J. Symbolic Computation (2000) **11**, 1–000

Classical Invariants and 2-descent on Elliptic Curves

J. E. Cremona

School of Mathematical Sciences, University of Nottingham,
University Park, Nottingham NG7 2RD, U.K.

(Received July 10, 1996
Revised September 14, 1998)

The classical theory of invariants of binary quartics is applied to the problem of determining the group of rational points of an elliptic curve defined over a field K by 2-descent. The results lead to some simplifications to the method first presented in (Birch and Swinnerton-Dyer, 1963), and can be applied to give a more efficient algorithm for determining Mordell-Weil groups over $\mathbb{Q}$, as well as being more readily extended to other number fields. In this paper we mainly restrict to general theory, valid over arbitrary fields of characteristic neither 2 nor 3.

1. Introduction

Computing the rank and a basis for the group of rational points of an elliptic curve over a number field is a highly non-trivial task, even over the field $\mathbb{Q}$ of rational numbers. This is particularly true when the curve has no rational 2-torsion. The only general method which avoids extending the ground field goes back to (Birch and Swinnerton-Dyer, 1963), and is based on classifying certain binary quartic forms. This method is described briefly in (Cremona, 1992), and in more detail in Serf's thesis (Serf, 1995), where it is also extended to real quadratic fields of class number one; see also (Cremona and Serf, 1998). In this paper we show how parts of this method may be simplified and improved by using more classical invariant theory and Galois theory than in the original treatment in (Birch and Swinnerton-Dyer, 1963). With this approach it has been possible to make the algorithm over $\mathbb{Q}$ simpler and more efficient: some of these improvements can already be seen in (Cremona, 1997), and have been implemented in the author's program `mwrank`, available from `ftp://euclid.ex.ac.uk/pub/cremona/progs` (see the `mwrank.readme` file there). It is also expected make the job of extending the implementation to other number fields more practical.

In this paper we restrict to general theory, valid over arbitrary fields of characteristic neither 2 nor 3; in subsequent papers, the case where K is a number field, and the specific case $K = \mathbb{Q}$, will be treated in detail from an algorithmic viewpoint.

I would like to thank Nigel Byott, Robin Chapman, Samir Siksek and Nigel Smart for useful conversations.

2. Invariant Theory for Binary Quartics

In this section we review some standard material on the invariant theory of binary quartic forms. Our references here are Hilbert's lecture notes (Hilbert, 1993) and also the book (Elliott, 1913). In these texts the ground field is never made explicit. We will work over an arbitrary field K whose characteristic is not 2 or 3. It will not be necessary to assume that K is a number field, although eventually this will be the case of most interest to us.

Let

$$g(X,Y) = aX^4 + bX^3Y + cX^2Y^2 + dXY^3 + eY^4$$

be a binary quartic form over K. In the classical treatments, the coefficients of the form would be denoted a_0, $4a_1$, $6a_2$, $4a_3$, and a_4. We have chosen the simpler notation to be consistent with (Birch and Swinnerton-Dyer, 1963), and also because for later purposes (when $K = \mathbb{Q}$, or a number field) the integrality of the coefficients a, b, c, d, e will be important. We will also denote the corresponding inhomogeneous polynomial by $g(X) = g(X,1)$, which is a quartic except in the degenerate case when $a = 0$.

The group $\mathrm{GL}(2,K)$ acts on the set of binary quartics via

$$\begin{aligned} A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : g(X,Y) &\mapsto g(\alpha X + \beta Y, \gamma X + \delta Y) \\ &= a^*X^4 + b^*X^3Y + c^*X^2Y^2 + d^*XY^3 + e^*Y^4. \end{aligned}$$

The coefficients a^*, b^*, c^*, d^* and e^* of the transform of g are linear combinations of a, b, c, d, e with coefficients which are polynomials in the matrix entries. We call two quartics g_1 and g_2 *equivalent* if they are in the same orbit under this action, and write this as $g_1 \sim g_2$.

An *invariant of weight w and degree n* of the binary quartic $g(X,Y)$ is a homogeneous polynomial I, of degree n in the variables a, b, c, d and e, satisfying

$$I(a^*, b^*, c^*, d^*, e^*) = \det(A)^w I(a,b,c,d,e)$$

for all transformation matrices A in $\mathrm{GL}(2,K)$. The degree n and weight w are related: $w = 2n$. (For invariants of forms g of general degree, the corresponding relation is $2w/n = \deg(g)$.)

Each term of an invariant of degree n, as well as being homogeneous of degree n, is also *isobaric* of weight $w(= 2n)$, in the sense that each term of $I(a,b,c,d,e)$ has the same weight w, when the coefficients a, b, c, d and e are given the weights 0, 1, 2, 3 and 4 respectively (as indicated by the subscripts in the traditional notation). This isobaric property follows easily from invariance under diagonal matrices.

Given an isobaric homogeneous form $I(a,b,c,d,e)$, the condition that I should be an invariant is that it should be annihilated by two differential operators:

$$\Omega I = 4a\frac{\partial I}{\partial b} + 3b\frac{\partial I}{\partial c} + 2c\frac{\partial I}{\partial d} + d\frac{\partial I}{\partial e} = 0$$

and

$$\Omega^* I = 4e\frac{\partial I}{\partial d} + 3d\frac{\partial I}{\partial c} + 2c\frac{\partial I}{\partial b} + b\frac{\partial I}{\partial a} = 0.$$

The second condition is redundant if the weight and degree of I are related by $w =$

$2n$. These follow from invariance under matrices of the form $\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$ respectively.

The two basic invariants for quartics are

$$I = 12ae - 3bd + c^2$$

of degree 2 and weight 4, and the so-called *catalecticant*

$$J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$$

of degree 3 and weight 6. The invariants of degree n form a vector space whose basis consists of the monomials $I^r J^s$ where $r, s \geq 0$ and $2r + 3s = n$. In particular, I and J are algebraically independent (this is easy to see, by specializing $a = 1$, $b = c = 0$). The discriminant Δ of the quartic has degree 6 and weight 12, hence must be a linear combination of I^3 and J^2; we will take

$$\Delta = 4I^3 - J^2$$

which is 27 times the usual discriminant. The condition for $g(X, Y)$ to have no repeated factors is of course $\Delta \neq 0$, and we will assume that this condition holds throughout.

A fundamental question to ask of a given field K is: given two values I and J in K satisfying $4I^3 - J^2 \neq 0$, find all quartics in $K[X, Y]$ with invariants I and J, up to $\mathrm{GL}(2, K)$-equivalence. For a number field such as $\mathbb{Q}$ we might also take integral I and J and ask for all integral quartics $g(X, Y) \in \mathbb{Z}[\mathbb{X}, \mathbb{Y}]$. Even over $\mathbb{Q}$ this question is highly non-trivial; as we shall see, a good algorithmic answer to this problem forms a substantial part of the process of full 2-descent on elliptic curves.

