An Elementary Proof of Fundamental Theorem of Algebra over Rationals

Liang Zhang* Xiaohua(Michael) Xuan†

Abstract

We, with the aid of AI, give an elementary proof of the Fundamental Theorem of Algebra over Rationals, i.e., for any nonconstant polynomial f with rational complex number coefficients and every positive rational number ε, there exists a rational complex number z such that $Q(f(z)) < \varepsilon^2$. The proof is constructive and relies only on finite rational arithmetic, without using real numbers, infinite sets, or related concepts.

hexagon:2611.00320v1

Contents

1 Introduction 1

2 Notation and conventions 2

3 Rational quadrance and variation estimates 3

4 A winding number for finite closed vertex lists 4

5 The winding number of the power cycle 6

6 The existence of suitable radius and mesh resolution 10

7 The existence of a good grid vertex 12

8 Proof of main theorem 13

9 Complete approximate factorization over Rationals 13

10 Complete approximate real factorization over Rationals 16

1 Introduction

The Fundamental Theorem of Algebra is a central result in mathematics. In its classical form, it states that every nonconstant polynomial f with complex number coefficients has a complex number z such that $f(z) = 0$.

Many mathematicians contributed to the historical development of the theorem, including d'Alembert, Euler, Lagrange, Laplace, Argand, Gauss, and Cauchy [4, 8]. Of particular relevance here, Gauss attempted to prove the theorem by tracking the winding of a polynomial image around the origin, though a topological step remained to be justified [5, 1]. Cauchy later gave

*Corresponding author: liang.zhang@unidt.com
†Email: michael.xuan@unidt.com

the winding number an integral formulation, supplying a rigorous analytic framework for the argument [3, 8].

Kuhn [6] gave a constructive combinatorial proof in 1974, using vertex labelling and a combinatorial lemma on triangulated regions of the complex plane. His proof is an important precedent for the present use of finite triangulations, and the augument in this paper is close in spirit to this approach.

Smale gave a short proof of the Fundamental Theorem of Algebra by using the inverse function theorem in his study of the complexity of algorithms for solving equations [9, 10]. He and Shub subsequently showed that the homotopy method combined with Newton's iteration yields an efficient algorithm with a provably good complexity bound for approximating a zero of a polynomial [11, 12, 2].

While all mentioned proofs of the Fundamental Theorem of Algebra depend on the real numbers and infinite processes, Wildberger called for a proof grounded strictly in finite rational arithmetic and formulated two alternative versions of the theorem in his online YouTube lectures [15] in 2017. This paper directly answers his call by providing the requested proof.

Using the quadrance terminology of rational trigonometry [14], write $Q(a+ib) \equiv a^2+b^2$. We prove the following statement:

Theorem (Main theorem)**.** *For any nonconstant polynomial f with rational complex number coefficients and any rational number $\varepsilon > 0$, there exists a rational complex number z such that*

$$Q\big(f(z)\big) < \varepsilon^2.$$

The proof uses the winding number of finite rational closed vertex lists, rational variation bounds, and a finite triangulation to obtain a contradiction if no grid point satisfies the conclusion. It involves only finite objects, rational number computation and comparisons.

2 Notation and conventions

Throughout, the symbol $\equiv$ introduces a definition, while $=$ denotes an asserted equality. We write

$$t \,\dot{\in}\, T$$

to mean that t is of type T. For example, $t \,\dot{\in}\, \mathbb{Q}$ and $t \,\dot{\in}\, \mathbb{Z}$ mean, respectively, that t is a rational number and that t is an integer. When no confusion can arise, we also use the ordinary notation $t \in T$ for this purpose.

A *rational complex number* is a finite datum consisting of two rational numbers a and b, written as $a+ib$. We write $z \,\dot{\in}\, K$ when z is such a datum, and $z \,\dot{\in}\, K^\times$ when, in addition, $z \neq 0$.

A polynomial with rational complex coefficients is specified by a finite coefficient list

$$(a_0, a_1, \ldots, a_n), \qquad a_j \,\dot{\in}\, K,$$

and is written as

$$f(X) = \sum_{j=0}^{n} a_j X^j.$$

The notation $f \,\dot{\in}\, K[X]$ asserts only that f is given by such finite data. Thus K, $K^\times$, and $K[X]$ are used solely as type labels.

We use the convention $u^0 \equiv 1$, including when $u = 0$; empty sums have value 0, and empty products have value 1.

We identify $a+ib$ with the point $[a,b]$. For points $A_1 = [x_1, y_1]$ and $A_2 = [x_2, y_2]$, define their *quadrance* by

$$Q(A_1, A_2) \equiv (x_2 - x_1)^2 + (y_2 - y_1)^2.$$

For $u = a + ib \in K$, we use the abbreviation

$$Q(u) \equiv Q([0,0],[a,b]) = a^2 + b^2.$$

Thus $Q(u)$ denotes the quadrance of u from the origin.

For a positive rational number R, let $\mathsf{Sq}(R)$ denote the square with vertices

$$-R - iR, \qquad R - iR, \qquad R + iR, \qquad -R + iR.$$

A point $z = a + ib$ lies in $\mathsf{Sq}(R)$ precisely when $|a| \le R$ and $|b| \le R$, and lies on its boundary $\partial\mathsf{Sq}(R)$ precisely when, in addition, $|a| = R$ or $|b| = R$. Here $|\cdot|$ denotes the usual absolute value on $\mathbb{Q}$.

For any three-point list (p_1, p_2, p_3), we say that z is a *nonnegative rational affine combination* of the list precisely when

$$z = \alpha p_1 + \beta p_2 + \gamma p_3, \qquad \alpha, \beta, \gamma \in \mathbb{Q}, \qquad \alpha, \beta, \gamma \ge 0, \qquad \alpha + \beta + \gamma = 1.$$

When p_1, p_2, p_3 are distinct and non-collinear, this condition means that z lies on the triangle $p_1p_2p_3$. Such a point is interior to the triangle precisely when $\alpha, \beta, \gamma > 0$, and it lies on a side precisely when $\alpha\beta\gamma = 0$. When the three-point list is degenerate, we retain the affine-combination language and do not call it a triangle.

3 Rational quadrance and variation estimates

Definition 3.1 (Auxiliary size)**.** For $u = a + ib \in K$, define

$$\sigma(u) \equiv |a| + |b|.$$

$\sigma(u)$ is called the *size* of u. Note that $Q(u) = u \cdot \overline{u}$, where $\overline{a + ib} \equiv a - ib$.

Lemma 3.2 (Basic inequalities)**.** *For all $u, v \in K$:*

$$Q(u) \le \sigma(u)^2, \qquad \sigma(u+v) \le \sigma(u) + \sigma(v), \qquad \sigma(u \cdot v) \le \sigma(u)\sigma(v). \tag{2.1}$$

Moreover σ is nonnegative, $\sigma(0) = 0$, $\sigma(1) = 1$, and $\sigma(u^n) \le \sigma(u)^n$ for all $n \ge 0$.

Proof. Set $u \equiv a + ib$, $v \equiv c + id$. Then

$$\sigma(u+v) = |a+c| + |b+d| \le |a| + |c| + |b| + |d| = \sigma(u) + \sigma(v).$$

$$\sigma(uv) = |ac - bd| + |ad + bc| \le |a||c| + |b||d| + |a||d| + |b||c| = (|a| + |b|)(|c| + |d|) = \sigma(u)\sigma(v).$$

Finally, $Q(u) = a^2 + b^2 \le (|a| + |b|)^2 = \sigma(u)^2$. The facts $\sigma(0) = 0$, $\sigma(1) = 1$, $\sigma \ge 0$ are immediate; $\sigma(u^n) \le \sigma(u)^n$ follows from submultiplicativity by induction. □

Lemma 3.3 (Power variation)**.** *Let $w, z \in K$, let $j \ge 1$ be an integer, and let $B \in \mathbb{Q}$ with $\sigma(w), \sigma(z) \le B$. Then*

$$\sigma(w^j - z^j) \le j \cdot B^{j-1} \cdot \sigma(w - z). \tag{2.2}$$

Proof. For $j \ge 1$, we note that

$$w^j - z^j = (w - z) \cdot \sum_{r=0}^{j-1} w^{j-1-r} z^r.$$

The result follows from the triangle inequality and submultiplicativity of σ, and also the fact that $\sigma(w), \sigma(z) \le B$. □

