

## 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  $\mathbb{N}$  to  $\mathbb{R}$ , Proposition 6.1.4), and an exercise there ran the same move for cube roots (Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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

$\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\geq 0$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , Theorem 5.6.3, Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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 $z^n = c$

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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\setminus(\setminus\mathbb{N}\setminus)$  to  $\setminus(\setminus\mathbb{N}\setminus)$ , 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  $\setminus(\setminus\mathbb{N}\setminus)$  to  $\setminus(\setminus\mathbb{N}\setminus)$ , 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

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

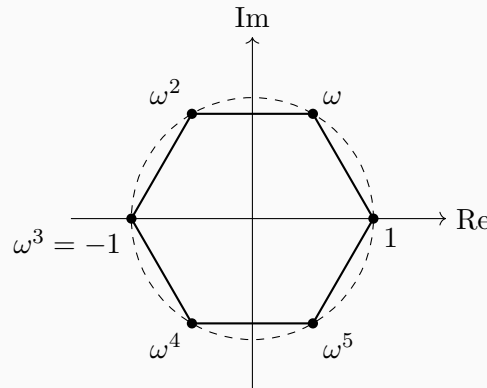
Put  $\omega := e^{2\pi i/n}$ . By [Theorem 1.5.5](#),  $z_k = (e^{2\pi i/n})^k = \omega^k$  for  $k \in \mathbb{N}$ . By [Theorem 1.6.2 \(c\)](#), there are exactly  $n$  solutions,

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

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  $\omega$  turns each one into the next ([Theorem 1.5.3 \(a\)](#)), and  $\omega^{n-1}$  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  $\mu_n$  (for  $n = 1$ ,  $\zeta^0 = 1$ ). *Algebraic Preliminaries*, Chapter 2 treats  $\mu_n$ , 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  $\zeta$  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  $1 + \zeta + \cdots + \zeta^{n-1}$ , 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  $\backslash(\backslash n \mathbb{N} \backslash)$  to  $\backslash(\backslash n \mathbb{R} \backslash)$ , 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  $\backslash(\backslash n \mathbb{N} \backslash)$  to  $\backslash(\backslash n \mathbb{R} \backslash)$ , 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  $\bar{z^k} = \bar{z}^k$ , 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  $\sum a_k \overline{z_0}^k = \overline{0} = 0$ . ■

A solution  $z_0$  that is not real gives a **second** solution:  $\overline{z_0} \neq z_0$ , since  $z_0 = x + yi$  with  $y \neq 0$  has  $\overline{z_0} = x - yi$ , 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

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

*Solution.*

- (a) By [Example \(Roots of Unity\)](#) with  $n = 4$ , the solutions are  $\omega^k$  for  $k = 0, 1, 2, 3$ , where  $\omega = e^{2\pi i/4} = e^{i\pi/2} = i$  ([Example \(Special Angles\) \(ii\)](#)):  $1, i, -1, -i$ .
- (b) 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  $\rho$ .
- (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),  $e^{-i\pi/2} = \overline{e^{i\pi/2}} = \overline{i} = -i$ , 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  $\mu_n$  is closed under multiplication, that for  $k = 1, \dots, n-1$  the inverse of  $\omega^k$  is  $\omega^{n-k}$ , 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  $\omega^{n-k}$  is the inverse of  $\omega^k$ , and it lies in  $\mu_n$ . 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  $z = re^{i\theta}$  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  $\omega$  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  $\omega$  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  $\setminus(\setminus n \setminus)$  to  $\setminus(\setminus n \mathbb{R} \setminus)$ , 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  $a \in \mathbb{R}$ .

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

*Solution.*

- (a) Since  $\sigma$  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  $z$ .

- (b) 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mu_n$  by Theorem 1.6.2 (a), and every element of  $\mu_n$  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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mu_n$ .

### 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , Proposition 4.1.3 (c)). So  $|x + y|^2 \leq (|x| + |y|)^2$ . If  $|x + y| > |x| + |y|$ , then Number Systems: From  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\mathbb{N}$  to  $\mathbb{R}$ , 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  $\zeta$  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.