

5.6 The Fundamental Theorem of Algebra

Over $\mathbb{Q}$ the polynomial $x^2 - 2$ has no root, and over $\mathbb{R}$ the polynomial $x^2 + 1$ has none. Chapter 1 announced that over $\mathbb{C}$ this stops: every non-constant complex polynomial has a root. This section proves it, and then reads off what it says about factoring complex and real polynomials.

No argument from the field axioms alone can prove the theorem. The field $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ of Example (Rational and Integer Complex Numbers) satisfies every field axiom, and it contains an element i with $i^2 = -1$, just as $\mathbb{C}$ does. Yet $x^2 - 2$ has no root in it. If $(a + bi)^2 = 2$ with $a, b \in \mathbb{Q}$, then comparing real and imaginary parts (Definition 1.1.1), $a^2 - b^2 = 2$ and $2ab = 0$, so $a = 0$ or $b = 0$ ($\mathbb{Q}$ has no zero divisors, Theorem 2.1.1 (f), and $2 \neq 0$). If $b = 0$, then $a^2 = 2$, which no rational satisfies (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1). If $a = 0$, then $-b^2 = 2$, impossible since $-b^2 \leq 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)). So the proof must use a property of $\mathbb{R}$ that $\mathbb{Q}$ lacks. It is the supremum property of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 5 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.6.3).

The plan has two halves. First, $|p|$ attains a smallest value on $\mathbb{C}$ (Theorem 5.6.3). Second, at any point where p is not 0, some nearby point gives $|p|$ a smaller value (Lemma 5.6.5). So at a point where the smallest value is attained, p must be 0. The first half is where completeness is invoked directly (Steps 2 and 5); the second half uses it only indirectly, through square roots (see the remark after the minimum theorem).

Throughout, p is a polynomial in $\mathbb{C}[x]$, and $p(z)$ is its value at $z \in \mathbb{C}$ (Definition 4.4.1). Inequalities are between real numbers; the modulus $|z|$ is a non-negative real (Definition 1.2.1).

5.6.1 Two estimates

🔄 **Second reading** · *The facts about the modulus used in this section*

All of them are from Chapter 1. For $z, w \in \mathbb{C}$: $|z|^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2$ (Definition 1.2.1); $|\operatorname{Re} z| \leq |z|$, $|\operatorname{Im} z| \leq |z|$ and $|z| \leq |\operatorname{Re} z| + |\operatorname{Im} z|$ (Lemma 1.3.1); $|zw| = |z||w|$, so $|z^j| = |z|^j$ by induction on j , and $|z| = 0$ only for $z = 0$ (Theorem 1.2.2 (d), (e)); $|z_1 + \cdots + z_m| \leq |z_1| + \cdots + |z_m|$ and $||z| - |w|| \leq |z - w|$ (Corollary 1.3.3 (b), (c)). For a real number the modulus is the absolute value of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 4 (Proposition 1.2.1), so the rules of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 apply to it.

Three facts about powers of non-negative reals are used as well, each by induction on the exponent with *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Proposition 2.3.5 (c): if $0 \leq a \leq b$, then $a^j \leq b^j$; if $a \geq 1$ and $i \leq j$, then $a^i \leq a^j$; if $0 < t \leq 1$ and $i \leq j$, then $t^j \leq t^i$.

The first estimate says that $|p(z)|$ is large when $|z|$ is large, so the search for a smallest value can be confined to a bounded region.

Lemma 5.6.1. Growth of a Complex Polynomial

Let $p = \sum_{j=0}^n a_j x^j \in \mathbb{C}[x]$ with $n = \deg p \geq 1$, so $a_n \neq 0$. Let

$$A := |a_0| + \cdots + |a_{n-1}|, \quad R := \max\left\{1, \frac{2A}{|a_n|}\right\}.$$

Then for every $z \in \mathbb{C}$ with $|z| \geq R$,

$$|p(z)| \geq \frac{1}{2}|a_n||z|^n \geq \frac{1}{2}|a_n||z|.$$

In words: beyond the radius R , the top term outweighs all the others together, at least by half.

🕒 **Second reading** • *The proof: the top term against the rest*

Proof. Let $|z| \geq R$. Then $|z| \geq 1$, so $|z|^j \leq |z|^{n-1}$ for $0 \leq j \leq n-1$. Write $p(z) = a_n z^n + w$ with $w := \sum_{j=0}^{n-1} a_j z^j$ (the sum recursion). By Corollary 1.3.3 (b) and Theorem 1.2.2 (d),

$$|w| \leq \sum_{j=0}^{n-1} |a_j| |z|^j \leq A |z|^{n-1}.$$

By Corollary 1.3.3 (c), which is the reverse triangle inequality (a) with the second number negated, $|p(z)| \geq |a_n||z|^n - |w| \geq |z|^{n-1}(|a_n||z| - A)$. Since $|z| \geq 2A/|a_n|$ and $|a_n| > 0$, $A \leq \frac{1}{2}|a_n||z|$, so $|a_n||z| - A \geq \frac{1}{2}|a_n||z|$. Hence $|p(z)| \geq \frac{1}{2}|a_n||z|^n$. Finally $|z|^n \geq |z|$, since $|z| \geq 1$ and $n \geq 1$. ■

The second estimate replaces continuity, which this volume does not have. It bounds how much p can change between two points of a bounded region, with an explicit constant.

Lemma 5.6.2. A Lipschitz Bound for a Complex Polynomial

Let $p = \sum_{j=0}^n a_j x^j \in \mathbb{C}[x]$ and let $M \in \mathbb{R}$ with $M \geq 0$. Put

$$L := \sum_{j=1}^n j |a_j| M^{j-1} \quad (j|a_j| \text{ the multiple } (j \cdot 1)|a_j| \text{ in } \mathbb{R}).$$

Then $|p(z) - p(w)| \leq L|z - w|$ for all $z, w \in \mathbb{C}$ with $|z| \leq M$ and $|w| \leq M$.

In words: on the disc of radius M , p moves at most L times as far as its argument.

🕒 **Second reading** • *The proof: factor each difference of powers*

Proof. Let $|z|, |w| \leq M$. Termwise (the sum rules $(\Sigma 1)$, $(\Sigma 2)$, $(\Sigma 4)$ of Lemma 4.1.1),

$p(z) - p(w) = \sum_{j=0}^n a_j(z^j - w^j)$, and the term $j = 0$ is 0. For $j \geq 1$, Lemma 1.1.4 gives

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

Each of the j terms of the sum has modulus $|z|^i |w|^{j-1-i} \leq M^i M^{j-1-i} = M^{j-1}$. So $|z^j - w^j| \leq j M^{j-1} |z - w|$ by Corollary 1.3.3 (b), and summing over j with the same corollary, $|p(z) - p(w)| \leq \sum_{j=1}^n |a_j| j M^{j-1} |z - w| = L |z - w|$.

■

This is the only “continuity” the proof below needs, and it comes with a constant that can be computed.

Quick check. For $p = x^2 + 1$, compute A and R of Lemma 5.6.1, and the constant L of Lemma 5.6.2 for $M = 4$.

Solution. Here $a_0 = 1$, $a_1 = 0$, $a_2 = 1$, $n = 2$. So $A = |1| + |0| = 1$ and $R = \max\{1, 2 \cdot 1/1\} = 2$. For $M = 4$, $L = 1 \cdot 0 \cdot 4^0 + 2 \cdot 1 \cdot 4^1 = 8$. (Check of the Lipschitz bound in one case: $|p(z) - p(w)| = |z^2 - w^2| = |z + w||z - w| \leq 8|z - w|$ when $|z|, |w| \leq 4$.)

5.6.2 The smallest value of the modulus is attained

We now look for a point where $|p|$ is smallest. The infimum of the values $|p(z)|$ exists by completeness; the work is to find a point **at** which it is attained. We trap such a point in smaller and smaller squares.

For $\sigma, \tau \in \mathbb{R}$ and $s \in \mathbb{R}$ with $s > 0$, let

$$S(\sigma, \tau, s) := \{z \in \mathbb{C} : \sigma \leq \operatorname{Re} z \leq \sigma + s, \tau \leq \operatorname{Im} z \leq \tau + s\},$$

the closed square with lower-left corner $\sigma + \tau i$ and side s . (In this section σ and τ are real numbers. Chapter 3 uses the same letters for permutations, which do not appear here.) Each such square contains its corner, so it is non-empty. Its four **quarters**, in this fixed order, are

$$\begin{aligned} S(\sigma, \tau, s/2), & \quad S(\sigma + s/2, \tau, s/2), \\ S(\sigma, \tau + s/2, s/2), & \quad S(\sigma + s/2, \tau + s/2, s/2). \end{aligned}$$

Each quarter lies in the square, and every point of the square lies in some quarter: $\operatorname{Re} z \leq \sigma + s/2$ or $\operatorname{Re} z \geq \sigma + s/2$, and likewise for $\operatorname{Im} z$, since $\leq$ is a total order on $\mathbb{R}$ (Number Systems: From $\setminus(\mathbb{N} \setminus)$ to $\setminus(\mathbb{N} \mathbb{R} \setminus)$, Proposition 2.3.5 (i)).

