Under revision for publication in the American Mathematical Monthly.
Preprint available at www.igt.uni-stuttgart.de/eiserm.

THE FUNDAMENTAL THEOREM OF ALGEBRA MADE EFFECTIVE: AN ELEMENTARY REAL-ALGEBRAIC PROOF VIA STURM CHAINS

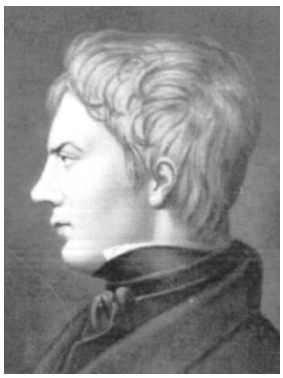
MICHAEL EISERMANN

ABSTRACT. Sturm's theorem (1829/35) provides an elegant algorithm to count and locate the real roots of any real polynomial. In his residue calculus (1831/37) Cauchy extended Sturm's method to count and locate the complex roots of any complex polynomial. For holomorphic functions Cauchy's index is based on contour integration, but in the special case of polynomials it can effectively be calculated via Sturm chains using euclidean division as in the real case. In this way we provide an algebraic proof of Cauchy's theorem for polynomials over any real closed field. As our main tool, we formalize Gauss' geometric notion of winding number (1799) in the real-algebraic setting, from which we derive a real-algebraic proof of the Fundamental Theorem of Algebra. The proof is elementary inasmuch as it uses only the intermediate value theorem and arithmetic of real polynomials. It can thus be formulated in the first-order language of real closed fields. Moreover, the proof is constructive and immediately translates to an algebraic root-finding algorithm.

L'algèbre est généreuse, elle donne souvent plus qu'on lui demande. (Jean le Rond d'Alembert)[1]

Carl Friedrich Gauß
(1777–1855)

Augustin Louis Cauchy
(1789–1857)



Charles-François Sturm
(1803–1855)

1. INTRODUCTION AND STATEMENT OF RESULTS

1.1. **Historical origins.** Sturm's theorem [54, 55], announced in 1829 and published in 1835, provides an elegant and ingeniously simple algorithm to determine for each real polynomial $P \in \mathbb{R}[X]$ the number of its real roots in any given interval $[x_0, x_1] \subset \mathbb{R}$. Sturm's breakthrough solved an outstanding problem of his time and earned him instant fame.

In his residue calculus, outlined in 1831 and fully developed in 1837, Cauchy [8, 9] extended Sturm's method to determine for each complex polynomial $F \in \mathbb{C}[Z]$ the number of

Date: first version March 2008; this version compiled April 1, 2012.

2010 *Mathematics Subject Classification.* 12D10; 26C10, 30C15, 65H04, 65G20.

Key words and phrases. Constructive and algorithmic aspects of the fundamental theorem of algebra, algebraic winding number, Sturm chains and Cauchy index, Sturm–Cauchy root-finding algorithm.

[1] This quotation is folklore [26, p. 285]. It corresponds, though not verbatim, to d'Alembert's article *Équation* in the *Encyclopédie* (1751–1765, tome 5, p. 850): "[L'algèbre] répond non seulement à ce qu'on lui demande, mais encore à ce qu'on ne lui demandoit pas, et qu'on ne songeoit pas à lui demander." The portraits of Gauss and Cauchy are taken from Wikimedia Commons, the portrait of Sturm is from Loria's biography [33].

its complex roots in a given domain, say in any rectangle of the form $[x_0,x_1]\times[y_0,y_1]\subset\mathbb{C}$, where we identify $\mathbb{C}$ with $\mathbb{R}^2$ in the usual way. For holomorphic functions Cauchy's index is based on contour integration, but in the special case of polynomials it can effectively be calculated via Sturm chains using euclidean division as in the real case.

Combining Sturm's real algorithm and Cauchy's complex approach, we provide an algebraic proof of Cauchy's theorem for polynomials over any real closed field. As our main tool, we formalize Gauss' geometric notion of winding number in real-algebraic language. This leads to a real-algebraic proof of the Fundamental Theorem of Algebra, assuring that every nonconstant complex polynomial has at least one complex zero. Since zeros split off as linear factors, this is equivalent to the following extensive formulation.

Theorem 1.1 (Fundamental Theorem of Algebra, existence only)**.** *For every polynomial*

$$F = Z^n + c_1 Z^{n-1} + \cdots + c_{n-1}Z + c_n$$

with complex coefficients $c_1,\dots,c_{n-1},c_n\in\mathbb{C}$ *there exist* $z_1,z_2,\dots,z_n\in\mathbb{C}$ *such that*

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

Numerous proofs of this important theorem have been published over the last two centuries. According to the tools used, they can be grouped into three families (§7):

(1) Analysis, using compactness, integration, transcendental functions, etc.;
(2) Algebra, using polynomials and the intermediate value theorem;
(3) Algebraic topology, using some form of the winding number.

There are proofs for every taste and each has its merits. From a more ambitious, constructive viewpoint, however, a mere existence proof only "announces the presence of a treasure, without divulging its location", as Hermann Weyl put it. "It is not the existence theorem that is valuable, but the construction carried out in its proof."[2]

The real-algebraic approach presented here is situated between (2) and (3). It combines algebraic computation (Cauchy's index and Sturm's algorithm) with geometric reasoning (Gauss' notion of winding number) and therefore enjoys some remarkable features.

- It uses only the intermediate value theorem and arithmetic of real polynomials.
- It is elementary, in the colloquial as well as the formal sense of first-order logic.
- All arguments and constructions hold verbatim over every real closed field.
- The proof is constructive and immediately translates to a root-finding algorithm.
- The algorithm is easy to implement, and reasonably efficient in moderate degree.
- It can be formalized to a computer-verifiable proof (of theorem *and* algorithm).

The logical structure of such a proof was already outlined by Sturm [56] in 1836, but his article lacks the elegance and perfection of his famous 1835 mémoire. This may explain why his sketch found little resonance, was not further worked out, and became forgotten by the end of the 19th century. The aim of the present article is to save the real-algebraic proof from oblivion and to develop Sturm's idea in due rigour. The presentation is intended for non-experts and thus contains much introductory and expository material.

1.2. **The algebraic winding number.** Our arguments work over every ordered field $\mathbf{R}$ that satisfies the intermediate value property for polynomials, i.e., a *real closed field* (§2). We choose this starting point as the axiomatic foundation of Sturm's theorem (§3). We then deduce that the field $\mathbf{C}=\mathbf{R}[i]$ with $i^2=-1$ is algebraically closed, which was first proven by Artin and Schreier [3, 4]. Moreover, we construct the algebraic winding number and establish an algorithm to locate the zeros of any given polynomial $F\in\mathbf{C}[Z]^*$. (Here for every ring A, we denote by $A^*=A\smallsetminus\{0\}$ the set of its nonzero elements.)

[2] "Bezeichne ich Erkenntnis als einen wertvollen Schatz, so ist das Urteilsabstrakt ein Papier, welches das Vorhandensein eines Schatzes anzeigt, ohne jedoch zu verraten, an welchem Ort." [66, p. 54] "Nicht das Existenztheorem ist das Wertvolle, sondern die im Beweise geführte Konstruktion." [66, p. 55]

The geometric idea is very intuitive: the winding number $w(\gamma)$ counts the number of turns that a loop $\gamma\colon [0,1] \to \mathbf{C}^*$ performs around 0. Theorem 1.2 turns the geometric idea into a rigorous algebraic construction and provides an effective computation.

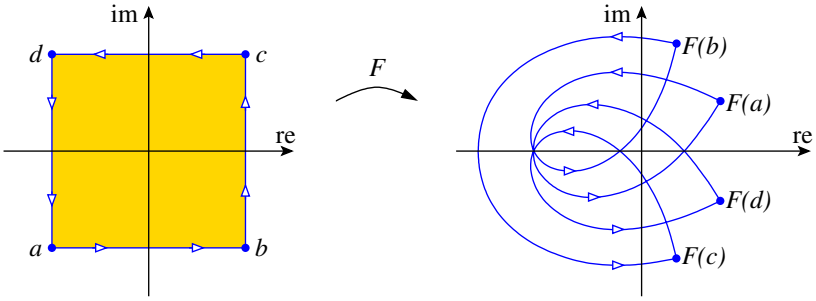


FIGURE 1. The winding number $w(F|\partial\Gamma)$ of a polynomial $F \in \mathbf{C}[Z]$ along the boundary of a rectangle $\Gamma \subset \mathbf{C}$. In this example $w(F|\partial\Gamma) = 2$.

In order to work algebraically, a *loop* γ will be understood to be a piecewise polynomial map from the interval $[0,1] = \{x \in \mathbf{R} \mid 0 \le x \le 1\}$ to $\mathbf{C}^*$ such that $\gamma(0) = \gamma(1)$; see §4.3. Likewise, a *homotopy* between loops will be required to be piecewise polynomial, as explained in §5.2. We can now formulate our main result.

Theorem 1.2 (algebraic winding number)**.** *Consider an ordered field* $\mathbf{R}$ *and its extension* $\mathbf{C} = \mathbf{R}[i]$ *where* $i^2 = -1$. *Let* Ω *be the set of piecewise polynomial loops* $\gamma\colon [0,1] \to \mathbf{C}^*$. *We define the* algebraic winding number $w\colon \Omega \to \mathbb{Z}$ *by the following algebraic property:*

(W0) *Computation:* $w(\gamma)$ *equals half the Cauchy index of* $\frac{\operatorname{re}\gamma}{\operatorname{im}\gamma}$, *recalled in* §3, *and can thus be calculated by Sturm's algorithm via iterated euclidean division.*

If $\mathbf{R}$ *is real closed, then* w *enjoys the following geometric properties:*

(W1) *Normalization: Let* $\Gamma \subset \mathbf{C}$ *be a rectangle of the form* $\Gamma = [x_0, x_1] \times [y_0, y_1]$. *If* γ *parametrizes the boundary* $\partial\Gamma \subset \mathbf{C}^*$, *positively oriented as in Figure 1 (left), then*

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

(W2) *Multiplicativity: For all* $\gamma_1, \gamma_2 \in \Omega$ *we have*

$$w(\gamma_1 \cdot \gamma_2) = w(\gamma_1) + w(\gamma_2),$$

(W3) *Homotopy invariance: For all* $\gamma_0, \gamma_1 \in \Omega$ *we have*

$$w(\gamma_0) = w(\gamma_1) \quad \text{whenever } \gamma_0 \text{ and } \gamma_1 \text{ are homotopic in } \mathbf{C}^*.$$

Conversely, if over some ordered field $\mathbf{R}$ *there exists a map* $w\colon \Omega \to \mathbb{Z}$ *satisfying properties* (W1), (W2), (W3), *then* $\mathbf{R}$ *is real closed and* w *can be calculated as in* (W0)

Remark 1.3. Since polynomials form the simplest function algebra and can immediately be used for computations, Theorem 1.2 has both practical and theoretical relevance. Over the real numbers $\mathbb{R}$, the Stone-Weierstrass theorem can be used to extend the winding number to continuous loops and homotopies, such that the geometric properties (W1), (W2), (W3) continue to hold. Several alternative constructions over $\mathbb{R}$ lead to this result:

(1) Fundamental group, $w\colon \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via the Seifert–van Kampen theorem,
(2) Covering theory, $\exp\colon \mathbb{C} \twoheadrightarrow \mathbb{C}^*$ with monodromy $w\colon \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$,
(3) Homology, $w\colon H_1(\mathbb{C}^*) \xrightarrow{\sim} \mathbb{Z}$ via the Eilenberg–Steenrod axioms,
(4) Complex analysis, analytic winding number $w(\gamma) = \frac{1}{2\pi i}\int_\gamma \frac{\mathrm{d}z}{z}$ via integration.

Each of these approaches relies on some characteristic property of the field $\mathbb{R}$ of real numbers, such as metric completeness or some equivalent, and therefore does not extend to any other real closed field. In this article we develop an independent algebraic proof using only polynomial arithmetic, avoiding compactness, integrals, covering spaces, etc.

We remark that constructions (1) and (2) are dual via Galois correspondence, while their abelian counterparts (3) and (4) are dual via the homology-cohomology pairing. The real-algebraic approach appears to be self-dual, as expressed in Theorem 1.2 by the equivalence of the algebraic computation (W0) with the geometric properties (W1), (W2), and (W3). This dual nature conjugates real-algebraic geometry and effective algebraic topology.

Remark 1.4. The algebraic winding number turns out to be slightly more general than stated in the theorem. The algebraic definition (W0) of $w(\gamma)$ also applies to loops γ that pass through 0. Normalization (W1) extends to $w(\gamma) = 1/2$ if 0 lies in an edge of Γ, and $w(\gamma) = 1/4$ if 0 is one of the vertices of Γ. Multiplicativity (W2) continues to hold provided that 0 is not a vertex of γ_1 or γ_2. Homotopy invariance (W3) applies only to loops in $\mathbf{C}^*$.

1.3. **Counting complex roots.** For the rest of this introduction, $\mathbf{R}$ denotes a real closed field and $\mathbf{C} = \mathbf{R}[i]$ its complex extension. From Theorem 1.2 we can deduce the Fundamental Theorem of Algebra using the geometric properties (W1), (W2), (W3) as follows.

As the first step (§4) we obtain the following algebraic version of Cauchy's theorem. We write $w(F|\partial\Gamma)$ as a short-hand for $w(F \circ \gamma)$ where γ parametrizes $\partial\Gamma$ as in Figure 1.

Theorem 1.5 (local winding number)**.** *If $F \in \mathbf{C}[Z]$ does not vanish at any of the four vertices of the rectangle $\Gamma \subset \mathbf{C}$, then the algebraic winding number $w(F|\partial\Gamma)$ equals the number of roots of F in Γ. Here each root in the interior of Γ is counted with its multiplicity, whereas each root in an edge of Γ is counted with half its multiplicity.*

To prove this, consider $F = (Z - z_1) \cdots (Z - z_m)G$ with $z_1, \ldots, z_m \in \Gamma$ such that G has no zeros in Γ. For $a \in \Gamma$ the homotopy $G_t = G(a + t(Z - a))$ deforms $G_1 = G$ to $G_0 = G(a)$, whence homotopy invariance (W3) implies that $w(G_1|\partial\Gamma) = w(G_0|\partial\Gamma) = 0$. The theorem then follows from multiplicativity (W2) and normalization (W1) as in Remark 1.4.

Example 1.6. Figure 1 displays the situation for $F = Z^5 - 5Z^4 - 2Z^3 - 2Z^2 - 3Z - 12$ and $\Gamma = [-1, +1]^2$. Here the winding number is $w(F|\partial\Gamma) = 2$. This is in accordance with the approximate location of zeros: Γ contains $z_{1,2} \approx -0.9 \pm 0.76i$ whereas $z_{3,4} \approx 0.67 \pm 1.06i$ and $z_5 \approx 5.46$ lie outside of Γ.

The hypothesis that F does not vanish at any of the vertices of Γ is very mild and easy to check in every concrete application. Unlike Cauchy's integral formula $w(\gamma) = \frac{1}{2\pi i} \int_\gamma \frac{\mathrm{d}z}{z}$, the algebraic winding number behaves well if zeros lie on (or close to) the boundary, and the uniform treatment of all configurations of roots simplifies theoretical arguments and practical implementations alike. This is yet another manifestation of the oft-quoted wisdom of d'Alembert that *Algebra is generous, she often gives more than we ask of her.*[1]

As the second step (§5) we formalize Gauss' geometric argument (1799) saying that $F \approx Z^n$ outside of a sufficiently big rectangle $\Gamma \subset \mathbf{C}$, whence $F|\partial\Gamma$ has winding number n.

Theorem 1.7 (global winding number)**.** *For each polynomial $F = Z^n + c_1 Z^{n-1} + \cdots + c_n$ in $\mathbf{C}[Z]$, we define its Cauchy radius to be $\rho_F := 1 + \max\{|c_1|, \ldots, |c_n|\}$. Then F satisfies $w(F|\partial\Gamma) = n$ on every rectangle Γ containing the Cauchy disk $B(\rho_F) = \{\, z \in \mathbf{C} \mid |z| < \rho_F \,\}$.*

The proof uses the homotopy $F_t = Z^n + t(c_1 Z^{n-1} + \cdots + c_n)$ to deform $F_1 = F$ to $F_0 = Z^n$. All zeros of F_t lie in $B(\rho_F)$. The hypothesis $\Gamma \supset B(\rho_F)$ ensures that F_t has no zeros on $\partial\Gamma$, so homotopy invariance (W3) allows us to conclude that $w(F_1|\partial\Gamma) = w(F_0|\partial\Gamma) = n$.

Theorems 1.5 and 1.7 imply that $\mathbf{C}$ is algebraically closed. Each polynomial $F \in \mathbf{C}[Z]$ of degree n has n roots in $\mathbf{C}$, more precisely in the square $\Gamma = [-\rho_F, \rho_F]^2 \subset \mathbf{C}$. (The latter is only a coarse estimate and can be improved for practical purposes; see Remark 5.10.)

1.4. **The Fundamental Theorem of Algebra made effective.** The winding number proves more than mere existence of roots: it also establishes a root-finding algorithm (§6.2). Here we have to assume that the ordered field $\mathbf{R}$ is archimedean, which amounts to $\mathbf{R} \subset \mathbb{R}$.

Theorem 1.8 (Fundamental Theorem of Algebra, effective version)**.** *For every complex polynomial $F = Z^n + c_1 Z^{n-1} + \cdots + c_n$ in $\mathbb{C}[Z]$ there exist complex roots $z_1, \ldots, z_n \in \mathbb{C}$ such that $F = (Z - z_1) \cdots (Z - z_n)$ and the algebraic winding number provides an algorithm to locate them. Starting from some rectangle containing all n roots, as in Theorem 1.7, we can subdivide and keep only those rectangles that actually contain roots, using Theorem 1.5. All computations can be carried out using Sturm chains according to Theorem 1.2. By iterated bisection we can thus approximate all roots to any desired precision.*

Remark 1.9 (computability). In the real-algebraic setting of this article we consider the field operations $(a,b) \mapsto a+b$, $a \mapsto -a$, $(a,b) \mapsto a \cdot b$, $a \mapsto a^{-1}$ and the comparisons $a = b$, $a < b$ as primitive operations. Over the real numbers $\mathbb{R}$, this point of view was advanced by Blum–Cucker–Shub–Smale [6] by postulating a hypothetical *real number machine*.

In order to implement the required real-algebraic operations on a Turing machine, however, a more careful analysis is necessary (§6.1). Given $F = c_0 Z^n + c_1 Z^{n-1} + \cdots + c_n$ we have to assume that the operations of the ordered field $\mathbb{Q}(\mathrm{re}(c_0), \mathrm{im}(c_0), \ldots, \mathrm{re}(c_n), \mathrm{im}(c_n))$ are computable in the Turing sense (§6.2). This is the case for the field $\mathbb{Q}$ of rational numbers, for example, or every real-algebraic number field $\mathbb{Q}(\alpha) \subset \mathbb{R}$.

Remark 1.10 (complexity). On a Turing machine we can compare time requirements by measuring bit-complexity. The above Sturm–Cauchy method requires $\tilde{O}(n^4 b^2)$ bit-operations to approximate all n roots to a precision of b bits (§6.4). Further improvement is necessary to reach the nearly optimal bit-complexity $\tilde{O}(n^3 b)$ of Schönhage [50] (§6.5).

