

6.5 The Fundamental Theorem of Algebra

Chapter 0 stated the Fundamental Theorem of Algebra (Theorem 0.6.7) and promised a proof. Everything algebraic that the proof needs is now in place: division, the Factor Theorem, multiplicities, and the polar form of complex numbers with De Moivre's formula. What algebra alone cannot supply is a property of the real numbers that goes beyond the field axioms, and some such property must enter, because $\mathbb{Q}$ is a field too and there $x^2 - 2$ has no root. We use completeness, in the form of the extreme value theorem. This section isolates the analytic input in two clearly labeled facts, proves everything else in full, and then draws the consequences for real polynomials: conjugate pairs, irreducible factors of degree at most 2, and real roots of odd-degree polynomials.

6.5.1 The goal and the plan

Here is the theorem we want, in the language of this chapter. A polynomial $p \in \mathbb{C}[x]$ of degree $n \geq 1$ is exactly the expression $a_n x^n + \cdots + a_0$ with $a_n \neq 0$ of Theorem 0.6.7.

Theorem 6.5.1. Fundamental Theorem of Algebra

Every nonconstant polynomial $p \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.

We prove it after three lemmas. The proof is a minimum argument, and it runs in three steps.

- ① **Growth.** Far from the origin, $|p(z)|$ is large, because the leading term $a_n z^n$ outweighs all the others. We will prove this with an explicit radius.
- ② **A minimum exists.** On a large closed disc, the continuous function $z \mapsto |p(z)|$ attains a smallest value. By ①, nothing outside the disc does better, so this is the smallest value of $|p|$ on all of $\mathbb{C}$.
- ③ **A nonzero value is never the minimum.** If $p(z_0) \neq 0$, we can move from z_0 a little in a well-chosen direction and make $|p|$ strictly smaller. This is d'Alembert's lemma, and it is pure algebra of $\mathbb{C}$.

Putting ② and ③ together, the minimum value must be 0, and the point where it is attained is a root.

Steps ① and ③ are proved from scratch. Step ② is where analysis enters, and we say exactly how.

Remark. What we assume from analysis. The proof uses exactly two facts from real analysis, and nothing else: no limits, no derivatives, no intermediate value theorem. We identify $\mathbb{C}$ with $\mathbb{R}^2$ as in Definition 0.6.1, so that $|z - w|$ is the usual distance in the plane.

- (A1) **Continuity of polynomial functions.** For every $p \in \mathbb{C}[x]$, the function $\mathbb{C} \rightarrow \mathbb{R}$, $z \mapsto |p(z)|$, is continuous.
- (A2) **Extreme value theorem on a closed disc.** Let $\rho \geq 0$ and $D = \{z \in \mathbb{C} : |z| \leq \rho\}$. If $g: D \rightarrow \mathbb{R}$ is continuous, then there is $w \in D$ with $g(w) \leq g(z)$ for **every** $z \in D$.

Fact (A2) is where the completeness of $\mathbb{R}$ is used. Everything else below is the arithmetic of $\mathbb{C}$ from Chapter 0, including polar form and Theorem 0.6.6.

6.5.2 Step 1: growth

We use three small facts about the modulus repeatedly. For $z, w, z_1, \dots, z_m \in \mathbb{C}$ and $j \in \mathbb{N}$:

$$|z^j| = |z|^j, \quad |z_1 + \dots + z_m| \leq |z_1| + \dots + |z_m|, \quad |z + w| \geq |z| - |w|.$$

The first follows from Theorem 0.6.2 (d) by induction on j , and the second from Theorem 0.6.4 by induction on m . For the third, apply the triangle inequality to $z = (z + w) + (-w)$ and use $|-w| = |w|$.

The leading term wins as soon as $|z|$ exceeds a radius computed from the coefficients.

Lemma 6.5.2. Growth of a Polynomial

Let $p = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ with $n \geq 1$ and $a_n \neq 0$. Put

$$A = |a_0| + |a_1| + \dots + |a_{n-1}|, \quad R = \max\left\{1, \frac{2A}{|a_n|}\right\}.$$

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 particular, for every real $M \geq 0$, we have $|p(z)| > M$ whenever $|z| \geq R$ and $|z| > 2M/|a_n|$.

Idea. Compare the leading term with the rest. When $|z| \geq 1$, every lower power $|z|^j$ is at most $|z|^{n-1}$, so the rest is at most $A|z|^{n-1}$, while the leading term is $|a_n||z|^n$. The rest is at most half the leading term once $A \leq \frac{1}{2}|a_n||z|$, which is how R was found.

Proof. Let $|z| \geq R$. Since $|z| \geq 1$, we have $|z|^j \leq |z|^{n-1}$ for $0 \leq j \leq n-1$. By the triangle inequality (Theorem 0.6.4),

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

Since $|z| \geq 2A/|a_n|$, we have $A \leq \frac{1}{2}|a_n||z|$. By the reverse triangle inequality,

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

Since $|z| \geq 1$ and $n \geq 1$, $|z|^n \geq |z|$, which gives the second inequality. Finally, if also $|z| > 2M/|a_n|$, then $|p(z)| \geq \frac{1}{2}|a_n||z| > M$. This proves the lemma. ■

For example, for $p = x^3 - 5x + 1$ we get $A = 6$ and $R = 12$, so $|p(z)| \geq \frac{1}{2}|z|^3$ whenever $|z| \geq 12$. The radius is far from optimal, and it does not need to be. We only need **some** radius beyond which $|p|$ is large.

6.5.3 Step 2: the minimum is attained

Lemma 6.5.3. The Minimum of $|p|$ Is Attained

Let $p \in \mathbb{C}[x]$. Then there is $z_0 \in \mathbb{C}$ with $|p(z_0)| \leq |p(z)|$ for **every** $z \in \mathbb{C}$.

