Glasgow Mathematical Journal (2026), 1–14
doi:10.1017/S0017089526101086

Glasgow
Mathematical
Journal

RESEARCH ARTICLE

On the equivalence of binary cubic forms

John Cremona

University of Warwick, UK
Email: j.e.cremona@warwick.ac.uk

Received: 3 December 2025 UTC; **Revised:** 22 June 2026 UTC; **Accepted:** 1 July 2026 UTC

Keywords: Binary cubic forms, Cardano's formula

2020 Mathematics Subject Classification: *Primary* - 11E6; *Secondary* - 12E05

Abstract

We consider the question of determining whether two binary cubic forms over an arbitrary field K whose characteristic is not 2 or 3 are equivalent under the actions of either $\mathrm{GL}(2, K)$ or $\mathrm{SL}(2, K)$, deriving two necessary and sufficient criteria for such equivalence in each case. One of these involves an algebraic invariant of binary cubic forms, which we call the Cardano invariant, as it is closely connected to classical formulas; it also appears in the work of Bhargava *et al.* The second criterion is in terms of the base field itself and also gives explicit matrices in $\mathrm{SL}(2, K)$ or $\mathrm{GL}(2, K)$ transforming one cubic into the other, if any exist, in terms of the coefficients of bilinear factors of a bicovariant of the two cubics. We also consider automorphisms of a single binary cubic form, show how to use our results to test equivalence of binary cubic forms over an integral domain such as $\mathbb{Z}$, and briefly recall some connections between binary cubic forms and the arithmetic of elliptic curves. The methods used are elementary and similar to those used in our work with Fisher concerning equivalences between binary quartic forms.

1. Introduction

We consider binary cubic forms over an arbitrary field K whose characteristic is not 2 or 3 and establish two necessary and sufficient conditions under which two cubics are equivalent under the actions of $\mathrm{GL}(2, K)$ or $\mathrm{SL}(2, K)$, which yield tests that are simple to apply. One of these conditions involves an algebraic invariant of binary cubic forms, which we call the Cardano invariant, as it is closely connected to classical formulas. A more general version of this invariant, involving ideal classes in quadratic rings, appears in the work of Bhargava, Elkies, and Shnidman [2], in the classification of $\mathrm{SL}(2, D)$-orbits of binary cubic forms over a Dedekind domain D: see Theorem 18 and Corollary 20 of [2]. The invariant was first introduced by Bhargava, in the case where the base ring is $\mathbb{Z}$, in [1]; it is defined as an element of the quadratic resolvent algebra associated to the cubic form. Our second result gives a test for equivalence in terms of the base field itself, which also gives explicit matrices transforming one cubic into a second when they are equivalent.

We also consider automorphisms of a single binary cubic form, recovering a result of Xiao in [8], which also follows (for $K = \mathbb{Q}$) from the Delone-Faddeev parametrization, and we show how to use our results to test equivalence of binary cubic forms over an integral domain such as $\mathbb{Z}$. Finally, we make some remarks on how such results relate to the arithmetic of elliptic curves, as in [2].

The methods used here, which are all elementary, are similar to those used in our work [4] with Fisher, concerning equivalences between binary quartic forms. While our first criterion for $\mathrm{SL}(2, K)$-equivalence may be found in the literature, our account is self-contained and more elementary, compares $\mathrm{SL}(2, K)$-equivalence with $\mathrm{GL}(2, K)$-equivalence, and our second criterion has the merit of being purely algebraic, without a need to extend the base field, together with the benefit of giving explicit transformation matrices.

© The Author(s), 2026. Published by Cambridge University Press on behalf of Glasgow Mathematical Journal Trust. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

Over an algebraically closed field $\overline{K}$, all binary cubic forms with nonzero discriminant are $\mathrm{GL}(2,\overline{K})$-equivalent (to $XY(X+Y)$, for example); the issue we address is whether equivalences exist that are defined over the ground field K itself and, if so, to find them explicitly using only arithmetic in K, without having to extend to the splitting field. We also consider the question of $\mathrm{SL}(2,K)$-equivalence.

In order to state our results, we make some definitions. Let $\mathcal{BC}(K)$ denote the set of all binary cubic forms in $K[X,Y]$ with nonzero discriminant and $\mathcal{BC}(K;\Delta)$ to be the subset with discriminant Δ, for each $\Delta \in K^*$. We define the *resolvent algebra* L associated to $\Delta \in K^*$ to be the quadratic étale algebra

$$L = K[\delta] = K[X]/(X^2 + 3\Delta).$$

We define the *twisted action* of $\mathrm{GL}(2,K)$ on $\mathcal{BC}(K)$ as follows: for $g \in \mathcal{BC}(K)$ and $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}(2,K)$, set

$$g^M(X,Y) = \det(M)^{-1} g(rX + tY, sX + uY) = \det(M)^{-1} g(X', Y'),$$

where $(X'\ Y') = (X\ Y)M$. Both the untwisted action (without the determinant factor) and this action appear in the literature: for example, the untwisted action is used in [2] and is also the subject of [6], while the twisted action is used in [3]. Clearly, they are the same for $M \in \mathrm{SL}(2,K)$, and the difference is only minor for our purposes.

In Section 3, we define the *Cardano invariant* $z(g)$ for $g \in \mathcal{BC}(K;\Delta)$ to be an element of L^*/L^{*3} and show that it has the following properties, where, as in [2], we denote the kernel of the induced norm map $\mathrm{N}_{L/K}: L^*/L^{*3} \to K^*/K^{*3}$ by $(L^*/L^{*3})_{N=1}$. We name this group the *Cardano group* for Δ.

Theorem 1. *Let K be any field with $\mathrm{char}(K) \neq 2, 3$. Let $\Delta \in K^*$, let L be the resolvent algebra $K[X]/(X^2+3\Delta)$, and let $z\colon \mathcal{BC}(K;\Delta) \to L^*/L^{*3}$ be the Cardano invariant map.*

(1) $z(g) \in (L^*/L^{*3})_{N=1}$ for all $g \in \mathcal{BC}(K;\Delta)$;
(2) $z(g) = 1$ if and only if g is reducible over K;
(3) $g_1, g_2 \in \mathcal{BC}(K;\Delta)$ are $\mathrm{SL}(2,K)$-equivalent if and only if $z(g_1) = z(g_2)$;
(4) $g_1, g_2 \in \mathcal{BC}(K;\Delta)$ are $\mathrm{GL}(2,K)$-equivalent if and only if $z(g_1) = z(g_2)^{\pm 1}$ (equivalently, if and only if $z(g_1)$ and $z(g_2)$ generate the same subgroup of the Cardano group $(L^*/L^{*3})_{N=1}$);
(5) z induces bijections between the $\mathrm{SL}(2,K)$-orbits on $\mathcal{BC}(K;\Delta)$ and the Cardano group, and between the $\mathrm{GL}(2,K)$-orbits on $\mathcal{BC}(K;\Delta)$ and its cyclic subgroups.

In fact, discriminant-preserving transformations all have determinant ± 1 (see Proposition 7 below); the Cardano invariant is preserved by those with determinant $+1$ and inverted by those of determinant -1.

The analog of part (3) of this theorem for binary cubic forms over $\mathbb{Z}$ follows from Theorem 13 of [1], and the proof there carries over without significant change: our Cardano invariant is denoted δ in [1]; a quadratic ring S (over $\mathbb{Z}$) is fixed, whereas we fix the discriminant $\Delta \in K^*$, and the ideal I of [1] is irrelevant, as our base ring is a field. This assumption enables us to give a simpler proof than in [1].

The last part of the Theorem, for the case of $\mathrm{SL}(2,K)$-orbits, is the same as Corollary 20 of [2].

