

Quantitative aspects of two algebraic proofs of the fundamental theorem of algebra

Marie-Françoise Roy

IRMAR, Université de Rennes 1, France

Work in progress with Daniel Perrucci

Perspectives in Real Algebraic Geometry,
Conference in memory of Jean-Jacques Risler
CIRM 18-22 september 2017

Real closed fields

Theorem

\mathbb{R} a totally ordered field. The following are equivalent definitions of being a real closed field.

1. *IVT: the Intermediate Value Theorem, holds for polynomials : if $P \in \mathbb{R}[X]$,*

$$a < b, P(a)P(b) < 0 \implies \exists c \in (a, b) P(c) = 0.$$

2. *FTA: $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[T]/(T^2 + 1)$ is an algebraically closed field.*
3. *all positive numbers have a square root, all polynomials of odd degree have a root.*

Real closed fields

1 \Rightarrow 3 is easy.

2 \Rightarrow 1 is easy: IVT follows from the factorization of P in linear and quadratic factors.

Laplace's proof of 3 \Rightarrow 2 (FTA) constructs a polynomial of very high odd degree.

Laplace's proof

Proof of 3 \Rightarrow 2 (Laplace's algebraic proof of fundamental theorem of algebra)

$P \in \mathbb{R}[X]$ of degree $d = 2^k s$ with s odd, P has a root in \mathbb{C} by induction on m . If $k = 0$, d is odd and P has a root in $\mathbb{R} \subset \mathbb{C}$. Otherwise, define for $h \in \mathbb{Z}$,

$$Q_h(X_1, \dots, X_d, X) = \prod_{\lambda < \mu} (X - X_\lambda - X_\mu - hX_\lambda X_\mu)$$

$\deg_X(Q_h) = d(d-1)/2 = 2^{k-1} s'$ with s' odd.

x_1, \dots, x_d roots of P in an algebraically closed field \mathbb{C}' containing \mathbb{R} (\mathbb{C}' contains \mathbb{C}),

$$Q_h(x_1, \dots, x_d, X) \in \mathbb{R}[X],$$

(symmetric in x_1, \dots, x_d , relation between elementary symmetric functions and coefficients).

Laplace's proof

By induction, $Q_h(x_1, \dots, x_d, X)$ has a root in \mathbb{C} , hence for each $h \in \mathbb{Z}$, there exist λ and μ with $x_\lambda + x_\mu + hx_\lambda x_\mu \in \mathbb{C}$.

Infinite number of elements in \mathbb{Z} , finite number of λ, μ .

By the pidgeon-hole principle, there exist λ, μ, h and h' , $h \neq h'$, such that $x_\lambda + x_\mu + hx_\lambda x_\mu \in \mathbb{C}$, $x_\lambda + x_\mu + h'x_\lambda x_\mu \in \mathbb{C}$. So $x_\lambda + x_\mu \in \mathbb{C}$ and $x_\lambda x_\mu \in \mathbb{C}$. x_λ and x_μ solutions of a quadratic equation with coefficients in \mathbb{C} , which has its two solutions in \mathbb{C} (classical method for solving polynomials of degree 2 works in \mathbb{C} when \mathbb{R} is real closed).

Thus P has a root in \mathbb{C} .

If $P \in \mathbb{C}[X]$, $P\bar{P} \in \mathbb{R}[X]$ had a root $z \in \mathbb{C}$. If z is a root of \bar{P} , \bar{z} is a root of P .

Real closed fields

Laplace's proof of the Fundamental Theorem of Algebra produces at the end of the induction a polynomial of very high odd degree.

A recent proof of the Fundamental Theorem of Algebra by Michael Eisermann in [Eis] is also based on [IVT], but involves the geometric concept of winding number.

Real closed fields

Laplace's proof of the Fundamental Theorem of Algebra produces at the end of the induction a polynomial of very high odd degree.

A recent proof of the Fundamental Theorem of Algebra by Michael Eisermann in [Eis] is also based on [IVT], but involves the geometric concept of winding number.

It is based on very classical ideas known already in the 19 th centuries but details (often non trivial) are fixed.

Can we say something about this proof compared to Laplace's proof from a quantitative point of view ?

