Equivalence of binary forms over a field

John Cremona

University of Warwick

Debrecen Online Number Theory Seminar
6 December 2024

Overview

1. Introduction: notation/definitions, statement of the problem
2. Warm-up: quadratics
3. Cubics: the Cardano covariant “fingerprint”
4. Cubics: using the bicovariant to recover the transform
5. Quartics
6. Elliptic curve applications

See `http://arxiv.org/abs/2212.02120` for binary cubics, and `http://dx.doi.org/10.1016/j.jsc.2008.09.004` (joint with Tom Fisher) for binary quartics.

Notations and definitions

- K is a field with $\mathrm{char}(K) \neq 2, 3$;
- $\mathcal{B}_n(K)$ is the set of degree n binary forms $g(X, Y) \in K[X, Y]$ (homogeneous of degree n, coefficients in K);
- For $g \in \mathcal{B}_n(K)$, $\Delta = \mathrm{disc}(g)$ is homogeneous of degree $2n - 2$ in the coefficients of g;
- for each $\Delta \in K^*$, $\mathcal{B}_n(K; \Delta) = \{g \in \mathcal{B}_n(K) \mid \mathrm{disc}(g) = \Delta\}$.
- $\mathrm{GL}(2, K)$ acts on $\mathcal{B}_n(K)$: we will use a twisted action where $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}(2, K)$ takes g to g^M:

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

  where $(X' \; Y') = (X \; Y)M$.
- $\mathrm{disc}(g^M) = \det(M)^{(n-1)(n-2)} \, \mathrm{disc}(g)$.

Statement of the problem

Fix K and $\Delta \in K^*$. Let $g_1, g_2 \in \mathcal{B}_n(K; \Delta)$.

- Are g_1 and g_2 equivalent under the action of $\mathrm{GL}(2, K)$?
- If so, find $M \in \mathrm{GL}(2, K)$ with $g_2 = g_1^M$.

Statement of the problem

Fix K and $\Delta \in K^*$. Let $g_1, g_2 \in \mathcal{B}_n(K;\Delta)$.

- Are g_1 and g_2 equivalent under the action of $\mathrm{GL}(2,K)$?
- If so, find $M \in \mathrm{GL}(2,K)$ with $g_2 = g_1^M$.

We may also ask the same question replacing $\mathrm{GL}(2,K)$ with $\mathrm{SL}(2,K)$. In any case, for the discriminant to preserved by the action so we must have $\det(M)^{(n-1)(n-2)} = 1$.

Quadratics

The discriminant of $g(X, Y) = aX^2 + bXY + cY^2$ is $\Delta = b^2 - 4ac$, which is preserved by the twisted $\mathrm{GL}(2, K)$-action.

If $a \neq 0$ then $M = \begin{pmatrix} 2 & 0 \\ -b & 2a \end{pmatrix}$ with $\det(M) = 4a \neq 0$ takes g to $g^M(X, Y) = X^2 - \frac{1}{4}\Delta Y^2$.

Quadratics

The discriminant of $g(X,Y) = aX^2 + bXY + cY^2$ is $\Delta = b^2 - 4ac$, which is preserved by the twisted $\mathrm{GL}(2,K)$-action.

If $a \neq 0$ then $M = \begin{pmatrix} 2 & 0 \\ -b & 2a \end{pmatrix}$ with $\det(M) = 4a \neq 0$ takes g to $g^M(X,Y) = X^2 - \frac{1}{4}\Delta Y^2$.

If $a = 0$ then $\Delta = b^2$ and $M = \begin{pmatrix} -2(1+bc)/b & 2b \\ 1 - bc & b^2 \end{pmatrix}$ with $\det(M) = -4b \neq 0$ also takes g to $g^M(X,Y) = X^2 - \frac{1}{4}\Delta Y^2$.

Quadratics

The discriminant of $g(X,Y) = aX^2 + bXY + cY^2$ is $\Delta = b^2 - 4ac$, which is preserved by the twisted $\mathrm{GL}(2,K)$-action.

