Around cubic hypersurfaces

Olivier Debarre

June 23, 2015

Abstract

A cubic hypersurface X is defined by one polynomial equation of degree 3 in n variables with coefficients in a field $\mathbf{K}$, such as

$$1 + x_1^3 + \cdots + x_n^3 = 0.$$

One is interested in the set $X(\mathbf{K})$ of solutions $(x_1, \ldots, x_n)$ of this equation in $\mathbf{K}^n$. Depending on the field $\mathbf{K}$ (which may be for example $\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$, or a finite field) one may ask various questions: is $X(\mathbf{K})$ nonempty? How large is it? What is the topology of $X(\mathbf{K})$? What is its geometry? Can one parametrize $X(\mathbf{K})$ by means of rational functions? This is a very classical subject: elliptic curves (which are cubics in the plane) and cubic surfaces have fascinated mathematicians from the 19^{th} century to the present day. Plaster models of the Clebsch cubic surface still decorate many mathematics libraries (or cafeterias, as in Düsseldorf) around the world. However, simple questions about cubics still remain unanswered, although actively researched. I will explain some classical facts about cubic hypersurfaces and give some answers to the questions asked above.

Contents

1 Introduction

Let $\mathbf{K}$ be a field. A hypersurface X (of dimension $n-1$) is a nonzero polynomial equation

$$F(x_1, \ldots, x_n) = 0$$

in n variables with coefficients in $\mathbf{K}$ (we allow multiplication of F by a nonzero scalar). We may consider the set of solutions of this equation in any field $\mathbf{L}$ with contains the coefficients of F, we will then write $X(\mathbf{L})$ for this set and we will say that X is *defined over* $\mathbf{L}$.

If d is the degree of F, one says that X is a hypersurface *of degree d.* Hypersurfaces of degree 1 are just linear affine hyperplanes. Hypersurfaces of degree 2 are called *quadrics* (*conics* if $n = 2$), hypersurfaces of degree 3 are called *cubics,* then we have *quartics, quintics,* and so on.

Here are a few questions one can ask:

- describe the geometry of $X(\mathbf{K})$, for example, the lines that it contains;
- describe the points of $X(\mathbf{K})$: are there any ? If yes, count them ($\mathbf{K}$ finite) or parametrize them;
- describe the topology of $X(\mathbf{K})$ ($\mathbf{K} = \mathbf{R}$ or $\mathbf{C}$).

2 Quadrics

2.1 Parametrization of nonempty conics

Let us begin with conics X. They may be empty, such as the conics

$$(x^2 + y^2 + 1 = 0) \subset \mathbf{R}^2 \qquad \text{or} \qquad (x^2 + y^2 - 7 = 0) \subset \mathbf{Q}^2.$$

But if $X(\mathbf{K})$ contains one point O, one may parametrize $X(\mathbf{K})$ by rational functions by

$$\begin{array}{ccc} \mathbf{K} & \to & X(\mathbf{K}) \\ t & \longmapsto & \begin{array}{c}\text{intersection point with } X \text{, other than } O\text{,} \\ \text{of the line through } O \text{ with slope } t. \end{array} \end{array}$$

The point here if that the restriction of the equation F of X to any such line is a quadratic equation with coefficients in $\mathbf{K}$ and one root in $\mathbf{K}$ (corresponding to O), so the other root in also in $\mathbf{K}$.

This parametrization is injective except when X is the union of two lines passing through O.

Example 1 The point $O = (1, 0)$ is on the conic X with equation $x^2 - y^2 - 1 = 0$. When the characteristic is not 2 (when the characteristic is 2, X is the line $y = x + 1$,"counted twice"), the process above gives the parametrization

$$\begin{array}{ccc} \mathbf{K} & \dashrightarrow & X(\mathbf{K}) \\ t & \longmapsto & \left(\dfrac{1+t^2}{1-t^2}, \dfrac{2t}{1-t^2}\right) \end{array}$$

which is not defined at $t = \pm 1$ and reaches all points of $X(\mathbf{K})$ except O (it corresponds to "$t = \infty$").

2.2 Projective conics

The parametrization above can be extended if one adds "points at infinity", i.e., if we work in the projective plane $\mathbf{P}^2$. A point in $\mathbf{P}^2(\mathbf{K})$ has projective coordinates $(x : y : z)$, not all zero and defined up to multiplication by a nonzero scalar. A point $(x, y) \in \mathbf{K}^2$ has projective coordinates $(x : y : 1)$ and points with $z = 0$ are then called points at infinity.

In our previous example (where we assume $\mathrm{char}(\mathbf{K}) \neq 2$), the equation of the "closure" $\overline{X}$ of X in $\mathbf{P}^2$ is obtained by homogenizing the equation of X as

$$x^2 - y^2 - z^2 = 0.$$

Note that the vanishing of this quantity does not depend on the choice of homogeneous coordinates. The projective conic $\overline{X}$ has two points at infinity, $(0 : 1 : 1) = (0 : -1 : -1)$

and $(0:1:-1)=(0:-1:1)$; they correspond to the directions of the two asymptotes of X. One can extend the parametrization as a well defined injective map

$$\begin{array}{rcl} \mathbf{K} & \longrightarrow & \overline{X}(\mathbf{K}) \\ t & \longmapsto & (1+t^2:2t:1-t^2) \end{array}$$

and even better, to an isomorphism

$$\begin{array}{rcl} \mathbf{P}^1(\mathbf{K}) & \longrightarrow & \overline{X}(\mathbf{K}) \\ (t:u) & \longmapsto & (u^2+t^2:2tu:u^2-t^2). \end{array}$$

The advantage of projectivizing is that, by the theory of quadratic forms, the equation of any projective conic can now be reduced, after a change of projective coordinates, to a sum of squares

$$ax^2+by^2+cz^2=0.$$

We assume $abc \neq 0$; this is equivalent to saying that the curve $\overline{X}$ has no singular point (i.e., is *smooth*) in the sense of differential geometry.

2.3 Topology

Case $\mathbf{K}=\mathbf{R}$. In the projective setting, and with the notation above, we may assume $a,b,c=\pm 1$. If a, b, c all have the same signs, the conic if empty; otherwise, we may assume that its equation is

$$x^2-y^2-z^2=0.$$

So, topologically, all smooth nonempty projective real conics are the same. This conic does not meet the " line at infinity" $x=0$. It is therefore contained in its complement, which we identify with $\mathbf{R}^2$ by taking $x=1$. There, it is the circle

$$y^2+z^2=1.$$

Topologically, all smooth nonempty projective real conics are $\mathbf{S}^1$ (which agrees with the fact that they are parametrized by $\mathbf{P}^1(\mathbf{R})=\mathbf{R}\cup\{\infty\}\simeq\mathbf{S}^1$).

Now it is well known that apart from degenerate cases, a real conic is either an ellipse, a parabola, or a hyperbola. Their projective closures are all " the same": one add respectively no points for an ellipse, the point at infinity corresponding to the direction of the axis for a parabola, the points at infinity corresponding to the directions of the two asymptotes for a hyperbola.

Case $\mathbf{K}=\mathbf{C}$. A smooth projective complex conic has equation

$$x^2+y^2+z^2=0$$

in suitable projective coordinates. It is topologically $\mathbf{P}^1(\mathbf{C})=\mathbf{C}\cup\{\infty\}\simeq\mathbf{S}^2$.

