About the Lebesgue's method and RC-constructibilty

Pascal Schreck
IGG-LSIIT
UMR CNRS 7005
Université Louis Pasteur - Strasbourg

Exact solutions in GCS

An exact solution of a constraint system is

a *formal* (*symbolic*) object *f*

one can *prove* that *f* satisfies the constraints

An exact solution *f* is usefull if

it is usable to compute other informations

one can compute controlled real approximations of *f*

f is expressed with a *set of basic operations*

Examples

algebraic equations and radicals $\sqrt[p]{x}$

geometric constructions and rule and compass operations

Plan

1- RC-constructibility

2- Computability of a field, RP-computability and factorization

3- RP-computability and field extensions

4- Lebegue's method

5- Conclusion

Rule and compass constructions

basic operations (considered as exact operations)

drawing a line passing through two points
drawing a circle whose radius is given by two points
considering the intersection(s) of lines and circles

it is not so easy to see if a GC-system is RC-constructible or not

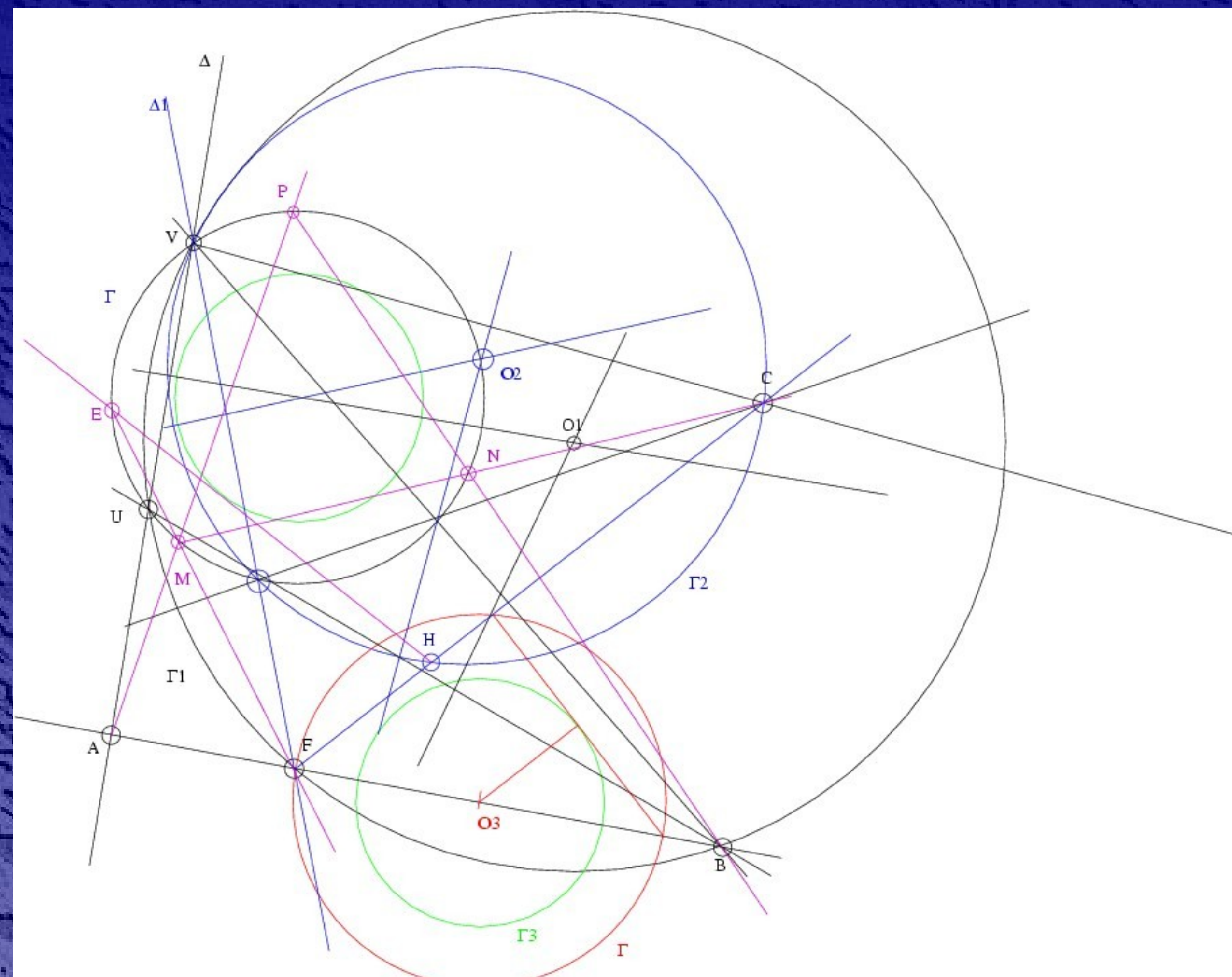
- angle trissection
- squaring the circle