Nevertheless, the Sturm–Cauchy method can be useful in hybrid algorithms, in order to verify numerical approximations and to improve them as necessary [48]. Once sufficient approximations of the roots have been obtained, one can switch to Newton's method, which converges much faster but vitally depends on good starting values (§6.3).

1.5. **How this article is organized.** Section 2 briefly recalls the notion of real closed fields, on which we build Sturm's theorem and the theory of Cauchy's index.

Section 3 presents Sturm's theorem [55] counting real roots of real polynomials. The only novelty is the extension to boundary points, which is needed in Section 4.

Section 4 proves Cauchy's theorem [9] counting complex roots of complex polynomials, by establishing multiplicativity (W2) of the algebraic winding number.

Section 5 establishes homotopy invariance (W3), and proves the Fundamental Theorem of Algebra by Gauss' winding number argument.

Section 6 discusses algorithmic aspects, such as Turing computability, the efficient computation of Cauchy indices, and the crossover to Newton's local method.

Section 7, finally, provides historical comments in order to put the real-algebraic approach into a wider perspective.

I have tried to keep the exposition elementary yet detailed. I hope that the interest of the subject justifies the resulting length of this article.

2. Real closed fields

This section sets the scene by recalling the notion of a real closed field, on which we build Sturm's theorem in §3, and also sketches its mathematical context.

2.1. **Real numbers.** As usual we denote by $\mathbb{R}$ the field of real numbers, that is, an ordered field $(\mathbb{R}, +, \cdot, <)$ such that every nonempty bounded subset $A \subset \mathbb{R}$ has a least upper bound in $\mathbb{R}$. This is a very strong property, and in fact it characterizes $\mathbb{R}$.

Theorem 2.1. *Let $\mathbf{R}$ be an ordered field, with the order-topology generated by the open intervals. Then the following conditions are equivalent:*

(1) *The ordered set* $(\mathbf{R},<)$ *satisfies the least upper bound property,*
(2) *Each interval* $[a,b]\subset\mathbf{R}$ *is compact as a topological space,*
(3) *Each interval* $[a,b]\subset\mathbf{R}$ *is connected as a topological space,*
(4) *The intermediate value property holds for all continuous functions* $f\colon\mathbf{R}\to\mathbf{R}$.

Any two ordered fields satisfying these properties are isomorphic by a unique field isomorphism, and this isomorphism preserves order. Any construction of the real numbers shows that one such field exists. □

2.2. **Real closed fields.** The field $\mathbb{R}$ of real numbers provides the foundation of analysis. In the present article it appears as the most prominent example of the much wider class of real closed fields. The reader who wishes to concentrate on the classical case may skip the rest of this section and assume $\mathbf{R}=\mathbb{R}$ throughout.

Definition 2.2. An ordered field $(\mathbf{R},+,\cdot,<)$ is *real closed* if it satisfies the intermediate value property for polynomials: whenever $P\in\mathbf{R}[X]$ satisfies $P(a)P(b)<0$ for some $a<b$ in $\mathbf{R}$, then there exists $x\in\mathbf{R}$ with $a<x<b$ such that $P(x)=0$.

Example 2.3. The field $\mathbb{R}$ of real numbers is real closed by Theorem 2.1 above. The field $\mathbb{Q}$ of rational numbers is not real closed, as shown by the example $P=X^2-2$ on $[1,2]$. The algebraic closure $\mathbb{Q}^c$ of $\mathbb{Q}$ in $\mathbb{R}$ is a real closed field. In fact, $\mathbb{Q}^c$ is the smallest real closed field, in the sense that $\mathbb{Q}^c$ is contained in any real closed field. Notice that $\mathbb{Q}^c$ is much smaller than $\mathbb{R}$, in fact $\mathbb{Q}^c$ is countable whereas $\mathbb{R}$ is uncountable.

The theory of real closed fields originated in the work of Artin and Schreier [3, 4] in the 1920s, culminating in Artin's solution [1] of Hilbert's 17th problem. Excellent textbook references include Jacobson [25, chap. I.5 and II.11] and Bochnak–Coste–Roy [7, chap. 1 and 6]. For the present article, Definition 2.2 above is the natural starting point because it captures the essential geometric feature. It deviates from the algebraic definition of Artin–Schreier [3], saying that an ordered field is real closed if no proper algebraic extension can be ordered. For a proof of their equivalence see [11, Prop. 8.8.9] or [7, §1.2].

Remark 2.4. In a real closed field $\mathbf{R}$ every positive element has a square root, and so the ordering on $\mathbf{R}$ can be characterized in algebraic terms: For every $a\in\mathbf{R}$ we have $a\geq 0$ if and only if there exists $b\in\mathbf{R}$ such that $b^2=a$. In particular, if a field is real closed, then it admits precisely one ordering that is compatible with the field structure.

Every archimedean ordered field can be embedded into $\mathbb{R}$; see [11, §8.7]. The field $\mathbb{R}(X)$ of rational functions can be ordered (in many different ways; see [7, §1.1]) but does not embed into $\mathbb{R}$. Nevertheless it can be embedded into its real closure.

Theorem 2.5 (Artin–Schreier [3, Satz 8])**.** *Every ordered field* $\mathbf{K}$ *admits a real closure, i.e., a real closed field that is algebraic over* $\mathbf{K}$ *and whose unique ordering extends that of* $\mathbf{K}$. *Any two real closures of* $\mathbf{K}$ *are isomorphic via a unique isomorphism fixing* $\mathbf{K}$. □

The real closure is thus completely rigid, in contrast to the algebraic closure.

Remark 2.6. Artin and Schreier [3, Satz 3] proved that if a field $\mathbf{R}$ is real closed, then $\mathbf{C}=\mathbf{R}[i]$ is algebraically closed, recasting the classical algebraic proof of the Fundamental Theorem of Algebra (§7.6.2). Conversely [4], if a field $\mathbf{C}$ is algebraically closed and contains a subfield $\mathbf{R}$ such that $1<\dim_{\mathbf{R}}(\mathbf{C})<\infty$, then $\mathbf{R}$ is real closed and $\mathbf{C}=\mathbf{R}[i]$.

2.3. **Elementary theory of ordered fields.** The axioms of an ordered field $(\mathbf{R},+,\cdot,<)$ are formulated in first-order logic, which means that we quantify over elements of $\mathbf{R}$, but not over subsets, functions, etc. By way of contrast, the characterization of the field $\mathbb{R}$ of real numbers (Theorem 2.1) is of a different nature: here we have to quantify over subsets of $\mathbb{R}$, or functions $\mathbb{R}\to\mathbb{R}$, and such a formulation uses second-order logic.

The algebraic condition for an ordered field $\mathbf{R}$ to be real closed is of first order. It is given by an axiom scheme where for each degree $n \in \mathbb{N}$ we have the axiom

$$\begin{aligned}(2.1)\quad \forall a,b,c_0,c_1,\dots,c_n \in \mathbf{R}\,\big[&(c_0+c_1a+\cdots+c_na^n)(c_0+c_1b+\cdots+c_nb^n)<0\\ &\Rightarrow \exists x\in\mathbf{R}\,\big((x-a)(x-b)<0 \wedge c_0+c_1x+\cdots+c_nx^n=0\big)\big].\end{aligned}$$

First-order formulae are customarily called *elementary*. The collection of all first-order formulae that are true over a given ordered field $\mathbf{R}$ is called its *elementary theory*.

Tarski's theorem [25, 7] says that all real closed fields share the same elementary theory: if an assertion in the first-order language of ordered fields is true over one real closed field, for example the real numbers, then it is true over every real closed field. (This no longer holds for second-order assertions, where $\mathbb{R}$ is singled out as in Theorem 2.1.)

Tarski's theorem implies that euclidean geometry, seen as cartesian geometry modeled on the vector space $\mathbb{R}^n$, remains unchanged if the field $\mathbb{R}$ of real numbers is replaced by any other real closed field $\mathbf{R}$. This is true as far as its first-order properties are concerned, and these comprise the core of classical geometry. In this vein we encode the geometric notion of winding number in the first-order theory of real closed fields.

Remark 2.7. Tarski's theorem is a vast generalization of Sturm's technique, and so is its effective formulation, called *quantifier elimination*, which provides explicit decision procedures. In principle such procedures could be used to generate a proof of the Fundamental Theorem of Algebra in every fixed degree. We will not use Tarski's theorem, however, and we only mention it in order to situate our approach in its logical context.

3. Sturm's theorem for real polynomials

This section recalls Sturm's theorem for polynomials over a real closed field – a gem of 19th century algebra and one of the greatest discoveries in the theory of polynomials.

It seems impossible to surpass the elegance of the original mémoires by Sturm [55] and Cauchy [9]. One technical improvement of our presentation, however, seems noteworthy: The inclusion of boundary points streamlines the arguments so that they will apply seamlessly to the complex setting in §4. The necessary amendments render the development hardly any longer or more complicated. They pervade, however, all statements and proofs, so that it seems worthwhile to review the classical arguments in full detail.

3.1. **Counting sign changes.** For every ordered field $\mathbf{R}$, we define $\operatorname{sign}\colon \mathbf{R}\to\{-1,0,+1\}$ by $\operatorname{sign}(x)=+1$ if $x>0$, $\operatorname{sign}(x)=-1$ if $x<0$, and $\operatorname{sign}(0)=0$. Given a finite sequence $s=(s_0,\dots,s_n)$ in $\mathbf{R}$, we say that the pair (s_{k-1},s_k) presents a *sign change* if $s_{k-1}s_k<0$. The pair presents *half a sign change* if one element is zero while the other is nonzero. In the remaining cases there is no sign change. All cases can be subsumed by the formula

$$V(s_{k-1},s_k) := \tfrac{1}{2}\big|\operatorname{sign}(s_{k-1})-\operatorname{sign}(s_k)\big|. \tag{3.1}$$

Definition 3.1. For a finite sequence $s=(s_0,\dots,s_n)$ in $\mathbf{R}$ the *number of sign changes* is

$$V(s) := \sum_{k=1}^{n} V(s_{k-1},s_k) = \sum_{k=1}^{n} \tfrac{1}{2}\big|\operatorname{sign}(s_{k-1})-\operatorname{sign}(s_k)\big|. \tag{3.2}$$

For a finite sequence $(S_0,\dots,S_n)$ of polynomials in $\mathbf{R}[X]$ and $a\in\mathbf{R}$ we set

$$V_a\big(S_0,\dots,S_n\big) := V\big(S_0(a),\dots,S_n(a)\big). \tag{3.3}$$

For the difference at two points $a,b\in\mathbf{R}$ we use the notation $V_a^b := V_a - V_b$.

There is no universal agreement how to count sign changes because each application requires its specific conventions. While there is no ambiguity for $s_{k-1}s_k<0$ and $s_{k-1}s_k>0$, some arbitration is needed to take care of possible zeros. Our definition (3.1) has been chosen to account for boundary points in Sturm's theorem, as explained below.

The traditional way of counting sign changes, following Descartes, is to extract the subsequence $\hat{s}$ by discarding all zeros of s and to define $\hat{V}(s) := V(\hat{s})$. (This counting rule is nonlocal whereas in (3.2) only neighbours interact.) As an illustration we recall Descartes' rule of signs and its generalization due to Budan and Fourier [42, chap. 10].

Theorem 3.2. *For every nonzero polynomial $P = c_0 + c_1X + \cdots + c_nX^n$ over an ordered field $\mathbf{R}$, the number of positive roots counted with multiplicity satisfies the inequality*

$$\underset{\text{mult}}{\#}\left\{x \in \mathbf{R}_{>0} \;\middle|\; P(x) = 0\right\} \quad \leq \quad \hat{V}(c_0, c_1, \ldots, c_n). \tag{3.4}$$

More generally, the number of roots in any interval $]a,b] \subset \mathbf{R}$ satisfies the inequality

$$\underset{\text{mult}}{\#}\left\{x \in]a,b] \;\middle|\; P(x) = 0\right\} \quad \leq \quad \hat{V}_a^b(P, P', \ldots, P^{(n)}). \tag{3.5}$$

Equality holds for every interval $]a,b] \subset \mathbf{R}$ if and only if P has n roots in $\mathbf{R}$.
The excess (r.h.s. $-$ l.h.s.) is even for all P, a, b if and only if $\mathbf{R}$ is real closed. □

Example 3.3 (signature). For a self-adjoint matrix $A \in \mathbb{C}^{n\times n}$, where $A^{\mathrm{T}} = \overline{A}$, all eigenvalues are real. Its *signature* is defined as the difference $p - q$ where p resp. q is the number of positive resp. negative eigenvalues. These can be read from the characteristic polynomial $P = c_0 + c_1X + \cdots + c_nX^n$ as $p = \hat{V}(c_0, c_1, \ldots, c_n)$ and $q = \hat{V}(c_0, -c_1, \ldots, (-1)^n c_n)$.

Remark 3.4. The Budan–Fourier bound is not restricted to polynomials. Over the real numbers $\mathbb{R}$ the inequality (3.5) holds for every n-times differentiable function $P \neq 0$ such that $P^{(n)}$ is of constant sign on $[a,b]$. This extends to every ordered field $\mathbf{R}$, provided that differentiability of $f\colon [a,b] \to \mathbf{R}$ means that there exists $f'\colon [a,b] \to \mathbf{R}$ and $C > 0$ such that $|f(x) - f(x_0) - f'(x_0)(x - x_0)| \leq C|x - x_0|^2$ for all $x, x_0 \in [a,b]$.

The upper bounds (3.4) and (3.5) are easy to compute but often overestimate the number of roots. This was the state of knowledge before Sturm's ground-breaking discovery in 1829. Sturm's theorem (Corollary 3.16 below) gives the precise number of roots.

3.2. **The Cauchy index.** The Cauchy index judiciously counts roots with a sign ± 1 encoding the passage from negative to positive or from positive to negative. Instead of zeros of P, it is customary to count poles of $f = \frac{1}{P}$, which is of course equivalent.

Informally, as illustrated in Figure 2, we set $\operatorname{Ind}_a(f) = +1$ if f jumps from $-\infty$ to $+\infty$, and $\operatorname{Ind}_a(f) = -1$ if f jumps from $+\infty$ to $-\infty$, and $\operatorname{Ind}_a(f) = 0$ in all other cases.

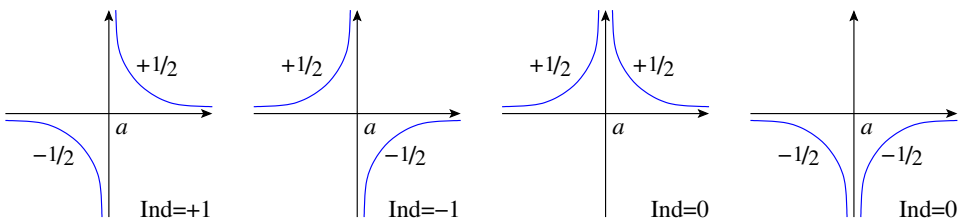


FIGURE 2. A pole a and its Cauchy index $\operatorname{Ind}_a(f) = \operatorname{Ind}_a^+(f) - \operatorname{Ind}_a^-(f)$

Formally, we define the right limit $\lim_a^+ f$ and the left limit $\lim_a^- f$ of $f \in \mathbf{R}(X)^*$ at $a \in \mathbf{R}$ by factoring $f = (X - a)^m g$ with $m \in \mathbb{Z}$ and $g \in \mathbf{R}(X)^*$ such that $g(a) \in \mathbf{R}^*$. If $m \geq 0$, then $\lim_a^\varepsilon f = f(a) \in \mathbf{R}$ for both $\varepsilon \in \{\pm\}$; if $m < 0$, then $\lim_a^\varepsilon f = \varepsilon^m \cdot \operatorname{sign} g(a) \cdot (+\infty) \in \{\pm\infty\}$.

Definition 3.5. The *Cauchy index* of a rational function $f \in \mathbf{R}(X)^*$ at a point $a \in \mathbf{R}$ is

$$\operatorname{Ind}_a(f) := \operatorname{Ind}_a^+(f) - \operatorname{Ind}_a^-(f) \quad \text{where} \quad \operatorname{Ind}_a^\varepsilon(f) := \begin{cases} +\frac{1}{2} & \text{if } \lim_a^\varepsilon f = +\infty, \\ -\frac{1}{2} & \text{if } \lim_a^\varepsilon f = -\infty, \\ 0 & \text{otherwise.} \end{cases} \tag{3.6}$$

For $a < b$ in $\mathbf{R}$ we define the Cauchy index of $f \in \mathbf{R}(X)^*$ on the interval $[a,b]$ by

$$\operatorname{Ind}_a^b(f) := \operatorname{Ind}_a^+(f) + \sum_{x \in]a,b[} \operatorname{Ind}_x(f) - \operatorname{Ind}_b^-(f). \tag{3.7}$$

The sum is well-defined because only finitely many points $x \in]a,b[$ contribute.
For $b < a$ we define $\operatorname{Ind}_a^b(f) := -\operatorname{Ind}_b^a(f)$, and for $a = b$ we set $\operatorname{Ind}_a^a(f) := 0$.
Finally, we set $\operatorname{Ind}_a^b(\frac{R}{S}) := 0$ in the degenerate case where $R = 0$ or $S = 0$.

Here we opt for a more comprehensive definition (3.7) than usual, in order to take care of boundary points. We will frequently subdivide intervals, and this technique works best with a uniform definition that avoids case distinctions. Moreover, we will have reason to consider piecewise rational functions in §4.

Proposition 3.6. *The Cauchy index enjoys the following properties.*

(a) *Subdivision:* $\operatorname{Ind}_a^b(f) + \operatorname{Ind}_b^c(f) = \operatorname{Ind}_a^c(f)$ *for all* $a,b,c \in \mathbf{R}$.
(b) *Invariance:* $\operatorname{Ind}_a^b(f \circ \tau) = \operatorname{Ind}_{\tau(a)}^{\tau(b)}(f)$ *for every linear fractional transformation* $\tau\colon [a,b] \to \mathbf{R}$, $\tau(x) = \frac{px+q}{rx+s}$ *where* $p,q,r,s \in \mathbf{R}$, *without poles on* $[a,b]$.
(c) *Scaling:* $\operatorname{Ind}_a^b(gf) = \operatorname{sign}(g)\operatorname{Ind}_a^b(f)$ *if* g *is of constant sign on* $[a,b]$.
(d) *Addition:* $\operatorname{Ind}_a^b(f+g) = \operatorname{Ind}_a^b(f) + \operatorname{Ind}_a^b(g)$ *if* f,g *have no common poles.* □

3.3. **Counting real roots.** The ring $\mathbf{R}[X]$ is equipped with a derivation $P \mapsto P'$ sending each polynomial $P = \sum_{k=0}^n p_k X^k$ to its formal derivative $P' = \sum_{k=1}^n k p_k X^{k-1}$. This extends in a unique way to a derivation on the field $\mathbf{R}(X)$ sending $f = \frac{R}{S}$ to $f' = \frac{R'S - RS'}{S^2}$. This is an $\mathbf{R}$-linear map satisfying Leibniz' rule $(fg)' = f'g + fg'$. For $f \in \mathbf{R}(X)^*$ the quotient f'/f is called the *logarithmic derivative* of f; it enjoys the following property.