2.4 Counting points over finite fields

We assume $\mathbf{K} = \mathbf{F}_q$, a finite field of characteristic $\neq 2$.

From the (elementary) theory of quadratic forms over finite fields, we know that a smooth projective conic over $\mathbf{F}_q$ has, in suitable projective coordinates, equation

$$x^2 + y^2 + z^2 = 0 \quad \text{or} \quad x^2 + y^2 + cz^2 = 0,$$

where $c \in \mathbf{F}_q - \mathbf{F}_q^2$. It always has a point in $\mathbf{F}_q$: the set $\mathbf{F}_q^2$ of squares in $\mathbf{F}_q$ has cardinality $(q+1)/2$, hence so has the set $S_a = \{-1 - az^2 \mid z \in \mathbf{F}_q\}$, for any $a \in \mathbf{F}_q - \{0\}$. Hence S_a must meet $\mathbf{F}_q^2$ and the statement follows.

It follows from the above parametrization that a smooth projective conic over $\mathbf{F}_q$ has the same number of points as $\mathbf{P}^1(\mathbf{F}_q) = \mathbf{F}_q \cup \{\infty\}$ that is, $q+1$ points.

2.5 Quadrics

Similar remarks can be made about quadric hypersurfaces, although there are some differences. One may compactify them as projective quadrics $\overline{X}$ in $\mathbf{P}^n$, whose equation can be written, in suitable projective coordinates, as

$$a_0 x_0^2 + \cdots + a_n x_n^2 = 0,$$

with $a_0 \cdots a_n \neq 0$ if and only if $\overline{X}$ is smooth. When this quadric is nonempty, one gets in the same way a parametrization

$$\mathbf{K}^{n-1} \dashrightarrow \overline{X}(\mathbf{K})$$

which is not defined everywhere (hence the dotted arrow) and which is moreover not injective.

For smooth quadric surfaces, when the equation can be put in the form

$$x_0 x_1 - x_2 x_3 = 0$$

(this is always the case when $\mathbf{K}$ is algebraically closed, or when $\mathbf{K} = \mathbf{R}$ and the signature is $(2,2)$, or when $\mathbf{K}$ is finite and the quadric is the standard quadric $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$), we have an injective parametrization

$$\begin{array}{rcl} \mathbf{K}^2 & \longrightarrow & \overline{X}(\mathbf{K}) \\ (t, t') & \longmapsto & (tt' : 1 : t : t'). \end{array}$$

which extends to an isomorphism

$$\begin{array}{rcl} \mathbf{P}^1(\mathbf{K}) \times \mathbf{P}^1(\mathbf{K}) & \longrightarrow & \overline{X}(\mathbf{K}) \\ \big((t : u), (t' : u')\big) & \longmapsto & (tt' : uu' : tu' : t'u). \end{array}$$

We say that this quadric is ruled (by lines) in two different ways.

When $\mathbf{K} = \mathbf{R}$, a quadric of signature $(2,2)$ is therefore topologically $\mathbf{S}^1 \times \mathbf{S}^1$. When the signature is $(1,3)$ or $(3,1)$, it is a sphere $\mathbf{S}^2$.

3 Cubic curves

The situation for cubics is more complicated because there is no standard form for their equation similar to the one obtained for quadrics from the theory of quadratic forms. In some sense (over an algebraically closed field), all smooth quadrics are the same, but smooth cubics are not.

Smooth cubic curves were studied intensively in the 19$^{\text{th}}$ century. Some are empty, such as the cubic

$$3x^3 + 4y^3 + 5 = 0$$

in $\mathbf{Q}^2$ (this is not easy to show; in general, there is no known method to determine in a finite number of steps whether a cubic equation with rational coefficients in two variables has a rational solution).

If $X \subset \mathbf{P}^2$ is a *smooth* projective cubic curve defined over a finite field $\mathbf{F}_q$, Hasse's estimate

$$|\operatorname{Card}(X(\mathbf{F}_q)) - q - 1| \leq 2\sqrt{q}$$

implies that X is nonempty! If X is not smooth, it might have no points: the projective cubic

$$x_1^3 + x_2^3 + x_3^3 + x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 + x_1 x_2 x_3 = 0$$

has no points over $\mathbf{F}_2$ (over the field $\mathbf{F}_8$, it is the union of 3 lines permuted by the action of the Galois group $\mathbf{Z}/3\mathbf{Z}$).

3.1 Elliptic curves

If a smooth cubic curve contains a point O, one can perform a change of coordinates to put its equation in a Weierstraß form (we assume for simplicity that the characteristic of the field $\mathbf{K}$ is neither 2 nor 3)

$$y^2 = x^3 + ax + b.$$

Smoothness then corresponds to the condition $4a^3 + 27b^2 \neq 0$ (so that the polynomial x^3+ax+b has three distinct roots in an algebraic closure of $\mathbf{K}$). Note that if $\mathbf{K}$ is algebraically closed, we may also write the equation as (Legendre form)

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

and smoothness is then equivalent to $\lambda \in \mathbf{K} - \{0,1\}$.

A smooth (projective) cubic curve with a point is called an *elliptic curve.*

One can, as we did for conics, homogenize the Weierstraß equation into

$$y^2 z = x^3 + axz^2 + bz^3$$

and the point $O = (0:1:0)$ is the (only) "point at infinity" of the elliptic curve.

3.2 Parametrization

The first difference with conics is that elliptic curves cannot be parametrized by rational functions.

Proposition 2 *An elliptic cubic cannot be parameterized by rational functions.*

PROOF. We may assume that $\mathbf{K}$ is algebraically closed. Given a Legendre equation as above, we need to show that we cannot find non constant polynomials $P, Q, R, S \in \mathbf{K}[T]$ with $P \wedge Q = R \wedge S = 1$ such that

$$(R/S)^2 = (P/Q)((P/Q) - 1)((P/Q) - \lambda).$$

Clearing denominators, we obtain

$$R^2 Q^3 = S^2 P(P - Q)(P - \lambda Q)$$

so that $S^2 \mid Q^3$ and $Q^3 \mid S^2$, hence $S^2 = Q^3$ (after adjusting the scalars) and

$$R^2 = P(P - Q)(P - \lambda Q).$$

Since the factors in the right-hand side are mutually coprime, we obtain, by unique factorization in $\mathbf{K}[T]$, that P, $P - Q$, and $P - \lambda Q$ are all squares, and so is Q since Q^3 is.

Now we prove that if $P, Q \in \mathbf{K}[T]$ are coprime and such that four different nonzero linear combinations $a_i P + b_i Q$ are squares, P and Q are constant.

By changing P and Q into $aP + bQ$ and $cP + dQ$, with $ad - bc \neq 0$, we may assume that the four different linear combinations are P, Q, $P - Q$, and $P - \lambda Q$. Write $\lambda = \mu^2$ and $P = U^2$ and $Q = V^2$, so that $P - Q = (U + V)(U - V)$ and $P - \lambda Q = (U + \mu V)(U - \mu V)$. Then U and V are coprime and, by unique factorization in $\mathbf{K}[T]$, $U + V$, $U - V$, $U + \mu V$ and $U - \mu V$ are all squares. By, if P and Q are not both constant, we have $\deg(U) + \deg(V) = \frac{1}{2}(\deg(P) + \deg(Q)) < \deg(P) + \deg(Q)$. So we can repeat the process and get a contradiction (this is Fermat's method of "descente infinie"). $\square$

3.3 The group law

The most beautiful fact about elliptic curves is that they can be made into abelian groups. If a cubic X is defined by a Weierstraß or Legendre equation, the group law on the set $X(\mathbf{K})$ is defined by

$$P + Q + R = 0 \iff P, Q, R \text{ are on a line.}$$

The neutral element is O, the point at infinity (this means that $-P$ is the reflection of P about the x axis).

