On the equivalence of binary quartics

J. E. Cremona

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, UK.

T.A.Fisher

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

Abstract

We give an extension and correction to a result stated in the first author's paper *Classical Invariants and 2-descent on elliptic curves*, J. Symb. Comp. **31** (2001), concerning the equivalence of binary quartics. In the earlier version the cases where $I = 0$ or $J = 0$ were not fully treated, and neither were the cases of reducible quartics or those whose resolvent cubic is reducible; these are dealt with here. We also give an alternative criterion for equivalence.

In the first author's paper Cremona (2001), which formed part of the Proceedings of the 1996 Magma conference in Milwaukee, a result was stated concerning the equivalence of binary quartics. A number of things were wrong with the result as stated there: the definition of equivalence was stated incorrectly, the proof was incomplete for quartics one of whose invariants I, J vanish, and also we did not handle the cases of reducible quartics, or those whose resolvent cubic is reducible. In this note we correct those shortcomings. We also give an alternative criterion for equivalence.

At the request of the referee we have included a section explaining the connection between binary quartics and 2-descent on elliptic curves, which was our motivation for studying quartic equivalence.

Throughout, K will denote a field whose characteristic is neither 2 nor 3.

1. Binary quartics, their invariants and covariants

Let $\mathcal{BQ}$ denote the space of binary quartic forms with non-zero discriminant; $\mathcal{BQ}(K)$ will denote the set of those forms with coefficients in K. For $g(X,Y) = aX^4 + bX^3Y + cX^2Y^2 + dXY^3 + eY^4 \in \mathcal{BQ}$ we define the usual invariants,

$$I = 12ae - 3bd + c^2 \qquad \text{and} \qquad J = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3,$$

Email addresses: J.E.Cremona@warwick.ac.uk (J. E. Cremona), T.A.Fisher@dpmms.cam.ac.uk (T.A.Fisher).

and the discriminant $\Delta = 4I^3 - J^2$. This is 27 times the usual discriminant of a quartic, but we keep the notation of Cremona (2001) here, and the scaling is irrelevant for our present purposes. By definition, $\Delta \neq 0$ for $g \in \mathcal{BQ}$.

We also define the seminvariants $p = 3b^2 - 8ac$, $r = b^3 + 8a^2d - 4abc$, and $q = \frac{1}{3}(p^2 - 16a^2I)$. These satisfy the syzygy

$$27r^2 = p^3 - 48Ia^2p - 64Ja^3.$$

The covariants of $g(X, Y)$ are generated by g itself and the invariants, together with the Hessian

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

and the sextic

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

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

$$27g_6^2 = g_4^3 - 48Ig^2g_4 - 64Jg^3.$$

2. Irrational invariants and covariants

Associated to $g \in \mathcal{BQ}$ we have the resolvent cubic polynomial

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

whose discriminant is 27Δ. We let $L = K[\varphi] = K[X]/(f(X))$ be the associated étale algebra, so that φ is a "generic" root of f; depending on the factorization of $f(X)$ in $K[X]$, this is either a cubic extension field of K, or is isomorphic to the direct sum of K and a quadratic field extension, or to the direct sum of three copies of K. These fields are the images of L under the three distinct K-algebra homomorphisms $L \to \overline{K}$, whose order we fix once and for all, taking φ to one of the roots of f in $\overline{K}$. The images of $w \in L$ under these maps will be denoted w_1, w_2, w_3; these will be referred to as the conjugates of w. The norm map $\mathrm{N}_{L/K}\colon L \to K$ is then given by $\mathrm{N}_{L/K}(w) = w_1w_2w_3$. We extend this to a map $L[X, Y] \to K[X, Y]$. Denote by L^* the unit group of the algebra L; this consists of those elements whose norm is non-zero.

Define

$$G(X,Y) = \frac{1}{3}(4\varphi g(X,Y) + g_4(X,Y)) \in L[X,Y].$$

This is an "irrational" covariant of g. The covariant syzygy may now be expressed as $\mathrm{N}_{L/K}(G) = g_6^2$. It follows that with at most 6 exceptions, for $(x : y) \in \mathbb{P}^1(K)$ the value $G(x, y)$ is an element of L^*, whose norm lies in K^{*2}. For this reason we will assume throughout that K is not the field with 5 elements.

Lemma 1 *We have the identity*

$$G(X_1,Y_1)G(X_2,Y_2) = F(X_1,Y_1,X_2,Y_2)^2$$

where $F \in L[X_1,Y_1,X_2,Y_2]$ *is given by*

$$\begin{aligned}9F(X_1,Y_1,X_2,Y_2) &= (12a\varphi - 24ac + 9b^2)X_1^2X_2^2 \\ &+ (6b\varphi - 36ad + 6bc)X_1X_2(X_1Y_2 + Y_1X_2) \\ &+ (-2\varphi^2 + 2c\varphi - 9bd + 4c^2)(X_1^2Y_2^2 + Y_1^2X_2^2) \\ &+ (4\varphi^2 + 8c\varphi - 144ae + 4c^2)X_1Y_1X_2Y_2 \\ &+ (6d\varphi - 36be + 6cd)Y_1Y_2(X_1Y_2 + Y_1X_2) \\ &+ (12e\varphi - 24ce + 9d^2)Y_1^2Y_2^2.\end{aligned}$$

