Some elliptic curves from the real world

Bas Edixhoven

Universiteit Leiden

NMC, 2014/04/17 (50 minutes)

Abstract

Elliptic curves are very important in my work in number theory and arithmetic geometry, and so it makes me happy to encounter them as well in other areas of mathematics, and even outside mathematics.

I will give a few examples of elliptic curves showing up in plane geometry (Poncelet), in Escher's "Print Gallery" (de Smit and Lenstra), in classical mechanics (Euler), and in the Guggenheim museum in Bilbao (minimal art by Richard Serra).

The first three examples are well known, but the last one appears to be new.

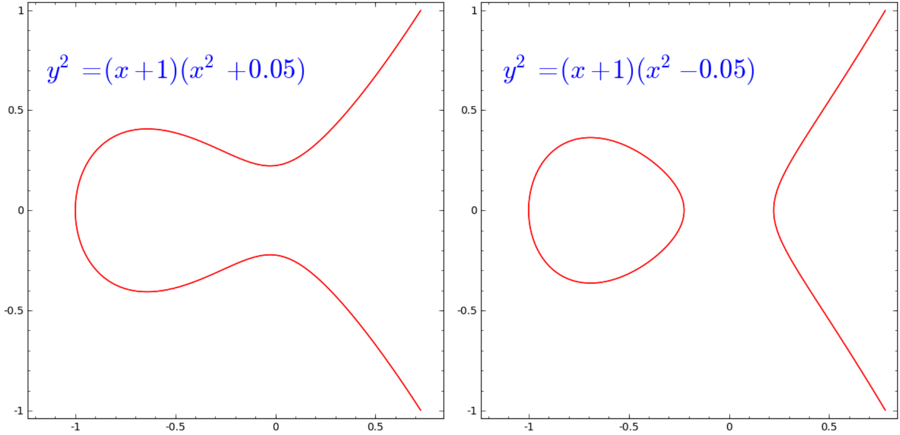
These notes can be downloaded from my homepage (talks/...).

Master students: this lecture is intended to be accessible to you. Please make sure that it is by asking questions, if necessary.

Real Elliptic curves in Weierstrass form

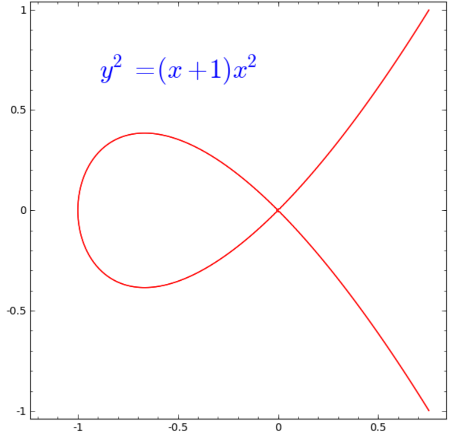
For $a, b \in \mathbb{R}$ with $4a^3 + 27b^2 \neq 0$:

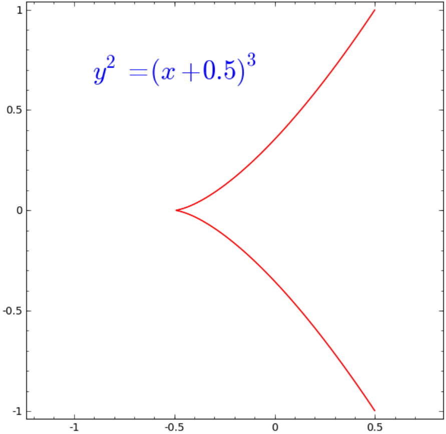
$$\{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\}.$$



Real Elliptic curves in Weierstrass form

$4a^3 + 27b^2 \neq 0 \Leftrightarrow$ the curve is non-singular.





All non-singular degree 3 curves in $\mathbb{R}^2$ can be brought in Weierstrass form by projective transformations.

The algebraic point of view (algebraic geometry)

Closed subvarieties in $\mathbb{R}^n$: solution sets of systems of polynomial equations.

Maps (morphisms) are “locally” given by rational functions without poles.