Proposition 3.7. *For every* $f \in \mathbf{R}(X)^*$ *we have* $\operatorname{Ind}_a(f'/f) = +1$ *if* a *is a zero of* f, $\operatorname{Ind}_a(f'/f) = -1$ *if* a *is a pole of* f, *and* $\operatorname{Ind}_a(f'/f) = 0$ *in all other cases.*

Proof. We have $f = (X-a)^m g$ with $m \in \mathbb{Z}$ and $g \in \mathbf{R}(X)^*$ such that $g(a) \in \mathbf{R}^*$. By Leibniz' rule we obtain $\frac{f'}{f} = \frac{m}{X-a} + \frac{g'}{g}$. The fraction $\frac{g'}{g}$ does not contribute to the index because it does not have a pole at a. We conclude that $\operatorname{Ind}_a(f'/f) = \operatorname{sign}(m)$. □

Corollary 3.8. *For every* $f \in \mathbf{R}(X)^*$ *and* $a < b$ *in* $\mathbf{R}$ *the index* $\operatorname{Ind}_a^b(f'/f)$ *equals the number of roots minus the number of poles of* f *in* $[a,b]$, *counted without multiplicity. Roots and poles on the boundary count for one half.* □

The corollary remains true for $f = \frac{R}{S}$ when $R = 0$ or $S = 0$, with the convention that we count only *isolated* roots and poles. Polynomials $P \in \mathbf{R}[X]^*$ have no poles, whence $\operatorname{Ind}_a^b(P'/P)$ simply counts the number of roots of P in $[a,b]$.

3.4. **The inversion formula.** While the Cauchy index can be defined over any ordered field $\mathbf{R}$, the following results require $\mathbf{R}$ to be real closed. They will allow us to calculate the Cauchy index by Sturm chains (§3.5) via iterated Euclidean division (§3.6).

The starting point is the observation that the intermediate value property of polynomials $P \in \mathbf{R}[X]$ can then be reformulated quantitatively as $\operatorname{Ind}_a^b(\frac{1}{P}) = V_a^b(1,P)$. More generally, we have the following inversion formula of Cauchy [9, §I, Thm. I].

Theorem 3.9. *Let* $\mathbf{R}$ *be a real closed field. For all* $P,Q \in \mathbf{R}[X]$ *and* $a,b \in \mathbf{R}$ *we have*

$$\operatorname{Ind}_a^b\Big(\frac{Q}{P}\Big) + \operatorname{Ind}_a^b\Big(\frac{P}{Q}\Big) = V_a^b\Big(1,\frac{P}{Q}\Big) = V_a^b\Big(1,\frac{Q}{P}\Big). \tag{3.8}$$

If P *and* Q *do not have common zeros at* a *or* b, *then this simplifies to*

$$\operatorname{Ind}_a^b\Big(\frac{Q}{P}\Big) + \operatorname{Ind}_a^b\Big(\frac{P}{Q}\Big) = V_a^b(P,Q). \tag{3.9}$$

If a or b is a pole of $\frac{P}{Q}$ or $\frac{Q}{P}$, then the signs in (3.8) are evaluated using the convention $\operatorname{sign}(\infty) = 0$. The inversion formula will follow as a special case from the product formula (4.3), but its proof is short enough to be given separately here.

Proof. We can assume $a < b$ and $P, Q \in \mathbf{R}[X]^*$ and $\gcd(P,Q) = 1$, so each pole is a zero of either P or Q, and Equations (3.8) and (3.9) become equivalent. They are additive with respect to subdivision of $[a,b]$, by Proposition 3.6(a), so it suffices to treat the case where $[a,b]$ contains at most one pole.

Global analysis away from poles: Suppose that $[a,b]$ does not contain zeros of P or Q. Then both indices $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right)$ and $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right)$ vanish in the absence of poles, and the intermediate value property ensures that P and Q are of constant sign on $[a,b]$, whence $V_a^b(P,Q) = 0$.

Local analysis at a pole: Suppose that $[a,b]$ contains a pole. Subdividing, if necessary, we can assume that this pole is either a or b. Applying the symmetry $X \mapsto a+b-X$, if necessary, we can assume that the pole is a. Since Equation (3.9) is symmetric in P and Q, we can assume that $P(a) = 0$. We then have $Q(a) \neq 0$, whence Q has constant sign on $[a,b]$ and $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right) = 0$. Likewise, P has constant sign on $]a,b]$ and $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) = \operatorname{Ind}_a^+\left(\frac{Q}{P}\right)$. On the right hand side we find $V_a(P,Q) = 1/2$, and for $V_b(P,Q)$ two cases occur:

- if $V_b(P,Q) = 0$, then $\frac{Q}{P} > 0$ on $]a,b]$, whence $\lim_a^+\left(\frac{Q}{P}\right) = +\infty$,
- if $V_b(P,Q) = 1$, then $\frac{Q}{P} < 0$ on $]a,b]$, whence $\lim_a^+\left(\frac{Q}{P}\right) = -\infty$.

In both cases we find $\operatorname{Ind}_a^+\left(\frac{Q}{P}\right) = V_a^b(P,Q)$, whence Equation (3.9) holds. □

3.5. **Sturm chains.** In the rest of this section we exploit the inversion formula (3.9), and we will therefore continue to assume $\mathbf{R}$ to be real closed. We can then calculate the Cauchy index $\operatorname{Ind}_a^b(\frac{R}{S})$ by iterated euclidean division (§3.6). The crucial condition is the following.

Definition 3.10. A sequence of polynomials $(S_0, \dots, S_n)$ in $\mathbf{R}[X]$ is a *Sturm chain* with respect to an interval $I \subset \mathbf{R}$ if it satisfies Sturm's condition:

$$\text{If } S_k(x) = 0 \text{ for some } x \in I \text{ and } 0 < k < n, \text{ then } S_{k-1}(x)S_{k+1}(x) < 0. \tag{3.10}$$

We will usually not explicitly mention the interval if it is understood from the context, or if $(S_0, \dots, S_n)$ is a Sturm chain on all of $\mathbf{R}$. For $n = 1$ Condition (3.10) is void and should be replaced by the requirement that S_0 and S_1 have no common zeros.

Theorem 3.11. *If $(S_0, S_1, \dots, S_{n-1}, S_n)$ is a Sturm chain in $\mathbf{R}[X]$ with respect to $[a,b]$, then*

$$\operatorname{Ind}_a^b\left(\frac{S_1}{S_0}\right) + \operatorname{Ind}_a^b\left(\frac{S_{n-1}}{S_n}\right) = V_a^b\left(S_0, S_1, \dots, S_{n-1}, S_n\right). \tag{3.11}$$

Proof. For $n = 1$ this is the inversion formula (3.9). For $n = 2$ the inversion formula implies

$$\operatorname{Ind}_a^b\left(\frac{S_1}{S_0}\right) + \operatorname{Ind}_a^b\left(\frac{S_0}{S_1}\right) + \operatorname{Ind}_a^b\left(\frac{S_2}{S_1}\right) + \operatorname{Ind}_a^b\left(\frac{S_1}{S_2}\right) = V_a^b\left(S_0, S_1, S_2\right).$$

This is a telescopic sum. Contributions to the middle indices arise at zeros of S_1, but at each zero of S_1 its neighbours S_0 and S_2 have opposite signs, which means that these terms cancel each other. Iterating this argument, we obtain (3.11) by induction on n. □

The following algebraic criterion for Sturm chains will be useful in §3.6 and §5.1:

Proposition 3.12. *Consider a sequence $(S_0, \dots, S_n)$ in $\mathbf{R}[X]$ such that*

$$A_k S_{k+1} + B_k S_k + C_k S_{k-1} = 0 \qquad \text{for} \qquad 0 < k < n, \tag{3.12}$$

with $A_k, B_k, C_k \in \mathbf{R}[X]$ satisfying $A_k > 0$ and $C_k \geq 0$ on some interval $I \subset \mathbf{R}$. Then $(S_0, \dots, S_n)$ is a Sturm chain on I if and only if the terminal pair (S_{n-1}, S_n) has no common zeros in I.

Proof. We assume that $n \geq 2$. If (S_{n-1}, S_n) has a common zero, then the Sturm condition (3.10) is obviously violated. Suppose that (S_{n-1}, S_n) has no common zeros in I. If $S_k(x) = 0$ for $x \in I$ and $0 < k < n$, then $S_{k+1}(x) \neq 0$. Otherwise Equation (3.12) would imply that $S_k, \ldots, S_n$ vanish at x, which is excluded by our hypothesis. Now, the equation $A_k(x)S_{k+1}(x) + C_k(x)S_{k-1}(x) = 0$ with $A_k(x)S_{k+1}(x) \neq 0$ implies $C_k(x)S_{k-1}(x) \neq 0$. Using $A_k(x) > 0$ and $C_k(x) > 0$ we conclude that $S_{k-1}(x)S_{k+1}(x) < 0$. □

For many calulcations $A_k = C_k = 1$ suffices, as in §3.6, but the general setting is more flexible because A_k and C_k can absorb positive factors and thus purge S_{k+1} and S_{k-1} of irrelevancy. Sturm chains as in (3.12) also occur naturally for orthogonal polynomials.

3.6. **Euclidean chains.** The definition of Sturm chains is fairly general and could be used for more general functions than polynomials. The crucial observation for polynomials is that the euclidean algorithm can be used to construct Sturm chains as follows.

Consider a rational function $f = \frac{R}{S} \in \mathbf{R}(X)^*$ represented by polynomials $R, S \in \mathbf{R}[X]^*$. Iterated euclidean division produces a sequence of polynomials starting with $P_0 = S$ and $P_1 = R$, such that $P_{k-1} = Q_k P_k - P_{k+1}$ and $\deg P_{k+1} < \deg P_k$ for all $k = 1, 2, 3, \ldots$. This process eventually stops when we reach $P_{n+1} = 0$, in which case $P_n \sim \gcd(P_0, P_1)$.

Stated differently, this construction is the expansion of f into the continued fraction

$$f = \frac{P_1}{P_0} = \frac{P_1}{Q_1 P_1 - P_2} = \cfrac{1}{Q_1 - \cfrac{P_2}{P_1}} = \cfrac{1}{Q_1 - \cfrac{1}{Q_2 - \cfrac{P_3}{P_2}}} = \cdots = \cfrac{1}{Q_1 - \cfrac{1}{Q_2 - \cfrac{\cdots}{Q_{n-1} - \cfrac{1}{Q_n}}}}.$$

Definition 3.13. In this euclidean remainder sequence, the last polynomial $P_n \neq 0$ divides all preceding polynomials $P_0, P_1, \ldots, P_{n-1}$. The *euclidean chain* $(S_0, S_1, \ldots, S_n)$ associated to the fraction $\frac{R}{S} \in \mathbf{R}(X)^*$ is defined by $S_k := P_k / P_n$ for $k = 0, \ldots, n$.

We thus obtain $\frac{R}{S} = \frac{S_1}{S_0}$ with $\gcd(S_0, S_1) = S_n = 1$, and by construction $(S_0, S_1, \ldots, S_n)$ depends only on the fraction $\frac{R}{S}$ and not on the polynomials R, S representing it. By Proposition 3.12 the equations $S_{k-1} + S_{k+1} = Q_k S_k$ ensure that $(S_0, S_1, \ldots, S_n)$ is a Sturm chain.

3.7. **Sturm's theorem.** We can now fix the following convenient notation.

Definition 3.14. For $\frac{R}{S} \in \mathbf{R}(X)$ and $a, b \in \mathbf{R}$ we define the *Sturm index* to be

$$\mathrm{Sturm}_a^b\Big(\frac{R}{S}\Big) := V_a^b\big(S_0, S_1, \ldots, S_n\big),$$

where $(S_0, S_1, \ldots, S_n)$ is the euclidean chain associated to $\frac{R}{S}$. We include two exceptional cases. If $S = 0$ and $R \neq 0$, the euclidean chain is $(0, 1)$ of length $n = 1$. If $R = 0$, we take the chain (1) of length $n = 0$. In both cases we obtain $\mathrm{Sturm}_a^b\big(\frac{R}{S}\big) = 0$.

This definition is effective in the sense that $\mathrm{Sturm}_a^b\big(\frac{R}{S}\big)$ can immediately be calculated. Definition 3.5 of the Cauchy index $\mathrm{Ind}_a^b\big(\frac{R}{S}\big)$, however, assumes knowledge of all roots of S in $[a, b]$. This difficulty is overcome by Sturm's celebrated theorem, generalized by Cauchy, equating the Cauchy index with the Sturm index over a real closed field.

Theorem 3.15 (Sturm 1829/35, Cauchy 1831/37)**.** *For every pair $R, S \in \mathbf{R}[X]$ of polynomials over a real closed field $\mathbf{R}$ we have*

$$\mathrm{Ind}_a^b\Big(\frac{R}{S}\Big) = \mathrm{Sturm}_a^b\Big(\frac{R}{S}\Big). \tag{3.13}$$

Proof. Equation (3.13) is trivially true if $R = 0$ or $S = 0$, according to our definitions. We can thus assume $R, S \in \mathbf{R}[X]^*$. Let $(S_0, S_1, \dots, S_n)$ be the euclidean chain associated to the fraction $\frac{R}{S}$. Since $\frac{R}{S} = \frac{S_1}{S_0}$ and $S_n = 1$, Theorem 3.11 implies that

$$\operatorname{Ind}_a^b\Big(\frac{R}{S}\Big) = \operatorname{Ind}_a^b\Big(\frac{S_1}{S_0}\Big) + \operatorname{Ind}_a^b\Big(\frac{S_{n-1}}{S_n}\Big) = V_a^b\big(S_0, S_1, \dots, S_n\big) = \operatorname{Sturm}_a^b\Big(\frac{R}{S}\Big). \qquad \square$$

This theorem is usually stated under the additional hypotheses that $\gcd(R,S) = 1$ and $S(a)S(b) \neq 0$. Our formulation of Theorem 3.15 does not require either of these conditions, because they are absorbed into our slightly refined definitions: $\gcd(R,S) = 1$ becomes superfluous by formulating Definitions 3.5 and 3.14 such that both indices become well-defined on $\mathbf{R}(X)$. The exception $S(a)S(b) = 0$ is anticipated in Definitions 3.1 and 3.5 by counting boundary points correctly. Arranging these details is not only an aesthetic preoccupation: it clears the way for a uniform treatment of the complex case in §4.

As an immediate consequence of §3.3 we obtain Sturm's classical theorem [55, §2].

Corollary 3.16 (Sturm 1829/35)**.** *For every polynomial $P \in \mathbf{R}[X]^*$ we have*

$$\#\big\{\, x \in [a,b] \;\big|\; P(x) = 0 \,\big\} = \operatorname{Sturm}_a^b\Big(\frac{P'}{P}\Big), \tag{3.14}$$

where roots on the boundary count for one half. $\square$

By the usual bisection method, Formula (3.14) provides an algorithm to locate all real roots of any given real polynomial. Once the roots are well separated, one can switch to Newton's method (§6.3), which is simpler to apply and converges much faster.

Remark 3.17. Formula (3.14) counts real roots of P without multiplicity. Multiplicities can be counted by observing that x is a root of P of multiplicity $m \geq 2$ if and only if x is a root of $\gcd(P, P')$ of multiplicity $m - 1$. See Rahman–Schmeisser [42, Thm. 10.5.6].

Remark 3.18. The intermediate value property is essential for (3.13) and (3.14). Over $\mathbb{Q}$, for example, the function $f(x) = 2x/(x^2 - 2)$ has no poles, whence $\operatorname{Ind}_1^2(f) = 0$. A Sturm chain is given by $S_0 = X^2 - 2$ and $S_1 = 2X$ and $S_2 = 2$, whence $V_1^2(S_0, S_1, S_2) = 1$. Here the Sturm index does not count zeros and poles in $\mathbb{Q}$ but in the real closure $\mathbb{Q}^c$.

Remark 3.19. Sturm's theorem can be seen as an algebraic analogue of the fundamental theorem of calculus. It reduces a 1–dimensional counting problem on the interval $[a,b]$ to a 0–dimensional counting problem on the boundary $\{a,b\}$. In §4 we will generalize this to the complex realm, reducing a 2–dimensional counting problem on a rectangle Γ to a 1–dimensional counting problem on the boundary $\partial\Gamma$.

3.8. **Pseudo-euclidean division.** Euclidean division works for polynomials over a field. In §5.1 we consider polynomials $S, P \in \mathbf{R}[Y,X] = \mathbf{K}[X]$ over $\mathbf{K} = \mathbf{R}[Y]$. To this end we introduce pseudo-euclidean division over an integral ring $\mathbf{K}$: for all $S, P \in \mathbf{K}[X]$ with $P \neq 0$ there exists a unique pair $Q^*, R^* \in \mathbf{K}[X]$ such that $c^d S = PQ^* - R^*$ and $\deg R^* < \deg P$, where $c \in \mathbf{K}$ is the leading coefficient of P and $d = \max\{\,0, 1 + \deg S - \deg P\,\}$.

When working over a field $\mathbf{F} \supset \mathbf{K}$, the leading coefficient $c \neq 0$ is invertible in $\mathbf{F}$, and we can divide $c^d S = PQ^* - R^*$ by c^d to recover $S = PQ - R$, where $Q = Q^*/c^d$ and $R = R^*/c^d$. Pseudo-euclidean division may nevertheless be more convenient. For polynomials in $\mathbb{Q}[X]$, for example, it is often more efficient to clear denominators and to work in $\mathbb{Z}[X]$ in order to avoid coefficient swell; see [17, §6.12].

For Sturm chains it is advantageous to have $c^d S = PQ^* - R^*$ with d even. In a typical Sturm chain we would expect $\deg S = \deg P + 1$ and thus $d = 2$. If d happens to be odd, we can multiply Q^* and R^* by c and augment d by 1. Starting from $S_0, S_1 \in \mathbf{K}[X]$ we can thus construct a chain $S_0, S_1, \dots, S_n \in \mathbf{K}[X]$ with $S_{k+1} = B_k S_k - c_k^2 S_{k-1}$ as in Proposition 3.12.

4. Cauchy's theorem for complex polynomials

We continue to work over a real closed field $\mathbf{R}$ and now consider its complex extension $\mathbf{C} = \mathbf{R}[i]$ where $i^2 = -1$. In this section we define the algebraic winding number and use it to prove Cauchy's theorem (Corollary 4.9). To this end we establish the product formula (4.3), which seems to be new. It ensures, for example, that the algebraic winding number can cope with roots on the boundary, as already emphasized in Theorem 1.5.

4.1. **Real and complex fields.** Let $\mathbf{R}$ be an ordered field. For every $x \in \mathbf{R}$ we have $x^2 \geq 0$, whence $x^2 + 1 > 0$. The polynomial $X^2 + 1$ is thus irreducible in $\mathbf{R}[X]$, and the quotient $\mathbf{C} = \mathbf{R}[X]/(X^2+1)$ is a field. It is denoted by $\mathbf{C} = \mathbf{R}[i]$ with $i^2 = -1$. Each element $z \in \mathbf{C}$ can be uniquely written as $z = x + yi$ with $x, y \in \mathbf{R}$. We can thus identify $\mathbf{C}$ with $\mathbf{R}^2$ via the map $\mathbf{R}^2 \to \mathbf{C}$, $(x,y) \mapsto z = x + yi$, and define $\operatorname{re}(z) := x$ and $\operatorname{im}(z) := y$.