Theorem 5.6.3. The Modulus of a Complex Polynomial Attains Its Minimum

For every $p \in \mathbb{C}[x]$ there is $z^* \in \mathbb{C}$ with $|p(z^*)| \leq |p(z)|$ for **every** $z \in \mathbb{C}$.

Idea. Confine the search to one big square S_0 by the growth lemma. The infimum m of $|p|$ over S_0 exists. Cut S_0 into four quarters: the infimum over S_0 is the least of the four infima, so some quarter has the **same** infimum m ; keep the first such quarter, and repeat. We call this move **keep the quarter that keeps the infimum**. The squares shrink to a single point z^* , which completeness supplies as a supremum of corners. Near z^* every square still has points where $|p|$ is almost m , and the Lipschitz bound says $|p(z^*)|$ is almost the same; so $|p(z^*)| = m$. This is the bisection of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 5, now in the plane. *Before reading on: why keep a quarter whose **infimum** equals the square's, rather than a quarter containing a point where $|p|$ is smallest?*

Proof. If p is a constant a_0 (including 0), then $p(z) = a_0$ for every z , and $z^* := 0$ works. Let $n := \deg p \geq 1$, with leading coefficient $a_n \neq 0$, let R be as in Lemma 5.6.1, and let

$$\rho := \max\left\{R, \frac{2|p(0)|}{|a_n|}\right\},$$

so $\rho \geq 1$.

Step 1 (a square that suffices). Let $S_0 := S(-\rho, -\rho, 2\rho)$. It contains 0. If $z \notin S_0$, then $|\operatorname{Re} z| > \rho$ or $|\operatorname{Im} z| > \rho$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 (d)), so $|z| > \rho \geq R$ (Lemma 1.3.1), and by Lemma 5.6.1,

$$|p(z)| \geq \frac{1}{2}|a_n||z| > \frac{1}{2}|a_n|\rho \geq |p(0)|. \quad (1)$$

Step 2 (the infimum; completeness, first use). For a square S , the set $V(S) := \{|p(z)| : z \in S\} \subseteq \mathbb{R}$ is non-empty and bounded below by 0. So it has an infimum $m(S)$ in $\mathbb{R}$ (Sets, Relations, and Cardinality, Definition 2.6.5); the fold after the proof derives this from the supremum property. Two consequences are used: $m(S) \leq |p(z)|$ for every $z \in S$; and for every $\varepsilon > 0$ there is $z \in S$ with $|p(z)| < m(S) + \varepsilon$, since otherwise $m(S) + \varepsilon$ would be a lower bound of $V(S)$ larger than the greatest one. If $S' \subseteq S$, then $m(S)$ is a lower bound of $V(S') \subseteq V(S)$, so $m(S) \leq m(S')$.

Step 3 (a quarter with the same infimum). Let S be a square and $Q_1, \dots, Q_4$ its quarters. Each $m(Q_i) \geq m(S)$ by Step 2. Let μ be the least of the four numbers $m(Q_i)$. Every $z \in S$ lies in some Q_i , so $|p(z)| \geq m(Q_i) \geq \mu$: μ is a lower bound of $V(S)$, hence $\mu \leq m(S)$. So $\mu = m(S)$, and some quarter has $m(Q_i) = m(S)$. Let $q(S)$ be the **first** quarter, in the fixed order, with $m(Q_i) = m(S)$. This is a rule: q is a function from squares to squares.

Step 4 (the nested squares). Identify the square $S(\sigma, \tau, s)$ with the triple (σ, τ, s) . By Sets, Relations, and Cardinality, Theorem 2.3.1 (read on $\mathbb{N} = \omega$ through Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 1.7.3), there is exactly one sequence of squares $S_k = S(\sigma_k, \tau_k, s_k)$, $k \in \mathbb{N}$, with S_0 as in Step 1 and $S_{k+1} = q(S_k)$. By induction on k :

- $s_k = 2\rho/2^k$, the power 2^k taken in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 4.2.1), since each quarter has half the side;
- $m(S_k) = m$, where $m := m(S_0)$, by the choice of q ;

- $\sigma_k \leq \sigma_{k'} \leq \sigma_k + s_k - s_{k'}$ and $\tau_k \leq \tau_{k'} \leq \tau_k + s_k - s_{k'}$ for all $k' \geq k$, since the corner of a quarter is σ or $\sigma + s/2$ and its far edge $\sigma + s/2$ or $\sigma + s$. In particular $S_{k'} \subseteq S_k \subseteq S_0$.

Step 5 (the common point; completeness, second use). The set $\{\sigma_k : k \in \mathbb{N}\}$ is non-empty and bounded above by $\sigma_0 + s_0$ (Step 4 with $k = 0$). By Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Theorem 5.6.3 it has a supremum σ^* (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Definition 5.6.1). Fix k . Then $\sigma_k \leq \sigma^*$, and $\sigma_k + s_k$ is an upper bound of the set: for $k' \geq k$, $\sigma_{k'} \leq \sigma_k + s_k$ by Step 4, and for $k' < k$, $\sigma_{k'} \leq \sigma_k$ by Step 4 with the roles of k and k' exchanged. So $\sigma_k \leq \sigma^* \leq \sigma_k + s_k$ for every k . In the same way $\tau^* := \sup\{\tau_k : k \in \mathbb{N}\}$ satisfies $\tau_k \leq \tau^* \leq \tau_k + s_k$. Hence $z^* := \sigma^* + \tau^*i$ lies in every S_k .

Step 6 (the value at the common point). For $z, w \in S_k$, $|\operatorname{Re}(z - w)| \leq s_k$ and $|\operatorname{Im}(z - w)| \leq s_k$, so $|z - w| \leq 2s_k$ (Lemma 1.3.1). Every point of S_0 has modulus at most $\rho + \rho = 2\rho$, by the same lemma. Let L be the constant of Lemma 5.6.2 for $M = 2\rho$.

Let $\varepsilon \in \mathbb{R}$ with $\varepsilon > 0$. By Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Theorem 5.4.2 there is $k \in \mathbb{N}$ with $k > 8\rho L/\varepsilon$; then $2^k \geq k + 1 > 8\rho L/\varepsilon$ by Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Lemma 5.6.1, so

$$2s_k L = \frac{4\rho L}{2^k} < \frac{\varepsilon}{2}. \quad (2)$$

This k depends on ε (and on p , through ρ and L). Since $m(S_k) = m$, Step 2 gives a point $w \in S_k$ with $|p(w)| < m + \varepsilon/2$ ($\exists E$: the point w is used only inside this argument for this ε). Both z^* and w lie in $S_k \subseteq S_0$, so by the triangle inequality (Theorem 1.3.2), the Lipschitz bound and (2),

$$|p(z^*)| \leq |p(w)| + |p(z^*) - p(w)| < m + \frac{\varepsilon}{2} + L \cdot 2s_k < m + \varepsilon.$$

As $\varepsilon > 0$ was arbitrary, $|p(z^*)| \leq m$: otherwise $\varepsilon := |p(z^*)| - m > 0$ would give $|p(z^*)| < |p(z^*)|$. Also $|p(z^*)| \geq m$, since $z^* \in S_0$. So $|p(z^*)| = m$.

Step 7 (the minimum over all of the plane). Let $z \in \mathbb{C}$. If $z \in S_0$, then $|p(z)| \geq m = |p(z^*)|$. If $z \notin S_0$, then $|p(z)| > |p(0)| \geq m$ by (1), since $0 \in S_0$. This proves the theorem. ■

○ **Second reading** · Step 2: why the infimum exists

Let $V \subseteq \mathbb{R}$ be non-empty and bounded below by 0, and let B be the set of lower bounds of V . Then $0 \in B$, and every element of V is an upper bound of B , so B is non-empty and bounded above; by Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Theorem 5.6.3 it has a supremum m (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Definition 5.6.1). Each $v \in V$ is an upper bound of B , so $m \leq v$: m is a lower bound of V . Each lower bound u of V is in B , so $u \leq m$. Thus m is the greatest lower bound of V , its infimum in the sense of Sets, Relations, and Cardinality, Definition 2.6.5.

The answer to the prompt. A quarter containing a point where $|p|$ is smallest is what the theorem is trying to prove exists, so it cannot be used to choose quarters. The infimum of a quarter always exists, by completeness, and Step 3 shows that some quarter keeps it. Choosing “the first such quarter in a fixed order” makes the step a rule, so the recursion theorem applies and no choice is made at any stage; compare Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Example (Picking

Representatives Is a Use of Choice), where a proof that picks infinitely many objects without a rule uses the axiom of choice.