Idea. Use (A2) on a disc so big that outside it, $|p|$ exceeds $|p(0)|$. The disc contains 0, so its minimum is at most $|p(0)|$, and the points outside cannot compete. Lemma 6.5.2 tells us how big “so big” is.

Proof. If p is constant, every z_0 works. Suppose $p = a_n x^n + \cdots + a_0$ with $n \geq 1$ and $a_n \neq 0$, and let R be the radius of Lemma 6.5.2. Put $M = |p(0)|$ and

$$\rho = R + \frac{2M}{|a_n|}, \quad D = \{z \in \mathbb{C} : |z| \leq \rho\}.$$

By (A1), $z \mapsto |p(z)|$ is continuous on D , so by (A2) there is $z_0 \in D$ with $|p(z_0)| \leq |p(z)|$ for every $z \in D$.

Now let $z \notin D$, so $|z| > \rho$. Then $|z| > R$, and $|z| > 2M/|a_n|$ because $R \geq 1 > 0$. By Lemma 6.5.2, $|p(z)| > M = |p(0)|$. Since $0 \in D$, $|p(0)| \geq |p(z_0)|$. Hence $|p(z)| > |p(z_0)|$ for $z \notin D$, and $|p(z)| \geq |p(z_0)|$ for $z \in D$. This proves the lemma. ■

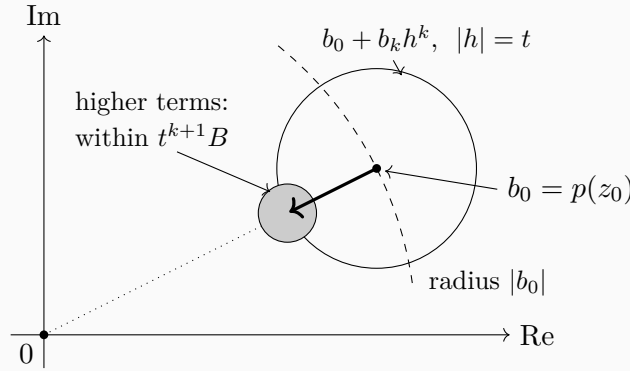
6.5.4 Step 3: d’Alembert’s lemma

It remains to show that a nonzero value of $|p|$ is never the smallest one. Near z_0 , write $p(z_0 + h) = b_0 + b_k h^k + (\text{terms of higher degree in } h)$, where $b_0 = p(z_0)$ and $b_k h^k$ is the first nonconstant term that is actually present. For small h , the term $b_k h^k$ dominates the later ones, so we choose the direction of h to make $b_k h^k$ point from b_0 straight toward 0.

Lemma 6.5.4. d’Alembert’s Lemma

Let $p \in \mathbb{C}[x]$ be nonconstant, 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. Picture the values $p(z_0 + h)$ in the plane. As $h = tu$ runs over a small circle $|h| = t$, the term $b_0 + b_k h^k$ runs k times around the circle of radius $t^k |b_k|$ centered at $b_0 = p(z_0)$. One point of that circle lies on the segment from b_0 to 0, at distance $|b_0| - t^k |b_k|$ from 0. Reaching it needs a k -th root of a unit complex number, which De Moivre supplies. The higher terms move the value by at most a multiple of t^{k+1} , a blur much smaller than the gain $t^k |b_k|$ when t is small.



The dashed arc is part of the circle of radius $|b_0|$ about 0, the old value of $|p|$. The solid circle shows where $b_0 + b_k h^k$ goes for $|h| = t$. The arrow is the chosen direction, and the shaded disc is the uncertainty caused by the higher terms. The whole shaded disc lies strictly inside the dashed circle, which is the inequality $|p(z_0 + h)| < |p(z_0)|$.

Proof. Let $n = \deg p \geq 1$.

Step 1: re-center at z_0 . By Theorem 6.4.7 (a), $(1, x - z_0, \dots, (x - z_0)^n)$ is a basis of $\mathbb{C}[x]_{\leq n}$, so $p = \sum_{j=0}^n b_j (x - z_0)^j$ for some $b_0, \dots, b_n \in \mathbb{C}$. Evaluating at z_0 gives $b_0 = p(z_0) \neq 0$. The coefficient of x^n on the right is b_n , since $(x - z_0)^j$ has degree j and $(x - z_0)^n$ is monic; so b_n is the leading coefficient of p , and $b_n \neq 0$. By Theorem 0.8.5, for every $h \in \mathbb{C}$,

$$p(z_0 + h) = \sum_{j=0}^n b_j h^j.$$

Since $b_n \neq 0$ and $n \geq 1$, there is a **smallest** $k \geq 1$ with $b_k \neq 0$. Then $b_1 = \dots = b_{k-1} = 0$, and

$$p(z_0 + h) = b_0 + b_k h^k + \sum_{j=k+1}^n b_j h^j. \quad (*)$$

Step 2: choose the direction. Since $b_0 \neq 0$ and $b_k \neq 0$, the number $w = -b_0/b_k$ is nonzero. Write it in polar form, $w = |w|e^{i\alpha}$ with $\alpha \in \mathbb{R}$, and put $u = e^{i\alpha/k}$. Then $|u| = 1$, and $u^k = e^{i\alpha}$ by Theorem 0.6.6. Using $b_k w = -b_0$ and $|w| = |b_0|/|b_k|$ (Theorem 0.6.2 (d)),

$$b_k u^k = \frac{b_k w}{|w|} = -\frac{|b_k|}{|b_0|} b_0.$$

Hence, for every real $t > 0$,

$$b_0 + b_k (tu)^k = b_0 \left(1 - t^k \frac{|b_k|}{|b_0|}\right).$$

Step 3: choose the size. Put $B = |b_{k+1}| + \dots + |b_n|$ (so $B = 0$ if $k = n$), and

$$t = \min \left\{ 1, \frac{|b_0|}{|b_k|}, \frac{|b_k|}{2B} \right\},$$

where the last entry is omitted if $B = 0$. Then $t > 0$, and t has three properties.

