# REAL ALGEBRA

In this lecture:

- Artin - Lang theorem
- Real Nullstellensatz
- Positivstellensatz
- proof of Hilbert 17, Artin solution.

Let R be a real closed field.

I ARTIN-LANG THEOREM

We begin with a consequence of the Tarski-Seidenberg principle.

**Proposition 4.1.1.** *Let $R_1$ be a real closed extension of $R$. Let $\mathcal{B}(X)$ be a boolean combination of polynomial equations and inequalities in the variables $X = (X_1, \ldots, X_n)$, with coefficients in $R$. If $\mathcal{B}(y)$ holds true for some $y \in R_1^n$, then $\mathcal{B}(x)$ holds true for some $x \in R^n$.*

Proof By induction on $n$.

- If $n=0$, no variable so ok!
- If $n \geq 1$, assume the result for $n-1$. By

Tarski-Seidenberg theorem (version with real fields), there exists a boolean combination $\mathcal{C}(X')$ of polynomial equations and inequalities in the variables $X' = (X_1, \ldots, X_{n-1})$, with coefficients in $R$, such that, for every real closed field $R_2$ containing $R$ and every $x' = (x_1, \ldots, x_{n-1}) \in R_2^{n-1}$, $\mathcal{B}(x', X_n)$ has a solution in $R_2$ if and only if $\mathcal{C}(x')$ holds true.

Therefore, if $y = (y_1, \ldots, y_n)$ is a solution of $\mathcal{B}(X)$ in $R_1^n$,

$\Rightarrow$

then $y' = (y_1, \ldots, y_{n-1})$ is a solution of $\mathcal{C}(X')$ in $R_1^{n-1}$. By induction, $\mathcal{C}(X')$ has a solution $x' = (x_1, \ldots, x_{n-1})$ in $R^{n-1}$. Hence, there exists $x_n \in R$, such that $x = (x', x_n)$ is a solution of $\mathcal{B}(X)$ in $R^n$. $\Leftarrow$ $\square$

As a consequence :

**Theorem 4.1.2 (Artin-Lang Homomorphism Theorem).** *Let $R$ be a real closed field and $A$ an $R$-algebra of finite type. If there exists an $R$-algebra homomorphism $\varphi : A \to R_1$ into a real closed extension $R_1$ of $R$, then there exists an $R$-algebra homomorphism $\psi : A \to R$.*

*Proof.* We may assume $A$ to be of the form $R[X_1, \dots, X_n]/I$, where $I$ is the ideal of $R[X_1, \dots, X_n]$ generated by $P_1, \dots, P_m$.

Then $\varphi : \dfrac{R[X_1, \dots, X_n]}{(P_1, \dots, P_m)} \longrightarrow R_1$.

. Let $b_i$ be the image of the class of $X_i$ by $\varphi$. Then $(b_1, \dots, b_n)$ is a solution of the system of equations $P_1 = \cdots = P_m = 0$ in $R_1^n$.

. By Proposition 4.1.1, this system of equations also has a solution $(a_1, \dots, a_n)$ in $R^n$. The homomorphism $\overline{\psi} : R[X_1, \dots, X_n] \to R$ defined by $\overline{\psi}(X_i) = a_i$ obviously induces a homomorphism $\psi : A \to R$. □

The homomorphism theorem is used to prove the real Nullstellensatz, which characterizes the ideal of polynomials vanishing on an algebraic set.

**Definition 4.1.3.** *Let $A$ be a commutative ring. An ideal $I$ of $A$ is said to be* real *if, for every sequence $a_1, \dots, a_p$ of elements of $A$, we have*

$$a_1^2 + \cdots + a_p^2 \in I \implies a_i \in I\ , \ \textit{for } i = 1, \dots, p\ .$$

<u>Counter-example</u> $(x^2+y^2)$ in $R[x,y]$

First a lemma.

**Lemma 4.1.5.** *Every real ideal $I$ of a commutative ring $A$ is radical. Moreover, if $A$ is noetherian, then all minimal prime ideals containing $I$ are real.*

$I \subseteq \mathfrak{p}$ minimal if $\begin{cases} I \subseteq \mathfrak{q} \\ \mathfrak{q} \subseteq \mathfrak{p} \\ \mathfrak{q} \text{ prime} \end{cases} \Rightarrow \mathfrak{q} = \mathfrak{p}$

- In a noetherian ring, there is a finite number of minimal prime ideals containing $I$, and
  $$I = \bigcap_{\substack{\mathfrak{p} \text{ minimal prime} \\ \mathfrak{p} \supseteq I}} \mathfrak{p}$$
- It corresponds to the decomposition in irreducible components.