Remark. The supremum property is invoked directly in Steps 2 and 5 and nowhere else in this chapter. It also enters indirectly, through the non-negative real square roots of Number Systems: From $(\mathbb{N})$ to $(\mathbb{R})$, Proposition 6.1.4, which that result derives from the supremum: they give the modulus used in every inequality of this section, and the complex square roots of Proposition 1.4.1 used in the next lemma. In $\mathbb{Q}(i)$, with $\mathbb{Q}$ in place of $\mathbb{R}$, both fail; Exercise C1 (c) asks where.

Quick check. In Step 3, why does it matter that there are only **four** quarters?

Solution. The proof takes μ , the least of the numbers $m(Q_1), \dots, m(Q_4)$. A finite list of real numbers has a least element, so μ exists and equals one of them; that is what produces a quarter with $m(Q_i) = m(S)$. With infinitely many pieces, the infimum of their infima need not be attained by any one piece.

5.6.3 A direction in which the modulus decreases

The second half of the plan is algebra, together with complex square roots (Proposition 1.4.1). Near a point z_0 , write $p(z_0 + h) = b_0 + b_k h^k + (\text{higher powers of } h)$, with $b_0 = p(z_0)$. If we can choose the direction of h so that $b_k h^k$ points back toward 0 from b_0 , and h so small that the higher terms do not undo the gain, then $|p|$ decreases. Dividing by b_0 , the first need is a ζ for which $c\zeta^k$ has negative real part.

Lemma 5.6.4. A Direction with Negative Real Part

Let $c \in \mathbb{C}$ with $c \neq 0$, and let $k \in \mathbb{N}$ with $k \geq 1$. Then there is $\zeta \in \mathbb{C}$ with $\operatorname{Re}(c\zeta^k) < 0$.

Try it first (ten minutes): for $c = i$, find ζ with $\operatorname{Re}(c\zeta^3) < 0$. Then find ζ with $\operatorname{Re}(c\zeta^2) < 0$.

Idea. For $k = 3$, the four “axis” directions $\zeta \in \{1, -1, i, -i\}$ already turn c around: ζ^3 runs through $1, -1, -i, i$, and $i \cdot i = -1$. For $k = 2$ they do not: $\zeta^2 \in \{1, -1\}$ for these four, and $c\zeta^2 \in \{i, -i\}$ has real part 0. What works for $k = 2$ is a square root of a direction that works for $k = 1$: $\eta = i$ gives $\operatorname{Re}(i \cdot i) = -1$, and if $\zeta^2 = \eta$, then $c\zeta^2 = c\eta$. So odd k is handled by the axes, and even $k = 2j$ by a square root of a direction for j , which is strong induction. Square roots of complex numbers come from real square roots (Proposition 1.4.1), so no polar form is needed.

Proof. We prove, by strong induction on k (Logic and Proof, Theorem 4.2.2, on $\mathbb{N} = \omega$), the statement: if $k \geq 1$, then for every non-zero $c \in \mathbb{C}$ there is ζ with $\operatorname{Re}(c\zeta^k) < 0$. For $k = 0$ there is nothing to prove. Let $k \geq 1$, assume the statement for every smaller exponent, and let $c \neq 0$. By Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 1.6.4 (d), $k = 2j + 1$ or $k = 2j$ for some $j \in \mathbb{N}$.

Case 1: k odd, $k = 2j + 1$. Since $i^2 = -1$, the power laws (Proposition 1.1.3 (a)–(c)) give $i^k = (i^2)^j i = (-1)^j i \in \{i, -i\}$, $(-1)^k = -1$ and $(-i)^k = (-1)^k i^k = -i^k$. So as ζ runs through $1, -1, i, -i$, the products $c\zeta^k$ run through $c, -c$ and $ic, -ic$ (in some order). If $\operatorname{Re} c \neq 0$, one of $\operatorname{Re} c$ and $\operatorname{Re}(-c) = -\operatorname{Re} c$ is negative. If $\operatorname{Re} c = 0$, then $c = bi$ with $b := \operatorname{Im} c \neq 0$, and $ic = -b, -ic = b$: one of them has negative real part.

Case 2: k even, $k = 2j$ with $1 \leq j < k$. By the induction hypothesis for j , there is η with $\operatorname{Re}(c\eta^j) < 0$. Then $\eta \neq 0$, since otherwise $c\eta^j = 0$. By Proposition 1.4.1 there is ζ with $\zeta^2 = \eta$, and $\zeta^k = (\zeta^2)^j = \eta^j$ (Proposition 1.1.3 (b)). So $\operatorname{Re}(c\zeta^k) = \operatorname{Re}(c\eta^j) < 0$. This proves the lemma. ■

With polar form one would take ζ to be a k -th root of $-\bar{c}/|c|$. This volume's k -th roots of complex numbers (Theorem 1.6.2) rest on the cosine and sine of Axiom 1.5.2, which it borrows from analysis. The proof above uses only the complex square roots of Proposition 1.4.1, which Section 1.4 builds from the real square roots of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 6.1.4).

Quick check. For $c = i$ and $k = 1$, which $\zeta \in \{1, -1, i, -i\}$ gives $\operatorname{Re}(c\zeta) < 0$?

Solution. $\zeta = i$: $c\zeta = i \cdot i = -1$, with real part $-1 < 0$. The others give $i, -i$ and $-i \cdot i = 1$, with real parts $0, 0, 1$.

Now the descent itself. Re-centering at z_0 is Theorem 5.4.3 of Section 5.4.

Lemma 5.6.5. d'Alembert's Lemma

Let $p \in \mathbb{C}[x]$ be non-constant, and let $z_0 \in \mathbb{C}$ with $p(z_0) \neq 0$. Then there is $z \in \mathbb{C}$ with $|p(z)| < |p(z_0)|$.

Idea. Expand around z_0 : $p(z_0 + h) = b_0(1 + (b_k/b_0)h^k + \dots)$, where k is the first index $j \geq 1$ with $b_j \neq 0$. With $h = t\zeta$, $t > 0$ real and ζ from the previous lemma, the bracket is $1 + t^k u + E$ with $\operatorname{Re} u < 0$. For small $s > 0$, $|1 + su|$ is about $1 - s\alpha$ with $\alpha = -\operatorname{Re} u$, and E is of order t^{k+1} , smaller than the gain $t^k \alpha$. The proof fixes t first and then checks the inequality. *Before reading on: where is k , the first index with $b_k \neq 0$, used?*

Proof. Let $n := \deg p \geq 1$. By Theorem 5.4.3 there are $b_0, \dots, b_n \in \mathbb{C}$ with $p = \sum_{j=0}^n b_j(x - z_0)^j$, $b_0 = p(z_0) \neq 0$ and $b_n \neq 0$ (the leading coefficient of p). So the set of $j \in \{1, \dots, n\}$ with $b_j \neq 0$ contains n , and it has a least element k (Sets, Relations, and Cardinality, Theorem 2.1.3): $k \geq 1$, $b_k \neq 0$, and $b_j = 0$ for $1 \leq j < k$.

Let $c := b_k/b_0 \neq 0$. By Lemma 5.6.4 there is ζ with $\operatorname{Re}(c\zeta^k) < 0$. Put

$$u := c\zeta^k, \quad \alpha := -\operatorname{Re} u > 0, \quad B := \sum_{j=k+1}^n \left| \frac{b_j}{b_0} \right| |\zeta|^j \geq 0.$$

Then $\alpha \leq |u|$ (Lemma 1.3.1), so $|u| > 0$. Choose

$$t := \min \left\{ 1, \frac{\alpha}{|u|^2}, \frac{\alpha}{4B} \right\} \quad (\text{the last entry omitted if } B = 0),$$

a real number with $0 < t \leq 1$. It depends only on p , z_0 and ζ . We show that $z := z_0 + t\zeta$ works.

The expansion. By Theorem 5.4.3 (c) with $h = t\zeta$, and since $b_j = 0$ for $1 \leq j < k$,

$$p(z_0 + t\zeta) = b_0 + b_k t^k \zeta^k + \sum_{j=k+1}^n b_j t^j \zeta^j = b_0(1 + t^k u + E),$$

where $E := \sum_{j=k+1}^n (b_j/b_0) t^j \zeta^j$. Since $0 < t \leq 1$, $t^j \leq t^{k+1}$ for $j \geq k+1$, so $|E| \leq t^{k+1} B$ (Corollary 1.3.3 (b)).