- (i) $0 < t^k |b_k|/|b_0| \leq 1$. Indeed, if $|b_0|/|b_k| \geq 1$, then $t^k \leq 1 \leq |b_0|/|b_k|$; otherwise $t \leq |b_0|/|b_k| < 1$, and $t^k \leq t \leq |b_0|/|b_k|$.
- (ii) $tB \leq \frac{1}{2}|b_k|$. This is trivial if $B = 0$, and follows from $t \leq |b_k|/(2B)$ otherwise.
- (iii) $t^j \leq t^{k+1}$ for every $j \geq k+1$, since $0 < t \leq 1$.

Step 4: estimate. Let $z = z_0 + tu$. By Step 2 and (i), the number $1 - t^k |b_k|/|b_0|$ is real and lies in $[0, 1)$, so

$$|b_0 + b_k(tu)^k| = |b_0| \left(1 - t^k \frac{|b_k|}{|b_0|}\right) = |b_0| - t^k |b_k|.$$

By the triangle inequality (Theorem 0.6.4), $|u| = 1$ and (iii),

$$\left| \sum_{j=k+1}^n b_j(tu)^j \right| \leq \sum_{j=k+1}^n |b_j| t^j \leq t^{k+1} B.$$

Combining these with (*), the triangle inequality, and (ii),

$$|p(z)| \leq |b_0| - t^k |b_k| + t^{k+1} B = |b_0| - t^k (|b_k| - tB) \leq |b_0| - \frac{1}{2} t^k |b_k| < |b_0|,$$

where the last step uses $t > 0$ and $b_k \neq 0$. Since $|b_0| = |p(z_0)|$, this proves the lemma. ■

Every hypothesis did a job. Nonconstant gave the index k . The condition $p(z_0) \neq 0$ let us divide by $|b_0|$ and fix a direction toward 0. And the field $\mathbb{C}$ supplied the k -th root u , the one step that has no analogue over $\mathbb{R}$.

Example. One Step Downhill

Let $p = x^3 + x^2 + 1 \in \mathbb{C}[x]$ and $z_0 = 0$. Follow the proof of [Lemma 6.5.4](#) to find z with $|p(z)| < |p(0)|$.

Solution. Here $p(0) = 1$ and the expansion at $z_0 = 0$ is p itself: $b_0 = 1$, $b_1 = 0$, $b_2 = 1$, $b_3 = 1$. The first nonzero b_j with $j \geq 1$ is b_2 , so $k = 2$ and $B = |b_3| = 1$.

Direction: $w = -b_0/b_2 = -1 = e^{i\pi}$, so $\alpha = \pi$ and $u = e^{i\pi/2} = i$. Indeed $b_2 u^2 = -1$ points from $b_0 = 1$ toward 0.

Size: $t = \min\{1, 1/1, 1/(2 \cdot 1)\} = \frac{1}{2}$. So $z = \frac{i}{2}$, and

$$p\left(\frac{i}{2}\right) = -\frac{i}{8} - \frac{1}{4} + 1 = \frac{3}{4} - \frac{i}{8}, \quad \left|p\left(\frac{i}{2}\right)\right| = \sqrt{\frac{9}{16} + \frac{1}{64}} = \frac{\sqrt{37}}{8} \approx 0.76 < 1.$$

The proof guarantees $|p(z)| \leq 1 - \frac{1}{2} \cdot \frac{1}{4} \cdot 1 = \frac{7}{8}$, and $\sqrt{37}/8 \leq \frac{7}{8}$ since $37 \leq 49$. The direction matters: along the real axis, $p(\frac{1}{2}) = \frac{1}{8} + \frac{1}{4} + 1 = \frac{11}{8} > 1$, because there $b_2 h^2 = \frac{1}{4}$ points away from 0.

6.5.5 The proof of the theorem

The three steps now combine into a proof of [Theorem 6.5.1](#).

Proof. Let $p \in \mathbb{C}[x]$ be nonconstant. By Lemma 6.5.3 there is $z_0 \in \mathbb{C}$ with $|p(z_0)| \leq |p(z)|$ for every $z \in \mathbb{C}$. Suppose, for a contradiction, that $p(z_0) \neq 0$. By Lemma 6.5.4 there is z with $|p(z)| < |p(z_0)|$, contradicting the choice of z_0 . Hence $p(z_0) = 0$, and z_0 is a root of p . ■

This proves Chapter 0's Theorem 0.6.7: a polynomial $a_n z^n + \cdots + a_0$ with $n \geq 1$ and $a_n \neq 0$ is a nonconstant element of $\mathbb{C}[x]$, and we have just shown that it has a root.

Quick check. The polynomial $p = x^2 + 1 \in \mathbb{R}[x]$ has no real root, yet the function $c \mapsto |p(c)|$ on $\mathbb{R}$ has a minimum, at $c = 0$. Which step of the argument breaks if we try to run it over $\mathbb{R}$?

Solution. Growth and the attained minimum both hold on $\mathbb{R}$: the minimum value is $|p(0)| = 1$. The step that fails is d'Alembert's lemma. At $z_0 = 0$ we have $b_0 = 1$, $k = 2$, $b_2 = 1$, so we need a direction u with $u^2 = w = -1$. There is no such real u , and indeed $p(h) = 1 + h^2 \geq 1$ for every real h . Over $\mathbb{C}$, $u = i$ works and $p(ti) = 1 - t^2 < 1$ for $0 < t \leq 1$.