As well as invariants we will also need to consider two related kinds of objects: seminvariants and covariants. A *seminvariant* is a form S in the variables a, b, c, d and e which is isobaric and homogeneous and satisfies $\Omega S = 0$. Thus all invariants are also seminvariants; but we also find three essentially new seminvariant quantities: these are a (the leading coefficient, of degree 1 and weight 0),

$$p = 3b^2 - 8ac$$

of degree 2 and weight 2, and

$$r = b^3 + 8a^2d - 4abc$$

of degree 3 and weight 3. For future reference we will also introduce the further seminvariant q defined by

$$q = \frac{1}{3}(p^2 - 16a^2I) = 3b^4 - 16ab^2c + 16a^2c^2 + 16a^2bd - 64a^3e. \qquad (2.1)$$

(The notation p, q, r is not standard in the literature, but will be used consistently throughout this paper.) Just as all invariants are polynomials in I and J, all seminvariants are polynomials in I, J, a, p and r; however these five are not algebraically independent, but are related by a syzygy:

$$p^3 - 48a^2pI - 64a^3J = 27r^2. \qquad (2.2)$$

(In general, a *syzygy* is an equation of algebraic dependence between invariants, seminvariants or covariants.) This syzygy, and its extension to covariants below (2.3), will play an important role later.

Seminvariants are unchanged by the substitution $X \mapsto X + Y$; it follows that if a seminvariant is expressed in terms of the roots x_i of g, it can be written as a function of the leading coefficient a and the differences $x_i - x_j$ of the roots. Conversely, every homogeneous function of the roots which can be expressed as a function of the differences between the roots is seminvariant (if multiplied by a suitable power of the leading coefficient a to make it integral); such a function of the roots is called an "irrational" seminvariant unless it is also symmetric in the roots, when it is "rational" and hence is an actual seminvariant in the sense defined here. We will make use of this observation in the next section.

Finally, a *covariant of order* w of the binary quartic is a form $C(a, b, c, d, e, X, Y)$, homogeneous separately in X, Y and in a, b, c, d, e, satisfying the following transformation law for all $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}(2, K)$:

$$C(a^*, b^*, c^*, d^*, e^*, X, Y) = \det(A)^w C(a, b, c, d, e, \alpha X + \beta Y, \gamma X + \delta Y).$$

There is a one-one correspondence between seminvariants and covariants: if C is a covariant of order w then the leading coefficient $S(a, b, c, d, e) = C(a, b, c, d, e, 1, 0)$ is a seminvariant. Conversely, every seminvariant S is the leading coefficient of a unique covariant C: one says that S is the *source* of C. If S has degree n (in the coefficients a, b, etc.) and weight w, then the degree (in X, Y) of the associated covariant C is $d = 4n-2w$; for invariants this is 0, and the associated covariant is just the invariant itself. In general, the covariant associated to the seminvariant S is

$$C(X, Y) = \sum_{i=0}^{d} \frac{(\Omega^*)^i(S)}{i!} X^{d-i} Y^i.$$

The seminvariant a is the source of the original form g, which is trivially a covariant of itself of order 0. The seminvariant p is the source of a quartic covariant g_4:

$$\begin{aligned} g_4(X, Y) &= (3b^2 - 8ac)X^4 + 4(bc - 6ad)X^3Y + 2(2c^2 - 24ae - 3bd)X^2Y^2 \\ &\quad +4(cd - 6be)XY^3 + (3d^2 - 8ce)Y^4, \end{aligned}$$

while the seminvariant r leads to the sextic covariant g_6:

$$\begin{aligned} g_6(X, Y) &= (b^3 + 8a^2d - 4abc)X^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)X^5Y \\ &\quad +5(8abe + b^2d - 4acd)X^4Y^2 + 20(b^2e - ad^2)X^3Y^3 \\ &\quad -5(8ade + bd^2 - 4bce)X^2Y^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)XY^5 \\ &\quad -(d^3 + 8be^2 - 4cde)Y^6. \end{aligned}$$

The syzygy between the seminvariants extends to a syzygy between the covariants:

$$27g_6^2 = g_4^3 - 48Ig^2g_4 - 64Jg^3. \tag{2.3}$$

This is an identity in X and Y; substituting $(X, Y) = (1, 0)$, we recover (2.2).

3. The Resolvent Cubic

We keep the notation of the previous section. Traditionally, the invariant theory of quartics can be used to derive the solution of quartics by radicals, by reducing the problem to that of solving an associated cubic equation, called the resolvent cubic. We will need to make the relation between a quartic and its resolvent cubic rather explicit, and to describe the situation in terms of Galois theory. This will lead us to a simple criterion for two quartics with the same invariants to be $\mathrm{GL}(2,K)$-equivalent.

Let I and J be the invariants of a quartic g defined over K, such that $\Delta = 4I^3 - J^2 \neq 0$. Suppose that the leading coefficient a of g is nonzero. Then g factorises over the algebraic closure $\overline{K}$ into 4 linear factors:

$$g(X,Y) = a\prod_{j=1}^{4}(X - x_iY).$$

Here the x_i are the four roots of the associated inhomogeneous quartic polynomial $g(X) = g(X,1)$. We will usually exclude as degenerate the case of quartics which have a root in K itself; these form precisely one orbit for each fixed pair (I,J), and include quartics with $a = 0$ (with a root at infinity), under the $GL(2)$ action.

Associated to the quartic g, or rather to its pair of invariants I, J, we have the cubic polynomial

$$F(X) = X^3 - 3IX + J$$

which has nonzero discriminant 27Δ. We are most interested in the case where $F(X)$ is irreducible over K; this is because in our application to 2-descent on elliptic curves, this case will arise when the curve has no K-rational 2-torsion. Hence we will make this assumption. In the sequel, this assumption is not strictly necessary, though some of the discussion would need to be reformulated if it did not hold; the fields L and $K(\varphi)$ defined below would need to be replaced by semisimple K-algebras, but essentially the same results would hold. This still leaves two distinct cases, according to whether the Galois group of F is or is not cyclic. For simplicity of exposition we will assume that we are in the generic case where the Galois group is the full symmetric group S_3; the groups S_4 and S_3 which appear below would need to be replaced by the alternating groups A_4 and A_3 in the non-cyclic case, and appropriate degrees of field extensions halved.

Let φ be a root of $F(X)$ in $\overline{K}$, so that φ satisfies $\varphi^3 = 3I\varphi - J$ and the field $K(\varphi)$ has degree 3 over K, with normal closure L of degree 6 (in the non-cyclic case). We denote by φ' and φ'' the conjugates of φ in L and view $\mathrm{Gal}(L/K) = S_3$ as acting by permutations on the set $\{\varphi, \varphi', \varphi''\}$. Note that $\mathrm{Tr}_{K(\varphi)/K}(\varphi) = 0$ since $F(X)$ has no X^2 term. We emphasise that neither φ nor the field L depend on the particular quartic g, but only on the pair of invariants I, J.

Let $M = K(x_1, x_2, x_3, x_4)$ be the splitting field of g over K. By sending x_1 to infinity a simple calculation shows that $g(X)$ is equivalent to $F(X)$ over $K(x_1)$; it follows that the degree $[M : K(x_1)] = 6$ with $\mathrm{Gal}(M/K(x_1)) \cong S_3$. For trivial quartics (with a root in K itself) this is still true, with $K = K(x_1)$ and $[M : K] = 6$; in the non-trivial case, however, it follows that g is irreducible over K and $[M : K] = 24$ with $\mathrm{Gal}(M/K) \cong S_4$. We view this Galois group as acting on the set of roots x_i by permutation in the natural way, once we have fixed an ordering of the roots x_i.

It also follows from this discussion that $L \subset M$, so that $S_3 = \mathrm{Gal}(L/K)$ is a quotient of $S_4 = \mathrm{Gal}(M/K)$. There is only one normal subgroup H of S_4 such that $S_4/H \cong S_3$, namely the Klein 4-group V_4, defined in terms of permutations as

$$V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

(S_4 acts by conjugation on the non-identity elements of V_4; this gives the homomorphism $S_4 \to S_3$ with V_4 as kernel.)