The main term. Let $s \in \mathbb{R}$ with $0 < s \leq \alpha/|u|^2$. Since $1 + su$ has real part $1 - s\alpha$ and imaginary part $s \operatorname{Im} u$,

$$|1 + su|^2 = (1 - s\alpha)^2 + s^2 (\operatorname{Im} u)^2 = 1 - 2s\alpha + s^2 |u|^2 \leq 1 - s\alpha,$$

where the last step uses $s|u|^2 \leq \alpha$. Also $(1 - s\alpha/2)^2 = 1 - s\alpha + s^2 \alpha^2/4 \geq 1 - s\alpha$, and $1 - s\alpha/2 > 0$ because $s\alpha \leq \alpha^2/|u|^2 \leq 1$. Two non-negative reals whose squares are in the order $|1 + su|^2 \leq (1 - s\alpha/2)^2$ are in the same order (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (g)), so

$$|1 + su| \leq 1 - \frac{s\alpha}{2}. \quad (3)$$

The choice of t at work. Let $s := t^k$. Then $0 < s \leq t \leq \alpha/|u|^2$, so (3) applies; and $tB \leq \alpha/4$. Hence, by Theorem 1.2.2 (d) and the triangle inequality,

$$\begin{aligned} |p(z_0 + t\zeta)| &\leq |b_0| (|1 + t^k u| + |E|) \leq |b_0| \left(1 - \frac{t^k \alpha}{2} + t^k \cdot tB \right) \\ &\leq |b_0| \left(1 - \frac{t^k \alpha}{4} \right) < |b_0| = |p(z_0)|, \end{aligned}$$

the last step because $|b_0| > 0$ and $t^k \alpha > 0$. This proves the lemma. ■

Where k is used. The index k is the first non-zero coefficient after b_0 , so the expansion has no terms between b_0 and $b_k t^k \zeta^k$. A term $b_j t^j \zeta^j$ with $1 \leq j < k$ would be of order t^j , larger than

the gain $t^k\alpha$ for small t , and in an uncontrolled direction. And the direction lemma is applied with this exponent k .

Example. One step of descent

Run the proof of [Lemma 5.6.5](#) for $p = x^3 + x^2 + 1$ at $z_0 = 0$, and compare with moving along the real axis.

Solution. Here the expansion around 0 is p itself: $b_0 = 1, b_1 = 0, b_2 = 1, b_3 = 1$. So $k = 2$ and $c = b_2/b_0 = 1$.

The direction. The proof of [Lemma 5.6.4](#) for $k = 2 = 2 \cdot 1$ first finds a direction for $j = 1$: since $\operatorname{Re} c = 1 \neq 0$, $\eta = -1$ works, with $\operatorname{Re}(c\eta) = -1$. Then it takes a square root of $\eta = -1$; the formula of Proposition 1.4.1 (with $a = -1, b = 0, r = 1$) gives $\zeta = 0 + 1 \cdot i = i$.

The constants. $u = c\zeta^2 = -1, \alpha = 1, |u|^2 = 1, B = |b_3/b_0||\zeta|^3 = 1$, so $t = \min\{1, 1, 1/4\} = 1/4$.

The new point. $z = i/4$, and

$$p(i/4) = -\frac{i}{64} - \frac{1}{16} + 1 = \frac{15}{16} - \frac{i}{64}, \quad |p(i/4)|^2 = \frac{225}{256} + \frac{1}{4096} = \frac{3601}{4096} < 1.$$

The proof's bound is $1 - t^2\alpha/4 = 63/64$, and indeed $3601/4096 \leq (63/64)^2 = 3969/4096$.

The real axis. $p(1/4) = 1/64 + 1/16 + 1 = 69/64 > 1$. Moving from 0 to the right increases $|p|$; the direction $\zeta = i$ chosen by the lemma decreases it. The direction matters.

5.6.4 The theorem, and complex polynomials

Theorem 5.6.6. Fundamental Theorem of Algebra

Every non-constant $p \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.

Proof. By [Theorem 5.6.3](#) there is $z^* \in \mathbb{C}$ with $|p(z^*)| \leq |p(z)|$ for every $z \in \mathbb{C}$. Suppose $p(z^*) \neq 0$. By [Lemma 5.6.5](#), applied at $z_0 = z^*$, some z has $|p(z)| < |p(z^*)|$, a contradiction. So $p(z^*) = 0$. ■

Chapter 1 announced the theorem for expressions $\sum_{k=0}^n a_k z^k$ with $a_n \neq 0$ and $n \geq 1$. Such an expression is the value at z of the non-constant polynomial $\sum_{k=0}^n a_k x^k$ (Definition 4.4.1), so every complex polynomial expression of positive degree has a root.

Corollary 5.6.7. Complex Polynomials Split

- (a) Every non-zero $p \in \mathbb{C}[x]$ splits over $\mathbb{C}$ (Definition 5.4.2): $p = a(x - z_1) \cdots (x - z_n)$ with $n = \deg p$, a the leading coefficient of p , and $z_1, \dots, z_n \in \mathbb{C}$. The multiplicities of the roots of p add up to n .

(b) The irreducible polynomials of $\mathbb{C}[x]$ are exactly those of degree 1.

Proof.

- (a) Let $c_1, \dots, c_k$ be the distinct roots of p in $\mathbb{C}$, with multiplicities $m_1, \dots, m_k$. By Theorem 5.4.6, $p = (x - c_1)^{m_1} \cdots (x - c_k)^{m_k} g$ with $g \in \mathbb{C}[x]$ having no root in $\mathbb{C}$. Then $g \neq 0$, since $p \neq 0$, and g is constant, since a non-constant g would have a root by Theorem 5.6.6. A product of monic polynomials is monic (Theorem 4.3.2 (b)), so comparing leading coefficients, $g = a$; and comparing degrees, $\deg p = m_1 + \cdots + m_k$. Writing each power $(x - c_i)^{m_i}$ as the product of m_i factors $x - c_i$ gives the displayed form.
- (b) A polynomial of degree 1 is irreducible (the examples after Definition 5.3.1). Conversely, let p be irreducible over $\mathbb{C}$. Then $\deg p \geq 1$, so p has a root c (Theorem 5.6.6), and $p = (x - c)h$ by Theorem 5.1.3 (b). Since $x - c$ is not constant, h is a non-zero constant, and $\deg p = 1$. ■

Example. Factoring a quartic over the reals and over the complex numbers

Factor $x^4 + 1$ into linear factors over $\mathbb{C}$, and into irreducible factors over $\mathbb{R}$.

Solution. Over $\mathbb{C}$. Since $i^2 = -1$, $x^4 + 1 = x^4 - i^2 = (x^2 - i)(x^2 + i)$. The formula of Proposition 1.4.1 gives the square roots: for i ($a = 0$, $b = 1$, $r = 1$), $w_1 := \frac{\sqrt{2}}{2}(1 + i)$; for $-i$ ($b = -1$), $w_2 := \frac{\sqrt{2}}{2}(1 - i)$. Here $\sqrt{1/2} = \sqrt{2}/2$, since $\sqrt{2}/2 \geq 0$ and $(\sqrt{2}/2)^2 = 1/2$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4). Since $w_1^2 = i$ and $w_2^2 = -i$ (Proposition 1.4.1 (a)), expanding gives $x^2 - i = x^2 - w_1^2 = (x - w_1)(x + w_1)$ and $x^2 + i = x^2 - w_2^2 = (x - w_2)(x + w_2)$, so

$$x^4 + 1 = (x - w_1)(x + w_1)(x - w_2)(x + w_2).$$

Over $\mathbb{R}$. Note $w_2 = \overline{w_1}$ and $-w_2 = \overline{-w_1}$. Pair each root with its conjugate:

$$(x - w_1)(x - \overline{w_1}) = x^2 - \sqrt{2}x + 1, \quad (x + w_1)(x + \overline{w_1}) = x^2 + \sqrt{2}x + 1,$$

since $w_1 + \overline{w_1} = 2 \operatorname{Re} w_1 = \sqrt{2}$ and $w_1 \overline{w_1} = |w_1|^2 = \frac{1}{2} + \frac{1}{2} = 1$ (Theorem 1.2.2 (c)). So

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1),$$

which can be checked directly: the right side is $(x^2 + 1)^2 - 2x^2 = x^4 + 1$. Neither quadratic has a real root, since for every $c \in \mathbb{R}$, $c^2 \pm \sqrt{2}c + 1 = (c \pm \frac{\sqrt{2}}{2})^2 + \frac{1}{2} > 0$; so both are irreducible over $\mathbb{R}$ (Proposition 5.3.1 (b)). No polar form was used: only the square roots of $\pm i$.

Quick check. Factor $x^3 - 1$ over $\mathbb{R}$ and over $\mathbb{C}$.

