

The Fundamental Theorem of Algebra made effective: an elementary real-algebraic proof via Sturm chains

Michael Eisermann

Institut Fourier, Université Grenoble
www-fourier.ujf-grenoble.fr/~eiserm

January 6, 2009



Carl Friedrich Gauss (1777-1855)



Augustin Louis Cauchy (1798-1857)



Charles-François Sturm (1803-1855)

MAA-AMS Joint Mathematics Meetings in Washington DC
AMS Session on Analytic Function Theory

1/10

Prologue

The fundamental theorem is a classical result of 19th century mathematics. It is often used, cited, taught, ... and thus deserves due attention. It is still of interest today, for example concerning its algorithmic and numerical aspects.

The statement of the theorem cannot surprise you, of course, but perhaps a beautiful proof can. I present here a real-algebraic proof that has the remarkable property of being elegant, elementary, and effective. The aim of my talk is to popularise this proof.

The proof is based on ideas of Gauß (1799), Cauchy (1831/37), and Sturm (1836), but seems to be unknown today. I have had the chance to discover it while preparing a computer algebra course, and was much astonished not to find it in the modern literature.

My contribution is thus to save this beautiful proof from oblivion and to develop and expound Sturm's sketch in modern rigour. (Since this is a short talk, I can only give an overview and have to refer to my article for details.)

2/10

Overview

- 1 The fundamental theorem of algebra
 - Three types of proofs
 - From the real numbers to real closed fields
 - Real roots of real polynomials
 - Complex roots of complex polynomials
 - From existence to locating complex roots

Reference:

*The Fundamental Theorem of Algebra made effective:
an elementary real-algebraic proof via Sturm chains*
www-fourier.ujf-grenoble.fr/~eiserm/publications.html#roots

3/10 1/0

The fundamental theorem of algebra

Theorem

Every complex polynomial of degree n has n complex roots.

More explicitly: Let \mathbb{R} be the field of real numbers and let $\mathbb{C} = \mathbb{R}[i]$, $i^2 = -1$.

Theorem

For every polynomial

$$F = Z^n + a_{n-1}Z^{n-1} + \dots + a_1Z + a_0$$

with complex coefficients $a_0, a_1, \dots, a_{n-1} \in \mathbb{C}$

there exist $z_1, z_2, \dots, z_n \in \mathbb{C}$ such that

$$F = (Z - z_1)(Z - z_2) \dots (Z - z_n).$$

Natural questions:

- Is there an elementary yet geometrically appealing proof?
- Can we weaken the hypothesis? to which ordered fields?
- Can we strengthen the conclusion? make it effective?

4/10

Three types of proofs

There are essentially three proof strategies:

- 1 analysis, using compactness, integration, Stokes, ...;
- 2 algebra, using symmetric functions, Galois theory, ...;
- 3 algebraic topology, using some form of winding number.

The proof I advertise here is of the last type but *real-algebraic*.

Why should we care for yet another proof?

- ✓ The proof is elementary: it uses only the intermediate value theorem and arithmetic of real polynomials in one variable.
- ✓ All arguments extend verbatim to all real closed fields.
- ✓ The proof is constructive and allows to locate the roots.
- ✓ The algorithm is easy to implement and reasonably efficient.
- ✓ Formal, computer-verifiable proof: theorem + algorithm.

Overall the real-algebraic proof offers an excellent cost-benefit ratio.

§1.1

§10 §1.2

From the real numbers to real closed fields

Theorem (the real numbers)

For every ordered field $(\mathbf{R}, +, \cdot, \leq)$ the following conditions are equivalent:

- 1 (\mathbf{R}, \leq) satisfies the least upper bound property.
- 2 Every interval $[a, b] \subset \mathbf{R}$ is compact.
- 3 Every interval $[a, b] \subset \mathbf{R}$ is connected.
- 4 Every continuous $f: \mathbf{R} \rightarrow \mathbf{R}$ satisfies the intermediate value property:
 $f(a)f(b) < 0 \implies \exists x \in \mathbf{R} : (x-a)(x-b) < 0 \wedge f(x) = 0$.

Any two such fields are isomorphic by a unique field isomorphism.
 One such object exists: we call it the field of real numbers.