Proof. This is an identity which may be checked using computer algebra; we will not need to use the explicit form of F, only that it exists with coefficients in L. Note that $F(X,Y,X,Y) = G(X,Y)$ and $\mathrm{N}_{L/K}\, F(X_1,Y_1,X_2,Y_2) = g_6(X_1,Y_1)g_6(X_2,Y_2)$. □

Remark. To see where the identity comes from, note that (over $\overline{K}$) G is a constant times the square of a quadratic (in fact, the condition that a linear combination of g and g_4 be the square of a quadratic is satisfied by precisely three elements of the pencil of quartics spanned by g and g_4; this may be used to motivate and define the resolvent cubic). Specifically, we can write $G(1,0)G(X,Y) = H(X,Y)^2$ where $H = \frac{1}{12}G_{XX} + \frac{2}{9}(I - \varphi^2)Y^2$ and G_{XX} is the second derivative of $G(X,Y)$ with respect to X. Provided that $G(1,0) \neq 0$, this identity is already sufficient to prove Proposition 2 below; to treat the general case we computed F generically, thereby obtaining the identity of Lemma 1.

The quantity $G(1,0) = \frac{1}{3}(4a\varphi + p) \in L$ was denoted z in Cremona (2001); here we will define an irrational invariant $z(g)$ slightly differently, as an element of L^*/L^{*2}.

Proposition 2 *The value of* $G(x,y) \in L^*/L^{*2}$ *is independent of* $(x,y) \in K \times K$ *(provided that* $G(x,y)$ *is a unit).*

Proof. This is immediate from the identity in Lemma 1. □

Hence we may define the *cubic invariant* $z(g)$ for $g \in \mathcal{BQ}$ by

$$z(g) = G(x,y) \in L^*/L^{*2} \qquad \text{for any choice of } (x,y) \text{ such that } G(x,y) \text{ is a unit.}$$

If $r = g_6(1,0) \neq 0$ then we may take $z(g) = G(1,0) = \frac{1}{3}(4a\varphi + p)$, as in Cremona (2001). Alternatively if $r^* = g_6(0,1) \neq 0$ then we may take $z(g) = G(0,1) = \frac{1}{3}(4e\varphi + p^*)$ where $p^* = g_4(0,1)$. In all cases we have

$$\mathrm{N}_{L/K}(z(g)) = \mathrm{N}_{L/K}(G(x,y)) = g_6(x,y)^2 \in K^{*2},$$

and see that (for $x,y \in K$) $G(x,y) \in L^*$ if and only if $g_6(x,y) \neq 0$.

Lemma 3 *If* $g \in \mathcal{BQ}(K)$ *has a linear factor in* $K[X,Y]$*, then* $z(g) = 1$.

Proof. Suppose that $g(x,y) = 0$ with $x,y \in K$ not both zero. Then $g_4(x,y) \neq 0$ and $g_6(x,y) \neq 0$, since the resultants of g with g_4 and g_6 are $\Delta^2/3^2$ and $\Delta^3/3^9$, hence nonzero; the syzygy then gives $G(x,y) = \frac{1}{3}g_4(x,y) = (3g_6(x,y)/g_4(x,y))^2$. □

Remarks. In Cremona (2001) we called $z = \frac{1}{3}(4a\varphi + p)$ an "irrational seminvariant" of g, viewing it as an element of (the field) L rather than L^*/L^{*2}. We were then assuming that both the quartic and the resolvent cubic were irreducible, so it was not necessary to consider the case $r = 0$. We will see below that $z(g)$, as an element of L^*/L^{*2}, is a genuine invariant (see below for precise definitions), so we may call it an "irrational invariant", keeping the term "invariant" for the classical "rational invariants" I and J.

In order to avoid having to omit values of $G(x, y)$ coming from roots of g_6, we may proceed as follows. If $g(x, y) = 0$ then $g_6(x, y) \neq 0$ (and $z(g) = 1$ anyway by Lemma 3). Otherwise, the three conjugates of $G(x, y)$ are distinct, so at most one can be zero; in that case we replace the zero conjugate by the product of the other two, which gives us a new element of L which lies in L^* and whose norm is in K^{*2}.

We will later give conditions, in terms of $z(g)$, under which two quartics with the same invariants are "equivalent". This requires us to define equivalence more precisely than in Cremona (2001).

3. Group actions, equivalence and proper equivalence

The group GL_2 acts on binary forms via linear substitution:

$$\begin{pmatrix} X & Y \end{pmatrix} \mapsto \begin{pmatrix} X & Y \end{pmatrix} M = \begin{pmatrix} \alpha X + \gamma Y & \beta X + \delta Y \end{pmatrix},$$

where $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$; that is, M maps

$$g(X, Y) \mapsto g^M(X, Y) = g(\alpha X + \gamma Y, \beta X + \delta Y).$$

We also need the following action of GL_1: $\lambda \in \mathrm{GL}_1$ maps

$$g(X, Y) \mapsto \lambda^2 g(X, Y).$$

Combining the two actions, the group $\mathrm{GL}_2 \times \mathrm{GL}_1$ acts on $\mathcal{BQ}$ as follows: the pair (M, λ) with $M \in \mathrm{GL}_2$ and $\lambda \in \mathrm{GL}_1$ maps

$$g(X, Y) \mapsto g'(X, Y) = \lambda^2 g^M(X, Y) = \lambda^2 g(\alpha X + \gamma Y, \beta X + \delta Y).$$

We will say that two quartics g_1 and g_2 are *equivalent*[1] if there exists (M, λ) mapping g_1 to g_2, and *properly equivalent* if there exists such (M, λ) with $\mu := \det(M)\lambda = \pm 1$. (Note that (M, λ) and $(M, -\lambda)$ have the same action, so the sign of μ is immaterial.)