If $a \neq 0$ then $M = \begin{pmatrix} 2 & 0 \\ -b & 2a \end{pmatrix}$ with $\det(M) = 4a \neq 0$ takes g to $g^M(X,Y) = X^2 - \frac{1}{4}\Delta Y^2$.

If $a = 0$ then $\Delta = b^2$ and $M = \begin{pmatrix} -2(1+bc)/b & 2b \\ 1-bc & b^2 \end{pmatrix}$ with $\det(M) = -4b \neq 0$ also takes g to $g^M(X,Y) = X^2 - \frac{1}{4}\Delta Y^2$.

Hence all forms with the same discriminant are $\mathrm{GL}(2,K)$-equivalent, and using these explicit matrices we can transform any one into any other one.

Cubics

Consider binary cubic forms $g \in \mathcal{B}_3(K; \Delta)$.
Since $\operatorname{disc}(g^M) = \det(M)^2 \operatorname{disc}(g)$, a matrix transforming a cubic into one with the same discriminant must have determinant ± 1.

Cubics

Consider binary cubic forms $g \in \mathcal{B}_3(K;\Delta)$.
Since $\operatorname{disc}(g^M) = \det(M)^2 \operatorname{disc}(g)$, a matrix transforming a cubic into one with the same discriminant must have determinant ± 1.
Noting that $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ takes $g(X,Y)$ to $g(-X,Y)$, we concentrate on $\mathrm{SL}(2,K)$-equivalence.

Cubics

Consider binary cubic forms $g \in \mathcal{B}_3(K;\Delta)$.
Since $\operatorname{disc}(g^M) = \det(M)^2 \operatorname{disc}(g)$, a matrix transforming a cubic into one with the same discriminant must have determinant ± 1.
Noting that $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ takes $g(X,Y)$ to $g(-X,Y)$, we concentrate on $\mathrm{SL}(2,K)$-equivalence.
Write $g(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3$ and set

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

these “seminvariants” satisfy the syzygy

$$4P^3 = U^2 + 27\Delta a^2. \tag{1}$$

The quadratic resolvent and Cardano invariant

For fixed $\Delta \in K^*$ define the *resolvent algebra*

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

which is a quadratic extension[1] of K, with $\delta^2 = -3\Delta$.

[1] L is a field, unless $\sqrt{-3\Delta} \in K$, when $L = K \oplus K$.

The quadratic resolvent and Cardano invariant

For fixed $\Delta \in K^*$ define the *resolvent algebra*

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

which is a quadratic extension[1] of K, with $\delta^2 = -3\Delta$.

To each $g \in \mathcal{B}_3(K;\Delta)$ we assign an element of L^* called the *Cardano invariant*. When $P \neq 0$ this is given by

$$z(g) = \frac{1}{2}(U + 3a\delta).$$

The syzygy (1) can then be written $\mathrm{N}_{L/K}(z) = P^3$.

[1] L is a field, unless $\sqrt{-3\Delta} \in K$, when $L = K \oplus K$.

The Cardano invariant (continued)

In the general case, the definition of $z(g)$ is a little more involved: one can show that for all the transforms g^M of g with $P(g^M) \neq 0$, the value of $z(g^M)$ is *the same modulo cubes*, so we always have a well-defined map

$$z : \mathcal{B}_3(K; \Delta) \to L^*/L^{*3}.$$

The Cardano invariant (continued)

In the general case, the definition of $z(g)$ is a little more involved: one can show that for all the transforms g^M of g with $P(g^M) \neq 0$, the value of $z(g^M)$ is *the same modulo cubes*, so we always have a well-defined map

$$z : \mathcal{B}_3(K;\Delta) \to L^*/L^{*3}.$$

In fact, P is the leading coefficient of the *Hessian covariant* of g,

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

The Cardano invariant (continued)

