

> with(plots) : with(LinearAlgebra) : with(Groebner);  
 [Basis, FGLM, HilbertDimension, HilbertPolynomial, HilbertSeries, Homogenize, InitialForm, InterReduce, IsProper, IsZeroDimensional, LeadingCoefficient, LeadingMonomial, LeadingTerm, MatrixOrder, MaximalIndependentSet, MonomialOrder, MultiplicationMatrix, MultivariateCyclicVector, NormalForm, NormalSet, RationalUnivariateRepresentation, Reduce, RememberBasis, SPolynomial, Solve, SuggestVariableOrder, TestOrder, ToricIdealBasis, TrailingTerm, UnivariatePolynomial, Walk, WeightedDegree]

We consider the following rational map from  $\mathbb{R}$  to  $\mathbb{R}^2$ .

>  $F := \text{Vector} \left( \left[ \frac{6 \cdot t}{1 + t^3}, \frac{6 \cdot t^2}{1 + t^3} \right] \right);$

$$F := \begin{bmatrix} \frac{6t}{1+t^3} \\ \frac{6t^2}{1+t^3} \end{bmatrix} \quad (2)$$

The image of this rational map is a parametrized curve known as the Descartes's folium. By a very simple computation show that this curve is included in the curve of implicit equation  $x^3 + y^3 - 6 \cdot x \cdot y = 0$ .

> 
$$0 \quad (3)$$

Draw the curve  $x^3 + y^3 - 6 \cdot x \cdot y$  using the function implicit plot with the option `grid = [100, 100]`.

The objectives of the two first part of this practical session is to rediscover this result in two different ways if you know the implicit equation in advance.

## I) Implicit equation via Groebner basis

If we consider  $\text{Im}(F)$ , it is the set of point  $\begin{pmatrix} x \\ y \end{pmatrix}$  such that there is a value of parameter  $t$  such that

$$x = \frac{6 \cdot t}{1 + t^3} \text{ and } y = \frac{6 \cdot t^2}{1 + t^3}.$$

In other words,  $\text{Im}(F)$  is contained in the projection of  $\mathbb{Z}((1 + t^3) \cdot x - 6 \cdot t, (1 + t^3) \cdot y - 6 \cdot t^2)$  on the  $(x, y)$ -plane. An ideal is just defined by the list of its generators.

>  $J := [(1 + t^3) \cdot x - 6 \cdot t, (1 + t^3) \cdot y - 6 \cdot t^2];$   

$$J := [(1 + t^3) x - 6 t, (1 + t^3) y - 6 t^2] \quad (1.1)$$

Read the documentation of the function `Basis` of the Groebner library. Choose an lexicographic order with  $t > x > y$  and compute a Groebner basis of  $J$ .

>

Remark that the Groebner basis contain an equation containing only the variables  $x$  and  $y$  and that this equation is the wanted one. This equation is the first one because Maple gives Groebner basis sorted by increasing order.

>

## II) Implicit equation via resultant

Compute the resultant of  $(1 + t^3) \cdot x - 6 \cdot t$  and  $(1 + t^3) \cdot y - 6 \cdot t^2$  with respect to  $t$ .

>

Remark that you obtain a multiple (here a scalar one) of the implicit equation. Look for the function content and find the implicit equation.

>

## III) An other example

Consider the map  $t \rightarrow \begin{pmatrix} t \\ \frac{1}{t} \end{pmatrix}$ . Then try the two preceding methods to find an implicit equation if such

an equation exist.

>

>

## IV) A more serious exemple

Consider the following rational map  $t \rightarrow \left( \frac{(1 + 4 \cdot t^2 - t^4)}{(3 - t + t^2)}, \frac{(1 + t - t^3)}{(2 - t^4)} \right)$ . Plot this curve for  $t \in [-1, 1]$  and give its implicit equation. Plot the implicit curve  $1 < x < 3$  and  $-5 < y < 5$ . You will remark somethings for  $0 < x < 1$  and  $0 < y < 2$ . Zoom here and explain what can happen.

