RATIONALITY AND IRRATIONALITY: WHEN CAN SOLUTIONS OF POLYNOMIAL EQUATIONS BE ALGEBRAICALLY PARAMETRIZED?

OLIVIER DEBARRE

ABSTRACT. The description of all the solutions of the equation $x^2 + y^2 = z^2$ in integral numbers (a.k.a. Pythagorean triples) is a very ancient problem: a Babylonian clay tablet from about 1800BC may contain some solutions, Pythagoras (about 500BC) seems to have known one infinite family of solutions, and so did Plato... This gives a first example of a rational variety: the rational points on the circle with equation $x^2 + y^2 = 1$ can be algebraically parametrized by one rational parameter. More generally, one says that a variety of dimension n, defined by a system of polynomial equations, is rational if its points (the solutions of the system) can be algebraically parametrized, in a one-to-one fashion, by n independent parameters. I will begin with easy standard examples, then explain and apply some (not-so-recent) techniques that can be used to prove that some varieties (such as the set of solutions of the equation $x^3 + y^3 + z^3 + w^3 = 1$) are not rational.

1. Introduction

1.1. About the word rational.

From the Merriam–Webster dictionary:

rational: relating to, based on, or agreeable to reason;

reason: proper exercise of the mind.

In mathematics, *rational numbers* are fractions a/b, where a and b are whole numbers (also called integers). The story goes that when Hippasus discovered that $\sqrt{2}$ was not a rational number, he was sentenced to death by drowning by Pythagoras, who could not accept the existence of *irrational numbers.*

Similar resistance was encountered when *imaginary numbers* (such as $\sqrt{-1}$) were introduced (hence their derogatory name). We now call them *complex numbers.*

Nowadays, mathematicians denote by $\mathbf{Q}$ the set of rational numbers and by $\mathbf{C}$ the set of complex numbers. The word rational is used in many places in mathematics. We will use for example *rational fractions,* which are quotient of polynomials (possibly in several variables), with rational or complex coefficients (to avoid confusion, we will say $\mathbf{Q}$- or $\mathbf{C}$-coefficients), depending on the situation.

1.2. **An example: Pythagorean triples ($3^3+4^2 = 5^2$).** We will start with a very old example: we want to solve the equation

$$x^2 + y^2 = 1 \tag{1}$$

where x and y are rational numbers, that is, we want to find points with rational coordinates on a circle. The geometrical approach is to start from one point, say $P_0 := (-1, 0)$. Any other point $P = (x, y)$ defines a line P_0P with rational slope. Conversely, any line with rational slope t passing through P_0 meets the circle in another point (x, y) with rational coordinates: the equation of that line is $y = t(x + 1)$ and one also has

$$x^2 + t^2(x + 1)^2 = 1.$$

This can also be written as $(x + 1)(x - 1 + t^2(x + 1)) = 0$, hence

$$x = \frac{1 - t^2}{1 + t^2} \qquad \text{and} \qquad y = \frac{2t}{1 + t^2}.$$

So we are successful in that case: we have parametrized solutions by rational functions in one parameter t, in a one-to-one fashion: each solution (except $(-1, 0)$: it corresponds to $t = \infty$) is reached by exactly one value of the parameter. Note that we obtain $\mathbf{Q}$-solutions by taking t in $\mathbf{Q}$, but also $\mathbf{C}$-solutions by taking t in $\mathbf{C}$ (although the geometric picture of a "circle" is wrong in that case).

Note finally that solving the equation (1) in rational numbers is the same as solving the homogenized equation

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

in integral numbers (the solutions are called "Pythagorean triples" because they are the lengths of the sides of a right triangle). We obtain in this way

$$(x, y, z) = (u^2 - t^2, 2tu, u^2 + t^2).$$

This is a parametrization of all solutions by polynomials in the parameters t and u, which is often easier to manipulate.