In the general case, the definition of $z(g)$ is a little more involved: one can show that for all the transforms g^M of g with $P(g^M) \neq 0$, the value of $z(g^M)$ is *the same modulo cubes*, so we always have a well-defined map

$$z : \mathcal{B}_3(K; \Delta) \to L^*/L^{*3}.$$

In fact, P is the leading coefficient of the *Hessian covariant* of g,

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

there is also a cubic covariant

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

and these satisfy the syzygy

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

The Cardano invariant (continued)

From these we may form the *Cardano covariant* in $L[X, Y]$

$$C(X, Y) = \frac{1}{2}(G(X, Y) + 3\delta g(X, Y)),$$

(whose leading coefficient $C(1, 0) = \frac{1}{2}(U + 3a\delta)$)

The Cardano invariant (continued)

From these we may form the *Cardano covariant* in $L[X, Y]$

$$C(X, Y) = \frac{1}{2}(G(X, Y) + 3\delta g(X, Y)),$$

(whose leading coefficient $C(1, 0) = \frac{1}{2}(U + 3a\delta)$) and the covariant syzygy (2) can be written as

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

The Cardano invariant (continued)

From these we may form the *Cardano covariant* in $L[X, Y]$

$$C(X, Y) = \frac{1}{2}(G(X, Y) + 3\delta g(X, Y)),$$

(whose leading coefficient $C(1, 0) = \frac{1}{2}(U + 3a\delta)$) and the covariant syzygy (2) can be written as

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

The general definition of the Cardano invariant in L^*/L^{*3} is *any* specialization $C(x, y)$ with $x, y \in K$ such that $H(x, y) \neq 0$. This lies in the kernel of the norm:

$$z(g) \in (L^*/L^{*3})_{N=1} := \ker(L^*/L^{*3} \to K^*/K^{*3}).$$

The Cardano invariant as a fingerprint for cubics

Our first main theorem for cubics may be summarised is:

$$\boxed{\begin{array}{c}\text{The Cardano group } (L^*/{L^*}^3)_{N=1} \\ \textit{exactly parametrises} \\ \text{the } \mathrm{SL}(2,K)\text{-orbits on } \mathcal{B}_3(K;\Delta).\end{array}}$$

The Cardano invariant as a fingerprint for cubics

Our first main theorem for cubics may be summarised is:

The Cardano group $(L^*/{L^*}^3)_{N=1}$
exactly parametrises
the $\mathrm{SL}(2, K)$-orbits on $\mathcal{B}_3(K; \Delta)$.

Details follow shortly, after we make a couple of digressions. . .

Why "Cardano" invariant?

Cardano's formula[2] for the roots of the cubic $g(X,1) \in K[X]$ is simply

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

where $z = (U + 3a\delta)/2$ and $\delta = \sqrt{-3\Delta}$.

[2]Gerolamo Cardano (1501–1576)

Why "Cardano" invariant?

Cardano's formula[2] for the roots of the cubic $g(X,1) \in K[X]$ is simply

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

where $z = (U + 3a\delta)/2$ and $\delta = \sqrt{-3\Delta}$.

From this we may guess that g has a root in K if and only if the Cardano invariant is a cube, i.e., trivial in L^*/L^{*3}, which is true: if $w = \sqrt[3]{z} \in L^*$, then $w\overline{w} = P$, and the formula is

$$x = -(b + w + \overline{w})/3a \in K.$$

[2] Gerolamo Cardano (1501–1576)

Digression: how to write down cubic extensions

We know that quadratic extensions of K all have the form $K(\sqrt{a})$ with $a \in K^*$ non-square, so they are parametrized by the nontrivial elements of the group K^*/K^{*2}.

Digression: how to write down cubic extensions

We know that quadratic extensions of K all have the form $K(\sqrt{a})$ with $a \in K^*$ non-square, so they are parametrized by the nontrivial elements of the group K^*/K^{*2}.