>

## V) Intersecting curves

One can try to find intersection points of the folium and the hyperbola. Use the knowledge of the parametric form of one of them and the implicit equation of the other to find a method in order to compute real intersection points  $\mathcal{Z}((1 + t^3) \cdot x - 6 \cdot t, (1 + t^3) \cdot y - 6 \cdot t^2, x - t, t \cdot y - 1)$ . (Hint : look at the function subs and think that a polynomial of degree 6 can have a solvable Galois group)

>

Check your solutions.

## VI) Intersecting curves : a more serious example

Here we choose a case where there is no help : no parametric form known and computations leads to equations with unsolvable Galois group.

>  $P1 := x^5 + 3 \cdot x \cdot y^4 - 6 \cdot x^2 \cdot y + 4 x \cdot y + y^3 - y - 1; P2 := x^2 + 2 \cdot y^2 - x \cdot y - 2;$

$$P1 := x^5 + 3 x y^4 - 6 x^2 y + 4 y x + y^3 - y - 1$$

$$P2 := x^2 + 2 y^2 - y x - 2$$

(6.1)

1) Draw the two curves.

>

2) Compute a Groebner basis of the intersection of this two implicit curves with respect to a lexicographical order with  $x > y$  and deduce that zeros are such that  $y$  is a roots of an univariate polynomial  $p(y)$  of degree 10 and that  $x = q(y)$  for a rational polynomial coefficients  $q(y)$ .

- 3) Give a bound on the module of the  $y$  coordinates of the zeros associated to the ideal associated to the intersection of the two curves.
- 4) Use the maple code on real root isolation and improve it eventually in order to find the number of real root of  $p(y)$ . Deduce the number of real intersection of those two curves.

## VII) Elliptic curves and application of resultant and Groebner basis to arithmetic of elliptic curves

In this section, we consider the elliptic curve  $C$  of Weierstrass equation

$W : y^2 - (x^3 + x^2 - 5 \cdot x) = 0$ . We will try to give a idea of the interplay between geometry and arithmetic on this curve.

1) Draw the curve  $C$  and the line  $x + y + 1 = 0$  on the same graph. Remark that if you take two point on the curve, the line passing through this two points seem to cut the curve on a third point. If the two points are distincts this is true on this curve. If the the "two points" are the same just take the tangent to the curve passing through this point, it generally cut the at one other point except when the tangent is vertical (indicating that we have to add a point "at infinity"). Wit all this remark, one can see that we have already define an intern law (called the Poincaré law) and we have something like a group but without unity. This object define only geometrically is the Poincaré groupoid, the base of the group associated to the curve.

$$\begin{aligned}
 > W := y^2 - (x^3 + x^2 - 5 \cdot x); l := x + y + 1; \\
 & \qquad \qquad \qquad W := y^2 - x^3 - x^2 + 5x \\
 & \qquad \qquad \qquad l := x + y + 1 \qquad \qquad \qquad (7.1)
 \end{aligned}$$

>

- 2) Take two distinct points on the curve, say  $(x_0, y_0)$  and  $(x_1, y_1)$ . Try to use resultant or Groebner basis to express the coordinates of the "sum" of this two points. Conclusion ?
- 3) Consider a generic line (not vertical)  $y - a \cdot x - b$ . We will try to understand what kind of intersection can be found between non vertical lines and this curve. Using resultant or Groebner basis, compute a polynomial  $f(a, b, x)$  such that the roots with respect to  $x$  are the first coordinate of intersection between the elliptic curve and the generic line.
- 4) Compute the discriminant  $\Delta(a, b)$  of  $f(a, b, x)$  with respect to  $x$ .  $\Delta(x, y)$  defines an implicit curve. Draw the graph of this curve in a way you can see that the curve decomposes the real plane in five distinct region (see it experimentally).
- 5) Give the sign of the discriminant in each region and explain the relation of this sign with the nature of the intersection of the line and the elliptic curve.

>