This theorem implies that the $\mathrm{SL}(2,K)$-orbits on $\mathcal{BC}(K;\Delta)$ carry a group structure, in which the identity is the class of reducible cubics. Testing whether $z(g_1) = z(g_2)$ amounts to testing whether a certain monic cubic over K, constructed from g_1 and g_2, has a root in K. In terms of the group structure, we are testing that the $\mathrm{SL}(2,K)$-orbits of $[g_1]$ and $[g_2]$ are equal by testing whether $[g_1][g_2]^{-1}$ is trivial. For an interpretation of this group in terms of Galois cohomology, see Section 7.

The reason we call $z(g)$ the Cardano invariant is that the classical formula of Cardano for solving cubic equations involves the cube root of an expression in $K(\sqrt{-3\Delta})$, and for monic cubics, this expression is precisely $z(g)$. See Remark 3 below for a precise statement.

Our second result gives conditions for two cubics with the same discriminant to be $\mathrm{SL}(2,K)$- or $\mathrm{GL}(2,K)$-equivalent, which only involve factorization of multivariate polynomials over K and which

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

also provide explicit matrices $M \in \mathrm{GL}(2, K)$ such that $g_1^M = g_2$, when such matrices exist. For brevity, we only state here the result for $\mathrm{SL}(2, K)$; see Proposition 14 and Theorem 15 for the general case.

For two cubic forms g_1, g_2 over K, with cubic covariants G_1, G_2 respectively (whose definition we recall in Section 2), we define the *bicubic bicovariant* $B_{g_1,g_2} \in K[X_1, Y_1, X_2, Y_2]$ to be

$$B_{g_1,g_2}(X_1, Y_1, X_2, Y_2) = g_2(X_2, Y_2)G_1(X_1, Y_1) - G_2(X_2, Y_2)g_1(X_1, Y_1);$$

this is a bihomogeneous form of degree 3 in each pair of variables X_1, Y_1 and X_2, Y_2.

Theorem 2. *Let g_1, g_2 be binary cubic forms over K with $\mathrm{disc}(g_1) = \mathrm{disc}(g_2) \neq 0$ and with bicovariant B_{g_1,g_2}. Then the following are equivalent:*

(1) B_{g_1,g_2} has a bilinear factor in $K[X_1, Y_1, X_2, Y_2]$;
(2) g_1 and g_2 are $\mathrm{SL}(2, K)$-equivalent.

More precisely, B_{g_1,g_2} has the factor $-sX_1X_2 + rX_1Y_2 - uY_1X_2 + tY_1Y_2$ (up to scaling) if and only if $g_1 = g_2^M$, where $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}(2, K)$.

Remark 1. *Over the algebraic closure $\overline{K}$, the bicovariant B_{g_1,g_2} factors as a product of three bilinear factors (i.e., bihomogeneous factors linear in each pair of variables), and there are precisely three matrices $M \in \mathrm{SL}(2, \overline{K})$ with $g_1 = g_2^M$. If M is one of these, then the other two are MT, MT^2 where $T \in \mathrm{SL}(2, \overline{K})$ satisfies $T^3 = I$ and $g_1^T = g_1$. Over K itself, there can be at most one $M \in \mathrm{SL}(2, K)$ satisfying $g_1^M = g_2$, unless Δ is a square in K, when there are three such (if any), related as above.*

Remark 2. *We show in Section 4 below (see Proposition 7) that $g_1, g_2 \in \mathcal{BC}(K;\Delta)$ are $\mathrm{GL}(2, K)$-equivalent if and only if $g_1(X, Y)$ is $\mathrm{SL}(2, K)$-equivalent to $g_2(X, Y)$ or to $g_2(X, -Y)$, the matrix transforming g_1 into g_2 having determinant $+1$ or -1 respectively. Transformations with determinant -1 are associated to bilinear factors of a twisted form of B_{g_1,g_2}; see see Proposition 14.*

In the following section, we recall the definitions of the invariants, seminvariants, and covariants associated with a binary cubic form. In Section 3, we define the Cardano covariant and Cardano invariant and establish their basic properties. In Section 4, we prove both of our main results. In the last three sections, we discuss automorphisms of binary cubic forms, how to extend our results to integral forms, and the connections between binary cubic forms and the arithmetic of elliptic curves.

2. Binary cubics, their invariants, and covariants

Let $\mathcal{BC}(K)$ denote the space of binary cubic forms in $K[X, Y]$ with nonzero discriminant, and for each $\Delta \in K^*$, let $\mathcal{BC}(K;\Delta)$ be the subset of those forms with discriminant Δ. Recall that for $g(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3 \in \mathcal{BC}(K)$, the *discriminant* $\mathrm{disc}(g)$ of g is given by

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd;$$

we also define the seminvariants[1]

$$P = b^2 - 3ac, \qquad \text{and} \qquad U = 2b^3 + 27a^2d - 9abc,$$

which satisfy the syzygy

$$4P^3 = U^2 + 27\Delta a^2.$$

[1] Seminvariants are the leading coefficients of covariants; they are invariant under upper triangular transformations, and include invariants as a special case.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

These are the leading coefficients of two covariant binary forms, the quadratic *Hessian*

$$H(X,Y) = (b^2 - 3ac)X^2 + (bc - 9ad)XY + (c^2 - 3bd)Y^2,$$

which has discriminant -3Δ, and the cubic

$$\begin{aligned} G(X,Y) = {} & (2b^3 + 27a^2d - 9abc)X^3 + 3(b^2c + 9abd - 6ac^2)X^2Y \\ & - 3(bc^2 + 9acd - 6b^2d)XY^2 - (2c^3 + 27ad^2 - 9bcd)Y^3, \end{aligned}$$

which has discriminant $729\Delta^3$; these satisfy the syzygy

$$4H(X,Y)^3 = G(X,Y)^2 + 27\Delta g(X,Y)^2, \tag{1}$$

extending the seminvariant syzygy, which is recovered on setting $(X,Y) = (1,0)$.

We define the *twisted action* of $\mathrm{GL}(2,K)$ on $\mathcal{BC}(K)$ as follows: for $g \in \mathcal{BC}(K)$ and $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}(2,K)$, set

$$g^M(X,Y) = \det(M)^{-1} g(rX + tY, sX + uY) = \det(M)^{-1} g(X', Y'),$$

where $(X'\ Y') = (X\ Y)M$. Both the untwisted action (without the determinant factor) and this action appear in the literature: for example, the untwisted action is used in [2] and is also the subject of [6], while the twisted action is used in [3]. Clearly, they are the same for $M \in \mathrm{SL}(2,K)$, and the difference is only minor for our purposes since we will mostly be concerned with matrices with determinant ± 1 and $-g = g^M$ with $M = -I$.

The discriminant and other covariants of g and g^M are related by[2]

$$\begin{aligned} \Delta(g^M) &= \det(M)^2 \Delta(g); \\ H(g^M) &= H(g)^M; \\ G(g^M) &= \det(M) G(g)^M; \end{aligned}$$

indeed, the definition of covariants is precisely that such identities hold; the invariant Δ is just a covariant of degree 0.

Below we will also need that $g \in \mathcal{BC}(K)$ is coprime to its covariant G, their resultant being $8\Delta^3$.

3. The resolvent algebra and the Cardano invariant

To each $\Delta \in K^*$, we associate the *resolvent algebra*

$$L = K[\delta] = K[T]/(T^2 + 3\Delta),$$

a quadratic étale algebra over K, with a fixed generator δ (the image of T in the quotient) such that $\delta^2 = -3\Delta$; it is a field unless -3Δ is a square in K. We denote by a bar the nontrivial K-automorphism of L, mapping $u + v\delta \mapsto u - v\delta$. Let L^* denote the unit group of L, which consists of the elements with nonzero norm; the norm map $\mathrm{N}_{L/K}: L \to K$ maps $z = u + v\delta \mapsto z\bar{z} = u^2 + 3\Delta v^2$. We extend these to maps $L[X,Y] \to L[X,Y]$ and $L[X,Y] \to K[X,Y]$, and also use the same notation for the induced group homomorphisms $L^*/L^{*3} \to L^*/L^{*3}$ and $L^*/L^{*3} \to K^*/K^{*3}$.