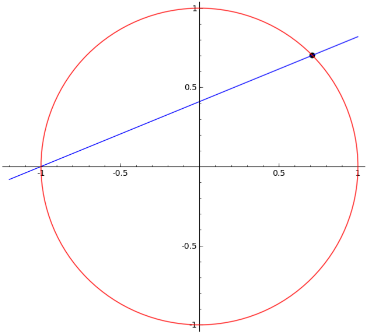
Locally: Zariski topology, the closed subsets are the closed subvarieties.

It is often useful to consider $\mathbb{R}^n \subset \mathbb{C}^n \subset \mathbb{P}^n(\mathbb{C})$: complex projective algebraic geometry.

Instead of $\mathbb{C}$ we can use any algebraically closed field, and, in fact, any ring (commutative, with 1).

Elliptic curves cannot be parametrised

Non-singular degree 2 curves in $\mathbb{R}^2$ are locally isomorphic to $\mathbb{R}$.



Lines through $(-1, 0)$:

$$y = a{\cdot}(x + 1).$$

Second intersection point:

$$\left(\frac{1 - a^2}{1 + a^2}, \frac{2a}{1 + a^2}\right).$$

$$\mathbb{R} \to \text{circle}, \quad a \mapsto \left(\frac{1 - a^2}{1 + a^2}, \frac{2a}{1 + a^2}\right).$$

Fact: elliptic curves cannot be parametrised, even locally. Lines intersect them in 1 or 3 points, if we count with multiplicity and use the "projective plane".

Parallel lines intersect on the horizon: one extra point for each direction in $\mathbb{R}^2$.

$E(\mathbb{R})$ has one point "O" for the vertical direction.

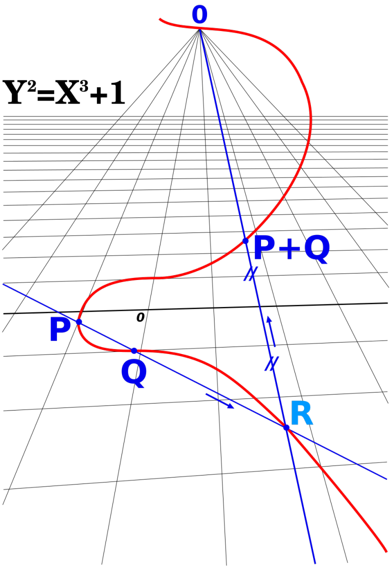
$E(\mathbb{R})$ (including O) has a *binary operation*:

$$E(\mathbb{R}) \times E(\mathbb{R}) \to E(\mathbb{R}),$$

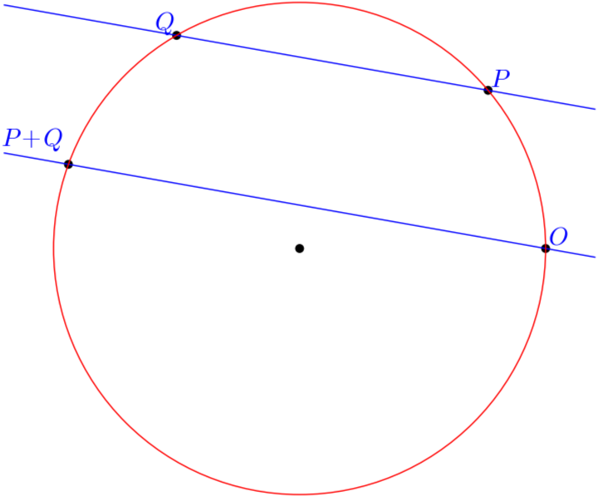
$$(P, Q) \mapsto P + Q.$$

This binary operation makes $E(\mathbb{R})$ into *commutative group*. The associativity is not at all obvious.

(Picture made by: Jean Brette.)



The degenerate case where $E(\mathbb{R})$ is the union of the unit circle and the line at infinity, with $(1, 0)$ as origin.



Conclusion: it is addition of angles!

Hence associative.

Complex elliptic curves, Weierstrass functions

Let $E(\mathbb{C})$ be a complex projective elliptic curve.