Warning. **The theorem is an existence theorem.** It says a root exists; it does not say how to find one, and the proof does not produce one. There is no formula for the roots of a general polynomial of degree 5 or more built from the coefficients by $+$, $-$, $\times$, $\div$ and k -th roots (a theorem from Galois theory, which we do not prove). Numerical root-finding algorithms approximate roots; that is a different subject, and the Fundamental Theorem of Algebra is not one of those algorithms.

6.5.6 Complex polynomials split

Combining the theorem with the root count of the previous section gives the form in which it is used most.

Corollary 6.5.5. Complex Polynomials Split

- (a) Every nonzero $p \in \mathbb{C}[x]$ splits over $\mathbb{C}$: if $\deg p = n$ and p has leading coefficient a , then $p = a(x - z_1)(x - z_2) \cdots (x - z_n)$ for some $z_1, \dots, z_n \in \mathbb{C}$. In particular the multiplicities of the roots of p add up to n .
- (b) The irreducible polynomials in $\mathbb{C}[x]$ are exactly the polynomials of degree 1.

Proof.

- (a) By Theorem 6.4.3, $p = (x - c_1)^{m_1} \cdots (x - c_k)^{m_k} g$, where $c_1, \dots, c_k$ are the distinct roots of p in $\mathbb{C}$ and $g \in \mathbb{C}[x]$ has no root in $\mathbb{C}$. By Theorem 6.5.1, g is constant, and $g \neq 0$ because $p \neq 0$. So p splits over $\mathbb{C}$, and the multiplicities add up to n by the same theorem. Comparing leading coefficients (Theorem 0.8.3), the constant is a .
- (b) A polynomial of degree 1 is irreducible, since a factorization into two nonconstant

factors would have degree at least 2. Conversely, let $p \in \mathbb{C}[x]$ be irreducible. It is nonconstant (Definition 6.3.1), so by (a) it has a factor $x - z_1$, say $p = (x - z_1)q$. Since p is irreducible and $x - z_1$ is not constant, q is a nonzero constant, and $\deg p = 1$. ■

So in $\mathbb{C}[x]$, unique factorization (Theorem 6.3.5) is completely explicit: the monic irreducible factors are the $x - z$, and the exponent of $x - z$ is the multiplicity of z . In Chapter 9 this is what gives every operator on a nonzero finite-dimensional complex vector space an eigenvalue. (That fact also has a proof using only linear algebra, and one can run the logic in the other direction; we will not need it.)

Example. Factoring $x^4 + 1$ over $\mathbb{C}$ and over $\mathbb{R}$

Factor $f = x^4 + 1$ into irreducible polynomials in $\mathbb{C}[x]$ and in $\mathbb{R}[x]$.

Solution. Roots. We solve $z^4 = -1 = e^{i\pi}$ as in Example (Roots of Unity). Write $z = re^{i\theta}$ with $r > 0$; by Theorem 0.6.6, $z^4 = r^4 e^{4i\theta}$. Comparing polar forms, $r^4 = 1$, so $r = 1$, and $4\theta = \pi + 2\pi j$ for an integer j . The values $j = 0, 1, 2, 3$ give four distinct roots

$$z_0 = e^{i\pi/4} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, \quad z_1 = e^{3i\pi/4} = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, \quad z_2 = \bar{z}_1, \quad z_3 = \bar{z}_0.$$

Over $\mathbb{C}$. Four distinct roots, each of multiplicity at least 1, and $\deg f = 4$, so by Theorem 6.4.3 each multiplicity is 1 and

$$x^4 + 1 = (x - z_0)(x - z_1)(x - z_2)(x - z_3),$$

the leading coefficient being 1. The factors are irreducible by Corollary 6.5.5 (b).

Over $\mathbb{R}$. Pair each root with its conjugate. For any $z \in \mathbb{C}$,

$$(x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z} = x^2 - 2\operatorname{Re}(z)x + |z|^2 \in \mathbb{R}[x],$$

by Theorem 0.6.2 (c). With $\operatorname{Re} z_0 = \frac{\sqrt{2}}{2}$, $\operatorname{Re} z_1 = -\frac{\sqrt{2}}{2}$, and $|z_0| = |z_1| = 1$,

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

Check: the product is $(x^2 + 1)^2 - 2x^2 = x^4 + 1$. Each quadratic has nonreal roots only, hence no real root, so it is irreducible over $\mathbb{R}$ by Theorem 6.3.1. Note that $x^4 + 1$ has no real root but is **reducible** over $\mathbb{R}$.

6.5.7 Real polynomials

A real polynomial is also a complex polynomial, so the theorem applies to it; the roots it provides may be nonreal. They are not scattered arbitrarily. Chapter 0 observed that nonreal roots of a real polynomial come in conjugate pairs; we now show that the pairs also share their multiplicity. For $g = \sum_j c_j x^j \in \mathbb{C}[x]$ write $\bar{g} = \sum_j \bar{c}_j x^j$, the polynomial with conjugated coefficients.

Theorem 6.5.6. Conjugate Roots Have Equal Multiplicity

Let $f \in \mathbb{R}[x]$ be nonzero, regarded as an element of $\mathbb{C}[x]$, and let $z \in \mathbb{C}$. Then $f(\bar{z}) = \overline{f(z)}$. In particular z is a root of f if and only if $\bar{z}$ is, and

$$\text{mult}_{\bar{z}}(f) = \text{mult}_z(f).$$

Idea. Conjugation respects sums and products of complex numbers, so applying it to all coefficients respects sums and products of polynomials. A real polynomial is unchanged by it. So conjugating a factorization $f = (x - z)^m g$ gives a factorization $f = (x - \bar{z})^m \bar{g}$, and the cofactor test transfers.