Points of order 2 correspond to points where the tangent is vertical, i.e., to the roots of the polynomial $x^3 + ax + b$ (there are either none, or 1, or 3). In Legendre form, they are $(0, 0)$, $(1, 0)$, and $(\lambda, 0)$.

Points of order 3 correspond to inflection points. They form a finite set $E[3]'$ with the property that the given any two points in $E[3]'$, there is a third point in $E[3]'$ collinear with the first two points.

It is a tricky exercise to show that such a set in $\mathbf{R}^2$ consists of collinear points. In particular, there are at most 2 real points of order 3.

Case $\mathbf{K} = \mathbf{R}$. If E is a real (projective) elliptic curve, it is known that the group $E(\mathbf{R})$ is (as a topological group) $\mathbf{R}/\mathbf{Z}$ when the polynomial $x^3 + ax + b$ has a single real root, and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{R}/\mathbf{Z}$ when it has 3 distinct real roots (there are then two connected components).

Case $\mathbf{K} = \mathbf{C}$. If E is a complex elliptic curve, $E(\mathbf{C})$ is (as a topological group) $\mathbf{R}/\mathbf{Z} \times \mathbf{R}/\mathbf{Z}$ (a torus $\mathbf{S}^1 \times \mathbf{S}^1$).

Case $\mathbf{K} = \mathbf{F}_q$. We already mentioned Hasse's estimate: if E is an elliptic curve over $\mathbf{F}_q$, one has

$$|\operatorname{Card}(E(\mathbf{F}_q)) - q - 1| \leq 2\sqrt{q}.$$

Example 3 Consider the elliptic curve E with Weierstraß equation $y^2 = x^3 + x + 1$. It is smooth over $\mathbf{F}_5$ $(4 \cdot 1^3 + 27 \cdot 1^2 = 1 \neq 0)$ and one can list all its points:

$$(0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2),$$

to which one should add the point at infinity $O = (0 : 1 : 0)$. So there is a total of 9 points in $E(\mathbf{F}_5)$. Call them $\pm P$, $\pm Q$, $\pm R$, $\pm S$, and O.

Let us compute $P + P$. The tangent to E at $P = (0, 1)$ has slope given by $2dy = dx$, i.e., $1/2 = 3$, hence its equation is $y - 1 = 3x$. Substituting in the equation of the cubic, we obtain

$$4x^2 + x + 1 = x^3 + x + 1.$$

This polynomial has a double root $x = 0$, as expected, and another root $x = 4$. We have then $y = 3 \cdot 4 + 1 = 3$ and $P + P + (4, 3) = 0$, so that $2P = S$. Similarly, we obtain $P + S + (2, -1) = 0$, hence $3P = Q$. In particular, P does not have order 3, hence $(E(\mathbf{F}_5), +) \simeq \mathbf{Z}/9\mathbf{Z}$.

Case $\mathbf{K} = \mathbf{Q}$. If E is an elliptic curve over $\mathbf{Q}$, the group $E(\mathbf{Q})$ of its rational points is an abelian group of finite type (Mordell's theorem): it has a (finite) rank and a torsion part. The possible torsion parts are known, but not the possible ranks: the highest exactly known rank is 19 (Elkies constructed in 2006 an elliptic curve over $\mathbf{Q}$ with rank ≥ 28). For some time, people expected the ranks to be unbounded, but this would contradict other conjectures in algebraic geometry, so this belief may not be widely shared anymore.

The group structure is a way to produce many rational points using the addition law.

Example 4 The elliptic curve E with Weierstraß equation $y^2 = x^3 + 1$ is smooth over $\mathbf{Q}$. It has exactly 5 points

$$(-1, 0), (0, \pm 1), (2, \pm 3),$$

to which one should add the point at infinity $O = (0 : 1 : 0)$. So there is a total of 9 points in $E(\mathbf{Q})$. Call them P, $\pm Q$, $\pm R$, and O. One checks (it is easy to see that from the graph once you know there are so few points!) $2R = Q$, $3R = Q + R = P$, and $2P = 0$ (or directly $3Q = 0$ because Q is an inflection point). Hence $(E(\mathbf{Q}), +) \simeq \mathbf{Z}/6\mathbf{Z}$ is generated by R.

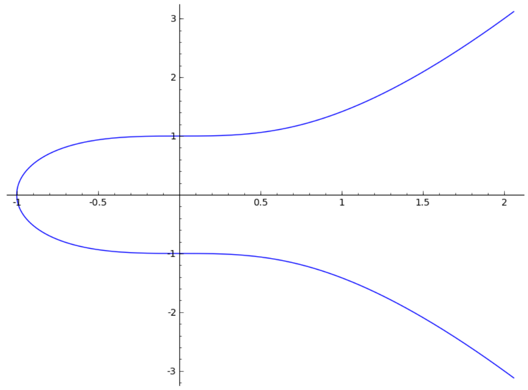

Figure 1: The elliptic curve $y^2 = x^3 + 1$

Example 5 The elliptic curve E with Weierstraß equation $y^2 = x^3 - x = x(x-1)(x+1)$ is smooth over $\mathbf{Q}$. It has exactly 3 points

$$(-1, 0), (0, 0), (1, 0),$$

to which one should add the point at infinity $O = (0 : 1 : 0)$. They are all of order 2 and $(E(\mathbf{Q}), +) \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

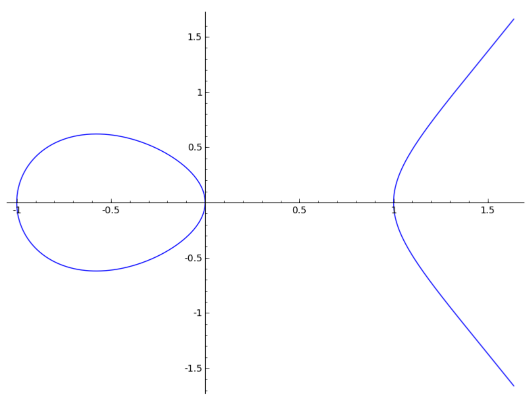

Figure 2: The elliptic curve $y^2 = x^3 - x$

Example 6 The elliptic curve E with Weierstraß equation $y^2 = x^3 - x + 1$ is smooth over $\mathbf{Q}$. The point $P = (1, 1)$ generates $(E(\mathbf{Q}), +) \simeq \mathbf{Z}$, and $2P = (-1, 1)$, $3P = (0, -1)$, $4P = (3, -5)$, $5P = (5, 11)$, $6P = (\frac{1}{4}, \frac{7}{8}), \ldots$

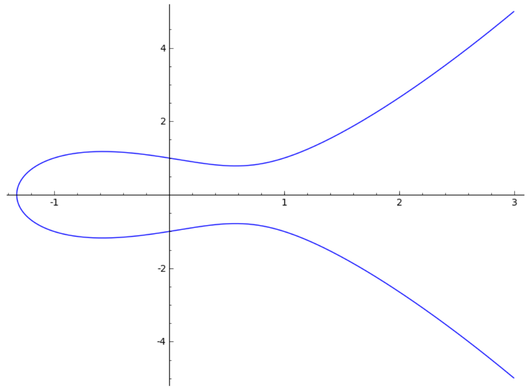

Figure 3: The elliptic curve $y^2 = x^3 - x + 1$

3.4 Elliptic curves and cryptography

The Diffie–Hellman key exchange[1] is based on the mathematical fact that, given a known cyclic group G and generator $g \in G$, it may be difficult to recover an integer r from the knowledge of $g^r \in G$ (this is called the discrete logarithm problem).