Motivation : transforming Laplace's proof of FTA into algebraic identities is an essential ingredient in the proof the elementary recursive bounds on Hilbert's 17 th problem (as well as for Positivstellensatz, real Nullstellensatz) in [LPR]. Another algebraic proof of FTA using polynomials of smaller degrees gives hope to improve these bounds.

Quantitative FTA

\mathbb{N}^* set of natural numbers ≥ 1 . For each $d \in \mathbb{N}^*$, define the following properties on a totally ordered field \mathbb{R} .

- ▶ $[\text{IVT}]_d$: for every polynomial $P \in \mathbb{R}[X]$ with $\deg P \leq d$ and every a, b in \mathbb{R} with $a < b$ such that $P(a)P(b) < 0$, there exists $c \in \mathbb{R}$ with $a < c < b$ such that $P(c) = 0$.
- ▶ $[\text{FTA}]_d$: for every polynomial $P \in \mathbb{R}[i][X] \setminus \mathbb{R}[i]$ with $\deg P \leq d$, there exists $z \in \mathbb{R}[i]$ such that $P(z) = 0$.

Problem

which is the lowest value of $\alpha(d) \in \mathbb{N}^*$ for which it can be shown that

$$[\text{IVT}]_{\alpha(d)} \text{ implies } [\text{FTA}]_d?$$

Degree bounds for Laplace

Notation

Let $\beta, \gamma : \mathbb{N}^* \rightarrow \mathbb{N}^*$ defined as follows:

$$\beta(d) = \begin{cases} d & \text{if } d \text{ is odd,} \\ \beta\left(\frac{d(d-1)}{2}\right) & \text{if } d \text{ is even,} \end{cases}$$

$$\gamma(d) = \max_{1 \leq e \leq d} \{\beta(2e)\}.$$

From Laplace's proof we deduce:

$$[\text{IVT}]_{\gamma(d)} \text{ implies } [\text{FTA}]_d.$$

So that $\alpha(d) \leq \gamma(d)$. It is not very difficult to prove that

$$\left(\frac{3}{8}\right)^{d-1} d^d \leq \gamma(d) \leq 2d^{2d}.$$

Our result

Recently, Eisermann wrote a proof of the Fundamental Theorem of Algebra [Eis] which is also based on [IVT], but involves the geometric concept of winding number. This proof is the essential path we follow to obtain our main result, which is the following:

Notation

Let $\delta : \mathbb{N}^* \rightarrow \mathbb{N}^*$:

$$\delta(d) = 2d^2$$

For $d \in \mathbb{N}^*$

$$[\text{IVT}]_{\delta(d)} \text{ implies } [\text{FTA}]_d.$$

Our main new ingredient compared to [Eis] is the use of subresultants.

The paper is not entirely written.

IVT of bounded degree

Set a fixed $e \in \mathbb{N}^*$ and suppose that \mathbb{R} is an ordered field satisfying $[\text{IVT}]_e$.

Aim: recall definition and properties of Cauchy index following [Eis] keeping in mind that we only assume that the Intermediate Value Theorem holds for polynomials of degree less than or equal to e . It is only for $P \in \mathbb{R}[X]$ with $\deg P \leq e$ that we know that if P has no roots on an interval $I \subset \mathbb{R}$, then P has constant sign (different from 0) on I .

Cauchy index

Let $P, Q \in \mathbb{R}[X] \setminus \{0\}$ and $a \in \mathbb{R}$.

► Suppose

$$\frac{P}{Q} = (X - a)^m \frac{\tilde{P}}{\tilde{Q}}$$

with $m \in \mathbb{Z}$ and $\tilde{P}(a) \neq 0, \tilde{Q}(a) \neq 0$.

For $\varepsilon \in \{+, -\}$,

$$\lim_a^\varepsilon \left(\frac{P}{Q} \right) = \begin{cases} 0 \in \mathbb{R} & \text{if } m > 0, \\ \frac{\tilde{P}(a)}{\tilde{Q}(a)} \in \mathbb{R} \setminus \{0\} & \text{if } m = 0, \\ \varepsilon^m \cdot \text{sign} \left(\frac{\tilde{P}(a)}{\tilde{Q}(a)} \right) \cdot (+\infty) \in \{+\infty, -\infty\} & \text{if } m < 0. \end{cases}$$