(open problems during ~2000 years)

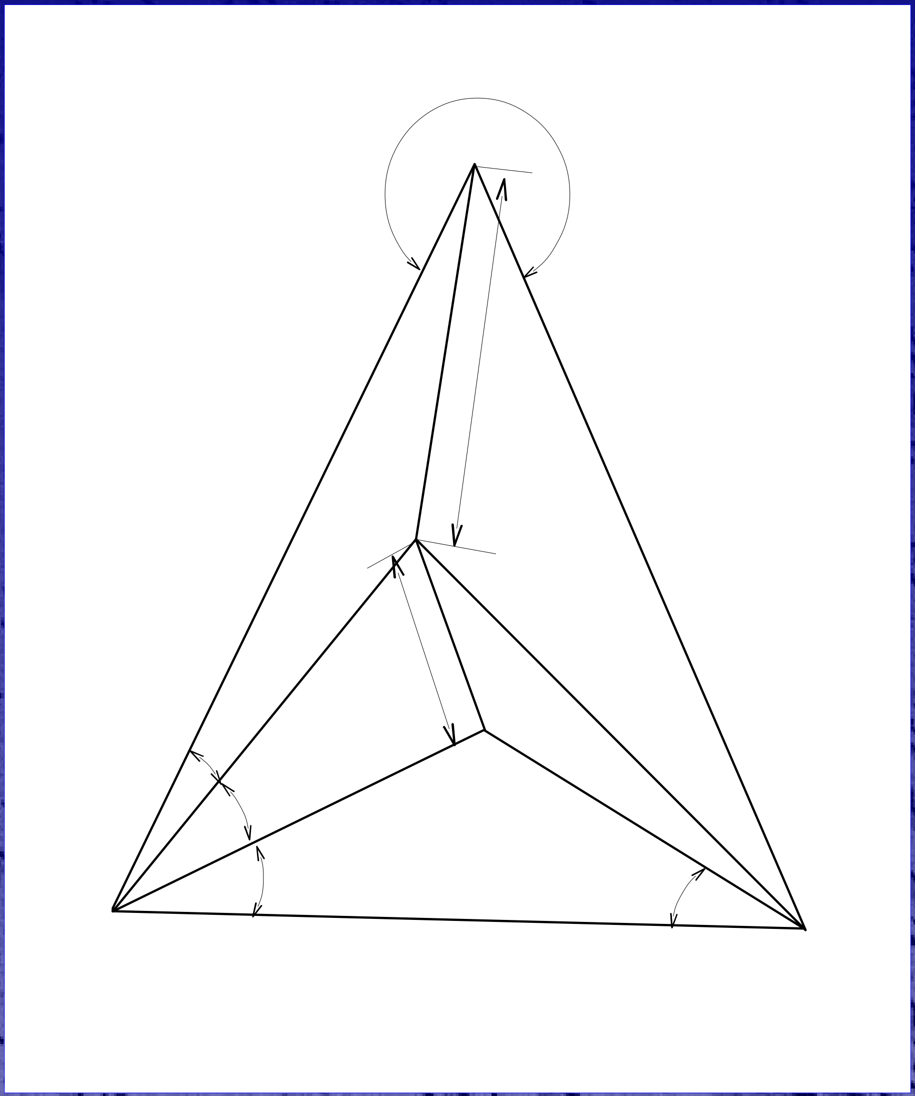
Cramer-Castillon 's problem (1742)