For $M \in \mathrm{GL}(2,K)$ and $g \in \mathcal{BC}(K)$, since $\Delta(g^M) = \det(M)^2\Delta(g)$, the resolvent algebras of g and g^M are isomorphic via $\delta \mapsto \det(M)\delta$. Transforms that preserve the discriminant, therefore, have determinant ± 1; however, we regard δ as a fixed generator of L, associated to Δ, which is the same for all cubics in $\mathcal{BC}(K;\Delta)$.

[2] The action on the binary quadratic form $H(g)$ is untwisted: $H(g)^M(X,Y) = H(g)(X',Y')$. The untwisted action on cubics gives a factor of $\det(M)^k$ on the right with $k = 6, 2, 3$ respectively.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

Definition 1. *The* Cardano covariant $C(X, Y)$ *of* $g \in \mathcal{BC}(K;\Delta)$ *is*

$$C(X, Y) = \frac{1}{2}(G(X, Y) + 3\delta g(X, Y)) \in L[X, Y].$$

Classically, this is called an "irrational" or algebraic covariant because its coefficients lie in the extension L rather than in K itself. It is a covariant for the action of $\mathrm{SL}(2, K)$; in general, we have

$$C(g^M) = \frac{1}{2}(\det(M)G + 3\delta g)^M; \tag{2}$$

this would be equal to $\det(M)C(g)^M$ if the value of δ for discriminant $\det(M)^2\Delta$ were fixed to be $\det(M)\delta$, but it is not possible to do this consistently for transformations with both determinants $\pm\det(M)$.

At first, we will restrict our attention to the action of $\mathrm{SL}(2, K)$.

In terms of C, the covariant syzygy may be simply written

$$\mathrm{N}_{L/K}(C) = C\overline{C} = H^3.$$

Hence, for all $x, y \in K$, not both 0, except for those satisfying $H(x, y) = 0$ (which only exist when -3Δ is a square in K), the value $C(x, y)$ lies in L^* and satisfies $\mathrm{N}_{L/K}(C(x, y)) = H(x, y)^3$ with $H(x, y) \in K^*$.

We will define the Cardano invariant in terms of values of the Cardano covariant. Before we give the general definition, first consider cubics with $P = H(1, 0) \neq 0$. Set $z = C(1, 0) = \frac{1}{2}(U + 3a\delta)$; then $\mathrm{N}_{L/K}(z) = P^3 \in K^{*3}$, so $z \in L^*$, and a provisional definition of the Cardano invariant of g with $P \neq 0$ is simply this quantity z. One can show (see Proposition 5 below) that $z \in L^{*3}$ if and only if g has a linear factor in $K[X, Y]$ and that for two cubics g_1, g_2 with the same discriminant Δ and hence the same resolvent algebra, they are $\mathrm{SL}(2, K)$-equivalent if and only if their z-invariants are equal modulo L^{*3}. Instead, however, we proceed as follows, leading to a general definition of the Cardano invariant $z(g)$ as a well-defined element of L^*/L^{*3} for all $g \in \mathcal{BC}(K;\Delta)$.

Observe that C, whose norm H^3 is a cube in $K[X, Y]$, is itself the cube of a linear form in $L[X, Y]$, up to a constant factor. Explicitly, we have

$$27c_0^2C(X, Y) = (3c_0X + c_1Y)^3,$$

where $C(X, Y) = c_0X^3 + c_1X^2Y + c_2XY^2 + c_3Y^3$, so $c_0 = z$ (as defined above) and $c_1 = \frac{3}{2}(b^2c - 6ac^2 + 9abd + b\delta)$. (This algebraic identity may be readily checked directly or derived by writing C as a constant times the cube of a linear form and differentiating twice.) This already shows that if $P \neq 0$, so that $c_0 \in L^*$, then for every $x, y \in K$ such that $H(x, y) \neq 0$, we have $C(x, y) \in L^*$ and $C(x, y) \equiv c_0 \mod L^{*3}$. For the general case, we use the following identity:

Proposition 3. *The identity*

$$C(X_1, Y_1)^2C(X_2, Y_2) = F(X_1, Y_1, X_2, Y_2)^3$$

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

$$3F(X_1, Y_1, X_2, Y_2) = (3c_0X_1^2 + 2c_1X_1Y_1 + c_2Y_1^2)X_2 + (c_1X_1^2 + 2c_2X_1Y_1 + 3c_3Y_1^2)Y_2.$$

Proof. This identity reduces to the previous one on specializing $(X_1, Y_1) = (1, 0)$ and may be checked using computer algebra. □

Also, $\mathrm{N}_{L/K}F(X_1, Y_1, X_2, Y_2) = H(X_1, Y_1)^2H(X_2, Y_2)$ and $C(X, Y) = F(X, Y, X, Y)$.

Corollary 4. *The value of* $C(x, y) \in L^*/L^{*3}$ *is independent of* $(x, y) \in K \times K$, *provided that* $H(x, y) \neq 0$, *so that* $C(x, y)$ *is a unit.*

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

Proof. By the proposition, for x_1, y_1, x_2, y_2 such that $H(x_1, y_1), H(x_2, y_2) \neq 0$, we have $C(x_1, y_1)$, $C(x_2, y_2) \in L^*$ and, modulo L^{*3}, we have

$$C(x_1, y_1)^{-1}C(x_2, y_2) \equiv C(x_1, y_1)^2 C(x_2, y_2) \equiv F(x_1, y_1, x_2, y_2)^3 \equiv 1. \qquad \square$$

Hence, we may define the *Cardano invariant* $z(g)$ of $g \in \mathcal{BC}(K;\Delta)$ as an element of L^*/L^{*3}, by setting

$$z(g) = C(x, y) \in L^*/L^{*3},$$

for any choice of $x, y \in K$ such that $C(x, y)$ is a unit. This is well-defined by the corollary, and if $P = H(1, 0) \neq 0$, then we may take $z(g) = C(1, 0) = z$ (modulo cubes), as above. In all cases we have, modulo K^{*3},

$$\mathrm{N}_{L/K}(z(g)) \equiv \mathrm{N}_{L/K}(C(x, y)) \equiv H(x, y)^3 \equiv 1,$$

so that $z(g) \in (L^*/L^{*3})_{N=1} := \ker(\mathrm{N}_{L/K} : L^*/L^{*3} \to K^*/K^{*3})$, the *Cardano group*. This establishes the first part of Theorem 1. The second part is the following:

Proposition 5. *$g \in \mathcal{BC}(K)$ has a linear factor in $K[X, Y]$ if and only if $z(g) = 1$.*

Proof. Writing $g = aX^3 + bX^2Y + cXY^2 + dY^3$, we first observe that when $a = 0$ we have $P = b^2 \neq 0$ (as otherwise $\Delta = 0$), so $z(g) = z = U/2 = b^3 \in K^{*3}$, and g has the factor Y.

Now assume that $a \neq 0$. The equations $z = \frac{1}{2}(U + 3a\delta) = (x + y\delta)^3$, together with[3] $\mathrm{N}_{L/K}(x + y\delta) = P$, have a solution $x, y \in K$ if and only if

$$f(x) = 0 \quad \text{and} \quad y = 9a/f'(x),$$

where $f(X) = 8X^3 - 6PX - U = a^{-1}g(2X + b, -3a)$. Hence, a solution $x, y \in K$ exists if and only if g has a linear factor (with $(2x + b)/(-3a)$ a root of $g(X, 1)$), noting that x cannot be a double root of f since $\Delta \neq 0$, so $f'(x) \neq 0$. $\square$

A special case of Theorem 8 below, combined with Proposition 5, is that all cubics with the same discriminant that have linear factors over K are $\mathrm{SL}(2, K)$-equivalent; this is also implied by the following.