Solution. $x^3 - 1 = (x - 1)(x^2 + x + 1)$ (Lemma 1.1.4, or expand). The quadratic has no real root, since for every $c \in \mathbb{R}$, $c^2 + c + 1 = (c + \frac{1}{2})^2 + \frac{3}{4} > 0$, so this is the factorization over $\mathbb{R}$ (Proposition 5.3.1 (b)). Over $\mathbb{C}$: a square root of -3 is $i\sqrt{3}$, and $z_{\pm} := (-1 \pm i\sqrt{3})/2$ satisfy $z^2 + z + 1 = 0$ (expand: $z_{\pm}^2 = (-1 \mp i\sqrt{3})/2$, and $z_{\pm}^2 + z_{\pm} + 1 = -1 + 1 = 0$). They are distinct roots, so $(x - z_+)(x - z_-) \mid x^2 + x + 1$ (Theorem 5.4.1); both are monic of degree 2, so they are equal, and $x^3 - 1 = (x - 1)(x - z_+)(x - z_-)$.

5.6.5 Real polynomials

A real polynomial is also a complex one, so it splits over $\mathbb{C}$. The question is what that says over $\mathbb{R}$. The answer comes from conjugation: the non-real roots of a real polynomial come in conjugate pairs, and each pair makes a real quadratic factor.

For $f = \sum_k f_k x^k \in \mathbb{C}[x]$, write $\bar{f} := \sum_k \bar{f}_k x^k$, the polynomial with conjugated coefficients. A polynomial in $\mathbb{R}[x]$ is one in $\mathbb{C}[x]$ whose coefficients are real ($\mathbb{R} \subseteq \mathbb{C}$, Proposition 1.1.1).

Proposition 5.6.8. Conjugate Roots of Real Polynomials

- (a) The map $\mathbb{C}[x] \rightarrow \mathbb{C}[x]$, $f \mapsto \bar{f}$, is a ring homomorphism (Definition 4.4.2), and $\overline{\bar{f}(z)} = f(\bar{z})$ for every $f \in \mathbb{C}[x]$ and $z \in \mathbb{C}$.
- (b) Let $f \in \mathbb{R}[x]$, $f \neq 0$, and $z \in \mathbb{C}$. Then z is a root of f if and only if $\bar{z}$ is, and $\text{mult}_{\bar{z}}(f) = \text{mult}_z(f)$.

Idea. Conjugating every coefficient is a substitution homomorphism, so it respects sums, products and powers, and it commutes with evaluation once the point is conjugated too. A real polynomial is its own conjugate; so conjugating a root, or a factorization $(x - z)^m g$, gives a root, or a factorization $(x - \bar{z})^m \bar{g}$, of the same polynomial.

Proof.

- (a) Conjugation $\mathbb{C} \rightarrow \mathbb{C}$ preserves $+$ and $\cdot$ (Theorem 1.2.2 (a), (b)) and sends 1 to 1, so it is a ring homomorphism (see also Example (Conjugation and Other Automorphisms)); followed by the constants $\mathbb{C} \rightarrow \mathbb{C}[x]$ (Theorem 4.2.4 (b)) it is a ring homomorphism $\varphi: \mathbb{C} \rightarrow \mathbb{C}[x]$, a composite of two. By Theorem 4.4.2 with $R = \mathbb{C}$, $S = \mathbb{C}[x]$ and $s = x$, the map $f \mapsto \sum_k \varphi(f_k) x^k = \bar{f}$ is a ring homomorphism. For the values, $\overline{z^k} = \bar{z}^k$ by induction with Theorem 1.2.2 (b), and then, through the sum recursion with Theorem 1.2.2 (a), (b),

$$\overline{f(z)} = \overline{\sum_k f_k z^k} = \sum_k \bar{f}_k \bar{z}^k = \bar{f}(\bar{z}).$$

For real coefficients this is the computation of Proposition 1.6.4.

- (b) The coefficients of f are real, so $\bar{f} = f$ (Proposition 1.2.1: $\bar{a} = a$ for $a \in \mathbb{R}$). By (a), $f(\bar{z}) = \bar{f}(z) = \overline{f(z)}$, and $\bar{w} = 0$ if and only if $w = 0$ ($\bar{0} = 0$ by Definition 1.2.1, and conversely $w = \bar{\bar{w}}$ by Theorem 1.2.2 (a)); so z is a root exactly when $\bar{z}$ is. Let $m := \text{mult}_z(f)$. By Lemma 5.4.4 (a), $f = (x - z)^m g$ with $g(z) \neq 0$. Apply the homomorphism of (a): $f = \bar{f} = (x - \bar{z})^m \bar{g}$, and $\bar{g}(\bar{z}) = \overline{g(z)} \neq 0$. By Lemma 5.4.4 (a) again, $\text{mult}_{\bar{z}}(f) = m$.

■

Quick check. The number $2 + i$ is a root of $x^2 - 4x + 5 \in \mathbb{R}[x]$. Name the other root without computing, and factor the polynomial over $\mathbb{C}$.

Solution. By [Proposition 5.6.8](#) (b), $\overline{2 + i} = 2 - i$ is a root. The two roots are distinct, so $(x - 2 - i)(x - 2 + i)$ divides the polynomial (Theorem 5.4.1); both are monic of degree 2, so $x^2 - 4x + 5 = (x - 2 - i)(x - 2 + i)$. (Check: the product is $(x - 2)^2 + 1$.)

Corollary 5.6.9. The Irreducible Real Polynomials

A polynomial $p \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$ if and only if $\deg p = 1$, or $\deg p = 2$ and p has no real root.

Idea. An irreducible real polynomial has a complex root z by the theorem. A real root splits off a real linear factor. A non-real root brings its conjugate along, and the two together split off the real quadratic $(x - z)(x - \bar{z})$, first in $\mathbb{C}[x]$ and then, because division does not depend on the field, in $\mathbb{R}[x]$. Irreducibility leaves nothing else.

Proof. ($\Leftarrow$) A polynomial of degree 1 is irreducible, and one of degree 2 without a root in $\mathbb{R}$ is irreducible by Proposition 5.3.1 (b).

($\Rightarrow$) Let p be irreducible over $\mathbb{R}$. Then $\deg p \geq 1$, and by [Theorem 5.6.6](#), p , as an element of $\mathbb{C}[x]$, has a root $z \in \mathbb{C}$.

Case 1: $z \in \mathbb{R}$. Then $x - z \mid p$ in $\mathbb{R}[x]$ (Theorem 5.1.3 (b), over $\mathbb{R}$), so $p = (x - z)h$ with $h \in \mathbb{R}[x]$; since $x - z$ is not constant, h is constant, and $\deg p = 1$.

Case 2: $z \notin \mathbb{R}$. Then $\bar{z} \neq z$ (Example (Conjugation and Other Automorphisms)), and $\bar{z}$ is also a root ([Proposition 5.6.8](#) (b)). So the two distinct roots give $q := (x - z)(x - \bar{z}) \mid p$ in $\mathbb{C}[x]$ (Theorem 5.4.1). By Theorem 1.2.2 (c),

$$q = x^2 - (z + \bar{z})x + z\bar{z} = x^2 - 2(\operatorname{Re} z)x + |z|^2,$$

which has real coefficients. Since $\mathbb{R}$ is a subfield of $\mathbb{C}$ (Example (Rational and Integer Complex Numbers)), Proposition 5.2.6 (b) gives $q \mid p$ in $\mathbb{R}[x]$: $p = qh$ with $h \in \mathbb{R}[x]$. Since q is not constant, h is constant, and $\deg p = 2$. Finally p has no real root: a root would make p , of degree 2, reducible (Proposition 5.3.1 (a)). This proves the corollary.

■

Theorem 5.6.10. Factorization of Real Polynomials

Let $f \in \mathbb{R}[x]$ be non-constant, with leading coefficient a . Then $f = ap_1 \cdots p_k$ for a list

$p_1, \dots, p_k$ ($k \geq 1$) of monic polynomials in $\mathbb{R}[x]$, each of the form $x - c$ with $c \in \mathbb{R}$ or a quadratic with no real root. If r entries are linear and s are quadratic, then $r + 2s = \deg f$. The list is unique up to order, in the sense of Theorem 5.3.6 (b).

Proof. By Theorem 5.3.6 (a) over $F = \mathbb{R}$, $f = a p_1 \cdots p_k$ with monic irreducible p_i , and the list is unique up to order by part (b). By Corollary 5.6.9 each p_i has degree 1, so it is $x - c$ with $c \in \mathbb{R}$ (monic), or degree 2 with no real root. Degrees add over a product (Theorem 4.3.2 (b), induction on k), so $\deg f = r \cdot 1 + s \cdot 2$. ■

When the linear entries come first in the list, the factorization reads $f = a(x - c_1) \cdots (x - c_r) q_1 \cdots q_s$, the familiar form. (Reordering a list does not change its product, by repeated use of commutativity; nothing below needs this.) For $x^4 + 1$, $r = 0$ and $s = 2$ (Example (Factoring a quartic over the reals and over the complex numbers)).

