

Contents

Preface	3
1 Chapter 1	5
Complex Numbers	5
1.0.1 Roadmap	7
1.0.2 Named moves	7
1.1 The Complex Numbers as Pairs of Reals	8
1.1.1 Building the new numbers	8
1.1.2 The real numbers inside the complex numbers	9
1.1.3 The laws of arithmetic	12
1.1.4 Powers and a factorization	13
1.1.5 Exercises	16
1.1.5.1 A. Check your understanding	16
1.1.5.2 B. Practice	16
1.1.5.3 C. Going deeper	18
1.2 Conjugate, Modulus, and Division	19
1.2.1 Conjugate and modulus	19
1.2.2 Rules for conjugate and modulus	21
1.2.3 Division	23
1.2.4 Exercises	25
1.2.4.1 A. Check your understanding	25
1.2.4.2 B. Practice	25
1.2.4.3 C. Going deeper	27
1.3 The Triangle Inequality	28
1.3.1 Why the old proof does not transfer	28
1.3.2 The real part is at most the modulus	29
1.3.3 The triangle inequality	30
1.3.4 Three variants	32
1.3.5 Exercises	33
1.3.5.1 A. Check your understanding	33
1.3.5.2 B. Practice	34
1.3.5.3 C. Going deeper	35
1.4 Square Roots, Quadratic Equations, and the Missing Order	37
1.4.1 Square roots from real square roots	37
1.4.2 The quadratic formula	40
1.4.3 No order on the complex numbers	41
1.4.4 The square-root rule does not survive	42

1.4.5	Exercises	42
1.4.5.1	A. Check your understanding	42
1.4.5.2	B. Practice	43
1.4.5.3	C. Going deeper	44
1.5	The Unit Circle and Polar Form	46
1.5.1	Length and direction	46
1.5.2	What this volume borrows about cosine and sine	48
1.5.3	Polar form	49
1.5.4	Powers	52
1.5.5	Exercises	54
1.5.5.1	A. Check your understanding	54
1.5.5.2	B. Practice	55
1.5.5.3	C. Going deeper	56
1.6	Higher Roots, Roots of Unity, and a Look Ahead	58
1.6.1	Real n -th roots	58
1.6.2	Solving the equation $z^n = c$	60
1.6.3	Roots of unity	62
1.6.4	Polynomial equations, and a look ahead	64
1.6.5	Exercises	65
1.6.5.1	A. Check your understanding	65
1.6.5.2	B. Practice	66
1.6.5.3	C. Going deeper	67
1.6.5.4	R. Review	68

Preface

Number Systems: From $\mathbb{N}$ to $\mathbb{R}$ ended with the real numbers as a complete ordered field. *Analysis on the Real Line* starts from the axioms of such a field and proves its first limit theorems at once. This volume supplies the working tools that analysis uses on every page without stopping to prove them: inequalities and finite sums, real functions and their graphs, coordinates and vectors in $\mathbb{R}^n$, lines, convex sets and isometries, the complex numbers and the plane they form, and distances in the general form of a metric.

Who it is for. The reader we have in mind has worked through *Logic and Proof*, *Sets and Functions* and the main line of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , or has their habits from elsewhere. Much of the material is familiar in outline from school; what is new is that every rule is proved from the axioms of a complete ordered field, and that nothing is used before it is proved.

What it covers. The volume is being written. Its finished chapter is:

Chapter	Title	What it does
1	Complex Numbers	$\mathbb{C}$ as pairs of real numbers, proved a field containing $\mathbb{R}$; conjugate, modulus and the triangle inequality; square roots and the quadratic formula; why $\mathbb{C}$ has no order; polar form, De Moivre's formula and the roots of unity

Six chapters are planned around it, in this reading order: *Inequalities*, *Finite Sums*, and *Real Powers*; *Real Functions and Their Graphs*; *Coordinates and Vectors in $\mathbb{R}^n$* ; *Lines*, *Convexity*, and *Isometries of $\mathbb{R}^n$* ; then *Complex Numbers*; then *Rotations*, *Angles*, and *the Complex Plane* and *Metrics and Norms*. When they are added, the chapters will be renumbered in that order.

How to read it. Every section has Quick checks with folded answers; answer each one before you unfold it. The exercises of a section come in three groups, A to check understanding, B for practice and C to go deeper, and the last section of each chapter adds R items that reach back to earlier chapters. A chapter's opening page lists what it needs, with links, and the time it takes. Second-reading folds hold edge cases and longer justifications. They can stay closed on a first reading, but they are not optional, since later proofs may use what they contain.

One borrowed fact. This volume does not define cosine, sine or π : defining them needs limits and power series, which belong to analysis. Section 1.5 states five facts about them, numbered (T1)–(T5), as an assumption, and *Analysis on the Real Line*, Chapter 10 proves them. They are used only for polar form and for the roots of complex numbers in Sections 1.5 and 1.6, and each proof that uses one names it.

Time. Chapter 1 takes about 25 hours on the core track and about 35 hours for everything.

What comes next. *Analysis on the Real Line* uses this volume from its second chapter on. *Algebraic Preliminaries* takes the complex numbers of Chapter 1 as its main example and builds fields, groups and polynomials on them, ending with the Fundamental Theorem of Algebra. The linear algebra volumes, beginning with *Spaces and Maps*, use the complex numbers throughout.

Chapter 1

Complex Numbers

No real number squares to -1 : in an ordered field a non-zero square is positive (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (e)), so $x^2 + 1 = 0$ has no solution in $\mathbb{R}$. The usual remedy, “invent a symbol i with $i^2 = -1$ ”, leaves open why such a symbol is safe when “a number z with $0 \cdot z = 1$ ” is not. This chapter does not invent anything. It takes pairs of real numbers, objects the reader already trusts, adds them coordinate by coordinate, and multiplies them by the one formula that $i^2 = -1$ would force. Then it checks, law by law, that nothing breaks: the complex numbers $\mathbb{C}$ form a field in the sense of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2, and they contain $\mathbb{R}$ as the pairs $(a, 0)$. Every later volume that computes with complex numbers, from inner products in linear algebra to roots of unity in algebra, starts from this field.

Two habits of $\mathbb{R}$ do not survive the passage. No order on $\mathbb{C}$ is compatible with its arithmetic, and no choice of “the” square root of each complex number keeps the rule $\sqrt{x}\sqrt{y} = \sqrt{xy}$. One new habit takes the place of order: measure a complex number by its modulus, a non-negative real, and compute with $|u|^2 = u\bar{u}$, which is algebra. The first four sections need nothing but the real numbers, and they reach far: division, the triangle inequality, and square roots and the quadratic formula without a single angle. The picture of multiplication as a turn and a stretch does need angles, and angles need cosine and sine, which belong to analysis. The chapter borrows exactly five facts about them, says so in one place, and derives everything else from those five: the familiar special values, De Moivre’s formula, the n different n -th roots of every non-zero complex number, and the roots of unity. It ends with a look ahead at the Fundamental Theorem of Algebra, which *Algebraic Preliminaries*, Chapter 4 proves without the borrowed facts.

What you need. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* above all, and in it chiefly Chapters 2, 4 and 6. From its Chapter 5: the real numbers as a complete ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 5.6.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 5.6.1), the standing setting of the whole chapter. From its Chapter 6: square roots of non-negative reals, existing and unique (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 6.1.4), which define the modulus in Section 1.2 and build complex square roots in Section 1.4; the uniqueness of the complete ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 6.3.1), which lets Section 1.5 carry the borrowed facts over to our $\mathbb{R}$; the automorphism theorem (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 6.3.4), used in the solution of review exercise R1 and compared there with the two such maps of $\mathbb{C}$; and the cube roots of its Exercise B2 of Section 6.2 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Exercise (B2: Cube roots)), whose method Section 1.6 runs for every exponent. From its Chapter 2: the axioms of a field and of an ordered field and their rules (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 2.3.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 2.3.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$).

(Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5), used on nearly every page; the finite ring that cannot be ordered (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Example (A field with two elements that cannot be ordered)), compared with in Section 1.4; and the gap at $\sqrt{2}$ in $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 2.6.1), which shows in Section 1.2 why the modulus needs completeness. From its Chapter 4: the rules for fractions in a field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Lemma 4.1.1), the absolute value of an ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 4.1.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 4.1.3), which the modulus extends and whose triangle inequality Section 1.3 reproves by a new route, and the natural numbers and powers in an ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 4.2.1); a remark of Section 1.4 recalls its exercise on fields with a square root of -1 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Exercise (C1: A field that cannot be ordered)). From its Chapter 3: division with remainder, divisibility and parity in $\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 3.1.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 3.1.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Corollary 3.1.3), in Exercise B1 of Section 1.1 and in Sections 1.5 and 1.6; and the rings $\mathbb{Z}/n\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 3.4.2, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 3.4.3), in a remark and Exercise C2 of Section 1.4 and in review exercise R2. From its Chapter 1: the citing rule by which induction and recursion apply to $\mathbb{N}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Corollary 1.7.3), and the laws of powers in $\mathbb{N}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 1.6.4), compared with in Section 1.1. From *Sets and Functions*: ordered pairs, Cartesian products and injective maps, Chapter 1 (Sets and Functions, Definition 1.4.1, Sets and Functions, Definition 1.4.2, Sets and Functions, Definition 1.5.3); divisibility, Section 1.1 (Sets and Functions, Definition 1.1.2); the recursion theorem, powers and finite sums, Section 2.3 (Sets and Functions, Theorem 2.3.1, Sets and Functions, Definition 2.3.2, Sets and Functions, Proposition 2.3.4, Sets and Functions, Definition 2.3.1), whose recursions Section 1.1 reuses in any commutative ring; and finite sets, Section 2.5 (Sets and Functions, Definition 2.5.2), for counting n -th roots. From *Logic and Proof*: induction, Chapter 4 (Logic and Proof, Axiom 4.2.1); the contrapositive, Chapter 2 (Logic and Proof, Proposition 2.3.2), in Exercise B3 of Section 1.1; and the catalogue of what a proof may not do, Chapter 8 (Logic and Proof, Example (What is not allowed)), in the proof-ordering and find-the-error exercises of Sections 1.4 and 1.6. Section 1.4 also proves the complex square roots that *Logic and Proof*, Section 7.1 took as a school fact. Nothing from linear algebra is used, and nothing from analysis before the box of borrowed facts in Section 1.5.

Which real numbers. The chapter builds $\mathbb{C}$ on the real numbers of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 5, whose elements are classes of Cauchy sequences of rationals (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 5.2.1). No proof looks inside a real number: every step uses only that $\mathbb{R}$ is a complete ordered field. By the uniqueness theorem of that volume's Chapter 6 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 6.3.1), any complete ordered field would give the same $\mathbb{C}$, up to the one isomorphism between the two fields.

What this chapter borrows. Everything in Sections 1.1–1.4, and in Section 1.5 up to its box of borrowed facts, is proved from the real numbers. From that box on, five facts (T1)–(T5) about $\cos$, $\sin$ and π are used without proof: the circle identity, the addition formulas, where the cosine equals 1, that every point of the unit circle is reached, and the sign of the sine on the first half turn. *Analysis on the Real Line*, Chapter 10 defines the two functions and the number and proves the five facts. No other fact about cosine and sine is used, and the results that rest on the five say so in their dependency ledgers.

Time. About 25 hours on the core track (all of A, one B and one C per section, the exit checks); about 35 hours for everything.

1.0.1 Roadmap

- **The Complex Numbers as Pairs of Reals.** $\mathbb{C}$ defined as $\mathbb{R} \times \mathbb{R}$ with the product that $i^2 = -1$ would force; the real numbers inside $\mathbb{C}$ as the pairs $(a, 0)$, which makes $a + bi$ honest notation and $i^2 = -1$ a computation; a product with one sign changed, which has zero divisors; the laws of arithmetic, which make $\mathbb{C}$ a commutative ring with $1 \neq 0$; powers and their laws in any commutative ring; and the factorization of $z^n - w^n$.
- **Conjugate, Modulus, and Division.** The conjugate and the modulus, a non-negative real square root and the place where the completeness of $\mathbb{R}$ enters; the modulus as an extension of the absolute value of $\mathbb{R}$; the rules for conjugate and modulus, with $|zw| = |z||w|$ proved by squaring; the inverse $\bar{z}/|z|^2$ of a non-zero z ; the theorem that $\mathbb{C}$ is a field in which $\mathbb{R}$ is closed under the field operations; and division by the conjugate of the denominator.
- **The Triangle Inequality.** Why the trapping proof for ordered fields cannot run in $\mathbb{C}$; comparing squares of non-negative reals; real and imaginary parts at most the modulus; the triangle inequality, by expanding $|z + w|^2$ and recognizing the cross term as a real part; and three variants: the reverse inequality, the inequality for n terms, and a lower bound for the modulus of a sum.
- **Square Roots, Quadratic Equations, and the Missing Order.** An explicit formula for a square root of a complex number, built from two real square roots, and the count of exactly two square roots of every non-zero number; the quadratic formula with complex coefficients; the proof that no order makes $\mathbb{C}$ an ordered field; and why no choice of square roots keeps the product rule $\sqrt{z}\sqrt{w} = \sqrt{zw}$.
- **The Unit Circle and Polar Form.** The unit circle $\mathbb{T}$, closed under products and inverses, and every non-zero number as a length times a direction in exactly one way, all without angles; the five borrowed facts about cosine and sine; $e^{i\theta}$ as an abbreviation for $\cos \theta + i \sin \theta$, multiplication as “multiply moduli, add angles”, and polar form, unique up to a multiple of 2π in the argument; De Moivre’s formula; and the values of cosine and sine at $\pi/6$, $\pi/4$, $\pi/3$, $\pi/2$ and π , derived from the five facts.
- **Higher Roots, Roots of Unity, and a Look Ahead.** The unique non-negative n -th root of a non-negative real, constructed as a supremum; exactly n solutions of $z^n = c$ for every non-zero c , listed by polar form; the roots of unity, the set μ_n , and the sums of their powers; a look ahead at the Fundamental Theorem of Algebra; the conjugate of a solution of an equation with real coefficients as a second solution; and review exercises on the maps of $\mathbb{C}$ to itself that respect sums, products and 1 and send $\mathbb{R}$ into $\mathbb{R}$, on $\mathbb{Z}/n\mathbb{Z}$ and μ_n , on the triangle inequality of an ordered field, and on the equation $\bar{z} = z^2$.

1.0.2 Named moves

- **Compare real and imaginary parts.** One equation between complex numbers is two equations between real numbers: for real a, b, c, d , $a + bi = c + di$ if and only if $a = c$ and $b = d$. It is named in Section 1.1, where it proves the laws of arithmetic; Section 1.4 uses it to turn $w^2 = z$ into two real equations, and Section 1.5 to turn $e^{i\theta} = 1$ into $\cos \theta = 1$ and $\sin \theta = 0$. The warning of Section 1.1 marks the hypothesis it needs: the four numbers must be real. Exercise C1 of Section 1.1 proves the same uniqueness of parts in any field that contains $\mathbb{R}$ and a square root of -1 .
- **Square the modulus.** The modulus is a square root, and square roots do not expand; its square $|u|^2 = u\bar{u}$ is a product, and products do. So square, expand with conjugates, bound or compare the real numbers that appear, and take the non-negative square root back, which is legitimate because non-negative reals compare as their squares do. Section 1.2 uses it first, for $|zw| = |z||w|$; Section 1.3 names it and runs it in full for the triangle inequality. Exercise B2 of Section 1.3 leaves the last step to you, and Exercise C2 of

Section 1.3 the last half.

- **Multiply moduli, add angles.** In polar form a product is the product of the moduli and the sum of the arguments, so an equation $z^n = c$ splits into a real equation $r^n = \rho$ for the length and an angle condition $n\theta \in \alpha + 2\pi\mathbb{Z}$. It is named in Section 1.5, after the multiplication theorem, and gives De Moivre's formula there; Section 1.6 uses it to solve $z^n = c$ and to count the solutions. The warning of Section 1.6 shows what goes wrong when the angle condition is read as an equation $n\theta = \alpha$: all roots but one are lost.

1.1 The Complex Numbers as Pairs of Reals

The equation $x^2 + 1 = 0$ has no real solution. In an ordered field every square is non-negative (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e) for a non-zero element, and $0^2 = 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b)), so $x^2 + 1 \geq 0 + 1 = 1 > 0$ for every real x (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b), (e)). For most of school mathematics this gap is harmless. Later volumes cannot live with it: the linear-algebra volumes meet real matrices, such as a rotation of the plane, whose most useful data are not real numbers. This section builds the complex numbers, the number system that closes the gap, and proves that they obey the familiar laws of arithmetic.

Standing setting. Throughout the chapter, $\mathbb{R}$ is the complete ordered field built in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 5 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.6.3). In particular $\mathbb{R}$ is a field in the sense of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1, and every rule that book proved for ordered fields holds in it. No proof below looks inside a real number. Letters a, b, c, d, e, f, x, y stand for real numbers, and z, w, u, v for complex numbers, unless we say otherwise.

1.1.1 Building the new numbers

The quick way to introduce complex numbers is to say “invent a symbol i with $i^2 = -1$ and compute as usual”. That raises a fair worry. How do we know that such a symbol does not lead to a contradiction, the way “invent a number z with $0 \cdot z = 1$ ” does? The answer is to build the new numbers out of objects we already trust: pairs of real numbers.

Here is the recurring expression that suggests the definition. If we pretend $i^2 = -1$ and expand, we get

$$(a + bi)(c + di) = ac + adi + bci + bd i^2 = (ac - bd) + (ad + bc)i.$$

So a “number $a + bi$ ” is really the pair (a, b) , and the product should be the pair $(ac - bd, ad + bc)$. We take this formula as the definition, so nothing is pretended.

A complex number is a pair of real numbers, multiplied as if $i^2 = -1$.

Definition 1.1.1. Complex Numbers

The set of **complex numbers** is

$$\mathbb{C} := \mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\},$$

the Cartesian product of Sets and Functions, Definition 1.4.2, with **addition** and **multipli-**

cation defined for all $(a, b), (c, d) \in \mathbb{C}$ by

$$\begin{aligned}(a, b) + (c, d) &:= (a + c, b + d), \\ (a, b)(c, d) &:= (ac - bd, ad + bc).\end{aligned}$$

We write $i := (0, 1)$. For $z = (a, b) \in \mathbb{C}$, the **real part** of z is $\operatorname{Re} z := a$ and the **imaginary part** of z is $\operatorname{Im} z := b$.

In words: addition is coordinate by coordinate, as for points of the plane. Multiplication is the formula found by expanding. Both right-hand sides are pairs of real numbers, computed with the operations of $\mathbb{R}$, so both operations are functions $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$. The point i is the point one unit up the vertical axis. The real part and the imaginary part of z are its two coordinates, and both are **real** numbers.

There is nothing to check for well-definedness: a pair determines its coordinates, by the characteristic property of ordered pairs (Sets and Functions, Definition 1.4.1),

$$(a, b) = (c, d) \iff a = c \text{ and } b = d.$$

In the language of the definition: two complex numbers z and w are equal **if and only if** $\operatorname{Re} z = \operatorname{Re} w$ **and** $\operatorname{Im} z = \operatorname{Im} w$. So one equation between complex numbers is two equations between real numbers. This is the first named move of the chapter, **compare real and imaginary parts**, and the proofs of [Proposition 1.1.1](#) and [Proposition 1.1.2](#) below rest on it.

The equation that motivated everything is now a computation:

$$i \cdot i = (0, 1)(0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0).$$

To read the right-hand side as “ -1 ”, we have to see the real numbers inside $\mathbb{C}$.

1.1.2 The real numbers inside the complex numbers

The real number a should be the point $(a, 0)$ on the horizontal axis. Before we write a for $(a, 0)$, we check that nothing is lost: different real numbers stay different, and adding or multiplying two real numbers gives the same answer in $\mathbb{C}$ as in $\mathbb{R}$.

Proposition 1.1.1. The Real Numbers inside the Complex Numbers

Let $\iota: \mathbb{R} \rightarrow \mathbb{C}$ be the map $\iota(a) := (a, 0)$. Then ι is injective (Sets and Functions, Definition 1.5.3), and for all $a, c \in \mathbb{R}$,

$$\iota(a + c) = \iota(a) + \iota(c), \quad \iota(ac) = \iota(a) \iota(c), \quad \iota(1) = (1, 0).$$

Moreover $(a, b) = \iota(a) + \iota(b)i$ for all $a, b \in \mathbb{R}$, and $i \cdot i = \iota(-1)$.

Idea. Each claim is one application of the definitions: write both sides as pairs and compare coordinates. The facts about $\mathbb{R}$ needed are that 0 is neutral for addition (so subtracting 0 changes nothing), that 1 is neutral for multiplication, and that a product with 0 is 0, which kills the extra terms of the multiplication formula.

Proof. Let $a, c \in \mathbb{R}$. If $\iota(a) = \iota(c)$, then $(a, 0) = (c, 0)$, so $a = c$ by Sets and Functions, Definition 1.4.1; hence ι is injective. By Definition 1.1.1,

$$\iota(a) + \iota(c) = (a + c, 0 + 0) = (a + c, 0) = \iota(a + c),$$

and, since $a \cdot 0 = 0 \cdot c = 0 \cdot 0 = 0$ in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.2 (b)),

$$\iota(a) \iota(c) = (ac - 0 \cdot 0, a \cdot 0 + 0 \cdot c) = (ac, 0) = \iota(ac).$$

The equation $\iota(1) = (1, 0)$ is the definition of ι . Next, for $a, b \in \mathbb{R}$,

$$\iota(b) i = (b, 0)(0, 1) = (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) = (0, b),$$

so $\iota(a) + \iota(b) i = (a, 0) + (0, b) = (a, b)$. Finally $i \cdot i = (-1, 0) = \iota(-1)$ by the computation before the proposition. ■

Identification. From now on we write a for $\iota(a)$ and regard $\mathbb{R}$ as a subset of $\mathbb{C}$. In particular $0 = (0, 0)$ and $1 = (1, 0)$. This is a convenient abuse of notation made honest by the injective embedding, exactly as *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 2.2 wrote n for the integer $\iota(n)$: because ι is injective, different real numbers stay different, and because it preserves $+$ and $\cdot$, a sum or product of real numbers is the same whether computed in $\mathbb{R}$ or in $\mathbb{C}$.

With this convention the proposition reads

$$(a, b) = a + bi \quad \text{for all } a, b \in \mathbb{R}, \quad i^2 = i \cdot i = -1.$$

So the notation $a + bi$ is honest: it is a computation with the definitions, not a new symbol. Comparing real and imaginary parts now reads: for $a, b, c, d \in \mathbb{R}$,

$$a + bi = c + di \iff a = c \text{ and } b = d.$$

For $z = a + bi$ with $a, b \in \mathbb{R}$ we have $\operatorname{Re} z = a$ and $\operatorname{Im} z = b$. A real number $a = a + 0i$ is a complex number whose imaginary part is 0, and $0 = 0 + 0i$ is the only complex number with both parts 0. The point $i = 0 + 1i$ has real part 0 and imaginary part 1.

Warning. The rule “ $a + bi = c + di$ gives $a = c$ and $b = d$ ” needs a, b, c, d to be **real**. Without that it fails: $0 + 1 \cdot i = i + 0 \cdot i$, yet $0 \neq i$. Before comparing parts, write each side as $a + bi$ with a and b known to be real.

Example. First Computations in $\mathbb{C}$

Compute $(2 + 3i)(1 - i)$, the products $i \cdot i$, $(i \cdot i) \cdot i$ and $((i \cdot i) \cdot i) \cdot i$, and the product $(a + bi)(a - bi)$ for real a, b .

Solution. Here $1 - i$ is $1 + (-1)i$. By the multiplication rule with $a = 2$, $b = 3$, $c = 1$, $d = -1$,

$$(2 + 3i)(1 - i) = (2 \cdot 1 - 3 \cdot (-1)) + (2 \cdot (-1) + 3 \cdot 1)i = 5 + i.$$

We already know $i \cdot i = -1 = (-1, 0)$. Then

$$(i \cdot i) \cdot i = (-1, 0)(0, 1) = (0 - 0, -1 + 0) = (0, -1) = -i,$$

writing $-i$ for $0 + (-1)i$, and

$$((i \cdot i) \cdot i) \cdot i = (0, -1)(0, 1) = (0 - (-1), 0 + 0) = (1, 0) = 1.$$

Finally, with $a - bi = a + (-b)i$,

$$(a + bi)(a - bi) = (a^2 - b(-b)) + (a(-b) + ba)i = a^2 + b^2,$$

where $a^2 = aa$ and $b^2 = bb$ are computed in $\mathbb{R}$. This product is a real number, and it is **non-negative**, since $a^2 \geq 0$ and $b^2 \geq 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (e) for a non-zero real, and $0^2 = 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b)), so $a^2 + b^2 \geq 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b). We meet it again in Section 1.2, as the square of the length of $a + bi$.

The last product is the first hint of how division will work: multiplying $a + bi$ by $a - bi$ lands in the real numbers, where division is familiar.

Quick check. Compute $(1 + i)(1 + i)$. Is $\text{Im}(3 - 4i)$ equal to $-4i$?

Solution. By the multiplication rule, $(1 + i)(1 + i) = (1 \cdot 1 - 1 \cdot 1) + (1 \cdot 1 + 1 \cdot 1)i = 2i$. No: $3 - 4i = 3 + (-4)i$ with $3, -4 \in \mathbb{R}$, so $\text{Im}(3 - 4i) = -4$, a real number. The number $-4i$ is not real, since its imaginary part is $-4 \neq 0$.

A non-example by minimal change. Change one sign in the multiplication rule: define

$$(a, b) * (c, d) := (ac + bd, ad + bc),$$

which is what expanding gives if we pretend $j^2 = +1$ instead. Addition is unchanged. This product is still commutative, by commutativity in $\mathbb{R}$, and $(1, 0)$ is still an identity element: $(a, b) * (1, 0) = (a + 0, 0 + b) = (a, b)$. But

$$(1, 1) * (1, -1) = (1 - 1, -1 + 1) = (0, 0),$$

so two non-zero elements multiply to zero. Division breaks down too: $(1, 1) * (c, d) = (c + d, d + c)$ can never equal the identity element $(1, 0)$, because that would need $c + d = 1$ and $d + c = 0$ at once. So the non-zero element $(1, 1)$ has no inverse. *The single sign in $ac - bd$ is what makes division possible*, as Section 1.2 will show. Exercise B3 finds every element that goes wrong in this way.

Why this definition. We could have tried to postulate a number i with $i^2 = -1$, but a postulate is only as safe as the consistency of what it asserts. Pairs of reals are sets we already have, so $\mathbb{C}$ exists as soon as $\mathbb{R}$ does, and every law we want must now be **proved**. The multiplication formula is not a free choice either: Exercise C1 shows that in any field K containing $\mathbb{R}$, whose sum and product agree with those of $\mathbb{R}$ on real numbers, and containing a square root j of -1 , the product of $a + bj$ and $c + dj$ is forced to be $(ac - bd) + (ad + bc)j$. The minimal change above shows that a different formula really does give a different, and worse, system.

1.1.3 The laws of arithmetic

Before computing freely, we should confirm that rearranging, regrouping and expanding brackets are legal in $\mathbb{C}$. The definition does not promise this; it has to be checked.

Proposition 1.1.2. Arithmetic Laws in $\mathbb{C}$

For all $z, w, u \in \mathbb{C}$:

- (a) $z + w = w + z$ and $zw = wz$;
- (b) $(z + w) + u = z + (w + u)$ and $(zw)u = z(wu)$;
- (c) $z(w + u) = zw + zu$;
- (d) $z + 0 = z$, $z \cdot 1 = z$, and $z + (-z) = 0$, where $-(a + bi) := (-a) + (-b)i$ for $a, b \in \mathbb{R}$.

Idea. Every law reduces to the corresponding law for real numbers once both sides are written as pairs and compared part by part. Addition is coordinate by coordinate, so its laws are immediate. For multiplication the only real work is associativity: expand both sides and see that they produce the same four terms in each coordinate.

Proof. Let $z = a+bi$, $w = c+di$ and $u = e+fi$ with $a, b, c, d, e, f \in \mathbb{R}$. In each part we compute both sides with Definition 1.1.1 and compare real and imaginary parts, using the field laws of $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1) and the algebra of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2. Since addition acts coordinate by coordinate, the laws for addition in (a), (b) and (d) are the same laws in $\mathbb{R}$, applied to each coordinate; for (d), $z + 0 = (a + 0) + (b + 0)i = z$ and $z + (-z) = (a + (-a)) + (b + (-b))i = 0$.