Lemma 3.4 (Polynomial variation)**.** *Let* $f(X) = \sum_{j=0}^{n} a_j X^j \in K[X]$ *and let* $B \in \mathbb{Q}$ *with* $\sigma(w), \sigma(z) \le B$*. Then*

$$\sigma\big(f(w) - f(z)\big) \le \sigma(w - z) \cdot \sum_{j=1}^{n} j\, \sigma(a_j)\, B^{j-1}. \tag{2.3}$$

Proof. By the power-variation estimate (2.2) and the submultiplicative inequality in (2.1),

$$\sigma(a_j w^j - a_j z^j) \le \sigma(a_j)\, jB^{j-1}\sigma(w - z).$$

Summing this inequality over $j = 1, \ldots, n$ and applying the triangle inequality in (2.1) gives (2.3). □

Lemma 3.5 (Affine exclusion)**.** *Let* $a, b, c \in K$ *and* $0 < \varepsilon \in \mathbb{Q}$*. If* $\sigma(a - b) < \varepsilon$*,* $\sigma(a - c) < \varepsilon$*, and* $\varepsilon^2 \le Q(a)$*, then the origin is not a nonnegative rational affine combination of* (a, b, c)*.*

Proof. If the origin were such an affine combination, then $a = \beta(a - b) + \gamma(a - c)$ with $\beta, \gamma \ge 0$, $\beta + \gamma \le 1$, so $\sigma(a) \le \beta\sigma(a - b) + \gamma\sigma(a - c) < \varepsilon$, giving $Q(a) \le \sigma(a)^2 < \varepsilon^2$, contradicting $\varepsilon^2 \le Q(a)$. □

4 A winding number for finite closed vertex lists

4.1 Definitions and the half-open convention

Throughout this section, a *closed vertex list* is an oriented list $P \equiv (p_0, p_1, \ldots, p_s)$ with $p_j \in K$ and $p_s = p_0$. The closed list (a, b, c, a) is the *three-cycle* determined by (a, b, c); its entries need not be distinct or non-collinear.

Definition 4.1 (Determinant)**.** For $u = x + iy$, $v = x' + iy'$, define

$$\Delta(u,\, v) \equiv xy' - yx'.$$

This is twice the signed area of the oriented three-point list $(0, u, v)$. The sign decisions below depend on this rational expression.

Definition 4.2 (Signed crossing, half-open convention)**.** For a directed edge $p \to q$, we define the *signed crossing contribution* $\chi(p, q) \in \mathbb{Z}$ by the half-open rule

$$\chi(p,q) \equiv \begin{cases} 1, & \mathrm{Im}(p) \le 0 < \mathrm{Im}(q) \text{ and } \Delta(p,\, q) > 0, \\ -1, & \mathrm{Im}(q) \le 0 < \mathrm{Im}(p) \text{ and } \Delta(p,\, q) < 0, \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

Here $\mathrm{Im}(p)$ denotes the imaginary part of p.

Remark 4.3 (Interpretation of (1))*.* Let's consider the case

$$\mathrm{Im}(p) \le 0 < \mathrm{Im}(q) \text{ and } \Delta(p,\, q) > 0,$$

Write $p = x + iy$, $q = x' + iy'$ with $\mathrm{Im}(p) = y \le 0$ and $\mathrm{Im}(q) = y' > 0$, and let the intersection of pq and $\mathrm{Im}(z) = 0$ be $r = x_r, x_r \in \mathbb{Q}$. Then $\Delta(p,\, q) = x_r\,(y' - y)$. Since $y' - y > 0$, $\Delta(p,\, q) > 0$ iff $\mathrm{Re}(r) > 0$.

Definition 4.4 (Winding number)**.** For a closed vertex list $P = (p_0, \ldots, p_s)$, its *winding number* is defined as follows:

$$\mathrm{W}(P) \equiv \sum_{i=0}^{s-1} \chi(p_i, p_{i+1}) \in \mathbb{Z}.$$

It is computable by finitely many rational number computations and comparisons.

Remark 4.5 (Positive scale invariance). Let $a \in \mathbb{Q}$ be positive and write $aP \equiv (ap_0, ap_1, \ldots, ap_s)$. Then

$$\mathrm{W}(aP) = \mathrm{W}(P).$$

Indeed, for any edge $p_i \to p_{i+1}$,

$$\mathrm{Im}(ap_i) = a\,\mathrm{Im}(p_i), \qquad \Delta(ap_i,\, ap_{i+1}) = a^2\Delta(p_i,\, p_{i+1})\,.$$

Since $a > 0$, all inequalities and signs in Definition 4.2 are unchanged. Hence $\chi(ap_i, ap_{i+1}) = \chi(p_i, p_{i+1})$ for any i, and summing over the edges gives $\mathrm{W}(aP) = \mathrm{W}(P)$ by Definition 4.4.

Theorem 4.6 (Structural properties of W)**.** *The winding number has the following properties, all of which can be proved by finite rational computations.*

(1) Reversal. $\chi(q,p) = -\chi(p,q)$*; hence reversing all edges of a closed vertex list negates its winding number.*

(2) Three-cycle vanishing. *If the origin is not a nonnegative rational affine combination of* (a,b,c)*, where* $a,b,c \in K$*, then* $\mathrm{W}(a,b,c,a) = 0$.

(3) Additivity under common triangulation. *Let* $P \equiv (p_0,\ldots,p_n)$ *and* $Q \equiv (q_0,\ldots,q_m)$ *be closed vertex lists. Inserting repeated vertices (equivalently, inserting zero-length edges) does not change winding number, so we may assume* $m = n$*. For each* $i = 0,\ldots,n-1$*, suppose the origin is not a nonnegative rational affine combination of either* (p_i, p_{i+1}, q_{i+1}) *or* (p_i, q_{i+1}, q_i)*. Then*

$$\mathrm{W}(P) = \mathrm{W}(Q).$$

(4) Base value. *For rational* $R > 0$*, the counterclockwise boundary of the square* $\mathsf{Sq}(R)$ *has winding number* 1*:*

$$\mathrm{W}(-R - iR,\, R - iR,\, R + iR,\, -R + iR,\, -R - iR) = 1.$$

Proof. (1) Exchanging p and q swaps the two branches of (1) and negates $\Delta(p,\,q)$, giving $\chi(q,p) = -\chi(p,q)$.

(2) Assume that the origin is not a nonnegative rational affine combination of (a,b,c).

Step 1: encode the half-open convention. For each vertex p, write $y_p \equiv \mathrm{Im}(p), x_p \equiv \mathrm{Re}(p)$ and define

$$h(p) \equiv \begin{cases} 1, & y_p > 0, \\ 0, & y_p \le 0. \end{cases}$$

For any directed edge $p \to q$ of (a,b,c,a), if $h(p) = h(q)$, then $\chi(p,q) = 0$ by (1). If $h(p) \neq h(q)$, then $y_q - y_p \neq 0$, so we may define the rational number

$$r_{pq} \equiv \frac{\Delta(p,\,q)}{y_q - y_p} = \frac{y_q p - y_p q}{y_q - y_p}.$$

Moreover,

$$r_{pq} = (1-t)p + tq, \qquad t \equiv \frac{-y_p}{y_q - y_p} \in \mathbb{Q}, \qquad 0 \le t \le 1.$$

Thus r_{pq} is a nonnegative rational affine combination of (a,b,c). Since

$$\Delta(p,\,q) = (y_q - y_p) r_{pq}$$

One can easily check

$$\chi(p,q) = \big(h(q) - h(p)\big)\mathbf{1}_{\{r_{pq}>0\}} \qquad \text{when } h(p) \neq h(q),$$

where $\mathbf{1}_{\{r_{pq}>0\}}$ is 1 if $r_{pq} > 0$ and 0 otherwise.

Step 2: the intersection values have a common strict sign. Each of the values r_{pq} just defined is nonzero, since otherwise it would express the origin as a nonnegative rational affine combination of (a, b, c). Nor can two such values have opposite signs: if $r_{pq} > 0 > r_{p'q'}$, then

$$0 = \frac{-r_{p'q'}}{r_{pq} - r_{p'q'}}\, r_{pq} + \frac{r_{pq}}{r_{pq} - r_{p'q'}}\, r_{p'q'}.$$

The two coefficients are positive rational numbers whose sum is 1. Substituting the nonnegative rational affine expressions for r_{pq} and $r_{p'q'}$ would therefore express the origin as a nonnegative rational affine combination of (a, b, c), again contradicting the hypothesis. Hence all the values r_{pq} for edges with $h(p) \neq h(q)$ have the same strict sign.