Cubics do *not* all have the form $K(\sqrt[3]{a})$ with $a \in K^*/K^{*3}$—these all have discriminant of the form -3 times a square. Instead, we may construct *all* cubic extensions of K, uniquely, as follows.

Digression: how to write down cubic extensions

We know that quadratic extensions of K all have the form $K(\sqrt{a})$ with $a \in K^*$ non-square, so they are parametrized by the nontrivial elements of the group K^*/K^{*2}.

Cubics do *not* all have the form $K(\sqrt[3]{a})$ with $a \in K^*/K^{*3}$—these all have discriminant of the form -3 times a square. Instead, we may construct *all* cubic extensions of K, uniquely, as follows.

Fix $\Delta \in K^*/K^{*2}$ and define $L = K(\sqrt{-3\Delta})$ as above. To each $z \in (L^*/L^{*3})_{N=1}$ let $\mathrm{N}_{L/K}(z) = P^3$ and $\mathrm{Tr}(z) = U$; then the cubic $f_z(X) = X^3 - 3PX - U$ has discriminant Δ (modulo squares), is irreducible if and only if z is not a cube, and every cubic extension of K arises uniquely in this way (except $f_z = f_{\bar{z}}$).

Cubic equivalence via the Cardano invariant

Theorem (A)

Let K be any field with $\mathrm{char}(K) \neq 2, 3$, let $\Delta \in K^*$, let $L = K[X]/(X^2 + 3\Delta)$, and let $z\colon \mathcal{B}_3(K;\Delta) \to L^*/L^{*3}$ be the Cardano invariant map.

1. $z(g) \in (L^*/L^{*3})_{N=1}$ *for all* $g \in \mathcal{B}_3(K;\Delta)$*;*
2. $z(g) = 1$ *if and only if* g *is reducible over* K*;*
3. $g_1, g_2 \in \mathcal{B}_3(K;\Delta)$ *are* $\mathrm{SL}(2,K)$*-equivalent if and only if* $z(g_1) = z(g_2)$*;*
4. $g_1, g_2 \in \mathcal{B}_3(K;\Delta)$ *are* $\mathrm{GL}(2,K)$*-equivalent if and only if* $z(g_1) = z(g_2)^{\pm 1}$ *(equivalently,* $z(g_1)$ *and* $z(g_2)$ *generate the same subgroup of* L^*/L^{*3}*);*
5. z *induces bijections between the* $\mathrm{SL}(2,K)$*-orbits on* $\mathcal{B}_3(K;\Delta)$ *and the Cardano group* $(L^*/L^{*3})_{N=1}$*, and between the* $\mathrm{GL}(2,K)$*-orbits and its cyclic subgroups.*

Explicit equivalence - introduction

So far we have shown how to test equivalence of two cubics $g_1, g_2 \in \mathcal{B}_3(K;\Delta)$, in a rather inconvenient way: test whether two elements of the quadratic resolvent algebra L are the same modulo cubes.

Explicit equivalence - introduction

So far we have shown how to test equivalence of two cubics $g_1, g_2 \in \mathcal{B}_3(K; \Delta)$, in a rather inconvenient way: test whether two elements of the quadratic resolvent algebra L are the same modulo cubes.

We would prefer a method which only uses arithmetic in the base field K, and we would also like to find a transforming matrix M with $g_1^M = g_2$ if the test returns "yes". Our second result on cubics achieves this.

Explicit equivalence - introduction

So far we have shown how to test equivalence of two cubics $g_1, g_2 \in \mathcal{B}_3(K;\Delta)$, in a rather inconvenient way: test whether two elements of the quadratic resolvent algebra L are the same modulo cubes.

We would prefer a method which only uses arithmetic in the base field K, and we would also like to find a transforming matrix M with $g_1^M = g_2$ if the test returns "yes". Our second result on cubics achieves this.