- (a) By definition $zw = (ac - bd) + (ad + bc)i$ and $wz = (ca - db) + (cb + da)i$. These are equal because real multiplication and addition are commutative.
- (b) Expanding with the definition twice gives

$$\begin{aligned} (zw)u &= ((ac - bd)e - (ad + bc)f) \\ &\quad + ((ac - bd)f + (ad + bc)e)i \end{aligned}$$

and

$$\begin{aligned} z(wu) &= (a(ce - df) - b(cf + de)) \\ &\quad + (a(cf + de) + b(ce - df))i. \end{aligned}$$

Multiplying out with the distributive law of $\mathbb{R}$, both real parts equal $ace - adf - bcf - bde$, and both imaginary parts equal $acf + ade + bce - bdf$. Hence $(zw)u = z(wu)$.

- (c) We have $w + u = (c + e) + (d + f)i$, so

$$\begin{aligned} z(w + u) &= (a(c + e) - b(d + f)) + (a(d + f) + b(c + e))i \\ &= ((ac - bd) + (ae - bf)) + ((ad + bc) + (af + be))i, \end{aligned}$$

which is $zw + zu$ by the definitions of the product and the sum.

- (d) With $1 = 1 + 0i$, we get $z \cdot 1 = (a \cdot 1 - b \cdot 0) + (a \cdot 0 + b \cdot 1)i = a + bi = z$. The equations for addition were shown above. This proves the proposition. ■

In the language of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 2.3, the proposition checks the axioms of a commutative ring (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1): (a) is (F1) and (F6), (b) is (F2) and (F5), (c) is (F9), and (d) is (F3), (F7) and (F4). Moreover $1 \neq 0$ in $\mathbb{C}$, since $(1, 0) \neq (0, 0)$ by *Sets and Functions*, Definition 1.4.1, as $1 \neq 0$ in $\mathbb{R}$.

Remark. So $\mathbb{C}$, with the operations of Definition 1.1.1, is a **commutative ring** with $1 \neq 0$. Every result proved for commutative rings therefore holds in $\mathbb{C}$ without a new proof. From *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Proposition 2.3.2: 0, 1 and negatives are unique, $-(-z) = z$, $z \cdot 0 = 0$, $(-z)w = -(zw)$, $(-z)(-w) = zw$, and $(z+w)^2 = z^2 + 2zw + w^2$, where $z^2 := zz$. The remaining field axiom (F8), inverses of non-zero elements, is the subject of Section 1.2.

From now on we compute in $\mathbb{C}$ exactly as in $\mathbb{R}$: expand brackets, collect terms, and replace i^2 by -1 . The proposition is what makes that habit legitimate. For instance, $(a + bi)(a - bi) = a^2 - abi + abi - b^2 i^2 = a^2 + b^2$ agrees with Example (First Computations in $\mathbb{C}$).

1.1.4 Powers and a factorization

Powers in $\mathbb{C}$ are defined exactly as powers in an ordered field were, and that definition never used the order. We state it, and the laws of powers, for an arbitrary commutative ring, because the same proofs serve every commutative ring and later chapters need them in that generality.

Powers. Let R be a commutative ring and $z \in R$. The **powers** z^n , for $n \in \mathbb{N}$, are given by *Sets and Functions*, Theorem 2.3.1, read on $\mathbb{N} = \omega$ through *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Corollary 1.7.3 (b), with $X = R$, starting value 1 and step $(k, y) \mapsto yz$:

$$z^0 := 1, \quad z^{n+1} := z^n z \quad \text{for every } n \in \mathbb{N}.$$

This is the recursion of *Sets and Functions*, Section 2.3 (*Sets and Functions*, Definition 2.3.2), stated there for real numbers, and the same recursion as *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Definition 4.2.1 (b). In particular $z^1 = 1 \cdot z = z$ and $z^2 = z^1 z = zz$, matching the z^2 of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Proposition 2.3.2 (d).

Proposition 1.1.3. Laws of Powers in a Commutative Ring

Let R be a commutative ring (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Definition 2.3.1), let $z, w \in R$, and let $m, n \in \mathbb{N}$.

- (a) $z^{m+n} = z^m z^n$.
- (b) $(z^m)^n = z^{mn}$.
- (c) $(zw)^n = z^n w^n$.
- (d) If R is a field and $z \neq 0$, then $z^n \neq 0$.

Idea. The definition of z^n is a recursion on n , so every law is proved by induction on n , peeling off the last factor with $z^{n+1} = z^n z$. Each inductive step rests on one ingredient: associativity (F5) for (a), the law (a) for (b), associativity and commutativity (F5), (F6) for (c), and the absence of zero divisors in a field for (d).

Proof. Each part is proved by Logic and Proof, Axiom 4.2.1 (through Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Corollary 1.7.3 (b)) on n , with z , w and m fixed.

- (a) For $n = 0$: $z^{m+0} = z^m = z^m \cdot 1 = z^m z^0$, by (F7). If $z^{m+n} = z^m z^n$, then

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

by the recursion, the hypothesis and associativity (F5).

- (b) For $n = 0$: $(z^m)^0 = 1 = z^0 = z^{m \cdot 0}$. If $(z^m)^n = z^{mn}$, then $(z^m)^{n+1} = (z^m)^n z^m = z^{mn} z^m = z^{mn+m} = z^{m(n+1)}$, by the recursion, the hypothesis and (a).

- (c) For $n = 0$: $(zw)^0 = 1 = 1 \cdot 1 = z^0 w^0$. If $(zw)^n = z^n w^n$, then

$$(zw)^{n+1} = (zw)^n (zw) = (z^n w^n) (zw) = (z^n z) (w^n w) = z^{n+1} w^{n+1},$$

where the third equality regroups and reorders the four factors by (F5) and (F6).

- (d) Let R be a field and $z \neq 0$. For $n = 0$: $z^0 = 1 \neq 0$, by the definition of a field. If $z^n \neq 0$, then $z^{n+1} = z^n z$ is a product of two non-zero elements, so it is non-zero, since a field has no zero divisors (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Lemma 4.1.1 (d)).

■

Parts (a)–(c) are the laws of *Sets and Functions*, Section 2.3 (Sets and Functions, Proposition 2.3.4 (a)–(c)), proved there for real numbers; on $\mathbb{N} = \omega$, which is not a ring, law (a) is Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 1.6.4 (a), proved by the same induction. The proofs above are the same inductions, and they use only the ring axioms.

For a real number a , the power a^n is the same whether computed in $\mathbb{R}$ or in $\mathbb{C}$. Indeed $\iota(a^0) = \iota(1) = 1$, and if $\iota(a^n) = \iota(a)^n$, then $\iota(a^{n+1}) = \iota(a^n a) = \iota(a^n) \iota(a) = \iota(a)^{n+1}$, by Proposition 1.1.1; induction (Logic and Proof, Axiom 4.2.1) does the rest. So the identification of $\mathbb{R}$ with a subset of $\mathbb{C}$ is safe for powers too.

In the notation of powers, Example (First Computations in $\mathbb{C}$) computed $i^2 = -1$, $i^3 = -i$ and $i^4 = 1$; by (a), (b), every multiple of 4 gives $i^{4q} = (i^4)^q = 1^q = 1$, since $1^{q+1} = 1^q \cdot 1$ and induction give $1^q = 1$. Exercise B1 turns this into a rule for every power of i .

Quick check. Compute i^{10} and $(1+i)^4$, citing the parts of Proposition 1.1.3 you use.

Solution. By (a) and (b), $i^{10} = i^8 i^2 = (i^4)^2 i^2 = 1^2 \cdot (-1) = -1$. By (b), $(1+i)^4 = ((1+i)^2)^2 = (2i)^2$, and by (c), $(2i)^2 = 2^2 i^2 = 4 \cdot (-1) = -4$, using $(1+i)^2 = 2i$ from the first Quick check.

Finite sums. One identity about powers is used repeatedly in this chapter and later, and it needs sums of several terms. For elements $a_0, a_1, a_2, \dots$ of a commutative ring R and $n \in \mathbb{N}$, the sum $\sum_{k=0}^n a_k$ is defined by the recursion of Sets and Functions, Definition 2.3.1, with R as the set of values and the index starting at 0: the empty sum $\sum_{k=0}^{-1} a_k$ is 0, and

$$\sum_{k=0}^n a_k := \sum_{k=0}^{n-1} a_k + a_n \quad \text{for every } n \in \mathbb{N}.$$

So the recursion appends the last term. We also write $a_0 + a_1 + \cdots + a_n$ for this sum. Multiplying a sum by $c \in R$ multiplies each term: $(\sum_{k=0}^n a_k)c = \sum_{k=0}^n a_k c$, by induction on n , since $0 \cdot c = 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}R\setminus)$, Proposition 2.3.2 (b)) and the step is one use of the distributive law (F9).

Lemma 1.1.4. Difference of Powers

Let R be a commutative ring, let $z, w \in R$, and let $n \in \mathbb{N}$ with $n \geq 1$. Then

$$z^n - w^n = (z - w) \sum_{k=0}^{n-1} z^k w^{n-1-k}.$$

In particular $z^n - 1 = (z - 1)(1 + z + z^2 + \cdots + z^{n-1})$.

Idea. For $n = 2$ this is $z^2 - w^2 = (z - w)(w + z)$, and for $n = 3$ it is $z^3 - w^3 = (z - w)(w^2 + zw + z^2)$. To pass from n to $n + 1$, split $z^{n+1} - w^{n+1}$ so that the case n appears: $z^{n+1} - w^{n+1} = (z^n - w^n)w + z^n(z - w)$. The first piece is $(z - w)$ times the old sum times w , and the second supplies the one new term z^n , which the recursion appends at the end.

Proof. For $n \geq 1$ write $S_n := \sum_{k=0}^{n-1} z^k w^{n-1-k}$. We prove $z^{m+1} - w^{m+1} = (z - w)S_{m+1}$ for every $m \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 (through Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}R\setminus)$, Corollary 1.7.3 (b)) on m .

For $m = 0$: $S_1 = z^0 w^0 = 1$, so $(z - w)S_1 = z - w = z^1 - w^1$.

Let $n := m + 1 \geq 1$ and suppose $z^n - w^n = (z - w)S_n$. Expanding with (F9) and Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}R\setminus)$, Proposition 2.3.2 (c),

$$(z^n - w^n)w + z^n(z - w) = z^n w - w^n w + z^n z - z^n w = z^{n+1} - w^{n+1},$$

by the recursion for powers. By the hypothesis and the rule for multiplying a sum by w ,

$$(z^n - w^n)w = (z - w)S_n w = (z - w) \sum_{k=0}^{n-1} z^k w^{n-k},$$

since $w^{n-1-k}w = w^{n-k}$ for $k \leq n - 1$ (Proposition 1.1.3 (a)). Since $z^n = z^n w^0$, the recursion for sums gives

$$\begin{aligned} z^{n+1} - w^{n+1} &= (z - w) \left(\sum_{k=0}^{n-1} z^k w^{n-k} + z^n w^0 \right) \\ &= (z - w) \sum_{k=0}^n z^k w^{n-k} = (z - w)S_{n+1}. \end{aligned}$$

This completes the induction. The particular case is $w = 1$, since $1^j = 1$ for every $j \in \mathbb{N}$. ■

The lemma is the algebra behind the formula for a finite geometric sum: if $z - 1$ has an inverse, then $1 + z + \cdots + z^{n-1} = (z^n - 1)(z - 1)^{-1}$. Section 1.6 uses it again, for real numbers, to show that $0 \leq s < t$ gives $s^n < t^n$. Here we need only the identity.

1.1.5 Exercises

1.1.5.1 A. Check your understanding

Exercise. A1

- (a) Compute $(2 - i)(3 + 4i)$, and the real and imaginary parts of $i(1 + i)$.
- (b) True or false, with a reason: the equation $(a, b) = a + bi$, for $a, b \in \mathbb{R}$, needs a proof.
- (c) Which laws in [Proposition 1.1.2](#) need a genuine computation, and which follow coordinate by coordinate from the same laws in $\mathbb{R}$?
- (d) True or false, with a reason: if $z \in \mathbb{C}$ and $z^2 = 0$, then $z = 0$. Prove it by comparing real and imaginary parts, without using that $\mathbb{C}$ is a field.

Solution.

- (a) $(2 - i)(3 + 4i) = 6 + 8i - 3i - 4i^2 = 6 + 4 + 5i = 10 + 5i$. And $i(1 + i) = i + i^2 = -1 + i$, so $\operatorname{Re}(i(1 + i)) = -1$ and $\operatorname{Im}(i(1 + i)) = 1$.
- (b) True. The symbols a , b and i denote the pairs $(a, 0)$, $(b, 0)$, $(0, 1)$, and $a + bi$ is a sum and a product of pairs. That it equals (a, b) is a computation with [Definition 1.1.1](#); it is part of [Proposition 1.1.1](#).
- (c) The laws for addition, in (a), (b) and (d), hold coordinate by coordinate. Commutativity of multiplication, distributivity and $z \cdot 1 = z$ are one-line computations. Associativity of multiplication is the one law that needs a genuine expansion: both sides have four terms in each part, and they agree only after multiplying out.
- (d) True. Let $z = a + bi$. Then $z^2 = (a^2 - b^2) + 2abi$, so $z^2 = 0$ gives $a^2 - b^2 = 0$ and $2ab = 0$, by comparing parts. Since $2 \neq 0$ in $\mathbb{R}$ and $\mathbb{R}$ has no zero divisors (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Lemma 4.1.1 (d)), $a = 0$ or $b = 0$. If $a = 0$, then $-b^2 = 0$, so $b^2 = 0$ and $b = 0$ by the same rule; if $b = 0$, then $a^2 = 0$ and $a = 0$. So $z = 0$. (Once Section 1.2 has shown that $\mathbb{C}$ is a field, this follows at once from Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Lemma 4.1.1 (d) in $\mathbb{C}$.)

1.1.5.2 B. Practice

Exercise. B1: Powers of i

Let $n \in \mathbb{N}$, and let r be the remainder of n on division by 4. Prove that $i^n = i^r$. Hence compute i^{2026} .

Solution. By division with remainder (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Theorem 3.1.2, with $n \in \mathbb{N} \subseteq \mathbb{Z}$ and divisor 4) there are integers q, r with $n = 4q + r$ and $0 \leq r < 4$. Also $q \geq 0$: if $q \leq -1$, then $n \leq -4 + r < 0$, which is false. So $q, r \in \mathbb{N}$. By [Proposition 1.1.3](#) (a) and (b), and $i^4 = 1$ ([Example \(First Computations in \$\mathbb{C}\$ \)](#)),

$$i^n = i^{4q}i^r = (i^4)^q i^r = 1^q i^r = i^r,$$

where $1^q = 1$ by induction on q ($1^{q+1} = 1^q \cdot 1$). So i^n is $1, i, -1, -i$ according as $r = 0, 1, 2, 3$.

Hence, since $2026 = 4 \cdot 506 + 2$, $i^{2026} = i^2 = -1$.

Exercise. B2

- (a) Use [Lemma 1.1.4](#) to factor $z^3 - 1$ and $z^4 - 1$ in $\mathbb{C}$, and check the second factorization at $z = i$.
- (b) Verify $(1 + i)^4 = -4$ using $(1 + i)^2 = 2i$ and [Proposition 1.1.3](#). Hence show that, for every $z \in \mathbb{C}$,

$$z^4 + 4 = (z - (1 + i))(z^3 + (1 + i)z^2 + 2iz + (-2 + 2i)).$$

Solution.

- (a) With $n = 3$ and $n = 4$,

$$z^3 - 1 = (z - 1)(1 + z + z^2), \quad z^4 - 1 = (z - 1)(1 + z + z^2 + z^3).$$

At $z = i$: the left side is $i^4 - 1 = 0$, and on the right $1 + i + i^2 + i^3 = 1 + i - 1 - i = 0$, so both sides are 0.

- (b) By (b) of the proposition with $m = n = 2$, and then (c),

$$(1 + i)^4 = ((1 + i)^2)^2 = (2i)^2 = 2^2 i^2 = -4.$$

Let $w := 1 + i$. Then $w^2 = 2i$ and $w^3 = w^2 w = 2i(1 + i) = -2 + 2i$. By [Lemma 1.1.4](#) with $n = 4$, whose sum is $w^3 + zw^2 + z^2 w + z^3$,

$$z^4 - w^4 = (z - w)(z^3 + wz^2 + w^2 z + w^3).$$

Since $w^4 = -4$, the left side is $z^4 + 4$, and substituting w, w^2, w^3 gives the displayed factorization. In particular $1 + i$ is a root of $z^4 + 4$.

Exercise. B3: The zero divisors of the minimal change

Let $*$ be the product $(a, b) * (c, d) := (ac + bd, ad + bc)$ on $\mathbb{R}^2$ of the non-example in this section. Call a non-zero $p \in \mathbb{R}^2$ a **zero divisor** if $p * q = (0, 0)$ for some non-zero $q \in \mathbb{R}^2$. Prove that a non-zero (a, b) is a zero divisor if and only if $a^2 = b^2$, that such an (a, b) has no inverse (no q gives $(a, b) * q = (1, 0)$), and that if $a^2 \neq b^2$, then $(a, b) * (ta, -tb) = (1, 0)$ for $t := (a^2 - b^2)^{-1}$.

Solution. First, for any real t ,

$$(a, b) * (ta, -tb) = (ta^2 - tb^2, -tab + tab) = (t(a^2 - b^2), 0).$$

If $a^2 \neq b^2$, then $a^2 - b^2 \neq 0$ has an inverse in $\mathbb{R}$, and $t := (a^2 - b^2)^{-1}$ gives $(1, 0)$.

($\Leftarrow$) Let $(a, b) \neq (0, 0)$ with $a^2 = b^2$. Then $(a - b)(a + b) = a^2 - b^2 = 0$, so $b = a$ or $b = -a$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 4.1.1 (d) in $\mathbb{R}$). If $b = a$, then $(a, a) * (1, -1) = (a - a, -a + a) = (0, 0)$; if $b = -a$, then $(a, -a) * (1, 1) = (a - a, a - a) = (0, 0)$. In both cases the second factor is non-zero, so (a, b) is a zero divisor. Such an element also has no inverse: $(a, a) * (c, d) = (a(c + d), a(c + d))$ has equal coordinates and $(a, -a) * (c, d) = (a(c - d), -a(c - d))$ has opposite coordinates, while $(1, 0)$ has neither,

since $1 \neq 0$ and $1 \neq -0 = 0$.

($\Rightarrow$) We prove the contrapositive (Logic and Proof, Proposition 2.3.2). Let $a^2 \neq b^2$, and suppose $(a, b) * (c, d) = (0, 0)$, that is, $ac + bd = 0$ and $ad + bc = 0$. Multiply the first equation by a and the second by b , and subtract: $a^2c + abd - abd - b^2c = 0$, that is, $(a^2 - b^2)c = 0$. Multiply the first by b and the second by a , and subtract: $(b^2 - a^2)d = 0$. Since $a^2 - b^2 \neq 0$ and $\mathbb{R}$ has no zero divisors, $c = 0$ and $d = 0$. So the only q with $(a, b) * q = (0, 0)$ is $q = (0, 0)$, and (a, b) is not a zero divisor. No associativity of $*$ was needed.

For example, $(1, 1)$ is a zero divisor, as in the text, and $(2, 1)$ is not: $(2, 1) * (2/3, -1/3) = (4/3 - 1/3, -2/3 + 2/3) = (1, 0)$.

1.1.5.3 C. Going deeper

Exercise. C1: There is only one way to adjoin a square root of minus one

Let K be a field (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Definition 2.3.1) with $\mathbb{R} \subseteq K$, such that the sum and the product of K , applied to two real numbers, are their sum and product in $\mathbb{R}$. Let $j \in K$ with $j^2 = -1$.

- (a) Show that 0 , 1 , negatives and inverses of non-zero real numbers are the same in K as in $\mathbb{R}$.
- (b) Show that if $a + bj = c + dj$ with $a, b, c, d \in \mathbb{R}$, then $a = c$ and $b = d$.
- (c) Let $\varphi: \mathbb{C} \rightarrow K$, $\varphi(a + bi) := a + bj$ for $a, b \in \mathbb{R}$. Show that φ is injective, $\varphi(1) = 1$, and $\varphi(z + w) = \varphi(z) + \varphi(w)$, $\varphi(zw) = \varphi(z)\varphi(w)$ for all $z, w \in \mathbb{C}$.

Solution (Hint 1). For (a), start from $0 + 0 = 0$ and $1 \cdot 1 = 1$ in $\mathbb{R}$ and cancel in K : add the negative of $0_{\mathbb{R}}$; for 1 , multiply by the inverse of $1_{\mathbb{R}}$, which exists because $1_{\mathbb{R}} \neq 0_{\mathbb{R}} = 0_K$. For $-a$ and a^{-1} , use that each is the **only** element with its property (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (a), Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Lemma 4.1.1 (a)). For (b), ask what happens if $b \neq d$.

Solution (Hint 2). For (b): suppose $b \neq d$. Then $(d - b)j = a - c$, and $d - b$ is a non-zero real number.

Solution.

- (a) In $\mathbb{R}$, $0_{\mathbb{R}} + 0_{\mathbb{R}} = 0_{\mathbb{R}}$; the same equation holds in K , since the sum of K on reals is that of $\mathbb{R}$. Adding $-0_{\mathbb{R}}$ (the negative in K) to both sides gives $0_{\mathbb{R}} = 0_K$. Next, $1_{\mathbb{R}} \cdot 1_{\mathbb{R}} = 1_{\mathbb{R}}$ in K , and $1_{\mathbb{R}} \neq 0_{\mathbb{R}} = 0_K$; multiplying by the inverse of $1_{\mathbb{R}}$ in K gives $1_{\mathbb{R}} = 1_K$. For $a \in \mathbb{R}$, the real negative $-a$ satisfies $a + (-a) = 0_{\mathbb{R}} = 0_K$ in K , so it is the negative of a in K , by uniqueness of negatives (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (a)). Likewise, for real $a \neq 0$, the real inverse satisfies $aa^{-1} = 1_{\mathbb{R}} = 1_K$ in K , so it is the inverse of a in K (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Lemma 4.1.1 (a)). So sums, products, differences and quotients of real numbers computed in K are real numbers.
- (b) Suppose $a + bj = c + dj$, and suppose, for contradiction, that $b \neq d$. Then $(d - b)j = a - c$,

with $d - b$ a non-zero real number, so $j = (a - c)(d - b)^{-1}$, which is real by (a). Then j^2 is the square of a real number, computed in $\mathbb{R}$. Here $j \neq 0$, since $0^2 = 0 \neq -1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b)), so $j^2 > 0$ in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)). But $j^2 = -1 < 0$ in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e), (a)), and $0 < j^2 < 0$ contradicts (O1). Hence $b = d$, and then $a = c$ by adding $-bj$ to both sides.

- (c) The map is a function, since $a + bi$ determines a and b (Proposition 1.1.1). It is injective by (b): $a + bj = c + dj$ gives $a = c$ and $b = d$, so $a + bi = c + di$. Also $\varphi(1) = \varphi(1 + 0i) = 1 + 0j = 1$. For $z = a + bi$ and $w = c + di$, the field laws of K give

$$\varphi(z) + \varphi(w) = (a + c) + (b + d)j = \varphi(z + w),$$

and, with $j^2 = -1$,

$$\begin{aligned}\varphi(z)\varphi(w) &= ac + adj + bcj + bdj^2 \\ &= (ac - bd) + (ad + bc)j = \varphi(zw),\end{aligned}$$

by Definition 1.1.1. This proves (c).

So any field that contains $\mathbb{R}$ and a square root j of -1 contains an exact copy of $\mathbb{C}$, namely $\{a + bj : a, b \in \mathbb{R}\}$, and its arithmetic is forced to be the arithmetic of Definition 1.1.1. *Algebraic Preliminaries*, Chapter 1 meets more fields of this shape, built from a smaller field and one new element, such as $\{a + bi : a, b \in \mathbb{Q}\}$.

Marking scheme. (10 points) - 2: (a) identifies 0 and 1 of $\mathbb{R}$ in K by cancellation, and negatives and inverses of reals by uniqueness. - 3: (b) shows that $b \neq d$ would make j real, with the division justified by $d - b \neq 0$. - 2: (b) derives the contradiction from $j^2 > 0$ in $\mathbb{R}$ (with $j \neq 0$) and $-1 < 0$, naming the ordered-field rule. - Second route for (b): squaring $(b - d)j = c - a$ with $j^2 = -1$, and noting by (a) that the result is an equation between real numbers, earns the 3 points; concluding from $(c - a)^2 + (b - d)^2 = 0$ that $a = c$ and $b = d$, from squares ≥ 0 in $\mathbb{R}$, naming the ordered-field rule, earns the 2 points. - 1: (c) injectivity, from (b). - 2: (c) the sum and the product, expanding with $j^2 = -1$ and comparing with Definition 1.1.1. Fatal errors (0 for the step): treating j as i (the point is that K is any field); claiming $j^2 \geq 0$ in K (there is no order on K).

1.2 Conjugate, Modulus, and Division

Section 1.1 built $\mathbb{C}$ and showed that it is a commutative ring with $1 \neq 0$ (Proposition 1.1.2). One field axiom is still missing: (F8), which asks for an inverse of every non-zero element. To divide by $3 + 4i$, we want a number to multiply by that lands in the real numbers, where division is familiar. The product $(a + bi)(a - bi) = a^2 + b^2$ of Example (First Computations in $\mathbb{C}$) shows which number does the job. This section gives its two ingredients names, the conjugate and the modulus, proves the rules they obey, and concludes that $\mathbb{C}$ is a field.

1.2.1 Conjugate and modulus

A complex number $z = a + bi$ is a point (a, b) of the plane. Two pieces of plane geometry turn out to be algebra in disguise: the mirror image of z in the horizontal axis, and the distance of z from 0. The mirror image changes the sign of b . The distance, by Pythagoras, is the square root of $a^2 + b^2$, the very number that appeared in Example (First Computations in $\mathbb{C}$). Square roots of non-negative real numbers exist and are unique in every complete ordered field (Number

Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4), so we may use them in $\mathbb{R}$: for $x \in \mathbb{R}$ with $x \geq 0$, $\sqrt{x}$ is the **unique** $y \in \mathbb{R}$ with $y \geq 0$ and $y^2 = x$.

Conjugating reflects a point in the real axis; the modulus is its distance from the origin.

Definition 1.2.1. Conjugate and Modulus

Let $z = a + bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$. The **complex conjugate** of z is

$$\bar{z} := a - bi.$$

The **modulus** (or absolute value) of z is the real number

$$|z| := \sqrt{a^2 + b^2},$$

the **non-negative** square root of $a^2 + b^2$. Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4 in $\mathbb{R}$.

In words: the conjugate keeps the real part and flips the sign of the imaginary part, $\operatorname{Re} \bar{z} = \operatorname{Re} z$ and $\operatorname{Im} \bar{z} = -\operatorname{Im} z$. The modulus is a **real** number, never negative, and its square is $a^2 + b^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2$.

Well-definedness. Since z determines a and b (compare real and imaginary parts, Section 1.1), the right-hand sides depend only on z . The square root exists because its argument is non-negative: $a^2 \geq 0$ and $b^2 \geq 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e), with $0^2 = 0$ when the number is 0), so $a^2 + b^2 \geq 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b)). And $\mathbb{R}$ is complete (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.6.3), which is the hypothesis of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4. This is where the completeness of $\mathbb{R}$ enters the chapter. Over $\mathbb{Q}$ alone the definition would break down at once: $|1 + i|$ would have to be a rational number whose square is 2, and there is none (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.6.1).

Examples.

A point with integer distance. For $z = 3 + 4i$: $\bar{z} = 3 - 4i$, and $|z| = \sqrt{9 + 16} = \sqrt{25} = 5$. The last step is the uniqueness clause of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4: $5 \geq 0$ and $5^2 = 25$, so 5 is **the** non-negative square root of 25.

The unit i . $\bar{i} = \overline{0 + 1i} = 0 - 1i = -i$, and $|i| = \sqrt{0 + 1} = 1$, since $1 \geq 0$ and $1^2 = 1$.

The degenerate case $z = 0$. $\bar{0} = 0$ and $|0| = \sqrt{0} = 0$. We show below that 0 is the **only** complex number with modulus 0; that one fact is what makes division possible.

A real number. For $a \in \mathbb{R}$, $\bar{a} = a$ and $|a| = \sqrt{a^2}$. The symbol $|a|$ already had a meaning for real a : the absolute value of an ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 4.1.1). The next proposition shows the two meanings agree, so the notation does not clash.