Proof. Let $g = \sum_j c_j x^j$ and $h = \sum_j d_j x^j$ be in $\mathbb{C}[x]$, and $z \in \mathbb{C}$. By Theorem 0.6.2 (a) and (b), the coefficient of x^k in $\overline{gh}$ is $\overline{\sum_{i+j=k} c_i d_j} = \sum_{i+j=k} \overline{c_i} \overline{d_j}$, which is the coefficient of x^k in $\bar{g} \bar{h}$. So $\overline{gh} = \bar{g} \bar{h}$. By the same parts, $\overline{g(z)} = \sum_j \overline{c_j} z^j = \sum_j c_j \bar{z}^j = \bar{g}(\bar{z})$.

Since f has real coefficients, $\bar{f} = f$. Hence $f(\bar{z}) = \bar{f}(z) = \overline{f(z)}$, and $f(z) = 0$ if and only if $f(\bar{z}) = 0$.

Let $m = \text{mult}_z(f)$. By Lemma 6.4.1, $f = (x - z)^m g$ with $g \in \mathbb{C}[x]$ and $g(z) \neq 0$. Conjugating, and using $\overline{x - z} = x - \bar{z}$,

$$f = \bar{f} = (x - \bar{z})^m \bar{g}, \quad \bar{g}(\bar{z}) = \overline{g(z)} \neq 0.$$

By Lemma 6.4.1 again, $\text{mult}_{\bar{z}}(f) = m$. This proves the theorem. ■

For instance, a real polynomial with $2 + i$ as a root of multiplicity 3 also has $2 - i$ as a root of multiplicity 3, so by Theorem 6.4.3 its degree is at least 6. Now the irreducible real polynomials can be listed.

Corollary 6.5.7. Irreducible Real Polynomials

The irreducible polynomials in $\mathbb{R}[x]$ are exactly the polynomials of degree 1, and the polynomials of degree 2 with no real root. In particular, every irreducible polynomial in $\mathbb{R}[x]$ has degree 1 or 2.

Idea. An irreducible real p has a complex root z by the theorem. If z is real, $x - z$ is a real factor and p is linear. If not, $\bar{z}$ is another root, and $(x - z)(x - \bar{z})$ is a **real** quadratic dividing p . The only subtle point is that it divides p in $\mathbb{R}[x]$ and not merely in $\mathbb{C}[x]$; uniqueness of division settles that.

Proof. ($\Leftarrow$) A polynomial of degree 1 is irreducible, since a product of two nonconstant polynomials has degree at least 2 (Theorem 0.8.3). A polynomial of degree 2 with no real root is irreducible by Theorem 6.3.1.

($\Rightarrow$) Let $p \in \mathbb{R}[x]$ be irreducible. It is nonconstant, so by [Theorem 6.5.1](#) it has a root $z \in \mathbb{C}$.

Case 1: $z \in \mathbb{R}$. By Lemma 3.7.1 in $\mathbb{R}[x]$, $p = (x - z)q$ with $q \in \mathbb{R}[x]$. Since p is irreducible and $x - z$ is not constant, q is a nonzero constant, so $\deg p = 1$.

Case 2: $z \notin \mathbb{R}$. Then $\bar{z} \neq z$, and $\bar{z}$ is also a root by [Theorem 6.5.6](#). Applying Corollary 6.1.4 in $\mathbb{C}[x]$ to the two distinct roots $z, \bar{z}$ gives $p = (x - z)(x - \bar{z})h$ for some $h \in \mathbb{C}[x]$. Put $q = (x - z)(x - \bar{z}) = x^2 - 2\operatorname{Re}(z)x + |z|^2$, which lies in $\mathbb{R}[x]$. Divide in $\mathbb{R}[x]$ (Theorem 6.1.1): $p = qh_1 + r$ with $h_1, r \in \mathbb{R}[x]$ and $\deg r < 2$. This is also a division with remainder in $\mathbb{C}[x]$, and so is $p = qh + 0$. By the uniqueness in Theorem 6.1.1 over $\mathbb{C}$, $r = 0$ and $h = h_1 \in \mathbb{R}[x]$. So $p = qh_1$ in $\mathbb{R}[x]$. Since p is irreducible and q is not constant, h_1 is a nonzero constant, and $\deg p = 2$. Finally, p has no real root, because a real root c would give a factor $x - c$ and $p = (x - c)q'$ with $\deg q' = 1$, contradicting irreducibility. This proves the corollary. ■

Remark. Completing the square decides which quadratics occur: $x^2 + \beta x + \gamma = (x + \frac{\beta}{2})^2 - \frac{\beta^2 - 4\gamma}{4}$ has a real root if and only if $\beta^2 - 4\gamma \geq 0$. So the monic irreducible real quadratics are those with $\beta^2 < 4\gamma$.

Unique factorization in $\mathbb{R}[x]$ now takes a concrete form.

Corollary 6.5.8. Factorization over $\mathbb{R}$

Every nonconstant $f \in \mathbb{R}[x]$ can be written as

$$f = a(x - c_1) \cdots (x - c_r) q_1 \cdots q_s,$$

where $a \in \mathbb{R}$ is the leading coefficient of f , $c_1, \dots, c_r \in \mathbb{R}$ (not necessarily distinct), and $q_1, \dots, q_s \in \mathbb{R}[x]$ are monic quadratics with no real root. Then $r + 2s = \deg f$, and r is the sum of the multiplicities of the real roots of f . The factorization is unique up to the order of the factors.

Proof. By Theorem 6.3.5, $f = ap_1 \cdots p_k$ with $p_i \in \mathbb{R}[x]$ monic irreducible, unique up to order. By [Corollary 6.5.7](#) each p_i is either $x - c$ with $c \in \mathbb{R}$ or a monic quadratic with no real root; list the first kind as $x - c_1, \dots, x - c_r$ and the second as $q_1, \dots, q_s$. Then $\deg f = r + 2s$ by Theorem 0.8.3. For a real number c , each q_j has multiplicity 0 at c , and $x - c_i$ has multiplicity 1 or 0 according as $c_i = c$ or not; by Theorem 6.4.2, $\operatorname{mult}_c(f)$ is the number of indices i with $c_i = c$. Adding over the real roots of f gives r . ■

The last consequence is one that calculus proves with the intermediate value theorem. Here it falls out of counting degrees.

