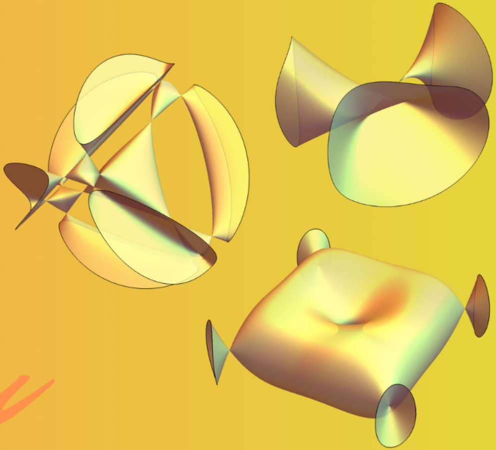
ALVARO GONZALEZ HERNANDEZ
University of Warwick

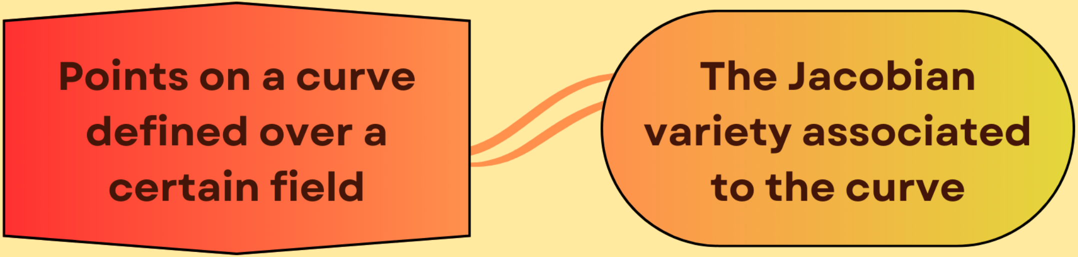


Crazy for you 2

Genus 2 curves in characteristic 2 via Kummer surfaces

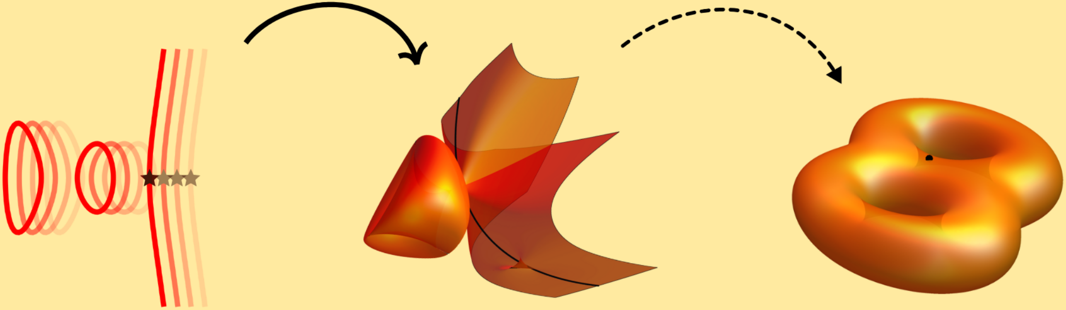
Points on a curve defined over a certain field

The Jacobian variety associated to the curve



Given a hyperelliptic curve, how can we compute an explicit model of its Jacobian as a projective variety?

The idea is



$$\mathcal{C}^{(g)} = \underbrace{\mathcal{C} \times \cdots \times \mathcal{C}}_{g} \;/\; S_g$$

Jacobian variety

Hyperelliptic curves

Let

$$\mathcal{C} : y^2 + h(x)y = f(x)$$

be a hyperelliptic curve of genus $g \geq 1$ where $f(x), h(x) \in k[x]$, $\deg f(x) = 2g + 2$ and $\deg h(x) \leq g + 1$.

The curve has two different points at infinity that I will denote by ∞_+ and ∞_-.

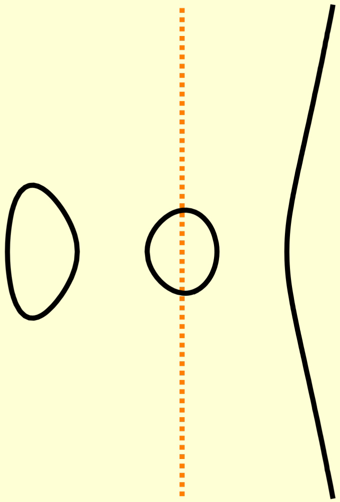
The hyperelliptic involution

The curve

$$\mathcal{C} : y^2 + h(x)y = f(x)$$

has a natural involution defined by

$$\begin{aligned} \iota_{\mathcal{C}} : \mathcal{C} &\longrightarrow \mathcal{C} \\ (x, y) &\longmapsto (x, -y - h(x)) \\ \infty_+ &\longmapsto \infty_- \\ \infty_- &\longmapsto \infty_+ \end{aligned}$$



How to compute an explicit model of the Jacobian

The following:

$$\Theta_+ = \underbrace{C \times \cdots \times C}_{g-1} \times \{\infty_+\} \quad \text{and} \quad \Theta_- = \underbrace{C \times \cdots \times C}_{g-1} \times \{\infty_-\}$$

define divisors of $\mathcal{C}^{(g)}$ and an embedding of the Jacobian into projective space is given by $\mathcal{L}(2(\Theta_+ + \Theta_-))$.