1.3. **Rational varieties.** The general problem that I want to discuss here is the following: we start from a system of polynomial equations in several unknowns $x_1, \ldots, x_n$:

$$P_1(x_1, \ldots, x_n) = \cdots = P_r(x_1, \ldots, x_n) = 0.$$

The set of solutions $(x_1, \ldots, x_n)$ is called an *algebraic variety.* We say that this variety is *rational* (over $\mathbf{Q}$ or $\mathbf{C}$) if it can be parametrized by rational functions depending on (several) parameters $t_1, \ldots, t_d$:

$$\left\{\begin{matrix}\text{parameters} \\ (\text{in } \mathbf{Q} \text{ or } \mathbf{C})\end{matrix}\right\} \leftarrow \dashrightarrow \left\{\begin{matrix}\text{solutions (in } \mathbf{Q} \text{ or } \mathbf{C}\text{) of} \\ P_1(x_1, \ldots, x_n) = \cdots = P_r(x_1, \ldots, x_n) = 0\end{matrix}\right\}$$

$$(t_1, \ldots, t_d) \longmapsto x_1 = \tfrac{A_1(t_1, \ldots, t_d)}{B_1(t_1, \ldots, t_d)}, \ldots, x_n = \tfrac{A_n(t_1, \ldots, t_d)}{B_n(t_1, \ldots, t_d)}.$$

The dashed arrow on top going from left to right means that the solutions are only be defined for *almost all* values of the parameters (those for which the denominators do not vanish). The dashed arrow going from right to left means that *almost all* solutions are reached by a unique value of the parameters. We say that this is an (almost) one-to-one parametrization and call this double dashed arrow a *birational map.* The number of parameters, d, is the dimension of the variety.

As we rermarked earlier, it is often a good idea to first homogenize the polynomials $P_1, \ldots, P_r$ (by adding an extra unknown x_0), so that we can cancel the denominators in the fractions A_j/B_j and obtain a parametrization that is polynomial in the parameters.

2. Parametrizing curves

2.1. **Plane curves of higher degrees.** If one tries to parametrize the curve with equation

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

by rational fractions, one sees quite quickly that this is impossible: such a parametrization by rational fractions with $\mathbf{Q}$-coefficients is impossible simply because the only rational solutions to this equation are $(0, 0)$ and $(\pm 1, 0)$, but more generally, a direct (elementary but lenghty) computation by substitution shows that such a parametrization is impossible even with rational fractions with $\mathbf{C}$-coefficients. This curve is not rational, even over $\mathbf{C}$.

However, this is possible for the curve with equation

$$y^2 = x^2(x+1)$$

because it is *singular* at $P_0 := (0,0)$: as before, we look for points on lines through P_0, that is, of the form (x, tx). We get $t^2x^2 = x^2(x+1)$, which solves as

$$(x,y) = (t^2-1, t(t^2-1)).$$

What is going on here is that a smooth compact complex curve is, topologically, a smooth compact real *surface* and as such, it has a *genus* $g \geq 0$. An algebraic parametrization by rational fractions with complex coefficients is possible only if $g = 0$. This is a topological condition. If the curve is defined by equations with rational coefficients and one wants a parametrization by rational fractions with rational coefficients, one also needs that the curve have a point with rational coordinates.

3. Parametrizations in higher dimensions

3.1. **Parametrizing quadrics.** One can keep the same degree, 2, but increase the number of unknowns, that is, consider an equation

$$Q(x_1, \dots, x_n) = 0,$$

where Q is a polynomial of degree 2 in n variables. We will assume that Q is homogeneous (this can be achieved by adding one variable). To parametrize (almost all) solutions by rational functions, we use the same trick: assuming that there is one solution $\mathbf{a} = (a_1, \dots, a_n)$, we take a line $\mathbf{a} + t\mathbf{x}$ through $\mathbf{a}$ and solve the equation

$$0 = Q(\mathbf{a} + t\mathbf{x}) = Q(\mathbf{a}) + 2tB(\mathbf{a}, \mathbf{x}) + t^2Q(\mathbf{x}) = 2tB(\mathbf{a}, \mathbf{x}) + t^2Q(\mathbf{x})$$

(here, B is the bilinear form associated with the quadratic form Q) as

$$t = -\frac{2B(\mathbf{a}, \mathbf{x})}{Q(\mathbf{x})}$$

which gives the solutions

$$Q(\mathbf{x})\mathbf{a} - 2B(\mathbf{a}, \mathbf{x})\mathbf{x},$$

for (almost) all $\mathbf{x}$. If one wants a one-to-one parametrization, one needs to take $\mathbf{x}$ in a hyperplane that does not contain $\mathbf{a}$.

3.2. **Parametrizing cubics.** Already in degree 3, the situation becomes more complicated. We already discussed a nonrational example in two variables. Let us consider the so-called Fermat cubic equation

$$x^3 + y^3 + z^3 + 1 = 0$$

in three variables (which can be homogenized as $x^3 + y^3 + z^3 + w^3 = 0$).