Using this notation, addition and multiplication in $\mathbf{C}$ are given by

$$(x+yi) + (x'+y'i) = (x+x') + (y+y')i,$$
$$(x+yi) \cdot (x'+y'i) = (xx'-yy') + (xy'+x'y)i.$$

The ring automorphism $\mathbf{R}[X] \to \mathbf{R}[X]$, $X \mapsto -X$, fixes X^2+1 and thus descends to a field automorphism $\mathbf{C} \to \mathbf{C}$ that maps each $z = x + yi$ to its conjugate $\bar{z} = x - yi$. We have $\operatorname{re}(z) = \frac{1}{2}(z + \bar{z})$ and $\operatorname{im}(z) = \frac{1}{2i}(z - \bar{z})$. The product $z\bar{z} = x^2 + y^2 \geq 0$ vanishes if and only if $z = 0$. For $z \neq 0$ we thus find

$$z^{-1} = \frac{\bar{z}}{z\bar{z}} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2} i.$$

If $\mathbf{R}$ is real closed, then every $x \in \mathbf{R}_{\geq 0}$ has a square root $\sqrt{x} \in \mathbf{R}_{\geq 0}$. For $z \in \mathbf{C}$ we can thus define $|z| := \sqrt{z\bar{z}}$, which extends the absolute value of $\mathbf{R}$. For all $u, v \in \mathbf{C}$ we have:

(0) $|\operatorname{re}(u)| \leq |u|$ and $|\operatorname{im}(u)| \leq |u|$,
(1) $|u| \geq 0$, and $|u| = 0$ if and only if $u = 0$,
(2) $|u \cdot v| = |u| \cdot |v|$ and $|\bar{u}| = |u|$,
(3) $|u + v| \leq |u| + |v|$.

All verifications are straightforward. The triangle inequality (3) can be derived from the preceding properties as follows. If $u + v = 0$, then (3) follows from (1). If $u + v \neq 0$, then $1 = \frac{u}{u+v} + \frac{v}{u+v}$, and applying (0) and (2) we find

$$1 = \operatorname{re}\Big(\frac{u}{u+v}\Big) + \operatorname{re}\Big(\frac{v}{u+v}\Big) \leq \Big|\frac{u}{u+v}\Big| + \Big|\frac{v}{u+v}\Big| = \frac{|u|}{|u+v|} + \frac{|v|}{|u+v|}.$$

4.2. **Real and complex variables.** Just as we identify $(x,y) \in \mathbf{R}^2$ with $z = x + iy \in \mathbf{C}$, we consider $\mathbf{C}[Z]$ as a subring of $\mathbf{C}[X,Y]$ with $Z = X + iY$. The conjugation on $\mathbf{C}$ extends to a ring automorphism of $\mathbf{C}[X,Y]$ fixing X and Y, so that the conjugate of $Z = X + iY$ is $\overline{Z} = X - iY$. In this sense, X and Y are real variables, whereas Z is a complex variable.

Every polynomial $F \in \mathbf{C}[X,Y]$ can be uniquely decomposed as $F = R + iS$ with $R, S \in \mathbf{R}[X,Y]$, namely $R = \operatorname{re} F := \frac{1}{2}(F + \overline{F})$ and $S = \operatorname{im} F := \frac{1}{2i}(F - \overline{F})$. In particular, we thus recover the familiar formulae $X = \operatorname{re} Z$ and $Y = \operatorname{im} Z$.

For $F, G \in \mathbf{C}[X,Y]$ we set $F \circ G := F(\operatorname{re} G, \operatorname{im} G)$. The map $F \mapsto F \circ G$ is the unique ring endomorphism $\mathbf{C}[X,Y] \to \mathbf{C}[X,Y]$ that maps $Z \mapsto G$ and is equivariant with respect to conjugation, because $Z \mapsto G$ and $\overline{Z} \mapsto \overline{G}$ are equivalent to $X \mapsto \operatorname{re} G$ and $Y \mapsto \operatorname{im} G$.

4.3. **The algebraic winding number.** Given a polynomial $P \in \mathbf{C}[X]$ and two parameters $t_0 < t_1$ in $\mathbf{R}$, the map $\gamma\colon [t_0, t_1] \to \mathbf{C}$ defined by $\gamma(t) = P(t)$ describes a polynomial path in $\mathbf{C}$. We define its winding number $w(\gamma)$ to be half the Cauchy index of $\frac{\operatorname{re} P}{\operatorname{im} P}$ on $[t_0, t_1]$:

$$w(P|[t_0,t_1]) := \tfrac{1}{2} \operatorname{Ind}_{t_0}^{t_1}\big(\tfrac{\operatorname{re} P}{\operatorname{im} P}\big).$$

This definition is geometrically motivated as follows. Assuming that $\gamma(t) \neq 0$ for all $t \in [t_0, t_1]$, the winding number $w(\gamma)$ counts the number of turns that γ performs around 0.

It changes by $+\frac{1}{2}$ each time γ crosses the real axis in counter-clockwise direction, and by $-\frac{1}{2}$ if the passage is clockwise. Our algebraic definition is slightly more comprehensive than the geometric one since it does not exclude zeros of γ.

Definition 4.1. Consider a subdivision $0 = t_0 < t_1 < \cdots < t_n = 1$ in $\mathbf{R}$ and polynomials $P_1, \ldots, P_n \in \mathbf{C}[X]$ that satisfy $P_k(t_k) = P_{k+1}(t_k)$ for $k = 1, \ldots, n-1$. This defines a *piecewise polynomial path* $\gamma\colon [0,1] \to \mathbf{C}$ by $\gamma(t) := P_k(t)$ for $t \in [t_{k-1}, t_k]$. If $\gamma(a) = \gamma(b)$, then γ is called a *closed path* or *loop*. Its *winding number* is defined as

$$w(\gamma) := \sum_{k=1}^{n} w(P_k|[t_{k-1}, t_k]). \tag{4.1}$$

This is well-defined according to Proposition 3.6(a), because it depends only on the path $\gamma\colon [0,1] \to \mathbf{R}$ and not on the chosen subdivision of the interval $[0,1]$.

4.4. **Normalization.** The following notation will be convenient. Given $a, b \in \mathbf{C}$, the map $\gamma\colon [0,1] \to \mathbf{C}$ defined by $\gamma(x) = a + x(b-a)$ joins $\gamma(0) = a$ and $\gamma(1) = b$ by a straight line segment. Its image will be denoted by $[a,b] := \gamma([0,1])$. For $a \neq b$ we set $]a,b[:= \gamma(]0,1[)$.

For $F \in \mathbf{C}[X,Y]$, we set $w(F|[a,b]) := w(F \circ \gamma)$. This is the winding number of the path traced by $F(z)$ as z runs from a straight to b. According to Proposition 3.6(b), the reverse orientation yields $w(F|[b,a]) = -w(F|[a,b])$.

A *rectangle* (with sides parallel to the axes) is a subset $\Gamma = [x_0, x_1] \times [y_0, y_1]$ in $\mathbf{C} = \mathbf{R}^2$ with $x_0 < x_1$ and $y_0 < y_1$ in $\mathbf{R}$. Its *interior* is $\operatorname{Int}\Gamma =]x_0, x_1[\times]y_0, y_1[$. Its *boundary* $\partial\Gamma$ consists of the four vertices $a = (x_0, y_0)$, $b = (x_1, y_0)$, $c = (x_1, y_1)$, $d = (x_0, y_1)$, and the four edges $]a,b[$, $]b,c[$, $]c,d[$, $]d,a[$ between them (see Figure 1).

Definition 4.2. Given a polynomial $F \in \mathbf{C}[X,Y]$ and a rectangle $\Gamma \subset \mathbf{C}$ as above, we set

$$w(F|\partial\Gamma) := w(F|[a,b]) + w(F|[b,c]) + w(F|[c,d]) + w(F|[d,a]). \tag{4.2}$$

Stated differently, we have $w(F|\partial\Gamma) = w(F \circ \gamma)$ where the path $\gamma\colon [0,1] \to \mathbf{C}$ linearly interpolates between the vertices $\gamma(0) = a$, $\gamma(1/4) = b$, $\gamma(1/2) = c$, $\gamma(3/4) = d$, and $\gamma(1) = a$.

Lemma 4.3 (subdivision)**.** *Suppose that we subdivide* $\Gamma = [x_0, x_2] \times [y_0, y_2]$

- *horizontally into* $\Gamma' = [x_0, x_1] \times [y_0, y_2]$ *and* $\Gamma'' = [x_1, x_2] \times [y_0, y_2]$,
- *or vertically into* $\Gamma' = [x_0, x_2] \times [y_0, y_1]$ *and* $\Gamma'' = [x_0, x_2] \times [y_1, y_2]$,

where $x_0 < x_1 < x_2$ *and* $y_0 < y_1 < y_2$. *Then* $w(F|\partial\Gamma) = w(F|\partial\Gamma') + w(F|\partial\Gamma'')$.

Proof. This follows from Definition 4.2 by one-dimensional subdivision (Proposition 3.6) and cancellation of the two internal edges having opposite orientations. □

We will frequently use subdivision in the sequel. As a first application we use it to establish the normalization (W1) of the algebraic winding number stated in Theorem 1.2.

Proposition 4.4. *For a linear polynomial* $F = Z - z_0$ *with* $z_0 \in \mathbf{C}$ *we find*

$$w(F|\partial\Gamma) = \begin{cases} 1 & \text{if } z_0 \text{ is in the interior of } \Gamma, \\ 1/2 & \text{if } z_0 \text{ is in one of the edges of } \Gamma, \\ 1/4 & \text{if } z_0 \text{ is in one of the vertices of } \Gamma, \\ 0 & \text{if } z_0 \text{ is in the exterior of } \Gamma. \end{cases}$$

Proof. By subdivision, all configurations can be reduced to the case where z_0 is a vertex of Γ. By symmetry, translation, and homothety we can assume that $z_0 = a = 0$, $b = 1$, $c = 1 + i$, $d = i$. Here an easy explicit calculation shows that $w(F|\partial\Gamma) = 1/4$ by adding

$$\begin{aligned} w(F|[a,b]) &= w(X|[0,1]) = \tfrac{1}{2}\operatorname{Ind}_0^1\left(\tfrac{X}{0}\right) = 0, \\ w(F|[b,c]) &= w(1+iX|[0,1]) = \tfrac{1}{2}\operatorname{Ind}_0^1\left(\tfrac{1}{X}\right) = \tfrac{1}{4}, \\ w(F|[c,d]) &= w(1+i-X|[0,1]) = \tfrac{1}{2}\operatorname{Ind}_0^1\left(\tfrac{1-X}{1}\right) = 0, \text{and} \\ w(F|[d,a]) &= w(i-iX|[0,1]) = \tfrac{1}{2}\operatorname{Ind}_0^1\left(\tfrac{0}{1-X}\right) = 0. \end{aligned}$$

□

4.5. **The product formula.** The product of two polynomials $F = P + iQ$ and $G = R + iS$ with $P, Q, R, S \in \mathbf{R}[X]$ is given by $FG = (PR - QS) + i(PS + QR)$. The following result relates the Cauchy indices of $\frac{P}{Q}$ and $\frac{R}{S}$ to that of $\frac{PR-QS}{PS+QR}$.

Theorem 4.5 (product formula)**.** *For all $P, Q, R, S \in \mathbf{R}[X]$ and $a, b \in \mathbf{R}$ we have*

$$\operatorname{Ind}_a^b\Big(\frac{PR-QS}{PS+QR}\Big) = \operatorname{Ind}_a^b\Big(\frac{P}{Q}\Big) + \operatorname{Ind}_a^b\Big(\frac{R}{S}\Big) - V_a^b\Big(1, \frac{P}{Q} + \frac{R}{S}\Big). \tag{4.3}$$

We remark that in the last term we have $\frac{P}{Q} + \frac{R}{S} = \frac{PS+QR}{QS} = \frac{\operatorname{im}(FG)}{\operatorname{im}(F)\operatorname{im}(G)}$, whence

$$V_a^b\big(1, \tfrac{P}{Q} + \tfrac{R}{S}\big) = \tfrac{1}{2}\big[\operatorname{sign}\big(\tfrac{PS+QR}{QS} \mid X \mapsto b\big) - \operatorname{sign}\big(\tfrac{PS+QR}{QS} \mid X \mapsto a\big)\big]. \tag{4.4}$$

If a or b is a pole, this is evaluated using the convention $\operatorname{sign}(\infty) = 0$.

For $(P = 0, Q = 1)$ or $(R = 0, S = 1)$ or $(P = S, Q = R)$, the product formula (4.3) reduces to the inversion formula (3.8). The proof of the general case follows the same lines.

Proof. Equation (4.3) trivially holds in the degenerate cases where $Q = 0$, $S = 0$, or $PS + QR = 0$; we can thus concentrate on the generic case where $Q, S, PS + QR \in \mathbf{R}[X]^*$. We can further assume $\gcd(P, Q) = \gcd(R, S) = 1$. Since (4.3) is additive with respect to subdivision of the interval $[a, b]$, we can assume that $[a, b]$ contains at most one pole.

Global analysis away from poles: Suppose that $[a, b]$ does not contain zeros of Q, S, or $PS + QR$. Then all three indices in (4.3) vanish in the absence of poles, and the intermediate value property ensures that Q, S, and $PS + QR$ are of constant sign on $[a, b]$, whence $V_a^b\big(1, \frac{PS+QR}{QS}\big) = 0$ and Equation (4.3) holds.

Local analysis at a pole: Suppose that $[a, b]$ contains a pole. Subdividing, if necessary, we can assume that this pole is either a or b. Applying the symmetry $X \mapsto a + b - X$, if necessary, we can assume that the pole is a. We thus have $V_a^b = \frac{1}{2}\operatorname{sign}(\frac{P}{Q} + \frac{R}{S} \mid X \mapsto b)$ and Q, S, $PS + QR$ are of constant sign on $]a, b]$. Applying the symmetry $(P, Q, R, S) \mapsto (P, -Q, R, -S)$, if necessary, we can assume that $\frac{P}{Q} + \frac{R}{S} > 0$ on $]a, b]$, whence $V_a^b = +\frac{1}{2}$. Based on these preparations we distinguish three cases.

First case. Suppose first that either $Q(a) = 0$ or $S(a) = 0$. Applying the symmetry $(P, Q, R, S) \mapsto (R, S, P, Q)$, if necessary, we can assume that $Q(a) = 0$ and $S(a) \neq 0$. Then $PS + QR$ does not vanish at a, whence $\operatorname{Ind}_a^b\big(\frac{PR-QS}{PS+QR}\big) = \operatorname{Ind}_a^b\big(\frac{R}{S}\big) = 0$. Since $\frac{P}{Q} + \frac{R}{S} > 0$ on $]a, b]$ we have $\lim_a^+ \frac{P}{Q} = +\infty$, whence $\operatorname{Ind}_a^b\big(\frac{P}{Q}\big) = +\frac{1}{2}$ and Equation (4.3) holds.

Second case. Suppose that $PS + QR$ vanishes at a, but $Q(a) \neq 0$ and $S(a) \neq 0$. Then $\operatorname{Ind}_a^b\big(\frac{P}{Q}\big) = \operatorname{Ind}_a^b\big(\frac{R}{S}\big) = 0$, and we only have to study the pole of

$$\frac{PR - QS}{PS + QR} = \frac{\frac{P}{Q} \cdot \frac{R}{S} - 1}{\frac{P}{Q} + \frac{R}{S}}. \tag{4.5}$$

At a the denominator vanishes and the numerator is negative:

$$\tfrac{P(a)}{Q(a)} + \tfrac{R(a)}{S(a)} = 0, \quad \text{whence} \quad \tfrac{P(a)}{Q(a)} \cdot \tfrac{R(a)}{S(a)} - 1 = -\tfrac{P^2(a)}{Q^2(a)} - 1 < 0.$$

This implies $\lim_a^+ \frac{PR-QS}{PS+QR} = -\infty$, whence $\operatorname{Ind}_a^b\big(\frac{PR-QS}{PS+QR}\big) = -\frac{1}{2}$ and Equation (4.3) holds.

Third case. Suppose that a is a common pole of $\frac{P}{Q}$ and $\frac{R}{S}$, whence also of $\frac{PR-QS}{PS+QR}$. Since $\frac{P}{Q} + \frac{R}{S} > 0$ on $]a, b]$, we have $\lim_a^+ \frac{P}{Q} = +\infty$ or $\lim_a^+ \frac{R}{S} = +\infty$. Equation (4.5) implies that $\lim_a^+\big(\frac{PR-QS}{PS+QR}\big) = \lim_a^+\big(\frac{P}{Q}\big) \cdot \lim_a^+\big(\frac{R}{S}\big)$, whence Equation (4.3) holds. □

The product formula (4.3) entails the multiplicativity (W2) stated in Theorem 1.2.

Corollary 4.6 (multiplicativity of winding numbers)**.** *We have $w(\gamma_1 \cdot \gamma_2) = w(\gamma_1) + w(\gamma_2)$ for all piecewise polynomial loops $\gamma_1, \gamma_2 \colon [0, 1] \to \mathbf{C}$ whose vertices are not mapped to* 0.

Proof. On a common subdivision $0 = t_0 < t_1 < \cdots < t_n = 1$, both γ_1, γ_2 are polynomials on each interval. There exist $F_k = P_k + iQ_k$ and $G_k = R_k + iS_k$ with $P_k, Q_k, R_k, S_k \in \mathbf{R}[X]$ such that $\gamma_1(t) = F_k(t)$ and $\gamma_2(t) = G_k(t)$ for all $t \in [t_{k-1}, t_k]$. By excluding zeros of γ_1, γ_2 on the vertices $t_0, t_1, \ldots, t_n$, we ensure that $\frac{P_k}{Q_k}(t_k) = \frac{P_{k+1}}{Q_{k+1}}(t_k)$ and $\frac{R_k}{S_k}(t_k) = \frac{R_{k+1}}{S_{k+1}}(t_k)$ for all $k = 1, \ldots, n-1$. Since both paths γ_1, γ_2 are closed, this also holds for $k = n$ with the understanding that $F_{n+1} = F_1$ and $G_{n+1} = G_1$. The desired result $w(\gamma_1 \cdot \gamma_2) = w(\gamma_1) + w(\gamma_2)$ now follows from the product formula (4.3), because at each vertex t_k the incoming and the outgoing boundary term from (4.4) cancel each other. □

Corollary 4.7. *Let $\gamma\colon [0,1] \to \mathbf{R}^2$ be a piecewise polynomial loop. If $F, G \in \mathbf{C}[X,Y]$ do not vanish at any of the vertices of γ, then $w(F \cdot G|\gamma) = w(F|\gamma) + w(G|\gamma)$.* □

More specifically, if F, G do not vanish at any of the vertices of the rectangle $\Gamma \subset \mathbf{R}^2$, then $w(F \cdot G|\partial\Gamma) = w(F|\partial\Gamma) + w(G|\partial\Gamma)$.

Remark 4.8. The corollary allows zeros of F or G on γ but excludes zeros on the vertices. This is not an artefact of our proof, but inherent to the algebraic winding number. As an illustration consider $\Gamma = [0,1] \times [0,1]$ and $H_s = Z \cdot (Z - 2 - is)$. The root $z_1 = 0$ lies on a vertex of Γ while the other root $z_2 = 2 + is$ is outside of Γ. In particular, we have $w(Z|\partial\Gamma) = 1/4$ and $w(Z - 2 - is|\partial\Gamma) = 0$. A little calculation shows that $w(H_1|\partial\Gamma) = 0$ and $w(H_0|\partial\Gamma) = 1/4$ and $w(H_{-1}|\partial\Gamma) = 1/2$, whence $w(H_s|\partial\Gamma)$ is not multiplicative.

Corollary 4.9. *Consider a split polynomial $F = (Z - z_1) \cdots (Z - z_n)$ in $\mathbf{C}[Z]$. If F does not vanish at any vertex of γ, then $w(F \circ \gamma) = \sum_{k=1}^{n} w(\gamma - z_k)$.* □

More specifically, if F does not vanish at any vertex of the rectangle $\Gamma \subset \mathbf{C}$, then $w(F|\partial\Gamma)$ counts the number of zeros in Γ. Each zero in the interior of Γ is counted with its multiplicity, whereas each zero in an edge of $\partial\Gamma$ is counted with half its multiplicity.

