Algebraic winding numbers

Marie-Françoise Roy, IRMAR, Université de Rennes 1
jointly with
Daniel Perrucci, University of Buenos Aires, Argentina

Inaugural meeting of Asian-Oceanian Women in Mathematics - 24/04/2023

Outline of the talk

- Algebraic proofs of the Fundamental Theorem of Algebra
- Cauchy Index and algebraic winding numbers
- Properties of algebraic winding numbers
- Quantitative Fundamental Theorem of Algebra (the problem and the statement)

Real closed fields

Theorem

$\mathbf{R}$ 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 $P \in \mathbf{R}[X]$,*

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

2. *FTA: $\mathbf{C} = \mathbf{R}[i] = \mathbf{R}[T]/(T^2+1)$ is an algebraically closed field.*

FTA implies IVT : factorization of P in linear and quadratic factors.

Real closed fields

Not only the field $\mathbb{R}$ of real numbers!

The field $\mathbb{R}_{\mathrm{alg}}$ of real algebraic numbers which is countable.

Also the field $\mathbb{R}\langle\varepsilon\rangle$ of real Puiseux series (series with rational exponents) which contains the infinitesimal ε.

One trend of modern real algebraic geometry is to provide proofs that work for any any real closed field, i.e. algebraic proofs. Quantitative and algorithmic results are welcome !

IVT implies FTA ?

There are many proofs of the Fundamental Theorem of Algebra, several of them by Gauss.

Some of them were false, or incomplete. Need for algebraic or topological facts proved later.

Fascinating topic in the History of Mathematics. See for example `https://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra`

Constructive proofs using numerical methods but for $\mathbb{R}$ only, not any real closed field.

IVT implies FTA ?

1) Through Laplace's proof [Lap,1795], improved by Gauss [Gau, 1815]. IVT implies that all positive numbers have a square root, all polynomials of odd degree have a root.
Proof by an induction on the exponent of 2 in the degree.
Indication : $P \in \mathbf{R}[X]$ of degree $d = 2^k s$ with s odd. If $k = 0$, d is odd and P has a root in $\mathbf{R} \subset \mathbf{C}$. Otherwise, define for $h \in \mathbb{Z}$,

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

$\deg_X(Q_h) = d(d-1)/2 = 2^{k-1}s'$ with s' odd.
Use induction hypothesis, pigeon hole principle and existence of complex roots of degree two complex polynomials. At the end of the induction, polynomial of (high) odd degree ...

IVT implies FTA

2) A recent proof of the Fundamental Theorem of Algebra by Michael Eisermann in [Eis, 2012] is also using only IVT, but involves the geometric concept of winding number, computed in a real-algebraic way through Cauchy index.
It is based on very classical ideas known already in the 19 th centuries (paper by Sturm and Liouville) but details (often non trivial) needed to be fixed.

3) Also a flaw in [Eis, 2012]. New proof [PR,2019]. Main new ingredient compared to [Eis] : a closer analysis of the "product formula" to fix the proof (see later) and the use of subresultants for computing the Cauchy index and the winding number with better degree bounds.

Cauchy index

- If $P, Q \in \mathbf{R}[X]$, both non zero, the polynomials P and Q can be written uniquely as

$$P = (X - x)^{\mathrm{mult}_x(P)} P_x,$$
$$Q = (X - x)^{\mathrm{mult}_x(Q)} Q_x,$$

with $\mathrm{mult}_x(P), \mathrm{mult}_x(Q) \in \mathbb{N}$ and $P_x(x) \neq 0, Q_x(x) \neq 0$.

$$\mathrm{val}_x(P/Q) = \mathrm{mult}_x(P) - \mathrm{mult}_x(Q) in \mathbb{Z}$$

For $\varepsilon \in \{+1, -1\}$, define

$$\mathrm{Ind}_x^\varepsilon(Q, P) = \begin{cases} \frac{1}{2}\varepsilon^{\mathrm{val}_x(P/Q)}\mathrm{sign}(Q_x(x)P_x(x)) & \text{if } \mathrm{val}_x(P/Q), \\ 0 & \text{in all other cases.} \end{cases}$$