Corollary 5.6.11. Real Polynomials of Odd Degree Have a Real Root

Every $f \in \mathbb{R}[x]$ of odd degree has a root in $\mathbb{R}$.

Proof. Factor $f = a p_1 \cdots p_k$ as in Theorem 5.6.10, with $r + 2s = \deg f$. If $r = 0$, then $\deg f = 2s$ is even, which an odd number is not (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Corollary 3.1.3 (a)). So $r \geq 1$: some $p_i = x - c$ with $c \in \mathbb{R}$. By (L2) of Section 5.3, $x - c$ divides $p_1 \cdots p_k$, hence divides $f = a p_1 \cdots p_k$ (Proposition 5.1.1 (b)), so $f(c) = 0$ by Theorem 5.1.3 (b). ■

Quick check. A real cubic f has exactly one real root c . What are r , s and $\text{mult}_c(f)$?

Solution. Every linear entry $x - c'$ divides f , so c' is a real root (Theorem 5.1.3 (b)); hence each linear entry is $x - c$. Then $r + 2s = 3$ is odd, so $r \geq 1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Corollary 3.1.3 (a), as in the proof of Corollary 5.6.11, and $(r, s) = (1, 1)$ or $(3, 0)$. Multiplicities add over the list (Proposition 5.4.5): a quadratic entry q has $q(c) \neq 0$, so $\text{mult}_c(q) = 0$, and $\text{mult}_c(f) = r$, which is 1 or 3. Examples: $x(x^2 + 1)$ and x^3 .

Warning. Beyond degree 2, “no real root” does not make a real polynomial irreducible. The polynomial $x^4 + 1$ has no real root, since $c^4 + 1 = (c^2)^2 + 1 \geq 1$ for every $c \in \mathbb{R}$, yet it is the product of two real quadratics (Example (Factoring a quartic over the reals and over the complex numbers)). Corollary 5.6.9 says that every irreducible real polynomial has degree at most 2; so a real polynomial of degree 4 or more is always reducible, root or no root.

Remark (Looking ahead). *Analysis on the Real Line*, Chapter 6 proves the intermediate value theorem for continuous functions on an interval. With it, the odd-degree corollary has a second proof that uses no complex numbers: a real polynomial of odd degree takes values of both signs.

5.6.6 Exercises

5.6.6.1 A. Check your understanding

Exercise. A1

These parts are about the proof of [Theorem 5.6.3](#).

- Where is the completeness of $\mathbb{R}$ used?
- Why does Step 3 take “the **first** quarter in a fixed order” with the same infimum, rather than “a quarter” with the same infimum?
- Run Steps 1–4 for $p = x^2 + 1$: find ρ , S_0 , m , S_1 and S_2 .
- Give the idea of the proof in two sentences.

Solution.

- Directly, twice: in Step 2, for the existence of each infimum $m(S)$, and in Step 5, for the suprema σ^* and τ^* that give the common point. Indirectly, through the real square roots behind the modulus (Definition 1.2.1, built on Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4), which every inequality of the proof uses.
- “A quarter with the same infimum” exists, but there may be several, and naming one at each of infinitely many stages without a rule is a use of the axiom of choice. “The first one in a fixed order” is a rule, a function q from squares to squares, so Sets, Relations, and Cardinality, Theorem 2.3.1 defines the whole sequence (S_k) at once.
- Here $a_0 = 1$, $a_1 = 0$, $a_2 = 1$, so $A = 1$, $R = \max\{1, 2\} = 2$, and $2|p(0)|/|a_2| = 2$; hence $\rho = 2$ and $S_0 = S(-2, -2, 4)$. The infimum is $m = 0$: $|p| \geq 0$, and $p(-i) = 0$ with $-i \in S_0$. The first quarter of S_0 is $S(-2, -2, 2)$, which contains $-i$ (real part $0 \in [-2, 0]$, imaginary part $-1 \in [-2, 0]$); so its infimum is $0 = m$, and $S_1 = S(-2, -2, 2)$. The quarters of S_1 have side 1. The first, $S(-2, -2, 1)$, has no point with $|p|$ small: for $z = a + bi$ in it, $a, b \in [-2, -1]$, so $|p(z)| \geq |\operatorname{Im}(z^2 + 1)| = |2ab| \geq 2$ (Lemma 1.3.1), and its infimum is at least $2 > 0$. The second, $S(-1, -2, 1)$, contains $-i$, so its infimum is 0, and $S_2 = S(-1, -2, 1)$.
- The infimum of $|p|$ over a big square is what we want to attain; halving keeps a quarter with the same infimum, chosen by a rule. The squares shrink to one point, and the Lipschitz bound forces the value there to be the infimum.

5.6.6.2 B. Practice

Exercise. B1

Factor $x^4 - x^2 - 2$ into irreducible factors over $\mathbb{Q}$, over $\mathbb{R}$ and over $\mathbb{C}$. Then factor $x^4 + 4$ over $\mathbb{R}$ and over $\mathbb{C}$.

Solution. $x^4 - x^2 - 2$. Expanding shows $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$. Over $\mathbb{Q}$: $x^2 - 2$ has no rational root (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1) and $x^2 + 1$ has none ($c^2 + 1 > 0$, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)), so both are irreducible (Proposition 5.3.1 (b)), and the factorization is $(x^2 - 2)(x^2 + 1)$. Over $\mathbb{R}$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4), while $x^2 + 1$ still has no real root: $(x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)$. Over $\mathbb{C}$: $x^2 + 1 = (x - i)(x + i)$, so $(x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i)$.

$x^4 + 4$. By the warning of Section 5.3, $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$, and $c^2 \pm 2c + 2 = (c \pm 1)^2 + 1 > 0$ for every $c \in \mathbb{R}$; so this is the factorization over $\mathbb{R}$ (Corollary 5.6.9). Over $\mathbb{C}$: $-1 \pm i$ are the roots of $x^2 + 2x + 2$ ($(-1 + i)^2 = -2i$, and $-2i + 2(-1 + i) + 2 = 0$; then its conjugate, by Proposition 5.6.8 (b)), and $1 \pm i$ those of $x^2 - 2x + 2$ likewise. So $x^4 + 4 = (x + 1 - i)(x + 1 + i)(x - 1 - i)(x - 1 + i)$, each quadratic being the product of its two distinct linear factors (Theorem 5.4.1, monic and of the same degree).

Exercise. B2

Run the proof of Lemma 5.6.5 for $p = x^3 - 2$ at $z_0 = 1$: find $b_0, \dots, b_3, k, c, \zeta, u, \alpha, B, t$ and the new point z , and compare $|p(z)|$ with $|p(1)|$.

Solution. *Expansion around 1.* Writing $x = (x - 1) + 1$ and expanding, $x^3 = (x - 1)^3 + 3(x - 1)^2 + 3(x - 1) + 1$, so

$$x^3 - 2 = -1 + 3(x - 1) + 3(x - 1)^2 + (x - 1)^3,$$

and by the uniqueness in Theorem 5.4.3, $(b_0, b_1, b_2, b_3) = (-1, 3, 3, 1)$. So $k = 1$ and $c = b_1/b_0 = -3$.

Direction. $k = 1$ is odd and $\operatorname{Re} c = -3 \neq 0$; $\zeta = 1$ gives $\operatorname{Re}(c\zeta) = -3 < 0$. So $u = -3$, $\alpha = 3$, $|u|^2 = 9$.

Constants. $B = |b_2/b_0||\zeta|^2 + |b_3/b_0||\zeta|^3 = 3 + 1 = 4$, and

$$t = \min\left\{1, \frac{3}{9}, \frac{3}{16}\right\} = \frac{3}{16}.$$

New point. $z = 1 + \frac{3}{16} = \frac{19}{16}$, and $p(19/16) = 6859/4096 - 2 = -1333/4096$. So $|p(z)| = 1333/4096 < 1 = |p(1)|$, well inside the proof's bound $1 - t\alpha/4 = 55/64$.

Exercise. B3

Let $f \in \mathbb{R}[x]$ have degree 5 and exactly one real root c . What can the multiplicity of c be, and how many quadratic factors without real root does f have? Give an example for each possibility.