Remark 4.10. If we assume that $\mathbf{C}$ is algebraically closed, then *every* polynomial $F \in \mathbf{C}[Z]^*$ splits into linear factors as required in Corollary 4.9. So if you prefer some other existence proof for the roots, then you may skip the next section and still benefit from root location (Theorem 1.8). This seems to be the point of view adopted by Cauchy [8, 9] in 1831/37, which may explain why he did not attempt to use his index for a constructive proof of the Fundamental Theorem of Algebra. (In 1820 he had already given a non-constructive proof; see §7.6.1.) In 1836 Sturm and Liouville [58, 56] proposed to extend Cauchy's approach so as to obtain an algebraic existence proof. This is our aim in the next section.

5. The Fundamental Theorem of Algebra

In the preceding section we have constructed the algebraic winding number and derived its multiplicativity. We will now show its homotopy invariance and thus complete the real-algebraic proof of the Fundamental Theorem of Algebra. The geometric idea goes back to Gauss' doctoral dissertation (see §7.2), but the algebraic proof seems to be new.

5.1. Counting complex roots.

The following algebraic method for counting complex roots is the counterpart of Sturm's theorem for counting real roots (§3.3).

Theorem 5.1 (root counting)**.** *Consider a polynomial $F \in \mathbf{C}[Z]^*$ and a rectangle $\Gamma \subset \mathbf{C}$ 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 zeros of F in Γ: each zero in the interior of Γ is counted with its multiplicity, whereas each zero in an edge of $\partial\Gamma$ is counted with half its multiplicity.*

Proof. We factor $F = (Z - z_1) \cdots (Z - z_m)G$ with $z_1, \ldots, z_m \in \Gamma$ such that $G \in \mathbf{C}[Z]^*$ has no zeros in Γ. Then $w(G|\partial\Gamma) = 0$ according to Lemma 5.3 below. The assertion now follows from normalization (Proposition 4.4) and the product formula (Corollary 4.7). □

The crucial point is to show that $w(F|\partial\Gamma) = 0$ whenever F has no zeros in Γ, or by contraposition, that $w(F|\partial\Gamma) \neq 0$ implies that F vanishes at some point in Γ.

Lemma 5.2 (local version)**.** *If $F \in \mathbf{C}[X,Y]$ satisfies $F(x,y) \neq 0$ for some point $(x,y) \in \mathbf{R}^2$, then there exists $\delta > 0$ such that $w(F|\partial\Gamma) = 0$ for every $\Gamma \subset [x-\delta, x+\delta] \times [y-\delta, y+\delta]$.*

Proof. Let us make the standard continuity argument explicit. For all $s,t \in \mathbf{R}$ we have $F(x+s, y+t) = a + \sum_{j+k\geq 1} a_{jk} s^j t^k$ with $a = F(x,y) \neq 0$ and certain coefficients $a_{jk} \in \mathbf{C}$. We set $M := \max \sqrt[j+k]{|a_{jk}/a|}$, so that $|a_{jk}| \leq |a| \cdot M^{j+k}$. For $\delta := \frac{1}{4M}$ and $|s|, |t| \leq \delta$ we find

$$\Big|\sum_{j+k\geq 1} a_{jk} s^j t^k\Big| \leq \sum_{n\geq 1} \sum_{j+k=n} |a| \cdot M^{j+k} \cdot |s|^j \cdot |t|^k \leq |a| \sum_{n\geq 1} (n+1)\big(\tfrac{1}{4}\big)^n = \tfrac{7}{9}|a|. \tag{5.1}$$

This shows that F does not vanish in $U := [x-\delta, x+\delta] \times [y-\delta, y+\delta]$. Corollary 4.7 ensures that $w(F|\partial\Gamma) = w(cF|\partial\Gamma)$ for every rectangle $\Gamma \subset U$ and every constant $c \in \mathbf{C}^*$. Choosing $c = i/a$ we can assume that $F(x,y) = i$. The estimate (5.1) then shows that $\operatorname{im} F > 0$ on U, whence $w(F|\partial\Gamma) = 0$ for every rectangle $\Gamma \subset U$. □

While the preceding local lemma uses only continuity of polynomials and thus holds over every ordered field, the following global version requires the field $\mathbf{R}$ to be real closed.

Lemma 5.3 (global version)**.** *Let $\Gamma = [x_0, x_1] \times [y_0, y_1]$ be a rectangle in $\mathbf{R}^2$. If the polynomial $F \in \mathbf{C}[X,Y]$ satisfies $F(x,y) \neq 0$ for all $(x,y) \in \Gamma$, then $w(F|\partial\Gamma) = 0$.*

We remark that over the real numbers $\mathbb{R}$, a short proof can be given as follows:

Proof of Lemma 5.3 for the case $\mathbf{R} = \mathbb{R}$, using compactness. The rectangle Γ is covered by open sets $U(x,y) =]x-\delta, x+\delta[\times]y-\delta, y+\delta[$ as in Lemma 5.2, where (x,y) ranges over Γ and $\delta > 0$ depends on (x,y). Compactness of Γ ensures that there exists $\lambda > 0$, called a Lebesgue number of the cover, such that every rectangle $\Gamma' \subset \Gamma$ of diameter $< \lambda$ is contained in $U(x,y)$ for some $(x,y) \in \Gamma$.

For all subdivisions $x_0 = s_0 < s_1 < \cdots < s_m = x_1$ and $y_0 = t_0 < t_1 < \cdots < t_n = y_1$, Lemma 4.3 ensures that $w(F|\partial\Gamma) = \sum_{j=1}^m \sum_{k=1}^n w(F|\partial\Gamma_{jk})$ where $\Gamma_{jk} = [s_{j-1}, s_j] \times [t_{k-1}, t_k]$. For $s_j = x_0 + j\frac{x_1 - x_0}{m}$ and $t_k = y_0 + k\frac{y_1 - y_0}{n}$ with m,n sufficiently large, each Γ_{jk} has diameter $< \lambda$, so Lemma 5.2 implies that $w(F|\partial\Gamma_{jk}) = 0$ for all j,k, whence $w(F|\partial\Gamma) = 0$. □

The preceding compactness argument applies only to $\mathbb{C} = \mathbb{R}[i]$ over the field $\mathbb{R}$ of real numbers (§2.1) and not to an arbitrary real closed field (§2.2). In particular, it is no longer elementary in the sense that it uses a second-order property (§2.3). We therefore provide an elementary real-algebraic proof using Sturm chains:

Algebraic proof of Lemma 5.3, using Sturm chains. Each $F \in \mathbf{C}[X,Y]$ can be written as $F = \sum_{k=0}^m f_k X^k$ with $f_k \in \mathbf{C}[Y]$. In this way we consider $\mathbf{R}[X,Y] = \mathbf{R}[Y][X]$ as a polynomial ring in one variable X over $\mathbf{R}[Y]$. We can reduce $\frac{\operatorname{re} F}{\operatorname{im} F} = \frac{S_1}{S_0}$ such that $S_0, S_1 \in \mathbf{R}[X,Y]$ satisfy $\gcd(S_0, S_1) = 1$ in $\mathbf{R}(Y)[X]$. Pseudo-euclidean division in $\mathbf{R}[Y][X]$, as explained in §3.8, produces a chain $(S_0, \ldots, S_n)$ with $S_{k+1} = Q_k S_k - c_k^2 S_{k-1}$ for some $Q_k \in \mathbf{R}[Y][X]$ and $c_k \in \mathbf{R}[Y]^*$ such that $\deg_X S_{k+1} < \deg_X S_k$. After n iterations we end up with $S_{n+1} = 0$ and $S_n \in \mathbf{R}[Y]^*$. (If $\deg_X S_n > 0$, then $\gcd(S_0, S_1)$ in $\mathbf{R}(Y)[X]$ would be of positive degree.)

Regular case. Assume first that $S_n \in \mathbf{R}[Y]^*$ does not vanish at any point $y \in [y_0, y_1]$. Proposition 3.12 ensures that for each $y \in [y_0, y_1]$ specializing $(S_0, \ldots, S_n)$ in $Y \mapsto y$ yields a Sturm chain in $\mathbf{R}[X]$. Likewise, for each $x \in [x_0, x_1]$, specializing $(S_0, \ldots, S_n)$ in $X \mapsto x$ yields a Sturm chain in $\mathbf{R}[Y]$ with respect to the interval $[y_0, y_1]$. In the sum over all four edges of Γ, all contributions cancel each other in pairs:

$$\begin{aligned}
2w(F|\partial\Gamma) &= +\operatorname{Ind}_{x_0}^{x_1}\big(\tfrac{\operatorname{re} F}{\operatorname{im} F} \,\big|\, Y \mapsto y_0\big) + \operatorname{Ind}_{y_0}^{y_1}\big(\tfrac{\operatorname{re} F}{\operatorname{im} F} \,\big|\, X \mapsto x_1\big) \\
&\quad + \operatorname{Ind}_{x_1}^{x_0}\big(\tfrac{\operatorname{re} F}{\operatorname{im} F} \,\big|\, Y \mapsto y_1\big) + \operatorname{Ind}_{y_1}^{y_0}\big(\tfrac{\operatorname{re} F}{\operatorname{im} F} \,\big|\, X \mapsto x_0\big) \\
&= +V_{x_0}^{x_1}\big(S_0, \ldots, S_n \,\big|\, Y \mapsto y_0\big) + V_{y_0}^{y_1}\big(S_0, \ldots, S_n \,\big|\, X \mapsto x_1\big) \\
&\quad + V_{x_1}^{x_0}\big(S_0, \ldots, S_n \,\big|\, Y \mapsto y_1\big) + V_{y_1}^{y_0}\big(S_0, \ldots, S_n \,\big|\, X \mapsto x_0\big) = 0.
\end{aligned}$$

Singular case. In general we have to cope with a finite set $\mathscr{Y} \subset [y_0, y_1]$ of zeros of S_n. We can change the roles of X and Y and apply pseudo-euclidean division in $\mathbf{R}[X][Y]$; this leads to a finite set of zeros $\mathscr{X} \subset [x_0, x_1]$. We obtain a finite set $\mathscr{Z} = \mathscr{X} \times \mathscr{Y}$ of singular points in Γ, where both chains fail. (These points are potential zeros of F.)

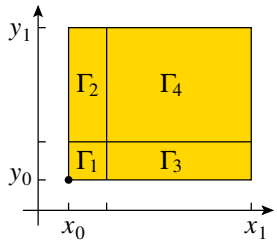


FIGURE 3. Isolating a singular point (x_0, y_0) within $\Gamma = [x_0, x_1] \times [y_0, y_1]$

By subdivision and symmetry we can assume that (x_0, y_0) is the only singular point in our rectangle $\Gamma = [x_0, x_1] \times [y_0, y_1]$. By hypothesis, F does not vanish in (x_0, y_0), so we can apply Lemma 5.2 to $\Gamma_1 = [x_0, x_0 + \delta] \times [y_0, y_0 + \delta]$ with $\delta > 0$ sufficiently small such that $w(F|\partial\Gamma_1) = 0$. The remaining three rectangles $\Gamma_2 = [x_0, x_0 + \delta] \times [y_0 + \delta, y_1]$, $\Gamma_3 = [x_0 + \delta, x_1] \times [y_0, y_0 + \delta]$, and $\Gamma_4 = [x_0 + \delta, x_1] \times [y_0 + \delta, y_1]$ do not contain any singular points, so that $w(F|\partial\Gamma_j) = 0$ by appealing to the regular case.

Summing over all sub-rectangles we conclude that $w(F|\partial\Gamma) = 0$. □

5.2. **Homotopy invariance.** We consider piecewise polynomial loops $\gamma_0, \gamma_1 \colon [0,1] \to \mathbf{C}^*$. A *homotopy* between γ_0 and γ_1 is a map $F \colon [0,1] \times [0,1] \to \mathbf{C}^*$ with $F(0,t) = \gamma_0(t)$ and $F(1,t) = \gamma_1(t)$ as well as $F(s,0) = F(s,1)$ for all $s, t \in [0,1]$. We also require that F be *piecewise polynomial*, which means that for some subdivision $0 = s_0 < s_1 < \cdots < s_m = 1$ and $0 = t_0 < t_1 < \cdots < t_n = 1$, the map F is polynomial on each $\Gamma_{jk} = [s_{j-1}, s_j] \times [t_{k-1}, t_k]$. We can now prove the homotopy invariance (W3) stated in Theorem 1.2.

Theorem 5.4. *We have $w(\gamma_0) = w(\gamma_1)$ whenever the loops γ_0, γ_1 are homotopic in $\mathbf{C}^*$.*

Proof. On $\Gamma = [0,1] \times [0,1]$ we have $w(F|\partial\Gamma) = w(\gamma_0) - w(\gamma_1)$. This follows from our hypothesis that $F(s,0) = F(s,1)$ for all $s \in [0,1]$, so these two opposite edges cancel each other. Subdivision as above yields $w(F|\partial\Gamma) = \sum_{jk} w(F|\partial\Gamma_{jk})$ according to Lemma 4.3. Since F has no zero, Lemma 5.3 ensures that $w(F|\partial\Gamma_{jk}) = 0$ for all j, k. □

As a consequence, the winding number $w(F_t|\partial\Gamma)$ does not change if we deform F_0 to F_1 avoiding zeros on $\partial\Gamma$. To make this precise, we consider $F \in \mathbf{C}[Z,T]$; for each $t \in [0,1]$ we denote by F_t the polynomial in $\mathbf{C}[Z]$ obtained by specializing $T \mapsto t$.

Corollary 5.5. *Suppose that $F \in \mathbf{C}[Z,T]$ is such that for each $t \in [0,1]$ the polynomial $F_t \in \mathbf{C}[Z]$ has no zeros on $\partial\Gamma$. Then $w(F_0|\partial\Gamma) = w(F_1|\partial\Gamma)$.* □

Remark 5.6. We have deduced homotopy invariance from the crucial Lemma 5.3 saying that $w(F|\partial\Gamma) = 0$ whenever F has no zeros in Γ. Both statements are in fact equivalent. After translation we can assume $(0,0) \in \Gamma$. The homotopy $F_t(X,Y) = F(tX, tY)$ deforms $F_1 = F$ to the constant $F_0 = F(0,0)$. If F has no zeros in Γ, then F_t has no zeros on the boundary $\partial\Gamma$, and homotopy invariance implies $w(F_1|\partial\Gamma) = w(F_0|\partial\Gamma) = 0$.

Homotopy invariance implies that small perturbations do not change the winding number and hence not the number of zeros. Rouché's theorem makes this explicit.

Corollary 5.7 (Rouché's theorem)**.** *Let $F, G \in \mathbf{C}[Z]$ be two complex polynomials such that $|F(z)| > |G(z)|$ for all $z \in \partial\Gamma$. Then F and $F + G$ have the same number of zeros in Γ.*

Proof. For $F_t = F + tG$ we find $|F_t| \geq |F| - t|G| > 0$ on $\partial\Gamma$ for all $t \in [0,1]$. By homotopy invariance (Corollary 5.5) $F_0 = F$ and $F_1 = F + G$ have the same winding number along $\partial\Gamma$, whence the same number of zeros in Γ (Theorem 5.1). □

5.3. **The global winding number.** We can now prove Theorem 1.7, stating that $w(F|\partial\Gamma) = \deg F$ for every polynomial $F \in \mathbf{C}[Z]^*$ and every sufficiently big rectangle Γ.

Proposition 5.8. *Given $F = Z^n + c_1 Z^{n-1} + \cdots + c_n$ in $\mathbf{C}[Z]$ we define its* Cauchy radius *to be $\rho_F := 1 + \max\{|c_1|, \ldots, |c_n|\}$. This implies that $|F(z)| \geq 1$ for every $z \in \mathbf{C}$ with $|z| \geq \rho_F$. Hence all zeros of F in $\mathbf{C}$ lie in the* Cauchy disk $B(\rho_F) = \{\, z \in \mathbf{C} \mid |z| < \rho_F \,\}$.

Proof. The assertion is true for $\rho_F = 1$, since then $F = Z^n$. We can thus assume $\rho_F > 1$. For all $z \in \mathbf{C}$ satisfying $|z| \geq \rho_F$ we find

$$\begin{aligned} |F(z) - z^n| &= |c_1 z^{n-1} + \cdots + c_{n-1} z + c_n| \leq |c_1||z^{n-1}| + \cdots + |c_{n-1}||z| + |c_n| \\ &\leq \max\{|c_1|, \ldots, |c_{n-1}|, |c_n|\} \left(|z|^{n-1} + \cdots + |z| + 1\right) = (\rho_F - 1)\frac{|z|^n - 1}{|z| - 1} \leq |z|^n - 1. \end{aligned}$$

We conclude that $|F(z)| \geq |z^n| - |F(z) - z^n| \geq 1$. □

This proposition holds over any ordered field $\mathbf{R}$ and its complex extension $\mathbf{C} = \mathbf{R}[i]$ because it uses only the general properties $|a+b| \leq |a| + |b|$ and $|a \cdot b| \leq |a| \cdot |b|$. It is not an existence result, but only an *a priori* bound. Over a real closed field $\mathbf{R}$, the algebraic winding number counts the number of zeros, and we arrive at the following conclusion.

Theorem 5.9. *For every polynomial $F \in \mathbf{C}[Z]^*$ and every rectangle $\Gamma \subset \mathbf{C}$ containing the Cauchy disk $B(\rho_F)$, we have $w(F|\partial\Gamma) = \deg F$.*

Proof. The assertion is clear for $F \in \mathbf{C}^*$ of degree 0. Consider $F = Z^n + c_1 Z^{n-1} + \cdots + c_n$ with $n \geq 1$ and set $M = \max\{|c_1|, \ldots, |c_n|\}$. The homotopy $F_t = Z^n + t(c_1 Z^{n-1} + \cdots + c_n)$ deforms $F_1 = F$ to $F_0 = Z^n$. The Cauchy radius of F_t is $\rho_t = 1 + tM$, which shrinks from $\rho_1 = \rho_F$ to $\rho_0 = 1$. By the previous proposition, the polynomial $F_t \in \mathbf{C}[Z]$ has no zeros on $\partial\Gamma$. We conclude that $w(F_1|\partial\Gamma) = w(F_0|\partial\Gamma) = n$, using Corollaries 5.5 and 4.9. □

This completes the proof of the Fundamental Theorem of Algebra. On the one hand Theorem 5.9 says that $w(F|\partial\Gamma) = \deg F$ provided that $\Gamma \supset B(\rho_F)$, and on the other hand Theorem 5.1 says that $w(F|\partial\Gamma)$ equals the number of zeros of F in $\Gamma \subset \mathbf{C}$.

Remark 5.10. The Cauchy radius of Proposition 5.8 is the simplest of an extensive family of root bounds, see Henrici [22, §6.4] and Rahman–Schmeisser [42, chap. 8]. We mention a nice and useful improvement: to each polynomial $F = c_0 Z^n + c_1 Z^{n-1} + \cdots + c_n$ in $\mathbf{C}[Z]$ we associate its *Cauchy polynomial* $F^\circ = |c_0|X^n - |c_1|X^{n-1} - \cdots - |c_n|$ in $\mathbf{R}[X]$. This implies $|F(z)| \geq F^\circ(|z|)$ for all $z \in \mathbf{C}$. We assume $c_0 \neq 0$ and $c_n \neq 0$, such that $F^\circ(0) < 0$ and $F^\circ(x) > 0$ for large $x \in \mathbf{R}$. According to Descartes' rule of signs (Theorem 3.2), the polynomial F° has a unique positive root ρ, whence $F^\circ(x) > 0$ for all $x > \rho$, and $F^\circ(x) < 0$ for all $0 \leq x < \rho$. Given some $r > 0$ with $F^\circ(r) > 0$, we have $|F(z)| > 0$ for all $|z| \geq r$, whence all zeros of F in $\mathbf{C}$ lie in the disk $B(r)$. (Again this holds over any ordered field $\mathbf{R}$.)