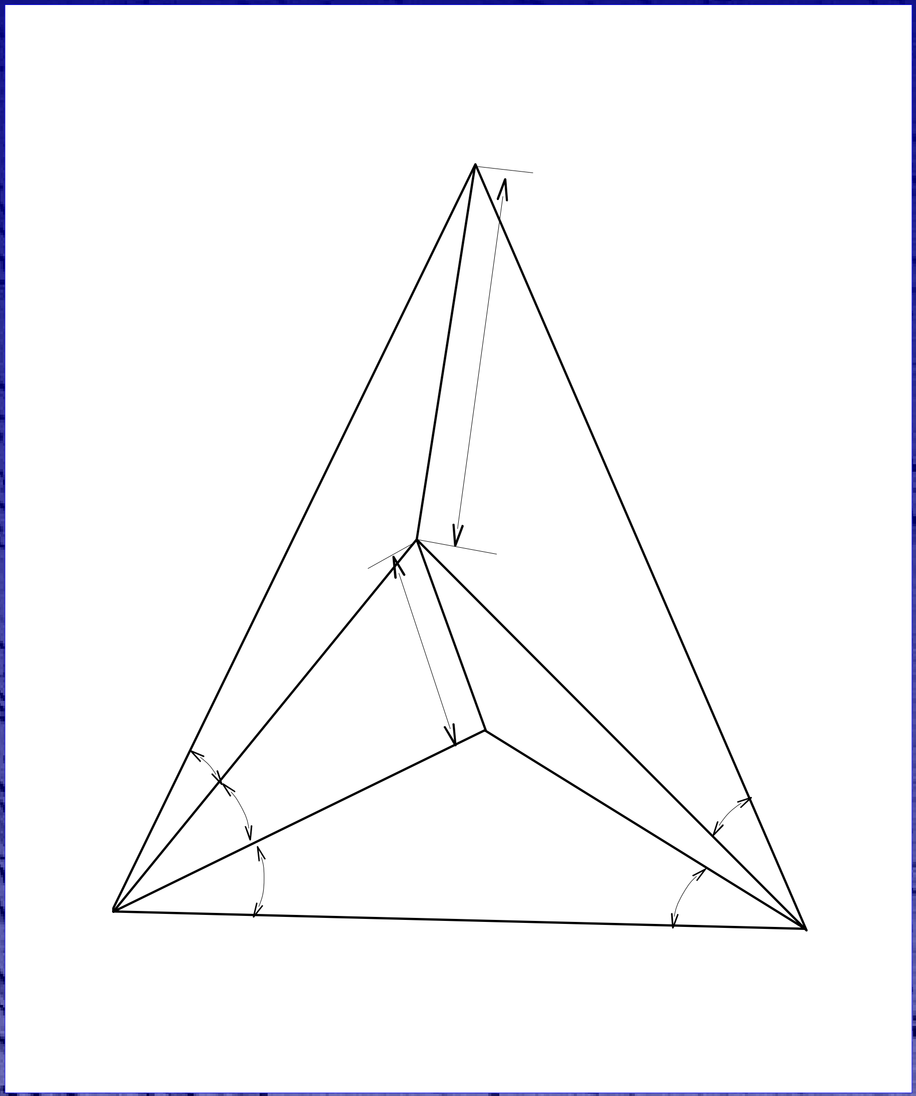
Given a circle *Γ* and three points *A*, *B* and *C* (out of *Γ*).

Construct points *M*, *N* and *P* on circle *Γ* such that
A *MP*, *B* *NP* and
C *MN*.



CAD problems





Only one of these two problems is RC-constructible, which one ?

Mathematical results

Def: *a real is RC-constructible (from points* (0,0) *and* (1,0)) *if it is a coordinate of a RC-constructible point (from points* (0,0) *and* (1,0)).

Thm(Wantzel 1837): *Each RC-constructible number is algebraic over* $\mathbb{Q}$ *and its degree is equal to* 2^k *for some* k *in* $\mathbb{N}$.

The reverse is false: one of the roots of X^4-X-1 is not RC-constructible

Mathematical results (2)

Thm (Gallois ~1870): *Let be an algebraic number over* $\mathbb{Q}$, $P(X)$ *be its minimal polynomial and K be the splitting field of* $P(X)$. *Number is RC-constructible iff* $[K:\mathbb{Q}] = 2^k$ *for some k in* $\mathbb{N}$.

an important consequence:

Thm : *Let be an algebraic number over* $\mathbb{Q}$, *is RC-constructible iff there is a sequence of fields* $L_0, \ldots, L_n$ *such that* $L_0 = \mathbb{Q}$, $L_n = \mathbb{Q}(\ )$ *and* $[L_{i+1}:Li] = 2$.

(G. Chen, H. Carrayol, 1992)

How to *compute* the splitting field of $P(X)$?