Cauchy index

- ▶ For $\varepsilon \in \{+, -\}$,

$$\text{Ind}_a^\varepsilon\left(\frac{P}{Q}\right) = \begin{cases} \frac{1}{2} & \text{if } \lim_a^\varepsilon\left(\frac{P}{Q}\right) = +\infty, \\ -\frac{1}{2} & \text{if } \lim_a^\varepsilon\left(\frac{P}{Q}\right) = -\infty, \\ 0 & \text{otherwise.} \end{cases}$$

- ▶ The Cauchy Index of the rational function $\frac{P}{Q}$ at a is

$$\text{Ind}_a\left(\frac{P}{Q}\right) = \text{Ind}_a^+\left(\frac{P}{Q}\right) - \text{Ind}_a^-\left(\frac{P}{Q}\right).$$

Cauchy index

Let $P, Q \in \mathbb{R}[X]$ and $a, b \in \mathbb{R}$.

- ▶ If $P, Q \neq 0$ and $a < b$, the Cauchy Index of $\frac{P}{Q}$ on the interval $[a, b]$ is

$$\text{Ind}_a^b\left(\frac{P}{Q}\right) = \text{Ind}_a^+\left(\frac{P}{Q}\right) + \sum_{x \in (a,b)} \text{Ind}_x\left(\frac{P}{Q}\right) - \text{Ind}_b^-\left(\frac{P}{Q}\right),$$

(middle sum well-defined since only roots x of Q in (a, b) contribute)

- ▶ If $P, Q \neq 0$ and $a > b$,

$$\text{Ind}_a^b\left(\frac{P}{Q}\right) = -\text{Ind}_b^a\left(\frac{P}{Q}\right).$$

- ▶ In every other case,

$$\text{Ind}_a^b\left(\frac{P}{Q}\right) = 0.$$

Additivity of Cauchy index

Lemma

For any $a, c_1, \dots, c_k, b \in \mathbb{R}$ and any $P, Q \in \mathbb{R}[X]$,

$$\text{Ind}_a^b \left(\frac{P}{Q} \right) = \text{Ind}_a^{c_1} \left(\frac{P}{Q} \right) + \sum_{1 \leq i \leq k-1} \text{Ind}_{c_i}^{c_{i+1}} \left(\frac{P}{Q} \right) + \text{Ind}_{c_k}^b \left(\frac{P}{Q} \right).$$

No condition at the extremities because of the $1/2$ in the definition given in [Eis]!

Proposition (Inversion formula)

Let $a, b \in \mathbb{R}$ and $P, Q \in \mathbb{R}[X]$ with $\deg P, \deg Q \leq e$ and such that P and Q have no common root in $[a, b]$. Then

$$\begin{aligned} & \operatorname{Ind}_a^b \left(\frac{Q}{P} \right) + \operatorname{Ind}_a^b \left(\frac{P}{Q} \right) \\ &= \frac{1}{2} \left| \operatorname{sign}(P(a)) - \operatorname{sign}(Q(a)) \right| - \frac{1}{2} \left| \operatorname{sign}(P(b)) - \operatorname{sign}(Q(b)) \right|. \end{aligned}$$

(keep in mind that we only assume that the Intermediate Value Theorem holds for polynomials of degree less than or equal to e)

σ, τ -Sturm chains

suitable generalizations of results from [Eis] needed to be able to use subresultants (aiming at good degree bound)s; fixed $e \in \mathbb{N}^*$ and suppose that \mathbb{R} is an ordered field satisfying $[\text{IVT}]_e$.

Let $n \in \mathbb{N}^*$, $\sigma, \tau \in \{-1, 1\}^{n-1}$ with $\sigma = (\sigma_1, \dots, \sigma_{n-1})$ and $\tau = (\tau_1, \dots, \tau_{n-1})$, and I be an interval of \mathbb{R} .

A sequence of polynomials (S_0, \dots, S_n) in $\mathbb{R}[X]$ is a (σ, τ) -chain with respect to I if for $1 \leq k \leq n-1$ there exists polynomials $A_k, B_k, C_k \in \mathbb{R}[X]$ such that

- ▶ $A_k S_{k+1} + B_k S_k + C_k S_{k-1} = 0$,
- ▶ for every $x \in I$, $\text{sign}(A_k(x)) = \sigma_k$,
- ▶ for every $x \in I$, $\text{sign}(C_k(x)) = \tau_k$ or $\text{sign}(C_k(x)) = 0$.