5.4. **Geometric characterization of the winding number.** We have constructed the algebraic winding number via Cauchy indices (W0) and then derived its geometric properties: normalization (W1), multiplicativity (W2), and homotopy invariance (W3). We now complete the circle by showing that (W1), (W2), (W3) characterize the winding number and imply (W0). We begin with two fundamental examples.

Example 5.11 (stars). Every loop γ in $U = \mathbf{C} \smallsetminus \mathbf{R}_{\leq 0}$ is homotopic in U to the constant loop $\gamma_0 = 1$ via $\gamma_s = 1 + s(\gamma - 1)$, whence (W1) and (W3) imply $w(\gamma) = 0$. The same holds in $\mathbf{C} \smallsetminus c\mathbf{R}_{\leq 0}$ for any $c \in \mathbf{C}^*$. Using (W2) we obtain $w(c\gamma) = w(\gamma)$ for all loops γ and $c \in \mathbf{C}^*$.

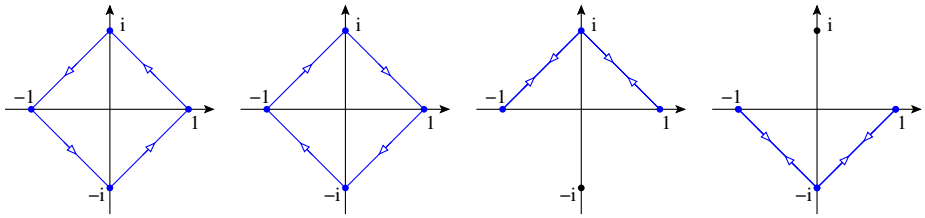


FIGURE 4. The winding number $w(\delta)$ of a diamond-shaped loop δ.

Example 5.12 (diamonds). For $0 < t_0 - \varepsilon < t_0 < t_0 + \varepsilon < 1$ let $\delta\colon [0,1] \to \mathbf{C}$ be the loop that linearly interpolates between $\delta(0) = \delta(t_0 - \varepsilon) = 1$, $\delta(t_0 - \varepsilon/2) = \pm i$, $\delta(t_0) = -1$, $\delta(t_0 + \varepsilon/2) = \pm i$, and $\delta(t_0 + \varepsilon) = \delta(1) = 1$. Then $w(\delta) = \frac{1}{2i}\bigl[\delta(t_0 - \varepsilon/2) - \delta(t_0 + \varepsilon/2)\bigr]$ can be deduced from (W1), (W2), (W3) alone. The proof is left as an exercise.

Theorem 5.13. *Consider an ordered field* $\mathbf{R}$ *and its complex extension* $\mathbf{C} = \mathbf{R}[i]$ *where* $i^2 = -1$. *Let* Ω *be the set of piecewise polynomial loops* $\gamma\colon [0,1] \to \mathbf{C}^*$.

(1) *If some map* $w\colon \Omega \to \mathbb{Z}$ *satisfies* (W1), (W2), (W3), *then* $\mathbf{C}$ *is algebraically closed.*
(2) *If the field* $\mathbf{C} = \mathbf{R}[i]$ *is algebraically closed, then the ordered field* $\mathbf{R}$ *is real closed.*
(3) *If two maps* $w, \tilde{w}\colon \Omega \to \mathbb{Z}$ *satisfy* (W1), (W2), (W3), *then* $w = \tilde{w}$.

Proof. The result (1) has been deduced in §1.3. Regarding (2), every $P \in \mathbf{R}[X]$ factors as $P = c_0(X - z_1)\dots(X - z_n)$ with $z_1, \dots, z_n \in \mathbf{C}$. Since $P(\overline{z_k}) = \overline{P(z_k)} = 0$, each $z_k \in \mathbf{C} \smallsetminus \mathbf{R}$ comes with its conjugate. Pairing these we have $P = c_0(X - x_1)\cdots(X - x_r)Q_1 \cdots Q_s$ where $x_1, \dots, x_r \in \mathbf{R}$ and $Q_j = (X - w_j)(X - \overline{w_j})$ with $w_1, \dots, w_s \in \mathbf{C} \smallsetminus \mathbf{R}$. The minimum of $Q_j = X^2 - 2\operatorname{re}(w_j)X + |w_j|^2$ is $Q_j(\operatorname{re} w_j) = |w_j|^2 - \operatorname{re}(w_j)^2 > 0$, whence $Q_j(x) > 0$ for all $x \in \mathbf{R}$. If $P(a)P(b) < 0$ for some $a < b$ in $\mathbf{R}$, then $a < x_k < b$ for some zero x_k of P.

It remains to prove unicity (3) of the winding number. Let $\gamma\colon [0,1] \to \mathbf{C}^*$ be a piecewise polynomial loop. If γ lies in $\mathbf{C} \smallsetminus \mathbf{R}_{\le 0}$, then we know $w(\gamma) = 0$ from Example 5.11. In general, γ will cross the negative real axis $\mathbf{R}_{<0}$. Since $\operatorname{im}\gamma\colon [0,1] \to \mathbf{R}$ is piecewise polynomial and $\mathbf{R}$ is real closed by (1) and (2), we can use the intermediate value property. We can assume that γ intersects $\mathbf{R}$ only a finite number of times $t_1, \dots, t_k$, where $0 < t_1 < \cdots < t_n < 1$; if not, then $c\gamma$ will do for some $c \in \mathbf{C}^*$. We separate $t_1, \dots, t_k$ in disjoint intervals $I_k = [t_k - \varepsilon, t_k + \varepsilon]$ for some sufficiently small $\varepsilon > 0$. If $\gamma(t_k) > 0$, we set $\delta_k = 1$. If $\gamma(t_k) < 0$, then we define δ_k to be the loop of Example 5.12 with support I_k: since $\operatorname{im}\gamma|I_k$ changes sign at most at t_k, the signs $\delta_k(t_k \pm \varepsilon/2) \in \{\pm i\}$ can be so chosen that $\operatorname{im}\gamma \cdot \operatorname{im}\delta_k \le 0$. Multiplication by δ_k changes γ only on I_k and ensures that $\gamma\delta_k|I_k$ intersects $\mathbf{R}$ only in $\mathbf{R}_{>0}$. We thus obtain $\gamma\delta_1 \cdots \delta_n$ in $\mathbf{C} \smallsetminus \mathbf{R}_{\le 0}$. From Example 5.11, we know $w(\gamma\delta_1 \cdots \delta_n) = 0$, whence $-w(\gamma) = w(\delta_1) + \cdots + w(\delta_n)$ by (W2), and the right hand side is determined by (W1), (W2), (W3) as in Example 5.12. □

6. ALGORITHMIC ASPECTS

The preceding sections §4 and §5 show how to construct the algebraic winding number over a real closed field $\mathbf{R}$. We have used it for proving existence and locating the roots of polynomials over $\mathbf{C} = \mathbf{R}[i]$. This section discusses algorithmic questions. To this end we have to narrow the scope: in order to work with convergence of sequences in $\mathbf{R}$, we additionally assume the ordered field $\mathbf{R}$ to be archimedean, which amounts to $\mathbf{R} \subset \mathbb{R}$.

The algorithm described here is often attributed to Wilf [70] in 1978, but it was already explicitly described by Sturm [56] and Cauchy [9] in the 1830s. It can also be found in Runge's *Encyklopädie* article [36, Kap. IB3, §a6] in 1898. Numerical variants are known as *Weyl's quadtree method* (1924) or *Lehmer's method* (1961); see §7.7. I propose to call it the *Sturm–Cauchy method*, or *Cauchy's algebraic method* if emphasis is needed to differentiate it from Cauchy's analytic method using integration. For a thorough study of

complex polynomials see Marden [35], Henrici [22], and Rahman–Schmeisser [42]; the latter contains extensive historical notes and a guide to the literature.

6.1. **Turing computability.** The theory of ordered or orderable fields, nowadays called *real algebra*, was initiated by Artin and Schreier [3, 4] in the 1920s; a spectacular early success was Artin's solution [1] of Hilbert's 17th problem. Since the 1970s real-algebraic geometry is flourishing anew [7] and, with the advent of computers, algorithmic aspects have gained importance [5]. We shall focus here on basic questions of computability.

Definition 6.1. We say that an ordered field $(\mathbf{R},+,\cdot,<)$ can be implemented on a Turing machine if each element $a \in \mathbf{R}$ can be coded as input/output for such a machine and each of the field operations $(a,b) \mapsto a+b$, $a \mapsto -a$, $(a,b) \mapsto a \cdot b$, $a \mapsto a^{-1}$ as well as the comparisons $a = b$, $a < b$ can be carried out by a uniform algorithm.

Example 6.2. The field $(\mathbb{R},+,\cdot,<)$ of real numbers cannot be implemented on a Turing machine because the set $\mathbb{R}$ is uncountable: it is impossible to code each real number by a finite string over a finite alphabet, as required for input/output. This argument is independent of the chosen representation. If we insist on representing each and every real number, then this fundamental obstacle can only be circumvented by postulating a hypothetical *real number machine* [6], which transcends the traditional setting of Turing machines.

Example 6.3. The subset $\mathbb{R}_{\mathrm{comp}} \subset \mathbb{R}$ of computable real numbers, as defined by Turing [61] in his famous 1936 article, forms a countable, real closed subfield of $\mathbb{R}$. Each computable number a can be represented as input/output for a universal Turing machine by an algorithm that approximates a to any desired precision. This overcomes the obstacle of the previous example by restriction to $\mathbb{R}_{\mathrm{comp}}$. Unfortunately, not all operations of $(\mathbb{R}_{\mathrm{comp}},+,\cdot,<)$ can be implemented. There exists no algorithm that for each computable real number a, given in form of an algorithm, determines whether $a = 0$, or more generally determines the sign of a. (This is an instance of the notorious Entscheidungsproblem.)

Example 6.4. The algebraic closure $\mathbb{Q}^c$ of $\mathbb{Q}$ in $\mathbb{R}$ is a real closed field. Unlike the field of computable real numbers, the much smaller subfield $(\mathbb{Q}^c,+,\cdot,<)$ can be implemented on a Turing machine [46, 45]. More specifically, consider a polynomial $F = c_0Z^n + c_1Z^{n-1} + \cdots + c_n$ whose coefficients $c_k \in \mathbb{C}$ are algebraic over $\mathbb{Q}$. Then $\mathrm{re}(c_k)$ and $\mathrm{im}(c_k)$ are also algebraic, and the field $\mathbf{R} = \mathbb{Q}(\mathrm{re}(c_0),\mathrm{im}(c_0),\ldots,\mathrm{re}(c_n),\mathrm{im}(c_n)) \subset \mathbb{Q}^c$ is a finite extension over $\mathbb{Q}$. It can be generated by one element, which means $\mathbf{R} = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbf{R}$, and such a presentation makes it convenient for implementation.

6.2. **The Sturm–Cauchy root-finding algorithm.** We consider a complex polynomial

$$F = c_0Z^n + c_1Z^{n-1} + \cdots + c_{n-1}Z + c_n \quad \text{in} \quad \mathbb{C}[Z]$$

that we assume to be *Turing implementable*, that is, we require the ordered field

$$\mathbb{Q}(\mathrm{re}(c_0),\mathrm{im}(c_0),\ldots,\mathrm{re}(c_n),\mathrm{im}(c_n)) \subset \mathbb{R}$$

to be implementable in the preceding sense. We begin with the following preparations.

- We divide F by $\gcd(F,F')$ to ensure that all roots of F are simple.
- As in Remark 5.10 we determine $r \in \mathbb{N}$ such that all roots of F lie in $B(r)$.

The following terminology will be convenient: a 0-*cell* is a singleton $\{a\}$ with $a \in \mathbb{C}$; a 1-*cell* is an open line segment, either vertical $\{x_0\} \times]y_0,y_1[$ or horizontal $]x_0,x_1[\times \{y_0\}$ with $x_0 < x_1$ and $y_0 < y_1$ in $\mathbb{R}$; a 2-*cell* is an open rectangle $]x_0,x_1[\times]y_0,y_1[$ in $\mathbb{C}$.

It is immediate to check whether a 0-cell contains a root of F. Sturm's theorem (Corollary 3.16) allows us to count the roots of F in a 1-cell $]a,b[$: for $G = F(a+X(b-a))$ in $\mathbb{C}[X]$ calculate $P = \gcd(\mathrm{re}\,G,\mathrm{im}\,G)$ in $\mathbb{R}[X]$ and count roots of P in $]0,1[$. Cauchy's theorem (Theorem 5.1) allows us to count the roots in a 2-cell. In both cases the crucial subalgorithm is the computation of Sturm chains which we will discuss in §6.4 below.

Building on these methods, the root-finding algorithm successively for $t = 0, 1, 2, 3 \dots$ constructs a list $L_t = \{\Gamma_1, \dots, \Gamma_{n_t}\}$ of disjoint cells, which behaves as follows.

- Each root of F is contained in exactly one cell $\Gamma \in L_t$.
- Each cell $\Gamma \in L_t$ contains at least one root of F.
- Each cell $\Gamma \in L_t$ has diameter $\leq 3r \cdot 2^{-t}$.

The algorithm proceeds as follows: To begin, we initialize $L_0 = \{\Gamma\}$ with the square $\Gamma =]-r, +r[\times]-r, +r[$. Given L_t we construct L_{t+1} by treating each cell in L_t as follows.

(0) Retain all 0-cells unchanged.
(1) Bisect each 1-cell into two 1-cells of equal length as in Figure 5, which also creates one interior 0-cell. Retain each new cell that contains a root of F.
(2) Quadrisect each 2-cell into four 2-cells of equal size as in Figure 5, which creates four interior 1-cells and one 0-cell. Retain each new cell that contains a root of F.

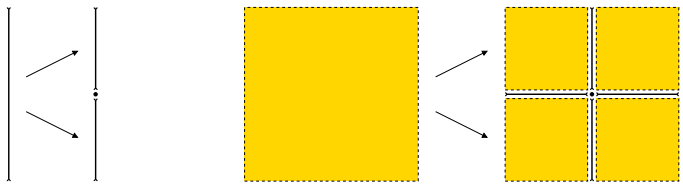


FIGURE 5. Bisecting a 1-cell and quadrisecting a 2-cell

Collecting all retained cells we obtain the new list L_{t+1}. After some initial iterations (§6.4) all roots will lie in disjoint cells $\Gamma_1, \dots, \Gamma_n$, each containing precisely one root. Taking the midpoint $u_k \in \Gamma_k$, this can be seen as n approximate roots $u_1, \dots, u_n$, each with an error bound $\delta_k \leq \sqrt{2}\, r/2^t$ such that each u_k is δ_k-close to a root of F.

6.3. **Crossover to Newton's local method.** For $F \in \mathbb{C}[Z]$, Newton's method consists in iterating the map $\Phi(z) = z - F(z)/F'(z)$ defined on $\{\, z \in \mathbb{C} \mid F'(z) \neq 0 \,\}$. This simple technique is very powerful because of its local behaviour around zeros.

Theorem 6.5. *The fixed points of Newton's map $\Phi(z) = z - F(z)/F'(z)$ are the simple zeros of F, that is, the points $z_0 \in \mathbb{C}$ such that $F(z_0) = 0$ and $F'(z_0) \neq 0$. For each fixed point z_0 there exists $\delta > 0$ such that every initial value $u_0 \in B(z_0, \delta)$ satisfies*

$$|\Phi^t(u_0) - z_0| \leq 2^{1-2^t} \cdot |u_0 - z_0| \qquad \text{for all } t \in \mathbb{N}. \tag{6.1}$$

The convergence to z_0 is thus very fast but requires a good initial approximation $u_0 \approx z_0$; otherwise Newton's iteration may be slow at first or not converge at all. On a practical level this raises two problems: first, how to find approximate zeros, and second, how to determine whether a given approximation is sufficiently good to guarantee fast convergence as in (6.1)? The global root-finding algorithm of §6.2 approximates all roots simultaneously, and the following criterion exploits this information for launching Newton's method:

Theorem 6.6. *Let $F \in \mathbb{C}[Z]$ be a separable polynomial of degree $n \geq 2$. Suppose we have separated the roots $z_1, \dots, z_n$ of F in closed disks $\bar{B}(u_1, \delta_1), \dots, \bar{B}(u_n, \delta_n)$ such that*

$$3n\delta_k \leq |u_k - u_j| \qquad \text{for all } j \neq k. \tag{6.2}$$

Then Newton's iteration satisfies $|\Phi^t(u_k) - z_k| \leq 2^{1-2^t} \cdot \delta_k$ for all $t \in \mathbb{N}$.

Proof. For $F = (Z - z_1) \cdots (Z - z_n)$ we have $F'/F = \sum_{j=1}^n (Z - z_j)^{-1}$. This implies that $\Phi(z) = z - 1/\sum_{j=1}^n (z - z_j)^{-1}$, provided that $F(z) \neq 0$ and $F'(z) \neq 0$, whence

$$\frac{\Phi(z) - z_k}{z - z_k} = 1 - \frac{1}{\sum_{j=1}^n \frac{z - z_k}{z - z_j}} = \frac{\sum_{j \neq k} \frac{z - z_k}{z - z_j}}{1 + \sum_{j \neq k} \frac{z - z_k}{z - z_j}}.$$

By hypothesis, we have approximate roots $u_1,\dots,u_n$ such that $|u_k - z_k| \le \delta_k$. Consider an arbitrary point $z \in \bar{B}(z_k,\delta_k)$, which entails $|z-u_k| \le 2\delta_k$. For all $j \ne k$ we find

$$|z-z_j| \ge |u_k-u_j| - |z-u_k| - |z_j-u_j| \ge |u_k-u_j| - 2\delta_k - \delta_j \ge (3n-3)\delta_k,$$

where the last inequality $(3n-1)\delta_k + \delta_j \le |u_k-u_j|$ is a convex linear combination of (6.2). This ensures that $\left|\sum_{j\ne k}\frac{z-z_k}{z-z_j}\right| \le \sum_{j\ne k}\left|\frac{z-z_k}{z-z_j}\right| \le \frac{|z-z_k|}{3\delta_k} \le \frac{1}{3}$. For $z \ne z_k$ this implies

$$\left|\frac{\Phi(z)-z_k}{z-z_k}\right| \le \frac{\left|\sum_{j\ne k}\frac{z-z_k}{z-z_j}\right|}{1-\left|\sum_{j\ne k}\frac{z-z_k}{z-z_j}\right|} \le \frac{\frac{1}{3\delta_k}|z-z_k|}{1-\frac{1}{3}} = \frac{|z-z_k|}{2\delta_k}.$$

For all $z \in \bar{B}(z_k,\delta_k)$ we conclude that $|\Phi(z)-z_k| \le \frac{1}{2\delta_k}|z-z_k|^2$, whence $|\Phi^t(z)-z_k| \le 2^{1-2^t}\cdot|z-z_k|$ by induction on $t \in \mathbb{N}$. In particular this holds for $z = u_k$. □

As an alternative to the tailor-made criterion of Theorem 6.6, the following theorem of Smale [6, chap. 8] provides a far more general convergence criterion in terms of local data. It applies in particular to polynomials, where it is most easily implemented.