Proposition 1.2.1. The Modulus Extends the Absolute Value

Let $a \in \mathbb{R} \subseteq \mathbb{C}$. Then $\bar{a} = a$, and the modulus $\sqrt{a^2 + 0^2}$ of a equals the absolute value of a in the ordered field $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 4.1.1).

Proof. Write $a = a + 0i$. Then $\bar{a} = a - 0i = a$, since $0 \cdot i = i \cdot 0 = 0$ by (F6) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b), and $-0 = 0$ because $0 + 0 = 0$ and negatives are unique (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (a)), all in the commutative ring $\mathbb{C}$. The modulus of a is $\sqrt{a^2 + 0^2} = \sqrt{a^2}$, the unique non-negative real number whose square is a^2 . The absolute value $|a|$ of the ordered field $\mathbb{R}$ is non-negative and satisfies $|a|^2 = a^2$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 (a), (b)). By the uniqueness clause of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4, the two are equal. ■

So the modulus **extends** the absolute value: on $\mathbb{R} \subseteq \mathbb{C}$ it is the old $|\cdot|$, and every result about $|x|$ for real x stays true with the new reading. For instance $|-3| = 3$, whichever definition we use.

Quick check. Find $\bar{z}$ and $|z|$ for $z = -2i$ and for $z = 1 - i$. For which of the two is $\bar{z} = z$?

Solution. For $z = -2i = 0 + (-2)i$: $\bar{z} = 0 - (-2)i = 2i$ and $|z| = \sqrt{0^2 + 4} = 2$, since $2 \geq 0$ and $2^2 = 4$. For $z = 1 - i$: $\bar{z} = 1 + i$ and $|z| = \sqrt{1^2 + 1} = \sqrt{2}$. In neither case is $\bar{z} = z$: comparing imaginary parts, $\bar{z} = z$ needs $\text{Im } z = -\text{Im } z$, that is $\text{Im } z = 0$, and both numbers have non-zero imaginary part.

Why this definition. The square root is what makes the modulus a length. Without it, the simpler quantity $N(z) := a^2 + b^2$ would do some of the same jobs: it is $z\bar{z}$, and it vanishes only at 0. But on real numbers it is $N(a) = a^2$, not $|a|$, so it does not extend the absolute value: $N(2) = 4$. And it is not a sensible distance: $N(1+1) = 4$, while $N(1) + N(1) = 2$, so the “side” from 0 to 2 would be longer than the two sides through 1. The modulus keeps the convenient algebra of N , since $|z|^2 = N(z)$, and adds the right size. Section 1.3 exploits exactly this square.

Warning. The modulus squared is $z\bar{z}$, **not** zz . In general $|z|^2 \neq z^2$: for $z = i$, $|i|^2 = 1$ but $i^2 = -1$. The two agree only when z is real. For $z = a + bi$, $z^2 = (a^2 - b^2) + 2abi$ and $|z|^2 = a^2 + b^2$; if they are equal, comparing real parts gives $a^2 - b^2 = a^2 + b^2$, so $2b^2 = 0$. Since $2 > 0$ in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (h)), $2 \neq 0$, so $b^2 = 0$ by part (f), and $b = 0$ by part (e). Conversely, for real $z = a$, $|a|^2 = a^2 + 0^2 = a^2$.

1.2.2 Rules for conjugate and modulus

The following rules are used constantly, in this chapter and much later for complex inner products. They say that conjugation respects both operations, and that the modulus respects products.

Theorem 1.2.2. Properties of Conjugation and Modulus

For all $z, w \in \mathbb{C}$:

- (a) $\overline{z+w} = \bar{z} + \bar{w}$ and $\overline{\bar{z}} = z$;
- (b) $\overline{zw} = \bar{z}\bar{w}$;
- (c) $z\bar{z} = |z|^2$ and $z + \bar{z} = 2\operatorname{Re} z$;
- (d) $|zw| = |z||w|$ and $|\bar{z}| = |z|$;
- (e) $|z| = 0$ if and only if $z = 0$.

Idea. Parts (a)–(c) and (e) are direct computations with real and imaginary parts. For (d), expanding $|zw|$ directly is legitimate but messy, since a square root of a long sum appears. It is cleaner to square: by (c) a squared modulus is a product with a conjugate, and (b) lets the conjugate split across the product. Two non-negative real numbers with the same square are equal, and that brings us back from squares to moduli.

Proof. Let $z = a + bi$ and $w = c + di$ with $a, b, c, d \in \mathbb{R}$.

- (a) We have $\overline{z+w} = (a+c) - (b+d)i = (a-bi) + (c-di) = \bar{z} + \bar{w}$, since $-(b+d) = (-b) + (-d)$: $(b+d) + ((-b) + (-d)) = 0$, and negatives are unique (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (a) in $\mathbb{R}$). And $\bar{\bar{z}} = a + (-b)i$, so $\bar{\bar{z}} = a - (-b)i = a + bi = z$, by Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (a) in $\mathbb{R}$.
- (b) Since $zw = (ac - bd) + (ad + bc)i$, we get $\overline{zw} = (ac - bd) - (ad + bc)i$. On the other hand, by Definition 1.1.1 and Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (c) in $\mathbb{R}$,

$$\begin{aligned}\bar{z}\bar{w} &= (a + (-b)i)(c + (-d)i) \\ &= (ac - (-b)(-d)) + (a(-d) + (-b)c)i \\ &= (ac - bd) - (ad + bc)i.\end{aligned}$$

- (c) By Example (First Computations in $\mathbb{C}$), $z\bar{z} = a^2 + b^2$, and $a^2 + b^2 = |z|^2$ because $|z|$ is a square root of $a^2 + b^2$. Also $z + \bar{z} = (a + a) + (b - b)i = 2a = 2\operatorname{Re} z$.
- (d) By (c), then (b), then Proposition 1.1.2 to regroup and reorder the four factors,

$$|zw|^2 = (zw)\overline{zw} = zw\bar{z}\bar{w} = (z\bar{z})(w\bar{w}) = |z|^2|w|^2.$$

In $\mathbb{R}$, $|z|^2|w|^2 = (|z||w|)^2$ (Proposition 1.1.3 (c)), and $|z||w| \geq 0$: it is 0 if one factor is 0 (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (b)), and positive otherwise, since a product of two positive elements of an ordered field is positive ((O4) of Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Definition 2.3.2). So $|zw|$ and $|z||w|$ are both non-negative real numbers whose square is $|z|^2|w|^2$. By the uniqueness clause of Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 6.1.4 they are equal. Finally $|\bar{z}| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$, since $(-b)^2 = b^2$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (c)).

- (e) If $z = 0$, then $|z| = \sqrt{0} = 0$. Conversely, let $|z| = 0$, so $a^2 + b^2 = |z|^2 = 0$. If $a \neq 0$, then $a^2 > 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (e)) and $b^2 \geq 0$, so $a^2 + b^2 > 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (b)), a contradiction; hence $a = 0$. Then $b^2 = 0$, and the same rule gives $b = 0$. So $z = 0$. This proves the theorem. ■

The proof of (d) is our first use of a move that runs through the whole chapter: a statement about a modulus $|u|$ becomes a statement about $|u|^2 = u\bar{u}$, which is algebra; we compute there, and come back by taking non-negative square roots. Section 1.3 names it, *square the modulus*, and uses it to prove the triangle inequality.

Two remarks on what the theorem says. First, (a) and (b) say that conjugation respects sums and products, and it fixes 1. Not every reflection does: the reflection in the vertical axis, $z \mapsto -\bar{z}$, respects sums, but it sends 1 to -1 , and $1 \cdot 1 = 1$ to -1 , while the product of the images is $(-1)(-1) = 1$. Second, (d) says that the size of a product is the product of the sizes. In the plane picture, multiplying by w stretches every length by $|w|$; Section 1.5 completes this picture with angles.

1.2.3 Division

The first payoff is division. If $z \neq 0$, then $|z| \neq 0$ by (e), so $|z|^2$ is a **strictly** positive real number, and we may divide by it in $\mathbb{R}$.

Proposition 1.2.3. Inverse of a Complex Number

Let $z \in \mathbb{C}$ with $z \neq 0$. Then

$$w := \frac{1}{|z|^2} \bar{z}$$

satisfies $zw = 1$. We write z^{-1} or $\frac{1}{z}$ for this w .

Proof. Since $z \neq 0$, $|z| \neq 0$ by Theorem 1.2.2 (e), so $|z|^2 > 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e). In particular $|z|^2 \neq 0$, so it has an inverse $1/|z|^2$ in the field $\mathbb{R}$. By Proposition 1.1.2 and Theorem 1.2.2 (c),

$$zw = \frac{1}{|z|^2} (z\bar{z}) = \frac{1}{|z|^2} |z|^2 = 1,$$

where the last product is computed in $\mathbb{R}$, which gives the same result as in $\mathbb{C}$ (Proposition 1.1.1). This proves the proposition. ■

The hypothesis $z \neq 0$ is used exactly once, to make $|z|^2$ non-zero, so that $1/|z|^2$ exists. For $z = 0$ there is nothing to rescue: $0 \cdot w = 0 \neq 1$ for every w (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b)). The proposition gives one inverse; that it is the only one is a fact about all fields, which we can cite as soon as we know that $\mathbb{C}$ is one.

Theorem 1.2.4. The Complex Numbers Form a Field

The set $\mathbb{C}$, with the operations of Definition 1.1.1, is a field in the sense of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1. Moreover $\mathbb{R} \subseteq \mathbb{C}$ (Proposition 1.1.1) is closed under the field operations of $\mathbb{C}$: for $a, c \in \mathbb{R}$, the sum $a + c$, the product ac , the negative $-a$ and, if $a \neq 0$, the inverse a^{-1} , computed in $\mathbb{C}$, are the real numbers computed in $\mathbb{R}$.

Proof. By [Proposition 1.1.2](#) and the remark after it, $\mathbb{C}$ satisfies (F1)–(F7) and (F9), and $1 \neq 0$ in $\mathbb{C}$. By [Proposition 1.2.3](#), every non-zero $z \in \mathbb{C}$ has an element z^{-1} with $zz^{-1} = 1$, which is (F8). So $\mathbb{C}$ is a field.

For $a, c \in \mathbb{R}$, the sum and product are those of $\mathbb{R}$ by [Proposition 1.1.1](#). The real negative $-a$ satisfies $a + (-a) = 0$ in $\mathbb{R}$, hence in $\mathbb{C}$, so it is the negative of a in $\mathbb{C}$, by uniqueness of negatives (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (a)). If $a \neq 0$, the real inverse a^{-1} satisfies $aa^{-1} = 1$ in $\mathbb{R}$, hence in $\mathbb{C}$; and $a \neq 0$ in $\mathbb{C}$, since ι is injective. So a^{-1} is the inverse of a in $\mathbb{C}$, by uniqueness of inverses in the field $\mathbb{C}$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Lemma 4.1.1 (a)).

■

Everything proved for an arbitrary field now holds in $\mathbb{C}$, without a new proof. From Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Lemma 4.1.1: the inverse z^{-1} is the **only** y with $zy = 1$, and $(zw)^{-1} = z^{-1}w^{-1}$ for non-zero z, w ; fractions $z/w := zw^{-1}$ add and multiply by the usual rules; and $\mathbb{C}$ has **no zero divisors**: $zw = 0$ forces $z = 0$ or $w = 0$. By [Proposition 1.1.3](#) (d), $z^n \neq 0$ whenever $z \neq 0$. These are the facts that the rest of the chapter uses when it cancels a non-zero factor.

Remark. *Algebraic Preliminaries*, Chapter 1 collects fields as a notion with many examples, finite and infinite. This theorem is the one it cites for $\mathbb{C}$, and $\mathbb{R} \subseteq \mathbb{C}$, with the closure just proved, is one of its examples of one field inside another.

In practice, a quotient is computed by “multiplying top and bottom by the conjugate”. For $w \neq 0$, [Proposition 1.2.3](#) gives

$$\frac{z}{w} = zw^{-1} = \frac{z\bar{w}}{|w|^2},$$

which is the fraction z/w multiplied by $\bar{w}/\bar{w} = 1$ (here $\bar{w} \neq 0$, since $|\bar{w}| = |w| \neq 0$ by [Theorem 1.2.2](#) (d), (e)) and simplified with the product rule for fractions (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Lemma 4.1.1 (b)): the new denominator $w\bar{w} = |w|^2$ is real.

Example. Dividing Complex Numbers

Write $\frac{1}{3+4i}$ and $\frac{5+i}{1-i}$ in the form $a+bi$ with $a, b \in \mathbb{R}$.

Solution. For the first, $|3+4i|^2 = 25$ and $\overline{3+4i} = 3-4i$, so by [Proposition 1.2.3](#)

$$\frac{1}{3+4i} = \frac{3-4i}{25} = \frac{3}{25} - \frac{4}{25}i.$$

Check: $(3+4i)(3-4i) = 9+16 = 25$, so the product with $3+4i$ is $25/25 = 1$.

For the second, $|1-i|^2 = 2$ and $\overline{1-i} = 1+i$, so

$$\frac{5+i}{1-i} = \frac{(5+i)(1+i)}{2} = \frac{5+5i+i+i^2}{2} = \frac{4+6i}{2} = 2+3i.$$

This agrees with $(2+3i)(1-i) = 5+i$ from [Example \(First Computations in \$\mathbb{C}\$ \)](#): since

$1 - i \neq 0$, the quotient is the **only** u with $u(1 - i) = 5 + i$. Indeed, if $u(1 - i) = 5 + i$, then $u = u \cdot 1 = u((1 - i)(1 - i)^{-1}) = (u(1 - i))(1 - i)^{-1} = (5 + i)(1 - i)^{-1}$, by (F7), (F8) and (F5) in the field $\mathbb{C}$ ([Theorem 1.2.4](#)).

Quick check. Compute $|(1+i)(1-i)|$ in two ways: by multiplying first, and by [Theorem 1.2.2](#) (d). Then compute $1/i$.

Solution. Multiplying first, $(1+i)(1-i) = 1+1 = 2$, so the modulus is $|2| = 2$. By (d), it is $|1+i||1-i| = \sqrt{2} \cdot \sqrt{2} = 2$, since $\sqrt{2}\sqrt{2} = (\sqrt{2})^2 = 2$. And $1/i = \bar{i}/|i|^2 = -i/1 = -i$; check: $i(-i) = -i^2 = 1$.

1.2.4 Exercises

1.2.4.1 A. Check your understanding

Exercise. A1

- (a) Define the complex conjugate $\bar{z}$ and the modulus $|z|$ of $z = a + bi$, where $a, b \in \mathbb{R}$. Which earlier result guarantees that $|z|$ exists?
- (b) True or false, with a reason: $z\bar{z}$ is a non-negative real number for every $z \in \mathbb{C}$.
- (c) Where exactly is the hypothesis $z \neq 0$ used in the proof of [Proposition 1.2.3](#)?
- (d) Write $1/(1+2i)$ in the form $a + bi$ with $a, b \in \mathbb{R}$.

Solution.

- (a) $\bar{z} := a - bi$ and $|z| := \sqrt{a^2 + b^2}$, the non-negative square root. It exists by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4, since $\mathbb{R}$ is a complete ordered field and $a^2 + b^2 \geq 0$.
- (b) True. By [Theorem 1.2.2](#) (c), $z\bar{z} = |z|^2$, the square of a real number, and squares of real numbers are non-negative (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e) when $|z| \neq 0$, and $0^2 = 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b) when $|z| = 0$).
- (c) It gives $|z| \neq 0$ by [Theorem 1.2.2](#) (e), hence $|z|^2 > 0$, so that $1/|z|^2$ exists in $\mathbb{R}$. Nowhere else.
- (d) $|1+2i|^2 = 1+4 = 5$ and $\overline{1+2i} = 1-2i$, so $1/(1+2i) = (1-2i)/5 = \frac{1}{5} - \frac{2}{5}i$. Check: $(1+2i)(1-2i) = 5$.

1.2.4.2 B. Practice

Exercise. B1: Arithmetic

Write each of the following in the form $a + bi$ with $a, b \in \mathbb{R}$, or as a real number where indicated.

- (a) $(3 - 2i)(4 + i)$.
 (b) $\frac{1 + 2i}{2 - i}$.
 (c) $|(3 + 4i)(5 - 12i)|$, without expanding the product.
 (d) $\operatorname{Re} \frac{1}{1 + i}$ and $\operatorname{Im} \frac{1}{1 + i}$.

Solution.

- (a) $(3 - 2i)(4 + i) = 12 + 3i - 8i - 2i^2 = 14 - 5i$.
 (b) By [Proposition 1.2.3](#), multiply by $\overline{2 - i} = 2 + i$ and divide by $|2 - i|^2 = 5$:

$$\frac{1 + 2i}{2 - i} = \frac{(1 + 2i)(2 + i)}{5} = \frac{2 + i + 4i + 2i^2}{5} = \frac{5i}{5} = i.$$

Check: $i(2 - i) = 2i - i^2 = 1 + 2i$.

- (c) By [Theorem 1.2.2](#) (d), $|(3 + 4i)(5 - 12i)| = |3 + 4i| |5 - 12i| = 5 \cdot 13 = 65$, since $|5 - 12i| = \sqrt{25 + 144} = \sqrt{169} = 13$ ($13 \geq 0$ and $13^2 = 169$).
 (d) $\frac{1}{1 + i} = \frac{1 - i}{2} = \frac{1}{2} - \frac{1}{2}i$, so the real part is $1/2$ and the imaginary part is $-1/2$.

Exercise. B2

Let $z \in \mathbb{C}$. Prove:

- (a) $\operatorname{Re} z = \frac{z + \bar{z}}{2}$ and $\operatorname{Im} z = \frac{z - \bar{z}}{2i}$;
 (b) $z \in \mathbb{R}$ if and only if $\bar{z} = z$;
 (c) $\operatorname{Re} z = 0$ if and only if $\bar{z} = -z$.

Solution. Write $z = a + bi$ with $a, b \in \mathbb{R}$.

- (a) By [Theorem 1.2.2](#) (c), $z + \bar{z} = 2a$, and $2 \neq 0$, so $(z + \bar{z})/2 = a = \operatorname{Re} z$. Also $z - \bar{z} = (a - a) + (b + b)i = 2bi$, and $2i \neq 0$, so $(z - \bar{z})/(2i) = (b(2i))(2i)^{-1} = b((2i)(2i)^{-1}) = b = \operatorname{Im} z$, using $2bi = b \cdot (2i)$ and (F5), (F8), (F7) in the field $\mathbb{C}$ ([Theorem 1.2.4](#)).
 (b) $\bar{z} = z$ means $a - bi = a + bi$, which by comparing imaginary parts holds if and only if $-b = b$, that is $2b = 0$, that is $b = 0$ (as $2 \neq 0$ in $\mathbb{R}$). And $b = 0$ means $z = a \in \mathbb{R}$.
 (c) $\bar{z} = -z$ means $a - bi = -a - bi$, which by comparing parts holds if and only if $a = -a$ (the imaginary parts agree), that is $2a = 0$, that is $a = 0$ (as in (b)).

Exercise. B3

Let $z, w \in \mathbb{C}$ with $w \neq 0$. Prove that $\overline{z/w} = \bar{z}/\bar{w}$ and $|z/w| = |z|/|w|$.

Hint: start from $w \cdot (z/w) = z$.

Solution. Let $q := z/w = zw^{-1}$, so $wq = z$. By Theorem 1.2.2 (b), $\overline{w} \overline{q} = \overline{z}$. Here $\overline{w} \neq 0$: $|\overline{w}| = |w| \neq 0$ by Theorem 1.2.2 (d), (e). Multiplying by $\overline{w}^{-1}$ gives $\overline{q} = \overline{z}/\overline{w}$.

Likewise, by Theorem 1.2.2 (d), $|w| |q| = |z|$, with $|w| \neq 0$ by (e). Dividing by $|w|$ in $\mathbb{R}$ gives $|q| = |z|/|w|$.

1.2.4.3 C. Going deeper

Exercise. C1: Exit check: the complex numbers form a field

Prove Theorem 1.2.2 (b) and (d) and Proposition 1.2.3, and conclude that $\mathbb{C}$ satisfies (F8). You may use Definition 1.1.1, Proposition 1.1.2, Proposition 1.1.1, Theorem 1.2.2 (c) and (e), and the rules of the ordered field $\mathbb{R}$, including Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 6.1.4.

Solution. (b). Let $z = a + bi$, $w = c + di$. Then $zw = (ac - bd) + (ad + bc)i$, so $\overline{zw} = (ac - bd) - (ad + bc)i$. And $\overline{z} \overline{w} = (a - bi)(c - di) = (ac - (-b)(-d)) + (-ad - bc)i = (ac - bd) - (ad + bc)i$. The two agree.

(d). By (c), (b), and commutativity and associativity of multiplication (Proposition 1.1.2 (a), (b)),

$$|zw|^2 = (zw)\overline{zw} = (zw)(\overline{z}\overline{w}) = (z\overline{z})(w\overline{w}) = |z|^2|w|^2 = (|z||w|)^2.$$

Both $|zw|$ and $|z||w|$ are non-negative ($|z||w|$ is 0 if a factor is 0, by Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (b), and positive by (O4) of Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Definition 2.3.2 otherwise), so both are the non-negative square root of $|z|^2|w|^2$, and they are equal by the uniqueness clause of Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 6.1.4. Also $|\overline{z}| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|$.

Inverse. Let $z \neq 0$. By (e), $|z| \neq 0$, so $|z|^2 > 0$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.5 (e)), and $r := 1/|z|^2$ exists in $\mathbb{R}$. With $w := r\overline{z}$, Proposition 1.1.2 and (c) give $zw = r(z\overline{z}) = r|z|^2 = 1$, where the last product is computed in $\mathbb{R}$, which agrees with the product in $\mathbb{C}$ (Proposition 1.1.1).

(F8). Every non-zero $z \in \mathbb{C}$ has an element w with $zw = 1$, which is (F8) of Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Definition 2.3.1.

Marking scheme. (10 points) - 2: (b) by expanding both sides in real and imaginary parts and comparing. - 3: (d) via $|zw|^2 = (zw)\overline{zw}$ and (b), with commutativity named for the reordering. - 1: equal non-negative squares give equal numbers, with a reason (uniqueness of the non-negative square root, or Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.5 (g) with trichotomy). - 2: $|z|^2 > 0$ for $z \neq 0$, with a reason. - 2: $zw = 1$ for $w = (1/|z|^2)\overline{z}$, and the conclusion stated as (F8). Fatal errors (0 for the step): dividing by z or by $|z|$ before showing it is non-zero; “ $|zw| = |z||w|$ because the modulus is a length and multiplication scales lengths” (circular: the scaling picture is a consequence of (d)). A second route to (d), expanding $(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2)$ and then taking square roots, earns the 3 points of the (d) step in full.

Exercise. C2: Gaussian rationals

Let $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$, where $\mathbb{Q} \subseteq \mathbb{R}$ as in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 5 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 5.6.3). Prove that $\mathbb{Q}(i)$ is closed under addition, negatives, multiplication, inverses of non-zero elements, and conjugation.

Solution. Under the identification of q with $\kappa(q)$, κ sends sums, products, negatives and inverses of non-zero rationals to the same operations in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 5.4.1 (a), (c)), so the copy of $\mathbb{Q}$ in $\mathbb{R}$ is closed under $+$, $\cdot$, negatives and inverses of non-zero elements.

Let $z = a + bi$ and $w = c + di$ with $a, b, c, d \in \mathbb{Q}$. Then $z + w = (a + c) + (b + d)i$, $-z = (-a) + (-b)i$ and $zw = (ac - bd) + (ad + bc)i$ have rational parts, and so does $\bar{z} = a + (-b)i$. If $z \neq 0$, then $a^2 + b^2 = |z|^2 \neq 0$ by Theorem 1.2.2 (e), and $a^2 + b^2 \in \mathbb{Q}$. By Proposition 1.2.3,

$$z^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i,$$

whose parts are quotients of rational numbers by a non-zero rational number, hence rational. So all five operations stay in $\mathbb{Q}(i)$. For example, $(1 + 2i)^{-1} = \frac{1}{5} - \frac{2}{5}i \in \mathbb{Q}(i)$.

Algebraic Preliminaries, Chapter 1 calls a subset of a field a subfield when it contains 0 and 1 and has these closure properties. $\mathbb{Q}(i)$ contains $0 = 0 + 0i$ and $1 = 1 + 0i$, and it is one of the examples there.

Marking scheme. (10 points) - 2: the copy of $\mathbb{Q}$ in $\mathbb{R}$ is closed under $+$, $\cdot$, negatives and inverses of non-zero elements, with a reason (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 5.4.1 (a), (c)). - 2: $z + w$, $-z$ and $\bar{z}$ have rational real and imaginary parts. - 2: $zw = (ac - bd) + (ad + bc)i$ has rational parts. - 3: for $z \neq 0$, $a^2 + b^2$ is non-zero (Theorem 1.2.2 (e)) and rational, and the formula of Proposition 1.2.3 then gives rational parts. - 1: the conclusion that all five operations stay in $\mathbb{Q}(i)$. Fatal errors (0 for the step): dividing by $a^2 + b^2$ without first using $z \neq 0$ to show it is non-zero; assuming without a reason that $\mathbb{Q} \subseteq \mathbb{R}$ is closed under the operations.

1.3 The Triangle Inequality

The modulus of Section 1.2 measures a complex number by a real one. Picture $z = a + bi$ as the point (a, b) of the plane: by Pythagoras, $|z| = \sqrt{a^2 + b^2}$ is its distance from the origin, and $|z - w|$ is the distance between the points z and w . In a triangle, one side is never longer than the other two together. This section proves the algebraic form of that fact, $|z + w| \leq |z| + |w|$, from the definitions alone. The picture motivates it; no step of the proof uses it.

1.3.1 Why the old proof does not transfer

For an ordered field, *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 4 proved $|x + y| \leq |x| + |y|$ by trapping (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 4.1.3 (e)). Each of x and y lies between $\pm$ its absolute value, $-|x| \leq x \leq |x|$ (part (c) there); adding the two traps traps $x + y$ between $\pm(|x| + |y|)$, and part (d) reads that as the inequality.

That route needs $x \leq |x|$: a comparison between x itself and a number. For a complex z , “ $z \leq |z|$ ” compares a complex number with a real one, and $\mathbb{C}$ has been given no order in which to make the comparison. Section 1.4 shows that no order compatible with the arithmetic of $\mathbb{C}$ exists (Proposition 1.4.3). So the proof must compare **real** numbers only.

Two kinds of real number are at hand. Moduli are real, and so are real parts. The device that connects them to the arithmetic of $\mathbb{C}$ is the identity $|u|^2 = u\bar{u}$ of Theorem 1.2.2 (c). A modulus is a square root, and square roots do not add well; its square is a product, and products expand. So we will compare squares and then come back.

Comparing squares. Coming back from squares to the numbers needs one rule about the real numbers. Let $p, q \in \mathbb{R}$ with $p \geq 0$ and $q \geq 0$. Then

$$p \leq q \iff p^2 \leq q^2, \quad p = q \iff p^2 = q^2,$$

and likewise with $<$ on both sides. The strict form is Number Systems: From $\setminus(\mathbb{N})$ to $\setminus(\mathbb{R})$, Proposition 2.3.5 (g). For the first equivalence: if $p < q$, then $p^2 < q^2$ by (g), and if $p = q$ the squares agree. Conversely, if $p^2 \leq q^2$ and yet $q < p$, then (g) gives $q^2 < p^2$, which contradicts $p^2 \leq q^2$ by trichotomy (O1); so $p \leq q$. The second equivalence follows from the first, applied in both directions, and trichotomy. In words: *for non-negative reals, squaring neither creates nor destroys a comparison*. Both hypotheses $p \geq 0$ and $q \geq 0$ matter: $(-2)^2 > 1^2$, and yet $-2 < 1$.

1.3.2 The real part is at most the modulus

The single estimate the proof needs is that a real part never exceeds the modulus. It comes with two companions, which say that the modulus and the “taxicab size” $|\operatorname{Re} u| + |\operatorname{Im} u|$ are comparable.

Lemma 1.3.1. Real and Imaginary Parts against the Modulus

For every $u \in \mathbb{C}$,

$$|\operatorname{Re} u| \leq |u|, \quad |\operatorname{Im} u| \leq |u|, \quad |u| \leq |\operatorname{Re} u| + |\operatorname{Im} u|.$$

In particular $\operatorname{Re} u \leq |u|$.