σ, τ -Sturm chains

A sequence of polynomials (S_0, \dots, S_n) in $\mathbb{R}[X]$ is a (σ, τ) -Sturm chain with respect to I if it is a (σ, τ) -chain with respect to I and S_{n-1} and S_n have no common root on I .

A sequence of polynomials (S_0, \dots, S_n) in $\mathbb{R}[X]$ is a *good* (σ, τ) -Sturm chain with respect to I if it is a (σ, τ) -chain with respect to I and S_n have no root on I .

Subresultant polynomials

Their coefficients are minors extracted of Sylvester matrix of P, Q .
 The subresultant polynomials are proportional to polynomials in the remainder sequence, or zero. A defective subresultant is proportional to the next non-zero one, which is non-defective.

$$SR_{11}(P, P') = X^{11} - X^{10} + 1,$$

$$SR_{10}(P, P') = 11X^{10} - 10X^9,$$

$$SR_9(P, P') = 10X^9 - 121,$$

$$SR_8(P, P') = -110X + 100,$$

$$SR_i(P, P') = 0, i = 2, \dots, 7$$

$$SR_1(P, P') = -214358881(-110 * X + 100),$$

$$SR_0(P, P') = -275311670611.$$

$SR_8(P, P')$ and $SR_1(P, P')$ are proportional and in between there are 0.

Examples

- ▶ The classical Sturm sequence of P, Q is a good Sturm σ, τ -Sturm chain, with σ, τ composed only of 1.
- ▶ It is the same for the signed subresultant sequence of P, Q in the non-defective case (when the degrees drop one by one)
- ▶ In the defective case, the non defective signed subresultant sequence form a good σ, τ - Sturm chain (for well chosen σ, τ -depending on the degree structure of the subresultant sequence).

Examples

Signs at 10/11, just before and just after. Usual subresultant theory

$$\begin{array}{rcccc}
 \text{SR}_9(P, P') & - & - & - \\
 \text{SR}_8(P, P') & + & 0 & - \\
 \text{SR}_1(P, P') & - & 0 & + \\
 \text{SR}_0(P, P') & - & - & - \\
 \hline
 V & 2 & 2 & 2
 \end{array}$$

Cannot be counted by 1/2. Not elegant at all.

New method

$$\begin{array}{rcccc}
 \text{SR}_9(P, P') & - & - & - \\
 \text{SR}_1(P, P') & - & 0 & + \\
 \text{SR}_0(P, P') & - & - & - \\
 \hline
 V(\epsilon) & 0 & 0 & 0
 \end{array}$$

Take $\epsilon_1 = -\epsilon_2$!

Examples

If $P(X, Y), Q(X, Y)$ are bivariate polynomials, denote by

$$S_0(X, Y), \dots, S_{n-1}(X, Y), S_n(X)$$

the signed pseudo-remainder sequence of P, Q with respect to Y

- ▶ $S_0(x, Y), \dots, S_{n-1}(x, Y), S_n(x)$ is a good Sturm chain for every $x \in \mathbb{R}, S_n(x) \neq 0$
- ▶ $S_0(X, y), \dots, S_{n-1}(X, y), S_n(X)$ is a good Sturm chain on any interval I does not containing a zero of S_n .

Examples

Denote by

$$R_0(X, Y), \dots, R_{n-1}(X, Y), R_n(X)$$

the non defective polynomials in the signed subresultant sequence of P, Q with respect to Y (note that $R_n(X)$ is -up to sign- the resultant of P, Q with respect to Y),

- ▶ $R_0(x, Y), \dots, R_{n-1}(x, Y), R_n(x)$ is a good σ, τ - Sturm chain for every $x \in \mathbb{R}, R_n(x) \neq 0$ (for well chosen σ, τ)
- ▶ $R_0(X, y), \dots, R_{n-1}(X, y), R_n(X)$ is a good σ, τ -Sturm chain on any interval I does not containing a zero of R_n (for well chosen σ, τ)

Note that when specializing y the degrees in X in the sequence are increasing in both cases. The degree bounds with respect to X are exponential for the pseudo-remainder sequence and of degree $2d^2$ for the subresultant sequence.