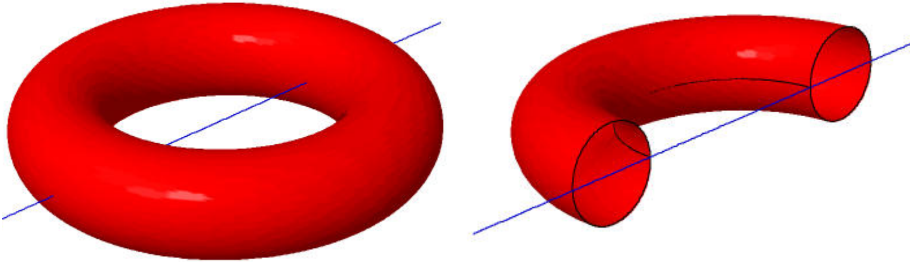
Fact: $E(\mathbb{C})$ is homeomorphic to $S^1 \times S^1$, for three reasons.

Topology. $E(\mathbb{C})$ is compact, oriented, connected and has a Lie group structure, hence a vector field without zeros, hence (Poincaré-Hopf) its Euler characteristic is zero.

Analysis. Weierstrass functions. Let $L \subset \mathbb{C}$ be a lattice. Then $P \colon \mathbb{C} - L \to \mathbb{C}$, $z \mapsto z^{-2} + \sum'_{\lambda \in L}((z-\lambda)^{-2} - \lambda^{-2})$ is L-periodic, and $z \mapsto (P(z), P'(z))$ gives $\mathbb{C}/L \to E(\mathbb{C})$.

Elliptic curves as double cover of $\mathbb{P}^1$

Riemann surfaces. $E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, $(x, y) \mapsto x$ is a 2 to 1 map with 4 ramification points. It is the quotient map for a rotation about 180°.



Automorphisms of elliptic curves

The translations acts transitively: all points are equal.

Fixing one point: automorphisms of E as algebraic group.

$\mathrm{Aut}(E, O)$ is cyclic of order 2, 4, or 6: symmetries of 2-dimensional lattices.

$\mathrm{Aut}(E) = (E, +) \rtimes \mathrm{Aut}(E, O)$.

These are affine transformations: $P \mapsto a(P) + B$, with a in $\mathrm{Aut}(E, O)$ and B in E.

Poncelet

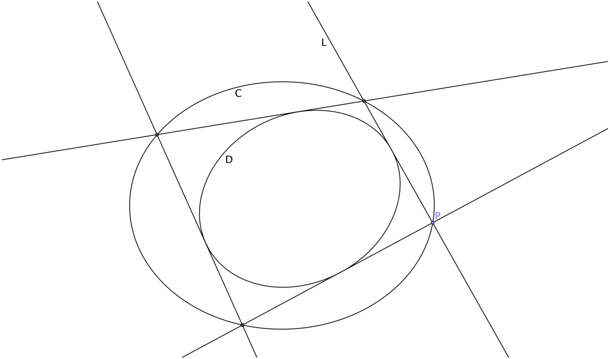
Jean-Victor Poncelet (1788–1867) was a French engineer and mathematician who served most notably as the commandant general of the École polytechnique. He is considered a reviver of projective geometry, and his work Traité des propriétés projectives des figures is considered the first definitive paper on the subject since Gérard Desargues' work on it in the 17th century.

Source: wikipedia.

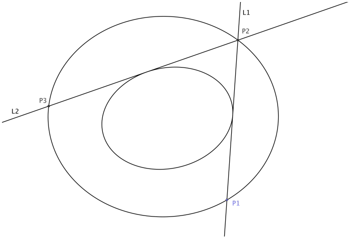
Poncelet's closure theorem, 1822

Let C and D be two plane conics. If it is possible to find, for a given $n > 2$, one n-sided polygon that is simultaneously inscribed in C and circumscribed around D, then it is possible to find infinitely many of them.

In fact, the construction "moves": one can move the starting point on C anywhere.



Proof of Poncelet's closure theorem ("Jacobi", 1826)



$X := \{(P, L) : P \text{ on } C, L \text{ tangent to } D, P \text{ on } L\}$.

$X \to C$, $(P, L) \mapsto P$ has degree 2 and ramifies precisely over the 4 points of $C \cap D$. We have already seen that complex conics are parametrisable by the Riemann sphere. Hence X is an elliptic curve.

Two involutions: $L \cap C = \{P, P'\}$, $\sigma : (P, L) \mapsto (P', L)$,

L and L' tangents through P, $\tau : (P, L) \mapsto (P, L')$.

In terms of group law: $\sigma(x) = -x + b$, $\tau(x) = -x + c$ for some b and c on X. Hence $(\tau \circ \sigma)x = x + (c - b)$, a translation. That explains all.