Using this explicit description of $\mathrm{Gal}(M/L)$ as a subgroup of $\mathrm{Gal}(M/K)$, we may easily write down elements of L in terms of the roots x_i. We define

$$z = a^2(x_1 + x_2 - x_3 - x_4)^2; \tag{3.1}$$

then permutations of the x_i take z to one of three values: z itself, and the conjugate quantities

$$z' = a^2(x_1 - x_2 + x_3 - x_4)^2 \quad \text{and} \quad z'' = a^2(x_1 - x_2 - x_3 + x_4)^2. \tag{3.2}$$

Since z is an integral function of the root differences, it is an example of an irrational seminvariant, as introduced in the previous section. Symmetric functions of z, z', z'' are therefore rational seminvariants. In particular, the coefficients of the minimal polynomial of z are seminvariants.

Proposition 3.1. *The minimal polynomial of z (defined in (3.1)) is*

$$\begin{aligned} h(Z) = (Z - z)(Z - z')(Z - z'') &= Z^3 - pZ^2 + qZ - r^2 \\ &= \left(\frac{4a}{3}\right)^3 F\left(\frac{3Z - p}{4a}\right). \end{aligned}$$

Hence $z \in K(\varphi)$; explicitly, $z = \frac{1}{3}(4a\varphi + p)$, and moreover $N_{K(\varphi)/K}(z) = r^2$.

Proof. The first equality can be obtained by manipulation of symmetric polynomials: the coefficients are seminvariants of degrees 2, 4 and 6. The second equality comes from expanding $F((3Z - p)/(4a))$ and using the syzygies (2.1) and (2.2) relating q and r^2 to the other seminvariants. The relation between z and φ follows immediately. This is to be interpreted as a generic relation, since both z and φ are only defined up to conjugacy: if we fix a numbering of the roots x_j we thereby fix an ordering of z and its conjugates, and we then choose the ordering of φ and its conjugates correspondingly. □

We will call the quantity z the *cubic seminvariant* associated to the quartic g. There are two crucial properties of the cubic seminvariant to notice: as an element of the cubic extension $K(\varphi)$ it is *linear* in φ, in the sense that when expressed in terms of the K-basis 1, φ, φ^2 for $K(\varphi)$ it has no φ^2 term. Secondly, its norm is a *square* in K. The latter fact is essentially due to the syzygy (2.2).

Given $z \in K(\varphi)^*$ with conjugates z', z'', such that the norm $N(z) = zz'z'' = r^2$ is a square in K, the normal closure of $K(\sqrt{z})$ will be a field M which is an S_4 extension of K containing L and with $\mathrm{Gal}(M/L) = V_4$. (In the degenerate case, z is itself a square, and $M = L$.) We may then construct a quartic g having M as its splitting field and z as its cubic seminvariant by working backwards: g is not uniquely defined, but only up to translation and scaling. Choosing a nonzero and b arbitrarily, we have the following explicit formulas:

$$\begin{aligned} 4ax_1 &= +\sqrt{z} + \sqrt{z'} - \sqrt{z''} - b, \\ 4ax_2 &= +\sqrt{z} - \sqrt{z'} + \sqrt{z''} - b, \\ 4ax_3 &= -\sqrt{z} + \sqrt{z'} + \sqrt{z''} - b, \\ 4ax_4 &= -\sqrt{z} - \sqrt{z'} - \sqrt{z''} - b. \end{aligned} \tag{3.3}$$

Here the square roots may be chosen in any way such that the product $\sqrt{z}\sqrt{z'}\sqrt{z''} = r$ (as opposed to $-r$). For compatibility with (3.2), we have arranged (3.3) so that $\sqrt{z} = a(x_1 + x_2 - x_3 - x_4)$, $\sqrt{z'} = a(x_1 - x_2 + x_3 - x_4)$ and $\sqrt{z''} = a(-x_1 + x_2 + x_3 - x_4)$.

Although the field $M = K(x_1, x_2, x_3, x_4)$ obtained thus will always have L as its cubic resolvent subfield, it is important to realise that the quartic g with the x_i as its roots will *not* necessarily have invariants I and J. This will only occur if the element z used, as well as having square norm, is linear in φ. This rather unnatural-looking condition can be interpreted as follows. The condition that z be linear in φ can be written as

$$\frac{z - z''}{z' - z''} = \frac{\varphi - \varphi''}{\varphi' - \varphi''},$$

and this common value is simply the cross-ratio

$$\frac{(x_1 - x_3)(x_2 - x_4)}{(x_1 - x_4)(x_2 - x_3)};$$

this may be readily checked by calculation from (3.3). Hence by requiring z to be linear in φ, we are simply specifying a fixed value for the cross-ratio of the roots of the associated quartic g, namely the value of the cross-ratio of the roots of $F(X)$ (including a “root at infinity”).

The fields involved are shown in the diagram, where the degrees indicated are for the non-trivial non-cyclic case (where g has no root in K, and $\mathrm{Gal}(L/K) \cong S_3$).

$$\begin{tikzcd}
 & M = K(x_1, x_2, x_3, x_4) \arrow[ddl, dash, "6"'] \arrow[ddd, <->, "S_4"] \arrow[dr, dash, "V_4\ \ 4"] & \\
 & & L = K(\varphi, \varphi', \varphi'') \arrow[d, dash, "2"] \arrow[ddl, <->, "S_3"'] \\
K(x_1) \arrow[dr, dash, "4"'] & & K(z) = K(\varphi) \arrow[dl, dash, "3"] \\
 & K &
\end{tikzcd}$$

In order to have an unambiguous definition of z applicable in all cases, we will in fact use the equation

$$z = \frac{4a\varphi + p}{3}$$

to define z as an element of $K(\varphi)$ for all quartics g with invariants I and J, where a and p are the seminvariants attached to g. This includes degenerate cases, such as when $a = 0$ (so that g is in fact a cubic): then $p = 3b^2$ and $z = b^2$ is actually in the ground field K. The fact that z is a square here is a special case of the following fundamental result.

Proposition 3.2. *(1) z is a square in $K(\varphi)$ if and only if g has a linear factor in $K[X, Y]$ (that is, one of the roots x_i is in $K \cup \{\infty\}$).*

(2) Let g and g^* be quartics with the same invariants I and J, with cubic seminvariants z and z^*. Then

$$g \sim g^* \iff zz^* \in (K(\varphi)^*)^2.$$

Proof. (1) Let $h(Z) = Z^3 - pZ^2 + qZ - r^2$ be the minimum polynomial of z. The condition that z be a square in $K(\varphi)$ is that $h(Z^2)$ should factorise over K as $h(Z^2) = -h_0(Z)h_0(-Z)$. Writing $h_0(Z) = Z^3 + uZ^2 + vZ + r$ and equating coefficients, we find that $v = (u^2 - p)/2$, where u satisfies the quartic equation

$$\tilde{g}(u) = (u^2 - p)^2 - 8ru - 4q = 0.$$

Manipulation now shows that

$$\tilde{g}(u) = \frac{1}{a} g(u + b, -4a),$$

from which the result follows when $a \neq 0$. If $a = 0$, we have already observed that $z = b^2$, and $h(Z) = (Z - b^2)^2$ in this case.