Sign variations

Let $n \in \mathbb{N}^*$, $\epsilon \in \{-1, 1\}^n$ with $\epsilon = (\epsilon_1, \dots, \epsilon_n)$, $a, b \in \mathbb{R}$ and (S_0, \dots, S_n) in $\mathbb{R}[X]$. Define

$$V(\epsilon)_a(S_0, \dots, S_n) = \sum_{1 \leq i \leq n} \frac{1}{2} \epsilon_i \left| \text{sign}(S_{i-1}(a)) - \text{sign}(S_i(a)) \right|$$

and

$$V(\epsilon)_a^b(S_0, \dots, S_n) = V(\epsilon)_a(S_0, \dots, S_n) - V(\epsilon)_b(S_0, \dots, S_n).$$

ϵ -sign variations and Cauchy index

Let $n \in \mathbb{N}^*$, $\sigma, \tau \in \{-1, 1\}^{n-1}$. Define $\epsilon(\sigma, \tau) = (\epsilon_1, \dots, \epsilon_n) \in \{-1, 1\}^n$ by

$$\epsilon_i = \prod_{1 \leq j \leq i-1} \sigma_j \tau_j$$

for $1 \leq i \leq n$. Note that it is always the case that $\epsilon_1 = 1$.

Proposition

Let $n \in \mathbb{N}^*$, $\sigma, \tau \in \{-1, 1\}^{n-1}$, $\epsilon = \epsilon(\sigma, \tau) \in \{-1, 1\}^n$, $a, b \in \mathbb{R}$ with $a < b$ and $I = [a, b]$. If (S_0, \dots, S_n) is a (σ, τ) -Sturm chain with respect to I and $\deg S_0, \dots, \deg S_n \leq e$, then

$$\text{Ind}_a^b \left(\frac{S_1}{S_0} \right) + \epsilon_n \text{Ind}_a^b \left(\frac{S_{n-1}}{S_n} \right) = V(\epsilon)_a^b(S_0, \dots, S_n).$$

generalization of a result of [Eis]. Note the condition on the degrees.

ϵ -sign variations and Cauchy index

Corollary

Let $n \in \mathbb{N}^*$, $\sigma, \tau \in \{-1, 1\}^{n-1}$, $\epsilon = \epsilon(\sigma, \tau) \in \{-1, 1\}^n$, $a, b \in \mathbb{R}$ with $a < b$ and $I = [a, b]$. If (S_0, \dots, S_n) is a good (σ, τ) -Sturm chain with respect to I and $\deg S_0, \dots, \deg S_n \leq e$, then

$$\text{Ind}_a^b \left(\frac{S_{n-1}}{S_n} \right) = 0$$

and therefore, by Proposition 2,

$$\text{Ind}_a^b \left(\frac{S_1}{S_0} \right) = V(\epsilon)_a^b(S_0, \dots, S_n).$$

Geometric intuition of the winding number

If γ is a piecewise polynomial loop, $w(\gamma)$ counts the number of turns that a loop γ performs around 0.

- ▶ normalization: the winding number of a the (counterclockwise) loop γ defined by a rectangle Γ

$$w(\gamma) = \begin{cases} 1 & \text{if } 0 \in \text{Int}(\Gamma), \\ 0 & \text{if } 0 \in \mathbb{C} \setminus \Gamma, \end{cases}$$

- ▶ multiplicativity: $w(\gamma_1 \cdot \gamma_2) = w(\gamma_1) + w(\gamma_2)$.
- ▶ homotopy invariance: two homotopic loop have the same winding number

Complex and real variables

$\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ with $Z = X + iY$ To $F \in \mathbb{C}[Z]$ is associated its conjugate \bar{F} , which makes it possible to define its real and imaginary part which are in $\mathbb{R}[X, Y]$.

