

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 (1789–1857)



Charles-François Sturm (1803–1855)

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

The fundamental theorem of algebra

Theorem

Every complex polynomial of degree n has n complex roots.

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 $\mathbb{C} = \mathbb{R}[i]$, $i^2 = -1$.

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

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

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

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

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

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

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

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

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

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

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

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

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

Natural questions:

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

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

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

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

Natural questions:

- Is there an elementary yet geometrically appealing proof?

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

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

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

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

Natural questions:

- Is there an elementary yet geometrically appealing proof?
- Can we weaken the hypothesis? to which ordered fields?

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

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

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

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

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?

Three types of proofs

There are essentially three proof strategies:

Three types of proofs

There are essentially three proof strategies:

- 1 analysis, using compactness, integration, Stokes, ... ;

Three types of proofs

There are essentially three proof strategies:

- 1 analysis, using compactness, integration, Stokes, ... ;
- 2 algebra, using symmetric functions, Galois theory, ... ;

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.

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*.

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?

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.

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.

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.

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.

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.

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.

Theorem (the real numbers)

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

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.

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.

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.*

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:*

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:
 $f(a)f(b) < 0 \implies \exists x \in \mathbf{R} : (x - a)(x - b) < 0 \wedge f(x) = 0.$

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.

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.

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.

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:

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.

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 $\mathbb{Q}^c \subset \mathbb{R}, \dots$

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)

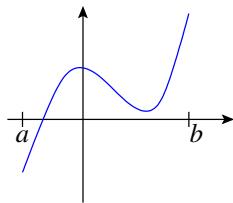
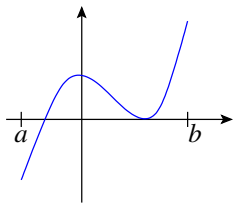
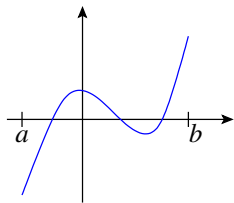
An ordered field $(\mathbf{R}, +, \cdot, \leq)$ is called *real closed* if every polynomial $P \in \mathbf{R}[X]$ satisfies the intermediate value property.

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

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

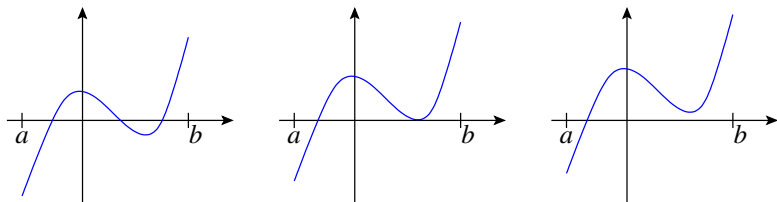
Real roots of real polynomials

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



Real roots of real polynomials

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



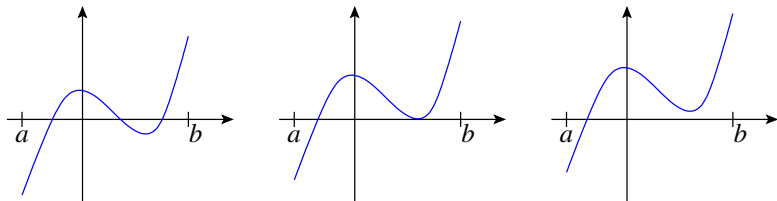
Sturm's theorem

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 $S_{n+1} = 0$.

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!

Complex roots of complex polynomials

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

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 $\gamma: [0, 1] \rightarrow \mathbf{C}^*$, $\gamma(0) = \gamma(1)$.

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:

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} .*

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

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

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:* $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

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}^* .

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!

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 $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$ with covering group \mathbb{Z} .

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 $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$ with covering group \mathbb{Z} .
- Fundamental group $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert–van Kampen.

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 $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$ with covering group \mathbb{Z} .
- Fundamental group $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert–van Kampen.
- Homology $\text{ind}: H_1(\mathbb{C}^*) \xrightarrow{\sim} \mathbb{Z}$ via Eilenberg–Steenrod axioms.

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 $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$ with covering group \mathbb{Z} .
- Fundamental group $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert–van Kampen.
- Homology $\text{ind}: H_1(\mathbb{C}^*) \xrightarrow{\sim} \mathbb{Z}$ via Eilenberg–Steenrod axioms.
- Differential topology, Sard's theorem and mapping degree

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

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 $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$ with covering group \mathbb{Z} .
- Fundamental group $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert–van Kampen.
- Homology $\text{ind}: H_1(\mathbb{C}^*) \xrightarrow{\sim} \mathbb{Z}$ 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.

From existence to locating complex roots

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

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,

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

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:

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

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

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

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 $F \in \mathbf{C}[Z]$ 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 .

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 $F \in \mathbf{C}[Z]$ 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 :

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,

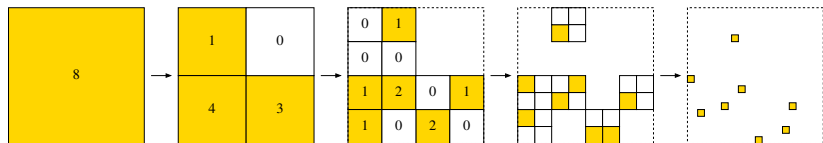
$$\text{ind}: \left\{ \begin{array}{l} \text{piecewise polynomial} \\ \text{loops } \gamma: [0, 1] \rightarrow \mathbf{C}^* \end{array} \right\} \rightarrow \mathbb{Z}.$$

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

Every complex polynomial $F \in \mathbf{C}[Z]$ 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 :



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,

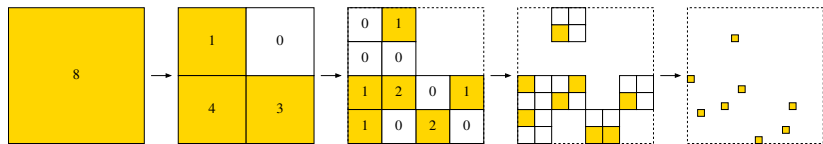
$$\text{ind}: \left\{ \begin{array}{l} \text{piecewise polynomial} \\ \text{loops } \gamma: [0, 1] \rightarrow \mathbf{C}^* \end{array} \right\} \rightarrow \mathbb{Z}.$$

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

Every complex polynomial $F \in \mathbf{C}[Z]$ 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*