Proposition 6. *Suppose that $g \in \mathcal{BC}(K;\Delta)$ has a linear factor in $K[X, Y]$. Then g is $\mathrm{SL}(2, K)$-equivalent to $Y(X^2 - \frac{1}{4}\Delta Y^2)$.*

Proof. Let the linear factor be $rX + sY$ with $r, s \in K$, not both zero. Let $M = \begin{pmatrix} s & -r \\ 0 & s^{-1} \end{pmatrix}$ if $s \neq 0$ and $M = \begin{pmatrix} s & -r \\ r^{-1} & 0 \end{pmatrix}$ otherwise; then $\det(M) = 1$ and g^M has the linear factor $(rX + sY)^M = Y$. Transforming g by M gives a cubic with coefficients $(0, b, c, d)$ where $b \neq 0$. Transforming again by $\mathrm{diag}(b^{-1}, b)$ gives coefficients $(0, 1, c', d')$, and then by $\begin{pmatrix} 1 & 0 \\ -c'/2 & 1 \end{pmatrix}$ gives coefficients $(0, 1, 0, d'')$. Comparing discriminants, which do not change under unimodular transformations, we see that $\Delta = -4d''$ as required. $\square$

Remark 3. *Cardano's formula for the roots of the cubic expresses them in terms of the cube root of a quantity in $L = K(\sqrt{-3\Delta})$. From the previous proof we see that, when $P \neq 0$, the roots of $g(X, 1)$ are given by*

$$x = -(b + \sqrt[3]{z} + P/\sqrt[3]{z})/3a,$$

[3] If K contains cube roots of unity, we may scale x and y by a cube root of unity if necessary, so that $\mathrm{N}_{L/K}(x + y\delta) = P$ exactly.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

where $z=(U+3a\sqrt{-3\Delta})/2$. *This is essentially Cardano's formula. If* $w=\sqrt[3]{z}\in L$ *with* $w\overline{w}=\sqrt[3]{\mathrm{N}_{L/K}(z)}=P$ *then we have* $x=-(b+w+\overline{w})/(3a)\in K$. *All three roots are in* K *when* $\sqrt{-3}\notin K$ *but* $\sqrt{-3}\in L$, *so* $L=K(\sqrt{-3})$ *and* $\Delta\in(K^*)^2$, *for then* L *contains a primitive roots of unity* ζ_3 *and* $\overline{\zeta_3}=\zeta_3^2$, *so that replacing* w *by* $\zeta_3 w$ *or* $\zeta_3^2 w$ *in the formula again gives an element of* K.

Remark 4. *If* $-3\Delta\in(K^*)^2$, *so that* $L\cong K\oplus K$, *the Cardano group* $(L^*/L^{*3})_{N=1}$ *is isomorphic to* K^*/K^{*3}.

Remark 5. *The formulas given here may be used to parametrize all cubic extensions of* K *as follows. (This construction may also be obtained from the Delone-Faddeev parametrization of cubic orders by binary cubic forms in [5], replacing their base ring* $\mathbb{Z}$ *by a field.) Each such extension* $M=K(\alpha)$ *has a discriminant* $\Delta\in K^*$, *well-defined modulo squares as the discriminant of the irreducible cubic minimal polynomial of* α *in* $K[X]$, *and* $\Delta=1$ *(modulo squares) if and only if the extension* M/K *is Galois. To each* $\Delta\in K^*$, *we form the cubic algebra* $L=K[T]/(T^2+3\Delta)$ *as above; then the cubics with discriminant* Δ *(modulo squares) are parametrized by the subgroups of the Cardano group* $(L^*/L^{*3})_{N=1}$. *Explicitly, for* $z\in(L^*/L^{*3})_{N=1}$ *with* $\mathrm{N}_{L/K}(z)=P^3$ *and* $\mathrm{Tr}_{L/K}(z)=U$, *the associated cubic is* $f_z(X)=X^3-3PX-U$. *(Note that* $\bar{z}$ *has the same trace and norm as* z, *and hence* $f_{\bar{z}}=f_z$, *in accordance with the fact that* $z\bar{z}=P^3$, *so that* $\bar{z}$ *generates the same subgroup of the Cardano group as* z.*) The root(s) of* $f_z(X)$ *are* $\alpha=w+P/w$ *where* $w^3=z$.

A refinement of this construction may be used when K *is a number field and* S *a finite set of primes of* K, *to determine all cubic extensions of* K *which are unramified outside* S. *For simplicity, we assume that* 6 *is an* S*-unit; otherwise, the cubic extensions constructed may be ramified at primes dividing* 6, *which are not in* S. *Recall that for an integer* $m\geq 2$ *the subgroup*

$$K(S,m)=\{x\in K^*/(K^*)^m \mid \mathrm{ord}_{\mathfrak{p}}(x)\equiv 0 \pmod m\ \forall \mathfrak{p}\notin S\}$$

of $K^*/(K^*)^m$ *is finite and may be computed in terms of the class group and unit group of* K. *First, we determine the possible quadratic subfields* $K(\sqrt{\Delta})$ *of the normal closure of the cubic, which must also be unramified outside* S, *by restricting* Δ *to lie in* $K(S,2)$. *For each such* Δ, *we also have that* $K(\sqrt{-3\Delta})/K$ *is unramified outside* S; *we then restrict* z *to the subgroup* $\ker(\mathrm{N}_{L/K}: L(S,3)\to K(S,3))$ *in the construction of the preceding paragraph.*

4. Equivalence of binary cubics

In this section, we consider necessary and sufficient conditions for two binary cubic forms over K with the same discriminant Δ to be $\mathrm{GL}(2,K)$-equivalent. We first observe that we need only consider transformations with determinant ± 1 and reduce the problem to testing $\mathrm{SL}(2,K)$-equivalence.

Proposition 7. *Let* $\Delta\in K^*$ *and* $g_1, g_2\in\mathcal{BC}(K;\Delta)$.

(1) If $g_1=g_2^M$ *with* $M\in\mathrm{GL}(2,K)$, *then* $\det(M)=\pm 1$.
(2) g_2 *is* $\mathrm{GL}(2,K)$*-equivalent to* g_1 *if and only if it is* $\mathrm{SL}(2,K)$*-equivalent to either* $g_1(X,Y)$ *or* $g_1(X,-Y)$.

Proof. If $g_1=g_2^M$ with $\mu=\det(M)\in K^*$, then $\mathrm{disc}(g_1)=\mu^2\mathrm{disc}(g_2)$, so $\mu^2=1$.

For the second part, it suffices to see that $g_1(X,-Y)=g_1(X,Y)^M$ where $M=\mathrm{diag}(-1,1)$ has determinant -1. □

For $i=1,2$, denote the coefficients of $g_i\in\mathcal{BC}(K;\Delta)$ by a_i,b_i,c_i,d_i, their seminvariants by P_i,U_i, and their Cardano covariants and invariants by C_i,z_i. Since $\mathrm{disc}(g_1)=\mathrm{disc}(g_2)=\Delta$, they have the same covariant algebra $L=K[\delta]$ where $\delta^2=-3\Delta$.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

We will give two criteria for the equivalence of a pair of binary cubic forms with the same discriminant: one in terms of their Cardano invariants and a second one in terms of a cubic bicovariant; the latter will also directly give a matrix (or matrices) $M \in \mathrm{SL}(2,K)$ transforming one to the other. Both criteria are similar to criteria (established in [4]) for the equivalence of a pair of binary quartic forms with the same invariants.

4.1. Cubic equivalence in terms of equality of Cardano invariants

We restate parts (3) and (4) of Theorem 1.