There are lots of $\mathbf{Q}$-solutions, for example, all $(t, -t, -1)$, for $t \in \mathbf{Q}$: this family of solutions corresponds to a line contained in the cubic surface defined by this equation, but there are many other solutions. Since we are dealing with a surface here, we would like to know whether it is possible to parametrize (almost all) $\mathbf{Q}$-solutions by rational fractions in two variables with $\mathbf{Q}$-coefficients, in a one-to-one fashion.

The answer (already known to Euler in the 18th century) is yes and the method is again geometric. The Fermat cubic surface contains many lines: 9 defined over $\mathbf{Q}$ and 18 others defined over $\mathbf{Q}(j)$ (where $j := e^{2i\pi/3}$), among which we find the skew lines $L := \{(t, -jt, -j)\}$ and its conjugate $\bar{L} = \{(t, -\bar{j}t, -\bar{j})\}$. We can use them to parametrize (almost all) solutions: if $P = (t, -jt, -j) \in L$ and $\bar{P} = (\bar{t}, -\bar{j}\bar{t}, -\bar{j}) \in \bar{L}$, where $t = a + ib \in \mathbf{C}$, the line $P\bar{P}$ meets the surface in a third point $P(a, b)$ whose coordinates are rational functions with $\mathbf{Q}$-coefficients in a and b.

Euler obtained in this way a parametrization of the solutions of the homogeneous Fermat cubic equation by quartic polynomials with three parameters a, b, c. More recently, Noam Elkies obtained a parametrization by cubic polynomials:

$$\begin{aligned}
x &= -a^3 - 2a^2c + 3a^2b + 12abc - 3ab^2 - 4ac^2 + 6b^2c + 12bc^2 + 9b^3,\\
y &= a^3 + 2a^2c + 3a^2b + 12abc + 3ab^2 + 4ac^2 - 6b^2c + 12bc^2 + 9b^3,\\
z &= -8c^3 - 8ac^2 - 9b^3 - a^3 - 3a^2b - 3ab^2 - 4a^2c - 12b^2c,\\
w &= 8c^3 + 8ac^2 - 9b^3 + a^3 - 3a^2b + 3ab^2 + 4a^2c + 12b^2c.
\end{aligned}$$

The general result is that *smooth complex cubic surfaces are always rational over* $\mathbf{C}$. Over $\mathbf{Q}$, the situation is more complicated. The surface defined by the equation

$$5x^3 + 12y^3 + 9z^3 + 10 = 0$$

has no $\mathbf{Q}$-solutions, so cannot be rational over $\mathbf{Q}$. The surface defined by

$$x^3 + y^3 + z^3 + 2 = 0$$

obviously has $\mathbf{Q}$-solutions, but it is not rational over $\mathbf{Q}$.

When the number of variables increases (keeping cubic equations), the problem of parametrizing solutions becomes much more difficult. A geometric argument easily gives (over $\mathbf{C}$) 2-to-1 parametrizations (in all dimensions ≥ 2). But for cubic equations in 4 complex variables, it was only shown in 1972 by Clemens and Griffiths that *1-to-1 parametrizations never exist: they are not rational over* $\mathbf{C}$. This applies for example to the Fermat cubic equation

$$x^3 + y^3 + z^3 + w^3 + 1 = 0.$$

In each even dimension $2m \geq 2$, there exist rational cubic equations whose solutions can be parametrized by rational functions. The idea is to copy what we did for surfaces: some cubics of dimension $2m$, such as the Fermat cubic

$$x_1^3 + \cdots + x_{2m+1}^3 + 1 = 0,$$

contain disjoint m-spaces P and Q and can be parametrized by $P \times Q$: they are rational (the Fermat cubic is even rational over $\mathbf{Q}$).

From now on, I will forget about $\mathbf{Q}$ and *only consider the problem of the rationality over* $\mathbf{C}$ *of complex varieties.* Here are two famous elementary looking problems whose solutions are unknown:

- are there smooth irrational cubic hypersurfaces of dimension 4?
- are there smooth rational cubic hypersurfaces of odd dimensions?

The expected answers are YES (most cubic hypersurfaces of dimension 4 should be irrational) and NO.

4. How to prove irrationality for varieties of dimension 3?

Most varieties are not rational! There are many "numerical invariants" that need to vanish for a (smooth projective complex) variety to be rational. For example, (smooth projective) varieties defined by one homogeneous equation of degree $\geq n$ in n variables are never rational.