It works as follows. Alice and Bob agree on the pair (G, g). Alice chooses a secret random integer a and sends g^a to Bob. Similarly, Bob chooses a secret random integer b and sends g^b to Alice. Alice then computes $(g^b)^a$ and Bob computes $(g^a)^b$. This common element g^{ab} of G will be used as an encryption key. Note that its inverse can be computed by Alice as $(g^b)^{|G|-a}$ and by Bob as $(g^a)^{|G|-b}$.

The data G, g, g^a, and g^b are all publicly known (or can be eavesdropped). The number a is only known to Alice, the number b is only known to Bob, and g^{ab} is only known to Alice and Bob.

Given a message, Alice transforms it into an element m of G. She then encrypts it as $e = mg^{ab}$ and sends it to Bob, who will decrypt it by computing $e(g^{ab})^{-1}$. The numbers a and b are discarded at the end of the session.

The group G can be chosen to be the cyclic multiplicative group $(\mathbf{Z}/p\mathbf{Z})^\times$, for some large prime p. If one chooses a generator g of $(\mathbf{Z}/p\mathbf{Z})^\times$, it is computationally difficult (impossible for modern supercomputers to do in a reasonable amount of time) to recover the integer r from the number $g^r \pmod p$.

In elliptic curve cryptography,[2] one chooses an elliptic curve E in Weierstraß form defined over a finite field $\mathbf{F}_q$ such that the group $G = E(\mathbf{F}_q)$ is cyclic of finite order, usually a large prime, and a generator $P \in E(\mathbf{F}_q)$, given by its coordinates. These data are difficult

[1]Named after Whitfield Diffie and Martin Hellman, who first described that system in an article in 1976, after the concept was developed by Ralph Merkle in 1975. By 1975, James H. Ellis, Clifford Cocks, and Malcolm J. Williamson had also shown how public-key cryptography could be achieved, but their work was kept secret until 1997.

[2]Suggested by Neal Koblitz and Victor S. Miller in 1985.

to produce, so they are made publicly available by standard trusted bodies.[3] The scheme is based on the fact that although it is rather easy to compute the multiples P, it is impossible in general to find r given rP. It is also more efficient than using $(\mathbf{Z}/p\mathbf{Z})^\times$, in the sense that it provides the same level of security with much smaller key size.

4 Cubic surfaces

We saw that some smooth cubic curves have no points over a finite field. This does not happen for cubic projective surfaces because of the following result.

Theorem 7 (Chevalley–Warning) *Let $\mathbf{K}$ be a finite field of characteristic p and let F be a polynomial of degree d in m variables. If $d < m$, the number of solutions in $\mathbf{K}^m$ of the equation*

$$F(x_1, \ldots, x_m) = 0$$

is divisible by p.

A refinement of this theorem (Ax–Katz) says that the number of solutions is in fact divisible by q.

Apply this result to the homogenization of the equation of a cubic surface: it is a polynomial of degree 3 in 4 variables with the obvious root $(0, \ldots, 0)$. By the Chevalley–Warning theorem, there must be some other point, which gives a point in the associated projective surface.

This result is optimal. For example, the projective cubic surface in $\mathbf{P}^3(\mathbf{F}_2)$ defined by the homogeneous equation

$$x_1^3 + x_2^3 + x_3^3 + x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1x_2x_3 + x_1x_4^2 + x_1^2x_4 = 0$$

is smooth and has a unique $\mathbf{F}_2$-point, $(0 : 0 : 0 : 1)$ (but this is the only example of a smooth projective cubic surface defined over a finite field with a single point; in particular, this does not happen on a smooth cubic surface over a finite field with more than 2 elements).

4.1 Lines on cubic surfaces

Cayley wrote in a 1869 memoir that any smooth complex cubic surface contains exactly 27 projective lines. I cannot resist quoting here Ron Donagi and Roy Smith (1981):

Wake an algebraic geometer in the dead of night, whispering: "27".
Chances are, he will respond: "lines on a cubic surface."

to show the importance of this result, which is by no means easy to prove. The miracle here is that all smooth cubic surfaces, over any algebraically closed field, contain exactly 27 lines

[3] One of these bodies is the NSA, which perhaps should not be trusted.

(singular cubics contain less than 27 lines, unless they are cones). The configuration of these lines (how they intersect) is also the same. On explicit examples, these lines are sometimes easy to find, but not always.

Diagonal cubics. Consider a diagonal cubic surface X in $\mathbf{P}^3$ with homogeneous equation

$$a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_4^3 = 0,$$

where $a_1, \dots, a_4 \in \mathbf{K}$ are all nonzero. It is smooth whenever $\mathbf{K}$ is not of characteristic 3, which we assume. Let b_{ij} be such that $b_{ij}^3 = a_i/a_j$. Then, if $\{1,2,3,4\} = \{i,j,k,l\}$, the projective line joining $e_i - b_{ij}e_j$ and $e_k - b_{kl}e_l$ is contained in X. Since we have 3 choices for $\{i,j\}$ and 3 choices for each b_{ij}, the 27 lines of the cubic X are all obtained in this fashion hence are defined over $\mathbf{K}[\sqrt[3]{a_i/a_j}, 1 \le i < j \le 4]$.

In particular, the 27 lines of the Fermat cubic

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 = 0$$

are defined over $\mathbf{Q}[\exp(2i\pi/3)]$ (9 of them are defined over $\mathbf{Q}$; the other 18 come in complex conjugate pairs).

In characteristic 2, the 27 lines on the Fermat cubic are all defined over $\mathbf{F}_4$ (but only 3 of them are defined over $\mathbf{F}_2$), whereas, if $a \in \mathbf{F}_4 - \{0,1\}$, the cubic surface defined by

$$x_1^3 + x_2^3 + x_3^3 + ax_4^3 = 0 \tag{1}$$

contains no lines defined over $\mathbf{F}_4$ (they are defined over $\mathbf{F}_{64}$).

Real lines. The 27 complex lines contained in a smooth real (projective) cubic surface X are either real or come in complex conjugate pairs. Since 27 is odd, X always contains a real line. In fact, one can prove that X contains exactly 3, 7, 15, or 27 real lines (actually, lines on real cubic surfaces should be counted with signs, in which case one gets that the total number is always 3).

In many mathematics departments around the world, there are plaster models of (real!) cubic surfaces with 27 (real) lines on them; it is usually the Clebsch cubic (1871), with equations in $\mathbf{P}^4$:

$$x_0 + \cdots + x_4 = x_0^3 + \cdots + x_4^3 = 0.$$

These 27 lines can be determined explicitly: 15 are defined over $\mathbf{Q}$, and the other 12 over the field $\mathbf{Q}(\sqrt{5})$.