Theorem 8. *Let $g_1, g_2 \in \mathcal{BC}(K;\Delta)$, with common resolvent algebra $L = K[\delta]$. Then*

(1) $g_2 = g_1^M$ with $\det(M) = +1$ if and only if $z(g_1) = z(g_2)$ in L^*/L^{*3};
(2) $g_2 = g_1^M$ with $\det(M) = -1$ if and only if $z(g_1) = z(g_2)^{-1}$ in L^*/L^{*3}.

Hence g_1 and g_2 are $\mathrm{GL}(2,K)$-equivalent if and only if $z(g_1)$ and $z(g_2)$ generate the same subgroup of L^*/L^{*3}.

Proof. (1) Suppose that $g_2 = g_1^M$ with $M \in \mathrm{SL}(2,K)$. Then $g_2(X_2, Y_2) = g_1(X_1, Y_1)$, where $(X_1\ Y_1) = (X_2\ Y_2)M$, and by the covariant property of C_1 we have that

$$C_2(X_2, Y_2) = C_1^M(X_2, Y_2) = C_1(X_1, Y_1).$$

It is now clear that the unit values taken by C_1 and C_2 are the same. Explicitly, we similarly have $H_2(X_2, Y_2) = H_1^M(X_2, Y_2) = H_1(X_1, Y_1)$; let $x_2, y_2 \in K$ be such that $H_2(x_2, y_2) \neq 0$, and set $(x_1\ y_1) = (x_2\ y_2)M$, so then also $H_1(x_1, y_1) = H_2(x_2, y_2) \neq 0$. (This will be true for all choices of $(x_2, y_2) \neq (0,0)$ when -3Δ is not a square, and for all but at most two choices, up to scaling, when -3Δ is a square in K.) Then $C_1(x_1, y_1) = C_2(x_2, y_2) \in L^*$, and so $z(g_1) = z(g_2)$.

For the converse, suppose that $z(g_1) = z(g_2)$. If $z(g_1) = z(g_2) = 1$, then by Proposition 5, both cubics have linear factors, and then Proposition 6 shows that both are $\mathrm{SL}(2,K)$-equivalent to $Y(X^2 - \frac{1}{4}\Delta Y^2)$, and hence to each other.

Now we may assume that neither cubic has a linear factor; in particular, $a_1, a_2 \neq 0$. Then also $U_1, U_2 \neq 0$, since otherwise $g_1(-b_1, 3a_1) = a_1 U_1 = 0$ and $g_1(X, Y)$ would be divisible by $3a_1X + b_1Y$; similarly for g_2. By taking suitable $\mathrm{SL}(2,K)$-transforms of g_1 and g_2 if necessary, we can assume that $P_1, P_2 \neq 0$ also. Then we may take as representatives of the Cardano covariants the elements $z_i = (U_i + 3\delta a_i)/2 \in L^*$ for $i = 1, 2$, with $\mathrm{N}_{L/K}(z_i) = P_i^3$.

Since $z_i\overline{z_i} = \mathrm{N}_{L/K}(z_i) = P_i^3$, the condition that $z_2/z_1 \in L^{*3}$ is equivalent to $\overline{z_1}z_2 \in L^{*3}$. A computation similar to that in the proof of Proposition 5 shows that $\overline{z_1}z_2 = (x + y\delta)^3$ with $\mathrm{N}_{L/K}(x + y\delta) = P_1P_2$ implies that x is a root of $f(X)$, where

$$f(X) = 16X^3 - 12P_1P_2X - (U_1U_2 + 27a_1a_2\Delta).$$

We now reduce to the case $a_2U_1 - a_1U_2 = 0$. If this does not hold, set $B(X, Y) = U_1 g_2(X, Y) - a_1 G_2(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3$, where $a = a_2U_1 - a_1U_2 \neq 0$. One may check that $B(4P_1X + b, -3a) = 4aP_1^3 f(X)$. Hence, since $z(g_1) = z(g_2)$ implies that $f(X)$ has a root in K, it follows that B has a linear factor over K. After an $\mathrm{SL}(2,K)$-transformation of g_2, we can take this linear factor to Y, so that $a_2U_1 - a_1U_2 = 0$. This transform does not change P_1, so we still have $P_1 \neq 0$.

Assuming that $a_2U_1 - a_1U_2 = 0$, let $\lambda = a_2/a_1 = U_2/U_1 \in K^*$. The seminvariant syzygy then gives $P_2^3 = \lambda^2 P_1^3$. Since $P_1 \neq 0$, then also $P_2 \neq 0$, and we may set $\mu = \lambda P_1/P_2$, so that $\lambda = \mu^3$ and $P_2/P_1 = \mu^2$. Let $g_3(X, Y) = g_1(\mu X, \mu^{-1}Y)$, the transform of g_1 by $\mathrm{diag}(\mu, \mu^{-1}) \in \mathrm{SL}(2,K)$; then the seminvariants a_3, P_3, U_3 of g_3 are the same as those of g_2, and we may check that $g_2 = g_3^M$ with $M = \begin{pmatrix} 1 & 0 \\ (b_2 - b_3)/3a_3 & 1 \end{pmatrix} \in \mathrm{SL}(2,K)$. Hence g_1 and g_2 are $\mathrm{SL}_2(K)$-equivalent.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

(2) Every $M \in \mathrm{GL}(2,K)$ with $\det(M) = -1$ can be written as $M = DM_1$, where $M_1 \in \mathrm{SL}(2,K)$ and $D = \mathrm{diag}(-1,1)$. By part (1), it suffices (for both implications) to show that $z(\tilde{g}) = z(g_1)^{-1}$, where $\tilde{g} = g_1^D$. We have $\tilde{g}(X,Y) = g_1(X,-Y)$, which has covariants $\tilde{H}(X,Y) = H_1(X,-Y)$ and $\tilde{G}(X,Y) = -G_1(X,-Y)$, so its Cardano covariant $\tilde{C}$ satisfies

$$\tilde{C}(X,-Y) = -\overline{C_1}(X,Y),$$

from which the syzygy implies

$$C_1(X,Y)\tilde{C}(X,-Y) = (-H_1(X,Y))^3.$$

Hence $z(\tilde{g}) = z(g_1)^{-1}$ as required.

The last part is now clear, using Proposition 7(1). □

One consequence of this result, combined with Proposition 5, is that two irreducible cubics cannot be equivalent via matrices of both determinants, $+1$ and -1; equivalently, only reducible cubics can have automorphisms with determinant -1. We will return to automorphisms in Section 5.

From the preceding proof, we may extract the following criterion for $\mathrm{SL}(2,K)$-equivalence for cubic forms with no linear factor, complementing Proposition 6 in the reducible case.

Corollary 9. *Let $g_1, g_2 \in \mathcal{BC}(K;\Delta)$ be irreducible. Then $g_2 = g_1^M$ with $M \in \mathrm{SL}(2,K)$ if and only if the polynomial $f(X) = 16X^3 - 12P_1P_2X - (U_1U_2 + 27a_1a_2\Delta)$ has a root in K.*

To complete the proof of Theorem 1, we only need to show that the Cardano invariant map is surjective.