Step 3: conclude by two cases.

Case 1. There exists an edge $p \to q$ with $h(p) \neq h(q)$ and $r_{pq} > 0$.

By Step 2, every edge with distinct h-values has a positive intersection value. Hence Step 1 gives

$$\chi(p, q) = h(q) - h(p)$$

for every such edge. The same identity holds when $h(p) = h(q)$, since both sides are zero. Consequently,

$$\begin{aligned} \mathrm{W}(a, b, c, a) &= \chi(a, b) + \chi(b, c) + \chi(c, a) \\ &= h(b) - h(a) + h(c) - h(b) + h(a) - h(c) \\ &= 0. \end{aligned}$$

Case 2. There is no edge with $h(p) \neq h(q)$ and $r_{pq} > 0$.

Consider any edge $p \to q$. If $h(p) = h(q)$, Step 1 gives $\chi(p, q) = 0$. Otherwise, $r_{pq} \neq 0$ by Step 2, and therefore $r_{pq} < 0$; Step 1 again gives $\chi(p, q) = 0$. Thus

$$\mathrm{W}(a, b, c, a) = \chi(a, b) + \chi(b, c) + \chi(c, a) = 0.$$

Both cases allow coincident vertices and collinear three-point lists.

(3) For each i, apply the three-cycle vanishing property established in part (2) above to (p_i, p_{i+1}, q_{i+1}) and (p_i, q_{i+1}, q_i), obtaining

$$\mathrm{W}(p_i, p_{i+1}, q_{i+1}, p_i) = 0, \qquad \mathrm{W}(p_i, q_{i+1}, q_i, p_i) = 0.$$

Summing these $2n$ equalities, each interior edge appears twice with opposite orientations and therefore cancels. Only the boundary edges of P and Q remain, yielding $\mathrm{W}(P) = \mathrm{W}(Q)$.

(4) Direct computation: among the four directed edges, only the right side $R - iR \to R + iR$ has an upward crossing point r with $\mathrm{Im}(r) = 0$ and $\mathrm{Re}(r) > 0$, and $\Delta(R - iR,\, R + iR) = 2R^2 > 0$, contributing $+1$; the other three edges contribute 0. □

5 The winding number of the power cycle

Let R be a positive rational number, and let $M \geq 2$ be an even integer. Set $h \equiv 2R/M$ and subdivide the counterclockwise boundary of $\mathsf{Sq}(R)$ into $4M$ segments, each of quadrance h^2. Let $z_0 \equiv R$, let $z_1, \ldots, z_{4M-1}$ be the remaining successive vertices in counterclockwise order, and set $z_{4M} \equiv z_0$.

Definition 5.1. (Power cycle): The *power cycle* of degree n for $(z_0, z_1, \ldots, z_{4M})$ is $P_n \equiv (z_0^n, z_1^n, \ldots, z_{4M}^n)$.

For a given power cycle $P_n \equiv (z_0^n, z_1^n, \ldots, z_{4M}^n)$, let $I_n \equiv \mathrm{W}(P_n)$ denote the *winding number* of P_n and let $E_n \equiv n\,(2R)^{n-1}\,h$.

Lemma 5.2 (Parametric bounds). *For any vertex z_j $(0 \le j \le 4M)$:*

$$Q(z_j) \ge R^2, \qquad \sigma(z_j) \le 2R, \qquad \sigma(z_{j+1} - z_j) = h \quad (0 \le j < 4M).$$

Consequently, for each $0 \le j < 4M$,

$$\sigma\big(z_{j+1}^n - z_j^n\big) \le E_n.$$

Proof. Since each z_j lies on $\partial\mathsf{Sq}(R)$, $Q(z_j) \ge R^2$ and $\sigma(z_j) \le 2R$. The difference $z_{j+1} - z_j$ is one of $\pm h$, $\pm hi$ so $\sigma(z_{j+1} - z_j) = h$. The last bound comes from Lemma 3.3 with $B = 2R$: $\sigma(z_{j+1}^n - z_j^n) \le n(2R)^{n-1}h = E_n$. □

Lemma 5.3 (Base winding number). $I_1 = \mathrm{W}(z_0, \ldots, z_{4M}) = 1$.

Proof. The edges on bottom, top, and left sides contribute 0. On the right side, exactly two edges have the common endpoint R, which satisfies $\mathrm{Im}(R) = 0$ and $\mathrm{Re}(R) = R > 0$. According to the half-open convention, the edge leaving R upward contributes $+1$, the other one contributes 0. Every other segment contributes 0. Hence the total is 1.

□

Theorem 5.4 (Additivity of the winding number). *Let $r, s \ge 1$. Assume the Fineness Condition $4E_{r+s}^2 < R^{2(r+s)}$. Then*

$$I_{r+s} = I_r + I_s. \tag{4.1}$$

Proof. On the parameter triangle $0 \le v \le u \le 1$, consider the map $H(u, v) \equiv \Gamma_R(u)^r \Gamma_R(v)^s$. Here Γ_R is the counterclockwise rational piecewise-affine parametrization of $\partial\mathsf{Sq}(R)$ starting at R, given explicitly by

$$\Gamma_R(t) \equiv \begin{cases} R + 8Rt\,i, & 0 \le t \le \frac{1}{8}, \\ (2R - 8Rt) + Ri, & \frac{1}{8} < t \le \frac{3}{8}, \\ -R + (4R - 8Rt)i, & \frac{3}{8} < t \le \frac{5}{8}, \\ (-6R + 8Rt) - Ri, & \frac{5}{8} < t \le \frac{7}{8}, \\ R + (8Rt - 8R)i, & \frac{7}{8} < t \le 1. \end{cases}$$

The first and last branches together in the above definition of Γ_R parametrize the right side of the square; the other three branches parametrize the top, left, and bottom sides, respectively.

Set $N \equiv 4M$ and consider the rational parameter grid

$$\mathcal{D}_N \equiv \left\{ \left(\frac{i}{N}, \frac{j}{N} \right) : 0 \le j \le i \le N \right\}$$

in the triangle $0 \le v \le u \le 1$. Triangulate it by the oriented three-point lists

$$T_{i,j}^+ \equiv \left(\left(\frac{i}{N}, \frac{j}{N} \right), \left(\frac{i+1}{N}, \frac{j}{N} \right), \left(\frac{i+1}{N}, \frac{j+1}{N} \right) \right), \quad 0 \le j \le i < N,$$
$$T_{i,j}^- \equiv \left(\left(\frac{i}{N}, \frac{j}{N} \right), \left(\frac{i+1}{N}, \frac{j+1}{N} \right), \left(\frac{i}{N}, \frac{j+1}{N} \right) \right), \quad 0 \le j < i < N.$$

For any such elementary triangle $T = (A, B, C)$, its *image three-point list* is $(H(A), H(B), H(C))$, and its *image three-cycle* is $(H(A), H(B), H(C), H(A))$.

Under H, the side $v = 0$ maps to $z_0^s \cdot P_r$, the side $u = 1$ maps to $z_0^r \cdot P_s$, and the diagonal $u = v$ maps to P_{r+s}. For every $(u, v) \in \mathcal{D}_N$, both $\Gamma_R(u)$ and $\Gamma_R(v)$ lie on $\partial\mathsf{Sq}(R)$. Hence

$$\sigma(\Gamma_R(u)), \sigma(\Gamma_R(v)) \le 2R, \qquad Q(\Gamma_R(u)), Q(\Gamma_R(v)) \ge R^2,$$

and therefore, by the multiplicativity of quadrance,

$$Q(H(u,v)) = Q(\Gamma_R(u))^r Q(\Gamma_R(v))^s \geq R^{2(r+s)}. \tag{4.2}$$

Let (u,v) and (u',v') be any two vertices of one elementary triangle, and write

$$x \equiv \Gamma_R(u), \qquad x' \equiv \Gamma_R(u'), \qquad y \equiv \Gamma_R(v), \qquad y' \equiv \Gamma_R(v').$$