(2) Suppose that $g \sim g^*$ via a matrix A in $\mathrm{GL}(2, K)$. Since $\mathrm{GL}(2, K)$ is generated by matrices of the form

$$\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}, \quad \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

it suffices to show that $z = z^*$ (modulo squares) in these three cases. In the first case, $z^* = (\alpha/\delta)^2 z$; in the second, $z^* = z$ (clear from the definition). In the third case, direct calculation shows that $zz^* = w^2$ where

$$9w = 2\varphi^2 - 2c\varphi + 9bd - 4c^2;$$

here b, c, d refer as usual to the coefficients of g.

For the converse, suppose that zz^* is a square in $K(\varphi)$, where both z and z^* are linear in φ. The splitting field M of g is the same as that of g^*, since it is the normal closure of $K(\varphi)(\sqrt{z})$. Let the roots of g be x_i, $i = 1, \ldots, 4$. As observed above, the cross-ratio of the x_i is equal to $\frac{z-z''}{z'-z''} = \frac{\varphi-\varphi''}{\varphi'-\varphi''}$, and the roots y_i of g^* have the same cross-ratio; hence there is a matrix $A \in \mathrm{GL}(2, M)$, uniquely determined up to scalar multiple, such that $A(x_i) = y_i$ for $i = 1, \ldots, 4$.

Finally we must show that A can be taken to have entries in K, for then it is easily seen that $g \sim g^*$ via A^{-1}. We may scale A so that one of its entries is 1; then it suffices to show that for all $\sigma \in \mathrm{Gal}(M/K)$ we have $A^\sigma = A$ (up to scalar multiple, and hence exactly, since $1^\sigma = 1$). Now σ acts on the x_i via some permutation $\pi \in S_4$: $x_i^\sigma = x_{\pi(i)}$. Using the explicit expressions for the x_i and y_i in terms of $\sqrt{z}$, $\sqrt{z^*}$ and their conjugates as in (3.3), and the fact that $z = w^2 z^*$ for some $w \in K(\varphi)$, it follows that σ acts on the y_i via the *same* permutation: $y_i^\sigma = y_{\pi(i)}$. Now applying σ to the four equations $A(x_i) = y_i$, we obtain $A^\sigma(x_{\pi(i)}) = y_{\pi(i)}$ for all i, and hence (permuting the equations), $A^\sigma(x_i) = y_i$ for all i. By uniqueness of A up to scalar multiple, we have $A^\sigma = A$ as required. □

Using this proposition, we can derive a simple test for whether a given pair of quartics g, g^* is equivalent. We form the two cubic seminvariants z, z^* and test whether zz^* is a square in $K(\varphi)$. This condition turns out to be simply whether a third quartic has a root in K, as in Proposition 3.2 (1).

Proposition 3.3. *Let g_1, g_2 be quartics over the field K, both having the same invariants I and J. Then $g_1 \sim g_2$ if and only if the quartic $u^4 - 2pu^2 - 8ru + s$ has a root in K, where*

$$p = (32a_1a_2I + p_1p_2)/3,$$

$$r = r_1 r_2,$$

and

$$s = (64I(a_1^2p_2^2 + a_2^2p_1^2 + a_1a_2p_1p_2) - 256a_1a_2J(a_1p_2 + a_2p_1) - p_1^2p_2^2)/27.$$

Here, a_i, p_i and r_i are the seminvariants attached to g_i for $i = 1, 2$.

Proof. We compute the minimum polynomial $h(Z)$ of z_1z_2, as the characteristic polynomial of the matrix A_1A_2, where A_i is the characteristic matrix of z_i:

$$A_i = \frac{1}{3}\left(4a_i\begin{pmatrix} 0 & 0 & -J \\ 1 & 0 & 3I \\ 0 & 1 & 0 \end{pmatrix} + p_i\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right);$$

here, $\begin{pmatrix} 0 & 0 & -J \\ 1 & 0 & 3I \\ 0 & 1 & 0 \end{pmatrix}$ is the characteristic matrix of φ. Writing $h(Z) = Z^3 - pZ^2 + qZ - r^2$, we have p and r as in the statement, and $s = p^2 - 4q$. The condition that the roots of $h(Z)$ be squares is, as in the proof of Proposition 3.2 (1), the condition that the given quartic $(u^2 - p)^2 - 8ru - 4q$ has a root in K. □

Implementation note: in practice we can write down the roots of the quartic constructed in the preceding proposition explicitly, in order to determine whether they lie in K, without having to use a general factorization procedure for quartic polynomials in $K[X]$, provided that we already know the roots x_i of $g_1(X)$. First we compute the values of z_i for $i = 1, 2, 3$ (the cubic seminvariants associated to $g_1(X)$), using (3.1) and (3.2). Let w_i denote the cubic seminvariants associated to $g_2(X)$; we do not compute these independently from the roots of g_2, since we must ensure that each w_i is Galois conjugate to z_i; instead we use the relations

$$3z_i = 4a_1\varphi_i + p_1, \qquad 3w_i = 4a_2\varphi_i + p_2$$

to compute $w_i = (3a_2z_i + a_1p_2 - a_2p_1)/(3a_1)$ for $i = 1, 2, 3$. Now the roots of the third quartic in Proposition 3.3 are amongst the values of $\pm\sqrt{z_1w_1} \pm \sqrt{z_2w_2} \pm \sqrt{z_3w_3}$.

We remark that this proposition gives a very simple, algebraic test for equivalence of quartics, over any field. Both the tests for triviality and equivalence only rely on being able to determine whether a certain quartic with coefficients in K has a root in K. This test is much simpler to implement than the test presented in (Birch and Swinnerton-Dyer, 1963) and (Cremona, 1992) for $K = \mathbb{Q}$, and in (Serf, 1995) for real quadratic fields. In the real quadratic case the new test also saves some computation time, particularly for curves of higher rank (where there are more possible equivalences to check), and it is expected that the saving would be even greater for fields of higher degree.

3.1. Interpretation in terms of Galois cohomology

Fix a field L which is Galois over K with group either S_3 or A_3. Let $\varphi \in L$ be of degree 3 over K, so that L is the Galois closure of $K(\varphi)$. There is a bijection between (a) S_4 (respectively A_4) extensions M of K containing L with $\mathrm{Gal}(M/L) \cong V_4$, and (b) nontrivial elements z of the group

$$H = \ker\left(N_{K(\varphi)/K} : K(\varphi)^*/\left(K(\varphi)^*\right)^2 \to K^*/\left(K^*\right)^2\right).$$

The group H may be interpreted as a Galois cohomology group, namely

$$H \cong H^1(\mathrm{Gal}(\overline{K}/K), V_4) \tag{3.4}$$

where the action of $\mathrm{Gal}(\overline{K}/K)$ on V_4 is via its quotient $\mathrm{Gal}(L/K)$ which acts on V_4 by permuting its nontrivial elements.

We briefly indicate one construction of the isomorphism (3.4); see (Schaefer, 1995) for another approach. Given $z_1 = z \in K(\varphi)$ with square norm representing a nontrivial element of H, with conjugates z_2 and z_3, for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we have $z_i^\sigma = z_{\overline{\sigma}(i)}$ where $\sigma \mapsto \overline{\sigma}$ is the quotient map $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(L/K)$, and we have identified $\mathrm{Gal}(L/K)$ with S_3 (or A_3). Now for $i = 1, 2, 3$, fix a square root $\sqrt{z_i} \in \overline{K}$; then for $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we have

$$(\sqrt{z_i})^\sigma = \epsilon_i(\sigma)\sqrt{z_{\overline{\sigma}(i)}}$$

where $\epsilon_i(\sigma) = \pm 1$ and $\epsilon_1(\sigma)\epsilon_2(\sigma)\epsilon_3(\sigma) = +1$ since $\sqrt{z_1}\sqrt{z_2}\sqrt{z_3} \in K$. Now

$$\left\{(\epsilon_1, \epsilon_2, \epsilon_3) \in \{\pm 1\}^3 \mid \epsilon_1\epsilon_2\epsilon_3 = +1\right\} \cong V_4,$$

and the map $\sigma \mapsto (\epsilon_1(\sigma), \epsilon_2(\sigma), \epsilon_3(\sigma))$ is the desired 1-cocycle in $H^1(\mathrm{Gal}(\overline{K}/K), V_4)$.