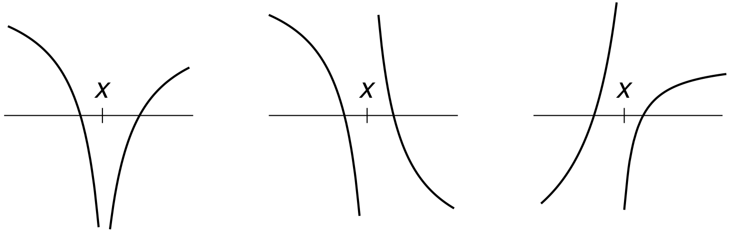
If one of P, Q is zero, $\mathrm{Ind}_x^\varepsilon(Q, P) = 0$.

Cauchy index

The Cauchy Index of Q, P at x is

$$\mathrm{Ind}_x(Q,P) = \mathrm{Ind}_x^{+1}(Q,P) - \mathrm{Ind}_x^{-1}(Q,P).$$

Illustration, considering the graph of the function $\frac{Q}{P}$ around x in different cases.



$\mathrm{Ind}_x\big(Q,P\big) = 0$ $\mathrm{Ind}_x\big(Q,P\big) = 1$ $\mathrm{Ind}_x\big(Q,P\big) = -1$

Cauchy index

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

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

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

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

- Additivity : for any $a, c_1, \ldots, c_k, b \in \mathbf{R}$ and any $P, Q \in \mathbf{R}[X]$,

$$\mathrm{Ind}_a^b(Q, P) = \mathrm{Ind}_a^{c_1}(Q, P) + \sum_{1 \le i \le k-1} \mathrm{Ind}_{c_i}^{c_{i+1}}(Q, P) + \mathrm{Ind}_{c_k}^b(Q, P).$$

- If $P, Q \neq 0$ and $a > b$, $\mathrm{Ind}_a^b(Q, P) = -\mathrm{Ind}_b^a(Q, P)$.

Definition of winding number

$w(\gamma)$ counts the number of turns that a loop γ performs around 0. Complex analysis notion.

Classical argument principle applied to a polynomial F on a rectangle Γ: as long as F has no zeros on $\partial\Gamma$, the winding number of the curve $F \circ \partial\Gamma$, defined analytically as

$$\frac{1}{2\pi i}\int_{\partial\Gamma}\frac{(F)'(z)}{(F)(z)}dz$$

counts the number of zeros (with multiplicity) of F inside Γ (see Chapter 4, Section 5.2 in [Ahl]).

Real-algebraic definition of winding number

Coming from [Eis]: $F \in \mathbf{C}[Z]$, $Z = X + iY$,
$\Gamma = [c_0, c_1] \times [d_0, d_1] \subset \mathbf{R}^2$ a rectangle.

$$F(X, Y) = F_{\mathrm{re}}(X, Y) + iF_{\mathrm{im}}(X, Y)$$

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

winding number $w(F|\partial\Gamma)$ defined by

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

Real-algebraic definition of winding number

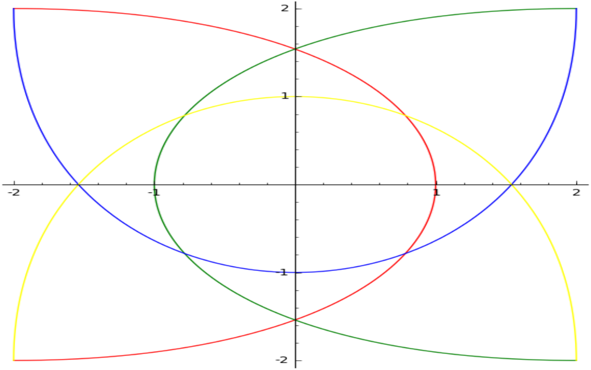


Figure: **Winding number** $(X + iY)^3$ **on** $[-1, 1] \times [-1, 1]$; $\mathrm{w} = 3$