*Proof.* If $a^n \in I$, $n > 1$, then $a^{n/2} \in I$ if $n$ is even, and $a^{(n+1)/2} \in I$ if $n$ is odd. In both cases the exponent has decreased, and we get $a \in I$ by iterating this process.

Let $\mathfrak{p}_1, \dots, \mathfrak{p}_q$ be the minimal prime ideals of $A$ containing $I$. We can assume $q > 1$. If, for instance, $\mathfrak{p}_1$ is not real, then we can find $a_1, \dots, a_p \in A \setminus \mathfrak{p}_1$, such that $a_1^2 + \dots + a_p^2 \in \mathfrak{p}_1$. Choose $b_i \in \mathfrak{p}_i \setminus \mathfrak{p}_1$, for $i = 2, \dots, q$, and set $b = \prod_{i=2}^q b_i$. Then $(a_1 b)^2 + \dots + (a_p b)^2 \in \bigcap_{i=1}^q \mathfrak{p}_i = I$, but $a_1 b \notin \mathfrak{p}_1$, which is a contradiction. $\square$

$a_1 \notin \mathfrak{p}_1$ and $b \notin \mathfrak{p}_1$

A second lemma:

<u>Lemma</u> Let $A$ be a commutative ring and $I \subseteq A$ prime ideal. Then

$$I \text{ is a real ideal } \iff \operatorname{Frac} \frac{A}{I} \text{ is a real field}$$

<u>Proof</u> Let $a_1, \dots, a_p \in A$. Then

$$a_1^2 + \dots + a_p^2 \in I \iff a_1^2 + \dots + a_p^2 = 0 \in A/I$$
$$\iff a_1^2 + \dots + a_p^2 = 0 \in \operatorname{Frac} A/I$$

So that

$$I \text{ real} \iff \operatorname{Frac} A/I \text{ real}.$$

by the characterization of real fields.

$\square$

Here is the real version of the classical Nullstellensatz.

[J.J. Risler, 1970]

**Theorem 4.1.4 (Real Nullstellensatz).** *Let $R$ be a real closed field and $I$ an ideal of $R[X_1, \dots, X_n]$. Then $I = \mathcal{I}(\mathcal{Z}(I))$ if and only if $I$ is real.*

<u>Proof of $\Rightarrow$</u>

- Assume $P_1^2 + \dots + P_n^2 \in I$.
- For $x \in \mathcal{Z}(I)$, we have $(P_1^2 + \dots + P_n^2)(x) = 0$ so
  $P_1(x) = \dots = P_n(x) = 0$.
- Then $P_i \in \mathcal{I}(\mathcal{Z}(I))$, so $P_i \in I$ $\forall i$

**Theorem 4.1.4 (Real Nullstellensatz).** *Let $R$ be a real closed field and $I$ an ideal of $R[X_1, \ldots, X_n]$. Then $I = \mathcal{I}(\mathcal{Z}(I))$ if and only if $I$ is real.*

<u>Proof of $\Leftarrow$</u> • First $I \subseteq \mathcal{I}(\mathcal{Z}(I))$ as usual.

• Assume $P \notin I$. We are going to prove $P \notin \mathcal{I}(\mathcal{Z}(I))$ hence the equality

• $I = \bigcap_{i=1}^{n} p_i$ with $p_i$ the minimal prime ideals containing $I$.

It suffices to proves the result for any $p_i$.

• By a Lemma : $I$ real $\Rightarrow$ $p_i$ real. So now we assume $I$ to be a real prime ideal.

• Let $S$ be the multiplicative set generated by $P$ in $\frac{R[X]}{I}$ and

$$A = \left(\frac{R[X]}{I}\right)_S \subseteq \operatorname{Frac} \frac{R[X]}{I}$$

the ring $\frac{R[X]}{I}$ localized at $S$.

• Choose an ordering on the real field (by a Lemma) $\operatorname{Frac} \frac{R[X]}{I}$

• Let $R_1$ denote the real closure of $\operatorname{Frac} \frac{R[X]}{I}$.