However, varieties defined by cubic equations in 4 variables satisfy none of the classical criteria for irrationality (mostly because they have two-to-one rational parametrizations) so it was a challenge to prove that they are. Clemens and Griffiths' proof is based on the introduction of a new (nonnumerical) "invariant." Assume that an algebraic variety X of dimension 3 is rational (over $\mathbf{C}$). This means that there exists a *birational map*

$$\mathbf{C}^3 \dashleftarrow\dashrightarrow X$$

("generically" one-to-one, not necessarily everywhere defined).

The "invariant" is the *intermediate Jacobian.* It is a complex torus whose definition involves the Hodge decomposition of the singular cohomology of the variety, so I will spare you the details. It can be associated with any (smooth projective) variety of odd dimension but the most interesting case (and the only we will deal with here) is when it is also an algebraic variety; it is then called an *abelian variety.* This is the case for curves; it is very well understood and was already known to mathematicians in the 19th century.

A birational map between varieties of dimension 3 can be decomposed as a composition of blow ups and blow downs of smooth curves and one can follow what happens to the intermediate Jacobians during each of these elementary steps. The upshot is that *if a (smooth projective) algebraic variety of dimension 3 is rational, its intermediate Jacobian is isomorphic to a product of Jacobians of curves.* So it is not quite an invariant but changes in a controlled way. We will use the equivalent statement that if its intermediate Jacobian is *not* a product of Jacobians of curves, a variety (of dimension 3) is not rational.

So what is so special about Jacobians of curves and how can one prove that an intermediate Jacobian is not a Jacobian of curve (or a product of such)?

4.1. **Singularities of the theta divisor.** All these Jacobians J carry an extra canonical object: a *theta divisor.* This is a hypersurface $\Theta \subset J$ and, for Jacobians of curves of their products, it is rather singular: one has

$$\dim(\mathrm{Sing}(\Theta)) \geq \dim(J) - 4.$$

It is however difficult to analyze Θ in general and even more its singularities. This has only been done in a few cases: for all smooth cubic hypersurfaces (J has dimension 5 but Θ has a unique singular point (Mumford, Beauville)), all smooth "double quartic solids" (J has dimension 10 but $\mathrm{Sing}(\Theta)$ has dimension 5 (Voisin)), and general "Gushel–Mukai" threefolds (J has dimension 10 but $\mathrm{Sing}(\Theta)$ has dimension ≤ 5 (Beauville); we will come back to them in Section 4.3).

4.2. **Counting points.** This may sound like a strange idea but here is how it goes. When we are dealing with varieties defined by equations with integral coefficients, we can always reduce these equations modulo a prime number p and look for solutions in the field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. There are then finitely many solutions so we can count these "$\mathbf{F}_p$-points." The Weil conjectures (established by Deligne) give a link between these numbers and the complex geometry of the variety. What we are going to use here is that the range for the possible numbers of points on the Jacobian of a curve is more restricted than on a general abelian variety.

When A is an abelian variety (such as a Jacobian) of dimension g defined by equations with coefficients in $\mathbf{F}_p$, one can define a polynomial

$$\begin{gathered} Q_A(T) = T^{2g} + a_1(A)T^{2g-1} + \cdots + a_{g-1}(A)T^{g+1} + a_g(A)T^g \\ + pa_{g-1}(A)T^{g-1} + \cdots + p^{g-1}a_1(A)T + p^g \end{gathered}$$

with integral coefficients which has the following properties.

- When A is the Jacobian JC of a curve C, one has

$$N(C) = p + 1 + a_1(JC), \tag{2}$$

  where $N(C)$ is the number of $\mathbf{F}_p$-points of C. More precisely, Q_{JC} determines the numbers of points of C with coordinates in all extensions $\mathbf{F}_{p^r}$ of $\mathbf{F}_p$ and conversely, the knowledge of these numbers, for g distinct values of r, determines Q_{JC}.
- When A is the intermediate Jacobian JX of a cubic X of dimension 3, the polynomial Q_{JX} determines the numbers of lines on X with coordinates in all extensions $\mathbf{F}_{p^r}$ of $\mathbf{F}_p$ and again, the knowledge of these numbers, for g distinct values of r, determines Q_{JX}.

