

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, Relations, and Cardinality, Definition 1.3.2, with **addition** and **multiplication** 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, Relations, and Cardinality, Definition 1.3.1),

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

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, Relations, and Cardinality, Definition 1.4.3), 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, Relations, and Cardinality, Definition 1.3.1; 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

$$(zw)u = ((ac - bd)e - (ad + bc)f) + ((ac - bd)f + (ad + bc)e)i$$

and

$$z(wu) = (a(ce - df) - b(cf + de)) + (a(cf + de) + b(ce - df))i.$$

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, Relations, and Cardinality, Definition 1.3.1, 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, $(a+bi)(a-bi) = a^2 - abi + abi - b^2i^2 = a^2 + b^2$ 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, Relations, and Cardinality, Theorem 2.3.1](#), read on $\mathbb{N} = \omega$ through [Number Systems: From \$\setminus\(\setminus\mathbb{N}\setminus\)\$ to \$\setminus\(\setminus\mathbb{N}\setminus\)\$](#) , [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, Relations, and Cardinality*, Section 2.3 ([Sets, Relations, and Cardinality, Definition 2.3.2](#)), stated there for real numbers, and the same recursion as [Number Systems: From \$\setminus\(\setminus\mathbb{N}\setminus\)\$ to \$\setminus\(\setminus\mathbb{N}\setminus\)\$](#) , [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 \$\setminus\(\setminus\mathbb{N}\setminus\)\$ to \$\setminus\(\setminus\mathbb{N}\setminus\)\$](#) , [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 \$\setminus\(\setminus\mathbb{N}\setminus\)\$ to \$\setminus\(\setminus\mathbb{N}\setminus\)\$](#) , [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 \$\setminus\(\setminus\mathbb{N}\setminus\)\$ to \$\setminus\(\setminus\mathbb{N}\setminus\)\$](#) , [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 $\setminus(\setminus \mathbb{N} \setminus)$ to $\setminus(\setminus \mathbb{R} \setminus)$, Lemma 4.1.1 (d)).

■

Parts (a)–(c) are the laws of *Sets, Relations, and Cardinality*, Section 2.3 (Sets, Relations, and Cardinality, 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 $\setminus(\setminus \mathbb{N} \setminus)$ to $\setminus(\setminus \mathbb{R} \setminus)$, 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, Relations, and Cardinality, 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 $a_0 + a_1 + \dots + a_n$ 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 $\setminus(\setminus \mathbb{R} \setminus)$, 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 $\setminus(\mathbb{N}\setminus)$ to $\setminus(\mathbb{NR}\setminus)$, 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 $\setminus(\mathbb{N}\setminus)$ to $\setminus(\mathbb{NR}\setminus)$, 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 $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, 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 \(First Computations in \$\mathbb{C}\$ \)](#)),

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

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. Chapter 2 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).