We have a natural inclusion :

$$A \longrightarrow \left(\frac{R[X]}{I}\right)_S \longrightarrow \operatorname{Frac} \frac{R[X]}{I} \longrightarrow R_1$$

• By Artin-Lang Theorem, we obtain an $R$-algebra morphism

$$\varphi : A \longrightarrow R$$

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, phantom, "\wr"] & R \\ \left(\frac{R[X]}{I}\right)_S & \end{tikzcd}$$

- Denote $x_i = \varphi(\overline{X_i}) \in R$. Then

  * $x \in Z(I)$ by the construction
  * $P(x) \neq 0$ because $P$ is invertible in $A$.

Therefore $P \notin \mathcal{J}(Z(I))$ as expected.

$\square$

<u>Proposition</u> If $P \in R[X_1, \dots, X_n]$ is irreducible, and there exist $a, b \in R^n$ with $P(a)P(b) < 0$, then $(P)$ is real.

<u>Idea of proof</u>

- one can show $\dim Z(P) = n-1$
- then height $\mathcal{J}(Z(P)) = 1$
- $(P)$ is prime of height $1$
- $(P) \subseteq \mathcal{J}(Z(P))$, so equality.

$\square$

The real Nullstellensatz leads to the notion of "real radical"!

**Proposition 4.1.7.** *Let $A$ be a commutative ring and $I$ an ideal of $A$. Then*

$$\sqrt[R]{I} = \{a \in A \mid \exists m \in \mathbb{N}\ \exists b_1, \dots, b_p \in A \quad a^{2m} + b_1^2 + \cdots + b_p^2 \in I\}$$

*is the smallest real ideal of $A$ containing $I$. The ideal $\sqrt[R]{I}$, called* the real radical of $I$, *is the intersection of all real prime ideals containing $I$ (or is $A$ itself, if there is no real prime ideal containing $I$).*

Partial proof: stability under addition

Assume $a^{2m} + b_1^2 + \dots + b_p^2 \in I$

and $\alpha^{2n} + \beta_1^2 + \dots + \beta_q^2 \in I$.

Then $(a+\alpha)^{2(n+m)} + (a-\alpha)^{2(n+m)}$

is of the form

$a^{2m} c + \alpha^{2n} \gamma$

all the odd powers vanish

where $c, \gamma \in \sum A^2$.

So $(a+\alpha)^{2(n+m)} + \sum A^2 \in I$

thus $a+\alpha \in \sqrt[R]{I}$.

$\square$

**Corollary 4.1.8.** *Let $I \subset R[X_1, \dots, X_n]$ be an ideal. Then $P \in \mathcal{I}(\mathcal{Z}(I))$ if and only if there exist finitely many polynomials $Q_1, \dots, Q_p$ and an integer $m \in \mathbb{N}$, such that $P^{2m} + Q_1^2 + \cdots + Q_p^2 \in I$. In short, $\mathcal{I}(\mathcal{Z}(I)) = \sqrt[R]{I}$.*

*Proof.* The real Nullstellensatz says that $\mathcal{I}(\mathcal{Z}(I))$ is the smallest real ideal containing $I$, that is, by Proposition 4.1.7, the ideal $\sqrt[R]{I}$. $\square$

Going further the study, one could study inequalities too in an algebraic manner

[Stengle, 1974]

in a ring, but same definition as in a field.

**Theorem 4.4.2.** *Let $R$ be a real closed field. Let $(f_j)_{j=1,\dots,s}$, $(g_k)_{k=1,\dots,t}$ and $(h_\ell)_{\ell=1,\dots,u}$ be finite families of polynomials in $R[X_1,\dots,X_n]$. Denote by $P$ the cone generated by $(f_j)_{j=1,\dots,s}$, $M$ the multiplicative monoid generated by $(g_k)_{k=1,\dots,t}$ and $I$ the ideal generated by $(h_\ell)_{\ell=1,\dots,u}$. Then the following properties are equivalent:*

stable under product

(i) *The set*

$$\{x \in R^n \mid f_j(x) \geq 0\,,\ j=1,\dots,s,\quad g_k(x) \neq 0\,,\ k=1,\dots,t,\\ h_\ell(x)=0\,,\ \ell=1,\dots,u\}$$

*is empty.*

(ii) *There exist $f \in P$, $g \in M$ and $h \in I$ such that $f + g^2 + h = 0$.*

Toward the proof

(ii) $\Rightarrow$ (i) If $f_j(x) \geq 0$ $\forall j$, then $f(x) \geqslant 0$

If $g_k(x) \neq 0$ $\forall k$, then $g(x) \neq 0$ and $g^2(x) > 0$.