We know that $g_1^M = g_2$ with $M \in \mathrm{SL}(2,K)$ iff $z = z(g_1)/z(g_2)$ is a cube in L^*. But z is the Cardano invariant of a third cubic in $\mathcal{B}_3(K;\Delta)$; hence g_1 and g_2 are equivalent iff a *third* cubic g (with the same discriminant) has a root.

Explicit equivalence - introduction

So far we have shown how to test equivalence of two cubics $g_1, g_2 \in \mathcal{B}_3(K;\Delta)$, in a rather inconvenient way: test whether two elements of the quadratic resolvent algebra L are the same modulo cubes.

We would prefer a method which only uses arithmetic in the base field K, and we would also like to find a transforming matrix M with $g_1^M = g_2$ if the test returns "yes". Our second result on cubics achieves this.

We know that $g_1^M = g_2$ with $M \in \mathrm{SL}(2,K)$ iff $z = z(g_1)/z(g_2)$ is a cube in L^*. But z is the Cardano invariant of a third cubic in $\mathcal{B}_3(K;\Delta)$; hence g_1 and g_2 are equivalent iff a *third* cubic g (with the same discriminant) has a root.

Explicitly, the third cubic is (at least when $P_1P_2 \neq 0$)

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

Can we use this to find M?

Explicit equivalence - the bi-covariant

The cubic $f(X)$ on the previous page is related (by a simple transform and homogenization) to the cubic form

$$\begin{aligned} B(X,Y) &= U_1 g_2(X,Y) - a_1 G_2(X,Y) \\ &= G_1(1,0) g_2(X,Y) - g_1(1,0) G_2(X,Y), \end{aligned}$$

where $a_i, b_i, \ldots, P_i, U_i$ are the coefficients/covariants of g_1, g_2.

Explicit equivalence - the bi-covariant

The cubic $f(X)$ on the previous page is related (by a simple transform and homogenization) to the cubic form

$$\begin{aligned} B(X,Y) &= U_1 g_2(X,Y) - a_1 G_2(X,Y) \\ &= G_1(1,0) g_2(X,Y) - g_1(1,0) G_2(X,Y), \end{aligned}$$

where $a_i, b_i, \ldots, P_i, U_i$ are the coefficients/covariants of g_1, g_2. To avoid handling special cases, we replace the specialization $(1,0)$ with two new variables and define

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

This is bi-homogeneous of degree $(3,3)$ and is bi-covariant (homogeneous and covariant in each set of variables separately).

Equivalence via bi-linear factors of the bi-covariant

It is not hard to see that

$$X_1Y_2 - X_2Y_1 \mid B_{g_1,g_2}(X_1, Y_1, X_2, Y_2) \iff g_2 = \pm g_1.$$

Equivalence via bi-linear factors of the bi-covariant

It is not hard to see that

$$X_1 Y_2 - X_2 Y_1 \mid B_{g_1,g_2}(X_1, Y_1, X_2, Y_2) \iff g_2 = \pm g_1.$$

Playing around with the bi-covariance of B_{g_1,g_2}, one finds that bi-linear factors of B_{g_1,g_2} (if any) all come from matrices M transforming g_1 to g_2.

Equivalence via bi-linear factors of the bi-covariant

It is not hard to see that

$$X_1Y_2 - X_2Y_1 \mid B_{g_1,g_2}(X_1, Y_1, X_2, Y_2) \iff g_2 = \pm g_1.$$

Playing around with the bi-covariance of B_{g_1,g_2}, one finds that bi-linear factors of B_{g_1,g_2} (if any) all come from matrices M transforming g_1 to g_2.

For $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ define L_M to be the bi-linear form

$$L_M = -sX_1X_2 + rX_1Y_2 - uY_1X_2 + tY_1Y_2.$$

Lemma

If $L_M \mid B_{g_1,g_2}$ *then* $\det(M) \in K^{*2}$ *and* $g_2^M = \pm \det(M)^{1/2} g_1$.