Remarks

1. If the two ellipses are confocal, then the dynamical system is really an elliptic billiard, with the usual rule of reflection.
2. Bos, Kes, Oort and Raven have written an article on historical aspects: *Poncelet's closure theorem.*
3. Duistermaat has written a whole book on such dynamical systems: *Discrete Integrable Systems, QRT maps and Elliptic Surfaces.*

Classical mechanics: free rotation of a rigid body

Let B be the block in $\mathbb{R}^3$: $|x_1| \leq b_1$, $|x_2| \leq b_2$, $|x_3| \leq b_3$, with a uniform mass distribution. Its center of gravity is at 0. We consider free rotation (no force on B) of B, preserving the center of gravity.

Such movement is given by a map $h\colon \mathbb{R} \to \mathrm{SO}_3(\mathbb{R})$, where $h(t){\cdot}b$ is the position of $b \in B$ at time t.

Main principle of classical mechanics: the movement is determined by position plus speed at time 0. The set of pairs, position and speed, is called the phase space.
In mathematical terms: the movement is given by a vector field on the tangent bundle T of $\mathrm{SO}_3(\mathbb{R})$. Indeed: $\mathrm{SO}_3(\mathbb{R})$ is a 3-dimensional manifold, evidently an algebraic variety. The question is: which vector field?

$T = \{(g, v) : g \in \mathrm{SO}_3(\mathbb{R}),\ v \in T(g)\}$, with $T(g)$ the tangent space of $\mathrm{SO}_3(\mathbb{R})$ at g. Concretely: $\mathrm{SO}_3(\mathbb{R}) \subset \mathrm{M}_3(\mathbb{R}) = \mathbb{R}^9$ defined by 6 equations, $T(g) \subset \mathrm{M}_3(\mathbb{R})$ of dimension 3.

Trivialisation of the tangent bundle

The movement is given by a map $h\colon \mathbb{R} \to T$, $t \mapsto (h(t), h'(t))$.

For g_1 in $\mathrm{SO}_3(\mathbb{R})$, the left translation $g_1\cdot\colon g_2 \mapsto g_1 g_2$ induces an isomorphism $T(g_2) \to T(g_1 g_2)$.

We have Lie $:= T(1) = \{a \in \mathrm{M}_3(\mathbb{R}) : a + a^* = 0\}$, where a^* is the transpose of a.

$$\Phi\colon\ T \to \mathrm{SO}_3(\mathbb{R}) \times \mathrm{Lie}, \quad (g, v) \mapsto (g, g^{-1}v).$$

$$\Phi^{-1}\colon\ \mathrm{SO}_3(\mathbb{R}) \times \mathrm{Lie} \to T, \quad (g, a) \mapsto (g, ga),$$

Write $\Phi \circ h\colon \mathbb{R} \to \mathrm{SO}_3(\mathbb{R}) \times \mathrm{Lie}, \quad t \mapsto (h(t), k(t))$,
where $k\colon \mathbb{R} \to \mathrm{Lie}$.

Euler's equations

Cross product: $\mathbb{R}^3 \times \mathbb{R}^3 \to \text{Lie}$, $(x, y) \mapsto x \times y$.

Angular momentum: $J\colon \text{SO}_3(\mathbb{R}) \times \text{Lie} \to \text{Lie}$,

$$J(a, g) = g \left(\int_{x \in B} x \times (ax) \cdot dx_1\, dx_2\, dx_3 \right) g^{-1} = g\, j(a) g^{-1},$$

with $j\colon \text{Lie} \to \text{Lie}$ self-adjoint and positive definite.

Preservation of angular momentum means that $J \circ \Phi \circ h$ is constant. The dynamics is given by the vector field (Euler's equations):

$$(g, a)' = (ga, j^{-1}[j(a), a]).$$

Remarkable fact: the RHS depends only on a, the dynamical system can be projected to Lie! Reason: the vector field on T is left-invariant, because of symmetry.

Projected Euler's equations in coordinates

We write $a = \begin{pmatrix} 0 & -a_3 & a_2 \\ a_3 & 0 & -a_1 \\ -a_2 & a_1 & 0 \end{pmatrix}$.