Solution. Factor $f = ap_1 \cdots p_k$ as in [Theorem 5.6.10](#), with r linear and s quadratic entries, $r + 2s = 5$. Each linear entry $x - c'$ divides f , so c' is a real root ([Theorem 5.1.3 \(b\)](#)); hence every linear entry is $x - c$. Multiplicities add over products ([Proposition 5.4.5](#), with induction on k); $\text{mult}_c(x - c) = 1$, a quadratic entry q has $q(c) \neq 0$ and so $\text{mult}_c(q) = 0$, and the constant $a \neq 0$ has multiplicity 0. So $\text{mult}_c(f) = r$. Since $r + 2s = 5$ is odd, $r \geq 1$ ([Number Systems: From \$\mathbb{N}\$ to \$\mathbb{R}\$](#) , [Corollary 3.1.3 \(a\)](#)), as in the proof of [Corollary 5.6.11](#), so the possibilities are $(r, s) = (1, 2), (3, 1), (5, 0)$: the multiplicity of c is 1, 3 or 5, with 2, 1 or 0 quadratic factors. Examples with $c = 0$: $x(x^2 + 1)^2, x^3(x^2 + 1), x^5$. Each has only the real root 0, since $t^2 + 1 > 0$ for every $t \in \mathbb{R}$.

5.6.6.3 C. Going deeper

Exercise. C1: Exit check: the descent and the theorem

- (a) Prove [Lemma 5.6.5](#) from [Lemma 5.6.4](#) and [Theorem 5.4.3](#).
- (b) Deduce [Theorem 5.6.6](#) from (a) and [Theorem 5.6.3](#).
- (c) The field $\mathbb{Q}(i)$ of Example (Rational and Integer Complex Numbers) satisfies the field axioms, and $x^2 - 2$ has no root in it. Say which steps of the whole proof fail when $\mathbb{R}$ is replaced by $\mathbb{Q}$ and $\mathbb{C}$ by $\mathbb{Q}(i)$, and why $x^2 - 2$ shows that some step must fail.

Solution (Hint 1). Expand p around z_0 and divide by $p(z_0)$. Which coefficient after the constant one decides what happens near z_0 ?

Solution (Hint 2). Let k be the least $j \geq 1$ with $b_j \neq 0$, and fix a real t with $0 < t \leq 1$ before estimating $|p(z_0 + t\zeta)|$.

Solution.

- (a) Let $n := \deg p \geq 1$. By [Theorem 5.4.3](#), $p = \sum_{j=0}^n b_j(x - z_0)^j$ with $b_0 = p(z_0) \neq 0$ and $b_n \neq 0$; let k be the least $j \geq 1$ with $b_j \neq 0$ ([Sets, Relations, and Cardinality](#), [Theorem 2.1.3](#); n is such a j). Let $c := b_k/b_0$, take ζ with $\text{Re}(c\zeta^k) < 0$ ([Lemma 5.6.4](#)), and put $u := c\zeta^k$, $\alpha := -\text{Re } u > 0$ (so $0 < \alpha \leq |u|$), $B := \sum_{j=k+1}^n |b_j/b_0||\zeta|^j$, and

$$t := \min\{1, \alpha/|u|^2, \alpha/(4B)\}$$

(the last entry omitted if $B = 0$). Then $p(z_0 + t\zeta) = b_0(1 + t^k u + E)$ with $|E| \leq t^{k+1}B$, since $b_j = 0$ for $1 \leq j < k$ and $t^j \leq t^{k+1}$ for $j > k$. With $s := t^k \leq t \leq \alpha/|u|^2$,

$$|1 + su|^2 = 1 - 2s\alpha + s^2|u|^2 \leq 1 - s\alpha \leq (1 - s\alpha/2)^2,$$

and $1 - s\alpha/2 > 0$ because $s\alpha \leq \alpha^2/|u|^2 \leq 1$ (as $\alpha \leq |u|$); two non-negative reals are ordered as their squares ([Number Systems: From \$\mathbb{N}\$ to \$\mathbb{R}\$](#) , [Proposition 2.3.5 \(g\)](#)), so $|1 + su| \leq 1 - s\alpha/2$. Using $tB \leq \alpha/4$,

$$|p(z_0 + t\zeta)| \leq |b_0|(1 - t^k\alpha/2 + t^{k+1}B) \leq |b_0|(1 - t^k\alpha/4) < |b_0|.$$

- (b) Let p be non-constant. By [Theorem 5.6.3](#), some z^* has $|p(z^*)| \leq |p(z)|$ for all z . If $p(z^*) \neq 0$, (a) gives z with $|p(z)| < |p(z^*)|$: a contradiction. So $p(z^*) = 0$.
- (c) Completeness fails in $\mathbb{Q}$, and with it two kinds of step. *The infimum and the supremum.* Step 2 of [Theorem 5.6.3](#) needs the infimum of a set of values, and Step 5 the supremum of the corners σ_k ; in $\mathbb{Q}$ a bounded set need not have either (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), [Theorem 2.6.2](#): the positive rationals q with $q^2 < 2$ have no rational supremum). *The square roots.* The modulus $\sqrt{a^2 + b^2}$ need not be rational ($|1+i| = \sqrt{2}$), and the square roots of [Proposition 1.4.1](#), used in Case 2 of [Lemma 5.6.4](#), need real square roots. The polynomial $x^2 - 2$ is non-constant with coefficients in $\mathbb{Q}(i)$ and no root there (the opening of this section), so the theorem is false for $\mathbb{Q}(i)$; a proof that went through unchanged would prove a falsehood, so some step must fail. In fact the failure for $x^2 - 2$ is exactly a missing square root: its roots in $\mathbb{C}$ are $\pm\sqrt{2}$.

Marking scheme. (10 points)

- 2: re-centers at z_0 with $b_0 = p(z_0) \neq 0$, and takes k to be the first index $j \geq 1$ with $b_j \neq 0$, with a reason that it exists.
- 1: obtains a direction ζ with $\operatorname{Re}(c\zeta^k) < 0$ from [Lemma 5.6.4](#).
- 2: proves that the leading term decreases by a definite amount: $|1 + su| \leq 1 - \kappa s$ or $|1 + su|^2 \leq 1 - \kappa s$ (or the same kind of bound for $|1 + su + E|^2$ directly), with an explicit $\kappa > 0$ (for example $\kappa = \alpha/2$, resp. α), for all s in an explicit range such as $0 < s \leq \alpha/|u|^2$.
- 2: bounds the tail by $t^{k+1}B$ and fixes t explicitly before the estimate that uses it.
- 2: concludes $|p(z_0 + t\zeta)| < |p(z_0)|$, and derives the theorem by contradiction with the minimum.
- 1: (c) names both uses of completeness (the infimum of Step 2, with the supremum of Step 5; the real square roots behind the modulus and behind the complex square roots of the direction lemma), and says why $x^2 - 2$ forces a failure.

Fatal errors (0 for the step): choosing t after the inequality that needs it, or letting it depend on the point being estimated; assuming the minimum exists without citing [Theorem 5.6.3](#); using polar form or k -th roots of complex numbers, which this chapter does not have (a k -th root is accepted only with a proof). A proof that obtains the direction by polar form, if the reader has it from elsewhere, earns the 1 point of the direction step only together with a proof of the k -th root it uses.

Exercise. C2: Faded: the real polynomials vanishing at a non-real number

Let $\alpha \in \mathbb{C}$ with $\alpha \notin \mathbb{R}$, and let $J := \{f \in \mathbb{R}[x] : f(\alpha) = 0\}$, evaluating in $\mathbb{C}$. You are given only: J is an ideal of $\mathbb{R}[x]$, and $q := x^2 - 2(\operatorname{Re} \alpha)x + |\alpha|^2 \in J$. Name the move, then complete it: show that $J = \langle q \rangle$ and that q is irreducible over $\mathbb{R}$.

Solution. The move is **least degree, then divide**, as in [Theorem 5.2.1](#). Since $q \neq 0$ is in J , the degrees of the non-zero elements of J form a non-empty subset of $\mathbb{N}$; let $e \in J$ have the least degree ([Sets, Relations, and Cardinality](#), [Theorem 2.1.3](#)), and let d be its monic associate, which is in J because J is an ideal. Divide q by d : $q = hd + r$ with $\deg r < \deg d$ ([Theorem 5.1.2](#)). Then $r = q - hd \in J$, and a non-zero r would have smaller degree than the least; so $r = 0$ and $d \mid q$.

The degree of d . A non-zero constant does not vanish at α , so $\deg d \geq 1$. If $\deg d = 1$, then

$d = x - c$ with $c \in \mathbb{R}$, and $d(\alpha) = 0$ gives $\alpha = c \in \mathbb{R}$, which is excluded. So $\deg d \geq 2$, and since $d \mid q$ with $\deg q = 2$, $\deg d = 2$ (Proposition 5.1.1 (d)). Then $q = hd$ with $\deg h = 0$, and comparing leading coefficients of the monic q and d , $h = 1$: $d = q$.

$J = \langle q \rangle$. Multiples of q are in J . For $f \in J$, divide: $f = gq + r$ with $\deg r < 2$; $r = f - gq \in J$, and a non-zero element of J has degree at least 2; so $r = 0$ and $f \in \langle q \rangle$.