Theorem 6.7 (Smale 1986)**.** *Let $f\colon U \to \mathbb{C}$ be an analytic function on some open set $U \subset \mathbb{C}$. Consider $u_0 \in U$ satisfying $f(u_0) \ne 0$ and $f'(u_0) \ne 0$, so that $\eta = |f(u_0)/f'(u_0)| > 0$ is the initial displacement in Newton's iteration. Suppose further that $B(u_0,2\eta) \subset U$ and the expansion $f(z) = \sum_{k=0}^{\infty} a_k(z-u_0)^k$ satisfies $|a_k| \le (8\eta)^{1-k}|a_1|$ for all $k \ge 2$. Then f has a unique zero z_0 in $B(u_0,2\eta)$ and Newton's iteration converges as in* (6.1)*.*

6.4. **Fast Cauchy index computation.** To complete the picture we briefly consider the bit-complexity of the Sturm–Cauchy algorithm described in §6.2. In order to simplify we will work over the rational numbers. The fundamental problem is, for given $R/S \in \mathbb{Q}(X)$, to compute $\mathrm{Ind}_0^1(\frac{R}{S})$. To this end we wish to construct some chain $S_0,S_1,\dots,S_n \in \mathbb{Q}[X]^*$ starting with $S_1/S_0 = R/S$ and ending with $S_n \in \mathbb{Q}^*$ such that

$$A_kS_{k+1} + B_kS_k + C_kS_{k-1} = 0 \quad \text{with} \quad A_k \in \mathbb{Q}^*,\ B_k \in \mathbb{Q}[X],\ C_k \in \mathbb{Q} \tag{6.3}$$

for all $k = 1,\dots,n-1$. The signs can then easily be arranged such that $A_k > 0$ and $C_k \ge 0$, which ensures that we have a Sturm chain according to Proposition 3.12.

The euclidean algorithm for polynomials of degree $\le n$ takes $O(n^3)$ operations in $\mathbb{Q}$. A suitable divide-and-conquer algorithm [17, chap. 11] reduces this to $\tilde{O}(n^2)$ operations in $\mathbb{Q}$; here the asymptotic complexity $\tilde{O}(n^\alpha)$ neglects logarithmic factors $\log(n)^\beta$. A closer look reveals that we only need the data A_k,B_k,C_k for $k = 1,\dots,n-1$, and these can be calculated with only $\tilde{O}(n)$ operations in $\mathbb{Q}$. Given S_0,S_1 and A_k,B_k,C_k for all k, we can evaluate $S_0(x),S_1(x),\dots,S_n(x)$ at any given $x \in \mathbb{Q}$ using the recursion (6.3) with $O(n)$ operations in $\mathbb{Q}$. Finally, we have to control the size of the coefficients that appear during the computation. According to Lickteig–Roy [32], the result is the following.

Theorem 6.8. *Given polynomials $R,S \in \mathbb{Z}[X]$ of degree $\le n$ and coefficients bounded by 2^a, the Cauchy index $\mathrm{Ind}_0^1(\frac{R}{S})$ can be computed using $\tilde{O}(n^2a)$ bit-operations.* □

This can be applied to locating complex roots. Let $F = c_0Z^n + c_1Z^{n-1} + \cdots + c_n$ be a polynomial with Gaussian integer coefficients $c_0,c_1,\dots,c_n \in \mathbb{Z}[i]$ bounded by $|\mathrm{re}\,c_k| < 2^a$ and $|\mathrm{im}\,c_k| < 2^a$ for all $k = 0,\dots,n$. For simplicity we further assume that $n < 2^a$ and $a \le nb$, where b is the desired bit-precision for approximating the roots.

Corollary 6.9. *Suppose that all roots of F lie in the disk $B(r)$. The Sturm–Cauchy algorithm determines all roots of F to a precision $\sqrt{2}\,r/2^b$ using $\tilde{O}(n^4b^2)$ bit-operations.*

Proof. According to Theorem 6.8, we can compute $\mathrm{Ind}_0^1(\frac{\mathrm{re}\,F}{\mathrm{im}\,F})$ using $\tilde{O}(n^2a)$ bit-operations. We can reparametrize F to calulcate the index along any line segment, and thus along the boundary of any rectangle. In the Sturm–Cauchy algorithm (§6.2), this has to be iterated b times in order to achieve the desired precision, and the coefficients are bounded by 2^{a+nb}.

Since we assume all roots of F to be distinct, they ultimately become separated so that the algorithm has to follow n approximations in parallel. This multiplies the previous bound by a factor nb, so we arrive at $\tilde{O}(n^3 b(a+nb))$ bit-operations. □

To which bit-precision b should we apply this algorithm? Here is an a priori estimate.

Corollary 6.10. *We can switch to Newton's method after at most $b = 3na$ iterations in the Sturm–Cauchy algorithm . This amounts to $\tilde{O}(n^6 a^2)$ bit-operations.*

Proof. Given $F = c_0 Z^n + c_1 Z^{n-1} + \cdots + c_n = c_0(Z - z_1)\cdots(Z - z_n)$ as above with $c_0 \neq 0$, its discriminant $\operatorname{disc}(F) = c_0^{2n-2} \prod_{j<k}(z_j - z_k)^2$ is an integer polynomial in the coefficients $c_0, c_1, \ldots, c_n$. Here $c_0, c_1, \ldots, c_n \in \mathbb{Z}[i]$, so $\operatorname{disc}(F) \in \mathbb{Z}[i]$. Since we assume $z_1, \ldots, z_n$ to be pairwise distinct, we have $\operatorname{disc}(F) \neq 0$, whence $|\operatorname{disc}(F)| \geq 1$. According to Mahler [34], the minimal root distance $\Delta(F) := \min_{j \neq k} |z_j - z_k|$ is bounded below by

$$\Delta(F) > \sqrt{3\,|\operatorname{disc}(F)|\,/n^{n+2}}\;|F|^{1-n},$$

where $|F| = |c_0| + |c_1| + \cdots + |c_n|$. Our hypothesis $|\operatorname{re} c_k| \leq 2^a - 1$ and $|\operatorname{im} c_k| \leq 2^a - 1$ implies $|c_k| \leq \sqrt{2}(2^a - 1)$ for all $k = 0, 1, \ldots, n$. By Proposition 5.8, the zeros $z_1, \ldots, z_n$ lie in the disk $B(r)$ of radius $r = \frac{3}{2} \cdot 2^a$. After b quadrisections of the square $[-r, +r]^2$, we have approximate roots $u_k \in \bar{B}(z_k, \delta_k)$ with $\delta_k \leq \sqrt{2}\, r/2^b$. Assuming $b = 3na$ and $2^a > n$ we find, after some calculation, that $3n\delta_k < \Delta(F)$, so we can apply Theorem 6.6. □

6.5. **What remains to be improved?** Root-finding algorithms of bit-complexity $\tilde{O}(n^3 b)$ are state-of-the-art since the ground-breaking work of Schönhage [50, Thm. 19.2] in the 1980s. The Sturm–Cauchy algorithm is of complexity $\tilde{O}(n^4 b^2)$ and thus comes close, but in its current form remains two orders of magnitude more expensive. Schönhage remarks:

> "It is not clear whether methods based on Sturm sequences can possibly become superior. Lehmer [30, 31] and Wilf [70] both do not solve the extra problems which arise, if there is a zero on the test contour (circle or rectangle) or very close to it." [50, p. 5]

Our algebraic development neatly solves the problem of roots on the boundary. Regarding complexity, we have applied the *divide-and-conquer* paradigm in the arithmetic subalgorithms (§6.4) but not yet in the root-finding method itself. In Schönhage's method this is achieved by approximately factoring F of degree n into two polynomials F_1, F_2 of degrees close to $\frac{n}{2}$. Perhaps an analogous strategy can be put into practice in the algebraic setting; some clever idea and a more detailed investigation are needed here.

Besides complexity there is still another problem: approximating the roots of a polynomial $F \in \mathbb{C}[Z]$ can only be as good as the initial data, and we therefore assume that F is known exactly. This is important because root-finding can be ill-conditioned [71]. Even if exact arithmetic can avoid this problem during the computation, it comes back into focus when the initial data is itself only an approximation. In this situation the real-algebraic approach requires a detailed error analysis, ideally in the setting of interval arithmetic.

6.6. **Formal proofs.** In recent years the theory and practice of *formal proofs* and *computer-verified theorems* have become a full fledged enterprise. Prominent examples include the Jordan Curve Theorem [21] and the Four Colour Theorem [20]. (For an overview of some "top 100" theorems see [69].) Driven by these achievements, the computer-verified proof community envisages much more ambitious goals, such as the classification of finite simple groups. Such gigantic projects make results like the Fundamental Theorem of Algebra look like toy examples, but their formalization is by no means a trivial task. The real-algebraic approach offers certain inherent advantages, mainly its simplicity and algorithmic nature. The latter is an important virtue: Theorem 1.8 is not only an existence statement but provides an algorithm. A formal proof of the theorem can thus serve as a formal correctness proof of an implementation.

7. Historical remarks

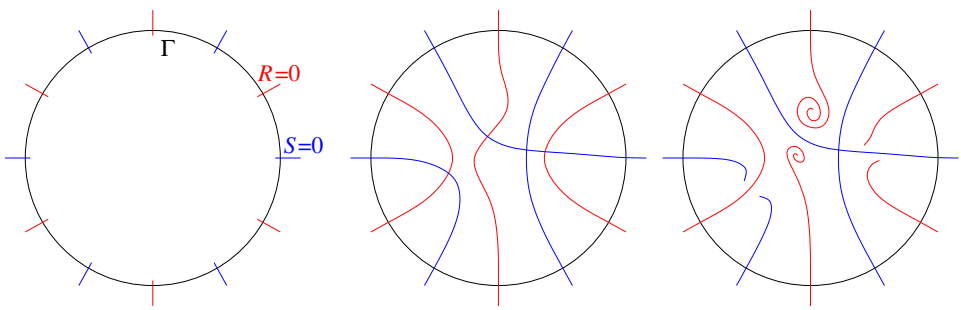
The Fundamental Theorem of Algebra is a crowning achievement in the history of mathematics. In order to place the real-algebraic approach into perspective, this section sketches its historical context. For the history of the Fundamental Theorem of Algebra we refer to Remmert [43], Dieudonné [13, chap. II, §III], and van der Waerden [64, chap. 5]. The history of Sturm's theorem has been examined in great depth by Sinaceur [52].

7.1. **Polynomial equations.** The method to solve quadratic equations was already known to the Babylonians. Not much progress was made until the 16th century, when del Ferro (around 1520) and Tartaglia (1535) discovered a solution for cubic equations by radicals. Cardano's student Ferrari extended this to a solution of quartic equations by radicals. Both formulae were published in Cardano's *Ars Magna* in 1545. Despite considerable efforts during the following centuries, no such formulae could be found for degree 5 and higher. They were finally shown not to exist by Ruffini (1805), Abel (1825), and Galois (1831). This solved one of the outstanding problems of algebra, alas in the negative.

The lack of general formulae provoked the question whether solutions exist at all. The existence of n roots for each real polynomial of degree n was mentioned by Roth (1608) and explicitly conjectured by Girard (1629) and Descartes (1637). They postulated these roots in some extension of $\mathbb{R}$ but did not claim that all roots are contained in the field $\mathbb{C} = \mathbb{R}[i]$ of complex numbers. Leibniz (1702) even speculated that this is in general not possible. The first attempts to prove the Fundamental Theorem of Algebra were made by d'Alembert (1746), Euler (1749), Lagrange (1772), and Laplace (1795).

7.2. **Gauss' geometric proof.** In his doctoral thesis (1799) Gauss criticized the shortcomings of all previous tentatives and presented a geometric argument, which is commonly considered the first satisfactory proof of the Fundamental Theorem of Algebra.

In summary, Gauss considers a polynomial $F = Z^n + c_1 Z^{n-1} + \cdots + c_{n-1} Z + c_n$ and upon substitution of $Z = X + iY$ obtains $F = R + iS$ with $R, S \in \mathbb{R}[X, Y]$. The zeros of F are precisely the intersections of the two curves $R = 0$ and $S = 0$ in the plane. Consider a disk Γ centered in 0 with sufficiently large radius. Near the circle $\partial\Gamma$ these curves resemble the zero sets of the real and imaginary parts of Z^n. The latter are $2n$ straight lines passing through the origin. Thus $\partial\Gamma$ intersects the curves $R = 0$ and $S = 0$ in two sets of $2n$ points placed in an alternating fashion around the circle. (See Figure 6.)



(A) The curves $R = 0$ and $S = 0$ outside of a sufficiently large disk Γ.

(B) Joining the ends inside of Γ forces the curves to intersect.

(C) Such pathological cases have to be ruled out, of course.

FIGURE 6. Gauss' geometric argument for the existence of zeros

Prolonging these curves into the interior of Γ, Gauss concludes that the curves $R = 0$ and $S = 0$ must intersect somewhere inside the disk Γ. The conclusion relies on certain (intuitively plausible) assumptions, which Gauss clearly states but does not prove:

> "It seems to have been proved with sufficient certainty that an algebraic curve can neither suddenly break off anywhere (as it happens, for example, with the transcendental curve whose equation is $y = 1/\log x$) nor lose itself, so to say, in some point after infinitely many coils (like the logarithmic spiral). As far as I know, nobody has raised any doubts about this. Should someone demand it, however, then I will undertake to give a proof that is not subject to any doubt, on some other occasion."[3]

This amounts to a version of the Jordan Curve Theorem [19]. By modern standards Gauss' geometric argument is thus incomplete. The unproven assertions are indeed correct, and were rigorously worked out by Ostrowski [38, 39] more than a century later. Gauss' ingenious insight was to apply geometric arguments to an algebraic problem. In terms of winding numbers he shows $w(F|\partial\Gamma) = n$ by an implicit homotopy $F \sim Z^n$. Our development shows how to complete the proof using real-algebraic techniques.

Gauss gave two further proofs in 1816; the second proof is algebraic (§7.6.2), whereas the third proof uses integration (§7.6.3) and foreshadows Cauchy's integral formula for the winding number. Gauss' fourth proof in 1849 is essentially an improved version of his first proof [64, chap. 5]. When Gauss published it for his doctorate jubilee, the works of Sturm (1835) and Cauchy (1837) had been known for several years. In particular Sturm's theorem had immediately risen to international acclaim, and was certainly familiar to Gauss. Gauss could have taken up his first proof and completed it by arguments similar to the ones presented here. Completing Gauss' geometric argument, Ostrowski [39] mentions the relationship with the Cauchy index but builds his proof on topological arguments.

7.3. **Cauchy, Sturm, Liouville.** Argand in 1814 and Cauchy in 1820 proved the Fundamental Theorem of Algebra by assuming the existence of a global minimum z_0 of $|F|$ and a local argument to show that $F(z_0) = 0$; see §7.6.1. While the local analysis is rigorous, the existence of a minimum requires some compactness argument, which was yet to be developed; see Remmert [43, §1.8].

Sturm's theorem for counting real roots was announced in 1829 [54] and published in 1835 [55]. It was immediately assimilated by Cauchy in his residue calculus [8], based on contour integration, which was published in 1831 during his exile in Turin. In 1837 he published a more detailed exposition [9] with analytic-geometric proofs, and explicitly recognizes the relation to Sturm's theorem and algebraic computations.

In the intervening years, Sturm and Liouville [58, 56] had elaborated their algebraic version of Cauchy's theorem, which they published in 1836. (Loria [33] and Sinaceur [52, I.VI] examine the interaction between Sturm, Liouville, and Cauchy in detail.) As opposed to Cauchy, their arguments are based on what they call the "first principles of algebra". In the terminology of their time this means the theory of complex numbers, including trigonometric coordinates $z = r(\cos\theta + i\sin\theta)$ and de Moivre's formula, but excluding integration. They use the intermediate value property of real polynomials as well as tacit compactness arguments.

7.4. **Sturm's algebraic vision.** Sturm, in his article [56] continuing his work with Liouville [58], presents arguments which closely parallel our real-algebraic proof: the argument principle (Prop. 1, p. 294), multiplicativity (Prop. 2, p. 295), counting roots of a split polynomial within a given region (Prop. 3, p. 297), the winding number in the absence of zeros (Prop. 4, p. 297), and finally Cauchy's theorem (p. 299). One crucial step is to show that

[3] "Satis bene certe demonstratum esse videtur, curvam algebraicam neque alicubi subito abrumpi posse (uti e.g. evenit in curva transscendente, cuius aequatio $y = 1/\log x$), neque post spiras infinitas in aliquo puncto se quasi perdere (ut spiralis logarithmica), quantumque scio nemo dubium contra hanc rem movit. Attamen si quis postulat, demonstrationem nullis dubiis obnoxiam alia occasione tradere suscipiam." [18, Bd. 3, p. 27] My translation is adapted from Prof. Ernest Fandreyer's (Fitchburg State College Library, Manuscript Collections), cf. van der Waerden [64, p. 96].

$w(F|\partial\Gamma) = 0$ when F does not vanish in Γ. This is solved by subdivision and a tacit compactness argument (pp. 298–299); our compactness proof of Lemma 5.3 makes this explicit and completes his argument. Sturm then deduces the Fundamental Theorem of Algebra (pp. 300–302) and expounds on the practical computation of the Cauchy index $w(F|\partial\Gamma)$ using Sturm chains as in the real case (pp. 303–308).

Sturm's exposition strives for algebraic simplicity, but his proofs are still based on geometric and analytic arguments. It is only on the final pages that Sturm employs his algebraic method for computing the Cauchy index. This mixed state of affairs has been passed on ever since, even though it is far less satisfactory than Sturm's purely algebraic treatment of the real case [55]. Our proof shows that Sturm's algebraic vision of the complex case can be salvaged and his arguments can be put on firm real-algebraic ground.

We note that Sturm and Liouville [58] explicitly exclude zeros on the boundary:

> "We formally exclude, however, the case where for some point of the curve we have simultaneously $P = 0$ and $Q = 0$: this special case does not enjoy any regular property and cannot give rise to any theorem."[4]

This seems overly pessimistic in view of our Theorem 1.5 above. In his continuation [56], Sturm formulates the same problem more cautiously:

> "It is under this hypothesis that we have proven the theorem of Mr. Cauchy; the necessary modifications in the case where roots were on the contour would require a long and meticulous discussion, which we wanted to avoid by neglecting this special case."[5]

It seems safe to say that our detailed discussion is just as "long and meticulous" as the usual development of Sturm's theorem. Modulo these details, the cited works of Gauss, Cauchy, and Sturm contain the essential ideas for the real-algebraic approach.

7.5. **Further development in the 19th century.** Sturm's theorem was a decisive step in the development of algebra as an autonomous field; see Sinaceur [52]. Algebraic generalizations to higher dimensions were conjectured by Sylvester in 1840 and developped by Hermite from 1852 onwards. In 1869 Kronecker [27] turned from algebra to integration in order to construct his higher-dimensional index (also called Kronecker characteristic). Subsequent work was likewise built on analytic or topological methods over $\mathbb{R}$: one gains in generality by extending the index to smooth or continuous functions, but one loses algebraic computability and the elementary setting of real closed fields.

7.5.1. *Applications.* Generalizing Example 3.3, the problem of *stability of motion* led Routh [44] in 1878 and Hurwitz [23] in 1895 to count, for a given polynomial, the number of complex roots having negative real part. With the celebrated Routh–Hurwitz theorem, the algebraic Cauchy index has transited from algebra to application, where it survives to the present day.