We have

$$\begin{aligned} I(g') &= \mu^4 I(g); \\ J(g') &= \mu^6 J(g); \\ \Delta(g') &= \mu^{12} \Delta(g). \end{aligned}$$

[1] The reason for considering equivalence by $\mathrm{GL}_2 \times \mathrm{GL}_1$ and not just GL_2 is that we are motivated by the application to 2-descent on elliptic curves. Each quartic g defines a curve of genus one with equation $Y^2 = g(X, Z)$, which is a 2-cover of its Jacobian, the elliptic curve $Y^2 = X^3 - 27IX - 27J$. Two quartics give isomorphic 2-coverings if and only if they are properly equivalent in the sense defined here.

Also, the quartic and sextic covariants of g' are easily seen to be

$$\det(M)^2\lambda^4 g_4^M = \lambda^2\mu^2 g_4^M \qquad \text{and} \qquad \det(M)^3\lambda^6 g_6^M = \lambda^3\mu^3 g_6^M$$

respectively. In particular, we see that the operation of taking the Hessian commutes with proper equivalence, and that the invariants I, J and Δ are unchanged under a proper equivalence.

We record these facts in the following lemmas.

Lemma 4 *(1) Properly equivalent quartics have the same invariants.*

(2) Equivalent quartics with the same invariants I, J such that $IJ \neq 0$ are properly equivalent.

Lemma 5 *A proper equivalence (M, λ), which sends g to $\lambda^2 g^M$, sends the Hessian covariant g_4 to $\lambda^2 g_4^M$, and hence the irrational covariant G to $\lambda^2 G^M$.*

4. A criterion for equivalence in terms of the cubic invariant $z(g)$

From the previous section, we already see that the cubic invariant $z(g)$ is indeed invariant under proper equivalence; note that since properly equivalent quartics have the same invariants they also have the same associated cubic algebra L, so it makes sense to compare their z-invariants. The following proposition replaces one direction of (Cremona, 2001, Proposition 3.2(2)).

Proposition 6 *Suppose that the two quartics g and g' are properly equivalent. Then $z(g) = z(g')$ in L^*/L^{*2}.*

Proof. Immediate from Proposition 2 and Lemma 5. □

We can, with a little care, extend the preceding result to non-proper equivalence via (M, λ) with $\mu = \det(M)\lambda \neq 1$. It suffices to consider the case where M is the identity matrix, so that $g' = \lambda^2 g$. Now the cubic algebras $L = K[\varphi]$, $L' = K[\varphi']$ are isomorphic via the identification $\varphi' = \lambda^2\varphi$. With this identification, $z(g') = \lambda^4 z(g) = z(g)$.

We saw earlier that quartics with a linear factor have $z(g) = 1$. We next see that all quartics with the same invariants and which have a linear factor are properly equivalent to each other.

Proposition 7 *Let g be a quartic with invariants I, J which has a linear factor in $K[X, Y]$. Then g is properly equivalent to*

$$\frac{1}{27}Y(27X^3 - 9IXY^2 - JY^3) = -\frac{1}{27}Y^4 F\left(\frac{-3X}{Y}\right).$$

Hence any two quartics with the same invariants and which both have linear factors are properly equivalent.

Proof. Use a suitable $M \in \mathrm{GL}_2(K)$ to take the linear factor to Y, so that $a = 0$ and $b \neq 0$. Replace X by $X - (c/3b)Y$ to make $c = 0$, and then transform with $M = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$ and $\lambda = 1/b$ to make $b = 1$. Now g has the form $Y(X^3 + dXY^2 + eY^3)$ where $I = -3d$ and $J = -27e$. □

In fact, the class of trivial quartics is characterized by the triviality of the z-invariant in L^*/L^{*2}. This was essentially the statement of (Cremona, 2001, Proposition 3.2(1)), where the proof given was valid only in the irreducible case.

Proposition 8 *$z(g) = 1$ in L^*/L^{*2} if and only if g has a linear factor in $K[X, Y]$.*

Proof. One direction is Lemma 3.

For the converse, we may assume (after a suitable proper transformation) that $r \neq 0$, so $z(g) = G(1, 0)$, with characteristic polynomial $h(Z) = Z^3 - pZ^2 + qZ - r^2$. Suppose that $z = z_1^2$ where $z_1 \in L$ has characteristic polynomial $h_1(Z) = Z^3 + uZ^2 + vZ + r$ (replacing z_1 by $-z_1$ if necessary). Then $h(Z^2) = -h_1(Z)h_1(-Z)$; comparing coefficients and a little algebra then shows that $-(u + b)/(4a)$ is a root of g. (This is essentially the same argument as used in Cremona (2001)). □

The next two lemmas will be used in the proof of Theorem 11 below.