Here $|\operatorname{Re} u|$ is the absolute value of a real number. By Proposition 1.2.1 it is the same whether it is read as the absolute value of the ordered field $\mathbb{R}$ from *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 4 (Number Systems: From $\setminus(\mathbb{N})$ to $\setminus(\mathbb{R})$, Definition 4.1.1) or as the modulus of a complex number that happens to be real, so the lemma has only one reading.

Idea. Every quantity in the lemma is a non-negative real, so compare squares. The square of $|u|$ is $x^2 + y^2$, and the squares of $|x|$ and $|y|$ are x^2 and y^2 , each at most the sum; the square of $|x| + |y|$ is the sum plus the non-negative cross term $2|x||y|$.

Proof. Write $u = x + yi$ with $x, y \in \mathbb{R}$. By Definition 1.2.1 and the defining property of the square root (Number Systems: From $\setminus(\mathbb{N})$ to $\setminus(\mathbb{R})$, Proposition 6.1.4), $|u| \geq 0$ and $|u|^2 = x^2 + y^2$.

Since $y^2 \geq 0$ (Number Systems: From $\setminus(\mathbb{N})$ to $\setminus(\mathbb{R})$, Proposition 2.3.5 (e) if $y \neq 0$;

$0^2 = 0$ otherwise), adding x^2 gives $x^2 \leq x^2 + y^2$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b). Also $|x|^2 = x^2$ and $|x| \geq 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 (a), (b)). Hence $|x|^2 \leq |u|^2$, with both $|x|$ and $|u|$ non-negative, and comparing squares gives $|x| \leq |u|$. The same argument with the roles of x and y exchanged gives $|y| \leq |u|$. Then $\operatorname{Re} u = x \leq |x|$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 (c), so $\operatorname{Re} u \leq |u|$.

For the last inequality, expand with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (d):

$$\begin{aligned} (|x| + |y|)^2 &= |x|^2 + 2|x||y| + |y|^2 \\ &= x^2 + y^2 + 2|x||y| \geq x^2 + y^2 = |u|^2, \end{aligned}$$

where the inequality holds because $|x||y| \geq 0$ as a product of non-negative reals, so $2|x||y| \geq 0$, and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b) adds it. Both $|x| + |y|$ and $|u|$ are non-negative, so comparing squares gives $|u| \leq |x| + |y|$. This proves the lemma. $\blacksquare$

For $u = 3 - 4i$ the three inequalities read $3 \leq 5$, $4 \leq 5$ and $5 \leq 7$. For $u = 2$ they read $2 \leq 2$, $0 \leq 2$ and $2 \leq 2$: a real u makes the first and third equalities. The inequality $\operatorname{Re} u \leq |u|$ is strict for $u = -1$, where it reads $-1 \leq 1$; the absolute value inside the first inequality is what makes it sharp for real u of either sign.

Quick check. Find a non-zero $u \in \mathbb{C}$ with $\operatorname{Re} u = 0$. What do the three inequalities of Lemma 1.3.1 say for it?

Solution. For example $u = 2i$, with $\operatorname{Re} u = 0$, $\operatorname{Im} u = 2$ and $|u| = \sqrt{0+4} = 2$. The inequalities read $0 \leq 2$, $2 \leq 2$ and $2 \leq 0 + 2$. Any $u = yi$ with $y \neq 0$ works the same way: $|u| = |y|$, so the second and third inequalities are equalities.

1.3.3 The triangle inequality

We can now state the theorem. Its proof is the first full run of the move this chapter is built around.

Theorem 1.3.2. Triangle Inequality for Complex Numbers

For all $z, w \in \mathbb{C}$,

$$|z + w| \leq |z| + |w|.$$

Try it first (ten minutes): show $|z + w|^2 \leq (|z| + |w|)^2$ by expanding both sides with $|u|^2 = u\bar{u}$, and note which term you cannot yet bound.

Idea. Expanding the left side with $|u|^2 = u\bar{u}$ and conjugation of sums gives $|z|^2 + z\bar{w} + \bar{z}w + |w|^2$; the right side is $|z|^2 + 2|z||w| + |w|^2$. Everything matches except the cross term $z\bar{w} + \bar{z}w$, and an attempt usually stops there: it looks like a complex number, and complex numbers cannot be compared with $2|z||w|$. The way out is to notice that $\bar{z}w$ is the conjugate of $z\bar{w}$,

so the cross term is $u + \bar{u} = 2 \operatorname{Re} u$ with $u = z\bar{w}$: a **real** number after all. A real part is at most the modulus, and $|z\bar{w}| = |z||w|$. Squares compare, so the moduli do.

Before reading on: where is $\operatorname{Re} u \leq |u|$ used, and why may we compare squares?

Proof. Let $z, w \in \mathbb{C}$. By [Theorem 1.2.2](#) (c), then (a), then [Proposition 1.1.2](#) (c) together with (a) and (b) (distributivity, commutativity, associativity),

$$\begin{aligned} |z + w|^2 &= (z + w) \overline{(z + w)} = (z + w)(\bar{z} + \bar{w}) \\ &= z\bar{z} + z\bar{w} + \bar{z}w + w\bar{w}. \end{aligned}$$

By [Theorem 1.2.2](#) (b) and (a), $\overline{z\bar{w}} = \bar{z}\bar{\bar{w}} = \bar{z}w$. So with $u := z\bar{w}$, the two middle terms are $u + \bar{u} = 2 \operatorname{Re} u$, by [Theorem 1.2.2](#) (c). Using (c) once more for $z\bar{z}$ and $w\bar{w}$,

$$|z + w|^2 = |z|^2 + 2 \operatorname{Re}(z\bar{w}) + |w|^2.$$

Every term here is real, and sums and products of real numbers are the same in $\mathbb{C}$ as in $\mathbb{R}$ ([Proposition 1.1.1](#)), so the inequalities below take place in the ordered field $\mathbb{R}$. By [Lemma 1.3.1](#), $\operatorname{Re}(z\bar{w}) \leq |z\bar{w}|$, and by [Theorem 1.2.2](#) (d), $|z\bar{w}| = |z||\bar{w}| = |z||w|$. Adding this inequality to itself ($2a = (1+1)a = a + a$ by distributivity) and then adding $|z|^2 + |w|^2$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b) twice), and expanding the square with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (d),

$$|z + w|^2 \leq |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2.$$

Both $|z + w|$ and $|z| + |w|$ are non-negative real numbers, so comparing squares gives $|z + w| \leq |z| + |w|$. This proves the triangle inequality. ■

The proof answers its prompt in two lines. $\operatorname{Re} u \leq |u|$ is used once, to bound the cross term $2 \operatorname{Re}(z\bar{w})$ by $2|z\bar{w}|$. Comparing squares is legitimate because the two quantities being compared, $|z + w|$ and $|z| + |w|$, are both non-negative; without that, a smaller square would say nothing about the numbers.

This route has a name in this chapter: **square the modulus**. *The modulus is a square root, and square roots are hard to handle; its square $|u|^2 = u\bar{u}$ is a product, so square, expand with conjugates, bound or compare the real numbers you get, and take the non-negative square root back.* Section 1.2 used the same move once already, for $|zw| = |z||w|$ ([Theorem 1.2.2](#) (d)). The linear algebra volumes take the same route, square, expand, bound the cross term, for the length of a vector in an inner product space.

Warning. The square of the modulus is $u\bar{u}$, not u^2 . Expanding $|z + w|^2$ as $(z + w)^2 = z^2 + 2zw + w^2$ gives nonsense: for $z = w = i$, $(z + w)^2 = (2i)^2 = -4$, while $|z + w|^2 = |2i|^2 = 4$. The cross term of the correct expansion is $z\bar{w} + \bar{z}w$, and only that form is real.

Remark. The inequality can be strict: for $z = 1$ and $w = -1$, the left side is $|0| = 0$ and the right side is 2. For real z, w , every modulus in the statement is the absolute value of *Number*

Systems: From $\mathbb{N}$ to $\mathbb{R}$, Chapter 4 ([Proposition 1.2.1](#)), and the theorem is Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 (e), reached by a different route.

Quick check. Compute $|3 + 4i| + |-3 + 4i|$ and $|(3 + 4i) + (-3 + 4i)|$, and check them against the triangle inequality.

Solution. $|3 + 4i| = \sqrt{9 + 16} = 5$ and $|-3 + 4i| = \sqrt{9 + 16} = 5$, so the right side is 10. The sum is $8i$, and $|8i| = \sqrt{0 + 64} = 8$. Indeed $8 \leq 10$. In the picture, the two points and $8i$ are three corners of a parallelogram with the origin as the fourth, and the diagonal 8 is shorter than the two sides $5 + 5$.

1.3.4 Three variants

Three consequences are used often enough to be stated once: a lower bound for the modulus of a difference, the inequality for any finite number of terms, and a lower bound for the modulus of a sum.

Corollary 1.3.3. Variants of the Triangle Inequality

Let $z, w \in \mathbb{C}$.

- (a) (*Reverse triangle inequality.*) $||z| - |w|| \leq |z - w|$.
- (b) For every $n \in \mathbb{N}$ with $n \geq 1$ and all $z_1, \dots, z_n \in \mathbb{C}$, $\left| \sum_{k=1}^n z_k \right| \leq \sum_{k=1}^n |z_k|$.
- (c) $|z| - |w| \leq |z + w|$.

In (a), the outer bars are the absolute value of the real number $|z| - |w|$. In words: (a) says that two points at distance $|z - w|$ from each other have distances from the origin that differ by at most that much; (b) says that a path of n steps is at least as long as the straight line from start to end; (c) says that adding w can lower the modulus by at most $|w|$.

Idea. For (a), split z as $(z - w) + w$ and apply the theorem; that bounds $|z| - |w|$ from above, and swapping z and w bounds it from below. For (b), add one term at a time. For (c), apply (a) to z and $-w$.

Proof.

- (a) Since $z = (z - w) + w$, [Theorem 1.3.2](#) gives $|z| \leq |z - w| + |w|$, so $|z| - |w| \leq |z - w|$. Exchanging z and w gives $|w| - |z| \leq |w - z|$. Moreover $w - z = (-1)(z - w)$, so by [Theorem 1.2.2](#) (d), $|w - z| = |-1| |z - w| = |z - w|$, where $|-1| = 1$ by [Proposition 1.2.1](#). Let $t := |z| - |w| \in \mathbb{R}$. We have shown $t \leq |z - w|$ and $-t \leq |z - w|$, that is, $-|z - w| \leq t \leq |z - w|$: if $-t < |z - w|$, then $-|z - w| < -(-t) = t$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (a) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (a), and if $-t = |z - w|$, then $-|z - w| = -(-t) = t$. By

Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 (d), $|t| \leq |z - w|$.

- (b) By induction on $n \geq 1$ (Logic and Proof, Axiom 4.2.1, through Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 1.7.3 (b), applied to the statement for $n = m + 1$, $m \in \mathbb{N}$), with the sums defined by appending the last term, as for real sums (Sets and Functions, Definition 2.3.1). For $n = 1$, both sides are $|z_1|$. Suppose the inequality holds for n , and let $z_1, \dots, z_{n+1} \in \mathbb{C}$. Then

$$\begin{aligned} \left| \sum_{k=1}^{n+1} z_k \right| &= \left| \sum_{k=1}^n z_k + z_{n+1} \right| \leq \left| \sum_{k=1}^n z_k \right| + |z_{n+1}| \\ &\leq \sum_{k=1}^n |z_k| + |z_{n+1}| = \sum_{k=1}^{n+1} |z_k|, \end{aligned}$$

by Theorem 1.3.2, then the induction hypothesis with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b).

- (c) Apply (a) to z and $-w$. Since $z - (-w) = z + w$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (a)) and $|-w| = |-1||w| = |w|$ as in (a), it reads $||z| - |w|| \leq |z + w|$. By Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 (c), $|z| - |w| \leq ||z| - |w||$. This proves the corollary. ■

Part (b) with $n = 2$ is the theorem itself, so the corollary contains it. *Algebraic Preliminaries*, Chapter 4 uses (b) and (c) to show that a polynomial expression of degree at least 1 is large in modulus when $|z|$ is large, a step towards the Fundamental Theorem of Algebra.

Quick check. Take $z = 5$ and $w = 3i$. Compute both sides of (a) and of (c).

Solution. $|z| = 5$ and $|w| = 3$, so $|z| - |w| = 2$. For (a): $|z - w| = |5 - 3i| = \sqrt{34}$, and $2 \leq \sqrt{34}$ because $2^2 = 4 \leq 34$ (comparing squares). For (c): $|z + w| = |5 + 3i| = \sqrt{34}$ too, and again $2 \leq \sqrt{34}$. Both bounds are far from sharp here; (a) is an equality when $w = 0$, for instance.

1.3.5 Exercises

1.3.5.1 A. Check your understanding

Exercise. A1

These questions are about the proof of Theorem 1.3.2.

- Where in the proof is $\operatorname{Re} u \leq |u|$ used, and for which u ?
- Why may the proof pass from $|z + w|^2 \leq (|z| + |w|)^2$ back to $|z + w| \leq |z| + |w|$?
- Run the proof on $z = 3$ and $w = 4i$: compute the cross term $2 \operatorname{Re}(z\bar{w})$, then both sides of the squared inequality.

- (d) State the idea of the proof in two sentences.
 (e) True or false: $|z + w| = |z| + |w|$ for all $z, w \in \mathbb{C}$. Justify your answer.

Solution.

- (a) Once, to bound the cross term: with $u = z\bar{w}$, $2 \operatorname{Re}(z\bar{w}) \leq 2|z\bar{w}|$.
 (b) Both $|z + w|$ and $|z| + |w|$ are non-negative reals, and for non-negative reals $p \leq q$ if and only if $p^2 \leq q^2$ (comparing squares, from Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (g) and trichotomy).
 (c) $\bar{w} = -4i$, so $z\bar{w} = 3 \cdot (-4i) = -12i$, with real part 0: the cross term is 0. Then $|z + w|^2 = 9 + 0 + 16 = 25$ and $(|z| + |w|)^2 = (3 + 4)^2 = 49$, and $25 \leq 49$. So $|3 + 4i| = 5 \leq 7$.
 (d) Square both sides and expand with $|u|^2 = u\bar{u}$: everything matches except the cross term, which is $2 \operatorname{Re}(z\bar{w})$. A real part is at most the modulus, and $|z\bar{w}| = |z||w|$, so the squares compare, and so do the non-negative moduli.
 (e) False. For $z = 1$ and $w = -1$, $|z + w| = 0$, but $|z| + |w| = 2$.

1.3.5.2 B. Practice

Exercise. B1: The equality case

Let $z, w \in \mathbb{C}$. Prove that $|z + w| = |z| + |w|$ if and only if $z\bar{w}$ is a non-negative real number, that is, $\operatorname{Im}(z\bar{w}) = 0$ and $\operatorname{Re}(z\bar{w}) \geq 0$.

Hint: trace the proof of the triangle inequality and ask where an inequality could be strict.

Solution. Let $u := z\bar{w} = x + yi$ with $x, y \in \mathbb{R}$. By the proof of [Theorem 1.3.2](#),

$$\begin{aligned} |z + w|^2 &= |z|^2 + 2x + |w|^2, \\ (|z| + |w|)^2 &= |z|^2 + 2|u| + |w|^2, \end{aligned}$$

the second because $|z||w| = |u|$ ([Theorem 1.2.2](#) (d)). Both moduli are non-negative, so (comparing squares) $|z + w| = |z| + |w|$ holds if and only if the squares are equal, that is, if and only if $2x = 2|u|$, that is, $x = |u|$.

It remains to show that $x = |u|$ holds exactly when $y = 0$ and $x \geq 0$. If $x = |u|$, then $x \geq 0$, and squaring gives $x^2 = x^2 + y^2$, so $y^2 = 0$ and $y = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e): a non-zero square is positive). Conversely, if $y = 0$ and $x \geq 0$, then $|u| = \sqrt{x^2} = x$, since $x \geq 0$ and $x^2 = x^2$ (uniqueness in Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4). Hence $|z + w| = |z| + |w|$ if and only if $z\bar{w}$ is a non-negative real number.

For instance $z = 1 + i$, $w = 2 + 2i$: $z\bar{w} = (1 + i)(2 - 2i) = 4 \geq 0$, and indeed $|3 + 3i| = \sqrt{18} = 3\sqrt{2} = \sqrt{2} + 2\sqrt{2} = |1 + i| + |2 + 2i|$. In the picture: equality holds exactly when one of z, w is 0 or they point in the same direction from the origin. The linear algebra volumes prove the version for n terms.

Exercise. B2: A distance that does not change

Let $z \in \mathbb{C}$ with $|z| = 1$. Prove that $|z - w| = |1 - \bar{z}w|$ for every $w \in \mathbb{C}$. The first two steps are done:

$$\begin{aligned}|z - w|^2 &= |z|^2 - z\bar{w} - \bar{z}w + |w|^2, \\ |1 - \bar{z}w|^2 &= 1 - z\bar{w} - \bar{z}w + |z|^2|w|^2,\end{aligned}$$

both by expanding $u\bar{u}$ with [Theorem 1.2.2](#). Name the move, then complete it.

Solution. The move is **square the modulus**: compare the squares, which are algebra, and take the non-negative square roots back.

Substitute $|z|^2 = 1$ into both lines. The first becomes $1 - z\bar{w} - \bar{z}w + |w|^2$, and so does the second, since $|z|^2|w|^2 = |w|^2$. So $|z - w|^2 = |1 - \bar{z}w|^2$. Both $|z - w|$ and $|1 - \bar{z}w|$ are non-negative, and non-negative reals with equal squares are equal (comparing squares). Hence $|z - w| = |1 - \bar{z}w|$.

(For the record, the given lines. Conjugation respects differences: $\overline{-v} = \overline{(-1)v} = \overline{-1}\bar{v} = -\bar{v}$ by [Theorem 1.2.2](#) (b), [Proposition 1.2.1](#) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (c), so with (a), $\overline{u - v} = \bar{u} - \bar{v}$; and $\bar{1} = 1$ by [Proposition 1.2.1](#). Then $(z - w)(\bar{z} - \bar{w}) = z\bar{z} - z\bar{w} - w\bar{z} + w\bar{w}$, and $\bar{1} - \bar{z}w = 1 - z\bar{w}$, so $(1 - \bar{z}w)(1 - z\bar{w}) = 1 - z\bar{w} - \bar{z}w + (z\bar{z})(w\bar{w})$.)

Exercise. B3

Prove that $|z| \leq |\operatorname{Re} z| + |\operatorname{Im} z| \leq \sqrt{2}|z|$ for every $z \in \mathbb{C}$, and, for each of the two inequalities, find a non-zero z for which it is an equality.

Solution. The first inequality is the last part of [Lemma 1.3.1](#). For the second, write $z = x + yi$. Both sides are non-negative ($\sqrt{2} \geq 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4), so it suffices to compare squares. The right side squared is $(\sqrt{2})^2|z|^2 = 2(x^2 + y^2)$, and the left side squared is $x^2 + 2|x||y| + y^2$, using $|x|^2 = x^2$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 4.1.3 (b)). Their difference is

$$\begin{aligned}2(x^2 + y^2) - (x^2 + 2|x||y| + y^2) &= |x|^2 - 2|x||y| + |y|^2 \\ &= (|x| - |y|)^2 \geq 0,\end{aligned}$$

a square in the ordered field $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)). So $(|x| + |y|)^2 \leq 2|z|^2$, and $|x| + |y| \leq \sqrt{2}|z|$.

Equality: $z = 1$ gives $1 = 1 + 0$ in the first; $z = 1 + i$ gives $1 + 1 = 2 = \sqrt{2} \cdot \sqrt{2}$ in the second.

1.3.5.3 C. Going deeper**Exercise. C1: Exit check: the triangle inequality**

State and prove the triangle inequality for complex numbers. Your proof must include a proof that $\operatorname{Re} u \leq |u|$ for every $u \in \mathbb{C}$.

Solution. Statement. For all $z, w \in \mathbb{C}$, $|z + w| \leq |z| + |w|$.

The estimate. Let $u = x + yi$ with $x, y \in \mathbb{R}$. Then $|u|^2 = x^2 + y^2 \geq x^2 = |x|^2$, since $y^2 \geq 0$. Both $|x|$ and $|u|$ are non-negative, so $|x| \leq |u|$ by comparing squares (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (g) with trichotomy). Hence $\operatorname{Re} u = x \leq |x| \leq |u|$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 4.1.3 (c)).

The inequality. Let $z, w \in \mathbb{C}$. By Theorem 1.2.2 (a)–(c),

$$\begin{aligned} |z + w|^2 &= (z + w)(\bar{z} + \bar{w}) = |z|^2 + (z\bar{w} + \bar{z}w) + |w|^2 \\ &= |z|^2 + 2\operatorname{Re}(z\bar{w}) + |w|^2. \end{aligned}$$

By the estimate and Theorem 1.2.2 (d), $2\operatorname{Re}(z\bar{w}) \leq 2|z\bar{w}| = 2|z||w|$. Hence $|z + w|^2 \leq (|z| + |w|)^2$. Both $|z + w|$ and $|z| + |w|$ are non-negative, so comparing squares gives $|z + w| \leq |z| + |w|$.

Marking scheme. (10 points) - 2: proves $\operatorname{Re} u \leq |u|$, with a reason for passing from squares to moduli. - 3: expands $|z + w|^2$ with conjugates and identifies the cross term as $2\operatorname{Re}(z\bar{w})$, a real number. - 2: bounds the cross term by $2|z||w|$, citing $|z\bar{w}| = |z||w|$. - 1: concludes $|z + w|^2 \leq (|z| + |w|)^2$. - 2: takes square roots, justified by the non-negativity of both sides. A second route, with coordinates $z = a + bi$, $w = c + di$: expanding $(a + c)^2 + (b + d)^2$ and isolating the cross term $2(ac + bd)$ earns the 3 points of the second line; proving $ac + bd \leq |z||w|$, for instance from $(ac + bd)^2 \leq (a^2 + b^2)(c^2 + d^2)$, which follows from $(ad - bc)^2 \geq 0$, earns the 2 points of the third line if proved, not if quoted; the last two lines are marked as above. The 2 points for $\operatorname{Re} u \leq |u|$ are still owed on that route, since the problem asks for it. Fatal errors (0 for the step): writing $z \leq |z|$ or any inequality between non-real complex numbers; dropping the conjugate, as in $|u|^2 = u^2$.

Exercise. C2: Inside the unit disc

Let $z, w \in \mathbb{C}$ with $|z| < 1$ and $|w| < 1$. Prove that $|z - w| < |1 - \bar{z}w|$. Here is the start of a proof: square both sides and expand. *Name the move, then complete it.*

Solution. The move is **square the modulus**. Both sides are non-negative, so it is enough to show $|z - w|^2 < |1 - \bar{z}w|^2$ (comparing squares, strict form: Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (g)). Expanding each as $u\bar{u}$, exactly as in Exercise (B2: A distance that does not change),

$$\begin{aligned} |z - w|^2 &= |z|^2 - z\bar{w} - \bar{z}w + |w|^2, \\ |1 - \bar{z}w|^2 &= 1 - z\bar{w} - \bar{z}w + |z|^2|w|^2. \end{aligned}$$

The non-real terms cancel in the difference:

$$\begin{aligned} |1 - \bar{z}w|^2 - |z - w|^2 &= 1 - |z|^2 - |w|^2 + |z|^2|w|^2 \\ &= (1 - |z|^2)(1 - |w|^2). \end{aligned}$$

Since $0 \leq |z| < 1$, comparing squares gives $|z|^2 < 1^2 = 1$, so $1 - |z|^2 > 0$; likewise $1 - |w|^2 > 0$. A product of two positive reals is positive ((O4)). So the difference is positive, $|z - w|^2 < |1 - \bar{z}w|^2$, and $|z - w| < |1 - \bar{z}w|$.

In particular $1 - \bar{z}w \neq 0$. Since $|1 - \bar{z}w| = |1 - z\bar{w}|$ (a modulus is unchanged by conjugation, [Theorem 1.2.2](#) (d)), the inequality says that $|z - w|/|1 - \bar{w}z| < 1$ for all z, w in the open unit disc: the map $z \mapsto (z - w)/(1 - \bar{w}z)$ sends the open unit disc into itself, a fact complex analysis builds on.

Marking scheme. (10 points) - 2: reduces to the squared inequality, with the non-negativity of both sides as the reason. - 3: expands both squares with conjugates. - 3: factors the difference as $(1 - |z|^2)(1 - |w|^2)$. - 2: shows both factors positive, from $|z|, |w| < 1$, and concludes strictly. Fatal errors (0 for the step): expanding $|z - w|^2$ as $(z - w)^2$; comparing $z\bar{w}$ with a real number.

1.4 Square Roots, Quadratic Equations, and the Missing Order

Logic and Proof, Section 7.1 needed, in one of its checks, the fact that every complex number has a complex square root, and took it there as a school fact about polar form. This section proves it, with no angles at all: a square root of a complex number is built from two square roots of non-negative reals, which *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 6 provides (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.1.4). The quadratic formula follows, for complex coefficients. Then we see what $\mathbb{C}$ has lost on the way from $\mathbb{R}$: it has no order compatible with its arithmetic, and the rule $\sqrt{x}\sqrt{y} = \sqrt{xy}$ has no complex version.

1.4.1 Square roots from real square roots

The question is: given $z = a + bi$, find $w = x + yi$ with $w^2 = z$. Since $w^2 = (x^2 - y^2) + 2xyi$, comparing real and imaginary parts turns the question into two real equations,

$$x^2 - y^2 = a, \quad 2xy = b.$$

The answer is an explicit formula in a, b and $|z|$.

Proposition 1.4.1. Square Roots of Complex Numbers

Let $z = a + bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$ and $z \neq 0$, and let $r := |z|$. Put $s := 1$ if $b \geq 0$ and $s := -1$ if $b < 0$, and

$$x := \sqrt{\frac{r+a}{2}}, \quad y := s\sqrt{\frac{r-a}{2}}, \quad w := x + yi.$$

Then:

- (a) $w^2 = z$;
- (b) for $u \in \mathbb{C}$, $u^2 = z$ if and only if $u = w$ or $u = -w$;
- (c) $w \neq -w$.

For $z = 0$: $u^2 = 0$ if and only if $u = 0$.

*In words: every non-zero complex number has **exactly two** square roots, w and $-w$, and the formula finds one of them; 0 has exactly one.*

Try it first (ten minutes): find w with $w^2 = 3 + 4i$ by writing $w = x + yi$. What do you do with the two equations you get?

Idea. For $3 + 4i$ the two equations are $x^2 - y^2 = 3$ and $2xy = 4$. The natural attempt eliminates $y = 2/x$ and arrives at $x^4 - 3x^2 - 4 = 0$, a quartic; it can be solved, but it hides what is going on, and in general it needs the quadratic formula before we have it. The missing piece is a **third** equation, and it comes from the modulus. If $w^2 = z$, then $|w|^2 = |w^2| = |z|$ by Theorem 1.2.2 (d), that is, $x^2 + y^2 = r$. Now the first equation and the third give x^2 and y^2 by adding and subtracting: $x^2 = (r + a)/2$, $y^2 = (r - a)/2$. That fixes x and y up to sign, and the second equation $2xy = b$ says which signs go together: xy has the sign of b . For $3 + 4i$: $r = 5$, $x^2 = 4$, $y^2 = 1$, $xy > 0$, so $w = \pm(2 + i)$.

The proof runs this forward: define x and y by the formulas, check $w^2 = z$, and get “only $\pm w$ ” from the field axioms.

Before reading on: why does the sign of b decide whether x and y have the same sign?

The proof uses one small rule about real square roots: for $p, q \in \mathbb{R}$ with $p, q \geq 0$,

$$\sqrt{p} \sqrt{q} = \sqrt{pq}.$$

Both sides are non-negative (a product of non-negative reals is non-negative), and the square of the left side is $(\sqrt{p})^2(\sqrt{q})^2 = pq$, by commutativity; so the left side is the non-negative number whose square is pq , which is the right side by the uniqueness in Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 6.1.4. The rule is about non-negative **reals** only; the last part of this section shows that it has no complex version.

Proof. The roots exist. By Lemma 1.3.1, $|a| = |\operatorname{Re} z| \leq r$, so $-r \leq a \leq r$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 4.1.3 (d)). Hence $r + a \geq 0$ and $r - a \geq 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (a), (b)). Halving keeps this: for $p \geq 0$, either $p > 0$ and then $p/2 > 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 4.1.2 (b), with $\varepsilon = p$), or $p = 0$ and then $p/2 = 0 \cdot (1/2) = 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (b)). So $(r + a)/2 \geq 0$ and $(r - a)/2 \geq 0$. So the two square roots in the definition of x and y exist (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 6.1.4).