Explicit equivalence - conclusion

Theorem (B)

Let $g_1, g_2 \in \mathcal{B}_3(K;\Delta)$. 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 $g_1 = g_2^M$.

Explicit equivalence - conclusion

Theorem (B)

Let $g_1, g_2 \in \mathcal{B}_3(K;\Delta)$. 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 $g_1 = g_2^M$.

We can similarly detect transforming matrices with determinant -1 using bi-linear factors of

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

Explicit equivalence - conclusion

Theorem (B)

Let $g_1, g_2 \in \mathcal{B}_3(K;\Delta)$. 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 $g_1 = g_2^M$.

We can similarly detect transforming matrices with determinant -1 using bi-linear factors of

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

This completes our discussion of cubics.

Quartics

The story for quartics is similar: Cremona & Fisher (2009).

- $g \in \mathcal{B}_4(K)$ has classical invariants I, J as well as Δ, with
$$\Delta = 4I^3 - J^2.$$
- There is a resolvent *cubic algebra*
$$L = K[T]/(T^3 - 3IT + J) = K[\varphi].$$
- The algebraic invariant $z(g) = \frac{1}{3}(4a\varphi + p) \in L^*$ with $p = 3b^2 - 8ac$, the leading coefficient of the Hessian covariant $H(g)$, has square norm:
$$\mathrm{N}_{L/K}(z) = r^2,$$
where $r = b^3 + 8a^2d - 4abc$ is the leading coefficient of a sextic covariant $G(g)$.

Quartic equivalence via the algebraic invariant

Just as for cubics we can give a better definition of the algebraic invariant $z(g)$ as any invertible value of the algebraic covariant

$$\frac{1}{3}(4\varphi g(X,Y) + H(X,Y))$$

(which has norm $G(X,Y)^2$). Then

- $z(g)$ is well-defined in L^*/L^{*2};
- $z(g) \in \ker(\mathrm{N}_{L/K} : L^*/L^{*2} \to K^*/K^{*2})$;
- $z(g) = 1$ iff g has a linear factor;
- $z(g_1) = z(g_2)$ iff g_1, g_2 are $\mathrm{GL}(2,K)$-equivalent.

Quartic equivalence via the algebraic invariant

Just as for cubics we can give a better definition of the algebraic invariant $z(g)$ as any invertible value of the algebraic covariant

$$\frac{1}{3}(4\varphi g(X,Y) + H(X,Y))$$

(which has norm $G(X,Y)^2$). Then

- $z(g)$ is well-defined in L^*/L^{*2};
- $z(g) \in \ker(\mathrm{N}_{L/K} : L^*/L^{*2} \to K^*/K^{*2})$;
- $z(g) = 1$ iff g has a linear factor;
- $z(g_1) = z(g_2)$ iff g_1, g_2 are $\mathrm{GL}(2,K)$-equivalent.

NB The image of $z()$ is a *subset* (not a subgroup!) of $\ker(\mathrm{N}_{L/K} : L^*/L^{*2} \to K^*/K^{*2})$, as it is *linear* in φ.

Construction of quartics via their cubic resolvents

We can also construct all quartics $g(X)$ with invariants I, J by forming the cubic resolvent algebra $L = K[T]/(T^3 - 3IT + J) = K[\varphi]$, taking $z \in \ker(\mathrm{N}_{L/K} : L^*/L^{*2} \to K^*/K^{*2})$ with minimal polynomial

$$Z^3 - pZ^2 + qZ - r^2,$$

and setting $g(X) = (X^2 - p)^2 - 8rX - 4q$.

Explicit equivalence of quartics via bi-covariants

If $g_1, g_2 \in \mathcal{B}_4(K)$ have the same invariants I, J, let their Hessian covariants be $H_1.H_2$.
Form the bi-covariant

$$F(X_1, Y_1, X_2, Y_2) = g_1(X_1, Y_1)H_2(X_2, Y_2) - g_2(X_2, Y_2)H_1(X_1, Y_1),$$

which is homogeneous of bi-degree $(4, 4)$. Then

- g_1, g_2 are $\mathrm{GL}(2, K)$-equivalent iff $F(X_1, Y_1, X_2, Y_2)$ has a bi-linear factor;
- the coefficients of such a factor give the entries in a matrix M with $g_2 = g_1^M$.