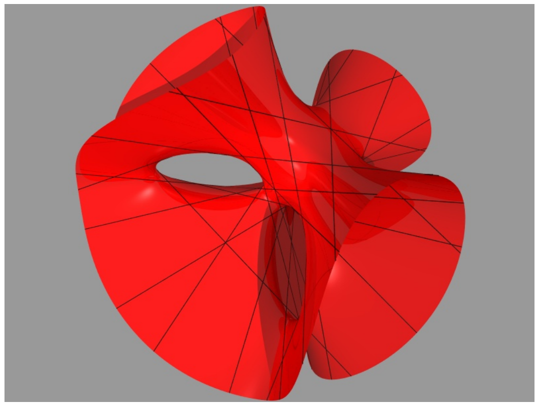

Figure 4: The Clebsch cubic with its 27 real lines

Rational lines. It is only recently that a rational cubic surface with all its 27 lines rational was found (Tetsuji Shioda, 1995). Its equation is

$$x_2^2 x_4 + 2x_2 x_3^2 = x_1^3 - x_1(59475x_4^2 + 78x_3^2) + 2848750x_4^3 + 18226x_3^2 x_4.$$

All 27 lines have explicit rational equations.

4.2 Parametrization

Let $X \subset \mathbf{P}^3$ be a smooth cubic surface and assume that it contains two disjoint lines L_1 and L_2 (this is always the case when the field is algebraically closed). One has an injective parametrization

$$\begin{array}{rcl} \Phi : L_1 \times L_2 & \dashrightarrow & X \\ (x_1, x_2) & \longmapsto & \begin{array}{c}\text{3rd point of intersection of} \\ \text{the line } \langle x_1, x_2 \rangle \text{ with } X.\end{array} \end{array}$$

It is not defined everywhere (for example not when the line $\langle x_1, x_2 \rangle$ is contained in X), hence the dotted arrow. But one checks that it is given by rational functions, so it proves that X has many points defined over $\mathbf{K}$. For example, the set of rational solutions of the Shioda cubic equation is dense in the real surface that it defines.

There is a geometric inverse to the parametrization Φ. It is defined by

$$\begin{array}{rcl} X - L_1 - L_2 & \dashrightarrow & L_1 \times L_2 \\ x & \longmapsto & (\langle x, L_2 \rangle \cap L_1, \langle x, L_1 \rangle \cap L_2) \end{array}$$

and it can be extended to a well defined map

$$\Psi : X \longrightarrow L_1 \times L_2$$

(when $x \in L_i$, juste replace the plane $\langle x, L_i \rangle$ by the plane tangent to X at x).

This shows that the parametrization Φ is "almost one-to-one." We say that the surface X is *rational* (over $\mathbf{K}$): the set $X(\mathbf{K})$ is almost isomorphic to $\mathbf{K}^2$.

A smooth cubic surface containing two disjoint lines is rational.

4.3 The plane blown up at six points

We still assume that $X \subset \mathbf{P}^3$ is a smooth projective cubic surface containing disjoint lines L_1 and L_2.

Exactly 5 lines contained in X meet both L_1 and L_2. Each such line L is "blown down" by the map Φ defined above to the point $(L \cap L_1, L \cap L_2)$ and Ψ is the blow-up of 5 distinct points on $L_1 \times L_2 \simeq \mathbf{P}^1 \times \mathbf{P}^1$. On the other hand, the blow-up of a point on $\mathbf{P}^1 \times \mathbf{P}^1$ is isomorphic to $\mathbf{P}^2$ blown up at two distinct points. We have therefore the more precise statement (Clebsch, 1871)

A smooth cubic surface containing two disjoint lines
is isomorphic to the projective plane blown up at 6 points.

One checks further that since X is smooth, these points are in *general position:* no 3 on a line, no 6 on a conic.

Conversely, given a set of 6 distinct points $P_1, \ldots, P_6 \in \mathbf{P}^2$ in general position, one can show that cubic plane curves passing through $P_1, \ldots, P_6$ define an injective map

$$\mathbf{P}^2 - \{P_1, \ldots, P_6\} \longrightarrow \mathbf{P}^3,$$

(the closure of) whose image X is a smooth cubic surface.

The 27 lines on this surface are then

- the images of the 6 "exceptional divisors;"
- the images of the 15 lines passing through 2 of the points;
- the images of the 5 conics passing through 5 of the points.

There is a subtlety here: for X to be defined over $\mathbf{K}$, we do not need each point P_i to be defined over $\mathbf{K}$, but only the whole set $\{P_1, \ldots, P_6\}$. For example, we may take 3 pairs of complex conjugate points; we will still get a real smooth surface, with only three real lines (which correspond to the (real!) lines connecting the 3 pairs of complex conjugate points).

4.4 Counting points over finite fields

The description above implies for example that for a smooth cubic surface X defined over a finite field $\mathbf{F}_q$ and containing 27 lines defined over $\mathbf{F}_q$, one has

$$\mathrm{Card}(X(\mathbf{F}_q)) = \mathrm{Card}(\mathbf{P}^2(\mathbf{F}_q)) - 6 + 6\,\mathrm{Card}(\mathbf{P}^1(\mathbf{F}_q)) = q^2 + 7q + 1.$$

Weil proved that for any smooth cubic surface X defined over $\mathbf{F}_q$, one has

$$\mathrm{Card}(X(\mathbf{F}_q)) = q^2 + t_X q + 1,$$

where $t_X \in \{-2,-1,0,1,2,3,4,5,7\}$ (this formula agrees with the Chevalley–Warning and Ax–Katz theorems). One has $t_X = 7$ if and only if X contains 27 lines defined over $\mathbf{F}_q$, which agrees with the formula above.[4]

All listed values for t_X are possible, except 7 when $q \in \{2,3,5\}$ (no surfaces over these fields can contain 27 lines) and 6 when $q \in \{2,3\}$.

Example 8 (The Fermat cubic over $\mathbf{F}_4$) This is the smooth cubic surface X with equation $x_1^3 + x_2^3 + x_3^3 + x_4^3 = 0$ in $\mathbf{P}^3$.

We saw earlier that X contains 27 lines defined over $\mathbf{F}_4$. It is therefore isomorphic to the plane $\mathbf{P}^2$ blown up in 6 points in general position. But, up to the action of $\mathrm{PGL}_3(\mathbf{F}_4)$, there is only one set of six points in $\mathbf{P}^2(\mathbf{F}_4)$ which are in general position : if $a \in \mathbf{F}_4 - \{0,1\}$, they are $(1:0,0)$, $(0:1:0)$, $(0:0:1)$, $(1:1:1)$, $(1:a:a^2)$, and $(1:a^2:a)$. It follows that all smooth cubic surfaces over $\mathbf{F}_4$ containing 27 lines defined over $\mathbf{F}_4$ are isomorphic to the Fermat cubic X.

The $4^2 + 7\cdot 4 + 1 = 45$ points of $X(\mathbf{F}_4)$ can be determined explicitely: since the cubes in $\mathbf{F}_4$ are 0 and 1, either all coordinates are nonzero (27 points), or exactly two are nonzero (6×3 points).