Conversely, given a nontrivial 1-cocycle in $H^1(\mathrm{Gal}(\overline{K}/K), V_4)$, consider its restriction to $\mathrm{Gal}(\overline{K}/L)$. This is just a homomorphism $\mathrm{Gal}(\overline{K}/L) \to V_4$, since $\mathrm{Gal}(\overline{K}/L)$ acts trivially on V_4 by definition, and it is in fact surjective. Hence its kernel cuts out a V_4 extension M of L which is Galois over K. This in turn determines a well-defined class z in H as required.

For these cohomology computations it is worth noticing that the restriction map

$$H^1(\mathrm{Gal}(\overline{K}/K), V_4) \to H^1(\mathrm{Gal}(\overline{K}/L), V_4)$$

is injective, since (by the restriction-inflation exact sequence) its kernel is $H^1(S_3, V_4)$ which is trivial, as a simple direct calculation shows.

To summarise this section, we have shown that there exists a bijection between (a) quartics g over K with invariants I, J, modulo $\mathrm{GL}(2, K)$-equivalence; and (b) nonzero elements $z \in K(\varphi)$ which are linear in φ and whose norms are squares in K, modulo squares in $K(\varphi)$. The bijection is defined by associating to a quartic g with seminvariants a and p the cubic seminvariant $z = (4a\varphi + p)/3$. Each of these sets in turn can be identified with a subset of the Galois cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), V_4)$, depending on the specific generator φ for $K(\varphi)$, or equivalently on the specific invariants I and J. We will return to this in Section 5.

In the next section we will introduce the third ingredient, which relates both these sets to the group of points on an elliptic curve defined over K.

4. 2-Descent on Elliptic Curves

We keep the notation of the previous sections: I and J are elements of the field K satisfying $\Delta = 4I^3 - J^2 \neq 0$, and $F(X) = X^3 - 3IX + J$ is irreducible with root φ. Set $\tilde{F}(X) = -27F(-X/3)$, and let $E_{I,J}$ be the elliptic curve

$$E_{I,J}: \quad Y^2 = \tilde{F}(X) = X^3 - 27IX - 27J.$$

There is a close connection between (equivalence classes of) quartics g with invariants I, J and arithmetic properties of $E_{I,J}(K)$. Since the invariants I and J will remain fixed throughout, we will sometimes drop the subscript and refer to the elliptic curve simply as E.

The syzygy (2.2) may be expressed as

$$(27r)^2 = (4a)^3 \tilde{F}\left(\frac{3p}{4a}\right),$$

so that

$$(X, Y) = \left(\frac{3p}{4a}, \frac{27r}{(4a)^{3/2}}\right)$$

is a point on the curve E. (We will also use projective coordinates on E, in which this point is $(X : Y : Z) = (6p\sqrt{a} : 27r : 8a\sqrt{a})$.) This point is not K-rational unless a is a square in K. This leads to the fundamental question: is there a quartic equivalent to g whose leading coefficient is a square? If this is the case, we call the quartic g *soluble*.

Associated to the quartic g is the plane curve $\mathcal{C}$:

$$\mathcal{C} : \quad Y^2 = g(X) = aX^4 + bX^3 + cX^2 + dX + e.$$

This affine curve is nonsingular, and has genus one. If $a \neq 0$ it has a double point at infinity, which can be desingularised by taking the affine curve

$$\mathcal{C}^* : \quad V^2 = g(1, U) = eU^4 + dU^3 + cU^2 + bU + a$$

and identifying the points (X, Y) on $\mathcal{C}$ with $X \neq 0$ with the points (U, V) on $\mathcal{C}^*$ with $U \neq 0$ via $(U, V) = (1/X, Y/X^2)$. The double point at infinity on the projective closure of $\mathcal{C}$ is replaced by the two points $(0, \pm\sqrt{a})$ on $\mathcal{C}^*$, which are K-rational if and only if a is a square in K. For simplicity we will use $\mathcal{C}$ to denote the desingularised projective curve, bearing in mind that it has two points at infinity which are rational if and only if a is a square.

The following result is now straightforward.

Proposition 4.1. *The curve $\mathcal{C}$ has a K-rational point if and only if there is a quartic equivalent to g whose leading coefficient is a square.*

Proof. If a is a square then the points at infinity on $\mathcal{C}$ are K-rational. Conversely, if $\mathcal{C}$ has a K-rational point, we may apply a projective transformation to send its X-coordinate to infinity, thereby replacing g by an equivalent quartic whose leading coefficient is a square. □

The seminvariant syzygy (2.2) only determined a rational point on $E_{I,J}(K)$ when a was a square. Using the covariant syzygy (2.3), we can define a rational map $\mathcal{C} \to E$ defined over K. This can be derived by taking a rational point on $\mathcal{C}(K)$, mapping the X-coordinate to infinity, thus replacing the quartic g by a quartic whose leading coefficient is a square, and writing down the corresponding seminvariant syzygy.

Proposition 4.2. *The map*

$$\xi : \quad (x : y : z) \mapsto (6yzg_4(x, z) : 27g_6(x, z) : (2yz)^3)$$

is a rational map from $\mathcal{C}$ to $E_{I,J}$ of degree 4.

Proof. The covariant syzygy (2.3) may be written

$$(27g_6(X,Z))^2 = (4g(X,Z))^3\tilde{F}\left(\frac{3g_4(X,Z)}{4g(X,Z)}\right);$$

given $y^2z^2 = g(x,z)$ and substituting, this becomes

$$\left(\frac{27g_6(x,z)}{(2yz)^3}\right)^2 = \tilde{F}\left(\frac{3g_4(x,z)}{(2yz)^2}\right),$$

so that $(6yzg_4(x,z) : 27g_6(x,z) : (2yz)^3) \in E(K)$ as required.

To see that the degree is 4, given $(x : y : z)$ on $E(K)$ in projective coordinates, $(x : z)$ must be a solution to the quartic equation $4Xg(x,z) - 3Zg_4(x,z)$, and then y is uniquely determined.

Note that for $i = 1, 2, 3, 4$ we have $\xi((x_i : 0 : 1)) = (0 : 1 : 0)$, the point at infinity on E. □

In our applications, we will only be interested in those quartics K which are soluble; then the curve $\mathcal{C}$ has a K-rational point and is thus itself an elliptic curve, isomorphic to E over K (see (5) in Proposition 4.3 below). In general, E is the jacobian of $\mathcal{C}$.