Corollary 6.5.9. Odd Degree Forces a Real Root

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

Proof. By [Corollary 6.5.8](#), $\deg f = r + 2s$. Since $\deg f$ is odd, r is odd, so $r \geq 1$, and c_1 is a real root of f . ■

Warning. **No real root does not mean irreducible over $\mathbb{R}$.** By [Corollary 6.5.7](#), an irreducible real polynomial has degree at most 2; so $x^4 + 1$, which has no real root, is still reducible over $\mathbb{R}$ ([Example \(Factoring \$x^4 + 1\$ over \$\mathbb{C}\$ and over \$\mathbb{R}\$ \)](#)). The test “reducible if and only if it has a root” is only valid in degrees 2 and 3 ([Theorem 6.3.1](#)).

6.5.8 Exercises

6.5.8.1 A. Check your understanding

Exercise. A1

- State the Fundamental Theorem of Algebra, and list the two facts from analysis used in its proof in this section.
- True or false: every polynomial in $\mathbb{R}[x]$ of degree 4 has a real root. Justify your answer.
- True or false: if $f \in \mathbb{R}[x]$ has $2 + i$ as a root of multiplicity 3, then $\deg f \geq 6$. Justify your answer.
- True or false: every polynomial in $\mathbb{R}[x]$ of degree 5 has a real root. Justify your answer.
- True or false: every irreducible polynomial in $\mathbb{F}_2[x]$ has degree at most 2. Justify your answer.
- In the proof of d’Alembert’s lemma ([Lemma 6.5.4](#)), which property of $\mathbb{C}$ is used that $\mathbb{R}$ lacks?

Solution.

- Every nonconstant $p \in \mathbb{C}[x]$ has a root in $\mathbb{C}$ ([Theorem 6.5.1](#)). The analytic facts are (A1) continuity of $z \mapsto |p(z)|$ on $\mathbb{C}$, and (A2) the extreme value theorem for continuous real functions on a closed disc.
- False. $x^4 + 1 \geq 1$ at every real number, so it has no real root.
- True. By [Theorem 6.5.6](#), $2 - i$ is also a root of multiplicity 3, and $2 - i \neq 2 + i$. By [Theorem 6.4.3](#), $\deg f \geq 3 + 3 = 6$.
- True, by [Corollary 6.5.9](#).
- False. $x^3 + x + 1$ takes the value 1 at both 0 and 1, so it has no root in $\mathbb{F}_2$, and a cubic without a root is irreducible by [Theorem 6.3.1](#). [Corollary 6.5.7](#) is special to $\mathbb{R}$.
- Every nonzero complex number has a k -th root; the proof takes a k -th root of a complex number of modulus 1 by [Theorem 0.6.6](#). Over $\mathbb{R}$, -1 has no square root.

6.5.8.2 B. Practice

Exercise. B1: $x^4 + 4$

Find all complex roots of $x^4 + 4$, and factor it into irreducible polynomials in $\mathbb{C}[x]$ and in $\mathbb{R}[x]$.

Solution. Write $z = re^{i\theta}$ with $r > 0$. By Theorem 0.6.6, $z^4 = r^4 e^{4i\theta}$, and $-4 = 4e^{i\pi}$. Comparing polar forms, $r^4 = 4$, so $r = \sqrt{2}$ (the only positive real number with fourth power 4, since $t \mapsto t^4$ is strictly increasing on positive reals), and $4\theta = \pi + 2\pi j$, $j \in \mathbb{Z}$. The values $j = 0, 1, 2, 3$ give the four distinct roots

$$\sqrt{2}e^{i\pi/4} = 1 + i, \quad \sqrt{2}e^{3i\pi/4} = -1 + i, \quad \sqrt{2}e^{5i\pi/4} = -1 - i, \quad \sqrt{2}e^{7i\pi/4} = 1 - i.$$

By Theorem 6.4.3, four distinct roots of a degree-4 monic polynomial each have multiplicity 1, and

$$x^4 + 4 = (x - 1 - i)(x - 1 + i)(x + 1 - i)(x + 1 + i) \quad \text{in } \mathbb{C}[x].$$

Pairing conjugates with $(x - z)(x - \bar{z}) = x^2 - 2\operatorname{Re}(z)x + |z|^2$, and $|1 \pm i|^2 = |-1 \pm i|^2 = 2$,

$$x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2) \quad \text{in } \mathbb{R}[x].$$

Check: $(x^2 + 2)^2 - (2x)^2 = x^4 + 4x^2 + 4 - 4x^2 = x^4 + 4$. Both quadratics have $\beta^2 - 4\gamma = 4 - 8 < 0$, so they have no real roots and are irreducible by [Corollary 6.5.7](#).

Exercise. B2: $x^6 + 1$

Find the factorization of $x^6 + 1$ into irreducible polynomials in $\mathbb{R}[x]$.

Solution. The roots solve $z^6 = -1 = e^{i\pi}$. As in B1, $z = e^{i\theta}$ with $6\theta = \pi + 2\pi j$, and $j = 0, \dots, 5$ give six distinct roots at the angles $30^\circ, 90^\circ, 150^\circ, 210^\circ, 270^\circ, 330^\circ$:

$$\frac{\sqrt{3}}{2} \pm \frac{1}{2}i, \quad \pm i, \quad -\frac{\sqrt{3}}{2} \pm \frac{1}{2}i.$$

Each has multiplicity 1 by Theorem 6.4.3, and none is real. They form three conjugate pairs, each of modulus 1, with real parts $\frac{\sqrt{3}}{2}, 0, -\frac{\sqrt{3}}{2}$. Pairing them as in [Example \(Factoring \$x^4 + 1\$ over \$\mathbb{C}\$ and over \$\mathbb{R}\$ \)](#),

$$x^6 + 1 = (x^2 + 1)(x^2 - \sqrt{3}x + 1)(x^2 + \sqrt{3}x + 1).$$

Check: $(x^2 - \sqrt{3}x + 1)(x^2 + \sqrt{3}x + 1) = (x^2 + 1)^2 - 3x^2 = x^4 - x^2 + 1$, and $(x^2 + 1)(x^4 - x^2 + 1) = x^6 + 1$. Each quadratic factor has only nonreal roots, so it is irreducible over $\mathbb{R}$ by [Corollary 6.5.7](#). By the uniqueness in [Corollary 6.5.8](#), this is the factorization.