The diagonal cubic X with equation $x_1^3 + x_2^3 + x_3^3 + ax_4^3 = 0$ where $a \in \mathbf{F}_4 - \{0,1\}$), which we discussed earlier, contains only nine $\mathbf{F}_4$-points (since the cubes in $\mathbf{F}_4$ are 0 and 1, we have $x_4 = 0$ and one exactly of x_1, x_2, x_3 is also 0); so we obtain $t_X = -2$. It is not rational because of the following difficult result.

Theorem 9 (B. Segre, 1943) *Let $\mathbf{K}$ be a field of characteristic $\neq 3$ and let $a_1,\dots,a_4 \in \mathbf{K} - \{0\}$. If, for all permutations $\sigma \in \mathfrak{S}_4$, the element $\frac{a_{\sigma(1)}a_{\sigma(2)}}{a_{\sigma(3)}a_{\sigma(4)}}$ of $\mathbf{K}$ is not a cube in $\mathbf{K}$, the smooth cubic surface over $\mathbf{K}$ defined by the equation*

$$a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_4^3 = 0$$

is not rational.

4.5 Topology

Case $\mathbf{K} = \mathbf{C}$. If X is a smooth complex projective cubic surface, the description of X as the blow-up of the projective plane in 6 points implies that $X(\mathbf{C})$ is diffeomorphic to the connected sum

$$\mathbf{P}^2(\mathbf{C})\#6\overline{\mathbf{P}^2(\mathbf{C})} := \mathbf{P}^2(\mathbf{C})\#\overline{\mathbf{P}^2(\mathbf{C})}\#\overline{\mathbf{P}^2(\mathbf{C})}\#\overline{\mathbf{P}^2(\mathbf{C})}\#\overline{\mathbf{P}^2(\mathbf{C})}\#\overline{\mathbf{P}^2(\mathbf{C})}\#\overline{\mathbf{P}^2(\mathbf{C})},$$

where $\overline{\mathbf{P}^2(\mathbf{C})}$ is $\mathbf{P}^2(\mathbf{C})$ with the reversed orientation.

Case $\mathbf{K} = \mathbf{R}$. The situation is more complicated: there are 5 topological types.

[4]The integer t_X is the trace of the Frobenius endomorphism Fr acting on the Picard group $\mathrm{Pic}(X_{\overline{\mathbf{F}}_q}) \simeq \mathbf{Z}^7$. The eigenvalues of Fr are roots of unity. It follows that its trace is 7 if and only if it acts as the identity, which happens exactly when the 27 lines of X are defined over $\mathbf{F}_q$, since they generate $\mathrm{Pic}(X_{\overline{\mathbf{F}}_q})$.

Let X be a smooth real projective cubic surface. If it contains two disjoint real lines, it is then isomorphic to the blow up of the real projective plane along a real set of 6 points. Topologically, $X(\mathbf{R})$ is then a nonorientable compact connected surface diffeomorphic to

$$\#7\mathbf{P}^2(\mathbf{R}), \#5\mathbf{P}^2(\mathbf{R}), \#3\mathbf{P}^2(\mathbf{R}), \text{or } \mathbf{P}^2(\mathbf{R}),$$

depending on the number of pairs of complex conjugate points (0, 1, 2, or 3). But there is one another case, where $X(\mathbf{R})$ is the disjoint sum $\mathbf{P}^2(\mathbf{R}) \sqcup \mathbf{S}^2$.

The following pictures are taken from the website http://cubics.algebraicsurface.net, designed by Oliver Labs.

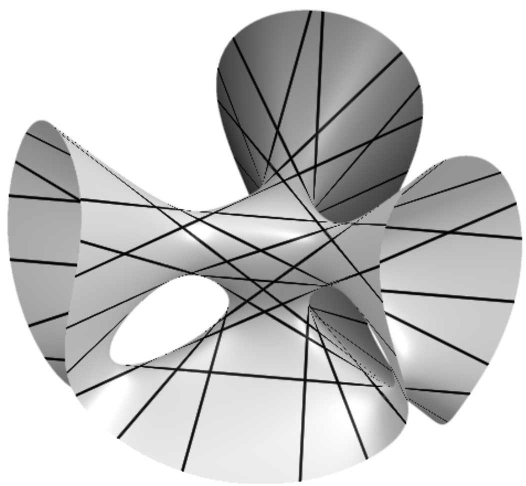

Figure 5: A cubic with 27 real lines, the nonorientable compact connected surface $\#7\mathbf{P}^2(\mathbf{R})$ with Euler characteristic -5.

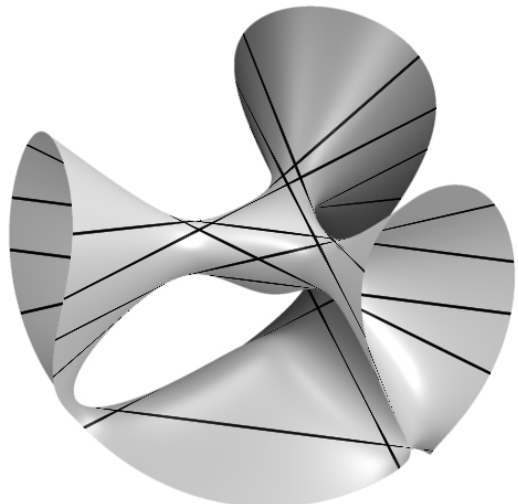

Figure 6: A cubic with 15 real lines, the nonorientable compact connected surface $\#5\mathbf{P}^2(\mathbf{R})$ with Euler characteristic -3.

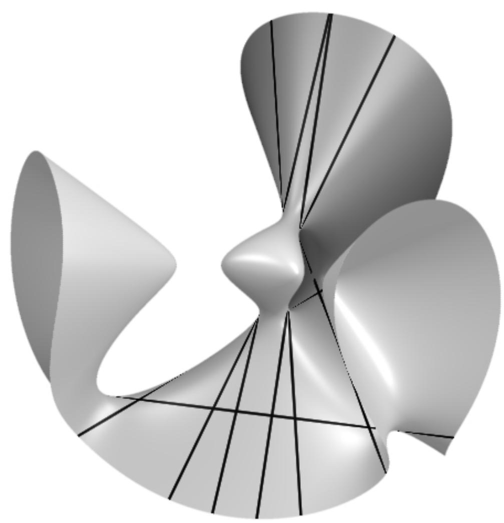

Figure 7: A cubic with 7 real lines, the nonorientable compact connected surface $\#3\mathbf{P}^2(\mathbf{R})$ with Euler characteristic -1.

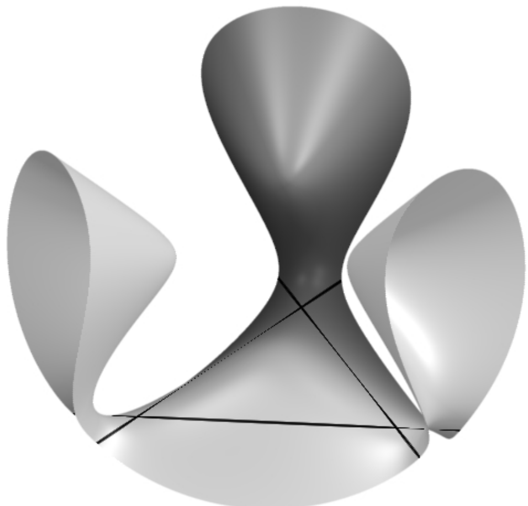

Figure 8: A cubic with 3 real lines, the nonorientable compact connected surface $\mathbf{P}^2(\mathbf{R})$ with Euler characteristic 1.