For $i \in \{1, 2, 3, 4\}$ we also have a map θ_i from $\mathcal{C}$ to E which is a birational isomorphism defined over $K(x_i)$. Since $g \sim \tilde{F}$ it is easy to see that a transformation $A \in \mathrm{GL}(2, K(x_1))$ such that $A(x_1) = \infty$ takes the other roots x_j for $2 \le j \le 4$ to the roots of $\tilde{F}$ in some order; these roots are -3φ and its conjugates. Hence θ_1 takes $(x_1, 0)$ on $\mathcal{C}$ to the point at infinity on E, and the other points $(x_j, 0)$ (for $j > 1$) to the three points $(-3\varphi, 0)$ of order 2 on E. Similarly for the conjugate maps θ_j. If we set $\theta = \alpha \circ \theta_1$ for a suitable automorphism of E, then the relation $\xi = [2] \circ \theta$ will hold, as in the following result. (Here, [2] denotes multiplication by 2 on E.)

Proposition 4.3. *(1) The following diagram commutes.*

$$\begin{tikzcd} E \arrow[r, "{[2]}"] & E \\ \mathcal{C} \arrow[u, "\theta"] \arrow[ur, "\xi"'] & \end{tikzcd} \quad (4.1)$$

(2) Let $P \in E(\overline{K})$ and let $[2]^{-1}(P) = \{Q_1, Q_2, Q_3, Q_4\} \subset E(\overline{K})$; then $\xi^{-1}(P) = \{\theta^{-1}(Q_i) \mid 1 \le i \le 4\}$. If in fact $P \in E(K)$, then (with a suitable numbering) Q_i is defined over $K(x_i)$ for $i = 1, 2, 3, 4$.

(3) For each $\sigma \in Gal(\overline{K}/K)$, there exists $T_\sigma \in E[2]$ such that $\theta^\sigma(R) = \theta(R) + T_\sigma$ for all $R \in \mathcal{C}(\overline{K})$.

(4) If $\mathcal{C}(K)$ is not empty, then the image of $\mathcal{C}(K)$ under ξ is a complete coset of $[2]E(K)$ in $E(K)$.

(5) If $\mathcal{C}(K)$ is not empty, then $\mathcal{C}$ and E are birationally isomorphic over K.

Proof. (1) Define $\mu = \xi \circ \theta_1^{-1} : E \to E$. Then μ has degree 4, and maps the four 2-torsion points $E[2]$ to 0, so must equal $[2] \circ \alpha$, for some automorphism α of E. So $\xi = [2] \circ \theta$, where $\theta = \alpha \circ \theta_1$.

(2) For $R \in \mathcal{C}(\overline{K})$ we have $\xi(R) = P \iff [2] \circ \theta(R) = P \iff \theta(R) = Q_i$ for some i. If $P \in E(K)$ then if we set $Q_i = \theta_i(P)$, we have $Q_i \in E(K(x_i))$ since θ_i is defined over

$K(x_i)$. The result follows, since the four fields $K(x_i)$ are distinct (under our permanent assumption that the cubic polynomial $F(X)$ is irreducible over K).

(3) Fix $\sigma \in G = \mathrm{Gal}(\overline{K}/K)$. Consider the map $\mathcal{C} \to E$ defined by $R \mapsto \theta^\sigma(R) - \theta(R)$. The image is contained in $E[2]$ since $[2](\theta^\sigma(R) - \theta(R)) = [2]\theta^\sigma(R) - [2]\theta(R) = \xi^\sigma(R) - \xi(R) = 0$, since both $[2]$ and ξ are defined over K. But maps between curves are either constant or surjective; it follows that $T_\sigma = \theta^\sigma(R) - \theta(R) \in E[2]$ is independent of R.

(4) Let R_1, $R_2 \in \mathcal{C}(K)$. Then for all $\sigma \in G$, $(\theta(R_2) - \theta(R_1))^\sigma - (\theta(R_2) - \theta(R_1)) = (\theta^\sigma(R_2) - \theta(R_2)) - (\theta^\sigma(R_1) - \theta(R_1)) = T_\sigma - T_\sigma = 0$ (using (3)). Hence $\theta(R_2) - \theta(R_1) \in E(K)$, so $\xi(R_2) - \xi(R_1) = [2](\theta(R_2) - \theta(R_1)) \in 2E(K)$. Thus the image of $\mathcal{C}(K)$ under ξ is contained in a single coset of $2E(K)$ in $E(K)$.

Conversely, if $R \in \mathcal{C}(K)$ with $P = \xi(R) \in E(K)$, then let $Q \in E(K)$ and set $R' = \theta^{-1}(\theta(R) + Q)$. Then $\xi(R') = [2](\theta(R) + Q) = \xi(R) + 2Q = P + 2Q$, and $R' \in \mathcal{C}(K)$ since $\theta^\sigma(R') = \theta^\sigma\theta^{-1}(\theta(R) + Q) = \theta(R) + Q + T_\sigma = \theta^\sigma(R) + Q = (\theta(R) + Q)^\sigma = (\theta(R'))^\sigma = \theta^\sigma((R')^\sigma)$, and hence $R' = (R')^\sigma$ for all $\sigma \in G$.

(5) Given $R \in \mathcal{C}(K)$, define $\alpha : \mathcal{C} \to E$ by $\alpha(S) = \theta(S) - \theta(R)$. Then α is a birational isomorphism, and is defined over K since for all $\sigma \in G$ and $S \in \mathcal{C}(\overline{K})$ we have $\alpha(S)^\sigma = \alpha^\sigma(S^\sigma) = \theta^\sigma(S^\sigma) - \theta^\sigma(R) = \theta(S^\sigma) + T_\sigma - \theta(R) - T_\sigma = \alpha(S^\sigma)$. □

Remark. A diagram such as (4.1) is called a 2-*covering* of $E_{I,J}$. There is a notion of equivalence of 2-coverings, which here corresponds exactly to replacing the quartic g defining $\mathcal{C}$ with an equivalent quartic. Thus there is an injection from equivalence classes of quartics with invariants I and J to 2-coverings of the elliptic curve $E_{I,J}$. Unfortunately, this is not in general a bijection: there exist 2-coverings which cannot be represented by quartics in this way. However, when K is a number field, then all 2-coverings which are everywhere locally soluble are representable by quartics (see Lemma 1 of (Birch and Swinnerton-Dyer, 1963)), and this is the case of most interest to us. We discuss this question further in the next section.

Finally in this section, we have a result which will have important implications for the efficient practical implementation of a 2-descent algorithm over number fields.

Proposition 4.4. *With the same notation as above, let K' be an extension field of K. Then there is a bijection between*
(i) points $Q \in E(K')$ with $[2]Q = P$; and
(ii) roots of $g(X)$ in K'.

Proof. This follows immediately from Proposition 4.3 (2). □

For example, if K is a subfield of $\mathbb{R}$ (such as $\mathbb{Q}$) we can take $K' = \mathbb{R}$ here. If $\Delta < 0$, then $E(\mathbb{R})$ is connected and isomorphic to the circle group, hence 2-divisible with one 2-torsion point. It follows that in this case all quartics will have exactly two real roots. These are the "Type 3" quartics of (Birch and Swinnerton-Dyer, 1963). On the other hand, if $\Delta > 0$ then $E(\mathbb{R})$ has two components, the connected component of the identity $E^0(\mathbb{R}) = [\nvDash]\mathbb{E}(\mathbb{R})$ and the "egg-shaped" component $E(\mathbb{R}) - \mathbb{E}^{\nvDash}(\mathbb{R}) = \mathbb{E}(\mathbb{R}) - [\nvDash]\mathbb{E}(\mathbb{R})$. All the 2-torsion is real in this case. Thus the quartics are of two types here: "Type 2" quartics with four real roots, giving points on $E(K) \cap E^0(\mathbb{R})$, and "Type 1" quartics with no real roots, giving points on $E(K) - E^0(\mathbb{R})$. If $E(K) \subset E^0(\mathbb{R})$, then there will be no Type 1 quartics, while otherwise there is a bijection between the (soluble) Type

1 quartics and the soluble Type 2 quartics. We can make use of this observation in a practical algorithm, where we search separately for quartics of each type depending on the sign of the discriminant Δ.