The two parameter coordinates differ by at most one grid step, so the corresponding boundary vertices are either equal or consecutive. Thus

$$\sigma(x' - x) \leq h, \qquad \sigma(y' - y) \leq h.$$

Applying Lemma 3.4 to the monomials X^r and X^s gives

$$\sigma(x'^r - x^r) \leq r(2R)^{r-1}h, \qquad \sigma(y'^s - y^s) \leq s(2R)^{s-1}h.$$

Using

$$H(u',v') - H(u,v) = (x'^r - x^r)y'^s + x^r(y'^s - y^s)$$

together with the triangle and submultiplicative inequalities in Lemma 3.2, we obtain

$$\begin{aligned}\sigma\big(H(u',v') - H(u,v)\big) &\leq r(2R)^{r-1}h(2R)^s + (2R)^r s(2R)^{s-1}h \\ &= (r+s)(2R)^{r+s-1}h = E_{r+s}.\end{aligned}$$

Now let (a,b,c) be the image three-point list of any elementary triangle. Applying the preceding estimate to its first vertex and each of the other two gives

$$\sigma(a-b) \leq E_{r+s} < 2E_{r+s}, \qquad \sigma(a-c) \leq E_{r+s} < 2E_{r+s}.$$

By the Fineness Condition and (4.2),

$$(2E_{r+s})^2 < R^{2(r+s)} \leq Q(a).$$

Lemma 3.5, applied with $\varepsilon \equiv 2E_{r+s}$, therefore shows that the origin is not a nonnegative rational affine combination of (a,b,c). Hence every corresponding image three-cycle has winding number 0 by Theorem 4.6(2). Summing over all image three-cycles and cancelling the contribution of interior edges gives

$$0 = \mathrm{W}(z_0^s \cdot P_r) + \mathrm{W}(z_0^r \cdot P_s) - \mathrm{W}(P_{r+s}) = I_r + I_s - I_{r+s}.$$

The last equality follows from $z_0 = R > 0$ and Remark 4.5. □

Theorem 5.5 (Winding number of the power cycle)**.** *If $4E_n^2 < R^{2n}$, then $I_n = n$.*

Proof. Suppose that $4E_n^2 < R^{2n}$. We first verify the Fineness Condition for every $1 \leq r < n$. Since $h = 2R/M$, for each integer $1 \leq k \leq n$ we have

$$E_k = k(2R)^{k-1}h = \frac{k(2R)^k}{M},$$

and hence

$$q_k \equiv \frac{4E_k^2}{R^{2k}} = \frac{4k^2\,4^k}{M^2}.$$

Moreover, for $1 \leq k < n$,

$$\frac{q_{k+1}}{q_k} = 4\left(\frac{k+1}{k}\right)^2 > 1,$$

so the finite list $q_1, \dots, q_n$ is strictly increasing. Hence $q_n < 1$ implies $q_r < q_n < 1$, or equivalently $4E_r^2 < R^{2r}$, for every $1 \le r < n$.

We now prove the result by induction on n. For $n = 1$, Lemma 5.3 gives $I_1 = 1$. For $n \ge 2$, the induction hypothesis and the preceding Fineness Condition give $I_{n-1} = n - 1$. Apply Theorem 5.4 with $r = n - 1$ and $s = 1$. Its required Fineness Condition is the assumed condition for n, and consequently

$$I_n = I_{n-1} + I_1 = n,$$

where Lemma 5.3 was used in the last equality. □

Remark 5.6 (On the choice of the starting vertex z_0). In Definition 5.1 we fixed $z_0 = R$ (the rightmost point on the boundary of the square) for concreteness. This choice is immaterial: the winding number $\mathrm{W}(P)$ of any closed vertex list is invariant under cyclic permutation of the list. Indeed, the sum in $\mathrm{W}(P) = \sum_i \chi(p_i, p_{i+1})$ is taken over all oriented edges exactly once; a cyclic shift merely reorders the summands, so the total is unchanged. Therefore, any other boundary vertex z_k $(0 \le k < 4M)$ could serve as the starting point, and the resulting power cycle would have the same winding number I_n. The half-open convention ensures consistent treatment of the edge that wraps around the chosen starting point, so no special handling is required.

Remark 5.7 (Multiplier comparison on refined boundary lists). Let $(\zeta_0, \dots, \zeta_N)$ be a *refinement* of $(z_0, \dots, z_{4M})$, obtained by inserting finitely many rational points along its boundary segments, in order, while retaining all original vertices. Thus $\zeta_0 = \zeta_N = R$. For an integer $n \ge 1$, write

$$P_n^* \equiv (\zeta_0^n, \dots, \zeta_N^n).$$

Keep h and $E_k = k(2R)^{k-1}h$ from the original subdivision. The refined points still satisfy

$$\sigma(\zeta_j) \le 2R, \qquad Q(\zeta_j) \ge R^2, \qquad \sigma(\zeta_{j+1} - \zeta_j) \le h \quad (0 \le j < N).$$

In particular, the refined list need not be uniformly spaced.

Fix two consecutive vertices u, v of this refined boundary list and assume $4E_{n+1}^2 < R^{2n+2}$. For $0 \le j \le N$, set

$$A_j \equiv u\zeta_j^n, \qquad B_j \equiv v\zeta_j^n.$$

For each $0 \le j < N$, split the four-point list $(A_j, B_j, B_{j+1}, A_{j+1})$ along A_jB_{j+1} into

$$(A_j, B_j, B_{j+1}), \qquad (A_j, B_{j+1}, A_{j+1}).$$

By Lemmas 3.3 and 3.2, the changes in the multiplier and in the powered boundary vertex are bounded respectively by $h(2R)^n$ and $2RE_n = n(2R)^n h$. Their sum is

$$E_{n+1} = (n+1)(2R)^n h.$$

Thus

$$\sigma(U - A_j) \le E_{n+1} < 2E_{n+1} \qquad \text{for } U \in \{B_j, B_{j+1}, A_{j+1}\}.$$

Since

$$Q(A_j) = Q(u)Q(\zeta_j)^n \ge R^{2(n+1)} > (2E_{n+1})^2,$$

Lemma 3.5, with $\varepsilon \equiv 2E_{n+1}$, excludes the origin from both three-point lists. Their three-cycles therefore have winding number 0 by Theorem 4.6(2). Summing over j cancels all diagonal and interior edges, leaving

$$0 = \mathrm{W}(vP_n^*) - \mathrm{W}(uP_n^*),$$

so $\mathrm{W}(uP_n^*) = \mathrm{W}(vP_n^*)$.

Theorem 5.8 (Conditional scale invariance)**.** *Let $a \in K^\times$, let $R > 0$ be rational, let $M \geq 2$ be an even integer, and let $n \geq 1$ be an integer. Assume the fineness condition $4E_{n+1}^2 < R^{2n+2}$. Then*

$$\mathrm{W}\big(a \cdot P_n\big) = I_n.$$

Proof. The assumed Fineness Condition also gives $4E_n^2 < R^{2n}$, by the calculation in the proof of Theorem 5.5.

Step 1: refinement preserves winding number. Insert a rational point ξ between consecutive boundary vertices u, v. The power-variation estimate gives

$$\sigma(\xi^n - u^n),\ \sigma(v^n - u^n) \leq E_n, \qquad Q(u^n) \geq R^{2n} > 4E_n^2.$$

Lemma 3.5, with precision $2E_n$, therefore excludes the origin from the nonnegative rational affine combinations of (u^n, ξ^n, v^n). For any $b \in K^\times$, the same holds for $(bu^n, b\xi^n, bv^n)$, since an affine expression for zero could be divided by b. Theorem 4.6(1)–(2) gives

$$\chi(bu^n, b\xi^n) + \chi(b\xi^n, bv^n) = \chi(bu^n, bv^n).$$

Thus repeating the old vertex bu^n and then replacing the repeated entry by $b\xi^n$ preserves winding number. Every subsequent insertion satisfies the same bounds, so any finite refinement obeys

$$\mathrm{W}(bP_n^*) = \mathrm{W}(bP_n) \qquad (b \in K^\times).$$

Step 2: compare multipliers on the refined list. Write $a = x + iy$ with $x, y \in \mathbb{Q}$, and set

$$t \equiv \frac{R}{\max\{|x|, |y|\}}, \qquad \widetilde{a} \equiv ta.$$

Then t is a positive rational and $\widetilde{a} \in \partial\mathsf{Sq}(R)$. Insert $\widetilde{a}$ into the original boundary list if necessary, and denote the resulting refined power cycle by P_n^*. Remark 5.7, applied successively along the refined boundary from R to $\widetilde{a}$, gives

$$\mathrm{W}(\widetilde{a}P_n^*) = \mathrm{W}(RP_n^*).$$

Together with positive scale invariance (Remark 4.5) and Step 1, this yields

$$\begin{aligned}\mathrm{W}(aP_n) &= \mathrm{W}(\widetilde{a}P_n) = \mathrm{W}(\widetilde{a}P_n^*)\\ &= \mathrm{W}(RP_n^*) = \mathrm{W}(P_n^*) = \mathrm{W}(P_n) = I_n.\end{aligned}$$