(a) Since $s^2 = 1$,

$$x^2 - y^2 = \frac{r + a}{2} - s^2 \frac{r - a}{2} = \frac{r + a}{2} - \frac{r - a}{2} = a.$$

For the imaginary part, the rule for real square roots gives

$$\begin{aligned} 2xy &= 2s \sqrt{\frac{r + a}{2}} \sqrt{\frac{r - a}{2}} = 2s \sqrt{\frac{r^2 - a^2}{4}} \\ &= s \sqrt{r^2 - a^2} = s \sqrt{b^2} = s|b| = b. \end{aligned}$$

Here the third equality is $2\sqrt{t/4} = \sqrt{4}\sqrt{t/4} = \sqrt{t}$, by the same rule and $\sqrt{4} = 2$; the fourth uses $r^2 = a^2 + b^2$ (Definition 1.2.1); the fifth holds because $|b| \geq 0$ and $|b|^2 = b^2$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 4.1.3 (a), (b)), with uniqueness in Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 6.1.4; and the last because $s|b| = b$ by the definitions of s and of $|b|$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Definition 4.1.1), in each of the two cases $b \geq 0$ and $b < 0$. Hence $w^2 = (x^2 - y^2) + 2xyi = a + bi = z$, by the multiplication rule of Definition 1.1.1.

(b) Let $u \in \mathbb{C}$. Since $\mathbb{C}$ is a commutative ring, $(u - w)(u + w) = u^2 - w^2$ (Proposition 1.1.2, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.2 (c)). If $u^2 = z$, then

$u^2 - w^2 = z - z = 0$ by (a), so $(u - w)(u + w) = 0$. Since $\mathbb{C}$ is a field ([Theorem 1.2.4](#)), it has no zero divisors (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 4.1.1 (d)), so $u - w = 0$ or $u + w = 0$, that is, $u = w$ or $u = -w$. Conversely $w^2 = z$ by (a), and $(-w)^2 = w^2 = z$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (c).

- (c) First $w \neq 0$, since $w^2 = z \neq 0$ and $0^2 = 0$. Suppose $w = -w$. Then $2w = w + w = 0$. But $2 = 1 + 1 \neq 0$ in $\mathbb{C}$: it is the real number 2, which is positive in $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (h)), and $\mathbb{R} \subseteq \mathbb{C}$ by the injective embedding of [Proposition 1.1.1](#). So $2w = 0$ with $2 \neq 0$ and $w \neq 0$ contradicts the absence of zero divisors. Hence $w \neq -w$.

Finally, for $z = 0$: $0^2 = 0$, and if $u^2 = u \cdot u = 0$, then $u = 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 4.1.1 (d). This proves the proposition. ■

The answer to the prompt: x is non-negative by construction, and y is s times a non-negative number, so xy is s times a non-negative number, and $2xy$ must equal b . If $b > 0$, then x and y must both be non-zero with the same sign; if $b < 0$, opposite signs. When $b = 0$ the choice of s does not matter, because then one of x, y is 0.

The proposition proves what *Logic and Proof*, Section 7.1 assumed, and it is stronger: it counts the roots. It uses only the field $\mathbb{C}$, its modulus, and square roots of non-negative reals; no angle, cosine or sine appears. That matters later: *Algebraic Preliminaries*, Chapter 4 proves the Fundamental Theorem of Algebra using square roots in exactly this form.

Example. Square Roots of $5 - 12i$

Find all $w \in \mathbb{C}$ with $w^2 = 5 - 12i$.

Solution. Write $w = x + yi$ with $x, y \in \mathbb{R}$. Comparing real and imaginary parts in $(x^2 - y^2) + 2xyi = 5 - 12i$ gives

$$x^2 - y^2 = 5 \quad \text{and} \quad xy = -6.$$

Taking moduli, by [Theorem 1.2.2](#) (d), $x^2 + y^2 = |w|^2 = |5 - 12i| = \sqrt{25 + 144} = 13$. Adding and subtracting, $x^2 = 9$ and $y^2 = 4$, so $x = \pm 3$ and $y = \pm 2$. Since $xy = -6 < 0$, x and y have opposite signs. Hence $w = 3 - 2i$ or $w = -3 + 2i$. Check: $(3 - 2i)^2 = 9 - 12i + 4i^2 = 5 - 12i$, and $(-3 + 2i)^2 = (3 - 2i)^2$.

The formula of [Proposition 1.4.1](#) gives the same root: $a = 5$, $b = -12 < 0$, so $s = -1$; $r = 13$, $x = \sqrt{18/2} = 3$ and $y = -\sqrt{8/2} = -2$. By part (b) there are no other roots.

Quick check. Find the square roots of -4 and of $2i$.

Solution. For -4 : $a = -4$, $b = 0$, $r = 4$, so $x = \sqrt{0} = 0$ and $y = \sqrt{8/2} = 2$; the roots are

$\pm 2i$, and indeed $(2i)^2 = -4$. For $2i$: $a = 0$, $b = 2$, $r = 2$, so $x = \sqrt{1} = 1$ and $y = 1$; the roots are $\pm(1 + i)$, and $(1 + i)^2 = 1 + 2i - 1 = 2i$.

1.4.2 The quadratic formula

With square roots in hand, a quadratic equation with complex coefficients is solved exactly as in school: complete the square. The only difference is that we never need to ask whether the discriminant is negative.

Corollary 1.4.2. Quadratic Formula over the Complex Numbers

Let $a, b, c \in \mathbb{C}$ with $a \neq 0$, and let $d \in \mathbb{C}$ be a square root of $b^2 - 4ac$ (one exists by [Proposition 1.4.1](#)). Then for $z \in \mathbb{C}$,

$$az^2 + bz + c = 0 \iff z = \frac{-b + d}{2a} \text{ or } z = \frac{-b - d}{2a}.$$

The two solutions coincide if and only if $b^2 - 4ac = 0$.

Here a, b, c are complex numbers, in a departure from the chapter's habit of reserving these letters for reals; the statement is the school formula, and keeps its letters. The choice of d does not matter: the other square root is $-d$ ([Proposition 1.4.1](#) (b)), which swaps the two solutions.

Idea. Complete the square, as in school: after multiplying by $4a$, the equation says that $2az + b$ is a square root of $b^2 - 4ac$. The square roots of $b^2 - 4ac$ are exactly d and $-d$, and solving the two linear equations $2az + b = \pm d$ gives the formula.

Proof. Multiply by $4a$ and complete the square. By the ring laws ([Proposition 1.1.2](#)) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (d),

$$4a(az^2 + bz + c) = 4a^2z^2 + 4abz + 4ac = (2az + b)^2 - (b^2 - 4ac).$$

Now $4a \neq 0$, since $4 \neq 0$ in $\mathbb{C}$ (as for 2 in the proof of [Proposition 1.4.1](#) (c)) and $a \neq 0$, and $\mathbb{C}$ has no zero divisors ([Theorem 1.2.4](#), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 4.1.1 (d)). So $az^2 + bz + c = 0$ if and only if $(2az + b)^2 = d^2$, that is, $(2az + b - d)(2az + b + d) = 0$, as in the proof of [Proposition 1.4.1](#) (b). By the absence of zero divisors again, this holds if and only if $2az + b = d$ or $2az + b = -d$. Since $2a \neq 0$, these say $z = (-b + d)/(2a)$ or $z = (-b - d)/(2a)$.

The two solutions coincide if and only if $d = -d$, that is, $2d = 0$, that is, $d = 0$ (as $2 \neq 0$). And $d = 0$ if and only if $d^2 = 0$ (no zero divisors), that is, $b^2 - 4ac = 0$. This proves the corollary. ■

Example. Solve $z^2 - (3 + i)z + (2 + 2i) = 0$. Here $a = 1$, and the discriminant is

$$(3 + i)^2 - 4(2 + 2i) = (8 + 6i) - (8 + 8i) = -2i.$$

The formula of [Proposition 1.4.1](#), applied to $-2i$ (real part 0, imaginary part $-2 < 0$, modulus

2), gives $x = \sqrt{2/2} = 1$ and $y = -\sqrt{2/2} = -1$, so $d = 1 - i$; indeed $(1 - i)^2 = 1 - 2i - 1 = -2i$. The solutions are

$$z = \frac{(3 + i) + (1 - i)}{2} = 2 \quad \text{and} \quad z = \frac{(3 + i) - (1 - i)}{2} = 1 + i.$$

Check: their sum is $3 + i$ and their product is $2 + 2i$, the negative of the middle coefficient and the constant term, as they should be for $(z - 2)(z - (1 + i))$.

1.4.3 No order on the complex numbers

In $\mathbb{R}$, and in every ordered field, a non-zero square is positive (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)). In $\mathbb{C}$, i is non-zero and its square is -1 . If $\mathbb{C}$ carried an order of the kind $\mathbb{R}$ has, -1 would have to be positive, and so would 1. That is already the proof.

Proposition 1.4.3. The Complex Numbers Cannot Be Ordered

There is **no** relation $<$ on $\mathbb{C}$ with which $(\mathbb{C}, +, \cdot, <)$ is an ordered field in the sense of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.2.

Proof. Suppose $<$ is a relation on $\mathbb{C}$ with which $\mathbb{C}$ is an ordered field. Since $i = (0, 1) \neq (0, 0) = 0$, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e) gives $i^2 > 0$, that is, $-1 > 0$ (Proposition 1.1.1: $i \cdot i = -1$). Since $1 \neq 0$ in the field $\mathbb{C}$, the same part (e) gives $1 > 0$. Adding, by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b), $0 = 1 + (-1) > 0 + 0 = 0$. But $0 < 0$ is impossible: (O1), with both elements equal to 0, says that exactly one of $0 < 0$ and $0 = 0$ holds, and $0 = 0$ does. So no such relation exists. ■

The proof never asks whether $i > 0$ or $i < 0$: part (e) covers both at once. It also never assumes that the hypothetical order agrees with the order of $\mathbb{R}$ on real numbers. It concludes $1 > 0$ and $-1 > 0$ in whatever order is supposed, and that is the contradiction.

Remark. Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Chapter 4 showed, in an exercise (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Exercise (C1: A field that cannot be ordered)), that a field containing a square root of -1 cannot be ordered, and named the complex numbers as such a field; the proposition proves that fact for $\mathbb{C}$ on its own. Compare Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (A field with two elements that cannot be ordered) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (e): there the obstacle to an order is $n \cdot 1 = 0$ for some $n \geq 1$. That obstacle is absent here, since $n \cdot 1$ in $\mathbb{C}$ is $\iota(n \cdot 1)$, the image of the real number $n \cdot 1 > 0$ of $\mathbb{R}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (h)), which is non-zero as ι is injective. (The identity $n \cdot 1 = \iota(n \cdot 1)$ is proved by Logic and Proof, Axiom 4.2.1 on n , as for powers in Section 1.1: $0 \cdot 1 = 0 = \iota(0)$, and if $n \cdot 1 = \iota(n \cdot 1)$, then $(n + 1) \cdot 1 = \iota(n \cdot 1) + \iota(1) = \iota((n + 1) \cdot 1)$ by Proposition 1.1.1.) The obstacle in $\mathbb{C}$ is $i^2 = -1$ instead.

Warning. An inequality $z < w$ between complex numbers means nothing: by Proposition 1.4.3 no order on $\mathbb{C}$ is compatible with its arithmetic. Apart from arguments that suppose an order on $\mathbb{C}$ in order to reach a contradiction (the proof above and Exercises B2

and $\mathbb{C}^2$), every inequality in this chapter compares **real** numbers in the order of $\mathbb{R}$: moduli, real parts, imaginary parts, or quantities proved to be real, as $2\operatorname{Re}(z\bar{w})$ was in Section 1.3. Writing $i > 0$ leads, by the proof above, to $0 > 0$; so does writing $i < 0$.

Quick check. Is the following a proof that $\mathbb{C}$ cannot be ordered? “Every real square is ≥ 0 , and $i^2 = -1 < 0$. So i is not a square of anything, a contradiction.”

Solution. No. The argument proves nothing about orders on $\mathbb{C}$. “ $-1 < 0$ ” is a statement in $\mathbb{R}$ ’s order, and a hypothetical order on $\mathbb{C}$ need not agree with it on the reals; the argument never even introduces the hypothetical order. And “ i is not a square” is false: $i = (\pm(1+i)/\sqrt{2})^2$ by [Proposition 1.4.1](#). The correct proof works inside the supposed order, where $i^2 > 0$ because $i \neq 0$.

1.4.4 The square-root rule does not survive

In $\mathbb{R}$, $\sqrt{x}\sqrt{y} = \sqrt{xy}$ for $x, y \geq 0$: that is the rule for real square roots used above. A non-zero complex number has two square roots and no preferred one, and no way of preferring one keeps the rule alive.

Warning. No choice of “the” square root $\sqrt{z}$ of each complex z can satisfy $\sqrt{z}\sqrt{w} = \sqrt{zw}$ for all $z, w \in \mathbb{C}$. Whatever is chosen for $\sqrt{-1}$, it is i or $-i$ ([Proposition 1.4.1](#) (b)), and in both cases $\sqrt{-1} \cdot \sqrt{-1} = (\pm i)^2 = -1$. But $\sqrt{(-1)(-1)} = \sqrt{1}$, and the rule itself forces $\sqrt{1} = 1$: since $\sqrt{1}$ is a square root of 1, $1 = \sqrt{1} \cdot \sqrt{1} = \sqrt{1 \cdot 1} = \sqrt{1}$. So the rule would give $-1 = 1$, which is false in $\mathbb{C}$ (the real parts $-1 < 1$ differ). So in this volume the symbol $\sqrt{}$ is applied only to non-negative reals; for any other z , say “a square root of z ” and solve $w^2 = z$.

1.4.5 Exercises

1.4.5.1 A. Check your understanding

Exercise. A1

- True or false: if $z, w \in \mathbb{C}$ and $z^2 = w^2$, then $z = w$. Justify your answer, and state what **is** true.
- Run the formula of [Proposition 1.4.1](#) on $z = -4$: compute a, b, r, s, x, y and both square roots.
- Where in the proof of [Proposition 1.4.1](#) is $r \geq |a|$ used?
- State the idea of the proof of [Proposition 1.4.1](#) in two sentences.

Solution.

- False: $z = 1, w = -1$ have $z^2 = w^2 = 1$ and $z \neq w$. What is true: $z^2 = w^2$ implies $z = w$ or $z = -w$, since $(z - w)(z + w) = z^2 - w^2 = 0$ and $\mathbb{C}$ has no zero divisors (this

is the argument of [Proposition 1.4.1](#) (b)).

- (b) $a = -4$, $b = 0$, $r = |-4| = 4$, $s = 1$ (as $b \geq 0$), $x = \sqrt{(4-4)/2} = 0$, $y = \sqrt{(4+4)/2} = 2$. So $w = 2i$, and the square roots are $\pm 2i$.
- (c) To take the square roots at all: $r \geq |a|$ gives $r + a \geq 0$ and $r - a \geq 0$, so $\sqrt{(r+a)/2}$ and $\sqrt{(r-a)/2}$ exist.
- (d) Comparing parts gives $x^2 - y^2 = a$ and $2xy = b$; taking moduli gives a third equation $x^2 + y^2 = r$, and the first and third give x^2 and y^2 by adding and subtracting. The signs are then fixed by $2xy = b$, and the absence of zero divisors shows that $\pm w$ are the only roots.

1.4.5.2 B. Practice

Exercise. B1

- (a) Find all $w \in \mathbb{C}$ with $w^2 = -3 + 4i$.
- (b) Hence solve $z^2 + 2z + 4 - 4i = 0$.

Solution.

- (a) Write $w = x + yi$. Comparing parts, $x^2 - y^2 = -3$ and $xy = 2$. Taking moduli ([Theorem 1.2.2](#) (d)), $x^2 + y^2 = |-3+4i| = \sqrt{9+16} = 5$. Adding and subtracting, $x^2 = 1$ and $y^2 = 4$. Since $xy = 2 > 0$, x and y have the same sign, so $w = 1 + 2i$ or $w = -1 - 2i$, and by [Proposition 1.4.1](#) (b) there are no others. Check: $(1+2i)^2 = 1+4i-4 = -3+4i$.
- (b) By [Corollary 1.4.2](#) with $a = 1$, $b = 2$, $c = 4 - 4i$: the discriminant is $4 - 4(4 - 4i) = -12 + 16i = 4(-3 + 4i)$, with square root $d = 2(1 + 2i) = 2 + 4i$ by (a), since $(2(1 + 2i))^2 = 4(1 + 2i)^2$. So

$$z = \frac{-2 + (2 + 4i)}{2} = 2i \quad \text{or} \quad z = \frac{-2 - (2 + 4i)}{2} = -2 - 2i.$$

Equivalently, completing the square, $z^2 + 2z + 4 - 4i = (z + 1)^2 - (-3 + 4i)$, so $z + 1 = \pm(1 + 2i)$. Check: $(2i)^2 + 2(2i) + 4 - 4i = -4 + 4i + 4 - 4i = 0$.

Exercise. B2: Put the proof in order

The nine lines below include the seven lines of a proof of [Proposition 1.4.3](#), shuffled, and two lines that do not belong. Write the seven lines in an order that makes a proof, and say what is wrong with each of the other two.

- (i) $i^2 = -1$, so $-1 > 0$.
- (ii) Since $i \neq 0$, we have $i > 0$.
- (iii) Suppose $<$ is a relation on $\mathbb{C}$ that makes $\mathbb{C}$ an ordered field.
- (iv) $0 < 0$ is impossible by (O1), so no such relation exists.
- (v) So $i^2 > 0$, because non-zero squares are positive in an ordered field.
- (vi) $1 \neq 0$, so $1 = 1^2 > 0$.
- (vii) $i^2 = -1 < 0$, because $-1 < 0$ in $\mathbb{R}$.
- (viii) $i \neq 0$, since $i = (0, 1) \neq (0, 0)$.

(ix) Adding, $0 = 1 + (-1) > 0 + 0 = 0$.

Solution. An admissible order is (iii), (viii), (v), (i), (vi), (ix), (iv). The constraints are what each line uses: (v), (vi), (i), (ix) and (iv) work in the supposed order, so they come after (iii); (v) also uses (viii); (i) uses (v); (ix) uses (i) and (vi); (iv) uses (ix). Line (viii) is a fact about $\mathbb{C}$ and uses no order, so it may stand anywhere before (v), even before (iii); line (vi) may stand anywhere after (iii) and before (ix). For instance (iii), (vi), (viii), (v), (i), (ix), (iv) and (viii), (iii), (v), (i), (vi), (ix), (iv) are also admissible. The admissible orders are exactly those that respect these constraints.

Line (ii) drops a case: from $i \neq 0$, trichotomy (O1) gives $i > 0$ **or** $i < 0$, and the line keeps only the first. That is (N7) of Logic and Proof, Example (What is not allowed), a missing case. Line (v) needs neither case, which is why the proof does not split.

Line (vii) cites a reason that is not available: the supposed order on $\mathbb{C}$ is arbitrary, and nothing says that it agrees with the order of $\mathbb{R}$ on the real numbers. The proposition is about **every** relation on $\mathbb{C}$, and (vii) quietly replaces “every” by “one that extends $\mathbb{R}$ ’s order”. (The inequality $-1 < 0$ does hold in any ordered field, by Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (a) applied to $1 > 0$, so the line could be repaired by citing that; as written its reason is (N9) of Logic and Proof, Example (What is not allowed), a fact that is not available.)

Exercise. B3

Let $a, b, c \in \mathbb{R}$ with $a \neq 0$ and $b^2 - 4ac < 0$. Prove that the equation $az^2 + bz + c = 0$ has exactly the two solutions

$$z = \frac{-b + i\sqrt{4ac - b^2}}{2a} \quad \text{and} \quad z = \frac{-b - i\sqrt{4ac - b^2}}{2a}$$

in $\mathbb{C}$, and that they are conjugate to each other.

Solution. Since $4ac - b^2 > 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (a)), $q := \sqrt{4ac - b^2}$ exists, $q > 0$, and $d := iq$ satisfies $d^2 = i^2 q^2 = -(4ac - b^2) = b^2 - 4ac$. So Corollary 1.4.2 with this d gives exactly the two solutions displayed, and they are distinct since $b^2 - 4ac \neq 0$. Since a, b, q are real and $2a \neq 0$, the two solutions are

$$-\frac{b}{2a} + \frac{q}{2a}i \quad \text{and} \quad -\frac{b}{2a} - \frac{q}{2a}i,$$

with the same real part and opposite imaginary parts: each is the conjugate of the other (Definition 1.2.1). For instance $z^2 - 2z + 5 = 0$ has $b^2 - 4ac = -16$, $q = 4$, and the solutions $1 \pm 2i$.

1.4.5.3 C. Going deeper

Exercise. C1: Find the error

Here is an argument.

Claim. For $z, w \in \mathbb{C}$, if $z^2 = w^2$, then $z = w$ or $z = -w$.

Proof. If $w = 0$, then $z^2 = 0$, so $z = 0 = w$, since $\mathbb{C}$ has no zero divisors. If $w \neq 0$, put $u := z/w$, which exists because $\mathbb{C}$ is a field; then $u^2 = z^2/w^2 = 1$. Taking square roots, $u = \sqrt{u^2} = \sqrt{1} = 1$. In particular, $u = 1$ or $u = -1$. Multiplying by w , $z = w$ or $z = -w$.

Is the claim true? Does the argument prove it? If not, name the line that fails and the reason, give a counterexample to that line, and repair the argument.

Solution. The claim is true: it is the argument of [Proposition 1.4.1](#) (b), and it also follows directly from $(z - w)(z + w) = z^2 - w^2 = 0$ and the absence of zero divisors in $\mathbb{C}$.

The argument does not prove it. The failing line is “ $u = \sqrt{u^2} = \sqrt{1} = 1$ ”. It uses the rule “ $u = \sqrt{u^2}$ whenever u^2 is a non-negative real”, which is neither proved nor true: it is a general “fact” of the kind (N9) of Logic and Proof, Example (What is not allowed) forbids. The symbol $\sqrt{}$ is defined only on non-negative reals, and u is a complex number; even for real u , $\sqrt{u^2} = |u|$, not u . Counterexample to the step: $u = -1$ has $u^2 = 1$, but $\sqrt{u^2} = \sqrt{1} = 1 \neq u$.

The next line, “ $u = 1$ or $u = -1$ ”, is a valid weakening of $u = 1$ (a disjunction follows from either part), so it is not itself an error; it only papers over the loss of the root -1 one line earlier. The rest of the argument (the case $w = 0$, the division, and multiplying back by w) is correct.

Repair: replace the two middle lines by “Then $(u - 1)(u + 1) = u^2 - 1 = 0$, and $\mathbb{C}$ has no zero divisors, so $u = 1$ or $u = -1$.”

Marking scheme. (10 points) - 2: says the claim is true, with a reason. - 3: names the line $u = \sqrt{u^2} = \sqrt{1} = 1$ as the failing one, and its illegal rule $u = \sqrt{u^2}$. - 2: a counterexample to that step ($u = -1$, or any u with $u^2 = 1$, $u \neq 1$). - 3: a correct repair, by factoring $u^2 - 1$ and using no zero divisors (or by [Proposition 1.4.1](#) (b) applied to $z = 1$). Fatal errors (0 for the step): declaring the claim false; naming the “In particular” line instead of the $\sqrt{}$ line as the failing one, since it is a valid weakening.

Exercise. C2: A second proof that there is no order

- Use [Proposition 1.4.1](#) to give a second proof of [Proposition 1.4.3](#) in which the element i is never mentioned.
- Say why the argument in (a) does not need the special element i .
- Is the converse of the principle behind (a) true? That is: if a commutative ring with $1 \neq 0$ admits no order, must -1 be a square in it? Test the ring $\mathbb{Z}/3\mathbb{Z}$.

Solution (Hint 1). In an ordered field, which elements can be squares? For (c), list the squares of the three classes.

Solution.

- Suppose $<$ makes $\mathbb{C}$ an ordered field. Every square is then ≥ 0 : a non-zero square

is positive by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e), and $0^2 = 0$. First, $-1 \neq 0$, since otherwise $1 = -(-1) = -0 = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (a)), against $1 \neq 0$ in the field $\mathbb{C}$ (Theorem 1.2.4). By Proposition 1.4.1 (a), applied to the non-zero number -1 , some $d \in \mathbb{C}$ has $d^2 = -1$. So $-1 = d^2 \geq 0$, and as $-1 \neq 0$, $-1 > 0$. By part (e) again, $1 > 0$. Adding (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (b)), $0 = 1 + (-1) > 0$, which (O1) forbids. This is the argument of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Exercise (C1: A field that cannot be ordered), with the square root of -1 supplied by a formula.

- (b) The argument uses only that -1 is a square in $\mathbb{C}$, and that is a property of the field, not of any named element. It does not matter that the formula of Proposition 1.4.1, applied to -1 , happens to produce i ($a = -1$, $b = 0$, $r = 1$: $x = 0$, $y = 1$). The same argument shows that no field in which -1 is a square can be ordered; in particular no field in which **every** element is a square.
- (c) No. The ring $\mathbb{Z}/3\mathbb{Z}$ is a commutative ring with $[1] \neq [0]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (a), (c)), and no relation makes it an ordered commutative ring (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (e)). Its three elements are $[0], [1], [2]$ (part (b) there), with squares $[0]^2 = [0]$, $[1]^2 = [1]$, $[2]^2 = [4] = [1]$. So the squares are $[0]$ and $[1]$, while $-[1] = [2]$. Hence -1 is not a square in $\mathbb{Z}/3\mathbb{Z}$, and yet the ring cannot be ordered: the obstacle there is $3 \cdot [1] = [0]$, not a square root of -1 .

1.5 The Unit Circle and Polar Form

Addition in $\mathbb{C}$ is addition of arrows in the plane: $(a, b) + (c, d) = (a + c, b + d)$ puts the second arrow at the tip of the first. Multiplication has a picture too, and Section 1.2 already holds half of it: the modulus of a product is the product of the moduli (Theorem 1.2.2 (d)). The other half is about angles, and angles need the functions cosine and sine, which this volume does not construct. This section first proves everything about directions that needs no angle at all, then states exactly five facts about cosine and sine that it borrows, and from those five builds the polar form of a complex number and the rule “multiply the lengths, add the angles”.

1.5.1 Length and direction

Every non-zero complex number should be a length times a direction. The length is the modulus. The directions are the complex numbers of length 1, and they deserve a name.

The unit circle is the set of complex numbers at distance 1 from 0.

We write

$$\mathbb{T} := \{u \in \mathbb{C} : |u| = 1\}$$

for the **unit circle**. For $u = x + yi$ with $x, y \in \mathbb{R}$, the condition $|u| = 1$ says $\sqrt{x^2 + y^2} = 1$, that is, $x^2 + y^2 = 1$: both sides of the first equation are non-negative, so it holds exactly when the squares agree (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (g)). So $\mathbb{T}$ is the circle of radius 1 about 0 in the plane. It contains 1, -1 , i and $-i$, and also $\frac{3}{5} + \frac{4}{5}i$, since $\frac{9}{25} + \frac{16}{25} = 1$. It does not contain $1 + i$, whose modulus is $\sqrt{2} \neq 1$.

The next proposition collects what the multiplication of $\mathbb{C}$ does on $\mathbb{T}$. None of it uses an angle.

Proposition 1.5.1. The Unit Circle

- (a) $1 \in \mathbb{T}$. If $u, v \in \mathbb{T}$, then $uv \in \mathbb{T}$. If $u \in \mathbb{T}$, then $u \neq 0$ and $u^{-1} = \bar{u} \in \mathbb{T}$.
- (b) For every $z \in \mathbb{C}$ with $z \neq 0$ there is **exactly one** pair (r, u) with $r \in \mathbb{R}$, $r > 0$, $u \in \mathbb{T}$ and $z = ru$, namely $r = |z|$ and $u = z/|z|$.
- (c) For $z \in \mathbb{C}$ with $z \neq 0$: $1/z = \bar{z}$ if and only if $|z| = 1$.

Idea. Every part is a statement about moduli, so each follows from the rules of Section 1.2: moduli multiply, $u\bar{u} = |u|^2$, and only 0 has modulus 0. For (b), divide z by its length; for the uniqueness, take moduli of $z = ru$.

Proof.