Computability, RP-computability

A computable field is a field (K,+,.) such that operations +, -, . and / are computable

(there are data structure for K, and algorithms for +,-,. and /)

Def: *a field K is RP-computable if*

- *it is a computable field*
- *and there is an algorithm to compute the roots in K for each polynomial in* $K[X]$.

Examples:

- each finite field is RP-computable;
- $\mathbb{Q}$ is RP-computable.

Factorization

Thm : *K is a RP-computable field, iff there is a factorization algorithm in K[X].*

Sketch of the proof :

if part is self-evident

Finding degree k factors of $P(X)$: $X^k + a_1X^{k-1} + \dots a_{k-1}X + a_k$

$$P(X) = Q(X)(X^k + a_1X^{k-1} + \dots + a_k) + R(X)$$

since $R(X)=0$ and coef. r_i of $R(X)$ are in $K[a_1, \dots a_k]$ we must have

$$\begin{cases} r_{k-1}(a_1, \dots, a_k) = 0 \\ \dots \\ r_0(a_1, \dots, a_k) = 0 \end{cases}$$

puting it under triangular form

$$\begin{cases} r'_{k-1}(a_1) = 0 \\ \dots \\ r'_0(a_1, \dots, a_k) = 0 \end{cases}$$

There is an algorithm to solve these equations *in K*

RP-computability and field extension

Thm: *Let $K \subset F$ be a field extension and υ be an element of F. If K is RP-computable, $K(\upsilon)$ is RP-computable too.*

constructive proof:

case where υ is transcendant

- computability: each element of $K(\upsilon)$ is a pair of polynomials over K

  +, _, * and / are computable operations

- RP-computability: this is basically the algorithm used to find the root in $\mathbb{Q}$ of polynomials in $\mathbb{Q}[X]$.

RP-computability and field extension

case where υ is algebraic over K

(υ is known through its irreducible polynomial P).

- computability: each element of $K(\upsilon)$ is a polynomial in υ of degree d°P_υ -1

  +,_, * and / are computable.

- RP-computability:

$f(X) = {}_0X^n + \ldots + {}_{n-1}X + {}_n$ where ${}_i$ in $K(\upsilon)$ ${}_i = a_{i,0}\upsilon^{k-1} + \ldots + a_{i,k-1}$

a root of f can be written $x_0 = b_0\upsilon^{k-1} + \ldots + b_{k-1}$ (b_i are unknown) so we have

$f(x_0) = 0 = {}_0\upsilon^{k-1} + \ldots + {}_{k-1}$

$$\begin{cases} \beta_0(b_0, \ldots, b_{k-1}) = 0 \\ \ldots \\ \beta_{k-1}(b_0, \ldots, b_{k-1}) = 0 \end{cases}$$

all the reductions are computable

Lebegue's method (~1940)

Thm (1992?): *let P(X) be irreducible in K[X]. If P(X)=0 is solvable using only square radicals, then there is a number r in K such that P(X) is reducible over* $K(\sqrt{r})$.

Utilization: let $P(X)$ be an irreducible polynomial over K, let us try to find r and to factorize P

let $Q(X)$ be such a factor, we have :

$$Q(X) = X^k + m_{1X}^{k-1} + \ldots + m_k + \sqrt{r}\,(m_{k+1} X^{k-1} + \ldots + m_{2k}) \qquad m_i \quad K, r \quad K$$

by Euclidean division P(X) = Q(X)*T(X) + R(X)

$$R(X) = (A_0(m_{1,}\ldots, m_{2k}, r) + \sqrt{r}\, B_0(m_{1,}\ldots, m_{2k}, r))\, X^{k-1} +$$

$$\ldots$$

$$+ A_{k-1}(m_{1,}\ldots, m_{2k}, r) + \sqrt{r}\, B_{k-1}(m_{1,}\ldots, m_{2k}, r)$$

and R(X) must vanish anywhere

Lebegue's method (suite)

$$\begin{cases} A_0(m_{1,}\ldots, m_{2\mathrm{k}}, r)=0 \\ \ldots \\ A_{k-1}(m_{1,}\ldots, m_{2\mathrm{k}}, r)=0 \\ B_0(m_{1,}\ldots, m_{2\mathrm{k}}, r)=0 \\ \ldots \\ B_{k-1}(m_{1,}\ldots, m_{2\mathrm{k}}, r)=0 \\ (m_{k+1}-1)(m_{k+2}-1)\ldots(m_{2k}-1)=0 \end{cases}$$

