [9] without proof; we give a brief proof here.

PROPOSITION 4.1. *Let E be an elliptic curve over K and* $\mathrm{WC}(E)$ *its Weil–Châtelet group. Let (C', i') be an element of* $\mathrm{WC}(E)$ *and C a genus one curve over K. If we have a map $\phi\colon C \to C'$ defined over K such that there exists a point $Q \in C'$ with $\phi^{-1}(Q)$ an n-torsion packet, then there exists an isomorphism $i\colon \mathrm{Jac}(C) \simeq E$ defined over K such that $\phi\colon (C, i) \to (C', i')$ becomes an n-covering.*

Proof. Let $O \in \phi^{-1}(Q)$. Then $\phi\colon (C, O) \to (C', Q)$ is a morphism of elliptic curves defined over $\overline{K}$. By Lemma 4.1, the kernel of ϕ is $C[n]$. Hence the kernel of $\phi_*\colon \mathrm{Jac}(C) \to \mathrm{Jac}(C')$ is $\mathrm{Jac}(C)[n]$, so by Lemma 4.2 there exists an isomorphism $j\colon \mathrm{Jac}(C') \to \mathrm{Jac}(C)$, defined over K, so that $j \circ \phi_* = [n]$. Define $i\colon \mathrm{Jac}(C) \to E$ by $i = i' \circ j^{-1}$. Then $i' \circ \phi_* = i \circ j \circ \phi_* = i \circ [n]$. Since i is a group homomorphism, $i \circ [n] = [n] \circ i$, hence $i' \circ \phi_* = [n] \circ i$, which makes ϕ into an n-covering. ∎

5. PROOF OF MAIN THEOREM

Denote the point $[0, 1, 0]$ on E by ∞. In each case we show that $\psi^{-1}(\infty)$ is an n-torsion packet, where $\psi\colon C \to E$ is defined by equations (7), (13), and (16) respectively. The main theorem then follows from Proposition 4.1.

5.1. Case $n = 2$

From (7) we see that $\psi^{-1}(\infty)$ comprises the points $[X, Y, 0]$ where $[X, Y]$ is a root of the binary quartic $U(X, Y)$. Those 4 points compose a 2-torsion packet: if $P = [X_1, Y_1, 0]$ and $Q = [X_2, Y_2, 0]$ are two of them, the rational function $(Y_1X - X_1Y)/(Y_2X - X_2Y)$ has divisor $2P - 2Q$. By Proposition 4.1, E must be J_C.

5.2. Case $n = 3$

From (13) we see that $\psi^{-1}(\infty)$ comprises those points on (3) where H vanishes. The covariant H is the so-called Hessian, and its zero locus intersects C in the set of 9 flex points on C (see [14, p. 145, Art. 173]).

Given two such points P and Q, there are lines $M = 0$, $N = 0$ meeting C only at P and Q, respectively; hence the divisor of M/N is $3P - 3Q$. Thus $\psi^{-1}(\infty)$ is a 3-torsion packet on C.

5.3. Case $n = 4$

From (15) we see that $\psi^{-1}(\infty)$ comprises those points on (4) where J vanishes. It is shown in [2] that the zero locus of J intersects C in the set of 16 hyperosculation points on C, that is, the set of points where the osculating plane meets C to order 4. (See also [13, Art. 362, p. 378]). By the same arguments as in the case $n = 3$, the set of 16 hyperosculation points is a 4-torsion packet.

ACKNOWLEDGMENTS

We thank John Cremona, Minhyong Kim, Barry Mazur, and Catherine O'Neil for useful conversations and comments.

REFERENCES

1. G. W. Anderson *The Universal Multisecant Identity and Symmetric Functions on Curves.* In preparation.
2. A. Clebsch. *Ueber die Wendungsberührebenen der Raumcurven. [On the hyperosculating planes of space curves.]* Journal für die reine und angewandte Mathematik **63** (1864), pp. 1–8. Annotated English translation available in [18].
3. J. Cremona. *Classical invariants and 2-descents on elliptic curves.* To appear in Journal of Symbolic Computation (Proceedings of the Second Magma Conference, Milwaukee, May 1996) in 2000.
4. J. Cremona and B. Mazur *Visualizing elements in the Shafarevich-Tate group.* To appear in Experimental Mathematics.
5. T. A. Fisher. *On 5 and 7 Descents for Elliptic Curves.* Ph. D. Thesis, University of Cambridge, 2000.
6. R. Hartshorne. *Algebraic geometry.* GTM 52, Springer-Verlag, 1977.
7. T. Klenke. *Visualizing elements of the Weil–Châtelet group. Ph. D. Thesis, Harvard University, 2000.*
8. B. Mazur. *Visualizing elements of order three in the Shafarevich-Tate group.* Asian J. Math **3** (1999), no. 1, 221–232.
9. J. R. Merriman, S. Siksek, N. P. Smart. *Explicit* 4*-descents on an elliptic curve.* Acta Arithmetica **77** (1996), no. 4, 385–404.
10. C. O'Neil. *Jacobians of Genus One Curves.* Preprint.
11. F. Rodriguez-Villegas and J. Tate. Preprint.
12. G. Salmon, *A treatise on the analytic geometry of three dimensions*, 2nd edition, Dublin, Hodges, Smith, and Co., 1865.
13. G. Salmon. *A treatise on the analytic geometry of three dimensions.* 7th edition, revised by R.A.P. Rogers and C.H. Rowe, London, Longmans, Green, and Company, 1928. Reprinted by Chelsea Publishing Company, New York, 1958. Note: [13, Art. 234, Ex. 2, p. 241] corresponds to [12, Art. 225, Ex. 2, p. 176], and [13, Art. 362, p. 378] corresponds to [12, Art. 356, p. 289].

14. G. Salmon. *A treatise on the higher plane curves*, 2nd edition, Dublin, Hodges, Smith, and Co., 1873.

15. G. Salmon. *A treatise on the higher plane curves.* 3rd edition. Reprinted by Chelsea Publishing Company, New York, 1960.

16. A. Weil. *Remarques sur un mémoire d'Hermite. [Remark on a paper of Hermite.]* Arch. Math. **V** (1954), pp. 197–202 ≡ Collected papers vol. II, Springer-Verlag, pp. 111–116.

17. A. Weil. *Euler and the jacobians of elliptic curves.* In *Arithmetic and geometry, Vol. I*, edited by Michael Artin and John Tate, Birkhäuser Boston Inc., Boston, 1983, pp. 353–359.

18. Website The authors are maintaining a website of material related to this paper. The site may be reached from `www.math.arizona.edu/~wmc`.