The vector field is: $\begin{cases} I_1 a_1' = (I_2 - I_3) a_2 a_3 \\ I_2 a_2' = (I_3 - I_1) a_3 a_1 . \\ I_3 a_3' = (I_1 - I_2) a_1 a_2 \end{cases}$ It is polynomial!

Two conserved quantities:

$$I_1 a_1^2 + I_2 a_2^2 + I_3 a_3^2, \quad \text{kinetic energy,}$$
$$I_1^2 a_1^2 + I_2^2 a_2^2 + I_3^2 a_3^2, \quad \text{length squared of angular momentum.}$$

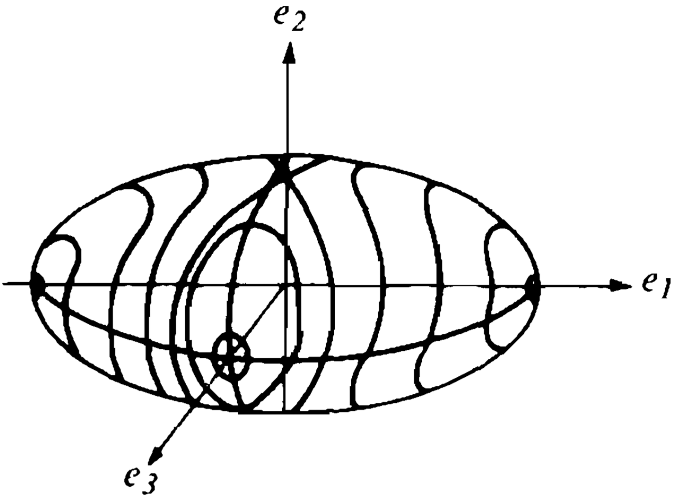
So the movement is over the intersection of the level surfaces: elliptic curves! Indeed, complex projectively, the first quadric is $\mathbb{P}^1 \times \mathbb{P}^1$, and the intersection with the second quadric is a $(2,2)$-curve! So, same situation as with Poncelet.

Moreover: the vector field on these curves is translation invariant. The group given by the flow *is* the addition law, it is algebraic!

Remarks

- Rotation in the plane with constant speed is also algebraic, although the parametrisation is not, but there the group is $SO_2(\mathbb{R})$.
- Explicit solutions involve Weierstrass functions, or other functions parametrising elliptic curves.
- To prove that the vector field is translation invariant, it suffices to see that on the projective complex elliptic curves it has no poles. A simple but annoying computation, and it makes the outcome look like a miracle. Conversely, if one knows that the translations by the flow are algebraic, then one deduces (without computation) that the vector field (on the complex projective curves) has no poles. But this doesn't seem to help, it is just a phenomenon that such algebraic dynamical systems have algebraic group of flow. More advanced way: Lax equations, spectral curves.... This is a very much studied area: integrable systems.

Intersections of 2 ellipsoids, one fixed



Picture from V.A. Arnold's book "Math. Methods of Class. Mech."

Back to dimension 6, a question

The dynamical system on Lie has periodic orbits. Circles for Arnold (analytic point of view), elliptic curves for me (algebraic point of view).

Back to the 6-dimensional system on $SO_3(\mathbb{R}) \times$ Lie.

There are 4 preserved quantities: kinetic energy, and angular momentum.
The map is: $SO_3(\mathbb{R}) \times \text{Lie} \to \mathbb{R} \times \text{Lie}$, $(g, a) \mapsto (K(a), gj(a)g^{-1})$.

The movement is on the fibres of this map. These fibres are of dimension 2, $S^1 \times S^1$ for Arnold, but algebraic circle bundles over elliptic curves for me. The movement is almost never periodic.

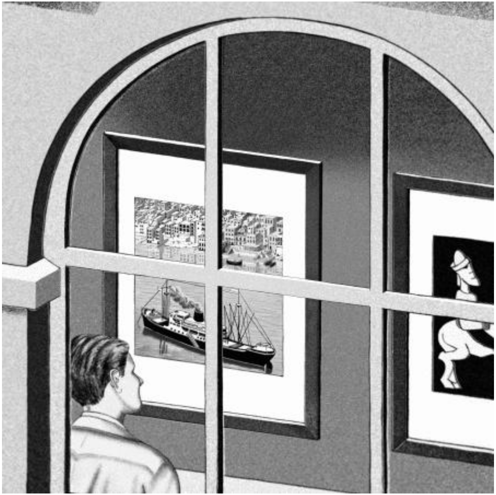
Question: what are these circle bundles, are there algebraic group laws on them such that the vector field is translation invariant? I have not seen the answer to these questions in the literature, although it should be there.

