MOTIVATION FOR REAL ALGEBRA : HILBERT 17th PROBLEM

MATHEMATICAL PROBLEMS

DAVID HILBERT

Lecture delivered before the International Congress of Mathematicians at Paris in 1900.

$\forall x \in \mathbb{R}^m, \ P(x) \geq 0.$

cf. Motzkin example, 1967

17. Expression of definite forms by squares

A rational integral function or form in any number of variables with real coefficients such that it becomes negative for no real values of these variables, is said to be *definite*. The system of all definite forms is invariant with respect to the operations of addition and multiplication, but the quotient of two definite forms—in case it should be an integral function of the variables—is also a definite form. The square of any form is evidently always a definite form. But since, as I have shown, not every definite form can be compounded by addition from squares of forms, the question arises—which I have answered affirmatively for ternary forms —whether every definite form may not be expressed as a quotient of sums of squares of forms. At the same time it is desirable, for certain questions as to the possibility of certain geometrical constructions, to know whether the coefficients of the forms to be used in the expression may always be taken from the realm of rationality given by the coefficients of the form represented.

Artin Theorem, 1927

H17 :
Let $P \in \mathbb{R}[X_1, \ldots, X_m]$ be such that $\forall x \in \mathbb{R}^m, \ P(x) \geq 0.$
Do there exist $P_1, \ldots, P_r, Q_1, \ldots, Q_r \in \mathbb{R}[X_1, \ldots, X_m]$ such that

$$P = \sum_{i=1}^{r} \left(\frac{P_i}{Q_i}\right)^2 \quad \text{in } \mathbb{R}(X_1, \ldots, X_m) \quad ?$$

<u>Answers</u> : • yes if $m=2$, Hilbert 1888

• yes ; Artin 1927

• one can choose $r \leq 2^m$; Pfister 1967

• false if $\mathbb{R}$ replaced by <u>ordered field</u>

↳ need a real closed field.

<u>Initial question</u> : $P = \sum_{i=1}^{r} P_i^2$?

• <u>ok if $m=1$</u>, and $r=2$ is possible

• $P = \prod_k P_k^{d_k}$ irreducible decomposition

with $P_k = X-a$, $a \in \mathbb{R}$ or $P_k = (X-\alpha)(X-\bar{\alpha})$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$
$= (X-a)^2 + b^2$ if $\alpha = a+ib$

• Note that $d_k \equiv 0 \ [2]$ if $\deg P_k = 1$ since $P \geq 0$.

So $P = Q^2 \prod_{k : d_k \text{ odd}} \left((X-a_k)^2 + b_k^2 \right)$

• Finally use

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

• <u>Case $m=2$</u> : • rational functions are needed (Hilbert 1888)

• first counter example by Motzkin 1967

$P = X^4Y^2 + X^2Y^4 + 1 - 3X^2Y^2$

- <u>proof of $P \geq 0$</u>

Arithmetic mean of x^4y^2, x^2y^4 and 1 : $m_a = \dfrac{x^4y^2 + x^2y^4 + 1}{3}$

Geometric ——————— : $m_g = \sqrt[3]{x^6y^6} = x^2y^2$

Then $m_a \geq m_g$ implies $x^4y^2 + x^2y^4 + 1 \geq 3x^2y^2$

- <u>$P \notin \sum \mathbb{R}[X,Y]^2$</u> By contradiction.

Assume $P = \sum_{i=1}^{n} P_i^2$

* $\deg P_i \leq 3$, write $P_i = X Q_i(X,Y) + R_i(Y)$

* make $X=0$ in P: $1 = P(0,Y) = \sum_i R_i^2$

So $R_i = r_i \in \mathbb{R}$.

* make $Y=0$ in P:

$$1 = P(X,0) = \sum_i \left(X^2 Q_i^2 + 2XQ_i r_i + r_i^2 \right)$$

$$= X^2 \sum_i Q_i(X,0)^2 + 2X \sum_i r_i Q_i + \underbrace{\sum_i r_i^2}_{=1}$$

hence

$$\boxed{X^2 \sum_i Q_i(X,0)^2 = 2X \sum_i r_i Q_i}$$

Choose i_0 such that $d = \deg Q_{i_0}(X,0)$ is maximal

LHS of degree $2d+2$

RHS ——— $\leq d+1$

So $d = -\infty$ and $Q_i(X,Y) = Y\, G_i(X,Y)$

Thus $P_i = XY\, G_i(X,Y) + r_i$, $\deg G_i \leq 1$.

* Rewrite $P = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$:

$$x^2y^2\sum_i G_i^2 + 2xy\sum_i r_iG_i + 1 = x^2y^2(x^2+y^2-3) + 1$$

hence

$$\underbrace{x^2y^2}_{\deg = 4}\left(\sum_i G_i^2 - x^2 - y^2 + 3\right) = \underbrace{-2xy\sum_i r_iG_i}_{\deg \leq 3}$$

Thus $\sum_i G_i^2 = x^2+y^2-3$

Apply at $x=y=0$ leads to a CONTRADICTION

<u>Remark</u> $P = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$ is equal to

$$\frac{x^2y^2(x^2+y^2+1)(x^2+y^2-2)^2 + (x^2-y^2)^2}{(x^2+y^2)^2}$$

so P is a sum of 4 squares in $\mathbb{R}(x,y)$.

<u>general ideas toward the proof of Artin</u>

- notion of ordered fields
- on a given field, several orderings may exist.
- a non negative element with respect to all orderings

will be the sum of squares.

- K ordered field $\rightsquigarrow$ there exist an ordering on the field $K(X_1,\dots,X_n)$ that extends the ordering on K.

- Let K admits a unique ordering. Are equivalent:

  $P \in K(X_1,\dots,X_n)$ is negative for a certain ordering

  $\iff$

  there exists an algebraic extension $K \hookrightarrow R$ compatible with ordering such that:

  $$\exists x \in R^n : \quad P(x) < 0$$

<u>Program</u>

- basics on semi-algebraic sets
- real closed fields
- Artin-Lang Theorem and H17
- real algebraic sets
- Euler characteristic and links
- algebraically constructible functions