(*These are functions in the function field of* $\mathcal{C}^{(g)}$ *that at worst can only possibly have poles in* $2(\Theta_+ + \Theta_-)$ *of the "right" multiplicity.*)

Example

For $g = 2$, let's consider two copies of a curve $\mathcal{C}$

$$y_1^2 + h(x_1)y_1 = f(x_1) \qquad y_2^2 + h(x_2)y_2 = f(x_2)$$

Then, some independent functions of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ are

$$1, x_1 + x_2, x_1x_2, (x_1 + x_2)^2, \frac{(2y_1+h(x_1))-(2y_2+h(x_2))}{x_1-x_2}, \ldots$$

In this case $|\mathcal{L}(2(\Theta_+ + \Theta_-))| = 16$.

Example

The embedding would be given by considering

$$[1 : x_1 + x_2 : x_1x_2 : (x_1 + x_2)^2 : \frac{(2y_1+h(x_1))-(2y_2+h(x_2))}{x_1-x_2}, \ldots] \hookrightarrow \mathbb{P}^{15}$$

where $(x_1, y_1), (x_2, y_2) \in \mathcal{C}$.

But there is a drawback...

WARWICK
THE UNIVERSITY OF WARWICK

The embedding by $\mathcal{L}(2(\Theta_+ + \Theta_-))$ is given by the intersection of **many** conics:

Genus	1	2	3	$\cdots$	g
$\mathbb{P}^n$ in which it embeds	3	15	63	$\cdots$	$4^g - 1$
Number of conics	2	72	1568	$\cdots$	$2^{2g-1}(2^g - 1)^2$

Simplifying models at the cost of losing information

$\iota_{\mathcal{C}}$ extends to an involution on $\mathcal{C}^{(g)}$, such that $\iota_{\mathcal{C}}$ acts linearly on the elements of $\mathcal{L}(2(\Theta_+ + \Theta_-))$. If the field of definition has characteristic different than 2, we can "diagonalise" this action to obtain a decomposition:

$$\mathcal{L}(2(\Theta_+ + \Theta_-)) = \{\text{even functions}\} \oplus \{\text{odd functions}\}$$

where

$$\iota_{\mathcal{C}}(\text{even}) = \text{even} \qquad\qquad \iota_{\mathcal{C}}(\text{odd}) = -\text{odd}$$

Going back to our example when $g = 2$

The functions

$$\{1, x_1 + x_2, x_1 x_2, (x_1 + x_2)^2, \dots\}$$

are even and $|\{\text{even functions}\}| = 10.$

The functions

$$\left\{\frac{(2y_1+h(x_1))-(2y_2+h(x_2))}{x_1-x_2}, \frac{(2y_1+h(x_1)x_2)-(2y_2+h(x_2))x_1}{x_1-x_2}, \dots\right\}$$

are odd and $|\{\text{odd functions}\}| = 6.$

Kummer varieties

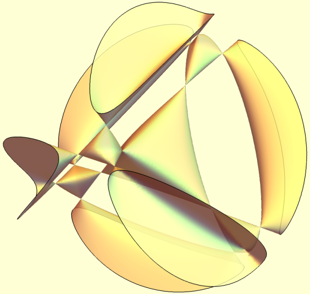
Kummer variety

Let $\mathcal{A}$ be an Abelian variety (e.g. the Jacobian of a hyperelliptic curve) and let ι be the involution in $\mathcal{A}$ that sends an element to its inverse. Then, the **Kummer variety** associated to $\mathcal{A}$, $\mathrm{Kum}(\mathcal{A})$ is the quotient variety $\mathcal{A}/\iota$.

Fact

For $g > 1$, $\mathcal{A}[2]$ is the set of all fixed points under the action of ι and these points are singular points of $\mathrm{Kum}(\mathcal{A})$.

Examples of Kummer varieties



Suppose that the field of definition has characteristic different than 2.

- If the dimension of $\mathcal{A}$ is 2, $\mathrm{Kum}(\mathcal{A})$ is a surface described by a quartic in $\mathbb{P}^3$ with 16 nodal singularities.
- Generally, if the dimension of $\mathcal{A}$ is g, $\mathrm{Kum}(\mathcal{A})$ can be found as an intersection in $\mathbb{P}^{2^g-1}$.

Why are Kummer varieties relevant?

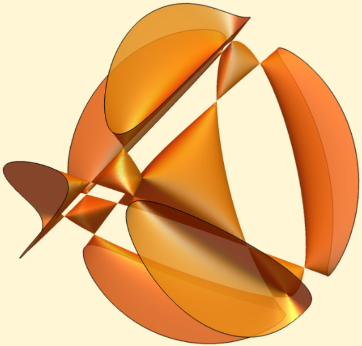
- Their models are considerably easier.
- They are **not** Abelian varieties, so they do not have a group law. However, they inherit a *pseudo-group law*.
- For a hyperelliptic curve $\mathcal{C}$, the projective embedding of the Kummer variety associated to the Jacobian of $\mathcal{C}$ is given by $\mathcal{L}(\Theta_+ + \Theta_-)$.