Properties of winding number

- additivity For any $c_0 = c'_1, \ldots, c'_k, = c_1 \in \mathbf{R}$, $d_0 = d'_1, \ldots, d'_\ell, = d_1 \in \mathbf{R}$, $\Gamma_{i,j} = [c'_{i-1}, c'_i] \times [d'_{j-1}, d'_j]$

$$w(F|\partial\Gamma) = \sum_{1 \le i \le k} \sum_{1 \le j \le \ell} w(F|\partial\Gamma_{i,j})$$

- Multiplicativity $w(F \times G|\partial\Gamma) = w(F|\partial\Gamma) + w(G|\partial\Gamma)$
- Main lemma: if $w(F|\partial\Gamma) \neq 0$, F has a root in Γ
- $F \in \mathbf{C}[Z]$, with $\deg F = e$. There exists $r \in \mathbf{R}$, $r > 0$ such that if $m \geq r$ and $\Gamma := [-m, m] \times [-m, m]$, then $w(F|\partial\Gamma) = e$.

As a consequence, the winding number counts the number of complex roots inside Γ with multiplicities when there are no roots on $\partial\Gamma$.

What about sides and edges ?

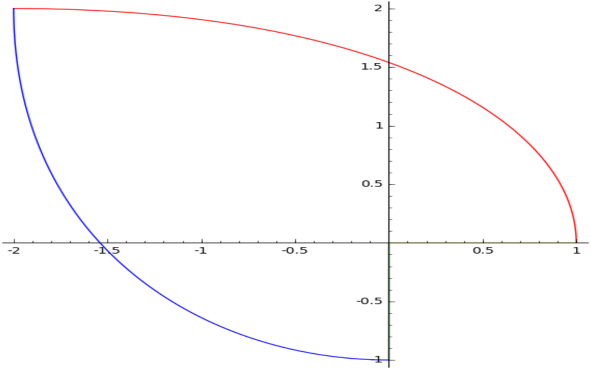
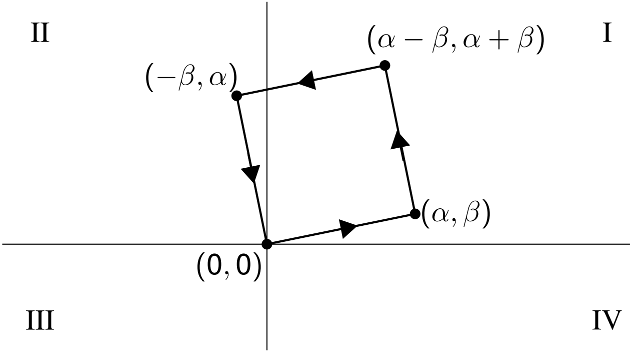


Figure: **Winding number** $(X + iY)^3$ **on** $[0, 1] \times [0, 1]$; $\mathrm{w} = 3/4$

Multiplying by a constant ?



$$\mathrm{w}(F \mid \partial\Gamma) = 0$$

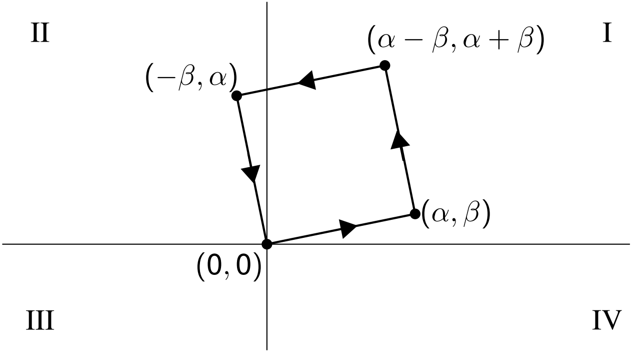
w and W

We need to take into account also the Y-axis.