Exercise. B3: Real cubics

Let $f \in \mathbb{R}[x]$ have degree 3, and suppose the multiplicities of the real roots of f add up to 1.

- (a) Prove that $f = a(x - c)(x - z)(x - \bar{z})$ for some $a, c \in \mathbb{R}$ and some $z \in \mathbb{C} \setminus \mathbb{R}$, and that z and $\bar{z}$ are simple roots.
- (b) Show that the hypothesis cannot be weakened to “ f has exactly one real root” by considering $(x - 1)^3$.

Solution.

- (a) By [Corollary 6.5.8](#), $f = a(x - c_1) \cdots (x - c_r) q_1 \cdots q_s$ with $r + 2s = 3$ and r equal to the sum of the real multiplicities, which is 1. So $r = 1$, $s = 1$, and $f = a(x - c)q$ with $c \in \mathbb{R}$ and q a monic real quadratic without real roots. By [Theorem 6.5.1](#), q has a root $z \in \mathbb{C}$, which is not real. By [Theorem 6.5.6](#), $\bar{z} \neq z$ is also a root of q . The two multiplicities in q are each at least 1 and add up to at most 2 ([Theorem 6.4.3](#)), so they equal 1 and $q = (x - z)(x - \bar{z})$, the leading coefficient being 1. Finally, by [Theorem 6.4.2](#), $\text{mult}_z(f) = \text{mult}_z(a(x - c)) + \text{mult}_z(q) = 0 + 1 = 1$, since $a(z - c) \neq 0$; similarly for $\bar{z}$.
- (b) $(x - 1)^3$ has exactly one real root, 1, but no nonreal roots at all: it already splits over $\mathbb{R}$. Here the real multiplicities add up to 3, not 1.

Exercise. B4: Running the proof on an example

Let $p = x^4 - x^2 + 2 \in \mathbb{C}[x]$.

- (a) Compute the radius R of [Lemma 6.5.2](#) for p .
- (b) Follow the proof of [Lemma 6.5.4](#) at $z_0 = 0$: find k , B , u , and t , and verify that $|p(tu)| < |p(0)|$.
- (c) Compute $p(i/2)$, and explain why the direction i does not work here, although it did in [Example \(One Step Downhill\)](#).

Solution.

- (a) Here $a_4 = 1$ and $A = |2| + |0| + |-1| + |0| = 3$, so $R = \max\{1, 6\} = 6$. Hence $|p(z)| \geq \frac{1}{2}|z|^4$ for $|z| \geq 6$.
- (b) At $z_0 = 0$ the coefficients are $b_0 = 2$, $b_1 = 0$, $b_2 = -1$, $b_3 = 0$, $b_4 = 1$. So $k = 2$ and $B = |b_3| + |b_4| = 1$. Then $w = -b_0/b_2 = 2 = 2e^{i \cdot 0}$, so $\alpha = 0$ and $u = 1$. Next $t = \min\{1, 2/1, 1/2\} = \frac{1}{2}$. So $z = \frac{1}{2}$, and $p(\frac{1}{2}) = \frac{1}{16} - \frac{1}{4} + 2 = \frac{29}{16} < 2 = |p(0)|$. The proof guarantees at most $2 - \frac{1}{2} \cdot \frac{1}{4} \cdot 1 = \frac{15}{8} = \frac{30}{16}$, consistent with $\frac{29}{16}$.
- (c) $p(i/2) = \frac{1}{16} + \frac{1}{4} + 2 = \frac{37}{16} > 2$. The right direction depends on the sign of b_k relative to b_0 : we need $b_2 u^2$ to point from b_0 toward 0, that is, $b_2 u^2$ a negative multiple of $b_0 = 2$. With $b_2 = -1$ this means $u^2 > 0$, so $u = \pm 1$; for $u = i$, $b_2 u^2 = 1$ points away from 0. In [Example \(One Step Downhill\)](#), $b_2 = +1$ and $u = i$ was the right choice.

6.5.8.3 C. Going deeper

Exercise. C1: Fields where the theorem fails

Call a field F **algebraically closed** if every nonconstant polynomial in $F[x]$ has a root in F .

- (a) Let p be a prime. Show that $x^p - x + 1$ has no root in $\mathbb{F}_p$. More generally, show that no finite field is algebraically closed.
- (b) Give explicit witnesses that $\mathbb{R}$ and $\mathbb{Q}$ are not algebraically closed.
- (c) For your witness over $\mathbb{R}$, explain which step of the proof of the Fundamental Theorem of Algebra (Theorem 6.5.1) breaks.
- (d) For $f = x^2 - 2$ over $\mathbb{Q}$, prove that $r \mapsto |f(r)|$ has **no** minimum on $\mathbb{Q}$. Which step of the proof breaks now?

Hint for (d): if r_0 were a minimum point with $r_0^2 > \frac{2}{5}$, compare r_0 with $r_1 = \frac{r_0^2 + 2}{2r_0}$.

Solution.