Thus $f(x) + g^2(x) > 0$. In particular $h(x) < 0$.

Since $h \in I = (h_1, \dots, h_u)$, at least one $h_\ell$ does not vanish at $x$.

(i) $\Rightarrow$ (ii) More involved, use the so-called "formal Positivstellensatz" + Artin-Lang theorem.

$\square$

A (geometric) Positivstellensatz follows:

<u>Definition</u> For a real algebraic set $V \subseteq \mathbb{R}^n$, denote by $\mathcal{P}(V)$ the ring $\mathcal{P}(V) = \dfrac{\mathbb{R}[X_1, \ldots, X_n]}{\mathcal{I}(V)}$ of polynomial functions on $V$.

**Corollary 4.4.3 (Positivstellensatz).** *Let $V \subset R^n$ be an algebraic set, $g_1, \ldots, g_s \in \mathcal{P}(V)$ and*

$$W = \{x \in V \mid g_1(x) \geq 0, \ldots, \; g_s(x) \geq 0\}.$$

*Let $P$ be the cone of $\mathcal{P}(V)$ generated by $g_1, \ldots, g_s$, and let $f \in \mathcal{P}(V)$. Then:*
(i) $\forall x \in W \;\; f(x) \geq 0 \Leftrightarrow \exists m \in \mathbb{N} \;\; \exists g, h \in P \;\; fg = f^{2m} + h$.
(ii) $\forall x \in W \;\; f(x) > 0 \Leftrightarrow \exists g, h \in P \;\; fg = 1 + h$.
(iii) $\forall x \in W \;\; f(x) = 0 \Leftrightarrow \exists m \in \mathbb{N} \;\; \exists g \in P \;\; f^{2m} + g = 0$.

<u>Proofs of $\Leftarrow$</u> Take $x \in W$.

(i) : $g, h \in P$ so $g(x) \geq 0$ and $h(x) \geq 0$.
Then $f^{2m}(x) + h(x) \geq 0$ so $f(x)\, g(x) \geq 0$.
Moreover * if $g(x) > 0$, then $f(x) \geq 0$
* if $g(x) = 0$, then $f^{2m}(x) + h(x) = 0$ so $f(x) = 0$.
In any case, $f(x) \geq 0$.

(ii) Same idea: $1 + h(x) \geq 1$ so $f(x)\, g(x) \geq 1$
Since $g(x) \geq 0$, it follows $g(x) > 0$ and $f(x) > 0$.

(iii) $g(x) \geq 0$ and $f^{2m}(x) \geq 0$ so $g(x) = f(x) = 0$

**Corollary 4.4.3 (Positivstellensatz).** *Let $V \subset R^n$ be an algebraic set, $g_1, \ldots, g_s \in \mathcal{P}(V)$ and*

$$W = \{x \in V \mid g_1(x) \geq 0, \ldots, \; g_s(x) \geq 0\}.$$

*Let $P$ be the cone of $\mathcal{P}(V)$ generated by $g_1, \ldots, g_s$, and let $f \in \mathcal{P}(V)$. Then:*

(i) $\forall x \in W \;\; f(x) \geq 0 \Leftrightarrow \exists m \in \mathbb{N} \;\; \exists g, h \in P \;\; fg = f^{2m} + h.$

(ii) $\forall x \in W \;\; f(x) > 0 \Leftrightarrow \exists g, h \in P \;\; fg = 1 + h.$

(iii) $\forall x \in W \;\; f(x) = 0 \Leftrightarrow \exists m \in \mathbb{N} \;\; \exists g \in P \;\; f^{2m} + g = 0.$

More formally, for the proof of (i) for instance:

*Proof.* Let $u_1, \ldots, u_k$ generate $\mathcal{I}(V)$. We denote by the same symbol polynomials in $R[X_1, \ldots, X_n]$ and their restrictions to $V$.

