



---

# Equivalence of Real Elliptic Curves

## Part 2 - Birational Equivalence

Allen Broughton  
Rose-Hulman Institute of Technology

# Credits

---

Discussion with Ken McMurdy

# Outline - 1

---

Recap of linear equivalence

Complex elliptic curves definitions and pictures

Linear equivalence applied to complex curves

Birational equivalence

Real forms and conjugations

Equivalence of real forms and complex automorphisms (results are here)

## Recap of Linear Equivalence - 1

---

A real elliptic curve is a curve defined by a polynomial equation of degree 3 with real coefficients

$$f(x,y)=0$$

Two curves are linearly equivalent if one can be mapped on to the other by a (projective) linear change of coordinates

## Recap of Linear Equivalence - 2

---

A real elliptic curve is linearly equivalent to a curve in one of these two forms

$$y^2 = x(x-1)(x-\lambda), \quad 0 < \lambda < 1$$

*(two components)*

or

$$y^2 = x(x^2 - 2\lambda x + 1), \quad -1 < \lambda < 1$$

*(one component)*

Pictures [pics.mws](#)

# Complex elliptic curves definition and pictures -1

---

A complex elliptic curve  $E$  is a curve defined by a degree 3 equation with complex coefficients.

There is a degree three polynomial  $f(x,y)$  and the complex curve  $E_C$  is given by

$$E_C = \{(x,y) \in \mathbf{C}^2 : f(x,y) = 0\}$$

A complex elliptic curve is a torus with one point at infinity if that point is a flex

# Complex elliptic curves definition and pictures -2

---

If the coefficients are real then

$$E_R = \{(x, y) \in \mathbf{R}^2 : f(x, y) = 0\}$$

is a real elliptic curve lying inside  $E_C$

When we want to consider the real and the complex curves in their own right we write  $E_C$  or  $E_R$  to distinguish

Here are some pictures

[complexelliptic1.mws](#), [complexelliptic2.mws](#)

For simplicity work with affine equations but think projective

# Linear equivalence ideas applied to complex elliptic curves - 1

---

Apply steps of reduction to a complex curve

$$0=f(x,y)=\sum_{i,j} a_{i,j} x^i y^j \text{ for } 0 \leq i+j \leq 3$$

there are 10 coefficients

By lining up the curve appropriately with the axes five coefficients become zero to get (much of the talk in part 1)

$$\begin{aligned} f(x,y) &= \alpha y^2 - \beta(x-\lambda_1)(x-\lambda_2)(x-\lambda_3) \\ &= \alpha y^2 - g(x) \end{aligned}$$

## Linear equivalence ideas applied to complex elliptic curves - 2

---

Apply a transformation of the type

$$f(x,y) \rightarrow f(ax+b, cy)/w$$

and we get a form of the type

$$f(x,y) = y^2 - x(x-1)(x-\lambda)$$

This was also a part of the Part 1 talk

## Linear equivalence ideas applied to complex elliptic curves - 3

---

Apply a transformation of the type

$$f(x,y) \rightarrow f(ax+b, cy)/w$$

and we get this form

$$f(x,y) = y^2 - x(x-1)(x-\lambda)$$

Call the corresponding curve  $E_\lambda$

## Linear equivalence ideas applied to complex elliptic curves - 4

---

Apply the transformation

$$f(x,y) \rightarrow f(1-x, iy)$$

and we get this form

$$f_1(x,y) = y^2 - x(x-1)(x-(1-\lambda))$$

## Linear equivalence ideas applied to complex elliptic curves - 5

---

Apply the transformation

$$f(x,y) \rightarrow f(\lambda x, \lambda^{3/2}y) / \lambda^3$$

and we get this form

$$f_2(x,y) = y^2 - x(x-1)(x-1/\lambda)$$

## Linear equivalence ideas applied to complex elliptic curves - 6

---

Thus  $E_\lambda$  is equivalent to

$E_{1-\lambda}$ ,  $E_{1/\lambda}$  and hence

$E_{(\lambda-1)/\lambda}$ ,  $E_{1/(1-\lambda)}$  and  $E_{\lambda/(\lambda-1)}$

There are 6 linearly equivalent equations

This exhausts all of the possibilities

Proof: [lambdagroup.mws](http://lambdagroup.mws)

## Linear equivalence ideas applied to complex elliptic curves - 7

---

Theorem 2: Linear equivalence of complex elliptic curves

Every (smooth, projective) complex elliptic curve is linearly equivalent to some  $E_\lambda$ ,  $\lambda \neq 0, 1$

If  $E_\lambda$  is equivalent to  $E_{\lambda'}$ , then

$$\lambda' \in \{\lambda, 1-\lambda, 1/\lambda, (\lambda-1)/\lambda, 1/(1-\lambda), \lambda/(1-\lambda)\}$$

# Linear equivalence ideas applied to complex elliptic curves - 8

---

The quantity

$$j(\lambda) = 256 (\lambda^2 - \lambda - 1)^3 / (\lambda^2 (\lambda - 1)^2)$$

is called the  $j$ -invariant of a complex elliptic curve

The quantities  $\lambda$  and  $\lambda'$  satisfy

$$\lambda' \in \{\lambda, 1 - \lambda, 1/\lambda, (\lambda - 1)/\lambda, 1/(1 - \lambda), \lambda/(1 - \lambda)\}$$

If and only if  $j(\lambda) = j(\lambda')$

## Birational equivalence - 1

---

Our curves, both real and complex live (locally) in Euclidean spaces, e.g.,  $\mathbf{R}^2$  and  $\mathbf{C}^2$ .