- (a) By Exercise (C2: A nonzero polynomial vanishing everywhere) (c), $a^p - a = 0$ for every $a \in \mathbb{F}_p$, so $a^p - a + 1 = 1 \neq 0$. For a finite field $F = \{c_1, \dots, c_q\}$, let $g = (x - c_1) \cdots (x - c_q) + 1$. It has degree $q \geq 2$ (Theorem 0.8.3), and $g(c_i) = 0 + 1 = 1 \neq 0$ for every i by Theorem 0.8.5. So g is a nonconstant polynomial without a root in F .
- (b) Over $\mathbb{R}$, $x^2 + 1$ has no root, since $c^2 + 1 \geq 1$. Over $\mathbb{Q}$, $x^2 - 2$ has no root, since $\sqrt{2}$ is irrational (Theorem 0.2.3) and the only real roots are $\pm\sqrt{2}$.
- (c) For $x^2 + 1$ over $\mathbb{R}$, growth holds, and $c \mapsto |c^2 + 1|$ attains its minimum 1 at $c = 0$. The step that breaks is d'Alembert's lemma (Lemma 6.5.4): at $z_0 = 0$ we have $b_0 = 1$, $k = 2$, $b_2 = 1$, and we need u with $u^2 = -1$, which does not exist in $\mathbb{R}$.
- (d) Suppose $r_0 \in \mathbb{Q}$ satisfies $|r_0^2 - 2| \leq |r^2 - 2|$ for every $r \in \mathbb{Q}$. Put $m = |r_0^2 - 2|$; then $m > 0$ by (b).
Case 1: $r_0^2 \leq \frac{2}{5}$. Then $m = 2 - r_0^2 \geq \frac{8}{5} > 1 = |1^2 - 2|$, contradicting minimality at $r = 1$.
Case 2: $r_0^2 > \frac{2}{5}$. Then $r_0 \neq 0$, and $r_1 = (r_0^2 + 2)/(2r_0) \in \mathbb{Q}$. Expanding,

$$r_1^2 - 2 = \frac{(r_0^2 + 2)^2 - 8r_0^2}{4r_0^2} = \frac{(r_0^2 - 2)^2}{4r_0^2}, \quad \text{so} \quad |r_1^2 - 2| = m \cdot \frac{m}{4r_0^2}.$$

We claim $m < 4r_0^2$. If $r_0^2 \geq 2$, then $m = r_0^2 - 2 < 4r_0^2$. If $\frac{2}{5} < r_0^2 < 2$, then $m = 2 - r_0^2 < \frac{8}{5} < 4r_0^2$. Hence $|r_1^2 - 2| < m$, contradicting minimality.

So there is no minimum. The step of the proof that breaks is Lemma 6.5.3, which rests on the extreme value theorem (A2). That fact is about the completeness of $\mathbb{R}$, and $\mathbb{Q}$ is not complete: the values $|r^2 - 2|$ get arbitrarily close to 0 without reaching it.

Exercise. C2: Sums of two squares

Let $f \in \mathbb{R}[x]$ be monic with **no** real root.

- (a) Prove that $\deg f$ is even and that $f(c) > 0$ for every $c \in \mathbb{R}$.
- (b) Prove that $f = g^2 + h^2$ for some $g, h \in \mathbb{R}[x]$.

Hint for (b): each irreducible factor of f is $(x - z)(x - \bar{z})$. Collect one root from each pair into a complex polynomial G , and split G into real and imaginary parts.

Solution.

- (a) By [Corollary 6.5.8](#), $f = (x - c_1) \cdots (x - c_r) q_1 \cdots q_s$, with leading coefficient 1 since f is monic. A factor $x - c_1$ would give the real root c_1 , so $r = 0$ and $\deg f = 2s$ is even. (If $s = 0$, then $f = 1$ and the claims hold.) Each $q_j = x^2 + \beta x + \gamma$ has no real root, so by the remark after [Corollary 6.5.7](#), $\beta^2 < 4\gamma$. For real c ,

$$q_j(c) = \left(c + \frac{\beta}{2}\right)^2 + \frac{4\gamma - \beta^2}{4} > 0.$$

By Theorem 0.8.5, $f(c) = q_1(c) \cdots q_s(c)$ is a product of positive reals, so $f(c) > 0$.

- (b) For each j , q_j is nonconstant, so by [Theorem 6.5.1](#) it has a root $z_j \in \mathbb{C}$, not real. As in [Exercise \(B3: Real cubics\)](#) (a), $q_j = (x - z_j)(x - \bar{z}_j)$. Let $G = (x - z_1) \cdots (x - z_s) \in \mathbb{C}[x]$. By the product rule for conjugate polynomials proved in [Theorem 6.5.6](#), $\bar{G} = (x - \bar{z}_1) \cdots (x - \bar{z}_s)$, so $f = G\bar{G}$ (commutativity, Theorem 0.8.1).

Write each coefficient of G as $\alpha_k + i\beta_k$ with $\alpha_k, \beta_k \in \mathbb{R}$, and put $g = \sum_k \alpha_k x^k$ and $h = \sum_k \beta_k x^k$ in $\mathbb{R}[x]$. Then $G = g + ih$ and $\bar{G} = g - ih$, so

$$f = (g + ih)(g - ih) = g^2 - i^2 h^2 + (ihg - igh) = g^2 + h^2.$$

For example, for $x^4 + 1$ take $z_1 = e^{i\pi/4}$ and $z_2 = e^{3i\pi/4}$ from [Example \(Factoring \$x^4 + 1\$ over \$\mathbb{C}\$ and over \$\mathbb{R}\$ \)](#). Then $z_1 + z_2 = i\sqrt{2}$ and $z_1 z_2 = e^{i\pi} = -1$, so $G = x^2 - i\sqrt{2}x - 1$, $g = x^2 - 1$, $h = -\sqrt{2}x$, and $x^4 + 1 = (x^2 - 1)^2 + 2x^2$.