For (i), we apply Theorem 4.4.2 to the set

$f(x) < 0$

$$\{x \in R^n \mid g_1(x) \geq 0, \ldots, \; g_s(x) \geq 0, \; -f(x) \geq 0, \; f(x) \neq 0, \; u_1(x) = \ldots = u_k(x) = 0\},$$

$x \in W$

obtaining $g$ and $h$ in $P$, $m$ in $\mathbb{N}$, such that $h - fg + f^{2m} = 0$.

$\exists F \in$ cone generated by $g_i$ and $-f$
$\exists G \in$ monoid ——— $f$
$\exists H \in$ ideal ——— $u_j$

$F + G^2 + H = 0$

$F = h + (-f)g$, $h, g \in P$
$G = f^m$ for some $m \in \mathbb{N}$
$H = 0$ in $\mathcal{P}(V)$

$h - fg + f^{2m} = 0$ in $\mathcal{P}(V)$.

$\square$

# II HILBERT 17th PROBLEM

**Theorem 6.1.1.** *Let $R$ be a real closed field and $f \in R[X_1, \dots, X_n]$. If $f$ is nonnegative on $R^n$, then $f$ is a sum of squares in the field of rational functions $R(X_1, \dots, X_n)$.*

<u>Proof</u>. We have seen that in a field $F$, $\sum F^2$ is the intersection of the positive cones for all orderings.
So if the conclusion is not valid, there exists an ordering $\leq$ on $R(X_1, \dots, X_n)$ such that $f$ is negative.

- Denote $K$ the real closure of $(R(X_1, \dots, X_n), \leq)$.
- Then $-f \in K_+ = K^2$ so $-f$ has a square root in $K$, noted $\sqrt{-f}$.

As a consequence, there exists an $R$-algebra homomorphism

$$\frac{R[X_1, \dots, X_n][T]}{(fT^2+1)} \longrightarrow K$$
$$T \longmapsto \frac{1}{\sqrt{-f}}$$

- By Artin-Lang Theorem, there exists an $R$-algebra homomorphism

$$\frac{R[X_1, \dots, X_n][T]}{(fT^2+1)} \longrightarrow R$$

- Such a morphism is given by the evaluation at $(x, t) \in R^n \times R$ satisfying $f(x)t^2 + 1 = 0$. In particular $f(x) < 0$.

$\square$

Remark Via the Positivstellensatz, one has a more precise version. Recall:

**Corollary 4.4.3 (Positivstellensatz).** *Let $V \subset R^n$ be an algebraic set, $g_1, \dots, g_s \in \mathcal{P}(V)$ and*

$$W = \{x \in V \mid g_1(x) \geq 0, \dots, g_s(x) \geq 0\}.$$

*Let $P$ be the cone of $\mathcal{P}(V)$ generated by $g_1, \dots, g_s$, and let $f \in \mathcal{P}(V)$. Then:*

(i) $\forall x \in W \;\; f(x) \geq 0 \Leftrightarrow \exists m \in \mathbb{N} \;\; \exists g, h \in P \;\; fg = f^{2m} + h.$

- With $V = R^n = W$, we have $P = \sum R[X_1, \dots, X_n]^2$ so $f \geq 0$ on $R^n \implies \exists m \in \mathbb{N}$, $\exists g, h \in \sum R[X_1, \dots, X_n]^2$ : $fg = f^{2m} + h$
- Then $f(f^{2m} + h) = f^2 g = g_1$ is a sum of squares

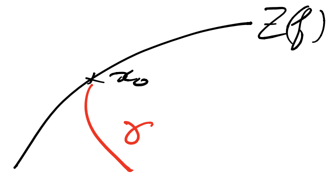
so
$$f = \frac{g_1}{f^{2m} + h} = \frac{g_1 (f^{2m} + h)}{(f^{2m} + h)^2} = \sum_{i=1}^{r} f_i^2$$

with $f_1, \dots, f_r \in R(X_1, \dots, X_n)$.

Note: • the rational functions $f_1, \dots, f_r$ are well-defined outside the zero set of $f$ ($f(x) \neq 0 \implies f^{2m}(x) + h(x) > 0$)

• they can be extended by continuity on their set of poles by the value $0$ as follows

<u>Actually</u> : • take $x_0 \in Z(f)$.