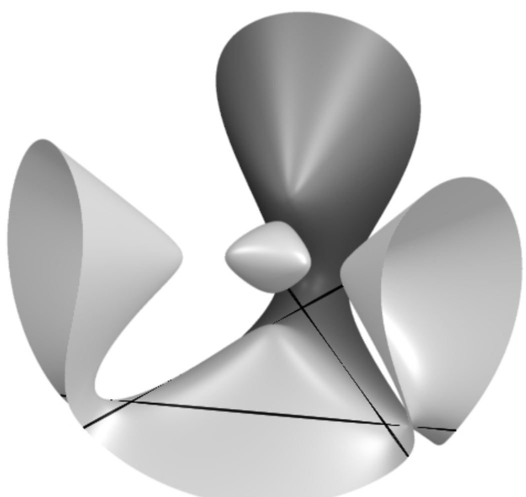

Figure 9: A nonconnected cubic with 3 real lines, homeomorphic to $\mathbf{P}^2(\mathbf{R}) \sqcup \mathbf{S}^2$.

5 Cubics in higher dimensions

5.1 Parametrization

Let $X \subset \mathbf{P}^n$ be a smooth hypersurface defined by the homogeneous cubic equation

$$F(x_0 : x_1 : \ldots : x_n) = 0$$

with coefficients in $\mathbf{K}$.

Assume that X contains a line L defined over $\mathbf{K}$.

This is alway the case when $\mathbf{K}$ is algebraically closed and $n \geq 3$, but also, by a refinement of the Chevalley–Warning theorem, when $\mathbf{K}$ is finite and $n \geq 7$.[5]

We construct a parametrization of $X(\mathbf{K})$ as follows.

Let x be any point of L and let L' be a line tangent to X at x. If L' is not contained in X, its intersection with X consists of the point x counted twice, and another point $\Phi(x, L')$ (this is because the restriction of the cubic polynomial F to the line L' is a cubic polynomial with a double root at x). If we set

$$\mathscr{L} := \{(x, L') \mid x \in L \text{ and } L' \text{ is a line tangent to } X \text{ at } x\},$$

this construction induces a "parametrization"

$$\Phi : \mathscr{L} \dashrightarrow X$$

which is not defined everywhere (hence the dotted arrow), but can be checked to be given by rational functions with coefficients in $\mathbf{K}$.

This "parametrization" is however not one-to-one, but rather two-to-one: given a point $y \in X - L$, the intersection of X with the plane spanned by L and y is a plane cubic curve which contains L; it is therefore the union of L and a conic C, and the two preimages of y by Φ are the two points of $C \cap L$.

On the other hand,we have the following.

Proposition 10 *The set $\mathscr{L}(\mathbf{K})$ can be parametrized in an (almost) one-to-one fashion by $\mathbf{K}^{n-1}$.*

PROOF. We choose coordinates so that L is the line through the origin and directed by the first basis vector. Write a point of $\mathbf{K}^n$ as (x_1, y), with $y \in \mathbf{K}^{n-1}$, and the cubic equation of X as

$$F(x_1, y) = x_1^2 F_1(y) + x_1 F_2(y) + F_3(y),$$

where F_i is a polynomial of degree $\leq i$ with no constant term (because $L \subset X$). Since X is smooth at the origin, F_3 must have a nonzero linear part; we assume $\frac{\partial F_3}{\partial x_2}(0) \neq 0$.

The line L' passing through $x = (x_1, 0)$ and directed by $(1, a_2, \ldots, a_n)$ is tangent to X at x if and only if

$$\sum_{i=2}^{n} \frac{\partial F}{\partial x_i}(x_1, 0)\, a_i = \sum_{i=2}^{n} \left(x_1^2 \frac{\partial F_1}{\partial x_i}(0) + x_1 \frac{\partial F_2}{\partial x_i}(0) + \frac{\partial F_3}{\partial x_i}(0) \right) a_i = 0. \tag{2}$$

[5] Assume $\mathbf{K}$ finite. When $n = 3$, X does not always contain a line defined over $\mathbf{K}$, since we saw earlier an example of a smooth cubic surface over $\mathbf{F}_2$ with a single point defined over $\mathbf{F}_2$. When $n = 4$, there are also examples of smooth cubic hypersurfaces defined over $\mathbf{K} = \mathbf{F}_2$, $\mathbf{F}_3$, or $\mathbf{F}_4$ with no lines defined over $\mathbf{K}$; by the Deligne–Weil estimates (see Section 5.2), there is always such a line for $q \geq 11$. When $n = 5$, there are no known examples of smooth cubic hypersurfaces over $\mathbf{K}$ with no lines defined over $\mathbf{K}$; it seems to be unknown whether X always contains a line defined over $\mathbf{K}$. When $n = 6$, one can prove, using a difficult theorem of H. Esnault, that there is always a line defined over $\mathbf{K}$.

Therefore, one can parametrize $\mathscr{L}(\mathbf{K})$ by sending $(x_1, a_3, \ldots, a_n)$ to the pair (x, L'), where $x = (x_1, 0)$ and L' is the line through x directed by the vector $(1, a_2, \ldots, a_n)$, where a_2 is given by the relation (2): since $\frac{\partial F_3}{\partial x_2}(0) \neq 0$, the factor $x_1^2 \frac{\partial F_1}{\partial x_2}(0) + x_1 \frac{\partial F_2}{\partial x_2}(0) + \frac{\partial F_3}{\partial x_2}(0)$ will be nonzero for almost all $x_1 \in \mathbf{K}$. $\square$

We say that X is *unirational.* The question of the rationality of smooth higher-dimensional cubics remained opened for decades (it was asked in the 19th century!), until it was finally solved (negatively), when $n = 4$ and $\mathbf{K} = \mathbf{C}$, by Clemens and Griffiths in 1972, using techniques which it would be too long to explain here (Fano claimed in 1942 that he had a proof, but it was incomplete; the Clemens-Griffiths result was later extended to positive characteristics by Murre).

No smooth complex cubic threefold is rational.

To put this result in constrast, it had been known for a long time that over the complex numbers, unirational curves or surfaces are rational (this is no longer true for surfaces in positive characteristic). So this was the first example of a nonrational unirational smooth complex variety (actually, other examples of nonrational unirational varieties were produced at roughly the same time by Iskovskikh–Manin (smooth quartic threefolds) and Artin–Mumford), solving the so-called Lüroth problem.

What about higher dimensions? Well, this is still an open problem.

Are there smooth complex cubic hypersurfaces of dimensions ≥ 4 which are not rational?

Specific rational examples are known, but people seem to believe that most smooth complex cubic hypersurfaces of dimensions ≥ 4 should be irrational, although no single example is known.