Proposition 10. *Every $z \in (L^*/L^{*3})_{N=1}$ arises as $z(g)$ for some $g \in \mathcal{BC}(K;\Delta)$.*

Proof. Let $z = x + y\delta \in L^*$ be such that $\mathrm{N}_{L/K}(z) = x^2 + 3\Delta y^2 = P^3$ with $P \in K^*$. Let $g \in \mathcal{BC}(K)$ have coefficients $(2y/3, 0, -P/2y, x/6y^2)$ if $y \neq 0$ or $(0, x/P, 0, -\Delta/4x)$ if $y = 0$. In each case, one may check that $\mathrm{disc}(g) = \Delta$ and that $U(g) = 2x$ and $P(g) = P$, so that $z(g) = z$ as required. □

4.2. Cubic equivalence in terms of factors of a cubic bicovariant

In the proof of Theorem 8, we saw two conditions equivalent to the $\mathrm{SL}(2,K)$-equivalence of the cubics g_1 and g_2: that a monic cubic (denoted $f(X)$ in the proof) had a root in K, or that a third cubic form $B(X,Y)$ had a linear factor over K. However, we only established these conditions under certain extra conditions, such as the irreducibility of the g_i. The cubic form $B(X,Y)$ used in the proof is the specialization at $(X_1,Y_1,X_2,Y_2) = (1,0,X,Y)$ of $g_2(X_2,Y_2)G_1(X_1,Y_1) - G_2(X_2,Y_2)g_1(X_1,Y_1)$. We now show how linear factors of this "bicovariant" directly give matrices $M \in \mathrm{SL}(2,K)$ such that $g_1 = g_2^M$ (of which there are at most three), in all cases. A twist of this bicovariant similarly produces matrices (again, at most three) of determinant -1 transforming g_1 into g_2.

We continue to use the earlier notation, where $g_1, g_2 \in \mathcal{BC}(K;\Delta)$ have covariants H_i and G_i. To the pair (g_1,g_2) we associate a *bicovariant* in $K[X_1,Y_1,X_2,Y_2]$:

$$B_{g_1,g_2}(X_1,Y_1,X_2,Y_2) = g_2(X_2,Y_2)G_1(X_1,Y_1) - G_2(X_2,Y_2)g_1(X_1,Y_1).$$

This is a bihomogeneous polynomial of bidegree $(3,3)$; that is, it is homogeneous of degree 3 in each pair of variables separately. It is also a bicovariant with respect to $\mathrm{SL}(2,K) \times \mathrm{SL}(2,K)$, meaning that, for $M_1, M_2 \in \mathrm{SL}(2,K)$, we have

$$\begin{aligned} B_{g_1^{M_1},g_2^{M_2}}(X_1,Y_1,X_2,Y_2) &= B_{g_1,g_2}(X_1,Y_1,X_2,Y_2)^{(M_1,M_2)} \\ &= B_{g_1,g_2}(X_1',Y_1',X_2',Y_2') \end{aligned}$$

where $(X_i'\ Y_i') = (X_i\ Y_i)M_i$ for $i = 1,2$.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

Lemma 11. *B_{g_1,g_2} is divisible by $X_1Y_2 - X_2Y_1$ if and only if $g_2 = \pm g_1$.*

Proof. Clearly, $B_{g,g}$ is divisible by $X_1Y_2 - X_2Y_1$, and so is $B_{g,-g} = -B_{g,g}$.

Conversely, if B_{g_1,g_2} is divisible by $X_1Y_2 - X_2Y_1$ then $B_{g_1,g_2}(X, Y, X, Y) = 0$, so $g_2(X, Y)G_1(X, Y) = g_1(X, Y)G_2(X, Y)$. By the coprimality of g_i and G_i for $i = 1, 2$, this implies that $g_2 = \lambda g_1$ and $G_2 = \lambda G_1$ for some $\lambda \in K^*$; but the first of these equations implies (using covariance of the G_i) that $G_2 = \lambda^3 G_1$; so $\lambda^2 = 1$. □

We now consider bilinear factors of B_{g_1,g_2}: factors of degree $(1, 1)$, of the form

$$L_M = (X_1\ Y_1)M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} X_2 \\ Y_2 \end{pmatrix} = -sX_1X_2 + rX_1Y_2 - uY_1X_2 + tY_1Y_2,$$

where $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ is a nonzero matrix. The previous lemma concerned the factor L_I associated with the identity matrix I.

Lemma 12. *L_M is irreducible if and only if* $\det(M) \neq 0$.

Proof. $(aX_1 + bY_1)(cX_2 + dY_2) = L_M$ with $M = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} d & -c \end{pmatrix}$, so M has rank 1 if and only if L_M is reducible. □

Lemma 13. *If L_M divides B_{g_1,g_2} for $g_1, g_2 \in \mathcal{BC}(K;\Delta)$, then* $\det(M) \in K^{*2}$ *and* $g_2^M = \pm \det(M)^{1/2} g_1$.

Proof. Suppose that L_M divides B_{g_1,g_2}. If $\det(M) = 0$, then by the previous lemma, B_{g_1,g_2} is divisible by $(aX_1 + bY_1)$ for some $a, b \in K$ not both zero. Then we have $B_{g_1,g_2}(b, -a, X_2, Y_2) = 0$ identically, so $g_2(X_2, Y_2)G_1(b, -a) = G_2(X_2, Y_2)g_1(b, -a)$. Since g_1 and G_1 are coprime, $g_1(b, -a)$ and $G_1(b, -a)$ are not both zero, so this equation contradicts the coprimality of g_2 and G_2.

Let $\mu = \det(M)$. Working over $\overline{K}$, we have $M = \mu^{1/2} M_1$ with $M_1 \in \mathrm{SL}(2, \overline{K})$. Then $L_M = \mu^{1/2} L_{M_1}$, so B_{g_1,g_2} is also divisible (over $\overline{K}$) by L_{M_1}. Hence, $B_{g_1^{M_1^{-1}},g_2} = B_{g_1,g_2}^{M_1^{-1},I}$ is divisible by $L_{M_1}^{M_1^{-1},I} = L_I = X_1Y_2 - X_2Y_1$ (over $\overline{K}$), so $g_1 = \pm g_2^{M_1}$ by Lemma 11. Hence, $g_2^M = \pm \mu^{1/2} g_1$, which implies that $\mu^{1/2} \in K^*$. □

Proposition 14. *For $g_1, g_2 \in \mathcal{BC}(K;\Delta)$:*

(1) Every bilinear factor of $B_{g_1,g_2}(X_1, Y_1, X_2, Y_2)$ in $K[X_1, Y_1, X_2, Y_2]$ is (up to scaling) of the form L_M with $M \in \mathrm{SL}(2, K)$ satisfying $g_1 = g_2^M$.

(2) Every bilinear factor of

$$g_2(X_2, Y_2)G_1(X_1, Y_1) + G_2(X_2, Y_2)g_1(X_1, Y_1).$$

in $K[X_1, Y_1, X_2, Y_2]$ is (up to scaling) of the form $sX_1X_2 + rX_1Y_2 - uY_1X_2 - tY_1Y_2$, where $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ satisfies $g_1 = g_2^M$ and $\det(M) = -1$.

(3) There are at most six $M \in \mathrm{GL}(2, K)$ such that $g_1 = g_2^M$, one for each bilinear factor in $K[X_1, Y_1, X_2, Y_2]$ of

$$g_2(X_2, Y_2)^2 G_1(X_1, Y_1)^2 - G_2(X_2, Y_2)^2 g_1(X_1, Y_1)^2$$

(which is equal to $g_2(X_2, Y_2)^2 H_1(X_1, Y_1)^3 - H_2(X_2, Y_2)^3 g_1(X_1, Y_1)^2$).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

Proof. (1) By the lemma, we may scale each linear factor L_M so that $\det(M) = 1$.

(2) Replace $g_1(X_1, Y_1)$ by $g_1(X_1, -Y_1)$ and $G_1(X_1, Y_1)$ by $G_1(X_1, -Y_1)$, which is minus the cubic covariant of $g_1(X_1, -Y_1)$, and apply (1).

(3) Immediate from (1) and (2); for the second expression, apply the covariant syzygy. □

All that remains to establish Theorem 2 is to check that every transform from g_2 to g_1 arises from bilinear factors in this way.