Lemma 9 *Let g_1, $g_2 \in \mathcal{BQ}(K)$ have the same invariants I, J. Denote their seminvariants by a_1, p_1, r_1 and a_2, p_2, r_2 respectively, and suppose that $r_1, r_2 \neq 0$. If $z(g_1) = z(g_2)$ then the quartic*

$$\widetilde{g}(X) = X^4 - 2s_1X^2 - 216r_1^2r_2X + s_1^2 - 36r_1^2s_2$$

has a root in K, where

$$s_1 = p_1^2p_2 - 16a_1(a_1p_2 + 2a_2p_1)I - 64a_1^2a_2J,$$
$$s_2 = p_1p_2^2 - 16a_2(a_2p_1 + 2a_1p_2)I - 64a_1a_2^2J.$$

Moreover if $g = p_1g_2 - a_1h_2$ has coefficients a, b, c, d, e, where h_2 is the Hessian covariant of g_2, and $a \neq 0$, then

$$\widetilde{g}(X) = \frac{1}{a}g(X + b, -4a).$$

Proof. The first part is a variant of (Cremona, 2001, Proposition 3.3).

We put $z_i = (4a_i\varphi + p_i)/3$ for $i = 1, 2$. Then $h(X) = \mathrm{N}_{L/K}(X - z_1^{-1}z_2) = X^3 - pX^2 + qX - r^2$ where

$$p = s_1/(3r_1)^2, \qquad q = s_2/(3r_1)^2, \qquad r = r_2/r_1.$$

Since $z(g_1) = z(g_2)$, there exists $w \in L^*$ with $w^2 = z_1^{-1}z_2$ and $N_{L/K}(w) = r$ (replacing w by $-w$ if necessary). We put $h_0(X) = N_{L/K}(X - w) = X^3 - uX^2 + vX - r$. Then comparing coefficients in $h(X^2) = -h_0(X)h_0(-X)$ gives

$$(u^2 - p)^2 - 8ru - 4q = 0, \qquad \text{i.e.,} \quad \widetilde{g}(3r_1u) = 0.$$

The required root of $\widetilde{g}$ is therefore $3r_1u$.

The second part follows by computer algebra. □

Lemma 10 *Let g_1, $g_2 \in \mathcal{BQ}(K)$ have the same invariants I, J. With notation as in Lemma 9, suppose that $r_1 \neq 0$ and that $g = p_1g_2 - a_1h_2$ has a linear factor over K. Then g_1 and g_2 are properly equivalent.*

Proof. Applying a suitable proper equivalence to g_2 we may assume that $g(1,0) = 0$, so that $p_1 a_2 = a_1 p_2$. Now $a_1 = 0$ implies $p_1 \neq 0$ (by nonsingularity) and hence $a_2 = 0$, in which case both g_1 and g_2 are trivial, hence equivalent. Otherwise $a_1 \neq 0$ and $a_2 \neq 0$. Set $t = a_2/a_1 = p_2/p_1$; then the seminvariant syzygy gives $r_2^2 = t^3 r_1^2$. Since $r_1 \neq 0$, it follows that t is a (non-zero) square; then after a proper diagonal transformation we may assume that $t = 1$, $a_2 = a_1$, $p_2 = p_1$, $r_2 = r_1$. Finally, a shift makes $b_2 = b_1$, from which the equality of invariants forces $g_2 = g_1$. □

We now state our main result, completing (Cremona, 2001, Proposition 3.2(2)).

Theorem 11 *Let g_1 and g_2 be quartics with the same invariants. Then $z(g_1) = z(g_2)$ if and only if g_1 and g_2 are properly equivalent.*

Proof. One direction is Proposition 6 above.

For the converse, suppose that $z(g_1) = z(g_2)$ where $I(g_1) = I(g_2)$ and $J(g_1) = J(g_2)$. We already know the result when $z(g_1) = z(g_2) = 1$, so we may assume that neither quartic has a linear factor; in particular, their leading coefficients are non-zero. Also by applying a suitable proper equivalence to each quartic, we may assume that $r_1, r_2 \neq 0$. Now Lemma 9 implies that $p_1 g_2 - a_1 h_2$ has a linear factor over K, from which the proper equivalence of g_1 and g_2 follows by Lemma 10. □

The above proof is rather different from the one given in Cremona (2001); for completeness we also give a correction to the original proof, which was incomplete in the case that either $I = 0$ or $J = 0$.

Proof. [Alternative proof of the converse]

As before we may assume that the leading coefficients a_1, a_2, r_1, r_2 of both g_1 and g_2 and their sextic covariants are non-zero. Then $z(g_1)$ and $z(g_2)$ are represented by $z = (4a_1\varphi + p_1)/3$ and $z^* = (4a_2\varphi + p_2)/3$. Our hypothesis is that $z = w^2 z^*$ for some w in $L = K[\varphi]$. The proof of (Cremona, 2001, Proposition 3.2) carries over to show that there exists $M \in \mathrm{GL}_2(K)$ taking the roots of g_1 to those of g_2.