Escher

Source: `http://escherdroste.math.leidenuniv.nl`

Droste-Escher

Escher's print gallery is a transformed Droste picture: the "straight picture" contains a copy of itself, scaled by $q := 1/256$.



A Droste picture is a picture on an elliptic curve!

We view the Droste picture as a function $f\colon \mathbb{C}^\times \to X$, where X is the set of colors.

The self-similarity is then expressed by:

$$\text{for all } t \text{ in } \mathbb{C}^\times,\ f(qt) = f(t).$$

So in fact, f induces a function $\bar{f}\colon \mathbb{C}^\times/q^{\mathbb{Z}} \to X$.

The quotient $\mathbb{C}^\times/q^{\mathbb{Z}}$ is a complex elliptic curve:

1. The annulus $\{t \in \mathbb{C}^\times : q \leq |t| \leq 1\}$ is a fundamental domain.
2. $\exp\colon \mathbb{C} \to \mathbb{C}^\times$, $z \mapsto e^z$ gives $\mathbb{C}^\times = \mathbb{C}/2\pi i\mathbb{Z}$, hence $\mathbb{C}^\times/q^{\mathbb{Z}} = \mathbb{C}/(\mathbb{Z}\cdot 2\pi i + \mathbb{Z}\cdot \log(q))$.

So, on $\mathbb{C}$ we have the picture $\tilde{f}\colon \mathbb{C} \to X$, invariant under the lattice $\mathbb{Z}\cdot 2\pi i + \mathbb{Z}\cdot \log(q) = \mathbb{Z}\cdot i\cdot 6.28\ldots + \mathbb{Z}\cdot 5.55\ldots$.

The lattice-invariant picture on $\mathbb{C}$

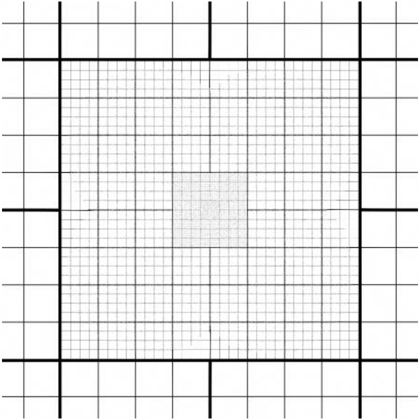
Transforming Droste to Escher

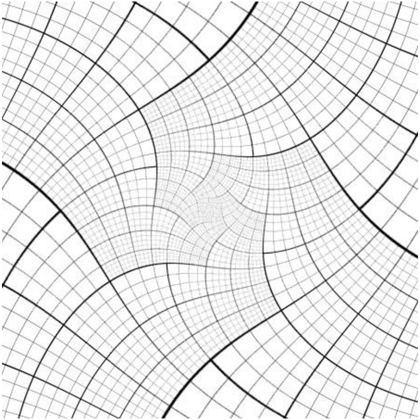
Instead of first dividing out by $\mathbb{Z}{\cdot}2\pi i$, first divide out by $z_1 := 2\pi i - \log(q)$, then by the rest.

So, let $a := 2\pi i/z_1 = 0.5621\ldots + i{\cdot}0.4961\ldots$,
and consider $\mathbb{C} \to \mathbb{C}^\times$, $z \mapsto \exp(az)$.
This maps $\mathbb{Z}{\cdot}z_1$ to 1, and $2\pi i$ to
$q_1 := \exp(2\pi i a) = -0.040946\ldots - i{\cdot}0.01685\ldots$, with
$|q_1| = 1/22.58\ldots$ and $\arg(q_1) = -157.6\ldots^\circ$.

Conclusion: Escher's picture is obtained by applying the multi-valued transformation $t \mapsto t^a = \exp(a\log(t))$ to the Droste picture, that is: $g(t) := f(t^a)$. The resulting picture is invariant under $t \mapsto q_1 t$.

The Droste and Escher grids





See the animation

http://escherdroste.math.leidenuniv.nl/index.php?menu=animation&sub=bmpeg&a=1&b=1

Richard Serra's "torqued ellipse", Guggenheim, Bilbao

How is this surface made?