Theorem 15. *Let $g_1, g_2 \in \mathcal{BC}(K;\Delta)$. Then g_1 and g_2 are $\mathrm{SL}(2,K)$-equivalent if and only if B_{g_1,g_2} has a bilinear factor in $K[X_1, Y_1, X_2, Y_2]$, and every bilinear factor of B_{g_1,g_2} has the form L_M with $M \in \mathrm{SL}(2,K)$, where $g_1 = g_2^M$.*

Proof. If $g_1 = g_2^M$ with $M \in \mathrm{SL}(2,K)$ then $B_{g_1,g_2} = B_{g_2,g_2}^{M,I}$, which is divisible by $(X_1Y_1 - X_2Y_1)^{M,I} = L_M$. The converse is Corollary 13. □

Remark 6. *It follows from Theorem 15 and Proposition 14 that the number of matrices $M \in \mathrm{GL}(2,K)$ with $g_1 = g_2^M$ is at most six, with at most three with each determinant ± 1. This number, if nonzero, is also the number of automorphisms in $\mathrm{GL}(2,K)$ of g_1 (or of g_2); in the next section, we study automorphisms in more detail and will see that the number of automorphisms in $\mathrm{SL}(2,K)$ is either 1 or 3, the latter occurring if and only if $\Delta \in K^{*2}$; hence B_{g_1,g_2} splits completely into bilinear factors if and only if g_1, g_2 are $\mathrm{SL}(2,K)$-equivalent and $\Delta \in K^{*2}$.*

5. Automorphisms of cubic forms

For $g \in \mathcal{BC}(K)$, the automorphism group of g is the subgroup $\mathcal{A}(g)$ of matrices $M \in \mathrm{GL}(2,K)$ such that $g^M = g$. Since for $M = \lambda I$, we have $g^M = \lambda g$, and the only[4] scalar matrix in $\mathcal{A}(g)$ is the identity. By Proposition 7, every $M \in \mathcal{A}(g)$ satisfies $\det(M) = \pm 1$.

Each $M \in \mathcal{A}(g)$ acts on the roots of g, viewed as lying in $\mathbb{P}^1(\overline{K})$, by linear fractional transformations. Since $\mathrm{PGL}(2,\overline{K})$ acts faithfully and transitively on ordered triples of distinct points on the projective line, the action on the roots induces an injective homomorphism $\mathcal{A}(g) \longrightarrow S_3$. Hence, $\mathcal{A}(g)$ has order at most 6. Set $\mathcal{A}_1(g) = \mathcal{A}(g) \cap \mathrm{SL}(2,K)$. Proposition 16 below implies that the above homomorphism restricts to an injection of $\mathcal{A}_1(g)$ into the alternating group A_3, so $\mathcal{A}_1(g)$ is either trivial or has order 3.

Also, since an automorphism M has finite order, it has distinct eigenvalues either both in K or in a quadratic extension, so M has exactly two fixed points in $\mathbb{P}^1(\overline{K})$.

We now determine when g has automorphisms of order 2 and 3, respectively.

Proposition 16. *$g \in \mathcal{BC}(K)$ has an automorphism M of order 2 if and only if g has a root in $\mathbb{P}^1(K)$; then $\det(M) = -1$ and M fixes the root.*

Proof. If M is an automorphism of g of order 2, then M fixes exactly one root of g. Moreover, $M^2 = I$ but $M \neq \pm I$, so the characteristic polynomial of M is $X^2 - 1$; hence $\det(M) = -1$, and the two eigenvalues ± 1 of M lie in K. This implies that the two fixed points of M in $\mathbb{P}^1(\overline{K})$ are K-rational; the root of g which is fixed by M is one of these, so is K-rational.

Conversely, if g has a K-rational root, then without loss of generality (by Proposition 6), $g = Y(X^2 - \frac{1}{4}\mathrm{disc}(g)Y^2)$, which has the automorphism $M = \mathrm{diag}(1,-1)$ of order 2. □

[4] Under the untwisted action of $\mathrm{GL}(2,K)$, transforming by ζI where ζ is a cube root of unity is also clearly trivial, and the maximum number of possible automorphisms over fields containing all cube roots of unity is 18.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

Proposition 17. *$g \in \mathcal{BC}(K;\Delta)$ has an automorphism M of order 3 if and only if $\Delta \in K^{*2}$; then* $\det(M) = +1$ *and M acts as a 3-cycle on the roots of g.*

Proof. Let M be an automorphism of g of order 3. Then M acts as a 3-cycle on the roots α, β, γ of g in $\mathbb{P}^1(\overline{K})$, and the characteristic polynomial of M is $X^2 + X + 1$, so $\det(M) = +1$. Label the roots so that $M(\alpha) = \beta$, $M(\beta) = \gamma$, and $M(\gamma) = \alpha$. Since the entries of M are in K this implies that $K(\alpha) = K(\beta) = K(\gamma)$. By the Galois theory of cubics, it follows that $\mathrm{disc}(g) \in K^{*2}$; the splitting field of g is either K itself, or a cyclic extension of K.

Conversely, suppose that $\mathrm{disc}(g) \in K^{*2}$; there is a unique element of $\mathrm{PGL}(2, \overline{K})$, which maps $\alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$; by symmetry, since every polynomial expression in α, β, γ which is fixed by cyclic permutations lies in K, this element actually lies in $\mathrm{PGL}(2, K)$. By a similar argument to that used in Lemma 13, any lift to $\mathrm{GL}(2, K)$ has a square determinant, so there is a lift to $M \in \mathrm{SL}(2, K)$ such that $g^M = g$, and M^3 acts trivially on the roots, so $M^3 = I$. □

Putting these parts together, we see that the automorphism group of a binary cubic form g depends only on the Galois group of the splitting field of g.

Theorem 18. *Let g be a binary cubic form defined over the field K, with $\Delta \in K^*$.*

(1) The group $\mathcal{A}_1(g)$ of $\mathrm{SL}(2, K)$*-automorphisms of g is trivial unless Δ is a square, in which case it is cyclic of order* 3.

(2) The group $\mathcal{A}(g)$ of $\mathrm{GL}(2, K)$*-automorphisms of g modulo scalars is isomorphic to a subgroup of the symmetric group S_3, namely the centralizer in S_3 of the Galois group of g. Specifically:*

- *$\mathcal{A}(g)$ is trivial if and only if if g is irreducible over K and $\Delta \notin K^{*2}$;*
- *$\mathcal{A}(g) \cong C_3$ if and only if g is irreducible over K and $\Delta \in K^{*2}$;*
- *$\mathcal{A}(g) \cong C_2$ if and only if g is reducible over K and $\Delta \notin K^{*2}$ (so that g has exactly one root over K);*
- *$\mathcal{A}(g) \cong S_3$ if and only if g is reducible over K and $\Delta \in K^{*2}$ (so that g splits completely over K).*

Part (2) of this result is the same as Theorem 3.1 in the work [8] of Xiao, which gives the result only for $K = \mathbb{Q}$, though the proof Xiao gives is general and similar to ours. He also states (in Proposition 2.1 of [8]) that $\mathcal{A}(g) \cong S_3$ when $K = \mathbb{C}$. Automorphisms of binary cubic forms over $\mathbb{Z}$ are also the subject of [7], which also considers the singular case; there, the author's motivation is to find all subgroups of $\mathrm{GL}(2, \mathbb{Z})$ whose invariant subring in $\mathbb{Z}[X, Y]$ contains a cubic form; they embed $\mathcal{A}(g)$ into $\mathrm{GL}(2, \mathbb{F}_3)$ by reduction modulo 3, and then consider all possible subgroups of that group, eventually reaching the same conclusion as here.

Part (2) also follows from the Delone-Faddeev parametrization of cubic orders by binary cubic forms from [5], whose proof goes through with their base ring $\mathbb{Z}$ replaced by any field: see Proposition 12 of [3].