Example 11 (Smooth rational cubic hypersurfaces) We generalize the construction given in §4.2 for cubic surfaces. Let $X \subset \mathbf{P}^{2m+1}$ be a smooth projective cubic hypersurface over $\mathbf{K}$ containing two disjoint linear spaces M_1 and M_2, both of dimension m and defined over $\mathbf{K}$. An example is given by diagonal cubics, with homogeneous equation

$$a_0 x_0^3 + \cdots + a_{2m+1} x_{2m+1}^3 = 0,$$

where $a_0, \ldots, a_n \in \mathbf{K}$ are nonzero and $\mathrm{char}(\mathbf{K}) \neq 3$. Let $b_{i,j}$ and $c_{i,j}$ be two distinct cubic roots of a_i/a_j (which we may assume to be all in $\mathbf{K}$, possibly upon passing to a finite extension of $\mathbf{K}$). Then the cubic contains the disjoint spaces

$$\begin{array}{lll} M_1, & \text{with equations} & x_0 + b_{0,1}x_1 = x_2 + b_{2,3}x_3 = \cdots = x_{2m} + b_{2m,2m+1}x_{2m+1} = 0, \\ M_2, & \text{with equations} & x_0 + c_{0,1}x_1 = x_2 + c_{2,3}x_3 = \cdots = x_{2m} + c_{2m,2m+1}x_{2m+1} = 0. \end{array}$$

One then has an injective parametrization

$$\begin{array}{rcc} \Phi : M_1 \times M_2 & \dashrightarrow & X \\ (x_1, x_2) & \longmapsto & \begin{array}{c}\text{3rd point of intersection of} \\ \text{the line } \langle x_1, x_2 \rangle \text{ with } X\end{array} \end{array}$$

which is given by rational functions and is (almost) injective (same proof as in §4.2). So X is rational over $\mathbf{K}$.

But, for $m \geq 2$, these cubics are very special: in general, a cubic of dimension $2m$ contains no linear spaces of dimension m at all!

There are no known examples of smooth rational cubic hypersurfaces in odd dimensions.

5.2 Counting points over finite fields

Let $\mathbf{F}_q$ be a finite field of characteristic $\neq 2$ and let $X \subset \mathbf{P}^n$ be a cubic hypersurface defined over $\mathbf{F}_q$. The Chevalley–Warning theorem mentioned earlier implies that $X(\mathbf{F}_q)$ is nonempty as soon as $n \geq 3$. One can do better.

Proposition 12 *Let $X \subset \mathbf{P}^n$ be a cubic hypersurface defined over $\mathbf{F}_q$. We have*

$$\operatorname{Card}(X(\mathbf{F}_q)) \geq \frac{q^{n-2}-1}{q-1}.$$

PROOF. We proceed by induction on n, the case $n = 3$ being a direct consequence of the Chevalley–Warning theorem. Consider the set

$$I := \{(x, H) \in X(\mathbf{F}_q) \times \mathscr{H} \mid x \in H\},$$

where $\mathscr{H}$ is the set of hyperplanes in $\mathbf{P}^n$ defined over $\mathbf{F}_q$. This set is in one-to-one correspondence with a set $\mathbf{P}^n(\mathbf{F}_q)$ (the "dual" projective space), so it has $\frac{q^{n+1}-1}{q-1}$ elements.

Any fiber of the first projection $I \to X(\mathbf{F}_q)$ is the subset of elements of $\mathscr{H}$ passing through a fixed $\mathbf{F}_q$-point x, and this is easily seen to be in one-to-one correspondence with a set $\mathbf{P}^{n-1}(\mathbf{F}_q)$, so it has $\frac{q^n-1}{q-1}$ elements. This implies

$$\operatorname{Card}(I) = \operatorname{Card}(X(\mathbf{F}_q))\frac{q^n-1}{q-1}.$$

On the other hand, the fiber of $H \in \mathscr{H}$ for the second projection $I \to \mathscr{H}$ is $(X \cap H)(\mathbf{F}_q)$. By induction, these fibers all have cardinality $\geq \frac{q^{n-3}-1}{q-1}$. This implies

$$\operatorname{Card}(I) \geq \operatorname{Card}(\mathscr{H})\frac{q^{n-3}-1}{q-1} = \frac{(q^{n+1}-1)(q^{n-3}-1)}{(q-1)^2}.$$

Putting everything together, we obtain

$$\begin{aligned}\operatorname{Card}(X(\mathbf{F}_q)) &\geq \frac{(q^{n+1}-1)(q^{n-3}-1)}{(q^n-1)(q-1)} > \frac{(q^{n+1}-q)(q^{n-3}-1)}{(q^n-1)(q-1)} \\ &= \frac{q(q^{n-3}-1)}{q-1} = \frac{q^{n-2}-1}{q-1} - 1,\end{aligned}$$

which implies what we want since we are dealing with integers. $\square$

When $X \subset \mathbf{P}^n$ is moreover smooth, we have the Deligne–Weil estimate (which generalizes Hasse's estimate (case $n = 2$))

$$\left|\operatorname{Card}(X(\mathbf{F}_q)) - \frac{q^n - 1}{q - 1}\right| \leq \big(\frac{1}{3}(2^{n+1} + (-1)^n) + (-1)^{n+1}\big)q^{(n-1)/2},$$

which often gives a better result.

5.3 Topology

Case $\mathbf{K} = \mathbf{C}$. All smooth cubic hypersurfaces of the same dimension $d = n - 1 \geq 2$ are diffeomorphic and simply connected. Mikhalkin showed that they can be decomposed in the union of 3^d generalized pairs of pants (the complement in $(\mathbf{C}^*)^d$ of the hyperplane $\sum_{i=1}^d x_i = 1$).

Case $\mathbf{K} = \mathbf{R}$. Although the different topological types of smooth real cubic surfaces were determined by Klein in the second half of the 19th century, it is only recently (2006) that Krasnov proved that there are 9 topological (actually, diffeomorphism) types for $X(\mathbf{R})$, where $X \subset \mathbf{P}^4$ is a smooth real cubic hypersurface. He determined 8 of them:

$$\mathbf{P}^3(\mathbf{R})\#k\mathbf{S}^3 \quad \text{for } k \in \{0, \dots, 6\}$$

and the disjoint sum $\mathbf{P}^3(\mathbf{R}) \sqcup \mathbf{S}^3$. The last case was worked out by Finashin and Kharlamov (see below), who proved that $X(\mathbf{R})$ is a Seifert manifold.

In 2009, Finashin and Kharlamov studied the next case and proved that there are 65 diffeomorphism types for $X(\mathbf{R})$, where $X \subset \mathbf{P}^5$ is a smooth real cubic hypersurface. They are

$$\mathbf{P}^4(\mathbf{R})\#k(\mathbf{S}^2 \times \mathbf{S}^2)\#\ell(\mathbf{S}^1 \times \mathbf{S}^3)$$

where the pair of integers (k, ℓ) varies in a set with 64 elements and satisfy $0 \leq k, \ell \leq 10$ and $k + \ell \leq 11$, and the disjoint sum $\mathbf{P}^4(\mathbf{R}) \sqcup \mathbf{S}^4$.

They also investigate, more generally, smooth real cubic hypersurfaces $X \subset \mathbf{P}^n$ of any dimensions. They prove that if $X(\mathbf{R})$ is disconnected, it is then diffeomorphic to $\mathbf{P}^{n-1}(\mathbf{R}) \sqcup \mathbf{S}^{n-1}$. They also construct, among others, for any $n \geq 3$, and any $a, b \in \{1, \dots, n-2\}$, smooth real cubic hypersurfaces $X \subset \mathbf{P}^n$ such that $X(\mathbf{R})$ is diffeomorphic to $\mathbf{P}^{n-1}(\mathbf{R})$, or to $\mathbf{P}^{n-1}(\mathbf{R})\#(\mathbf{S}^a \times \mathbf{S}^{n-1-a})\#(\mathbf{S}^b \times \mathbf{S}^{n-1-b})$.