Similar comments apply to the p-adic completions of a number field K. In a sequel to this paper we will discuss how this may be used to make 2-descent more efficient.

5. Galois Cohomology and Group Structure

It is easy to see that the map $\sigma \mapsto T_\sigma$ used in the proof of Proposition 4.3 is a cocycle, representing an element of the Galois cohomology group $H^1(\mathrm{Gal}(\overline{K}/K), E[2])$, and is in fact the image of $P = \xi(R)$ under the connecting homomorphism δ in the long exact sequence of Galois cohomology:

$$0 \hookrightarrow E(K)/2E(K) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[2]) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), E)[2].$$

This cocycle is independent of $R \in \mathcal{C}(K)$; changing θ to a different isomorphism $\mathcal{C} \to E$ which makes (4.1) commute has the effect of replacing the cocycle T_σ by a cohomologous cocycle: in fact, any such isomorphism must have the form θ^τ for some $\tau \in \mathrm{Gal}(\overline{K}/K)$, and the effect of replacing θ by θ^τ is to replace T_σ by $T_\sigma + (T_\tau^\sigma - T_\tau)$.

There is a bijection between the set of equivalence classes of 2-coverings of E and $H^1(\mathrm{Gal}(\overline{K}/K), E[2])$. In the application to 2-descent, one is only interested in the subgroup of $H^1(\mathrm{Gal}(\overline{K}/K), E[2])$ coming from K-rational points on E (the image of δ). These correspond to 2-coverings $\mathcal{C}$ which are soluble (meaning $\mathcal{C}(K) \neq \emptyset$); such cocycles become trivial in $H^1(\mathrm{Gal}(\overline{K}/K), E)$, as is evident from their representation as the coboundary $Q^\sigma - Q$ with $Q = \theta(R) \in E(\overline{K})$. When K is a number field, one can often only determine the 2-coverings which are everywhere locally soluble (meaning $\mathcal{C}(K_\mathcal{P}) \neq \emptyset$ for all completions $K_\mathcal{P}$ of K at primes $\mathcal{P}$ of K, including the infinite primes). As remarked above, these are all represented by quartics.

It is not true in general that the subset of elements of $H^1(\mathrm{Gal}(\overline{K}/K), E[2])$ representable by quartics with a fixed pair of invariants I, J is a subgroup (see below for an example). This cohomology group does not depend on the particular elliptic curve $E = E_{I,J}$, but rather only on its 2-division field L; for if E_1 and E_2 are two curves defined over K with the same 2-division field, then the 2-torsion subgroups $E_1[2]$ and $E_2[2]$ are isomorphic as Galois modules for $\mathrm{Gal}(\overline{K}/K)$, so we may identify $H^1(\mathrm{Gal}(\overline{K}/K), E_1[2])$ and $H^1(\mathrm{Gal}(\overline{K}/K), E_2[2])$; however the curves will (in general) have different invariants I, J, and the subsets of those elements of $H^1(\mathrm{Gal}(\overline{K}/K), E[2])$ which can be represented by quartics with each pair of invariants will be different.

The obstruction to an arbitrary 2-covering $\mathcal{C}$ of a given curve E being representable by a quartic is that, as an algebraic curve, $\mathcal{C}$ may have no positive K-rational divisor of degree 2. If $\mathcal{C}$ has such a divisor, then a straightforward application of the Riemann-Roch Theorem shows that $\mathcal{C}$ has an equation of the form $y^2 =$ quartic; see (Birch and Swinnerton-Dyer, 1963, Lemma 2). In (Birch and Swinnerton-Dyer, 1963, Lemma 1) it is shown (though not by explicit equations) that this obstruction is represented by the non-existence of a K-rational point on a certain curve of genus 0 defined over K, associated with the 2-covering. Using the Galois theory developed in Section 3, we can see this obstruction explicitly.

To a 2-covering $\mathcal{C}$ of E we have associated an element of $H^1(\mathrm{Gal}(\overline{K}/K), E[2])$ and also a "cubic seminvariant" $z \in K(\varphi)$ of square norm, uniquely determined modulo squares. Here the generator φ of the cubic field $K(\varphi)$ has trace 0 and determines the invariants

I and J via its minimal equation $\varphi^3 = 3I\varphi - J$. For the 2-covering to be representable by a quartic with invariants I, J, it is necessary and sufficient that we may choose a representative for the coset $z\,(K(\varphi)^*)^2$ which is linear in φ. Set $z = a + b\varphi + c\varphi^2$ and $z_1 = u + v\varphi + w\varphi^2$ with a, b, c, u, v and $w \in K$. Expanding zz_1^2, the coefficient of φ^2 is a quadratic form $Q(u, v, w)$ with coefficients which are functions of I, J, a, b, c:

$$\begin{aligned} Q(u,v,w) &= cu^2 + (a+3cI)v^2 + (3I(a+3cI) - bJ)w^2 \\ &\quad +2buv + 2(3bI - cJ)vw + 2(a+3cI)uw. \end{aligned}$$

Set $\alpha = 3c^2I + ac - b^2$ and $\beta = ab + c^2J$, and suppose that $N(z) = r^2$. (Note that we may assume that $c \neq 0$, else z is already linear in φ; and also that $\alpha \neq 0$, since α is (minus) the coefficient of φ^2 in r^2/z, so that if α were 0 then we could replace z by r^2/z which is linear in φ, and equivalent to z modulo squares.) Then with the linear change of variables $u_1 = cu + bv + (3cI + a)w$, $v_1 = \alpha v - \beta w$, $w_1 = rw$, we find that

$$\tilde{Q}(u_1, v_1, w_1) = \alpha c Q(u, v, w) = \alpha u_1^2 + v_1^2 - c w_1^2.$$

We require a nontrivial solution $(u, v, w) \neq (0, 0, 0)$ to $Q(u, v, w) = 0$. This equation is evidently the genus zero curve of (Birch and Swinnerton-Dyer, 1963, Lemma 1). If K is a number field and z represents a 2-covering which is everywhere locally soluble, then $Q(u, v, w) = 0$ will have points everywhere locally, and hence globally by the Hasse principle, so a solution will exist over K. Thus we will be able to find $z_1 \in K(\varphi)$ such that zz_1^2 is linear in φ, from which we may construct a quartic to represent the 2-covering as in Section 3.

We can now express the problem of whether the subset of $H^1(\mathrm{Gal}(\overline{K}/K), E[2])$, consisting of cocycles for which the corresponding 2-covering can be represented by quartics with invariants I, J, is closed under multiplication, in purely algebraic terms. Let $K(\varphi)$ be a cubic extension of the field K. Let H be the subgroup of $K(\varphi)^*/(K(\varphi)^*)^2$ consisting of those cosets whose representative elements z have square norm in K. From Section 3, we know that there is a bijection between (nontrivial elements of) H and the set of S_4 (respectively, A_4) extensions M of K containing the Galois closure L of $K(\varphi)$, according as $\mathrm{Gal}(L/K)$ is isomorphic to S_3 or A_3 respectively. We also have a bijection between H and $H^1(\mathrm{Gal}(\overline{K}/K), V_4)$, where the action of $\mathrm{Gal}(\overline{K}/K)$ on V_4 is via its S_3 (respectively A_3) quotient $\mathrm{Gal}(\overline{K}/L)$ which acts faithfully on V_4 by permuting its non-identity elements.