6. Integral equivalence

Our results so far concern binary cubic forms over a field K (with $\mathrm{char}(K) \neq 2, 3$) and their equivalence under the actions of $\mathrm{SL}(2, K)$ and $\mathrm{GL}(2, K)$. In applications, one may be interested in forms with coefficients in some subring R of K and their orbits under $\mathrm{SL}(2, R)$ and $\mathrm{GL}(2, R)$. One classical example is when $R = \mathbb{Z}$ and $K = \mathbb{Q}$, or more generally when K is a number field and R its ring of integers.

Using Theorem 18 of [2], it would be possible to write down an equivalence test in terms of a generalized Cardano invariant, at least when R is a Dedekind domain. However, it is simpler to use our

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

second criterion. Since, $\mathrm{GL}(2,R)$-equivalence implies $\mathrm{GL}(2,K)$-equivalence, and similarly for $\mathrm{SL}(2)$, it is easy to adapt our results to give a test for $\mathrm{GL}(2,R)$- or $\mathrm{SL}(2,R)$-equivalence. First, let g_1, g_2 be two cubic forms with coefficients in R and the same nonzero discriminant Δ. Using Theorem 15, we can find all $M \in \mathrm{SL}(2,K)$ such that $g_1 = g_2^M$, if any. If there are none, then certainly the forms are not $\mathrm{SL}(2,R)$-equivalent; if any such M exist, their number will be either 1 or 3, the latter if and only if Δ is a square, and the forms are $\mathrm{SL}(2,R)$-equivalent if and only if at least one of the matrices has entries in R. For $\mathrm{GL}(2,R)$-equivalence, we repeat using $g_1(X,Y)$ and $g_2(X,-Y)$.

For example, let $g_1(X,Y) = X^3 - 16Y^3$ and $g_2(X,Y) = g_1(2X, Y/2) = 8X^3 - 2Y^3$. Both have integral coefficients, and they are $\mathrm{SL}(2,\mathbb{Q})$-equivalent via $\mathrm{diag}(2, 1/2)$. Since the common discriminant is $-2^8 3^3$ which is not a square, this is the unique $\mathrm{SL}(2,\mathbb{Q})$-equivalence, so they are not $\mathrm{SL}(2,\mathbb{Z})$-equivalent. Since the cubics are irreducible, neither has an automorphism of determinant -1, hence there are no other $\mathrm{GL}(2,\mathbb{Q})$-equivalences between them and they are therefore not $\mathrm{GL}(2,\mathbb{Z})$-equivalent.

As a second example, let $g(X,Y) = (X-Y)(X-2Y)(X-3Y)$. This has cubic covariant $G(X,Y) = -2Y(3X-7Y)(3X-5Y)$. Its self-bicovariant $B_{g,g}$ has three linear factors:

$$\begin{aligned} &Y_1X_2 - X_1Y_2, \\ -3&X_1X_2 + 7X_1Y_2 + 5Y_1X_2 - 13Y_1Y_2, \\ -3&X_1X_2 + 5X_1Y_2 + 7Y_1X_2 - 13Y_1Y_2. \end{aligned}$$

From the coefficients of the three factors we find that $\mathcal{A}_1(g) = \{I, M, M^2\}$, where $M = \frac{1}{2}\begin{pmatrix} -5 & -3 \\ 13 & 7 \end{pmatrix}$ and $M^2 = \frac{1}{2}\begin{pmatrix} 7 & 3 \\ -13 & -5 \end{pmatrix}$. This shows that it is possible for two integral forms to be $\mathrm{SL}(2,\mathbb{Q})$-equivalent via a non-integral matrix M, while also being $\mathrm{SL}(2,\mathbb{Z})$-equivalent. Hence when testing for $\mathrm{SL}(2,\mathbb{Z})$-equivalence (and similarly for $\mathrm{GL}(2,\mathbb{Z})$-equivalence) it is important to consider all possible $\mathrm{GL}(2,\mathbb{Q})$-equivalences, to determine whether one is integral.

7. Applications to elliptic curves

Our work [4] with Fisher, on binary quartic forms and their equivalence, was motivated by the application to 2-descent on elliptic curves. Specifically, there is a bijection between orbits of binary quartic forms with classical invariants I, J under a suitably twisted group action, and 2-covers of the elliptic curve $Y^2 = X^3 - 27IX - 27J$, with the 2-covering maps being given by the syzygy between covariants of the quartic.

There is a similar application for binary cubic forms, this time to 3-isogeny descent on elliptic curves with j-invariant 0. This connection is treated in detail by Bhargava *et al.* in [2]. We briefly describe the connection here, summarizing Section 3 of [2]

Let E_k denote the elliptic curve with Weierstrass equation $Y^2 = X^3 + k$, where $k \in K^*$. There is a 3-isogeny $\phi: E_k \to E_{-27k}$ with dual $\hat{\phi}$. Elements of the Galois cohomology group $H^1(G_K, E_{-27k}[\hat{\phi}])$, which are locally trivial and so represent ϕ-Selmer elements, can be represented by cubic curves $\mathcal{C}_g : Z^3 = g(X,Y)$, where $g \in \mathcal{BC}(K; -108k)$; these are ϕ-coverings of E_k. They are trivial (coming from K-rational points on E_k) if and only if $\mathcal{C}(K) \neq \emptyset$. The covering map $\mathcal{C}_g \to E_k$ is given by the covariant syzygy (1), which implies that

$$(x,y,z) \in \mathcal{C}_g(K) \quad \Longrightarrow \quad \left(\frac{H(x,y)}{(3z)^2}, \frac{G(x,y)}{2(3z)^3}\right) \in E_k(K).$$

This is stated (with slightly different notation) in Remark 30 in [2], the syzygy being equation (16) there. In [2] the $\mathrm{GL}(2,K)$-action is untwisted, but as the results there concern orbits under $\mathrm{SL}(2,K)$ this is immaterial: for example, [2, Theorem 27] states that there is a bijection between $H^1(G_K, E_{-27k}[\hat{\phi}])$ and the set of $\mathrm{SL}(2,K)$-orbits on $\mathcal{BC}(K; -108k)$.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086

The untwisted GL(2)-action is also studied by Kulkarni and Ure in [6], who give (under the assumption that K contains the cube roots of unity) a different relation between the (untwisted) GL(2, K)-orbits on $\mathcal{BC}(K)$ and elliptic curves over K with j-invariant 0.

Acknowledgements. We thank Tom Fisher and a referee for helpful comments and some additional references.

References

[1] M. Bhargava, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, *Ann. Math.* **159** (2004), no. 1, 217–250.
[2] M. Bhargava, N. Elkies and A. Shnidman, *The average size of the* 3*-isogeny Selmer groups of elliptic curves* $y^2 = x^3 + k$, *J. London Math. Soc.* **101** (2020), no. 1, 299–327.
[3] M. Bhargava, A. Shankar and J. Tsimerman, On the Davenport–Heilbronn theorems and second order terms, *Invent. Math.* **193** (2013), no. 2, 439–499.
[4] J. E. Cremona and T. A. Fisher, On the equivalence of binary quartics, *J. Symbolic Comput.* **44** (2009), no. 6, 673–682, (2010c: 11049).
[5] B. N. Delone and D. K. Faddeev, "The Theory of Irrationalities of the Third Degree," Trudy Mat. Inst. Steklov, Vol. **11** (1940).
[6] R. S. Kulkarni and C. Ure, A moduli interpretation of untwisted binary cubic forms, arXiv preprint arXiv:2103.16691 (2021).
[7] M. D. Neusel, Cubic invariants of $GL(2, \mathbb{Z})$, *Commun. Algebra* **24** (1996), no. 1, 247–257.
[8] S. Y. Xiao, On binary cubic and quartic forms, *Journal de Théorie des Nombres de Bordeaux* **31** (2019), no. 2, 323–341.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 11:56:41, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0017089526101086