A map  $\varphi : E \rightarrow F$  of elliptic curves is called *rational* if the map is given in local affine coordinates by rational functions of the coordinates.

A map is *birational* if it is 1-1 & onto and has a rational map as an inverse.

## Birational equivalence - 2

---

Two curves are birationally equivalent if there is a birational map  $\varphi : E \rightarrow F$

If the curves are real then we insist that the map restricts  $\varphi_R : E_R \rightarrow F_R$  and that the coefficients of  $\varphi$  are real

A birational equivalence of a curve to itself is called an automorphism.

Linear equivalence is a special case of birational equivalence

## Birational equivalence - 3

---

Example: Group law maps

- Given a points  $P, Q$  on  $E$  there is a (involuntary) birational map  $\varphi : E \rightarrow E$  such that  $\varphi(P)=Q$  and  $\varphi(Q)=P$
- [grouplaw.mws](#)

Theorem 3: Two complex curves are birationally equivalent if and only if their  $j$ -invariants are equal

This is *not true* for real elliptic curves. The rest of the talk discusses the difference.

# Real forms and complex conjugations -1

---

- Let  $E_C$  be a complex curve whose affine part is defined by

$$E_C = \{(x, y) \in \mathbf{C}^2 : f(x, y) = 0\}$$

where  $f(x, y)$  has real coefficients

- the map  $\sigma : (x, y) \rightarrow (x^-, y^-)$  (conjugation) maps  $E_C$  to itself and  $E_R$  is the set of fixed points of  $\sigma$
- We call  $E_R$  a real form of  $E_C$  and  $\sigma$  is the corresponding *symmetry* or *complex conjugation* of  $E_C$

## Real forms and complex conjugations - 2

---

- Given another birationally isomorphic realization of  $E_C$  by a real equation  $f_1(x,y)=0$  then we get another real form and another symmetry  $\sigma_1$
- The symmetries are related by

$$\sigma_1 = \sigma \circ \varphi \text{ (composition)}$$

where  $\varphi$  is a automorphism of the complex curve.

# Real forms and complex conjugations - 3

---

Canonical example

- Let  $g(x)$  be a real cubic in  $x$ .
- Then

$$\begin{aligned}y^2 &= g(x) \\ y^2 &= -g(x)\end{aligned}$$

define distinct real forms  $E^+$  and  $E^-$  of the same complex curve

- We have

$$\begin{aligned}\sigma &: (x, y) \rightarrow (x^-, y^-) \\ \sigma_I &: (x, y) \rightarrow (x^-, -y^-) \\ \varphi &: (x, y) \rightarrow (x, -y)\end{aligned}$$

# Real forms and complex conjugations - 4

---

- Each point  $(x,y)$  on  $E^+$  corresponds to a point  $(x,y)$  on  $(x,iy)$
- Pictures
  - [complexelliptic2.mws](#)
  - [complexelliptic1.mws](#)
- Note that the real forms cannot be simultaneously realized at the real points of a complex cubic but that the complex curve can be linearly transformed so that the points of a real form are the real points of the curve.
- More pictures on  $E^+$  and  $E^-$  [realforms.mws](#)

# Equivalence of real forms and complex automorphisms - 1

---

## Theorem

- A complex curve has a real form if and only if the  $j$ -invariant is real.
- Any two real forms of a complex curve have the same  $j$ -invariant
- Let  $E_1$  and  $E_2$  be two real forms of a complex curve and  $\sigma_1$  and  $\sigma_2$  the corresponding symmetries. The two real elliptic curves are birationally isomorphic if and only if there is an automorphism of the elliptic curve satisfying

$$\sigma_2 = \varphi \sigma_1 \varphi^{-1}$$

# Equivalence of real forms and complex automorphisms - 2

---

- All real numbers are realized as a  $j$ -invariants for some curve.
- A real elliptic curve has one component if and on if the  $j$ -invariant  $\leq 1728$
- A real elliptic curve has two components if and on if the  $j$ -invariant  $\geq 1728$
- All complex curves have exactly two non-isomorphic real forms passing through the point at infinity
- Only curves with  $j$ -invariant =  $1728$  have real forms of both topological types

# Equivalence of real forms and complex automorphisms - 3

---

- Theorem 1 : A real smooth elliptic curve is (projectively) birationally equivalent to exactly one equation of the form

$$y^2 = x(x-1)(x-\lambda), \quad 0 < \lambda < 1$$

*(two components)*

- or

$$y^2 = x(x^2 - 2\lambda x + 1), \quad -1 < \lambda < 1$$

*(one component)*

# Equivalence of real forms and complex automorphisms - 4

---

- The special curve is

$$y^2 = x^3 - x$$

*(two components)*

- which is complex isomorphic  $(x,y) \rightarrow (-x, iy)$  to

$$y^2 = x^3 + x$$

*(one component)*

**All Done**

---

*Any questions?*