7.5.2. *Encyclopaedic surveys.* In the 1898 *Encyklopädie der mathematischen Wissenschaften* [36], Netto's survey on the Fundamental Theorem of Algebra (Kap. IB1, §a7) mentions Cauchy's algebraic approach only briefly (p. 236), whereas Runge's article on approximation of complex roots (Kap. IB3, §a6) discusses the Sturm–Cauchy method in detail (pp. 418–422). In the 1907 *Encyclopédie des Sciences Mathématiques* [37], Netto and le

[4] "Toutefois nous excluons formellement le cas particulier où, pour quelque point de la courbe *ABC*, on aurait à la fois $P = 0$, $Q = 0$: ce cas particulier ne jouit d'aucune propriété régulière et ne peut donner lieu à aucun théorème." [58, p. 288]

[5] "C'est en admettant cette hypothèse que nous avons démontré le théorème de M. Cauchy ; les modifications qu'il faudrait y apporter dans le cas où il aurait des racines sur le contour même *ABC*, exigeraient une discussion longue et minutieuse que nous avons voulu éviter en faisant abstraction de ce cas particulier." [56, p. 306]

Vavasseur give an overview of nearly 100 published proofs (tome I, vol. 2, chap. I-9, §80–88), including Cauchy's argument principle (§87). The work of Sturm–Liouville [58, 56] is listed but the algebraic approach via Sturm chains is not mentioned.

7.5.3. *Nineteenth-century textbooks.* While Sturm's theorem made its way to modern algebra textbooks, the algebraic approach to the complex case seems to have been lost on the way. I will illustrate this by two prominent and perhaps representative textbooks.

In his 1866 textbook *Cours d'algèbre supérieure*, starting with the third edition, Serret [51, pp. 117–131] presents the proof of the Fundamental Theorem of Algebra following Cauchy and Sturm–Liouville, with only minor modifications.

In his 1898 textbook *Lehrbuch der Algebra*, Weber [65] devotes over 100 pages to real-algebraic equations, where he presents Sturm's theorem in great detail (§91–106). Calling upon Kronecker's index theory (§100–102), he sketches how to count complex roots (§103–104). Quite surprisingly, he uses only $\operatorname{Ind}\left(\frac{P'}{P}\right)$ and Corollary 3.16 where the general case $\operatorname{Ind}\left(\frac{R}{S}\right)$ and Theorem 3.15 would have been optimal. Here Cauchy's algebraic method [9], apparently unknown to Weber, had gone much further concerning explicit formulae and concrete computations.

7.6. **Survey of proof strategies.** Since the time of Gauss numerous proofs of the Fundamental Theorem of Algebra have been developed. We refer to Remmert [43] for a concise overview and to Fine–Rosenberger [15] for a textbook presentation. As mentioned in §1.1, the proof strategies can be grouped into three families:

7.6.1. *Analysis.* Early proofs in this family are based on the existence of a global minimum z_0 of $|F|$ and some local argument from complex analysis showing that $F(z_0) = 0$ (d'Alembert 1746, Argand 1814, Cauchy 1820). See Remmert [43, §2] for a presentation in its historical context, or Rudin [47, chap. 8] in the context of a modern analysis course. The most succinct formulation follows from Liouville's theorem for entire functions.

These existence proofs are in general not constructive and do not indicate the location of zeros. For a discussion of constructive refinements see [43, §2.5].

7.6.2. *Algebra.* Proofs in this family use the fundamental theorem of symmetric polynomials in order to reduce the problem from real polynomials of degree $2^k m$ with m odd to degree $2^{k-1}m'$ with m' odd (Euler 1749, Lagrange 1772, Laplace 1795, Gauss 1816; see [43, appendix]). The argument can also be reformulated using Galois theory; see Cohn [11, Thm. 8.8.7], Jacobson [25, Thm. 5.2], or Lang [29, §VI.2, Ex. 5]. The induction is based, for $k = 0$, on real polynomials of odd degree, where the existence of at least one real root is guaranteed by the intermediate value theorem.

This algebraic proof works over every real closed field, as elaborated by Artin and Schreier [3] in 1926. It is constructive but ill-suited to actual computations.

7.6.3. *Topology.* Proofs in this family use some form of the winding number $w(\gamma)$ of closed paths $\gamma\colon [0,1] \to \mathbb{C}^*$ (Gauss 1799/1816, Cauchy 1831/37, Sturm–Liouville 1836). The winding number appears in various guises; see Remark 1.3. In each case the difficulty is a rigorous construction and to establish its characteristic properties: normalization, multiplicativity and homotopy invariance, as stated in Theorem 1.2.

Our proof belongs to this last family. Unlike previous proofs, however, we do not base the winding number on analytic or topological arguments, but on real algebra.

7.7. **Constructive and algorithmic aspects.** Sturm's method is eminently practical, by the standards of 19th century mathematics as for modern-day implementations. As early as 1840 Sylvester [59] wrote "Through the well-known ingenuity and proferred help of a distinguished friend, I trust to be able to get a machine made for working Sturm's theorem (...)". It seems, however, that such a machine was never built. Calculating machines had been devised by Pascal, Leibniz, and Babbage; the latter was Lucasian Professor of

Mathematics when Sylvester studied at Cambridge in the 1830s. The idea of computing machinery seems to have been popular among mid-19th century mathematicians. For example, in a small note of 1846, Ullherr [63] remarks that the argument principle "provides a method to find the roots of higher-degree equations by means of a mechanical apparatus."[6]

For separating and approximating roots, the state of the art at the end of the 19th century was surveyed in Runge's *Encyklopädie* article [36, Kap. IB3, §a], and in particular the Sturm–Cauchy method is discussed in detail (pp. 416–422).

In 1924 Weyl [67] reemphasized that the analytic winding number can be used to find and approximate the roots of F. In this vein Weyl formulated his constructive proof of the Fundamental Theorem of Algebra, which indeed translates to an algorithm: a careful numerical approximation can be used to calculate the integer $w(F|\partial\Gamma)$; see Henrici [22, §6.11]. While Weyl's motivation may have been philosophical, it is the practical aspect that has proven most successful. Variants of Weyl's algorithm are used in modern computer implementations for finding approximate roots, and are among the asymptotically fastest known algorithms. The question of algorithmic complexity was pursued by Schönhage [50] and others since the 1980s. See Pan [41] for an overview.

The fact that Sturm's and Cauchy's theorems can be combined to count complex roots seems not to be as widely known as it should be. It is surprising that the original publications in the 1830s did not have a lasting effect (§7.5) and likewise Runge's presentation in the 1898 *Encyklopädie* fell into oblivion. In the 1969 Proceedings [12] on constructive aspects of the Fundamental Theorem of Algebra, the Sturm–Cauchy method is not mentioned. It reappears in 1978 in a small note by Wilf [70], and is briefly mentioned in Schönhage's report [49, p. 5]. Most often the computer algebra literature credits Weyl for the analytic-numeric method, and Lehmer or Wilf for the algebraic-numeric method, but not Cauchy or Sturm. Their real-algebraic method for complex root location seems largely ignored.

Acknowledgments

Many colleagues had the kindness to comment on successive versions of this article and to share their expertise on different facets of this venerable topic. It is my heartfelt pleasure to thank Roland Bacher, Theo de Jong, Christoph Lamm, Bernard Parisse, Cody Roux, Marie-Françoise Roy, Siegfried Rump, Francis Sergeraert, and Duco van Straten. Numerous suggestions of referees and editors greatly helped to improve the exposition.

References

[1] E. Artin, Über die Zerlegung definiter Funktionen in Quadrate, *Abh. Math. Sem. Univ. Hamburg* **5** (1926) 100–115, Collected Papers [2], pp. 273–288.

[2] ———, *Collected Papers*, Edited by S. Lang and J. T. Tate, Springer-Verlag, New York, 1982, Reprint of the 1965 original.

[3] E. Artin and O. Schreier, Algebraische Konstruktion reeller Körper, *Abh. Math. Sem. Univ. Hamburg* **5** (1926) 85–99, Collected Papers [2], pp. 258–272.

[4] ———, Eine Kennzeichnung der reell abgeschlossenen Körper, *Abh. Math. Sem. Univ. Hamburg* **5** (1927) 225–231, Collected Papers [2], pp. 289–295.

[5] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in Real Algebraic Geometry*, second ed., Springer-Verlag, Berlin, 2006, Available at `perso.univ-rennes1.fr/marie-francoise.roy`.

[6] L. Blum, F. Cucker, M. Shub, and S. Smale, *Complexity and Real Computation*, Springer-Verlag, New York, 1998.

[7] J. Bochnak, M. Coste, and M.-F. Roy, *Real Algebraic Geometry*, Springer-Verlag, Berlin, 1998.

[8] A.-L. Cauchy, Sur les rapports qui existent entre le calcul des résidus et le calcul des limites, *Bulletin des Sciences de Férussac* **16** (1831) 116–128, Œuvres [10], Série 2, tome 2, pp. 169–183.

[9] ———, Calcul des indices des fonctions, *Journal de l'École Polytechnique* **15** (1837) 176–229, Œuvres [10], Série 2, tome 1, pp. 416–466.

[6] "Die bei dem ersten Beweise gebrauchte Betrachtungsart giebt ein Mittel an die Hand, die Wurzeln der höheren Gleichungen mittels eines Apparates mechanisch zu finden." [63, p. 234]

[10] ———, *Œuvres complètes*, Gauthier-Villars, Paris, 1882–1974, Available at `mathdoc.emath.fr/OEUVRES/`.
[11] P. M. Cohn, *Basic Algebra*, Springer-Verlag, London, 2003.
[12] B. Dejon and P. Henrici, eds., *Constructive Aspects of the Fundamental Theorem of Algebra*, John Wiley & Sons, London, 1969.
[13] J. Dieudonné, *Abrégé d'Histoire des Mathématiques. 1700–1900.*, Hermann, Paris, 1978.
[14] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, and R. Remmert, *Numbers*, Graduate Texts in Mathematics, vol. 123, Springer-Verlag, New York, 1991.
[15] B. Fine and G. Rosenberger, *The Fundamental Theorem of Algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997.
[16] A. T. Fuller, ed., *Stability of Motion*, Taylor & Francis, London, 1975, A collection of early scientific publications by E. J. Routh, W. K. Clifford, C. Sturm and M. Bôcher.
[17] J. v. z. Gathen and J. Gerhard, *Modern Computer Algebra*, second ed., Cambridge University Press, Cambridge, 2003.
[18] C. F. Gauß, *Werke. Band I–XII*, Georg Olms Verlag, Hildesheim, 1973, Reprint of the 1863–1929 original, available at `resolver.sub.uni-goettingen.de/purl?PPN235993352`.
[19] S. M. Gersten and J. R. Stallings, On Gauss's first proof of the fundamental theorem of algebra, *Proc. Amer. Math. Soc.* **103** (1988) 331–332.
[20] G. Gonthier, The four colour theorem, *Notices Amer. Math. Soc.* **55** (2008) 1382–1393, Available at `www.ams.org/notices/200811`.
[21] T. C. Hales, The Jordan curve theorem, formally and informally, *Amer. Math. Monthly* **114** (2007) 882–894.
[22] P. Henrici, *Applied and Computational Complex Analysis*, vol. 1, John Wiley & Sons, New York, 1974.
[23] A. Hurwitz, Ueber die Bedingungen, unter welchen eine Gleichung nur Wurzeln mit negativen reellen Theilen besitzt, *Math. Ann.* **46** (1895) 273–284, Math. Werke [24], Band 2, pp. 533–545. Reprinted in [16].
[24] ———, *Mathematische Werke*, Birkhäuser, Basel, 1962–1963.
[25] N. Jacobson, *Basic Algebra I-II*, second ed., W. H. Freeman, New York, 1985, 1989.
[26] E. Kasner, The present problems of geometry, *Bull. Amer. Math. Soc.* **11** (1905) 283–314.
[27] L. Kronecker, Ueber Systeme von Functionen mehrer Variabeln, *Monatsberichte Akademie Berlin* (1869) 159–193, 688–698, Werke [28], Band I, pp. 175–226.
[28] ———, *Werke*, Chelsea Publishing Co., New York, 1968, Reprint of the 1895–1930 original.
[29] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
[30] D. H. Lehmer, A machine method for solving polynomial equations, *J. Assoc. Comput. Mach.* **8** (1961) 151–162.
[31] ———, Search procedures for polynomial equation solving, in *Constructive Aspects of the Fundamental Theorem of Algebra* [12], John Wiley & Sons, 1969, 193–208.
[32] T. Lickteig and M.-F. Roy, Sylvester-Habicht sequences and fast Cauchy index computation, *J. Symbolic Comput.* **31** (2001) 315–341.
[33] G. Loria, Charles Sturm et son œuvre mathématique, *Enseign. Math.* **37** (1938) 249–274.
[34] K. Mahler, An inequality for the discriminant of a polynomial, *Michigan Math. J.* **11** (1964) 257–262.
[35] M. Marden, *Geometry of Polynomials*, second ed., Mathematical Surveys, vol. 3, American Mathematical Society, Providence, RI, 1966.
[36] W. F. Meyer, ed., *Encyklopädie der mathematischen Wissenschaften*, B. G. Teubner, Leipzig, 1898.
[37] J. Molk, ed., *Encyclopédie des Sciences Mathématiques*, Gauthier-Villars, Paris, 1907.
[38] A. Ostrowski, *Über den ersten und vierten Gaußschen Beweis des Fundamentalsatzes der Algebra*, vol. X.2, ch. 3 in [18], Georg Olms Verlag, 1920, Collected Papers [40], vol. 1, pp. 538–553.
[39] ———, Über Nullstellen stetiger Funktionen zweier Variablen, *J. Reine Angew. Math.* **170** (1933) 83–94, Collected Papers [40], vol. 3, pp. 269–280.
[40] ———, *Collected Mathematical Papers*, Birkhäuser, Basel, 1983.
[41] V. Y. Pan, Solving polynomials with computers, *American Scientist* **86** (1998) 62–69.
[42] Q. I. Rahman and G. Schmeisser, *Analytic Theory of Polynomials*, London Mathematical Society Monographs. New Series, vol. 26, Oxford University Press, Oxford, 2002.
[43] R. Remmert, *The fundamental theorem of algebra*, ch. 4 in [14], Springer-Verlag, New York, 1991.
[44] E. J. Routh, *A Treatise on the Stability of a Given State of Motion*, Macmillan, London, 1878, Reprinted in [16], pp. 19–138.
[45] M.-F. Roy, Basic algorithms in real algebraic geometry and their complexity: from Sturm's theorem to the existential theory of reals, in *Lectures in Real Geometry (Madrid, 1994)*, de Gruyter Exp. Math., vol. 23, de Gruyter, Berlin, 1996, 1–67.
[46] M.-F. Roy and A. Szpirglas, Complexity of computation on real algebraic numbers, *J. Symbolic Comput.* **10** (1990) 39–51.
[47] W. Rudin, *Principles of Mathematical Analysis*, third ed., McGraw-Hill Book Co., New York, 1976.
[48] S. M. Rump, Ten methods to bound multiple roots of polynomials, *J. Comput. Appl. Math.* **156** (2003) 403–432.

[49] A. Schönhage, The fundamental theorem of algebra in terms of computational complexity, Preliminary report, Math. Inst. Univ. Tübingen, Tübingen, Germany, 1982, 49 pages, available at `www.informatik.uni-bonn.de/~schoe/fdthmrep.ps.gz`.

[50] ———, Equation solving in terms of computational complexity, in *Proc. Int. Congress of Math., Berkeley, 1986*, vol. 1, American Mathematical Society, 1987, 131–153.

[51] J. A. Serret, *Cours d'algèbre supérieure*, third ed., Gauthier-Villars, Paris, 1866, Available at `www.archive.org/details/coursdalgbresup06serrgoog`.

[52] H. Sinaceur, *Corps et Modèles*, Librairie Philosophique J. Vrin, Paris, 1991, Translated as [53].

[53] ———, *Fields and Models*, Birkhäuser, Basel, 2008.

[54] C.-F. Sturm, Mémoire sur la résolution des équations numériques, *Bulletin des Sciences de Férussac* **11** (1829) 419–422, Collected Works [57], pp. 323–326.

[55] ———, Mémoire sur la résolution des équations numériques, *Académie Royale des Sciences de l'Institut de France* **6** (1835) 271–318, Collected Works [57], pp. 345–390.

[56] ———, Autres démonstrations du même théorème, *J. Math. Pures Appl.* **1** (1836) 290–308, Collected Works [57], pp. 486–504, English translation in [16], pp. 189–207.

[57] ———, *Collected Works*, Edited by J.-C. Pont, Birkhäuser, Basel, 2009, Some of the articles are also available at `www-mathdoc.ujf-grenoble.fr/pole-bnf/Sturm.html`.

[58] C.-F. Sturm and J. Liouville, Démonstration d'un théorème de M. Cauchy, relatif aux racines imaginaires des équations, *J. Math. Pures Appl.* **1** (1836) 278–289, Collected Works [57], pp. 474–485.

[59] J. J. Sylvester, A method of determining by mere inspection the derivatives from two equations of any degree, *Philosophical Magazine* **16** (1840) 132–135, Collected Papers [60], vol. I, pp. 54–57.

[60] ———, *Collected Mathematical Papers*, Cambridge University Press, Cambridge, 1904–1912.

[61] A. M. Turing, On computable numbers, with an application to the Entscheidungsproblem, *Proc. Lond. Math. Soc., II. Ser.* **42** (1936) 230–265, Collected Works [62], vol. IV, pp. 18–56.

[62] ———, *Collected Works*, North-Holland Publishing Co., Amsterdam, 1992.

[63] J. C. Ullherr, Zwei Beweise für die Existenz der Wurzeln der höhern algebraischen Gleichungen, *J. Reine Angew. Math.* **31** (1846) 231–234.

[64] B. L. van der Waerden, *A History of Algebra*, Springer-Verlag, Berlin, 1985.

[65] H. Weber, *Lehrbuch der Algebra*, second ed., vol. 1, F. Vieweg & Sohn, Braunschweig, 1898, Reprinted by AMS Chelsea Publishing, New York, 2002.

[66] H. Weyl, Über die neue Grundlagenkrise der Mathematik. (Vorträge gehalten im mathematischen Kolloquium Zürich), *Math. Z.* **10** (1921) 39–79, Ges. Abh. [68], Band II, pp. 143–180.

[67] ———, Randbemerkungen zu Hauptproblemen der Mathematik, II. Fundamentalsatz der Algebra und Grundlagen der Mathematik, *Math. Z.* **20** (1924) 131–150, Ges. Abh. [68], Band II, pp. 433–453.

[68] ———, *Gesammelte Abhandlungen*, Springer-Verlag, Berlin, 1968.

[69] F. Wiedijk, Formalizing 100 theorems, `www.cs.ru.nl/~freek/100`, accessed 25/03/2012.

[70] H. S. Wilf, A global bisection algorithm for computing the zeros of polynomials in the complex plane, *J. Assoc. Comput. Mach.* **25** (1978) 415–420.

[71] J. H. Wilkinson, The evaluation of the zeros of ill-conditioned polynomials, *Numer. Math.* **1** (1959) 150–180.

INSTITUT FÜR GEOMETRIE UND TOPOLOGIE, UNIVERSITÄT STUTTGART, GERMANY
E-mail address: `Michael.Eisermann@mathematik.uni-stuttgart.de`
URL: `www.igt.uni-stuttgart.de/eiserm`