See Cremona & Fisher (2009) for details.

Elliptic curve connections 1: cubics

Mordell elliptic curves are $E_k: \; Y^2 = X^3 + k$; there is a 3-isogeny $\phi: \; E_k \to E_{-27k}$. Using this and its dual $\hat{\phi}$ one can carry out 3-isogeny descent on E_k and obtain information about its rank.

Elliptic curve connections 1: cubics

Mordell elliptic curves are $E_k : \ Y^2 = X^3 + k$; there is a 3-isogeny $\phi : \ E_k \to E_{-27k}$. Using this and its dual $\hat{\phi}$ one can carry out 3-isogeny descent on E_k and obtain information about its rank. There is a bijection (due to Bhargava) between $H^1(G_K, E_{-27k}[\hat{\phi}])$ and the set of $\mathrm{SL}(2,K)$-orbits on $\mathcal{B}_3(K; -108k)$: elements of the former are represented by genus one covering curves $C_g : \ Z^3 = g(X, Y)$ with $g \in \mathcal{B}_3(K; -108k)$, and the covariant syzygy gives the covering map $C_g \to E_k$ since

$$(x, y, z) \in C_g(K) \longrightarrow \left(\frac{H(x,y)}{(3z)^2}, \frac{G(x,y)}{2((3z)^3)} \right) \in E_k(K).$$

Elliptic curve connections 1: cubics

Mordell elliptic curves are $E_k: \ Y^2 = X^3 + k$; there is a 3-isogeny $\phi: \ E_k \to E_{-27k}$. Using this and its dual $\hat{\phi}$ one can carry out 3-isogeny descent on E_k and obtain information about its rank. There is a bijection (due to Bhargava) between $H^1(G_K, E_{-27k}[\hat{\phi}])$ and the set of $\mathrm{SL}(2,K)$-orbits on $\mathcal{B}_3(K; -108k)$: elements of the former are represented by genus one covering curves $C_g: \ Z^3 = g(X,Y)$ with $g \in \mathcal{B}_3(K; -108k)$, and the covariant syzygy gives the covering map $C_g \to E_k$ since

$$(x,y,z) \in C_g(K) \longrightarrow \left(\frac{H(x,y)}{(3z)^2}, \frac{G(x,y)}{2((3z)^3)} \right) \in E_k(K).$$

Hence, enumerating binary cubics up to equivalence gives information about the size of the 3-Selmer group of these (special) elliptic curves.

Elliptic curve connections 2: quartics

The connection between quartics and their in/covariants appeared in the papers of Birch and Swinnerton-Dyer in the 1960s, and a more detailed description appeared in my 2001 paper “Classical invariants and 2-descent on elliptic curves” and the 2009 joint paper with Tom Fisher already mentioned.

Elliptic curve connections 2: quartics

The connection between quartics and their in/covariants appeared in the papers of Birch and Swinnerton-Dyer in the 1960s, and a more detailed description appeared in my 2001 paper "Classical invariants and 2-descent on elliptic curves" and the 2009 joint paper with Tom Fisher already mentioned.

Quartics $g \in \mathcal{B}_4(\Delta)$ with fixed invariants I, J define genus one 2-covering curves $C_g : \ Y^2 = g(X, 1)$ of the elliptic curve $E_{I,J} : \ Y^2 = X^3 - 27IX - 27J$. Again the covariant syzygy gives the 2-covering map $C_g \to E_{I,J}$:

$$(x, y) \in C_g(K) \longrightarrow \left(\frac{3H(x, 1)}{4y^2}, \frac{27G(x, 1)}{8y^3} \right) \in E_{I,J}(K).$$