- (a) By [Proposition 1.2.1](#), the modulus of the real number 1 is its absolute value, which is 1; so $1 \in \mathbb{T}$. If $|u| = |v| = 1$, then $|uv| = |u||v| = 1$ by [Theorem 1.2.2](#) (d). Let $u \in \mathbb{T}$. Then $u \neq 0$, since $|0| = 0 \neq 1$ ([Theorem 1.2.2](#) (e)). By [Theorem 1.2.2](#) (c), $u\bar{u} = |u|^2 = 1$, so $\bar{u}$ satisfies the defining equation of u^{-1} . Since $\mathbb{C}$ is a field ([Theorem 1.2.4](#)), inverses are unique (Number Systems: From $\setminus(\mathbb{N})$ to $\setminus(\mathbb{R})$, Lemma 4.1.1 (a)), and $u^{-1} = \bar{u}$. Finally $|\bar{u}| = |u| = 1$ by [Theorem 1.2.2](#) (d).
- (b) *Existence.* Let $r := |z|$. Then $r \geq 0$, and $r \neq 0$ because $z \neq 0$ ([Theorem 1.2.2](#) (e)); so $r > 0$, and its inverse r^{-1} is a positive real number (Number Systems: From $\setminus(\mathbb{N})$ to $\setminus(\mathbb{R})$, Proposition 2.5.2 (a)). By [Theorem 1.2.4](#) the inverse of r in $\mathbb{C}$ is this real number, so $u := z/|z| = r^{-1}z$ is defined, and $z = ru$. By [Theorem 1.2.2](#) (d) and [Proposition 1.2.1](#), $|u| = |r^{-1}||z| = r^{-1}r = 1$, where $|r^{-1}| = r^{-1}$ because the absolute value of a positive real number is the number itself (Number Systems: From $\setminus(\mathbb{N})$ to $\setminus(\mathbb{R})$, Definition 4.1.1). So $u \in \mathbb{T}$.
Uniqueness. Let $z = ru$ with $r > 0$ and $u \in \mathbb{T}$. Taking moduli, $|z| = |r||u| = r \cdot 1 = r$, again by [Theorem 1.2.2](#) (d) and [Proposition 1.2.1](#). Then $u = r^{-1}z = z/|z|$. So the pair is the one named in the statement.
- (c) Since inverses are unique, $1/z = \bar{z}$ holds if and only if $z\bar{z} = 1$, that is, by [Theorem 1.2.2](#) (c), if and only if $|z|^2 = 1 = 1^2$. Both $|z|$ and 1 are non-negative, so by Number Systems: From $\setminus(\mathbb{N})$ to $\setminus(\mathbb{R})$, Proposition 2.3.5 (g) neither can be strictly smaller than the other, and $|z|^2 = 1$ holds if and only if $|z| = 1$.

■

Part (b) is the picture we wanted: $z = |z| \cdot u$, a length times a direction, and both factors are forced. Part (a) says that the directions are closed under multiplication and inversion and contain 1; *Algebraic Preliminaries*, Chapter 2 calls a set with these properties, under an associative product, a group, and $\mathbb{T}$ is one of its first examples. Part (c) is a practical test: on the unit circle, and only there, dividing by z is the same as conjugating.

Quick check. Write $z = 3 + 4i$ as ru with $r > 0$ and $u \in \mathbb{T}$. What is $1/u$?

Solution. By Proposition 1.5.1 (b), $r = |3+4i| = 5$ and $u = \frac{3}{5} + \frac{4}{5}i$. By (a), $1/u = \bar{u} = \frac{3}{5} - \frac{4}{5}i$. Check: $(\frac{3}{5} + \frac{4}{5}i)(\frac{3}{5} - \frac{4}{5}i) = \frac{9}{25} + \frac{16}{25} = 1$.

So far a direction is a point u of $\mathbb{T}$, and multiplying two directions gives a third. What we cannot yet say is **how much** a direction turns the plane. For that we need to measure positions on the circle by a real number, an angle, so that multiplying directions adds angles. That is a job for cosine and sine.

1.5.2 What this volume borrows about cosine and sine

An angle should be a real number θ that walks around the circle: a point $(\cos \theta, \sin \theta)$ on $\mathbb{T}$, moving as θ moves, returning to its start after a full turn of length 2π . Defining such functions needs limits of functions, by power series or by integrals. This volume develops no limits of functions, so it does not define cosine and sine. *Analysis on the Real Line*, Chapter 10 does: there $\cos$ and $\sin$ are defined by power series, π is defined as twice the least positive zero of $\cos$, and the facts below are proved. Its $\mathbb{R}$ is a complete ordered field, so by Number Systems: From $(\mathbb{N})$ to $(\mathbb{R})$, Theorem 6.3.1 it is our $\mathbb{R}$, up to the one order-preserving field isomorphism; the functions and the number carry over along it.

We write $2\pi\mathbb{Z} := \{2\pi k : k \in \mathbb{Z}\}$, the integer multiples of 2π in $\mathbb{R}$.

Axiom 1.5.2. What This Volume Borrows about Cosine and Sine

There are functions $\cos, \sin: \mathbb{R} \rightarrow \mathbb{R}$ and a real number $\pi > 0$ with the following properties. They are **assumed here and proved in *Analysis on the Real Line*, Chapter 10.**

(T1) $\cos^2 \theta + \sin^2 \theta = 1$ for every $\theta \in \mathbb{R}$.

(T2) For all $\theta, \varphi \in \mathbb{R}$,

$$\cos(\theta + \varphi) = \cos \theta \cos \varphi - \sin \theta \sin \varphi,$$

$$\sin(\theta + \varphi) = \sin \theta \cos \varphi + \cos \theta \sin \varphi.$$

(T3) For $\theta \in \mathbb{R}$: $\cos \theta = 1$ if and only if $\theta \in 2\pi\mathbb{Z}$.

(T4) For every $(x, y) \in \mathbb{R}^2$ with $x^2 + y^2 = 1$ there is $\theta \in \mathbb{R}$ with $\cos \theta = x$ and $\sin \theta = y$.

(T5) $\sin \theta > 0$ whenever $0 < \theta < \pi$.

In words: (T1) puts the point $(\cos \theta, \sin \theta)$ on the unit circle; (T2) is the pair of addition formulas; (T3) says that the cosine reaches 1 exactly at the multiples of a full turn; (T4) says that every point of the circle is reached; (T5) says that during the first half turn the point stays in the upper half plane.

This box is where the chapter borrows. Like Logic and Proof, Axiom 4.2.1, which *Logic and Proof* assumed and *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 1 proved, it is a statement assumed in one volume and proved in another. Nothing in Sections 1.1–1.4, and nothing in this section above the box, uses it. From here on we use these five facts about $\cos$, $\sin$ and π and **no others**: no value such as $\cos(\pi/3) = \frac{1}{2}$, no periodicity, no picture of a graph. Whatever else we need, we derive, and each proof that uses one of the facts names it by its number. Two consequences come at once.

- $\cos 0 = 1$, by (T3), since $0 = 2\pi \cdot 0 \in 2\pi\mathbb{Z}$. Then (T1) gives $\sin^2 0 = 1 - 1 = 0$, so $\sin 0 = 0$, because a non-zero real number has a positive square (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.3.5 (e)).
- $\cos(2\pi k) = 1$ and $\sin(2\pi k) = 0$ for every $k \in \mathbb{Z}$, by (T3) and then (T1) in the same way.

Warning. The five facts are about $\cos$, $\sin$ and π only. A school fact such as $\sin(\pi/6) = \frac{1}{2}$ is not among them, and a proof in this volume may not quote it: [Example \(Special Angles\)](#) below derives the few values we use. Nor do the facts say that $\cos$ and $\sin$ are “periodic with period 2π ” as functions; that is true, and derivable from (T2) and (T3), but no proof here needs it.

1.5.3 Polar form

With angles available, we can name the point of $\mathbb{T}$ at angle θ .

$e^{i\theta}$ is the point of the unit circle at angle θ .

Definition 1.5.1. Polar Form

For $\theta \in \mathbb{R}$ we write

$$e^{i\theta} := \cos \theta + i \sin \theta.$$

Let $z \in \mathbb{C}$ with $z \neq 0$. A **polar form** of z is an expression $z = re^{i\theta}$ with $r \in \mathbb{R}$, $r > 0$, and $\theta \in \mathbb{R}$. Then θ is **an** argument of z .

In words: the first line is an abbreviation, not an exponential. This volume has no exponential function, the letter e on its own means nothing here, and the only rule of exponents we will use for $e^{i\theta}$ is the one proved below ([Theorem 1.5.3](#) (a)). *Analysis on the Real Line*, Chapter 10 shows that $e^{i\theta}$ is indeed the value of the complex exponential function at $i\theta$; the notation anticipates that, and the linear algebra volumes write their roots of unity with it. The exponent may be written in any form equal to $i\theta$ with θ real, and the symbol then means $e^{i\theta}$: for example $e^{-i\theta} = e^{i(-\theta)}$, $e^{2\pi i} = e^{i \cdot 2\pi}$, $e^{in\theta} = e^{i(n\theta)}$ and $e^{-2\pi i} = e^{i(-2\pi)}$. This is unambiguous, because the real number θ is determined by $i\theta$ (it is its imaginary part). The second part asks for a **positive** real r and allows **any** real θ .

The point $e^{i\theta}$ lies on $\mathbb{T}$. Indeed $|e^{i\theta}| = \sqrt{\cos^2 \theta + \sin^2 \theta} = \sqrt{1} = 1$, by [Definition 1.2.1](#) and (T1). So $re^{i\theta}$ is a length r times a direction, as in [Proposition 1.5.1](#) (b), and that proposition gives $r = |z|$ for every polar form of z .

Examples.

- $e^{i0} = \cos 0 + i \sin 0 = 1$, by the consequences of the box. So $1 = 1 \cdot e^{i0}$ and $5 = 5e^{i0}$ are polar forms.
- $e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$, by the second consequence with $k = 1$. So $1 = 1 \cdot e^{2\pi i}$ as well: 0 and 2π are both arguments of 1, and they differ, since $\pi > 0$.
- The number 0 has no polar form, since $|re^{i\theta}| = r > 0$.

A non-example by minimal change. Allow $r < 0$: then $-1 = (-1) \cdot e^{i0}$ looks like a polar form of -1 with argument 0. The clause that fails is $r > 0$, and it matters: with negative r allowed, the length could no longer be read off as $|z|$, and $1 = 1 \cdot e^{i0}$ and $-1 = (-1)e^{i0}$ would share the argument 0. We will see in [Example \(Special Angles\)](#) that $-1 = 1 \cdot e^{i\pi}$ is a genuine polar form.

The examples already show why the definition says **an** argument: $1 = e^{i0} = e^{2\pi i}$. How much freedom there is, exactly, is part (b) of [Proposition 1.5.4](#) below. First, the reason for the notation: these numbers multiply the way exponentials do.

Theorem 1.5.3. Multiplication in Polar Form

- (a) $e^{i\theta}e^{i\varphi} = e^{i(\theta+\varphi)}$ for all $\theta, \varphi \in \mathbb{R}$.
- (b) $e^{i0} = 1$, and $(e^{i\theta})^{-1} = e^{-i\theta} = \overline{e^{i\theta}}$ for every $\theta \in \mathbb{R}$.
- (c) If $r, s \in \mathbb{R}$ with $r, s > 0$ and $\theta, \varphi \in \mathbb{R}$, then $(re^{i\theta})(se^{i\varphi}) = rs e^{i(\theta+\varphi)}$, and this is a polar form of the product.

Idea. Multiply out $(\cos \theta + i \sin \theta)(\cos \varphi + i \sin \varphi)$ with the rule of [Definition 1.1.1](#): the real and imaginary parts that appear are exactly the right-hand sides of the addition formulas (T2). The rest is bookkeeping with inverses and moduli.

Proof.

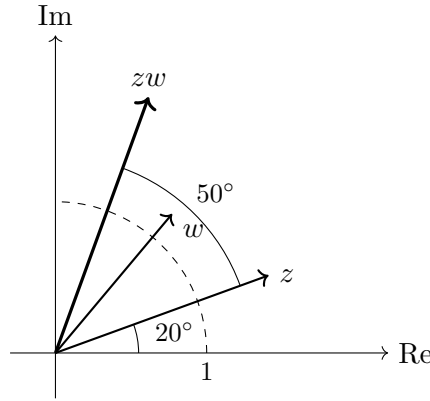
- (a) By the multiplication rule of [Definition 1.1.1](#),

$$\begin{aligned} e^{i\theta}e^{i\varphi} &= (\cos \theta \cos \varphi - \sin \theta \sin \varphi) + (\cos \theta \sin \varphi + \sin \theta \cos \varphi)i \\ &= \cos(\theta + \varphi) + i \sin(\theta + \varphi), \end{aligned}$$

where the second equality is (T2), with the two products in the imaginary part re-ordered by commutativity in $\mathbb{R}$. The right-hand side is $e^{i(\theta+\varphi)}$.

- (b) $e^{i0} = 1$ was shown in the first example above. By (a) with $\varphi = -\theta$, $e^{i\theta}e^{-i\theta} = e^{i0} = 1$, so $e^{-i\theta}$ is the inverse of $e^{i\theta}$, by uniqueness of inverses in the field $\mathbb{C}$ ([Theorem 1.2.4](#), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 4.1.1 (a)). Since $e^{i\theta} \in \mathbb{T}$, its inverse is also its conjugate ([Proposition 1.5.1](#) (a)).
- (c) By [Proposition 1.1.2](#) (commutativity and associativity of $\cdot$), $(re^{i\theta})(se^{i\varphi}) = (rs)(e^{i\theta}e^{i\varphi})$, and (a) turns this into $rs e^{i(\theta+\varphi)}$. Here $rs > 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (c) (multiply $0 < r$ by $s > 0$), so this is a polar form. ■

In words: **to multiply two complex numbers, multiply their moduli and add their arguments**. This is the chapter's third named move, **multiply moduli, add angles**. Multiplying by a fixed $w = se^{i\varphi}$ therefore turns the plane about 0 by the angle φ and stretches it by the factor s . The picture shows z , w and zw for $|z| = 1.5$, $|w| = 1.2$, and arguments of 20° and 50° (a full turn being 360° , that is, 2π).



The arrow for zw has length $1.5 \times 1.2 = 1.8$ and makes the angle $20^\circ + 50^\circ = 70^\circ$ with the positive real axis: it is the arrow for z , turned by the argument of w and stretched by the modulus of w . The small arc marks the argument of z , the large arc the extra turn by the argument of w , and the dashed arc is part of the unit circle, where the numbers $e^{i\theta}$ live.

Now the freedom in the argument. Every non-zero number has a polar form, and its arguments are determined up to a whole number of full turns.

Proposition 1.5.4. Existence and Uniqueness of Polar Form

- (a) Every $z \in \mathbb{C}$ with $z \neq 0$ has a polar form, and every polar form $z = re^{i\theta}$ has $r = |z|$.
- (b) For $r, s \in \mathbb{R}$ with $r, s > 0$ and $\theta, \varphi \in \mathbb{R}$,

$$re^{i\theta} = se^{i\varphi} \iff r = s \text{ and } \theta - \varphi \in 2\pi\mathbb{Z}.$$

Proof.

- (a) By Proposition 1.5.1 (b), $z = |z| \cdot u$ with $u = x + yi \in \mathbb{T}$, so $x^2 + y^2 = 1$. By (T4) there is $\theta \in \mathbb{R}$ with $\cos \theta = x$ and $\sin \theta = y$, that is, $u = e^{i\theta}$. Hence $z = |z|e^{i\theta}$, with $|z| > 0$. Conversely, if $z = re^{i\theta}$ is a polar form, then $e^{i\theta} \in \mathbb{T}$, and the uniqueness in Proposition 1.5.1 (b) gives $r = |z|$.
- (b) Suppose first that $re^{i\theta} = se^{i\varphi}$. The number $re^{i\theta}$ is non-zero: $r \neq 0$, $e^{i\theta} \in \mathbb{T}$ is non-zero (Proposition 1.5.1 (a)), and a product of non-zero elements of the field $\mathbb{C}$ is non-zero (Theorem 1.2.4, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 4.1.1 (d)). So both sides are polar forms of the same non-zero number, and $r = s$ by (a). Multiplying by r^{-1} gives $e^{i\theta} = e^{i\varphi}$. In the other direction, if $r = s$, the two sides are equal exactly when $e^{i\theta} = e^{i\varphi}$. So it remains to show that $e^{i\theta} = e^{i\varphi}$ if and only if $\theta - \varphi \in 2\pi\mathbb{Z}$.

Multiplying by $e^{-i\varphi}$, and back by $e^{i\varphi}$, shows that $e^{i\theta} = e^{i\varphi}$ holds if and only if $e^{i\theta}e^{-i\varphi} = e^{i\varphi}e^{-i\varphi}$, that is, by Theorem 1.5.3 (a) and (b), if and only if $e^{i(\theta-\varphi)} = 1$. Comparing real and imaginary parts, this says $\cos(\theta - \varphi) = 1$ and $\sin(\theta - \varphi) = 0$. The second condition follows from the first: by (T1), $\cos(\theta - \varphi) = 1$ gives $\sin^2(\theta - \varphi) = 0$, hence $\sin(\theta - \varphi) = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)). So $e^{i\theta} = e^{i\varphi}$ if and only if $\cos(\theta - \varphi) = 1$, and by (T3) that holds if and only if $\theta - \varphi \in 2\pi\mathbb{Z}$. ■

Existence came from (T4), and uniqueness from (T3), with (T1) helping and (T2) entering through Theorem 1.5.3. “Comparing arguments” therefore always means comparing them up to

a multiple of 2π , and the next warning is the trap this sets.

Warning. From $e^{i\theta} = e^{i\varphi}$ one may **not** conclude $\theta = \varphi$: $e^{i0} = e^{2\pi i} = 1$, and $0 \neq 2\pi$. Only $\theta - \varphi \in 2\pi\mathbb{Z}$ follows (Proposition 1.5.4 (b)). Forgetting this loses solutions as soon as an equation is solved for an angle; Section 1.6 meets an equation where it would lose all but one of them.

1.5.4 Powers

Repeating Theorem 1.5.3 gives powers. The powers z^n are those of the recursion $z^0 = 1$, $z^{n+1} = z^n z$ (Proposition 1.1.3).

Theorem 1.5.5. De Moivre's Formula

For every $\theta \in \mathbb{R}$ and every $n \in \mathbb{N}$,

$$(e^{i\theta})^n = e^{in\theta}, \quad \text{that is,} \quad (\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta.$$

Consequently $(re^{i\theta})^n = r^n e^{in\theta}$ for every real $r > 0$, and this is a polar form.

Idea. A power is a repeated product, and each new factor $e^{i\theta}$ adds θ to the argument, by Theorem 1.5.3 (a). So induction on n , along the recursion $z^{n+1} = z^n z$.

Proof. We use Logic and Proof, Axiom 4.2.1 on n , read on $\mathbb{N} = \omega$ through Number Systems: From $\backslash(\backslash n \mathbb{N} \backslash)$ to $\backslash(\backslash n \mathbb{R} \backslash)$, Corollary 1.7.3 (b); here $n\theta$ is the product in $\mathbb{R}$ of $n \cdot 1_{\mathbb{R}}$ and θ (Number Systems: From $\backslash(\backslash n \mathbb{N} \backslash)$ to $\backslash(\backslash n \mathbb{R} \backslash)$, Definition 4.2.1 (a)). For $n = 0$, the left side is $(e^{i\theta})^0 = 1$ by the recursion, and the right side is $e^{i0} = 1$ by Theorem 1.5.3 (b). Suppose $(e^{i\theta})^n = e^{in\theta}$ for some $n \in \mathbb{N}$. Then

$$(e^{i\theta})^{n+1} = (e^{i\theta})^n e^{i\theta} = e^{in\theta} e^{i\theta} = e^{i(n\theta+\theta)} = e^{i(n+1)\theta},$$

by the recursion, the induction hypothesis, Theorem 1.5.3 (a), and $(n+1) \cdot 1_{\mathbb{R}} = n \cdot 1_{\mathbb{R}} + 1_{\mathbb{R}}$ (Number Systems: From $\backslash(\backslash n \mathbb{N} \backslash)$ to $\backslash(\backslash n \mathbb{R} \backslash)$, Definition 4.2.1 (a)) with distributivity in $\mathbb{R}$. This proves the formula for every $n \in \mathbb{N}$.

For the consequence, Proposition 1.1.3 (c) gives $(re^{i\theta})^n = r^n (e^{i\theta})^n = r^n e^{in\theta}$. The power r^n is the same whether it is computed in $\mathbb{R}$ or in $\mathbb{C}$, by the remark after Proposition 1.1.3 in Section 1.1, and $r^n > 0$ because a product of positive reals is positive (Number Systems: From $\backslash(\backslash n \mathbb{N} \backslash)$ to $\backslash(\backslash n \mathbb{R} \backslash)$, Proposition 2.3.5 (c); induction on n , with $r^0 = 1 > 0$).

■

For a negative exponent, Exercise C1 below defines z^{-n} locally and proves the matching formula; nothing in the text uses it.

The five borrowed facts give no particular value of $\cos$ or $\sin$ except at multiples of 2π . Every other value this chapter uses is derived next, from (T1)–(T5) and the algebra of Sections 1.1–1.4.

Example. Special Angles

Show, using only (T1)–(T5) and the results proved so far, that

$$\begin{aligned} e^{i\pi} &= -1, & e^{i\pi/2} &= i, & e^{i\pi/3} &= \frac{1}{2} + \frac{\sqrt{3}}{2}i, \\ e^{i\pi/6} &= \frac{\sqrt{3}}{2} + \frac{1}{2}i, & e^{i\pi/4} &= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i. \end{aligned}$$

Solution. Each value is found the same way: a power of the unknown point is a point we already know, and (T5) chooses between the candidates. Since $\pi > 0$, each of $\pi/2, \pi/3, \pi/4, \pi/6$ lies strictly between 0 and π , so (T5) gives $\operatorname{Im} e^{i\theta} = \sin \theta > 0$ for each of them.

- (i) $e^{i\pi} = -1$. Let $u := e^{i\pi}$. By [Theorem 1.5.5](#), $u^2 = e^{2\pi i} = 1$, so $(u-1)(u+1) = u^2 - 1 = 0$, and since $\mathbb{C}$ has no zero divisors ([Theorem 1.2.4](#), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Lemma 4.1.1 (d)), $u = 1$ or $u = -1$. Suppose $u = 1$. Then $\cos \pi = 1$, so $\pi = 2\pi k$ for some $k \in \mathbb{Z}$ by (T3); dividing by $\pi \neq 0$ gives $1 = 2k$ in $\mathbb{R}$, an equation between images of integers. The embedding of $\mathbb{Z}$ into $\mathbb{R}$, through $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.4.4) and κ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 5.6.3), is injective and preserves $+$ and $\cdot$, so $1 = 2k$ holds in $\mathbb{Z}$. But $1 = 2 \cdot 0 + 1$ is odd, and an odd integer is not of the form $2k$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Corollary 3.1.3 (a)). So $u \neq 1$, and $e^{i\pi} = -1$.
- (ii) $e^{i\pi/2} = i$. Let $u := e^{i\pi/2}$. By [Theorem 1.5.3](#) (a), $u^2 = e^{i\pi} = -1 = i^2$, so $(u-i)(u+i) = 0$ and $u = \pm i$. Since $\operatorname{Im} u > 0$ and $\operatorname{Im}(-i) = -1 < 0$, $u = i$.
- (iii) $e^{i\pi/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Let $u := e^{i\pi/3}$. By [Theorem 1.5.5](#), $u^3 = e^{i\pi} = -1$. Multiplying out shows $(u+1)(u^2-u+1) = u^3+1 = 0$. Now $u \neq -1$, since $\operatorname{Im} u > 0$; so $u^2-u+1 = 0$. By [Corollary 1.4.2](#) with $a = 1, b = -1, c = 1$, and $d := \sqrt{3}i$, a square root of $b^2 - 4ac = -3$ (indeed $(\sqrt{3}i)^2 = 3i^2 = -3$),

$$u = \frac{1 + \sqrt{3}i}{2} \quad \text{or} \quad u = \frac{1 - \sqrt{3}i}{2}.$$

Since $\operatorname{Im} u > 0$, $u = \frac{1}{2} + \frac{\sqrt{3}}{2}i$.

- (iv) $e^{i\pi/6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i$. Since $\pi/6 = \pi/2 + (-\pi/3)$, [Theorem 1.5.3](#) (a) and (b) give

$$e^{i\pi/6} = e^{i\pi/2} e^{-i\pi/3} = i \cdot \overline{e^{i\pi/3}} = i \left(\frac{1}{2} - \frac{\sqrt{3}}{2}i \right) = \frac{\sqrt{3}}{2} + \frac{1}{2}i,$$

by (ii) and (iii).

- (v) $e^{i\pi/4} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$. Let $u := e^{i\pi/4}$. By [Theorem 1.5.3](#) (a) and (ii), $u^2 = e^{i\pi/2} = i$. The formula of [Proposition 1.4.1](#) for $z = i$ (so $a = 0, b = 1, r = |i| = 1$) gives the square root $w = \sqrt{1/2} + \sqrt{1/2}i$, and $\sqrt{1/2} = 1/\sqrt{2}$, since both are non-negative and square to $\frac{1}{2}$. By [Proposition 1.4.1](#) (b), $u = w$ or $u = -w$, and $\operatorname{Im} u > 0$ rules out $-w$. So $u = w$.

Comparing real and imaginary parts turns these into values of $\cos$ and $\sin$:

θ	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$	π
$\cos \theta$	1	$\sqrt{3}/2$	$1/\sqrt{2}$	$1/2$	0	-1
$\sin \theta$	0	$1/2$	$1/\sqrt{2}$	$\sqrt{3}/2$	1	0

These are the familiar values, now proved from the five facts.

Two special cases of the rotation picture are worth isolating. Multiplying by $i = e^{i\pi/2}$ turns the plane by a quarter turn, counterclockwise; two quarter turns make a half turn, and this is the picture behind $i^2 = -1 = e^{i\pi}$. And multiplying by $e^{-i\theta} = \overline{e^{i\theta}}$ undoes the turn by θ (Theorem 1.5.3 (b)).

Powers that are tedious to expand become one line in polar form.

Example. A Power via Polar Form

Compute $(\sqrt{3} + i)^6$.

Solution. We have $\sqrt{3} + i = 2(\frac{\sqrt{3}}{2} + \frac{1}{2}i) = 2e^{i\pi/6}$, by Example (Special Angles) (iv). By Theorem 1.5.5 and Example (Special Angles) (i),

$$(\sqrt{3} + i)^6 = 2^6 e^{i \cdot 6\pi/6} = 64 e^{i\pi} = -64.$$

By hand: $(\sqrt{3} + i)^2 = 3 + 2\sqrt{3}i - 1 = 2 + 2\sqrt{3}i = 2(1 + \sqrt{3}i)$, and $(1 + \sqrt{3}i)^3 = (1 + \sqrt{3}i)(-2 + 2\sqrt{3}i) = -2 - 6 = -8$, so $(\sqrt{3} + i)^6 = (2(1 + \sqrt{3}i))^3 = 8 \cdot (-8) = -64$ (Proposition 1.1.3 (b), (c)), the same answer.

Quick check. Use polar form to compute $(1 + i)^8$, and check the answer with $(1 + i)^2 = 2i$.

Solution. By Example (Special Angles) (v), $1 + i = \sqrt{2}(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i) = \sqrt{2}e^{i\pi/4}$. By Theorem 1.5.5, $(1 + i)^8 = (\sqrt{2})^8 e^{i \cdot 8\pi/4} = 16 e^{2\pi i} = 16$, since $(\sqrt{2})^8 = ((\sqrt{2})^2)^4 = 2^4 = 16$ and $e^{2\pi i} = 1$. Check: $(1 + i)^8 = ((1 + i)^2)^4 = (2i)^4 = 16i^4 = 16$, by Proposition 1.1.3 (b), (c).

1.5.5 Exercises

1.5.5.1 A. Check your understanding

Exercise. A1

- Give a polar form of -2 and of $3i$.
- True or false: if $e^{i\theta} = e^{i\varphi}$, then $\theta = \varphi$. Justify your answer.
- In Proposition 1.5.4, which of the borrowed facts (T1)–(T5) gives the existence of a polar form, and which gives the uniqueness of the argument up to $2\pi\mathbb{Z}$?
- Which results of Sections 1.1–1.5 use none of the borrowed facts? Is Proposition 1.5.1 among them?