In the case of Kummer surfaces

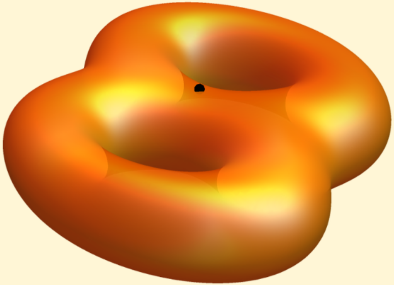
$$\mathcal{L}(\Theta_+ + \Theta_-) \subset \{\text{even functions of } \mathcal{L}(2(\Theta_+ + \Theta_-))\}$$

In fact, the space of even functions of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ is generated as a vector space by the products of every two functions of $\mathcal{L}(\Theta_+ + \Theta_-)$.

Furthermore, the space of odd functions of $\mathcal{L}(2(\Theta_+ + \Theta_-))$ defines a model of the desingularisation of the Kummer surface as the intersection of 3 quadrics in $\mathbb{P}^5$.



Desingularisation of the Kummer surface



Explicit projective models of the Jacobian of a genus 2 curve

1 **Canonical form.** We shall normally suppose that the characteristic¶ of the ground field is not 2 and consider curves $\mathcal{C}$ of genus 2 in the shape

$$\mathcal{C}: \quad Y^2 = F(X), \tag{1.1.1}$$

where

$$F(X) = f_0 + f_1 X + \ldots + f_6 X^6 \in k[X] \tag{1.1.2}$$

1. *The Jacobian variety*

We shall work with a general curve $\mathscr{C}$ of genus 2, over a ground field K of characteristic not equal to 2, 3 or 5, which may be taken to have hyperelliptic form

$$\mathscr{C}: Y^2 = F(X) = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0 \qquad (1)$$

with $f_0, \ldots, f_6$ in K, $f_6 \neq 0$, and $\Delta(F) \neq 0$, where $\Delta(F)$ is the discriminant of F. In $\mathbb{F}_5$ there is, for example, the curve $Y^2 = X^5 - X$ which is not birationally equivalent to the above form.

1 **Canonical form.** We shall normally suppose that the characteristic¶ of the ground field is not 2 and consider curves $\mathcal{C}$ of genus 2 in the shape

$$\mathcal{C}: \quad Y^2 = F(X), \qquad (1.1.1)$$

where

$$F(X) = f_0 + f_1X + \ldots + f_6X^6 \in k[X] \qquad (1.1.2)$$

2. Set-up

Let k be a field of characteristic not equal to two, k^{s} a separable closure of k, and $f = \sum_{i=0}^{6} f_iX^i \in k[X]$ a separable polynomial with $f_6 \neq 0$. Denote by Ω the set of the six roots of f in k^{s}, so that $k(\Omega)$ is the splitting field of f over k in k^{s}. Let C be the smooth projective

But, what is so special about characteristic 2?

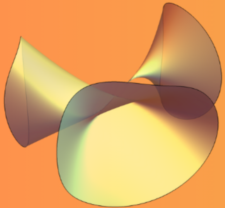
In algebraically closed fields of characteristic 2, the 2-torsion of the Jacobian of a curve $\mathcal{C}$ of genus g is

$$\mathcal{J}(\mathcal{C})[2] \cong (\mathbb{Z}/2\mathbb{Z})^r$$

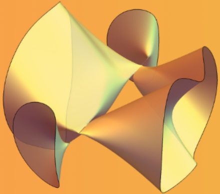
for some $0 \leq r \leq g$.

Characteristic	2			Not 2
2-rank	0	1	2	
Number of singularities	1	2	4	16
Singularity type	Elliptic	D_8	D_4	A_1

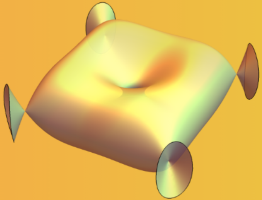
Characteristic 2



Supersingular

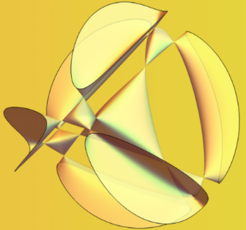


"Almost" Ordinary



Ordinary

Characteristic different than 2



But, what is so special about characteristic 2? Part II

In characteristic 2 we cannot diagonalise the action of $\iota_{\mathcal{C}}$, so it does no longer makes sense to talk about even and odd functions.

So what can be said about the desingularisation of Kummer surfaces in characteristic 2?

Work in progress

Computing

$$\mathcal{L}(2(\Theta_+ + \Theta_-))$$

for genus 2 curves in characteristic 2

Studying the desingularisation of Kummer surfaces

Finding explicit models that can be used for computation

Thank you!

Any questions?