Markushevich and Roulleau (2017) then consider the cubic X defined by the homogeneous equation

$$\begin{aligned} &x_1^3 + 2x_1^2x_2 + 2x_1x_2^2 + x_1^2x_3 + 2x_1x_2x_3 + 2x_1x_3^2 + 2x_2x_3^2 \\ &+ x_3^3 + x_1^2x_4 + 2x_1x_2x_4 + x_2^2x_4 + x_2x_3x_4 + x_1x_4^2 + 2x_3x_4^2 + x_4^3 + x_2^2x_5 \\ &+ 2x_2x_3x_5 + 2x_3^2x_5 + x_1x_4x_5 + x_2x_4x_5 + x_4^2x_5 + x_2x_5^2 + 2x_4x_5^2 + x_5^3 = 0. \end{aligned} \tag{3}$$

They compute the number of $\mathbf{F}_{3^r}$-lines contained in X for $1 \leq r \leq 5$ and obtain the polynomial attached to the intermediate Jacobian JX:

$$\begin{aligned} Q_{JX}(T) = T^{10} - 6T^9 + 15T^8 - 10T^7 - 41T^6 + 125T^5 \\ - 41 \cdot 3T^4 - 10 \cdot 3^2T^3 + 15 \cdot 3^3T^2 - 6 \cdot 3^4T + 3^5. \end{aligned}$$

If JX is the Jacobian of a curve C, we then get from (2)

$$N(C) = 3 + 1 + a_1(JC) = 4 + a_1(JX) = -2,$$

which is absurd.[1]

Of course, this only proves that the cubic defined by the equation (3) is not rational, but a general "continuity argument" implies that this is still true for almost all cubics of dimension 3. I think this is the only instance were this method has been successfully used to prove irrationality.

4.3. **Symmetries.** A curve cannot have too many symmetries: the maximal number is $84(g-1)$, where g is the genus of the curve (it is attained by Hurwitz curves for infinitely many, but far from all, values of g). This is also the maximal number of symmetries for the Jacobian of a curve (more exactly, for the pair (J, Θ)). If one can show that an intermediate Jacobian JX of dimension g has more than $84(g-1)$ symmetries, this will be (almost: one has to exclude products of Jacobians of curves, but let us not worry about that) enough to prove that X is not rational.

Consider the Klein cubic X defined by the homogeneous equation

$$x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_5^2 + x_5x_1^2 = 0.$$

Klein noted in 1878 that, in addition to the obvious order-5 symmetry and the less obvious order-11 symmetry

$$(x_1, x_2, x_3, x_4, x_5) \longmapsto (x_1, \zeta x_2, \zeta^6 x_3, \zeta^9 x_4, \zeta^2 x_5),$$

where $\zeta := e^{2i\pi/11}$, the symmetry group has in fact 660 elements. Since JX has dimension 5 and

$$660 > 84 \cdot (5-1),$$

[1] I have cheated quite a bit in several places and the actual argument is a bit more involved.

we see that JX cannot be the Jacobian of a curve, hence X is not rational. Again, a general argument implies that this is still true for almost all cubics of dimension 3. The counting argument presented above does not work in this seemingly simpler case.

This symmetry argument has been applied (by Beauville) for many examples. Recently, Giovanni Mongardi (from Bologna) and I used it to give a new example of an irrational variety of this type. The definition is a bit more complicated: we look at varieties defined as follows. Start from the Grassmannian $\mathrm{Gr}(2,5) \subset \mathbf{P}(\bigwedge^2 V_5) = \mathbf{P}^9$ and consider a smooth intersection $W := \mathrm{Gr}(2,5) \cap \mathbf{P}^7$ (they are all isomorphic). We consider varieties defined as

$$X = W \cap (\text{quadric}).$$

For almost all quadrics, X is smooth of dimension 3 and Beauville showed (by a degeneration argument to the case where X acquires a single singular point) that for almost all X (that is, for almost all quadrics), the 10-dimensional intermediate Jacobian JX is not the Jacobian of a curve because its theta divisor is not singular enough (see Section 4.1). This method does not produce any *explicit* irrational X, though.

Giovanni and I constructed a variety X of this type with a symmetry of order 11, which is clearly not enough. However, we prove that the intermediate Jacobian JX has 660 symmetries (the same symmetries as the Klein cubic). Unfortunately, this is still not enough because this is below the Hurwitz bound:

$$660 \leq 84 \cdot (10 - 1).$$

But, luckily for us, when $g = 10$, the number of symmetries of a curve is actually bounded by 432, so JX cannot be the Jacobian of a curve and X is not rational!

Université de Paris, CNRS, IMJ-PRG, F-75013 Paris, France

E-mail address: olivier.debarre@imj-prg.fr