Hence, after replacing g_2 by its properly equivalent image under $(M, \det(M)^{-1})$, we may assume that g_1 and g_2 have the same roots, so that $g_2 = m g_1$ for some $m \in K^*$.

Comparing the I and J invariants we see that if $I \neq 0$ then $m^2 = 1$ and if $J \neq 0$ then $m^3 = 1$. So when $IJ \neq 0$ we have $m = 1$ and the proof is then complete. We now consider the cases $I = 0$ and $J = 0$ separately.

Suppose that $I = 0$.

Then we only know that $m^3 = 1$, and so m could be a primitive cube root of unity (provided that these lie in K). Suppose then that ζ is a primitive cube root of unity; we will show that if $z(g) = z(\zeta g)$ then g and ζg are properly equivalent. In fact, in this case g has a linear factor over K, from which the proper equivalence of g and ζg follows from Proposition 7.

Since $I = 0$ we have $\varphi^3 = -J$, and the conjugates of φ are φ_1, $\varphi_2 = \zeta\varphi_1$ and $\varphi_3 = \zeta^2\varphi_1$, so the conjugates of $z = (4a\varphi + p)/3$ are $z_1 = (4a\varphi_1 + p)/3$, $z_2 = (4a\zeta\varphi_1 + p)/3$ and $z_3 = (4a\zeta^2\varphi_1 + p)/3$. The product of these is in K^{*2}.

Now $z(\zeta g) = (4\zeta a\varphi + \zeta^2 p)/3 = \zeta^2(4a\zeta^2\varphi + p)/3$, so the conjugates of $z(\zeta g)$ are $\zeta^2 z_3$, $\zeta^2 z_1$, $\zeta^2 z_2$ (in that order). Since $z(g) = z(\zeta g)$, it follows that $z(g)$ is a square, so g has a linear factor by Proposition 8.

Suppose that $J = 0$.

Then we only know that $m^2 = 1$, and so possibly $m = -1$. Suppose then that g is a quartic with $J = 0$ such that $z(g) = z(-g)$. We will show that g and $-g$ are properly equivalent.

If $a = 0$ then we are done by Proposition 7 since both g and $-g$ have a linear factor, namely Y. Multiplying g by a constant we may assume that $a = 1$. After a proper equivalence we may assume that $p \neq 0$. After a substitution of the form $X \mapsto X + \alpha Y$ we may suppose that $b = 3r/p$, so that $bc = 6d$. Write $b = 4\beta$ and $c = 6\gamma$. Then $p = 48(\beta^2 - \gamma)$ and $J = 432(\beta^2 - \gamma)(\gamma^2 - e)$; but $J = 0$ and $p \neq 0$, so we have $e = \gamma^2$ and the coefficients of g are $(1, 4\beta, 6\gamma, 4\beta\gamma, \gamma^2)$.

The condition that $z(g) = z(-g)$ now implies that at least one of $-\gamma$, $\beta^2 - \gamma$ is in K^{*2}. If $\gamma = -u^2$ with $u \in K$ then the identity

$$g(uX + \gamma Y, X + uY) = -4u^4 g(X, Y)$$

shows that g and $-g$ are properly equivalent. If $\gamma = \beta^2 - u^2$ for some $u \in K$ then the identity

$$g((\beta + u)X + \gamma Y, -X - (\beta + u)Y) = -4u^2(\beta + u)^2 g(X, Y)$$

again shows that g and $-g$ are properly equivalent. □

5. A new criterion for equivalence of quartics

In (Cremona, 2001, Proposition 3.3), we gave a simple and practical criterion for two quartics with the same invariants to be equivalent, in terms of a third quartic having a root (all over the same field K). However, the criterion stated in Cremona (2001) is incorrect when the cubic resolvent is reducible. For example, let $g_1(X) = 2X^4 - 8X^2 - 8X + 22$ and $g_2(X) = 3X^4 + 22X^2 - 16X + 3$, both in $\mathbb{Q}[X]$ with $I = 592$ and $J = -27776$. The algebra L is isomorphic to the direct sum of $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{33})$. The criterion in (Cremona, 2001, Proposition 3.3) incorrectly predicts that g_1 and g_2 are equivalent, since the auxiliary quartic defined there does have a root. In fact, for this example, $z = z(g_1)z(g_2)/32^2$ has characteristic polynomial $h(Z) = (Z - 9)(Z - 3)^2$ and $h(Z^2)$ does factorise as $h(Z^2) = -h_1(Z)h_1(-Z)$ with $h_1(Z) = (Z - 3)(Z^2 - 3)$, but z is not a square in L since its conjugates are $9, 3, 3$ and 3 is not a square in $\mathbb{Q}(\sqrt{33})$.

Here we describe a new criterion for the proper equivalence of two quartics, essentially coming from Lemma 10 above, again saying that two quartics with the same invariants are equivalent if a third quartic has a linear factor over K.

Let g_1 and g_2 be two binary quartics, with Hessian covariants h_1 and h_2 respectively. Define $F = F_{g_1,g_2} \in K[X_1, Y_1, X_2, Y_2]$ by

$$F(X_1, Y_1, X_2, Y_2) = g_1(X_1, Y_1)h_2(X_2, Y_2) - g_2(X_2, Y_2)h_1(X_1, Y_1).$$

Then F is bi-homogeneous of bi-degree $(4, 4)$ in the pairs of variables X_1, Y_1 and X_2, Y_2 respectively.