Fixing a generator φ for $K(\varphi)$ with trace 0, we determine elements I and J of K such that $\varphi^3 = 3I\varphi - J$. Then M is the splitting field of a quartic $g(X) \in K[X]$ with invariants I, J if and only if it corresponds to an element of H which has a representative which is linear in φ. The question is then: is the subset of such elements of H a subgroup?

To see that the answer to this question may be negative, let $\varphi = \sqrt[3]{2}$, and set $z_1 = 3(1 + \varphi)$ and $z_2 = 10(2 + \varphi)$. Then z_1 and z_2 have square norms 3^4 and 10^4 respectively. Setting $z_3 = z_1 z_2 = 30(2 + 3\varphi + \varphi^2)$, we can try to adjust z_3 modulo squares to eliminate the φ^2 term. This leads to the quadratic form

$$\begin{aligned} Q(u,v,w) &= u^2 + 6uv + 2v^2 + 4uw + 4vw + 6w^2 \\ &= (u + 3v + 2w)^2 + 2(w - 2v)^2 - 15v^2, \end{aligned}$$

which is 2-adically and 5-adically insoluble. Hence there are two quartics over $\mathbb{Q}$, with invariants $I = 0$ and $J = -2$, for which there is no product with these invariants. The associated elliptic curve E is $Y^2 = X^3 + 54$ with infinite cyclic Mordell-Weil group $E(\mathbb{Q})$;

the quartics are g_1 with coefficients $\frac{1}{108}(243, 0, -54, 24, -1)$, which is soluble and leads to the generator $(X, Y) = (3, 9)$ of $E(\mathbb{Q})$, and g_2 with coefficients $\frac{1}{90}(675, 0, -90, 20, -1)$ which is insoluble in $\mathbb{Q}_{\nvDash}$ and $\mathbb{Q}_{\ntrianglelefteq}$.

Hence, in general, the GL_2-equivalence classes of quartics with a fixed pair of invariants I, J in K cannot be made into an elementary abelian 2-group. However we do have a partial product, which can be useful.

Let g_1, g_2 and g_3 be three quartics all with the same invariants I and J. We say that $g_1 * g_2 = g_3$ if the associated cubic seminvariants satisfy $z_1 z_2 = z_3 \pmod{(K(\varphi))^2}$. Note that by Proposition 3.2, this relation is well-defined on equivalence classes of quartics. We can test the relation $g_1 * g_2 = g_3$ in practice, since the condition $z_1 z_2 z_3 =$ square is equivalent to the existence of a root in K of a certain fourth quartic over K (just as Proposition 3.3 gave a test for the equivalence of quartics, following Proposition 3.2).

Given two quartics g_1 and g_2 with invariants I and J, when can we construct a "product" quartic g_3 with $g_1 * g_2 = g_3$? If both g_1 and g_2 are soluble, then one could map each to a point on the elliptic curve $E_{I,J}$, add the points and construct the quartic g_3 from their sum. However, it is of interest to express this partial group law purely algebraically, without reference to elliptic curves. As we have seen, this can be done if certain conditions on the solubility of the corresponding homogeneous spaces hold. More generally, we can always form the associated ternary quadratic form $Q(u, v, w)$, as in the example above, and determine whether it has a zero. This is done in the next proposition, where $Q(u, v, w)$ is diagonalised explicitly, enabling certain cases to be dealt with simply.

Proposition 5.1. *Let $I, J \in K$ satisfy $4I^3 - J^2 \neq 0$ and let $g_i(X, Y) \in K[X, Y]$ for $i = 1, 2$ be quartics with invariants I and J. Suppose that the leading coefficients a_1, a_2 are equal modulo squares: $a_1 a_2 \in (K^*)^2$. Then there exists a quartic $g_3(X, Y)$ with invariants I and J such that $g_3 = g_1 * g_2$.*

Remark. Since we are free to replace g_1 or g_2 by equivalent quartics, we can also form $g_1 * g_2$ provided that there exist (x_1, y_1), $(x_2, y_2) \in K \times K \setminus (0, 0)$ such that $g_1(x_1, y_1) g_2(x_2, y_2) \in (K^*)^2$.

Proof. Let $z_i = (4a_i\varphi + p_i)/3$ be the cubic seminvariant of g_i for $i = 1, 2$, where $\varphi^3 = 3I\varphi - J$ as usual. The coefficient of φ^2 in $z_1 z_2 (u + v\varphi + w\varphi^2)^2$ is a ternary quadratic form $Q(u, v, w)$, and it suffices to find a non-trivial solution to $Q(u, v, w) = 0$. We have $N(z_i) = r_i^2$ for $i = 1, 2$ where $r_i \in K$.

Set

$$\begin{aligned} \alpha &= 16(a_1 a_2 p_1 p_2 + a_1^2 p_2^2 + a_2^2 p_1^2 - 48 I a_1^2 a_2^2), \\ \beta &= 4(a_1 p_1 p_2^2 + a_2 p_1^2 p_2 + 64 J a_1^2 a_2^2), \end{aligned}$$

and

$$\gamma = p_1^2 p_2^2 + 48 I a_1 a_2 p_1 p_2 + 64 J (a_1^2 a_2 p_2 + a_1 a_2^2 p_1),$$

and introduce new variables $\tilde{u}$, $\tilde{v}$, $\tilde{w}$ where

$$\begin{aligned} \tilde{u} &= 16 a_1 a_2 u + 4(a_1 p_2 + a_2 p_1) v + (p_1 p_2 + 48 I a_1 a_2) w, \\ \tilde{v} &= \alpha v + \beta w, \end{aligned}$$

and

$$\tilde{w} = 108 r_1 r_2 w.$$

The seminvariant syzygy (2.2) implies that

$$\beta^2 - \alpha\gamma = 16a_1a_2(27r_1^2)(27r_2^2) = (108r_1r_2)^2a_1a_2.$$

Using computer algebra we then find that

$$16\alpha a_1a_2Q(u,v,w) = \alpha\tilde{u}^2 - \tilde{v}^2 + a_1a_2\tilde{w}^2.$$

Hence there is a nontrivial solution when a_1a_2 is a square. □

References

Birch, B. J., Swinnerton-Dyer, H. P. F. (1963). Notes on elliptic curves I. *J. Reine Angew. Math.*, **212**:7–25.

Cremona, J. E. (1992). *Algorithms for Modular Elliptic Curves.* Cambridge University Press.

Cremona, J. E. (1997). *Algorithms for Modular Elliptic Curves.* Cambridge University Press, second edition.

Cremona, J. E., Serf, P. (1998). Computing the rank of elliptic curves over real quadratic fields of class number 1. *Mathematics of Computation.* to appear.

Elliott, E. B. (1913). *An Introduction to the Algebra of Quantics (Second Edition).* Oxford University Press.

Hilbert, D. (1993). *Theory of Algebraic Invariants.* Cambridge Mathematical Library. Cambridge University Press.

Schaefer, E. F. (1995). 2-descent on the jacobians of hyperelliptic curves. *Journal of Number Theory*, **51**(2):219–232.

Serf, P. (1995). *The rank of elliptic curves over real quadratic number fields of class number 1.* PhD thesis, Universität des Saarlandes.