Solution.

- (a) $-2 = 2e^{i\pi}$ and $3i = 3e^{i\pi/2}$, by [Example \(Special Angles\)](#) (i) and (ii); the moduli 2 and 3 are positive, as a polar form requires. (Any $\pi + 2\pi k$, respectively $\pi/2 + 2\pi k$, with $k \in \mathbb{Z}$, is also an argument, by [Proposition 1.5.4](#) (b).)
- (b) False. $e^{i0} = 1 = e^{2\pi i}$, but $0 \neq 2\pi$ since $\pi > 0$. What is true is $\theta - \varphi \in 2\pi\mathbb{Z}$ ([Proposition 1.5.4](#) (b)).
- (c) Existence: (T4), which provides an angle for the point $z/|z|$ of $\mathbb{T}$. Uniqueness: (T3), which turns $\cos(\theta - \varphi) = 1$ into $\theta - \varphi \in 2\pi\mathbb{Z}$; (T1) is used alongside it, to see that $\sin(\theta - \varphi) = 0$ follows from $\cos(\theta - \varphi) = 1$, and (T2) enters through [Theorem 1.5.3](#), which turns $e^{i\theta} = e^{i\varphi}$ into $e^{i(\theta-\varphi)} = 1$.
- (d) Everything in Sections 1.1–1.4, and the part of this section before [Axiom 1.5.2](#); after the box, only Exercise C2, which is set up to avoid them. In particular [Proposition 1.5.1](#) uses none of them: its proof uses only the modulus rules of Section 1.2, the field properties of $\mathbb{C}$, and order facts about $\mathbb{R}$ from *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* .

1.5.5.2 B. Practice

Exercise. B1

Compute $(1 - \sqrt{3}i)^6$.

Solution. We have $1 - \sqrt{3}i = 2(\frac{1}{2} - \frac{\sqrt{3}}{2}i) = 2e^{i\pi/3} = 2e^{-i\pi/3}$, by [Example \(Special Angles\)](#) (iii) and [Theorem 1.5.3](#) (b). By [Theorem 1.5.5](#),

$$(1 - \sqrt{3}i)^6 = 2^6 e^{-6i\pi/3} = 64 e^{-2\pi i} = 64,$$

since $-2\pi = 2\pi \cdot (-1) \in 2\pi\mathbb{Z}$, so $\cos(-2\pi) = 1$ and $\sin(-2\pi) = 0$ by (T3) and (T1), and $e^{-2\pi i} = 1$.

Exercise. B2: Symmetries of Cosine and Sine

Prove that for every $\theta \in \mathbb{R}$:

$$\begin{aligned} \cos(-\theta) &= \cos \theta, & \sin(-\theta) &= -\sin \theta, & \cos(\theta + \pi) &= -\cos \theta, \\ \sin(\theta + \pi) &= \sin \theta, & \cos \theta &= \sin(\theta + \pi/2). \end{aligned}$$

Hint: write each left side as a part of some $e^{i\psi}$, and compute that $e^{i\psi}$ with [Theorem 1.5.3](#).

Solution. By [Theorem 1.5.3](#) (b), $e^{-i\theta} = \overline{e^{i\theta}}$, that is, $\cos(-\theta) + i\sin(-\theta) = \cos \theta - i\sin \theta$. Comparing real and imaginary parts gives $\cos(-\theta) = \cos \theta$ and $\sin(-\theta) = -\sin \theta$.

By [Theorem 1.5.3](#) (a) and [Example \(Special Angles\)](#) (i), $e^{i(\theta+\pi)} = e^{i\theta} e^{i\pi} = -e^{i\theta}$, that is, $\cos(\theta + \pi) + i\sin(\theta + \pi) = -\cos \theta - i\sin \theta$. Comparing parts gives the next two identities.

By [Theorem 1.5.3](#) (a) and [Example \(Special Angles\)](#) (ii), $e^{i(\theta+\pi/2)} = ie^{i\theta} = i\cos \theta - \sin \theta$.

Comparing imaginary parts gives $\sin(\theta + \pi/2) = \cos \theta$. (Comparing real parts gives, in addition, $\cos(\theta + \pi/2) = -\sin \theta$.)

Exercise. B3

Let $\theta \in \mathbb{R}$. Show that $|e^{i\theta} - 1|^2 = 2 - 2\cos \theta$. Hence show again that $e^{i\theta} = 1$ if and only if $\cos \theta = 1$.

Solution. Let $u := e^{i\theta}$, so $u\bar{u} = |u|^2 = 1$. Squaring the modulus, by [Theorem 1.2.2](#) (a)–(c),

$$|u - 1|^2 = (u - 1)\overline{(u - 1)} = (u - 1)(\bar{u} - 1) = u\bar{u} - (u + \bar{u}) + 1 = 2 - 2\operatorname{Re} u,$$

and $\operatorname{Re} u = \cos \theta$. Hence $|u - 1|^2 = 2 - 2\cos \theta$.

Now $u = 1$ if and only if $|u - 1| = 0$ ([Theorem 1.2.2](#) (e)), if and only if $|u - 1|^2 = 0$ (a real number is 0 exactly when its square is: $0^2 = 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b), and a non-zero square is positive by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)), if and only if $2 - 2\cos \theta = 0$, that is, $\cos \theta = 1$.

1.5.5.3 C. Going deeper

Exercise. C1: Triple Angles and Negative Powers

- (a) Prove that $\cos 3\theta = 4\cos^3 \theta - 3\cos \theta$ and $\sin 3\theta = 3\sin \theta - 4\sin^3 \theta$ for every $\theta \in \mathbb{R}$.
- (b) For $z \in \mathbb{C}$ with $z \neq 0$ and $n \in \mathbb{N}$, put $z^{-n} := (z^{-1})^n$ (a definition local to this exercise). Show that $(e^{i\theta})^{-n} = e^{-in\theta}$.

Solution.

- (a) Write $c := \cos \theta$ and $s := \sin \theta$. By [Theorem 1.5.5](#), $\cos 3\theta + i\sin 3\theta = (c + is)^3$. Now $(c + is)^2 = (c^2 - s^2) + 2csi$, and

$$\begin{aligned} (c + is)^3 &= ((c^2 - s^2) + 2csi)(c + is) \\ &= (c^3 - 3cs^2) + (3c^2s - s^3)i. \end{aligned}$$

Comparing real parts and using $s^2 = 1 - c^2$ (T1), $\cos 3\theta = c^3 - 3c(1 - c^2) = 4c^3 - 3c$. Comparing imaginary parts and using $c^2 = 1 - s^2$, $\sin 3\theta = 3(1 - s^2)s - s^3 = 3s - 4s^3$.

- (b) By [Theorem 1.5.3](#) (b), $(e^{i\theta})^{-1} = e^{-i\theta} = e^{i(-\theta)}$. By [Theorem 1.5.5](#) applied to $-\theta$, $(e^{i\theta})^{-n} = (e^{i(-\theta)})^n = e^{in(-\theta)} = e^{-in\theta}$.

Nothing in this chapter uses negative powers of complex numbers; the definition in (b) is for practice only.

Exercise. C2: Points on the Circle without Angles

For $t \in \mathbb{R}$ put

$$u_t := \frac{1 + it}{1 - it}.$$

- (a) Show that u_t is defined, that $u_t \in \mathbb{T}$, and that $u_t \neq -1$.
- (b) Show that every $u \in \mathbb{T}$ with $u \neq -1$ equals u_t for **exactly one** $t \in \mathbb{R}$, namely $t = \operatorname{Im} u / (1 + \operatorname{Re} u)$.
- (c) Compute $u_{1/2}$ in the form $a + bi$.

Use none of the borrowed facts (T1)–(T5).

Solution (Hint 1). For (b), on the unit circle the conjugate is the inverse: $\bar{u} = 1/u$.

Solution (Hint 2). Clearing the denominator, $u = u_t$ is equivalent to $u - 1 = it(u + 1)$, and $u + 1 \neq 0$, so t is determined; it remains to show that $(u - 1)/(i(u + 1))$ is real.

Solution.

- (a) The real part of $1 - it$ is 1, so $1 - it \neq 0$ and the quotient is defined. The numbers $1 + it$ and $1 - it$ are conjugate, so they have the same modulus ([Theorem 1.2.2 \(d\)](#)), which is non-zero. From $u_t(1 - it) = 1 + it$ and [Theorem 1.2.2 \(d\)](#), $|u_t||1 - it| = |1 + it| = |1 - it|$, and canceling the non-zero real number $|1 - it|$ gives $|u_t| = 1$. If $u_t = -1$, then $1 + it = -(1 - it) = -1 + it$, so $1 = -1$, which is false. So $u_t \neq -1$.
- (b) Let $u \in \mathbb{T}$ with $u \neq -1$, and let $t \in \mathbb{R}$. Since $1 - it \neq 0$, the equation $u = u_t$ is equivalent to $u(1 - it) = 1 + it$, that is, to

$$u - 1 = it(u + 1).$$

Since $i(u + 1) \neq 0$, this holds if and only if $t = t_0$, where $t_0 := (u - 1)/(i(u + 1)) \in \mathbb{C}$. So at most one real t has $u_t = u$, and one does exactly when t_0 is real. Using $u\bar{u} = 1$,

$$(u - 1)(\bar{u} + 1) = u\bar{u} + u - \bar{u} - 1 = u - \bar{u} = 2i \operatorname{Im} u,$$

where $u - \bar{u} = 2i \operatorname{Im} u$ by [Definition 1.2.1](#) (with $u = a + bi$, $(a + bi) - (a - bi) = 2bi$); and $(u + 1)(\bar{u} + 1) = |u + 1|^2 = 2 + 2 \operatorname{Re} u$, by [Theorem 1.2.2 \(a\)](#), (c). This is a positive real number, since $u + 1 \neq 0$. Multiplying numerator and denominator of $(u - 1)/(u + 1)$ by $\bar{u} + 1 = \overline{u + 1} \neq 0$,

$$t_0 = \frac{1}{i} \cdot \frac{2i \operatorname{Im} u}{2 + 2 \operatorname{Re} u} = \frac{\operatorname{Im} u}{1 + \operatorname{Re} u},$$

a real number. So exactly one $t \in \mathbb{R}$ has $u_t = u$, namely t_0 .

- (c) Multiplying numerator and denominator by the conjugate $1 + \frac{1}{2}i$ of the denominator,

$$u_{1/2} = \frac{(1 + \frac{1}{2}i)^2}{1 + \frac{1}{4}} = \frac{\frac{3}{4} + i}{\frac{5}{4}} = \frac{3}{5} + \frac{4}{5}i.$$

Check against (b): $\operatorname{Im} u / (1 + \operatorname{Re} u) = \frac{4/5}{8/5} = \frac{1}{2}$.

So the map $t \mapsto u_t$ is a bijection from $\mathbb{R}$ onto $\mathbb{T} \setminus \{-1\}$, and it was found with no angle. For rational t , the point u_t has rational coordinates: the computation in (c) with t in place of $\frac{1}{2}$ gives $u_t = ((1 - t^2) + 2ti)/(1 + t^2)$, and $t = 1/2$ gives the point $(3/5, 4/5)$ behind the right triangle with sides 3, 4, 5.

Marking scheme. (10 points) - 2: $1 - it \neq 0$ with a reason, and $|u_t| = 1$ from the equal moduli of conjugates. - 1: $u_t \neq -1$. - 2: $u = u_t$ rewritten as a linear equation in t , with $u + 1 \neq 0$ used to solve it uniquely. - 3: shows that the unique solution is real and equals $\operatorname{Im} u / (1 + \operatorname{Re} u)$, with $1 + \operatorname{Re} u \neq 0$ justified (for example by multiplying by $\overline{u + 1}$ and using $u\bar{u} = 1$, with $2 + 2\operatorname{Re} u > 0$). - Second route (coordinates $u = x + yi$, $x^2 + y^2 = 1$): the two lines above (5 points) become 2 for splitting $u - 1 = it(u + 1)$ into $x - 1 = -ty$ and $y = t(1 + x)$, showing $x \neq -1$ (otherwise $u = -1$) and so $t = y/(1 + x)$ is forced; and 3 for checking that this t satisfies $x - 1 = -ty$, using $x^2 + y^2 = 1$. - 2: (c) computed and checked. Fatal errors (0 for the step): writing $u = e^{i\theta}$ and using a half-angle formula (borrowed facts, and values not derived here); dividing by $1 + \operatorname{Re} u$ without showing it is non-zero.

1.6 Higher Roots, Roots of Unity, and a Look Ahead

Section 1.4 solved $z^2 = c$ with real square roots alone. Polar form turns the general equation $z^n = c$ into a question about lengths and angles: by De Moivre's formula ([Theorem 1.5.5](#)), raising to the n -th power raises the modulus to the n -th power and multiplies the argument by n . The angle part is a linear equation for a real number, with the ambiguity $2\pi\mathbb{Z}$ of [Proposition 1.5.4](#) attached. The length part is the real equation $r^n = \rho$ with $\rho > 0$, and before anything else we must know that it has exactly one positive solution. This section proves that, solves $z^n = c$, counts the solutions, studies the case $c = 1$, and ends with a look ahead at polynomial equations in general.

1.6.1 Real n -th roots

For $n = 2$, *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 6 built the square root by the move **construct a point as a supremum** (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 6.1.4), and an exercise there ran the same move for cube roots (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Exercise (B2: Cube roots)). For a general exponent the move is the same; only the estimate for $(s + h)^n$ needs a new tool, and [Lemma 1.1.4](#) supplies it. Here $n \cdot 1_{\mathbb{R}}$ is written n , and powers in $\mathbb{R}$ are those of [Proposition 1.1.3](#) with $R = \mathbb{R}$, the same recursion as Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Definition 4.2.1 (b).

Lemma 1.6.1. Real n -th Roots

Let $n \in \mathbb{N}$ with $n \geq 1$.

- (a) If $s, t \in \mathbb{R}$ and $0 \leq s < t$, then $s^n < t^n$.
- (b) For every $a \in \mathbb{R}$ with $a \geq 0$ there is **exactly one** $b \in \mathbb{R}$ with $b \geq 0$ and $b^n = a$. We write $\sqrt[n]{a} := b$. For $n = 2$ it is the square root $\sqrt{a}$ of Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 6.1.4.

Idea. Part (a) is the factorization $t^n - s^n = (t - s)(t^{n-1} + t^{n-2}s + \cdots + s^{n-1})$: both factors are positive. For (b), let s be the supremum of the set S of non-negative y with $y^n \leq a$, and rule out $s^n < a$ and $s^n > a$.

If $s^n < a$, we want $h > 0$ with $(s + h)^n \leq a$. Working backwards: for $0 < h \leq 1$, the same factorization writes $(s + h)^n - s^n$ as h times a sum of n terms, each at most $(s + 1)^{n-1}$. So $(s + h)^n - s^n \leq h \cdot n(s + 1)^{n-1}$, and it is enough that this be at most half the room $a - s^n$. That gives $h := \min\{1, (a - s^n)/(2n(s + 1)^{n-1})\}$.

If $s^n > a$, we want $h > 0$ with $(s - h)^n \geq a$ still, which makes $s - h$ a smaller upper bound. Now $s^n - (s - h)^n \leq h \cdot ns^{n-1}$, and it is enough that this equal the excess $s^n - a$. That gives $h := (s^n - a)/(ns^{n-1})$.

Proof. Three facts are used throughout: a power of a non-negative real number is non-negative and a power of a positive one is positive (induction on the exponent with Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (c)); if $0 \leq y \leq 1$ then $y^k \leq y$ for every $k \geq 1$, while if $y \geq 1$ then $y^k \geq y$ (induction: $y^{k+1} = y^k y$, and Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (c) or equality); and if $0 \leq x \leq x'$ and $0 \leq y \leq y'$, then $xy \leq x'y \leq x'y'$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (c) twice, or equality).

(a) By Lemma 1.1.4 in the commutative ring $\mathbb{R}$,

$$t^n - s^n = (t - s) \sum_{k=0}^{n-1} t^k s^{n-1-k}.$$

Every term of the sum is ≥ 0 , and the term with $k = n - 1$ is $t^{n-1} > 0$, since $t > s \geq 0$. So the sum is $\geq t^{n-1} > 0$. Also $t - s > 0$. Hence $t^n - s^n > 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (c)).

(b) *Uniqueness.* If $b, c \geq 0$ and $b \neq c$, say $b < c$, then $b^n < c^n$ by (a); so at most one non-negative b has $b^n = a$.

Existence. If $a = 0$, then $b := 0$ works, since $0^n = 0^{n-1} \cdot 0 = 0$. Let $a > 0$, and let

$$S := \{y \in \mathbb{R} : y \geq 0 \text{ and } y^n \leq a\}.$$

Put $m := \min\{1, a\} > 0$. Since $0 < m \leq 1$, $m^n \leq m \leq a$, so $m \in S$. Put $M := \max\{1, a\}$. If $y > M$, then $y > 1$, so $y^n \geq y > M \geq a$ and $y \notin S$; hence M is an upper bound of S . Since $\mathbb{R}$ is a complete ordered field (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Theorem 5.6.3, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Definition 5.6.1), S has a supremum; let $s := \sup S$. Then $s \geq m > 0$.

Case $s^n < a$. Let

$$h := \min\left\{1, \frac{a - s^n}{2n(s + 1)^{n-1}}\right\}.$$

It depends only on a , n and s , and $h > 0$, since $a - s^n > 0$ and $2n(s + 1)^{n-1} > 0$. By Lemma 1.1.4,

$$(s + h)^n - s^n = h \sum_{k=0}^{n-1} (s + h)^k s^{n-1-k}.$$

Since $0 \leq s < s + h \leq s + 1$, each term satisfies $(s + h)^k s^{n-1-k} \leq (s + 1)^k (s + 1)^{n-1-k} = (s + 1)^{n-1}$, by (a) (or equality), the third fact, and [Proposition 1.1.3](#) (a). A sum of n terms, each at most $(s + 1)^{n-1}$, is at most $n(s + 1)^{n-1}$. Hence

$$(s + h)^n \leq s^n + h \cdot n(s + 1)^{n-1} \leq s^n + \frac{a - s^n}{2} < a.$$

So $s + h \in S$, and $s + h > s$, against s being an upper bound of S .

Case $s^n > a$. Let

$$h := \frac{s^n - a}{ns^{n-1}},$$

which depends only on a , n and s , and is positive. Since $a > 0$, we have $s^n - a < s^n \leq ns^n$, so $h < s^n/(ns^{n-1}) = s/n \leq s$; thus $0 < s - h < s$. By [Lemma 1.1.4](#) and the same bound, with $0 < s - h < s$, each of the n terms of $\sum_{k=0}^{n-1} s^k (s - h)^{n-1-k}$ is at most s^{n-1} , so

$$s^n - (s - h)^n \leq h \cdot ns^{n-1} = s^n - a,$$

that is, $(s - h)^n \geq a$. Now let $y \in S$. If $y > s - h$, then (a) gives $y^n > (s - h)^n \geq a$, against $y \in S$. So $y \leq s - h$, and $s - h$ is an upper bound of S smaller than s , against s being the **least** upper bound.

Both cases are impossible, so $s^n = a$ by trichotomy, and $b := s \geq 0$ works.

For $n = 2$, the number $\sqrt[n]{a}$ is non-negative and squares to a , so it is $\sqrt{a}$, by the uniqueness in Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, [Proposition 6.1.4](#).

■

The constants were found backwards in the Idea and placed first in the proof, and each depends on a , n and s only. Completeness was used once, to produce s . For $a > 0$ the root is positive, since $0^n = 0 \neq a$. For instance $\sqrt[3]{8} = 2$ and $\sqrt[4]{4} = \sqrt{2}$, since $2^3 = 8$ and $(\sqrt{2})^4 = ((\sqrt{2})^2)^2 = 4$, and both are non-negative. The symbol $\sqrt[n]{a}$ is used only for **non-negative real** a ; the next theorem shows why it could not mean “the” n -th root of a complex number.

1.6.2 Solving the equation z to the n equals c

Now the main result. Every non-zero complex number has exactly n different n -th roots, and polar form lists them.

Theorem 1.6.2. n -th Roots of a Complex Number

Let $n \in \mathbb{N}$ with $n \geq 1$, and let $c \in \mathbb{C}$ with $c \neq 0$. Let $c = \rho e^{i\alpha}$ be a polar form of c ([Proposition 1.5.4](#)), and for $k \in \mathbb{Z}$ put

$$z_k := \sqrt[n]{\rho} e^{i(\alpha+2\pi k)/n}.$$

- (a) For $z \in \mathbb{C}$: $z^n = c$ if and only if $z = z_k$ for some $k \in \mathbb{Z}$.
- (b) For $k, l \in \mathbb{Z}$: $z_k = z_l$ if and only if $n \mid k - l$ (Sets and Functions, Definition 1.1.2).
- (c) The map $\{0, 1, \dots, n-1\} \rightarrow \{z \in \mathbb{C} : z^n = c\}$, $k \mapsto z_k$, is a bijection. So c has exactly n n -th roots (Sets and Functions, Definition 2.5.2).

In particular every non-zero complex number has an n -th root, and every $u \in \mathbb{T}$ has one in

$\mathbb{T}$.

Idea. Write the unknown in polar form, $z = re^{i\theta}$. De Moivre turns $z^n = c$ into $r^n e^{in\theta} = \rho e^{i\alpha}$, and the uniqueness half of polar form splits that into a real equation for the length, $r^n = \rho$, and an equation for the angle, $n\theta \in \alpha + 2\pi\mathbb{Z}$. The first has one solution, $r = \sqrt[n]{\rho}$. The second has the solutions $\theta = (\alpha + 2\pi k)/n$, one for each integer k . Different k can give the same point, and they do exactly when the angles differ by a whole number of turns, that is, when $n \mid k - l$. So the k that matter are the remainders $0, \dots, n - 1$.

Before reading on: where is the uniqueness half of the polar form used, and where the uniqueness of the real n -th root?

Proof. Here $\rho = |c| > 0$ by Proposition 1.5.4 (a), so $\sqrt[n]{\rho} > 0$ exists by Lemma 1.6.1 (b).

- (a) Let $z \in \mathbb{C}$. If $z = 0$, then $z^n = 0^{n-1} \cdot 0 = 0 \neq c$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.3.2 (b)), and z is no z_k , since every z_k has modulus $\sqrt[n]{\rho} > 0$. So let $z \neq 0$, and fix a polar form $z = re^{i\theta}$ (Proposition 1.5.4 (a)). By Theorem 1.5.5, $z^n = r^n e^{in\theta}$, a polar form with $r^n > 0$. By Proposition 1.5.4 (b),

$$z^n = c \iff r^n = \rho \text{ and } n\theta - \alpha \in 2\pi\mathbb{Z}.$$

Since $r > 0$, the uniqueness in Lemma 1.6.1 (b) gives $r^n = \rho \iff r = \sqrt[n]{\rho}$. And $n\theta - \alpha = 2\pi k$ holds for a given $k \in \mathbb{Z}$ exactly when $\theta = (\alpha + 2\pi k)/n$.

($\Rightarrow$) If $z^n = c$, then $r = \sqrt[n]{\rho}$ and $\theta = (\alpha + 2\pi k)/n$ for some $k \in \mathbb{Z}$, so $z = z_k$.

($\Leftarrow$) If $z = z_k$, use the polar form $r := \sqrt[n]{\rho}$, $\theta := (\alpha + 2\pi k)/n$ of z in the equivalence above. Both conditions on the right hold, so $z^n = c$.

- (b) The numbers z_k and z_l are given in polar form with the same modulus. By Proposition 1.5.4 (b), $z_k = z_l$ if and only if

$$\frac{\alpha + 2\pi k}{n} - \frac{\alpha + 2\pi l}{n} = \frac{2\pi(k - l)}{n} \in 2\pi\mathbb{Z},$$

that is, if and only if $2\pi(k - l)/n = 2\pi m$ for some $m \in \mathbb{Z}$. Multiplying by $n/(2\pi)$, and back, this says $k - l = mn$, an equation between integers. So $z_k = z_l$ if and only if $n \mid k - l$.

- (c) By (a), each z_k is a solution, so the map is into the set of solutions. *Injective:* let $0 \leq l < k \leq n - 1$. Then $0 < k - l < n$. If $z_k = z_l$, then $n \mid k - l$ by (b), and since $n > 0$ and $k - l > 0$, Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 3.1.1 (e) gives $n \leq k - l$, a contradiction. So $z_k \neq z_l$. *Surjective:* let $z^n = c$. By (a), $z = z_k$ for some $k \in \mathbb{Z}$. Division with remainder (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.1.2 (a)) gives $k = qn + j$ with $q \in \mathbb{Z}$ and $0 \leq j \leq n - 1$. Then $n \mid k - j$, so $z = z_k = z_j$ by (b). Hence the map is a bijection. Composing it with the bijection $\{1, \dots, n\} \rightarrow \{0, \dots, n - 1\}$, $j \mapsto j - 1$, shows that the set of solutions has n elements (Sets and Functions, Definition 2.5.2).

Finally, z_0 is an n -th root of c . If $|c| = 1$, then $\rho = 1$ and $\sqrt[n]{1} = 1$, since $1 \geq 0$ and $1^n = 1$; so every z_k has modulus 1 and lies in $\mathbb{T}$. ■

The answer to the prompt: the uniqueness half of the polar form, [Proposition 1.5.4](#) (b), turns the one complex equation $z^n = c$ into the two real conditions, and is used again in (b) to decide when two of the z_k coincide. The uniqueness of the real root forces the modulus, $r = \sqrt[n]{\rho}$. The ambiguity $2\pi\mathbb{Z}$ in the angle is what produces n roots instead of one.

Warning. Dividing the angle equation by n too early loses roots. From $z^3 = 1$, $z = e^{i\theta}$, one might write $e^{3i\theta} = e^{i0}$, “so $3\theta = 0$ and $z = 1$ ”. But $e^{3i\theta} = e^{i0}$ only gives $3\theta \in 2\pi\mathbb{Z}$ ([Proposition 1.5.4](#) (b)), and the angles $2\pi/3$ and $4\pi/3$ give two more cube roots of 1. Only the remainders $0, \dots, n-1$ of k matter, but all of them do.

1.6.3 Roots of unity

The most important case is $c = 1$.

Example. Roots of Unity

Let $n \geq 1$ be an integer. Find all $z \in \mathbb{C}$ with $z^n = 1$, and draw them for $n = 6$.

Solution. Apply [Theorem 1.6.2](#) with $c = 1 = 1 \cdot e^{i0}$ ([Theorem 1.5.3](#) (b)): $\rho = 1$, $\alpha = 0$, and $\sqrt[n]{1} = 1$. The solutions are

$$z_k = e^{2\pi i k/n}, \quad k \in \mathbb{Z}.$$

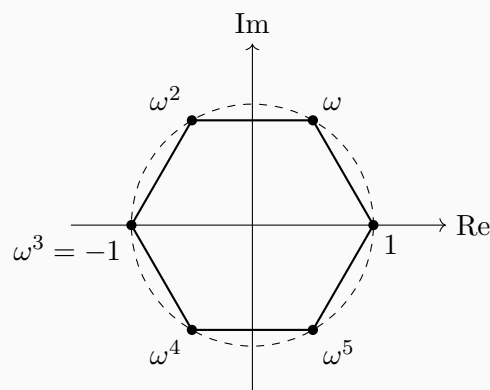
Put $\omega := e^{2\pi i/n}$. By [Theorem 1.5.5](#), $z_k = (e^{2\pi i/n})^k = \omega^k$ for $k \in \mathbb{N}$. By [Theorem 1.6.2](#) (c), there are exactly n solutions,

$$1, \omega, \omega^2, \dots, \omega^{n-1},$$

the **n -th roots of unity**. They lie on $\mathbb{T}$, at the arguments $2\pi k/n$, equally spaced around the circle: multiplying by ω turns each one into the next ([Theorem 1.5.3](#) (a)), and ω^{n-1} back into $\omega^n = z_n = z_0 = 1$ ([Theorem 1.6.2](#) (b)). For $n \geq 3$ they are the corners of a regular polygon with n corners, one of them at 1; for $n = 2$ they are 1 and $\omega = e^{i\pi} = -1$ ([Example \(Special Angles\)](#) (i)); for $n = 1$ only 1.