□

6 The existence of suitable radius and mesh resolution

Throughout, $f(X) = \sum_{j=0}^n a_j X^j \in K[X]$ with $n \geq 1$, $a_n \neq 0$, and a rational $\varepsilon > 0$. Let $A_j \equiv \sigma(a_j)$ and

$$C \equiv \sum_{j=0}^{n-1} 2^j A_j, \qquad G \equiv CR^{n-1}, \qquad m \equiv Q(a_n)\, R^{2n}, \qquad L \equiv \sum_{j=1}^{n} j\, A_j (2R)^{j-1}.$$

Lemma 6.1 (Choice of R)**.** *There is an integer $R \geq 1$ such that*

$$Q(a_n)\, R^2 > 2\, C^2. \tag{5.1}$$

For any such R one also has $2G^2 < m$.

Proof. Set $\nu \equiv Q(a_n) > 0$ and choose

$$R \equiv 1 + \left\lceil \frac{2C^2}{\nu} \right\rceil .$$

The ceiling of a rational number is computed by integer division of its numerator by its positive denominator, with a remainder check. Thus R is an explicitly determined integer with $R \geq 1$ and $R^2 \geq R > 2C^2/\nu$, proving (5.1). Multiplying (5.1) by the positive factor R^{2n-2} gives $2G^2 < m$. □

Lemma 6.2 (Choice of M)**.** *Let $R \geq 1$ be an integer satisfying (5.1), whose existence is guaranteed by Lemma 6.1. Then there exists an explicitly determined even integer $M \geq 2$ such that, writing $h \equiv 2R/M$ and $D \equiv A_n E_n$, all three strict rational number inequalities hold:*

$$2hL < \varepsilon, \qquad (D+G)^2 < m, \qquad 4E_{n+1}^2 < R^{2n+2}. \tag{5.2}$$

The last inequality also implies $4E_n^2 < R^{2n}$.

Proof. For $k = n, n+1$, write

$$e_k \equiv 2Rk(2R)^{k-1},$$

and set $d_0 \equiv A_n e_n$. Thus $E_k = e_k/M$ for $k = n, n+1$, and $D = d_0/M$. By Lemma 6.1, $\delta \equiv m - G^2 > 0$. Since

$$\frac{4E_{n+1}^2}{R^{2n+2}} = \frac{4(n+1)^2\, 4^{n+1}}{M^2},$$

the degree-$(n+1)$ Fineness Condition is equivalent to $M > 2(n+1)2^{n+1}$. Define

$$B_M \equiv \max\left\{1,\ \frac{4RL}{\varepsilon},\ \frac{4Gd_0}{\delta}, \frac{2d_0^2}{\delta},\ 2(n+1)2^{n+1}\right\},$$
$$M \equiv 2\left(1 + \left\lfloor \frac{B_M}{2} \right\rfloor\right).$$

These choices require only finitely many rational computations and comparisons and an integer division. The integer M is even, $M \geq 2$, and $M > B_M$. In particular, $M^2 \geq M > B_M \geq 2d_0^2/\delta$, so all four inequalities

$$\frac{4RL}{M} < \varepsilon, \qquad \frac{2Gd_0}{M} < \frac{\delta}{2}, \qquad \frac{d_0^2}{M^2} < \frac{\delta}{2}, \qquad \frac{4e_{n+1}^2}{M^2} < R^{2n+2}$$

hold. The first is exactly $2hL < \varepsilon$, the fourth gives $4E_{n+1}^2 < R^{2n+2}$, and

$$(D+G)^2 = G^2 + \frac{2Gd_0}{M} + \frac{d_0^2}{M^2} < G^2 + \frac{\delta}{2} + \frac{\delta}{2} = m.$$

Finally, the proof of Theorem 5.5 shows that

$$q_k \equiv \frac{4E_k^2}{R^{2k}}$$

is strictly increasing in k. Hence $q_{n+1} < 1$ implies $q_n < 1$, which is precisely $4E_n^2 < R^{2n}$. □

7 The existence of a good grid vertex

Choose R, M, h as in §6; in particular, $4E_{n+1}^2 < R^{2n+2}$. Consider the finite rational grid

$$\mathcal{G} \equiv \{-R + ih + i(-R + jh) : 0 \le i, j \le M\},$$

listed lexicographically (the i-coordinate outer, j inner); it has exactly $(M+1)^2$ points. As in §5, let $\partial\mathcal{G}$ denote the counterclockwise closed list of boundary grid vertices, whose successive vertices subdivide $\partial\mathsf{Sq}(R)$ into $4M$ segments, each of quadrance h^2. Each of the M^2 cells is split by its positive diagonal into two triangles.

Theorem 7.1 (Existence of a good grid vertex)**.** *There exists $z \in \mathcal{G}$ with*

$$Q\big(f(z)\big) < \varepsilon^2.$$

Proof. Suppose, for contradiction, that

$$Q(f(z)) \ge \varepsilon^2 \qquad \text{for all } z \in \mathcal{G}. \tag{6.1}$$

(a) Image three-point lists exclude 0. For two vertices z, w of one grid triangle, $\sigma(w - z) \le 2h$; since all grid points lie in $\mathcal{G}$, each grid vertex has real and imaginary parts bounded by R in absolute value, so for vertices z, w we have $|\Re(z)|, |\Im(z)|, |\Re(w)|, |\Im(w)| \le R$. Lemma 3.4 and (5.2) give, for vertices z, w of the same triangle,

$$\sigma\big(f(w) - f(z)\big) \le \sigma(w - z) \sum_{j=1}^{n} j\, A_j (2R)^{j-1} = \sigma(w - z)\, L \le 2hL < \varepsilon. \tag{6.2}$$

Let $p_0 \equiv f(z_0), p_1 \equiv f(z_1), p_2 \equiv f(z_2)$ be the three image values of a grid triangle. If the origin were a nonnegative rational affine combination of (p_0, p_1, p_2), there would exist nonnegative rationals $\theta_0, \theta_1, \theta_2$ with $\theta_0 + \theta_1 + \theta_2 = 1$ and $0 = \theta_0 p_0 + \theta_1 p_1 + \theta_2 p_2$. Then

$$p_0 = \theta_1(p_0 - p_1) + \theta_2(p_0 - p_2),$$

so by (6.2) and the affine-exclusion argument (Lemma 3.5) $\sigma(p_0) < \varepsilon$, hence $Q(p_0) \le \sigma(p_0)^2 < \varepsilon^2$, contradicting (6.1). Thus no image three-point list admits such an affine combination of the origin, and by Theorem 4.6(2) each image three-cycle has winding number 0: $\mathrm{W}(f(z_0), f(z_1), f(z_2), f(z_0)) = 0$.