Let us watch Serra's explanation in
`http://www.youtube.com/watch?v=iRMvqOwtFno&feature=youtube_gdata_player`:
(minutes 16–18).

So, it is obtained from two ellipses in horizontal planes, one on the ground and one at the top, with their long axes in different directions. But Serra did not explain here how the joining is done. The fact however that the side contours of the surfaces are straight lines reveals the joining process.

Each such side contour corresponds to a plane through our eye. Such a plane "touches" both ellipses. Its intersections with the two horizontal planes containing the ellipses are tangent lines of the ellipses.

The surface is a part of the boundary of the convex hull of the union of the two ellipses.

How is this surface made?

The surface is the union of lines that join points of the two ellipses where the tangent lines are parallel.

Serra describes it mechanically:
`http://www.youtube.com/watch?v=G-mBR26bAzA`
Start at 1:35.

So he rolls a plane around the ellipses, or rolls his wheel on a sheet of lead.

What is it to an algebraic geometer?

First question: is it algebraic? Can it be described by a polynomial equation?

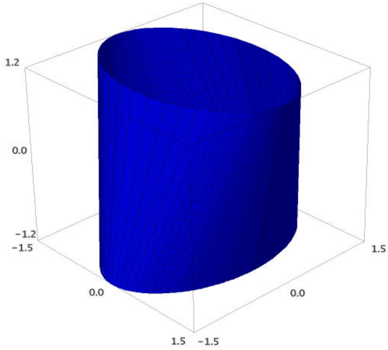
Yes! Well,... half.

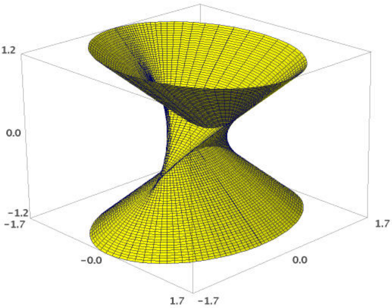
There is an irreducible F in $\mathbb{R}[x, y, z]$, of degree 8 (I computed this in two ways), such that Serra's surface is half of the zero set of F. I do not know F.

The other half consists of lines joining a point below to the "opposite" of the point above: opposite points have parallel tangents.

These two halves cannot be separated algebraically, Serra's surface has a siamese twin.

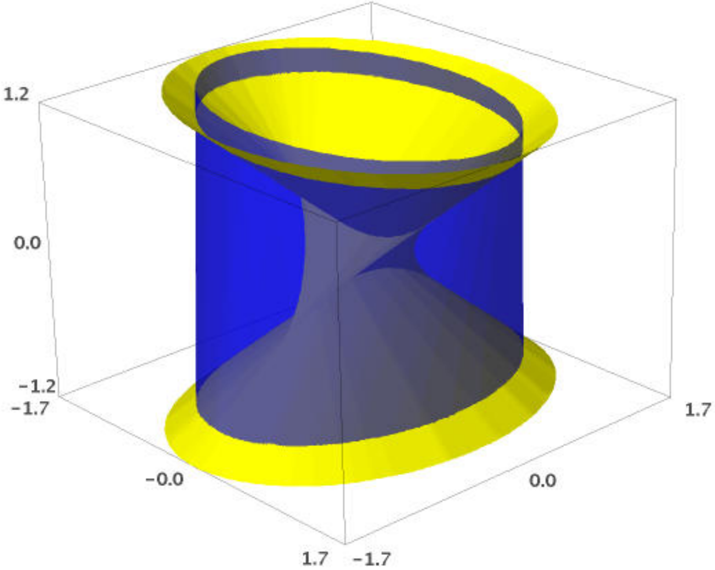
Siamese twins, apart





Pictures and computations by sage.

Siamese twins, together



Parametrisation by an elliptic curve

Let C_1 and C_2 be the two ellipses, in their planes H_1 and H_2.

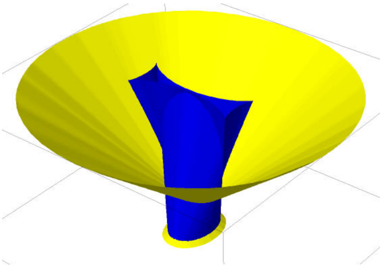
For P_i on C_i, let $T_{C_i}(P_i)$ be the tangent of C_i at P_i.