For $n = 6$, $\omega = e^{i\pi/3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ ([Example \(Special Angles\)](#) (iii)), and $\omega^3 = e^{i\pi} = -1$. Hence $\omega^2 = (\frac{1}{2} + \frac{\sqrt{3}}{2}i)^2 = \frac{1}{4} - \frac{3}{4} + \frac{\sqrt{3}}{2}i = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\omega^4 = -\omega$ and $\omega^5 = -\omega^2$. The six roots are

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



The six roots sum to 0: since $\omega^3 = -1$, we have $\omega^{k+3} = -\omega^k$, so the roots cancel in the

opposite pairs $\{1, \omega^3\}$, $\{\omega, \omega^4\}$, $\{\omega^2, \omega^5\}$. In the picture, the hexagon is symmetric about its center 0. In general the sum is [Proposition 1.6.3](#) below.

We write $\mu_n := \{z \in \mathbb{C} : z^n = 1\} = \{1, \omega, \dots, \omega^{n-1}\}$ for the set of n -th roots of unity. It is a subset of $\mathbb{T}$, since each element is some $z_k = e^{2\pi i k/n}$ ([Theorem 1.6.2](#) (a)). It contains 1, and it is closed under products, since $(\zeta\eta)^n = \zeta^n\eta^n = 1$ for $\zeta, \eta \in \mu_n$ ([Proposition 1.1.3](#) (c)). It is closed under inverses, since $\zeta \cdot \zeta^{n-1} = \zeta^n = 1$ gives $\zeta^{-1} = \zeta^{n-1}$, a product of elements of μ_n (for $n = 1$, $\zeta^0 = 1$). *Algebraic Preliminaries*, Chapter 2 treats μ_n , like $\mathbb{T}$, as an example of a group.

The roots of unity also describe the roots of any $c \neq 0$: the root $z_0 = \sqrt[n]{\rho} e^{i\alpha/n}$ of [Theorem 1.6.2](#) satisfies $z_k = z_0 \omega^k$ for $k \in \mathbb{N}$, by [Theorem 1.5.3](#) (a) and [Theorem 1.5.5](#), since $(\alpha + 2\pi k)/n = \alpha/n + 2\pi k/n$. So by [Theorem 1.6.2](#) (c) the n -th roots of c are $z_0, z_0\omega, \dots, z_0\omega^{n-1}$: one of them times the n -th roots of unity.

The six roots canceled in pairs. The same pairing works for every even n , since $\omega^{n/2} = e^{i\pi} = -1$ ([Theorem 1.5.5](#), [Example \(Special Angles\)](#) (i)) gives $\omega^{k+n/2} = -\omega^k$; but for odd n there are no opposite pairs: if ζ and $-\zeta$ were both n -th roots of unity, then $1 = (-\zeta)^n = (-1)^n \zeta^n = -1$. A different argument is needed. It is [Lemma 1.1.4](#) once more.

Proposition 1.6.3. Sums of Roots of Unity

Let $n \in \mathbb{N}$ with $n \geq 2$, and let $\omega := e^{2\pi i/n}$.

(a) For $m \in \mathbb{N}$: $\omega^m = 1$ if and only if $n \mid m$. In particular $\omega \neq 1$.

(b) $\sum_{k=0}^{n-1} \omega^k = 0$.

(c) For $m \in \mathbb{N}$,

$$\sum_{k=0}^{n-1} \omega^{mk} = \begin{cases} n & \text{if } n \mid m, \\ 0 & \text{otherwise.} \end{cases}$$

Idea. Put $\zeta := \omega^m$. The sum in (c) is $1 + \zeta + \dots + \zeta^{n-1}$, and [Lemma 1.1.4](#) multiplies it by $\zeta - 1$ to give $\zeta^n - 1 = 0$. If $\zeta \neq 1$ we may cancel, and the sum is 0; if $\zeta = 1$ it is n . Part (a) decides which case occurs.

Proof. We use the notation of [Example \(Roots of Unity\)](#): $z_k = e^{2\pi i k/n}$ are the roots of $c = 1$ in [Theorem 1.6.2](#), and $\omega^m = z_m$ for $m \in \mathbb{N}$ ([Theorem 1.5.5](#)).

(a) Since $1 = z_0$, [Theorem 1.6.2](#) (b) gives $\omega^m = 1 \iff z_m = z_0 \iff n \mid m$. For $m = 1$: if $n \mid 1$, then $n \leq 1$ by Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, [Proposition 3.1.1](#) (e), against $n \geq 2$. So $\omega \neq 1$.

(b) Let $\zeta := \omega^m$. By [Proposition 1.1.3](#) (b), $\omega^{mk} = \zeta^k$ for each k , and $\zeta^n = \omega^{mn} = (\omega^n)^m = 1^m = 1$, since $\omega^n = z_n = z_0 = 1$ by [Theorem 1.6.2](#) (b).

Case $n \mid m$. Then $\zeta = 1$ by (a), and the sum is $\sum_{k=0}^{n-1} 1 = n$.

Case $n \nmid m$. Then $\zeta \neq 1$ by (a). By Lemma 1.1.4 with $w = 1$,

$$0 = \zeta^n - 1 = (\zeta - 1) \sum_{k=0}^{n-1} \zeta^k.$$

Since $\zeta - 1 \neq 0$ and $\mathbb{C}$ has no zero divisors (Theorem 1.2.4, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Lemma 4.1.1 (d)), the sum is 0.

(b) This is (c) with $m = 1$, since $n \nmid 1$ by (a). ■

Comparing real and imaginary parts in (b), with $\omega^k = \cos(2\pi k/n) + i \sin(2\pi k/n)$ (Theorem 1.5.5), gives two real identities that are awkward to prove any other way: for $n \geq 2$,

$$\sum_{k=0}^{n-1} \cos \frac{2\pi k}{n} = 0 \quad \text{and} \quad \sum_{k=0}^{n-1} \sin \frac{2\pi k}{n} = 0.$$

Part (c) says more: the sum of the m -th powers of the roots of unity detects whether n divides m .

Quick check. Write the three cube roots of unity in the form $a + bi$.

Solution. By Example (Roots of Unity) with $n = 3$, they are $1, \omega, \omega^2$ with $\omega = e^{2\pi i/3} = (e^{i\pi/3})^2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ (Theorem 1.5.5, and the square computed for $n = 6$ above). Since $\omega \in \mathbb{T}$ and $\omega \cdot \omega^2 = \omega^3 = 1$, $\omega^2 = \omega^{-1} = \bar{\omega} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ (Proposition 1.5.1 (a)). So the cube roots of unity are 1 and $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Without angles: $z^3 - 1 = (z - 1)(z^2 + z + 1)$, and Corollary 1.4.2 applied to $z^2 + z + 1 = 0$, with $d = \sqrt{3}i$ a square root of $1 - 4 = -3$, gives $z = (-1 \pm \sqrt{3}i)/2$.

1.6.4 Polynomial equations, and a look ahead

An n -th root of c solves $z^n - c = 0$, a polynomial equation of degree n with only two non-zero coefficients. The general question is whether every equation

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0, \quad a_0, \dots, a_n \in \mathbb{C}, \quad a_n \neq 0, \quad n \geq 1,$$

has a solution in $\mathbb{C}$. Here the left side is a **polynomial expression** $\sum_{k=0}^n a_k z^k$, a finite sum; *Algebraic Preliminaries*, Chapter 3 makes polynomials objects in their own right. We built $\mathbb{C}$ so that one such equation, $z^2 + 1 = 0$, has a solution, and Section 1.4 solved every equation of degree 2. It turns out that nothing more ever needs to be added.

Remark (Looking ahead). *Algebraic Preliminaries*, Section 4.6 proves that every such equation has a solution in $\mathbb{C}$: the Fundamental Theorem of Algebra. Its proof uses only the square roots of Section 1.4 and the completeness of $\mathbb{R}$, not polar form and not the borrowed facts about cosine and sine. With division of polynomials, *Algebraic Preliminaries*, Chapter 4 deduces that every complex polynomial of degree $n \geq 1$ is a non-zero constant times a product of n factors of the form $z - z_j$. Nothing in this chapter or in *Algebraic Preliminaries*,

Chapters 1–3 uses the theorem.

One companion fact needs no heavy machinery: when the coefficients are real, the solutions that are not real come in conjugate pairs.

Proposition 1.6.4. Real Coefficients and Conjugate Roots

Let $n \in \mathbb{N}$, let $a_0, \dots, a_n \in \mathbb{R}$, and let $z \in \mathbb{C}$. Then

$$\overline{\sum_{k=0}^n a_k z^k} = \sum_{k=0}^n a_k \bar{z}^k.$$

Hence, if $\sum_{k=0}^n a_k z_0^k = 0$ for some $z_0 \in \mathbb{C}$, then also $\sum_{k=0}^n a_k \bar{z}_0^k = 0$.

Proof. First, $\overline{z^k} = \bar{z}^k$ for every $k \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 on k : $\bar{z^0} = \bar{1} = 1 = \bar{z}^0$, since 1 is real (Proposition 1.2.1); and if $\overline{z^k} = \bar{z}^k$, then $\overline{z^{k+1}} = \overline{z^k z} = \overline{z^k} \bar{z} = \bar{z}^k \bar{z} = \bar{z}^{k+1}$, by Theorem 1.2.2 (b). Next, $\overline{a_k} = a_k$ since a_k is real (Proposition 1.2.1), so $\overline{a_k z^k} = a_k \bar{z}^k$, again by Theorem 1.2.2 (b). Finally, the conjugate of a finite sum is the sum of the conjugates, by induction on the number of terms along the recursion for finite sums, with Theorem 1.2.2 (a) in the step. This proves the identity. If $\sum a_k z_0^k = 0$, then $\sum a_k \bar{z}_0^k = \bar{0} = 0$. ■

A solution z_0 that is not real gives a **second** solution: $\bar{z}_0 \neq z_0$, since $z_0 = x + yi$ with $y \neq 0$ has $\bar{z}_0 = x - yi$, and $-y \neq y$. For example, $z^2 - 2z + 5 = 0$ has the solution $1 + 2i$, since $(1 + 2i)^2 - 2(1 + 2i) + 5 = (-3 + 4i) - (2 + 4i) + 5 = 0$; so it also has the solution $1 - 2i$. *Algebraic Preliminaries*, Chapter 4 uses this to factor real polynomials into real factors of degree 1 and 2.

1.6.5 Exercises

1.6.5.1 A. Check your understanding

Exercise. A1

- Find all $z \in \mathbb{C}$ with $z^4 = 1$.
- In the proof of Theorem 1.6.2, where is the uniqueness half of Proposition 1.5.4 used?
- In the same proof, why is the modulus r of a solution forced to be $\sqrt[n]{\rho}$?
- True or false: $z^3 = 1$ has exactly three solutions in $\mathbb{C}$, and exactly one of them is real. Justify your answer.
- State the idea of the proof of Theorem 1.6.2 in two sentences.

Solution.

- By Example (Roots of Unity) with $n = 4$, the solutions are ω^k for $k = 0, 1, 2, 3$, where $\omega = e^{2\pi i/4} = e^{i\pi/2} = i$ (Example (Special Angles) (ii)): $1, i, -1, -i$.
- Twice. In (a), to turn $r^n e^{in\theta} = \rho e^{i\alpha}$ into the two conditions $r^n = \rho$ and $n\theta - \alpha \in 2\pi\mathbb{Z}$. In (b), to decide when $z_k = z_l$.

- (c) Because $r > 0$ and $r^n = \rho$, and [Lemma 1.6.1](#) (b) says that $\sqrt[n]{\rho}$ is the **only** non-negative real number with n -th power ρ .
- (d) True. By [Theorem 1.6.2](#) (c) there are exactly three. By the Check above they are 1 and $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$; the last two have imaginary part $\pm \frac{\sqrt{3}}{2} \neq 0$, so only 1 is real.
- (e) Polar form and De Moivre split $z^n = c$ into a real equation for the modulus, which has exactly one positive solution, and an equation for the argument, which is solved up to the ambiguity $2\pi\mathbb{Z}$. That ambiguity, divided by n , produces n different roots, one for each remainder modulo n .

1.6.5.2 B. Practice

Exercise. B1

Find all $z \in \mathbb{C}$ with $z^3 = -8i$, in the form $a + bi$.

Solution. By [Example \(Special Angles\)](#) (ii) and [Theorem 1.5.3](#) (b), $e^{-i\pi/2} = \overline{e^{i\pi/2}} = \bar{i} = -i$, so $-8i = 8e^{-i\pi/2}$ is a polar form, with $\rho = 8$ and $\alpha = -\pi/2$. Also $\sqrt[3]{8} = 2$. By [Theorem 1.6.2](#), the solutions are $z_k = 2e^{i(-\pi/2+2\pi k)/3} = 2e^{i(-\pi/6+2\pi k/3)}$ for $k = 0, 1, 2$, with arguments $-\pi/6$, $\pi/2$ and $7\pi/6$:

$$\begin{aligned} z_0 &= 2e^{-i\pi/6} = 2\overline{e^{i\pi/6}} = \sqrt{3} - i, & z_1 &= 2e^{i\pi/2} = 2i, \\ z_2 &= 2e^{i\pi} e^{i\pi/6} = -2\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) = -\sqrt{3} - i, \end{aligned}$$

by [Example \(Special Angles\)](#) (i), (ii), (iv) and [Theorem 1.5.3](#). Check: $(2i)^3 = 8i^3 = -8i$, and $(\sqrt{3} - i)^2 = 2 - 2\sqrt{3}i$, so $(\sqrt{3} - i)^3 = (2 - 2\sqrt{3}i)(\sqrt{3} - i) = 2\sqrt{3} - 2i - 6i - 2\sqrt{3} = -8i$.

Exercise. B2

Find all $z \in \mathbb{C}$ with $z^4 = -4$, in the form $a + bi$, and check one of them directly.

Solution. A polar form is $-4 = 4e^{i\pi}$ ([Example \(Special Angles\)](#) (i)), and $\sqrt[4]{4} = \sqrt{2}$, since $\sqrt{2} \geq 0$ and $(\sqrt{2})^4 = 4$. By [Theorem 1.6.2](#), the solutions are $z_k = \sqrt{2}e^{i(\pi+2\pi k)/4}$ for $k = 0, 1, 2, 3$. First, $z_0 = \sqrt{2}e^{i\pi/4} = 1 + i$ ([Example \(Special Angles\)](#) (v)). Next, $(\pi + 2\pi(k+1))/4 = (\pi + 2\pi k)/4 + \pi/2$, so $z_{k+1} = z_k e^{i\pi/2} = iz_k$ ([Theorem 1.5.3](#) (a), [Example \(Special Angles\)](#) (ii)). Hence

$$z_0 = 1 + i, \quad z_1 = -1 + i, \quad z_2 = -1 - i, \quad z_3 = 1 - i,$$

that is, $z = \pm 1 \pm i$ with all four choices of signs. Check: $(1+i)^2 = 2i$, so $(1+i)^4 = (2i)^2 = -4$.

Exercise. B3

Let $n \geq 1$ and $\omega := e^{2\pi i/n}$. Show that $1 \in \mu_n$, that μ_n is closed under multiplication, that for $k = 1, \dots, n-1$ the inverse of ω^k is ω^{n-k} , and that $\mu_n \subseteq \mathbb{T}$.

Solution. $1^n = 1$, so $1 \in \mu_n$. If $\zeta^n = \eta^n = 1$, then $(\zeta\eta)^n = \zeta^n\eta^n = 1$ by Proposition 1.1.3 (c). For $1 \leq k \leq n-1$, $\omega^k\omega^{n-k} = \omega^n = 1$ by Proposition 1.1.3 (a) and Proposition 1.6.3 (a) (or Example (Roots of Unity)), so ω^{n-k} is the inverse of ω^k , and it lies in μ_n . Finally let $\zeta \in \mu_n$. Then $|\zeta|^n = |\zeta^n| = |1| = 1$, where the first equality is Theorem 1.2.2 (d) applied n times (induction on n). Since $|\zeta| \geq 0$ and also $1 \geq 0$ with $1^n = 1$, the uniqueness in Lemma 1.6.1 (b) gives $|\zeta| = 1$. So $\zeta \in \mathbb{T}$. (This last argument uses no borrowed fact.)

1.6.5.3 C. Going deeper

Exercise. C1: Exit check: n-th roots

Let $n \geq 1$ and $c \in \mathbb{C}$ with $c \neq 0$, and let $c = \rho e^{i\alpha}$ be a polar form. Prove parts (a) and (b) of Theorem 1.6.2: the solutions of $z^n = c$ are exactly the numbers $z_k = \sqrt[n]{\rho} e^{i(\alpha+2\pi k)/n}$, $k \in \mathbb{Z}$, and $z_k = z_l$ if and only if $n \mid k-l$. Cite the polar form, De Moivre's formula and the real n -th root where you use them.

Solution. Here $\rho = |c| > 0$ (Proposition 1.5.4 (a)). The number 0 is not a solution, since $0^n = 0 \neq c$, and is no z_k , since $|z_k| = \sqrt[n]{\rho} > 0$ (Lemma 1.6.1 (b)). For $z \neq 0$, fix a polar form $z = r e^{i\theta}$ with $r > 0$ (Proposition 1.5.4 (a)); then $z^n = r^n e^{in\theta}$ (Theorem 1.5.5), a polar form with $r^n > 0$, and by the uniqueness of polar form (Proposition 1.5.4 (b)), $z^n = \rho e^{i\alpha}$ if and only if $r^n = \rho$ and $n\theta - \alpha \in 2\pi\mathbb{Z}$. The first condition is $r = \sqrt[n]{\rho}$, by existence and uniqueness of the real n -th root (Lemma 1.6.1 (b)); the second is $\theta = (\alpha + 2\pi k)/n$ for some $k \in \mathbb{Z}$. So $z^n = c$ implies $z = z_k$; conversely, applied to the polar form $r := \sqrt[n]{\rho}$, $\theta := (\alpha + 2\pi k)/n$ of $z = z_k$, the equivalence gives $z^n = c$. For (b), z_k and z_l are given in polar form with the same modulus, so the same uniqueness gives $z_k = z_l$ if and only if $2\pi(k-l)/n \in 2\pi\mathbb{Z}$, if and only if $k-l = mn$ for some $m \in \mathbb{Z}$, that is, $n \mid k-l$.

Marking scheme. (10 points) - 1: rules out $z = 0$, with the reason $0^n = 0 \neq c$. - 2: writes z (and c) in polar form and applies De Moivre's formula to get $z^n = r^n e^{in\theta}$. - 3: splits $z^n = c$ into $r^n = \rho$ and $n\theta - \alpha \in 2\pi\mathbb{Z}$, citing the uniqueness of polar form, and states both directions (every z_k is a solution, every solution is some z_k). - 1: $r = \sqrt[n]{\rho}$, with both existence and uniqueness of the real n -th root cited (the point is lost if either is assumed without citation). - 3: (b), $z_k = z_l \iff n \mid k-l$, both directions. Fatal errors (0 for the step): concluding $n\theta = \alpha$, or $\theta = \alpha/n$, from $e^{in\theta} = e^{i\alpha}$ (dropping $2\pi\mathbb{Z}$); writing $\sqrt[n]{c}$ for a complex c . Second route: find one root z_0 and show that $z^n = c$ if and only if $(z/z_0)^n = 1$, then solve $w^n = 1$ by polar form. The same points apply, with the 3 points of the third line awarded for the roots of unity, and (b) replaced by the distinctness of $1, \omega, \dots, \omega^{n-1}$ and the periodicity $\omega^{k+n} = \omega^k$.

Exercise. C2: Find the error

Here is an argument.

Claim. For $n \geq 2$, the n -th roots of unity sum to 0.

- (1) Let $\omega := e^{2\pi i/n}$ and $S := 1 + \omega + \dots + \omega^{n-1}$. (2) Then $\omega S = \omega + \omega^2 + \dots + \omega^n = S$, since $\omega^n = 1$. (3) So $(\omega - 1)S = 0$. (4) Since ω is an n -th root of unity, $\omega^n = 1$, so $\omega \neq 1$. (5) Hence $\omega - 1 \neq 0$, and $S = 0$.

Is the claim true? Does the argument prove it? If not, name the first line that fails, say what is wrong with it, give a counterexample to the step, and repair the argument.

Solution. The claim is true: it is [Proposition 1.6.3](#) (b).

The argument does not prove it. Lines (1)–(3) are correct: $\omega^n = 1$ by [Example \(Roots of Unity\)](#), and (3) is (2) rearranged. Line (5) is correct **given** (4), since $\mathbb{C}$ has no zero divisors. Line (4) fails. “ $\omega^n = 1$, so $\omega \neq 1$ ” cites a general “fact”, that an n -th root of unity is not 1, which is false: this is the error (N9) of Logic and Proof, Example (What is not allowed). *Counterexample to the step:* 1 itself satisfies $1^n = 1$, and $1 = 1$. Being an n -th root of unity gives no information that separates ω from 1; the information is in the particular choice $\omega = e^{2\pi i/n}$ with $n \geq 2$.

Repair. If $\omega = e^{2\pi i/n} = 1 = e^{i0}$, then $2\pi/n \in 2\pi\mathbb{Z}$ by [Proposition 1.5.4](#) (b), so $1/n = m$ for some $m \in \mathbb{Z}$, that is, $1 = mn$ and $n \mid 1$. Since $n \geq 2 > 0$, *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Proposition 3.1.1 (e) gives $n \leq 1$, a contradiction. So $\omega \neq 1$, and lines (5) and the conclusion stand. (This repair uses (T1)–(T3) of [Axiom 1.5.2](#), through [Proposition 1.5.4](#) (b), and no value of the cosine.)

1.6.5.4 R. Review

Exercise. R1

Let $\sigma: \mathbb{C} \rightarrow \mathbb{C}$ satisfy $\sigma(z + w) = \sigma(z) + \sigma(w)$ and $\sigma(zw) = \sigma(z)\sigma(w)$ for all $z, w \in \mathbb{C}$, $\sigma(1) = 1$, and $\sigma(a) \in \mathbb{R}$ for every $a \in \mathbb{R}$.

- Prove that either $\sigma(z) = z$ for every $z \in \mathbb{C}$, or $\sigma(z) = \bar{z}$ for every $z \in \mathbb{C}$.
- Show that conjugation $z \mapsto \bar{z}$ satisfies all the hypotheses on σ .

Solution.

- Since σ maps $\mathbb{R}$ into $\mathbb{R}$, it restricts to a map $\tau: \mathbb{R} \rightarrow \mathbb{R}$, $\tau(a) := \sigma(a)$, which preserves sums and products and sends 1 to 1. Since $\mathbb{R}$ is a complete ordered field (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Theorem 5.6.3), *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Theorem 6.3.4 gives $\tau = \text{id}_{\mathbb{R}}$: $\sigma(a) = a$ for every real a . In particular $\sigma(-1) = -1$, so

$$\sigma(i)^2 = \sigma(i \cdot i) = \sigma(-1) = -1 = i^2.$$

So $(\sigma(i) - i)(\sigma(i) + i) = 0$, and $\sigma(i) = i$ or $\sigma(i) = -i$ (no zero divisors in $\mathbb{C}$; or [Proposition 1.4.1](#) (b)). For $z = a + bi$ with $a, b \in \mathbb{R}$,

$$\sigma(z) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i).$$

If $\sigma(i) = i$, then $\sigma(z) = z$ for every z ; if $\sigma(i) = -i$, then $\sigma(z) = a - bi = \bar{z}$ for every z .

- Conjugation preserves sums and products by [Theorem 1.2.2](#) (a), (b), and $\bar{\bar{a}} = a$ for every real a ([Proposition 1.2.1](#)), so in particular $\bar{1} = 1$ and real numbers go to real numbers.

The comparison with *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 6 (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Theorem 6.3.4) is the point: $\mathbb{R}$ has only the identity, while $\mathbb{C}$ has

exactly two such maps. In $\mathbb{R}$ the order can be read off from the field operations (the non-negative numbers are exactly the squares, Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 6.1.4), and a map preserving $+$ and $\cdot$ must preserve it. In $\mathbb{C}$ there is no order (Proposition 1.4.3), and nothing written with $+$, $\cdot$ and real numbers alone tells i from $-i$.

Exercise. R2

Let $n \geq 1$. Show that $[k] \mapsto e^{2\pi i k/n}$ is a well-defined bijection $f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mu_n$, and that $f([k] + [l]) = f([k]) f([l])$ for all $k, l \in \mathbb{Z}$.

Solution. Write $z_k := e^{2\pi i k/n}$, the roots of $c = 1$ in Theorem 1.6.2 (with $\rho = 1$, $\alpha = 0$, as in Example (Roots of Unity)). The classes of Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Definition 3.4.2 are congruence classes: $[k] = [l]$ if and only if $n \mid k - l$. By Theorem 1.6.2 (b), $n \mid k - l$ if and only if $z_k = z_l$. Reading this equivalence from left to right, $f([k]) := z_k$ does not depend on the representative k of the class, so f is well defined; reading it from right to left, f is injective. Each z_k lies in μ_n by Theorem 1.6.2 (a), and every element of μ_n is some z_k , again by (a); so f is surjective. Finally, $[k] + [l] = [k + l]$, and by Theorem 1.5.3 (a),

$$f([k] + [l]) = z_{k+l} = e^{2\pi i k/n} e^{2\pi i l/n} = f([k]) f([l]).$$

As a check on the count, both sets have n elements (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.4.3 (b) and Theorem 1.6.2 (c)). In the language of *Algebraic Preliminaries*, Chapter 2, f is an isomorphism from the additive structure of $\mathbb{Z}/n\mathbb{Z}$ to the multiplicative structure of μ_n .

Exercise. R3

Let F be an ordered field and $x, y \in F$.

- Prove that $|x + y| \leq |x| + |y|$ by comparing the squares of the two sides.
- The proof of the same inequality by “trapping” x between $-|x|$ and $|x|$, and adding the traps for x and y , works in every ordered field. Which step of it cannot be carried out for complex x, y , and what replaces it in the complex triangle inequality?

Solution.

- Both sides are non-negative. By Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 4.1.3 (b), $|x|^2 = x^2$, $|y|^2 = y^2$, $|x + y|^2 = (x + y)^2$ and $|x||y| = |xy|$. Hence

$$(|x| + |y|)^2 - |x + y|^2 = |x|^2 + 2|x||y| + |y|^2 - x^2 - 2xy - y^2 = 2(|xy| - xy) \geq 0,$$

since $xy \leq |xy|$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 4.1.3 (c)). So $|x + y|^2 \leq (|x| + |y|)^2$. If $|x + y| > |x| + |y|$, then Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.3.5 (g), applied to these non-negative elements, would give $|x + y|^2 > (|x| + |y|)^2$; so $|x + y| \leq |x| + |y|$.

- The trapping proof (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 4.1.3 (e), proved from (c)) uses $-|x| \leq x \leq |x|$: it compares x itself with real numbers. For

a complex x that is not real such a comparison means nothing, since no order on $\mathbb{C}$ is compatible with its arithmetic (Proposition 1.4.3). The squaring proof of (a) is the one that survives: in the complex triangle inequality (Theorem 1.3.2) the cross term $2 \operatorname{Re}(z\bar{w})$ is bounded by a comparison between **real** numbers, $\operatorname{Re} u \leq |u|$ (Lemma 1.3.1), which replaces $xy \leq |xy|$ here.

Exercise. R4

Find all $z \in \mathbb{C}$ with $\bar{z} = z^2$.

Solution. The tool: take moduli first. If $\bar{z} = z^2$, then $|z| = |\bar{z}| = |z^2| = |z|^2$ (Theorem 1.2.2 (d)), so $|z|(|z| - 1) = 0$ and $|z| = 0$ or $|z| = 1$.

If $|z| = 0$, then $z = 0$ (Theorem 1.2.2 (e)), and $z = 0$ is a solution.

If $|z| = 1$, multiply $\bar{z} = z^2$ by z : $1 = z\bar{z} = z^3$ (Theorem 1.2.2 (c)). So z is a cube root of unity: $z = 1$ or $z = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ (the Check above). Conversely, each cube root of unity ζ lies in $\mathbb{T}$ (Exercise B3), so $\bar{\zeta} = \zeta^{-1}$ (Proposition 1.5.1 (a)), and $\zeta^{-1} = \zeta^2$ because $\zeta \cdot \zeta^2 = \zeta^3 = 1$. So each is a solution.

The solutions are $0, 1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

Why the look-alike tools are worse. Comparing real and imaginary parts, with $z = x + yi$, gives $x^2 - y^2 = x$ and $2xy = -y$, which can be solved, but only with a case split by hand ($y = 0$ or $x = -\frac{1}{2}$). “Divide $\bar{z} = z^2$ by z ” silently loses the solution $z = 0$. Polar form works, but it is not needed: the moduli settle $|z|$, and the cube roots of unity can be found without angles, as in the Check.