all the equations are over K

m_1, m_2 ... $m_{2\mathrm{k}}$ and r are the unknowns

which have to be searched in K

There is an algorithm to solve this kind of system

Lebegue's method (summary)

let P(X) be an irreducible polynomial in K[X]

if P(X)=0 is solvable using only square roots, it can be factorized into factors of degree 1 by using recursively the previous algorithm

then all the numbers r_i such that $K\left(\sqrt{r_1},\ldots,\sqrt{r_n}\right)$ is the splitting field of P are computed during the factorization.

if the factorization cannot be done, then P(X) is not solvable using only square radicals

This method was implemented in Mapple by G. Chen.

Exemple : Appolonius's problem

Given three circles

$$C_1 : (x - p_1)^2 + (y - p_2)^2 = p_3^2$$

$$C_2 : (x - p_4)^2 + (y - p_5)^2 = p_6^2$$

$$C_3 : x^2 + y^2 = p_7^2$$

find $C : (x - x_1)^2 + (y - x_2)^2 = x_3^2$

such that

$$f_1 = \left((x_1 - p_1)^2 + (x_2 - p_2)^2\right)^2 - (p_3^2 - x_3^2)^2 = 0$$

$$f_2 = \left((x_1 - p_4)^2 + (x_2 - p_5)^2\right)^2 - (p_6^2 - x_3^2)^2 = 0$$

$$f_3 = \left(x_1^2 + x_2^2\right)^2 - (p_7^2 - x_3^2)^2 = 0$$

First, we have to put this system into a triangular form

The Wu-Ritt algorithm gives 8 characteristic sets

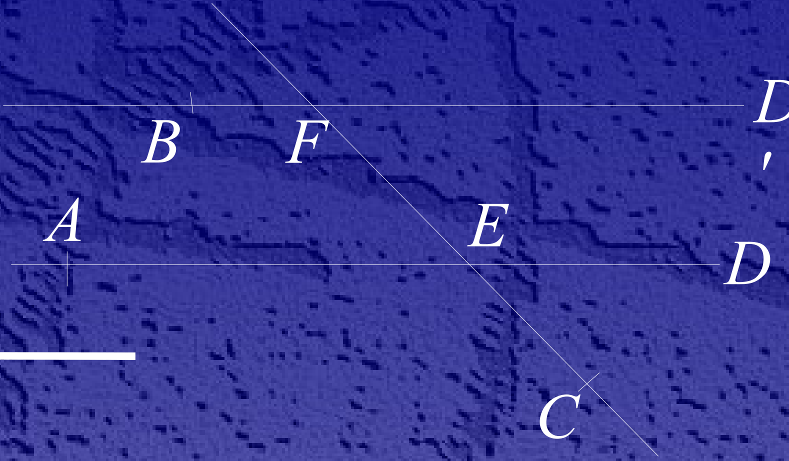
... the equations to be solved have at most degree 2

Exemple 2

Given two parallel lines D and D' and three points : A on D, B on D' and C. Construct a line passing through C and which intersect line D in E and line D' in F such that $AE+BF$ equals a given value p_1.

$B(0,0)$, $D'=Ox$

$A(p_2,p_3)$, $C(p_4,p_5)$, $E(x_1,x_2)$, $F(x_3,x_4)$



$$f_1 : x_4 = 0$$

$$f_2 : x_2 - p_3 = 0$$

$$f_3 : (x_2 - p_5)(x_3 - p_4) - (x_1 - p_4)(x_4 - p_5) = 0$$

$$f_4 : \left((x_1 - p_2)^2 + (x_2 - p_3)^2 + x_3^2 + x_4^2 - p_1^2\right)^2 - 4(x_1 - p_2)^2$$
$$-4(x_2 - p_3)^2 - 4\mathrm{x}_3^2 - 4\mathrm{x}_4^2 = 0$$

Exemple 2 (suite)

$x_1 = s_1 + s_2$ wher e $s_1 = \frac{\sqrt{u}}{v}$ and $s_2 = \frac{-q}{r}$ with

$u = 8p_5^4 + 8p_5^4\sqrt{1+p_1^2} - 4p^{4p}\ 2 + 4p^{4p}\ 2 + 8p\ 3p\ 32p\ 3 + 8p^{3p}\ 2p_5 - 32p^{3p}\ 1 + p_1^2$