The group $\mathrm{GL}_2 \times \mathrm{GL}_1$ acts on such forms in two ways, via linear substitution in either set of variables. For example, if we replace g_1 by its image under the proper transformation (M, λ) (with $\lambda = \det(M)^{-1}$) then g_1 is replaced by $\det(M)^{-2} g_1^M$ and h_1 by $\det(M)^{-2} h_1^M$, so F is transformed to $\det(M)^{-2} F(X_1', Y_1', X_2, Y_2)$ where $\begin{pmatrix} X_1' & Y_1' \end{pmatrix} = \begin{pmatrix} X_1 & Y_1 \end{pmatrix} M$.

We will be considering bi-linear factors in $K[X_1, Y_1, X_2, Y_2]$ of bi-homogeneous forms; by this we mean bi-homogeneous factors of bi-degree $(1,1)$, of the form

$$\alpha X_1X_2 + \beta X_1Y_2 + \gamma Y_1X_2 + \delta Y_1Y_2 = \begin{pmatrix} X_1 & Y_1 \end{pmatrix} A \begin{pmatrix} X_2 \\ Y_2 \end{pmatrix}$$

where $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(K)$.

Our result is as follows.

Theorem 12 *Let g_1 and g_2 be quartics with the same invariants. Then g_1 and g_2 are properly equivalent if and only if F_{g_1,g_2} has a K-rational bi-linear factor. Moreover, if this factor has associated matrix $A \in \mathrm{GL}_2(K)$, then g_2 is the transform of g_1 via the proper equivalence $(M, \det(M)^{-1})$ where $M = A^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.*

Proof. First we observe that in the case $g_1 = g_2$ we have $F_{g_1,g_1} = g_1(X_1, Y_1)h_1(X_2, Y_2) - g_1(X_2, Y_2)h_1(X_1, Y_1)$ which has the bi-linear factor $X_1Y_2 - Y_1X_2$.

Next, replace the second g_1 by the properly equivalent $g_2 = \det(M)^{-2} g_1^M$ where $M \in \mathrm{GL}_2(K)$; then $F_{g_1,g_2} = \det(M)^{-2} F_{g_1,g_1}(X_1, Y_1, X_2', Y_2')$ where $\begin{pmatrix} X_2' & Y_2' \end{pmatrix} = \begin{pmatrix} X_2 & Y_2 \end{pmatrix} M$. This has the bi-linear factor

$$X_1Y_2' - Y_1X_2' = \begin{pmatrix} X_1 & Y_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} X_2' \\ Y_2' \end{pmatrix} = \begin{pmatrix} X_1 & Y_1 \end{pmatrix} A \begin{pmatrix} X_2 \\ Y_2 \end{pmatrix}$$

where $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M^T$.

So far we have established that if g_2 is properly equivalent to g_1 then F_{g_1,g_2} has a bi-linear factor, from which we can recover the equivalence as in the statement of the theorem.

Conversely, if F_{g_1,g_2} has a bi-linear factor, we may again assume that $r_1, r_2 \neq 0$; then specialising $(X_1, Y_1) = (1, 0)$ reduces to the situation in Lemma 10, and hence g_1 and g_2 are properly equivalent. $\square$

Remarks

1. Over $\overline{K}$ we see that there are always exactly four proper equivalences between any two quartics with the same invariants, coming from the four bi-linear factors of F_{g_1,g_2}. In particular there are always exactly three non-trivial proper equivalences from a quartic g to itself; these are defined over the resolvent cubic extension L. They permute the roots while leaving the cross-ratio invariant. In terms of the genus one curve with equation $Z^2 = g(X, Y)$, these self-equivalences come from the addition of two-torsion points on the Jacobian, which are defined over L.

2. In practice we may simplify the test for equivalence given by Theorem 12 by specialisation, as in Lemma 10: it is easier to check that a binary quartic has a root than to

work with bi-quartics. To test for a bi-linear factor of $F(X_1, Y_1, X_2, Y_2)$, it is enough to do so after specialising X_1, Y_1 to values $x_1, y_1 \in K$, provided that the specialised polynomial (which is a homogeneous quartic in X_2, Y_2) has distinct factors; this is the case provided that $g_6(x_1, y_1) \neq 0$. Hence, unless $r_1 = 0$, we may specialise to $(x_1, y_1) = (1, 0)$, in which case our test for equivalence is simply whether $a_1h_2 - p_1g_2$ has a linear factor as in Lemma 10. In case $r_1 = 0$, we merely have to apply a suitable preliminary proper transformation to g_1 to bring us to the case $r_1 \neq 0$.

6. Relation to the theory of 2-descent on elliptic curves

Let E/K be an elliptic curve with Weierstrass equation

$$y^2 = x^3 - 27Ix - 27J.$$

(Since $\mathrm{char}(K) \neq 2, 3$, every elliptic curve defined over K has a model of this form.) As before, we let $L = K[\varphi]$ where φ is a root of $f(X) = X^3 - 3IX + J$. The 2-torsion points of E are the points $(x, y) = (-3\varphi_i, 0)$ for $i = 1, 2, 3$. We write H for the subgroup of $L^*/(L^*)^2$ consisting of elements of square norm, and S for the set of proper K-equivalence classes of binary quartics with invariants I and J.