This requires second-order logic. Much less is sufficient:

Definition (real closed field)

An ordered field $(\mathbf{R}, +, \cdot, \leq)$ is called *real closed* if every polynomial $P \in \mathbf{R}[X]$ satisfies the intermediate value property.

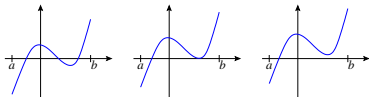
Examples: the real numbers \mathbb{R} , the real-algebraic numbers $\mathbb{Q}^c \subset \mathbb{C}$, ...

Every ordered field has a unique real closure. Example: $\mathbb{R}(X)^c$.

§10

Real roots of real polynomials

How can we determine the number of roots of $P \in \mathbf{R}[X]$ in $[a, b]$?



Sturm's theorem

If \mathbf{R} is real closed, then $\#\{x \in [a, b] \mid P(x) = 0\} = V_a^b(S_0, S_1, \dots, S_n)$.

Here the Sturm chain S_0, S_1, \dots, S_n is obtained from $S_0 = P$ and $S_1 = P'$ by euclidean division $S_{k-1} = Q_k S_k - S_{k+1}$ until eventually $S_{n+1} = 0$.

This provides an explicit and efficient algorithm!

§1.3

§10 §1.4

Complex roots of complex polynomials

Let \mathbf{R} be a real closed field and let $\mathbf{C} = \mathbf{R}[i]$ where $i^2 = -1$.

Let Ω be the set of piecewise polynomial loops $\gamma: [0, 1] \rightarrow \mathbf{C}^*$, $\gamma(0) = \gamma(1)$.

Theorem

We can construct a map $\text{ind}: \Omega \rightarrow \mathbb{Z}$ satisfying the following properties:

- 0 Computation: $\text{ind}(\gamma)$ is calculated by Sturm's algorithm over \mathbf{R} .
- 1 Normalization: for every rectangle $\Gamma \subset \mathbf{C}^*$ we have

$$\text{ind}(\partial\Gamma) = \begin{cases} 1 & \text{if } 0 \in \text{Int } \Gamma, \\ 0 & \text{if } 0 \in \mathbf{C} \setminus \Gamma. \end{cases}$$

- 2 Multiplicativity: $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 Homotopy invariance: $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ whenever $\gamma_0 \sim \gamma_1$ in \mathbf{C}^* .

The difficulty is to prove the existence of such a map! Possible approaches:

- Covering theory, applied to $\exp: \mathbf{C} \rightarrow \mathbf{C}^*$ with covering group \mathbb{Z} .
- Fundamental group $\text{ind}: \pi_1(\mathbf{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert-van Kampen.
- Homology $\text{ind}: H_1(\mathbf{C}^*) \xrightarrow{\sim} \mathbb{Z}$ via Eilenberg-Steenrod axioms.
- Differential topology, Sard's theorem and mapping degree
- Complex analysis, analytic index $\text{ind}(\gamma) = \frac{1}{2i\pi} \int_{\gamma} \frac{dz}{z}$.
- Real algebra, Cauchy index calculated via Sturm chains.

§10

From existence to locating complex roots

Let \mathbf{R} be a real closed field and let $\mathbf{C} = \mathbf{R}[i]$ where $i^2 = -1$.

We can construct an algebraic index, having the right properties,

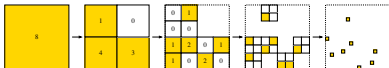
$$\text{ind}: \left\{ \begin{array}{l} \text{piecewise polynomial} \\ \text{loops } \gamma: [0, 1] \rightarrow \mathbf{C}^* \end{array} \right\} \rightarrow \mathbb{Z}.$$

This provides an elementary proof of the fundamental theorem of algebra:

Every complex polynomial $F \in \mathbf{C}[\mathbb{Z}]$ of degree n has n complex roots.

- $\text{ind}_{\partial\Gamma}(F)$ counts the roots of F in Γ .
- $\text{ind}_{\partial\Gamma}(F) = n$ for sufficiently large Γ .

The index thus allows us to locate all complex roots of F :



Once sufficient approximations have been found, switch to Newton's method.



Thank you for your attention!

Michael.Eisermann@ujf-grenoble.fr
www-fourier.ujf-grenoble.fr/~eiserm

*The Fundamental Theorem of Algebra made effective:
 an elementary real-algebraic proof via Sturm chains*