Definition of winding number

algebraic definition coming from [Eis] $\Gamma = [c_0, c_1] \times [d_0, d_1] \subset \mathbb{R}^2$
 be a rectangle.

$$\begin{aligned} \gamma_1 : [0, 1] &\rightarrow \mathbb{R}^2, & \gamma_1(X) &= (c_1, d_0 + X(d_1 - d_0)), \\ \gamma_2 : [0, 1] &\rightarrow \mathbb{R}^2, & \gamma_2(X) &= (c_1 + X(c_0 - c_1), d_1), \\ \gamma_3 : [0, 1] &\rightarrow \mathbb{R}^2, & \gamma_3(X) &= (c_0, d_1 + X(d_0 - d_1)), \\ \gamma_4 : [0, 1] &\rightarrow \mathbb{R}^2, & \gamma_4(X) &= (c_0 + X(c_1 - c_0), d_0). \end{aligned}$$

$F \in C[Z]$, *winding number* $w(F|\partial\Gamma)$ defined by

$$\begin{aligned} 2w(F|\partial\Gamma) &= \text{Ind}_0^1 \left(\frac{\text{re}(F \circ \gamma_1)}{\text{im}(F \circ \gamma_1)} \right) + \text{Ind}_0^1 \left(\frac{\text{re}(F \circ \gamma_2)}{\text{im}(F \circ \gamma_2)} \right) \\ &\quad + \text{Ind}_0^1 \left(\frac{\text{re}(F \circ \gamma_3)}{\text{im}(F \circ \gamma_3)} \right) + \text{Ind}_0^1 \left(\frac{\text{re}(F \circ \gamma_4)}{\text{im}(F \circ \gamma_4)} \right). \end{aligned}$$

Additivity of winding number

Let $\Gamma = [c_0, c_1] \times [d_0, d_1] \subset \mathbb{R}^2$ be a rectangle and consider a partition of Γ in a finite number of rectangles $\Gamma_1, \dots, \Gamma_n$ whose sides are parallel to the axis. For $F \in \mathbb{R}[i][Z]$, we have

$$w(F|\partial\Gamma) = \sum_{1 \leq i \leq n} w(F|\partial\Gamma_i).$$

Also normalization, multiplicativity, homotopy ...

Eisermann's result

Consider a polynomial $F \in \mathbb{C}[Z]$ and a rectangle $\Gamma \subset \mathbb{C} = \mathbb{R}^2$ such that F does not vanish at any of the vertices of Γ . Then the algebraic winding number $w(F|\partial\Gamma)$ counts the number of zeroes of F in Γ : each zero in the interior of Γ is counted with its multiplicity, whereas each zero on an edge of $\partial\Gamma$ is counted with half its multiplicity.

Key result

Lemma

Let $\Gamma = [c_0, c_1] \times [d_0, d_1] \subset \mathbb{R}^2$ be a rectangle. If the polynomial $F \in \mathbb{C}[X, Y]$ satisfies $F(x, y) \neq 0$ for all $(x, y) \in \Gamma$, then $w(F|\partial\Gamma) = 0$.

By contraposition if $w(F|\partial\Gamma) \neq 0$, F has a root in Γ .

Proved by [Eis] using pseudo-remainders with respect to Y and specializing in both directions. Compatibilities at the corners of the rectangle are needed.

Improved by us using subresultants with respect to Y , which provides degree bounds $2d^2$ when specializing with respect to y .

Conclusion

We studied the following problem **Problem**

which is the lowest value of $\alpha(d) \in \mathbb{N}^*$ for which it can be shown that

$$[\text{IVT}]_{\alpha(d)} \text{ implies } [\text{FTA}]_d?$$

- ▶ Laplace's proof gives

$$[\text{IVT}]_{\gamma(d)} \text{ implies } [\text{FTA}]_d$$

with $\gamma(d)$ exponential in d

- ▶ Using subresultant and the notion of σ, τ -chain, we improved Eisermann's method and proved that

$$[\text{IVT}]_{2d^2} \text{ implies } [\text{FTA}]_d$$

We do not know if this can be useful to get better degree bounds for Hilbert's 17 th problem, Positivstellensatz and real Nullstellensatz.

Références

[BPR] Basu S., Pollack R. and Roy M.-F. *Algorithms in real algebraic geometry*, Springer 2nd edition (2006), revised and completed version of 2nd edition, <https://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted3.html> (2016)

[Eis] M. Eisermann, The fundamental theorem of algebra made effective: an elementary real-algebraic proof via Sturm chains. *Amer. Math. Monthly* 119 (2012), no. 9, 715–752.

[LPR] H. Lombardi, D. Perrucci, M.-F. Roy, An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem. Accepted for publication at *Mem. Amer. Math. Soc.*