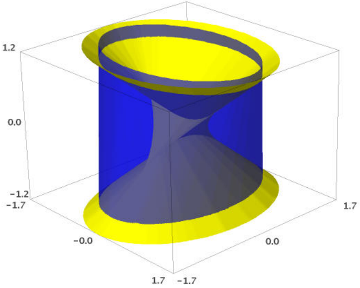
Then $E := \{(P_1, P_2) : P_1 \in C_1,\ P_2 \in C_2,\ T_{C_1}(P_1) \text{ and } T_{C_2}(P_2) \text{ parallel}\}$ is an elliptic curve.

Proof: use complex projective geometry. $L := H_1 \cap H_2$.
Then we have $p_i \colon C_i \to L$, $p_i\{P_i\} = L \cap T_{C_i}(P_i)$,
p_i is a degree 2 cover, ramified over $C_i \cap L$, two points,
long axes of C_1 and C_2 not parallel implies $C_1 \cap C_2 = \emptyset$.
Hence $E \to C_i$ is of degree 2, and ramifies over 4 points. Q.E.D.

$E(\mathbb{R})$ is homeomorphic to $S^1 \coprod S^1$.
Serra's surface S is parametrised by a $\mathbb{P}^1$-bundle over E, in fact by $\mathbb{P}^1 \times E$.
In technical terms: the normalisation is $\mathbb{P}^1 \times E$.

Some more pictures, and an automorphism

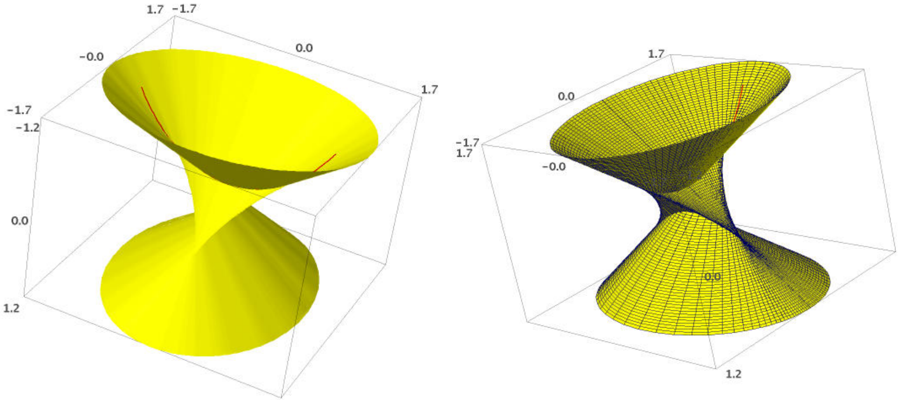




The singularities suggest that there is an automorphism of S exchanging blue and yellow.

Indeed (Maarten Derickx): the reflection in $\mathbb{P}^3$ with respect to the plane H_1 and the center of C_2 does this.

A one-dimensional part of $S(\mathbb{R})$



The red ellipse is part of $S(\mathbb{R})$! Only a segment of it is in the yellow part.
It is explained by conjugate intersecting lines.

Some metric properties

Away from the singularities, the yellow and blue surfaces have Gaussian curvature zero: they are locally convex, and are ruled. The Gaussian curvature is the product of the two main curvatures, one of which is zero.

Minding's theorem (1839) says that locally, the surface is isometric to the plane.

Intuitively this means: the surface can roll on the plane, giving a mathematical explanation of Serra's wheel.

The yellow part is obtained by letting one ellips roll on top of the paper, and the other below it!

Hard to imagine, but we can imagine the case of two circles, giving a cone. The cone can roll on the plane.

3D-printing

Oliver Labs is a mathematician in Mainz, with an interest in computer science and design.
He converted my Sage output to input for a 3d-printer, so that I could have it printed by Shapeways.
Check it out!

http://www.oliverlabs.net/

http://www.shapeways.com/art/mathematical-art?li=nav

Thanks

- Thanks to Robert-Jan Kooman for conversations on Euler's equations.
- Thanks to Ton Van de Ven for quite a few conversations about Serra's work.
- To Maarten Derickx for the automorphism exchanging Serra's surface and its twin.
- To Oliver Labs for 3d-printing it from my sage output.
- To you for your attention!