Let $F \in \mathbf{C}[X, Y]$, $x_0, x_1, y_0, y_1 \in \mathbf{R}$ with $x_0 < x_1$ and $y_0 < y_1$, and $\Gamma := [x_0, x_1] \times [y_0, y_1] \subset \mathbf{R}^2$.
Consider the *modified winding number* of F on $\partial\Gamma$:

$$\mathrm{W}(F \,|\, \partial\Gamma) \quad := \quad \frac{1}{2}\Big(\mathrm{w}(F \,|\, \partial\Gamma) + \mathrm{w}(iF \,|\, \partial\Gamma)\Big).$$

Multiplying by a constant ?



$$\mathrm{W}(F \mid \partial\Gamma) = 1/4$$

Multiplicativity of W and w

Let $F, G \in \mathbf{C}[Z]$ and$\Gamma = [x_0, x_1] \times [y_0, y_1]$.

Proposition

Then

$$\mathrm{W}(FG \,|\, \partial\Gamma) = \mathrm{W}(F \,|\, \partial\Gamma) + \mathrm{W}(G \,|\, \partial\Gamma).$$

Proposition

If $F, G \in \mathbf{C}[Z]$ are such that the sum of the multiplicities of F and G at the corners are all even,

$$\mathrm{w}(FG \,|\, \partial\Gamma) = \mathrm{w}(F \,|\, \partial\Gamma) + \mathrm{w}(G \,|\, \partial\Gamma).$$

How to prove multiplicativity ?

$P, Q, R, S \in \mathbf{R}[X]$ with P and Q (resp. R and S) not simultaneously equal to 0, $a, b \in \mathbf{R}$ with $a < b$. Eisermann introduced the auxiliary product formula

$$\mathrm{Ind}_a^b(PR - QS, PS + QR) =$$
$$\mathrm{Ind}_a^b(P, Q) + \mathrm{Ind}_a^b(R, S) - \mathrm{Var}_a^b(PS + QR, QS)$$

For $P, Q \in \mathbf{R}[X]$ and $x \in \mathbf{R}$,

$$\mathrm{Var}_x(P, Q) = \begin{cases} \frac{1}{2} - \frac{1}{2}\mathrm{sign}\left(P_x(x)Q_x(x)\right) & \text{if } \mathrm{val}_x(P/Q) = 0, \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

$$\mathrm{Var}_a^b(P, Q) = \mathrm{Var}_a(P, Q) - \mathrm{Var}_b(P, Q).$$

Auxiliary product formula

Unfortunately false. Counter-example.
Let $a = 0$, $b = 1$, $P = 1$, $Q = X$, $R = X - 1$, $S = X$. Then
$PR - QS = -X^2 + X - 1$, $PS + QR = X^2$ and

$$\begin{aligned} \mathrm{Ind}_0^1(PR - QS, PS + QR) &= -1/2, \\ \mathrm{Ind}_0^1(P, Q) &= 1/2, \\ \mathrm{Ind}_0^1(R, S) &= -1/2, \\ \mathrm{Var}_0^1(PS + QR, QS) &= 0, \\ -\frac{1}{2} &\neq \frac{1}{2} - \frac{1}{2} - 0. \end{aligned}$$

Note that for $F = iZ + 1$ and $G = (1 + i)Z - 1$, P, Q, R, S are the restrictions of F_{re}, F_{im}, G_{re}, G_{im} to the bottom side of $\Gamma = [0, 1] \times [0, 1]$.

Auxiliary product formula

We say that $c \in \mathbf{R}$ is a *bad number* for P, Q, R, S, if $Q, S \neq 0$ and c satisfies the following two conditions:

- $\mathrm{val}_c(P/Q) = \mathrm{val}_c(R/S) < 0$,
- $\mathrm{val}_c((PS + QR)/QS) = 0$.