(b) Edge cancellation. Summing the winding numbers of all $2M^2$ image three-cycles: every interior edge of the triangulation occurs twice, in opposite orientations, and cancels by Theorem 4.6(1). What remains is the image of the outer boundary:

$$\mathrm{W}\big(f(\partial\mathcal{G})\big) = \mathrm{W}\big(f((z_j)_{j=0,1,2,\ldots,4M})\big) = 0. \tag{6.3}$$

(c) The boundary winding number is the leading-term winding number. Write $f(z) = l(z) + g(z)$ with $l(z) \equiv a_n z^n$ and $g(z) \equiv \sum_{j<n} a_j z^j$. At a boundary grid vertex, $\sigma(z) \le 2R$, $Q(z) \ge R^2$, and $R \ge 1$; hence

$$\sigma(g(z)) \le \sum_{j<n} A_j (2R)^j \le C R^{n-1} = G, \qquad Q(l(z)) \ge Q(a_n)\, R^{2n} = m. \tag{6.4}$$

For consecutive boundary vertices z, z' (with $\sigma(z' - z) = h$), the power estimate gives

$$\sigma\big(l(z') - l(z)\big) \le D. \tag{6.5}$$

Join the leading-term closed vertex list $(l(z_j))_j$ to the full-value closed vertex list $(l(z_j)+g(z_j))_j$ by the closed four-vertex list $(l(z_j),\ f(z_j),\ f(z_{j+1}),\ l(z_{j+1}),\ l(z_j))$, and split this list along a diagonal into the two closed three-cycles

$$\big(l(z_j),\ f(z_j),\ f(z_{j+1}),\ l(z_j)\big), \qquad \big(l(z_j),\ f(z_{j+1}),\ l(z_{j+1}),\ l(z_j)\big).$$

Every vertex u of either three-cycle satisfies $\sigma(u-l(z_j)) \le D+G$ (using (6.4)–(6.5)). If the origin were a nonnegative rational affine combination of either determining three-point list, the same argument as in Lemma 3.5 would give $Q(l(z_j)) \le (D+G)^2 < m$, contradicting (6.4). Since neither list admits such a combination, each three-cycle has winding number 0, again finite edge cancellation yields

$$\mathrm{W}\big(f(\partial\mathcal{G})\big) = \mathrm{W}\big((a_n z_j^n)_{j=0,1,2,\dots,4M}\big). \tag{6.6}$$

(d) The boundary winding number is n. Lemma 6.2 also gives the degree-n Fineness Condition. Therefore, by Theorems 5.5 and 5.8,

$$\mathrm{W}\big((a_n z_j^n)_{j=0,1,2,\dots,4M}\big) = \mathrm{W}\big(a_n \cdot P_n\big) = I_n = n. \tag{6.7}$$

Equations (6.3) and (6.7) give $0 = n$, contradicting $n \ge 1$. Hence (6.1) is false, i.e. some grid vertex satisfies $Q(f(z)) < \varepsilon^2$. □

8 Proof of main theorem

Theorem 8.1 (Main theorem)**.** *For any nonconstant polynomial f with rational complex number coefficients and every rational number $\varepsilon > 0$, there exists a rational complex number z such that*

$$Q\big(f(z)\big) < \varepsilon^2.$$

Proof. Write $f(X) = \sum_{j=0}^{n} a_j X^j$ with $n \ge 1$, $a_n \ne 0$. Let $A_j \equiv \sigma(a_j)$ and $\nu \equiv Q(a_n) > 0$. By Lemmas 6.1 and 6.2 we obtain an integer $R \ge 1$ and an even integer $M \ge 2$ satisfying the three strict inequalities (5.2). Form the finite grid $\mathcal{G}$ and apply Theorem 7.1 : there exists some $z \in \mathcal{G}$ satisfying $Q(f(z)) < \varepsilon^2$. □

The proof of theorem is also constructive with an algorithm for finding an approximate zero: construct the finite grid $\mathcal{G}$ used in its proof and test its vertices one by one until finding a vertex z such that $Q(f(z)) < \varepsilon^2$. The theorem guarantees that the algorithm will terminate after finitely many steps. This exhaustive search is generally slow; finding an elementary proof with more effective algorithm is left for future work.

Remark 8.2. Given a positive integer k, set $k_1 \equiv k+1$ and $\varepsilon \equiv 1/k_1 > 0$. Since $(k+1)^2 > k$, one has $1/k_1^2 < 1/k$. By the main theorem (Theorem 8.1), there exists a rational complex number z such that

$$Q(f(z)) < \frac{1}{k_1^2} < \frac{1}{k}.$$

This is one of Wildberger's formulation of the Fundamental Theorem of Algebra over Rationals, which he named FTA I.

9 Complete approximate factorization over Rationals

We now establish a complete approximate factorization theorem: every nonconstant polynomial over K can be approximated, up to any prescribed precision, by a monic (up to its leading coefficient) product of linear factors over K.

9.1 Polynomial coefficient quadrance

For a polynomial

$$P(X) = \sum_{j=0}^{m} c_j X^j \in K[X],$$

define its *coefficient quadrance* by

$$Q_{\text{coeff}}(P) \equiv \max_{0 \le j \le m} Q(c_j), \qquad Q_{\text{coeff}}(0) \equiv 0.$$

For $P, H \in K[X]$, the elementary inequality $Q(u+v) \le 2(Q(u)+Q(v))$ gives

$$Q_{\text{coeff}}(P+H) \le 2\big(Q_{\text{coeff}}(P) + Q_{\text{coeff}}(H)\big)$$

and, when multiplied by a linear factor,

$$Q_{\text{coeff}}((X-z)P) \le 2(1+Q(z))\, Q_{\text{coeff}}(P) \qquad (z \in K),$$

because the coefficients of $(X-z)P$ are of the form $c_{j-1} - zc_j$, whose quadrance is bounded by $2\big(Q(c_{j-1}) + Q(z)Q(c_j)\big)$.

The main goal of this section is to prove the following theorem.

Theorem 9.1 (Complete approximate factorization over Rationals)**.** *Let $f \in K[X]$ be nonconstant with leading coefficient $a_n \neq 0$ and degree $n \ge 1$. For any rational $\varepsilon > 0$ there exist $z_1, \ldots, z_n \in K$ such that*

$$Q_{\text{coeff}}\left(f - a_n \prod_{i=1}^{n} (X - z_i) \right) < \varepsilon.$$

9.2 Proof of Theorem 9.1

We prove the theorem by induction on $n \ge 1$.

Base case $n = 1$. Write $f(X) = a_1 X + a_0$ with $a_1 \neq 0$. Take $z_1 = -a_0/a_1 \in K$. Then

$$f(X) - a_1(X - z_1) = 0,$$

so the desired inequality holds with any $\varepsilon > 0$.

Inductive step. Assume the theorem holds for all polynomials of degree $< n$ (with $n \ge 2$). Let f be as above and fix $\varepsilon > 0$.

Set

$$\eta \equiv \frac{\min(1, \varepsilon)}{4},$$

so that $\eta^2 < \varepsilon/4$. Apply the main theorem (Theorem 8.1) to f with precision η: there exists $z_1 \in K$ such that

$$Q\big(f(z_1)\big) < \eta^2 < \varepsilon/4.$$

Set

$$T \equiv \lceil Q(z_1) \rceil,$$

so that T is a nonnegative integer and $Q(z_1) \le T$.

Let $r \equiv f(z_1)$. By our assumption,

$$Q(r) < \frac{\varepsilon}{4} \tag{9.1}$$

. By polynomial division by the monic linear factor $X - z_1$, we obtain

$$f(X) = (X - z_1)\, g(X) + r,$$

where $g \in K[X]$ has degree $n-1$ and leading coefficient a_n. Set

$$\varepsilon_1 \equiv \frac{\varepsilon}{8(T+1)}.$$

Since $n - 1 \geq 1$ (because $n \geq 2$), the induction hypothesis applies to g: there exist $z_2, \ldots, z_n \in K$ such that

$$Q_{\text{coeff}}\left(g - a_n \prod_{i=2}^{n}(X - z_i)\right) < \varepsilon_1. \tag{9.2}$$

Define the remainder polynomial

$$h(X) \equiv g(X) - a_n \prod_{i=2}^{n}(X - z_i) = \sum_{j=0}^{n-1} b_j X^j,$$

thus $Q(b_j) < \varepsilon_1$ for every $j = 0, 1, \ldots, n-1$.

Now compute the global error:

$$\begin{aligned} f(X) - a_n \prod_{i=1}^{n}(X - z_i) &= (X - z_1)g(X) + r - (X - z_1)a_n \prod_{i=2}^{n}(X - z_i) \\ &= (X - z_1)h(X) + r. \end{aligned}$$

Let

$$(X - z_1)h(X) = \sum_{j=0}^{n} c_j X^j,$$

where

$$c_0 = -z_1 b_0, \qquad c_j = b_{j-1} - z_1 b_j \quad (1 \leq j \leq n-1), \qquad c_n = b_{n-1}.$$

Thus the coefficients of the polynomial $f(X) - a_n \prod_{i=1}^{n}(X - z_i)$ are

$$c_0 + r, \quad c_1, \ \ldots, \ c_{n-1}, \quad c_n.$$

We next estimate their quadrances. For $1 \leq j \leq n-1$,

$$Q(c_j) \leq 2\big(Q(b_{j-1}) + Q(z_1)Q(b_j)\big) < 2(1+T)\varepsilon_1 = \frac{\varepsilon}{4} < \varepsilon.$$

For the leading coefficient,

$$Q(c_n) = Q(b_{n-1}) < \varepsilon_1 < \varepsilon.$$

For the constant term,

$$Q(c_0 + r) \leq 2\big(Q(r) + Q(z_1)Q(b_0)\big) < \frac{\varepsilon}{2} + 2T\varepsilon_1 = \frac{\varepsilon}{2} + \frac{T\varepsilon}{4(T+1)} < \frac{3\varepsilon}{4} < \varepsilon,$$

by using (9.1) and $Q(b_0) < \varepsilon_1$.