Consider the following three maps:

- The Cassels map is a group homomorphism $\delta : \ E(K)/2E(K) \to H$ given for $P \in E(K) \setminus E[2]$ by
$$P = (\xi, \eta) \mapsto \xi + 3\varphi;$$
the case P is a non-trivial 2-torsion point is treated exactly as in the remarks at the end of §2, *i.e.* by replacing the zero conjugate by the product of the other two.
- There is a map $q : \ E(K)/2E(K) \to S$ given by
$$P = (\xi, \eta) \mapsto g$$
where
$$g(X, Y) = X^4 - \tfrac{1}{6}\xi X^2Y^2 - \tfrac{1}{27}\eta XY^3 + \tfrac{1}{432}(-\xi^2 + 36I)Y^4;$$
the identity $0 \in E(K)$ is sent to the class in S consisting of quartics with a K-rational linear factor.
- There is a map $z : \ S \to H$ given by $g \mapsto z(g)$ where $z(g)$ is the cubic invariant introduced in §2.

Theorem 13 *(1) Each of the above three maps is well-defined and injective. Moreover $\delta = z \circ q$.*

(2) The image of q consists of those classes in S that are represented by K-soluble quartics. (We say that a quartic $g(X, Y)$ is K-soluble if the smooth projective curve with affine equation $y^2 = g(x, 1)$ has a K-rational point.)

(3) The image of z consists of those classes in H that may be represented by an element of L that is linear in φ.

Proof. (1) The properties of the Cassels map are established in (Cassels, 1991, §15). The map z is well-defined and injective by Theorem 11. The cubic invariant of $g = q(P)$ is

$$z(g) = \frac{1}{3}(4\varphi g(1, 0) + g_4(1, 0)) = \left(\frac{2}{3}\right)^2 (\xi + 3\varphi).$$

This proves the compatibility of the maps. It follows that q is also well-defined and injective.

(2) The leading coefficient of $g = q(P)$ is a square, so $q(P)$ is clearly soluble. Conversely if $g(X, Y)$ is soluble, but does not have a K-rational root, then by a proper equivalence we may assume it has leading coefficient $a = 1$. A substitution of the form $X \leftarrow X + \lambda Y$ reduces us to the case $b = 0$. We put $\xi = -6c$ and $\eta = -27d$. Then by the formulae defining I and J we have $e = (-\xi^2 + 36I)/432$ and $\eta^2 = \xi^3 - 27I\xi - 27J$. Hence q maps $(\xi, \eta) \in E(K)$ to g.

(3) It is clear from the definition of $z(g)$ that it is represented by an element linear in φ. Conversely, suppose that $z = u + v\varphi$ and $N_{L/K}(z) = r^2$ for some $u, v, r \in K$. If $v = 0$ then the norm condition forces z to be a square, in which case we take g with a K-rational linear factor. Otherwise, following (Simon, 2002, §1.4) we put

$$g(X, Y) = \frac{1}{12v}(X^4 - 6uX^2Y^2 + 8rXY^3 + (12Iv^2 - 3u^2)Y^4).$$

It is routine to check that g has invariants I and J, while

$$z(g) = \frac{1}{3}(4\varphi g(1, 0) + g_4(1, 0)) = \frac{1}{9v^2}(u + v\varphi).$$

□

Remarks

(1) There is a natural identification of H with the Galois cohomology group $H^1(K, E[2])$; see Cremona (2001) or Schaefer (1995). With this identification the Cassels map δ becomes the connecting map of Galois cohomology.

(2) We may identify S as a subset of H. In general it is *not* a subgroup; see (Cremona, 2001, §5) for an example in the case $K = \mathbb{Q}$ where S is not closed under multiplication. In the terminology of Cremona et al. (2008), O'Neil (2002), S is called the kernel of the obstruction map. (As noted there, the obstruction map is quadratic, and so its kernel need not be a subgroup.)

(3) Let $g(X, Y)$ be a binary quartic with invariants I and J. Let $\mathcal{C}$ be the smooth projective curve with affine equation $y^2 = g(x, 1)$. The 2-covering map $\pi : \mathcal{C} \to E$ (see An et al. (2001) or Cremona (2001)) is given by

$$(x, y) \mapsto \left(\frac{3g_4(x, 1)}{4y^2}, \frac{27g_6(x, 1)}{8y^3}\right).$$

If $Q = (x, y) \in \mathcal{C}(K)$ with $\pi(Q) = P = (\xi, \eta)$ then $\delta(P) = z(g)$, since

$$\xi + 3\varphi = \frac{3g_4(x, 1)}{4y^2} + 3\varphi = \frac{3}{4y^2}(4\varphi g(x, 1) + g_4(x, 1)).$$

This gives another proof of Theorem 13(2).

Each binary quartic with invariants I and J determines a 2-covering $(\mathcal{C}, \pi)$ of E as above. It may be checked that properly equivalent binary quartics give rise to isomorphic 2-coverings. There is also a standard identification of $H^1(K, E[2])$, and hence of H, with the set of 2-coverings of E up to isomorphism. Combining these two constructions gives a map $S \to H$. There is some interest in checking this map agrees with that defined by the cubic invariant, which we now do.