Proposition

Let $P, Q, R, S \in \mathbf{R}[X]$ with P and Q not simultaneously equal to 0 and R and S not simultaneously equal to 0, and let $a, b \in \mathbf{R}$ with $a < b$. If a and b are not bad numbers,

$$\begin{aligned} &\mathrm{Ind}_a^b(PR - QS, PS + QR) \\ &= \mathrm{Ind}_a^b(P, Q) + \mathrm{Ind}_a^b(R, S) - \mathrm{Var}_a^b(PS + QR, QS) \end{aligned}$$

Strategy for multiplicity of W and w

Strategy proposed by Eisermann.
Use the auxiliary product formula for each side of Γ and prove that the sum of the Var is 0.

Is does work. Quite subtle, need to take care of bad points and to take into account the parity of the multiplicities at the corners.

The multiplicativity always holds for W, there are restrictions for w.

Complex root counting with W

Let $F \in \mathbf{C}(Z) \setminus \{0\}$ $\Gamma \subset \mathbf{C}$ a rectangle.

Theorem

Then $\mathrm{W}(F \mid \partial\Gamma)$ counts the number of zeros (with multiplicity) of F. Zeros on the edges count for one half. Zeros on the vertices count for one quarter.

Multiplicativity and Main Lemma

Lemma (Main Lemma)

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

Complex root counting with w

Theorem

If F has even multiplicities at all the vertices of Γ. Then $\mathrm{w}(F \mid \partial\Gamma)$ counts the number of zeros (with multiplicity) of F. Zeros on the edges count for one half. Zeros on the vertices count for one quarter.

Quantitative FTA

How to compare Laplace's proof and algebraic winding number proofs from a quantitative point of view ? $\mathbb{N}^\star$ set of natural numbers ≥ 1. For each $d \in \mathbb{N}^\star$, define the following properties on a totally ordered field $\mathbf{R}$.

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

Problem

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

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

Degree bounds for Laplace

From Laplace's proof we deduce the existence of a function $\gamma(d)$:

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

with

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

Key ingredient of the Proof of QFTA

Multiplcativity and Main Lemma.

Lemma (Main Lemma)

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

By contraposition, in the special case $P \in \mathbf{C}[Z = X + iY]$, if $w(P|\partial\Gamma) \neq 0$, P 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 essential. No good degree bounds when specializing with respect to Y.

Improved by us using subresultants with respect to Y, which provides degree bounds d when specializing with respect to X.

Our [PR] result

A recent proof the Fundamental Theorem of Algebra by Michael Eisermann in [Eis] is based only on IVT, but involves the geometric concept of winding number, computed in a real-algebraic way through Cauchy index.
Our main new ingredient compared to [Eis] is the use of subresultants for computing the Cauchy index and the winding number.
We obtain the following result:

Theorem (Quantitative Fundamental Theorem of Algebra)

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

$$\mathrm{IVT}_{d^2} \textit{ implies } \mathrm{FTA}_d.$$

References

[Ahl] L.V. Ahlfors, Complex Analysis. An introduction to the theory of analytic functions of one complex variable. Ed. McGraw-Hill Book Company, 1966.
[BPR] S. Basu, R. Pollack, M.-F. Roy *Algorithms in real algebraic geometry*, Springer 2nd edition (2006).
[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.
[Gau] C. F. Gauss, Collected Works, Volume 3, pages 33-56 (in latin), english translation Eureka 45 (1985).
[Lap] P-S. Laplace. Leçons de mathématiques données à l'école normale en 1795,
[PR] D. Perrucci, M.-F. Roy, Quantitative Fundamental Theorem of Algebra, *The Quarterly Journal of Mathematics*.

[PR2] D. Perrucci, M.-F. Roy, Algebraic winding numbers, (in preparation).