

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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 4.1.3 (d)). Hence $r + a \geq 0$ and $r - a \geq 0$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 2.3.5 (a), (b)). Halving keeps this: for $p \geq 0$, either $p > 0$ and then $p/2 > 0$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 4.1.2 (b), with $\varepsilon = p$), or $p = 0$ and then $p/2 = 0 \cdot (1/2) = 0$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 4.1.3 (a), (b)), with uniqueness in Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, Proposition 6.1.4; and the last because $s|b| = b$ by the definitions of s and of $|b|$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{R}\backslash)$, 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 $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, 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 $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, 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 $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, 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 C2), 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)).
- $a = -4, b = 0, r = |-4| = 4, s = 1$ (as $b \geq 0$), $x = \sqrt{(4 - 4)/2} = 0, y = \sqrt{(4 + 4)/2} = 2$. So $w = 2i$, and the square roots are $\pm 2i$.
- 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.
- 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 $\mathbb{N}$ to $\mathbb{R}$, 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 $\mathbb{N}$ to $\mathbb{R}$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.5 (e), and $0^2 = 0$. First, $-1 \neq 0$, since otherwise $1 = -(-1) = -0 = 0$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, 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 $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.5 (b)), $0 = 1 + (-1) > 0$, which (O1) forbids. This is the argument of Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Exercise (C1: A field that cannot be ordered), with the square root of -1 supplied by a formula.
- 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 .