According to (Cremona et al., 2008, Lemma 3.10) the image of the 2-covering $(\mathcal{C}, \pi)$ in H is given by $\det(M)/\det(M_E)$ where $M \in \mathrm{GL}_2(L)$ describes the action of $E[2]$ on $\mathcal{C}$, and M_E performs the same role for the trivial 2-covering. We now compute these matrices and check that the ratio of their determinants agrees with the cubic invariant.

Let $B = B(u, v)$ be the bilinear form on K^3 uniquely determined by

$$F(X_1, Y_1, X_2, Y_2) = B(X_1^2, 2X_1Y_1, Y_1^2; X_2^2, 2X_2Y_2, Y_2^2)$$

where F is as given in the statement of Lemma 1. Let $R = R(u)$ be the cubic form uniquely determined by

$$\begin{aligned} g(X_1, Y_1)g_4(X_2, Y_2) - g(X_2, Y_2)g_4(X_1, Y_1) \\ = -3(X_1Y_2 - Y_1X_2)R(X_1X_2, X_1Y_2 + X_2Y_1, Y_1Y_2). \end{aligned} \tag{1}$$

By computer algebra we are able to verify that $B(u, u)$ is a rank 1 quadratic form, and that

$$N_{L/K}(B(u, v)) = R(u)R(v) \tag{2}$$

for all $u, v \in K^3$. (This reduces in the special case $u = v = (X^2, 2XY, Y^2)$ to the identity $N_{L/K}(G(X, Y)) = g_6(X, Y)^2$ already encountered in §2.) It follows that $z(g) = B(u, u)$ for any vector $u \in K^3$ with $R(u) \neq 0$. We now fix such a u and put $\alpha_i = B(e_i, u)$ where $e_1, e_2, e_3 \in K^3$ are the standard basis vectors. By (1) and (2), the latter with $v = (X_1X_2, X_1Y_2 + X_2Y_1, Y_1Y_2)$, we deduce

$$\begin{aligned} R(u)\big(g(X_1, Y_1)g_4(X_2, Y_2) - g(X_2, Y_2)g_4(X_1, Y_1)\big) \\ = -3(X_1Y_2 - Y_1X_2)N_{L/K}\left(\begin{pmatrix} X_1 & Y_1 \end{pmatrix}\begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_3 \end{pmatrix}\begin{pmatrix} X_2 \\ Y_2 \end{pmatrix}\right). \end{aligned}$$

Hence by Theorem 12 the action of $E[2]$ on $\mathcal{C}$ is given by

$$M = \begin{pmatrix} -\alpha_2 & \alpha_1 \\ -\alpha_3 & \alpha_2 \end{pmatrix}.$$

Using that B has rank 1 we compute

$$\begin{aligned} \det(M) &= B(e_1, u)B(e_3, u) - B(e_2, u)^2 \\ &= (B(e_1, e_3) - B(e_2, e_2))B(u, u) \\ &= -f'(\varphi)z(g). \end{aligned}$$

The (non-zero) factor $-f'(\varphi)$ cancels when we take the ratio $\det(M)/\det(M_E)$.

Final Remarks

Although the results in Cremona (2001) are not all stated correctly, users of the program `mwrank` Cremona (1990–2006) need not worry about the effect of this on the program's correctness, since the test for quartic equivalence is only carried out there in the case where the resolvent cubic is irreducible (or, in terms of 2-descent on elliptic curves, when the curve has no rational 2-torsion).

A similar study of equivalence of ternary cubics, related to 3-descent on elliptic curves, can be found in Fisher (2006).

References

An, S. Y., Kim, S. Y., Marshall, D. C., Marshall, S. H., McCallum, W. G., Perlis, A. R., 2001. Jacobians of genus one curves. J. Number Theory 90 (2), 304–315.

Cassels, J. W. S., 1991. Lectures on Elliptic Curves. No. 24 in London Mathematical Society Student Texts. Cambridge University Press.

Cremona, J. E., 1990–2006. `mwrank` and related programs for elliptic curves over $\mathbf{Q}$. `http://www.warwick.ac.uk/staff/J.E.Cremona/mwrank/index.html`.

Cremona, J. E., 2001. Classical invariants and 2-descent on elliptic curves. J. Symbolic Comput. 31 (1-2), 71–87, computational algebra and number theory (Milwaukee, WI, 1996).

Cremona, J. E., Fisher, T. A., O'Neil, C., Simon, D., Stoll, M., 2008. Explicit n-descent on elliptic curves. I. Algebra. J. Reine Angew. Math. 615, 121–155.

Fisher, T. A., 2006. Testing equivalence of ternary cubics. In: Hess, F., Pauli, S., M.Pohst (Eds.), Algorithmic Number Theory. No. 4076 in Lecture Notes in Computer Science. Springer-Verlag, pp. 33–345.

O'Neil, C., 2002. The period-index obstruction for elliptic curves. J. Number Theory 95 (2), 329–339.

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

Simon, D., 2002. Computing the rank of elliptic curves over number fields. LMS J. Comput. Math. 5, 7–17 (electronic).