Therefore every coefficient of the error polynomial has quadrance strictly less than ε, i.e.

$$Q_{\text{coeff}}\left(f - a_n \prod_{i=1}^{n}(X - z_i)\right) < \varepsilon.$$

This completes the induction and proves the theorem.

Proposition 9.2 (Wildberger's FTA II)**.** *Let $f \in K[X]$ be nonconstant with leading coefficient $a_n \neq 0$ and degree $n \geq 1$. For any integer $k \geq 1$, there exist $z_1, \ldots, z_n \in K$ such that, if*

$$f(X) - a_n \prod_{i=1}^{n} (X - z_i) = \sum_{j=0}^{n} e_j X^j,$$

then

$$\sum_{j=0}^{n} Q(e_j) < \frac{1}{k}.$$

Proof. Apply Theorem 9.1 with $\varepsilon = 1/(k(n+1))$. Then $Q(e_j) < \varepsilon$ for every j, and hence

$$\sum_{j=0}^{n} Q(e_j) < (n+1)\varepsilon = \frac{1}{k}.$$

□

Remark 9.3. Theorem 8.1 and Proposition 9.2 are, respectively, Wildberger's two formulations of the Fundamental Theorem of Algebra over Rationals.

10 Complete approximate real factorization over Rationals

Suppose that the imaginary part of every coefficient a_i of a polynomial f is zero. Theorem 9.1 does not by itself give an approximation by rational real linear and quadratic factors. In this section we prove such a result directly.

For

$$P(X) = \sum_{j=0}^{m} c_j X^j \in \mathbb{Q}[X],$$

define its *coefficient square-sum* by

$$\mathcal{S}(P) \equiv \sum_{j=0}^{m} c_j^2, \qquad \mathcal{S}(0) \equiv 0.$$

Coefficients outside the displayed degree range are understood to be zero.

Lemma 10.1 (Coefficient square-sum estimates)**.** *For $P, H, F \in \mathbb{Q}[X]$, with $\deg F = \ell$, one has*

$$\mathcal{S}(P+H) \leq 2\big(\mathcal{S}(P) + \mathcal{S}(H)\big) \tag{10.1}$$

and

$$\mathcal{S}(FP) \leq (\ell+1)\mathcal{S}(F)\mathcal{S}(P). \tag{10.2}$$

Proof. The first inequality follows, coefficient by coefficient, from $(x+y)^2 \leq 2(x^2+y^2)$. Write $F(X) = \sum_{i=0}^{\ell} b_i X^i$ and $P(X) = \sum_{j=0}^{m} c_j X^j$, where $m \geq 0$. For $0 \leq k \leq m+\ell$, the coefficient of X^k in FP is $\sum_{i=0}^{\ell} b_i c_{k-i}$. The finite rational inequality

$$\left(\sum_{i=0}^{\ell} x_i\right)^2 \leq (\ell+1) \sum_{i=0}^{\ell} x_i^2$$

therefore gives

$$\begin{aligned} \mathcal{S}(FP) &\leq (\ell+1) \sum_{k=0}^{m+\ell} \sum_{i=0}^{\ell} b_i^2 c_{k-i}^2 \\ &= (\ell+1) \left(\sum_{i=0}^{\ell} b_i^2\right) \left(\sum_{j=0}^{m} c_j^2\right), \end{aligned}$$

which is (10.2). □

The next lemma is the conjugation-symmetric replacement for extracting one approximate complex linear factor.

Lemma 10.2 (Approximate real divisor)**.** *Let*

$$f(X) = \sum_{j=0}^{n} a_j X^j \in \mathbb{Q}[X], \qquad n \geq 2, \qquad a_n \neq 0,$$

and let $\varepsilon > 0$ be rational. There exist polynomials $d, g, e \in \mathbb{Q}[X]$ such that

$$f = dg + e, \tag{10.3}$$

with the following properties:

(i) *d is monic of degree $\ell \in \{1, 2\}$, while g has degree $n - \ell$ and leading coefficient a_n;*

(ii) *Either $e = 0$ or $\deg e < \ell$, and every coefficient of e has absolute value strictly less than ε;*

(iii) *if $\ell = 1$, then $d = X - q_1$ for some $q_1 \in \mathbb{Q}$; if $\ell = 2$, then*

$$d = X^2 - 2q_1 X + (q_1^2 + q_2^2)$$

for some $q_1, q_2 \in \mathbb{Q}$ with $q_2 \neq 0$. In the latter case the discriminant of d is $-4q_2^2 < 0$.

Proof. For $0 \leq j \leq n$, set

$$A_j \equiv \sigma(a_j) = |a_j|.$$

As in Section 6, define

$$C \equiv \sum_{j=0}^{n-1} 2^j A_j.$$

Choose an integer $R \geq 1$ satisfying

$$Q(a_n) R^2 > 2C^2. \tag{10.4}$$

This is precisely the radius condition of Lemma 6.1, applied to f. In particular, R depends on f but not on the precision used below. Define

$$L \equiv \sum_{j=1}^{n} j A_j (2R)^{j-1} > 0$$

and the positive rationals

$$\delta \equiv \min\left(1, \frac{\varepsilon}{4L}\right), \qquad \varepsilon_1 \equiv \min\left(\frac{\varepsilon}{8}, \frac{\varepsilon\delta}{4(\delta + R)}\right). \tag{10.5}$$

Thus

$$L\delta \leq \frac{\varepsilon}{4}, \qquad 2\varepsilon_1 \leq \frac{\varepsilon}{4}, \qquad \varepsilon_1 \frac{\delta + R}{\delta} \leq \frac{\varepsilon}{4}. \tag{10.6}$$

Use Lemma 6.2, with the fixed radius R and precision ε_1, to construct the finite grid in Theorem 7.1. That theorem supplies a grid vertex

$$z = q_1 + iq_2, \qquad q_1, q_2 \in \mathbb{Q}, \qquad |q_1|, |q_2| \leq R,$$

such that

$$Q(f(z)) < \varepsilon_1^2. \tag{10.7}$$

Write $f(z) = \alpha + i\beta$. Since all quantities are rational, (10.7) implies directly that

$$|\alpha| < \varepsilon_1, \qquad |\beta| < \varepsilon_1, \qquad \sigma(f(z)) < 2\varepsilon_1. \tag{10.8}$$

Suppose first that $|q_2| \le \delta$. Both z and q_1 have size at most $2R$. Lemma 3.4 and (10.6) give

$$\begin{aligned} |f(q_1)| &\le \sigma\big(f(q_1) - f(z)\big) + \sigma(f(z)) \\ &\le |q_2|L + \sigma(f(z)) < \delta L + 2\varepsilon_1 \le \frac{\varepsilon}{2} < \varepsilon. \end{aligned} \tag{10.9}$$

Division by $X - q_1$ gives

$$f = (X - q_1)g + f(q_1),$$

which has all the required properties with $\ell = 1$.