Irreducible. If $q = gh$ with $g, h \in \mathbb{R}[x]$ non-constant, both have degree 1, and $0 = q(\alpha) = g(\alpha)h(\alpha)$ (Theorem 4.4.1), so $g(\alpha) = 0$ or $h(\alpha) = 0$ (Theorem 2.1.1 (f)): an element of J of degree 1, which was just excluded. So q is irreducible.

Exercise. C3: Find the error

Here is an argument.

Claim. For every non-constant $p \in \mathbb{C}[x]$, $|p|$ attains a minimum on $\mathbb{C}$.

Proof. (1) Let $m := \inf\{|p(z)| : z \in \mathbb{C}\}$, which exists since the set is non-empty and bounded below by 0. (2) For each $k \geq 1$, pick $z_k \in \mathbb{C}$ with $|p(z_k)| < m + 1/k$. (3) Since $|p(z_k)| < m + 1 \leq |p(0)| + 1$, Lemma 5.6.1 puts the z_k in a bounded set. (4) So they converge to some $z^* \in \mathbb{C}$. (5) Then $|p(z^*)| = \lim |p(z_k)| = m$.

Is the claim true? Does the argument prove it? Name the line that fails and the reason, give a counterexample to the illegal step, and say how the proof in the text avoids it.

Solution (Hint 1). For each line, ask which result of this volume or of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* justifies it.

Solution (Hint 2). Is every bounded sequence of real numbers convergent?

Solution. **The claim is true:** it is Theorem 5.6.3. **The argument does not prove it.**

Line (4) fails. “The z_k lie in a bounded set, so they converge” uses a general “fact” that is neither proved here nor true: entry (N9) of Logic and Proof, Example (What is not allowed). Counterexample to the step: $z_k := (-1)^k$ lies in the bounded set $\{z : |z| \leq 1\}$ and does not converge. (What is true, that a bounded sequence has a convergent **subsequence**, is not available in this volume; and the subsequence would still have to be chosen by a rule.) There is no counterexample to the conclusion.

Two further slips. Line (2) picks infinitely many z_k with no rule given, which is a use of the axiom of choice (compare Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Picking Representatives Is a Use of Choice)). Line (5) moves $|p|$ past a limit, which needs continuity; Lemma 5.6.2 would supply it, but the line cites nothing.

The repair is the bisection of Theorem 5.6.3: it chooses squares by a rule (“the first quarter with the same infimum”), finds the common point as a supremum of corners, and replaces the limit by the Lipschitz estimate of Step 6. No sequence is ever asked to converge.

Marking scheme. (10 points)

- 2: says the claim is true and the argument, as written, does not prove it.
- 3: names line (4) and the reason: “bounded implies convergent” is unproved and false, (N9).
- 2: a counterexample to the step, such as $z_k = (-1)^k$.
- 1: names one further slip: the rule-less choice in line (2), or the unproved continuity in line (5).
- 2: describes the repair: squares chosen by a rule, the common point from completeness, the Lipschitz bound in place of a limit.

Fatal errors (0 for the step): a counterexample to the conclusion (there is none); “repairing” line (4) by citing Bolzano–Weierstrass as if it were proved in this volume.

5.6.6.4 R. Review

Exercise. R1

Let F be a field. Show that there are no non-zero $f, g \in F[x]$ with $f^2 = xg^2$.

Solution. This uses the degree of a product from Chapter 4 (Theorem 4.3.2 (b)), which holds over a field since a field has no zero divisors. Suppose $f, g \neq 0$ and $f^2 = xg^2$. Then $\deg(f^2) = 2 \deg f$, and $\deg(xg^2) = 1 + 2 \deg g$. So the natural number $2 \deg f$ would equal $2 \deg g + 1$: even and odd at once, which Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.1.3 (a) rules out. Hence no such f, g exist.

Exercise. R2

In $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$, show that every non-zero class $[a + bx]$ ($a, b \in \mathbb{Q}$) is a unit, by multiplying it by $[a - bx]$. Compute $[1 + x]^{-1}$.

Solution. In $\mathbb{Q}[x]$, $(a + bx)(a - bx) = a^2 - b^2x^2 = (a^2 - 2b^2) - b^2(x^2 - 2)$, so $[a + bx][a - bx] = [a^2 - 2b^2]$. If $(a, b) \neq (0, 0)$, the rational number $N := a^2 - 2b^2$ is non-zero: if $b = 0$, then $N = a^2 \neq 0$; if $b \neq 0$, then $N = 0$ would give $(a/b)^2 = 2$, against Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1. So $[a + bx] \cdot [N^{-1}(a - bx)] = [1]$, and $[a + bx]$ is a unit. Every class is $[a + bx]$ for exactly one pair (Theorem 5.5.2 (b)), and the zero class is the pair $(0, 0)$, so every non-zero class is a unit: $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ is a field, as Theorem 5.5.3 also says ($x^2 - 2$ is irreducible over $\mathbb{Q}$). For $1 + x$: $N = 1 - 2 = -1$, so $[1 + x]^{-1} = [-(1 - x)] = [x - 1]$. Check: $(1 + x)(x - 1) = x^2 - 1 = 1 + (x^2 - 2)$.

This is the computation of Example (The Field Generated by the Square Root of Two) in Chapter 2, “multiply by the conjugate”, with $[x]$ in place of $\sqrt{2}$: the class $[a + bx]$ behaves as $a + b\sqrt{2}$, and $(1 + \sqrt{2})^{-1} = \sqrt{2} - 1$.

Exercise. R3

Let $m, n \in \mathbb{Z}_{>0}$. Prove that $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m, n)} - 1$ in $\mathbb{Z}$.

Solution. The method is the integer Euclidean step of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Lemma 3.2.3), used on the exponents and on the numbers at once. We prove the claim for all $m, n \geq 1$ by strong induction on $m + n$ (Logic and Proof, Theorem 4.2.2).

If $m = n$, both sides are $2^m - 1$: the gcd of a positive integer with itself is that integer (it divides both, and every common divisor is at most it, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.2.2), and $\gcd(m, m) = m$. If $m > n$, then

$$2^m - 1 = 2^{m-n}(2^n - 1) + (2^{m-n} - 1),$$

and $2^n - 1 > 0$, so Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 3.2.3 gives $\gcd(2^m - 1, 2^n - 1) = \gcd(2^n - 1, 2^{m-n} - 1)$. Likewise $m = 1 \cdot n + (m - n)$ gives $\gcd(m, n) = \gcd(n, m - n)$. Since $n + (m - n) = m < m + n$ and $m - n \geq 1$, the induction hypothesis gives $\gcd(2^n - 1, 2^{m-n} - 1) = 2^{\gcd(n, m-n)} - 1 = 2^{\gcd(m, n)} - 1$. If $m < n$, exchange the roles (the gcd is symmetric). For example, $\gcd(2^{12} - 1, 2^{18} - 1) = \gcd(4095, 262143) = 63 = 2^6 - 1$.

This is the integer twin of Exercise C3 of Section 5.2 (Exercise (C3: The gcd of two binomials)), where $x^m - 1$ and $x^n - 1$ play the parts of $2^m - 1$ and $2^n - 1$.

Exercise. R4

Is $x^4 + x + 1$ irreducible over $\mathbb{F}_2$?

Solution. Yes. The tool is a degree count over a finite field: list the possible factorizations and check each.

The values are $0+0+1 = 1$ at 0 and $1+1+1 = 1$ at 1, so $f := x^4 + x + 1$ has no root in $\mathbb{F}_2$, and hence no factor of degree 1 (Theorem 5.1.3 (c)). A factorization into non-constant factors would then be $f = gh$ with $\deg g = \deg h = 2$. Over $\mathbb{F}_2$ the only non-zero constant is 1, so g and h are monic. A root of g or h would be a root of f , so both are rootless quadratics, hence irreducible (Proposition 5.3.1 (b)). The monic quadratics over $\mathbb{F}_2$ are x^2 , $x^2 + 1 = (x + 1)^2$, $x^2 + x = x(x + 1)$ and $x^2 + x + 1$; only the last is rootless. So $g = h = x^2 + x + 1$, and $gh = x^4 + 2x^3 + 3x^2 + 2x + 1 = x^4 + x^2 + 1 \neq f$ in $\mathbb{F}_2[x]$. So f is irreducible.

Look-alikes that fail. “No root, hence irreducible” (Proposition 5.3.1) applies only in degrees 2 and 3; in degree 4 it is the error of Exercise C2 of Section 5.3, and $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ is a rootless reducible quartic over $\mathbb{F}_2$. The rational root test (Theorem 5.3.7) is about $\mathbb{Q}$, not $\mathbb{F}_2$. Eisenstein’s criterion is not in this volume.