• By the Curve Selection Lemma,
there exists a continuous semi-algebraic curve
$\gamma : [0,1) \to \mathbb{R}^n$ such that $\gamma(0,1) \subseteq \mathbb{R}^n \setminus Z(f)$ and $\gamma(0) = x$.

• Then

$$f \circ \gamma(t) \xrightarrow[t \to 0]{} f(x) = 0$$

so that

$$\sum_{i=1}^{n} (f_i \circ \gamma(t))^2 \xrightarrow[t \to 0]{} 0$$

and thus

$$f_i \circ \gamma(t) \xrightarrow[t \to 0]{} 0 .$$

Such functions are called "continuous rational functions"

<u>Example</u> $\dfrac{x^3}{x^2+y^2}$ on $\mathbb{R}^2$.

<u>Remark</u> Hilbert $17^{th}$ problem is false on a real field

For instance, take:

- $F = \mathbb{R}(t)$ with the ordering $\mathcal{O}_+$
- the real closure of $(F, \mathcal{O}_+)$ is $\mathbb{R}((t^{\frac{1}{\mathbb{N}}}))_{alg}$
- consider $f(X) = (X^2 - t)^2 - t^3 \in F[X]$

- For $x \in F$, $x = \frac{p(t)}{q(t)}$ for $p, q \in \mathbb{R}[t]$ with $p \wedge q = 1$
- $f(x) = \left(\frac{p(t)^2 - t\, q^2(t)}{q^2(t)}\right)^2 - t^3 = \frac{(p(t)^2 - t\, q(t)^2)^2 - t^3 q(t)^4}{q(t)^4}$

and the numerator equals

$$p(t)^4 + t^2 \underbrace{(1-t)}_{>0} q(t)^4 - 2t\, p^2(t)\, q^2(t)$$

Its sign is given by the term of smaller order;

- if $p(0) \neq 0$, it is $p(0)^4$
- if $p(0) = 0$, then $q(0) \neq 0$ since $p \wedge q = 1$ and it is $t^2 q(0)^4$

In any case the sign is positive.

- However $f$ is not a sum of squares.
- Actually, $f$ is negative on $I$ and $-I$ where:

$$I = \Big(\underbrace{\sqrt{t(1-\sqrt{t})}}_{x_-}, \underbrace{\sqrt{t(1+\sqrt{t})}}_{x_+}\Big)$$

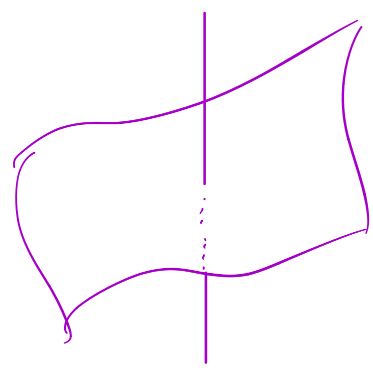
- $f$ has at most 4 roots.
- $f(x_\pm) = (t(1 \pm \sqrt{t}) - t)^2 - t^3 = (\pm t\sqrt{t})^2 - t^3 = t^3 - t^3 = 0$

  so the roots are $\{\pm x_\pm\}$
- Between $x_+$ and $x_-$ $f$ is negative: $f(\sqrt{t}) = -t^3 < 0$.

E. Artin also considered Hilbert's $17^{\text{th}}$ problem for an irreducible algebraic subset $V$ of $R^n$, instead of $R^n$. This is different from the case of affine space: a polynomial that is a sum of squares in $R(X_1, \ldots, X_n)$ is clearly nonnegative on $R^n$, but an element of $\mathcal{P}(V)$ that is a sum of squares in $\mathcal{K}(V)$ (the field of fractions of $\mathcal{P}(V)$) is not necessarily nonnegative everywhere on $V$!!!

*Example 6.1.8.* Let $V$ be the Cartan umbrella in $R^3$, given by the equation $x^3 = z(x^2 + y^2)$. Then $f = x^2 + y^2 - z^2 \in \mathcal{P}(V)$ is negative on the stick $x = y = 0$ outside the origin. Nevertheless, $f$ is a sum of squares in $\mathcal{K}(V)$:

$$f = x^2 + y^2 - \frac{x^6}{(x^2+y^2)^2} = \frac{3x^4y^2 + 3x^2y^4 + y^6}{(x^2+y^2)^2} .$$



Remark This phenomenon has to do with the singularities of the Cartan umbrella.