$- 16p\ 3p_1^2 - 4\ p^{2p}\ 2 - 16p^{2p}\ 2p\ 56\ p^{2p}\ 2 + 28\ p^{2p}\ 2p_1^2 + 56\ p_3^2\ p_5^{2sqrt}\ 1 + p_1^2$

$- 4p^{2p}\ 2p_5^2 + 8p^{3p}\ 2p_3 + 8p^{3p}\ 4p_2 - 48\ p^{3p}\ 24\ p^{3p}\ 1^2 - 48p\ 3sqrt\ 1 + p_1^2 + 16p_5^4$

$\frac{1}{2}$

$8p^{4p}\ 2 + 16p_5^{4sqrt}\ 1 + p_1^2 - 4p^{4p}\ 2$

5

$v = 2p_3^2 - 4p\ 4p_5^2$

and

$q = -4p\ 3p_5 - 28p^{2p}\ 3^2 + 24p^{2p}\ 3 - 8\ p\ 5^2 + 8p\ 2p_5^2 + 16p\ 3 - 8p^{3p}\ 4p\ 4$

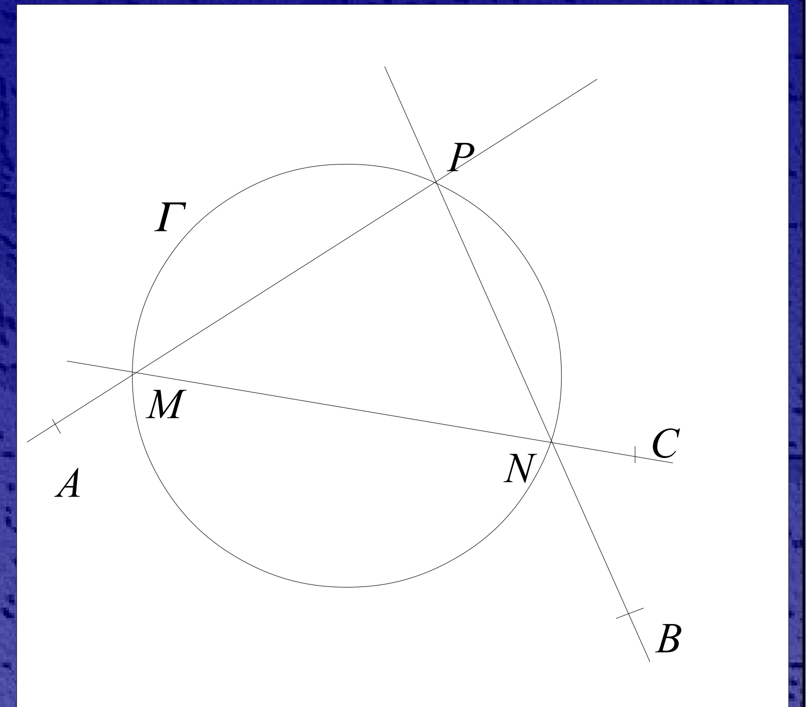
3
3
3

$r = 16p_5^4 - 16p\ 3 + 4p_3^4 - 32p^{3p}\ 32p^{2p}\ 2$

Exemple 3 : Cramer-Castillon's problem

$O(0,0)$ center of (radius =1)
$A(p_1,p_2), B(p_3,p_4), C(p_5,0)$ and
$M(x_1,x_2)$, $N(x_3,x_4)$, $P(x_5,x_6)$

$$f_1 : (x_1 - p_1)(x_6 - p_2) - (x_2 - p_2)(x_5 - p_1) = 0$$
$$f_2 : (x_1 - p_5)x_4 - x_2(x_3 - p_5) = 0$$
$$f_3 : (x_5 - p_3)(x_4 - p_4) - (x_3 - p_3)(x_6 - p_4)$$
$$f_4 : x_1^2 + x_2^2 - 1 = 0$$
$$f_5 : x_3^2 + x_4^2 - 1 = 0$$
$$f_6 : x_5^2 + x_6^2 - 1 = 0$$



The Wu-Ritt algorithm failed (with the 92' mapple implementation)

Conclusion

The Lebesgue's method seems different from the Gao-Chou method

It is not efficient but it gives a theoretical result about decidability of RC-contructibility

It can be improved to take « Origamis » constructions into account