Suppose instead that $|q_2| > \delta$. Set

$$d(X) \equiv (X - z)(X - \overline{z}) = X^2 - 2q_1X + (q_1^2 + q_2^2) \in \mathbb{Q}[X].$$

Polynomial division in $\mathbb{Q}[X]$ gives

$$f(X) = d(X)g(X) + uX + v \tag{10.10}$$

for some $g \in \mathbb{Q}[X]$ of degree $n - 2$ and some $u, v \in \mathbb{Q}$. Since $d(z) = 0$, evaluation at z gives

$$\alpha + i\beta = f(z) = uz + v = (uq_1 + v) + iuq_2.$$

Consequently, using $|q_2| > \delta$, $|q_1| \le R$, and (10.6),

$$|u| = \frac{|\beta|}{|q_2|} < \frac{\varepsilon_1}{\delta} < \varepsilon \tag{10.11}$$

and

$$|v| = |\alpha - q_1u| < \varepsilon_1 + \frac{R\varepsilon_1}{\delta} = \varepsilon_1\frac{\delta + R}{\delta} \le \frac{\varepsilon}{4} < \varepsilon. \tag{10.12}$$

Finally,

$$\operatorname{disc}(d) = (-2q_1)^2 - 4(q_1^2 + q_2^2) = -4q_2^2 < 0.$$

Thus (10.10) has all the required properties with $\ell = 2$. Both cases use only a finite grid search, rational comparisons, and rational polynomial division. □

Theorem 10.3 (Complete approximate real factorization over Rationals)**.** *Let*

$$f(X) = \sum_{j=0}^{n} a_jX^j \in \mathbb{Q}[X], \qquad n \ge 1, \qquad a_n \ne 0.$$

For every rational $\varepsilon > 0$, there exist nonnegative integers s, t and rational numbers

$$r_1, \dots, r_s, \qquad q_{1,1}, q_{1,2}, \dots, q_{t,1}, q_{t,2}$$

such that

$$s + 2t = n, \qquad q_{j,2} \ne 0 \quad (1 \le j \le t), \tag{10.13}$$

and

$$\mathcal{S}\left(f - a_n\prod_{i=1}^{s}(X - r_i)\prod_{j=1}^{t}\big(X^2 - 2q_{j,1}X + (q_{j,1}^2 + q_{j,2}^2)\big)\right) < \varepsilon. \tag{10.14}$$

Proof. We prove the slightly stronger assertion allowing degree $n = 0$, with both products then empty. The proof is by induction on n.

If $n = 0$, the empty product is 1 by default, and the error is zero.

If $n = 1$, write $f = a_1X + a_0$ and take $r_1 = -a_0/a_1$; again the factorization is exact.

Now let $n \geq 2$ and assume the assertion for all smaller degrees. Set

$$\varepsilon_1 \equiv \frac{\min(1, \varepsilon)}{4},$$

so that

$$8\varepsilon_1^2 < \varepsilon. \tag{10.15}$$

Apply Lemma 10.2 to f and ε_1. We obtain

$$f = dg + e, \tag{10.16}$$

where d has degree $\ell \in \{1, 2\}$, g has degree $n - \ell$ and its leading coefficient is a_n, and

$$\mathcal{S}(e) < 2\varepsilon_1^2. \tag{10.17}$$

The last inequality holds because e has at most two coefficients and each has absolute value less than ε_1.

Define the positive rational number

$$C_d \equiv (\ell + 1)\mathcal{S}(d) > 0, \qquad \varepsilon_2 \equiv \frac{\varepsilon}{4C_d} > 0.$$

By the induction hypothesis, there is a monic product P of allowed rational linear and negative-discriminant quadratic factors, of total degree $n - \ell$, such that

$$\mathcal{S}(g - a_nP) < \varepsilon_2. \tag{10.18}$$

Set $E \equiv g - a_nP$. Equations (10.1), (10.2), (10.15), (10.16), (10.17), and (10.18) give

$$\begin{aligned}
\mathcal{S}(f - a_ndP) &= \mathcal{S}(dE + e) \\
&\leq 2\big(\mathcal{S}(dE) + \mathcal{S}(e)\big) \\
&\leq 2\big(C_d\mathcal{S}(E) + \mathcal{S}(e)\big) \\
&< 2\left(C_d\frac{\varepsilon}{4C_d} + 2\varepsilon_1^2\right) = \frac{\varepsilon}{2} + 4\varepsilon_1^2 < \varepsilon.
\end{aligned}$$

Adjoining d to the factors of P preserves the required factor forms, and their total degree is $\ell + (n - \ell) = n$. In the quadratic case, Lemma 10.2 gives the strict negative-discriminant condition. This completes the induction. □

Corollary 10.4 (Real factorization)**.** *Under the hypotheses of Theorem 10.3, for every integer $k \geq 1$ there is a product of the form*

$$G(X) = a_n \prod_{i=1}^{s}(X - r_i) \prod_{j=1}^{t}\big(X^2 - 2q_{j,1}X + (q_{j,1}^2 + q_{j,2}^2)\big),$$

with all displayed parameters rational, $s + 2t = n$, and $q_{j,2} \neq 0$ for $1 \leq j \leq t$, such that, if

$$f(X) - G(X) = \sum_{j=0}^{n} e_jX^j,$$

then

$$\sum_{j=0}^{n} e_j^2 < \frac{1}{k}.$$

Proof. Apply Theorem 10.3 with $\varepsilon = 1/k$. □

Remark 10.5 (Finite character of the construction). The constructions in Sections 9 and 10 are finite. At each inductive step, one performs a finite grid search followed by rational polynomial division, and the degree drops by at least one. Therefore the induction terminates after at most n steps. For each prescribed rational precision, Theorems 9.1 and 10.3 construct finite lists of rational coefficients using only rational number computations and comparisons.

Acknowledgments

We acknowledge the use of the Math AI agents Rethlas and Archon (developed by Bin Dong's group at Peking University), utilizing GPT-5.6-sol and Deepseek-V4-Flash, to assist in reasoning and verification for portions of this work. All outputs were independently evaluated and refined by the authors, who retain full responsibility for the results.

The second author respectfully dedicates this paper to the memory of his former advisor, Professor Xinghua Wang, for guiding his entrance into computational mathematics [13] and for his lasting friendship.

We are also grateful to Norman Wildberger for proofreading the manuscript.

This work is partially supported by Smale Institute.

References

[1] S. Basu and D. J. Velleman, On Gauss's first proof of the fundamental theorem of algebra, *The American Mathematical Monthly* **124** (2017), no. 8, 688–694. doi:10.4169/amer.math.monthly.124.8.688.

[2] L. Blum, F. Cucker, M. Shub, and S. Smale, *Complexity and Real Computation*, Springer-Verlag, New York, 1998. doi:10.1007/978-1-4612-0701-6.

[3] A.-L. Cauchy, *Cours d'analyse de l'École Royale Polytechnique, première partie: Analyse algébrique*, Imprimerie Royale and Debure frères, Paris, 1821. doi:10.3931/e-rara-26185.

[4] B. Fine and G. Rosenberger, *The Fundamental Theorem of Algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997. doi:10.1007/978-1-4612-1928-6.

[5] C. F. Gauss, *Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*, doctoral dissertation, Helmstedt, 1799. doi:10.18452/80.

[6] H. W. Kuhn, A new proof of the fundamental theorem of algebra, *Mathematical Programming Studies* **1** (1974), 148–158. doi:10.1007/BFb0121246.

[7] J. Lützen, *Joseph Liouville 1809–1882: Master of Pure and Applied Mathematics*, Studies in the History of Mathematics and Physical Sciences, vol. 15, Springer-Verlag, New York, 1990. doi:10.1007/978-1-4612-0989-8.

[8] S. S. Petrova, Sur l'histoire des démonstrations analytiques du théorème fondamental de l'algèbre, *Historia Mathematica* **1** (1974), no. 3, 255–261. doi:10.1016/0315-0860(74)90062-7.

[9] S. Smale, The fundamental theorem of algebra and complexity theory, *Bulletin of the American Mathematical Society (N.S.)* **4** (1981), no. 1, 1–36. doi:10.1090/S0273-0979-1981-14858-8.

[10] S. Smale, On the efficiency of algorithms of analysis, *Bulletin of the American Mathematical Society (N.S.)* **13** (1985), no. 2, 87–121.

[11] M. Shub and S. Smale, Computational complexity: On the geometry of polynomials and a theory of cost I, *Annales Scientifiques de l'École Normale Supérieure* **18** (1985), no. 1, 107–142.

[12] M. Shub and S. Smale, Computational complexity: On the geometry of polynomials and a theory of cost II, *SIAM Journal on Computing* **15** (1986), no. 1, 145–161.

[13] X. H. Wang and X. H. Xuan, Random polynomial space and computational complexity theory, *Science in China, Series A* **30** (1987), 673–684.

[14] N. J. Wildberger, *Divine Proportions: Rational Trigonometry to Universal Geometry*, Wild Egg Pty Ltd, Australia, 2005. ISBN 0-9757492-0-X.

[15] N. J. Wildberger, *What is the Fundamental Theorem of Algebra, Really?*, Abstract Algebra Math Foundations 217, online lecture, 2017. https://www.youtube.com/watch?v=qoSGtoy7DlI.